PUBLIC (公開)
SAP BusinessObjects Business Intelligence プラットフォーム
ドキュメントバージョン: 4.3 Support Package 4 – 2023-12-07

Business Intelligence プラットフォーム管理者ガイド

© 2024 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

目次

1 ドキュメント履歴 . . . 21

2 はじめに . . . 22

2.1 このガイドについて . . . 22

このガイドの対象読者 . . . 22

Business Intelligence プラットフォームについて . . . 22

変数 . . . 23

用語 . . . 23

2.2 開始前の準備 . . . 25

基本概念 . . . 25

主な管理ツール . . . 28

主要タスク . . . 31

3 アーキテクチャ . . . 34

3.1 アーキテクチャの概要 . . . 34

コンポーネント図 . . . 35

アーキテクチャの各層 . . . 36

データベース . . . 37

サーバ、ホスト、およびクラスタ . . . 38

Web アプリケーションサーバ . . . 39

ソフトウェア開発キット . . . 44

データソース . . . 45

認証とシングルサインオン . . . 46

SAP 統合 . . . 48

統合バージョン管理 . . . 49

3.2 サーバ、サービス、ノード、およびホスト . . . 49

XI 3.1 からのサーバの変更点 . . . 51

サービス . . . 53

サービスカテゴリ . . . 59

サーバタイプ . . . 61

サーバ . . . 65

3.3 クライアントアプリケーション . . . 66

SAP BusinessObjects Business Intelligence プラットフォームクライアントツールとともにインストール . . . 67

SAP BusinessObjects Business Intelligence プラットフォームとともにインストール . . . 70

個別入手可能 . . . 70

Web アプリケーションクライアント . . . 71

3.4 プロセスのワークフロー. 74
起動と認証. 74
プログラムオブジェクト. 76
Crystal Reports. 77
Web Intelligence. 81
分析. 83
3.5 SAP Enterprise Portal での Fiori ランチパッドとの統合. 84

4 システム設定ウィザード. 86
4.1 システム設定ウィザードの概要. 86
4.2 使用する製品の指定. 86
4.3 デプロイメントテンプレートの選択. 88
4.4 データフォルダの場所の指定. 90
4.5 変更の確認. 91
4.6 ログファイルおよび応答ファイル. 91
応答ファイルの使用. 92

5 ライセンスの管理. 96
5.1 ライセンスキーの管理. 96
ライセンス情報を表示する. 96
ライセンスキーを追加する. 96
現在のアカウントの利用状況を表示する. 97

6 ユーザとグループの管理. 98
6.1 アカウント管理の概要. 98
ユーザ管理. 98
グループ管理. 99
利用可能な認証タイプ. 99
6.2 Enterprise および通常のアカウントの管理. 101
ユーザアカウントを作成する. 101
ユーザアカウントを変更する. 102
ユーザアカウントを削除する. 102
新規グループを作成する. 103
グループのプロパティを変更する. 103
グループメンバーを表示する. 104
サブグループを追加する. 104
グループメンバーシップを指定する. 105
グループを削除する. 105
ユーザまたはユーザグループを一括して追加する. 106
Guest アカウントを有効にする. 106
グループへのユーザの追加. 107
パスワード設定を変更する. 108

ユーザおよびグループへのアクセスの許可. 110
ユーザの受信ボックスへのアクセスの制御. 110
Fiorified BI ラウンチパッドのオプションの設定. 111
システムユーザの属性の管理 114
複数の認証オプションに対するユーザ属性の優先順位付け. 115
新しいユーザ属性を追加する. 115
カスタマイズされたユーザ属性を編集する. 117
6.3 エイリアスの管理. 117
ユーザを作成しサードパーティエイリアスを追加する. 117
既存のユーザの新しいエイリアスを作成する. 118
別のユーザのエイリアスを割り当てる. 119
エイリアスを削除する. 119
エイリアスを無効化する. 120

7 アクセス権の設定. 121
7.1 BI プラットフォームでのアクセス権の動作. 121
アクセスレベル. 121
詳細アクセス権の設定. 122
継承. 123
種類固有アクセス権. 127
実効アクセス権の決定. 129
7.2 CMC でのオブジェクトのセキュリティ設定の管理. 129
オブジェクトの主体のセキュリティを表示する. 130
オブジェクトのアクセスコントロールリストに主体を割り当てる. 130
オブジェクトの主体のセキュリティを変更する. 131
BI プラットフォームの最上位フォルダにアクセス権を設定する. 132
主体のセキュリティ設定の確認. 132
7.3 アクセスレベルの使用. 134
表示およびオンデマンド表示アクセスレベルの選択. 136
既存のアクセスレベルをコピーする. 137
新しいアクセスレベルを作成する. 138
アクセスレベルの名前を変更する. 138
アクセスレベルを削除する. 138
アクセスレベルの権限を変更する. 138
アクセスレベルとオブジェクト間の関係のトレース. 139
サイト間でのアクセスレベルの管理. 140
7.4 継承の破棄. 141
継承を無効にする. 142
7.5 アクセス権の使用による管理の委任. 143
“オブジェクトに対するユーザの権限を変更する”オプションの選択. 144
オーナー権限. 145
7.6 アクセス権管理の推奨事項のまとめ. 146

8 BI プラットフォームのセキュリティ確保 . . . 147
8.1 セキュリティの概要 . . . 147
8.2 プログラムオブジェクトの安全な使用 . . . 147
8.3 障害復旧計画 . . . 148
8.4 デプロイメントのセキュリティを確保するための一般的な推奨事項 . . . 149
8.5 同梱されたサードパーティサーバのセキュリティ設定 . . . 150
8.6 アクティブな信頼関係 . . . 150
ログオントークン . . . 150
分散セキュリティのチケットメカニズム . . . 151
8.7 セッションとセッショントラッキング . . . 151
CMS セッショントラッキング . . . 152
セッションの管理 . . . 152
要再起動セッションをクリアするスクリプト . . . 154
8.8 環境の保護 . . . 154
Web ブラウザから Web サーバへ . . . 154
BI プラットフォームを対象とする Web サーバ . . . 155
悪意あるログオンに対する保護 . . . 155
パスワード制限 . . . 155
ログオンの制限 . . . 155
ユーザ制限 . . . 156
guest アカウントの制限 . . . 156
8.9 監査セキュリティ設定の変更 . . . 156
8.10 処理拡張機能 . . . 157
8.11 ウィルススキャンインタフェース . . . 157
ウィルススキャンの有効化 . . . 158
8.12 BI プラットフォームのデータセキュリティ . . . 158
データ処理セキュリティモード . . . 159
Administrator アカウント . . . 161
接続のアクセス権 . . . 161
8.13 BI プラットフォームの暗号化 . . . 162
クラスタキーの操作 . . . 162
暗号管理者 . . . 164
CMC での暗号化キーの管理 . . . 166
8.14 データの保護とプライバシー . . . 170
用語集 . . . 170
ユーザの承諾 . . . 172
情報レポート . . . 172
読込アクセスロギング . . . 172
個人データの削除 . . . 173
変更ログ . . . 174
8.15 バックエンドサーバの SSL 設定 . . . 174

デフォルト設定ファイルを作成する. 175
キーファイルと証明書ファイルの作成. 176
証明書が認証機関によって管理されている場合の SSL の設定. 178
SSL プロトコルの設定. 180
8.16 BI プラットフォームコンポーネント間の通信について. 184
BI プラットフォームサーバと通信ポートの概要. 184
BI プラットフォームコンポーネント間の通信 186
8.17 ファイアウォール用の BI プラットフォームの設定. 197
ファイアウォール用にシステムを設定する. 197
ファイアウォールを使用したデプロイメントのデバッグ. 200
8.18 一般的なファイアウォールシナリオの例. 201
例: 別のネットワークにデプロイされたアプリケーション層. 202
例: ファイアウォールによって BI プラットフォームサーバから隔てられたシッククライアントとデータベース層. 204
8.19 統合環境でのファイアウォールの設定. 206
SAP 統合に固有のファイアウォールガイドライン. 206
JD Edwards EnterpriseOne 統合向けのファイアウォール設定. 208
Oracle EBS に固有のファイアウォールガイドライン. 209
PeopleSoft Enterprise 統合向けのファイアウォール設定. 210
Siebel 統合向けのファイアウォール設定. 211
8.20 BI プラットフォームおよびリバースプロキシサーバ 213
Web アプリケーションのデプロイ方法について. 213
8.21 BI プラットフォーム Web アプリケーションに対するリバースプロキシサーバの設定. 214
リバースプロキシサーバの設定の詳細な手順. 214
リバースプロキシサーバを設定する. 215
BI プラットフォーム用に Apache 2.2 リバースプロキシサーバを設定する 215
BI プラットフォーム用に WebSEAL 6.0 リバースプロキシサーバを設定する 216
BI プラットフォーム用に Microsoft ISA 2006 を設定する 216
8.22 リバースプロキシデプロイメントでの BI プラットフォームに固有の設定. 218
Web サービスのリバースプロキシの有効化. 218
ISA 2006 に対するセッション cookie のルートパスの有効化. 220
SAP BusinessObjects Live Office に対するリバースプロキシの有効化. 223

9 認証. 224
9.1 BI プラットフォームの認証オプション. 224
一次認証. 224
セキュリティプラグイン. 225
BI プラットフォームへのシングルサインオン. 226
9.2 Enterprise 認証. 229
Enterprise 認証の概要. 229
Enterprise 認証の設定. 229
Enterprise 設定を変更する. 230

SAML 2.0 認証. 232
SAP NetWeaver Java Application Server と BI プラットフォーム間に信用できる認証を確立する 244
SAP NetWeaver Java アプリケーションサーバとともに SAML 2.0 認証を使用する. 248
信用できる認証の有効化. 248
Web アプリケーションに対する信用できる認証の設定. 251
9.3 LDAP 認証. 260
LDAP 認証の使用. 260
LDAP 認証の設定. 261
LDAP グループのマッピング. 272
9.4 Windows AD 認証. 282
Windows AD 認証の使用. 282
ドメインコントローラの準備. 283
CMC での AD 認証の設定. 284
SIA 実行のための BI プラットフォームサービスの設定. 292
AD 認証用の Web アプリケーションサーバの設定. 294
シングルサインオンの設定. 303
Windows AD 認証のトラブルシューティング. 319
9.5 SAP 認証. 321
SAP 認証の設定 321
BI プラットフォームのユーザアカウントの作成. 322
SAP 権限認証システムへの接続. 323
SAP 認証オプションの設定. 325
SAP ロールのインポート. 329
セキュアネットワークコミュニケーション (SNC) の設定. 332
SAP システムへのシングルサインオンの設定. 345
SAP Crystal Reports および SAP NetWeaver の SSO の設定. 349
9.6 PeopleSoft 認証. 350
概要. 350
PeopleSoft Enterprise 認証の有効化. 351
BI プラットフォームへの PeopleSoft ロールのマップ. 351
ユーザの更新のスケジュール. 354
PeopleSoft セキュリティブリッジの使用. 356
9.7 JD Edwards 認証. 365
概要. 365
JD Edwards EnterpriseOne 認証の有効化. 365
BI プラットフォームへの JD Edwards EnterpriseOne ロールのマップ. 366
ユーザの更新のスケジュール. 369
9.8 Siebel 認証. 370
Siebel 認証の有効化. 370
BI プラットフォームへのマッピング. 371

ユーザの更新のスケジュール. 374
9.9 Oracle EBS 認証. 375
Oracle EBS 認証の有効化. 375
BI プラットフォームへの Oracle E-Business Suite ロールのマップ. 376
ロールのマップ解除 380
マップされた Oracle EBS のグループ権限とユーザ権限のカスタマイズ 380
SAP Crystal Reports および Oracle EBS のシングルサインオン (SSO) の設定. 382
9.10 X.509 認証. 383
BI ラウンチパッドの X.509 認証. 383
Web サービスの X.509 認証. 390
CMC の X.509 認証. 393
9.11 OpenID 接続認証. 396
OpenID 接続認証の有効化. 396

10 データソース参照. 398
10.1 拡張認証情報マッピング. 398
データソース参照の作成. 399
CMC におけるユーザのデータソース参照に対するデータベース認証情報の定義. 400
BI ラウンチパッドにおけるユーザのデータソース参照に対するデータベース認証情報の定義 400
グループのデータソース参照に対するデータベース認証情報の定義. 401
OLAP 接続へのデータソース参照の関連付け. 401

11 サーバの管理. 402
11.1 CMC の[サーバ]管理エリアの使用. 402
11.2 Windows でのスクリプトを使用したサーバ管理 405
11.3 Unix でのサーバ管理 405
11.4 サーバのステータスの表示および変更. 405
サーバのステータスの表示. 405
サーバの開始、停止、再起動. 407
Central Management Server の停止. 409
サーバの有効化/無効化. 410
11.5 サーバの追加、クローン、または削除. 411
サーバの追加、クローン、および削除. 411
11.6 カスタムインターネットヘッダの追加. 413
11.7 Central Management Server のクラスタ化. 414
Central Management Server のクラスタ化. 414
11.8 サーバグループの管理. 418
サーバグループの作成. 419
排他的サーバグループを非排他的サーバグループに変換するおよびその逆も可能です。. 421
サーバサブグループの使用. 423
サーバのグループメンバーシップの変更. 424

サーバおよびサーバグループへのユーザの管理アクセス. 425
サーバグループへのユーザグループのマップ. 426
サーバグループへのフォルダのマップ. 429
サーバグループのアクセス権の管理の理解. 431
11.9 本稼働システムの Adaptive Processing Server の設定. 436
11.10 システムのパフォーマンスの評価. 437
BI プラットフォームの監視. 437
サーバメトリクスの分析. 437
システムメトリクスの表示. 438
サーバの利用状況の記録. 438
11.11 サーバの設定. 439
サーバのプロパティを変更する. 439
複数のサーバにｻｰ ビス設定を適用する. 440
設定テンプレートの使用. 440
11.12 サーバネットワークの設定. 443
ネットワーク環境オプション. 443
サーバホスト ID オプション. 444
マルチホームマシンの設定. 446
ポート番号の設定. 448
11.13 ノードの管理. 451
ノードの使用. 451
新しいノードの追加. 453
ノードの再作成. 457
ノードの削除. 461
ノードの名前の変更. 464
ノードの移動. 465
スクリプトパラメータ. 469
Windows サーバ依存関係の追加. 474
ノードに対するユーザ認証情報の変更. 474
11.14 BI プラットフォームデプロイメントでのマシン名の変更. 475
クラスタ名の変更. 475
IP アドレスの変更. 475
マシンの名前変更. 477
11.15 32 ビットおよび 64 ビットのサードパーティ製ライブラリの BI プラットフォームでの使用. 480
11.16 サーバおよびノードのプレースホルダの管理. 481
サーバプレースホルダを表示する. 481
ノードのプレースホルダを表示および編集する. 481

12 Central Management Server (CMS) データベースの管理. 482
12.1 CMS システムデータベース接続の管理. 482
SQL Anywhere を CMS データベースとして選択する. 482
SAP HANA を CMS データベースとして選択する. 483

12.2 新規または既存の CMS データベースの選択. 484
Windows で新しいまたは既存の CMS データベースを選択する. 485
UNIX で新しいまたは既存の CMS データベースを選択する. 486
12.3 CMS システムデータベースの再作成. 486
Windows で CMS システムデータベースを作成し直す. 487
UNIX 上で CMS システムデータベースを再作成する. 488
12.4 CMS データベース間でのデータのコピー. 488
CMS システムデータベースのコピーの準備. 489
Windows で CMS システムデータベースをコピーする. 490
UNIX 上の CMS システムデータベースからデータをコピーする. 490
12.5 Central Management Server データベースドライバ. 491

13 Web アプリケーションコンテナサーバ (WACS) の管理. 492
13.1 WACS. 492
Web アプリケーションコンテナサーバ (WACS). 492
デプロイメントへの WACS の追加または削除. 494
WACS に対するサービスの追加または削除. 498
HTTPS/SSL の設定. 499
サポートされる認証方法. 502
WACS への AD Kerberos の設定 503
AD Kerberos シングルサインオンの設定 510
RESTful Web サービスの設定. 512
WACS と IT 環境. 522
Web アプリケーションプロパティの設定. 524
トラブルシューティング. 525
WACS プロパティ. 529

14 システムのバックアップと復元. 530
14.1 バックアップと復元の概要. 530
14.2 用語. 530
14.3 バックアップおよび復元の使用事例. 532
14.4 バックアップ. 533
システム全体のバックアップ. 534
サーバの設定のバックアップ. 537
BI コンテンツのバックアップ. 539
14.5 システムの復元. 540
システム全体の復元. 540
サーバ設定の復元[サーバセッテイノフクゲン]. 547
BI コンテンツの復元. 550
14.6 BackupCluster スクリプトおよび RestoreCluster スクリプト. 550

15 BI プラットフォームデプロイメントのコピー. 553

15.1 システムコピーの概要. 553
15.2 用語. 553
15.3 システムコピーの使用事例. 553
15.4 システムのコピーの計画. 554
15.5 考慮点および制限. 555
15.6 システムコピー手順. 557
ソースシステムからエクスポートする. 557
ターゲットシステムにインポートする. 561

16 プロモーション管理. 564
16.1 プロモーションマネジメントへようこそ. 564
概要. 564
機能. 564
アプリケーションアクセス権. 565
プロモーションマネジメントでの WinAD のサポート. 566
16.2 プロモーションマネジメントツールを使用する前に. 566
プロモーションマネジメントツールへのアクセス. 566
ユーザインタフェースコンポーネント. 567
設定オプションの使用. 568
16.3 プロモーションマネジメントツールの使用. 576
フォルダを作成、削除する. 577
ジョブを作成する. 578
既存ジョブをコピーして新規ジョブを作成する. 580
ジョブを検索する. 581
ジョブを編集する. 581
ジョブに InfoObject を追加する. 582
ジョブの依存関係を管理する. 583
依存関係を検索する. 584
リポジトリに接続しているときのジョブを昇格する. 585
LCMBIAR ファイルを使用したジョブの昇格. 587
ジョブの昇格をスケジュールする. 591
ジョブ履歴を表示する. 592
ジョブをロールバックする. 593
16.4 プロモーションマネジメントツールを使用するリポジトリのフルコンテンツの昇格. 595
ソースシステムおよびターゲットシステムを準備する. 596
移行ストラテジー. 597
16.5 システム全体の昇格ステップ. 598
ユーザおよびユーザグループを昇格する (ジョブ 1). 599
依存オブジェクトを昇格する (ジョブ 2). 599
1 次オブジェクトを昇格する (ジョブ 3). 601
昇格後の作業. 602
16.6 コマンドラインオプションの使用. 602

Windows でコマンドラインツールを実行する. 602
Unix でコマンドラインツールを実行する. 603
コマンドラインツールパラメータ. 603
サンプルプロパティファイル. 626
16.7 拡張移送/修正システムの使用. 627
前提条件. 627
BI プラットフォームと CTS+ との統合を設定する. 628
CTS を使用してジョブを昇格する. 634
16.8 プロモーション管理ウィザードの使用 637
昇格からオブジェクトを除外する. 638
プロモーション管理ウィザードを使用する場合. 639
シナリオ. 640
オブジェクト. 642
依存関係. 646
概要. 646
(オプション) プロパティファイル. 647
Linux のプロモーション管理ウィザード. 650

17 バージョン管理. 651
17.1 InfoObject のさまざまなバージョンを管理する. 651
バージョン管理アプリケーションのアクセス権限. 651
Subversion ファイルのバックアップと復元. 652
17.2 異なるバージョンの BI リソースを管理する. 653
17.3 Unix での Subversion の手動による開始および停止. 655
17.4 Solaris 10 および RedHat Linux 5 の Subversion に必要なファイル. 655
17.5 バージョン管理システムとして Apache Subversion を使用する. 655
17.6 バージョン管理システムとして Git を使用する. 656
17.7 デフォルトバージョン管理システムの設定. 657
17.8 同じジョブの異なるバージョンを比較する. 658
17.9 Subversion コンテンツをアップグレードする. 658
17.10 クラスタ化された Processing Job Server の Subversion の設定. 659
選択肢 A: すべてのバージョン管理システム操作の前にメインの Subversion マシンを設定する 659
選択肢 B: バージョン管理システムで作業コピーディレクトリを作成した後に Subversion を設定する 660
他の Subversion マシンの設定. 660

18 アプリケーションの管理. 662
18.1 GDPR ポップアップメッセージの無効化. 662
18.2 CMC を介したアプリケーションの管理. 664
概要. 664
アプリケーションの共通設定. 665

アプリケーション固有の設定. 666
18.3 セマンティックレイヤプロパティを使用したアプリケーションの管理. 723
18.4 BOE.war プロパティを介したアプリケーションの管理. 724
BOE war ファイル. 724
18.5 BI 起動パッドおよび OpenDocument ログオンエントリポイントのカスタマイズ. 741
BI 起動パッドおよび OpenDocument ファイルの場所. 741
カスタムログオンページを定義する. 742
信用できる認証をログオンに追加する. 743
18.6 アプリケーションユーザインタフェースのカスタマイズ. 744
Web Intelligence. 744
BI ラウンチパッド. 750
18.7 Web サーバでの BI プラットフォーム RESTful Web サービスの設定. 750
18.8 ハイブリッドユーザ管理. 753
18.9 オンプレミスユーザの SAP Analytics Cloud へのプロビジョニング. 754
オンプレミスシステムとクラウド間の接続の確立. 754
18.10 SAP Analytics Cloud での OAuth クライアント認証情報の作成. 756
18.11 ソースシステムの設定. 756
18.12 ターゲットシステムの設定. 758
18.13 SAP Analytics Cloud へのユーザおよびユーザグループのプロビジョニング. 758
18.14 SAP Analytics Cloud でのプロビジョニングされたユーザの表示. 759
18.15 サンプルテンプレート. 759

19 接続とユニバースの管理. 763
19.1 接続の管理. 763
ユニバース接続を削除する. 763
19.2 ユニバースの管理. 764
ユニバースを削除する. 764

20 BI 管理スタジオ. 766
20.1 管理コックピット. 767
管理コックピット. 767
BI のサーバ. 768
ドキュメントインスタンスに関する BI. 769
BI のユーザとセッション. 770
BI におけるコンテンツの使用. 770
BI のアプリケーション. 771
20.2 モニタリング. 771
モニタリング用語. 772
モニタリング用のデータベースサポートの設定. 776
設定プロパティ. 784
その他アプリケーションとの統合. 790
モニタリングサーバのクラスタサポート. 790

トラブルシューティング. 791
20.3 Visual Difference. 794
Visual Difference を使用してオブジェクトまたはファイルを比較する. 795
バージョン管理システムを使用してオブジェクトまたはファイルを比較する. 796
20.4 HTML 要素の許可. 797
権限のある HTML 要素の一覧を変更する. 799

21 CMS レポーティング. 800
21.1 CMS レポーティング. 800
SAP BusinessObjects プラットフォームのアーキテクチャ. 800
CMS システムデータベースの構造. 801
InfoObject について. 803
21.2 CMS レポーティングの概要. 805
21.3 CMS データベース接続. 806
21.4 CMS レポーティングサンプルキット. 807
プロモーションマネジメントを使用した CMS レポーティングサンプルキットのインポート 808
CMS サンプルユニバース 808
CMS サンプルユニバースの拡張. 809
21.5 CMS レポートの作成. 809

22 ワークフローアシスタント. 811
22.1 対象読者. 812
22.2 アーキテクチャの理解. 813
22.3 用語集. 814
22.4 インストールおよび更新について. 816
22.5 ワークフローアシスタントの設定. 816
基本設定. 817
22.6 セントラル管理コンソールでのワークフローアシスタントの権限の管理. 819
22.7 ワークフローアシスタントの使用. 824
標準タスクテンプレートについて. 824
標準ワークフローテンプレートについて. 833
カスタムタスクテンプレートについて. 834
ワークフローテンプレートの管理. 834
シナリオの管理および結果の表示. 836
タスクテンプレート、ワークフローテンプレート、およびシナリオのステータスの理解. 841
システムの使用. 843
ワークフローアシスタントのエンドツーエンドのプロセスフロー. 845
22.8 ログファイルのチェック. 846

23 リサイクルビン. 847
23.1 ごみ箱. 847
アイテムをごみ箱から復元する. 847

アイテムをごみ箱から完全に削除する. 848
ごみ箱の自動クリーンアップを有効にする. 848

24 監査. 849
24.1 概要. 849
24.2 CMC 監査ページ. 855
監査ステータス. 855
監査イベントの設定. 857
監査データストア設定. 861
24.3 監査イベント. 862
Audit events and details. 871

25 イベント. 893
25.1 イベントについて. 893
ユーザ通知. 894

26 プラットフォーム検索. 898
26.1 プラットフォーム検索について. 898
プラットフォーム検索 SDK. 898
クラスタ環境. 898
26.2 プラットフォーム検索の設定. 899
OpenSearch のデプロイ. 899
リバースプロキシの設定. 901
CMC でのアプリケーションプロパティの設定. 901
26.3 プラットフォーム検索の使用. 909
CMS リポジトリコンテンツのインデックス処理. 909
インデックス処理失敗一覧. 910
検索結果. 911
26.4 プラットフォーム検索と SAP NetWeaver Enterprise Search の統合. 917
SAP NetWeaver Enterprise Search でのコネクタの作成. 917
BI プラットフォームへのユーザのロールのインポート. 918
26.5 SAP NetWeaver Enterprise Search からの検索. 918
26.6 監査. 919
26.7 トラブルシューティング. 920
セルフヒーリング. 920
問題のシナリオ. 920

27 フェデレーション. 923
27.1 フェデレーション. 923
27.2 フェデレーションの用語. 924
27.3 セキュリティアクセス権の管理. 925
レプリケート元サイトで必要な権限. 926
レプリケート先サイトで必要な権限. 927

フェデレーション固有の権限. 927
オブジェクトに対するセキュリティの複製. 929
アクセスレベルを使用したセキュリティの複製. 929
27.4 レプリケーションの種類とモードのオプション. 930
一方向レプリケーション 930
双方向レプリケーション 930
[レプリケート元から最新表示]または[レプリケート先から最新表示]. 931
27.5 サードパーティユーザとグループの複製. 932
27.6 ユニバースおよびユニバース接続の複製. 933
27.7 レプリケーション一覧の管理. 934
レプリケーション一覧の作成. 935
レプリケーション一覧の変更. 937
27.8 リモート接続の管理. 938
リモート接続の作成. 938
リモート接続の変更. 940
27.9 レプリケーションジョブの管理. 941
レプリケーションジョブの作成. 941
レプリケーションジョブのスケジュール. 943
レプリケーションジョブの変更. 943
レプリケーションジョブ後のログの表示. 944
27.10 オブジェクトのクリーンアップの管理. 945
オブジェクトのクリーンアップ方法. 945
オブジェクトのクリーンアップの制限. 946
オブジェクトのクリーンアップ間隔. 946
27.11 競合の検出と解決の管理. 947
一方向レプリケーションの競合の解決. 947
双方向レプリケーションの競合の解決. 949
27.12 フェデレーションでの Web サービスの使用. 952
セッション変数 953
ファイルのキャッシュ 953
カスタムデプロイメント 954
27.13 リモートスケジュールおよびローカルで実行したインスタンス. 955
リモートスケジュール. 955
ローカルで実行したインスタンス. 956
インスタンス共有. 957
27.14 複製したコンテンツのインポートと昇格. 958
複製したコンテンツのインポート. 958
複製したコンテンツのインポートとレプリケーションの継続 959
テスト環境からのコンテンツの昇格. 959
レプリケート先サイトの再指定. 960
27.15 ベストプラクティス. 960

現在のリリースの制限. 964
エラーメッセージのトラブルシューティング. 965

28 ERP 環境の追加設定. 969
28.1 SAP NetWeaver 統合の設定. 969
SAP Business Warehouse (BW) との統合. 969
28.2 JD Edwards 統合の設定. 1013
SAP Crystal Reports のシングルサインオンの設定. 1013
JD Edwards Integrations のセキュアソケットレイヤの設定. 1014
28.3 PeopleSoft Enterprise 統合の設定. 1015
SAP Crystal Reports および PeopleSoft Enterprise のシングルサインオン (SSO) の設定. 1015
Secure Sockets Layer (SSL) 通信の設定. 1016
PeopleSoft システムのパフォーマンスチューニング. 1018
28.4 Siebel 統合の設定. 1019
SAP BI プラットフォームと統合するための Siebel の設定. 1019
Crystal Reports のメニュー項目の作成. 1020
コンテキスト認識. 1021
SAP Crystal Reports および Siebel のシングルサインオン (SSO) の設定. 1023
Secure Sockets Layer (SSL) 通信の設定. 1024

29 管理および設定ログ. 1026
29.1 コンポーネントのトレースのログ. 1026
29.2 トレースログレベル. 1026
29.3 サーバのトレースの設定. 1027
CMC にログレベルを設定する. 1027
CMC の複数のサーバにログレベルを設定する. 1028
BO_trace.ini ファイルを使ってサーバトレースを設定する. 1029
29.4 Web アプリケーションのトレース設定. 1031
CMC の Web アプリケーショントレースログレベルを設定する. 1031
`BO_trace.ini` ファイルを使ってトレース設定を設定する. 1032
29.5 BI プラットフォームクライアントアプリケーションのトレース設定. 1036
29.6 拡張エラーメッセージトレーシングの設定. 1037
29.7 エラーメッセージ詳細情報ログファイルを有効にする. 1037

30 SAP Solution Manager への統合. 1039
30.1 統合の概要. 1039
30.2 SAP Solution Manager の統合のチェックリスト. 1039
30.3 システムランドスケープディレクトリ登録の管理. 1040
システムランドスケープでの BI プラットフォームの登録. 1040
SLD 登録がトリガーされるタイミング. 1042
パッチインストール前の SLD クリーンアップ. 1042
SLD 接続のログ作成. 1043

仮想ホスト名. 1043
30.4 ソリューション管理診断エージェントの管理. 1044
Solution Manager Diagnostics (SMD) の概要. 1044
SMD エージェントの操作. 1044
SMAdmin ユーザアカウント. 1045
30.5 パフォーマンス計測の管理. 1045
BI プラットフォームのパフォーマンス計測. 1045
BI プラットフォームのパフォーマンス計測の設定. 1046
Web Tier のパフォーマンス計測. 1047
計測ログファイル. 1047
30.6 SAP パスポートを使用したトレース. 1047

31 コマンドライン管理. 1049
31.1 Unix スクリプト. 1049
スクリプトユーティリティ. 1049
スクリプトテンプレート. 1054
BI プラットフォームによって使用されるスクリプト. 1055
31.2 Windows スクリプト. 1056
ccm.exe. 1056
31.3 サーバコマンドライン. 1059
コマンドラインの概要. 1059
すべてのサーバに使用できる標準オプション. 1060
Central Management Server. 1060
Crystal Reports Processing Server と Crystal Reports Cache Server. 1062
Job Server. 1063
Adaptive Processing Server. 1064
Report Application Server. 1064
Web Intelligence Processing Server. 1065
Input/Output File Repository Server. 1067
Event Server. 1069

32 リポジトリ診断ツール. 1070
32.1 リポジトリ診断ツールの概要. 1070
32.2 リポジトリ診断ツールの使用. 1070
リポジトリ診断ツールを使用する. 1071
リポジトリ診断ツールのパラメータ. 1072
32.3 CMS と FRS 間の不整合. 1079
32.4 CMS メタデータの不整合. 1080
32.5 BOE WebApp 内の Restful SDK の管理. 1083

33 HTTP Strict Transport Security (HSTS). 1085
33.1 HTTP Strict Transport Security (HSTS) の設定. 1085

34 アクセス権に関する付録 . . . 1086
34.1 付録 - 権限について . . . 1086
34.2 全般の権限 . . . 1086
出力先権限 . . . 1090
34.3 特定のオブジェクトの種類のアクセス権 . . . 1091
フォルダのアクセス権 . . . 1091
カテゴリ . . . 1091
Crystal レポート . . . 1091
Web Intelligence ドキュメント . . . 1092
ユーザとグループ . . . 1093
アクセスレベル . . . 1094
ユニバース (.unv) のアクセス権 . . . 1095
ユニバース (.unx) のアクセス権 . . . 1096
ユニバースオブジェクトのアクセスレベル . . . 1098
接続のアクセス権 . . . 1099
アプリケーション . . . 1100

35 サーバのプロパティに関する付録 . . . 1108
35.1 サーバのプロパティに関する付録について . . . 1108
共通サーバのプロパティ . . . 1108
コアサービスのプロパティ . . . 1110
接続サービスのプロパティ . . . 1121
Crystal Reports サービスのプロパティ . . . 1125
Analysis サービスのプロパティ . . . 1133
データフェデレーションサービスのプロパティ . . . 1134
Web Intelligence サービスのプロパティ . . . 1134

36 サーバのメトリクスに関する付録 . . . 1142
36.1 サーバのメトリクスに関する付録について . . . 1142
一般的なサーバのメトリクス . . . 1142
Central Management Server のメトリクス . . . 1144
Connection Server のメトリクス . . . 1147
Event Server のメトリクス . . . 1147
File Repository Server のメトリクス . . . 1148
Adaptive Processing Server のメトリクス . . . 1148
Web アプリケーションコンテナサーバのメトリクス . . . 1152
Adaptive Job Server のメトリクス . . . 1153
Crystal Reports Server のメトリクス . . . 1154
Web Intelligence サーバのメトリクス . . . 1156

37 サーバおよびノードのプレースホルダに関する付録 . . . 1158
37.1 サーバとノードプレースホルダ . . . 1158

38 監査データストアスキーマに関する付録 1167
38.1 概要 1167
38.2 スキーマ図 1167
38.3 Auditing Data Store Tables 1167

39 モニタリングデータベーススキーマに関する付録 1175
39.1 トレンドデータベーススキーマ 1175

40 システムコピーワークシートに関する付録 1178
40.1 システムコピーワークシート 1178

1 ドキュメント履歴

下の表は、最も重要なドキュメント変更の概要です。

バージョン	日付	説明
SAP BusinessObjects Business Intelligence プラットフォーム 4.3 SP3	2022 年 12 月	以下のトピックが Enterprise 認証の新しいパスワードの最大文字数フィールドで更新されました。 • Enterprise 認証の設定 [229 ページ] • ユーザアカウントを作成する [101 ページ] • 一般的なパスワード設定を変更する [109 ページ] • 一般的なパスワード設定を変更する [231 ページ] • ブラウザの相対 URL を使用する [相対 URL パスを使用] を有効にするオプションが導入されました。
SAP BusinessObjects Business Intelligence プラットフォーム 4.3 SP2	2021 年 12 月	認可サーバの設定 [719 ページ]が追加されました。 ユーザグループおよびフォルダによる Web Intelligence インタフェース要素のカスタマイズ [744 ページ]が更新されました。

SAP BusinessObjects Business Intelligence プラットフォーム 4.3 SP1	2020 年 12 月	• 次の新しいトピックが追加されました。
		  • Web Intelligence UI のカスタマイズに関するトピック。ユーザグループおよびフォルダによる Web Intelligence インタフェース要素のカスタマイズ [744 ページ]を参照してください。
		  • 要再起動セッションをクリアするスクリプト [154 ページ]
		  • BI ラウンチパッドにおけるユーザのデータソース参照に対するデータベース認証情報の定義 [400 ページ]
		  • JMX SSL 設定 [787 ページ]
		• 次の 2 つのトピックが更新されました。
		  • アップグレードパス [30 ページ]
		  • 出力先オプションおよび電子メールの出力先のプロパティの出力先権限 [1090 ページ]が、すべてのパブリケーションシナリオで新たに導入された [返信先] フィールドにより更新されました。

SAP BusinessObjects Business Intelligence プラットフォーム 4.3	2020 年 6 月	• SAP BusinessObjects Explorer、SAP BusinessObjects Dashboards、レポート変換ツール、アップグレードマネジメントツール、および BI ウィジェットは、4.3 リリースで使用できなくなりました。 • 新しいトピック ワークフローアシスタント [811 ページ] が追加されました。

2 はじめに

2.1 このガイドについて

このガイドでは SAP BusinessObjects Business Intelligence プラットフォーム (“BI プラットフォーム”) のデプロイおよび設定に関する情報および手順について説明しています。手順は、一般的なタスクを対象に説明します。概念情報と技術に関する詳細情報は、すべての詳細トピックで提供します。

この製品のインストールの詳細については、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドを参照してください。

2.1.1 このガイドの対象読者

このガイドでは BI プラットフォームのデプロイメントおよび設定について説明しています。次の作業のいずれかを行うユーザは、このガイドを参照することをお勧めします。

- 初めてのデプロイメントの計画
- 初めてのデプロイメントの設定
- 既存のデプロイメントのアーキテクチャに対する大幅な変更
- システムのパフォーマンスの改善

このガイドは、インストールした BI プラットフォームの設定、管理、およびメンテナンスを担当するシステム管理者を対象としています。Web アプリケーションサーバ管理やスクリプトテクノロジーについての一般的理解と同様に、オペレーティングシステムやネットワーク環境に関する知識があると役に立ちます。ただし、このガイドでは、あらゆるレベルの管理経験者に合わせて、すべての管理タスクおよび機能を明確にするための十分な背景情報や製品概念を提供しています。

2.1.2 Business Intelligence プラットフォームについて

Business Intelligence (BI) プラットフォームは、柔軟でスケーラブルな情報配布ソリューションです。イントラネットやエクストラネット、インターネット、企業ポータルなどのあらゆる Web アプリケーションを介して、ダッシュボードや対話型レポートなど複数の書式によるエンドユーザへの情報の配布を実現します。

このプラットフォームは、レポーティング、データ分析、および情報配信のための統合スイートとして、組織内だけでなくその範囲を超えて利益をもたらします。

また、エンドユーザの生産性を向上し、管理の労力を減少させるソリューションを提供します。

BI プラットフォームは、たとえば、週次販売レポートの配布、顧客用に特化したサービスの提供、企業ポータルの重要情報の統合などの目的で使用されます。

2.1.3 変数

以下の変数は、このマニュアル全体を通して使用しています。

変数	説明
`<INSTALLDIR >`	BI プラットフォームのインストールディレクトリ。 Windows の場合、デフォルトのディレクトリは `C:¥Program Files (x86)¥SAP BusinessObjects¥` です。
`<PLATFORM64DIR>`	Unix オペレーティングシステムの名前。次の値を指定できます。 • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64
`<SCRIPTDIR>`	BI プラットフォームを管理するためのスクリプトが保存されているディレクトリ。 Windows では、ディレクトリは `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥scripts` です。 Unix では、ディレクトリは `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64DIR>/scripts` です。

2.1.4 用語

BI プラットフォームのドキュメントでは、次の用語が使用されます。

用語	定義
アドオン製品	BI プラットフォームで動作する一方、独自のインストールプログラムがある製品です。
監査データストア (ADS)	監査データを保存するために使用されるデータベースです。
BI プラットフォーム	SAP BusinessObjects Business Intelligence プラットフォームの略語です。
バンドルされたデータベース、バンドルされた Web アプリケーションサーバ	BI プラットフォームに同梱されているデータベースまたは Web アプリケーションサーバのことです。
クラスタ (名詞)	1 つの CMS データベースを使用し、同時に動作する 2 つ以上の Central Management Server (CMS) です。

用語	定義
クラスタ化する (動詞)	クラスタを作成することです。 1. マシン A に CMS および CMS データベースをインストールします。 2. マシン B に CMS をインストールします。 3. マシン B の CMS がマシン A の CMS データベースを使用するように指定します。
クラスタキー	CMS データベースでキーを解読するのに使用されます。 CCM を使用してクラスタキーを変更できますが、パスワードのようにキーをリセットすることはできません。暗号化されたコンテンツが含まれており、紛失しないようにすることが重要です。
CMS	Central Management Server の略語です。
CMS データベース	BI プラットフォームに関する情報を保存するために CMS で使用されるデータベースです。
デプロイメント	1 つ以上のマシンにおいてインストール、設定、実行されている BI プラットフォームソフトウェアのことです。
インストール	インストールプログラムによって 1 つのマシン上に作成される BI プラットフォームファイルのインスタンスです。
マシン	BI プラットフォームソフトウェアがインストールされるコンピュータです。
メジャーリリース	ソフトウェアのフルリリースです。
マイナーリリース	ソフトウェアの一部のコンポーネントのリリースです。
ノード	同じマシンで実行され、同じ Server Intelligence Agent (SIA) で管理される BI プラットフォームサーバのグループです。
パッチ	特定のサポートパッケージバージョンの小規模な更新です。
昇格	BI コンテンツを同じメジャーリリース (4.3 から 4.3 など) のデプロイメント間で、プロモーションマネジメントアプリケーションを使用して移行するプロセスです。
サーバ	BI プラットフォームのプロセスの 1 つです。サーバは、1 つ以上のサービスをホストします。
Server Intelligence Agent(SIA)	サーバの停止、起動、起動など、サーバのグループを管理するプロセスです。
サポートパッケージ	マイナーリリースまたはメジャーリリースに対するソフトウェアの更新です。

用語	定義
Web アプリケーションサーバ	動的コンテンツを処理するサーバです。
アップグレード	移行プロセスを完了するために必要な計画、準備、移行、後処理のことです。
ONE Installer	ONE Installer は、サービスパッケージまたはパッチのフレッシュインストール、パッチからパッチへの更新、サービスパッケージからパッチへの更新などの複数の BI インストールシナリオをサポートする単一のインストールパッケージです。

2.2 開始前の準備

2.2.1 基本概念

2.2.1.1 Server Intelligence

Server Intelligence は、BI プラットフォームのコアコンポーネントです。セントラル管理コンソール (CMC) で適用されたサーバプロセスの変更は、Central Management Server (CMS) により、対応するサーバオブジェクトに伝播されます。Server Intelligence Agent (SIA) は、予期しない状況が発生した場合のサーバの自動再起動またはシャットダウンに使用されます。また、ノードを管理する際に管理者に使用されます。

CMS は、サーバ情報を CMS システムデータベースに保存するため、デフォルトのサーバ設定を簡単に復元できます。SIA は、定期的に CMS を検索して管理するサーバの情報を要求するため、サーバのあるべき状態および操作する時期を判断できます。

> ⓘ 注記
>
> BI プラットフォームインストールとはインストーラによって 1 つのマシン上に作成される BI プラットフォームファイルの一意のインスタンスです。BI プラットフォームインストールのインスタンスは、単一クラスタ内でのみ使用できます。同一の BI プラットフォームインストールを共有している異なるクラスタに属するノードは、サポートされません。このタイプのデプロイメントではパッチやアップデートの適用ができないためです。同一マシン上でソフトウェアの複数インストールをサポートするのは UNIX プラットフォームのみです。各インストールが一意のユーザアカウントで実行され、個別のフォルダにインストールされる場合、インストール間でファイルは共有されません。クラスタ内のすべてのマシンで、バージョンとパッチレベルを同じにする必要があります。

関連情報

サーバ、ホスト、およびクラスタ [38 ページ]

2.2.1.2 サーバ、サービス、ノード、およびホスト

BI プラットフォームでは、サーバおよびサービスという用語を使用して、BI プラットフォームコンピュータで実行される 2 種類のソフトウェアを表します。

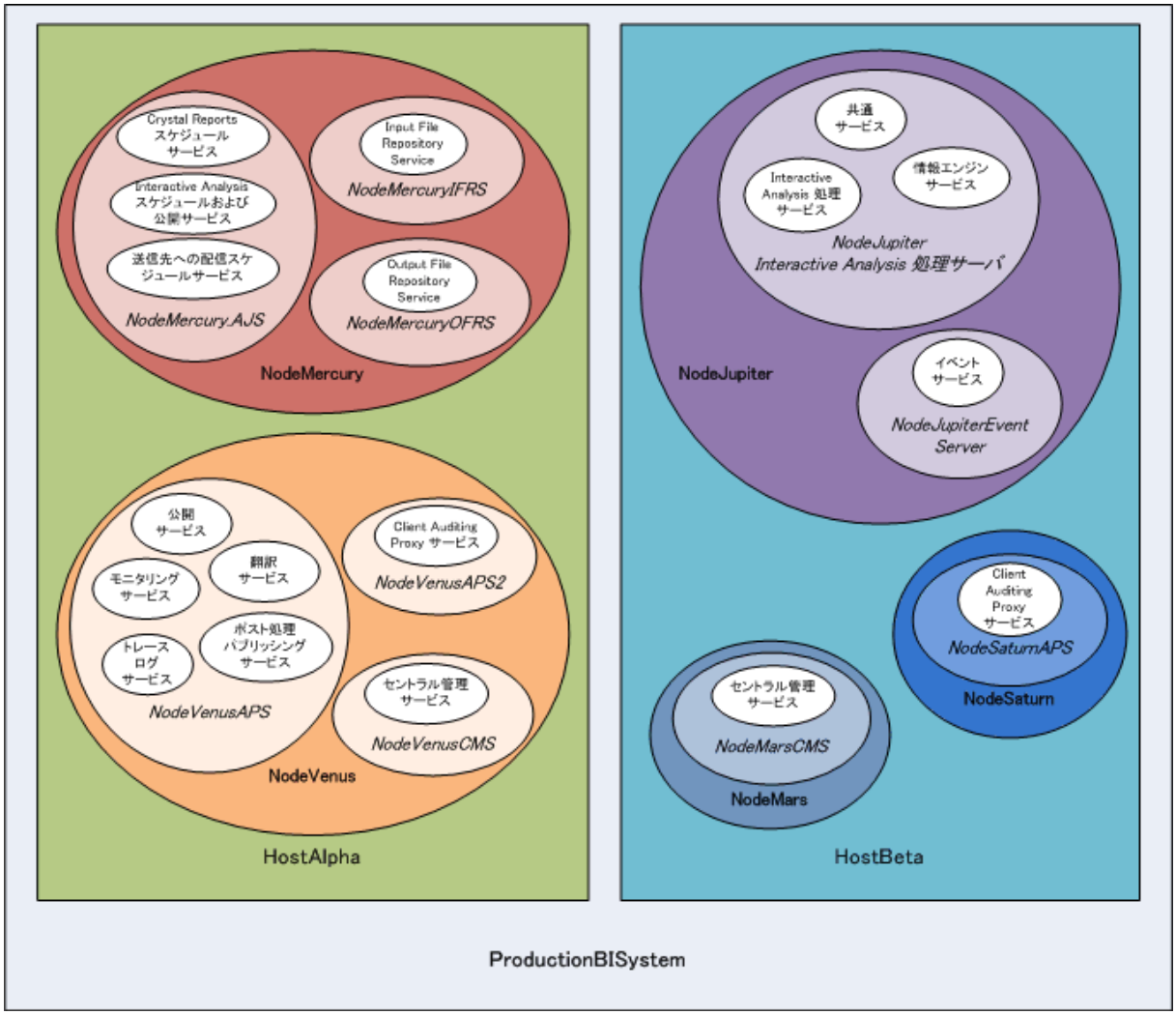
“server” という用語は、1 つ以上のサービスをホストするオペレーティングシステムレベルのプロセスを表します (一部のシステムでは、daemon と呼ばれます)。たとえば、Central Management Server (CMS) と Adaptive Processing Server はサーバです。サーバは、特定のオペレーティングシステムアカウントで実行され、独自のプロセス ID (PID) を持ちます。

サービスは、特定の機能を実行するサーバサブシステムです。サービスは、親コンテナ (サーバ) のプロセス ID を使用して、そのサーバのメモリスペース内で実行されます。たとえば、Web Intelligence スケジュールサービスは、Adaptive Job Server 内で実行されるサブシステムです。

ノードは、同じホストで実行され、同じ Server Intelligence Agent (SIA) で管理される、BI プラットフォームサーバのコレクションです。1 つまたは複数のノードを 1 つのホストに置くことができます。

BI プラットフォームは、1 台のコンピュータにインストールするか、イントラネット上で複数のコンピュータに分散するか、広域ネットワーク (WAN) を介して分散することができます。

次の図は、架空の BI プラットフォームのインストール例です。ホスト、ノード、サーバ、サービスの数、およびサーバとサービスの種類は、実際のインストールによって異なります。



ProductionBISystem というクラスタが、次の 2 つのホストによって形成されています。

- HostAlpha という名前のホストには BI プラットフォームがインストールされ、次の 2 つのノードが設定されています。
  - `NodeMercury` には、レポートをスケジュールおよび公開するサービスを含む Adaptive Job Server (`NodeMercury.AJS`)、入力レポートを格納するサービスを含む Input File Repository Server (`NodeMercury.IFRS`)、およびレポート出力を格納するサービスを含む Output File Repository Server (NodeMercury.OFRS) が含まれます。
  - `NodeVenus` には、公開、監視、翻訳機能を提供するサービスを含む Adaptive Processing Server (`NodeVenus.APS`)、クライアント監査を提供するサービスを含む Adaptive Processing Server (`NodeVenus.APS2`)、および CMS サービスを提供するサービスを含む Central Management Server (NodeVenus.CMS) が含まれます。
- HostBeta という名前のホストには BI プラットフォームがインストールされ、次の 3 つのノードが設定されています。
  - NodeMars: CMS サービスを提供するサービスを含む Central Management Server (`NodeMars.CMS`) が含まれます。CMS を 2 つのコンピュータで実行すると、負荷が均衡および軽減され、フェイルオーバーが可能になります。

- NodeJupiter には、Web Intelligence レポーティングを提供するサービスを含む Web Intelligence Processing Server (`NodeJupiter.Web Intelligence`)、およびファイルのレポート監視を提供する Event Server (`NodeJupiter.EventServer`) が含まれます。
- `NodeSaturn` には、クライアント監査を提供するサービスを含む Adaptive Processing Server (NodeSaturn.APS) が含まれます。

2.2.2 主な管理ツール

2.2.2.1 システム設定ウィザード

システム設定ウィザードは、BI プラットフォームデプロイメントを簡単に素早く設定するために使用できるツールです。このウィザードでは基本設定オプションを介してユーザをガイドし、以下のような共通設定を使用して動作するデプロイメントを設定できるようにします。

- BI プラットフォームを使用して自動的に起動する製品のサーバ
- デプロイメントの最適化で優先するのは、パフォーマンスの最大化か制限されたハードウェアリソースか
- システムフォルダの場所

デフォルトで、ウィザードはユーザがセントラル管理コンソール (CMC) にログインすると自動的に実行されるように設定されていますが、ウィザードでこの設定を変更できます。CMC の管理エリアからもいつでもウィザードを起動することができます。

> ⓘ 注記
>
> 本稼働システムでウィザードが自動的に実行されないように設定して、誤って再設定されないようにしておくことをお勧めします。

> ⓘ 注記
>
> ウィザードを使用して既存のシステムを変更する前に、完全バックアップを作成しておくことをお勧めします。

2.2.2.2 セントラル管理コンソール(CMC)

セントラル管理コンソール (CMC) は Web ベースのツールで、ユーザ管理、コンテンツ管理、サーバ管理などの管理タスクの実行、およびセキュリティの設定に使用できます。CMC は Web ベースのアプリケーションであるため、すべての管理タスクを、Web アプリケーションサーバに接続可能な任意のコンピュータの Web ブラウザで実行できます。

明示的にユーザに権限が付与されている場合を除き、管理設定を変更できるのは Administrators グループのメンバーだけです。ロールは CMC で割り当てることができ、グループ内のユーザの管理、チームのフォルダにあるレポートの管理など、最低限の管理タスクを実行できる権限をユーザに付与することができます。

2.2.2.3 セントラル設定マネージャ(CCM)

セントラル設定マネージャ (CCM) は、2 つのフォームで提供されるサーバトラブルシューティングおよびノード管理ツールです。Microsoft Windows 環境では、CCM を使用して、そのグラフィカルユーザインタフェース (GUI) またはコマンドラインからローカルサーバとリモートサーバを管理できます。Unix 環境では、CCM シェルスクリプト (`ccm.sh`) を使用してコマンドラインからサーバを管理できます。

CCM がデフォルトで Tomcat Web アプリケーションサーバにバンドルされている場合、CCM を使用して、ノードを作成および設定したり、Web アプリケーションサーバを起動または停止することができます。Windows では、Secure Sockets Layer (SSL) 暗号化などのネットワークパラメータも設定できます。これらのパラメータは、ノード内のすべてのサーバに適用されます。

> ⓘ 注記
>
> サーバ管理タスクの大半は、現在は CCM ではなく CMC で処理されます。現在は、CCM はトラブルシューティングとノードの設定のために使用されます。

2.2.2.4 リポジトリ診断ツール

リポジトリ診断ツール (RDT) を使用すると、Central Management Server (CMS) システムデータベースと File Repository Servers (FRS) のファイルストアの間の不整合をスキャン、診断、および修復できます。 RDT が検出または修復するエラーの数 (それを超えると停止します) を制限できます。

RDT は、BI プラットフォームシステムを修復してから使用する必要があります。

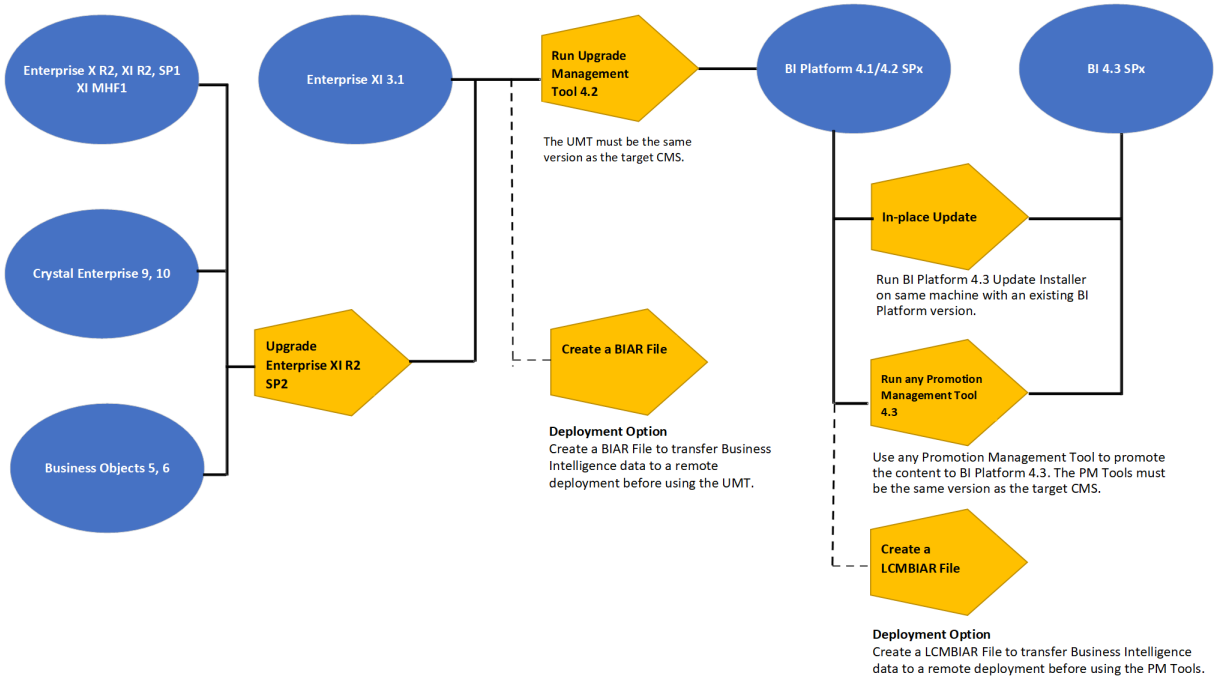
> ⓘ 注記
>
> 本稼働システムでは、RDT を定期的に実行しますが、基盤となるシステムの健全性の問題に注意するため、“修復”オプションは無効にしておくことをお勧めします。 RDT でシステムに修復を実行すると確信している場合にだけ、修復オプションを有効にして RDT を実行してください。

2.2.2.5 アップグレードマネジメントツール

UMT は、BI 4.3 リリースで非推奨になります。詳細については、2801797 を参照してください。

2.2.2.6 アップグレードパス

以前の BI 4.x バージョンから SAP BusinessObjects Business Intelligence プラットフォーム 4.3 に、システムデータやビジネスインテリジェンスコンテンツを移行できます。



アップグレードマネジメントツールは SAP BusinessObjects Business Intelligence プラットフォーム 4.3 では非推奨となっていますが、下記のアップグレードパスに従って 4.3 に移行できます。

旧バージョンのデプロイメントで既存のデプロイメントを BI プラットフォーム 4.3 にアップグレードする場合は、以下のガイドラインに従ってください。

1. 既存のデプロイメントが XI R2、XI MHF1、XI R2 SP1、BusinessObjects 5/6、または Crystal Enterprise 9/10 である場合は、最初に XI R2 SP2 (またはそれ以上) にアップグレードし、ステップ 3 から続行してください。
2. 既存のデプロイメントが XI 3.x である場合は、ステップ 3 からアップグレードを直接進めることができます。
3. BI 4.1/4.2 SPx を個別のマシンにインストールし、4.1/4.2 SPx からアップグレードマネジメントツールを実行して、上記のバージョンから BI 4.1/4.2 SPx レベルにコンテンツを移行します。
4. コンテンツを BI 4.1/4.2 SPx レベルに移行したら、以下のいずれかの方法を選択して 4.3 に移行することができます。
   1. 4.1/4.2 SPx レベルのマシンで BI 4.3.x のアップデートインストールソフトウェアを実行します。または
   2. BI 4.3 を別のマシンにインストールし、BI 4.3.x のプロモーションマネジメントツールを使用して、コンテンツを BI 4.1/4.2 SPx レベルから BI 4.3.x レベルに昇格します。

ⓘ 注記

1. コンテンツを BI 4.1/4.2 SPx レベルから BI 4.3.x レベルに昇格するには、プロモーションマネジメントツールのバージョンが、ターゲット CMS と同じである必要があります。
2. BusinessObjects 5/6 から XI 3.1 の詳細については、https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_ENTERPRISE_BUSINESS_INTELLIGENCE_PLATFORM/XI.3.1/en-US にある移行ガイドおよびご使用のバージョンの BI プラットフォームインストールガイドを参照してください。
3. アップグレードマネジメントツールで (UMT) は、デプロイメント内のサーバと Web Tier 機能のみがアップグレードされます。UMT の詳細については、https://help.sap.com/viewer/product/SAP_BUSINESSOBJECTS_BUSINESS_INTELLIGENCE_PLATFORM/4.2/en-US にあるご使用のバージョンの Business Intelligence プラットフォームアップグレードガイドを参照してください。

2.2.3 主要タスク

状況に合わせて、このガイドの特定の節に焦点を絞って参照できます。また、他にも参照できるリソースがあります。 各状況について、推奨されるタスクと参照先のトピックのリストを示します。

関連情報

初めてのデプロイメントの計画または実行 [31 ページ]
デプロイメントの設定 [32 ページ]
システムのパフォーマンスの改善 [32 ページ]
セントラル管理コンソール(CMC) [28 ページ]

2.2.3.1 初めてのデプロイメントの計画または実行

BI プラットフォームの初めてのデプロイメントを計画または実行する場合は、このガイドの次の節の参照をお勧めします。

- BI プラットフォームコンポーネントの概要については、「“アーキテクチャの概要”」を参照してください。
- “BI プラットフォームコンポーネント間の通信について”
- “セキュリティの概要”
- サードパーティ認証を使用する場合は、「“BI プラットフォームの認証オプション”」を参照してください。
- インストール後は、「“CMC の [サーバ] 管理エリアの使用”」を参照してください。

BI プラットフォームのインストールの詳細については、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドを参照してください。ニーズを確認し、最適な状態で機能するデプロイメントのアーキテクチャを設計するには、*SAP BusinessObjects Business Intelligence* プラットフォーム計画ガイドを参照してください。

関連情報

アーキテクチャの概要 [34 ページ]
BI プラットフォームコンポーネント間の通信 [186 ページ]
セキュリティの概要 [147 ページ]
BI プラットフォームの認証オプション [224 ページ]
CMC の[サーバ]管理エリアの使用 [402 ページ]

2.2.3.2 デプロイメントの設定

BI プラットフォームのインストールが完了し、ファイアウォール設定やユーザ管理などの初期設定タスクを実行する必要がある場合は、次の節を参照することをお勧めします。

関連情報

システム設定ウィザードの概要 [86 ページ]
BI プラットフォームコンポーネント間の通信 [186 ページ]
セキュリティの概要 [147 ページ]
モニタリング [771 ページ]

2.2.3.3 システムのパフォーマンスの改善

デプロイメントの効果を評価し、リソースを最大限活用できるように調整する場合は、次の節を参照してください。

- デプロイメントテンプレートを使用してシステムを設定する場合は、「“システム設定ウィザードの概要”」を参照してください。
- 既存のシステムを監視する場合は、「“モニタリング”」を参照してください。
- CMC でサーバを使用するための日常的なメンテナンスタスクや手順については、「“CMC の [サーバ] 管理エリアの使用”」を参照してください。

関連情報

システム設定ウィザードの概要 [86 ページ]
モニタリング [771 ページ]
CMC の[サーバ]管理エリアの使用 [402 ページ]

2.2.3.4 CMC でのオブジェクトの使用

オブジェクトは、BI プラットフォームまたはその他のソフトウェアで作成され、BI プラットフォームリポジトリに保存され管理されるドキュメントまたはファイルです。CMC でオブジェクトを使用している場合は、次の節を参照してください。

- CMC でのユーザとグループの設定については、「"アカウント管理の概要"」を参照してください。
- オブジェクトにセキュリティを設定するには、「"BI プラットフォームのアクセス権の動作"」を参照してください。
- オブジェクトの使用の概要については、*SAP BusinessObjects Business Intelligence* プラットフォームユーザガイドを参照してください。

関連情報

アカウント管理の概要 [98 ページ]
BI プラットフォームでのアクセス権の動作 [121 ページ]

3 アーキテクチャ

3.1 アーキテクチャの概要

ここでは、全体的なプラットフォームアーキテクチャ、システム、および SAP BusinessObjects Business Intelligence プラットフォームを構成しているサービスコンポーネントの概要を説明します。この情報は、管理者がシステムの必須要素を理解したり、システムのデプロイメント、管理、およびメンテナンスの計画を立てたりするうえで役立ちます。

> **注記**
>
> サポートされるプラットフォーム、言語、データベース、Web アプリケーションサーバ、Web サーバ、およびこのリリースでサポートされるその他のシステムの一覧については、http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540 で入手可能な *Product Availability Matrix* (PAM) を参照してください。

> **注記**
>
> PAM は継続的に更新されるため、ダウンロードされたコピーではなく、必ず PAM のオンラインバージョンを参照してください。

Business Intelligence (BI) プラットフォームは、幅広いユーザおよびデプロイメントシナリオで優れたパフォーマンスを実現できるよう設計されています。特定のサービスをホストする専用サーバを作成することにより、プロセッサ集中型のスケジュールや処理を専用サーバにオフロードすることができます。アーキテクチャは、どの BI デプロイメントのニーズにも合うように設計されており、1 つのツールを使用する数人のユーザから、複数のツールを使用する何万人のユーザ、およびインタフェースまで柔軟に対応できます。

開発者は、Web サービス、Java、または .NET アプリケーションプログラミングインタフェース (API) を使用して、BI プラットフォームを組織のその他のテクノロジーシステムに統合することができます。

エンドユーザは、次のような専門のツールやアプリケーションを使用してレポートにアクセスし、レポートを作成、編集、および操作することができます。

- BI プラットフォームクライアントツールのインストールプログラムによってインストールされたクライアント:
  - Web Intelligence リッチクライアント
  - ビジネスビューマネージャ
  - ユニバースデザインツール
  - Query as a Web Service
  - インフォメーションデザインツール (旧インフォメーションデザイナ)
  - トランスレーションマネジメントツール (旧トランスレーションマネージャ)
- 個別入手可能クライアント:
  - SAP Crystal Reports
  - SAP BusinessObjects Analysis (旧 Voyager)
  - BI ワークスペース (旧 Dashboard Builder)

IT 部門では、次のようなデータおよびシステム管理ツールを使用できます。

- レポートビューア
- セントラル管理コンソール (CMC)
- セントラル設定マネージャ (CCM)
- リポジトリ診断ツール (RDT)
- データフェデレーション管理ツール
- ユニバースデザインツール (旧 Universe Designer)
- SAP BusinessObjects Mobile

柔軟性、信頼性、およびスケーラビリティを実現するため、BI プラットフォームコンポーネントは、1 台のマシンにインストールすることも、複数台のマシンにインストールすることもできます。場合によっては、バージョンが異なる 2 つの BI プラットフォームを同じコンピュータに同時にインストールすることもできますが、この構成は、アップグレードプロセスの一部として、またはテスト目的のみで推奨されます。

サーバプロセスを垂直的に拡張 (複数またはすべてのサーバ側プロセスを 1 台のコンピュータで実行) してコストを削減したり、水平的に拡張 (サーバ側プロセスを 2 台以上のネットワーク化されたマシンに分散) してパフォーマンスを向上させたりすることができます。同じサーバプロセスの複数の冗長バージョンを複数のマシンで実行し、一次プロセスで問題が発生した場合に処理を続行できるようにすることもできます。

> ⓘ 注記
>
> Windows プラットフォームと UNIX または Linux プラットフォームを組み合わせて使用することもできますが、Central Management Server (CMS) プロセスについてはオペレーティングシステムを組み合わせて使用しないことをお勧めします。

3.1.1 コンポーネント図

SAP BusinessObjects Business Intelligence プラットフォームは、情報配信を促進するエンタープライズレベルの分析およびレポーティングツールを提供するビジネスインテリジェンス (BI) プラットフォームです。データはサポートされる任意のデータベースシステム (テキストまたは多次元 OLAP システムを含む) から分析でき、BI レポートはさまざまな形式でさまざまな公開システムに公開することができます。

このアーキテクチャ図は、サーバおよびクライアントツールを含む BI プラットフォームコンポーネントと、BI プラットフォームランドスケープの一部として使用できる追加のアナリティクス製品、Web アプリケーションコンポーネント、およびデータベースを示しています。BI 4.3 のアーキテクチャ図。

BI プラットフォームは、組織のデータベースへの読み取り専用接続からレポートを作成し、独自のデータベースを使用してその設定情報、監査情報、およびその他のオペレーション情報を保存します。システムによって作成された BI レポートは、ファイルシステム、電子メールなどのさまざまな宛先に送信したり、Web サイトまたはポータルからアクセスできます。

BI プラットフォームは、(小規模な開発環境や本稼動前テスト環境などとして) 単一のマシンにインストールすることも、(大規模な本稼働環境などとして) 異なるコンポーネントを実行する複数のマシンのクラスタに拡張することもできます。

3.1.2 アーキテクチャの各層

SAP BusinessObjects Business Intelligence プラットフォームは、一連の概念層と考えることができます。

クライアント層

クライアント層には、BI プラットフォームとやりとりして、さまざまなレポーティング、アナリティクス、管理機能を提供するようなすべてのデスクトップクライアントアプリケーションが含まれます。たとえば、セントラル設定マネージャ (BI プラットフォームのインストールプログラム)、インフォメーションデザインツール (BI プラットフォームクライアントツールのインストールプログラム)、SAP Crystal Reports (別個に利用およびインストールが可能) などがあります。

SAP BI 4.3 以降は、デスクトップクライアントアプリケーション (Web Intelligence リッチクライアント、インフォメーションデザインツール、ユニバースデザインツールなど) は 64 ビットアプリケーションです。32 ビットではありません。

Web Tier

Web Tier には、Java Web アプリケーションサーバにデプロイされた Web アプリケーションが含まれます。Web アプリケーションは、Web ブラウザを介してエンドユーザに BI プラットフォーム機能を提供します。Web アプリケーションの例としては、セントラル管理コンソール (CMC) の管理 Web インタフェースや BI 起動パッドなどがあります。

Web Tier には、Web サービスも含まれます。Web サービスは、Web アプリケーションサーバを介して、セッション認証、ユーザ権限管理、スケジュール、検索、管理、レポーティング、およびクエリ管理などの BI プラットフォーム機能を各種ソフトウェアツールに提供します。たとえば、Live Office は、Web サービスを使用して BI プラットフォームレポーティングを Microsoft Office 製品に統合します。

管理層

管理層 (別名インテリジェンス層) は、BI プラットフォームを構成するすべてのコンポーネントを調整および管理します。管理層は、Central Management Server (CMS) と Event Server、および関連サービスで構成されます。CMS は、セキュリティおよび設定情報の維持、サーバへのサービス要求の送信、監査の管理、および CMS システムデータベースの維持を行います。Event Server は、ストレージ層で発生するファイルベースのイベントを管理します。

Strage 層

ストレージ層は、ドキュメントやレポートなどのファイルを処理します。

Input File Repository Server は、レポートで使用される情報が入っているファイル (`.rpt`、`.car`、`.exe`、`.bat`、`.js`、`.xls`、`.doc`、`.ppt`、`.rtf`、`.txt`、`.pdf`、`.wid`、`.rep`、`.unv`、`.unx` などのファイルタイプ) を管理します。

> **注記**
>
> Input File Repository Server ファイルストアのサイズはシステムで管理されないため、管理者は監視およびメンテナンス計画を管理する必要があります。

Output File Repository Server は、システムによって作成されるレポート (`.rpt`、`.csv`、`.xls`、`.doc`、`.rtf`、`.txt`、`.pdf`、`.wid`、`.rep` などのファイルタイプ) を管理します。

また、ストレージ層はユーザがレポートにアクセスするときにシステムリソースを節約するために、レポートのキャッシングも行います。

処理層

処理層では、データの分析や、レポートおよびその他の出力タイプの作成が行われます。処理層は、レポートデータを含むデータベースにアクセスする唯一の層です。この層は、Adaptive Job Server、Connection Server (64 ビット)、および Adaptive Processing Server や Crystal Reports Processing Server などの処理サーバで構成されます。

データ層

データ層は、CMS システムデータベースおよび監査データストアをホストする複数のデータベースサーバで構成されます。また、リレーショナルデータ、OLAP データ、またはレポーティングアプリケーションおよび分析アプリケーション用の他の種類のデータを含む任意のデータベースサーバでも構成されます。

3.1.3 データベース

BI プラットフォームでは、複数の異なるデータベースを使用します。

- レポーティングデータベース
  組織のデータを参照します。SAP BusinessObjects Business Intelligence Suite 製品によって分析およびレポートされるソースデータとなります。通常、このデータはリレーショナルデータベース内に保存されますが、テキストファイル、Microsoft Office ドキュメント、または OLAP システムに保存することもできます。
- CMS システムデータベース
  CMS システムデータベースは、ユーザ、サーバ、フォルダ、ドキュメント、設定、認証の詳細などの BI プラットフォーム情報の格納に使用されます。このデータベースは、Central Management Server (CMS) によって保守され、システムリポジトリとも呼ばれます。
- 監査データストア
  監査データストア (ADS) を使用して、BI プラットフォームで発生する追跡可能なイベントに関する情報を保存します。この情報を使用して、システムコンポーネントの使用状況、ユーザアクティビティ、または日常業務のその他の要素を監視することができます。

- モニタリングデータベース
  モニタリングでは、監査データストア (ADS) データベースを使用してシステム設定およびコンポーネント情報を格納し、SAP 保守性を確保します。
- Commentary ベース
  BI Commentary は、CMC に導入されているアプリケーションです。ユーザは、指定されたドキュメントで使用できるデータ/統計に関するコメントを作成することによって、相互にコラボレーションすることができます。
  Commentary データベースは、監査データベースと同じデータベースに設定されます。デフォルトでは、監査データベースに作成されます。

CMS システムデータベースおよび監査データストアデータベースで使用するデータベースサーバがない場合は、BI プラットフォームインストールプログラムによってインストールおよび設定することができます。お使いのデータベースサーバベンダから入手した情報と照らし合わせて要件を評価し、ユーザの組織の要件に最も適したサポートされるデータベースを決定することをお奨めします。

> ⓘ 注記
>
> デフォルトの SQL Anywhere データベースを本稼働システムにすることはお勧めできません。このデータベースは BI プラットフォームのサーバパッケージにバンドルされ、BI プラットフォームをただちにデプロイしてテストできます。しかし、データベースの管理に必要な機能が制限されています。CMS データベースはデータセンタに置くことが不可欠です。したがって、機能の制限されない SQL Anywhere を使用するか、または本稼働システム用にサポートされた既存のデータベースインスタンスを使用することをお奨めします。これは、データセキュリティとサーバの可用性のために確立された適切なプロセスを使用してデータベース管理者が管理します。

3.1.4 サーバ、ホスト、およびクラスタ

BI プラットフォームは、1 つまたは複数のホストで実行されるサーバのコレクションで構成されます。小規模のインストール (テストシステムや開発システムなど) では、Web アプリケーションサーバ、データベースサーバ、およびすべての BI プラットフォームサーバに対して単一のホストを使用することができます。

中規模および大規模のインストールでは、複数のホスト上でサーバを実行することができます。たとえば、1 つの Web アプリケーションサーバホストを 1 つの BI プラットフォームサーバホストと組み合わせて使用することができます。これにより BI プラットフォームサーバホストのリソースが解放されるため、Web アプリケーションサーバもホストする場合より多くの情報を処理することができます。

大規模のインストールでは、複数の BI プラットフォームサーバホストを 1 つのクラスタで連携させることができます。たとえば、ある組織に多数の SAP Crystal Reports ユーザが存在する場合は、クライアントからのリクエストを処理する十分なリソースを確保するために、複数の BI プラットフォームサーバホスト上に Crystal Reports 処理サーバを作成することができます。

複数のサーバを配置する利点は、以下のとおりです。

- パフォーマンスの改善
  複数の BI プラットフォームサーバホストは、単一の BI プラットフォームサーバホストより迅速にレポーティング情報のキューを処理することができます。
- 負荷分散
  あるサーバが高負荷になると、CMS は自動的に新規作業をクラスタ内の別のサーバに送信します。
- 可用性の改善

サーバが予期しない状態になると、CMS は条件が修正されるまで自動的に別のサーバに作業をルート変更します。

3.1.5 Web アプリケーションサーバ

Web アプリケーションサーバは、Web ブラウザまたはリッチアプリケーションと BI プラットフォーム間の変換層として機能します。 Windows、UNIX、および Linux で実行される Web アプリケーションサーバがサポートされます。

サポートされる Web アプリケーションサーバの詳細一覧については、https://support.sap.com/home.html で入手可能なサポートされるプラットフォーム/*PAR* を参照してください。

BI プラットフォームと一緒に使用する Web アプリケーションサーバを準備していない場合は、Tomcat Web アプリケーションサーバをインストールおよび設定することができます。 お使いの Web アプリケーションサーバベンダから入手した情報と照らし合わせて要件を評価し、ユーザの組織の要件に最も適したサポートされる Web アプリケーションを決定することをお勧めします。

> **注記**
>
> 本稼働環境を設定する場合には、Web アプリケーションサーバを独立したシステムでホストすることをお勧めします。 本稼働環境で BI プラットフォームと Web アプリケーションサーバを同じホストで実行すると、パフォーマンスが低下する可能性があります。

3.1.5.1 セッションフェイルオーバーおよびスケーラビリティをサポートする BI ラウンチパッド Web アプリケーションのクラスタリングの有効化

この節では、BI ラウンチパッド Web アプリケーションでクラスタリングを有効化して、セッションフェイルオーバーおよびスケーラビリティをサポートする方法について説明します。また、同じ目的のために Apache Tomcat および WebSphere アプリケーションサーバを設定する手順について説明します。

Tomcat や WebSphere のようなアプリケーションサーバのクラスタリングを有効化するには、以下のコンポーネントが必要となります。

- HTTP サーバ
- 互換性のあるロードバランサ
- 必要な Web アプリケーションがすでにインストールされているアプリケーションサーバの 2 つ以上のインスタンス
- 完全な BOE インストール (リポジトリ)

> **注記**
>
> この節で説明されている手順は汎用的なものであり、その他のアプリケーションのクラスタリングの有効化に使用することができます。唯一の相違点は、Web アプリケーション (web.xml) のデプロイメント記述子での変更です。Web 層の負荷分散の設定方法については、Web アプリケーションサーバのベンダに問い合わせることをお奨めします。

3.1.5.1.1 Apache Tomcat のインストール

Apache Tomcat サーバをインストールするには、次の手順に従います。

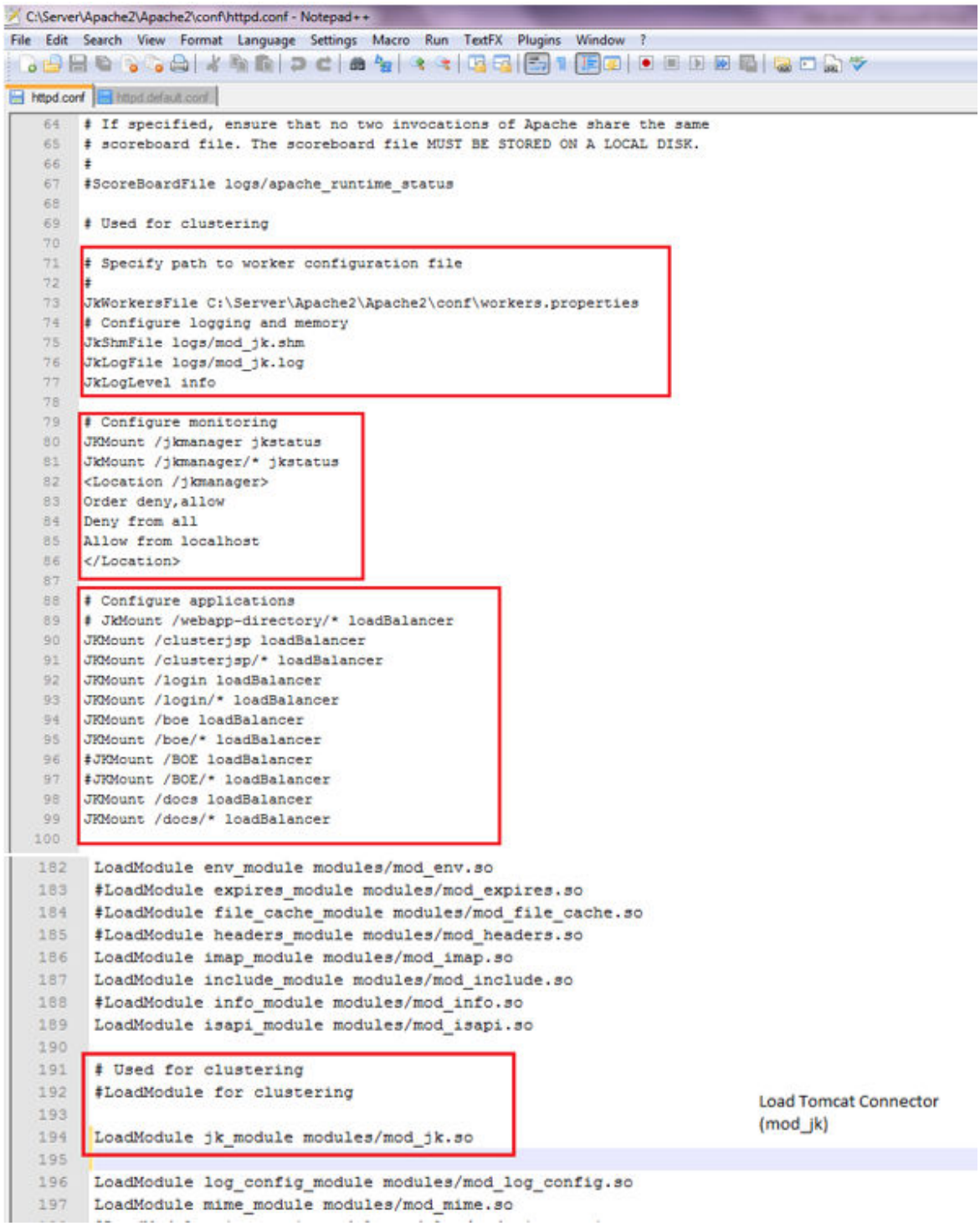
1. Apache HTTP サーバをインストールします。
2. インスタンスマシンに Apache Tomcat サーバをインストールします。
3. http://tomcat.apache.org/download-connectors.cgi から mod_jk (ロードバランサ) をダウンロードして、Apache HTTPD サーバの "modules" ディレクトリに保存します。
4. BOE の完全インストールがすでにインストールされているマシンで、SI エージェントを実行します。

> **注記**
>
> mod_jk の互換性をチェックするには、HTTP サーバを起動します。ダウンロードした mod_jk のバージョンにご使用の HTTP サーバのバージョンとの互換性がない場合は、エラーメッセージが表示されます。

Apache Tomcat の設定

Apache Tomcat を設定するには、次の手順に従います。

1. Apache HTTP サーバを設定します。
   a. httpd.conf (ロードバランサ、ロード Web アプリケーション、モニタリング、worker.properties ファイルへのパス)。
   b. workers.properties ファイルを設定して、Apache¥Conf ライブラリに保存します。



2. Tomcat で server.xml を設定します (クラスタリングタグの追加)。
   a. server.xml では、jvmRoute 属性が workers.properties ファイルで使用した名称に対応している必要があります。
   b. Tomcat 8 以上を使用している場合は、JvmRouteSessionIDBinderListener を削除します (非推奨)。
3. クラスタリングがサポートされるようにする Web アプリケーションの web.xml ファイル (デプロイメント記述子) に配布可能なタグを追加します。

以下では、各要求のデフォルトバルブを呼び出すカスタムバルブが指定されています。Tomcat 8 を使用している場合は、すべての Tomcat の server.xml で、以下の操作を実行します。

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Inte
rceptor"/>
```

これを以下で置き換えます。

```
<Interceptor
className="org.apache.catalina.tribes.group.interceptors.MessageDispatchInterc
eptor"/>
```

```
    <Sender className="org.apache.catalina.tribes.transport.ReplicationTransmitter">
      <Transport className="org.apache.catalina.tribes.transport.nio.PooledParallelSender"/>
    </Sender>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.TcpFailureDetector"/>
    <Interceptor className="org.apache.catalina.tribes.group.interceptors.MessageDispatch15Interceptor"/>
  </Channel>

  <Valve className="com.sap.customvalve.ForceReplicationValve"/>
   <Valve className="org.apache.catalina.ha.tcp.ReplicationValve" filter=".*\.gif;.*\.jpg;.*\.png;.*\.js;.*\.htm
  <Valve className="org.apache.catalina.ha.session.JvmRouteBinderValve"/>

  <Deployer className="org.apache.catalina.ha.deploy.FarmWarDeployer" deployDir="/tmp/war-deploy/" tempDir="/tmp
```

4. コードからカスタムバルブの jar をエクスポートします (変更が必要な場合)。`<BOEInstallDir>/SAP BusinessObjects XI 4.0/java/lib` にある `forcereplicationvalve.jar` ファイルをコピーし、(すべての Tomcat ノードの) `<TomcatInstallDir>/tomcat/lib` に貼り付けます。
5. この jar を各インスタンスの `tomcat/lib` フォルダに格納します。
6. すべてのサーバを再起動します。

> ⓘ 注記
>
> - ベストプラクティスとして、サーバを一度に 1 台ずつ起動することをお勧めします。1 台のサーバが完全に起動してから、別のサーバを起動します。
> - ラウンチパッドのログイン画面でシステム名として localhost:6400 を使用しないでください。特定の BOE インストールマシンの名称 (または IP) を指定します。そのインストールで SI エージェントが実行中であることを確認します。
> - channelSendOptions 属性で最適なオプションを見つけます。この属性を使用して、同期応答、非同期応答などのオプションを設定します。
> - コードからカスタムバルブの jar を参照する場合は、jar の適切なパッケージ階層を登録し、この階層を server.xml に含めます。

3.1.5.1.2 WebSphere のインストール

WebSphere の設定

WebSphere を設定するには、次の手順に従います。

1. 両方の WebSphere アプリケーションサーバインスタンスの BOE Web アプリケーションの web.xml で、配布可能なタグを追加します。
2. IBM コンソールで、[すべてのサーバ] > [*member1*] > [セッション管理] に移動します。
   a. Cookie をチェックし、有効化します。
   b. [*Allow serial access*] を有効化し、タイムアウトを 10 秒に変更します。
3. [分散環境設定] > [メモリ間の複製] に移動します。
   a. レプリケーションドメインを登録して選択します。
   b. クライアントとサーバの両方のレプリケーションモードを選択します。
4. [すべてのサーバ] の各インスタンスから、前の手順で選択したレプリケーションドメインを選択します。
5. [分散環境設定] > [カスタムチューニングパラメータ] に移動します。
   a. フェイルオーバーについて、チューニングレベルとして [低値] を選択します。
6. すべてのサーバを再起動します。

3.1.5.2 Web アプリケーションコンテナサーバ (WACS)

BI プラットフォーム Web アプリケーションをホストするには、Web アプリケーションサーバが必要です。

高度な管理ニーズを有する上級 Java Web アプリケーションサーバ管理者の場合は、サポートされている Java Web アプリケーションサーバを使用して BI プラットフォーム Web アプリケーションをホストしてください。サポートされている Windows オペレーティングシステムを使用して BI プラットフォームをホストし、簡単な Web アプリケーションサーバのインストールプロセスを望む場合、または Java Web アプリケーションサーバを管理するリソースがない場合は、BI プラットフォームをインストールする際に Web アプリケーションコンテナサーバ (WACS) をインストールできます。

WACS は、BI プラットフォームサーバの 1 つで、これを使用することにより、Java Web アプリケーションサーバがインストールされていなくてもセントラル管理コンソール (CMC)、BI ラウンチパッド、および Web サービスなどの BI プラットフォーム Web アプリケーションを実行できます。

WACS を使用する利点

- WACS のインストール、管理、設定は最小限の作業で済みます。WACS は、BI プラットフォームインストールプログラムによってインストールおよび設定されます。WACS の使用を開始するために追加のステップは必要ありません。
- WACS では、Java アプリケーションサーバの管理および保守に関するスキルは不要です。
- WACS には、他の BI プラットフォームサーバと一貫性のある管理インタフェースが用意されています。
- その他の BI プラットフォームサーバと同様、WACS は専用ホストにインストールできます。

> **注記**
>
> 専用 Java Web アプリケーションサーバではなく WACS を使用する場合には、以下ような制約があります。
>
> - WACS を使用できるのは、サポートされている Windows オペレーティングシステム上のみです。
> - カスタム Web アプリケーションは、BI プラットフォームにインストールされた Web アプリケーションのみをサポートするため、WACS にはデプロイできません。
> - WACS は Apache ロードバランサーとは併用できません。

WACS のほかに専用 Web アプリケーションサーバを使用することができます。これにより、専用 Web アプリケーションサーバはカスタム Web アプリケーションをホストでき、CMC およびその他の BI プラットフォーム Web アプリケーションは WACS によってホストされます。

3.1.6 ソフトウェア開発キット

ソフトウェア開発キット (SDK) を使用すると、開発者は、SAP BusinessObjects Business Intelligence プラットフォームのアスペクトを組織の独自のアプリケーションおよびシステムに組み入れることができます。

BI プラットフォームには、Java および .NET プラットフォーム上のソフトウェア開発用の SDK があります。

> ⓘ 注記
>
> BI プラットフォームの .NET SDK は、デフォルトではインストールされていません。SAP Service Marketplace からダウンロードする必要があります。

BI プラットフォームでは、次の SDK をサポートしています。

- Business Intelligence プラットフォームの Java SDK および .NET SDK
  BI プラットフォームの SDK を使用すると、認証、セッション管理、リポジトリオブジェクト、レポートスケジュールおよびパブリケーションでの作業、さらにサーバ管理などのタスクをアプリケーションで実行することができます。

  > ⓘ 注記
  >
  > セキュリティ、サーバ管理および監査の各機能にフルアクセスするには、Java SDK を使用します。

- Business Intelligence プラットフォーム RESTful Web サービス SDK
  BI プラットフォーム RESTful Web サービス SDK により、HTTP プロトコルを使用して BI プラットフォームにアクセスできます。この SDK を使用すると、BI プラットフォームへのログオン、BI プラットフォームリポジトリへの移動、リソースへのアクセス、および基本リソースのスケジュールを実行することができます。この SDK にアクセスするには、HTTP プロトコルをサポートする任意のプログラミング言語を使用してアプリケーションを記述するか、HTTP 要求の作成をサポートする任意のツールを使用します。
- Business Intelligence プラットフォームの Java コンシューマ SDK および .NET コンシューマ SDK
  ユーザ認証とセキュリティ、ドキュメントとレポートアクセス、スケジュール、パブリケーション、およびサーバ管理を処理できる SOAP ベースの Web サービスを実装。
  BI プラットフォーム Web サービスは、XML、SOAP、AXIS 2.0、および WSDL などの標準を使用します。プラットフォームは、WS-Interoperability Basic Profile 1.0 Web サービス仕様に準拠しています。

  > ⓘ 注記
  >
  > Web サービスアプリケーションは、現在、次に示すロードバランサ構成のみをサポートします。
  > 1. ソース IP アドレスの永続性
  > 2. ソース IP および出力ポートの永続性 (Cisco コンテントサービススイッチで使用可能)
  > 3. SSL 永続性
  > 4. セッション永続性に基づく Cookie

  > ⓘ 注記
  >
  > SSL 永続性は、一部の Web ブラウザでセキュリティおよび信頼性に関する問題の原因となる可能性があります。ネットワーク管理者に確認してから、SSL 永続性が適切かどうかを判断してください。

- データアクセスドライバ SDK および接続 Java SDK
  これらの SDK を使用すると、Connection Server 用のデータベースドライバを作成してデータベース接続を管理できます。
- セマンティックレイヤ Java SDK
  セマンティックレイヤ Java SDK を使用すると、ユニバースおよび接続上で管理タスクとセキュリティタスクを実行する Java アプリケーションを開発することができます。たとえば、ユニバースをリポジトリに公開するサービスや、セキュリティ保護された接続をリポジトリから取得してワークスペースに渡すサービスを実装できます。このアプリケーションは、BI プラットフォームが OEM として統合されている BI プラットフォームソリューションに埋め込むことができます。
- Report Application Server Java SDK および .NET SDK
  Report Application Server SDK を使用すると、アプリケーションで既存の Crystal Reports を開いて、作成および変更 (パラメータ値の設定、データソースの変更、他の形式 (XML、PDF、Microsoft Word、Microsoft Excel など) へのエクスポートなど) を行うことができます。
- Java および .NET の Crystal Reports Viewer
  ビューアを使用すると、アプリケーションで Crystal レポートを表示およびエクスポートできます。次のビューアを使用できます。
  - DHTML レポートページビューア: データを表示し、ドリルダウン、ページナビゲーション、ズーム、プロンプト、検索、強調表示、エクスポート、および印刷を行うことができます。
  - レポートパーツビューア: 個々のレポートパーツ (チャート、テキスト、フィールドなど) を表示する機能を提供します。
- Report Engine Jave SDK および .NET SDK
  Report Engine SDK を使用すると、SAP BusinessObjects Web Intelligence で作成されたレポートとやりとりすることができます。
  Report Engine SDK には、Web レポートデザインツールを構築するためのライブラリが含まれています。この SDK で作成されたアプリケーションでは、さまざまな Web Intelligence ドキュメントを表示、作成、変更できます。ユーザは、テーブル、チャート、条件、フィルタなどのオブジェクトを追加、削除、変更することで、ドキュメントを変更できます。
- プラットフォーム検索 SDK: プラットフォーム検索 SDK は、クライアントアプリケーションとプラットフォーム検索サービスの間のインタフェースです。プラットフォーム検索は、プラットフォーム検索 SDK の一部として提供される公開 SDK をサポートします。
  検索要求パラメータがクライアントアプリケーションから SDK レイヤに送信されると、SDK レイヤが要求パラメータを XML にエンコードされた形式に変換し、プラットフォーム検索サービスに渡します。

SDK は、さまざまな BI 機能をアプリケーションに提供するために、組み合わせて使用されます。開発者ガイドや API リファレンスを含むこれら SDK の詳細については、SAP BusinessObjects Business Intelligence プラットフォームの製品ページを参照してください。

3.1.7 データソース

3.1.7.1 ユニバース

ユニバースは、データへのアクセス、操作、および整理にデータ言語ではなくビジネス言語を使用することによって、データの複雑性を取り除くセマンティックレイヤです。 そのビジネス言語は、ユニバースファイルにオブジェクトとして格納されます。 Web Intelligence、Crystal Reports などのアプリケーションは、ユニバースを使用して、単純または複雑なエンドユーザクエリおよび分析に必要なユーザ作成プロセスを簡略化します。

ユニバースは、BI プラットフォームのコアコンポーネントです。 すべてのユニバースオブジェクトと接続は、Connection Server により中央のリポジトリに格納され、セキュリティで保護されます。 ユニバースデザイン用のクライアントツールでは、BI プラットフォームにログインしてシステムにアクセスし、ユニバースを作成する必要があります。 ユニバースアクセスと行/列レベルのセキュリティは、デザイン環境内からグループレベルまたは個々のユーザレベルで管理することもできます。

セマンティックレイヤを使用すると、Web Intelligence では、オンライン分析処理 (OLAP) や共通ウェアハウスメタモデル (CWM) データソースを含む、複数の同期データプロバイダを利用してドキュメントを配信できます。

3.1.7.2 ビジネスビュー

ビジネスビューは、レポート開発者用データの複雑さを取り除くことで、レポート作成操作を簡略化するツールです。ビジネスビューを使用すると、データ接続、データアクセス、ビジネスエレメント、およびアクセス制御を分離できます。

ビジネスビューは Crystal Reports でのみ使用でき、Crystal レポートの作成に必要なデータアクセスとビュータイムセキュリティを簡略化できます。ビジネスビューは、1 つのビューで複数のデータソースを組み合わせて使用できます。ビジネスビューは、BI プラットフォームで完全にサポートされます。

3.1.8 認証とシングルサインオン

システムのセキュリティは、Central Management Server (CMS)、セキュリティプラグイン、およびサードパーティ製認証ツール (SiteMinder や Kerberos など) によって管理されます。 これらのコンポーネントは、ユーザを認証し、BI プラットフォーム、そのフォルダ、およびその他のオブジェクトに対するユーザアクセスを承認します。

以下のユーザ認証シングルサインオンのセキュリティプラグインを使用できます。

- Enterprise (デフォルト)、SAML、X.509、SAP NW SSO などの認証方式や使用しているアプリケーションサーバでサポートされる他の方式と併用するための信用できる認証のサポートを含みます。
- LDAP
- Windows Active Directory (AD)

Enterprise Resource Planning (ERP) システムを使用中の場合は、シングルサインオンを使用して ERP システムへのユーザアクセスを認証し、ERP データをソースとすることができるようにします。 ERP システムに対しては、以下のユーザ認証シングルサインオンがサポートされています。

- SAP ERP およびビジネスウェアハウス (BW)
- Oracle E-Business Suite (EBS)
- Siebel Enterprise
- JD Edwards Enterprise One
- PeopleSoft Enterprise

3.1.8.1 セキュリティプラグイン

セキュリティプラグインを使用すると、ユーザアカウントとグループをサードパーティシステムから BI プラットフォームにマップできるので、アカウントの作成および管理が自動化されます。サードパーティのユーザアカウントを既存の Enterprise ユーザアカウントにマップしたり、外部システム内のマップされた各エントリに対応する新しい Enterprise ユーザアカウントを作成できます。

セキュリティプラグインは、サードパーティのユーザとグループのリストを動的に管理します。そのため、Lightweight Directory Access Protocol (LDAP) または Windows Active Directory (AD) グループを BI プラットフォームにマップすると、そのグループに属するすべてのユーザが BI プラットフォームにログインできるようになります。サードパーティグループのメンバーシップの後続変更は自動的に反映されます。

BI プラットフォームは、次のセキュリティプラグインをサポートします。

- Enterprise セキュリティプラグイン
  Central Management Server (CMS) は、ユーザアカウント、グループメンバーシップ、オブジェクトアクセス権 (ユーザとグループのアクセス権の定義) などのセキュリティ情報を処理します。この処理は、Enterprise 認証と呼ばれます。
  Enterprise 認証は常に有効で、無効にすることはできません。BI プラットフォームに使用する専用のアカウントおよびグループを作成する場合、または LDAP または Windows AD サーバにユーザとグループの階層をまだ設定していない場合は、デフォルトの Enterprise 認証を使用します。
  信用できる認証とは、Java Authentication and Authorization Service (JAAS) などの、サードパーティのシングルサインオンソリューションと統合する Enterprise 認証のコンポーネントです。Central Management Server と信用を確立したアプリケーションでは、信用できる認証を使用してユーザがパスワードを指定せずにログオンできます。
- LDAP セキュリティプラグイン
- Windows AD

> ⓘ 注記
>
> ユーザは、CMC を介して BI プラットフォームおよびカスタムアプリケーション向けに Windows AD 認証を設定できますが、CMC および BI ラウンチパッドは、Windows AD 認証と NTLM の併用はサポートしていません。CMC および BI ラウンチパッドがサポートしている認証方法は、Windows AD と Kerberos の併用、LDAP 認証、Enterprise 認証、および信用できる認証です。

3.1.8.2 企業資源計画 (ERP) 統合

企業資源計画 (ERP) アプリケーションは、日常業務に関連するリアルタイムな情報を収集することにより、組織のプロセスに不可欠な機能をサポートします。 BI プラットフォームでは、以下の ERP システムからのシングルサインオンとレポーティングをサポートします。

- SAP ERP およびビジネスウェアハウス (BW)
- Siebel Enterprise
- Oracle E-Business Suite
- JD Edwards EnterpriseOne
- PeopleSoft Enterprise

> ⓘ 注記
>
> - SAP ERP および BW サポートはデフォルトでインストールされます。 SAP ERP または BW のサポートが不要の場合は、カスタム/拡張インストールオプションを使用して、SAP 統合サポートを選択解除します。
> - デフォルトでは、Siebel Enterprise、Oracle E-Business Suite、JD Edwards EnterpriseOne または PeopleSoft のサポートはインストールされません。 SAP 以外の ERP システムの統合を選択してインストールするには、[カスタム/拡張] インストールオプションを使用します。

BI プラットフォームでサポートされている特定のバージョンの詳細については、https://support.sap.com/home.html で入手可能なサポートプラットフォーム/*PAR* を参照してください。

ERP 統合を設定する場合は、このガイドの *ERP* 環境の追加設定の章を参照してください。

3.1.9 SAP 統合

BI プラットフォームは、既存の SAP インフラストラクチャと以下の SAP ツールを統合します。

- SAP システムランドスケープディレクトリ (SLD)
  SAP NetWeaver のシステムランドスケープディレクトリは、ソフトウェアライフサイクルの管理に関連するシステムランドスケープ情報のセントラルソースです。SAP から入手できるすべてのインストール可能なソフトウェアに関する情報およびランドスケープにすでにインストールされているシステムに関する自動更新済みデータで構成されるディレクトリを提供することによって、ツールサポートのファンデーションを取得し、システムランドスケープでソフトウェアライフサイクルのタスクを計画します。
  BI プラットフォームのインストールプログラムによって、SLD のベンダ、製品名およびバージョン、ならびにサーバとフロントエンドのコンポーネント名、バージョンおよびロケーションが登録されます。
- SAP Solution Manager
  SAP Solution Manager は、組織の SAP および非 SAP ソリューションの実装、サポート、操作、およびモニタリングに使用する、統合されたコンテンツ、ツール、および方法を提供するプラットフォームです。
  SAP Certified Integration の認定を受けた非 SAP ソフトウェアは、セントラルリポジトリに配置されてから、ユーザの SAP システムランドスケープディレクトリ (SLD) に自動的に転送されます。SAP カスタマは、SAP システム環境において、SAP が認定しているサードパーティ製品統合のバージョンを簡単に特定することができます。このサービスにより、サードパーティ製品のオンラインカタログにないサードパーティ製品についても知ることができます。
  SAP カスタマは、追加料金を支払わずに、SAP Solution Manager を使用することができます。SAP Solution Manager には、SAP サポートへのダイレクトアクセス、SAP 製品のアップグレードパス情報などがあります。SLD の詳細については、「“システムランドスケープでの BI プラットフォームの登録”」に関する項目を参照してください。
- 移送/修正システム (CTS+)
  CTS は、ABAP ワークベンチおよびカスタマイジングで開発プロジェクトを整理し、システムランドスケープで SAP システム間の変更を移送する際に有用です。ABAP オブジェクトと同様に、Java オブジェクト (J2EE、JEE) と SAP 固有の非 ABAP テクノロジー (Web Dynpro Java または SAP NetWeaver Portal など) もランドスケープで移送することができます。
- CA Wily Introscope を使用したモニタリング
  CA Wily Introscope は、カスタム Java アプリケーションへの表示およびバックエンドシステムへの接続を含む、本稼動の Java ベース SAP モジュール内で発生する可能性のあるパフォーマンスの問題をモニタし、診断する機能を提供する Web アプリケーションの管理製品です。CA Wily Introscope を使用すると、個々のサーブレット、JSP、EJB、JCO、クラス、メソッドなどを含む NetWeaver モジュールのパフォーマンスボトルネ

ックを分離することができます。CA Wily Introscope では、リアルタイム、低オーバーヘッドモニタリング、エンドツーエンドトランザクション表示、分析または能力計画の履歴データ、カスタマイズ可能なダッシュボード、自動しきい値アラーム、NetWeaver 環境以外のモニタリングを拡張するオープンアーキテクチャが提供されます。

3.1.10 統合バージョン管理

サーバシステムで BI プラットフォームを構成するファイルは、バージョン管理で保存されています。インストールプログラムによって、SubVersion のバージョン管理システムが、インストールおよび設定されます。または、詳細を入力して、既存の SubVersion または ClearCase のバージョン管理システムを使用することができます。

バージョン管理システムを使用すると、さまざまなバージョンの設定と他のファイルを保存したり復元したりすることができます。つまり、常に、過去の任意の時点の状態にシステムを戻すことができます。

3.2 サーバ、サービス、ノード、およびホスト

BI プラットフォームでは、サーバおよびサービスという用語を使用して、BI プラットフォームコンピュータで実行される 2 種類のソフトウェアを表します。

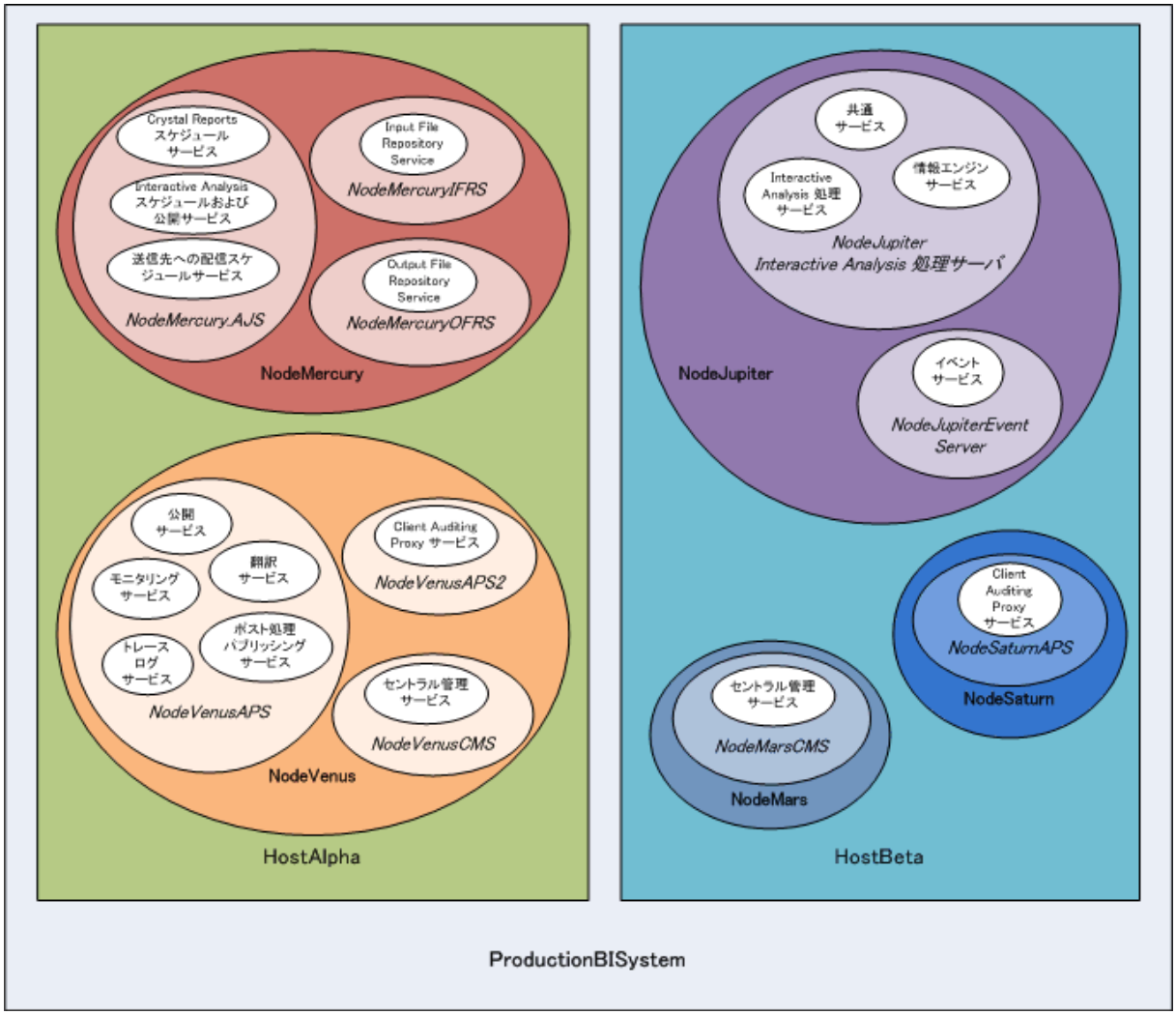
“server” という用語は、1 つ以上のサービスをホストするオペレーティングシステムレベルのプロセスを表します (一部のシステムでは、daemon と呼ばれます)。たとえば、Central Management Server (CMS) と Adaptive Processing Server はサーバです。サーバは、特定のオペレーティングシステムアカウントで実行され、独自のプロセス ID (PID) を持ちます。

サービスは、特定の機能を実行するサーバサブシステムです。サービスは、親コンテナ (サーバ) のプロセス ID を使用して、そのサーバのメモリスペース内で実行されます。たとえば、Web Intelligence スケジュールサービスは、Adaptive Job Server 内で実行されるサブシステムです。

ノードは、同じホストで実行され、同じ Server Intelligence Agent (SIA) で管理される、BI プラットフォームサーバのコレクションです。1 つまたは複数のノードを 1 つのホストに置くことができます。

BI プラットフォームは、1 台のコンピュータにインストールするか、イントラネット上で複数のコンピュータに分散するか、広域ネットワーク (WAN) を介して分散することができます。

次の図は、架空の BI プラットフォームのインストール例です。ホスト、ノード、サーバ、サービスの数、およびサーバとサービスの種類は、実際のインストールによって異なります。



ProductionBISystem というクラスタが、次の 2 つのホストによって形成されています。

- HostAlpha という名前のホストには BI プラットフォームがインストールされ、次の 2 つのノードが設定されています。
  - `NodeMercury` には、レポートをスケジュールおよび公開するサービスを含む Adaptive Job Server (`NodeMercury.AJS`)、入力レポートを格納するサービスを含む Input File Repository Server (`NodeMercury.IFRS`)、およびレポート出力を格納するサービスを含む Output File Repository Server (NodeMercury.OFRS) が含まれます。
  - `NodeVenus` には、公開、監視、翻訳機能を提供するサービスを含む Adaptive Processing Server (`NodeVenus.APS`)、クライアント監査を提供するサービスを含む Adaptive Processing Server (`NodeVenus.APS2`)、および CMS サービスを提供するサービスを含む Central Management Server (NodeVenus.CMS) が含まれます。
- HostBeta という名前のホストには BI プラットフォームがインストールされ、次の 3 つのノードが設定されています。
  - NodeMars: CMS サービスを提供するサービスを含む Central Management Server (`NodeMars.CMS`) が含まれます。CMS を 2 つのコンピュータで実行すると、負荷が均衡および軽減され、フェイルオーバーが可能になります。

- NodeJupiter には、Web Intelligence レポーティングを提供するサービスを含む Web Intelligence Processing Server (`NodeJupiter.Web Intelligence`)、およびファイルのレポート監視を提供する Event Server (`NodeJupiter.EventServer`) が含まれます。
- `NodeSaturn` には、クライアント監査を提供するサービスを含む Adaptive Processing Server (NodeSaturn.APS) が含まれます。

3.2.1 XI 3.1 からのサーバの変更点

以下の表に、XI 3.1 からの BI プラットフォームサーバの主な変更点について示します。次のような種類の変更が実施されています。

- バージョン間で名前が変更されたサーバ (機能が同じまたは類似)
- 新しいバージョンでの提供が終了したサーバ
- Adaptive Server に統合された共通サービスまたは関連サービス
  たとえば、XI 3.1 で個々の Job Server が提供していたスケジュールサービスは、4.0 から Adaptive Job Server に移行されました。
- 新しく導入されたサーバ

サーバの変更点

XI 3.1	4.0	4.0 Feature Pack 3	4.1	4.2	4.3
Connection Server [1]	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server Connection Server 32
Crystal Reports Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Crystal Reports Processing Server	Crystal Reports 2011 Processing Server Crystal Reports Processing Server (SAP Crystal Reports for Enterprise レポート向け)	Crystal Reports 2011 Processing Server Crystal Reports Processing Server (SAP Crystal Reports for Enterprise レポート向け)	Crystal Reports 2013 Processing Server Crystal Reports Processing Server (SAP Crystal Reports for Enterprise レポート向け)	Crystal Reports 2016 Processing Server Crystal Reports Processing Server (SAP Crystal Reports for Enterprise レポート向け)	Crystal Reports 2020 Processing Server Crystal Reports Processing Server (SAP Crystal Reports for Enterprise レポート向け)
Dashboard Server (Dashboard Builder) [2]	Dashboard Server (BI ワークスペース)	4.0 Feature Pack 3 以降は利用不可	4.1 では利用不可	4.2 では利用不可	4.3 では利用不可
Dashboard Analytics Server (Dashboard Builder) [2]	Dashboard Analytics Server (BI ワークスペース)	4.0 Feature Pack 3 以降は利用不可	4.1 では利用不可	4.2 では利用不可	4.3 では利用不可

XI 3.1	4.0	4.0 Feature Pack 3	4.1	4.2	4.3
Desktop Intelligence Cache Server [3]	4.0 以降は利用不可	4.0 以降は利用不可	4.1 では利用不可 [3]	4.2 では利用不可 [3]	4.3 では利用不可 [3]
Desktop Intelligence Job Server [3]	4.0 以降は利用不可	4.0 以降は利用不可	4.1 では利用不可 [3]	4.2 では利用不可 [3]	4.3 では利用不可 [3]
Desktop Intelligence Processing Server [3]	4.0 以降は利用不可	4.0 以降は利用不可	4.1 では利用不可 [3]	4.2 では利用不可 [3]	4.3 では利用不可 [3]
Destination Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Multi-Dimensional Analysis Services	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server
Program Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2013 Report Application Server (RAS)	Crystal Reports 2016 Report Application Server (RAS)	Crystal Reports 2020 Report Application Server (RAS)
Web Intelligence Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Xcelsius Cache Server [4]	Dashboard Design Cache Server (Xcelsius) [5]	Dashboards Cache Server (Xcelsius)	Dashboards Cache Server (Xcelsius)	Dashboards Cache Server (Xcelsius)	4.3 では利用不可 [7]
Xcelsius Processing Server [4]	Dashboard Design Processing Server (Xcelsius) [5]	Dashboards Processing Server (Xcelsius)	Dashboards Processing Server (Xcelsius)	Dashboards Processing Server (Xcelsius)	4.3 では利用不可 [7]
コンテンツ固有の Web パーツ [6]	Crystal レポートビューア、Xcelsius ビューア、およびアナリティカルレポートビューア	Crystal レポートビューア、Xcelsius ビューア、およびアナリティカルレポートビューア	Crystal レポートビューア、Xcelsius ビューア、およびアナリティカルレポートビューア	Crystal レポートビューア、Xcelsius ビューア、およびアナリティカルレポートビューア	コンテンツ固有の Web パーツは 4.3 で非推奨になります。

- [1] 4.0 では、Connection Server 32 は 32 ビットであり、特に 64 ビットのミドルウェアをサポートしていないデータソースに対する接続を実行します。Connection Server は 64 ビットであり、その他のすべてのデータソースに対する接続を実行します。詳細については、データアクセスガイドを参照してください。
- [2] Dashboard Server および Dashboard Analytics Server は、4.0 Feature Pack 3 からは削除されました。サーバ設定は、BI ワークスペース機能 (以前の XI 3.1 での Dashboard Builder) で必要なくなりました。

- [3] Desktop Intelligence は、バージョン 4.0 および 4.0 メンテナンスパックでは利用できませんでした。Desktop Intelligence クライアントアプリケーションはバージョン 4.1 で利用できますが、Desktop Intelligence サーバは利用できません。Desktop Intelligence レポートはレポート変換ツールを使用して Web Intelligence ドキュメントに変換できます。
- [4] Xcelsius キャッシュサービスおよび処理サービスは、Xcelsius からリレーショナルデータソースの Query as a Web Service 要求を最適化するために、XI 3.1 Service Pack 3 に導入されました。同様のキャッシュサービスおよび処理サービスは、4.0 Feature Pack 3 で導入された Dashboards Cache Server と Dashboards Processing Server で利用できます。
- [5] 4.0 の Dashboard Design サーバは、4.0 Feature Pack 3 では SAP BusinessObjects Dashboards への製品名の変更と整合をとるため、名前が "Dashboards" に変更されました。
- [6] 以下のコンテンツ固有の Web パーツは 4.3 で非推奨になります。
  - Crystal レポートビューア
  - Xcelsius ビューア
  - アナリティカルレポートビューア
- [7] Dashboards Processing Server (Xcelsius) と Dashboards Cache Server (Xcelsius) の両方が非推奨になります。

3.2.2 サービス

サーバを追加する際には、Adaptive Job Server の一部のサービスを含める必要があります。たとえば、送信先への配信スケジュールサービスなどがあります。

> ⓘ 注記
>
> - 今後のメンテナンスリリースで新しいサービスまたはサーバタイプが追加される可能性があります。
> - サンプル Java スケジュールサービスは、内部開発を目的としてのみ使用され、外部関係者には使用可能になりません。

サービス	サービスカテゴリ	サーバタイプ	サービスの説明
Adaptive Connectivity サービス	接続サービス	Adaptive Processing Server	Java ベースのドライバ用の接続サービスを提供します
Analytics Hub サービス	コアサービス	Adaptive Processing Server	このサービスは、Adaptive Processing Server で実行され、SAP Analytics Cloud および SAP Analytics Hub システムと通信します。
認証更新スケジュールサービス	コアサービス	Adaptive Job Server	サードパーティセキュリティのプラグインに対する更新の同期を提供します
BEx Web アプリケーションサービス	Analysis サービス	Adaptive Processing Server	SAP Business Warehouse (BW) Business Explorer (BEx) Web アプリケーションと BI ラウンチパッドの統合を提供します

サービス	サービスカテゴリ	サーバタイプ	サービスの説明
BIMobileService (OCA)	コアサービス	Adaptive Processing Server	モバイルデバイスでのプッシュ通知を可能にします。
Web アプリケーションコンテナサービス	コアサービス	Web アプリケーションコンテナサーバ	WACS 向けの Web アプリケーションを提供します。これには、セントラル管理コンソール (CMC)、BI 起動パッド、および OpenDocument が含まれます
セントラル管理サービス	コアサービス	Central Management Server	サーバ、ユーザ、セッションの管理、およびセキュリティ (アクセス権および認証) の管理を提供します。クラスタを運用するには、クラスタ内で少なくとも 1 つのセントラル管理サービスが使用可能になっている必要があります。
クライアント監査プロキシサービス	コアサービス	Adaptive Processing Server	クライアントから送信された監査イベントを収集し、CMS サーバに転送します
Commentary サービス	コアサービス	Adaptive Processing Server	ドキュメントで操作のコメントを作成できます。
Crystal Reports 2020 処理サービス	Crystal Reports サービス	Crystal Reports Processing Server	Crystal Reports 2020 レポートを受け入れて処理します。レポート間でデータを共有し、データベースへのアクセス数を削減できます
Crystal Reports 2020 スケジュールサービス	Crystal Reports サービス	Adaptive Job Server	スケジュールされた従来の Crystal Reports のジョブを実行し、出力場所に結果を公開します
Crystal Reports 2020 表示および変更サービス	Crystal Reports サービス	Report Application Server (RAS)	Crystal Reports 2020 レポートに対する表示要求および変更要求を処理します。
Crystal Reports キャッシュサービス	Crystal Reports サービス	Crystal Reports Cache Server	レポートのキャッシュを管理することで、Crystal レポートからのデータベースへのアクセス数を制限し、レポート作成を高速化します
Crystal Reports 処理サービス	Crystal Reports サービス	Crystal Reports Processing Server	Crystal レポートを受け入れて処理します。レポート間でデータを共有し、データベースへのアクセス数を削減できます

サービス	サービスカテゴリ	サーバタイプ	サービスの説明
Crystal Reports スケジュールサービス	Crystal Reports サービス	Adaptive Job Server	スケジュールされた新しい Crystal Reports のジョブを実行し、出力場所に結果を公開します
カスタムデータアクセスサービス	Web Intelligence サービス	Adaptive Processing Server	Connection Server が不要なデータソースへの動的接続を提供します。このサービスでは、CSV ファイルなどの個人用データプロバイダを使用して作成したレポートへのアクセスおよびレポートの更新を行うことができます。テキストファイルベースのクエリの構築やドキュメントの更新の詳細については、*SAP BusinessObjects Web Intelligence* リッチクライアントユーザガイドを参照してください。
データフェデレーションサービス	データフェデレーションサービス	Adaptive Processing Server	マルチソースユニバースの基となるデータソースをクエリして処理します
送信先への配信スケジュールサービス	コアサービス	Adaptive Job Server	スケジュールされたジョブを実行して、結果を出力場所 (ファイルシステム、FTP サーバ、SFTP サーバ、電子メール、ユーザの受信ボックスなど) に公開します **注記** サーバを追加する際には、一部の Adaptive Job Server サービス (このサービスなど) を含める必要があります。
ドキュメント回復サービス	Web Intelligence サービス	Adaptive Processing Server	Web Intelligence ドキュメントの自動保存および回復
DSL ブリッジサービス	Web Intelligence サービス	Adaptive Processing Server	ディメンションセマンティックレイヤ (DSL) セッションのサポート
イベントサービス	コアサービス	Event Server	File Repository Server (FRS) でファイルイベントをモニタリングし、必要なときにレポートの実行をトリガします

サービス	サービスカテゴリ	サーバタイプ	サービスの説明
Excel データアクセスサービス	Web Intelligence サービス	Adaptive Processing Server	BI プラットフォームにアップロードされた Excel ファイルをデータソースとしてサポートします。Excel ファイルベースのクエリの構築やドキュメントの更新の詳細については、*SAP BusinessObjects Web Intelligence* リッチクライアントユーザガイドを参照してください。
情報エンジンサービス	Web Intelligence サービス	Web Intelligence Processing Server	Web Intelligence ドキュメントの処理に必要なサービス
インプットファイルストアサービス	コアサービス	Input File Repository Server	公開されたレポートと、入力ファイルを受け取ったときに新しいレポートの作成に使用できるプログラムオブジェクトを管理します
Insight to Action サービス	コアサービス	Adaptive Processing Server	呼び出されたアクションを有効化して、RRI のサポートを提供します
プロモーションマネジメント ClearCase サービス	プロモーションマネジメントサービス	Adaptive Processing Server	LCM のための ClearCase サポートを提供します
プロモーションマネジメントスケジュールサービス	プロモーションマネジメントサービス	Adaptive Job Server	スケジュールされたプロモーションマネジメントジョブを実行します
プロモーションマネジメントサービス	プロモーションマネジメントサービス	Adaptive Processing Server	プロモーションマネジメントコアサービス
モニタリングサービス	コアサービス	Adaptive Processing Server	監視機能を提供します
Multi-Dimensional Analysis Service	Analysis サービス	Adaptive Processing Server	多次元の Online Analytical Processing (OLAP) データへのアクセスを提供し、未処理データを XML に変換します。データはその後、Excel、PDF、または Analysis (旧 Voyager) のクロスタブおよびチャートに変換できます
ネイティブ接続サービス	接続サービス	Connection Server	64 ビットアーキテクチャ用のネイティブ接続サービスを提供します
ネイティブ接続サービス (32 ビット)	接続サービス	Connection Server	32 ビットアーキテクチャ用のネイティブ接続サービスを提供します
アウトプットファイルストアサービス	コアサービス	Output File Repository Server	完了したドキュメントのコレクションを管理します

サービス	サービスカテゴリ	サーバタイプ	サービスの説明
プラットフォーム検索スケジュールサービス	コアサービス	Adaptive Job Server	スケジュールされた検索を実行し、Central Management Server (CMS) リポジトリ内のすべてのコンテンツをインデックス化します
プラットフォーム検索サービス	コアサービス	Adaptive Processing Server	BI プラットフォームに対する検索機能を提供します
プローブスケジュールサービス	コアサービス	Adaptive Job Server	スケジュールされたプローブジョブを提供し、出力場所に結果を公開します
プログラムスケジュールサービス	コアサービス	Adaptive Job Server	指定した時間に実行するようにスケジュールされたプログラムを実行します
パブリケーションスケジュールサービス	コアサービス	Adaptive Job Server	スケジュールされた公開ジョブを実行し、出力場所に結果を公開します
パブリッシングポスト処理サービス	コアサービス	Adaptive Processing Server	レポートの完了後に、レポートを出力場所に送信するなどのアクションを実行します
公開サービス	コアサービス	Adaptive Processing Server	パブリッシングポスト処理サービスおよび宛先ジョブサービスと連携して、レポートを出力場所 (ファイルシステム、FTP サーバ、SFTP サーバ、電子メール、ユーザの受信ボックスなど) に公開します
Rebean サービス	Web Intelligence サービス	Adaptive Processing Server	Web Intelligence および Explorer によって使用される SDK
レプリケーションサービス	コアサービス	Adaptive Job Server	スケジュールされたフェデレーションジョブを実行して、連合されたサイト間でコンテンツの複製を行います
RESTful Web サービス	コアサービス	Web アプリケーションコンテナサーバ (WACS)	RESTful Web サービス要求に対するセッション処理を提供します。
セキュリティクエリスケジュールサービス	コアサービス	Adaptive Job Server	スケジュールされたセキュリティクエリジョブを実行します
セキュリティトークンサービス	コアサービス	Adaptive Processing Server	SAP Single Sign-On のサポート

サービス	サービスカテゴリ	サーバタイプ	サービスの説明
セットマテリアライゼーションサービス	コアサービス	Adaptive Processing Server	セットおよびセットグループのマテリアライゼーションを操作します。
セットマテリアライゼーションスケジューリングサービス	コアサービス	Adaptive Job Server	マテリアライゼーションするセットおよびセットグループをスケジュールできます。
翻訳サービス	コアサービス	Adaptive Processing Server	トランスレーションマネージャクライアントからの入力を使用して InfoObjects を翻訳します
ユーザとグループのインポートスケジュールサービス	コアサービス	Adaptive Job Server	プリンシパルファイルのインポートのスケジュールを許可
Visual Difference スケジュールサービス	プロモーションマネジメントサービス	Adaptive Job Server	スケジュールされた Visual Difference (プロモーションマネジメント) ジョブを実行し、出力場所に結果を公開します
Visual Difference サービス	プロモーションマネジメントサービス	Adaptive Processing Server	ドキュメントの昇格およびプロモーションマネジメントのために、複数のドキュメントが視覚的に同一であるかどうかを判別します
ビジュアライゼーションサービス	Web Intelligence サービス	Adaptive Processing Server	Web Intelligence によって使用される Common Visualization Object Model サービス
Web Intelligence 共通サービス	Web Intelligence サービス	Web Intelligence Processing Server	Web Intelligence ドキュメント処理をサポートします
Web Intelligence コアサービス	Web Intelligence サービス	Web Intelligence Processing Server	Web Intelligence ドキュメント処理をサポートします
Web Intelligence 処理サービス	Web Intelligence サービス	Web Intelligence Processing Server	Web Intelligence ドキュメントを受け入れて処理します
Web Intelligence スケジュールサービス	Web Intelligence サービス	Adaptive Job Server	スケジュールされた Web Intelligence ジョブのサポートを可能にします
バージョン管理サービス	プロモーションマネジメントサービス	Adaptive Processing Server	IBM Rational ClearCase または Apache Subversion を使用する複数のバージョンの BI リソースを管理します。

3.2.3 サービスカテゴリ

> ⓘ 注記
>
> 今後のメンテナンスリリースで新しいサービスまたはサーバタイプが追加される可能性があります。

サービスカテゴリ	サービス	サーバタイプ
Analysis サービス	BEx Web アプリケーションサービス	Adaptive Processing Server
Analysis サービス	Multi-Dimensional Analysis Service	Adaptive Processing Server
接続サービス	Adaptive Connectivity サービス	Adaptive Processing Server
接続サービス	ネイティブ接続サービス	Connection Server
接続サービス	ネイティブ接続サービス (32 ビット)	Connection Server
コアサービス	Analytics Hub サービス	Adaptive Processing Server
コアサービス	認証更新スケジュールサービス	Adaptive Job Server
コアサービス	BIMobileService(OCA)	Adaptive Processing Server
コアサービス	Central Management Service	Central Management Server
コアサービス	Client Auditing Proxy Service	Adaptive Processing Server
コアサービス	Commentary サービス	Adaptive Processing Server
コアサービス	出力先設定サービス*	Adaptive Job Server
コアサービス	送信先への配信スケジュールサービス	Adaptive Job Server
コアサービス	イベントサービス	Event Server
コアサービス	Insight to Action サービス	Adaptive Processing Server
コアサービス	Input Filestore サービス	Input File Repository Server
コアサービス	モニタリングサービス	Adaptive Processing Server
コアサービス	Output Filestore サービス	Output File Repository Server
コアサービス	プラットフォーム検索スケジュールサービス	Adaptive Job Server
コアサービス	プラットフォーム検索サービス	Adaptive Processing Server
コアサービス	プローブスケジュールサービス	Adaptive Job Server
コアサービス	プログラムスケジュールサービス	Adaptive Job Server
コアサービス	パブリケーションスケジュールサービス	Adaptive Job Server
コアサービス	パブリッシングポスト処理サービス	Adaptive Processing Server
コアサービス	公開サービス	Adaptive Processing Server
コアサービス	RESTful Web サービス	Web アプリケーションコンテナサーバ
コアサービス	レプリケーションサービス	Adaptive Job Server
コアサービス	セキュリティクエリスケジュールサービス	Adaptive Job Server

サービスカテゴリ	サービス	サーバタイプ
コアサービス	セキュリティトークンサービス	Adaptive Processing Server
コアサービス	セットマテリアライゼーションサービス	Adaptive Processing Server
コアサービス	セットマテリアライゼーションスケジュールサービス	Adaptive Processing Server
コアサービス	シングルサインオンサービス[シングルサインオンサービス]	Central Management Server、Connection Server、Crystal Reports Processing Server、RAS、および Web Intelligence Processing Server
コアサービス	トレースログサービス*	すべてのサーバ
コアサービス	翻訳サービス	Adaptive Processing Server
コアサービス	ユーザとグループのインポートスケジュールサービス*	Adaptive Job Server
コアサービス	Web アプリケーションコンテナサービス*	Web アプリケーションコンテナサーバ
Crystal Reports サービス	Crystal Reports 2020 処理サービス	Crystal Reports Processing Server
Crystal Reports サービス	Crystal Reports 2020 スケジュールサービス	Adaptive Job Server
Crystal Reports サービス	Crystal Reports 2020 Viewing and Modification Service	Report Application Server (RAS)
Crystal Reports サービス	Crystal Reports キャッシュサービス	Crystal Reports Cache Server
Crystal Reports サービス	Crystal Reports 処理サービス	Crystal Reports Processing Server
Crystal Reports サービス	Crystal Reports スケジュールサービス	Adaptive Job Server
データフェデレーションサービス	データフェデレーションサービス	Adaptive Processing Server
ライフサイクルマネジメントサービス	プロモーションマネジメント ClearCase サービス	Adaptive Processing Server
ライフサイクルマネジメントサービス	プロモーションマネジメントスケジュールサービス	Adaptive Job Server
ライフサイクルマネジメントサービス	プロモーションマネジメントサービス	Adaptive Processing Server
ライフサイクルマネジメントサービス	Visual Difference スケジュールサービス	Adaptive Job Server
ライフサイクルマネジメントサービス	Visual Difference サービス	Adaptive Processing Server
Web Intelligence サービス	カスタムデータアクセスサービス	Adaptive Processing Server
Web Intelligence サービス	ドキュメントリカバリサービス	Adaptive Processing Server
Web Intelligence サービス	DSL ブリッジサービス	Adaptive Processing Server
Web Intelligence サービス	Excel データアクセスサービス	Adaptive Processing Server
Web Intelligence サービス	情報エンジンサービス	Web Intelligence Processing Server
Web Intelligence サービス	Rebean サービス	Adaptive Processing Server
Web Intelligence サービス	ビジュアライゼーションサービス	Adaptive Processing Server
Web Intelligence サービス	Web Intelligence 共通サービス	Web Intelligence Processing Server

サービスカテゴリ	サービス	サーバタイプ
Web Intelligence サービス	Web Intelligence コアサービス	Web Intelligence Processing Server
Web Intelligence サービス	Web Intelligence モニタリングサービス *	Adaptive Processing Server
Web Intelligence サービス	Web Intelligence 処理サービス	Web Intelligence Processing Server
Web Intelligence サービス	Web Intelligence スケジュールサービス	Adaptive Job Server
プロモーションマネジメントサービス	バージョン管理サービス	Adaptive Processing Server

3.2.4 サーバタイプ

サービス名の横に付いているアスタリスクは、サービスがセカンダリサービスであることを表しています。一部のセカンダリサービスは自動的に作成されますが、それ以外のセカンダリサービスは、セカンダリサービスが依存するプライマリサービスを選択した後に選択して含める必要があります。

> ⓘ 注記
>
> 今後の保守リリースに新しいサービスまたはサーバタイプを追加することができます。

サーバタイプ	サービス	サービスカテゴリ
すべてのサーバ	トレースログサービス[トレースログサービス]	コアサービス
Adaptive Job Server	認証更新スケジュールサービス	コアサービス
Adaptive Job Server	Crystal Reports 2020 スケジュールサービス	Crystal Reports サービス
Adaptive Job Server	Crystal Reports スケジュールサービス	Crystal Reports サービス
Adaptive Job Server	出力先設定サービス[シュツリョクセッテイサービス]	コアサービス
Adaptive Job Server	送信先への配信スケジュールサービス	コアサービス
Adaptive Job Server	プロモーションマネジメントスケジュールサービス	プロモーションマネジメントサービス
Adaptive Job Server	プラットフォーム検索スケジュールサービス	コアサービス
Adaptive Job Server	プローブスケジュールサービス	コアサービス
Adaptive Job Server	プログラムスケジュールサービス	コアサービス
Adaptive Job Server	パブリケーションスケジュールサービス	コアサービス
Adaptive Job Server	レプリケーションサービス	コアサービス
Adaptive Job Server	セキュリティクエリスケジュールサービス	コアサービス

サーバタイプ	サービス	サービスカテゴリ
Adaptive Job Server	セットマテリアライゼーションスケジューリングサービス	コアサービス
Adaptive Job Server	ユーザとグループのインポートスケジュールサービス[ユーザとグループのインポートスケジュールサービス]	コアサービス
Adaptive Job Server	Visual Difference スケジュールサービス	プロモーションマネジメントサービス
Adaptive Job Server	Web Intelligence スケジュールサービス	Web Intelligence サービス
Adaptive Processing Server	Adaptive Connectivity サービス	接続サービス
Adaptive Processing Server	Analytics Hub サービス	コアサービス
Adaptive Processing Server	BEx Web アプリケーションサービス	Analysis サービス
Adaptive Processing Server	クライアント監査プロキシサービス	コアサービス
Adaptive Processing Server	カスタムデータアクセスサービス	Web Intelligence サービス
Adaptive Processing Server	データフェデレーションサービス	データフェデレーションサービス
Adaptive Processing Server	ドキュメント回復サービス	Web Intelligence サービス
Adaptive Processing Server	DSL ブリッジサービス	Web Intelligence サービス
Adaptive Processing Server	Excel データアクセスサービス	Web Intelligence サービス
Adaptive Processing Server	Insight to Action サービス	コアサービス
Adaptive Processing Server	プロモーションマネジメント ClearCase サービス	プロモーションマネジメントサービス
Adaptive Processing Server	プロモーションマネジメントサービス	プロモーションマネジメントサービス
Adaptive Processing Server	モニタリングサービス	コアサービス
Adaptive Processing Server	Multi-Dimensional Analysis Service	Analysis サービス
Adaptive Processing Server	プラットフォーム検索サービス	コアサービス
Adaptive Processing Server	パブリッシングポスト処理サービス	コアサービス
Adaptive Processing Server	公開サービス	コアサービス
Adaptive Processing Server	Rebean サービス	Web Intelligence サービス
Adaptive Processing Server	セキュリティトークンサービス	コアサービス
Adaptive Processing Server	セットマテリアライゼーションサービス	コアサービス
Adaptive Processing Server	翻訳サービス	コアサービス
Adaptive Processing Server	Visual Difference サービス	プロモーションマネジメントサービス
Adaptive Processing Server	ビジュアライゼーションサービス	Web Intelligence サービス
Adaptive Processing Server	Web Intelligence モニタリングサービス [webintelligence モニタリングサービス]	Web Intelligence サービス
Central Management Server	セントラル管理サービス	コアサービス
Central Management Server	シングルサインオンサービス[シングルサインオンサービス]	コアサービス

サーバタイプ	サービス	サービスカテゴリ
Connection Server	ネイティブ接続サービス	接続サービス
Connection Server	ネイティブ接続サービス (32 ビット)	接続サービス
Connection Server	シングルサインオンサービス *	コアサービス
Crystal Reports Cache Server	Crystal Reports キャッシュサービス	Crystal Reports サービス
Crystal Reports Processing Server	Crystal Reports 2020 処理サービス	Crystal Reports サービス
Crystal Reports Processing Server	Crystal Reports 処理サービス	Crystal Reports サービス
Crystal Reports Processing Server	シングルサインオンサービス *	コアサービス
Event Server	イベントサービス	コアサービス
Input File Repository Server	インプットファイルストアサービス	コアサービス
Output File Repository Server	アウトプットファイルストアサービス	コアサービス
Report Application Server (RAS)	Crystal Reports 2020 表示および変更サービス	Crystal Reports サービス
RAS	シングルサインオンサービス *	コアサービス
Web アプリケーションコンテナサーバ	RESTful Web サービス	コアサービス
Web アプリケーションコンテナサーバ	Web アプリケーションコンテナサービス[web アプリケーションコンテナサービス]	コアサービス
Web Intelligence Processing Server	情報エンジンサービス	Web Intelligence サービス
Web Intelligence Processing Server	シングルサインオンサービス *	コアサービス
Web Intelligence Processing Server	Web Intelligence 共通サービス	Web Intelligence サービス
Web Intelligence Processing Server	Web Intelligence コアサービス	Web Intelligence サービス
Web Intelligence Processing Server	Web Intelligence 処理サービス	Web Intelligence サービス

サーバタイプ	サービス	サービスカテゴリ
Adaptive Job Server	認証更新スケジュールサービス	コアサービス
Adaptive Job Server	Crystal Reports 2020 スケジュールサービス	Crystal Reports サービス
Adaptive Job Server	Crystal Reports スケジュールサービス	Crystal Reports サービス
Adaptive Job Server	送信先への配信スケジュールサービス	コアサービス
Adaptive Job Server	プロモーションマネジメントスケジュールサービス	プロモーションマネジメントサービス
Adaptive Job Server	プラットフォーム検索スケジュールサービス	コアサービス
Adaptive Job Server	プローブスケジュールサービス	コアサービス
Adaptive Job Server	プログラムスケジュールサービス	コアサービス
Adaptive Job Server	パブリケーションスケジュールサービス	コアサービス
Adaptive Job Server	レプリケーションサービス	コアサービス

サーバタイプ	サービス	サービスカテゴリ
Adaptive Job Server	セキュリティクエリスケジュールサービス	コアサービス
Adaptive Job Server	Visual Difference スケジュールサービス	プロモーションマネジメントサービス
Adaptive Job Server	Web Intelligence スケジュールサービス	Web Intelligence サービス
Adaptive Processing Server	Adaptive Connectivity サービス	接続サービス
Adaptive Processing Server	BEx Web アプリケーションサービス	Analysis サービス
Adaptive Processing Server	クライアント監査プロキシサービス	コアサービス
Adaptive Processing Server	カスタムデータアクセスサービス	Web Intelligence サービス
Adaptive Processing Server	データフェデレーションサービス	データフェデレーションサービス
Adaptive Processing Server	ドキュメント回復サービス	Web Intelligence サービス
Adaptive Processing Server	DSL ブリッジサービス	Web Intelligence サービス
Adaptive Processing Server	Excel データアクセスサービス	Web Intelligence サービス
Adaptive Processing Server	Insight to Action サービス	コアサービス
Adaptive Processing Server	プロモーションマネジメント ClearCase サービス	プロモーションマネジメントサービス
Adaptive Processing Server	プロモーションマネジメントサービス	プロモーションマネジメントサービス
Adaptive Processing Server	モニタリングサービス	コアサービス
Adaptive Processing Server	Multi-Dimensional Analysis Service	Analysis サービス
Adaptive Processing Server	プラットフォーム検索サービス	コアサービス
Adaptive Processing Server	パブリッシングポスト処理サービス	コアサービス
Adaptive Processing Server	公開サービス	コアサービス
Adaptive Processing Server	Rebean サービス	Web Intelligence サービス
Adaptive Processing Server	セキュリティトークンサービス	コアサービス
Adaptive Processing Server	翻訳サービス	コアサービス
Adaptive Processing Server	Visual Difference サービス	プロモーションマネジメントサービス
Adaptive Processing Server	ビジュアライゼーションサービス	Web Intelligence サービス
Central Management Server	セントラル管理サービス	コアサービス
Connection Server	ネイティブ接続サービス	接続サービス
Connection Server	ネイティブ接続サービス (32 ビット)	接続サービス
Crystal Reports Cache Server	Crystal Reports キャッシュサービス	Crystal Reports サービス
Crystal Reports Processing Server	Crystal Reports 2020 処理サービス	Crystal Reports サービス
Crystal Reports Processing Server	Crystal Reports 処理サービス	Crystal Reports サービス
Event Server	イベントサービス	コアサービス
Input File Repository Server	インプットファイルストアサービス	コアサービス
Output File Repository Server	アウトプットファイルストアサービス	コアサービス

サーバタイプ	サービス	サービスカテゴリ
Report Application Server (RAS)	Crystal Reports 2020 表示および変更サービス	Crystal Reports サービス
Web アプリケーションコンテナサーバ	RESTful Web サービス	コアサービス
Web Intelligence Processing Server	情報エンジンサービス	Web Intelligence サービス
Web Intelligence Processing Server	Web Intelligence 共通サービス	Web Intelligence サービス
Web Intelligence Processing Server	Web Intelligence コアサービス	Web Intelligence サービス
Web Intelligence Processing Server	Web Intelligence 処理サービス	Web Intelligence サービス

3.2.5 サーバ

サーバは、ホストの Server Intelligence Agent (SIA) の下で実行されるサービスのコレクションです。サーバのタイプはそのサーバ内で実行されるサービスによって示されます。サーバは、セントラル管理コンソール (CMC) で作成できます。以下の表は、CMC で作成できる各種サーバタイプの一覧です。

サーバ	説明
Adaptive Job Server	スケジュールされたジョブを処理する汎用サーバ。BI プラットフォームシステムに Job Server を追加すると、Job Server でレポート、ドキュメント、プログラムまたはパブリケーションを処理し、その結果をさまざまな宛先に送信するように設定できます。
Adaptive Processing Server	さまざまなソースからのリクエストを処理するサービスをホストする汎用サーバ ホストシステムごとに 1 つの Automated Process Server (APS) がインストールプログラムによりインストールされます。インストールした機能に応じて、この APS はモニタリングサービス、ライフサイクルマネジメントサービス、多次元分析サービス (MDAS)、公開サービスなど、多くのサービスを提供することができます。 本稼働システムまたはテストシステムでは、追加の APS を作成し、ビジネス要件に合わせて APS を設定するのが最適です。詳細については、システム設定ウィザードの概要 [86 ページ]および本稼働システムの Adaptive Processing Server の設定 [436 ページ]を参照してください。
Central Management Server(CMS)	BI プラットフォームシステム (CMS システムデータベース) および監査済みユーザアクション (監査データストア) に関する情報のデータベースを管理します。すべてのプラットフォームサービスは、CMS によって管理されます。CMS はドキュメントが格納されるシステムファイル、およびユーザ、ユーザグループ、セキュリティレベル (認証および権限を含む)、およびコンテンツに関する情報も制御します。
Connection Server	ソースデータへのデータベースアクセスを提供します。リレーショナルデータベースのほか、OLAP およびその他の形式

サーバ	説明
	をサポートします。Connection Server は、さまざまなデータソースとの接続および対話を処理し、クライアントに共通の機能セットを提供します。
Crystal Reports Cache Server	クライアントから Page Server へ送信されるレポートリクエストを受信します。Cache Server は、キャッシュされたレポートページでリクエストに応じることができない場合、そのリクエストを Crystal Reports Processing Server に渡し、Crystal Reports Processing Server でレポートが実行され、結果が返されます。次に、Cache Server は、今後の使用に備えてそのレポートページをキャッシュします。
Crystal Reports Processing Server	レポートを処理し、Encapsulated Page Format (EPF) ページを生成して、ページリクエストに応答します。EPF の主な利点は、ページオンデマンドアクセスをサポートして、レポート全体ではなく、リクエストされたページのみ返される点です。これにより、大規模なレポートでのシステムパフォーマンスが大幅に向上し、不要なネットワークトラフィックが削減されます。
Event Server	レポート実行の呼び出しとして機能するイベントをシステムで監視します。イベントの呼び出しを設定すると、Event Server は状況を監視し、イベントが発生したことを CMS に通知します。次に CMS は、イベントの発生時に実行するように設定したジョブを開始します。Event Server は、ストレージ層で発生するファイルベースのイベントを管理します。
File Repository Server	エクスポート済みファイルや、非ネイティブ形式のインポート済みファイルなど、ファイルシステムオブジェクトを作成します。入力 FRS は、管理者またはエンドユーザによってシステムに公開されたレポートオブジェクトおよびプログラムオブジェクトを保存します。出力 FRS には Job Server によって生成されたすべてのレポートインスタンスが格納されます。
Web Intelligence Processing Server	SAP BusinessObjects Web Intelligence ドキュメントを処理します。
Report Application Server	アドホックレポーティング機能があり、ユーザは SAP Crystal Reports Server Embedded ソフトウェア開発キット (SDK) を介して Crystal レポートの作成や編集を行うことができます。

3.3 クライアントアプリケーション

2 つの主なタイプのクライアントアプリケーションを使用して、BI プラットフォームとやりとりすることができます。

- デスクトップ用アプリケーション
  これらのアプリケーションは、サポートされている Microsoft Windows のオペレーティングシステムにインストールする必要があります。これにより、ローカルでのデータ処理とレポート作成が可能になります。

> ⓘ 注記
>
> BI プラットフォームのインストールプログラムでは、デスクトップアプリケーションはインストールされなくなりました。デスクトップアプリケーションをサーバにインストールするには、スタンドアロンの SAP BusinessObjects Business Intelligence プラットフォームクライアントツールのインストールプログラムを使用します。

デスクトップクライアントを使用すると、BI レポート処理を個々のクライアントコンピュータにオフロードできます。多くのデスクトップアプリケーションは、デスクトップにインストールされているドライバを使って組織のデータに直接アクセスし、CORBA または暗号化された CORBA SSL を使用して BI プラットフォームデプロイメントと通信します。
この種類のアプリケーションには、Crystal Reports および Live Office があります。

> ⓘ 注記
>
> Live Office は機能豊富なアプリケーションですが、HTTP を使って BI プラットフォーム Web サービスと連動します。

- Web アプリケーション
  これらのアプリケーションは、Web アプリケーションサーバによってホストされていて、Windows、Macintosh、Unix、および Linux のオペレーティングシステム上でサポートされている Web ブラウザとのアクセスが可能です。
  この方法を使用すると、デスクトップソフトウェア製品を展開しなくても、多くのユーザグループがビジネスインテリジェンス (BI) にアクセスできます。通信は、SLL の暗号化 (HTTPS) に関係なく、HTTP を使って行われます。
  この種類のアプリケーションには、BI 起動パッド、SAP BusinessObjects Web Intelligence、セントラル管理コンソール (CMC)、およびレポートビューアがあります。

3.3.1 SAP BusinessObjects Business Intelligence プラットフォームクライアントツールとともにインストール

3.3.1.1 Web Intelligence リッチクライアント

Web Intelligence リッチクライアントは、BI プラットフォームへのアクセス権を持つビジネスユーザ、またはアクセス権を持たないビジネスユーザ向けの、アドホック分析およびレポーティングツールです。

これにより、使い慣れたビジネス用語をドラッグアンドドロップインタフェースで使用して、ユニバース (.unv および .unx)、BEx クエリ、またはほかのソースからデータにアクセスすることができます。ワークフローを使用して、非常に範囲の広い質問または非常に範囲の狭い質問を分析し、また分析ワークフローの任意のポイントで追加の質問を行うことができます。

Web Intelligence リッチクライアントユーザは、Central Management Server (CMS) に接続できない場合でも、引き続き Web Intelligence ドキュメントファイル (.wid) を処理することができます。

> ⓘ 注記
>
> - Web Intelligence リッチクライアントを BI プラットフォームサーバと同じマシンにインストールすることはお奨めしません。Web Intelligence リッチクライアントと BI プラットフォームサーバには共通するバイナリがあるため、インストール (クライアントまたはサーバ) をアップグレードすると、デプロイメン

トに問題が生じる可能性があります。Web Intelligence リッチクライアントをインストールする場合は、別のマシンにインストールしてください。

- 4.2 からアップグレードする場合は、4.3 バージョンをインストールする前に、前のバージョンを停止して閉じてください。Windows システムトレイを確認してください。リッチクライアントが最小化されている可能性があり、その場合はまだ実行中です。

3.3.1.2 ビジネスビューマネージャ

ビジネスビューマネージャを使用して、基になるデータベースの複雑さを簡略化するセマンティックレイヤオブジェクトを作成することができます。

ビジネスビューマネージャにより、データコネクション、ダイナミックデータコネクション、データファンデーション、ビジネスエレメント、ビジネスビュー、およびリレーショナルビューを作成することができます。これを使用し、レポート内のオブジェクトに対して、詳細な列レベルおよび行レベルのセキュリティを設定することもできます。

デザイナは、複数のデータソースへの接続を作成し、テーブルを結合して、フィールド名のエイリアスを作成し、計算されたフィールドを作成して、この簡略化された構造をビジネスビューとして利用できます。レポート作成者とユーザは、ビジネスビューをレポートの基礎として使用することができ、データから直接独自のクエリを作成する必要はありません。

3.3.1.3 レポート変換ツール

RCT は、BI 4.3 リリースで非推奨になっています。詳細については、2801797 を参照してください。

3.3.1.4 ユニバースデザインツール

データ作成者は、ユニバースデザインツール (旧ユニバースデザイナ) を使用して、データベースの複雑性をエンドユーザから隠すセマンティックレイヤで複数のソースからのデータを結合します。データへのアクセス、操作、および整理に技術言語ではなくビジネス用語を使用することによって、データの複雑性を取り除きます。

ユニバースデザインツールには、データベース内のテーブルを選択および表示するためのグラフィカルインタフェースがあります。データベーステーブルは、スキーマ図内にテーブルシンボルを使って表示されます。データ作成者は、このインタフェースを使用して、テーブルの操作、テーブル間の結合の作成、エイリアステーブルの作成、コンテキストの作成、スキーマ内のループの解決を実行できます。

また、メタデータソースからユニバースを作成することもできます。ユニバースデザインツールは、作成プロセスの最後にユニバースを生成するために使用されます。

3.3.1.5 インフォメーションデザインツール

インフォメーションデザインツール (旧インフォメーションデザイナ) は、デザイナが SAP BusinessObjects ユニバースを作成およびデプロイするために、リレーショナルおよび OLAP ソースからメタデータを抽出、定義、および編集できるようにするメタデータデザイン環境です。

3.3.1.6 トランスレーションマネジメントツール

BI プラットフォームは、複数言語のドキュメントおよびユニバースをサポートします。複数言語ドキュメントには、ローカライズされたユニバースメタデータおよびドキュメントプロンプトが含まれます。ユーザは、たとえば選択した言語の同じユニバースから、レポートを作成できます。

トランスレーションマネジメントツール (旧トランスレーションマネージャ) は、複数言語ユニバースを定義し、CMS リポジトリ内のユニバース、その他レポートおよび分析リソースの翻訳を管理するツールです。

トランスレーションマネジメントツール

- ユニバースまたはドキュメントを複数言語の対象ユーザのために翻訳します。
- ドキュメントのメタデータ言語部分と適切な翻訳を定義します。外部 XLIFF 形式を生成し、XLIFF ファイルをインポートして翻訳済みの情報を取得します。
- 翻訳対象のユニバースまたはドキュメントの構造を一覧表示します。
- ユーザインタフェースを介して、または XLIFF ファイルをエクスポートおよびインポートし、外部翻訳ツールを使用してメタデータを翻訳できるようにします。
- 複数言語ドキュメントを作成します。

3.3.1.7 データフェデレーション管理ツール

データフェデレーション管理ツール (旧 Data Federator) は、データフェデレーションサービスを管理するための使いやすい機能を提供するリッチクライアントアプリケーションです。

BI プラットフォームと緊密に統合されているデータフェデレーションサービスは、異なるデータソースにクエリを分散することにより複数のソースユニバースの利用を可能にし、単一のデータファンデーションを通してデータを連合させることができます。

データフェデレーション管理ツールを使用してデータフェデレーションクエリを最適化し、最大限のパフォーマンスを発揮できるようデータフェデレーションクエリエンジンを微調整できます。

以下を実行するためにデータフェデレーション管理ツールを使用します。

- SQL クエリをテストします。
- 連合されたクエリの各ソースへの分散方法の詳細を規定する最適化計画を視覚化します。
- 最高のパフォーマンスを達成するよう、統計情報を計算し、データフェデレーションサービスを微調整するシステムパラメータを設定します。
- クエリがコネクタレベルの各データソースでどのように実行されるかを制御するプロパティを管理します。
- SQL クエリの実行を監視します。
- 実行されたクエリの履歴を参照する。

3.3.2 SAP BusinessObjects Business Intelligence プラットフォームとともにインストール

3.3.2.1 セントラル設定マネージャ(CCM)

セントラル設定マネージャ (CCM) は、2 つのフォームで提供されるサーバトラブルシューティングおよびノード管理ツールです。Microsoft Windows 環境では、CCM を使用して、そのグラフィカルユーザインタフェース (GUI) またはコマンドラインからローカルサーバとリモートサーバを管理できます。Unix 環境では、CCM シェルスクリプト (`ccm.sh`) を使用してコマンドラインからサーバを管理できます。

CCM がデフォルトで Tomcat Web アプリケーションサーバにバンドルされている場合、CCM を使用して、ノードを作成および設定したり、Web アプリケーションサーバを起動または停止することができます。Windows では、Secure Sockets Layer (SSL) 暗号化などのネットワークパラメータも設定できます。これらのパラメータは、ノード内のすべてのサーバに適用されます。

> ⓘ 注記
>
> サーバ管理タスクの大半は、現在は CCM ではなく CMC で処理されます。現在は、CCM はトラブルシューティングとノードの設定のために使用されます。

3.3.2.2 アップグレードマネジメントツール

UMT は、BI 4.3 リリースで非推奨になります。詳細については、2801797 を参照してください。

3.3.2.3 リポジトリ診断ツール

リポジトリ診断ツール (RDT) を使用すると、Central Management Server (CMS) システムデータベースと File Repository Servers (FRS) のファイルストアの間の不整合をスキャン、診断、および修復できます。

また、修復の状態と実行したアクションも報告します。ファイルシステムとデータベースの間の同期を調べるには、まずホットバックアップを完了した後で RDT を使用する必要があります。また、RDT は修復後、および BI プラットフォームサービスの開始前に使用することもできます。ユーザは、RDT が検出または修復するエラーの数 (それを超えると停止します) を制限できます。

3.3.3 個別入手可能

3.3.3.1 SAP BusinessObjects Analysis, edition for Microsoft Office

SAP BusinessObjects Analysis, edition for Microsoft Office は、Business Explorer (BEx) の上位版として代わりとなるもので、ビジネスアナリストは、多次元の Online Analytical Processing (OLAP) データを展開できます。

アナリストは、ビジネスの疑問に答え、自分の分析結果とワークスペースを分析結果として他のユーザと共有できます。

SAP BusinessObjects Analysis, edition for Microsoft Office で、アナリストは次のことを実行できます。

- データベース管理者の助けを借りることなく、財務システムに蓄えられているトレンド、異常値、詳細を発見する。
- 大小の多次元データセットを効率的に表示しながらビジネスの疑問に回答する。
- 組織にある、あらゆる範囲の OLAP データソースにアクセスし、簡単で直観的なインタフェースで結果を共有する。
- 同じ分析結果内にあるさまざまな OLAP ソースにアクセスし、ビジネスの全体像と、あるトレンドが他に及ぼす相互影響を把握する。
- ビジネスドライバを検索、分析、比較、予測する。
- ビジネスや時間に関する計算を包括的に使用する。

3.3.3.2 SAP Crystal Reports

SAP Crystal Reports ソフトウェアを使用すると、データソースから対話式のレポートを作成できます。

3.3.3.3 SAP Lumira

SAP Lumira は、データを視覚化してデータに関するストーリーを作成するため役立つアプリケーションです。SAP Lumira を使用して、データの加工、編集、書式設定および絞り込みを行い、ビジュアライゼーションを作成してデータをグラフィカルに表示し、ストーリーを使用してビジュアライゼーションを共有できます。

SAP Lumira は、CMC のアプリケーションとしてリストされました。これにより、各ユーザまたはユーザグループに対して SAP Lumira のデータ取得およびコンテンツ共有機能に関連するアクセス権を管理することができます。

> ⓘ 注記
>
> SAP Lumira アプリケーションに関連するすべてのイベントは、監査データベースのクライアント ID なしで登録されます。

3.3.4 Web アプリケーションクライアント

Web アプリケーションクライアントは、Web アプリケーションサーバ上にあり、クライアント Web ブラウザでアクセスされます。Web アプリケーションは、BI プラットフォームのインストール時に自動的にデプロイされます。

Web アプリケーションは、Web ブラウザから容易にアクセスすることができ、組織ネットワークの外部からのユーザアクセスを許可する予定である場合、SSL 暗号化で通信を保護することができます。

付属の WDeploy コマンドラインツールを使用して、初期インストールの後に Java Web アプリケーションを再設定またはデプロイすることもできます。このツールを使用して、Web アプリケーションを 2 つの方法で Web アプリケーションサーバにデプロイすることができます。

1. スタンドアロンモード
   すべての Web アプリケーションリソースが、動的コンテンツと静的コンテンツの両方を処理する Web アプリケーションサーバにデプロイされます。このモードは、小さなインストールに適しています。
2. 分割モード
   Web アプリケーションの静的コンテンツ (HTML、画像、CSS) は専用の Web サーバにデプロイされ、動的コンテンツ (JSP) は Web アプリケーションサーバにデプロイされます。このモードは、Web アプリケーションサーバが静的 Web コンテンツを処理しないことによるメリットがある大きなインストールに適しています。

WDeploy の詳細については、*SAP BusinessObjects Business Intelligence* プラットフォーム *Web* アプリケーションデプロイメントガイドを参照してください。

3.3.4.1 セントラル管理コンソール(CMC)

セントラル管理コンソール (CMC) は Web ベースのツールで、ユーザ管理、コンテンツ管理、サーバ管理などの管理タスクの実行、およびセキュリティの設定に使用できます。CMC は Web ベースのアプリケーションであるため、すべての管理タスクを、Web アプリケーションサーバに接続可能な任意のコンピュータの Web ブラウザで実行できます。

明示的にユーザに権限が付与されている場合を除き、管理設定を変更できるのは Administrators グループのメンバーだけです。ロールは CMC で割り当てることができ、グループ内のユーザの管理、チームのフォルダにあるレポートの管理など、最低限の管理タスクを実行できる権限をユーザに付与することができます。

3.3.4.2 Fiorified BI ラウンチパッド

Fiorified BI ラウンチパッド (旧 InfoView) は、Web ベースのインタフェースです。エンドユーザは BI ラウンチパッドを使用して公開されているビジネスインテリジェンス (BI) レポートの表示、スケジュール、管理を行うことができます。Fiorified BI ラウンチパッドを使用して、レポート、アナリティクス、ダッシュボードなどのあらゆる種類のビジネスインテリジェンスへのアクセス、操作、およびエクスポートを実行できます。

Fiorified BI ラウンチパッドでは、以下を管理できます。

- BI コンテンツの閲覧と検索
- BI コンテンツへのアクセス(作成、編集、および表示)
- BI コンテンツのスケジュールと公開

3.3.4.3 BI ワークスペース

BI ワークスペースのモジュール (データのテンプレート) と BI ワークスペース (1 つ以上のモジュールのデータを表示) を使用して、ビジネスアクティビティおよびパフォーマンスを追跡することができます。モジュールおよび BI ワークスペースは、条件が変更されるたびにビジネスルールを調整する必要のある情報を提供します。BI ワー

クスペースおよびモジュールを管理することにより、主要なビジネスデータを追跡および分析できます。さらに、統合コラボレーションやワークフロー機能によって、グループによる決定や分析もサポートします。BI ワークスペースには、次の機能があります。

- タブベースの参照
- ページの作成: BI ワークスペースおよびモジュールを管理する
- クリック方式の Application Builder
- 詳細なデータ分析のためのモジュール間のコンテンツリンク

> ⓘ 注記
>
> コンテンツリンクは Design Studio 文書ではサポートされていません。

3.3.4.4 SAP BusinessObjects Web Intelligence

SAP BusinessObjects Web Intelligence は、1 つの Web ベース製品のリレーショナルデータソースのクエリ、レポーティングおよび分析機能を提供する Web ベースのツールです。

Web Intelligence では、ドラッグアンドドロップインタフェースを使用してレポートを作成し、アドホッククエリを実行し、データを分析し、レポートの書式設定を行うことができます。Web Intelligence では、基になるデータソースの複雑な部分は表示されません。

レポートは、サポートされている Web ポータル、または Microsoft Office アプリケーションに SAP BusinessObjects Live Office を使用して公開できます。

3.3.4.5 SAP BusinessObjects Analysis, edition for OLAP

SAP BusinessObjects Analysis, edition for OLAP (旧 Voyager) は、多次元データを操作する BI 起動パッドポータルのオンライン分析処理 (OLAP) ツールです。Voyager は、異なる OLAP データソースからの情報を単一のワークスペース内で統合することもできます。サポートされている OLAP プロバイダには、SAP BW、および Microsoft Analysis Services が含まれます。

Analysis OLAP 機能セットは、SAP Crystal Reports (実稼働レポートを作成するために OLAP キューブに直接アクセスする場合) と SAP BusinessObjects Web Intelligence (OLAP データソースに基づいて構築されたユニバースを使用してアドホック分析レポートを行う場合) の要素を組み合わせたものです。Voyager は、包括的な範囲のビジネスおよび時間計算機能を提供し、OLAP データをできる限り簡素化するための時間スライダなどの機能を備えています。

> ⓘ 注記
>
> Analysis, edition for OLAP Web アプリケーションは、Java Web アプリケーションとしてのみ使用できます。.NET に対応しているアプリケーションはありません。

3.3.4.6 SAP BusinessObjects Mobile

SAP BusinessObjects Mobile を使用して、デスクトップクライアントで利用できるビジネスインテリジェンス (BI) レポート、メトリクス、およびリアルタイムデータに、ワイアレスデバイスからリモートでアクセスすることができます。追加のトレーニングを必要としない、使い慣れたレポートの容易なアクセス、ナビゲート、および分析を可能にするため、コンテンツはモバイルデバイス向けに最適化されます。

SAP BusinessObjects Mobile により、経営層や情報を利用する従業員は、最新情報をいつでも入手でき、それに基づいて最適な意思決定を行うことができます。販売スタッフおよび現場スタッフは、必要な場所および必要なタイミングで顧客、製品、および作業オーダーに関する適切な情報を提供できます。

SAP BusinessObjects Mobile は、BlackBerry、Windows Mobile、Symbian など、幅広いモバイルデバイスをサポートします。

SAP BusinessObjects Mobile のインストール、設定、およびデプロイメントについては、*SAP BusinessObjects Mobile* のインストールとデプロイメントガイドを参照してください。SAP BusinessObjects Mobile の使用方法については、*SAP BusinessObjects Mobile* の使用方法を参照してください。

3.4 プロセスのワークフロー

ログイン、レポートのスケジュール、レポートの表示などのタスクが実行されると、システムとサーバとの間で情報フローが相互にやりとりされます。次の節では、BI プラットフォームで行われるプロセスフローのいくつかについて説明します。

視覚的な補助情報を含むその他のプロセスのワークフローを参照するには、SAP BusinessObjects Business Intelligence 4.x プラットフォームの公式の製品チュートリアル (http://scn.sap.com/docs/DOC-8292) を参照してください。

3.4.1 起動と認証

3.4.1.1 BI プラットフォームへのログオン

このワークフローでは、Web ブラウザから BI プラットフォーム Web アプリケーションへのユーザのログオンについて説明します。このワークフローは、BI 起動パッド、セントラル管理コンソール (CMC) などの Web アプリケーションに適用されます。

1. ブラウザ (Web クライアント) は、Web アプリケーションの実行中に、ログインリクエストを Web サーバを経由して Web アプリケーションサーバに送信します。
2. Web アプリケーションサーバは、リクエストがログオンリクエストであることを確認します。Web アプリケーションサーバは、ユーザ名、パスワード、認証の種類を、認証を行うために CMS に送信します。
3. CMS は、適切なデータベースに照らし合わせてユーザ名とパスワードを検証します。この例では Enterprise 認証が使用され、ユーザの認証情報が CMS システムデータベースに対して認証されます。
4. 検証が成功すると、CMS はメモリ内にユーザ用のセッションを作成します。
5. CMS は、検証が成功したことを知らせる応答を Web アプリケーションサーバに送信します。

6. Web アプリケーションサーバは、メモリ内にユーザセッション用のログオントークンを生成します。このセッションの以降の部分で、Web アプリケーションサーバはこのログオントークンを使用して CMS に対してユーザを検証します。Web アプリケーションサーバは、Web クライアントに送信する 次の Web ページを生成します。
7. Web アプリケーションサーバは、その Web ページを Web サーバに送信します。
8. Web サーバは、その Web ページを Web クライアントに送信し、そのページがユーザのブラウザに表示されます。

3.4.1.2 SIA スタートアップ

Server Intelligence Agent (SIA) は、ホストオペレーティングシステムで自動的に開始するように設定することも、セントラル設定マネージャ (CCM) を使用して手動で開始することもできます。

SIA は、管理するサーバに関する情報を Central Management Server (CMS) から取得します。SIA がローカル CMS を使用し、CMS が実行中でない場合、SIA は CMS を開始します。SIA がリモート CMS を使用する場合、SIA は CMS に接続しようとします。

SIA が開始されると、次のイベントシーケンスが実行されます。

1. SIA は、CMS を見つけるためにキャッシュを検索します。
   a. ローカル CMS を開始するように SIA が設定されていて、CMS が実行中でない場合、SIA は CMS を開始し、接続します。
   b. 実行中の CMS (ローカルまたはリモート) を使用するように SIA が設定されている場合、SIA はキャッシュの最初の CMS に接続しようとします。CMS が現在使用可能でない場合、キャッシュの次の CMS に接続しようとします。キャッシュされた CMS のいずれも使用可能でない場合、いずれかが使用可能になるまで SIA は待機します。
2. CMS は、有効であることを確認するために、SIA の ID を確認します。
3. SIA は、正常に CMS に接続すると、管理対象のサーバの一覧をリクエストします。

   > ⓘ 注記
   >
   > SIA には、管理対象のサーバに関する情報は保存されません。SIA によって管理されるサーバが示された設定情報は、CMS システムデータベースに保存されており、開始時に SIA によって CMS から取得されます。

4. CMS は、SIA によって管理されるサーバの一覧について CMS システムデータベースをクエリします。各サーバの設定も取得されます。
5. CMS は、サーバの一覧と設定情報を SIA に返します。
6. 自動的に開始するように設定されたサーバごとに、SIA は適切な設定を使用してサーバを開始し、ステータスをモニタします。SIA によって開始される各サーバは、SIA によって使用される同じ CMS を使用するように設定されます。

   SIA と自動的に開始するように設定されていないサーバは、未開始のままです。

3.4.1.3 SIA シャットダウン

Server Intelligence Agent (SIA) は、ホストのオペレーティングシステムをシャットダウンすると自動的に停止します。また、セントラル設定マネージャ (CCM) から手動で停止することができます。

SIA のシャットダウン時に、次のステップが実行されます。

SIA は、シャットダウン中であることを CMS に通知します。

a. ホストオペレーティングシステムがシャットダウン中であるため、SIA が停止している場合、SIA はそのサーバの停止を要求します。25 秒以内に停止しないサーバは、強制終了されます。
b. SIA をマニュアルで指定している場合、マネージドサーバが既存のジョブの処理を終了するまで SIA は待機します。マネージドサーバでは、新規のジョブは許可されません。すべてのジョブが完了すると、サーバは停止します。すべてのサーバが停止すると、SIA も終了します。

強制シャットダウン中に、SIA はすべてのマネージドサーバに即時停止を指示します。

3.4.2 プログラムオブジェクト

3.4.2.1 プログラムオブジェクトのスケジュールの設定

このワークフローでは、セントラル管理コンソール (CMC) や BI ラウンチパッドなどの Web アプリケーションから、プログラムオブジェクトを将来実行するようにスケジュールする方法を説明します。

1. ユーザは、スケジュールリクエストを Web サーバを経由して Web クライアントから Web アプリケーションサーバに送信します。
2. Web アプリケーションサーバは、リクエストを受信し、リクエストがスケジュールリクエストであることを確認します。Web アプリケーションサーバはスケジュール時刻、データベースログイン値、パラメータ値、出力先、および書式を、指定された Central Management Server (CMS) に送信します。
3. CMS は、オブジェクトをスケジュールするためのアクセス権をユーザが持っていることを確認します。ユーザが適切なアクセス権を持っている場合、CMS は新しいレコードを CMS システムデータベースに追加し、保留中のスケジュールの一覧にインスタンスを追加します。
4. CMS は、スケジュール処理が成功したことを知らせる応答を Web アプリケーションサーバに送信します。
5. Web アプリケーションサーバは、次の HTML ページを生成し、Web サーバを経由して Web クライアントに送信します。

3.4.2.2 スケジュールされたプログラムオブジェクトの実行

このワークフローでは、スケジュールされた時間に実行するスケジュールされたプログラムオブジェクトのプロセスについて説明します。Adaptive Job Server および Input File Repository Server も実行する必要があります。

> **注記**
>
> このワークフローでは、CMS、Adaptive Job Server、および Input File Repository Server を実行する必要があります。

1. Central Management Server (CMS) は CMS システムデータベースをチェックして、その時点で実行されるスケジュール済み SAP Crystal レポートがないか確認します。
2. スケジュールされたジョブ実行時間になると、CMS は Adaptive Job Server で実行中の使用可能なプログラムスケジュールサービスを見つけます。CMS は、ジョブ情報をそのプログラムスケジュールサービスに送信します。
3. プログラムスケジュールサービスは Input File Repository Server (FRS) と通信し、プログラムオブジェクトを取得します。

   > ⓘ 注記
   >
   > この手順では、必要なサーバおよびオブジェクトを探すために CMS との通信も必要になります。

4. プログラムスケジュールサービスは、そのプログラムを起動します。
5. プログラムスケジュールサービスは、ジョブのステータスで CMS を定期的に更新します。現在のステータスは "処理中" です。
6. プログラムスケジュールサービスは、ログファイルを Output FRS に送信します。Output FRS は、プログラムスケジュールサービスにオブジェクトのログファイルを送信することで、オブジェクトが正常にスケジュールされたことを伝えます。

   > ⓘ 注記
   >
   > この手順では、必要なサーバおよびオブジェクトを探すために CMS との通信も必要になります。

7. プログラムスケジュールサービスは、ジョブのステータスで CMS を更新します。現在のステータスは "成功" です。
8. CMS は、そのメモリ内のジョブのステータスを更新してから、インスタンス情報を CMS システムデータベースに書き込みます。

3.4.3 Crystal Reports

3.4.3.1 キャッシュされた SAP Crystal レポートページの表示

このワークフローでは、レポートページがキャッシュサーバにすでに存在している場合に、ユーザが SAP Crystal レポートのページを (たとえば BI 起動パッドのレポートビューアから) リクエストするプロセスについて説明します。このワークフローは、SAP Crystal Reports 2020 と SAP Crystal Reports for Enterprise の両方に適用されます。

> ⓘ 注記
>
> このワークフローでは、CMS および Crystal Reports Cache Server を実行する必要があります。

1. Web クライアントは、URL 形式の表示リクエストを、Web サーバを経由して Web アプリケーションサーバに送信します。
2. Web アプリケーションサーバはリクエストを受信し、それが選択したレポートページを表示するリクエストであることを確認します。Web アプリケーションサーバはレポートを表示するために必要なアクセス権をユーザが持っているか確認するリクエストを Central Management Server (CMS) に送信します。
3. CMS は CMS システムデータベースをチェックして、レポートを表示するために必要なアクセス権をユーザが持っているか確認します。

4. CMS は、レポートを表示するために必要なアクセス権をユーザが持っていることを確認する応答を Web アプリケーションサーバに送信します。
5. Web アプリケーションサーバは、レポートのページ (`.epf` ファイル) を要求するリクエストを Crystal Reports Cache Server に送信します。
6. Crystal Reports Cache Server は、リクエストされた `.epf` ファイルがキャッシュディレクトリ内に存在するかどうかを確認します。この例では、`.epf` ファイルが見つかります。
7. Crystal Reports Cache Server は、リクエストされたページを Web アプリケーションサーバに返します。
8. Web アプリケーションサーバは、ページを Web サーバを経由して Web クライアントに送信し、そこでページがレンダリングされて表示されます。

3.4.3.2 キャッシュされていない SAP Crystal Reports 2020 ページの表示

このワークフローでは、レポートページがキャッシュサーバに存在しない場合に、ユーザが SAP Crystal Reports 2020 レポートのページを (たとえば BI ラウンチパッドのレポートビューアから) リクエストするプロセスについて説明します。

> **注記**
>
> このワークフローでは、CMS、Crystal Reports Cache Server、Crystal Reports 2020 Processing Server、および Output File Repository Server を実行する必要があります。

1. ユーザは、表示リクエストを Web サーバを経由して Web アプリケーションサーバに送信します。
2. Web アプリケーションサーバはリクエストを受信し、選択したレポートページを表示するリクエストであることを確認し、レポートを表示するために必要なアクセス権をユーザが持っているか確認するリクエストを Central Management Server (CMS) に送信します。
3. CMS は CMS システムデータベースをチェックして、レポートを表示するために必要なアクセス権をユーザが持っているか確認します。
4. CMS は、レポートを表示するために必要なアクセス権をユーザが持っていることを確認する応答を Web アプリケーションサーバに送信します。
5. Web アプリケーションサーバは、レポートのページ (`.epf` ファイル) を要求するリクエストを Crystal Reports Cache Server に送信します。
6. Crystal Reports Cache Server は、リクエストされたファイルがキャッシュディレクトリ内に存在するかどうかを確認します。
   この例では、リクエストされた `.epf` ファイルはキャッシュディレクトリにありません。
7. Crystal Reports Cache Server は、リクエストを Crystal Reports 2020 Processing Server に送信します。
8. Crystal Reports 2020 Processing Server は、リクエストされたレポートインスタンスについて Output File Repository Server (FRS) に照会し、Output FRS はリクエストされたレポートインスタンスを Crystal Reports 2020 Processing Server に送信します。

   > **注記**
   >
   > この手順では、必要なサーバおよびオブジェクトを探すために CMS との通信も必要になります。

9. Crystal Reports 2020 Processing Server は、レポートインスタンスを開き、レポートをチェックしてデータが含まれているかどうかを確認します。

Crystal Reports 2020 Processing Server は、レポートにデータが含まれていることを確認し、運用データベースに接続せずに、リクエストされたレポートページの .epf ファイルを作成します。

10. Crystal Reports 2020 Processing Server は、.epf ファイルを Crystal Reports Cache Server に送信します。
11. Crystal Reports Cache Server は、.epf ファイルをキャッシュディレクトリに書き込みます。
12. Crystal Reports Cache Server は、リクエストされたページを Web アプリケーションサーバに送信します。
13. Web アプリケーションサーバは、ページを Web サーバを経由して Web クライアントに送信し、そこでページがレンダリングされて表示されます。

3.4.3.3 オンデマンドでの SAP Crystal Reports 2020 レポートの表示

このワークフローでは、ユーザが最新のデータを参照するために BI ラウンチパッドのレポートビューアなどからオンデマンドで SAP Crystal Reports 2020 レポートページをリクエストするプロセスについて説明します。

> **注記**
>
> このワークフローでは、CMS、Crystal Reports Cache Server、Crystal Reports 2020 Processing Server、および Input File Repository Server を実行する必要があります。

1. ユーザは、表示リクエストを Web サーバを経由して Web アプリケーションサーバに送信します。
2. Web アプリケーションサーバはリクエストを受信し、それが選択したレポートページを表示するリクエストであることを確認します。Web アプリケーションサーバはレポートを表示するために必要なアクセス権をユーザが持っているか確認するリクエストを Central Management Server (CMS) に送信します。
3. CMS は CMS システムデータベースをチェックして、レポートを表示するために必要なアクセス権をユーザが持っているか確認します。
4. CMS は、レポートを表示するために必要なアクセス権をユーザが持っていることを確認する応答を Web アプリケーションサーバに送信します。
5. Web アプリケーションサーバは、レポートのページ (.epf ファイル) を要求するリクエストを Crystal Reports Cache Server に送信します。
6. Crystal Reports Cache Server は、該当のページが存在するかどうかを確認します。レポートが、(別のオンデマンドリクエスト、データベースログイン、パラメータの設定時間内で) オンデマンドレポート共有の要件を満たさない場合、Crystal Reports Cache Server は、Crystal Reports 2020 Processing Server に対してページ生成リクエストを送信します。
7. Crystal Reports 2020 Processing Server は、Input File Repository Server (FRS) に対してレポートオブジェクトを要求します。Input FRS は、オブジェクトのコピーを Crystal Reports 2020 Processing Server に送信します。

   > **注記**
   >
   > この手順では、必要なサーバおよびオブジェクトを探すために CMS との通信も必要になります。

8. Crystal Reports 2020 Processing Server は、そのメモリ内のレポートを開き、レポートにデータが含まれているかどうかを確認します。この例では、レポートオブジェクトにデータがないため、Crystal Reports 2020 Processing Server はデータソースに接続してデータを取得し、レポートを生成します。
9. Crystal Reports 2020 Processing Server は、ページ (.epf ファイル) を Crystal Reports Cache Server に送信します。Crystal Reports Cache Server は、新しい表示リクエストに備えてそのキャッシュディレクトリに .epf ファイルのコピーを保存します。

10. Crystal Reports Cache Server は、ページを Web アプリケーションサーバに送信します。
11. Web アプリケーションサーバは、ページを Web サーバを経由して Web クライアントに送信し、そこでページがレンダリングされて表示されます。

3.4.3.4 SAP Crystal レポートのスケジュールの設定

このワークフローでは、ユーザがセントラル管理コンソール (CMC) や BI 起動パッドなどの Web アプリケーションから、SAP Crystal レポートを将来実行するようにスケジュールするプロセスについて説明します。このワークフローは、SAP Crystal Reports 2020 と SAP Crystal Reports for Enterprise の両方に適用されます。

1. Web クライアントは、URL 形式のスケジュールリクエストを、Web サーバを経由して Web アプリケーションサーバに送信します。
2. Web アプリケーションサーバは、URL リクエストを受信し、リクエストがスケジュールリクエストであることを確認します。Web アプリケーションサーバはスケジュール時刻、データベースログイン値、パラメータ値、出力先、および書式を、指定された Central Management Server (CMS) に送信します。
3. CMS は、オブジェクトをスケジュールするためのアクセス権をユーザが持っていることを確認します。ユーザが適切なアクセス権を持っている場合、CMS は新しいレコードを CMS システムデータベースに追加します。また、CMS はこのインスタンスを保留中のスケジュールの一覧にも追加します。
4. CMS は、スケジュール処理が成功したことを知らせる応答を Web アプリケーションサーバに送信します。
5. Web アプリケーションサーバは、次の HTML ページを生成し、Web サーバを経由して Web クライアントに送信します。

3.4.3.5 スケジュールされた SAP Crystal Reports 2020 レポートの実行

このワークフローでは、スケジュールされた時間に実行するスケジュール済み SAP Crystal Reports 2020 レポートのプロセスについて説明します。

1. Central Management Server (CMS) は CMS システムデータベースをチェックして、その時点で実行されるスケジュール済み SAP Crystal レポートがないか確認します。
2. スケジュールされたジョブ実行時間になると、CMS は各 Adaptive Job Server に設定された [最大ジョブ数] 値に基づいて、Adaptive Job Server で実行中の使用可能な Crystal Reports 2020 スケジュールサービスを検索します。CMS はジョブ情報 (レポート ID、書式、出力先、ログオン情報、パラメータ、および選択式) を、Crystal Reports 2020 スケジュールサービスに送信します。
3. Crystal Reports 2020 スケジュールサービスは、Input File Repository Server (FRS) と通信し、リクエストされたレポート ID に従ってレポートテンプレートを取得します。

   > ⓘ 注記
   >
   > この手順では、必要なサーバおよびオブジェクトを探すために CMS との通信も必要になります。

4. Crystal Reports 2020 スケジュールサービスは、JobChildserver プロセスを開始します。
5. 子プロセス (JobChildserver) は、Input File Repository Server からテンプレートを受信すると、`ProcReport.dll` を開始します。`ProcReport.dll` には、CMS から Crystal Reports 2020 スケジュールサービスに渡されたすべてのパラメータが含まれています。

6. `ProcReport.dll` は、渡されたパラメータに従ってレポートを処理する `crpe32.dll` を開始します。
7. `crpe32.dll` がレポートを処理している間も、レポートに定義されているとおりにデータソースからレコードを受信します。
8. Crystal Reports 2020 スケジュールサービスは、ジョブのステータスで CMS を定期的に更新します。現在のステータスは "処理中" です。
9. レポートが Crystal Reports 2020 スケジュールサービスのメモリにコンパイルされたら、そのレポートを Portable Document Format (PDF) などの別の形式にエクスポートすることもできます。PDF にエクスポートする場合は、`crxfpdf.dll` が使用されます。
10. 保存されたデータを含むレポートが、スケジュールされた場所 (電子メールなど) に送信され、次にそれが Output FRS に送信されます。

> ⓘ 注記
>
> この手順では、必要なサーバおよびオブジェクトを探すために CMS との通信も必要になります。

11. Crystal Reports 2020 スケジュールサービスは、ジョブのステータスで CMS を更新します。現在のステータスは "成功" です。
12. CMS は、そのメモリ内のジョブのステータスを更新してから、インスタンス情報を CMS システムデータベースに書き込みます。

3.4.4 Web Intelligence

3.4.4.1 SAP BusinessObjects Web Intelligence ドキュメントのオンデマンドでの表示

このワークフローでは、ユーザが最新のデータを参照するために BI ラウンチパッドの Web Intelligence レポートビューアなどから SAP BusinessObjects Web Intelligence ドキュメントをオンデマンドで表示するプロセスについて説明します。

1. Web ブラウザは、表示リクエストを Web サーバを経由して Web アプリケーションサーバに送信します。
2. Web アプリケーションサーバはリクエストを受信し、それが Web Intelligence ドキュメントを表示するリクエストであることを確認します。Web アプリケーションサーバはドキュメントを表示するために必要なアクセス権をユーザが持っているか確認するリクエストを Central Management Server (CMS) に送信します。
3. CMS は CMS システムデータベースをチェックして、ドキュメントを表示するために必要なアクセス権をユーザが持っているか確認します。
4. CMS は、ドキュメントを表示するために必要なアクセス権をユーザが持っていることを確認する応答を Web アプリケーションサーバに送信します。
5. Web アプリケーションサーバは、ドキュメントを要求するリクエストを Web Intelligence Processing Server に送信します。
6. Web Intelligence Processing Server は、Input File Repository Server (FRS) に対して、ドキュメントと、そのドキュメントの作成元のユニバースファイルをリクエストします。ユニバースファイルには、行レベルおよび列レベルのセキュリティを含むメタレイヤ情報が含まれます。
7. Input FRS は、ドキュメントのコピーと、そのドキュメントの作成元のユニバースファイルを Web Intelligence Processing Server に送信します。

> ⓘ 注記
>
> この手順では、必要なサーバおよびオブジェクトを探すために CMS との通信も必要になります。

8. Web Intelligence レポートエンジン (Web Intelligence Processing Server に存在) は、メモリ内のドキュメントを開いて `QT.dll` および実行中の Connection Server を起動します。
9. `QT.dll` は SQL を生成、検証、および再生成し、データベースに接続してクエリを実行します。ConnectionServer では SQL を使用してデータベースからデータを取得し、ドキュメントが処理されるレポートエンジンに送ります。
10. Web Intelligence Processing Server は、リクエストされた表示可能なドキュメントページを Web アプリケーションサーバに送信します。
11. Web アプリケーションサーバは、ドキュメントページを Web サーバを経由して Web クライアントに送信し、そこでページがレンダリングされて表示されます。

3.4.4.2 SAP BusinessObjects Web Intelligence ドキュメントのスケジュールの設定

このワークフローでは、ユーザがセントラル管理コンソール (CMC) や BI 起動パッドなどの Web アプリケーションから、SAP BusinessObjects Web Intelligence ドキュメントを将来実行するようにスケジュールするプロセスについて説明します。

1. Web クライアントは、URL 形式のスケジュールリクエストを、Web サーバを経由して Web アプリケーションサーバに送信します。
2. Web アプリケーションサーバは、URL リクエストを受信し、リクエストがスケジュールリクエストであることを確認します。Web アプリケーションサーバはスケジュール時刻、データベースログイン値、パラメータ値、出力先、および書式を、指定された Central Management Server (CMS) に送信します。
3. CMS は、オブジェクトをスケジュールするためのアクセス権をユーザが持っていることを確認します。ユーザが適切なアクセス権を持っている場合、CMS は新しいレコードを CMS システムデータベースに追加します。また、CMS はこのインスタンスを保留中のスケジュールの一覧にも追加します。
4. CMS は、スケジュール処理が成功したことを知らせる応答を Web アプリケーションサーバに送信します。
5. Web アプリケーションサーバは、次の HTML ページを生成し、Web サーバを経由して Web クライアントに送信します。

3.4.4.3 スケジュール済み SAP BusinessObjects Web Intelligence ドキュメントの実行

このワークフローでは、スケジュール済み SAP BusinessObjects Web Intelligence ドキュメントがスケジュールされた時間に実行されるプロセスについて説明します。

1. Central Management Server (CMS) は CMS システムデータベースをチェックして、Web Intelligence ドキュメントを実行するようスケジュールされていないか確認します。
2. スケジュールされた時間になると、CMS は Adaptive Job Server で実行中の使用可能な Web Intelligence スケジュールサービスを見つけます。 CMS はスケジュールリクエストおよびリクエストに関するすべての情報を、Web Intelligence スケジュールサービスに送信します。

3. Web Intelligence スケジュールサービスは、各 Web Intelligence Processing Server に設定された [最大接続数] 値に基づいて使用可能な Web Intelligence Processing Server を見つけます。
4. Web Intelligence Processing Server は、ドキュメントおよびそのドキュメントの基になっているユニバース メタレイヤ ファイルが保存されている Input File Repository Server（FRS）の場所を確認します。 次に、Web Intelligence Processing Server は Input FRS に対してドキュメントを要求します。 Input FRS は、Web Intelligence ドキュメント、およびそのドキュメントの基になっているユニバース ファイルを見つけて、Web Intelligence Processing Server に送信します。

   > ⓘ 注記
   >
   > この手順では、必要なサーバおよびオブジェクトを探すために CMS との通信も必要になります。

5. Web Intelligence ドキュメントは、Web Intelligence Processing Server の一時ディレクトリに保存されます。 Web Intelligence Processing Server がドキュメントをメモリ内に開き、`QT.dll` が、ドキュメントが基づいているユニバースから SQL を生成します。 Web Intelligence Processing Server に含まれている Connection Server ライブラリが、データソースに接続します。 ドキュメントが処理される Web Intelligence Processing Server 内のレポートエンジンに `QT.dll` を通じてクエリデータが返されます。 新しい正常なインスタンスが作成されます。
6. Web Intelligence Processing Server は、ドキュメント インスタンスを Output FRS にアップロードします。

   > ⓘ 注記
   >
   > この手順では、必要なサーバおよびオブジェクトを探すために CMS との通信も必要になります。

7. Web Intelligence Processing Server は、Adaptive Job Server 上の Web Intelligence スケジュールサービスに、ドキュメントの作成が完了したことを伝えます。 ドキュメントが出力先(ファイルシステム、FTP、SFTP、SMTP、または受信ボックス)に配信されるようにスケジュールされている場合、Adaptive Job Server は、Output FRS から処理済みのドキュメントを取得し、指定された出力先に配信します。 これは、この例の内容とは異なります。
8. Web Intelligence スケジュールサービスは、ジョブのステータスで CMS を更新します。
9. CMS は、そのメモリ内のジョブのステータスを更新してから、インスタンス情報を CMS システムデータベースに書き込みます。

3.4.5 分析

3.4.5.1 SAP BusinessObjects Analysis, edition for OLAP ワークスペースの表示

このワークフローでは、ユーザが BI ラウンチパッドから SAP BusinessObjects Analysis, edition for OLAP ワークスペースの表示をリクエストするプロセスについて説明します。

> ⓘ 注記
>
> このワークフローでは、CMS、Adaptive Processing Server (Multi-Dimensional Analysis Service (MDAS) を含む)、および Input File Repository Server を実行する必要があります。

1. Web クライアントは、新しいワークスペースの表示リクエストを Web サーバ経由で Web アプリケーション サーバに送信します。Web クライアントは、DHTML AJAX(Asynchronous JavaScript and XML)テクノロジ

を使用して、Web アプリケーションサーバと通信します。AJAX テクノロジでは部分的なページ更新が可能であるため、新しいリクエストごとに新しいページを表示する必要がありません。

2. Web アプリケーションサーバはリクエストを変換して Central Management Server (CMS) に送信し、ユーザに新しいワークスペースを表示または作成する権限があるかどうかを確認します。
3. CMS は、ユーザの認証情報を CMS システムデータベースから取得します。
4. ユーザがワークスペースを表示または作成できる場合、CMS はそれを Web アプリケーションサーバに通知します。同時に、1 つ以上の使用可能な Multi-Dimensional Analysis Service (MDAS) の一覧も送信します。
5. Web アプリケーションサーバは、使用可能な選択項目の一覧から MDAS を選択し、CORBA リクエストをサービスに送信して、新しいワークスペースを作成するか、既存のワークスペースを最新表示する適切な OLAP サーバを見つけます。
6. MDAS は Input File Repository Server (FRS) と通信して、基になる OLAP データベースとそのデータベースに保存されている初期の OLAP クエリに関する情報を含む適切なワークスペースドキュメントを取得する必要があります。Input FRS は、基になるディレクトリから適切な Analysis ワークスペースを取得し、そのワークスペースを MDAS に返します。
7. MDAS はワークスペースを開き、クエリを作成し、OLAP データベースサーバに送信します。MDAS では、OLAP データソースに対して適切な OLAP データベースクライアントが設定されている必要があります。Web クライアントクエリを適切な OLAP クエリに変換する必要があります。OLAP データベースサーバは、クエリの結果を MDAS に返します。
8. リクエストが作成、表示、印刷、またはエクスポートのどの操作を行うものであるかに応じて、MDAS は結果を事前処理し、Java WAS でよりすばやく表示が完了できるようにします。MDAS は、表示された結果の XML パッケージを Web アプリケーションサーバに返します。
9. Web アプリケーションサーバはワークスペースを表示し、書式設定されたページまたはページの一部を Web サーバ経由で Web クライアントに送信します。Web クライアントには、更新されたページまたは新しくリクエストされたページが表示されます。これは、Java コンポーネントや ActiveX コンポーネントをダウンロードする必要のないゼロクライアントソリューションです。

3.5 SAP Enterprise Portal での Fiori ラウンチパッドとの統合

概要

Fiori ラウンチパッドプラットフォームとの SAP BusinessObjects BI 統合により、SAP Enterprise Portal のエンドユーザは SAP BusinessObjects CMS 上の BI レポートを表示できます。[ユーザメニュー] タブで、エンドユーザは、SAP BusinessObjects CMS 上のフォルダ階層に対応するフォルダ階層を持つ BI レポートにアクセスできます。

前提条件

- Business Intelligence 4.2 SP4
- 接続用の Web ディスパッチャ 7.49
- NetWeaver 7.5 SP7
- Active Directory 認証および Kerberos ベース SSO 設定 (SAP ノート 1631734 を参照)

手順

Fiori ラウンチパッドのコンテンツ管理者と Enterprise Portal 管理者は、SAP BusinessObjects Enterprise を Fiori ラウンチパッドと統合できます。

詳細な設定情報については、SAP NetWeaver 7.5 Portal 文書の SAP BusinessObjects Enterprise の統合を参照してください。

> ⓘ 注記
>
> - BI プラットフォームでは、Fiori ラウンチパッドと SAP Enterprise Portal 間の統合のための OData サービスがサポートされています。
> - BI プラットフォームでは、NetWeaver アプリケーションサーバにおける OData サービスがサポートされます。
> - 統合が成功すると、SAP Enterprise Portal からパブリックフォルダ、個人用フォルダ、および BI 受信ボックスにアクセスすることができます。

4 システム設定ウィザード

4.1 システム設定ウィザードの概要

SAP BusinessObjects Business Intelligence プラットフォームのインストール後、デプロイメントテンプレートの選択や、組織で使用する SAP BusinessObjects 製品の選択などの必要なインストール後設定を実行します。この設定を行い、可能な限り短時間で BI プラットフォームを稼働させるには、[システム設定ウィザード] を実行します。

ウィザードを使用する利点は次のとおりです。

- ウィザードによって、必要な設定ステップの説明およびガイドが提供されます。
- ウィザードを使用すると、システムが間違って設定される可能性が軽減されます。
- ウィザードによって自動的に設定が実行されるため、システム設定を迅速化できます。

デフォルトで、ウィザードはユーザがセントラル管理コンソール (CMC) にログインすると自動的に実行されるように設定されていますが、CMC の [管理] エリアからウィザードを開始することもできます。いつでもウィザードを再実行して設定を調整したり、CMC の [サーバ] 管理ページを使用して、ウィザードで行った設定を含む任意の設定を微調整することができます。

> ⓘ 注記
>
> セキュリティ強化のため、ウィザードにアクセスできるのは Administrators グループのメンバーのみです。

> ⓘ 注記
>
> ウィザードが自動的に実行されないようにするには、“Administrator” ユーザはウィザードの最初のページにある [*CMC の起動時にこのウィザードを表示しない*] チェックボックスを選択します。

> ⓘ 注記
>
> アドオンをインストールしたり、BI プラットフォームデプロイメントにノードを追加したりする予定がある場合は、システム設定ウィザードを実行する前にこれらの手順を実行することをお勧めします。

4.2 使用する製品の指定

組織で使用する製品を指定することで BI プラットフォームサーバの設定を簡単にしたり、組織で使用しない製品用のサーバを停止することでリソースの割り当てを最適化することができます。これを行うには、[製品] ページで製品を選択します。組織で使用する製品を指定すると、ウィザードはすべてのサーバおよびそれらの製品の実行に必要な依存サーバを開始し、BI プラットフォームを起動するとそれらのサーバおよび依存サーバも自動的に起動するように設定します。また、使用しない製品を選択解除することにより、BI プラットフォームの起動にかかる時間およびリソース使用量が改善されます。

たとえば、Crystal Reports 製品を選択すると、BI プラットフォームはすべての Crystal Reports サーバと該当する依存サーバを起動します。

各製品で自動的に起動されるサーバの一覧については、製品名の横にある [?] アイコンをクリックしてください。

ウィザードでは、以下のようにして製品のサーバが設定されます。

- 製品を選択すると、ウィザードの完了時にその製品に属するすべてのサーバとその製品が機能するために必要なその他のサーバ (依存サーバ) が起動します。また、製品を選択すると、その製品のサーバが BI プラットフォームと一緒に自動的に起動するように設定されます。サーバが複数の製品のサービスをホストしている場合、サーバは、それらの製品のいずれかが選択されると起動します。選択していない製品のサービスが起動する場合がありますが、これはそのサービスも、選択されている製品のサービスをホストしているサーバにホストされているためです。
- 製品の選択を解除すると、その製品が使用するサーバが停止します。ただし、そのサーバが現在も選択されている製品のサービス、またはコアサービスカテゴリに属するサービスをホストしている場合を除きます。停止された製品サーバは、BI プラットフォームと一緒に自動起動されないように設定されます。サーバが選択されている製品と選択解除された製品の両方のサービスをホストしている場合、そのサーバは起動したままになります。
- 製品を選択解除したときにその製品に属さないサーバが停止することがありますが、これは選択解除された製品にのみ使用されている依存サービスがあるためです。これらの依存サーバが不要になるため、これによりリソースが解放されます。
- 製品を選択または選択解除するたびに、BI プラットフォームのコアサービスカテゴリに属するサービス (WACS がホストするサービスを除く) をホストするすべてのサーバが自動的に起動します。WACS は現在の状態を維持します。
- 製品を選択解除しても、その製品のファイルがアンインストールまたは削除されるわけではありません。

[製品] ページを開くたびに、このページの製品状態に現在のシステム状態が表示されます。

製品のすべてのサーバが起動している場合は、その製品のチェックボックスが選択されます。製品のすべてのサーバが停止している場合は、チェックボックスがクリアされます。製品の一部のサーバのみが実行されており、他のサーバがその他の状態 (停止など) である場合、[製品] ページには [既存の設定を維持する] チェックボックスが表示され、システムがウィザードを使用せずに設定されたことを示します。ウィザードを使用して設定を変更する場合は、チェックボックスをクリアできます。

> ⓘ 注記
>
> [製品] ページには、クラスタにインストールされているすべての製品が表示されます。たとえば、マシン A に製品 P1 および P2 がインストールされ、マシン B に製品 P2 および P3 がインストールされている場合、[製品] ページには P1、P2、および P3 が表示されます。インストールされていない製品は、[製品] ページに表示されません。

> ⓘ 注記
>
> デプロイメントの単純化のため、このページの設定はクラスタ全体に適用されるようになっており、各ノードで設定を繰り返す必要はありません。

> ⓘ 注記
>
> 設定が以前に CMC で変更されている場合は、設定がウィザードを使用せずに変更されていることを示すメッセージがウィザードに表示されます。既存の設定を保持するか、現在の設定を上書きするかを選択できます。

> ⓘ 注記
>
> ウィザードで行った変更は、[確認] ページの [適用] をクリックするまで適用されません。

変更の操作が終了したら、[次へ] をクリックしてウィザードの次のページに進みます。左側にあるナビゲーションパネルを使用して、すでに使用した任意のページに直接ジャンプすることもできます。

4.3 デプロイメントテンプレートの選択

BI プラットフォームのデフォルトインストールでは、制限されたシステムハードウェア上のデモ環境に適した小規模なデプロイメントが設定されます。ご使用のハードウェアおよび用途 (テストシステムまたは本稼働システムの準備など) に適合するように、[容量] ページから定義済みデプロイメントテンプレートのいずれかを選択してください。これらのテンプレートは、BI プラットフォームシステムを迅速に稼働させ、最初のデプロイメント時間を短縮することを目的としています。

適切なデプロイメントテンプレートを選択することは、初期設定に役立ち、良いスタート地点にはなりますが、これによってシステムのサイズ設定とチューニングを実行する必要がなくなるわけではありません。最適なパフォーマンスを実現するため、サイズ設定に関するガイド (http://www.sap.com/bisizing) を参照して、システムのサイズ設定を行ってください。

適切なデプロイメントテンプレートの選択が重要な理由は以下のとおりです。

- システムの要求処理能力は、ユーザが選択するデプロイメントテンプレートに影響されます。デプロイメントの規模が大きいほど処理能力が向上し、より多くの要求または複雑な要求を処理できます。しかし、デプロイメントの規模が大きくなるほどより多くのシステムリソースが必要になります。
- 大規模なデプロイメントを選択しても、パフォーマンスが向上する保証はありません (特に、十分なハードウェアリソースがない場合)。
- 選択するデプロイメントテンプレートは、ビジネスのニーズおよび使用可能なハードウェアリソースに見合ったものである必要があります。ビジネスニーズに対して小さすぎたり、使用可能なハードウェアリソースに対して大きすぎるデプロイメントテンプレートを選択すると、システムの容量およびパフォーマンスが低下する可能性があります。
- 大規模なデプロイメントテンプレートではより効果的なパーティション分割を行うことができるため、1 つの製品で発生した障害が他の製品に影響する可能性が少なくなります。リソース (RAM) の使用量とパフォーマンスのバランスが取れたテンプレートを選択してください。たとえば、大量の RAM が使用可能である場合は、RAM で可能な最大のデプロイメントテンプレートを選択することをお勧めします。これにより、システムを効果的にパーティション分割できます。

スライダを使用してデプロイメントテンプレートを選択するか、ドロップダウンリストから RAM の容量を選択できます。設定を変更する際には、[*Adaptive Processing Servers の数*] インジケータが変化し、選択しようとしている設定によってシステムがどのように設定されるかを確認できます。

> ⓘ 注記
>
> 選択するデプロイメントテンプレートは Adaptive Processing Servers (APS) にのみ影響します。CMS または Adaptive Job Servers などのその他のサーバは影響を受けません。

> ⓘ 注記
>
> [RAM 必須] は、BI プラットフォームサーバで最低限必要な RAM 容量です。たとえば、RAM が 16 GB のマシンにおいてオペレーティングシステムで 1 GB、データベースサーバで 1 GB、および BI プラットフォームサー

バで 10 GB の RAM を使用している場合、必要な RAM は 12 GB や 16 GB ではなく 10 GB になります。[RAM 必須] の数値は、一般的な値を示したものにすぎません。システムの負荷が大きいときには、より多くの RAM が必要な場合があります。最適なシステムパフォーマンスを実現するには、常にシステムのサイズ設定を行う必要があります。

ⓘ 注記

システム状態が定義済みのデプロイメントテンプレートのいずれかに一致している場合、[容量] ページを開くたびに、ページ上にデプロイメントテンプレートに現在のシステム状態が表示されます。たとえば、CMC を使用して手動で追加の Adaptive Processing Server を作成している場合、現在のシステム状態はデプロイメントテンプレートのいずれにも一致しません。そのため、[容量] ページには、システムがウィザードを使用せずに設定されたことを示す [既存の設定を維持する] チェックボックスが表示されます。複数ノードデプロイメントでは、一部のノードの APS 数がデプロイメントテンプレートと一致しない場合や、ノードごとに APS 数が異なる場合にも [既存の設定を維持する] チェックボックスが表示されます。ウィザードを使用して設定を変更する場合は、チェックボックスをクリアできます。

ⓘ 注記

デプロイメントの単純化のため、選択した APS 設定は各ノードに適用されるようになっており (ノードに APS がインストールされている場合)、ノード数が多くなるほどクラスタの容量が大きくなります。

ⓘ 注記

アドオン (たとえば、Data Services または Analysis Application Design Service (AADS)) は、ウィザードでは管理されません。アドオンで作成されたサービスは、ウィザードによって異なる APS に移動されることはありません。

例

- メインの BI プラットフォームインストールから他のサービスをホストする APS によって AADS がホストされている場合、ウィザードを実行して、デプロイメントテンプレートサイズを XS から M に変更すると、ウィザードは、新しい APS を 7 個作成し、最初の APS に残る AADS サービス以外のすべてのサービスを 7 個の APS に移動します。
- Data Services のアドオンによって、専用の APS が作成されます。ウィザードでは、この専用 APS を変更されません。また、システム内の APS 数のレポート時に、この APS がカウントされることもありません。

DeploymentTemplates.pdf ファイル

ウィザードによるデプロイメントテンプレートの設定に関する詳しい説明については、[容量] ページで [デプロイメントテンプレート] リンクをクリックして、`DeploymentTemplates.pdf` ファイルを開きます。

`DeploymentTemplates.pdf` ファイルにはデプロイメントテンプレートの詳細な説明が記載されています。テンプレートでは、サポートされるユーザ数は指定しません。これは、サポート可能なユーザ数は負荷によって異なるためです。サポートが必要なユーザ数、およびそれに伴う RAM 容量、CPU 要件などを決定するためにはシステムのサイズ設定を行う必要があります。

4.4 データフォルダの場所の指定

[フォルダ] ページを使用して、BI プラットフォームのデータおよびログファイルを保存する場所を指定します。フォルダの場所を指定するか、現在の場所を受け入れることができます。

BI プラットフォームデプロイメントに複数のノードがある場合は、フォルダの場所を定義するのに次の 2 つのオプションを使用できます。

- すべてのノードについて同じフォルダの場所を設定する場合は、[すべてのノードのフォルダの場所は同じです] オプションを選択します。
- クラスタ内のすべてのサーバが同じように設定されていない場合は、インストールパスまたはファイルディレクトリ構造が異なる可能性があります。[ノードでフォルダの場所が異なります] オプションを選択すると、ノードごとに固有のフォルダの場所を設定できます。

ウィザードで [フォルダ] ページを開くたびに、以下のフォルダ名が表示されます。

- すべてのノードのフォルダの値が同一 (つまり、クラスタのすべてのサーバのログフォルダや、クラスタのすべてのサーバのデータフォルダなどが同一) である場合は、[すべてのノードのフォルダの場所は同じです] オプションが選択され、現在のフォルダ名が表示されます。
- 各ノード内の特定のタイプ (ログ、データ、監査、入力ファイルストア、出力ファイルストア) のすべてのフォルダが同一であるがノード間で異なる場合は、[ノードでフォルダの場所が異なります] オプションが選択され、現在のフォルダ名が表示されます。
- 各ノード内の特定のタイプのすべてのフォルダが同一ではなく、ノード間でも異なる場合は、[ノードでフォルダの場所が異なります] オプションが選択され、フォルダ名は空白になります。

フォルダの場所を変更する場合は、ウィザードによってシステムが新しいフォルダを使用するように設定されます。ウィザードでは、監査データフォルダを除き、元のフォルダのコンテンツを新しいフォルダにコピーまたは移動しません。新しいフォルダに正しいコンテンツがまだ含まれていない場合、または元のフォルダにあるデータを移行する必要がある場合は、それらのデータを新しいフォルダに移動またはコピーしてください。

入力ファイルストア、出力ファイルストア、およびデータフォルダについては、新しいフォルダの場所が空である場合は、元のフォルダの場所からファイルを手動でコピーするか、バックアップからファイルを復元する必要があります。ログフォルダの場合は、元のフォルダの場所に存在するログファイルが新しいフォルダに必要な場合にのみファイルをコピーします。

> → ヒント
>
> 新しいフォルダにファイルをコピーまたは復元する場合は、ノードを再起動する前に行ってください。

シナリオ例:

- フォルダの場所を変更する際に元のフォルダにレポートが含まれている場合は、それらのレポートを新しいフォルダにコピーしてノードを再起動しないと BI プラットフォームで使用することはできません。
- 元のフォルダのレポートが壊れているか変更されており、これを以前の良好なバックアップの状態に戻す必要がある場合は、元のフォルダからコンテンツをコピーせずに、バックアップからレポートを取得してそれらを新しいフォルダに配置します。
- データファイルが当初ドライブ文字 X のディスク上にあり、これをオペレーティングシステムのドライブ文字 Y に変更する場合は、データファイルをコピーまたは移動する必要はありません。BI プラットフォームでフォルダの場所を変更するだけで済みます。

フォルダの場所の一部を手動で変更してノード上のサーバ間で異なるフォルダを使用するようにしている場合、[フォルダ] ページには [既存の設定を維持する] チェックボックスが表示され、システムがウィザードを使用せず

に設定されたことを示します。たとえば、同じノードの 2 つの File Repository Server が異なるログフォルダパスを使用するように設定することができます。ウィザードを使用して現在の設定を変更する場合は、チェックボックスをクリアできます。

各フォルダに格納されるファイルの種類の詳細については、[?] アイコンをクリックしてください。

> ⓘ 注記
>
> 以下のいずれかのフォルダの場所を変更する場合は、ウィザードの完了後、変更内容を有効化するためにすべてのノードを手動で再起動する必要があります。
>
> - 入力ファイルストア
> - 出力ファイルストア
> - ログフォルダ
> - データフォルダ

4.5 変更の確認

設定の選択の終了後、BI プラットフォームシステムに変更が適用される前に、それらの設定が確認用に [確認] ページに表示されます。設定のカテゴリごとに、[詳細] をクリックして、適用される設定および変更の詳細説明または一覧を確認できます。

設定を変更する場合は、ウィザードの左側にあるナビゲーションメニューから個別のページに直接アクセスできます。

選択内容はログファイルに保存され、[完了] ページからダウンロードできます。

また、応答ファイルも生成され保存されます。応答ファイルはシステム設定を自動化するのに役立ちます。[ダウンロード] ボタンをクリックして、応答ファイルを表示したり、ローカルディスクにダウンロードしたりすることができます。

[適用] をクリックすると、設定が BI プラットフォームデプロイメントに適用されます。ウィザードが完了すると、[完了] ページが開き、手動で実行する必要がある次のステップが表示されます。

関連情報

ログファイルおよび応答ファイル [91 ページ]

4.6 ログファイルおよび応答ファイル

[完了] ページでは変更のステータスを確認したり、セッションのログおよび応答ファイルをダウンロードして表示することができます。

ログファイルおよび応答ファイルはシステム設定ウィザードフォルダに自動的に保存され、CMC からアクセスすることができます。ファイル名にはタイムスタンプが year_month_day_hour_minute_second の形式で付けられます。ログファイルは .log 拡張子を使用し、応答ファイルは .ini 拡張子を使用します。

[ダウンロード] ボタンをクリックして、ログおよび応答ファイルを表示したり、それらのファイルをローカルディスクにダウンロードしたりすることもできます。

ログファイルには、以下の内容が含まれます。

- この設定セッションで行ったすべての変更の記録
- 応答ファイルが保存されている場所
- 実行する必要のある次のステップを説明するリスト

関連情報

応答ファイルの使用 [92 ページ]

4.6.1 応答ファイルの使用

ウィザードを完了するたびに、ウィザードのページに表示されたすべての質問の回答 (応答) を含む応答ファイルが保存されます。応答ファイルを使用して、BI プラットフォームデプロイメントの他のクラスタの設定をウィザードを繰り返し実行せずに行うことができます。また、システムを同じ設定状態に設定するために後日に使用することもできます。応答ファイルを使用することで、デプロイメントを自動化し、ユーザによる操作エラーを避けることができます。

応答ファイルを使用するには、応答ファイルをパラメータとして取るスクリプトを実行します。最初に、使用する応答ファイルを見つけ、ディスクに保存します。応答ファイルはシステム設定ウィザードフォルダに自動的に保存され、CMC からアクセスすることができます。ファイル名には year_month_day_hour_minute_second の形式のタイムスタンプと拡張子 .ini が付けられます。CMC から、応答ファイルを表示してディスクに表示するか、メニューコマンド 整理 > 送信 > ファイルの場所 を使用します。

[確認] ページまたは [完了] ページから応答ファイルを現在のウィザードセッション用にダウンロードして、ディスクに保存することもできます。

応答ファイルを使用する前にその設定を変更する場合は、テキストエディタで応答ファイルを編集できます。詳細については、以下に示す応答ファイルのサンプルを参照してください。

スクリプトの実行

適切な応答ファイルを準備できたら、そのファイルを、ウィザードを実行するスクリプトのコマンドラインパラメータとして使用します。

- Windows の場合は、バッチファイル SCW.bat を実行します。
- Unix の場合は、スクリプトファイル scw.sh を実行します。

バッチファイルおよびスクリプトファイルは、その他のサーバ管理スクリプトの保存場所と同じフォルダにあります。

- Windows の場合: `<installdir>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥scripts`
- Unix の場合: `<installdir>/sap_bobj/enterprise_xi40/linux_x64/scripts`

バッチファイルおよびスクリプトファイルは、以下のコマンドラインパラメータを取ります。

- `-help`: コマンドラインのヘルプを表示します。
- `-r`: 応答ファイルのパスおよび名前を指定します。
- `-cms`: ログインする Central Management Server (CMS) を指定します。このパラメータを省略すると、CMS はデフォルトでローカルマシンおよびデフォルトポート (6400) になります。例: `machine_name:6500`
- `-username`: BI プラットフォームに対する管理権限を付与するアカウントを指定します。このパラメータを省略すると、デフォルトの Administrator アカウントが使用されます。
- `-password`: アカウントのパスワードを指定します。指定しない場合、空のパスワードが使用されます。`-password` パラメータを使用するには、`-username` パラメータも使用する必要があります。

例

Windows の場合: `SCW.bat –r c:¥folder¥filename.ini –cms cmsname:6400 –username "administrator" –password samplepassword`

Unix の場合: `./scw.sh –r /home/folder/filename.ini –cms cmsname:6400 –username "administrator" –password samplepassword`

サンプル応答ファイル

```
# ********************************************
# ***************** Products *****************
# ********************************************
# Keep the existing configuration for products.
# Valid values = true or false.
# "true": the existing product configuration will be preserved.
# "false": the product configuration will be modified according to the
“Products.” settings below.
Products.KeepExistingConfiguration = true
# The “Products.” settings below will be ignored if
Products.KeepExistingConfiguration = true.
# Auto-start the servers for these products.
# Valid values = true or false.
# "true": the product's servers and their dependencies are auto-started with BI
platform.
# "false": the product's servers are not auto-started with BI platform.
# Crystal Reports
Products.crystalreports = true
# Analysis edition for OLAP
Products.olap = true
# Web Intelligence
Products.webintelligence = false
# Dashboards (Xcelsius)
Products.dashboards = false
```

```
# Data Federator
Products.datafederator = true
# Lifecycle Manager
Products.LCM = true
# *******************************************************
# ***************** Deployment Template *****************
# *******************************************************
# Keep the existing configuration for the deployment template.
# Valid values = true or false.
# "true": the existing deployment template configuration will be preserved and
the Capacity.DeploymentTemplate setting below will be ignored.
# "false": the deployment template configuration will be modified according to
the Capacity.DeploymentTemplate setting below.
Capacity.KeepExistingConfiguration = true
# Specify the deployment template for all nodes.
# Valid values = xs, s, m, l, xl.
Capacity.DeploymentTemplate = xs
# *********************************************
# ***************** Folders *****************
# *********************************************
# Keep the existing configuration for folder locations.
# Valid values = true or false.
# "true": the existing folder configuration will be preserved.
# "false": the folder configuration will be modified according to the "Folders."
settings below.
Folders.KeepExistingConfiguration = true
# The “Folders.” settings below will be ignored if
Folders.KeepExistingConfiguration = true.
# ------ All nodes use the same folders ------
# Use this section when you have one node, or when all nodes have the same
folder locations. Otherwise, comment it out.
Folders.InputFileStore = <Path>
Folders.OutputFileStore = <Path>
Folders.Log = <Path>
Folders.Data = <Path>
Folders.Auditing = <Path>
# ------ Nodes use different folders ------
# Use this section when nodes have different folder locations. Otherwise,
comment it out.
# ------ NodeOne ------
# Folders.NodeOne.InputFileStore = <Path>
# Folders.NodeOne.OutputFileStore = <Path>
# Folders.NodeOne.Log = <Path>
# Folders.NodeOne.Data = <Path>
# Folders.NodeOne.Auditing = <Path>
# ------ NodeTwo ------
# Folders.NodeTwo.InputFileStore = <Path>
# Folders.NodeTwo.OutputFileStore = <Path>
# Folders.NodeTwo.Log = <Path>
# Folders.NodeTwo.Data = <Path>
# Folders.NodeTwo.Auditing = <Path>
```

応答ファイルのすべての設定項目を指定する必要があります。以下の場合を除き、どの設定項目も空にすることはできません。

- 複数ノードのデプロイメントを使用している場合は、1 つ以上のノードのフォルダ設定を省略して、それらのノードのフォルダを変更しないようにすることができます。ただし、応答ファイルで指定したノードについては、すべてのフォルダの場所を指定する必要があります。
- `KeepExistingConfiguration` パラメータを `true` に設定している場合は、そのページの残りの設定項目を省略できます。たとえば、`Products.KeepExistingConfiguration = true` の場合、応答ファイルの残りの [製品] 設定項目を省略できます。

応答ファイルに、ターゲットクラスタにインストールされている製品とは異なる製品が含まれている場合があります。このような場合は、以下のように動作します。

- 応答ファイルに、ターゲットクラスタにインストールされている製品の定義が含まれていない場合は、操作が失敗します。
- ターゲットクラスタに存在しない製品の定義が応答ファイルに含まれている場合は、ログファイルに警告メッセージが追加され、その他の製品は適切に設定されます。

> **注記**
>
> 応答ファイルを使用してクラスタを設定した後、ログファイルの「“次のステップ”」セクションに記述されている追加のステップを手動で実行する必要があります。

> **注記**
>
> セキュリティ強化のため、必要なのは (Windows AD、LDAP、SAP ではなく) Enterprise 認証サポートのみです。

> **注記**
>
> ノードの再起動を次にスケジュールされた再起動まで延期する場合は、スケジュールされたシステムダウンタイムの直前にスクリプトを実行します。

5 ライセンスの管理

5.1 ライセンスキーの管理

この節では、BI プラットフォームデプロイメントのライセンスキーを管理する方法について説明します。

関連情報

ライセンス情報を表示する [96 ページ]
ライセンスキーを追加する [96 ページ]
現在のアカウントの利用状況を表示する [97 ページ]

5.1.1 ライセンス情報を表示する

CMC の [ライセンスキー] 管理エリアでは、各キーに関連付けられた同時接続ライセンス、指定ライセンス、およびプロセッサライセンスの数を識別します。

1. CMC の[ライセンスキー]管理エリアを表示します。
2. ライセンスキーを選択します。

   キーに関連付けられた詳細情報が[ライセンスキー情報]エリアに表示されます。ライセンスキーの追加購入については、SAP 営業担当者にお問い合わせください。

関連情報

ライセンスキーを追加する [96 ページ]
現在のアカウントの利用状況を表示する [97 ページ]

5.1.2 ライセンスキーを追加する

製品の評価版からアップグレードする場合、評価版キーを削除してから、新しいライセンスキーまたは製品アクティベーションコードを追加してください。新しいライセンスキーを追加した後、すべてのサーバを再度有効化する必要があります。

> ⓘ 注記
>
> BI プラットフォームのライセンスを組織で実装する方法が変更された結果、新しいライセンスキーを受け取った場合は、整合性を維持するために、以前のライセンスキーをシステムからすべて削除する必要があります。

> ⓘ 注記
>
> SAP BusinessObjects Business Intelligence プラットフォーム 4.2 サポートパッケージ 2 より前のバージョンから、SAP BusinessObjects Business Intelligence プラットフォーム 4.2 サポートパッケージ 2 以降のバージョンにアップデートすると、既存のライセンスは失効したライセンスとして機能します。SAP BusinessObjects Business Intelligence プラットフォーム 4.2 の新しいライセンスキーを生成する必要があります。

1. CMC の[ライセンスキー]管理エリアを表示します。
2. *[キーの追加]*フィールドにキーを入力します。
3. [追加] をクリックします。

キーが一覧に追加されます。

関連情報

ライセンス情報を表示する [96 ページ]
現在のアカウントの利用状況を表示する [97 ページ]

5.1.3 現在のアカウントの利用状況を表示する

1. CMC の[設定]管理エリアを表示します。
2. [グローバルシステムメトリクスの表示]をクリックします。

   このセクションには、現在のライセンス使用状況がその他のジョブメトリクスと共に表示されます。

関連情報

ライセンスキーを追加する [96 ページ]
ライセンス情報を表示する [96 ページ]

6 ユーザとグループの管理

6.1 アカウント管理の概要

アカウント管理とは、ユーザおよびグループの情報の作成、マッピング、変更、および編成に関連するすべてのタスクのことです。セントラル管理コンソール (CMC) 内にある [ユーザとグループ] 管理エリアは、これらのタスクを実行する場所です。

ユーザアカウントとグループを作成した後、オブジェクトを追加し、それらにアクセス権を指定することができます。ユーザはログインすると、BI 起動パッド またはカスタム Web アプリケーションを使用してオブジェクトを表示できます。

6.1.1 ユーザ管理

[ユーザとグループ] 管理エリアでは、ユーザが BI プラットフォームにアクセスするために必要となるすべての項目を指定できます。また、“デフォルトユーザアカウント”に、2 つのデフォルトユーザアカウントを示します。

デフォルトユーザアカウント

アカウント名	説明
Administrator	このユーザは、*Administrators* グループと *Everyone* グループに属します。管理者は、すべての BI プラットフォームアプリケーション (CMC、CCM、公開ウィザード、BI 起動パッドなど) ですべてのタスクを実行できます。
Guest	このユーザは *Everyone* グループに属します。このアカウントはデフォルトで有効で、システムによるパスワードの割り当てはありません。パスワードを割り当てると、BI 起動パッドへのシングルサインオンは無効になります。
SMAdmin	これは、BI プラットフォームコンポーネントへのアクセスに SAP Solution Manager が使用する読み取り専用アカウントです。

ⓘ 注記

オブジェクトの移行に最も適しているのは、Administrators グループに属するメンバー、特に Administrator ユーザアカウント内のメンバーです。オブジェクトを移行するためには、多数の関連オブジェクトも移行する必要がある場合があります。すべてのオブジェクトについて必要となるセキュリティ権限を取得することは、場合によっては委任管理者アカウントでは不可能です。

6.1.2 グループ管理

グループは、同じアカウント権限を共有するユーザの集合で、部署、役職、配属場所などに基づいてグループを作成できます。グループを使用することで、各ユーザアカウントのアクセス権を個別に変更する代わりに、1 か所(1 つのグループ)でユーザのアクセス権を変更できます。また、グループにオブジェクトアクセス権を割り当てることもできます。

[ユーザとグループ]エリアでは、多数のユーザにレポートまたはフォルダへのアクセス権を与えるグループを作成できます。これにより、各ユーザアカウントを個別ではなく 1 箇所で変更できます。また、“デフォルトグループアカウント”に、いくつかのデフォルトグループアカウントを示します。

CMC で使用可能なグループを表示するには、ツリー パネルの[グループ一覧]をクリックします。または、[グループ階層]をクリックして使用可能なすべてのグループを階層構造で一覧表示することもできます。

デフォルトグループアカウント

アカウント名	説明
Administrators	このグループのメンバーは、すべての BI プラットフォームアプリケーション (CMC、CCM、公開ウィザード、および BI 起動パッドなど) ですべてのタスクを実行できます。デフォルトでは、*Administrators* グループには Administrator ユーザのみが含まれます。
Everyone	各ユーザは、*Everyone* グループのメンバーです。
QaaWS グループデザイナ	このグループのメンバーは、Query as a Web Service へのアクセス権を持っています。
レポート変換ツールユーザ	このグループのメンバーは、レポート変換ツールアプリケーションへのアクセス権を持っています。
トランスレータ	このグループのメンバーは、トランスレーションマネージャアプリケーションへのアクセス権を持っています。
Universe Designer のユーザ	このグループに所属するユーザには、[*Universe Designer*]フォルダおよび[接続]フォルダへのアクセスが許可されています。これらのユーザは、Designer アプリケーションへのアクセス権を持つユーザを制御できます。必要に応じて、このグループにユーザを追加してください。デフォルトでは、このグループに所属するユーザはいません。

関連情報

BI プラットフォームでのアクセス権の動作 [121 ページ]
ユーザおよびグループへのアクセスの許可 [110 ページ]

6.1.3 利用可能な認証タイプ

BI プラットフォーム内にユーザアカウントおよびグループを設定する前に、使用する認証タイプを決定します。“認証の種類”に、組織が使用しているセキュリティツールごとに使用可能な認証オプションを示します。

認証の種類

認証の種類	説明
Enterprise	BI プラットフォームを使用するユーザ専用のアカウントおよびグループを作成する場合、または LDAP ディレクトリサーバ、Windows AD サーバのいずれかにユーザとグループの階層をまだ設定していない場合は、デフォルトの Enterprise 認証を使用します。
LDAP	LDAP ディレクトリサーバを設定している場合は、BI プラットフォームの既存の LDAP ユーザアカウントおよびグループを使用できます。LDAP アカウントを BI プラットフォームにマップすると、ユーザは、LDAP ユーザ名とパスワードを使って BI プラットフォームアプリケーションにアクセスできます。これによって BI プラットフォーム内で個々のユーザアカウントとグループアカウントを再作成する必要がなくなります。
Windows AD	BI プラットフォームの既存の Windows AD ユーザアカウントおよびグループを使用できます。AD アカウントを BI プラットフォームにマップすると、ユーザは、AD ユーザ名とパスワードを使って BI プラットフォームアプリケーションにログオンできます。これによって BI プラットフォーム内で個々のユーザアカウントとグループアカウントを再作成する必要がなくなります。
SAP	既存の SAP ロールを BI プラットフォームアカウントにマップすることができます。SAP ロールをマップすると、ユーザは、SAP 認証情報を使用して BI プラットフォームアプリケーションにログオンできます。これによって BI プラットフォーム内で個々のユーザアカウントとグループアカウントを再作成する必要がなくなります。
Oracle EBS	既存の Oracle EBS ロールを BI プラットフォームアカウントにマップすることができます。Oracle EBS ロールをマップすると、ユーザは、Oracle EBS 認証情報を使用して BI プラットフォームアプリケーションにログオンできます。これによって BI プラットフォーム内で個々のユーザアカウントとグループアカウントを再作成する必要がなくなります。
Siebel	既存の Siebel ロールを BI プラットフォームアカウントにマップすることができます。Siebel ロールをマップすると、ユーザは、Siebel 認証情報を使用して BI プラットフォームアプリケーションにログオンできます。これによって BI プラットフォーム内で個々のユーザアカウントとグループアカウントを再作成する必要がなくなります。
PeopleSoft Enterprise	既存の PeopleSoft ロールを BI プラットフォームアカウントにマップすることができます。PeopleSoft ロールをマップすると、ユーザは、PeopleSoft 認証情報を使用して BI プラットフォームアプリケーションにログオンできます。これによって BI プラットフォーム内で個々のユーザアカウントとグループアカウントを再作成する必要がなくなります。
JD Edwards EnterpriseOne	既存の JD Edwards ロールを BI プラットフォームアカウントにマップすることができます。JD Edwards ロールをマップすると、ユーザは、JD Edwards 認証情報を使用して BI プラットフォームアプリケーションにログオンできます。これによって BI プラットフォーム内で個々のユーザアカウントとグループアカウントを再作成する必要がなくなります。

6.2 Enterprise および通常のアカウントの管理

Enterprise 認証は BI プラットフォームのデフォルトの認証方法で、最初にシステムをインストールすると自動的に有効になります。ユーザとグループを追加して管理する場合、そのユーザとグループの情報は BI プラットフォームのデータベース内に保持されます。

> ⓘ 注記
>
> BI プラットフォームの Web セッション中に、BI プラットフォーム以外のページに移動したり Web ブラウザを閉じたりしてログオフしても、Enterprise セッションからはログオフされず、ライセンスは保持されます。Enterprise セッションは、約 24 時間後にタイムアウトします。ユーザの Enterprise セッションを終了し、ライセンスを解放して他のユーザが使用できるようにするには、BI プラットフォームからログアウトする必要があります。

6.2.1 ユーザアカウントを作成する

新しいユーザを作成する場合、ユーザのプロパティを指定し、そのユーザのグループ (複数可) を選択します。

1. CMC の [ユーザとグループ] 管理エリアを表示します。
2. 管理 > 新規 > 新しいユーザ の順にクリックします。
   [新しいユーザ] ダイアログボックスが表示されます。
3. Enterprise ユーザを作成するには、次の手順を実行します。
   a. [認証の種類] の一覧で、[*Enterprise*] を選択します。
   b. アカウント名、フルネーム、電子メールおよび説明を入力します。

      > → ヒント
      >
      > 説明のエリアは、ユーザまたはアカウントに関する補足情報を含める場合に使用します。

   c. Enterprise 認証に対して定義されたパスワード基準に準拠するパスワード情報と設定を指定します。
4. 異なる認証の種類を使用してログオするユーザを作成するには、[認証の種類] 一覧から適切なオプションを選択して、アカウント名を入力します。
5. 次の操作のいずれかを実行して、BI プラットフォーム使用権許諾契約に基づいてユーザアカウントを指定します。
   - このユーザが、同時にアクセスすることが許されるユーザ数を規定する使用権許諾契約に属する場合は、[同時接続ユーザ] を選択します。
   - このユーザが、各ライセンスを特定のユーザに関連付ける使用権許諾に属する場合は、[登録ユーザ] を選択します。登録ユーザライセンスは、接続している他のユーザの数に関係なく、BI プラットフォームへのアクセスを必要とする場合に便利です。

     > ⓘ 注記
     >
     > 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。

> ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。

6. [作成して閉じる] をクリックします。

   ユーザはシステムに追加され、自動的に Everyone グループに追加されます。ユーザに対し、受信ボックスが Enterprise のエイリアスを使用して自動的に作成されます。

これで、グループへのユーザの追加、またはユーザのアクセス権の指定ができます。

6.2.2 ユーザアカウントを変更する

次の手順に従って、ユーザのプロパティまたはグループメンバーシップを変更します。

> ⓘ 注記
>
> 変更の対象となるユーザがログオン中の場合、ユーザはその変更の影響を受けます。

1. CMC の[ユーザとグループ]管理エリアを表示します。
2. プロパティを変更するユーザを選択します。
3. 管理 > プロパティ をクリックします。
   ユーザの[プロパティ]ダイアログボックスが開きます。
4. ユーザのプロパティを変更します。

   最初にアカウントを作成したときに利用できたすべてのオプションの他に、[アカウントを無効にする]チェックボックスをオンにしてアカウントを無効にすることができます。

   > ⓘ 注記
   >
   > ユーザアカウントに対する変更は、そのユーザが次回ログオンしたときに表示されます。

5. [保存して閉じる]をクリックします。

関連情報

既存のユーザの新しいエイリアスを作成する [118 ページ]

6.2.3 ユーザアカウントを削除する

次の手順に従って、ユーザのアカウントを削除します。ユーザがログオンしていた場合、そのアカウントが削除されるとエラーメッセージを受け取ります。ユーザアカウントを削除すると、そのユーザのお気に入りフォルダ、個人用カテゴリ、および受信ボックスも削除されます。

将来、アカウントが再び必要になると思われる場合は、アカウントを削除する代わりに、選択したユーザの [プロパティ] ダイアログボックスで [アカウントを無効にする] チェックボックスをオンにします。

> ⓘ 注記
>
> ユーザアカウントを削除しても、必ずしもユーザが BI プラットフォームに再度ログオンできなくなるわけではありません。ユーザアカウントがサードパーティのシステムに存在し、そのアカウントが BI プラットフォームにマップされるサードパーティのグループに所属する場合、ユーザは依然としてログオンできます。

1. CMC の [ユーザとグループ] 管理エリアを表示します。
2. 削除するユーザを選択します。
3. 管理 > 削除 をクリックします。

   削除の確認ダイアログボックスが表示され、選択したユーザが 1 つ以上のプロジェクトの所有者であるかどうかが通知されます。
4. [*OK*] を選択します。
   ユーザアカウントが削除されます。

関連情報

ユーザアカウントを変更する [102 ページ]
エイリアスを無効化する [120 ページ]

6.2.4 新規グループを作成する

1. CMC の[ユーザとグループ]管理エリアを表示します。
2. 管理 > 新規 > 新規グループ の順にクリックします。
   [新規ユーザグループの作成]ダイアログボックスが開きます。
3. グループ名と説明を入力します。
4. [*OK*]をクリックします。

新しいグループを作成したら、そこにユーザやサブグループを追加したり、その新しいグループがサブグループになるようなグループメンバーシップを設定できます。サブグループで組織に追加のレベルを作成できるため、オブジェクトアクセス権を設定して BI プラットフォームコンテンツへのユーザのアクセスを制御するのに便利です。

6.2.5 グループのプロパティを変更する

設定を変更することによって、グループのプロパティを変更できます。

> ⓘ 注記
>
> グループに所属するユーザが次にログオンしたときに、この変更が有効になります。

1. CMC の[ユーザとグループ]管理エリアで、グループを選択します。

2. 管理 > プロパティ をクリックします。
   [プロパティ]ダイアログボックスが表示されます。
3. グループのプロパティを変更します。

   ナビゲーション一覧からリンクをクリックして、さまざまなダイアログボックスを表示し、それぞれのプロパティを変更できます。

   - グループのタイトルや説明を変更する場合は、[プロパティ]をクリックします。
   - グループに対して主体が持っているアクセス権を変更する場合は、[ユーザセキュリティ]をクリックします。
   - グループメンバーのプロパティ値を変更する場合は、[プロファイル値]をクリックします。
   - グループを別のグループにサブグループとして追加する場合は、[所属するグループ]をクリックします。
4. [保存]をクリックします。

6.2.6 グループメンバーを表示する

次の手順で、指定したグループに所属するユーザを表示できます。

1. CMC の[ユーザとグループ]管理エリアを表示します。
2. ツリー パネルの[グループ階層]を展開します。
3. ツリー パネルでグループを選択します。

   > ⓘ 注記
   >
   > グループ内に多数のユーザがいる場合、またはグループがサードパーティディレクトリにマップされている場合、リストが表示されるのにしばらく時間がかかることがあります。

   グループに所属するユーザのリストが表示されます。

6.2.7 サブグループを追加する

あるグループを別のグループに追加できます。このようにすると、追加したグループはサブグループになります。

> ⓘ 注記
>
> サブグループを追加することは、グループのメンバーシップを指定することに似ています。

1. CMC の[ユーザとグループ]管理エリアで、他のグループにサブグループとして追加するグループを選択します。
2. アクション > グループを結合 をクリックします。
   [グループを結合]ダイアログボックスが表示されます。
3. 最初のグループを追加するグループを[利用可能なグループ]一覧から[送信先グループ]一覧に移動します。
4. [*OK*]をクリックします。

関連情報

グループメンバーシップを指定する [105 ページ]

6.2.8 グループメンバーシップを指定する

あるグループを別のグループのメンバーにすることができます。メンバーになったグループは、サブグループと呼ばれます。サブグループの追加先のグループは親グループです。サブグループは親グループのアクセス権を継承します。

1. CMC の[ユーザとグループ]管理エリアで、他のグループに追加するグループを選択します。
2. ▶ アクション ▶ 所属するグループ ▶をクリックします。
   [所属するグループ]ダイアログボックスが表示されます。
3. [グループを結合]をクリックします。
   [グループを結合]ダイアログボックスが表示されます。
4. 最初のグループを追加するグループを[利用可能なグループ]一覧から[送信先グループ]一覧に移動します。

   親グループに関連付けられたすべてのアクセス権は、作成した新しいグループによって継承されます。
5. [*OK*]をクリックします。
   [所属するグループ]ダイアログボックスに戻ると、親グループの一覧に親グループが表示されます。

6.2.9 グループを削除する

グループが必要でなくなった場合には、グループを削除できます。デフォルトグループである Administrators および Everyone は削除できません。

> ⓘ 注記
>
> 削除されたグループに所属するユーザが次にログオンしたときに、この変更が有効になります。

> ⓘ 注記
>
> 削除されたグループに所属するユーザは、そのグループから継承したすべてのアクセス権を失います。

Windows AD Users グループなどのサードパーティの認証グループを削除するには、CMC の [認証] 管理エリアを使用します。

1. CMC の[ユーザとグループ]管理エリアを表示します。
2. 削除するグループを選択します。
3. ▶ 管理 ▶ 削除 ▶をクリックします。
   削除を確認するダイアログボックスが表示されます。
4. [*OK*]をクリックします。
   グループが削除されます。

6.2.10 ユーザまたはユーザグループを一括して追加する

複数のユーザまたはユーザグループを一括して CMC に追加するのに、CSV (カンマ区切り値) ファイルを使用できます。 適切な形式の CSV ファイルでは、次の例のように、カンマ区切りデータが順に並びます。

```
Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue
```

一括追加処理には、以下の条件が適用されます。

- CSV ファイルにエラーが含まれる行が存在する場合、その行はインポート処理対象から除外されます。
- インポート後の最初の段階では、ユーザアカウントは無効になっています。
- 新しいユーザを作成する際には空のパスワードを使用できます。 ただし、その後既存のユーザに対して更新を行うには、有効な Enterprise 認証パスワードを使用する必要があります。
- アカウントにデータベース認証を追加すると、そのユーザのプロファイルでデータベース認証が有効になります。

> **注記**
>
> デフォルトの管理者グループの一部であるユーザのみが、一括でユーザを追加することができます。 この機能は、委任管理ではサポートされません。

1. CMC の [ユーザとグループ] 管理エリアで、管理 > インポート > ユーザ/グループ/データベース認証 を選択します。

   [ユーザ/グループ/データベース認証のインポート] ダイアログボックスが表示されます。
2. [参照] をクリックして CSV ファイルを選択し、[確認] をクリックします。

   ファイルが処理されます。 ファイルのデータ形式が適切な場合に、[インポート] ボタンがアクティブになります。 データの形式が適切ではない場合、エラーに関する情報が表示されるので、CMC がファイルをインポートできるか検証できるように、そのエラーを解決する必要があります。
3. [インポート] をクリックします。

CMC に、ユーザまたはユーザグループがインポートされます。

追加したユーザまたはユーザグループを確認するには、[ユーザとグループ] 管理エリアで 管理 > インポート > 履歴 を選択します。

6.2.11 Guest アカウントを有効にする

Guest アカウントはデフォルトで無効になっており、このアカウントでは BI プラットフォームにログオンできません。このデフォルト設定によって、BI プラットフォームの匿名シングルサインオン機能も無効になります。したがって、ユーザは有効なユーザ名とパスワードを指定しないと BI ラウンチパッドにアクセスできなくなります。

ユーザが BI ラウンチパッドにアクセスするために自分のアカウントを必要としないようにするには、Guest アカウントを有効にしてください。

1. CMC の[ユーザとグループ]管理エリアを表示します。
2. ナビゲーションパネルで [ユーザ一覧] をクリックします。

3. [*Guest*]を選択します。
4. 管理 > プロパティ をクリックします。
   [プロパティ]ダイアログボックスが表示されます。
5. [アカウントを無効にする]チェックボックスをオフにします。
6. *[保存して閉じる]*をクリックします。

6.2.12 グループへのユーザの追加

ユーザグループを使用すると、管理者は BI ラウンチパッドのタスクを複数のユーザにまとめて実行できます。たとえば、特定のユーザグループに対して基本設定をカスタマイズしたり、パブリケーションをスケジュールすることができます。

次の方法でユーザをグループに追加できます。

- グループを選択し、アクション > グループにメンバーを追加 をクリックします。
- ユーザを選択し、アクション > 所属するグループ をクリックします。
- ユーザを選択し、アクション > グループを結合 をクリックします。

1 人のユーザを複数のユーザグループに追加できます。 ただし、ユーザが 2 つ以上のユーザグループに属している場合、BI ラウンチパッドには、1 つのグループ用の基本設定のみが表示されます。

関連情報

グループメンバーシップを指定する [105 ページ]

6.2.12.1 1 つまたは複数のユーザグループへの 1 人のユーザの追加

1 人のユーザを複数のユーザグループに追加できます。 ただし、BI ラウンチパッドで表示されるのは、1 つのユーザグループの基本設定のみです。

1. CMC のユーザとグループ管理エリアで、グループに追加するユーザを選択します。
2. アクション > グループを結合 をクリックします。

   > ⓘ 注記
   >
   > システムのすべての BI プラットフォームユーザは Everyone グループに属します。

3. グループを結合ダイアログボックスで、ユーザの追加先となるグループを、利用可能なグループ一覧から送信先グループ一覧に移動します。

   > → ヒント
   >
   > 複数のグループを選択するには、`Shift` + `クリック` または `Ctrl` + `クリック` を使用します。

4. *OK* をクリックします。

6.2.12.2 1 つのユーザグループへの 1 人または複数のユーザの追加

複数のユーザを 1 つのユーザグループに追加できます。

ユーザグループに設定された基本設定は、そのグループのすべてのユーザに適用されます。 BI ラウンチパッドには、1 つのユーザグループの基本設定が一度に表示されます。

1. CMC のユーザとグループ管理エリアで、ユーザグループを選択します。
2. アクション > グループにメンバーを追加 を選択します。
3. 追加ダイアログボックスで、ユーザ一覧をクリックします。
   [利用可能なユーザ/グループ]一覧が最新表示されて、システム内のすべてのユーザアカウントが表示されます。
4. 利用可能なユーザ/グループ一覧から選択されたユーザ/グループ一覧に、グループに追加する 1 人または複数のユーザを移動します。

   > → ヒント
   >
   > 複数のユーザを選択するには、`Shift` + `クリック` または `Ctrl` + `クリック` を使用します。 特定のユーザを検索するには、ユーザ名を検索ボックスに入力します。

   > → ヒント
   >
   > システム内のユーザ数が多い場合は、前へおよび次へボタンをクリックして、ユーザの一覧内を移動します。

5. *OK* をクリックします。

6.2.13 パスワード設定を変更する

CMC を使用して、特定ユーザまたはシステムのすべてのユーザのパスワード設定を変更できます。次に示すさまざまな制限は、Enterprise アカウントのみに適用されます。つまり、これらの制限は外部ユーザデータベース (LDAP または Windows AD)にマップしたアカウントには適用されません。ただし、通常は外部システムでも、同じような制限を外部アカウントに設定することができます。

6.2.13.1 ユーザのパスワード設定を変更する

1. CMC の [ユーザとグループ] 管理エリアを表示します。
2. パスワード設定を変更するユーザを選択します。
3. 管理 > プロパティ をクリックします。
   [プロパティ] ダイアログボックスが表示されます。

4. 変更するパスワード設定に関連するチェックボックスをオンまたはオフにします。

   選択可能なオプションは、次のとおりです。

   - パスワードを無期限にする
   - ユーザは次回ログオン時にパスワード変更が必要
   - ユーザはパスワードを変更できない
5. [保存して閉じる] をクリックします。

> ⓘ 注記
>
> ユーザのパスワードを変更するとき、そのユーザは既存のすべてのセッションからログアウトされ、再度ログインするためにホームページに移動されます。

6.2.13.2 一般的なパスワード設定を変更する

> ⓘ 注記
>
> アクティブでないユーザアカウントは、自動では無効化されません。

1. CMC の認証管理エリアを表示します。
2. [*Enterprise*]をダブルクリックします。
   [*Enterprise*] ダイアログボックスが表示されます。
3. 使用する各パスワード設定のチェックボックスをオンにして、必要であれば値を指定します。

   次の表は、各設定に対する最小値および最大値を示します。

   パスワード設定

パスワード設定	デフォルト	最小値	推奨される最大値
少なくとも *N* 文字以上のパスワードを要求する	8 文字	6 文字	255 文字
N 文字を超えることはできません	255 文字	13 文字	255 文字
N 日ごとにパスワードの変更を要求する	30 日	2 日	100 日
最近使用した *N* 個のパスワードの再使用を禁止する	3 個	1 個	100 個
N 分経過するまでパスワードの変更を禁止する	0 分	0 分	100 分
ログオンに *N* 回失敗した後はアカウントを無効にする	10 回	1 回	100 回

パスワード設定	デフォルト	最小値	推奨される最大値
ログオン失敗回数を *N* 分後にリセットする	5 分	1 分後	100 分
N 分後に再びアカウントを有効にする	5 分	0 分	100 分

> **注記**
>
> 下位バージョンの SAP BusinessObjects Business Intelligence プラットフォームを上位バージョンにアップグレードするか、何らかの種類の拡張インストールを実行しようとする場合は、[ログオンに *N* 回失敗した後はアカウントを無効にする] をデフォルト値に設定する必要があります。

> **注記**
>
> 上記のルールは、Enterprise ユーザにのみ適用され、その他すべてのサードパーティ認証タイプには適用されません。

4. [更新] をクリックします。

6.2.14 ユーザおよびグループへのアクセスの許可

ユーザおよびグループへの管理アクセスを他のユーザやグループに許可することができます。管理者権限には、オブジェクトの表示、編集、削除と、オブジェクトインスタンスの表示、削除、一時停止が含まれます。たとえば、トラブルシューティングやシステムメンテナンスの場合、IT 部署にオブジェクトの編集や削除を許可することができます。

関連情報

オブジェクトのアクセスコントロールリストに主体を割り当てる [130 ページ]

6.2.15 ユーザの受信ボックスへのアクセスの制御

ユーザを追加すると、そのユーザ用の受信ボックスが自動的に作成されます。 受信ボックスには、ユーザと同じ名前が付けられます。 デフォルトでは、そのユーザと管理者だけがユーザの受信ボックスへのアクセス権を持ちます。

関連情報

CMC でのオブジェクトのセキュリティ設定の管理 [129 ページ]

6.2.16 Fiorified BI ラウンチパッドのオプションの設定

CMC で、管理者はユーザグループの Fiorified BI ラウンチパッド基本設定を設定できます。

> ⓘ 注記
>
> ユーザが 2 つ以上のユーザグループに属している場合、Fiorified BI ラウンチパッドには、1 つのグループ用に設定された基本設定のみが表示されます。

6.2.16.1 Fiorified BI ラウンチパッドログオン画面の設定

デフォルトでは、BI ラウンチパッドログオン画面には、ユーザ名とパスワードの入力を求めるプロンプトが表示されます。また、CMS 名と認証の種類の入力を求めることもできます。この設定を変更するには、BOE.war ファイルの Fiorified BI ラウンチパッドプロパティを編集する必要があります。

6.2.16.1.1 Fiorified BI ラウンチパッドログオン画面を設定する

Fiorified BI ラウンチパッドのデフォルト設定を変更するには、BOE war ファイルのカスタムプロパティを設定する必要があります。このファイルは、Web アプリケーションサーバをホストするマシン上にデプロイされます。

1. インストールされている BI プラットフォームの次のディレクトリに移動します。

   `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥`

2. テキストエディタで新しいファイルを作成します。
3. 次の名前でファイルを保存します。

   `FioriBI.properties`

4. Fiorified BI ラウンチパッドのログオン画面に認証オプションを含めるには、以下の行を追加します。

   ```
   authentication.visible=true
   ```

5. デフォルト認証タイプを変更するには、以下の行を追加します。

   ```
   authentication.default=<authentication>
   ```

   `<authentication>` を以下のオプションのいずれかに置き換えます。

認証の種類	<authentication> 値
Enterprise	`secEnterprise`
LDAP	`secLDAP`
Windows AD	`secWinAD`
SAP	`secSAPR3`

6. Fiorified BI ラウンチパッドのログオン画面に CMS 名のプロンプトを表示するには、以下の行を追加します。

```
cms.visible=true
```

7. ファイルを保存して閉じます。
8. Web アプリケーションサーバを再起動します。

WDeploy を使用して、Web アプリケーションサーバに `BOE.war` ファイルを再デプロイします。WDeploy の使用の詳細については、*SAP BusinessObjects Business Intelligence* プラットフォーム *Web* アプリケーションデプロイメントガイドを参照してください。

6.2.16.2 CMC でのユーザグループの Fiorified BI ラウンチパッドの基本設定

管理者は、CMC でユーザグループにデフォルトの Fiorified BI ラウンチパッドの基本設定を行います。

ユーザグループ用に管理者が設定した基本設定は、そのグループのすべてのユーザに適用されます。ユーザが 2 つ以上のユーザグループに属している場合、Fiorified BI ラウンチパッドには、1 つのグループ用に設定された基本設定のみが表示されます。

ユーザは Fiorified BI ラウンチバッドで独自の基本設定を設定可能であり、その基本設定はデフォルト値より優先されます(いつでもデフォルトの基本設定に戻すこともできます)。*Fiorified Business Intelligence* ラウンチパッドユーザガイドのページ基本設定セクションを参照してください。

ただし、管理者が CMC で Fiorified BI ラウンチパッドのデフォルトの基本設定を変更すると、そのデフォルト値がユーザ定義の値よりも優先されます。

6.2.16.2.1 ユーザグループの Fiori 対応 BI ラウンチパッド基本設定の設定

1. CMC の [ユーザとグループ管理] エリアに移動します。
2. [グループリスト] で、Fiori 対応 BI ラウンチパッド基本設定を設定するユーザグループを選択します。
3. [*Fiori BI* ラウンチパッド基本設定] を右クリックして選択します。
4. [基本設定が定義されていません] チェックボックスをオフにします。
5. [ホーム] タブをカスタマイズするには、以下のいずれかの操作を実行して、タブで希望のホームページを選択します。

ホームページタブのオプション	アクション
デフォルトの Fiori BI ラウンチパッドホームタブの表示	[デフォルトのホームタブ] を選択します。
特定のホームタブの表示	[ホームタブの選択] を選択して、次のようにします。 1. [ランディングページ] フィールドで、次のランディングページを選択します。 • マイホーム • スケジュール • 受信ボックス • フォルダ • リサイクルビン 2. [ドキュメントの表示形式] フィールドで、[タイルビュー (デフォルト)] または [一覧ビュー] を選択します。 3. [ランディングフィルタ] フィールドで、以下のランディングフィルタを選択します。 • すべて表示 • マイドキュメント • すべてのカテゴリ • お気に入り • 最近の表示 • 最近の実行 [マイフォルダ]、[パブリックフォルダ]、[個人用カテゴリ]、および [会社用カテゴリ] からオブジェクトを選択して、デフォルトのランディングページとして表示することができます。
特定のレポートをホームページとして表示	[レポートの選択] を選択してから、[ドキュメントの参照] をクリックして、[マイフォルダ] または [パブリックフォルダ] からドキュメントを選択します。
カテゴリをホームページとして表示	[カテゴリの選択] を選択してから、[カテゴリの参照] をクリックして、[個人用カテゴリ] または [会社用カテゴリ] からカテゴリを選択します。

6. [ドキュメントタブで表示する列を選択] フィールドで、以下の列の基本設定を選択します。
   - タイプ
   - 最終実行日時
   - インスタンス
   - 説明
   - 作成者
   - 最終更新日時
   - 作成日
   - 場所 (カテゴリ)
   - お気に入り (ホームページ)
   - ステータス (スケジュール)

- インスタンスの日時 (スケジュール)
- フォルダパス

> ⓘ 注記
>
> [タイプ]、[説明]、[最終更新日時]、[お気に入り (ホームページ)]、[ステータス (スケジュール)]、および [インスタンスの日時 (スケジュール)] の列は、デフォルトで選択されています。表示する列の選択は変更することができます。

7. [保存して閉じる] を選択します。

管理者によって定義された基本設定がインタフェースに反映されるように、ユーザは Fiori 対応 BI ラウンチパッドにログオンして、設定 > アカウント基本設定 > ページ基本設定 を選択して、[管理者が指定した設定を使用] を有効化する必要があります。

6.2.17 システムユーザの属性の管理

*BI プラットフォーム*の管理者は、セントラル管理コンソール (CMC) の [ユーザ属性管理] エリアでユーザ属性を定義し、システムユーザに対して追加します。次のユーザディレクトリの属性を管理および拡張できます。

- Enterprise
- SAP
- LDAP
- Windows AD

ユーザが SAP、LDAP、Windows AD などの外部ディレクトリからインポートされている場合、そのユーザアカウントでは一般的に次の属性を使用できます。

- フルネーム
- 電子メールアドレス

属性名

システムに追加したすべてのユーザ属性に次のプロパティが含まれている必要があります。

- 名前
- 内部名

“名前”プロパティは、属性のわかりやすい識別子であり、ユニバースのセマンティックレイヤを扱うときにフィルタをクエリするために使用されます。詳細については、ユニバースデザインツールのマニュアルを参照してください。“内部名”は、BI プラットフォーム SDK を扱う開発者によって使用されます。このプロパティは、自動的に生成された名前です。

属性名は 256 文字以下にする必要があります。また、使用できるのは英数字とアンダースコアのみになります。

→ ヒント

名前属性に無効な文字を指定すると、BI プラットフォームで内部名が生成されません。内部名はシステムに追加すると変更できなくなるため、英数字とアンダースコアを含む適切な属性名を慎重に選択することをお勧めします。

マップされたユーザ属性を拡張するための前提条件

システムにユーザ属性を追加する前に、ユーザをマップおよびインポートするように外部ユーザディレクトリのすべての関連する認証プラグインを設定する必要があります。また、外部ディレクトリ、特にターゲット属性に使用する名前のスキーマに精通している必要があります。

ⓘ 注記

SAP 認証プラグインの場合、BAPIADDR3 構造に含まれる属性のみを指定できます。

新しいユーザ属性をマップするように BI プラットフォームが設定されると、次にスケジュールされている更新後に値が入力されます。CMC の [ユーザとグループ] 管理エリアにすべてのユーザ属性が表示されます。

6.2.18 複数の認証オプションに対するユーザ属性の優先順位付け

SAP、LDAP、および AD の認証プラグインを設定する場合、プラグインごとに他の 2 つのプラグインに対する優先順位レベルを指定できます。 たとえば、LDAP 認証エリアでは、[別の属性バインディングに関連する *LDAP* 属性バインディングの優先順位を設定する] オプションを使用して、SAP および AD に対する LDAP の優先順位を指定します。 デフォルトでは、Enterprise 属性値が外部ディレクトリの値よりも優先されます。 属性バインディングの優先順位は、特定の属性ではなく認証プラグインレベルで設定されます。

関連情報

LDAP ホストを設定する [262 ページ]
SAP ロールをインポートする [330 ページ]

6.2.19 新しいユーザ属性を追加する

新しいユーザ属性を BI プラットフォームに追加するには、ユーザアカウントをマップする外部ディレクトリの認証プラグインを設定する必要があります。これは、SAP、LDAP、および Windows AD に適用されます。具体的には、必要なすべてのプラグインの [フルネーム、電子メールアドレス、およびその他の属性のインポート] オプションをオンにする必要があります。

> ⓘ 注記
>
> Enterprise ユーザアカウントの属性を拡張する前に準備タスクを実行する必要はありません。

> → ヒント
>
> 複数のプラグインで同じ属性を拡張する場合、組織の要件に基づいて適切な属性バインディングの優先順位レベルを設定することをお勧めします。

1. CMC の [ユーザ属性管理] 管理エリアに移動します。
2. [新規カスタムマップ属性を追加します] アイコンをクリックします。
   [属性の追加] ダイアログボックスが表示されます。
3. [名前] フィールドで新しい属性の名前を指定します。

   BI プラットフォームでは、新しい属性のフレンドリ名として入力された名前が使用されます。

   フレンドリ名を入力すると、`SI_[Friendlyname]` の形式に従って [内部名] フィールドが自動的に設定されます。システム管理者が属性の "フレンドリ" 名を指定すると、BI プラットフォームによって自動的に "内部" 名が生成されます。
4. 必要な場合は、文字、数字またはアンダースコアを使用して [内部名] フィールドを変更します。

   > → ヒント
   >
   > [内部名] フィールドの値は、この段階でのみ変更できます。新しい属性を保存したら、この値は編集できなくなります。

   新しい属性が Enterprise アカウント用の属性である場合、手順 8 に進みます。
5. リストから [新しいソースの追加先] の適切なオプションを選択して [追加] アイコンをクリックします。次のオプションがあります。

   - *SAP*
   - *LDAP*
   - *AD*

   指定した属性ソースに対応するテーブル行が作成されます。
6. [属性ソース名] 列で、ソースディレクトリの属性名を指定します。

   BI プラットフォームには、入力した属性名が外部ディレクトリに存在しているかどうかを自動的に検証するメカニズムは備わっていません。入力した名前が正しく有効であることを確認してください。
7. 新しい属性のソースを追加する必要がある場合、手順 5 ～ 6 を繰り返します。
8. [*OK*] をクリックし、新しい属性を保存して BI プラットフォームに送信します。
   CMC の [ユーザ属性管理] 管理エリアに新しい属性の名前、内部名、ソース、および属性ソース名が表示されます。

対象となる各ユーザアカウントの新しい属性とそれに対応する値が、次にスケジュールされている最新表示で [ユーザとグループ] 管理エリアに表示されます。

新しい属性に複数のソースを使用している場合、認証プラグインごとに正しい属性バインディングの優先順位が指定されていることを確認します。

6.2.20 カスタマイズされたユーザ属性を編集する

BI プラットフォームで作成されたユーザ属性を編集するには、次の手順に従います。以下を編集できます。

- BI プラットフォームの属性名

> ⓘ 注記
>
> これは、属性に使用される内部名ではありません。属性を作成して BI プラットフォームに追加したら、内部名は編集できなくなります。内部名を削除するには、管理者が関連する属性を削除する必要があります。

- 属性ソース名
- 属性の追加ソース

1. CMC の [ユーザ属性管理] 管理エリアに移動します。
2. 編集する属性を選択します。
3. [選択した属性を編集します] アイコンをクリックします。
   [編集] ダイアログ ボックスが表示されます。
4. 属性の名前やソース情報を変更します。
5. [*OK*] をクリックし、変更を保存して BI プラットフォームに送信します。
   変更した値が CMC の [ユーザ属性管理] 管理エリアに表示されます。

次にスケジュールされている最新表示の後に [ユーザとグループ] 管理エリアに変更した属性名と値が表示されます。

6.3 エイリアスの管理

1 人のユーザが BI プラットフォームに複数のアカウントを持っている場合、[エイリアスの割り当て] 機能を使ってそれらをリンクできます。これは、ユーザが Enterprise および Enterprise アカウントにマップされているサードパーティアカウントを持っている場合に便利です。

エイリアスをユーザに割り当てると、ユーザはサードパーティのユーザ名とパスワード、または Enterprise ユーザ名とパスワードのいずれかを使用してログオンできます。したがって、エイリアス機能によってユーザは複数の認証タイプでログオンできます。

CMC では、ユーザの[プロパティ]ダイアログボックスの最下部にエイリアス情報が表示されます。ユーザは、Enterprise エイリアス、LDAP エイリアス、Windows AD エイリアスをさまざまな組み合わせで持つことができます。

6.3.1 ユーザを作成しサードパーティエイリアスを追加する

ユーザを作成し、Enterprise 以外の認証タイプを選択すると、システムは BI プラットフォームに新しいユーザを作成し、そのユーザに対してサードパーティのエイリアスを作成します。

> **注記**
>
> システムがサードパーティのエイリアスを作成するには、以下の条件が満たされていなければなりません。
>
> - CMC で認証ツールが有効になっている必要があります。
> - アカウント名の形式がその認証タイプで求められる形式に合っている必要があります。
> - サードパーティの認証ツールにユーザアカウントが存在する必要があります。また、そのユーザアカウントは、すでに BI プラットフォームにマップされているグループに属している必要があります。

1. CMC のユーザとグループ管理エリアを表示します。
2. 管理 > 新規 > 新しいユーザ の順にクリックします。
   [新しいユーザ]ダイアログボックスが表示されます。
3. ユーザに対する認証タイプ（たとえば Windows AD）を選択します。
4. ユーザのサードパーティアカウント名 (たとえば **bsmith**) を入力します。
5. ユーザの接続タイプを選択します。
6. [作成して閉じる]をクリックします。

   ユーザが BI プラットフォームに追加され、選択した認証タイプ用のエイリアス (たとえば secWindowsAD:ENTERPRISE:bsmith) が割り当てられます。 必要に応じて、ユーザにエイリアスを追加、割り当て、および再割り当てできます。

6.3.2 既存のユーザの新しいエイリアスを作成する

既存の BI プラットフォームユーザにエイリアスを作成できます。 エイリアスは Enterprise エイリアス、またはサードパーティの認証ツール用のエイリアスにすることもできます。

> **注記**
>
> システムがサードパーティのエイリアスを作成するには、以下の条件が満たされていなければなりません。
>
> - CMC で認証ツールが有効になっている必要があります。
> - アカウント名の形式がその認証タイプで求められる形式に合っている必要があります。
> - サードパーティの認証ツールにユーザアカウントが存在する必要があります。また、そのユーザアカウントは、BI プラットフォームにマップされているグループに属している必要があります。

1. CMC のユーザとグループ管理エリアを表示します。
2. エイリアスの追加先のユーザを選択します。
3. 管理 > プロパティ をクリックします。
   [プロパティ] ダイアログボックスが表示されます。
4. [新しいエイリアス]をクリックします。
5. 認証の種類を選択します。
6. ユーザのアカウント名を入力します。
7. 更新をクリックします。

   ユーザのエイリアスが作成されます。 CMC でユーザを表示すると、ユーザにすでに割り当てられているエイリアスと、ここで作成されたエイリアスの、少なくとも 2 つのエイリアスが表示されます。

8. [保存して閉じる]をクリックして[プロパティ]ダイアログボックスを閉じます。

6.3.3 別のユーザのエイリアスを割り当てる

あるエイリアスをユーザに割り当てるとき、別のユーザのサードパーティのエイリアスを、現在表示しているユーザに移動します。Enterprise エイリアスは、割り当てまたは再割り当てできません。

> ⓘ 注記
>
> ユーザがエイリアスを 1 つだけ持っていて、その唯一のエイリアスを別のユーザに割り当てる場合、システムはそのユーザアカウント、およびそのアカウントのお気に入りフォルダ、個人用カテゴリ、および受信ボックスを削除します。

1. CMC の[ユーザとグループ]管理エリアを表示します。
2. エイリアスを割り当てるユーザを選択します。
3. 管理 > プロパティ をクリックします。
   [プロパティ]ダイアログボックスが表示されます。
4. *[エイリアスの割り当て]*をクリックします。
5. 割り当てるエイリアスを持っているユーザアカウントを入力し、[検索開始]をクリックします。
6. [利用可能なエイリアス]一覧から割り当てるエイリアスを[`<Username>` に追加されるエイリアス]一覧に移動します。

   ここで、`<Username>` は、エイリアスを割り当てるユーザの名前を表します。

   > → ヒント
   >
   > 複数のエイリアスを選択するには、`Shift` + `クリック`または`Ctrl` + `クリック`を使用します。

7. [*OK*] をクリックします。

6.3.4 エイリアスを削除する

エイリアスを削除すると、そのエイリアスはシステムから削除されます。ユーザがエイリアスを 1 つだけ持っていて、そのエイリアスを削除する場合、システムはそのユーザアカウント、およびそのアカウントのお気に入りフォルダ、個人用カテゴリ、および受信ボックスを自動的に削除します。

> ⓘ 注記
>
> ユーザのエイリアスを削除しても、必ずしもユーザが BI プラットフォームに再度ログオンできなくなるわけではありません。ユーザアカウントがサードパーティシステムにまだ存在し、そのアカウントが BI プラットフォームにマップされるグループに所属する場合、ユーザは依然として BI プラットフォームにログオンできます。システムが新しいユーザを作成するか、既存のユーザにエイリアスを割り当てるかは、CMC の[認証]管理エリアの認証ツールで選択した更新オプションに依存します。

1. CMC の[ユーザとグループ]管理エリアを表示します。
2. 削除するエイリアスを持つユーザを選択します。

3. 管理 > プロパティ をクリックします。
   [プロパティ]ダイアログボックスが表示されます。
4. 削除するエイリアスの横にある[エイリアスの削除]ボタンをクリックします。
5. 確認を求めるメッセージが表示されたら、[*OK*]をクリックします。
   エイリアスは削除されます。
6. [保存して閉じる]をクリックして[プロパティ]ダイアログボックスを閉じます。

6.3.5 エイリアスを無効化する

認証方法に関連付けられているユーザのエイリアスを無効にすることで、ユーザが特定の認証手順を使用して BI プラットフォームにログオンしないようにできます。ユーザが BI プラットフォームに完全にアクセスできないようにするには、そのユーザのすべてのエイリアスを無効にします。

> ⓘ 注記
>
> ユーザをシステムから削除しても、必ずしもそのユーザが BI プラットフォームに再度ログオンできなくなるわけではありません。ユーザアカウントがサードパーティシステムにまだ存在し、そのアカウントが BI プラットフォームにマップされるグループに所属する場合、ユーザは依然として BI プラットフォームにログオンできます。ユーザが BI プラットフォームにログオンするために自分のエイリアスを使用できないようにするには、エイリアスを無効にするのが最もよい方法です。

1. CMC の[ユーザとグループ]管理エリアを表示します。
2. 無効にするエイリアスを持つユーザを選択します。
3. 管理 > プロパティ をクリックします。
   [プロパティ]ダイアログボックスが表示されます。
4. 無効にするエイリアスの[有効]チェックボックスをオフにします。

   無効にする各エイリアスに対して、この手順を繰り返します。
5. *[保存して閉じる]*をクリックします。
   そのユーザは、ここで無効にした種類の認証を使用してログオンできなくなります。

関連情報

エイリアスを削除する [119 ページ]

7 アクセス権の設定

7.1 BI プラットフォームでのアクセス権の動作

アクセス権とは、BI プラットフォーム内のオブジェクト、ユーザ、アプリケーション、サーバ、およびその他の機能へのユーザアクセスを制御するための基本単位です。オブジェクトに対してユーザが実行できる個々の操作を指定することで、システムを保護する重要な役割を果たします。また、BI プラットフォームコンテンツへのアクセスを制御したり、ユーザ管理やグループ管理を別の部署に委任したり、サーバやサーバグループへの管理アクセスを IT 担当者に与えたりすることができます。

アクセス権は、レポートやフォルダなどのオブジェクトにアクセスする主体(ユーザおよびグループ)に対してではなく、オブジェクトに対して設定されることに注意してください。たとえば、マネージャに特定のフォルダへのアクセス権を付与する場合は、[フォルダ]領域で、マネージャをそのフォルダのアクセスコントロールリスト(オブジェクトに対するアクセス権を持つ主体のリスト)に追加します。[ユーザとグループ]領域でマネージャのアクセス権を設定して、マネージャにアクセス権を付与することはできません。[ユーザとグループ]領域でのマネージャへのアクセス権の設定は、システム内のオブジェクトとしてのマネージャに対するアクセス権を、他の主体(委任管理者など)に付与するために使用します。このように、主体は、より強いアクセス権を持つ他の主体に管理されるオブジェクトになります。

オブジェクトのアクセス権は、[許可]、[拒否]、または[指定なし]のいずれかに設定できます。BI プラットフォームセキュリティモデルでは、あるアクセス権が [指定なし] になっていると、そのアクセス権は拒否されます。さらに、設定によって、あるアクセス権がユーザやグループに対して許可されると同時に拒否されるような場合、そのアクセス権は拒否されます。このような“拒否ベースのアクセス権設計”に基づいて、ユーザやグループが、明示的に許可されていないアクセス権を自動的に取得できないようになっています。

ただし、この規則には重要な例外があります。親オブジェクトから継承したアクセス権と相反するアクセス権が子オブジェクトに明示的に設定されている場合は、子オブジェクトに設定されているアクセス権が継承されたアクセス権よりも優先されます。この例外は、グループのメンバーのユーザにも適用されます。ユーザのグループが拒否されているアクセス権が、そのユーザに対して明示的に許可されている場合、ユーザに設定されたアクセス権が継承された権限よりも優先されます。

関連情報

権限の上書き [125 ページ]

7.1.1 アクセスレベル

アクセスレベルは、ユーザが頻繁に必要とするアクセス権のグループです。それによって、管理者は共通するセキュリティレベルをすばやく一律に設定できます。個別のアクセス権を 1 つずつ設定する必要はなくなります。

BI プラットフォームにはいくつかの定義済みのアクセスレベルがあります。これらの定義済みアクセスレベルは、[表示]から[フルコントロール]までのアクセス権の拡大モデルに基づき、それぞれが前のレベルで許可されたアクセス権に別のアクセス権を加える形で設定されます。

ただし、独自のアクセスレベルを作成してカスタマイズすることもできます。これにより、セキュリティに関する管理コストやメンテナンスコストを大幅に削減できます。例として、管理者が営業マネージャと営業員という 2 つのグループを管理する必要がある場合を考えてみます。どちらのグループも、BI プラットフォームシステム内の 5 つのレポートにアクセスする必要がありますが、営業マネージャは営業員よりも多くの権限が必要です。定義済みのアクセスレベルは、いずれのグループのニーズにも対応していません。管理者は、各レポートにプリンシパルとしてグループを追加して、5 つの異なる場所でそれらのグループの権限を変更するのではなく、"営業マネージャ"と"営業員" という 2 つのアクセスレベルを作成できます。次に、両方のグループをプリンシパルとしてレポートに追加し、それらのグループにそれぞれアクセスレベルを割り当てます。権限を変更する必要がある場合、管理者はアクセスレベルを変更できます。5 つのレポートすべてに対するアクセスレベルは両方のグループに適用されるため、レポートに対してそれらのグループが持っている権限はすぐに更新されます。

関連情報

アクセスレベルの使用 [134 ページ]

7.1.2 詳細アクセス権の設定

オブジェクトのセキュリティを完全に制御できるようにするために、CMC では詳細アクセス権を設定できます。この詳細アクセス権によって、詳細レベルでオブジェクトのセキュリティをより柔軟に定義できるようになります。

詳細なアクセス権の設定は、たとえば、特定のオブジェクトや複数のオブジェクトに対する主体のアクセス権をカスタマイズする必要がある場合に使用します。ユーザやグループに対して絶対に許可すべきでないアクセス権を詳細なアクセス権を使って明示的に拒否することにより、将来グループのメンバーシップやフォルダのセキュリティレベルを変更しても拒否の状態をそのまま保持できる点で、詳細なアクセス権は重要です。

以下の表に、詳細アクセス権を設定するときに使用できるオプションの概要を示します。

アクセス権オプション

アイコン	アクセス権オプション	説明
	許可	アクセス権は主体に対して許可されます。
	拒否	アクセス権は主体に対して拒否されます。
	指定なし	アクセス権は主体に対して指定されていません。デフォルトでは、[指定なし]に設定されたアクセス権は拒否されます。
	オブジェクトに適用	アクセス権はオブジェクトに適用されます。このオプションは、[許可]または[拒否]をクリックすると使用できるようになります。

アイコン	アクセス権オプション	説明
	サブオブジェクトに適用	アクセス権はサブオブジェクトに適用されます。このオプションは、[許可]または[拒否]をクリックすると使用できるようになります。

関連情報

種類固有アクセス権 [127 ページ]

7.1.3 継承

アクセス権はオブジェクトに設定され、主体のオブジェクトに対するアクセスを制御しますが、すべてのオブジェクトに対してすべての主体のすべての設定可能なアクセス権を明示的に設定することは実行不可能です。100 個のアクセス権、1000 人のユーザ、10,000 個のオブジェクトが 1 つのシステムに含まれていると考えてみます。それぞれのオブジェクトのアクセス権を明示的に設定するには、CMS のメモリに何十億ものアクセス権情報を格納する必要があります。さらに、それぞれを管理者が手動で設定する必要があります。

継承パターンは、この非実用的な作業に代わるものです。継承によって、システム内のオブジェクトに対するユーザのアクセス権は、そのユーザが属するさまざまなグループおよびサブグループのメンバーシップの組み合わせと、親フォルダやサブフォルダからアクセス権を継承したオブジェクトに由来します。これらのユーザはグループメンバーシップによってアクセス権を継承し、サブグループは親グループから、ユーザとグループは共に親フォルダからアクセス権を継承します。

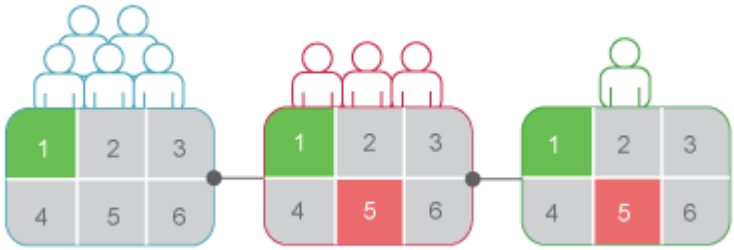
デフォルトでは、あるフォルダに対するアクセス権が付与されているユーザやグループは、以後そのフォルダに公開されるどのオブジェクトに対しても同じアクセス権を継承します。したがって、最も望ましい方法として、まずフォルダレベルでユーザおよびグループに適切なアクセス権を設定してから、そのフォルダにオブジェクトを公開します。

BI プラットフォームでは、グループ継承とフォルダ継承の 2 種類が区別されます。

7.1.3.1 グループ継承

グループ継承は、グループメンバーシップによるアクセス権の継承を主体に許可します。これは、ユーザを組織の現行セキュリティ規則に合わせたグループに編成するのに特に有効です。

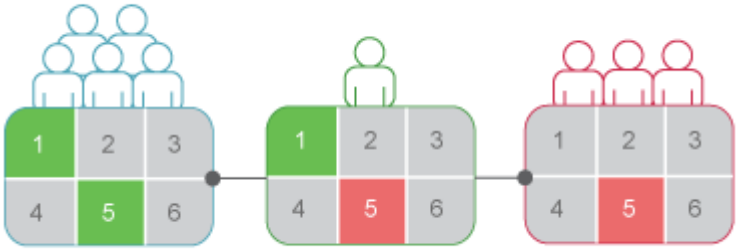
「“グループ継承の例 1”」に、グループ継承のしくみを示します。赤のグループは青のグループのサブグループなので、青のグループのアクセス権を継承します。この場合、アクセス権 1 は[許可]されるものとして継承され、それ以外のアクセス権は[指定なし]です。赤のグループのすべてのメンバーは、このアクセス権を継承します。さらに、このサブグループに設定された他のすべてのアクセス権も、メンバーに継承されます。この例では、緑のユーザは赤のグループのメンバーで、アクセス権 1 が[許可]、アクセス権 2、3、4 と 6 は[指定なし]、アクセス権 5 は[拒否]です。



グループ継承の例 1

複数のグループに所属しているユーザに対してグループ継承を有効にすると、システムがアカウント情報をチェックするときに、すべての親グループのアクセス権が考慮されます。その場合、いずれかの親グループで明示的に拒否されているアクセス権は拒否され、いずれかのグループで[指定なし]の状態にあるアクセス権もすべて拒否されます。したがって、ユーザには、1 つまたは複数のグループで(明示的に、またはアクセスレベルによって)許可され、明示的に拒否されていないアクセス権だけが許可されます。

「“グループ継承の例 2”」では、緑のユーザは 2 つの関連のないグループのメンバーです。青のグループからアクセス権 1 と 5 が[許可]でそれ以外は[指定なし]として継承しています。しかし、緑のユーザは赤のグループにも属しており、赤のグループはアクセス権 5 が明示的に拒否されているので、青のグループから継承したアクセス権 5 は無効になります。



グループ継承の例 2

関連情報

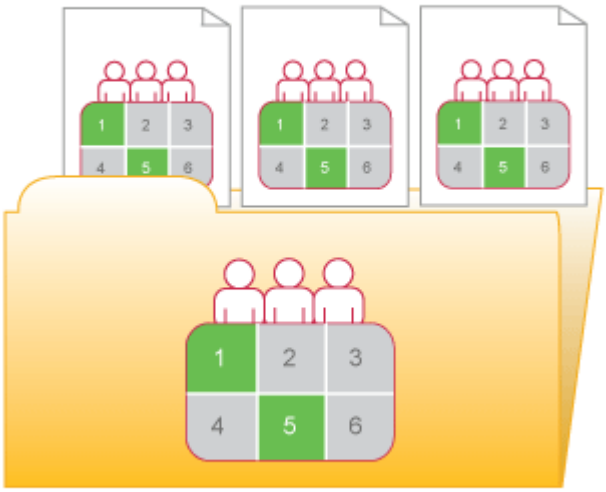
権限の上書き [125 ページ]

7.1.3.2 フォルダ継承

フォルダ継承は、オブジェクトの親フォルダで許可されているすべてのアクセス権の継承を主体に許可します。組織の現行のセキュリティ規則が反映されているフォルダ階層に合わせて BI プラットフォームのコンテンツをフォルダに編成する場合は、フォルダ継承を使用すると特に便利です。フォルダ継承では、たとえば、"営業レポート"という名前のフォルダを作成し、このフォルダへの[オンデマンド表示]アクセス権を"営業"グループに付与したとします。その場合、デフォルトでは、[営業レポート]フォルダに対するアクセス権を持つユーザ全員が、そ

の後このフォルダに公開されるレポートに対して同じアクセス権を継承します。したがって、"営業"グループには、すべてのレポートに対する[オンデマンド表示]アクセス権が付与され、オブジェクトのアクセス権をフォルダレベルで一度設定するだけで済みます。

「“フォルダ継承の例”」では、赤のグループに対してフォルダにアクセス権が設定されています。アクセス権 1 と 5 は許可され、それ以外は指定されていません。フォルダの継承が有効なので、赤のグループのメンバーは、フォルダレベルのグループのアクセス権と同じアクセス権をオブジェクトレベルで持ちます。アクセス権 1 と 5 は許可として継承され、それ以外は指定されません。



フォルダ継承の例

関連情報

権限の上書き [125 ページ]

7.1.3.3 権限の上書き

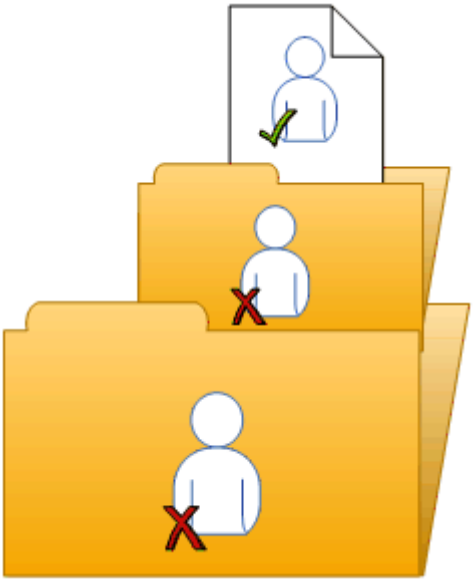
権限の上書きは、子オブジェクトに設定されている権限が親オブジェクトに設定されている権限より優先される権限の動作です。権限の上書きは、次の状況で発生します。

- 一般的に、子オブジェクトに設定された権限が、親オブジェクトに設定された対応する権限をオーバーライドします。
- 一般的に、グループのサブグループまたはメンバーに設定されている権限が、グループに設定されている対応する権限をオーバーライドします。

オブジェクトにカスタマイズした権限を設定するために、継承を無効にする必要はありません。子オブジェクトは、子オブジェクトに明示的に設定されている権限を除き、親オブジェクトの権限設定を継承します。また、親オブジェクトの権限設定を変更すると、子オブジェクトに適用されます。

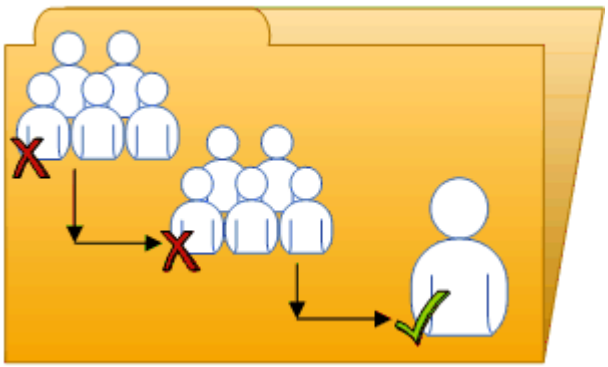
“権限の上書きの例 1”は、親オブジェクトと子オブジェクトでの権限の上書きの動作を示しています。青のグループはフォルダの内容を編集する権限を拒否されています。青のサブグループはこの権限設定を継承します。ただ

し、管理者は青のユーザにサブフォルダ内の 1 つのドキュメントに対する編集権限を許可しています。青のユーザが受け取った、ドキュメントの編集権限は、フォルダまたはサブフォルダから継承した権限より優先されます。



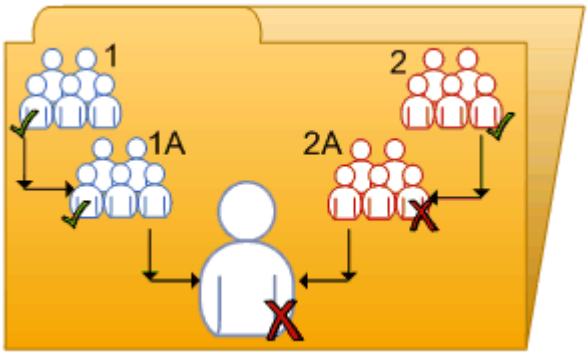
権限の上書きの例 1

“権限の上書きの例 2”は、メンバーおよびグループでの権限の上書きの動作を示しています。青のグループはフォルダを編集する権限を拒否されています。青のサブグループはこの権限設定を継承します。ただし、管理者は、青のグループおよび青のサブグループのメンバーである青のユーザに、フォルダに対する編集権限を許可します。青のユーザが受け取った、フォルダの編集権限は、青のグループおよび青のサブグループから継承した権限をオーバーライドします。



権限の上書きの例 2

“複雑な権限の優先”は、権限の優先の効果を確認するのが難しい状況を示しています。紫のユーザはサブグループ 1A および 2A のメンバーで、それぞれグループ 1 とグループ 2 に所属しています。グループ 1 と 2 は両方ともフォルダに対する編集権限を持っています。1A はグループ 1 の持っている編集権限を継承しますが、管理者は 2A に対して編集権限を拒否します。2A の権限設定は、権限の上書きのためグループ 2 の権限設定より優先されます。したがって、紫のユーザは 1A と 2A から相反する権限設定を継承します。1A と 2A には親子関係がないため、権限の上書きは発生しません。つまり、これら 2 つのサブグループのステータスは同じなので、一方の権限設定がもう一方の権限設定を上書きすることはありません。結局、紫のユーザは、BI プラットフォームの“拒否ベース”の権限モデルが原因で、編集権限が拒否されます。



複雑な権限の上書き

権限の上書きにより、継承された権限設定を破棄せずに、子オブジェクトに対する権限設定を調整することができます。販売マネージャが、"機密"フォルダに保存されている機密レポートを表示する必要がある例を考えてみます。販売マネージャは販売グループに属し、販売グループは、"機密"フォルダおよびその内容へのアクセスを拒否されています。管理者は、販売マネージャに"機密"フォルダへの表示権限を許可し、販売グループのアクセスは引き続き拒否します。この場合、販売マネージャに許可された表示権限は、販売グループのメンバーシップからマネージャが継承する、拒否されているアクセス権よりも優先されます。

7.1.3.4 アクセス権の範囲

アクセス権の範囲とは、アクセス権の継承の範囲を制御する機能です。アクセス権の範囲を定義するには、アクセス権をオブジェクト、そのサブジェクト、またはその両方のどれに適用するか決定します。デフォルトでは、アクセス権の範囲は、オブジェクトとサブオブジェクトの両方まで拡張されます。

アクセス権の範囲を使用して、共有の場所にある個人用のコンテンツを保護できます。たとえば、財務部門に、各従業員の "個人経費請求" サブフォルダを含む共有の "経費請求" フォルダがあるとします。従業員は、"経費請求" フォルダを表示したり、オブジェクトをそのフォルダに追加できるようにしたいと考えていますが、各自の "個人用経費経費" サブフォルダの内容は保護したいと考えています。管理者は、すべての従業員に "経費請求" フォルダに対する [表示] および [追加] アクセス権を付与し、これらのアクセス権の範囲を "経費請求" フォルダにのみ制限します。つまり、[表示] アクセス権と [追加] アクセス権は、"経費請求" フォルダ内のサブオブジェクトには適用されません。次に管理者は、従業員に対して、各自の "個人用経費請求" サブフォルダに対する [表示] および [追加] アクセス権を付与します。

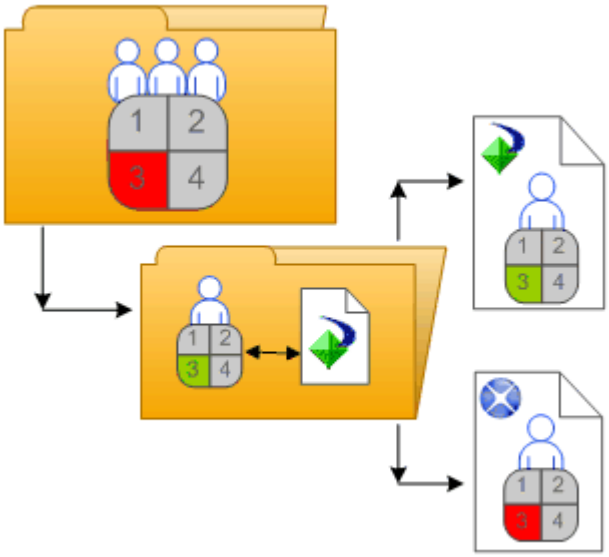
アクセス権の範囲によって、委任管理者の実効アクセス権が制限されることがあります。たとえば、委任管理者が、あるフォルダに対する[アクセス権を安全に変更する]および[編集]アクセス権を持っていてる場合でも、これらのアクセス権の範囲はフォルダのみに制限され、そのサブオブジェクトには適用されません。委任管理者は、これらのアクセス権を、フォルダのサブオブジェクトのいずれかについて別のユーザに許可することはできません。

7.1.4 種類固有アクセス権

種類固有アクセス権は、Crystal レポート、フォルダ、アクセスレベルなど特定のオブジェクトの種類にのみ影響を与えるアクセス権です。種類固有のアクセス権は、次の権限で構成されています。

- オブジェクトの種類に対する一般権限
  これらの権限は一般グローバル権限(オブジェクトを追加、削除、編集する権限など)と同じですが、それらの権限は特定のオブジェクトの種類に設定され、一般グローバル権限設定より優先されます。
- オブジェクトの種類に固有の権限
  これらの権限は、特定のオブジェクトの種類でのみ使用できます。たとえば、レポートのデータをエクスポートする権限は Crystal レポートで表示されても、Word ドキュメントでは表示されません。

「"種類固有アクセス権の例"」の図は、種類に固有のアクセス権の動作を示しています。この例で、権限 3 はオブジェクトを編集する権限を表しています。青のグループは、最上位フォルダに対する編集権限が拒否され、フォルダおよびサブフォルダ内にある Crystal レポートの編集権限は許可されます。編集権限は Crystal レポートに固有で、一般グローバルレベルの権限設定よりも優先されます。 その結果、青のグループのメンバーは、サブフォルダ内の Crystal レポートに対する編集権限は持ちますが、XLF ファイルの編集権限は持ちません。



種類固有アクセス権の例

種類固有アクセス権は、オブジェクトの種類に基づいて主体のアクセス権を制限できるので便利です。従業員がオブジェクトをフォルダに追加できても、サブフォルダは作成できないように管理者が設定する例を考えてみます。管理者は、フォルダに対する追加権限を一般グローバルレベルで許可してから、フォルダオブジェクトの種類に対して追加権限を拒否します。

アクセス権は、適用先のオブジェクトの種類に基づいて次のコレクションに分割されます。

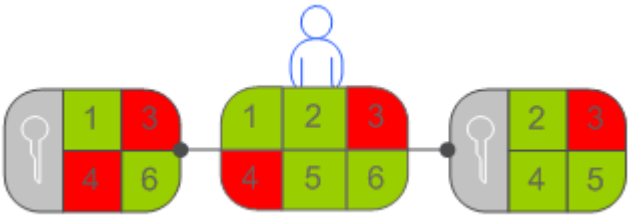
- 一般
  これらのアクセス権はすべてのオブジェクトに影響します。
- コンテンツ
  これらのアクセス権は、特定のコンテンツオブジェクトの種類に従って分割されます。コンテンツオブジェクトの種類の例として、Crystal レポート、Adobe Acrobat PDF があります。
- アプリケーション
  これらのアクセス権は、それらが影響を与える BI プラットフォームアプリケーションに従って分割されます。アプリケーションの例として、CMC と BI 起動パッドなどがあります。
- システム
  これらのアクセス権は、それらが影響を与えるコアシステムコンポーネントに従って分割されます。コアシステムコンポーネントの例として、カレンダ、イベント、およびユーザとグループがあります。

種類固有アクセス権はコンテンツ、アプリケーション、およびシステム コレクションに含まれます。各コレクションでは、オブジェクトの種類に基づいて、それらの権限をさらにカテゴリに分割します。

7.1.5 実効アクセス権の決定

オブジェクトにアクセス権を設定するときは、以下の点に注意してください。

- アクセスレベルごとに、許可および拒否されるアクセス権、および未指定のアクセス権があります。ユーザにいくつかのアクセスレベルが与えられている場合、実効アクセス権が集計されて、デフォルトでは未指定のアクセス権は拒否されます。
- オブジェクトに対する複数のアクセスレベルを主体に割り当てる場合、主体は各アクセスレベルのアクセス権の組み合わせを持つことになります。“複数アクセスレベル”のユーザに 2 つのアクセスレベルが割り当てられているとします。1 つのアクセスレベルは、ユーザアクセス権 3 と 4 で、もう 1 つのアクセスレベルは、アクセス権 3 のみを許可するとします。この場合、ユーザの実効アクセス権は 3 と 4 になります。



複数アクセスレベル

- 詳細アクセス権をアクセスレベルと組み合わせて、オブジェクトに対する主体のアクセス権の設定をカスタマイズできます。たとえば、オブジェクトに対する詳細アクセス権とアクセスレベルの両方を主体に割り当て、詳細アクセス権がアクセスレベルのアクセス権と矛盾する場合、アクセスレベルのアクセス権よりも詳細アクセス権が優先されます。
  詳細アクセス権は、同じ主体の同じオブジェクトに対して設定されている場合にのみ、アクセスレベルの対応するアクセス権を上書きできます。たとえば、一般グローバルレベルで設定された [追加] 詳細アクセス権は、アクセスレベルの一般的な [追加] アクセス権設定を上書きできますが、アクセスレベルの種類に固有の [追加] アクセス権設定は上書きできません。
  ただし、詳細アクセス権は常にアクセスレベルを上書きすると限りません。たとえば、親オブジェクトに対する編集アクセス権を主体が拒否されているとします。子オブジェクトで、主体には、編集アクセス権を許可するアクセスレベルが割り当てられています。最終的に、主体には子オブジェクトに対する編集アクセス権が割り当てられます。子オブジェクトに設定されているアクセス権は、親オブジェクトに設定されているアクセス権を上書きするからです。
- 権限の上書きによって、子オブジェクトに設定された権限は、親オブジェクトから継承された権限を上書きできます。

7.2 CMC でのオブジェクトのセキュリティ設定の管理

[管理]メニューのセキュリティオプションを使用して、CMC で多くのオブジェクトのセキュリティ設定を管理できます。これらのオプションを使用すると、オブジェクトのアクセスコントロールリストに主体を割り当てたり、主体が持っているアクセス権を表示したり、主体がオブジェクトに対して持っているアクセス権を変更できます。

セキュリティ管理の詳細は、セキュリティのニーズ、およびアクセス権を設定しているオブジェクトの種類によって変わります。ただし、一般的には次に示すタスクのワークフローに非常に似ています。

- オブジェクトに対する主体のアクセス権を表示する。
- オブジェクトのアクセスコントロールリストに主体を割り当て、それらの主体が持つアクセス権およびアクセスレベルを指定する。
- BI プラットフォームの最上位フォルダにアクセス権を設定する。

7.2.1 オブジェクトの主体のセキュリティを表示する

通常、オブジェクトの主体のアクセス権を表示するには、次のワークフローに従います。

1. セキュリティ設定を表示するオブジェクトを選択します。
2. 管理 > ユーザセキュリティ をクリックします。
   [ユーザセキュリティ] ダイアログボックスが開き、オブジェクトのアクセスコントロールリストが表示されます。
3. アクセスコントロールリストから主体を選択し、[セキュリティの表示] をクリックします。

   権限エクスプローラが開き、オブジェクトの主体に対する実効アクセス権のリストが表示されます。また、権限エクスプローラでは、次のことも実行できます。

   - アクセス権を表示する別の主体を検索する。
   - 表示されるアクセス権を次の基準に従ってフィルタする。

     割り当てられた権限
     付与された権限
     割り当てられていない権限
     アクセスレベルから
     オブジェクトタイプ
     権限の名前
   - 次の基準に従って、表示されるアクセス権の一覧を昇順または降順に並べ替えます。

     コレクション
     タイプ
     権限名
     権限のステータス (許可、拒否、指定なし)

   また、[ソース] 列内のリンクのいずれかをクリックして、継承された権限のソースを表示できます。

7.2.2 オブジェクトのアクセスコントロールリストに主体を割り当てる

アクセスコントロールリストでは、オブジェクトでアクセス権が許可または拒否されるユーザを指定します。通常、アクセスコントロールリストに主体を割り当て、主体がオブジェクトに対して持つアクセス権を指定するには、次のワークフローに従います。

1. 主体を追加するオブジェクトを選択します。
2. 管理 > ユーザセキュリティ をクリックします。
   [ユーザセキュリティ]ダイアログボックスが開き、アクセスコントロールリストが表示されます。
3. [主体の追加]をクリックします。
   [主体の追加]ダイアログボックスが表示されます。
4. [利用可能なユーザ/グループ]一覧から主体として追加するユーザおよびグループを選択し、[選択されたユーザ/グループ]一覧に移動します。
5. [セキュリティを追加して割り当てる]をクリックします。
6. 主体に許可するアクセスレベルを選択します。
7. フォルダまたはグループの継承を有効にするかどうかを選択します。

必要に応じて、詳細レベルでアクセス権を変更し、アクセスレベルの特定のアクセス権を上書きすることもできます。

関連情報

オブジェクトの主体のセキュリティを変更する [131 ページ]

7.2.3 オブジェクトの主体のセキュリティを変更する

通常は、アクセスレベルを使用して主体にアクセス権を割り当てることをお勧めします。ただし、アクセスレベルの特定の詳細権限の上書きが必要になる場合があります。詳細なアクセス権を使用すると、主体がすでに持っているアクセスレベルの上で、主体のアクセス権をカスタマイズできます。通常、オブジェクトの主体に詳細なアクセス権を割り当てる場合は、次のワークフローに従います。

1. オブジェクトのアクセスコントロールリストに主体を割り当てます。
2. 主体が追加されている場合は、管理 > ユーザセキュリティ の順に選択して、オブジェクトのアクセスコントロールリストを表示します。
3. アクセスコントロールリストから主体を選択し、[セキュリティの割り当て]をクリックします。
   [セキュリティの割り当て]ダイアログボックスが表示されます。
4. *[詳細]*タブをクリックします。
5. [権限の追加/削除]をクリックします。
6. 主体のアクセス権を変更します。
   使用可能なすべての権限は、権限付録に要約されています。

関連情報

オブジェクトのアクセスコントロールリストに主体を割り当てる [130 ページ]

7.2.4 BI プラットフォームの最上位フォルダにアクセス権を設定する

通常、BI プラットフォームの最上位フォルダにアクセス権を設定するには、次のワークフローに従います。

> **注記**
>
> このリリースでは、主体は、コンテナフォルダ内を移動したり、サブオブジェクトを表示するために、そのフォルダへの表示アクセス権が必要になります。つまり、フォルダ内に含まれているオブジェクトを表示するためには、主体に最上位レベルのフォルダへの表示アクセス権が必要です。表示アクセス権を 1 つの主体に限定する場合は、1 つの主体に 1 つのフォルダに対する表示アクセス権を許可し、そのフォルダにのみ適用するアクセス権の範囲を設定します。

1. アクセス権を設定する最上位レベルのフォルダを含む CMC エリアに移動します。
2. 管理 > 最上位セキュリティ > すべての<オブジェクト> をクリックします。

   ここで、<オブジェクト> は、最上位フォルダの内容を表します。確認を求めるメッセージが表示されたら、*[OK]*をクリックします。

   [ユーザセキュリティ]ダイアログボックスが開き、最上位フォルダのアクセスコントロールリストが表示されます。
3. 最上位フォルダのアクセスコントロールリストに主体を割り当てます。
4. 必要に応じて、主体に詳細なアクセス権を割り当てます。

関連情報

オブジェクトのアクセスコントロールリストに主体を割り当てる [130 ページ]
オブジェクトの主体のセキュリティを変更する [131 ページ]

7.2.5 主体のセキュリティ設定の確認

主体がアクセスを許可または拒否されているオブジェクトを確認する必要がある場合があります。これを確認するには、セキュリティクエリを使用できます。セキュリティクエリを使用して、主体が特定のアクセス権を持っているオブジェクトを確認したり、ユーザのアクセス権を管理できます。各セキュリティクエリで、次の情報を指定します。

- クエリ主体
  セキュリティクエリの実行対象となるユーザまたはグループを指定します。セキュリティクエリごとに 1 つの主体を指定できます。
- クエリ権限
  セキュリティクエリの実行対象となる 1 つまたは複数の権限、これらの権限のステータス、およびこれらの権限を設定するオブジェクトの種類を指定します。たとえば、主体が最新表示できるすべてのレポート、または主体がエクスポートできないすべてのレポートに対して 1 つのセキュリティクエリを実行できます。
- クエリコンテキスト
  セキュリティクエリで検索する CMC 領域を指定します。各領域について、セキュリティクエリにサブオブジェクトを含めるかどうか選択できます。セキュリティクエリには最大 4 つの領域を含めることができます。

セキュリティクエリを実行すると、ツリー パネルの[セキュリティクエリ]エリアの下にある[クエリの結果]に結果が表示されます。セキュリティクエリを調整する場合は、最初のクエリの結果内で 2 つ目のクエリを実行できます。

セキュリティクエリを使用すると、プリンシパルが特定の権限を持っているオブジェクトを確認でき、それらの権限を変更する場合にこれらのオブジェクトの場所も示されるので便利です。営業員が営業マネージャに昇格する例を考えてみます。営業マネージャには、Crystal レポートに対するスケジュール権限が必要ですが、以前は表示権限しか持っていませんでした。これらのレポートはそれぞれ別の場所にあります。この場合、管理者は、すべてのフォルダに含まれている Crystal レポートを表示するための営業マネージャの権限についてセキュリティクエリを実行し、クエリにサブオブジェクトを含めます。セキュリティクエリの実行後、管理者は、[クエリの結果]エリアで営業マネージャが表示権限を持っているすべての Crystal レポートを参照できます。詳細パネルには各 Crystal レポートの場所が表示されるので、管理者は各レポートを閲覧し、そのレポートに対する営業マネージャの権限を変更できます。

7.2.5.1 セキュリティクエリを実行する

1. [ユーザとグループ]エリアの詳細パネルで、セキュリティクエリを実行するユーザまたはグループを選択します。
2. 管理 > ツール > セキュリティクエリの作成 をクリックします。

[セキュリティクエリの作成]ダイアログボックスが表示されます。

3. [クエリ主体]エリアの主体が正しいことを確認します。

   別の主体からセキュリティクエリを実行する場合は、[参照]をクリックして別の主体を選択します。[クエリ主体の参照]ダイアログボックスで、[ユーザ一覧]または[グループ一覧]を展開し、主体を探すか、名前で主体を検索します。完了したら、[OK]をクリックし、[セキュリティクエリの作成]ダイアログボックスに戻ります。

4. [クエリ権限]エリアで、クエリを実行する権限と各権限のステータスを指定します。
   - オブジェクトに対して主体が持っている特定の権限についてクエリを実行するには、[参照]をクリックして、セキュリティクエリを実行する各権限のステータスを設定し、[*OK*]をクリックします。

     > → ヒント
     >
     > 権限の横にある削除ボタンをクリックしてクエリから特定の権限を削除したり、ヘッダ行の削除ボタンをクリックしてクエリからすべての権限を削除することができます。

   - 一般的なセキュリティクエリを実行する場合は、[権限別にクエリを実行しない]チェックボックスをオンにします。
     これを実行すると、BI プラットフォームでは、オブジェクトに対して主体が持っている権限に関係なく、アクセスコントロールリスト内の主体を持つすべてのオブジェクトの一般的なセキュリティクエリが実行されます。
5. [クエリコンテキスト]エリアで、クエリを実行する CMC エリアを指定します。
   a. 一覧の横にあるチェックボックスをオンにします。
   b. 一覧で、クエリを実行する CMC エリアを選択します。
      エリア内のより特定した場所でクエリを実行する場合([フォルダ]の下にある特定のフォルダなど)、[参照]をクリックし、[クエリコンテキストの参照]ダイアログボックスを開きます。詳細ウィンドウで、クエリを実行するフォルダを選択し、[*OK*]をクリックします。[セキュリティクエリ]ダイアログボックスに戻ると、指定したフォルダが一覧の下のボックスに表示されます。
   c. [クエリサブオブジェクト]を選択します。
   d. クエリを実行する CMC エリアごとに上記の手順を繰り返します。

      > ⓘ 注記
      >
      > 最大 4 つのエリアでクエリを実行できます。

6. [*OK*]をクリックします。
   セキュリティクエリが実行されて、[クエリの結果]エリアが表示されます。
7. クエリ結果を表示するには、ツリー パネルで、[セキュリティクエリ]を展開し、クエリ結果をクリックします。

   > → ヒント
   >
   > クエリ結果が、主体の名前に従って一覧表示されます。

   クエリ結果は、詳細パネルに表示されます。

[クエリの結果]エリアでは、ユーザがログオフするまで単一のユーザセッションからのセキュリティクエリ結果がすべて保持されます。クエリを新しい指定で実行する場合は、アクション > クエリの編集 をクリックします。クエリを選択し、アクション > クエリの再実行 をクリックして、まったく同じクエリを再実行することもできます。セキュリティクエリ結果を維持する場合は、アクション > エクスポート をクリックして、セキュリティクエリ結果を CSV ファイルにエクスポートします。

7.3 アクセスレベルの使用

アクセスレベルを使用して、次のことを実行できます。

- 既存のアクセスレベルをコピーし、コピーに変更を加えて、名前を変更し、新しいアクセスレベルとして保存する。
- アクセスレベルを作成、名前変更、削除する。
- アクセスレベルの権限を変更する。
- アクセスレベルと、システム内の他のオブジェクトとの関係をトレースする。
- サイト間でアクセスレベルを複製および管理する。
- BI プラットフォームで定義されているアクセスレベルの 1 つを使用して、多くの主体にすばやく、均一に権限を設定する。

次の表に、定義済みの各アクセスレベルに含まれる権限の概要を示します。

定義済みのアクセスレベル

アクセスレベル	説明	関連するアクセス権
表示	フォルダレベルで設定された場合、主体はそのフォルダ、その中のオブジェクト、および各オブジェクトから生成されたインスタンスを表示できます。オブジェクトレベルで設定された場合、主体はそのオブジェクトとその履歴、およびそのオブジェクトから生成されたインスタンスを表示できます。	• オブジェクトを表示する • ドキュメントのインスタンスを表示する
スケジュール	主体は、オブジェクトが指定されたデータソースに対して 1 回または定期的に実行するようにスケジュールすることで、インスタンスを生成できます。主体は、各自が所有するインスタンスのスケジュールを表示、削除、および一時停止できます。また、別の形式や出力先へのスケジュール、パラメータとデータベースログオン情報の設定、ジョブを処理するサーバの選択、フォルダへのコンテンツの追加、オブジェクトやフォルダのコピーもできます。	[表示]アクセスレベルのアクセス権と以下の権限が含まれます。 • ドキュメントの実行をスケジュールする • ジョブを処理するサーバグループを定義する • オブジェクトを別のフォルダにコピーする • 別の出力先へスケジュールする • レポートのデータを出力する • レポートのデータをエクスポートする • ユーザが所有するオブジェクトを編集する • ユーザが所有するインスタンスを削除する • ユーザが所有するドキュメントのインスタンスを一時停止して再開する
オンデマンド表示	主体はオンデマンドでデータソースのデータを最新表示できます。	[スケジュール]アクセスレベルのアクセス権と以下の権限が含まれます。 • レポートのデータを最新表示する

アクセスレベル	説明	関連するアクセス権
フルコントロール	主体は、オブジェクトに対して完全な管理権限を持ちます。	次のようなすべてのアクセス権を利用できます。 • オブジェクトをフォルダに追加する • オブジェクトを編集する • オブジェクトに対するユーザの権限を変更する • オブジェクトを削除する • インスタンスを削除する

次の表に、アクセスレベルで特定のタスクを実行するために必要な権限の概要を示します。

アクセスレベルのタスク	必要な権限
アクセスレベルを作成する	最上位のアクセスレベル フォルダへの追加権限
アクセスレベル内の詳細権限を表示する	アクセスレベルに対する表示権限
オブジェクトの主体にアクセスレベルを割り当てる	アクセスレベルに対する表示権限 アクセスレベルに対するセキュリティの割り当てにアクセスレベルを使用する権限 オブジェクトに対するアクセス権の変更、またはオブジェクトと主体に対するアクセス権の安全な変更権限 **注記** アクセス権の安全な変更権限を持ち、アクセスレベルを主体に割り当てるユーザには、そのアクセスレベルと同じアクセスレベルが割り当てられている必要があります。
アクセスレベルを変更する	アクセスレベルに対する表示および編集権限
アクセスレベルを削除する	アクセスレベルに対する表示および削除権限
アクセスレベルのクローンを作成する	アクセスレベルに対する表示権限 アクセスレベルに対するコピー権限 最上位のアクセスレベル フォルダへの追加権限

7.3.1 表示およびオンデマンド表示アクセスレベルの選択

Web でレポートする場合、ライブデータと保存データのどちらを使用するかは、最も重要な決定事項の 1 つです。ただし、どちらの場合でも BI プラットフォームは最初のページをすばやく表示できるため、残りのデータの処理中にレポートを参照できます。ここでは、この選択を行う場合に参考にできる、2 つの定義済みアクセスレベルの違いを説明します。

オンデマンド表示アクセスレベル

オンデマンドレポートでは、ユーザがデータベースサーバから直接ライブデータにリアルタイムでアクセスできます。ライブデータを使用すると、ユーザは常に変化するデータを基に最新の情報を取得できます。たとえば、大規模な配送センタのマネージャが継続的に出荷される製品の在庫状況を確認する必要がある場合、ライブレポーティングを使用すると必要な情報が得られます。

ただし、すべてのレポートでライブデータが使用できるようにする前に、すべてのユーザが常にデータベースサーバに接続できるようにするかどうかを検討します。データが繰り返し変更されない場合、または絶えず変更されない場合は、データベースへのこれらの要求はネットワークトラフィックを増加させ、サーバのリソースを消費するだけです。このような場合、ユーザがデータベースサーバに接続することなく常に最新のデータ(レポートインスタンス)を表示できるよう、レポートに定期的な実行スケジュールを設定することができます。

ユーザには、データベースに対してレポートを最新表示する[オンデマンド表示]アクセス権が必要です。

表示アクセスレベル

ネットワークトラフィックの量とデータベースサーバのヒット数を減らすために、レポートを指定時刻に実行するようにスケジュールできます。レポートが実行されるとき、ユーザは必要に応じてレポートインスタンスを表示できます。データベースへのヒットがさらに発生することはありません。

レポートインスタンスは、継続して更新されることのないデータを使用する場合に便利です。ユーザがレポートインスタンス内を移動して、列またはチャートの詳細にドリルダウンすると、データベースサーバに直接アクセスする代わりに保存データにアクセスします。つまり、保存データを持つレポートは、ネットワーク上のデータ転送を最小化するだけでなく、データベースサーバの負荷も軽減します。

たとえば、販売データベースが 1 日に 1 回更新される場合、同様のスケジュールでレポートを実行できます。これにより、販売担当者は、レポートを開くたびにデータベースにアクセスすることなく、最新の販売データを得ることができます。

ユーザには、レポートインスタンスを表示する[表示]アクセス権のみ必要です。

7.3.2 既存のアクセスレベルをコピーする

これは、既存のアクセスレベルと若干異なるアクセスレベルが必要な場合のアクセスレベルの最良の作成方法です。

1. [アクセスレベル]エリアを表示します。
2. 詳細パネルで、アクセスレベルを選択します。

   > → ヒント
   >
   > アクセスレベルに必要な内容と同じアクセス権を含むアクセスレベルを選択します。

3. 整理 > コピー をクリックします。
   選択したアクセスレベルのコピーが詳細パネルに表示されます。

7.3.3 新しいアクセスレベルを作成する

これは、既存のアクセスレベルと大幅に異なるアクセスレベルが必要な場合のアクセスレベルの最良の作成方法です。

1. [アクセスレベル]エリアを表示します。
2. 管理 > 新規 > アクセスレベルの作成 の順にクリックします。
   [アクセスレベルの新規作成]ダイアログボックスが開きます。
3. 新しいアクセスレベルのタイトルと説明を入力し、[*OK*]をクリックします。
   [アクセスレベル]エリアに戻り、新しいアクセスレベルが詳細パネルに表示されます。

7.3.4 アクセスレベルの名前を変更する

1. [アクセスレベル]エリアの詳細パネルで、名前を変更するアクセスレベルを変更します。
2. 管理 > プロパティ をクリックします。
   [プロパティ]ダイアログボックスが表示されます。
3. [タイトル]フィールドに、アクセスレベルの新しい名前を入力し、[保存して閉じる]をクリックします。
   [アクセスレベル]エリアに戻ります。

7.3.5 アクセスレベルを削除する

1. [アクセスレベル]エリアの詳細パネルで、削除するアクセスレベルを選択します。
2. 管理 > アクセスレベルの削除 をクリックします。

   > **注記**
   >
   > 事前定義されたアクセスレベルは削除できません。

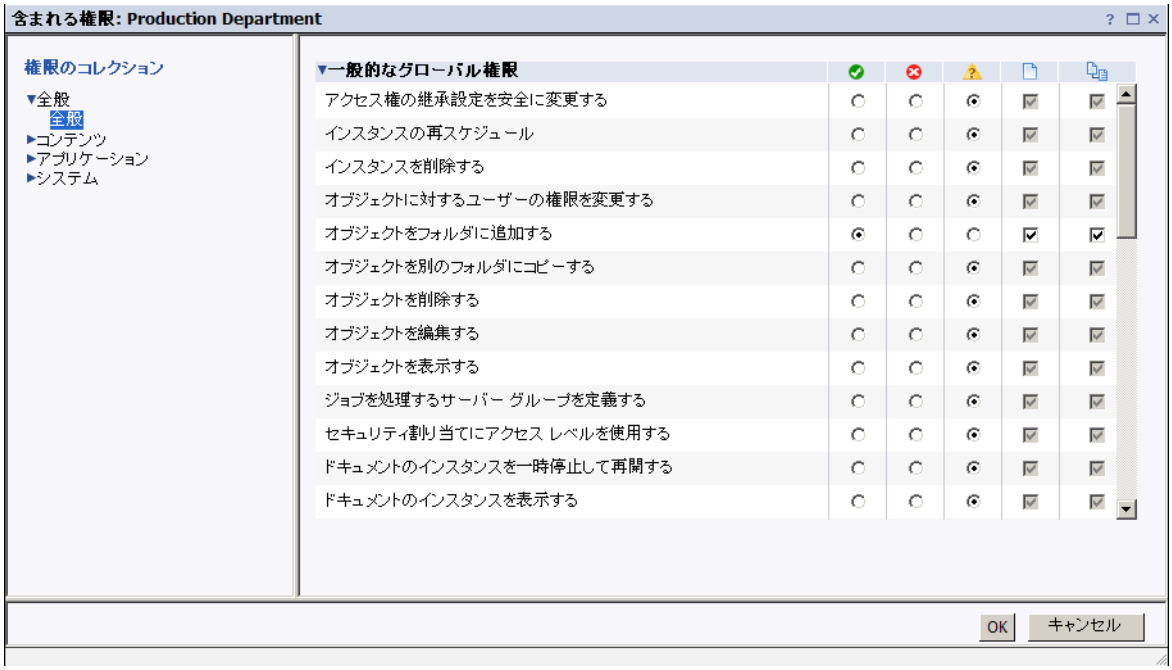
   このアクセスレベルの影響を受けるオブジェクトに関する情報を示すダイアログボックスが表示されます。
   アクセスレベルを削除しない場合は、[キャンセル]をクリックしてダイアログボックスを終了します。
3. [削除]をクリックします。
   アクセスレベルは削除され、[アクセスレベル]エリアに戻ります。

7.3.6 アクセスレベルの権限を変更する

アクセスレベルの権限を設定するには、種類に関係なくすべてのオブジェクトに適用される一般的なグローバル権限を最初に設定し、特定のオブジェクトの種類に基づいて一般的な設定より優先されるようにしたい場合は該当の権限を指定します。

1. [アクセスレベル] エリアの [詳細] パネルで、権限を変更するアクセスレベルを選択します。
2. アクション > 含まれる権限 をクリックします。
   [含まれる権限]ダイアログボックスが開き、実効アクセス権の一覧が表示されます。

3. [権限の追加/削除]をクリックします。



[含まれる権限]ダイアログボックスが表示されて、ナビゲーションリストにアクセスレベルの権限コレクションが表示されます。 デフォルトでは、[一般的なグローバル権限]セクションが展開されています。

4. 一般的なグローバル権限を設定します。

   各権限は、[許可]、[拒否]、[指定なし] のステータスを持つことができます。 権限を、該当のオブジェクトにのみ適用するか、サブオブジェクトにのみ適用するか、あるいはその両方に適用するか選択することもできます。

5. アクセスレベルの種類別権限を設定するには、ナビゲーションリストで、該当の権限コレクションをクリックし、権限を設定するオブジェクトの種類に適用されるサブコレクションをクリックします。

6. 完了したら、[*OK*]をクリックします。
   実効アクセス権の一覧に戻ります。

7.3.7 アクセスレベルとオブジェクト間の関係のトレース

アクセスレベルを変更または削除する前に、アクセスレベルに加える変更が CMC のオブジェクトに悪影響を及ぼさないか確認することが重要です。これを確認するには、アクセスレベルで関係クエリを実行します。

関係クエリは、1 つの便利な場所でアクセスレベルによって影響を受けるすべてのオブジェクトを確認できるので、権限管理に役に立ちます。会社が組織の編成を行い、2 つの部署、部署 A と部署 B を部署 C に統合する例を考えてみます。管理者は、部署 A と部署 B は存在しなくなるので、それらのアクセスレベルを削除することにしました。管理者は、両方のアクセスレベルに対して関係クエリを実行してから、それらを削除します。管理者は、*[クエリの結果]*領域で、アクセスレベルを削除した場合に影響を受けるオブジェクトを確認できます。オブジェクトの権限を変更してからアクセスレベルを削除する場合、管理者は詳細パネルで CMC 内のオブジェクトの場所も確認できます。

> ⓘ 注記
>
> 影響を受けるオブジェクトの一覧を表示するには、それらのオブジェクトに対する表示権限が必要です。

> ⓘ 注記
>
> アクセスレベルの関係クエリ結果には、アクセスレベルが明示的に割り当てられているオブジェクトのみ示されます。オブジェクトが継承設定によりアクセスレベルを使用している場合、そのオブジェクトはクエリ結果に表示されません。

7.3.8 サイト間でのアクセスレベルの管理

アクセスレベルは、レプリケート元サイトからレプリケート先サイトに複製できるオブジェクトの 1 つです。レプリケーションオブジェクトのアクセスコントロールリストに表示された場合は、そのアクセスレベルの複製を選択できます。たとえば、ある主体にはある Crystal レポートに対するアクセスレベル A が付与され、その Crystal レポートが別のサイトに複製された場合、アクセスレベル A も複製されます。

> ⓘ 注記
>
> レプリケート先サイトに同じ名前のアクセスレベルが存在する場合は、そのアクセスレベルの複製は失敗します。レプリケート元サイトまたはレプリケート先サイトの管理者は、複製前にそのアクセスレベルの名前を変更する必要があります。

サイト間でアクセスレベルを複製したら、ここに挙げた管理上の留意点に注意してください。

レプリケート元サイトでの複製されたアクセスレベルの修正

複製されたアクセスレベルがレプリケート元サイトで修正されると、レプリケート先サイトのそのアクセスレベルは、次にスケジュールによって複製が実行されたときに更新されます。双方向レプリケーションシナリオで、レプリケート先サイトで複製されたアクセスレベルを修正した場合、レプリケート元サイトのアクセスレベルも変更されます。

> ⓘ 注記
>
> 1 つのサイトでアクセスレベルを変更しても、他のサイトのオブジェクトには影響しないことを確認してください。変更する前に、複製されたアクセスレベルについて関係クエリを実行するように、サイト管理者に連絡してください。

レプリケート先サイトでの複製されたアクセスレベルの修正

> ⓘ 注記
>
> これは、一方向レプリケーションのみに適用されます。

レプリケート先サイトで複製されたアクセスレベルに対して変更しても、レプリケート元サイトには反映されません。たとえば、レプリケート先サイトの管理者は、レプリケート元サイトで拒否されている場合でも、複製されたアクセスレベルで Crystal レポートのスケジュールの権限を付与することができます。結果的に、アクセスレ

ベル名と複製されたオブジェクト名は同じままでも、ある主体がオブジェクトに対して持つその実効アクセス権はレプリケート先サイトごとに異なることがあります。

複製されたアクセスレベルがレプリケート元サイトとレプリケート先サイトで異なる場合、スケジュールによってレプリケーションジョブが次に実行されたときにその実効アクセス権の相違が検出されます。レプリケート元サイトのアクセスレベルがレプリケート先サイトのアクセスレベルより優先されるようにしたり、レプリケート先サイトのアクセスレベルが変更されないようにすることができます。しかし、レプリケート元サイトのアクセスレベルがレプリケート先サイトのアクセスレベルより優先されるようにしない場合、そのアクセスレベルを使用するレプリケーションを待機しているすべてのオブジェクトは複製されません。

レプリケート先サイトでユーザが複製されたアクセスレベルを修正しないように制限するには、そのレプリケート先サイトのユーザをアクセスレベルに主体として追加して、そのユーザに[表示]の権限のみを付与します。これによって、レプリケート先サイトのユーザはそのアクセスレベルを表示できますが、その権限の設定を修正したり他のユーザに割り当てることができなくなります。

関連情報

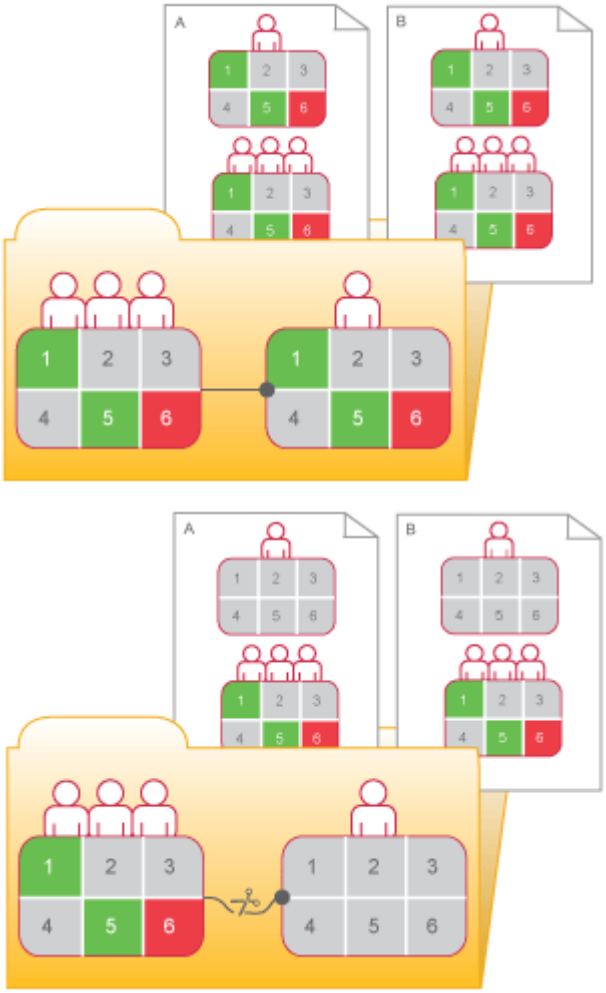
フェデレーション [923 ページ]
アクセスレベルとオブジェクト間の関係のトレース [139 ページ]

7.4 継承の破棄

継承を使用すると、オブジェクトごとにアクセス権を設定しなくても、セキュリティ設定を管理できます。ただし、場合によっては、アクセス権を継承しないようにする必要があります。たとえば、各オブジェクトの権限をカスタマイズする場合があります。オブジェクトのアクセスコントロールリストのプリンシパルに対して継承を無効にできます。これを行う場合は、グループ継承とフォルダ継承、あるいはその両方を無効にするか選択することができます。

> **注記**
>
> 継承が破棄されると、すべてのアクセス権について継承が破棄されます。一部のアクセス権についてだけ継承を破棄して他のアクセス権は継承するということはできません。

“継承の破棄”の図では、グループとフォルダの継承が最初は有効です。赤いユーザが継承したアクセス権では、1 と 5 は許可、2、3、4 は指定なし、6 は明示的に拒否されています。これらのアクセス権はグループに対してフォルダレベルで設定されます。したがって、赤いユーザとそのグループの他のすべてのメンバーは、フォルダのオブジェクト A と B に対してこれらのアクセス権を持っています。フォルダレベルでの継承が破棄されると、赤いユーザがこのフォルダのオブジェクトに対して持つアクセス権の組み合わせは、管理者が赤いユーザに新しいアクセス権を割り当てない限り、クリアされます。



継承の破棄

7.4.1 継承を無効にする

この手順では、オブジェクトのアクセスコントロールリストの主体に対して、グループ継承またはフォルダ継承(あるいはその両方)を無効にできます。

1. 継承を無効にするオブジェクトを選択します。
2. 管理 > ユーザセキュリティ をクリックします。
   [ユーザセキュリティ]ダイアログボックスが表示されます。
3. 継承を無効にする主体を選択し、[セキュリティの割り当て]をクリックします。
   [セキュリティの割り当て]ダイアログボックスが表示されます。
4. 継承を設定します。
   - グループ継承(主体がグループメンバーシップから継承するアクセス権)を無効にする場合は、[親グループからの継承]チェックボックスをオフにします。
   - フォルダ継承(オブジェクトがフォルダから継承するアクセス権)を無効にする場合は、[親フォルダからの継承]チェックボックスをオフにします。
5. [*OK*]をクリックします。

7.5 アクセス権の使用による管理の委任

アクセス権を使用すると、オブジェクトおよび設定へのアクセスを制御できるほかに、管理タスクを組織内の機能グループ間で分割できます。たとえば、ユーザおよびグループの管理は、それぞれの部署の担当者に任せることができます。また、BI プラットフォームの高レベルの管理は 1 人の管理者が行い、サーバ管理はすべて IT 部門内の担当者に任せてもかまいません。

組織のグループ構造およびフォルダの構造が委任管理のセキュリティ構造と一致している場合、委任管理者のアクセス権をユーザグループ全体に許可する必要があります。ただし、委任管理者には制御するユーザに対して[フルコントロール]アクセス権より低いアクセス権を許可することが必要です。たとえば、委任管理者がユーザの属性を編集したりユーザを別のグループに再割り当てしたりできないようにする場合があります。

> **注記**
>
> オブジェクトの移行に最も適しているのは、Administrators グループに属するメンバー、特に Administrator ユーザアカウント内のメンバーです。オブジェクトを移行するためには、多数の関連オブジェクトも移行する必要がある場合があります。すべてのオブジェクトについて必要となるセキュリティ権限を取得することは、場合によっては委任管理者アカウントでは不可能です。

“委任管理者のアクセス権”の表に、一般的なアクションを実行するために委任管理者に必要なアクセス権の要約を示します。

委任管理者のアクセス権

委任管理者の作業	委任管理者に必要なアクセス権
新しいユーザを作成する	最上位のユーザ フォルダへの"追加"アクセス権
新しいグループを作成する	最上位のユーザグループ フォルダへの"追加"アクセス権
制御下にあるグループとそのグループ内の個別のユーザを削除する	関連するグループへの"削除"アクセス権
委任管理者が作成したユーザだけを削除する	最上位のユーザ フォルダへの"所有者 による削除"アクセス権
委任管理者が作成したユーザとグループだけを削除する	最上位のユーザグループ フォルダへの"所有者による削除" アクセス権
委任管理者が作成したユーザだけを操作する(それらのユーザのグループへの追加など)	最上位のユーザ フォルダへの"所有者による編集"および"所有者による保護された変更"アクセス権
委任管理者が作成したグループだけを操作する(それらのグループへのユーザの追加など)	最上位のユーザグループ フォルダへの"所有者による編集"および"所有者による保護された変更"アクセス権
制御下にあるグループのユーザのパスワードを変更する	関連するグループへの"パスワードの変更"アクセス権

委任管理者の作業	委任管理者に必要なアクセス権
委任管理者が作成した主体だけのパスワードを変更する	最上位のユーザ フォルダまたは関連するグループへの"所有者によるパスワードの変更"アクセス権 **注記** グループへの"所有者によるパスワードの変更"アクセス権を設定すると、関連するグループにユーザを追加したときのみ、そのユーザに対してこのアクセス権が有効になります。
ユーザの名前、説明、その他の属性を変更し、別のグループにそのユーザを再割り当てする	関連するグループへの"編集"アクセス権
委任管理者が作成したユーザに対してのみ、ユーザの名前、説明、その他の属性を変更し、別のグループにそのユーザを再割り当てする	最上位のユーザ フォルダまたは関連するグループへの"所有者による編集"アクセス権 **注記** 関連グループへの"所有者による編集"アクセス権を設定すると、その関連するグループにユーザを追加したときのみ、そのユーザに対してこのアクセス権が有効になります。

7.5.1 "オブジェクトに対するユーザの権限を変更する"オプションの選択

管理の委任を設定するときは、委任管理者が制御する主体に対するアクセス権をその管理者に許可します。委任管理者には、すべてのアクセス権 ([フルコントロール]) を許可することもありますが、[詳細アクセス権]設定を使用して、[アクセス権の変更] アクセス権は許可せず、[アクセス権を安全に変更する] アクセス権を許可することをお勧めします。また、管理者に [アクセス権の継承設定を変更する] アクセス権ではなく、[アクセス権の継承設定を安全に変更する] アクセス権を許可することもできます。これらのアクセス権の相違を要約すると、次のようになります。

オブジェクトに対するユーザの権限を変更する

このアクセス権では、ユーザはそのオブジェクトに対するすべてのユーザのすべてのアクセス権を変更できます。たとえば、ユーザ A が[オブジェクトを表示する]と[オブジェクトに対するユーザの権限を変更する]というアクセス権を持つ場合、ユーザ A はそのオブジェクトのアクセス権を変更して、自分や他の任意のユーザがそのオブジェクトにフルコントロールアクセスできるようにすることができます。

ユーザがオブジェクトに対して持っているアクセス権を安全に変更する

このアクセス権では、ユーザはすでに許可されているアクセス権についてだけ、許可、拒否、または指定なしの復元ができます。たとえば、ユーザ A が "オブジェクトを表示する" と "ユーザがオブジェクトに対して持っているアクセス権を安全に変更する" というアクセス権を持つ場合、ユーザ A は自分にそれ以上のアクセス権を許可できず、他のユーザに対してもこの 2 つのアクセス権 ("表示" と "アクセス権を安全に変更する") についてだけ許可または拒否できます。さらに、ユーザ A は、自分が[アクセス権を安全に変更する]アクセス権を持っているユーザについてだけ、オブジェクトへのアクセス権を変更できます。

次に、ユーザ A がユーザ B のオブジェクト O へのアクセス権を変更できる条件を示します。

- ユーザ A がオブジェクトに対する[アクセス権を安全に変更する]アクセス権を持つ。
- ユーザ B の、ユーザ A が変更しようとしている各アクセス権またはアクセスレベルが、ユーザ A に許可されている。
- ユーザ A が、ユーザ B に対する[アクセス権を安全に変更する]アクセス権を持つ。
- アクセスレベルが割り当てられている場合、ユーザ A が、変更しようとしているユーザ B のアクセスレベルに対して[アクセスレベルの割り当て]アクセス権を持つ。

アクセス権の範囲によって、委任管理者が割り当てることができる実効アクセス権をさらに制限できます。たとえば、委任管理者が、あるフォルダに対する[アクセス権を安全に変更する]および[編集]アクセス権を持っていてる場合でも、これらのアクセス権の範囲はフォルダのみに制限され、そのサブオブジェクトには適用されません。委任管理者はフォルダ(そのサブオブジェクトではなく)に対する[編集]アクセス権を許可し、そのアクセス権の範囲を["オブジェクトに適用"]に設定できます。一方、委任管理者に、ファイルに対する[編集]アクセス権が許可され、"サブオブジェクトに適用"範囲が設定されている場合、委任管理者はフォルダのサブフォルダに対して両方の範囲が設定された[編集]アクセス権を他の主体に許可できます。ただし、フォルダそのものについては、委任管理者は"サブオブジェクトに適用"範囲が設定された[編集]アクセス権しか許可できません。

さらに、委任管理者は、自分がアクセス権を安全に変更するアクセス権を持っていない他の主体が属するグループのアクセス権を変更することができません。これは、たとえば、同じフォルダに対するアクセス権を異なるユーザグループに許可する委任管理者を 2 人置き、一方の委任管理者がもう一方の委任管理者が制御するグループへのアクセスを拒否できないようにする場合に役に立ちます。[アクセス権を安全に変更する]権限はこれを保証します。通常、委任管理者は、別の委任管理者に対して[アクセス権を安全に変更する]権限を持つことができないためです。

アクセス権の継承設定を安全に変更する

このアクセス権を持っている委任管理者は、その委任管理者がアクセス権を持っているオブジェクトに対する他の主体の継承設定を変更することができます。他の主体の継承設定を正しく変更するには、委任管理者はオブジェクトおよび主体のユーザアカウントに対して、このアクセス権を持っていることが必要です。

7.5.2 オーナー権限

所有者権限は、アクセス権がチェックされるオブジェクトの所有者にのみ適用されるアクセス権です。BI プラットフォームでは、オブジェクトの所有者はそのオブジェクトを作成した主体です。その主体がシステムから削除された場合はオーナーシップは Administrator に戻ります。

所有者権限は、所有者ベースのセキュリティの管理で役に立ちます。たとえば、フォルダまたはフォルダの階層を作成して、そこでさまざまなユーザがドキュメントの作成や表示ができるようにし、自分自身のドキュメントしか修正または削除できないようようにすることができます。さらに、所有者権限は、ユーザが操作できるのは自分が作成したレポートのインスタンスのみとし、他のユーザのインスタンスは操作できないようにする場合にも役に立ちます。[スケジュール]アクセスレベルの場合は、この制限によって、ユーザは自分のインスタンスのみを編集、削除、一時停止、および再スケジュールできます。

所有者権限は対応する普通のアクセス権と似ていますが、主体が所有者権限を許可されていても、普通のアクセス権は拒否または指定されていない場合にのみ有効です。

7.6 アクセス権管理の推奨事項のまとめ

アクセス権管理について以下の点に注意してください。

- できるだけ[アクセスレベル]を使用します。これらの事前定義されたアクセス権のセットを使用すると、一般的なユーザの要件に関連するアクセス権をグループ化することで、管理を簡素化できます。
- アクセス権やアクセスレベルを最上位フォルダで設定します。継承を有効にすることで、これらのアクセス権は最小限の操作でシステムの最下位まで渡されます。
- 可能な限り、継承の破棄は避けてください。これによって、BI プラットフォームに追加したコンテンツのセキュリティを確保するための時間を削減できます。
- まずフォルダレベルでユーザおよびグループに適切なアクセス権を設定してから、そのフォルダにオブジェクトを公開します。デフォルトでは、あるフォルダに対するアクセス権が付与されているユーザやグループは、そのフォルダに以降公開するどのオブジェクトに対しても同じアクセス権を継承します。
- ユーザをユーザグループに整理し、アクセスレベルとアクセス権をグループ全体に割り当て、必要な場合はアクセスレベルとアクセス権を特定のメンバーに割り当てます。
- システム内の管理者ごとに個別の Administrator アカウントを作成し、それらを Administrators グループに追加して、システム変更の説明責任を向上させます。
- デフォルトでは、Everyone グループに付与される BI プラットフォームの最上位フォルダへのアクセス権は、極めて限定的です。インストール後に、Everyone グループメンバーのアクセス権を確認し、それに合わせてセキュリティを割り当てることをお勧めします。

8 BI プラットフォームのセキュリティ確保

8.1 セキュリティの概要

この節では、企業におけるセキュリティ問題に対する BI プラットフォームの取り組みと、管理者やシステム設計者がセキュリティに関する一般的な問題を解決する際に利用できる方法について説明します。

BI プラットフォームのアーキテクチャは、今日のビジネスや組織に影響を及ぼすさまざまなセキュリティの問題に対応できるよう設計されています。現在のリリースでは、不正アクセスから保護するために、分散セキュリティ、シングルサインオン、リソースアクセスセキュリティ、オブジェクトアクセス権の詳細な設定、サードパーティ認証など、さまざまな機能をサポートしています。

BI プラットフォームは、SAP BusinessObjects の Enterprise 製品シリーズのさまざまなコンポーネントに対応するフレームワークを備えています。この節では、セキュリティおよび関連機能を説明し、フレームワーク自体がどのように拡張され、セキュリティを維持しているかを説明します。したがって、この節では具体的な実行手順ではなく、概念的な情報を主に扱います。また、重要な手順へのリンクも提供します。

セキュリティ概念を簡単に説明後、以下のトピックについて詳しく説明します。

- データを保護するための暗号化モードおよびデータ処理セキュリティモードの使用方法。
- BI プラットフォームデプロイメント用の Secure Sockets Layer の設定方法。
- BI プラットフォームのファイアウォールの設定および更新のガイドライン。
- リバースプロキシサーバの設定。

8.2 プログラムオブジェクトの安全な使用

プログラムオブジェクトのスケジュール権限を持っているユーザには、そのプログラムを実行する権限があります。

Java プログラムの場合、ユーザは以下の処理を行うことができます。

- メインクラスを指定できます。プログラムの作成者は、セカンダリ/テストメインクラスが意図に反してプログラムに残っていないことを確認する必要があります。
- クラスパスを指定できます。システムに jar をアップロードする権限はありません。これは、特別に作成されたコードを実行する場合に使用できる場合があります。

プログラムオブジェクトのセキュリティを保護するための一般的な推奨事項

- サーバのログイン認証情報をユーザに提供しないでください。

- サーバでプログラムを実行するユーザアカウントには、最小限の権限を付与します。特に、SAP BusinessObjects Business Intelligence プラットフォームのインストールパスにはアクセスできないようにしてください。
- アプリケーション > セントラル管理コンソール > プログラムオブジェクト権限 でジョブを失敗させるを選択することをお奨めします。
- アクセス制御にはフォルダを使用することをお奨めします。セキュリティレベルが異なるプログラムオブジェクトは、異なるフォルダに配置する必要があります。

8.3 障害復旧計画

障害発生時に業務の機能ラインの継続を最大限に確保するには、特定の手順を実行して BI プラットフォームにおける組織の投資を保護する必要があります。この節では、組織の障害復旧計画のドラフトを作成するガイドラインを説明します。詳細については、この SAP ノートも参照してください。

一般的なガイドライン

- 定期的なシステムバックアップを実行し、必要に応じて、オフサイトのバックアップ媒体の一部のコピーを送信します。
- すべてのソフトウェア媒体を安全に保存します。
- すべてのライセンス文書を安全に保存します。

特定のガイドライン

災害復旧計画という点で特別な注意が必要なシステムリソースは、以下の 3 つです。

- ファイルリポジトリサーバのコンテンツ: レポートなど、所有権のあるコンテンツが含まれます。このコンテンツは定期的にバックアップする必要があります。障害が発生した場合、定期的なバックアップ処理をしていないと、そのようなコンテンツを再生成する方法はありません。
- CMS で使用されるシステムデータベース: このリソースには、ユーザ情報、レポート、その他の組織固有の機密情報など、デプロイメント用のすべての重要なメタデータが含まれます。
- データベース情報のキーファイル (.dbinfo ファイル): このリソースには、システムデータベースへのマスタキーが含まれます。何らかの理由でこのキーが使用不可の場合、システムデータベースにアクセスすることはできません。BI プラットフォームをデプロイ後、このリソースのパスワードを安全な既知の場所に格納することを強くお勧めします。パスワードがないとファイルを再生成できないため、システムデータベースへのアクセス権は失われます。

8.4 デプロイメントのセキュリティを確保するための一般的な推奨事項

以下は、BI プラットフォームのデプロイメントのセキュリティを確保するための推奨ガイドラインです。

- ファイアウォールを使用して、CMS とその他のシステムコンポーネント間の通信を保護します。可能な場合は、常に CMS をファイアウォールの後ろに隠します。最低限でも、システムデータベースがファイアウォールの後ろで安全になるようにします。
- ファイルリポジトリサーバに暗号化を追加します。システムを実行すると、所有権のあるコンテンツはこれらのサーバに格納されます。OS またはサードパーティツールを使用して、暗号化を追加します。
- リバースプロキシサーバは、Web アプリケーションサーバの前面にデプロイされ、1 つの IP アドレスの背後にその Web アプリケーションサーバが隠されます。この設定では、プライベートな Web アプリケーションサーバに向けたすべてのインターネットトラフィックはリバースプロキシサーバを通過するため、プライベート IP アドレスは隠されます。
- 企業のパスワードポリシーを厳重にします。ユーザパスワードが定期的に変更されるようにします。
- BI プラットフォームに同梱されたシステムデータベースおよび Web アプリケーションサーバのインストールを選択した場合は、関連ドキュメントにアクセスして、これらのコンポーネントが十分なセキュリティ設定でデプロイされるようにする必要があります。
- デプロイメントのクライアントとサーバの間で行われるすべてのネットワーク通信に、Secure Sockets Layer(SSL)プロトコルを使用します。
- プラットフォームのインストールディレクトリとサブディレクトリがセキュリティ保護されていることを確認します。システム操作時に、重要な一時データがこれらのディレクトリに保存される場合があるためです。
- Central Management Console (CMC) へのアクセスは、ローカルアクセスのみに制限する必要があります。CMC のデプロイメントオプションの詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。
- デフォルトでは、Web Intelligence エラーメッセージにはデータベーススキーマの情報が含まれます。データベーススキーマの情報を除いたエラーメッセージを表示するには、次の手順に従います。
  1. `WebIContainer_ServerDescriptor.xml` 設定ファイルを開いて編集します。デフォルトでは、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64config` にあります。
  2. 以下のパラメータを False に変更します。`WebiParamDetailedDbErrorsEnabled = False`。

> **⚠ 警告**
>
> 編集用以外のプレースホルダは、いかなる手段でも変更しないでください。システム管理者は、(ノード管理を目的とする) 管理者グループの適切な担当者のみがノードに対する編集権限を持っていることを確認する必要があります。管理者グループの他のメンバーを含むすべてのユーザは、適切なセキュリティ権限を適用することで、ノードオブジェクトの表示/管理を制限する必要があります。プレースホルダ値のいずれかが誤って破損し、CMS が起動しない場合は、SAP ノート 3269127 を参照してください。

> **ⓘ 注記**
>
> BI ランドスケープへの悪意のある干渉を回避するためにプレースホルダの変更を制限する方法については、以下の SAP Knowledge Base Article 3278916 を参照してください。

関連情報

SSL プロトコルの設定 [180 ページ]
パスワード制限 [155 ページ]
同梱されたサードパーティサーバのセキュリティ設定 [150 ページ]

8.5 同梱されたサードパーティサーバのセキュリティ設定

BI プラットフォームに同梱されたサードパーティのサーバコンポーネントのインストールを選択した場合は、SAP SQL Anywhere および Apache Tomcat の公式ドキュメントのセキュリティの節を確認することをお奨めします。

8.6 アクティブな信頼関係

ネットワーク接続環境での 2 つのドメイン間の信頼関係とは通常、一方のドメインで認証されたユーザを、もう一方のドメインで認識できるようにする接続を意味します。信頼関係によりセキュリティを維持したまま、ユーザはアカウント情報を何度も入力することなく、複数のドメインにあるリソースにアクセスできるようになります。

BI プラットフォーム環境内でアクティブな信頼関係は同じように機能し、各ユーザはシステム上のリソースにシームレスにアクセスできます。ユーザが認証されてアクティブなセッションを許可されると、ほかのすべての BI プラットフォームコンポーネントで、アカウント情報の入力なしにユーザのリクエストとアクションを処理できます。したがって、アクティブな信頼関係は、BI プラットフォームの分散セキュリティの基盤となります。

8.6.1 ログオントークン

エンコードされた文字列のログオントークンは、その使用属性を定義してユーザのセッション情報を保存します。ログオントークンの使用属性は、その生成時に指定されます。これらの属性により、ログオントークンに制限を適用して、悪意のあるユーザがログオントークンを使用する危険性を減らすことができます。現在のログオントークンの使用属性は、次のとおりです。

- 分数
  この属性は、ログオントークンの有効期間を制限します。
- ログオン数
  この属性は、ログオントークンを使用して BI プラットフォームにログオンできる回数を制限します。

いずれの属性も、権限を持たないユーザが権限を持つユーザから取得したログオントークンを使用して BI プラットフォームに不正にアクセスするのを防ぐことができます。

> **注記**
>
> ログオントークンの Cookie への保存は、ブラウザとアプリケーションサーバまたは Web サーバの間のネットワークがセキュリティで保護されていない場合、たとえば、接続がパブリックネットワーク上で確立されてい

て、SSL または信頼できる認証を使用していない場合、セキュリティ上のリスクになる可能性があります。ブラウザとアプリケーションサーバまたは Web サーバの間のセキュリティ上のリスクを減らすために、Secure Sockets Layer(SSL)を使用することをお勧めします。

ログオン Cookie が無効になっており、Web サーバまたは Web ブラウザでタイムアウトが発生した場合、ユーザにはログオン画面が表示されます。Cookie が有効になっており、サーバまたはブラウザでタイムアウトが発生した場合、ユーザは、再度シームレスにシステムにログオンされます。ただし、状態の情報は Web セッションと結びついているため、そのユーザの状態は失われます。たとえば、ユーザがナビゲーションツリーを展開して特定のアイテムを選択していた場合、ツリーはリセットされます。

BI プラットフォームの場合、デフォルトでは、Web クライアントでログオントークンが有効になっていますが、BI ラウンチパッドのログオントークンは無効にできます。クライアントでログオントークンを無効にすると、ユーザセッションは Web サーバまたは Web ブラウザのタイムアウトにより制限されます。セッションの期限が切れた場合、ユーザは BI プラットフォームに再度ログオンする必要があります。

8.6.2 分散セキュリティのチケットメカニズム

通常、多数のユーザへのサービス専用に使用される企業システムでは、分散セキュリティが必須となります。企業システムでは、信頼の委任 (ユーザの代理として別のコンポーネントを動作できる機能) などの機能をサポートするために、分散セキュリティが必要になる場合があります。

BI プラットフォームは、分散セキュリティに対応できるように、チケットメカニズム (Kerberos チケットメカニズムに類似したメカニズム) を実装しています。CMS は、コンポーネントが特定のユーザに代わってアクションを実行することを承認するチケットを付与します。BI プラットフォームでは、チケットのことをログオントークンといいます。

このログオントークンは、Web 上で一般的に使用されています。BI プラットフォームで初めて認証されたユーザには、CMS からログオントークンが与えられます。ユーザの Web ブラウザでは、このログオントークンをキャッシュに保存します。ユーザが新しいリクエストを送信すると、ほかの BI プラットフォームコンポーネントは、ログオントークンをユーザの Web ブラウザから読み込むことができます。

8.7 セッションとセッショントラッキング

"セッション"とは一般に、2 つのコンピュータ間の情報交換を可能にするクライアント/サーバ接続を指します。セッションの"状態"とは、セッションの属性、設定、内容を表すデータのセットを指します。Web 上でクライアント/サーバ接続を確立すると、HTTP の特性により、各セッションの有効期間は単一ページの情報に制限されます。このため、Web ブラウザでは単一の Web ページが表示されている間だけ、各セッションの状態をメモリに保持します。別の Web ページに移動すると、最初のセッションの状態はすぐに破棄され、次のセッションの状態に置き換えられます。したがって、1 つのセッションの状態に含まれる情報を別のセッションで再使用する場合、Web サイトや Web アプリケーションでは何らかの方法でセッションの状態を保存する必要があります。

BI プラットフォームでは、2 つの一般的な方法によってセッション状態を保存します。

- "Cookie" は、セッション状態を保存する、クライアント側の小さいテキストファイルです。Cookie は、後で使用できるように、ユーザの Web ブラウザによってキャッシュされます。BI プラットフォームログオントークンは、この方法の一例です。

- セッション変数は、セッション状態を保存する、サーバ側のメモリの一部分です。BI プラットフォームからユーザにシステム上のアクティブな ID が付与されると、ユーザの認証の種類などの情報がセッション変数に保存されます。セッションが継続している間、ユーザにアカウント情報の再入力を要求したり、次のリクエストの完了に必要なタスクを繰り返す必要はありません。
  Java デプロイメントでは、セッションは .jsp リクエストを処理するために使用されます。.NET デプロイメントでは、.aspx リクエストを処理するために使用されます。

> **注記**
>
> 理想的には、ユーザがシステム上でアクティブになっている間は、セッション変数が保持される必要があります。また、セキュリティを確保して、リソースの使用量を最小限にするには、ユーザがシステム上での作業を完了した時点ですぐにセッション変数が破棄される必要があります。ただし、Web ブラウザと Web サーバ間のやり取りがステートレスになることがあるので、ユーザが明示的にログオフしない場合は、いつユーザがシステムからログオフしたか、わかりにくい場合があります。この問題に対処するため、BI プラットフォームはセッショントラッキングを実装しています。

8.7.1 CMS セッショントラッキング

CMS は単純なトラッキングアルゴリズムを実装しています。ユーザがログオンすると、CMS セッションがユーザに付与されます。ユーザがログオフするか、Web アプリケーションサーバセッション変数が解放されるまで CMS はそのセッションを維持します。

Web アプリケーションサーバセッションは、まだセッションがアクティブであることを繰り返し CMS に通知するように設計されているので、CMS セッションは Web アプリケーションサーバセッションが存在する限り維持されます。Web アプリケーションサーバセッションが CMS と通信できないまま 10 分経過すると、CMS は CMS セッションを終了します。この方法によって、クライアント側のコンポーネントが不正にシャットダウンした場合に対処します。

8.7.2 セッションの管理

CMC で、セッションを表示および終了できます。

セントラル管理コンソール (CMC) で、ユーザセッションを表示および終了できます。 たとえば、複数のセッションを使用中のユーザを確認することができます。 システムリソースの使用量が多すぎるセッションや、非常に古いセッションを終了することもできます。 また、システムのダウンタイムやアップグレードの準備をする際に、セッションを終了する必要が生じることもあります。

8.7.2.1 セッションリストを表示する

CMC でセッションを表示します。

セントラル管理コンソールで、セッションのリストを表示できます。

1. 管理者として CMC にログインします。

2. 管理エリアで、セッションをクリックします。

クラスタのユーザセッションのリストが表示されます。 列ヘッダをクリックして、ユーザ名、開いているセッションの数、またはログオン時刻によってリストを並べ替えることができます。 また、ユーザ名、セッション数、またはログオン時刻をクリックして、そのユーザのセッションの詳細を下側のペインに表示することもできます。

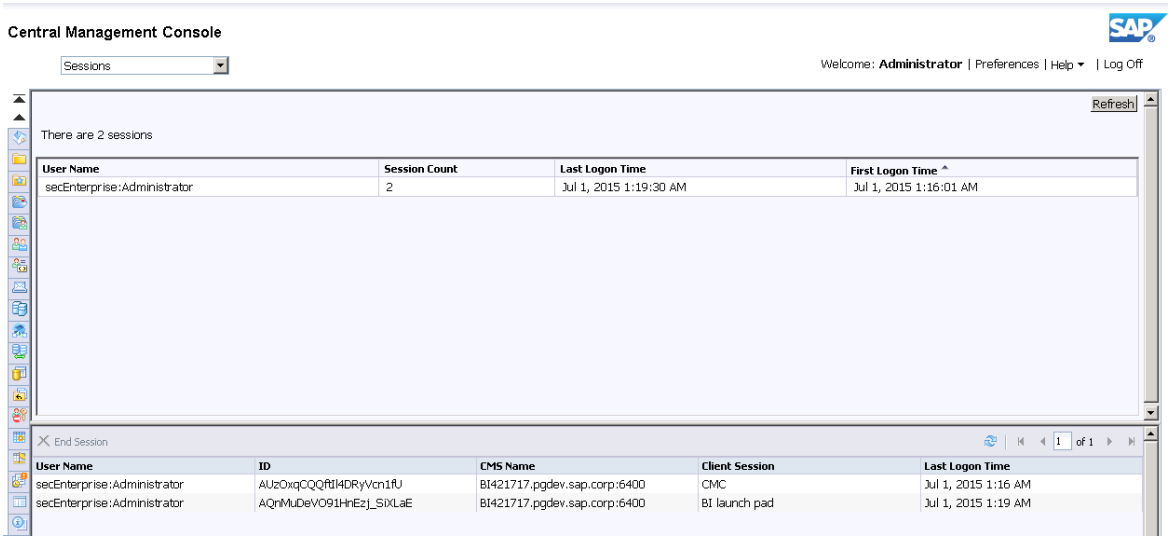
8.7.2.2 セッションを終了する

CMC でセッションを終了します。

1 つまたは複数のセッションを終了できます。

1. 管理者として CMC にログインします。
2. 管理エリアで、セッションをクリックします。

   クラスタのユーザセッションのリストが表示されます。



3. ユーザ名、セッション数、またはログオン時刻をクリックして、下側のペインにユーザのセッションを表示します。
4. クリックして 1 つのセッションを選択するか、`Ctrl` + `クリック` で複数のセッションを選択します。
5. セッション終了をクリックします。

> ⓘ 注記
>
> ユーザがブラウザを閉じると、ユーザセッションがリリースされます。

> ⓘ 注記
>
> セッションを終了するには、CMS オブジェクトの右側に“オブジェクトを編集する”が表示される必要があります。

> ⓘ 注記
>
> 現在の管理者セッションを終了することはできません。

8.7.3 要再起動セッションをクリアするスクリプト

スクリプト

要再起動セッションをクリアし、ログイン待ち状態のユーザ向けに不使用ライセンスを解放するためのスクリプトが導入されました。このスクリプトは手動で終了するまで実行され、要再起動セッションのチェックと強制終了が 10 分おきに行われます。

- Windows では、このスクリプトは `<BI_Install_Dir>¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib¥StaleSessionCleaner.jar` にあります。
- UNIX では、このスクリプトは `<BI_Install_Dir>/sap_bobj/enterprise_xi40/java/lib/StaleSessionCleaner.jar` にあります。

このスクリプトでは、以下の構文が使用されます。

コード構文

```
java -jar StaleSessionCleaner.jar <username> <password>
<machine:port><authentication> <logdir>
```

8.8 環境の保護

"環境の保護"とは、クライアントとサーバのコンポーネントが通信する環境全体のセキュリティのことです。インターネットと Web ベースのシステムは柔軟性に富んでいて機能範囲が広いため、ますます普及していますが、実行環境のセキュリティを確保しにくいという側面があります。BI プラットフォームをデプロイする場合、環境の保護は次の 2 つの通信領域に分けられます。Web ブラウザから Web サーバへの通信領域と、Web サーバから BI プラットフォームへの通信領域です。

8.8.1 Web ブラウザから Web サーバへ

Web ブラウザと Web サーバ間でデータが転送されるときには、ある程度のセキュリティが一般的に必要です。適切なセキュリティ対策には通常、次の一般的なタスクが含まれます。

- データ通信が安全に行われるようにする
- 有効なユーザだけが Web サーバから情報を取得できるようにする

注記

これらのタスクは通常、Secure Sockets Layer (SSL) プロトコルやそれに類似するその他のメカニズムなど、さまざまなセキュリティメカニズムを使用して Web サーバで処理されます。ブラウザとアプリケーションサーバまたは Web サーバの間のセキュリティ上のリスクを減らすために、SSL を使用することをお勧めします。

Web ブラウザと Web サーバ間の通信のセキュリティは、BI プラットフォームから独立して維持する必要があります。クライアント接続のセキュリティの維持や管理の詳細は、Web サーバのマニュアルを参照してください。

8.8.2 BI プラットフォームを対象とする Web サーバ

一般に、Web サーバとその他の企業イントラネット (BI プラットフォームなど) の間の通信領域のセキュリティを維持するには、ファイアウォールが使用されます。BI プラットフォームは、IP フィルタリングまたは静的ネットワークアドレス変換 (NAT) を使用するファイアウォールをサポートします。サポートされる環境には、複数のファイアウォール、Web サーバ、またはアプリケーションサーバなどが含まれます。

8.8.3 悪意あるログオンに対する保護

多くの場合、システムのセキュリティレベルがどれほど高くても、攻撃を受けやすい場所が少なくとも 1 つは存在します。それは、ユーザがシステムに接続する場所などです。システムに不正にアクセスしようとする悪意のあるユーザには、有効なユーザ名とパスワードを単に推測するという方法が残されているため、このような場所を完全に保護することはほとんど不可能です。

BI プラットフォームでは、悪意のあるユーザがシステムにアクセスする可能性を減らすための技術をいくつか実装しています。次に示すさまざまな制限は、Enterprise アカウントのみに適用されます。つまり、これらの制限は外部ユーザデータベース(LDAP または Windows AD)にマップしたアカウントには適用されません。ただし、通常は外部システムでも、同じような制限を外部アカウントに設定することができます。

8.8.4 パスワード制限

パスワード制限を適用すると、デフォルト Enterprise 認証を行うユーザに比較的複雑なパスワードを作成させることができます。次のオプションを有効にできます。

1. 大文字と小文字を含むパスワードを要求する
   このオプションによって、少なくとも 1 つの大文字と 1 つの小文字がパスワードに含まれるようになります。このオプションは、管理者が変更しない限り、デフォルトで選択されています。
2. 数値を含むパスワードを要求する
   このオプションによって、少なくとも 1 つの数字がパスワードに含まれるようになります。
3. 特殊文字を含むパスワードを要求する
   このオプションによって、少なくとも 1 つの特殊文字がパスワードに含まれるようになります。

多少でも複雑なパスワードを使用することで、悪意のあるユーザが有効なユーザのパスワードを簡単に推測する可能性を減らすことができます。

8.8.5 ログオンの制限

ログオンの制限は主に、辞書攻撃(悪意のあるユーザが有効なユーザ名を取得し、辞書のあらゆる語句を試すことによって対応するパスワードを探し当てるという攻撃方法)を防止する役割を果たします。最新のハードウェアの処理速度であれば、悪質なプログラムで 1 分間に何百万ものパスワードを推測できます。辞書攻撃を防止するため、BI プラットフォームは、次のログオン試行までの時間遅延 (0.5 ～ 1.0 秒) を強制する内部メカニズムを備えています。さらに、BI プラットフォームには辞書攻撃のリスク減少に使用できる次のカスタマイズ可能オプションも用意されています。

- ログオンに N 回失敗した後はアカウントを無効にする
- ログオン失敗回数を N 分後にリセットする
- N 分後に再びアカウントを有効にする

8.8.6 ユーザ制限

ユーザ制限を適用すると、デフォルト Enterprise 認証を行うユーザに新しいパスワードを定期的に作成させることができます。次のオプションを有効にできます。

- N 日ごとにパスワードの変更を要求する
- 最近使用した N 個のパスワードの再使用を禁止する
- N 分経過するまでパスワードの変更を禁止する

これらのオプションには、さまざまな利点があります。第一に、辞書攻撃を試みる悪意のあるユーザは、パスワードが変更されるたびに、最初からやり直さなければならなくなります。しかも、パスワードの変更は各ユーザの最初のログオン時刻に基づいて行われるため、悪意のあるユーザは、特定のパスワードがいつ変更されるかを簡単に判断できません。また、悪意のあるユーザがほかのユーザのアカウント情報を推測するか取得した場合でも、それらのアカウント情報の有効期間は限られています。

8.8.7 guest アカウントの制限

BI プラットフォームは、guest アカウントの匿名シングルサインオンをサポートします。そのため、ユーザ名とパスワードを指定せずに BI プラットフォームに接続すると、システムにより guest アカウントのユーザとして自動的に記録されます。guest アカウントに保護されたパスワードを割り当てたり、guest アカウントを完全に無効にすると、このデフォルトの動作は無効になります。

8.9 監査セキュリティ設定の変更

以下のデフォルトのセキュリティ設定に対する変更は、BI プラットフォームによって監査されません。

- Web アプリケーションのプロパティファイル (BOE、Web サービス)
- TrustedPrincipal.conf
- BI 起動パッドおよび OpenDocument で実行されたカスタマイズ

通常、CMC の外部で実行されたすべてのセキュリティ設定の変更は、監査されません。これはまた、セントラル設定マネージャ (CCM) を介して実行された変更にも適用されます。CMC を介してコミットされた変更は、監査することができます。

8.10 処理拡張機能

BI プラットフォームでは、カスタマイズした処理拡張機能を使用して、レポート環境のセキュリティをさらに強化できます。処理拡張機能は、動的にロードされるコードのライブラリであり、特定の BI プラットフォームの表示またはスケジュールリクエストに対して、システムで処理される前にビジネスロジックを適用します。

処理拡張機能のサポートにより、BI プラットフォーム管理 SDK では、リクエストに対する開発者の介入を可能にする "ハンドル" が事実上公開されています。これにより、開発者は、レポートの処理前に実行される選択式をリクエストに追加できます。

代表的な例として、行レベルセキュリティを適用するレポート処理拡張機能があります。この種類のセキュリティは、1 つまたは複数のデータベーステーブル内の行ごとのデータアクセスを制限します。開発者は、レポートの表示リクエストまたはスケジュールリクエストを(Job Server、Processing Server または Report Application Server によって処理される前に)受信する、動的にロードされるライブラリを作成します。開発者のコードで処理ジョブを所有しているユーザがまず特定され、サードパーティシステムでユーザのデータアクセス権が検索されます。次に、データベースから返されるデータを制限するために、レコード選択式が生成されて、レポートに追加されます。この処理拡張機能は、カスタマイズした行レベルのセキュリティを BI プラットフォーム環境に組み込む手段として動作します。

処理拡張機能を有効にすると、適切な BI プラットフォームサーバコンポーネントが実行時に動的に処理拡張機能をロードするよう設定できます。SDK には、開発者が処理拡張機能の作成に使用できる API が用意されています。この API の完全な情報は文書化されています。詳細については、製品メディアに収録されている開発者用ドキュメントを参照してください。

8.11 ウィルススキャンインタフェース

CMC、BI ラウンチパッド、Rest Web サービス、およびカスタム SDK アプリケーションを使用して、さまざまな種類のファイル (Adobe Acrobat、Microsoft Excel、Microsoft Word、Microsoft PowerPoint、Lumira、Crystal Reports、Web Intelligence など) を BI プラットフォームにコミットできます。これらのファイルは、サイズチェック (ファイルサイズがゼロでないことを確認するため) および出力先ディレクトリに対する権限チェックの対象になります。BI 4.2 SP4 でのウィルススキャンインタフェースの導入により、BI プラットフォームにコミットするファイルもウィルススキャンにコミットされるため、このようなファイルの内容は感染していない、ウィルスが除去された状態になります。

ファイルは、以下の場合にウィルススキャンの対象になります。

- 新しいファイルを追加する
- ドキュメントを '名前を付けて保存' する
- ドキュメントをコピーする
- 'ドキュメントを BI 受信ボックスに送信' する
- ドキュメントのインスタンスを作成する
- ファイルリポジトリサーバに新しいファイルをコミットする操作を実行する

> **注記**
>
> BI 4.2 SP4 で (ウィルススキャンを有効にした後) BI プラットフォームに新しくコミットされたファイルのみがウィルススキャンの対象になります。

8.11.1 ウィルススキャンの有効化

入力と出力の両方のファイルリポジトリサーバについて、BI プラットフォームにコミットされたファイルに対してウィルススキャンを有効にできます。

SAP 認定ベンダーからウィルススキャンアダプタ (VSA) ライブラリをダウンロードしておきます。SAP 認定ベンダーの一覧については、http://global.sap.com/community/ebook/2013_09_adpd/enEN/search.html#search=NW-VSI を参照してください。

> **注記**
>
> 新しいプラットフォームまたはベンダーのサポートが必要な場合は、それぞれのベンダーにお問い合わせください。

入力ファイルリポジトリサーバでウィルススキャンを有効にするには、以下の手順を実行します。

1. CMC にログオンします。
2. サーバ > サーバの一覧 に移動します。
3. 入力ファイルリポジトリサーバを右クリックし、ドロップダウンから [プロパティ] を選択します。

   [プロパティ] ウィンドウが表示されます。
4. [*Input Filestore* サービス] セクションで、[ウィルススキャンの有効化] チェックボックスをオンにします。
5. [ウィルススキャンアダプタファイルの場所] フィールドに、ウィルススキャンアダプタライブラリファイルへの絶対パスを入力します。
6. [保存して閉じる] を選択します。

   > **注記**
   >
   > - BI 4.2 SP4 では、BI プラットフォームにコミットされたすべてのファイルに対してウィルススキャンがデフォルトで無効になっています。
   > - ウィルススキャンを有効にするには、GUI または CLI を使用します。ウィルススキャンを有効にするためにファイルリポジトリサーバで指定する必要があるコマンドライン引数は `vsaFileLoc` です。
   > - 同様の手順に従って、出力ファイルリポジトリサーバでウィルススキャンを有効にできます。入力および出力ファイルリポジトリサーバが複数ある場合は、各サーバでウィルススキャンを有効にしてください。
   > - ウィルススキャンを有効にした後で変更を有効にするには、ファイルリポジトリサーバを再起動する必要があります。

8.12 BI プラットフォームのデータセキュリティ

BI プラットフォームシステムの管理者は、以下の方法で機密データのセキュリティを管理します。

- クラスタレベルのセキュリティ設定によって、どのアプリケーションおよびクライアントが CMS にアクセスできるかが指定されます。この設定は、セントラル設定マネージャで管理します。
- 2 つのキーを使用する暗号化システムによって、CMS リポジトリへのアクセスと、リポジトリ内のオブジェクトの暗号化/解読に使用するキーが管理されます。CMS リポジトリへのアクセスは、セントラル設定マネー

ジャを使って設定します。これに対し、セントラル管理コンソールには、暗号キーの専用管理エリアがあります。

これらの機能を使用して、管理者は特定のデータセキュリティコンプライアンスのレベルに BI プラットフォームデプロイメントを設定し、CMS リポジトリ内のデータの暗号化と解読に使用される暗号キーを管理できます。

8.12.1 データ処理セキュリティモード

BI プラットフォームは、2 つのデータ処理セキュリティモードで動作できます。

- デフォルトのデータ処理セキュリティモード。このモードで実行されているシステムでは、ハードコードされた暗号キーが使用され、特定の標準に準拠しない場合があります。デフォルトモードでは、旧バージョンの BI プラットフォームクライアントツールおよびアプリケーションとの下方互換性を維持できます。
- データセキュリティモードは、FIPS 140-2 標準に規定されている連邦情報処理標準 (FIPS) のガイドラインに準拠するよう作られています。このモードでは、FIPS 準拠のアルゴリズムと暗号化モジュールを使用して機密データを保護します。BI プラットフォームが FIPS 準拠モードで実行されている場合は、FIPS ガイドラインに準拠しないすべてのクライアントツールおよびアプリケーションは自動的に無効化されます。BI プラットフォームクライアントツールおよびアプリケーションは、FIPS 2 標準に準拠するよう作られています。BI プラットフォームが FIPS 準拠モードで実行されている場合は、旧バージョンのクライアントおよびアプリケーションは動作しません。

データ処理モードは、システムユーザに明白です。両方のデータ処理セキュリティモードで、機密データは内部暗号化エンジンによってバックグラウンドで暗号化および解読されます。

以下の場合は、FIPS 準拠モードを使用することをお勧めします。

- BI プラットフォームデプロイメントが、従来の BI プラットフォームクライアントツールまたはアプリケーションを使用またはこれらと通信する必要がない場合。
- 組織のデータ処理標準およびガイドラインでハードコードされた暗号化キーの使用が禁止されている場合。
- 組織で、FIPS 140-2 標準に従って機密データのセキュリティを保護することが求められている場合。

データ処理セキュリティモードが、Windows と UNIX の両プラットフォームでセントラル設定マネージャを使って設定される場合。クラスタ環境のすべてのノードを同じモードに設定する必要がある場合。

8.12.1.1 Windows で FIPS 準拠モードをオンにする

BI プラットフォームのインストール後、デフォルトで FIPS 準拠モードはオンになっています。

1. CCM を起動するには、[プログラム] > *SAP Business Intelligence* > *SAP BusinessObjects BI プラットフォーム 4* > [セントラル設定マネージャ] をクリックします。
2. CCM で Server Intelligence Agent (SIA) を右クリックし、[停止] を選択します。

   > ⚠ 警告
   >
   > SIA ステータスが [停止] になるまで、手順 3 に進まないでください。

3. SIA を右クリックして、[プロパティ] を選択します。
   [プロパティ] ダイアログボックスが表示され、[プロパティ] タブが表示されます。

4. [コマンド] フィールドに -fips を追加し、[適用] クリックします。
5. [*OK*] をクリックして [プロパティ] ダイアログボックスを閉じます。
6. SIA を再起動します。

これで、SIA は FIPS 準拠モードで動作しています。

BI プラットフォームデプロイメント内のすべての SIA で FIPS 準拠設定をオンにする必要があります。

8.12.1.2 UNIX で FIPS 準拠モードをオンにする

以下の手順を実行する前に、BI プラットフォームデプロイメントのすべてのノードを停止する必要があります。

BI プラットフォームのインストール後、デフォルトで FIPS 準拠モードはオフになっています。デプロイメント内のすべてのノードの FIPS 準拠モード設定をオンにするには、以下の手順を実行します。

1. <INSTALLDIR>/sap_bobj ディレクトリから、編集用の ccm.config ファイルを開きます。
2. ノード起動コマンドパラメータに -fips を追加します。

   ノード起動コマンドパラメータは、<NODENAME>LAUNCH という形式で表示されます。たとえば、ノード名が "SAP" の場合、ノード起動コマンドパラメータは SAPLAUNCH となります。
3. 変更を保存し、[終了] します。
4. ノードを再起動します。

これで、ノードは FIPS 準拠モードで動作しています。

BI プラットフォームデプロイメント内のすべてのノードで FIPS 準拠設定をオンにする必要があります。

8.12.1.3 Windows で FIPS 準拠モードをオフにする

以下の手順を実行する前に、BI プラットフォームデプロイメントのすべてのサーバを停止する必要があります。

デプロイメントが FIPS 準拠モードで実行されている場合は、以下の手順を実行して、設定をオフにします。

1. CCM で Server Intelligence Agent (SIA) を右クリックし、[停止] を選択します。

   > ⚠ 警告
   >
   > ノードのステータスが [停止] になるまで、手順 2 に進まないでください。

2. SIA を右クリックし、[プロパティ]を選択します。
   [プロパティ] ダイアログボックスが表示され、[プロパティ] タブが表示されます。
3. [コマンド] フィールドから -FIPS を削除し、[適用] をクリックします。
4. [*OK*] をクリックして [プロパティ] ダイアログボックスを閉じます。
5. SIA を再起動します。

8.12.2 Administrator アカウント

BI プラットフォームでは、自動的に最初の Administrator アカウントが作成されます。個人ごとに、Administrators グループにアカウントを作成することをお奨めします。

管理者ユーザには、[オブジェクトに対するユーザの権限を変更する] 権限が自動的に付与されます。管理者のアカウントを作成したら、必ず初期管理者アカウントを無効化してください。

8.12.3 接続のアクセス権

デフォルトでは、接続が認証情報を使用して定義されている場合、管理者はパスワードを含む接続詳細にアクセスできます。

ここでは、管理者がデータソースにアクセスすることが想定されていない場合に、接続に最小権限の原則を適用する方法について説明します。

[接続をローカルにダウンロード] 権限の制限

[接続をローカルにダウンロード] 権限は、接続を管理するユーザにのみ厳密に必要となります (接続のアクセス権 [1099 ページ]を参照)。この権限は、グループではなく、個々のユーザにのみ付与する必要があります。グループに権限がある場合、そのグループに追加されたすべてのユーザが接続の詳細にアクセスできます。

接続を完全に保護するには、次の手順に従います。

1. 接続を管理するユーザに [接続をローカルにダウンロード] 権限を付与します。
2. Administrators と Universe Designer のユーザグループについて、接続の最上位フォルダに対する [接続をローカルにダウンロード] を拒否します。

ユーザが自分自身に権限を付与できないようにするには、以下の節を参照してください。

[オブジェクトに対するユーザの権限を変更する] 権限の保護

デフォルトの [オブジェクトに対するユーザの権限を変更する] 権限によって、ユーザは、アクセス権を持っていない場合でも、その権限を付与できます。接続について、これを [ユーザがオブジェクトに対して持っているアクセス権を安全に変更する] 権限によって置き換える必要があります。Administrators が [接続をローカルにダウンロード] 権限を持っていない場合は、他のユーザに付与する権限を持っていないことが必要です。

最上位の接続フォルダ:

1. Administrators および Universe Designer グループに対して、[ユーザがオブジェクトに対して持っているアクセス権を安全に変更する] 権限を付与します。
2. 前のセクションで定義したように、[ユーザがオブジェクトに対して持っているアクセス権を安全に変更する] 権限を、接続を管理するユーザに付与します。これらのユーザは、[接続をローカルにダウンロード] 権限を付与する権限を持つようになります。

3. Administrators および Universe Designer グループの [オブジェクトに対するユーザの権限を変更する] 権限を拒否します。

8.13 BI プラットフォームの暗号化

機密データ

BI プラットフォームの暗号化は、CMS リポジトリに保存された機密データを保護します。機密データには、ユーザの認証情報、データソース接続データ、およびパスワードを保存するその他の情報オブジェクトなどがあります。このデータは、個人情報を保証し、データの破損を防止し、アクセスコントロールを維持するために暗号化されます。必要なすべての暗号化リソース (暗号化エンジン、RSA ライブラリなど) は、各 BI プラットフォームデプロイメントにデフォルトでインストールされています。

BI プラットフォームシステムでは、2 つのキーを使用する暗号化システムを使用します。

暗号化キー

機密データの暗号化と解読は、内部の暗号化エンジンと通信する SDK によってバックグラウンドで処理されます。システム管理者は対称暗号化キーを使って、特定のデータブロックを直接、暗号化または解読することなく、データセキュリティを管理します。

BI プラットフォームでは、暗号化キーと呼ばれる対称暗号化キーを使用して機密データを暗号化/解読します。セントラル管理コンソールには、暗号化キーのための専用管理エリアがあります。[暗号化キー] を使用して、キーを表示、生成、無効化、削除します。 機密データの暗号化に必要なキーは削除できません。

クラスタキー[クラスタキー]

クラスタキーは、CMS リポジトリに保存されている暗号化キーを保護するための対称キーラッピングキーです。対称キーアルゴリズムを使用して、クラスタキーは CMS リポジトリへのアクセスコントロールのレベルを維持します。BI プラットフォームの各ノードには、インストールセットアップ時にクラスタキーが割り当てられます。システム管理者は、CCM を使用してクラスタキーをリセットできます。

8.13.1 クラスタキーの操作

BI プラットフォームのインストール設定中、Server Intelligence Agent 用に 8 文字のクラスタキーが作成されます。このキーは、CMS リポジトリ内のすべての暗号化キーを暗号化するときに使用されます。クラスタキーが正しくない場合は、CMS にアクセスできません。

クラスタキーは、`dbinfo` ファイルに暗号化された形式で保存されます。`dbinfo` ファイル名は、次の規則に従います。`_boe_<sia_name>.dbinfo`。`<sia_name>` は、クラスタの Server Intelligence Agent の名前です。

Windows では、このファイルは次のディレクトリに保存されます。`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64`

Unix システムでは、このファイルは以下の `<INSTALLDIR>/sap_bobj/enterprise_xi40/` の下のプラットフォームディレクトリに格納されます。

Unix プラットフォーム	プラットフォームディレクトリ
AIX	`<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000_64/`
Solaris	`<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparcv9/`
Linux	`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/`

> **注記**
>
> 指定されたノードのクラスタキーは、dbinfo ファイルからは取得できません。クラスタキーの保護については、システム管理者がよく検討して慎重に行うことをお勧めします。

管理者権限を持つユーザのみがクラスタキーをリセットできます。リセットが必要な場合は、CCM を使用し、デプロイメント内のすべてのノードに対してクラスタキーをリセットします。新しいクラスタキーが自動的に使用され、CMS リポジトリ内の暗号化キーがラップされます。

8.13.1.1 Windows 上でクラスタキーをリセットする

ノードのクラスタキーをリセットする前に、Server Intelligence Agent によって管理されているすべてのサーバが停止していることを確認します。

1. CCM を起動するには、[プログラム] > *SAP Business Intelligence* > *SAP BusinessObjects BI プラットフォーム 4* > [セントラル設定マネージャ] に移動します。
2. CCM で Server Intelligence Agent (SIA) を右クリックし、[停止] を選択します。

   > **警告**
   >
   > SIA ステータスが [停止] になるまで、手順 3 に進まないでください。

3. Server Intelligence Agent (SIA) を右クリックし、[プロパティ] を選択します。
   [プロパティ]ダイアログボックスが表示されます。
4. [設定] タブをクリックします。
5. [*CMS クラスタキー設定*] の [変更] をクリックします。
   警告メッセージが表示されます。
6. [はい] をクリックして続行します。
   [クラスタキーの変更] ダイアログボックスが表示されます。
7. [新規クラスタキー] フィールドおよび [新規クラスタキーの確認] フィールドに同じ 8 文字のキーを入力します。

> ⓘ 注記
>
> Windows では、クラスタキーは大文字と小文字を組み合わせた文字で構成される必要があります。または、ランダムキーを生成することもできます。FIPS に準拠するには、ランダムキーが必要です。

8. [*OK*] をクリックすると、新しいクラスタキーがシステムに送信されます。
   クラスタキーが正常にリセットされたことを確認するメッセージが表示されます。
9. SIA を再起動します。

複数ノードのクラスタでは、BI プラットフォームデプロイメント内のすべての SIA のクラスタキーを新しいクラスタキーにリセットする必要があります。

8.13.1.2 UNIX 上でクラスタキーをリセットする

ノードのクラスタキーをリセットする前に、そのノードによって管理されているすべてのサーバが停止していることを確認します。

1. `<INSTALLDIR>/sap_bobj` ディレクトリに移動します。
2. 「**`./cmsdbsetup.sh`**」と入力して *Enter* キーをを押します。
   [*CMS データベースのセットアップ*] 画面が表示されます。
3. ノードの名前を入力し、*Enter* キーを押します。
4. 「**2**」と入力してクラスタキーを変更します。
   警告メッセージが表示されます。
5. [はい] を選択して続行します。
6. 指定されたフィールドに新しいクラスタキーを入力し、*Enter* キーを押します。

> ⓘ 注記
>
> キーが 6 文字以上で、大文字、小文字、数字、または区切り記号の 2 つの文字タイプを組み合わせていることを確認してください。たとえば、小文字 1 文字と数字 1 文字や、大文字 1 文字と句読点 1 つなどを指定できます。

7. 指定されたフィールドに新しいクラスタキーを再入力し、*Enter* キーを押します。
   クラスタキーが正常にリセットされたことを通知するメッセージが表示されます。
8. ノードを再起動します。

同じクラスタキーを使用する BI プラットフォームデプロイメント内のすべてのノードをリセットする必要があります。

8.13.2 暗号管理者

CMC で暗号化キーを管理するには、暗号管理者グループのメンバーである必要があります。BI プラットフォームで作成されたデフォルトの管理者アカウントは、暗号管理者グループのメンバーでもあります。必要に応じて、このアカウントを使用して、ユーザを暗号管理者グループに追加します。グループのメンバーシップを、限定された人数のユーザに制限することをお勧めします。

> ⓘ 注記
>
> ユーザを管理者グループに追加しても、暗号化キーに管理タスクを実行するために必要な権限は継承しません。

8.13.2.1 ユーザを暗号管理者グループに追加する

ユーザアカウントを暗号管理者グループに追加するには、ユーザアカウントが BI プラットフォーム内に存在する必要があります。

> ⓘ 注記
>
> ユーザを暗号管理者グループに追加するには、管理者と暗号管理者グループの両方のメンバーである必要があります。

1. CMC の [ユーザとグループ] 管理エリアで、[暗号管理者] グループを選択します。
2. ▶ アクション ▶ グループにメンバーを追加 ▶をクリックします。
   [追加]ダイアログボックスが開きます。
3. [ユーザ一覧]をクリックします。
   [利用可能なユーザまたはグループ] 一覧が最新表示されて、システム内のすべてのユーザアカウントが表示されます。
4. [利用可能なユーザまたはグループ] 一覧から、暗号管理者グループに追加するユーザを、[選択されたユーザまたはグループ] 一覧に移動します。

   > → ヒント
   >
   > 特定のユーザを検索するには、[検索]フィールドを使用します。

5. [*OK*] をクリックします。

暗号管理者グループのメンバーは、新しく追加されたアカウントから CMC の [暗号化キー] 管理エリアにアクセスで ます。

8.13.2.2 CMC で暗号化キーを表示する

CMC アプリケーションには、BI プラットフォームシステムで使用された暗号化キーに対する専用の管理エリアがあります。このエリアへのアクセスは、暗号管理者グループのメンバーに限定されます。

1. CMC を起動するには、▶ プログラム ▶ *SAP Business Intelligence* ▶ *SAP BusinessObjects BI プラットフォーム 4* ▶ *SAP BusinessObjects BI プラットフォームセントラル管理コンソール* ▶をクリックします。
   CMC のホーム ページが表示されます。
2. [暗号化キー] タブをクリックします。
   [暗号化キー] 管理エリアが表示されます。
3. 詳細を参照する暗号化キーをダブルクリックします。

関連情報

暗号化キーに関連付けられているオブジェクトを表示する [167 ページ]

8.13.3 CMC での暗号化キーの管理

暗号管理者は、[暗号化キー] 管理エリアを使用して、CMS リポジトリに格納された機密データを保護するキーの見直し、生成、無効化、使用の中止、および削除を行います。

現在システムで定義されている暗号化キーはすべて、[暗号化キー] 管理エリアに一覧表示されます。各キーの基本情報は、以下の表に示されたヘッダに表示されます。

ヘッダ	説明
タイトル	暗号化キーの名称 ID
ステータス	キーの現在のステータス
最終ステータス変更	暗号化キーに関連した最終変更に対する日付およびタイムスタンプ
オブジェクト	キーに関連するオブジェクトの数

関連情報

暗号化キーのステータス [166 ページ]
新しい暗号化キーを作成する [168 ページ]
システムから暗号化キーを削除する [169 ページ]
暗号化キーを無効化する [169 ページ]
暗号化キーに関連付けられているオブジェクトを表示する [167 ページ]
暗号化キーを改ざんありにする [168 ページ]

8.13.3.1 暗号化キーのステータス

次の表には、BI プラットフォームシステムの暗号化キーに対して設定可能なすべてのステータスオプションが一覧表示されています。

ステータス	説明
アクティブ	[アクティブ] は、システム内の 1 つの暗号化キーのみに指定できます。このキーは、CMS データベースに保存される予定の、現在の重要データの暗号化に使用します。さらに、オブジェクトリスト内に表示されるすべてのオブジェクトの解読にも使用します。新しい暗号化キーが作成されると、現在の

ステータス	説明
	[アクティブ] ステータスは [無効にする] ステータスに戻ります。アクティブなキーはシステムから削除できません。
無効にする	[無効にする] キーは、データの暗号化に使用できません。ただし、オブジェクトリストに表示されているすべてのオブジェクトの解読に使用することはできます。一度無効にしたキーを再度アクティブにすることはできません。[無効にする] とマークされたキーは、システムから削除できません。削除するには、キーのステータスを [無効] にしておく必要があります。
改ざんあり	安全でないと考えられる暗号化キーは、改ざんありとマークすることができます。キーにこのようなフラグを付けることによって、そのキーに関連付けられているデータオブジェクトの再暗号化を後で進めることができます。改ざんありと一度マークされたキーをシステムから削除するには、そのキーを無効にしておく必要があります。
無効	暗号化キーが無効になると、そのキーに現在割り当てられているすべてのオブジェクトが現在の [アクティブ] な暗号化キーによって再暗号化される処理が開始されます。キーを無効にすると、システムから安全に削除することができます。この無効化メカニズムにより、CMC データベース内のデータは常に解読可能となります。一度無効にしたキーを再度アクティブにすることはできません。
無効にする - 再暗号化を実行中	暗号化キーが現在無効化されていることを示します。この処理が終了すると、キーは [無効] とマークされます。
無効にする - 再暗号化が一時停止	暗号化キーを無効にするための処理が一時停止していることを示します。このステータスは、通常、この無効化処理が故意に一時停止された場合、またはこのキーに関連付けられているデータオブジェクトが使用できない場合に発生します。
無効 - 改ざんあり	キーが改ざんありとマークされており、以前そのキーに関連付けられていたすべてのデータが別のキーで暗号化された場合に、[無効 - 改ざんあり] のフラグが付きます。[無効にする] キーが改ざんありとマークされた場合、何の処理も行わないか、またはそのキーを無効にするかのどちらかを選択できます。改ざんありのキーを無効にすると、そのキーを削除できるようになります。

8.13.3.2 暗号化キーに関連付けられているオブジェクトを表示する

1. CMC の [暗号化キー] 管理エリアでキーを選択します。
2. 管理 > プロパティ をクリックします。
   暗号化キーの [プロパティ] ダイアログボックスが表示されます。
3. [プロパティ] ダイアログボックスの左側にある ナビゲーションペインの [オブジェクト一覧] をクリックします。
   暗号化キーに関連付けられたすべてのオブジェクトの一覧が、ナビゲーションペインの右側に表示されます。

→ ヒント

特定のオブジェクトを検索するには検索機能を使用します。

8.13.3.3 新しい暗号化キーを作成する

⚠ 警告

新しい暗号化キーを作成すると、現在の [アクティブ] キーは自動的に無効化されます。キーが無効化されると、[アクティブ] キーとして復元することはできません。

1. CMC の [暗号化キー] 管理エリアで、▶ 管理 ▶ 新規 ▶ 暗号化キー ▶ の順にクリックします。
   [新しい暗号化キーの作成] ダイアログボックスが表示されます。
2. [続行] をクリックして、新しい暗号化キーを作成します。
3. 新しい暗号化キーの名称と説明を入力し、[*OK*] をクリックして情報を保存します。
   [暗号化キー] 管理エリアに、アクティブキーとしてのみ新しいキーが一覧表示されます。以前の [アクティブ] キーは、[無効にする] とマークされています。

CMS データベースに新たに生成され、格納された機密データはすべて、新しい暗号化キーで暗号化されます。以前のキーを無効化し、そのデータオブジェクトを新しいアクティブキーですべて再暗号化するオプションがあります。

8.13.3.4 暗号化キーを改ざんありにする

何らかの理由で暗号化キーが安全でなくなったと考えられる場合、暗号化キーを改ざんありとマークすることができます。これは、追跡目的には便利で、どのデータオブジェクトがこのキーに関連しているかを特定することができます。暗号化キーは、改ざんありにする前に無効化される必要があります。

ⓘ 注記

キーの使用を取り消した後で、改ざんありにすることもできます。

1. CMC の [暗号化キー] 管理エリアにジャンプします。
2. 改ざんありにする暗号化キーを選択します。
3. ▶ アクション ▶ 改ざんありにする ▶ の順にクリックします。
   [改ざんありにする] ダイアログボックスが表示されます。
4. [続行] をクリックします。
5. [改ざんありにする] ダイアログボックスから、以下のいずれかのオプションを選択します。
   - はい: 改ざんありにするキーと関連するすべてのデータオブジェクトを再暗号化するプロセスを起動します。
   - いいえ: [改ざんありにする] ダイアログボックスが閉じられ、[暗号化キー] 管理エリアで暗号化キーが [改ざんあり] とマークされます。

> ⓘ 注記
>
> [いいえ] を選択すると、機密データは改ざんありにするキーとの関連がそのまま維持されます。改ざんありとしたキーは、システムによって関連オブジェクトの暗号を解除するために使用されます。

関連情報

暗号化キーを無効化する [169 ページ]
暗号化キーのステータス [166 ページ]
暗号化キーに関連付けられているオブジェクトを表示する [167 ページ]

8.13.3.5 暗号化キーを無効化する

[無効にする] 暗号化キーは、関連するデータオブジェクトではまだ使用されている可能性があります。暗号化されたオブジェクトと無効化キーとの関連を切り離すには、キーを無効化する必要があります。

1. [暗号化キー] 管理エリアに一覧表示されているキーから、無効化するキーを選択します。
2. ▶ アクション ▶ 無効化 ▶ をクリックします。
   [無効化] ダイアログボックスが表示されます。
3. [*OK*] をクリックします。
   現在のアクティブキーでキーのオブジェクトすべてを暗号化するプロセスが起動されます。キーが多数のデータオブジェクトに関連している場合、再暗号化プロセスが完了するまで、[無効にする: 再暗号化を実行中] とマークされます。

暗号化キーが無効化されると、機密データオブジェクトが暗号解除のためのキーを必要としなくなるため、システムからキーを安全に削除することができます。

8.13.3.6 システムから暗号化キーを削除する

BI プラットフォームから暗号化キーを削除する前に、そのキーを必要とするデータオブジェクトがシステムに存在しないことを確認する必要があります。この制約により、CMS リポジトリに格納されているすべての機密データを、いつでも暗号解除することができます。

暗号化キーの無効化が完了した後で、以下の手順に従ってシステムからキーを削除します。

1. CMC の [暗号化キー] 管理エリアにジャンプします。
2. 削除する暗号化キーを選択します。
3. ▶ 管理 ▶ 削除 ▶をクリックします。
   [削除]ダイアログボックスが表示されます。
4. [削除] をクリックして、システムから暗号化キーを削除します。
   削除されたキーは、CMC の [暗号化キー] 管理エリアには表示されなくなります。

> ⓘ 注記
>
> 暗号化キーがシステムから削除されてしまうと、復元することはできません。

関連情報

暗号化キーを無効化する [169 ページ]
暗号化キーのステータス [166 ページ]

8.14 データの保護とプライバシー

データ保護は、数多くの法的要件およびプライバシーの懸念事項に関連しています。適用されるデータプライバシー規制の順守に加えて、国によっては業界固有の法律の順守も考慮する必要があります。SAP では、データ保護を含む関連法的要件の順守をサポートする、特定の機能を提供しています。これらの機能が会社、業界、地域または国固有の要件をサポートするのに最善の方法であるかどうかについて SAP がアドバイスすることはありません。さらに、この情報では特定の IT 環境で必要になる追加機能に関するアドバイスや推奨事項は提供されません。データ保護に関連する決定は、状況に応じて、特定のシステムランドスケープや適用される法的要件を考慮して行う必要があります。

> ⓘ 注記
>
> ほとんどの場合において、製品の機能が該当のデータ保護およびプライバシーに関する法律の順守をカバーすることはありません。SAP ソフトウェアでは、セキュリティ機能や個人データの簡易ブロックおよび削除などのデータ保護関連機能を提供することによって、データ保護の順守がサポートされます。SAP では、いかなる種類の法的なアドバイスも提供しません。このドキュメントで使用される定義やその他の用語は、特定の法的ソースから採用されたものではありません。

8.14.1 用語集

用語	定義
個人データ	特定済の、または特定可能な個人に関連するあらゆるデータ ("データ主体")。特定可能な個人とは、直接的または間接的に、特に名前、ID 番号、場所データ、オンライン ID などの識別子、またはその個人の物理的、心理的、遺伝子的、精神的、経済的、文化的、または社会的アイデンティティに固有の 1 つ以上の要素を参照することによって特定できる個人を指します。

用語	定義
目的	個人データの処理についての法的、契約上、またはその他の形式による正当な理由。いかなる目的にも、その目的の開始時にはすでに終了が定義されているものと想定されています。
ブロック	主要なビジネス上の目的が終了しデータへのアクセスを制限する方法。
削除	取り消すことのできない個人データの破棄。
保持期間	データセットの目的の終了 (EoP) と、該当する法律に基づいたデータセットの削除時の間の期間。これは保存期間とブロック期間を組み合わせたものになります。
目的の終了 **(EoP)**	主要なビジネス目的について個人データの処理が必要なくなった場合のデータセットの時点を特定する方法。**EoP** に到達した後、データはブロックされ、特別な権限 (例: 税務監査官) が付与されているユーザのみがアクセスできます。
機密個人データ	通常、以下のタイプの情報が含まれる個人データのカテゴリ: • 人種的または民族的出自、政治的意見、宗教上または哲学上の信念、もしくは労働組合への加入状態を明らかにする個人データ、および遺伝データ、生体認証データ、健康または性生活、性的指向に関する個人データの特別なカテゴリ • 専門の秘密保持が必要な個人データ • 犯罪または規制違反に関連する個人データ • 保険、銀行、またはクレジットカードのアカウントに関する個人データ
保存期間	データセットの目的の終了 (EoP) 後、データがデータベースに残り、元の目的に関連する後続処理がある場合に使用できる期間。最も長く設定された期間の終了時に、データはブロックまたは削除されます。保存期間は全体的な保持期間の一部です。
使用先チェック **(WUC)**	ビジネスパートナデータがブロックされる可能性が生じた場合に、データ完全性が確保されるように設計されているプロセス。アプリケーションの使用先チェック (WUC) により、特定のビジネスパートナに依存するデータがデータベースにあるかどうかが特定されます。依存データが存在する場合、そのデータがまだビジネスアクティビティに必要であることを意味しています。これにより、データで参照されているビジネスパートナのブロックが阻止されます。
承諾	個人データの所定の目的への使用を許可することを確認する、データ主体のアクション。承諾機能により、特定の目的に関連した承諾レコードが保存され、対象者が承諾を実行、取消、または拒否したことが表示されます。

8.14.2 ユーザの承諾

SAP アプリケーションでは、個人データを収集する前にユーザに同意を求めます。SAP BusinessObjects Business Intelligence プラットフォームには、データ主体が自分の個人データの収集および処理について承諾できる機能が用意されています。SAP では、ユーザ、たとえばデータを収集している SAP カスタマは、そのデータ主体 (顧客、担当、アカウントなどの個人) からデータの収集またはソリューションへの転送についての承諾を得ていると想定しています。

> ⓘ 注記
>
> ユーザ同意メッセージ
>
> この製品には、オープンまたは自由設定可能な入力フィールドが含まれています。これらは、データ保護とプライバシーを確保するための追加の技術的/組織的手段なしで個人データを保護することを目的としていません。

8.14.3 情報レポート

ユーザにはそれぞれ、自分に関する個人データが処理中であるかどうかの確認を行う権利があります。SAP BusinessObjects Business Intelligence プラットフォームでは、特定のデータ主体に関する保存済みのすべての情報を表示することができます。

データ主体に関して保存された情報にユーザがアクセスする方法の詳細については、SAP Help Portal の *Fiori* 対応 *Business Intelligence* ラウンチパッドユーザガイドの「自分の情報へのアクセス」の節を参照してください。

> ⓘ 注記
>
> ローカルに保存されたドキュメントは、SAP BusinessObjects Business Intelligence プラットフォームで保護されません。保護はそれぞれのデバイス管理 (アクセス制御や暗号化など) で提供される必要があります。

8.14.4 読込アクセスロギング

読み込みアクセスロギング (RAL) は、機密データへの読み込みアクセスを監視し、記録するために使用されます。このデータは法律、外部の会社ポリシー、または内部の会社ポリシーによって、機密として分類されている可能性があります。これらの共通質問は、読込アクセスロギングを使用するアプリケーションにとって関心の対象である可能性があります。

- 特定のビジネスエンティティ (例: 銀行口座) のデータにアクセスしたユーザは誰ですか。
- (ビジネスパートナなどの) 個人データにアクセスしたユーザは誰ですか。
- (宗教などの) 個人情報にアクセスした従業員は誰ですか。
- どのアカウントまたはビジネスパートナがどのユーザによってアクセスされましたか。

これらの質問には、特定の時間枠内に誰がどのデータにアクセスしたかに関する情報を使用して、回答できる可能性があります。技術的には、これはデータにアクセスするすべてのリモート API および UI インフォストラクチャがロギングに対して有効化されている必要があることを意味します。

SAP BusinessObjects BI プラットフォームでは、機密個人データの特定、処理、保存は行われません。このため、読み取りアクセスは、BI プラットフォームによってログに記録されません。

8.14.5 個人データの削除

- シンプルなブロックおよび削除: 適用されるデータプライバシー規制の順守に加えて、国によっては業界固有の法律の順守も考慮する必要があります。一般的にある特定の国々で起こりうるシナリオとして、個人データの処理のために指定された、明示的かつ正当な目的が終了した後に個人データが削除されますが、それは財務伝票の保持期間など、その他の保持期間が法律で定義されていない場合のみに限ります。特定のシナリオまたは国における法的要件でも、このデータの処理のために指定された、明示的かつ正当な目的が終了した場合に、データのブロックが必要となる場合が頻繁にありますが、その他の法的に定義された保持期間により、データをデータベースに保持する必要があります。一部のシナリオでは、個人データには参照データも含まれます。そのため、削除またはブロックを行う際の課題は参照データ、最終的にはその他のデータ (例: ビジネスパートナデータ) の処理となります。
- 個人データの削除: 個人データの処理には、目的の終了 (EoP) 時における該当データの削除に関連する法律の順守が必要となります。個人データの使用を必要とする正当な目的がない場合、そのデータは削除しなければなりません。データセットのデータを削除する際、このデータセットに関連して参照されるすべてのオブジェクトも削除する必要があります。一般的なデータ保護法に加えて、国によっては業界固有の法律も考慮する必要があります。最も長い保持期間が終了した後は、データを削除する必要があります。

SAP BusinessObjects BI プラットフォームでの個人データの削除

SAP BusinessObjects BI プラットフォームとそのクライアントでは、分析とレポートのためにデータソースから取得されたデータを個人データとして特定および分類することはありません。このようなデータについて、情報の取得および透明性に関する要件は、データを所有するシステムによって管理される必要があります。データが、データを所有するシステムの標準機能であることを確認します。さらに、SAP BusinessObjects BI プラットフォームとそのクライアントは、データを所有するシステムとの間でデータを常に同期する機能 (データソースへのライブ接続) も提供します。

ただし、システムに保持されているユーザデータにアクセスできるのは、そのユーザ自身、またはそのユーザのためにこのデータを管理する権限を持つユーザです。アイデンティティプロバイダ (Windows AD や LDAP など) からインポートされたユーザはこれらと同期され、これらのユーザはアイデンティティプロバイダで保守する必要があります。

SAP BusinessObjects BI プラットフォームで作成された Enterprise ユーザは、そのユーザのためにこのデータを管理する権限を持つユーザが削除または無効化することができます。この場合、保存は、単にユーザをシステムで無効にすることによって処理することができ、保持期間の後、これらのユーザは、該当ユーザの該当データを管理する権限を持つユーザが手動でシステムから削除することができます。

ユーザアカウントを削除すると、そのユーザのお気に入りフォルダ、個人用カテゴリ、および受信ボックスも削除されます。パブリックフォルダ内のアーティファクトの所有権は、削除されたユーザから管理者に転送されます。無効化されたユーザについては、このことは該当するユーザのデータを管理する権限を持つユーザが手動で実行する必要があります。

ユーザオブジェクトの識別子は、監査データベースと Commentary データベースに保存されます。ただし、これはユーザを削除するときにクリアされません。監査ログのユーザ ID は、法的要件およびセキュリティ要件によっ

て必要となるためです。同様に、ユーザが作成したコメントはビジネスの目的のためのものであるため、対話の履歴として保持する必要があります。ユーザには公開されるフィールドに個人データを含めないように事前に伝えられるため、コメントには個人情報は含まれません。

また、監査データベースと Commentary データベースのエントリは、権限のあるユーザが手動で削除することができます。

ユーザを無効にする方法の詳細については、ユーザアカウントを変更する [102 ページ]を参照してください。

ユーザが作成したコメントエントリを削除する方法の詳細については、BI Commentary アプリケーション設定の管理 [692 ページ]を参照してください。

8.14.6 変更ログ

SAP BusinessObjects Business Intelligence プラットフォームの変更ログは、変更依頼およびアクティビティに関連するビジネスパートナの個人データを処理します。ビジネスパートナに関する変更が行われると、変更依頼とアクティビティごとに以下の個人データ情報が記録されます。

- データを変更したユーザ
- 変更日時
- 変更の種類 (更新、挿入、削除、単一フィールドの文書化)
- データレコードの ID キーおよびその値
- 変更された属性の古い値と新しい値
- 変更された属性のヘッダ名

ログに記録するフィールドを定義できます。

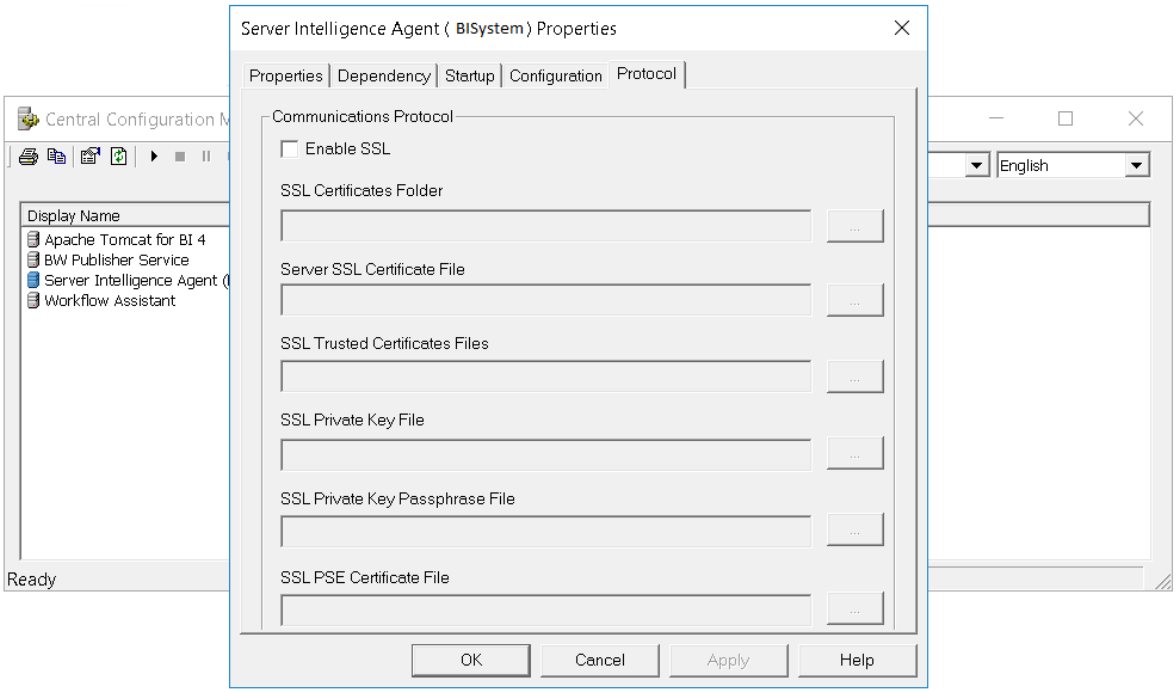
ユーザアカウント更新のログの詳細については、Audit events and details [871 ページ]でイベントタイプ ID: 1007 を参照してください。

8.15 バックエンドサーバの SSL 設定

BI プラットフォームデプロイメントの BI クライアントと BI サーバの間で行われるすべてのネットワーク通信について、Secure Sockets Layer (SSL) プロトコルを使用できます。

すべてのサーバ通信に使用する SSL を設定するには、次の手順を実行する必要があります。

- SSL を有効にして BI プラットフォームをデプロイします。
- デプロイメントの各マシンに対して、キーファイルと証明書ファイルを作成します。
- セントラル設定マネージャ(CCM)と Web アプリケーションサーバで、これらのファイルの場所を設定します。
- 自己署名証明書または認証機関によって管理される証明書に対して SSL を設定することもできます。



> ⓘ 注記
>
> Crystal Reports などのシッククライアントを使用していて、CMS に接続する場合は、SSL 用にこれらのシッククライアントを設定する必要もあります。設定しない場合、同じ方法で設定されていないシッククライアントから SSL 用に設定されている CMS に接続しようとすると、エラーが表示されます。

8.15.1 デフォルト設定ファイルを作成する

デフォルト設定ファイルを作成して、証明書または証明書署名依頼の生成中に値を繰り返し追加するのを回避することができます。

> ⓘ 注記
>
> デフォルト設定ファイルを作成中は、下記のルールに従う必要があります。
>
> - 左側の値を下記とまったく同じに追加します。
> - 左側の値では大文字と小文字が区別されます。
> - 値と等号 (=) の間にはスペースを 1 つのみ入れます。たとえば、*CA_Common_Name* と等号の間にはスペースが 1 つのみあります。
> - 右側の値の後にスペースがないことを確認する必要があります。

次のステップに従い、**Name.cnf** という名前のデフォルト設定ファイルを作成します。

1. テキストエディタで新規ドキュメントを開きます。
2. 下で示すとおりに値を追加します。

```
CA_Common_Name = rootnm
```

```
CA_Country = DE
CA_State = BW
CA_Locality = RRR
CA_Email = example@example.com
CA_Unit = root_u
CA_Expiration[YYMMDD] = yymmdd
User_Expiration[YYMMDD] = yymmdd
User_Country = IN
User_State = KA
User_Locality = BLR
User_Organization = SSS
User_Unit = Unit
User_Common_Name = UserName
```

3. **Name.cnf** という名前のファイルを、Windows 環境では `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64`、UNIX 環境では `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` に保存します。

8.15.2 キーファイルと証明書ファイルの作成

サーバ通信用に SSL プロトコルを設定するには、GENPSE コマンドラインツールを使用して、デプロイメントの各マシンに対してキーファイルと証明書ファイルを作成します。

> **注記**
>
> Crystal Reports のようなシッククライアントコンポーネントを実行するマシンを含む、デプロイメント内のすべてのマシンに対して、証明書を再作成する必要があります。これらのクライアントマシンでは、設定を行うために `sslconfig` コマンド行ツールを使用します。

> **注記**
>
> セキュリティを最大にするために、すべての秘密鍵を保護し、それを非セキュア通信チャネル経由で送信しないようにする必要があります。

8.15.2.1 マシンに対してキーファイルと証明書ファイルを作成する

この節では、サーバ間、またはサーバとクライアントの間のセキュアな通信に必要な自己署名鍵および証明書の生成を扱います。公開鍵インフラストラクチャに関連する多数のタスクを実行するためのコマンドラインツールである GENPSE ツールを使用して、証明書を生成することができます。GENPSE ツールは、X.509 証明書、証明書署名依頼、および CORBA SSL ワークフローで使用される PSE ファイルを生成するために使用します。これは SAP の暗号ライブラリ **CommonCryptoLib** を基盤とし、SHA-2 ハッシュメカニズムをサポートしています。

下記のステップに従い、セキュアな通信に必要な証明書を作成します。

> **注記**
>
> 証明書を生成中に依頼される情報のデフォルト値を持つデフォルト設定ファイル **Name.cnf** を作成することができます。デフォルト設定ファイルのおかげで、証明書ごとに詳細を繰り返し追加する必要がなくなります。詳細については、デフォルト設定ファイルを作成する [175 ページ] を参照してください。

1. Windows では `<INSTALLDIR>¥ SAP BusinessObjects Enterprise XI 4.0¥win64_x64` に、UNIX では `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` に移動します。
2. 次のコマンドを実行します。
   - Windows の場合: `GenPSE.exe selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`
   - UNIX の場合: `GenPSE.sh selfsigned <Name.pse> <Name.der> <root Cert.der> <Name.key> <private key password.txt> <path to Name.cnf>`

   このコマンドを理解するには、次の表を参照してください。

コマンド	機能
GenPSE.exe または GenPSE.sh	暗号ツールの起動
selfsigned	自己署名証明書を生成する
<Name.pse>	サーバ PSE ファイル名
<Name.der>	サーバ証明書のファイル名
<root Cert.der>	認証機関証明書名
<Name.key>	サーバ秘密鍵のファイル名
<private key password.txt>	サーバ秘密鍵ファイルのパスフレーズ
<path to Name.cnf>	デフォルト設定ファイルのファイルパス

3. 次の詳細を入力して、ルート認証機関、サーバ、およびクライアント証明書を生成します。
   - 国名
   - 都道府県名
   - 地域名
   - 組織名
   - 部門名
   - 名前を入力してください
   - 共通名
   - 電子メールアドレス
   - 有効期限を *YYMMDD* 書式で入力してください
4. PSE ファイルと証明書は、Windows では `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64`、UNIX では `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` で生成され、格納されます。

   → ヒント

   ユーザ証明書を生成中に、追加パラメータユーザ証明書タイプを使用して、サーバまたはクライアント認証用の証明書を識別および作成できます。現時点では、このパラメータのもとで行う選択は CORBA SSL 設定にまったく影響しません。

> ⓘ 注記
>
> - サーバ PSE ファイルと認証機関証明書ファイルは異なる名前にしてください。
> - 有効期限は 2049 年までサポートされます。

8.15.3 証明書が認証機関によって管理されている場合の SSL の設定

サードパーティ認証機関に証明書に署名するよう求める証明書署名依頼を生成する必要があります。単純なコマンドを実行し、求められた場合は必要な情報を提供することによって、GenPSE ツールから証明書署名依頼が生成されます。

以下のステップに従い、証明書署名依頼を生成します。

> ⓘ 注記
>
> 証明書を生成中に依頼される情報のデフォルト値を持つデフォルト設定ファイル `Name.cnf` を作成することができます。デフォルト設定ファイルのおかげで、証明書ごとに詳細を繰り返し追加する必要がなくなります。詳細については、デフォルト設定ファイルを作成する [175 ページ] を参照してください。

1. Windows では `<INSTALLDIR>¥ SAP BusinessObjects Enterprise XI 4.0¥win64_x64` に、UNIX では `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` に移動します。
2. 次のコマンドを実行します。
   - Windows の場合: `GenPSE.exe gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`
   - UNIX の場合: `GenPSE.sh gencsr <csrname.p10> <Name.key> <private key password.txt> <path to Name.cnf>`

コマンド	機能
GenPSE.exe または GenPSE.sh	暗号ツールの起動
gencsr	証明書署名依頼を生成する
<csrname.p10>	証明書署名依頼のファイル名
<Name.key>	サーバ秘密鍵のファイル名
<private key password.txt>	サーバ秘密鍵ファイルのパスフレーズ
<path to Name.cnf>	デフォルト設定ファイルのパス

3. 次の情報を入力します。
   - 設定する秘密鍵パスフレーズを入力してください
   - 秘密鍵パスフレーズを確認のために再入力してください
   - 国名
   - 都道府県名

- 地域名
- 部門名
- 共通名
- 電子メールアドレス

4. p10 形式の CSR ファイル、サーバの秘密鍵、およびパスフレーズファイルは、Windows では `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64`、UNIX では `<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64` で生成され、格納されます。生成された CSR ファイルは、署名付き証明書を生成するために認証機関に送信されます。

8.15.3.1 PSE ファイルの生成

証明書が外部認証機関によって管理されている場合は、PSE ファイルを生成する必要があります。以下の手順に従って、PSE ファイルを生成してください。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64` を開きます。
2. コマンドラインコンソールを起動し、Windows の場合は `set SECUDIR=.`、Linux の場合は `export SECUDIR=.` を実行します。
3. `sapgenpse import_p8 -p <file_path_PSE> -c <file_path_server_certificate> -r <file_path_CA_certificate> -z <file_path_passphrase_text_file> <file_path_server_key>` を実行します。

   このコマンドの意味については、以下の表を参照してください。

コマンド	説明
sapgenpse	暗号ツールの起動
import_p8	PKCS#8 形式の秘密鍵 (オプションで PKCS#5 パスワードベースの暗号化による保護) から新しい PSE ファイルと必要なすべての X.509 証明書を作成します。
-p <file_path_PSE>	作成される新しい PSE ファイルのパス
-c <file_path_server_certificate>	サーバ証明書のファイルパス
-r <file_path_CA_certificate>	CA 証明書のファイルパス
-z <file_path_passphrase_text_file>	パスフレーズのテキストファイルのファイルパス
<file_path_server_key>	サーバの秘密鍵ファイルのファイルパス

例

sapgenpse import_p8 -p C:¥SSL¥cert.pse -c C:¥SSL¥servercert.der -r C:¥SSL¥cacert.der -z C:¥SSL¥passphrase.txt C:¥SSL¥server.key

4. パスワードのプロンプトで Enter を押して、空のパスワードを指定します。

5. 作成した PSE ファイルにユーザ認証情報を追加します。

> → ヒント
>
> LocalSystem アカウントで SIA を実行中の場合は、次のコマンドを実行する必要があります。`sapgenpse seclogin -p C:¥SSL¥cert.pse -O SYSTEM` を実行して、PSE ファイルにユーザ認証情報を追加します。

> ⓘ 注記
>
> PSE ファイルは、任意の名前を使用することができます。

8.15.4 SSL プロトコルの設定

デプロイメントの各マシンに対して鍵と証明書を作成し、安全な場所にそれらを格納したら、その場所を、セントラル設定マネージャ (CCM) と Web アプリケーションサーバに指定する必要があります。

Web アプリケーションサーバおよびシッククライアントアプリケーションを実行中のマシンに、SSL プロトコルを設定する特定のステップも実装する必要があります。

SSL を設定するための UNIX ベースのプラットフォームでの FIPS の有効化

FIPS は、4.2 SP04 以上の完全なインストールの場合はデフォルトで有効になりますが、以下に示すシナリオの場合にはマニュアルで有効にする必要があります。

- 4.1 SPXX から 4.2 SP04 へのパッチアップデート
- 4.1 SPXX から 4.2 SP02 または SP03 へのパッチアップデート、およびその後の 4.2 SP04 へのアップデート

> ⓘ 注記
>
> Windows では、FIPS が有効になっていなくても CORBA SSL が機能しますが、UNIX ベースのプラットフォームでは、CORBA SSL を設定する前に、サーバに対して FIPS が有効になっていることを確認する必要があります。

FIPS を有効にするための手順は次のとおりです。

- `<INSTALLDIR>/sap_bobj` に移動します。
- `./stopservers` を実行します。
- ccm.config ファイルを開きます。
- SIA ノードのプロパティ一覧からの '-FIPS' というテキストを追加します。
- `./startservers` を実行します。

8.15.4.1 CCM で SSL プロトコルを設定する

1. CCM で Server Intelligence Agent を右クリックし、[プロパティ]を選択します。
2. [プロパティ]ダイアログボックスで、[プロトコル]タブをクリックします。
3. [*SSL を有効にする*] が選択されていることを確認します。
4. キー ファイルと証明書ファイルを格納したディレクトリのファイル パスを指定します。

フィールド	説明
SSL 証明書フォルダ	必要な SSL 証明書とファイルがすべて保存されているフォルダ。例: `d:¥ssl`
サーバ SSL 証明書ファイル	サーバ SSL 証明書を保存するために使用されるファイルの名前。デフォルトは、`servercert.der`
SSL トラステッド証明書ファイル	SSL トラステッド証明書を含むファイル名。デフォルトでは、`cacert.der` です。
SSL 秘密鍵ファイル	証明書へのアクセスに使用する SSL 秘密キーファイル名。デフォルトでは、`server.key` です。
SSL 秘密鍵パスフレーズファイル	秘密鍵にアクセスするために使用されるパスフレーズを含むテキストファイルの名前。デフォルトでは、`passphrase.txt` です。
SSL PSE 証明書ファイル	トラステッド証明書とサーバ証明書に関する情報を含む PSE ファイルの名前。

> **注記**
>
> ディレクトリはサーバが稼動中のマシンに対して指定する必要があります。

8.15.4.2 Unix で SSL プロトコルを設定する

SIA では SSL プロトコルを設定するには、`serverconfig.sh` スクリプトを使用する必要があります。このスクリプトによって、サーバ情報の表示、インストールしたシステムへのサーバの追加、インストールしたシステムからのサーバの削除などを可能にするテキストベースのプログラムが使用可能になります。`serverconfig.sh` スクリプトは、インストール先の `sap_bobj` ディレクトリにインストールされます。

1. SIA およびすべての SAP BusinessObjects サーバを停止するには、`ccm.sh` スクリプトを使用します。
2. `serverconfig.sh` スクリプトを実行します。
3. [*3 - ノードの変更*] を選択し、`Enter` キーを押します。
4. ターゲット SIA を指定し、`Enter` キーを押します。
5. [*1 - Server Intelligence Agent SSL 設定の変更*] を選択します。
6. [*SSL*] を選択します。
   プロンプトが表示されたら、SSL 証明書の場所を指定します。
7. BI プラットフォームデプロイメントが SIA クラスタの場合、各 SIA に対して手順 1 ～ 6 を繰り返します。
8. `ccm.sh` を使用して SIA を起動し、サーバが起動するまで待機します。

8.15.4.3 Web アプリケーションサーバに対して SSL プロトコルを設定する

1. J2EE Web アプリケーションサーバの場合には、次のシステムプロパティセットを使用して Java SDK を実行します。例:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=d:¥ssl
-DtrustedCert=cacert.der -DsslCert=clientcert.der -DsslKey=client.key
-Dpassphrase=passphrase.txt
```

   次の表は、これらの例に対応する説明を示しています。

例	説明
`<DcertDir>=d:¥ssl`	すべての証明書と鍵を格納するディレクトリ。
`<DtrustedCert>=cacert.der`	信頼できる証明書ファイル。複数ファイルを指定する場合は、セミコロンで区切ります。
`<DsslCert>=clientcert.der`	SDK によって使用される証明書。
`<DsslKey>=client.key`	SDK 証明書の秘密鍵。
`<Dpassphrase>=passphrase.txt`	秘密鍵のパスフレーズを格納するファイル。
`<Dpsecert>=cert.pse`	PSE は、通信の保護に使用されるキーおよび証明書が含まれるリポジトリです。 詳細については、3026364 を参照してください。

2. IIS Web アプリケーションサーバを使用している場合は、コマンドラインから `sslconfig` ツールを実行し、SSL プロトコル設定手順に従います。

8.15.4.4 シッククライアントを設定する

以下の手順を実行する前に、証明書および秘密キーなどの必要な SSL リソースをすべて作成し、既知のディレクトリに保存しておく必要があります。

下の手順では、以下の SSL リソースを作成するための手順に従っていることを前提としています。

SSL リソース	
SSL 証明書フォルダ	**`d:¥ssl`**
サーバ SSL 証明書ファイル名	**`servercert.der`**
信頼できる SSL 証明書またはルート証明書ファイル名	**`cacert.der`**
SSL 秘密キーファイル名	**`server.key`**

SSL リソース	
SSL 秘密キーファイルにアクセスするパスフレーズを含むファイル	`passphrase.txt`
SSL PSE 証明書ファイル名	cert.pse

一度上記のリソースが作成されると、以下の手順に従って、セントラル設定マネージャ (CCM) などのシッククライアントアプリケーションを設定できるようになります。

1. シッククライアントアプリケーションが起動中でないことを確認します。

   > **注記**
   >
   > ディレクトリはサーバが稼動中のマシンに対して指定する必要があります。

2. `sslconfig.exe` コマンドラインツールを実行します。設定に応じて、32 ビットクライアントの場合は win32_x86 から、64 ビットクライアントの場合は win64_x64 からツールを実行します。

   SSLC ツールは、BI プラットフォームソフトウェアとともにインストールされます(たとえば、Windows の場合は、デフォルトで `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64` にインストールされます)。

3. 次のコマンドを入力します。

```
sslconfig.exe -dir d:¥SSL -mycert servercert.der -rootcert cacert.der -mykey
server.key
-passphrase     passphrase.txt -psecert cert.pse -protocol ssl
```

4. シッククライアントアプリケーションを再起動します。

関連情報

マシンに対してキーファイルと証明書ファイルを作成する [176 ページ]

8.15.4.4.1 トランスレーションマネジメントツールに対して SSL ログインを設定する

トランスレーションマネジメントツールで SSL ログインを使用できるようにするには、SSL リソースに関する情報をツールの設定ファイル (`.ini`) に追加する必要があります。

1. `TransMgr.ini` ファイルを `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86` ディレクトリで探します。
2. テキストエディタを使用して、`TransMgr.ini` を開きます。
3. 次のパラメータを追加します。

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=<D:¥SSLCert>
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. ファイルを保存してテキストエディタを閉じます。

これで、SSL を使用してトランスレーションマネジメントツールにログインすることができます。

8.15.4.4.2 レポート変換ツールに対して SSL を設定する

RCT は、BI 4.3 リリースで非推奨になります。詳細については、2801797 を参照してください。

8.16 BI プラットフォームコンポーネント間の通信について

BI プラットフォームシステム全体が同一のセキュアサブネット上にデプロイされている場合、ファイアウォールを特に設定する必要はありません。ただし、1 つまたは複数のファイアウォールで隔てられた別のサブネットに一部のコンポーネントをデプロイする場合もあります。

BI プラットフォームサーバ、リッチクライアント、および SAP BusinessObjects SDK をホストする Web アプリケーションサーバ間の通信について理解してから、システムがファイアウォールを使用するように設定します。

関連情報

ファイアウォール用の BI プラットフォームの設定 [197 ページ]
一般的なファイアウォールシナリオの例 [201 ページ]

8.16.1 BI プラットフォームサーバと通信ポートの概要

システムがファイアウォールと共にデプロイされている場合、BI プラットフォームサーバとそれらの通信ポートについて理解することが重要になります。

8.16.1.1 リクエストポートをバインドする各 BI プラットフォームサーバ

BI プラットフォームサーバ (Input File Repository Server など) は、起動時にリクエストポートにバインドします。それ以外の BI プラットフォームコンポーネント (サーバ、リッチクライアント、Web アプリケーションサーバにホストされる SDK など) は、このリクエストポートを使用してサーバと通信します。

特定のポート番号を使用するように設定されている場合を除き、サーバは起動時および再起動時に動的にリクエストポート番号を選択します。特定のリクエストポート番号を、ファイアウォールを通過して他の BI プラットフォームコンポーネントと通信するサーバに、手動で設定する必要があります。

8.16.1.2 CMS に登録される各 BI プラットフォームサーバ

BI プラットフォームサーバは、起動時に CMS に登録されます。サーバが登録されるとき、CMS は次の情報を記録します。

- サーバのホストマシンのホスト名(または IP アドレス)
- サーバのリクエストポート番号

8.16.1.3 CMS は 2 つのポートを使用します。

CMS は、リクエストポートとネームサーバポートという 2 つのポートを使用します。リクエストポートは、デフォルトでは動的に選択されます。ネームサーバポートは、デフォルトでは 6400 です。

すべての BI プラットフォームサーバおよびクライアントアプリケーションは、最初に CMS™ のネームサーバポートにアクセスします。CMS™ は、その最初のアクセスに応答してリクエストポートの値を返します。サーバは、それ以降の CMS™ との通信にこのリクエストポートを使用します。

8.16.1.4 登録したサービスの Central Management Server (CMS) ディレクトリ

CMS は、登録したサービスのディレクトリを提供します。他の BI プラットフォームコンポーネント (Web サービス、リッチクライアント、および Web アプリケーションサーバにホストされている SDK など) は、CMS にアクセスして特定のサービスへの参照をリクエストできます。サービスの参照には、そのサービスのリクエストポート番号、サーバのホストマシンのホスト名 (または IP アドレス)、およびサービス ID が含まれます。

BI プラットフォームコンポーネントは、使用しているサーバとは異なるサブネットに含まれることがあります。サービスへの参照に含まれるホスト名 (または IP アドレス) は、そのコンポーネントのマシンから到達できる必要があります。

> ⓘ 注記
>
> BI プラットフォームサーバへの参照には、デフォルトでそのサーバマシンのホスト名が含まれます。(マシンに複数のホスト名がある場合は、プライマリホスト名が選択されます。)参照に名前ではなく IP アドレスが含まれるように、サーバを設定することもできます。

関連情報

BI プラットフォームコンポーネント間の通信 [186 ページ]

8.16.1.5 Server Intelligence Agents(SIA)と Central Management Server(CMS)の通信

Server Intelligence Agent(SIA)と Central Management Server(CMS)が相互に通信できない場合、デプロイメントは機能しません。クラスタ内のすべての SIA と CMS 間の通信を許可するようにファイアウォールポートが設定されていることを確認します。

8.16.1.6 データ層および CMS と通信する Job Server の子プロセス

多くの Job Server は子プロセスを作成して、レポート生成のようなタスクを処理させます。Job Server は 1 つまたは複数の子プロセスを作成します。すべての子プロセスにはそれ自体のリクエストポートがあります。

デフォルトでは、Job Server は各子プロセスのリクエストポートを動的に選択します。Job Server が選択できるポート番号の範囲を指定できます。

すべての子プロセスは、CMS と通信します。この通信がファイアウォールを通過する場合、次の操作が必要になります。

- `-requestJSChildPorts <lowestport>-<highestport>` および `-requestPort <port>` パラメータをサーバのコマンドラインに追加することにより、Job Server が選択できるポート番号の範囲を指定します。ポートの範囲は、`-maxJobs` で指定された子プロセスの最大数が使用するために十分な大きさが必要です。
- ファイアウォールで、指定されたポート範囲を開きます。

多くの子プロセスがデータ層と通信します。たとえば、ある子プロセスはレポーティングデータベースと接続し、データを取得して、レポートのために計算を実行します。Job Server の子プロセスがファイアウォールを通過してデータ層と通信する場合、次の操作が必要になります。

- Job Server マシンの任意のポートからデータベースサーバマシンのデータベースリスニングポートに向けて、ファイアウォールに通信経路を開きます。

関連情報

コマンドラインの概要 [1059 ページ]

8.16.2 BI プラットフォームコンポーネント間の通信

BI プラットフォームコンポーネント (ブラウザクライアント、リッチクライアント、サーバ、Web アプリケーションサーバにホストされている SDK など) は、通常のワークフローではネットワークを越えて互いに通信します。ファイアウォールで隔てられた複数のサブネットに SAP BusinessObjects 製品をデプロイするには、このようなワークフローについて理解する必要があります。

8.16.2.1 BI プラットフォームコンポーネント間の通信の要件

BI プラットフォームのデプロイメントは、次のような一般的な要件に準拠する必要があります。

1. 各サーバが、そのサーバのリクエストポートで、他の各 BI プラットフォームサーバとの通信を開始できる必要があります。
2. 2 つのポートを使用する Central Management Server。 BI プラットフォームサーバ、リッチクライアント、および SDK をホストする Web アプリケーションサーバはそれぞれ、その両方のポートで CMS との通信を開始できる必要があります。
3. Job Server の各子プロセスが、CMS と通信できる必要があります。
4. シッククライアントは、Input File Repository Server および Output File Repository Server のリクエストポートとの通信を開始できる必要があります。
5. シッククライアントおよび Web アプリケーションで監査を有効にする場合は、クライアント監査プロキシサービスをホストする Adaptive Processing Server のリクエストポートとの通信を開始できる必要があります。
6. 通常は、SDK をホストする Web アプリケーションサーバが、各 BI プラットフォームサーバのリクエストポートと通信できる必要があります。

   > **注記**
   >
   > Web アプリケーションサーバは、デプロイメントで使用されている BI プラットフォームサーバと通信する必要があります。 たとえば、Crystal Reports が使用されない場合、Web アプリケーションサーバは Crystal Reports Cache Server と通信する必要はありません。

7. Job Server は、`-requestJSChildPorts <lowestport>-<highestport>` コマンドで指定されたポート番号を使用します。 コマンドラインで範囲が指定されていない場合、サーバはランダムなポート番号を使用します。 Job Server が CMS、FTP、SFTP、または別のマシンのメールサーバと通信できるようにするには、ファイアウォール上の `-requestJSChildPorts` で指定された範囲内のすべてのポートを開きます。
8. CMS は、CMS データベースのリスニングポートと通信できる必要があります。
9. Connection Server、Job Server の多くの子プロセス、ならびに各システムデータベースおよび監査用の Processing Server は、レポーティングデータベースのリスニングポートとの通信を開始できる必要があります。

関連情報

BI プラットフォームのポート要件 [187 ページ]

8.16.2.2 BI プラットフォームのポート要件

この節では、BI プラットフォームサーバ、シッククライアント、SDK をホストしている Web アプリケーションサーバ、およびサードパーティソフトウェアアプリケーションが使用する通信ポートについて説明します。ファイアウォールを使用して BI プラットフォームをデプロイする場合、この情報を使用して、ファイアウォールで開くポートの数を最小限に抑えられます。

8.16.2.2.1 BI プラットフォームアプリケーションのポート要件

次の表に、BI プラットフォームアプリケーションが使用するサーバとポート番号を示します。

製品	クライアントアプリケーション	関連するサーバ	サーバのポート要件
Crystal Reports	SAP Crystal Reports 2020 Designer	CMS Input File Repository Server (FRS) Output File Repository Server (FRS) Crystal Reports 2020 Report Application Server (RAS) Crystal Reports 2020 Processing Server Crystal Reports Cache Server	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート Input FRS リクエストポート Output FRS リクエストポート Crystal Reports 2020 Report Application Server リクエストポート Crystal Reports 2020 Processing Server リクエストポート Crystal Reports Cache Server リクエストポート
Crystal Reports	SAP Crystal Reports for Enterprise designer	CMS Input File Repository Server (FRS) Output File Repository Server (FRS) Crystal Reports Processing Server Crystal Reports Cache Server	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート Input FRS リクエストポート Output FRS リクエストポート Crystal Reports Processing Server リクエストポート Crystal Reports Cache Server リクエストポート
Live Office	Live Office クライアント	Live Office Web サービスをホストする Web サービスプロバイダアプリケーション (`dswsbobje.war`)	HTTP ポート (デフォルトは 80)
SAP Analysis for Microsoft Office	SAP Analysis for Microsoft Office	CMS Multi-Dimensional Analysis Service をホストしている Adaptive Processing Server Input File Repository Server (FRS) Output File Repository Server (FRS)	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート Adaptive Processing Server リクエストポート Input File Repository Server (FRS) リクエストポート Output FRS リクエストポート

製品	クライアントアプリケーション	関連するサーバ	サーバのポート要件
BI プラットフォーム	SAP BusinessObjects Web Intelligence リッチクライアント	CMS Input File Repository Server (FRS)	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート Input FRS リクエストポート
BI プラットフォーム	ユニバースデザインツール	CMS Input File Repository Server (FRS) Connection Server	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート Input FRS リクエストポート Connection Server ポート
BI プラットフォーム	ビジネスビューマネージャ	CMS Input File Repository Server (FRS)	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート Input FRS リクエストポート
BI プラットフォーム	セントラル設定マネージャ (CCM)	CMS Server Intelligence Agent(SIA)	CCM でリモートの BI プラットフォームサーバを管理するためには次のポートを開いておく必要があります。 CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート CCM でリモートの SIA プロセスを管理するためには、次のポートを開いておく必要があります。 Microsoft Directory Services(TCP ポート 445) NetBIOS Session Service(TCP ポート 139) NetBIOS Datagram Service(UDP ポート 138) NetBIOS Name Service(UDP ポート 137) DNS(TCP/UDP ポート 53) ここに示す一部のポートは必須でない場合があります。Windows 管理者に確認してください。
BI プラットフォーム	Server Intelligence Agent (SIA)	CMS を含むすべての BI プラットフォームサーバ	SIA リクエストポート (デフォルトでは 6410) CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート

製品	クライアントアプリケーション	関連するサーバ	サーバのポート要件
BI プラットフォーム	リポジトリ診断ツール	CMS Input File Repository Server (FRS) Output File Repository Server (FRS)	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート Input FRS リクエストポート Output FRS リクエストポート
BI プラットフォーム	Web アプリケーションサーバでホストされる BI プラットフォーム SDK	デプロイされた製品によって必要とされるすべての BI プラットフォームサーバ。 たとえば、SDK が CMS からの Crystal レポートを受信しこれと交信するには、Crystal Reports 2020 Processing Server リクエストポートを使った通信が必要です。	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート 必要な各サーバに対するリクエストポート。たとえば、Crystal Reports 2020 Processing Server リクエストポート。
BI プラットフォーム	Web サービスプロバイダ (`dswsbobje.war`)	Web サービスにアクセスする製品によって必要とされる、すべての BI プラットフォームサーバ。 たとえば、SAP BusinessObjects Dashboards が Web サービスプロバイダを介して Enterprise データソース接続にアクセスしている場合は、Dashboards Cache および Processing Server のリクエストポートとの通信が必要です。	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート 必要な各サーバに対するリクエストポート。たとえば、Dashboards Cache Server および Dashboards Processing Server リクエストポート。
BI プラットフォーム	SAP BusinessObjects Analysis, edition for OLAP	CMS Multi-Dimensional Analysis Service をホストしている Adaptive Processing Server Input File Repository Server (FRS) Output File Repository Server (FRS)	CMS ネームサーバポート (デフォルトでは 6400) CMS リクエストポート Adaptive Processing Server リクエストポート Input File Repository Server (FRS) リクエストポート Output FRS リクエストポート

8.16.2.2.2 サードパーティアプリケーションのポートの要件

次の表に、SAP BusinessObjects 製品が使用するサードパーティソフトウェアを示します。一部のソフトウェアベンダーに対する固有の例が含まれます。ベンダーが異なるとポートの要件も異なります。

サードパーティアプリケーション	サードパーティ製品を使用する **SAP BusinessObjects** コンポーネント	サードパーティアプリケーションのポートの要件	説明
CMS システムデータベース	Central Management Server (CMS)	データベースサーバのリスニングポート	CMS は、CMS システムデータベースと通信する唯一のサーバです。
CMS 監査データベース	Central Management Server (CMS)	データベースサーバのリスニングポート	CMS は、CMS 監査データベースと通信する唯一のサーバです。
レポーティングデータベース	Connection Server Job Server の各子プロセス 各処理サーバ	データベースサーバのリスニングポート	これらのサーバは、レポーティングデータベースから情報を取得します。
Web アプリケーションサーバ	BI ラウンチパッドおよび CMC を含むすべての SAP BusinessObjects Web サービスおよび Web アプリケーション	HTTP ポートおよび HTTPS ポート たとえば、Tomcat ではデフォルトの HTTP ポートは 8080 で、デフォルトの HTTPS ポートは 443 です。	HTTPS は、セキュリティで保護された HTTP 通信を使用する場合にのみ必要になります。
FTP サーバ	すべての Job Server	FTP 入力(ポート 21) FTP 出力(ポート 22)	Job Server は FTP ポートを使用して、*FTP* への送信を許可します。

サードパーティアプリケーション	サードパーティ製品を使用する **SAP BusinessObjects** コンポーネント	サードパーティアプリケーションのポートの要件	説明
SFTP サーバ	すべての Job Server	SFTP (ポート 22)	Job Server は SFTP ポートを使用して、*SFTP への送信*を許可します。 **注記** ホストキーフィンガープリントは、SSH 接続のセキュリティを確保するために使用され、これにより中間者攻撃を防ぐことができます。これは、SFTP を設定するために必要な、NULL でない必須のパラメータです。ホストキーフィンガープリントを生成するプロセスは、使用する SFTP サーバによって異なります。 管理者およびユーザは、SFTP を有効にするために SHA-2 フィンガープリントを設定する必要があります。管理者およびユーザは、使用している SSH/SFTP サーバ実装の製品ドキュメントを参照して、SHA-2 フィンガープリントを生成することができます。 **例** PuTTY や WinSCP などの共通 SFTP クライアントは、MD5 フィンガープリントを使用して SFTP サーバを一意に識別します。MD5 フィンガープリントは機能しません。SHA-2 フィンガープリントを取得する方法については、SFTP サーバのドキュメントを参照してください。公開鍵ファイルと OpenSSH UNIX ツールを使用するサンプルの方法については、以下で説明します。以下を含む公開鍵ファイル RSAKey.pub があります。 `ssh-rsa <base64 encoded key>`。この場合には、以下のスクリプトを実行します。`cut -d ' ' -f 2 < RSAKey.pub | base64 -d | openssl dgst -c -sha256`.

サードパーティアプリケーション	サードパーティ製品を使用する SAP BusinessObjects コンポーネント	サードパーティアプリケーションのポートの要件	説明
			これにより、以下のように出力されます。`(stdin)= 00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8`。ここで、20 桁のダイジェストは、base64 でエンコードされた公開鍵の値によって異なります。ホストキーフィンガープリントに 20 桁の値 `00:93:1e:cc:bd:cc:43:05:41:89:5f:5c:c7:91:1d:11:a0:1e:58:e8` を使用します。 → 推奨事項 推奨のベストプラクティスは、BOE 内の CMC のサーバページで SFTP 設定を有効にし、SFTP サーバ間で送信する際にデフォルト設定を使用することです。

サードパーティアプリケーション	サードパーティ製品を使用する **SAP BusinessObjects** コンポーネント	サードパーティアプリケーションのポートの要件	説明
電子メールサーバ	すべての Job Server	SMTP (SMTP サーバのポート)	SMTPS と SMTP に同じポートを使用できます。ただし、SMTPS の場合は、STARTTLS smtp コマンドを使用して SSL/TLS が有効になっていることを確認してください。 Job Server は SMTP ポートを使用して、電子メールへの送信を許可します。 **Adaptive Job Server** の設定: Adaptive Job Server を設定するには、下記のステップに従います。 1. セントラル管理コンソール (CMC) を起動します。 2. ドロップダウンからサーバを選択します。 3. [**AdaptiveJobServer**] を右クリックして、出力先を選択します。 4. ドロップダウンから電子メールを選択します。 電子メールサーバを出力先としてまだ追加していない場合は、処理を進める前にまず出力先として電子メールサーバを追加する必要があります。 5. 必要な詳細を入力します。 6. 必要に応じて *SSL を有効にする* オプションにチェックを付けます。 7. 保存して終了を選択します。 **SMTP over SSL** のセットアップ: SMTP over SSL をセットアップするには、サーバと BOE システムに SMTP サーバ証明書があることが必要です。 SMTP over SSL をセットアップするには、次の手順に従います。 1. SMTP サーバから証明書を生成します。 2. [出力先] ウィンドウで、[*SSL を有効にする*] チェックボックスを選択します。

サードパーティアプリケーション	サードパーティ製品を使用する SAP BusinessObjects コンポーネント	サードパーティアプリケーションのポートの要件	説明
			3. SMTP 証明書の絶対パスを入力します。 **注記** SMTP 証明書の絶対パスを入力します。SMTP 証明書の絶対パスを入力しない場合には、プレースホルダ (%SI_DEFAULT_CERT_LOC%) を入力すると、システムではこれがデフォルトの場所 (つまり、`¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥` または `¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86¥`) として読み込まれ、証明書 (証明書のデフォルト名は certificate.crt) が検索されます。 4. 目的の [接続セキュリティ] を選択します。 **注記** デフォルトでは、[*StartTLS*] オプションが選択されています。[*SSL/TLS*] を選択することができます。 5. 目的の TLS バージョンを選択します。 **注記** デフォルトでは、TLS v1.0 が選択されています。TLS v1.1 または TLS v1.2 を選択することができます。 6. [保存して閉じる] を選択します。

サードパーティアプリケーション	サードパーティ製品を使用する **SAP BusinessObjects** コンポーネント	サードパーティアプリケーションのポートの要件	説明
			これで、SMTP over SSL がセットアップされました。 **注記** BI 4.1 SP6 から任意の新しいバージョンへのパッチアップデートを実行すると、デフォルトで、[StartTLS] オプションおよび [TLS v1.0] が選択されます。 **注記** • ユーザが [*SSL を有効にする*] チェックボックスにチェックを入れている場合、セキュリティ保護されたチャネルが有効になります。これにより、セキュリティ保護された SMTP over SSL 通信が可能になります。 • Adaptive Job Server ごとに 1 つの SMTP 証明書のみを設定できます。1 つの Job Server に複数の証明書を設定することはできません。 • [*SSL を有効にする*] オプションは Adaptive Job Server でのみ使用可能であり、ドキュメントレベルでは使用できません。
Job Server がコンテンツを送信できる Unix サーバ	すべての Job Server	rexec 出力(ポート 512) (Unix のみ)rsh 出力(ポート 514)	(Unix のみ) Job Server はこれらのポートを使用して、ディスクへの送信を許可します。
認証サーバ	CMS™ SDK をホストする Web アプリケーションサーバ すべてのシッククライアント (Live Office など)	サードパーティ認証の接続ポート たとえば、Oracle LDAP サーバの接続サーバは、ユーザによってファイル ldap.ora に定義されます。	ユーザの認証情報は、そのサードパーティ認証サーバに格納されます。ここに示した CMS™、SDK、およびシッククライアントは、ユーザがログオンするときにサードパーティの認証サーバと通信する必要があります。

8.17 ファイアウォール用の BI プラットフォームの設定

この節では、ファイアウォール環境で動作するように、BI プラットフォームシステムを設定するための方法を、手順を追って説明します。

8.17.1 ファイアウォール用にシステムを設定する

1. ファイアウォールを通過して通信する必要がある BI プラットフォームコンポーネントを決定します。
2. ファイアウォールを通過して通信する必要がある各 BI プラットフォームサーバに、リクエストポートを手動で設定します。
3. `-requestJSChildPorts <lowestport>-<highestport>` および `-requestPort <port>` パラメータをサーバのコマンドラインに追加することにより、ファイアウォールを超えて通信する必要がある Job Server の子のポートの範囲を手動で設定します。
4. 前の手順で設定した BI プラットフォームサーバのリクエストポートおよび Job Server のポート範囲との通信を許可するように、ファイアウォールを設定します。
5. (オプション) ファイアウォールを通過して通信する必要がある BI プラットフォームサーバをホストするマシンごとに hosts ファイルを設定します。

関連情報

BI プラットフォームコンポーネント間の通信 [186 ページ]
ポート番号の設定 [448 ページ]
コマンドラインの概要 [1059 ページ]
ファイアウォール規則の指定 [197 ページ]
NAT を使用するファイアウォールの hosts ファイルの設定 [199 ページ]

8.17.1.1 ファイアウォール規則の指定

BI プラットフォームのコンポーネント間で必要なトラフィックが許可されるように、ファイアウォールを設定する必要があります。この規則の指定方法の詳細は、ファイアウォールのマニュアルを参照してください。

ファイアウォールを通過する通信経路ごとに、インバウンドアクセス規則を 1 つ指定します。ファイアウォールの背後にある各 BI プラットフォームサーバに対しては、アクセス規則を指定する必要はありません。

CMC でサーバの [プロパティ] ページにあるサーバの [リクエストポート] ボックスに指定したポート番号を使用します。マシンの各サーバがそれぞれ一意のポート番号を使用する必要があります。一部の SAP BusinessObjects サーバは、複数のポートを使用します。

> ⓘ 注記
>
> BI プラットフォームが NAT を使用するファイアウォールの両側にデプロイされている場合、すべてのマシンの各サーバが一意のリクエストポート番号を持つ必要があります。つまり、デプロイメント全体で、2 つのサーバが同じリクエストポート番号を共有することはできません。

> ⓘ 注記
>
> アウトバウンドアクセス規則を指定する必要はありません。BI プラットフォームサーバは、Web アプリケーションサーバやクライアントアプリケーションとの通信を開始しません。BI プラットフォームサーバは、同じクラスタ内のほかのプラットフォームサーバとの通信を開始することができます。アウトバウンドファイアウォール環境でクラスタ化されたサーバのデプロイメントは、サポートされていません。

例

この例では、Web アプリケーションサーバと BI プラットフォームサーバの間のファイアウォールに対する、インバウンドアクセス規則を示します。この場合は CMS に対して 2 つのポートを開きます。1 つのポートは Input File Repository Server (FRS) 用で、もう 1 つは Output File Repository Server (FRS) 用です。リクエストポート番号は、サーバの CMC の設定ページの [リクエストポート] ボックスで指定したポート番号です。

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
Web アプリケーションサーバ	任意	CMS	6400	許可
Web アプリケーションサーバ	任意	CMS	<リクエストポート番号>	許可
Web アプリケーションサーバ	任意	Input File Repository Server(FRS)	<リクエストポート番号>	許可
Web アプリケーションサーバ	任意	Output File Repository Server(FRS)	<リクエストポート番号>	許可
任意	任意	CMS	任意	拒否
任意	任意	その他のプラットフォームサーバ	任意	拒否

関連情報

BI プラットフォームコンポーネント間の通信 [186 ページ]

8.17.1.2 NAT を使用するファイアウォールの hosts ファイルの設定

この手順は、Network Address Translation (NAT) が有効になっているファイアウォールを通過して BI プラットフォームサーバが通信を行う必要がある場合にのみ必要です。この手順を実行すると、クライアントマシンはサーバのホスト名をルーティング可能な IP アドレスにマップできます。

> ⓘ 注記
>
> BI プラットフォームは、Domain Name System (DNS) を使用するマシンにデプロイできます。この場合、サーバマシンのホスト名は、各マシンの `hosts` ファイルではなく、DNS サーバ上の外部でルーティング可能な IP アドレスにマップできます。

Network Address Translation の概要

ファイアウォールは、認証されていないアクセスから内部ネットワークを保護するためにデプロイされます。NAT を使用するファイアウォールは、内部ネットワークから、外部ネットワークが使用する別のアドレスに IP アドレスをマップします。このアドレス変換により、外部ネットワークに対して内部の IP アドレスが非表示となり、セキュリティが強化されます。

サーバ、シッククライアント、SDK をホストする Web アプリケーションサーバなどの BI プラットフォームコンポーネントは、サービス参照を使用してサーバに接続します。サービス参照には、サーバのマシンのホスト名が含まれています。このホスト名は BI プラットフォームコンポーネントのマシンからルーティング可能である必要があります。つまり、コンポーネントのマシン上の `hosts` ファイルで、サーバマシンのホスト名がサーバマシンの外部 IP アドレスにマップされる必要があります。サーバマシンの外部 IP アドレスはファイアウォールの外側からルーティング可能ですが、内部 IP アドレスはルーティング可能ではありません。

`hosts` ファイルの設定手順は、Windows と Unix で異なります。

8.17.1.2.1 Windows で hosts ファイルを設定する

1. Network Address Translation (NAT) が有効になっているファイアウォールを通過して通信する必要がある BI プラットフォームコンポーネントが実行されているすべてのマシンを特定します。
2. 前の手順で見つかった各マシンで、メモ帳などのテキストエディタを使用して `hosts` ファイルを開きます。`hosts` ファイルは、`¥Windows¥System32¥drivers¥etc¥hosts` にあります。
3. `hosts` ファイル内の指示に従って、ファイアウォールの背後にある各マシンのうち、BI プラットフォームサーバ (複数も可) を実行しているものにエントリを追加します。サーバマシンのホスト名または完全修飾ドメイン名を外部の IP アドレスにマップします。
4. `hosts` ファイルを保存します。

8.17.1.2.2 UNIX で hosts ファイルを設定する

> **注記**
>
> UNIX オペレーティングシステムは、DNS と通信する前に、まず hosts ファイルに問い合わせて、ドメイン名を解決するように設定する必要があります。詳細は、UNIX システムのマニュアルを参照してください。

1. Network Address Translation (NAT) が有効になっているファイアウォールを通過して通信する必要がある BI プラットフォームコンポーネントが実行されているすべてのマシンを特定します。
2. vi などのエディタを使用して、`hosts` ファイルを開きます。`hosts` ファイルは、ディレクトリ `¥etc` にあります。
3. `hosts` ファイル内の指示に従って、ファイアウォールの背後にある各マシンのうち、BI プラットフォームサーバ (複数も可) を実行しているものにエントリを追加します。サーバマシンのホスト名または完全修飾ドメイン名を外部の IP アドレスにマップします。
4. `hosts` ファイルを保存します。

8.17.2 ファイアウォールを使用したデプロイメントのデバッグ

ファイアウォールで適切なポートが開いているのにファイアウォールを有効にすると機能しなくなる BI プラットフォームサーバがある場合は、イベントログを使ってどのサーバがどのポートまたは IP アドレスをリスニングしているかを特定できます。これらのポートをファイアウォールで開くか、セントラル管理コンソール (CMC) を使用してサーバがリスニングしようとするポート番号または IP アドレスを変更できます。

BI プラットフォームサーバが起動すると、サーバはバインドしようとするリクエストポートごとに以下の情報をイベントログに書き込みます。

- [*Server*] - 問題なく起動したサーバ名。
- [*Published Address(es)*] - 他のサーバがこのサーバと通信するときに使用する、ネームサービスにポストされた IP アドレスとポート番号の組み合わせの一覧。

サーバがポートにバインドすると、ログファイルの [ポートで受信中です] にもサーバがリスニングしている IP アドレスとポートが記録されます。サーバがポートのバインドに失敗すると、ログファイルの [ポートでの受信に失敗しました] に、サーバがリスニングしようとして失敗した IP アドレスとポートが記録されます。

Central Management Server が起動したときも、サーバのネームサービスポートの [Published Address(es)]、[Listening on port(s)]、および [Failed To Listen On] 情報が書き込まれます。

> **注記**
>
> サーバが自動的に割り当てられたポートを使用するよう設定されており、無効なホスト名または IP アドレスを使用する場合は、イベントログにサーバがそのホスト名または IP アドレスおよびポート “0” のリスニングに失敗したことが記録されます。特定のホスト名または IP アドレスが無効な場合は、サーバは、ホストオペレーティングシステムがポートを割り当てる前に失敗します。

例

以下の例は、2 つのリクエストポートとネームサービスポートをリスニングしている Central Management Server のエントリを示します。

```
Server mynode.cms1 successfully started.
Request Port :
     Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
     Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032,
10.90.172.216:8765
Name Service Port :
     Published Address(es): mymachine.corp.com:6400
     Listening on port(s):  [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400,
10.90.172.216:6400
```

8.17.2.1 ファイアウォールを使用したデプロイメントをデバッグする

1. イベントログで、指定したポートにサーバが正しくバインドされているかを確認します。

   サーバがポートに正しくバインドできない場合は、サーバと、同じマシン上で実行されている他のプロセスとの間にポート競合が発生している可能性があります。[*Failed to List On*] エントリは、サーバがリスニングしようとしたポートを示します。netstat などのユーティリティを実行してポートを使用しているプロセスを特定し、他のプロセスまたはサーバを、別のポートをリスニングするよう設定します。
2. サーバがポートに正しくバインドできると、[*Listening On*] にサーバがリスニングしているポートが記録されます。サーバがポートをリスニングしているのに正しく動作しない場合は、ファイアウォールでポートが開いているか確認するか、開いているポートをリスニングするようサーバを設定します。

デプロイメント内のすべての Central Management Server が、使用できないポートまたは IP アドレスをリスニングしようとしている場合は、CMS は起動せず、CMC にログオンできません。CMS がリスニングするポート番号または IP アドレスを変更する場合は、セントラル設定マネージャ (CCM) を使用して有効なポート番号または IP アドレスを指定する必要があります。

関連情報

ポート番号の設定 [448 ページ]

8.18 一般的なファイアウォールシナリオの例

ここでは、一般的なファイアウォールデプロイメントのシナリオの例を示します。

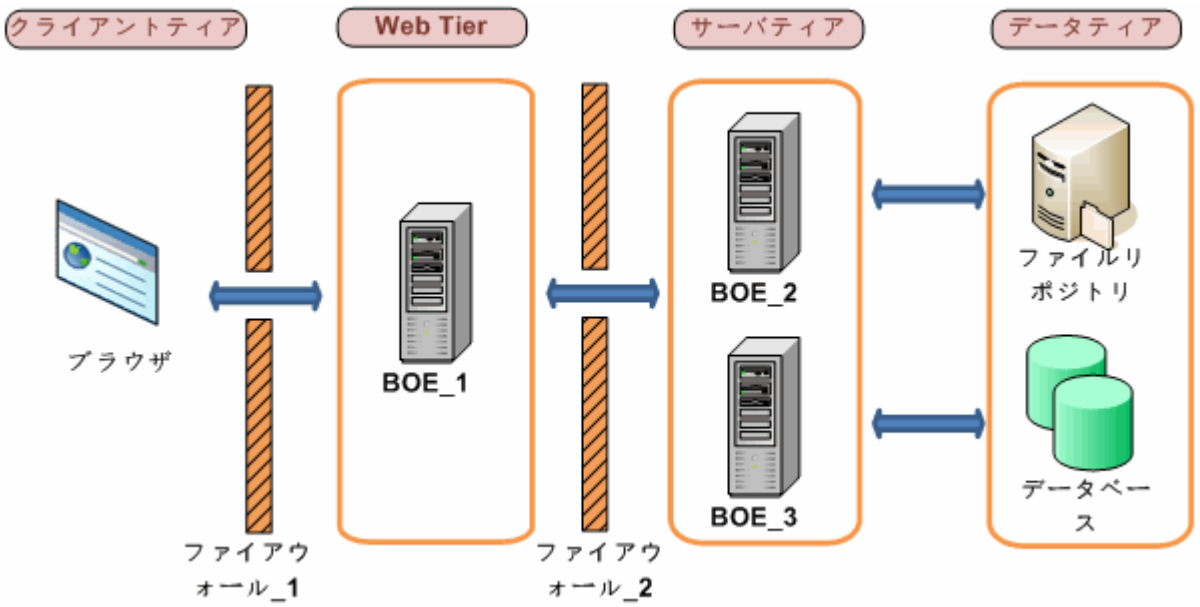
8.18.1 例: 別のネットワークにデプロイされたアプリケーション層

この例では、ファイアウォールによって Web アプリケーションサーバとそれ以外の BI プラットフォームサーバが隔てられているようなデプロイメントで、ファイアウォールと BI プラットフォームが協調するように設定する方法を示します。

この例では、BI プラットフォームコンポーネントは次の各マシンに分散してデプロイされます。

- マシン boe_1 は、Web アプリケーションサーバと SDK をホストします。
- マシン boe_2 は、インテリジェンス層のサーバ (Central Management Server、Input File Repository Server、Output File Repository Server、Event Server など) をホストします。
- マシン boe_3 は、プロセス層のサーバ (Adaptive Job Server、Web Intelligence Processing Server、Report Application Server、Crystal Reports Cache Server、および Crystal Reports Processing Server など) をホストします。

別のネットワークにデプロイされたアプリケーション層



8.18.1.1 別のネットワークにデプロイされたアプリケーション層を設定する

次に、この例を設定する方法を説明します。

1. この例には、次の通信要件が適用されます。
   - SDK をホストする Web アプリケーションサーバが、その両方のポートで CMS と通信できる必要があります。
   - SDK をホストする Web アプリケーションサーバが、各 BI プラットフォームサーバと通信できる必要があります。
   - ブラウザが、Web アプリケーションサーバの、http リクエストポートまたは https リクエストポートにアクセスできる必要があります。

2. Web アプリケーションサーバは、マシン boe_2 および boe_3 のすべての BI プラットフォームサーバと通信する必要がありますこれらのマシンで各サーバのポート番号を設定します。1,025 ～ 65,535 の空のポートをどれでも使用できます。
次の表に、この例で選択したポート番号を示します。

サーバ	ポート番号
Central Management Server	6400
Central Management Server	6411
Input File Repository Server	6415
Output File Repository Server	6420
Event Server	6425
Adaptive Job Server	6435
Crystal Reports Cache Server	6440
Web Intelligence Processing Server	6460
Report Application Server	6465
Crystal Reports Processing Server	6470

3. 前の手順で設定した BI プラットフォームサーバの固定ポートと Web アプリケーションサーバとの通信を許可するように、ファイアウォール Firewall_1 および Firewall_2 を設定します。

この例では、Tomcat アプリケーションサーバの HTTP ポートを開いています。

Firewall_1 の設定

ポート	送信先コンピュータ	ポート	アクション
任意	BOE_1	8080	許可

Firewall_2 の設定

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
BOE_1	任意	BOE_2	6400	許可
BOE_1	任意	BOE_2	6411	許可
BOE_1	任意	BOE_2	6415	許可
BOE_1	任意	BOE_2	6420	許可
BOE_1	任意	BOE_2	6425	許可
BOE_1	任意	BOE_3	6435	許可
BOE_1	任意	BOE_3	6440	許可
BOE_1	任意	BOE_3	6460	許可
BOE_1	任意	BOE_3	6465	許可
BOE_1	任意	BOE_3	6470	許可

4. このファイアウォールでは NAT は有効ではないため、hosts ファイルを設定する必要はありません。

関連情報

ポート番号の設定 [448 ページ]
BI プラットフォームコンポーネント間の通信について [184 ページ]

8.18.2 例: ファイアウォールによって BI プラットフォームサーバから隔てられたシッククライアントとデータベース層

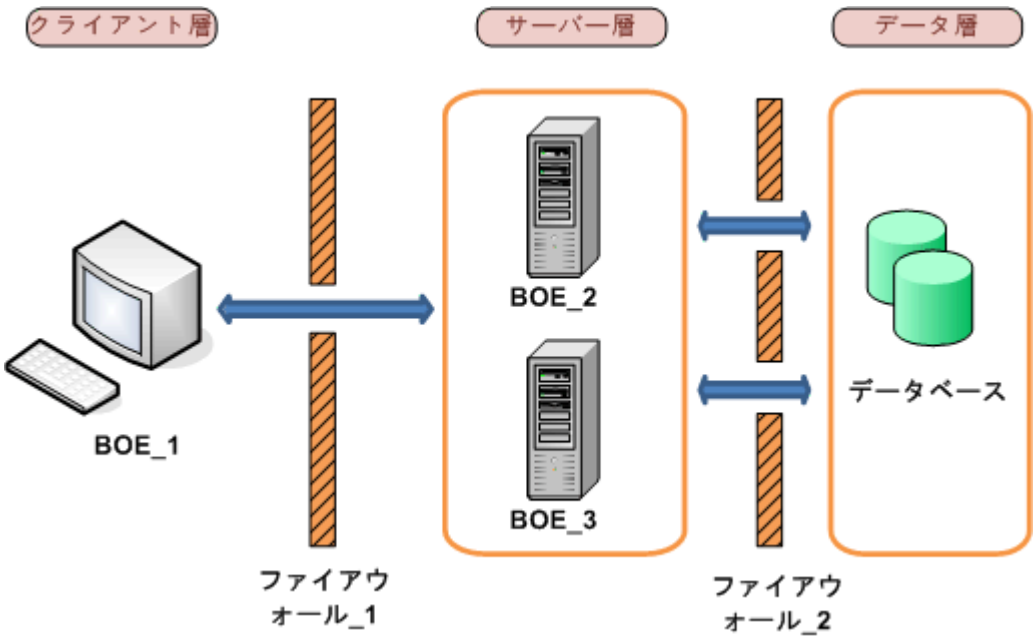
この例では、次のようなデプロイメントシナリオでファイアウォールと BI プラットフォームが協調するように設定する方法を示します。

- 1 つのファイアウォールでシッククライアントが BI プラットフォームサーバから隔てられています。
- 1 つのファイアウォールで BI プラットフォームサーバがデータベース層から隔てられています。

この例では、BI プラットフォームコンポーネントは次の各マシンに分散してデプロイされます。

- マシン `BOE_1` は公開ウィザードをホストします。公開ウィザードは BI プラットフォームのシッククライアントです。
- マシン `boe_2` はインテリジェンス層のサーバ (Central Management Server (CMS)、Input File Repository Server、Output File Repository Server、Event Server など) をホストします。
- マシン `boe_3` はプロセス層のサーバ (Adaptive Job Server、Web Intelligence Processing Server、Report Application Server、Crystal Reports Processing Server、および Crystal Reports Cache Server など) をホストします。
- マシン `Databases` は、CMS システムデータベース、監査データベース、およびレポーティングデータベースをホストします。両方のデータベースを同じデータベースサーバにデプロイすることも、それぞれ個別のデータベースサーバにデプロイすることもできます。この例では、CMS データベースとレポーティングデータベースのすべてが同じデータベースサーバにデプロイされています。

別のネットワークにデプロイされたリッチクライアントとデータベース層



8.18.2.1 ファイアウォールによって BI プラットフォームサーバから隔てられた層を設定する

次に、この例を設定する方法を説明します。

1. この例には、次の通信要件が適用されます。
   - 公開ウィザードが、その両方のポートで CMS™ との通信を開始できる必要があります。
   - 公開ウィザードが、Input File Repository Server および Output File Repository Server との通信を開始できる必要があります。
   - Connection Server、Job Server の各子プロセス、および各 Processing Server が、レポーティングデータベースサーバのリスニングポートにアクセスできる必要があります。
   - CMS™ が CMS™ データベースサーバのリスニングポートにアクセスできる必要があります。
2. CMS™、Input File Repository Server(FRS)および Output File Repository Server(FRS)の専用ポートを設定します。1,025 ～ 65,535 の空のポートをどれでも使用できます。
   次の表に、この例で選択したポート番号を示します。

サーバ	ポート番号
Central Management Server™	6411
Input File Repository Server	6415
Output File Repository Server	6416

3. Job Server の子のためにポート範囲を設定する必要はありません。これは、 Job Server とデータベースサーバの間のファイアウォールの設定によって、任意のポートで通信を開始できるようになるためです。
4. 前の手順で設定したプラットフォームサーバの固定ポートとの通信を許可するように、`<Firewall_1>` を設定します。ポート 6400 は CMS™ ネームサーバポートのデフォルトのポート番号で、前の手順で明示的に設定する必要はありません。

ポート	送信先コンピュータ	ポート	アクション
任意	BOE_2	6400	許可
任意	BOE_2	6411	許可
任意	BOE_2	6415	許可
任意	BOE_2	6416	許可

   データベースサーバのリスニングポートとの通信を許可するように、`<Firewall_2>` を設定します。CMS™ (*boe_2*) は、CMS™ システムデータベースおよび監査データベースにアクセスできる必要があり、Job Server (*boe_3*) は、システムデータベースおよび監査データベースにアクセスできる必要があります。Job Server の子プロセスに対するポート範囲は設定していません。これは、子プロセスと CMS の通信はファイアウォールを通過しないためです。

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
BOE_2	任意	データベース	3306	許可
BOE_3	任意	データベース	3306	許可

5. このファイアウォールでは NAT は有効ではないため、`hosts` ファイルを設定する必要はありません。

関連情報

BI プラットフォームコンポーネント間の通信について [184 ページ]
ファイアウォール用の BI プラットフォームの設定 [197 ページ]

8.19 統合環境でのファイアウォールの設定

この節では、以下の ERP 環境に統合されている BI プラットフォームデプロイメントに特有の考慮事項およびポート設定について説明します。

- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

BI プラットフォームコンポーネントには、ブラウザクライアント、リッチクライアント、サーバ、および Web アプリケーションサーバでホストされるソフトウェア開発キット (SDK) が含まれます。システムコンポーネントは、複数のマシンにインストールできます。ファイアウォールと動作するようにシステムを設定するにあたって、BI プラットフォームと ERP コンポーネント間の通信の基本事項を理解しておくことは有益です。

BI プラットフォームサーバのポート要件

次のポートは、BI プラットフォームで対応するサーバに必要です。

サーバのポート要件
• Central Management Server ネームサーバポート • Central Management Server リクエストポート • Input File Repository Server(FRS)リクエストポート • Output File Repository Server(FRS)リクエストポート • Report Application Server リクエストポート • Crystal Reports Cache Server リクエストポート • Crystal Reports Page Server リクエストポート • Crystal Reports Processing Server リクエストポート

8.19.1 SAP 統合に固有のファイアウォールガイドライン

BI プラットフォームデプロイメントは、以下の通信ルールに従う必要があります。

- CMS は、SAP System Gateway ポートで SAP システムとの通信を開始できる必要があります。
- データアクセスコンポーネントを使用した Adaptive Job Server と Crystal Reports Processing Server が、SAP System Gateway ポートで SAP システムとの通信を開始できる必要があります。
- BW Publisher コンポーネントが、SAP System Gateway ポートで SAP システムとの通信を開始できる必要があります。
- SAP Enterprise Portal 側 (iView および KMC など) にデプロイされた BI プラットフォームコンポーネントは、HTTP/HTTPS ポートで BI プラットフォーム Web アプリケーションとの通信を開始できる必要があります。
- Web アプリケーションサーバが、SAP System Gateway サービスで通信を開始できる必要があります。
- Crystal Reports が、SAP System Gateway ポートおよび SAP System Dispatcher で SAP ホストとの通信を開始できる必要があります。

SAP Gateway サービスが通信するポートは、インストール時に指定したポートになります。

> **注記**
>
> コンポーネントを SAP システムに接続するために SAP ルータが必要な場合、SAP ルータ文字列を使用してコンポーネントを設定できます。たとえば、ロールとユーザをインポートするように SAP 権限認証システムを設定する場合、アプリケーションサーバ名の代わりに SAP ルータ文字列を使用できます。これにより、CMS は SAP ルータを通じて SAP システムと通信できるようになります。

関連情報

ローカル SAP ゲートウェイのインストール [976 ページ]

8.19.1.1 ポート要件の詳細

SAP のポート要件

BI プラットフォームは SAP NetWeaver との通信に SAP Java Connector (SAP JCO) を使用します。以下のポートを設定し、使用できるようにする必要があります。

- SAP Gateway サービスリスニングポート(3300 など)
- SAP Dispathcer サービスリスニングポート(3200 など)

次の表に、必要な固有のポート設定の概要を示します。

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
SAP	任意	BI プラットフォーム Web アプリケーションサーバ	Web サービス HTTP/HTTPS ポート	許可
SAP	任意	CMS	CMS ネームサーバポート	許可

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
SAP	任意	CMS	CMS リクエストポート	許可
Web アプリケーションサーバ	任意	SAP	SAP System Gateway サービスポート	許可
Central Management Server(CMS)	任意	SAP	SAP System Gateway サービスポート	許可
Crystal Reports™	任意	SAP	SAP System Gateway サービスポートおよび SAP System Dispatcher ポート	許可

8.19.2 JD Edwards EnterpriseOne 統合向けのファイアウォール設定

JD Edwards ソフトウェアと通信する BI プラットフォームのデプロイメントは、次の一般的な通信規則に従う必要があります。

- セントラル管理コンソール Web アプリケーションが、JDENET ポートとランダムに選択されたポートを通じて JD Edwards EnterpriseOne と通信できる必要があります。
- データコネクティビティクライアント側コンポーネントを搭載した Crystal Reports が、JDNET ポートを通じて JD Edwards EnterpriseOne と通信を開始できる必要があります。JD Edwards EnterpriseOne 側では、データを取得するため、制御不可能なランダムポートを通じてドライバと通信できる必要があります。
- Central Managment Server が、JDENET ポートとランダムに選択されたポートを通じて JD Edwards EnterpriseOne と通信できる必要があります。
- JDENET ポートの番号は、[JDENET] セクションの下の JD Edwards EntperiseOne アプリケーションサーバ設定ファイル (`JDE.INI`) にあります。

BI プラットフォームサーバのポート要件

製品	サーバのポート要件
SAP BusinessObjects Business Intelligence プラットフォーム	BI プラットフォーム Sign-on Server のポート

JD Edwards EnterpriseOne のポート要件

製品	ポート要件	説明
JD Edwards EnterpriseOne	JDENET ポートおよびランダムに選択されたポート	BI プラットフォームと JD Edwards EnterpriseOne アプリケーションサーバ間の通信に使用します。

JD Edwards と通信するための Web アプリケーションサーバの設定

この節では、ファイアウォールによって Web アプリケーションサーバとそれ以外のプラットフォームサーバが隔てられているようなデプロイメントシナリオで、ファイアウォールと BI プラットフォームが協調するように設定する方法を示します。

BI プラットフォームサーバおよびクライアントでのファイアウォールの設定については、このガイドの *BI プラットフォームのポート要件の節を参照してください。JD Edwards サーバとの通信では、標準的なファイアウォール設定のほかに、特別なポートを開く必要があります。

JD Edwards EnterpriseOne Enterprise

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
JD Edwards EnterpriseOne 用セキュリティコネクティビティ機能搭載 CMS	任意	JD Edwards EnterpriseOne	任意	許可
JD Edwards EnterpriseOne 用データコネクティビティ搭載 BI プラットフォームサーバ	任意	JD Edwards EnterpriseOne	任意	許可
JD Edwards EnterpriseOne 用クライアントサイドデータコネクティビティを搭載した Crystal Reports	任意	JD Edwards EnterpriseOne	任意	許可
Web アプリケーションサーバ	任意	JD Edwards EnterpriseOne	任意	許可

8.19.3 Oracle EBS に固有のファイアウォールガイドライン

BI プラットフォームのデプロイメントでは、以下のコンポーネントが Oracle データベースリスナポートを使って通信を開始できる必要があります。

- BI プラットフォーム Web コンポーネント
- CMS (特に Oracle EBS セキュリティプラグイン)
- BI プラットフォームバックエンドサーバ (特に EBS Data Access コンポーネント)
- Crystal Reports (特に EBS Data Access コンポーネント)

> ⓘ 注記
>
> 上記のすべてで Oracle データベースリスナポートのデフォルト値は、1521 です。

8.19.3.1 ポート要件の詳細

統合 Oracle EBS 環境で作業するには、BI プラットフォームの標準のファイアウォール設定のほかに追加のポートを開く必要があります。

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
Web アプリケーションサーバ	任意	Oracle EBS	Oracle データベースポート	許可
Oracle EBS 対応のセキュリティコネクティビティを搭載した CMS	任意	Oracle EBS	Oracle データベースポート	許可
Oracle EBS 対応のサーバ側データコネクティビティを搭載した BI プラットフォームサーバ	任意	Oracle EBS	Oracle データベースポート	許可
Oracle EBS 対応のクライアント側データコネクティビティを搭載した Crystal Reports	任意	Oracle EBS	Oracle データベースポート	許可

8.19.4 PeopleSoft Enterprise 統合向けのファイアウォール設定

PeopleSoft Enterprise と通信する BI プラットフォームのデプロイメントは、次の一般的な通信規則に従う必要があります。

- セキュリティコネクティビティコンポーネントを搭載した Central Management Server (CMS) が、PeopleSoft Query Access (QAS) Web サービスと通信を開始できる必要があります。
- データコネクティビティコンポーネントを搭載した BI プラットフォームサーバが、PeopleSoft QAS Web サービスと通信を開始できる必要があります。
- データコネクティビティクライアントコンポーネントを搭載した Crystal Reports が、PeopleSoft QAS Web サービスと通信を開始できる必要があります。
- Enterprise Management(EPM)Bridge が、CMS および Input File Repository Server と通信できる必要があります。
- EPM Bridge が、ODBC 接続を使用して PeopleSoft データベースと通信できる必要があります。

Web サービスのポート番号は、PeopleSoft Enterprise のドメイン名で指定したポートと同じです。

BI プラットフォームサーバのポート要件

製品	サーバのポート要件
SAP BI プラットフォーム	BI プラットフォーム Sign-on Server のポート

PeopleSoft のポート要件

製品	ポート要件	説明
PeopleSoft Enterprise: People Tools 8.46 以降	Web サービス HTTP/HTTPS ポート	このポートは、PeopleSoft Enterprise for People Tools 8.46 およびそれ以降のソリューションで SOAP 接続を使用する際に必要です。

BI プラットフォームおよび PeopleSoft のファイアウォールの設定

この節では、ファイアウォールによって Web アプリケーションサーバとそれ以外の BI プラットフォームサーバが隔てられているようなデプロイメントシナリオで、BI プラットフォームと PeopleSoft Enterprise が協調するように設定する方法を示します。

BI プラットフォームサーバおよびクライアントでのファイアウォールの設定については、*SAP BusinessObjects Business Intelligence* プラットフォーム管理者ガイドを参照してください。

BI プラットフォームでのファイアウォールの設定のほか、いくつかの特別な設定が必要です。

PeopleSoft Enterprise: PeopleTools 8.46 以降

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
PeopleSoft 対応のセキュリティコネクティビティ機能を搭載した CMS	任意	PeopleSoft	PeopleSoft Web サービス HTTP/HTTPS ポート	許可
PeopleSoft 対応のデータコネクティビティを搭載した BI プラットフォームサーバ	任意	PeopleSoft	PeopleSoft Web サービス HTTP/HTTPS ポート	許可
PeopleSoft 対応のクライアント側データコネクティビティを搭載した Crystal Reports	任意	PeopleSoft	PeopleSoft Web サービス HTTP/HTTPS ポート	許可
EPM Bridge	任意	CMS	CMS ネームサーバポート	許可
EPM Bridge	任意	CMS	CMS リクエストポート	許可
EPM Bridge	任意	Input File Repository Server	Input File Repository Server(FRS) ポート	許可
EPM Bridge	任意	PeopleSoft	PeopleSoft データベースポート	許可

8.19.5 Siebel 統合向けのファイアウォール設定

この節では、ファイアウォールで隔てられた BI プラットフォームと Siebel eBusiness Application システム間の通信に使用する特定のポートを示します。

- Web アプリケーションが、BI プラットフォーム Sign-on Server for Siebel と通信を開始できる必要があります。Enterprise Sign-on Server for Siebel の場合、3 つのポートが必要です。

1. Echo(TCP)ポート 7。Sign-on Server へのアクセスを確認します。
2. BI プラットフォーム Sign-on Server for Siebel ポート (デフォルトは 8448)。CORBA IOR リスニング用ポートです。
3. ランダム POA ポート。制御不可能な CORBA 通信用で、すべてのポートを開く必要があります。

- CMS では、BI プラットフォーム Sign-on Server for Siebel と通信を開始できる必要があります。CORBA IOR リスニングポートは、各 Sign-on Server に設定します (たとえば 8448)。また、BI プラットフォームをインストールすると確認できるランダム POA ポート番号も開く必要があります。
- BI プラットフォーム Sign-on Server for Siebel は、SCBroker (Siebel 接続ブローカ) ポート (たとえば 2321) と通信を開始できる必要があります。
- BI プラットフォームバックエンドサーバ (Siebel Data Access コンポーネント) は、SCBroker (Siebel 接続ブローカ) ポート (例 2321) と通信を開始できる必要があります。
- Crystal Reports (Siebel Data Access コンポーネント) は、SCBroker (Siebel 接続ブローカ) ポート (例 2321) と通信を開始できる必要があります。

ポートの詳細説明

この節では、BI プラットフォームで使用するポートの一覧を示します。ファイアウォールを伴って BI プラットフォームをデプロイする場合、この情報を使用すると Siebel との統合に固有のファイアウォールで開くポートの数を最小限にできます。

BI プラットフォームサーバのポート要件

製品	サーバのポート要件
SAP BI プラットフォーム	BI プラットフォーム Sign-on Server のポート

Siebel のポート要件

製品	ポート要件	説明
Siebel eBusiness アプリケーション	2321	デフォルトの SCBroker (Siebel 接続ブローカ) ポート

Siebel との統合のための **BI** プラットフォームファイアウォールの設定

この節では、ファイアウォールによって Web アプリケーションサーバとそれ以外のプラットフォームサーバが隔てられているようなデプロイメントシナリオで、Siebel と BI プラットフォームが協調するようにファイアウォールを設定する方法を示します。

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
Web アプリケーションサーバ	任意	Siebel 対応 BI プラットフォーム Sign-on Server	任意	許可
CMS	任意	Siebel 対応 BI プラットフォーム Sign-on Server	任意	許可

送信元コンピュータ	ポート	送信先コンピュータ	ポート	アクション
Siebel 対応 BI プラットフォーム Sign-on Server	任意	Siebel	SCBroker ポート	許可
Siebel 対応のサーバ側データコネクティビティを搭載した BI プラットフォームサーバ	任意	Siebel	SCBroker ポート	許可
Siebel 対応のクライアント側データコネクティビティを搭載した Crystal Reports	任意	Siebel	SCBroker ポート	許可

8.20 BI プラットフォームおよびリバースプロキシサーバ

BI プラットフォームは、1 つまたは複数のリバースプロキシサーバを含む環境にデプロイできます。リバースプロキシサーバは、通常は Web アプリケーションサーバの前面にデプロイされて、1 つの IP アドレスの背後にその Web アプリケーションサーバを隠します。この設定では、プライベートな Web アプリケーションサーバに向けたすべてのインターネットトラフィックはリバースプロキシサーバを通過するため、プライベート IP アドレスは隠されます。

リバースプロキシサーバはパブリック URL を内部 URL に変換するため、内部ネットワークにデプロイされた BI プラットフォーム Web アプリケーションの URL と共に設定する必要があります。

8.20.1 Web アプリケーションのデプロイ方法について

BI プラットフォーム Web アプリケーションは、Web アプリケーションサーバにデプロイされます。アプリケーションは、WDeploy ツールを使用したインストール中に、自動的にデプロイされます。またこのツールを使用して、BI プラットフォームがデプロイされた後で、アプリケーションを手動でデプロイすることもできます。Web アプリケーションは、デフォルトの Windows インストールでは、次のディレクトリに保存されます。

```
C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI
4.0¥warfiles¥webapps
```

WDeploy は、次に示すような WAR ファイルのデプロイに使用されます。

- `BOE`: セントラル管理コンソール (CMC)、BI ラウンチパッド、および OpenDocument を含みます。
- `dswsbobje`: Web サービスアプリケーションを含みます。

Web アプリケーションサーバがリバースプロキシサーバの背後にある場合、リバースプロキシサーバには、WAR ファイルの正しいコンテキストパスを設定する必要があります。BI プラットフォームの機能をすべて公開するには、デプロイされているすべての BI プラットフォーム WAR ファイルのコンテキストパスを設定します。

8.21 BI プラットフォーム Web アプリケーションに対するリバースプロキシサーバの設定

リバースプロキシサーバは、デプロイメント (BI プラットフォーム Web アプリケーションがそのリバースプロキシサーバの背後にデプロイされている) 内の正しい Web アプリケーションに、入力 URL リクエストをマップするように設定する必要があります。

ここでは、一部のサポートされているリバースプロキシサーバに固有の設定例を示しています。使用しているリバースプロキシサーバの詳細については、ベンダーのマニュアルを参照してください。

8.21.1 リバースプロキシサーバの設定の詳細な手順

WAR ファイルの設定

BI プラットフォーム Web アプリケーションは、Web アプリケーションサーバの WAR ファイルとしてデプロイされています。リバースプロキシサーバで、デプロイメントに必要な WAR ファイルに対する指示子を設定したことを確認します。WDeploy を使用して、`BOE` または `dswsbobje` WAR ファイルのいずれかをデプロイできます。WDeploy の詳細については、*BI プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

カスタム設定ディレクトリで BOE プロパティを指定します。

`BOE.war` ファイルには、グローバルプロパティとアプリケーション固有のプロパティが含まれます。プロパティを変更する必要がある場合、カスタム設定ディレクトリを使用します。デフォルトでは、このディレクトリは、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にあります。

> ⚠ 警告
>
> デフォルトディレクトリのファイルを上書きしないように、`config¥default` ディレクトリにあるプロパティは変更しないでください。`custom` ディレクトリを使用する必要があります。

> ⓘ 注記
>
> BI プラットフォームにバンドルされている Tomcat バージョンなどの Web アプリケーションサーバの一部では、`BOE.war` ファイルに直接アクセスすることができます。そのようなシナリオでは、WAR ファイルをアンデプロイすることなく、カスタム設定を直接設定できます。`BOE.war` ファイルにアクセスできない場合は、ファイルをアンデプロイしてからカスタマイズし、再デプロイする必要があります。

スラッシュ (/) の一貫した使用

リバースプロキシサーバでは、ブラウザ URL に入力するときと同じ方法でコンテキストパスを定義します。たとえば、指示子のリバースプロキシサーバのミラーパスの最後にスラッシュ (/) が含まれている場合、ブラウザ URL の最後にも「/」を入力します。

リバースプロキシサーバの指示子のソース URL と出力先の URL の両方で、"/"文字が一貫して使用されていることを確認してください。ソース URL の最後に"/"文字が追加されている場合は出力先 URL の最後にも追加する必要があります。

8.21.2 リバースプロキシサーバを設定する

下記の手順は、BI プラットフォーム Web アプリケーションをサポートされているリバースプロキシサーバ上で機能させるために実行する必要があります。

1. リバースプロキシサーバがベンダの指示とデプロイメントのネットワークトポロジに従って正しく設定されていることを確認します。
2. 必要な BI プラットフォーム WAR ファイルを特定します。
3. BI プラットフォームの各 WAR ファイルに対して、リバースプロキシサーバを設定します。リバースプロキシサーバの種類によって、指定される規則が異なります。
4. 固有の設定が必要な場合は、それを実行します。一部の Web アプリケーションは、特定の Web アプリケーションサーバにデプロイされた場合に、固有の設定が必要になります。

8.21.3 BI プラットフォーム用に Apache 2.2 リバースプロキシサーバを設定する

ここでは、BI プラットフォームと Apache 2.2 を連携させる設定のワークフローを提供します。

1. BI プラットフォームと Apache 2.2 が、別のマシンにインストールされていることを確認します。
2. ベンダのマニュアルの説明どおりに Apache 2.2 がインストールされ、リバースプロキシサーバとして設定されていることを確認します。
3. リバースプロキシサーバの背後にデプロイされている各 WAR ファイルに対して、`ProxyPass` を設定します。
4. Apache リバースプロキシのインストールフォルダにある *httpd.conf* ファイルを開きます。
5. リバースプロキシサーバの背後にデプロイされている各 Web アプリケーションに対して、`ProxyPassReverseCookiePath` を設定します。以下はその例です。

```
ProxyPass /C1/BOE/ http://<appservername>:80/BOE/
ProxyPassReverseCookiePath /BOE/C1/BOE/
ProxyPassReverse /C1/BOE/ http://<appservername>:80/BOE/
ProxyPass /C1/explorer/ http://<appservername>:80/explorer/
ProxyPassReverseCookiePath /BOE/C1/explorer/
ProxyPassReverse /C1/explorer/ http://<appservername>:80/explorer/
```

8.21.4 BI プラットフォーム用に WebSEAL 6.0 リバースプロキシサーバを設定する

ここでは、BI プラットフォームと WebSEAL 6.0 を連携させるための設定方法について説明します。

推奨される設定方法は、内部の Web アプリケーションサーバまたは Web サーバがホストしているすべての BI プラットフォーム Web アプリケーションを 1 つのマウントポイントにマップする、1 つの標準的なジャンクションを作成することです。

1. BI プラットフォームと WebSEAL 6.0 が、別のマシンにインストールされていることを確認します。

   BI プラットフォームと WebSEAL 6.0 を同じマシンにデプロイすることは、可能ですが推奨はされません。このデプロイメントシナリオの設定手順の詳細は、WebSEAL 6.0 のベンダーマニュアルを参照してください。
2. WebSeal 6.0 が、ベンダのマニュアルの説明どおりにインストールおよび設定されていることを確認します。
3. WebSeal の *pdadmin* コマンドラインユーティリティを起動します。管理者権限を持つユーザとして、*sec_master* などの安全なドメインにログインします。
4. *pdadmin sec_master* のプロンプトで、次のコマンドを入力します。

   ```
   server task <instance_name-webseald-host_name> create -t
   <type> -h <host_name> -p <port> <junction_point>
   ```

   場所:

   - `<instance_name-webseald-host_name>` には、インストールされている WebSEAL インスタンスの完全なサーバ名を指定します。この完全なサーバ名は、`server list` コマンドの出力結果と同じ形式で指定します。
   - `<type>` には、ジャンクションの種類を指定します。ジャンクションが内部の HTTP ポートにマップしている場合は、`tcp` を使用します。ジャンクションが内部の HTTPS ポートにマップしている場合は、`ssl` を使用します。
   - `<host_name>` には、リクエストを受信する内部サーバの DNS ホスト名または IP アドレスを指定します。
   - `<port>` には、リクエストを受信する内部サーバの TCP ポートを指定します。
   - `<junction_point>` には、WebSEAL で保護されたオブジェクト空間(内部サーバのドキュメント空間がマウントされる)のディレクトリを指定します。

例

```
server task default-webseald-webseal.rp.sap.com
create -t tcp -h 10.50.130.123 -p 8080/hr
```

8.21.5 BI プラットフォーム用に Microsoft ISA 2006 を設定する

ここでは、BI プラットフォームと ISA 2006 を連携させるための設定方法について説明します。

推奨される設定方法は、内部の Web アプリケーションサーバまたは Web サーバがホストしているすべての BI プラットフォーム WAR ファイルを 1 つのマウントポイントにマップする、1 つの標準的なジャンクションを作成す

ることです。Web アプリケーションサーバによっては、ISA 2006 と連携するために、アプリケーションサーバに追加の設定が必要になる場合があります。

1. BI プラットフォームと ISA 2006 が、別のマシンにインストールされていることを確認します。

   BI プラットフォームと ISA 2006 を同じマシンにデプロイすることは、可能ですが推奨はされません。このデプロイメントシナリオの設定手順の詳細は、ISA 2006 のマニュアルを参照してください。
2. ISA 2006 が、ベンダーのマニュアルの説明どおりにインストールおよび設定されていることを確認します。
3. ISA Server 管理ユーティリティを起動します。
4. ナビゲーションパネルを使用して、新しい公開ルールを呼び出します。
   a. 次の操作を実行します。

      アレイ > *MachineName* > ファイアウォールポリシー > 新規 > *Web* サイト公開ルール

      > **→ 注意**
      >
      > `MachineName` は、ISA 2006 がインストールされているマシンの名前に置き換えます。

   b. [*Web* 公開ルールの名前]にルール名を入力し、[次へ]をクリックします。
   c. ルールアクションとして[許可する]を選択し、[次へ]をクリックします。
   d. 公開の種類として[*1 つの Web サイトまたは負荷分散装置を公開する*]を選択し、[次へ]をクリックします。
   e. ISA Server と公開される Web サイト間の接続の種類を選択し、[次へ]をクリックします。

      たとえば、[公開された *Web* サーバまたはサーバファームの接続に、セキュリティで保護されていない接続を使用する]を選択します。
   f. [内部サイト名] に、公開している Web サイトの内部名 (BI プラットフォームをホストしているマシン名など) を入力し、[次へ] をクリックします。

      > **ⓘ 注記**
      >
      > ISA 2006 をホストしているマシンがターゲットサーバに接続できない場合は、[コンピュータ名または *IP* アドレスを使用して、公開されたサーバに接続する] を選択し、該当のフィールドに名前または IP アドレスを入力します。

   g. [パブリック名の詳細] で、ドメイン名 (たとえば *Any domain name* など) を選択し、内部公開の詳細 (たとえば `/*` など) を指定します。[次へ]をクリックします。
      次に、着信した Web リクエストを監視するための新しい Web リスナを作成する必要があります。
5. [新規]をクリックし、新しい Web リスナの定義ウィザードを起動します。
   a. [*Web* リスナ名] に名前を入力し、[次へ] をクリックします。
   b. ISA Server と公開される Web サイト間の接続の種類を選択し、[次へ]をクリックします。

      たとえば、[クライアントとの *SSL* セキュリティ保護接続を必要としない]を選択します。
   c. [*Web* リスナの *IP* アドレス] セクションで、次を選択し、[次へ] をクリックします。
      - 内部
      - 外部
      - ローカルホスト
      - すべてのネットワーク

      これで、ISA Server は、HTTP を介してのみ公開を行うように設定されました。
   d. [認証設定] オプションを選択し、[次へ] をクリックしてから、[完了] をクリックします。
      Web 公開ルールの新しいリスナが設定されます。
6. [ユーザセット] で [次へ] をクリックし、[完了] をクリックします。

7. [適用] をクリックして、Web 公開ルールのすべての設定を保存し、ISA 2006 の設定を更新します。
   次に、Web 公開ルールのプロパティを更新して、Web アプリケーションのパスにマップする必要があります。
8. ナビゲーションパネルで、[ファイアウォールポリシー]を右クリックし、[プロパティ]を選択します。
9. [パス] タブで [追加] をクリックして、ルートを SAP BusinessObjects Web アプリケーションにマップします。
10. [パブリック名] タブで、[次の *Web* サイトを要求する] を選択し、[追加] をクリックします。
11. [パブリック名] ダイアログボックスで、ISA 2006 サーバ名を入力し、[*OK*] をクリックします。
12. [適用] をクリックして、Web 公開ルールのすべての設定を保存し、ISA 2006 の設定を更新します。
13. 次の URL にアクセスして接続を確認します。

    `http://<ISA Server のホスト名>:<Web リスナのポート番号>/<アプリケーションの外部パス>`

    例: **`http://myISAserver:80/Product/BOE/CMC`**

    > ⓘ 注記
    >
    > ブラウザを何度か最新表示しなければならない場合があります。

設定したルールの HTTP ポリシーを変更して、CMC にログオンできるようにする必要があります。ISA Server 管理ユーティリティで作成したルールを右クリックし、[*HTTP* の構成]を選択します。[*URL* 保護]エリアで、[正規化を検証する]をオフにする必要があります。

BI プラットフォームにリモートでアクセスするには、アクセスルールを作成する必要があります。

8.22 リバースプロキシデプロイメントでの BI プラットフォームに固有の設定

一部の BI プラットフォーム製品では、リバースプロキシデプロイメントで正しく機能するために、追加の設定が必要になります。ここでは、追加の設定を実行する方法について説明します。

8.22.1 Web サービスのリバースプロキシの有効化

この節では、Web サービスのリバースプロキシを有効にするために必要な手順について説明します。

8.22.1.1 Tomcat でリバースプロキシを有効化する

Tomcat Web アプリケーションサーバでリバースプロキシを有効にするには、`server.xml` ファイルを変更する必要があります。リバースプロキシサーバのリスニングポートとして `proxyPort` を設定することや、新しい `proxyName` を追加することが、必要な変更に含まれます。ここでは、その手順を説明します。

1. Tomcat を停止します。
2. Tomcat の `server.xml` を開きます。

Windows では、server.xml は C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥conf にあります。

Unix では、 server.xml は <CATALINA_HOME>/conf にあります。<CATALINA_HOME> のデフォルト値は <INSTALLDIR>/sap_bobj/tomcat です。

3. server.xml ファイル内で次のセクションを探します。

```
<!-- A "Connector" represents an endpoint by which requests are received
         and responses are returned. Documentation at :
         Java HTTP Connector: /docs/config/http.html (blocking & non-blocking)
         Java AJP  Connector: /docs/config/ajp.html
         APR (HTTP/AJP) Connector: /docs/apr.html
         Define a non-SSL/TLS HTTP/1.1 Connector on port 8080
    -->
    <Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443" compression="on" URIEncoding="UTF-8"
compressionMinSize="2048" noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml,text/plain,text/css,text/
javascript,text/json,application/javascript,application/json"/>
```

4. <!-- と -->. を削除して、Connector 要素のコメントを解除します。
5. proxyPort の値をリバースプロキシサーバのリスニングポートに修正します。
6. Connector の属性リストに新しい proxyName 属性を追加します。proxyName の値は、プロキシサーバ名にします。そのプロキシサーバ名は、Tomcat が正しい IP アドレスに解決できるものである必要があります。

   例:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082 -->
                <!--See proxy documentation for more information about using
                  this.-->
                <Connector port="8082"
                maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
                enableLookups="false"
                acceptCount="100" debug="0"
connectionTimeout="20000"
                proxyName="my_reverse_proxy_server.domain.com"
                proxyPort="ReverseProxyServerPort"
                disableUploadTimeout="true" />
```

   この例では、my_reverse_proxy_server.domain.com と ReverseProxyServerPort を正しいリバースプロキシサーバ名とそのリスニングポートで置き換える必要があります。

7. server.xml ファイルを保存して閉じます。
8. Tomcat を再起動します。
9. リバースプロキシサーバの仮想パスが正しい Tomcat connector ポートにマッピングされていることを確認します。この例では、ポートは 8082 です。

   次の例では、Apache HTTP Server 2.2 から Tomcat に導入されたリバースプロキシ SAP BusinessObjects™ Web Services への設定を示します。

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/
dswsbobje
                ProxyPassReverseCookiePath /dswsbobje /XI3.0/
dswsbobje
```

Web サービスを有効にするには、コネクタのプロキシ名とポート番号を同一にする必要があります。

8.22.1.2 Tomcat 以外の Web アプリケーションサーバでの Web サービスに対するリバースプロキシの有効化

次の手順には、BI プラットフォーム Web アプリケーションが、選択した Web アプリケーションサーバに対して正常に設定されている必要があります。`wsresources` では、大文字と小文字が区別されます。

1. Web アプリケーションサーバを停止します。
2. `dsws.properties` ファイル内の Web サービスの外部 URL を指定します。

   このファイルは、`dswsbobje` Web アプリケーションにあります。たとえば、外部 URL が `http://my_reverse_proxy_server.domain.com/dswsbobje/` の場合、dsws.properties ファイルの次のプロパティを更新します。

   - `wsresource1=ReportEngine|reportengine web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/ReportEngine`
   - `wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatalog`
   - `wsresource3=Publish|publish web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/Publish`
   - `wsresource4=QueryService|query web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/QueryService`
   - `wsresource5=BIPlatform|BIPlatform web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BIPlatform`
   - `wsresource6=LiveOffice|Live Office web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/LiveOffice`
3. `dsws.properties` ファイルを保存して閉じます。
4. Web アプリケーションサーバを再起動します。
5. リバースプロキシサーバの仮想パスが正しい Web アプリケーションサーバの Connector ポートにマッピングされていることを確認します。次の例では、Apache HTTP Server 2.2 から、選択した Web アプリケーションサーバにデプロイされたリバースプロキシ BI プラットフォーム Web サービスへの設定を示します。

   ```
   ProxyPass /SAP/dswsbobje http://internalServer:<listening port> /dswsbobje
   ```

   ```
   ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
   ```

   この例で、`<listening port>` は Web アプリケーションサーバのリスニングポートです。

8.22.2 ISA 2006 に対するセッション cookie のルートパスの有効化

ここでは、セッション cookie のルートパスで ISA 2006 をリバースプロキシサーバとして使用できるようにするための、各 Web アプリケーションサーバの設定方法を説明します。

8.22.2.1 Apache Tomcat を設定する

ISA 2006 をリバースプロキシサーバとして使用するようにセッション cookie のルートパスを設定するには、`server.xml` の `<Connector>` 要素に次の行を追加します。

```
emptySessionPath="true"
```

1. Tomcat を停止します。
2. 次のディレクトリにある server.xml ファイルを開きます。

   `<CATALINA_HOME>¥conf`
3. server.xml ファイルで次のセクションを見つけます。

   ```
   <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
   <!-- See proxy documentation for more information about using this -->
   <!--
   <Connector port="8082"
   maxThreads="150" minSpareThreads="25" maxS
   pareThreads="75" enableLookups="false"
   acceptCount="100" debug="0" connectionTimeout="20000"
   proxyPort="80" disableUploadTimeout="true" />
   -->
   ```
4. `<!--` と `-->` を削除して、Connector 要素のコメントを解除します。
5. ISA 2006 をリバースプロキシサーバとして使用するようにセッション cookie のルートパスを設定するには、`server.xml` の `<Connector>` 要素に次の行を追加します。

   ```
   emptySessionPath="true"
   ```
6. `proxyPort` の値をリバースプロキシサーバのリスニングポートに修正します。
7. Connector の属性リストに新しい `proxyName` 属性を追加します。この値は、プロキシサーバ名にします。そのプロキシサーバ名は、Tomcat が正しい IP アドレスに解決できるものである必要があります。

   以下はその例です。

   ```
   <!--Define a Proxied HTTP/1.1 Connector on port 8082
   -->
   <!-- See proxy documentation for more information about using
   this -->
   <Connector port="8082"
   maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
   enableLookups="false" emptySessionPath="true"
   acceptCount="100" debug="0" connectionTimeout="20000"
   proxyName="my_reverse_proxy_server.domain.com"
   proxyPort="ReverseProxyServerPort"
   disableUploadTimeout="true" />
   ```
8. `server.xml` ファイルを保存して閉じます。
9. Tomcat を再起動します。

リバースプロキシサーバの仮想パスが正しい Tomcat connector ポートにマッピングされていることを確認します。この例では、ポートは 8082 です。

8.22.2.2 Sun Java 8.2 を設定する

すべての BI プラットフォーム Web アプリケーションで、`sun-web.xml` を変更する必要があります。

1. <SUN_WEBAPP_DOMAIN>¥generated¥xml¥j2ee-modules¥webapps¥BOE¥WEB-INF に移動します。
2. sun-web.xml を開きます。
3. <context-root> コンテナの後に、次の行を追加します。

```
        <session-config>
                <cookie-properties>
                        <property name="cookiePath" value="/" />
                </cookie-properties>
        </session-config>
    <property name="reuseSessionID" value="true"/>
```

4. 保存して、sun-web.xml を閉じます。
5. すべての Web アプリケーションについて手順 1 ～ 4 を繰り返します。

8.22.2.3 Oracle Application Server 10gR3 を設定する

すべての BI プラットフォーム Web アプリケーションのデプロイメントディレクトリの global-web-application.xml または orion-web.xml を変更する必要があります。

1. <ORACLE_HOME>¥j2ee¥home¥config¥ に移動します。
2. global-web-application.xml または orion-web.xml を開きます。
3. 次の行を <orion-web-app> コンテナに追加します。

```
<session-tracking cookie-path="/" />
```

4. 設定ファイルを保存して閉じます。
5. Oracle 管理コンソールにログオンします。
   a. *OC4J:home* > 管理 > サーバプロパティ の順に選択します。
   b. [コマンドラインオプション]で[オプション]を選択します。
   c. [一行追加]をクリックし、次の行を入力します。

   ```
   Doracle.useSessionIDFromCookie=true
   ```

6. Oracle サーバを再起動します。

8.22.2.4 WebSphere Community Edition 2.0 を設定する

1. WebSphere Community Edition 2.0 管理コンソールを開きます。
2. 左側のナビゲーションパネルで、[サーバ] を見つけ、[*Web* サーバ] を選択します。
3. コネクタを選択し、[編集] クリックします。
4. [*emptySessionPath*] チェックボックスをオンにし、[保存] をクリックします。
5. [*ProxyName*] に ISA サーバの名前を入力します。
6. [*ProxyPort*] に ISA リスナポート番号を入力します。
7. コネクタを停止し、再起動します。

8.22.3 SAP BusinessObjects Live Office に対するリバースプロキシの有効化

SAP BusinessObjects Live Office のビューオブジェクトを Web ブラウザ機能の中でリバースプロキシに対して有効にするには、デフォルトビューアの URL を調整します。これは、セントラル管理コンソール(CMC)または Live Office オプションによって実行します。

> **注記**
>
> この節では、BI 起動パッドのリバースプロキシおよび BI プラットフォーム Web サービスが正常に有効化されていると想定します。

8.22.3.1 CMC でデフォルトビューアの URL を調整する

1. CMC にログオンします。
2. [アプリケーション] ページで、[セントラル管理コンソール] をクリックします。
3. アクション > 処理設定 を選択します。
4. [*URL*] フィールドで、正しいデフォルトビューアの URL を選択して [保存して閉じる] をクリックします。
   例:

   ```
   http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?
   sIDType=CUID&iDocID=%SI_CUID%
   ```

   この例で、`ReverseProxyServer` と `ReverseProxyServerPort` は、正しいリバースプロキシサーバ名とそのリスニングポートです。

9 認証

9.1 BI プラットフォームの認証オプション

認証とは、システムにアクセスしようとするユーザの身元情報を確認するプロセスです。権限管理とは、そのユーザが指定のオブジェクトに対して要求したアクションを実行するための十分なアクセス権を持っているかどうかを確認するプロセスです。

セキュリティプラグインにより、BI プラットフォームがユーザを認証する方法を拡張およびカスタマイズできます。 セキュリティプラグインを使用すると、ユーザアカウントとグループをサードパーティシステムから BI プラットフォームにマップできるので、アカウントの作成および管理が簡単になります。 サードパーティのユーザアカウントまたはグループを既存の BI プラットフォームユーザアカウントまたはグループにマップしたり、外部システム内のマップされた各エントリに対応する新しい Enterprise ユーザアカウントまたはグループを作成したりすることができます。

最新リリースでは、次の認証方法がサポートされています。

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

BI プラットフォームは使用環境に合わせてカスタマイズできるので、認証やプロセスは、システムによって異なる場合があります。

9.1.1 一次認証

一次認証は、ユーザが初めてシステムにアクセスするときに実行されます。一次認証中、次のいずれかが行われます。

- シングルサインオンが設定されていない場合、ユーザが、ユーザ名、パスワード、認証の種類など各自の認証情報を指定します。
  これらの詳細については、ログオン画面でユーザが入力します。

  > ⓘ 注記
  >
  > デフォルトでは、管理者が変更しない限り、大文字と小文字を含むパスワードの使用を求める設定のみが選択されています。この場合、少なくとも 1 つの大文字と 1 つの小文字がパスワードに含まれている必要があります。必要に応じて、管理者はその他のパスワード設定を強制することができます。

- シングルサインオン方法が設定されている場合、ユーザの認証情報はサイレントに伝達されます。これらの詳細情報は、Kerberos、SiteMinder などの他の方法を使用して抽出されます。

認証の種類は、セントラル管理コンソール (CMC) の [認証] 管理エリアで設定および有効化した種類に応じて、Enterprise、LDAP、Windows AD、SAP、Oracle EBS、Siebel、JD Edwards EnterpriseOne、PeopleSoft Enterprise となります。ユーザの Web ブラウザは、HTTP を使用して情報を Web サーバに送信します。次にその情報は、Web サーバから CMS または適切なプラットフォームサーバに転送されます。

Web アプリケーションサーバは、ユーザの情報をサーバ側のスクリプトに渡します。このスクリプトは内部的に SDK と通信し、最終的に適切なセキュリティプラグインによってユーザがユーザデータベースに照会されて認証されます。

たとえば、ユーザが BI ラウンチパッドにログオンして Enterprise 認証を指定すると、SDK により BI プラットフォームセキュリティプラグインを使用して認証が実行されます。Central Management Server (CMS) は、セキュリティプラグインを使用し、システムデータベースと照合してユーザ名とパスワードを確認します。あるいは、ユーザが異なる認証方法を指定した場合、SDK ではそれに対応するセキュリティプラグインを使用して、ユーザを認証します。

セキュリティプラグインによりアカウント情報の一致が通知されると、CMS によりアクティブなシステム ID がユーザに与えられ、次のアクションが実行されます。

- CMS は、ユーザの Enterprise セッションを作成します。セッションがアクティブな間、このセッションによりシステムの 1 ユーザライセンスが使用されます。
- CMS によりログオントークンが生成およびエンコードされ、Web アプリケーションサーバに送信されます。
- Web アプリケーションサーバは、メモリのセッション変数にユーザの情報を保存します。このセッションがアクティブな間、BI プラットフォームがユーザのリクエストに応答できるよう、セッションに情報が保存されます。

  > ⓘ 注記
  >
  > セッション変数には、ユーザのパスワードは含まれません。

- Web アプリケーションサーバは、クライアントのブラウザの Cookie でログオントークンを維持します。これは、クラスタ化した CMS がある場合、または BI ラウンチパッドがセッションアフィニティに対してクラスタ化されている場合などに、フェイルオーバー目的でのみ使用されます。

  > ⓘ 注記
  >
  > ログオントークンは無効にすることができます。ただし、ログオントークンを無効にすると、フェイルオーバーも無効になります。

9.1.2 セキュリティプラグイン

セキュリティプラグインにより、BI プラットフォームがユーザを認証する方法を拡張およびカスタマイズできます。BI プラットフォームには、次のプラグインが含まれます。

- Enterprise
- LDAP
- Windows AD
- SAP

- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

セキュリティプラグインを使用すると、ユーザアカウントとグループをサードパーティシステムから BI プラットフォームにマップできるので、アカウントの作成および管理が簡単になります。サードパーティのユーザアカウントまたはグループを既存の BI プラットフォームユーザアカウントまたはグループにマップしたり、外部システム内のマップされた各エントリに対応する新しい Enterprise ユーザアカウントまたはグループを作成したりすることができます。

セキュリティプラグインは、サードパーティのユーザとグループのリストを動的に管理します。外部グループを BI プラットフォームにマップすると、そのグループに属するすべてのユーザが BI プラットフォームに正常にログオンできるようになります。その後にサードパーティのグループメンバーシップに変更を加えるときには、BI プラットフォームでリストを更新したり最新表示したりする必要はありません。たとえば、LDAP グループを BI プラットフォームにマップして、新しいユーザをこのグループに追加すると、その新しいユーザが有効な LDAP 認証情報を使用して BI プラットフォームに最初にログオンするときに、そのユーザ用のエイリアスがセキュリティプラグインによって動的に作成されます。

また、セキュリティプラグインを使用すると、マップされたユーザとグループが Enterprise アカウントとして扱われるので、一貫した方法でユーザとグループにアクセス権を割り当てることができます。たとえば、いくつかのユーザアカウントまたはグループを Windows AD からマップして、別のユーザアカウントまたはグループを LDAP ディレクトリサーバからマップできます。BI プラットフォーム内でアクセス権を割り当てるか、新しいカスタムグループを作成する必要がある場合は、すべての設定を CMC で行います。

各セキュリティプラグインは、適切なユーザデータベースを照会してユーザのアカウント情報を確認する認証プロバイダとして動作します。ユーザは BI プラットフォームにログオンするときに認証の種類を選択します。認証の種類は、CMC の [認証] 管理エリアで設定し、有効にされたものです。

> **注記**
>
> BI プラットフォームサーバコンポーネントを UNIX 上で実行している場合、Windows AD セキュリティプラグインではユーザ認証を行うことができません。

9.1.3 BI プラットフォームへのシングルサインオン

BI プラットフォームへのシングルサインオンとは、ユーザが一度オペレーティングシステムにログオンすると、ログオン情報を再度入力しなくても SSO をサポートするアプリケーションにアクセスできるということです。ユーザがログオンすると、そのユーザのセキュリティコンテキストが作成されます。このコンテキストは、SSO を実行するために BI プラットフォームに反映することができます。

“匿名シングルサインオン”も BI プラットフォームへのシングルサインオンを表しますが、この場合は特に、guest ユーザアカウントに対するシングルサインオン機能のことを意味します。guest ユーザアカウントが有効の場合は (デフォルト)、だれでも guest として BI プラットフォームにログオンでき、ログオンしたユーザには、システムへのアクセス権が付与されます。

9.1.3.1 シングルサインオンのサポート

シングルサインオンという用語は、さまざまなシナリオを表すために使用されます。最も基本的なレベルでは、ユーザがログオン情報を一度入力するだけで 2 つ以上のアプリケーションやシステムにアクセスできる状況のことを表します。ログオン情報の入力が一度で済むので、システムとの対話が簡素化されます。

BI ラウンチパッドへのシングルサインオンは、BI プラットフォームで提供するか、または使用しているアプリケーションサーバの種類とオペレーティングシステムに応じて、別の認証ツールで提供されます。

Windows で Java アプリケーションサーバを使用している場合は、以下のシングルサインオン方法を利用できます。

- Windows AD と Kerberos の併用
- Windows AD と SiteMinder の併用

Windows で IIS を使用している場合は、以下のシングルサインオン方法を利用できます。

- Windows AD と Kerberos の併用
- Windows AD と NTLM の併用
- Windows AD と SiteMinder の併用

Windows または UNIX で、プラットフォームでサポートされるいずれかの Web アプリケーションサーバを使用している場合に利用可能なシングルサインオンのサポート方法は、次のとおりです。

- LDAP と SiteMinder の併用
- 信用できる認証
- Windows AD と Kerberos の併用
- SUSE 11 での Kerberos 経由の LDAP
- 信用できる認証を介した SAP NetWeaver SSO

> ⓘ 注記
>
> UNIX の Java アプリケーションがある場合は、Windows AD と Kerberos を併用できます。ただし、BI プラットフォームサービスは、Windows サーバで実行する必要があります。

次の表に、BI 起動パッドに対して利用可能なシングルサインオンのサポート方法を示します。

認証モード	CMS サーバ	オプション	注
Windows AD	Windows のみ	Windows AD と Kerberos の併用のみ	BI 起動パッドおよび CMC に対する Windows AD 認証は、このボックスから利用できます。
LDAP	サポートされている任意のプラットフォーム	サポートされている LDAP ディレクトリサーバと SiteMinder の併用のみ。	BI 起動パッドおよび CMC に対する LDAP 認証は、このボックスから利用できます。BI 起動パッドや CMC への SSO には SiteMinder が必要です。
Enterprise	サポートされている任意のプラットフォーム	信用できる認証	BI 起動パッドおよび CMC に対する Enterprise 認証は、このボックスから利用できます。BI 起動パッドや CMC に対する Enterprise 認証による

認証モード	CMS サーバ	オプション	注
			SSO には、信用できる認証が必要です。

9.1.3.1.1 CMC のシングルサインオンの有効化

CMC の SSO を有効化するには、次の手順に従います。

クライアント側で、CMC の初期設定の前にキャッシュをクリアする必要があります。 そうしないと、Enterprise 認証方法がキャッシュされます。

Tomcat サーバで、次の手順を実行します。

1. BILP の SSO 用にすでに設定されているシステムで、`C:¥Program Files (x86)¥SAP BusinessObjects¥tomcat¥webapps¥BOE¥WEB-INF¥config¥custom` に移動します。
2. CmcApp.properties ファイルを登録して、ファイル内に
   - sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter, trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela, trustedX509, sapSSO, siteminder
   - authentication.default=secWinAD

   と記述します。
3. Tomcat を再起動します。

   CMC の SSO が有効化されています。

   > ⓘ 注記
   >
   > BI ラウンチパッドまたは CMC のセッションタイムアウト後、両方のケースで SSO が有効になっている場合は、ユーザにログインが要求されます。 ページを最新表示すると、ユーザはパスワードを入力しなくても再度ログインされます。 処理中は警告を無効にできません。

9.1.3.2 データベースへのシングル サインオン

BI プラットフォームに一度ログオンすると、データベースへのシングルサインオンによって、ログオン情報を再度入力しなくてもデータベースアクセスに必要なアクション、特にレポートの表示や最新表示を行うことができます。データベースへのシングルサインオンを BI プラットフォームへのシングルサインオンと組み合わせて、必要なリソースへのアクセスをさらに容易にすることができます。

9.1.3.3 エンドツーエンドシングルサインオン

エンドツーエンドシングルサインオンとは、ユーザが、フロントエンドにある BI プラットフォームへのシングルサインオンアクセス権と、バックエンドにあるデータベースへのシングルサインオンアクセス権の両方を持っている設定のことです。したがって、ユーザはオペレーティングシステムへのログオン時にログオン情報を一度入

力するだけで、BI プラットフォームへのアクセス権を持つことができ、さらにデータベースアクセスに必要なレポートの表示などのアクションを実行することができます。

BI プラットフォームでは、エンドツーエンドシングルサインオンは、Windows AD と Kerberos を通じてサポートされます。

9.2 Enterprise 認証

9.2.1 Enterprise 認証の概要

Enterprise 認証は、BI プラットフォームのデフォルトの認証方法です。これは、システムの初回インストール時に自動的に有効化されます (無効化できません)。ユーザとグループを追加して管理する場合、そのユーザとグループの情報は BI プラットフォームのデータベース内に保持されます。

> → ヒント
>
> BI プラットフォーム専用のアカウントとグループを作成する場合、またはサードパーティのディレクトリサーバにユーザとグループの階層をまだ設定していない場合は、デフォルトの Enterprise 認証を使用します。
>
> Enterprise 認証を設定したり、有効にする必要はありません。ただし、組織固有のセキュリティ要件に合わせて、Enterprise 認証設定を変更することができます。Enterprise 認証設定は、セントラル管理コンソール (CMC) を使用する場合に変更できます。

9.2.2 Enterprise 認証の設定

設定	オプション	説明
パスワード制限	大文字と小文字を含むパスワードを要求する	このオプションによって、少なくとも 1 つの大文字と 1 つの小文字がパスワードに含まれるようになります。 ⓘ 注記 デフォルトでは、このオプションはオンになっています。管理者は、必要に応じて、このオプションをオフにできます。
	数値を含むパスワードを要求する	このオプションによって、少なくとも 1 つの数字がパスワードに含まれるようになります。
	特殊文字を含むパスワードを要求する	このオプションによって、少なくとも 1 つの特殊文字がパスワードに含まれるようになります。

設定	オプション	説明
	少なくとも *N* 文字を含む必要があります。*N* の値	このオプションによって、パスワードは少なくとも N 文字の長さになります。
	N 文字を超えることはできません。*N* の値:	このオプションにより、パスワードは N 文字を超えないようにします。
	以下の文字列の使用を禁止する	このオプションにより、パスワードに制限された一連の文字列が含まれないように強制できます。このデフォルト値は以下のとおりです。Password 12345678 administrator
ユーザ制限	*N* 日ごとにパスワードの変更を要求する	パスワードが障害にならないように、定期的な更新を強制できます。
	最近使用した *N* 個のパスワードの再使用を禁止する	パスワードが定期的に繰り返して使用されないように強制できます。
	N 分経過するまでパスワードの変更を禁止する	新しいパスワードをシステムに入力した直後に変更できないように強制できます。
	非アクティブ状態が *N* 日間を経過した場合にパスワードの変更を要求する	このオプションにより、非アクティブな日数が N 日間を経過した後にパスワードを変更するように強制できます。
	N 日経過後に初期パスワードの変更を要求する	このオプションにより、N 日間を経過した後に初期パスワードを変更するように強制できます。
ログオン制限	ログオンに *N* 回失敗した後はアカウントを無効にする	アカウントが無効にならずに、ユーザがシステムへのログオンを試行できる回数を指定できます。
	ログオン失敗回数を *N* 分後にリセットする	ログオン試行カウンタをリセットする時間間隔を指定できます。
	N 分後に再びアカウントを有効にする	N 回のログオン試行失敗後にアカウントを一時停止にさせる時間を指定できます。
データソース認証情報をログオン時に同期	ログオン時に、ユーザのログオン情報をデータソースログオン情報として有効化、更新する	ユーザがログオンした後にデータソース認証情報を有効にすることができます。
信用できる認証	信用できる認証を有効にする	信用できる認証設定用の設定を提供します。
OpenID 接続認証	*OpenID* 接続認証有効	*OpenID* 接続認証を有効にするには、[*OpenID* 接続認証有効] チェックボックスをオンにします。OpenID 接続による認証では、BI プラットフォームで内部 Enterprise セッションが作成されます。

9.2.3 Enterprise 設定を変更する

1. CMC の [認証] 管理エリアを表示します。

2. [*Enterprise*]をダブルクリックします。
   [*Enterprise*]ダイアログボックスが表示されます。
3. 設定を変更します。

> → ヒント
>
> すべての設定をデフォルトの値に戻すには、[リセット] をクリックします。

4. [更新] をクリックして、変更内容を保存します。

9.2.3.1 一般的なパスワード設定を変更する

> ⓘ 注記
>
> 延長期間に使用されないアカウントが自動的に無効になることはありません。管理者が無効なアカウントを手動で削除する必要があります。

1. CMC の [認証] 管理エリアを表示します。
2. [*Enterprise*]をダブルクリックします。
   [*Enterprise*] ダイアログボックスが表示されます。
3. 使用する各パスワード設定のチェックボックスをオンにして、必要であれば値を指定します。

   次の表は、設定可能なパスワード関連の各設定の最小値と最大値を示します。

パスワード設定	デフォルト	最小値	推奨される最大値
以下の文字列の使用を禁止する	password 12345678 administrator	1 文字	25550 文字
少なくとも *N* 文字以上のパスワードを要求する	8 文字	6 文字	255 文字
N 文字を超えることはできません	255 文字	13 文字	255 文字
N 日ごとにパスワードの変更を要求する	30 日	2 日	100 日
最近使用した *N* 個のパスワードの再使用を禁止する	3 個	1 個	100 個
N 分経過するまでパスワードの変更を禁止する	0 分	0 分	100 分
非アクティブ状態が *N* 日間を経過した場合にパスワードの変更を要求する	20 日	2 日	365 日

パスワード設定	デフォルト	最小値	推奨される最大値
N 日経過後に初期パスワードの変更を要求する	7 日	2 日	15 日
ログオンに *N* 回失敗した後はアカウントを無効にする	10 回	1 回	100 回
ログオン失敗回数を *N* 分後にリセットする	5 分	1 分後	100 分
N 分後に再びアカウントを有効にする	5 分	0 分	100 分

4. [更新] をクリックします。

9.2.4 SAML 2.0 認証

9.2.4.1 SAML 2.0 経由でシングルサインオンを達成する

Business Intelligence プラットフォームは、任意の SAML 対応ポータルまたはアプリケーションにシングルサインオンの認証メカニズムとして統合できるようになりました。つまり、Analytics Hub や SAP Analytics Cloud のようなクラウドアプリケーションにログインし、同じログオンセッションで Fiorified BI ラウンチパッドや OpenDocument などの BI アプリケーションのリソースにアクセスできるようになりました。

SAML 2.0 を経由するシングルサインオンを達成するようにアプリケーションサーバを設定する必要があります。

> **注記**
>
> SAML 認証機能を使用して電子メールアドレスでログインするには、以下の前提条件を設定します。
>
> - サードパーティユーザ。
> コマンドラインパラメータ “`-importtpemailduringsync`” を使用して、サードパーティシステムからの電子メールアドレスのインポートを有効にします。
> 1. パラメータ “`-importtpemailduringsync`” を *CMS* > プロパティ > コマンドラインパラメータ に追加します。
> 2. CMS を再起動します。
> 3. ユーザの電子メールをログインに使用するサードパーティのサードーパーティ認証更新を実行します。
> この機能でサポートされるサードパーティ認証の種類には、SAP、LDAP、WinAD があります。
> - Enterprise ユーザ。
> SAP ノート 2642247 を参照してください。

9.2.4.2 SAML サービスプロバイダとしての BI プラットフォームの設定

SAML サービスプロバイダとして BI プラットフォームを使用するには、SAML 2.0 認証用に BI プラットフォームを設定する必要があります。

このリリースでは、SAML サービスプロバイダとしてアプリケーションサーバを設定する手順が簡略化されています。この簡略化の一環として、以下の手順が省略されています。

- SAML JAR ファイルのコピーを BI プラットフォームのインストールディレクトリにコピーする
- securitycontext.xml ファイルを編集する
- web.xml ファイルを編集する

つまり、デフォルトで SAML JAR ファイル、securitycontext.xml ファイルの各 Web アプリケーションの XML タグ、および web.xml ファイルのフィルタが使用可能になっています。したがって、以下の手順の実行後、各 Web アプリケーションのプロパティファイルを使用して Web アプリケーションごとに SAML 2.0 認証を有効化または無効化することができます。

> **注記**
>
> デフォルトのアイデンティティプロバイダとして SAP Cloud Identity Provider を使用します。

> **注記**
>
> Tomcat、WebSphere、および Jboss アプリケーションサーバを SAML サービスプロバイダとして使用できるようになりました。

1. Web セッションでの信頼できる認証の設定 [235 ページ]の手順に従います。
2. SAP Cloud Platform Identity Provider を使用している場合、すべてのユーザをエクスポートしてから、BI プラットフォームにインポートします。セントラル管理コンソールから一括でユーザをインポートする方法を参照してください。

   SAP Cloud Platform ユーザを CSV にエクスポートするには、SAP Cloud Platform Identity 認証サービスのテナントの既存ユーザのエクスポートを参照してください。
3. properties ファイルを編集するために、`logon.webssoauthnetication.framework=None` を `logon.webssoauthnetication.framework=SAML` に変更します。
   - Fiorified BI ラウンチパッドの場合は、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` に移動して、`fioriBI.properties` ファイルを編集します。
   - Open Document の場合は、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` に移動して、`OpenDocument.properties` ファイルを編集します。
   - CMC の場合は、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` に移動して、`CMCApp.properties` ファイルを編集します。

     > **注記**
     >
     > `saml.enabled=true` を追加するのに加えて、`CMC¥FioriBI¥OpenDocument` プロパティファイル内でプロパティ `sso.supported.types = trustedSession` を設定します。

4. SP の IDP メタデータを更新するには、最初に該当する IDP サービスプロバイダから IDP メタデータをダウンロードし、次にメタデータファイルを `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF` にコピーして名前を `idp-meta-downloaded.xml` に変更します。

   IDP メタデータのダウンロード方法の詳細については、テナント SAML 2.0 設定を参照してください。

   > ⓘ 注記
   >
   > BI プラットフォームが非 Windows マシン上でデプロイされる場合、Bean **FilesystemMetadataProvider** での IDP メタデータのファイルパスにおけるパス区切り記号を `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥` にある `securityContext.xml` で変更する必要があります。
   >
   > たとえば、`<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value>` を `<value type="java.io.File">¥WEB-INF¥idp-meta-downloaded.xml</value>` に変更します。

   SAML 2.0 を有効化するためにキーストアを生成する場合は、SAML 2.0 のキーストアの生成 [236 ページ]を参照してください。
5. (オプション) SAML アサーション属性として電子メールアドレスを使用できます。詳細については、トピックSAML アサーション属性として電子メールアドレスを使用するには [238 ページ]を参照してください。
6. (オプション) ロードバランサまたはリバースプロキシサーバを使用している場合、詳細については、2621904 を参照してください。
7. WDeploy ツールを使用して WAR ファイルを作成します。
   a. パス `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥wdeploy` に移動します。
   b. 適切なデプロイコマンドを使用して、アプリケーション固有のバージョンの WAR ファイルを作成します。

   - Windows の場合: `wdeploy.bat <App_Server_Name><Version_Name> -DAPP=BOE predeploy`
   - UNIX の場合: `wdeploy.sh <App_Server_Name><Version_Name> -DAPP=BOE predeploy`

   > ⓘ 注記
   >
   > <App_Server><Version_Name> をアプリケーションサーバのタイプとそのバージョンに置き換える必要があります。たとえば、Tomcat アプリケーションサーバ v8.0 の場合は tomcat8 を使用できます。同様に、Jboss アプリケーションサーバ v7.0 の場合は jboss7 を、WebSphere アプリケーションサーバ v9.0 の場合は websphere9 を使用できます。
8. WAR ファイルを作成したら、WAR ファイルをコピーしてアプリケーションサーバにデプロイします。
9. サービスプロバイダメタデータを生成およびアップロードします。

   > ⓘ 注記
   >
   > securitycontext.xml ファイルでプロパティエンティティベース URL を定義して、エンドポイント URL でサービスプロバイダメタデータを生成することができます。デフォルトでは、サービスプロバイダメタデータのダウンロードには、URL で指定したホスト名とポート番号が考慮されます。

   a. `http(s)://host:port/BOE/saml/metadata` に移動します。

      XML ファイルは自動的にダウンロードされます。

b. XML ファイルをアイデンティティプロバイダにアップロードします。アイデンティティプロバイダとして Microsoft Active Directory Federation Services を使用している場合、詳細については、証明書利用者信頼の作成 [239 ページ]を参照してください。

> ⓘ 注記
>
> マニュアルで生成する代わりに、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥` にあるデフォルトサービスプロバイダのメタデータファイル `spring_saml_metadata.xml` を使用することができます。使用するネットワークに基づいて、XML タグ`<replace_withip>` はマシンの IP アドレスまたはホスト名に置き換え、`<replace_withport>` はアプリケーションサーバのポート番号に置き換える必要があります。アプリケーションサーバで HTTPS を有効化してある場合は、HTTP を HTTPS に置き換えます。

10. SAP Cloud Identity を使用している場合に、IDP で SAML アプリケーションを作成し、SAML SSO を設定するための IDP にある SP `metadata.xml` を BI プラットフォームにアップロードするには、信頼できるサービスプロバイダの設定を参照してください。

> ⓘ 注記
>
> キーストアファイルが修正された後に、最新のサービスプロバイダメタデータを生成する必要があります。

> → ヒント
>
> SAML 統合が正常に行われたかどうかをチェックするには、SAML 設定アプリケーション (BI ラウンチパッド、Fiorified BI ラウンチパッド、または OpenDocument) を起動すると、IDP にリダイレクトされます。

9.2.4.2.1 Web セッションでの信頼できる認証の設定

アプリケーションサーバを SAML サービスプロバイダとして設定する一部として、Web セッションで信頼できる認証を設定する必要があります。

> ⓘ 注記
>
> セキュリティ上の理由から、信用できる認証を HTTPS なしで有効化しないでください。信用できる認証を https なしで有効にすると、URL が認証されていないユーザに公開されるため、セキュリティ侵害とみなされます。セキュリティ侵害を防ぐために、有効な証明書を使用してユーザーの情報を検証できます。詳細については、1388240 を参照してください。

1. `global.properties` ファイルをカスタムフォルダ `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` の下に作成します。
2. `global.properties` ファイルの内容として以下を入力します。

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

> ⓘ 注記
>
> `trusted.auth.user.param` および `trusted.auth.shared.secret` パラメータの値が *custom.jsp* ファイルで更新された値と同じであることを確認する必要があります。

3. *CMC* > 認証 > *Enterprise* に移動します。
4. [有効期限] として 0 ～ 365 の値 ([日]) の観点で) を設定します。
5. [新規共有シークレット] を選択します。
6. 生成された共有シークレットをダウンロードするには、[共有シークレットのダウンロード] を選択します。

   `TrustedPrincipal.conf` ファイルがダウンロードされます。
7. `TrustedPrincipal.conf` ファイルをコピーして `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86` および `¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64` に貼り付けます。
8. *CMC* > 認証 > *Enterprise* に移動し、[更新] を選択します。
9. Custom.jsp ファイルを従来の BI ラウンチパッドおよび Fiorified BI ラウンチパッドの共有シークレットの値で更新します。詳細については、custom.jsp ファイルの編集 [388 ページ]を参照してください。

> ⓘ 注記
>
> アイデンティティプロバイダとして Microsoft ADFS と Microsoft Azure を使用している場合は、custom.jsp ファイルを更新する必要があります。

9.2.4.2.2 SAML 2.0 のキーストアの生成

SAML 2.0 に独自のキーストアファイルを使用するには、そのファイルを生成する必要があります。

SAML 交換では、データの署名と暗号化に暗号を使用します。サンプル自己署名キーストアファイル `sampletestKeystore.jks` が製品とともにパッケージ化されており、2019 年 10 月 18 日まで有効です。`sampletestKeystore.jks` には、エイリアス名 **Testkey** とパスワード **Password1** があります。

Java ユーティリティ keytool を使用して、自己署名キーストアファイルを生成できるようになりました。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥bin` に移動します。
2. 次のコマンドを実行します。`keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays`

コマンド	説明
-alias	証明書のエイリアス名を入力
-keypass	証明書のパスワードを入力
-keystore	キーストアファイルの名前
-validity	証明書の有効期限

コマンド	説明
numberofdays	自己署名証明書が有効な日数

コマンドを実行した後、次の質問が表示されます。

- キーストアパスワードを入力してください: *****
- 新しいパスワードを再入力してください: *****
- 姓と名は何ですか: **MY_FIRST_AND_LAST_NAME**
- 部門の名前は何ですか: **MY_ORGANIZATIONAL_UNIT**
- 組織の名前は何ですか: **MY_ORGANIZATION**
- 市区町村または地域の名前は何ですか: **MY_CITY**
- 都道府県の名前は何ですか: **MY_STATE**
- この部門の 2 桁の国コードは何ですか: **COUNTRY_CODE**

キーストアファイルが `INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥bin` で生成されます。

3. キーストアファイルを `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥` に移動します。
4. 新しいエイリアス名、パスワード、およびキーストアファイル名を用いて、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥` にある `securityContext.xml` ファイルを編集します。

   下記の XML コードを参照してください。

   サンプルコード

```
<bean id="keyManager"
class="org.springframework.security.saml.key.JKSKeyManager">
<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
<constructor-arg type="java.lang.String" value="Password1"/>
<constructor-arg>
<map>
<entry key="aliasname" value="password"/>
</map>
</constructor-arg>
<constructor-arg type="java.lang.String" value="Testkey"/>
</bean>
```

引数を理解するには、次の表を参照してください。

XML タグ	説明
`<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>`	キーストアファイルの場所を特定します。
`<constructor-arg type="java.lang.String" value="Password1"/>`	キーストアファイルのパスワード

XML タグ	説明
`<entry key="aliasname" value="password"/>`	エイリアスパスワード
`<constructor-arg type="java.lang.String" value="Testkey"/>`	デフォルト証明書のエイリアス

9.2.4.2.3 SAML アサーション属性として電子メールアドレスを使用するには

BI ラウンチパッド、Fiorified BI ラウンチパッド、OpenDocument、セントラル管理コンソール (CMC) に対して、SAML での電子メール認証を有効にすることができます。

1. 作業しているアプリケーションに応じて、以下の 2 つの行を追加して適切なプロパティを編集します。

```
saml.enabled=true
saml.isUseEmailAddress=true
saml.authType=secEnterprise
```

> ⓘ 注記
>
> `saml.isUseEmailAddress` は論理値を取り、`saml.authType` は、ログインでの使用が必須とされるユーザ/エイリアスの詳細の認証の種類に対応します。電子メール機能は、上記に示したアプリケーションごとに個別に処理できます。`saml.isUseEmailAddress` が `false` に設定されている場合、ログインは name パラメータに基づいて行われます。`true` に設定されている場合、ログインは email パラメータに基づいて行われます。`saml.authType` は潜在的な重複をチェックし、認証の種類が同じ 2 つのエイリアスが同じ電子メールアドレスを持つことができないようにします。

- Fiorified BI ラウンチパッドの場合: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にある `fioriBI.properties`
- Opendocument の場合: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にある `OpenDocument.properties`
- CMC の場合: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にある `CMCApp.properties`

> ⓘ 注記
>
> CMC については、`CMCApp.properties` ファイルで `sso.supported.types = trustedSession` プロパティを設定することを確認してください。

2. 電子メールサポート用に IDP を設定します。SAP Cloud Identity Provider を使用している場合は、詳細について SAP Cloud Platform Identity Authentication サービスガイドを参照することもできます。
   a. SAP Cloud Platform Identity Authentication サービスのテナントの管理コンソールにアクセスします。

> ⓘ 注記
>
> URL の形式は `https://<tenant ID>.accounts.ondemand.com/admin` です。テナント ID はシステムによって自動的に生成されます。テナントに対して最初に作成された管理者は、テナント ID を含む URL が記載された有効化電子メールを受信します。

b. [アプリケーション] を選択します。
c. アプリケーションを選択します。
d. [トラスト] タブの [*SAML 2.0*] セクションの下で、[名前 *ID* 属性] をクリックします。
e. [電子メール] を選択します。
f. [保存] をクリックします。

9.2.4.2.4 証明書利用者信頼の作成

サービスプロバイダのメタデータを更新するには、Microsoft ADFS 管理ツールで証明書利用者信頼と要求規則を作成する必要があります。

1. [サーバー マネージャー] を起動します。
2. ▶ ツール ▶ *AD FS* の管理 ▶ に移動します。
3. [信頼関係] を展開します。
4. [証明書利用者信頼] を右クリックして [証明書利用者信頼の追加] を選択します。
5. [証明書利用者信頼の追加] ウィザードで [開始] を選択します。
6. [証明書利用者についてのデータをファイルからインポートする] を選択し、[参照] を選択します。
7. ダウンロードしたサービスプロバイダのメタデータを参照して選択します。
8. [次へ] を選択します。
9. [表示名] を入力し、[次へ] を選択します。
10. [今すぐ多要素認証を構成しますか?] ステップで、[次へ] を選択します。
11. [すべてのユーザーに対してこの証明書利用者へのアクセスを許可する] を選択し、[次へ] を選択します。
12. [信頼の追加の準備完了] 画面で情報をレビューし、[次へ] を選択します。
13. [完了] を選択します。
    [要求規則の編集] ダイアログボックスが表示されます。属性としてユーザ名または電子メールアドレスを使用して要求規則を作成できます。

これで、証明書利用者信頼が正常に作成されました。

9.2.4.2.4.1 属性としてユーザ名を使用した要求規則の作成

SAML アサーション属性としてユーザ名を使用して要求規則を作成することができます。

証明書利用者信頼を利用可能にしておく必要があります。

1. [要求規則の編集] ダイアログボックスで、[規則の追加] を選択します。
2. [変換要求規則の追加] ウィザードで、[*LDAP* 属性を要求として送信] を選択し、[次へ]を選択します。
3. [要求規則名] を入力し、[属性ストア] として [*Active Directory*] を選択します。

4. [*LDAP* 属性] で、[*SAM* アカウント名] を選択します。
5. [出力方向の要求の種類] で、[名前 *ID*] を選択します。
6. [完了] を選択します。

属性としてユーザ名を使用した要求規則が作成されます。

9.2.4.2.4.2 属性として電子メールアドレスを使用した要求規則の作成

電子メールアドレスを SAML アサーション属性として使用するには、2 つの要求規則を作成する必要があります。

1. [要求規則の編集] ダイアログボックスで、[規則の追加] を選択します。
2. [変換要求規則の追加] ウィザードで、[*LDAP* 属性を要求として送信] を選択し、[次へ]を選択します。
3. [要求規則名] を入力し、[属性ストア] として [*Active Directory*] を選択します。
4. [*LDAP* 属性] で [電子メールアドレス] を選択し、次に [出力方向の要求の種類] で [電子メールアドレス] を選択します。
5. 2 番目のエントリでは、[*LDAP* 属性] で [名] を選択し、次に [出力方向の要求の種類] で [名] を選択します。
6. [完了] を選択します。

   これで、最初の規則が作成されます。以下の手順に従って 2 番目の要求規則を作成します。
7. [要求規則の編集] ダイアログボックスで、[規則の追加] を選択します。
8. [変換要求規則の追加] ウィザードで、[入力方向の要求の変換] を選択し、[次へ] を選択します。
9. [要求規則名] を入力し、[入力方向の要求の種類] として [電子メールアドレス] を、[出力方向の要求の種類] として [名前 *ID*] を、[出力方向の名前の形式] として [電子メール] を選択します。
10. [完了] を選択します。

9.2.4.3 WebSphere アプリケーションサーバを SAML サービスプロバイダとして使用する

このトピックには、WebSphere アプリケーションサーバを SAML 2.0 認証用に設定するための手順が含まれます。

> ⓘ 注記
>
> 下記の手順では SAP Cloud Identity Provider をデフォルトのアイデンティティプロバイダとして使用します。

以下の手順に従います。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥SAMLJARS` にある SAML JAR ファイルを `<WebSphere_InstallDir>¥WebSphere¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥WEB-INF¥lib` にコピーします。
2. Web セッションでの信頼できる認証を設定するには、下記の手順に従います。

1. global.properties ファイルをカスタムフォルダ `<WebSphere_InstallDir>¥WebSphere¥¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥WEB-INF¥config¥custom` に追加します。global.properties の内容は次のとおりです。
   ```
   sso.enabled=true
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.user.param=UserName
   ```
2. *CMC* > 認証 > *Enterprise* に移動します。
3. [信用できる認証] を有効にします。
4. [有効期限] を設定します。
5. [新規共有シークレット] を選択します。
6. 生成された共有シークレットをダウンロードするには、[共有シークレットのダウンロード] を選択します。
   `TrustedPrincipal.conf` ファイルがダウンロードされます。
7. TrustedPrincipal.conf ファイルを `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86` および `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64` に貼り付けます。
8. *CMC* > 認証 > *Enterprise* に移動し、[更新] を選択します。
9. WebSphere アプリケーションサーバを再起動します。

3. SAP Cloud Platform Identity Provider を使用している場合、すべてのユーザをエクスポートしてから、BI プラットフォームにインポートします。セントラル管理コンソールから一括でユーザをインポートする方法を参照してください。

   SAP Cloud Platform ユーザを CSV にエクスポートするには、SAP Cloud Platform Identity 認証サービスのテナントの既存ユーザのエクスポートを参照してください。

4. properties ファイルを編集するために、`saml.enabled=true` を追加します。下記のファイル名とその場所を参照してください。
   1. Fiorified BI ラウンチパッドの場合は、`<WebSphere_InstallDir>¥WebSphere¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥WEB-INF¥config¥custom` に移動して、*fioriBI.properties* ファイルを編集します。
   2. Open Document の場合は、`<WebSphere_InstallDir>¥WebSphere¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥WEB-INF¥config¥custom` に移動して、*OpenDocument.properties* ファイルを編集します。
   3. CMC の場合は、`<WebSphere_InstallDir>¥WebSphere¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥WEB-INF¥config¥custom` に移動して、*CMCApp.properties* ファイルを編集します。

   > **注記**
   >
   > CMC については、*CMCApp.properties* ファイルで別のプロパティ `sso.supported.types = trustedSession` を設定する必要があります。

   > **注記**
   >
   > アプリケーションにカスタムプロパティファイルが含まれない場合は、新しく作成します。

5. SP の IDP メタデータを更新するために、該当する IDP サービスプロバイダから IDP メタデータをダウンロードします。メタデータファイルを

<WebSphere_InstallDir>¥WebSphere¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥WEB-INF にコピーし、**idp-meta-downloaded.xml** に変更します。IDP メタデータのダウンロードの詳細については、テナント SAML 2.0 設定を参照してください。

> ⓘ 注記
>
> 新しいアルゴリズム SHA-256 が SAML 統合でサポートされるようになりました。

6. WebSphere アプリケーションサーバを再起動します。

> ⓘ 注記
>
> BOE が非 Windows マシン上でデプロイされる場合、Bean **FilesystemMetadataProvider** での IDP メタデータのファイルパスにおけるパス区切り記号は、<WebSphere_InstallDir>¥WebSphere¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥WEB-INF にある securityContext.xml で変更してください。
>
> つまり、<value type="java.io.File">/WEB-INF/idp-meta-downloaded.xml</value> を <value type="java.io.File">¥WEB-INF¥idp-meta-downloaded.xml</value> に変更する必要があります。

SAML 2.0 を有効化するためにキーストアを生成する (オプション)

この手順を適用できるのは、独自のキーストアファイルを使用する場合のみです。

SAML 交換には、データの署名と暗号化のための暗号の使用が伴います。サンプル自己署名キーストア sampletestKeystore.jks が製品とともにパッケージ化されており、2019 年 10 月 18 日まで有効です。sampletestKeystore.jks にはエイリアス名 Testkey およびパスワード Password1 があります。Java ユーティリティ keytool を使用して、自己署名キーストアファイルを生成できるようになりました。下記の手順に従い、キーストアファイルを生成します。

1. <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥bin に移動します。
2. 次のコマンドを実行します。keytool -genkeypair -alias aliasname -keypass password -keystore samplekeystore.jks -validity numberofdays

コマンド	説明
-alias	証明書のエイリアス名を入力
-keypass	証明書のパスワードを入力
-keystore	キーストアファイルの名前
-validity	証明書の有効期限
numberofdays	自己署名証明書が有効な日数

コマンドを実行した後、次の質問が表示されます。

- キーストアパスワードを入力してください: *****
- 新しいパスワードを再入力してください: *****

- 姓と名は何ですか: <姓と名>
- 部門の名前は何ですか: <部門名>
- 組織の名前は何ですか: <会社名>
- 市区町村および地域の名前は何ですか: <市区町村名>
- 都道府県の名前は何ですか: <都道府県名>
- この部門の 2 桁の国コードは何ですか: <国名または ISO コード>

3. WebSphere アプリケーションサーバを停止します。
   キーストアファイルが `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥bin` で生成されます。
4. キーストアファイルを `<WebSphere_InstallDir>¥WebSphere¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥WEB-INF` に移動します。
5. 新しいエイリアス名、パスワード、およびキーストアファイル名を使用して、`<WebSphere_InstallDir>¥WebSphere¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥WEB-INF` にある `securityContext.xml` ファイルを編集します。下記の XML コードを参照してください。

   サンプルコード

   ```
   <bean id="keyManager"
   class="org.springframework.security.saml.key.JKSKeyManager">
   <constructor-arg value="/WEB-INF/sampleKeystore.jks"/>
   <constructor-arg type="java.lang.String" value="Password1"/>
   <constructor-arg>
   <map>
   <entry key="aliasname" value="password"/>
   </map>
   </constructor-arg>
   <constructor-arg type="java.lang.String" value="Testkey"/>
   </bean>
   ```

   引数を理解するには、次の表を参照してください。

XML タグ	説明
`<constructor-arg value="/WEB-INF/sampleKeystore.jks"/>`	キーストアファイルの場所を特定します。
`<constructor-arg type="java.lang.String" value="Password1"/>`	キーストアファイルのパスワード
`<entry key="aliasname" value="password"/>`	エイリアスパスワード
`<constructor-arg type="java.lang.String" value="Testkey"/>`	デフォルト証明書のエイリアス

7. サービスプロバイダメタデータを生成およびアップロードします。

1. http(s)://host:port/BOE/saml/metadata に移動します。上記 URL に移動した後、XML ファイルが自動的にダウンロードされます。
2. XML ファイルをアイデンティティプロバイダにアップロードします。

> ⓘ 注記
>
> 手動で生成する代わりに、`<WebSphere_InstallDir>¥WebSphere¥AppServer¥profiles¥<Profile_Name>¥installedApps¥<Node_Name>¥BOE.ear¥BOE.war¥biprws¥WEB-INF` にあるデフォルトサービスプロバイダのメタデータファイル `spring_saml_metadata.xml` を使用できます。使用するネットワークに基づいて、XML タグ `<replace_withip>` はマシンの IP アドレスまたはホスト名に置き換え、`<replace_withport>` は WebSphere アプリケーションサーバのポート番号に置き換える必要があります。WebSphere で HTTPS を有効化してある場合は、HTTP を HTTPS に置換します。

8. SAP Cloud Identity を使用している場合に、IDP で SAML アプリケーションを作成し、SAML SSO を設定するための IDP にある SP `metadata.xml` を BI プラットフォームにアップロードするには、信頼できるサービスプロバイダの設定を参照してください。
9. WebSphere アプリケーションサーバを再起動します。

> ⓘ 注記
>
> キーストアファイルが修正された後には、最新のサービスプロバイダメタデータを生成する必要があります。

> → ヒント
>
> SAML 統合が正常に行われたかどうかをチェックするには、SAML 設定アプリケーション (BI ラウンチパッド、Fiori 対応 BI ラウンチパッドまたは OpenDocument) を起動すると、IDP にリダイレクトされます。

9.2.5 SAP NetWeaver Java Application Server と BI プラットフォーム間に信用できる認証を確立する

- SAP NetWeaver Java Application Server はサービスプロバイダとして SAML 2.0 認証用に設定します。
- ユーザは SAP NetWeaver Java Application Server に存在する必要があります。
- サービスプロバイダとアイデンティティプロバイダの SAML 2.0 証明書が交換されて、両者の間にトラストを設定しておきます。
  同じユーザを BI プラットフォームのエンタープライズユーザとしてインポートする必要があります。

SAP NetWeaver Java Application Server と BI プラットフォームの間に信用できる認証を確立するには、下記の手順に従います。

> ⓘ 注記
>
> - `USER_PRINCIPAL` メソッドを使用して、Web アプリケーション用の信用できる認証を有効化中にユーザを取得してください。
> - セキュリティ上の理由から、信用できる認証を HTTPS なしで有効化しないでください。信用できる認証を https なしで有効にすると、URL が認証されていないユーザに公開されるため、セキュリティ侵害とみなされます。セキュリティ侵害を防ぐために、有効な証明書を使用してユーザーの情報を検証できます。詳細については、1388240 を参照してください。

1. WDeploy を使用して BI Web アプリケーションを生成します。
   a. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥wdeploy` に移動します。
   b. `BOE.sca` ファイルを生成するためのコマンド `wdeploy.bat sapappsvr73 -DAPP=BOE predeploy` を実行します。

      `BOE.sca` が `<INSTALLDIR>¥ SAP BusinessObjects Enterprise XI 4.0¥wdeploy¥workdir¥sapappsvr73¥application` で生成されます。
2. `web.xml` ファイルを編集して、信用できる認証を有効化します。
   a. winrar または winzip などのツールを使用して、`BOE.sca` ファイルを `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥wdeploy¥workdir¥sapappsvr73¥application` で抽出します。
   b. 変更を行う前に、`BOE.sca` ファイルのコピーを作成します。`BOE.sca` で、*DEPLOYARCHIVES* > *BOE.ear* > *BOE.war* > *WEB-INF* に移動します。
   c. `web.xml` ファイルを編集するために、下記の XML タグを `</web-app>` の前に追加します。

> **注記**
>
> ロール (下記 XML コードで記載) を SAP NetWeaver Java Application Server で追加して、ユーザグループまたはユーザに割り当てる必要があります。
>
> - j2ee-admin
> - j2ee-guest
> - j2ee-special

サンプルコード

```
<security-constraint>
<web-resource-collection>
 <web-resource-name>InfoView</web-resource-name>
<url-pattern>*</url-pattern>
<http-method>DELETE</http-method>
<http-method>GET</http-method>
<http-method>POST</http-method>
<http-method>PUT</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>j2ee-admin</role-name>
<role-name>j2ee-guest</role-name>
<role-name>j2ee-special</role-name>
</auth-constraint>
<user-data-constraint>
<transport-guarantee>NONE</transport-guarantee>
</user-data-constraint>
</security-constraint>
<login-config>
<auth-method>BASIC</auth-method>
<realm-name>InfoView</realm-name>
</login-config>
<security-role>
<description>Assigned to the SAP J2EE Engine System Administrators</
description>
<role-name>j2ee-admin</role-name>
</security-role>
<security-role>
<description>Assigned to all users</description>
<role-name>j2ee-guest</role-name>
</security-role>
<security-role>
<description>Assigned to a special group of users</description>
```

```
<role-name>j2ee-special</role-name>
</security-role>
```

d. 下記の XML タグがある XML ファイル `web-j2ee-engine.xml` を作成し、ファイルを `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥wdeploy¥workdir¥sapappsvr73¥application¥BOE.sca¥DEPLOYARCHIVES¥BOE.ear¥BOE.war¥WEB-INF` に保存します。

サンプルコード

```
<?xml version="1.0" encoding="UTF-8"?>
<web-j2ee-engine xsi:noNamespaceSchemaLocation="web-j2ee-engine.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<security-role-map>
    <role-name>j2ee-admin</role-name>
    <server-role-name>administrators</server-role-name>
</security-role-map>
<security-role-map>
      <role-name>j2ee-guest</role-name>
      <server-role-name>guests</server-role-name>
</security-role-map>
<security-role-map>
      <role-name>j2ee-special</role-name>
      <server-role-name>all</server-role-name>
</security-role-map>
 <login-module-configuration>
      <security-policy-domain>/irj</security-policy-domain>
 </login-module-configuration>
</web-j2ee-engine>
```

e. `web-j2ee-engine.xml` ファイルを保存します。

f. ファイルを `BOE.war` アーカイブの `WEB-INF` フォルダにドラッグします。

BIP における SSO の有効化 - USER PRINCIPAL、共有シークレット – `Trustedprincipal.conf`

SSO を有効化するために、USER PRINCIPAL メソッドを使用して、NW ユーザ名と `Trustedprincipal.conf` ファイルを渡し、共有シークレットを渡します。

信用できる認証を有効化し、共有シークレットを生成するには、下記の手順に従います。

1. *CMC* > 認証 > *Enterprise* に移動します。
2. [信用できる認証] を有効にします。
3. [新規共有シークレットの作成] を選択します。
4. [共有シークレットのダウンロード] を選択して、BOE マシンに保存します。
5. [更新] を選択します。
6. `BOE.war/web-inf/config/default/folder` で、次のファイルを `BOE.war/web-inf/config/custom/folder` に抽出します。
   - `global.properties`
7. 次を `global.properties` に追加します。
   - `sso.enabled=true`
   - `trusted.auth.user.retrieval=USER_PRINCIPAL`
   - `trusted.auth.user.namespace.enabled=true`
   - `trusted.auth.shared.secret=MySecret`

> **注記**
>
> trusted.auth.user.namespace.enabled=true を有効化しました

初めての場合は、次のエラーメッセージを受信する必要があります。ログオン拒否: ユーザ "secExternal:samltest" が見つかりません (FWB 00007)。`secExternal: samltest` をエイリアスとして BOE ユーザにマップする自動バインド機能があります。InfoView のログインフォームから通常どおりにログインします。使用する BOE 認証情報には、このために作成された `secExternal: samltest` エイリアスがあります。たとえば、samltest ユーザアカウントをそのユーザプロパティで使用する場合、`secExternal: samltest` がエイリアスとして割り当てられているのを確認できます。

8. `<INSTALLDIR>¥ SAP BusinessObjects Enterprise XI 4.0¥wdeploy¥workdir¥sapappsvr73¥application¥ BOE.sca¥DEPLOYARCHIVES¥BOE.ear¥BOE.war¥ WEB-INF¥ Eclipse¥plugins¥webpath.InfoView¥web¥custom.jsp` に移動します。
9. 下記の XML タグを `custom.jsp` ファイルに追加します。
   コードブロック:

   > **サンプルコード**
   >
   > ```
   > <%@ page language="java" contentType="text/html;charset=utf-8"%>
   > <%@ page
   > import="com.businessobjects.bip.core.web.appcontext.RequestInfo"%>
   > <%
   > request.getSession().setAttribute("MySecret","Your generated shared
   > secret content");
   > %>
   > <html>
   > <head>
   > <title></title>
   > </head>
   > <body>
   > <script type="text/javascript" src="noCacheCustomResources/
   > custom.js"></script>
   > <script type="text/javascript">
   > window.location = "logon.faces";
   > </script>
   > </body>
   > </html>
   > ```

10. ファイルを保存します。

3. アーカイブファイルを更新して閉じます。
4. 上記の手順を `BOE.sca` ファイルで実行した後、NetWeaver 上でデプロイします。
5. BOE.sca を正常にデプロイしたら、起動して検証します (http://<hostname>:<port_number>/nwa)。
6. BASIC 認証が `web.xml` で宣言されているので、認証用のブラウザポップアップが表示されます。

SAP NetWeaver Java Application Server と BI プラットフォームの間で信頼できる認証を確立しました。

> **注記**
>
> 認証用のブラウザポップアップを確認したら、下記の手順に従います。
>
> 1. http://<hostname>:<port_number>/nwa で SAP NetWeaver Java Application Server にログオンします。
> 2. 設定 > セキュリティ > 認証 > シングルサインオン に移動します。

3. BI アプリケーションのポリシーコンフィグレーションを特定します。
4. [編集] モードに切り替えます。
5. [ログインモジュールスタック] タブで、[使用テンプレート] 項目を空白のままにして、「*SAML2LoginModule*」をフラグ [*SUFFICIENT*] とともにスタックの最上部に追加します。
6. 変更を保存して閉じます。

9.2.6 SAP NetWeaver Java アプリケーションサーバとともに SAML 2.0 認証を使用する

SAP NetWeaver Application Server Java ユーザが SAP Business Intelligence プラットフォームコンテンツにシングルサインオン (SSO) 経由でアクセスできるようにするには、これらのアプリケーションへのアクセスを認可するメカニズムを確立する必要があります。次の手順では、NetWeaver Application Server Java と Business Intelligence の間で信頼できる認証を確立する方法を説明します。

範囲 – IDP はベンダごとに変化することがあるので、これらの手順の範囲は SAML 認証を設定するためではありません。SAML 認証を設定するには、ベンダ固有ドキュメントを参照してください。

設定は次のように分割されます。

1. SAP NetWeaver Java アプリケーションサーバで SAML 認証を設定します。
2. BI プラットフォームの信頼できる認証を設定します。

SAP NetWeaver Java アプリケーションサーバでの SAML 認証の有効化に関する詳細については、SAML 2.0 の使用を参照してください。

9.2.7 信用できる認証の有効化

シングルサインオンを実行するには、Enterprise の信用できる認証を使用して、Web アプリケーションサーバによってユーザの ID を確認します。この認証方法では、Central Management Server (CMS) と BI プラットフォーム Web アプリケーションをホストする Web アプリケーションサーバ間に信用を確立する必要があります。信用が確立されると、システムは、ユーザの ID の確認を Web アプリケーションサーバに委任します。信用できる認証は、SAML、x.509、および専用の認証プラグインを持たないその他の認証方法をサポートするために使用できます。

一度システムにログオンしたら、そのセッションの間に何回もパスワードを入力する必要がない方が好まれます。信用できる認証では、BI プラットフォーム認証ソリューションをサードパーティの認証ソリューションと統合するための Java シングルサインオンを提供します。Central Management Server (CMS) と信用を確立したアプリケーションでは、信用できる認証を使用してユーザがパスワードを指定せずにログオンできます。

信用できる認証を有効にするには、Enterprise 認証設定でサーバ上の共有シークレットを設定し、同時に、BOE war ファイルのプロパティ指定でクライアントを設定する必要があります。

ⓘ 注記

- 信用できる認証を使用できるようにする前に、BI プラットフォームにサインオンする必要のある、Enterprise ユーザを作成するか、サードパーティユーザをマップしておく必要があります。
- セキュリティ上の理由から、信用できる認証を HTTPS なしで有効化しないでください。信用できる認証を https なしで有効にすると、URL が認証されていないユーザに公開されるため、セキュリティ侵害とみ

なされます。セキュリティ侵害を防ぐために、有効な証明書を使用してユーザの情報を検証できます。詳細については、1388240 を参照してください。

関連情報

信用できる認証を使用するサーバを設定する [250 ページ]
Web アプリケーションに対して信用できる認証を設定する [254 ページ]

9.2.7.1 Web サーバでの RESTful Web サービスの信頼できる認証

このトピックでは、Web サーバ上の RESTful Web サービスに対して信頼できる認証を有効化する手順について説明します。

> **注記**
>
> セキュリティ上の理由から、信用できる認証を HTTPS なしで有効化しないでください。信用できる認証を https なしで有効にすると、URL が認証されていないユーザに公開されるため、セキュリティ侵害とみなされます。セキュリティ侵害を防ぐために、有効な証明書を使用してユーザの情報を検証できます。詳細については、1388240 を参照してください。

以下の手順に従って信用できる認証を有効化します。

1. 共有秘密鍵を生成します。詳細については、共有シークレットの値の生成 [392 ページ] を参照してください。
2. その共有秘密鍵を、Windows では `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥container¥bin` に保存します。
3. テキストエディタで共有秘密鍵を開きます。
4. 共有秘密鍵をコピーします。
5. 5. ファイル biprws.properties を `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps` からコピーして、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps ¥biprws¥WEB-INF¥config¥custom` にペーストします。
6. ファイル *biprws.properties* をテキストエディタで開きます。
7. 値 *Trusted_Auth_Shared_Secret=* に対して共有秘密鍵をペーストします。
8. [取得方法] および [ユーザ名パラメータ] パラメータを追加します。下記の表を参照して、取得方法とユーザ名パラメータを追加します。

RESTful Web サービス - 信頼できる認証設定プロパティ

プロパティ	説明	デフォルト値
取得方法	これは、RESTful Web サービス API `/logon/trusted` を使用する場合に、信頼できる認証ログオントークンを取得するために使用するクエリメソッドを設定するメニューです。 • [*HTTP_HEADER*] は、要求ヘッダ accept=application/xml (または application/json) を使用する GET クエリで使用されます。 • [*QUERY_STRING*] は、RESTful Web サービス API を使用する URL クエリの末尾にログオン名を追加するのに使用します (例: /logon/trusted/?user=johndoe)。 • [*COOKIE*] は、Web ブラウザの Cookie からログイン名を取得する場合に使用します。ドメイン、名前、値、およびパスは Cookie に保存されている必要があります。	**HTTP_HEADER**
ユーザ名パラメータ	これは、ログオントークンを取得する目的で信頼できるユーザを識別するために使用するラベルです。	**X-SAP-TRUSTED-USER**

9. ファイル *biprws.properties* を保存します。
10. Web サーバを再起動してください。

9.2.7.2 信用できる認証を使用するサーバを設定する

信用できる認証を設定する前に、BI プラットフォームにサインオンする必要のある、Enterprise ユーザを作成するか、サードパーティユーザをマップしておく必要があります。

> **注記**
>
> セキュリティ上の理由から、信用できる認証を HTTPS なしで有効化しないでください。信用できる認証を https なしで有効にすると、URL が認証されていないユーザに公開されるため、セキュリティ侵害とみなされます。セキュリティ侵害を防ぐために、有効な証明書を使用してユーザの情報を検証できます。詳細については、1388240 を参照してください。

1. CMC にログオンします。
2. [認証] 管理エリアを表示します。
3. [*Enterprise*] オプションをクリックします。
   [*Enterprise*] ダイアログボックスが表示されます。
4. [信用できる認証] で、次のようにします。
   a. *[信用できる認証を有効にする]*をクリックします。
   b. [新規共有シークレット] をクリックします。
      "共有シークレットキーが生成され、ダウンロードが可能です。" というメッセージが表示されます。
   c. [共有シークレットのダウンロード] をクリックします。

      共有シークレットは、クライアントおよび CMS が信用を確立するために使用されます。最初に信用できる認証用のサーバを設定してから、クライアントを設定する必要があります。

      [ファイルのダウンロード] ダイアログボックスが表示されます
   d. [保存] をクリックして、次のいずれかのディレクトリに `TrustedPrincipal.conf` ファイルを保存します。

> ⚠ 警告
>
> タイムアウトを「**0** (ゼロ)」に設定しないでください。「**0**」値を設定すると、2 つのクロック時間で許容できる時間差が無制限であるという意味になり、これはリプレイアタックに対する脆弱性を高める可能性があります。

e. [共有シークレット有効期間] フィールドに、共有シークレットが有効となる日数を入力します。
f. 信用できる認証の要求でのクライアントと CMS のクロックの許容できる最大時間差 (ミリ秒) を指定します。
g. Web セッションではなく TrustedPrincipal.conf ファイルを介してシークレットを共有する場合は、このファイルを次のいずれかのディレクトリにコピーします。
   - `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥`
   - `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86¥`

5. [更新] をクリックして、共有シークレットをコミットします。

BI プラットフォームでは、信用できる認証の各パラメータに対するすべての変更の監査は行われません。信用できる認証の情報は手動でバックアップする必要があります。

共有シークレットは、クライアントおよび CMS が信用を確立するために使用されます。次の手順では、信用できる認証のクライアントを設定します。

9.2.8 Web アプリケーションに対する信用できる認証の設定

クライアントに対する信用できる認証を設定するには、`BOE.war` ファイルのグローバルプロパティと、BI ラウンチパッドおよび OpenDocument アプリケーションの特定のプロパティを変更する必要があります。

次のいずれかの方法を使用して、共有シークレットをクライアントに渡します。

- `WEB_SESSION` オプション
- `TrustedPrincipal.conf` ファイル

次のいずれかの方法を使用して、ユーザ名をクライアントに渡します。

- `REMOTE_USER`
- `HTTP_HEADER`
- `COOKIE`
- `QUERY_STRING`
- `WEB_SESSION`
- `USER_PRINCIPAL`

いずれの方法で共有シークレットを渡す場合でも、`BOE.war` ファイルの `Trusted.auth.user.retrieval` グローバルプロパティで、使用する方法をカスタマイズする必要があります。

> ⓘ 注記
>
> セキュリティ上の理由から、信用できる認証を HTTPS なしで有効化しないでください。信用できる認証を https なしで有効にすると、URL が認証されていないユーザに公開されるため、セキュリティ侵害とみなされます。セキュリティ侵害を防ぐために、有効な証明書を使用してユーザの情報を検証できます。詳細については、1388240 を参照してください。

9.2.8.1 SAML シングルサインオンに対する信用できる認証の使用

Security Assertion Markup Language (SAML) は、ID 情報を交換する XML ベースの標準です。SAML は ID と信用を交換する安全な接続を提供するため、BI プラットフォームにアクセスする信用できるユーザには、追加ログインが不要なシングルサインオンメカニズムが可能になります。

SAML 認証の有効化

アプリケーションサーバが SAML サービスプロバイダとして機能できる場合は、信用できる認証を使用して BI プラットフォームに SAML SSO を提供できます。

そのためには、まず SAML 認証に対する Web アプリケーションサーバを設定する必要があります。

また、ユーザ名をクライアントに渡すには、次のいずれかの方法を使用する必要があります。

- `REMOTE_USER`
- `USER_PRINCIPAL`

次の例には、SAML 認証用に設定されたサンプル web.xml が含まれています。

```
<security-constraint>
      <web-resource-collection>
        <web-resource-name>InfoView</web-resource-name>
        <url-pattern>*</url-pattern>
      </web-resource-collection>
      <auth-constraint>
        <role-name>j2ee-admin</role-name>
        <role-name>j2ee-guest</role-name>
        <role-name>j2ee-special</role-name>
      </auth-constraint>
      <user-data-constraint>
        <transport-guarantee>NONE</transport-guarantee>
      </user-data-constraint>
    </security-constraint>
    <login-config>
      <auth-method>FORM</auth-method>
      <realm-name>InfoView</realm-name>
      <form-login-config>
        <form-login-page>/logon.jsp</form-login-page>
        <form-error-page>/logon.jsp</form-error-page>
      </form-login-config>
    </login-config>
    <security-role>
      <description>Assigned to the SAP J2EE Engine System Administrators</
description>
      <role-name>j2ee-admin</role-name>
    </security-role>
    <security-role>
      <description>Assigned to all users</description>
      <role-name>j2ee-guest</role-name>
    </security-role>
    <security-role>
      <description>Assigned to a special group of users</description>
      <role-name>j2ee-special</role-name>
    </security-role>
```

設定方法の詳細については、アプリケーションサーバによって異なるため、各アプリケーションサーバのマニュアルを参照してください。

信用できる認証の使用

Web アプリケーションサーバを SAML サービスプロバイダとして機能できるように設定すると、信用できる認証を使用して SAML SSO を提供できます。

動的エイリアスを使用して SSO を有効にします。ユーザが初めて SAML でログオンページにアクセスすると、既存の BI プラットフォームアカウント認証情報を使用して手動でログオンするよう要求されます。ユーザの認証情報が確認されると、ユーザの SAML ID のエイリアスが BI プラットフォームアカウントに使用されます。システムには既存のアカウントに動的に一致するユーザの ID エイリアスが付与されるため、ユーザの後続ログオン試行は SSO を使用して実行されます。

> ⓘ 注記
>
> ユーザを BI プラットフォームにインポート、またはユーザに Enterprise アカウントを付与する必要があります。

> ⓘ 注記
>
> このメカニズムを機能させるには、BOE war ファイルの特定のプロパティ - `trusted.auth.user.namespace.enabled` - を有効にする必要があります。

9.2.8.2 Web アプリケーションの信用できる認証プロパティ

以下の表は、`BOE.war` ファイルのデフォルト `global.properties` 内の信用できる認証設定を一覧表示したものです。これらの設定を上書きするには、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` に新しいファイルを作成します。

> ⓘ 注記
>
> セキュリティ上の理由から、信用できる認証を HTTPS なしで有効化しないでください。信用できる認証を https なしで有効にすると、URL が認証されていないユーザに公開されるため、セキュリティ侵害とみなされます。セキュリティ侵害を防ぐために、有効な証明書を使用してユーザの情報を検証できます。詳細については、1388240 を参照してください。

プロパティ	デフォルト値	説明
`sso.enabled=true`	`sso.enabled=false`	BI プラットフォームへのシングルサインオン (SSO) を有効化または無効化します。信頼済み認証を有効にするには `true` に設定します。
`trusted.auth.shared.secret`	なし	信用できる認証のシークレットの取得に使用するセッション変数名。共有シ

プロパティ	デフォルト値	説明
		ークレットを渡すために Web セッションを使用する場合のみ適用されます。
trusted.auth.user.param	なし	信用できる認証のユーザ名の取得に使用する変数を指定します。
trusted.auth.user.retrieval	なし	信用できる認証のユーザ名の取得に使用する方法を指定します。 • REMOTE_USER • HTTP_HEADER • COOKIE • QUERY_STRING • WEB_SESSION • USER_PRINCIPAL 信用できる認証を無効化するには、空白を設定します。
trusted.auth.user.namespace.enabled	なし	既存のユーザアカウントへのエイリアスの動的バインディングを有効化および無効化します。true に設定されている場合は、信用できる認証ではユーザを BI プラットフォームに認証するためにエイリアスバインディングを使用します。エイリアスバインディングを使用すると、アプリケーションサーバは SAML サービスプロバイダとして機能できるため、信用できる認証でシステムへの SAML シングルサインオンを実行できます。 このプロパティが空白の場合は、信用できる認証はユーザ認証時に一致する名前を使用します。

9.2.8.3 Web アプリケーションに対して信用できる認証を設定する

TrustedPrincipal.conf ファイルに共有シークレットを格納する場合は、ファイルが適切なプラットフォームディレクトリに格納されていることを確認してください。

プラットフォーム	TrustedPrincipal.conf の場所
Windows、デフォルトインストール	• <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86¥ • <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥
AIX	<INSTALLDIR>/sap_bobj/enterprise_xi40/ aix_rs6000/
Solaris	<INSTALLDIR>/sap_bobj/enterprise_xi40/ solaris_sparc/
Linux	<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x86

さまざまなメカニズムによって、Web アプリケーションをホストするクライアントに信用できる認証を設定する際に使用するユーザ名変数を入力できます。ユーザ名の取得方法を使用する前に、Web アプリケーションサーバを設定またはセットアップして、ユーザ名が公開されるようにします。詳細については、http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html を参照してください。

クライアントに対する信用できる認証を設定するには、BOE.war ファイルのプロパティにアクセスしてプロパティを変更する必要があります。このプロパティには、BI ラウンチパッドおよび OpenDocument Web アプリケーションの一般プロパティおよび特定プロパティが含まれます。

> **注記**
>
> ユーザ名または共有シークレットの取得方法に応じて、追加手順が必要な場合があります。

1. Web アプリケーションをホストするコンピュータ上の BOE.war ファイルのカスタムフォルダにアクセスします。

   <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥.

   後で、変更した BOE.war ファイルを再デプロイする必要があります。
2. メモ帳などのテキスト編集ユーティリティを使用して新しいファイルを作成します。
3. 信用できる認証に関する次のプロパティを入力します。

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=<Method for user ID retrieval>
   trusted.auth.user.param=<User Variable>
   trusted.auth.shared.secret=<Secret Variable>
   ```

   trusted.auth.user.retrieval プロパティには、ユーザ名の取得用の次のオプションのいずれかを選択します。

オプション	ユーザ名の取得方法
HTTP_HEADER	ユーザ名は、HTTP ヘッダのコンテンツから取得されます。使用する HTTP ヘッダを、trusted.auth.user.param プロパティに指定します。

オプション	ユーザ名の取得方法
QUERY_STRING	ユーザ名はリクエスト URL のパラメータから取得されます。使用するクエリ文字列を、trusted.auth.user.param プロパティに指定します。
COOKIE	ユーザ名は指定された Cookie から取得されます。使用する Cookie を、trusted.auth.user.param プロパティに指定します。
WEB_SESSION	ユーザ名は、指定されたセッション変数のコンテンツから取得されます。使用する Web セッション変数を、global.properties の trusted.auth.user.param プロパティに指定します。
REMOTE_USER	ユーザ名は HttpServletRequest.getRemoteUser() を呼び出して取得されます。
USER_PRINCIPAL	ユーザは、サーブレットまたは JSP 内の現在のリクエストに対する HttpServletRequest オブジェクトで getUserPrincipal().getName() を呼び出して取得されます。

→ 推奨事項

HTTP_HEADER ベースの SSO または QUERY_STRING ベースの SSO を使用している場合、エンドユーザ (ブラウザ) は認証のために直接 BOE にアクセスすることはありません。代わりに、エンドユーザ (ブラウザ) は、ポータルまたはカスタムアプリケーションでのみ BOE にアクセスします。

ⓘ 注記

一部の Web アプリケーションサーバでは、サーバ上で環境変数 REMOTE_USER を true に設定する必要があります。この設定が必要かどうかについては、Web アプリケーションサーバのマニュアルを参照してください。必要な場合には、この環境変数が true に設定されていることを確認してください。

ⓘ 注記

USER_PRINCIPAL または REMOTE_USER を使用してユーザ名を渡す場合、trusted.auth.user.param は空白のままにしておいてください。

4. global.properties という名前でファイルを保存します。
5. Web アプリケーションサーバを再起動します。

これらの新しいプロパティが有効になるのは、変更された BOE Web アプリケーションが Web アプリケーションサーバを実行しているコンピュータ上に再デプロイされてからです。WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。WDeploy の使用の詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

9.2.8.3.1 サンプル設定

9.2.8.3.1.1 TrustedPrincipal.conf ファイル経由で共有シークレットを渡す

ユーザ情報は、Web セッションを介して保存され渡されます。共有シークレットは、`TrustedPrincipal.conf` ファイルを介して渡されます。このファイルはデフォルトで、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64` ディレクトリに保存されています。Tomcat のバンドルバージョンは Web アプリケーションサーバです。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥` ディレクトリで、メモ帳などのテキスト編集ユーティリティを使用して新しいファイルを作成します。
2. 信用できる認証のプロパティを指定するには、次の値を入力します。

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=<Method for user ID retrieval>
   trusted.auth.user.param=<User Variable>
   ```

3. **`global.properties`** という名前でファイルを保存します。
4. `C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥eclipse¥plugins` にある `com.businessobjects.webpath.InfoView.jar` ファイル内の `web` フォルダの中に、`custom.jsp` ファイルがあることを確認します。
5. `com.businessobjects.webpath.InfoView.jar` ファイル内の `custom.jsp` ファイルに以下のカスタム Java コードを挿入します。

   ```
   <%
   //custom Java code
   request.getSession().setAttribute("MyUser","<Username>");
   %>
   ```

   > ⓘ 注記
   >
   > 上記のコードスニペットで、変数 <Username> は BI プラットフォームの有効な Enterprise ユーザである必要があります。

6. Web アプリケーションサーバを再起動します。
7. WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。

   WDeploy の使用については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

信用できる認証を適切に設定したことを確認するには、次の URL で BI ラウンチパッドにアクセスします。`http://<[cmsname]>:8080/BOE/BI/custom.jsp`。ここで、`<[cmsname]>` は CMS をホストするマシンの名前です。初回のみ、ユーザ名とパスワードの入力を求められます。認証が成功すると、BI ラウンチパッドに自動的にリダイレクトされます。

9.2.8.3.1.2 Web セッション変数経由で共有シークレットを渡す

ユーザ情報と共有シークレットの両方が Web セッション変数経由で保存され渡されます。以前に保存した TrustedPrincipal.conf ファイルを開き、ファイルの内容に注意します。このサンプル設定では、共有シークレットが以下の内容であることを前提にしています。

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc6577
3841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

Tomcat のバンドルバージョンは Web アプリケーションサーバです。

1. 次のディレクトリにアクセスします。

   `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥`

2. テキストエディタで新しいファイルを作成します。
3. 以下を入力して、信用できる認証プロパティを指定します。

   ```
   sso.enabled=true
   trusted.auth.user.retrieval=WEB_SESSION
   trusted.auth.user.param=MyUser
   trusted.auth.shared.secret=MySecret
   ```

4. 次の名前でファイルを保存します。

   `global.properties`

5. 次のファイルにアクセスします。

   従来の BI ラウンチパッド: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥eclipse¥plugins¥webpath.InfoView¥web¥custom.jsp`

   Fiorified BI ラウンチパッド: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥eclipse¥plugins¥webpath.FioriBI¥web¥custom.jsp`

6. ファイルのコンテンツを変更し、以下を含めます。

   ```
   <%
   //custom Java code
   request.getSession().setAttribute("MySecret","9ecb0778edcff048edae0fcdde1a5db8
   211293486774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b
   6a3f1345285b55a0a7");
   request.getSession().setAttribute("MyUser","<Username>");
   %>
   ```

   > ⓘ 注記
   >
   > 上記のコードスニペットで、変数 <Username> は BI プラットフォームの有効な Enterprise ユーザである必要があります。

7. Web アプリケーションサーバを再起動します。
8. WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。

   WDeploy の使用については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

信用できる認証を適切に設定したことを確認するには、次の URL で BI 起動パッドアプリケーションにアクセスします。`http://[cmsname]:8080/BOE/BI/custom.jsp`。ここで、[cmsname] は CMS をホストするマシンの名前です。初回のみ、ユーザ名とパスワードの入力を求められます。認証が成功すると、BI ラウンチパッドに自動的にリダイレクトされます。

9.2.8.3.1.3 ユーザプリンシパルからユーザ名を渡す

以下のサンプル設定では、“JohnDoe” という名前のユーザが BI プラットフォームに作成されていることを前提にしています。

ユーザ情報は、ユーザプリンシパルオプションを介して保存され渡されます。共有シークレットは、`TrustedPrincipal.conf` ファイルを介して渡されます。このファイルはデフォルトで、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86` ディレクトリに保存されています。Tomcat のバンドルバージョンは Web アプリケーションサーバです。

1. Tomcat サーバを停止します。
2. デフォルトで `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥conf¥` ディレクトリにある、Tomcat の `server.xml` ファイルを開きます。
3. `<Realm className="org.apache.catalina.realm.UserDatabaseRealm"..../>` を探して、次の値に変更します。

   ```
   Realm className=" org.apache.catalina.realm.UserDatabaseRealm".../
   ```

4. デフォルトで `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥conf¥` ディレクトリにある `tomcat-users.xml` ファイルを開きます。
5. `<tomcat-users>` タグを検索し、以下の値を変更します。

   ```
   <user name=“JohnDoe” password=“password”
   roles=“onjavauser”/>
   ```

6. `C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥` ディレクトリにある `web.xml` ファイルを開きます。
7. `</web-app>` タグの前に、次の値を追加します。

   ```
   <security-constraint>
       <web-resource-collection>
            <web-resource-name>OnJavaApplication</web-resource-name>
            <url-pattern>/*</url-pattern>
       </web-resource-collection>
       <auth-constraint>
            <role-name>onjavauser</role-name>
       </auth-constraint>
   </security-constraint>
   <login-config>
       <auth-method>BASIC</auth-method>
       <realm-name>OnJava Application</realm-name>
   </login-config>
   ```

   `<url-pattern></url-pattern>` パラメータに特定ページを入力します。通常、このページは BI ラウンチパッドまたはその他の Web アプリケーションのデフォルト URL ではありません。

8. カスタムの `global.properties` ファイルで、次の値を入力します。

   ```
   trusted.auth.user.retrieval=USER_PRINCIPAL
   trusted.auth.user.namespace.enabled=true
   ```

   > ⓘ 注記
   >
   > `trusted.auth.user.namespace.enabled=true` の設定はオプションです。外部ユーザ名を別の BI プラットフォームユーザ名にマップする場合に、このパラメータを追加します。

9. Web アプリケーションサーバを再起動します。
10. WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。

    WDeploy の使用については、*SAP BusinessObjects Business Intelligence* プラットフォーム *Web* アプリケーションデプロイメントガイドを参照してください。

リモートユーザ方法を使用中の場合、Web アプリケーションサーバ上のこの設定は同じです。

信用できる認証を適切に設定したことを確認するには、次の URL を使用して BI ラウンチパッドにアクセスします。`http://<[cmsname]>:8080/BOE/BI` (`<[cmsname]>` は CMS をホスティングしているマシンの名称です。)しばらくすると、ログオンダイアログボックスが表示されます。

9.3 LDAP 認証

9.3.1 LDAP 認証の使用

この節では、BI プラットフォームでの LDAP 認証の使用方法の概要について説明します。また、LDAP アカウントを BI プラットフォームで管理、設定できる管理ツールについても紹介します。

BI プラットフォームのインストール時に、LDAP 認証プラグインは自動的にインストールされますが、デフォルトでは有効になりません。 LDAP 認証を使用するには、最初にそれぞれの LDAP ディレクトリが設定されていることを確認する必要があります。LDAP の詳細については、LDAP のマニュアルを参照してください。

アプリケーションに依存しない共通のディレクトリ環境として LDAP(Lightweight Directory Access Protocol)を使用すると、さまざまなアプリケーション間で情報を共有できます。LDAP はオープン標準に基づいており、ディレクトリ内の情報のアクセスや更新の手段を提供します。

LDAP は、ディレクトリクライアントとディレクトリサーバ間の通信にディレクトリアクセスプロトコル(DAP)を使用する X.500 標準に基づいています。LDAP は、より少ないリソースを使用して、X.500 の処理と機能の一部を簡略化および省略するので、DAP の代替プロトコルして効果を発揮します。

LDAP 内のディレクトリ構造には、特定のスキーマで配置されたエントリが含まれます。エントリは、対応する識別名(DN)または共通名(CN)で識別されます。その他の共通属性として、組織単位名(OU)と組織名(O)があります。たとえばメンバーグループは、ディレクトリツリー内に、cn=BI platform Users、ou=Enterprise Users A、o=Research のように位置しています。詳細は、LDAP に関する文書を参照してください。

LDAP はアプリケーションに依存していないので、適切な権限があればどのクライアントでもそのディレクトリにアクセスできます。LDAP を使用すると、ユーザが LDAP 認証を介して BI プラットフォームにログオンするように設定できます。これによりユーザはシステム内のオブジェクトへのアクセス権限を使用できます。LDAP サーバ (または複数のサーバ) が実行中で、既存のネットワーク接続されたコンピュータシステムで LDAP を使用していれば、(Enterprise 認証、Windows AD 認証と共に) LDAP 認証を使用できます。

必要があれば、BI プラットフォームに組み込まれた LDAP セキュリティプラグインで、サーバ認証または相互認証のいずれかを使用して確立された SSL 接続を使用して、LDAP サーバと通信できます。サーバ認証では、LDAP サーバが、サーバの信頼性を検証するために BI プラットフォームが使用するセキュリティ証明書を持ち、一方で匿名クライアントからの接続を許可します。相互認証では、LDAP サーバと BI プラットフォームの両方がセキュリティ証明書を持ち、接続が確立する前に LDAP サーバがクライアントの証明書を検証する必要があります。

BI プラットフォームに組み込まれた LDAP セキュリティプラグインでは、SSL を介して LDAP サーバと通信するように設定できますが、ユーザの認証情報を検証するときには常に Basic 認証が実行されます。BI プラットフォームとともに LDAP 認証をデプロイする前に、これらの LDAP の種類の違いを熟知しておく必要があります。詳

細については RFC2251 を参照してください。この資料は、現在 http://www.faqs.org/rfcs/rfc2251.html で入手できます。

関連情報

LDAP 認証の設定 [261 ページ]
LDAP グループのマッピング [272 ページ]

9.3.1.1 LDAP セキュリティプラグイン

LDAP セキュリティプラグインを使用して、ユーザアカウントとグループを LDAP ディレクトリサーバから BI プラットフォームにマップできます。LDAP 認証を指定するすべてのログオンリクエストをシステムで検証することもできます。ユーザは LDAP ディレクトリサーバに照会されて認証を受け、マップされた LDAP グループのメンバーシップが検証されてから、CMS からアクティブな BI プラットフォームセッションが許可されます。ユーザリストとグループメンバーシップは、システムによって動的に管理されます。BI プラットフォームが SSL (Secure Sockets Layer) 接続を使用するように指定して、セキュリティを強化する LDAP ディレクトリサーバと通信させることができます。

BI プラットフォームの LDAP 認証は、グループをマップして、認証、アクセス権限、およびエイリアスの作成を設定できる点で、Windows AD 認証によく似ています。NT 認証や AD 認証の場合と同じように、既存の LDAP ユーザに対して新しい Enterprise アカウントを作成することができ、ユーザ名が Enterprise ユーザ名と同じであれば、LDAP エイリアスを既存のユーザに割り当てることができます。さらに、次のことも実行できます。

- LDAP ディレクトリサーバからユーザーとグループをマップします。
- AD に対して LDAP をマップします。AD に対して LDAP を設定する場合には制限があります。
- 複数のホスト名とそのポートを指定します。
- SiteMinder を使用する LDAP を設定します。

LDAP ユーザとグループをマップすると、すべての BI プラットフォームクライアントツールで LDAP 認証がサポートされます。LDAP 認証をサポートする独自のアプリケーションを作成することもできます。

関連情報

LDAP サーバまたは相互認証の SSL 設定 [265 ページ]
Windows AD に対する LDAP のマッピング [274 ページ]
SiteMinder での LDAP プラグインの設定 [270 ページ]

9.3.2 LDAP 認証の設定

管理を簡単にするために、BI プラットフォームでは、ユーザアカウントおよびグループアカウントの LDAP 認証をサポートしています。ユーザが LDAP ユーザ名とパスワードを使ってシステムにログオンできるようにするに

は、LDAP ユーザアカウントを BI プラットフォームにマップする必要があります。LDAP アカウントをマップする場合、新しいアカウントを作成するか、既存の BI プラットフォームアカウントにリンクできます。

LDAP 認証を設定して有効にする前に、LDAP ディレクトリが設定されていることを確認してください。詳細については、LDAP のマニュアルを参照してください。

LDAP 認証の設定には、次のタスクが含まれます。

- LDAP ホストの設定
- SSL 用の LDAP サーバの準備 (必要な場合)
- SiteMinder での LDAP プラグインの設定 (必要な場合)

> ⓘ 注記
>
> AD に対して LDAP を設定すると、ユーザをマッピングすることができますが、シングルサインオンまたはデータベースへのシングルサインオンを設定できなくなります。ただし、SiteMinder や信用できる認証のような LDAP シングルサインオン方法も使用できます。

9.3.2.1 LDAP ホストを設定する

LDAP ホストを設定する前に、LDAP サーバをインストールして実行中にしておくことをお勧めします。

1. ナビゲーション一覧から、[認証] を選択し、CMC の [認証] 管理エリアに移動します。
2. [*LDAP*] をダブルクリックします。
3. 初めて LDAP 認証を設定する場合、[*LDAP 設定ウィザードの起動*] をクリックします。
4. [*LDAP ホストの追加 (ホスト名:ポート)*] フィールドに LDAP ホストの名前とポート番号 (たとえば、"myserver:123") を入力し、[追加] をクリックし、[次へ] をクリックします。

   > → ヒント
   >
   > フェールオーバーに使用するホストを追加する場合は、この手順を繰り返して、同じサーバタイプの LDAP ホストを複数追加します。ホストを削除するには、ホスト名を強調表示して [削除] をクリックします。

5. [*LDAP サーバの種類*] 一覧からサーバのタイプを選択します。

   > ⓘ 注記
   >
   > LDAP を AD にマッピングしている場合は、サーバの種類として [*Microsoft Active Directory Application Server*] を選択します。

6. LDAP サーバ属性マッピングまたは LDAP デフォルト検索属性を表示または変更する場合は、[属性マッピングの表示] をクリックします。

   デフォルトでは、サポートされている各サーバタイプのサーバ属性マッピングおよび検索属性は設定済みです。

7. [次へ] をクリックします。
8. [*ベース LDAP 識別名*] フィールドに、LDAP サーバの識別名 (たとえば、o=SomeBase) を入力し、[次へ] をクリックします。
9. [*LDAP サーバ管理認証情報*] エリアに、ディレクトリへの読み取りアクセス権を持つユーザアカウントの識別名とパスワードを入力します。

管理者認証情報は不要です。

LDAP サーバで匿名バインドを許可する場合は、このエリアを空白のままにします。BI プラットフォームサーバとクライアントは、匿名ログオンを介してプライマリホストにバインドされます。

10. LDAP ホストに紹介を設定している場合は、[*LDAP* 紹介の認証情報] エリアに認証情報を入力し、[紹介のホップ最大数] フィールドに紹介ホップの数を入力します。

    [*LDAP* 紹介の認証情報] エリアは、次のすべての条件に該当する場合に設定する必要があります。

    - プライマリホストが、指定された基準でエントリのクエリを処理する別のディレクトリサーバに紹介されるように設定されている。
    - 紹介されるホストは、匿名バインドを許可しないように設定されている。
    - 紹介されるホストからのグループが、BI プラットフォームにマップされる。

    > ⓘ 注記
    >
    > グループは複数のホストからマップできますが、設定できる紹介認証情報は 1 組のみです。したがって、紹介ホストが複数ある場合は、各ホストのユーザアカウントを作成するときに同じ識別名とパスワードを使用しなければなりません。

    > ⓘ 注記
    >
    > [紹介のホップ最大数] を 0 に設定すると、紹介は行われません。

11. [次へ] をクリックします。
12. 使用する Secure Sockets Layer (SSL) 認証の種類を選択します。

    - *Basic (SSL なし)*
    - サーバ認証
    - 相互認証

    サーバ認証および相互認証の詳細と前提条件については、後の節で説明します。いずれかの種類の SSL を使用して LDAP 認証を正常に設定するために、この手順を先に進める前に、このドキュメント内の *LDAP* サーバまたは相互認証の *SSL* 設定を読んでください。

13. [次へ] をクリックして、LDAP シングルサインオン認証の方法を選択します。

    - *Basic (SSL なし)*
    - *SiteMinder*

14. [次へ] をクリックして、BI プラットフォームアカウントへのエイリアスとユーザのマッピング方法を選択します。

    a. [新しいエイリアスのオプション] エリアを使用して、Enterprise アカウントに新しいエイリアスをマップする方法を指定します。

       - 追加した各 *LDAP* エイリアスを同一名のアカウントに割り当てる
         このオプションは、複数のユーザが同じ名前の Enterprise アカウントを持っている場合、つまり LDAP エイリアスが既存のユーザに割り当てられる (自動エイリアス作成がオンである) 場合に使用します。既存の Enterprise アカウントを持っていないユーザや Enterprise と LDAP で同じアカウント名を使用していないユーザは、新しいユーザとして追加されます。
       - 追加するすべての *LDAP* エイリアスに新しいアカウントを作成する
         このオプションは、ユーザごとに新しいアカウントを作成する場合に使用します。

    b. [エイリアス更新オプション] エリアで、Enterprise アカウントのエイリアスの更新を管理する方法を選択します。

       - エイリアスの更新時に新しいエイリアスを作成する

このオプションを使用すると、BI プラットフォームにマップされたすべての LDAP ユーザに対して、新しいエイリアスを自動的に作成します。新しい LDAP アカウントが BI プラットフォームアカウントを持たないユーザに対して作成されます。または [追加するすべての *LDAP* エイリアスに新しいアカウントを作成する] を選択している場合は、新しい LDAP アカウントがすべてのユーザに対して作成されます。

- ユーザのログオン時にのみ新しいエイリアスを作成する
  マッピングしている LDAP ディレクトリに多くのユーザが含まれており、その一部のユーザだけが BI プラットフォームを使用する場合に、このオプションを使用します。プログラムは、すべてのユーザに対してエイリアスや Enterprise アカウントを自動で作成するわけではありません。代わりに、BI プラットフォームにログオンするユーザだけにエイリアスを (必要な場合は、アカウントも) 作成します。

c. [新しいユーザのオプション] エリアで、新しいユーザを作成する方法を指定します。

- 新しいユーザを登録ユーザとして作成する
  登録ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。登録ユーザライセンスは特定のユーザに関連付けられており、ユーザはそのユーザ名およびパスワードに基づいてシステムにアクセスすることができます。このため、登録ユーザは、システムに接続している他のユーザの数に関係なく接続できます。このオプションを使用して作成したユーザアカウントに使用できる登録ユーザライセンスを持っている必要があります。

  > **注記**
  >
  > 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。
  >
  > ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。

- 新しいユーザを同時接続ユーザとして作成する
  同時接続ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。同時接続ライセンスでは BI プラットフォームに同時接続できるユーザ数が指定されます。この種類のライセンスは、少ないユーザ数の同時接続ライセンスで多数のユーザをサポートできるため、柔軟性に優れています。たとえば、ユーザがプラットフォームにアクセスする頻度と時間の長さによって、100 ユーザ同時接続ライセンスで 250、500、または 700 のユーザをサポートできます。

15. ユーザ属性マッピングを設定する場合、または、電子メールアドレスを LDAP サーバからインポートする予定がある場合は、この手順を実行します。[属性バインディングオプション] エリアで、LDAP プラグインの属性バインディングの優先順位を指定します。

    a. [フルネーム、電子メールアドレス、およびその他の属性のインポート] ボックスをクリックします。
    LDAP アカウントで使用するフルネームと説明がインポートされ、ユーザオブジェクトとともにシステムに格納されます。

    b. [別の属性バインディングに関連する *LDAP* 属性バインディングの優先順位を設定する] のオプションを指定します。

    > **注記**
    >
    > オプションが [1] に設定されている場合は、LDAP およびその他のプラグイン (Windows AD および SAP) が有効なシナリオでは、LDAP 属性が優先されます。オプションが「3」に設定されている場合は、その他の有効化プラグインの属性が優先されます。

16. [完了] をクリックします。

関連情報

LDAP サーバまたは相互認証の SSL 設定 [265 ページ]
SiteMinder での LDAP プラグインの設定 [270 ページ]

9.3.2.2 複数の LDAP ホストの管理

LDAP と BI プラットフォームを使用すると、複数の LDAP ホストを追加することで、システムにフォールトトレランスを持たせることができます。システムは、プライマリ LDAP ホストとして追加した、1 つめのホストを使用します。それ以降のホストはフェールオーバーホストとして扱われます。

プライマリ LDAP ホストとすべてのフェールオーバーホストは、完全に同じ方法で設定する必要があります。各 LDAP ホストは、グループをマップするすべての追加ホストを参照する必要があります。LDAP ホストと参照の詳細については、LDAP のマニュアルを参照してください。

複数の LDAP ホストを追加するには、LDAP の設定時に LDAP 設定ウィザードを使用して、すべてのホストを入力します (詳細参照)。また、LDAP をすでに設定してある場合、セントラル管理コンソールの[認証管理]エリアを表示して、[LDAP]タブをクリックします。[LDAP サーバの設定の概要]エリアで LDAP のホスト名をクリックし、ホストの追加または削除ができるページを開きます。

> ⓘ 注記
>
> プライマリホストを最初に追加してから、残りのフェールオーバーホストを追加してください。

> ⓘ 注記
>
> フェールオーバー LDAP ホストを使用する場合、最高レベルの SSL セキュリティは使用できません (つまり、[信頼できる認証機関からのサーバの証明書であり、証明書の CN 属性とサーバの DNS ホスト名が一致する場合のみ許可する] オプションを選択できません)。

関連情報

LDAP 認証の設定 [261 ページ]

9.3.2.3 LDAP サーバまたは相互認証の SSL 設定

この節には、LDAP に対する SSL に基づくサーバまたは相互認証に関する詳細な情報が含まれます。SSL に基づく認証の設定には、事前ステップが必要です。ここでは、CMC での LDAP サーバ認証および相互認証の設定について、詳細な情報を説明します。ここで説明する内容は、LDAP ホストが設定済みであり、SSL 認証用に以下のいずれかを選択していることを前提にしています。

その他の情報、または LDAP ホストサーバ設定の情報については、LDAP ベンダーのドキュメントを参照してください。

Windows システムの場合、デフォルトの SSL 通信は TLS 1.2 を介して行われます。Linux システムについては、SAP ノート 2623529 を参照してください。

関連情報

LDAP ホストを設定する [262 ページ]

9.3.2.3.1 LDAP サーバまたは相互認証を設定する

リソース	このタスクを開始する前に実行する操作
CA 証明書	この操作は、SSL を用いる、サーバ認証および相互認証の両方で必要です。 1. 認証機関 (CA) を取得し、CA 証明書を生成します。 2. LDAP サーバにその証明書を追加します。 詳細については、LDAP ベンダーのマニュアルを参照してください。
サーバ証明書	この操作は、SSL を用いる、サーバ認証および相互認証の両方で必要です。 1. サーバ証明書を要求し、生成します。 2. その証明書を承認し、その後 LDAP サーバに追加します。

cert7.db または cert8.db、key3.db	これらのファイルは、SSL を用いる、サーバ認証および相互認証の両方で必要です。
	1. 要件に応じて、`cert7.db` または `cert8.db` ファイルを生成する certutil アプリケーションを https://developer.mozilla.org/en-US/docs/NSS/tools から ダウンロードします。
	2. CA 証明書を certutil アプリケーションと同じディレクトリにコピーします。
	3. 次のコマンドを使用して、`cert7.db` または `cert8.db` ファイルと、`key3.db` および `secmod.db` ファイルを生成します。
	`certutil -N -d .`
	4. 次のコマンドを使用して、`cert7.db` または `cert8.db` ファイルに CA 証明書を追加します。
	`certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer`
	5. BI プラットフォームをホストするコンピュータのディレクトリに、これら 3 つのファイルを保存します。

cacerts	このファイルは、BI ラウンチパッドのような Java アプリケーションの SSL を用いる相互認証に必要です。

リソース	このタスクを開始する前に実行する操作
	1. Java bin ディレクトリの keytool ファイルを探します。 2. 次のコマンドを使用して、cacerts ファイルを作成します。 `keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore` 3. cert7.db または cert8.db ファイル、および key3.db ファイルと同じディレクトリに cacerts ファイルを保存します。

クライアント証明書	1. cert7.db または cert8.db ファイル、および .keystore ファイルのそれぞれに対してクライアント要求を作成します。
	• LDAP プラグインを設定するには、certutil アプリケーションを使用してクライアント証明書要求を生成します。
	• 次のコマンドを使用して、クライアント証明書要求を生成します。
	`certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .`
	<client_dn> には、"CN=<client_name>、OU=<org unit>、O=<Companyname>、L=<city>、ST=<province>、および C=<country> のような情報が含まれます。
	2. CA を使用して、この証明書要求を認証します。次のコマンドを使用して証明書を取得し、cert7.db または cert8.db ファイルにその証明書を挿入します。
	`certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name>`
	3. SSL を用いた Java 認証を容易に行うには、次の操作を実行します。
	• Java bin ディレクトリにある keytool ユーティリティを使用して、クライアント証明書要求を生成します。
	• 次のコマンドを使用して、キーペアを生成します。
	`keytool -genkey -keystore .keystore`

リソース	このタスクを開始する前に実行する操作

	4. クライアントに関する情報を指定した後で、次のコマンドを使用して、クライアント証明書要求を生成します。
	`keytool -certreq -file <certificate_request_name> -keystore .keystore`
	5. クライアント証明書要求が CA に承認された後で、次のコマンドを使用して、CA 証明書を `.keystore` ファイルに追加します。
	`keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore`
	6. CA からクライアント証明書要求を取得し、次のコマンドを使用して、それを `.keystore` ファイルに追加します。
	`keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore`
	7. BI プラットフォームをホストするコンピュータの `cert7.db` または `cert8.db` ファイル、および `cacerts` ファイルと同じディレクトリに `.keystore` ファイルを保存します。

1. 使用する SSL セキュリティのレベルを選択します。

   初めて LDAP 設定ウィザードを使用して LDAP 認証を設定する場合、*SSL 認証の種類*リストから相互認証を選択し、次へをクリックします。または、LDAP 認証設定を再度行う場合、CMC の [認証] エリアに移動し、[*LDAP*] をダブルクリックします。*LDAP サーバの設定の概要*ページが表示されます。*SSL タイプ*の値をクリックし、*SSL 認証の種類*リストから相互認証を選択します。

   - サーバの証明書を常時許可する
     これはセキュリティが最も低いオプションです。LDAP ホストとの SSL 接続を確立して LDAP ユーザとグループを認証する前に、BI プラットフォームは、LDAP ホストからセキュリティ証明書を受信する必要があります。BI プラットフォームは、受信する証明書を検証しません。
   - 信頼できる認証機関からのサーバの証明書のみ許可する
     これはセキュリティが中程度のオプションです。LDAP ホストとの SSL 接続を確立して LDAP ユーザとグループを認証する前に、BI プラットフォームは、LDAP ホストから送信されたセキュリティ証明書を受け取り、それを検証する必要があります。証明書を検証するために、BI プラットフォームは証明書データベースを検索して、その証明書を発行した CA を確認する必要があります。
   - 信頼できる認証機関からのサーバの証明書であり、証明書の *CN* 属性とサーバの *DNS* ホスト名が一致する場合のみ許可する
     これはセキュリティが最も高いオプションです。LDAP ホストとの SSL 接続を確立して LDAP ユーザとグループを認証する前に、BI プラットフォームは、LDAP ホストから送信されたセキュリティ証明書を受け取り、それを検証する必要があります。証明書を検証するために、BI プラットフォームは証明書データベースを検索して、その証明書を発行した CA を確認し、サーバ証明書の CN 属性が、ウィザードの最初の手順で [*LDAP ホストの追加*] ボックスに入力した LDAP ホスト名と完全に一致することを確認できる必要があります (LDAP ホスト名に「**`ABALONE.rd.crystald.net:389`**」と入力した場合)。証明書で **`CN =ABALONE:389`** として使用されている場合は、機能しません。

サーバセキュリティ証明書のホスト名は、プライマリ LDAP のホスト名です。このオプションを選択した場合は、フェールオーバー LDAP ホストを使用できません。

> ⓘ 注記
>
> Java アプリケーションは、最初と最後の設定を無視し、信頼できる CA からのサーバ証明書のみを受け入れます。

2. [*SSL ホスト*] ボックスに各コンピュータのホスト名を入力し、[追加] をクリックします。

   次に、BI プラットフォーム SDK を使用する BI プラットフォームデプロイメントの各コンピュータのホスト名を追加する必要があります。これには、Central Management Server を実行中のコンピュータ、および Web アプリケーションサーバを実行中のコンピュータが含まれます。

3. 一覧に追加した各 SSL ホストに SSL 設定を指定します。
   a. SSL 一覧から [デフォルト] を選択します。
   b. [デフォルト値を使用] チェックボックスをオフにします。
   c. [証明書とキーデータベースファイルのパス] ボックスおよび [キーデータベースのパスワード] ボックスに値を入力します。
   d. 相互認証の設定を指定している場合は、[認証データベースでのクライアント認証用ニックネーム] ボックスに値を入力します。

> ⓘ 注記
>
> デフォルト設定は、任意のホストの [デフォルト値を使用] チェックボックスがオンになっている設定、または SSL ホストの一覧に名前を追加しないすべてのコンピュータに対して使用されます。

4. 一覧にない各ホストのデフォルト設定を指定して、[次へ] をクリックします。

   別のホストの設定を指定するには、ホスト名を左側のリストで選択し、右側のボックスに値を入力します。

> ⓘ 注記
>
> デフォルト設定は、任意のホストの [デフォルト値を使用] チェックボックスがオンになっている設定、または SSL ホストの一覧に名前を追加しないすべてのコンピュータに対して使用されます。

5. LDAP シングルサインオン認証の方法として [*Basic (SSL なし)*] または [*SiteMinder*] を選択します。
6. 新しい LDAP ユーザおよびエイリアスの作成方法を選択します。
7. 完了をクリックします。

関連情報

SiteMinder での LDAP プラグインの設定 [270 ページ]

9.3.2.4 LDAP の設定を変更する

LDAP 設定ウィザードを使用して LDAP 認証を設定すると、[*LDAP サーバの設定の概要*] ページで LDAP の接続パラメータとメンバーグループを変更できるようになります。

1. CMC の[認証]管理エリアを表示します。
2. [*LDAP*]をダブルクリックします。

   LDAP 認証が設定されていると、[*LDAP サーバの設定の概要*] ページが表示されます。このページでは、すべての接続パラメータエリアまたはフィールドを変更したり、[マップされた *LDAP* メンバーグループ] エリアのオプションを変更することができます。
3. 新しい接続設定ではアクセスできない、現在マップされているグループを削除し、[更新] をクリックします。

   ユーザグループを選択し、[マップされた *LDAP* メンバーグループ] セクションで [削除] ボタンをクリックすることにより、マップされているグループを削除できます。
4. 接続設定を変更し、[更新] をクリックします。
5. 必要に応じて、[新しいエイリアスのオプション]、[エイリアス更新オプション]、および [新しいユーザのオプション] を変更し、[更新] をクリックします。
6. 新しい LDAP メンバーグループをマップし、[更新] をクリックします。

9.3.2.5 SiteMinder での LDAP プラグインの設定

ここでは、LDAP と SiteMinder を併用するように CMC を設定する方法を説明します。SiteMinder はサードパーティ製のユーザアクセスおよび認証ツールであり、LDAP セキュリティプラグインとともに使用して BI プラットフォームへのシングルサインオンを作成できます。

BI プラットフォームで SiteMinder と LDAP を使用するには、次の 2 つの箇所で設定を変更する必要があります。

- CMC を介した LDAP プラグイン
- `BOE.war` ファイルのプロパティ

> ⓘ 注記
>
> SiteMinder 管理者が 4.x エージェントに対するサポートを有効にしていることを確認してください。これは、ご使用の SiteMinder のサポートされているバージョンにかかわらず、実行する必要があります。SiteMinder の詳細とインストール方法については、SiteMinder のマニュアルを参照してください。

関連情報

LDAP ホストを設定する [262 ページ]

9.3.2.5.1 ETPKI ライブラリをインストールする

CA Single Sign-on Policy Server と BI プラットフォーム間で交換される情報を安全にするために、ETPKI ライブラリをインストールしてください。

ETPKI ライブラリをインストールする前に、CA Single Sign-On SDK をダウンロードする必要があります。

BI プラットフォームでは CA Single Sign-On 12.x のみがサポートされます。これより前のバージョンの CA Single Sign-On (以前の名前は CA Siteminder) がある場合、バージョン 12.x にアップグレードする必要があります。

1. 64 ビットの場合は `<CA Single Sign-On_INSTALLDIR>¥CA¥sdk¥etpki-install-64` に、32 ビットの場合は `<CA Single Sign-On_INSTALLDIR>¥CA¥sdk¥etpki-install` に移動します。

   > ⓘ 注記
   >
   > BI プラットフォームがインストールされているマシンに CA Single Sign-On セットアップがインストールされていない場合、ETPKI ライブラリを同じマシンにコピーします。

2. Linux 環境で　ETPKI ライブラリをインストール:
   a. root 権限を使用してログインし、コマンド `./setup install caller=sdk veryverbose` を実行します。
      インストールが成功したというメッセージがコンソールまたはインストールの最後に表示されます。
   b. コマンド `export CAPKIHOME=/opt/CA/SharedComponents/CAPKI` および `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<BOE_INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/` を実行して、BI プラットフォームユーザを使用してパスをインストールディレクトリとして設定します。
   c. *Server Intelligence Agent* を再起動します。
3. Windows 環境で ETPKI ライブラリをインストール:
   a. ETPKI ライブラリの場所から管理者権限を使用してコマンドプロンプトを起動します。
   b. コマンド `setup.exe install caller=sdk veryverbose` を実行します。
   c. *%temp%* 内部の *capki_install.log* にインストールが成功したというメッセージがあるかどうかをチェックします。
   d. *Server Intelligence Agent* を再起動します。

ETPKI ライブラリをインストールしました。

9.3.2.5.2 SiteMinder を使用したシングルサインオン用に LDAP に設定する

1. 次のいずれかの方法を使用して、[*SiteMinder* 設定を入力してください]画面を開きます。
   - LDAP 設定ウィザードの[*LDAP* シングルサインオン認証の方法を選択してください] 画面で SiteMinder を選択します。
   - LDAP を設定済みで SSO を追加している場合に使用できる LDAP 認証画面で [シングルサインオンの種類] を選択します。
2. [ポリシーサーバホスト] ボックスに各ポリシーサーバ名を入力し、[追加] をクリックします。
3. それぞれのポリシーサーバホストについて、[アカウントポート]、[認証ポート]、および[承認ポート]の番号を指定します。
4. [エージェント名]に名前、[共有シークレット]に共有シークレットを入力します。共有シークレットを [共有シークレットの確認] ボックスに再度入力します。
5. [次へ]をクリックします。
6. LDAP オプションの設定に進みます。

9.3.2.5.3 BOE war ファイルで LDAP と SiteMinder を有効化する

LDAP セキュリティプラグインの SiteMinder 設定の指定に加えて、BOE war プロパティの SiteMinder 設定も指定する必要があります。

1. BI プラットフォームインストール内にある `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥` ディレクトリに移動します。
2. メモ帳などのテキスト編集ユーティリティを使用して新しいファイルを作成します。
3. 次の文を入力します。

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

4. **`global.properties`** という名前でファイルの拡張子を付けずにファイルを保存し、ファイルを閉じます。
5. 同じディレクトリで別のファイルを作成します。
6. 次の文を入力します。

```
authentication.default=secLDAP
cms.default=[<your cms name>]:[<the CMS port number>]
```

例:

```
authentication.default=secLDAP
cms.default=mycms:6400
```

7. `bilaunchpad.properties` という名前でファイルを保存し、ファイルを閉じます。

これらの新しいプロパティが有効になるのは、変更した BOE Web アプリケーションが Web アプリケーションサーバを実行しているマシン上に再デプロイされてからです。WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。WDeploy の使用については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

9.3.3 LDAP グループのマッピング

LDAP 設定ウィザードを使用して LDAP ホストを設定すると、LDAP グループを Enterprise グループにマップできるようになります。

LDAP グループをマップすると、[認証] 管理領域で LDAP オプションをクリックして、そのグループを表示できます。 LDAP 認証が設定されていれば、BI プラットフォームにマップされた LDAP グループが [マップされた LDAP メンバーグループ] エリアに表示されます。

> **注記**
>
> また、Windows AD グループをマップして、LDAP セキュリティプラグインを介して BI プラットフォームで認証することもできます。

> **注記**
>
> AD に対して LDAP を設定している場合、この手順によって AD グループがマッピングされます。

9.3.3.1 BI プラットフォームを使用して LDAP グループをマップする

1. CMC の [認証] 管理エリアに移動します。
2. [*LDAP*] をダブルクリックします。

   LDAP 認証が設定されていると、LDAP サマリページが表示されます。
3. [マップされた *LDAP* メンバーグループ] エリアの [*LDAP* グループの追加 (*cn* または *dn* ごと)] フィールドに LDAP グループを (共通名または識別名で) 指定して、[追加] をクリックします。

   複数の LDAP グループを追加するには、この手順を繰り返します。グループを削除するには、LDAP グループを強調表示して [削除] をクリックします。
4. [新しいエイリアスのオプション] エリアを使用して、Enterprise アカウントに LDAP エイリアスをマップする方法を指定するためのオプションを選択します。
   - 追加した各 *LDAP* エイリアスを同一名のアカウントに割り当てる
     このオプションは、複数のユーザが同じ名前で既存の Enterprise アカウントを持っている場合、つまり LDAP エイリアスが既存のユーザに割り当てられる (自動エイリアス作成がオンである) 場合に使用します。既存の Enterprise アカウントを持っていないユーザや Enterprise と LDAP で同じアカウント名を使用していないユーザは、新しい LDAP ユーザとして追加されます。
   - 追加するすべての *LDAP* エイリアスに新しいアカウントを作成する
     このオプションは、ユーザごとに新しいアカウントを作成する場合に使用します。
5. [エイリアス更新オプション] エリアで、すべての新しいユーザに対して LDAP エイリアスを自動的に作成するかどうかを指定するためのオプションを選択します。
   - エイリアスの更新時に新しいエイリアスを作成する
     このオプションを使用すると、BI プラットフォームにマップされたすべての LDAP ユーザに対して、新しいエイリアスを自動的に作成します。新しい LDAP アカウントが BI プラットフォームアカウントを持たないユーザに対して作成されます。または [追加するすべての *LDAP* エイリアスに新しいアカウントを作成する] を選択し、[更新] をクリックしている場合は、新しい LDAP アカウントがすべてのユーザに対して作成されます。
   - ユーザのログオン時にのみ新しいエイリアスを作成する
     マッピングしている LDAP ディレクトリに多くのユーザが含まれており、その一部のユーザだけが BI プラットフォームを使用する場合に、このオプションを使用します。プログラムは、すべてのユーザに対してエイリアスや Enterprise アカウントを自動で作成するわけではありません。代わりに、BI プラットフォームにログオンするユーザだけにエイリアスを (必要な場合は、アカウントも) 作成します。
6. BI プラットフォームのライセンスがユーザロールに基づいている場合は、[新しいユーザのオプション] エリアで、LDAP アカウントにマップするために作成された新しい Enterprise アカウントのプロパティを指定するオプションを選択します。
   - 新しいユーザを登録ユーザとして作成する
     登録ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。登録ユーザライセンスは特定のユーザに関連付けられており、ユーザはそのユーザ名およびパスワードに基づいてシステムにアクセスすることができます。このため、登録ユーザは、システムに接続している他のユーザの数に関係なく接続できます。このオプションを使用して作成したユーザアカウントに使用できる登録ユーザライセンスを持っている必要があります。

     > **注記**
     >
     > 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、

> 該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。
>
> ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。

- 新しいユーザを同時接続ユーザとして作成する
  同時接続ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。同時接続ライセンスでは BI プラットフォームに同時接続できるユーザ数が指定されます。この種類のライセンスは、少ないユーザ数の同時接続ライセンスで多数のユーザをサポートできるため、柔軟性に優れています。たとえば、ユーザがシステムにアクセスする頻度と時間の長さによって、100 ユーザ同時接続ライセンスで 250、500、または 700 のユーザをサポートできます。

7. [更新] をクリックします。

9.3.3.2 BI プラットフォームを使用して LDAP グループをマップ解除する

1. CMC の[認証]管理エリアを表示します。
2. [*LDAP*]をダブルクリックします。

   LDAP 認証が設定されていると、LDAP サマリページが表示されます。
3. [マップされた LDAP メンバーグループ]エリアで、削除する LDAP グループを選択します。
4. [削除]をクリックし、[更新]をクリックします。

   このグループのユーザは BI プラットフォームにアクセスできません。

> ⓘ 注記
>
> ユーザが Enterprise アカウントに対するエイリアスを持つ場合のみ、この例外となります。アクセスを制限するには、ユーザの Enterprise アカウントを無効にするか、または削除します。

すべてのグループの LDAP 認証を拒否するには、[LDAP 認証を有効にする] チェックボックスをオフにしてから、[更新] をクリックします。

9.3.3.3 Windows AD に対する LDAP のマッピング

Windows AD (AD) に対して LDAP を設定する場合は、次の制限に注意してください。

- AD に対して LDAP を設定すると、ユーザをマッピングすることができますが、シングルサインオンまたはデータベースへのシングルサインオンを設定できなくなります。ただし、SiteMinder や信用できる認証のような LDAP シングルサインオン方法も使用できます。
- AD からのデフォルトグループにのみ属しているユーザは正常にログインできません。ユーザは、AD で明示的に作成された別のグループのメンバーでもあることが必要です。さらに、このグループはマッピングする必要があります。このようなグループの例として"ドメインユーザ"グループがあります。
- マップされたドメインローカルグループにフォレスト内の別のドメインのユーザが含まれる場合、フォレスト内の別のドメインのユーザは正常にログインできません。

- LDAP ホストとして指定された DC とは異なるドメインのユニバーサルグループのユーザは正常にログインできません。
- LDAP プラグインを使用して、BI プラットフォームがインストールされているフォレスト以外の AD フォレストからユーザおよびグループをマップすることはできません。
- AD のドメインユーザグループではマップできません。
- マシンのローカルグループはマップできません。
- グローバルカタログドメインコントローラを使用している場合は、AD に対して LDAP をマップしている際に追加で注意する点があります。

状況	留意点
複数のドメインでグローバルカタログドメインコントローラを指し示している場合	次ではマッピングでできます。 • 子ドメインのユニバーサルグループ • 子ドメインのユニバーサルグループを含む同じドメインのグループ • クロスドメインのユニバーサルグループ 次ではマップできません。 • 子ドメインのグローバルグループ • 子ドメインのローカルグループ • 子ドメインのグローバルグループを含む同じドメインのグループ • クロスドメインのグローバルグループ 一般的に、グループがユニバーサルグループの場合、クロスドメインまたは子ドメインからのユーザをサポートします。クロスドメインまたは子ドメインからのユーザが含まれる場合、他のグループはマップされません。指し示しているドメイン内で、ドメインのローカルグループ、グローバルグループ、およびユニバースグループをマッピングできます。
ユニバースグループでのマッピング	ユニバースグループでマッピングするには、グローバルカタログドメインコントローラを指し示す必要があります。また、ポート番号はデフォルトの 389 ではなく 3268 を使用する必要があります。

- 複数のドメインを使用していても、グローバルカタログドメインコントローラを指し示していない場合は、クロスドメインまたは子ドメインのどの種類のグループもマップできません。指し示している特定のドメインからのみすべての種類のグループでマッピングできます。

9.3.3.4 LDAP プラグインを使用した SAP HANA データベースへの SSO の設定

この節では、管理者が SUSE Linux 11 上で実行する BI プラットフォームと SAP HANA データベース間にシングルサインオン (SSO) を設定するために必要な手順について説明します。Kerberos を使用した LDAP 認証によって、AD ユーザは Linux、特に SUSE 上で実行する BI プラットフォームで認証を受けることができます。このシナリオでは、レポーティングデータベースとしての SAP HANA に対するシングルサインオンもサポートしています。

> **注記**
>
> SAP HANA データベースの設定方法については、*SAP HANA* データベース - サーバインストールと更新ガイドを参照してください。SAP HANA のデータアクセスコンポーネントの設定方法については、データアクセスガイドを参照してください。

実装の概要

Kerberos SSO が動作するには、次のコンポーネントが必要です。

コンポーネント	要件
ドメインコントローラ	Kerberos 認証を使用するよう設定された Active Directory を実行するマシンにホストされていること。
Central Management Server	SUSE Linux Enterprise 11 (SUSE) を実行するマシンにインストールおよび実行されていること。
Kerberos V5 クライアント	必要なユーティリティおよびライブラリとともに SUSE ホストにインストールされていること。 **注記** 最新バージョンの Kerberos V5 クライアントを使用してください。`bin` および `lib` フォルダを `PATH` および `LD_LIBRARY_PATH` 環境変数に追加してください。
LDAP 認証プラグイン	SUSE ホスト上で有効化すること。
Kerberos ログイン設定ファイル	Web アプリケーションサーバをホストするマシン上に作成すること。

実装ワークフロー

BI プラットフォームユーザが JDBC 経由の Kerberos 認証を使用して SAP HANA への SSO を実行できるようにするには、次のタスクを実行する必要があります。

1. AD ホストを設定します。
2. SUSE ホストと、AD ホスト上の BI プラットフォーム用に、アカウントと Keytab ファイルを作成します。
3. SUSE ホストに Kerberos リソースをインストールします。
4. Kerberos 認証を使用するように SUSE ホストを設定します。
5. LDAP 認証プラグインの Kerberos 認証のオプションを設定します。
6. Web アプリケーションホストの Kerberos ログイン設定ファイルを作成します。

9.3.3.4.1 ドメインコントローラを設定する

SUSE ホストとドメインコントローラ間に信頼関係を設定する必要がある場合があります。SUSE ホストが Windows ドメインコントローラ内にある場合は、信頼関係を設定する必要はありません。一方、BI プラットフォ

ームデプロイメントとドメインコントローラが異なるドメインにある場合は、SUSE Linux マシンとドメインコントローラ間に信頼関係を設定する必要がある場合があります。この設定には次の操作が必要です。

1. BI プラットフォームを実行する SUSE マシンにユーザアカウントを作成します。
2. ホストのサービスプリンシパル名 (SPN) を作成します。

> **注記**
>
> SPN の形式は、host/<hostname>@<DNS_REALM_NAME> という Windows AD の規則に従う必要があります。/<hostname> には、小文字の完全修飾ドメイン名を使用します。<DNS_REALM_NAME> は大文字で指定する必要があります。

3. Kerberos Keytab 設定コマンドの ktpass を実行して、SPN をユーザアカウントと関連付けます。

```
c:¥> ktpass -princ host/<hostname>@<DNS_REALM_NAME>-mapuser <username> -pass
Password1 -crypto RC4-HMAC-NT -out <username>base.keytab
```

ドメインコントローラをホストするマシン上で、次の手順を実行する必要があります。

1. BI プラットフォームを実行するサービス用のユーザアカウントを作成します。
2. [ユーザー アカウント] ページで新しいサービスアカウントを右クリックし、プロパティ > 委任 をクリックします。
3. [任意のサービスへの委任でこのユーザーを信頼する *(Kerberos のみ)*] を選択します。
4. Kerberos Keytab 設定コマンドの ktpass を実行して、新しいサービスアカウント用の SPN アカウントを作成します。

```
c:¥>ktpass -princ <sianame>/<service_name>@<DNS_REALM_NAME> -mapuser
<service_name> -pass <password> -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
-out <sianame>.keytab
```

> **注記**
>
> SPN の形式は、sianame/<service_name>@<DNS_REALM_NAME> という Windows AD の規則に従う必要があります。<service name> は小文字で指定します。小文字で指定しないと、SUSE プラットフォームでこの名前を解決できない可能性があります。<DNS_REALM_NAME> は大文字で指定する必要があります。

パラメータ	説明
-princ	Kerberos 認証の主体名を指定します。
-out	生成する Kerberos Keytab ファイルの名前を指定します。この名前は、-princ で使用した <sianame> と一致する必要があります。
-mapuser	SPN のマップ先ユーザアカウントの名前を指定します。Server Intelligence Agent はこのアカウントで実行されます。
-pass	サービスアカウントが使用するパスワードを指定します。
-ptype	主体の種類を指定します。 `-ptype KRB5_NT_PRINCIPAL`

パラメータ	説明
`-crypto`	サービスアカウントに使用する暗号の種類を指定します。 `-crypto RC4-HMAC-NT`

これで、SUSE マシンとドメインコントローラ間の信頼関係のために必要となる Keytab ファイルが生成されました。

この Keytab ファイルを SUSE マシンに送信し、`/etc` ディレクトリに保存する必要があります。

9.3.3.4.2 SUSE Linux Enterprise 11 マシンを設定する

BI プラットフォームを実行する SUSE Linux マシンで Kerberos を設定するには、次のリソースが必要です。

- ドメインコントローラ上に作成する Keytab ファイル。BI プラットフォームサービス用に作成する Keytab ファイルは必須です。SUSE ホスト用の Keytab は、特に BI プラットフォームホストとドメインコントローラを異なるドメインに配置するシナリオで使用することをお勧めします。
- 最新の Kerberos V5 ライブラリ (Kerberos クライアントを含む) を SUSE ホストにインストールする必要があります。バイナリの場所を `PATH` および `LD_LIBRARY_PATH` 環境変数に追加する必要があります。Kerberos クライアントが正しくインストールおよび設定されていることを検証するには、次のユーティリティとライブラリが SUSE ホストに存在することを確認してください。
  - `kinit`
  - `ktutil`
  - `kdestroy`
  - `klist`
  - `/lib64/libgssapi_krb5.so.2.2`
  - `/lib64/libkrb5.so.3.3`
  - `/lib/libkrb5support.so.0.1`
  - `/lib64/libk5crypto.so.3`
  - `/lib64/libcom_err.so.2`

> **→ ヒント**
>
> これらのライブラリのバージョンを確認するには、`rpm -qa | grep krb` を実行します。最新の Kerberos クライアント、ライブラリ、および Unix ホストの設定については、http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-install.html#Installing%20Kerberos%20V5 を参照してください。

すべての必要なリソースを SUSE ホストに用意した後、次の説明に従って Kerberos 認証を設定します。

> **ⓘ 注記**
>
> これらの手順を実行するには、root 権限が必要です。

1. Keytab ファイルを結合するために、次のコマンドを実行します。

```
> ktutil
ktutil: rkt <susemachine>.keytab
```

```
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

2. /etc/kerb5.conf ファイルを編集し、Windows プラットフォーム上のドメインコントローラを Kerberos ドメインコントローラ (KDC) として参照するようにします。

   次の例を使用してください。

```
[domain_realm]
 .name.mycompany.corp = DOMAINNAME.COM
  name.mycompany.corp = DOMAINNAME.COM

[libdefaults]
        forwardable = true
           default_realm = DOMAINNAME.COM
           default_tkt_enctypes = rc4-hmac
           default_tgs_enctypes = rc4-hmac

[realms]
        DOMAINNAME.COM = {
             kdc = machinename.domainname.com
            }
```

   > ⓘ 注記
   >
   > krb5.conf ファイルには、対象となる Kerberos 領域の KDC とサーバの場所、Kerberos アプリケーション、Kerberos 領域へのホスト名のマッピングなどの Kerberos 設定情報が含まれています。通常、krb5.conf ファイルは /etc ディレクトリにインストールされます。

3. SUSE ホストが KDC を検索できるように、ドメインコントローラを /etc/hosts に追加します。
4. /usr/local/bin ディレクトリの kinit プログラムを実行し、Kerberos が正しく設定されていることを確認します。AD アカウントのユーザアカウントで SUSE マシンにログインできることを確認します。

   > → ヒント
   >
   > KDC はチケット保証チケット (TGT) を発行します。TGT はキャッシュで参照できます。TGT を参照するには、klist プログラムを使用します。

例

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>
> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal08/10/11 17:33:43 08/11/11 03:33:46
krbtgt/<domain>@<domain>renew until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached
>klist -k
Keytab name: FILE:/etc/krb5.keytabKVNO Principal-3hdb/<FQDN>@<Domain>
```

また、kinit を使用して SPN をテストする必要があります。

9.3.3.4.3 LDAP 用の Kerberos 認証のオプションを設定する

LDAP 用の Kerberos 認証を設定する前に、まず BI プラットフォーム LDAP 認証プラグインを有効にして、AD ディレクトリに接続するように設定する必要があります。 LDAP 認証を使用するには、最初にそれぞれの LDAP ディレクトリが設定されていることを確認する必要があります。

> ⓘ 注記
>
> *LDAP 設定ウィザード*を実行する際に、*Microsoft Active Directory Application Server* を指定し、求められた設定の詳細情報を入力する必要があります。

LDAP 認証を有効にし、Microsoft Active Directory Application Server に接続した後、[LDAP サーバの設定の概要] ページに [*Kerberos 認証の有効化*] エリアが表示されるようになります。 このエリアを使用して Kerberos 認証を設定します。この設定は、SUSE 上の BI プラットフォームデプロイメントから SAP HANA データベースへのシングルサインオンを実行するために必要です。

1. CMC の認証管理エリアを表示します。
2. [*LDAP*]をダブルクリックします。

   [*LDAP サーバの設定の概要*] ページが表示されます。このページで、接続パラメータまたはフィールドを変更できます。
3. Kerberos 認証を設定するには、[*Kerberos 認証の有効化*] エリアで次の手順を実行します。
   a. [*Kerberos 認証の有効化*] をクリックします。
   b. [*セキュリティコンテキストをキャッシュする (データベースへの SSO に必要)*] をクリックします。

      > ⓘ 注記
      >
      > セキュリティコンテキストのキャッシュの有効化は、特に SAP HANA へのシングルサインオンの場合に必要になります。

   c. サービスプリンシパル名に、BI プラットフォームアカウントのサービスプリンシパル名 (SPN) を指定します。

      SPN を指定するための形式は、`<sianame/service>@<DNS_REALM_NAME>` です。それぞれ、次の項目を指定します。

`<sianame>`	Server Intelligence Agent の名前
`<service >`	BI プラットフォームの実行に使用するサービスアカウントの名前
DNS_REALM_NAME	ドメインコントローラのドメイン名 (大文字で指定)

      > → ヒント
      >
      > SPN を指定する際に、`<sianame/service>` で大文字と小文字が区別されることに注意してください。

   d. デフォルト *Kerberos 領域*にドメインコントローラのドメインを指定します。
   e. [ユーザプリンシパル名] に `userPrincipalName` を指定します。

      この値は、Kerberos が求めるユーザ ID 値を示すために、LDAP 認証アプリケーションによって使用されます。 指定した値は、Keytab ファイル作成時に入力した名前と一致している必要があります。
4. [更新] をクリックして、変更内容を送信および保存します。

これで、AD ディレクトリ内のユーザアカウントを参照するための Kerberos 認証のオプションが設定されました。

Kerberos ログオンおよびシングルサインオンを有効にするには、Kerberos ログイン設定ファイルの `bscLogin.conf` を作成する必要があります。

関連情報

LDAP 認証の設定 [261 ページ]

9.3.3.4.4 Kerberos ログイン設定ファイルを作成する

Kerberos ログオンおよびシングルサインオンを有効にするには、BI プラットフォーム Web アプリケーションサーバをホストするマシン上でログイン設定ファイルを追加する必要があります。

1. `bscLogin.conf` という名前のファイルを作成し、`/etc` ディレクトリに保存します。

   > **注記**
   >
   > このファイルは別の場所に保存することができます。 ただし、このファイルを別の場所に保存する場合は、Java のオプションでその場所を指定する必要があります。 `bscLogin.conf` および Kerberos Keytab ファイルは同じディレクトリに保存することをお勧めします。 分散デプロイメントでは、Web アプリケーションサーバをホストするすべてのマシンに `bscLogin.conf` ファイルを追加する必要があります。

2. `bscLogin.conf` ログイン設定ファイルに次のコードを追加します。

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="<principal name>";
};
```

   > **注記**
   >
   > 次のセクションは、特にシングルサインオンで必要となる部分です。
   >
   > ```
   > com.businessobjects.security.jgss.accept {
   > com.sun.security.auth.module.Krb5LoginModule required
   > storeKey=true
   > useKeyTab=true
   > keyTab="/etc/krb5.keytab"
   > principal="<principal name>";
   > };
   > ```

3. ファイルを保存して閉じます。

9.3.3.5 新しい LDAP アカウントのトラブルシューティング

- 新しい LDAP ユーザアカウントを作成したが、そのアカウントが BI プラットフォームにマップされているグループアカウントに属していない場合は、そのグループにマップするか、システムにすでにマップされているグループに新しい LDAP ユーザアカウントを追加します。
- 新しい LDAP ユーザアカウントを作成して、そのアカウントが BI プラットフォームにマップされているグループアカウントに属している場合は、ユーザのリストを最新表示します。

関連情報

LDAP 認証の設定 [261 ページ]
LDAP グループのマッピング [272 ページ]

9.4 Windows AD 認証

9.4.1 Windows AD 認証の使用

9.4.1.1 Windows AD サポート要件と初期設定

この節では、Windows Active Directory (AD) 認証を BI プラットフォームで動作するように設定するプロセスについて説明します。実行する必要のあるすべてのエンドツーエンドのワークフローを、検証テストおよび要件の確認とあわせて示します。

> **注記**
>
> Windows AD 認証の設定の詳細については、SAP ナレッジベース KBA 1631734 (https://service.sap.com/sap/support/notes/1631734) を参照してください。

サポート要件

BI プラットフォームで AD 認証を行うためには、次のサポート要件を覚えておく必要があります。

- CMS は常に、サポートされる Windows プラットフォームにインストールされる必要があります。
- 特定の BI プラットフォームアプリケーションでは特定の認証方法のみが使用される場合があります。たとえば、BI 起動パッドやセントラル管理コンソールのようなアプリケーションは、Kerberos のみをサポートします。

推奨される AD 設定のワークフロー

BI プラットフォームで手動 AD 認証を初めて設定する場合は、次のワークフローに従います。

1. ドメインコントローラの設定
2. CMC での AD 認証の設定
3. Server Intelligence Agent (SIA) での AD ユーザアカウントの設定
4. Kerberos での AD 認証に対応する Web アプリケーションサーバの設定

> ⓘ 注記
>
> シングルサインオン (SSO) が必要なくても、このワークフローに従ってください。次の節で説明しているワークフローでは、まず、手動で (AD ユーザ名およびパスワードを使用して) BI プラットフォームにログインできるようになります。手動 AD 認証の設定が正常に行われたら、AD 認証用に SSO を設定する手順について、詳細に説明します。

9.4.2 ドメインコントローラの準備

9.4.2.1 Kerberos での AD 認証用サービスアカウントの設定

Windows AD (Kerberos) 認証に対して BI プラットフォームを設定するには、サービスアカウントが必要です。新しいドメインアカウントを作成することも、既存のドメインアカウントを使用することもできます。サービスアカウントは、BI プラットフォームサーバの実行に使用されます。アカウントの設定後に、このアカウントの SPN を設定する必要があります。この SPN を使用して、AD ユーザグループを BI プラットフォームにインポートします。

> ⓘ 注記
>
> SSO で AD を使用するには、サービスアカウントのセットアップを後で再度見直して、アカウントに適切な権限を与え、制限された委任用に設定する必要があります。

9.4.2.1.1 Windows 2008 ドメインでサービスアカウントを設定する

Kerberos プロトコルを使用した Windows AD 認証を正常に有効にするには、新しいサービスアカウントを設定する必要があります。このサービスアカウントは、指定した AD グループのユーザに、BI 起動パッドへのログオンを許可するために、主に使用されます。次のタスクは、AD ドメインコントローラマシンで実行されます。

1. プライマリドメインコントローラで、新しいパスワード付きのサービスアカウントを作成します。
2. `setspn -s` コマンドを使用して、サービスプリンシパル名 (SPN) を、手順 1 で作成したサービスアカウントに追加します。サーバおよびサービスアカウントのサービスプリンシパル名 (SPN)、および BI ラウンチパッドがデプロイされるマシンの IP アドレスと完全修飾ドメインサーバを指定します。
   例:

   ```
   setspn –s BICMS/service_account_name.domain.com serviceaccountname
   ```

```
setspn -s HTTP/<servername> <servicename>
setspn -s HTTP/<servername.domain.com> <servicename>
setspn -s HTTP/<ip address of server> <servicename>
```

BICMS は SIA が実行中のマシンの名前、<servername> は BI ラウンチパッドがデプロイされるサーバの名前、<servernamedomain> は完全修飾ドメイン名です。

3. setspn -l <servicename> を実行して、サービスプリンシパル名がサービスアカウントに追加されていることを検証します。
コマンドの出力には、次のように、すべての登録済み SPN が含まれます。

```
Registered ServicePrincipalNames for
CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
HTTP/<ip address of server>
HTTP/<servername>.@example.com
HTTP/<servername>
<servername>/<servicename>@example.com
```

サンプル出力が次のように表示されます。

```
C:¥Users¥Admin>setspn -L bossosvcacct
Registered ServicePrincipalNames for
CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:
        BICMS/bossosvcacct@example.com
        HTTP/Tomcat HTTP/Tomcat@example.com
        HTTP/Load_Balancer.@example.com
```

サービスアカウントは、作成後に権限を付与し、サーバのローカル Administrators グループに追加する必要があります。SPN は、次の節で説明するように、AD グループをインポートするために使用します。

9.4.3 CMC での AD 認証の設定

9.4.3.1 Windows AD セキュリティプラグイン

Windows AD セキュリティプラグインを使用すると、AD 2008 のユーザデータベースから BI プラットフォームにユーザアカウントとグループをマップできます。また、すべてのログオンリクエストを検証し、AD 認証を指定することができます。ユーザは、AD ユーザデータベースに照会されて認証を受け、マップされた AD グループのメンバーシップが検証されると、アクティブなセッションを Central Management Server (CMS) から許可されます。プラグインを使用して、インポートされた AD グループの更新を設定できます。

Windows AD セキュリティプラグインでは、次の設定もできます。

- Kerberos での Windows AD 認証
- NTLM での Windows AD 認証
- シングルサインオンに対応する SiteMinder での Windows AD 認証

AD セキュリティプラグインは、ネイティブモードまたは混在モードで動作する AD 2008 ドメインに対応しています。

AD ユーザとグループをマップすると、これらのユーザとグループは [*Windows AD*] 認証オプションを使用して BI プラットフォームクライアントツールにアクセスできるようになります。

- Windows AD 認証は CMS が Windows で実行されている場合に機能します。データベースへの SSO を使用するには、Windows 上でレポーティングサーバも実行されている必要があります。それ以外の場合は、他のすべてのサーバとサービスを、BI プラットフォームでサポートされるすべてのプラットフォームで実行できます。

  > ⓘ 注記
  >
  > 設定は、SUSE Linux Enterprise 11 でのみ行われ、テストされています。

- BI プラットフォーム対応の Windows AD プラグインは、複数のフォレスト内のドメインをサポートします。

9.4.3.2 Windows AD ユーザとグループをマップする

AD ユーザグループを BI プラットフォームにインポートする前に、前提条件となる次のアクションを完了する必要があります。

- サービスアカウントを BI プラットフォームのドメインコントローラで作成しておきます。このサービスアカウントは、BI プラットフォームサーバの実行に使用されます。

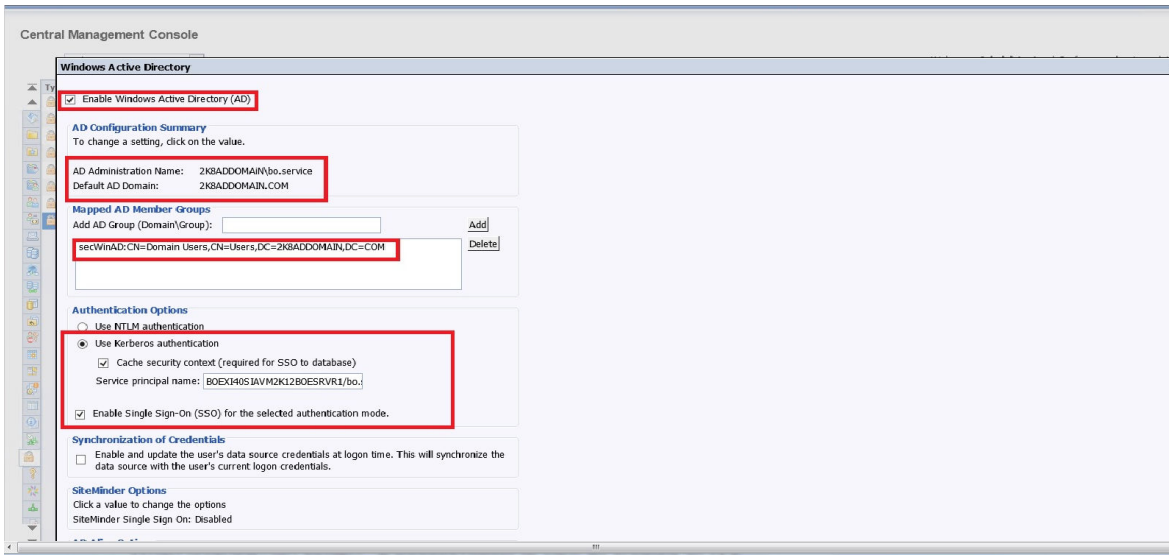
> **注記**
>
> Vintela シングルサインオン (SSO) での AD 認証を有効にするには、このために設定した SPN が必要です。次の手順では、BI プラットフォームに手動 AD 認証を設定します。手動 AD 認証を設定したら、AD 認証設定に SSO を追加する方法の詳細について、この章のシングルサインオンの設定の節を参照してください。

- SIA を実行中のマシン名を含む SPN が、サービスアカウントに追加されていることを確認しておきます。

次の手順 1 ～ 11 は、BI プラットフォームに AD グループをインポートするための必須の手順です。

1. CMC の [認証] 管理エリアに移動します。
2. [*Windows AD*] をダブルクリックします。
3. [*Windows Active Directory (AD) を有効にする*] チェックボックスを選択します。
4. [*AD 設定の概要*] エリアで、[*AD 管理名*] の横にあるリンクをクリックします。

> **注記**
>
> Windows AD プラグインを設定する前は、このリンクは引用符で表示されます。設定が保存されると、リンクには AD 管理名が表示されます。



5. 有効なドメインユーザアカウントの名前とパスワードを入力します。

   管理認証情報では、以下の形式のいずれかを使用できます。

   - NT 名 (ドメイン名¥ユーザ名)
   - UPN (`user@DNS_domain_name`)

   BI プラットフォームでは、このアカウントを使用して AD の情報をクエリします。BI プラットフォームが AD の内容を変更、追加、または削除することはありません。情報を読み取るだけであるので、適切な権限のみ必要です。

> **注記**
>
> AD 認証は、AD ディレクトリの読み取りに使用されたアカウントが無効になった場合には維持されません (たとえば、アカウントのパスワードが変更または期限切れになった場合やアカウントが無効になった場合)。

6. [デフォルトの *AD* ドメイン] ボックスに、AD ドメインを入力します。

   ドメインは、完全なドメイン名としてすべて大文字で指定するか、ほとんどのユーザが BI プラットフォームにログインする子ドメイン名を指定する必要があります。このドメイン名は通常、アプリケーションサーバの設定に使用する Kerberos 設定ファイル内で指定されているデフォルトドメインと一致します。デフォルトのドメインにあるグループは、ドメイン名のプレフィックスを指定しなくてもマップすることができます。デフォルトの AD ドメイン名を入力すると、デフォルトドメインのユーザが AD 認証を使用して BI プラットフォームにログオンする際に、AD ドメイン名を指定する必要がなくなります。

7. [マップされた *AD* メンバーグループ] エリアで、[*AD* グループの追加 (ドメイン¥グループ)] ボックスに AD ドメイン¥グループを次のいずれかの形式で入力して、グループをマップします。

   - NT 名とも呼ばれるセキュリティアカウントマネージャのアカウント名 (SAM) (ドメイン名¥グループ名)
   - DN (`cn=GroupName, ....., dc=DomainName, dc=com`)

   > **注記**
   >
   > ローカルグループをマップする場合、次の NT 名形式のみを使用します。`¥¥<ServerName>¥<GroupName>`。AD ではローカルユーザはサポートされません。つまり、マップされたローカルグループに所属するローカルユーザは、BI プラットフォームにマップされません。このため、ローカルユーザはシステムにアクセスできません。

   > **ヒント**
   >
   > BI ラウンチパッドに手動でログオンする場合、他のドメインに属するユーザは、ユーザ名の後に大文字のドメイン名を追加する必要があります。たとえば、`CHILD.PARENTDOMAIN.COM` は次の場所にあるドメインです。
   >
   > ```
   > user@CHILD.PARENTDOMAIN.COM
   > ```

8. [追加] をクリックします。

   このグループは、[マップされた *AD* メンバーグループ] の下のリストに追加されます。

9. [マップされた *AD* メンバーグループ] エリアで、[*AD* グループの検索 (ドメイン¥グループ)] フィールドに AD ドメイン¥グループを入力します。

   これにより、一覧で目的のグループが検索されます。また、[表示] を選択して、AD グループの完全な一覧を個別のダイアログボックスで表示することもできます。

10. [認証のオプション] エリアで [*Kerberos* 認証を使用する] を選択します。

11. [サービスプリンシパル名] ボックスに、BI プラットフォームサーバで実行するよう作成したサービスアカウントにマップされた SPN を入力します。

    > **注記**
    >
    > SIA を実行するサービスアカウントの SPN を指定する必要があります。例: `BICMS/bossosvcacct.domain.com`。

12. [更新] をクリックします。

    > **警告**
    >
    > ユーザおよびグループが正しくマッピングされていない場合は、先に進まないでください。特定の AD グループマッピングの問題を解決するには、SAP ノート 1631734 を参照してください。

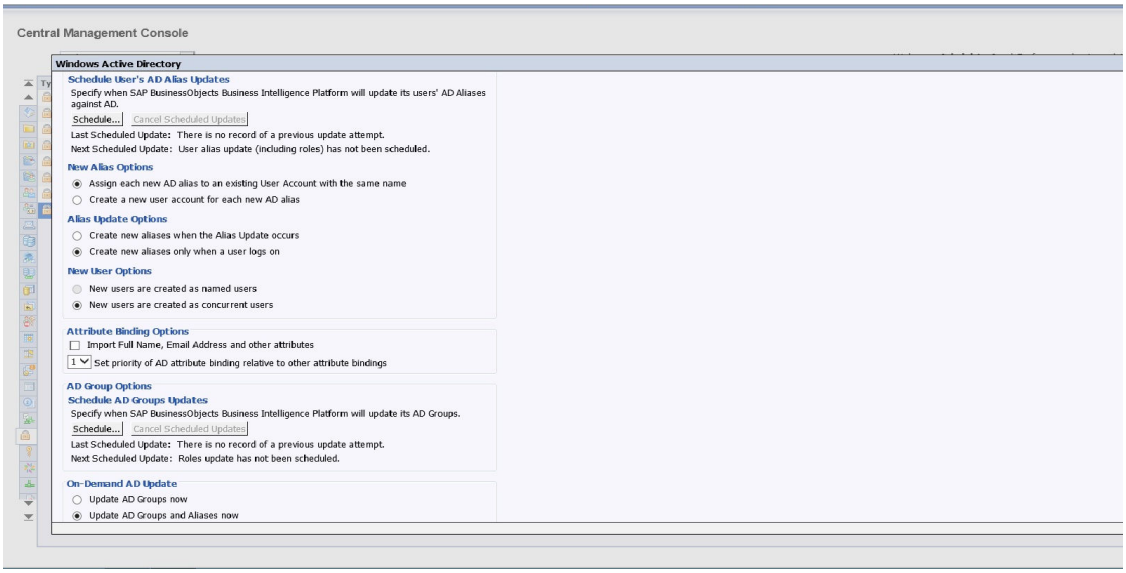
> ⓘ 注記
>
> AD グループアカウントが正常にマップされていて、AD 認証オプションや AD グループの更新を設定しない場合は、手順 12 ～ 19 は省略してください。手動 AD Kerberos 認証が正常に設定できたら、これらのオプションを設定することができます。

13. データベースへの SSO を設定する場合、[セキュリティコンテキストをキャッシュする] を選択します。

> ⓘ 注記
>
> ここで、初めて AD 認証設定を行う場合、まず、手動 AD 認証が正常に設定できてから、SSO に必要な追加の設定について検討することをお勧めします。

14. AD 認証設定で SSO が必要な場合、[選択した認証モードでのシングルサインオン *(SSO)* を有効にする] を選択します。
15. [認証情報の同期] エリアで、いずれかのオプションを選択し、AD ユーザのデータソースログオン認証情報を有効化して更新します。

    このオプションにより、ユーザの現在のログオン認証情報を使用してデータソースが同期化されます。そのため、ユーザが BI プラットフォームにログオンしていない場合、および Kerberos SSO が使用できない場合に、スケジュールされたレポートを実行できます。
16. [*AD* エイリアスのオプション] エリアで、BI プラットフォームでの新しいエイリアスの追加および更新方法を指定します。
    a. [新しいエイリアスのオプション] エリアで、Enterprise アカウントに新しいエイリアスをマップするためのオプションを選択します。
       - 同じ名前の既存のユーザアカウントに新しい *AD* エイリアスをそれぞれ割り当てる
         このオプションは、複数のユーザが同じ名前で既存の Enterprise アカウントを持っている場合、つまり AD エイリアスが既存のユーザに割り当てられる (自動エイリアス作成がオンである) 場合に選択します。既存の Enterprise アカウントを持っていないユーザや Enterprise と AD で同じアカウント名を使用していないユーザは、新しいユーザとして追加されます。
       - 新しい *AD* エイリアスごとに新しいユーザアカウントを作成する
         このオプションは、ユーザごとに新しいアカウントを作成する場合に選択します。
    b. [エイリアス更新オプション] エリアで、Enterprise アカウントのエイリアスの更新を管理するためのオプションを選択します。
       - エイリアスの更新時に新しいエイリアスを作成する
         このオプションを選択すると、BI プラットフォームにマップされた各 AD ユーザに対して、新しいエイリアスを自動的に作成します。新しい AD アカウントが BI プラットフォームアカウントを持たないユーザに対して作成されます。または [新しい *AD* エイリアスごとに新しいユーザアカウントを作成する] を選択し、[更新] をクリックした場合は、新しい AD アカウントがすべてのユーザに対して作成されます。
       - ユーザのログオン時にのみ新しいエイリアスを作成する
         マッピングしている AD ディレクトリに多くのユーザが含まれており、その一部のユーザだけが BI プラットフォームを使用する場合に、このオプションを選択します。BI プラットフォームは、すべてのユーザに対してエイリアスや Enterprise アカウントを自動で作成するわけではありません。代わりに、BI プラットフォームにログオンするユーザだけにエイリアスを (必要な場合は、アカウントも) 作成します。



c. [新しいユーザのオプション] エリアで、次の新しいユーザを作成するためのオプションを選択します。

- 新しいユーザを登録ユーザとして作成する
  登録ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。登録ユーザライセンスは特定のユーザに関連付けられており、ユーザはそのユーザ名およびパスワードに基づいて BI プラットフォームにアクセスすることができます。このため、登録ユーザは、システムに接続しているユーザの数に関係なく接続できます。このオプションを使用して作成したユーザアカウントに使用できる登録ユーザライセンスを持っている必要があります。

  > ⓘ 注記
  >
  > 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。
  >
  > ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。

- 新しいユーザを同時接続ユーザとして作成する
  同時接続ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。同時接続ライセンスでは BI プラットフォームに同時接続できるユーザ数が指定されます。この種類のライセンスは、少ないユーザ数の同時接続ライセンスで多数のユーザをサポートできるため、柔軟性に優れています。たとえば、ユーザがシステムにアクセスする頻度と時間の長さによって、100 ユーザ同時接続ライセンスで 250、500、または 700 のユーザをサポートできます。

17. AD エイリアスの更新のスケジュール方法を設定するには、[スケジュール] をクリックします。
    a. [スケジュール] ダイアログボックスで、[オブジェクトの実行] リストから繰り返しを選択します。
    b. 必要に応じて、その他のスケジュールオプションやパラメータを設定します。
    c. [スケジュール] をクリックします。
    エイリアスの更新が行われると、グループ情報も更新されます。
18. [属性バインディングオプション] エリアで、AD プラグインの属性バインディングの優先順位を指定します。
    a. [フルネーム、電子メールアドレス、およびその他の属性のインポート] チェックボックスを選択します。
    AD アカウントで使用するフルネームと説明がインポートされ、ユーザオブジェクトとともに BI プラットフォームに格納されます。

b. [別の属性バインディングに関連する *AD* 属性バインディングの優先順位を設定する] のオプションを指定します。

オプションが 1 に設定されていると、AD およびその他のプラグイン (LDAP および SAP) が有効な場合、AD 属性が優先されます。オプションが「3」に設定されている場合は、その他の有効化プラグインの属性が優先されます。バインディングは、異なる値に設定する必要があります。複数の認証プラグインを同じバインディング値に設定すると、予期しない結果が発生します。

19. [*AD* グループオプション] エリアで、AD グループの更新について設定します。
    a. [スケジュール] をクリックします。
    スケジュールダイアログボックスが表示されます。
    b. [オブジェクトの実行] リストから繰り返しを選択します。
    c. 必要に応じて、その他のスケジュールオプションやパラメータを設定します。
    d. [スケジュール] をクリックします。

    更新がスケジュールされ、指定したスケジュールに従って実行されます。AD グループアカウントに対して次にスケジュールされている更新は、[*AD* グループオプション] に表示されます。
20. [オンデマンド *AD* の更新] エリアで、次のオプションのいずれかを選択します。
    - *AD* グループを今すぐ更新する
      [更新] をクリックしたときに、すべてのスケジュールされている AD グループの更新を開始する場合は、このオプションを選択します。次にスケジュールされている AD グループの更新が [*AD* グループオプション] にリストされます。
    - *AD* グループとエイリアスを今すぐ更新する
      [更新] をクリックしたときに、すべてのスケジュールされている AD グループおよびユーザエイリアスの更新を開始する場合は、このオプションを選択します。次にスケジュールされている更新は、*AD* グループオプションおよび *AD* エイリアスのオプションにリストされます。
    - *AD* グループとエイリアスを今すぐ更新しない
      [更新] をクリックしても、AD グループまたはユーザエイリアスの更新は行われません。
21. [更新] をクリックし、[*OK*] をクリックします。

AD ユーザアカウントが実際にインポートされていることを検証するには、*CMC* > ユーザとグループ > グループ階層 に移動して、そのグループ内でユーザを表示するようにマップした AD グループを選択します。AD グループ内の現在のユーザおよびネストされたユーザが表示されます。

関連情報

Kerberos 設定ファイルを作成する [295 ページ]

9.4.3.3 Windows AD グループの更新のスケジュール

BI プラットフォームでは、管理者が AD グループとユーザエイリアスの更新をスケジュールできます。この機能は、AD 認証と Kerberos または NTLM を併用している場合に使用できます。CMC では、最後に更新が実行された日時を表示することもできます。

> ⓘ 注記
>
> BI プラットフォームで使用する AD 認証の場合、AD グループとエイリアスの更新をスケジュールする方法を設定する必要があります。

更新をスケジュールする場合、次の表に示した定期スケジュールパターンの中から選択することができます。

定期スケジュールパターン	説明
時間単位	更新は毎時間実行されます。開始時間、開始および終了日を指定します。
日単位	更新は毎日または指定した日数ごとに実行されます。実行時刻、開始日および終了日を指定することができます。
週単位	更新は毎週実行されます。1 週間に 1 回または数回実行することができます。実行する曜日、時間、開始および終了日を指定することができます。
月単位	更新は毎月または数カ月ごとに実行されます。実行時刻、開始日および終了日を指定することができます。
N 日	更新は毎月指定された日付に実行されます。実行する日にち、時間、開始および終了日を指定することができます。
第 1 月曜日	更新は毎月第 1 月曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
月末日	オブジェクトは毎月末日に実行されます。実行時刻、開始日および終了日を指定することができます。
第 N 週の X 日	更新は毎月特定の週の特定の曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
カレンダ	更新は、すでに作成されているカレンダで指定した日付に実行されます。

AD グループ更新のスケジュール

BI プラットフォームは、ユーザとグループの情報を AD に依存しています。AD に送信されるクエリの量を最小限にするために、AD プラグインはグループに関する情報、それらのグループとほかのグループとの関係およびユーザのメンバーシップに関する情報をキャッシュします。特定のスケジュールが定義されていない場合、更新は実行されません。

CMC を使用して、グループ更新の最新表示の定期スケジュールを設定する必要があります。これは、グループメンバーシップ情報が変更される頻度を考慮してスケジュールする必要があります。

AD ユーザエイリアスの更新のスケジュール

AD アカウントにユーザオブジェクトのエイリアスが作成されると、ユーザは AD 認証情報を使用して BI プラットフォームにログオンすることができます。AD アカウントの更新は、AD プラグインによって BI プラットフォームに反映されます。AD 内で作成、削除、無効化されたアカウントは、それに対応して、BI プラットフォームで作成、削除、または無効化されます。

AD エイリアスの更新をスケジュールしない場合、更新は次の場合にのみ行われます。

- ユーザがログオンします。
- 管理者は、CMC の [オンデマンド *AD* の更新] エリアで [*AD* グループとエイリアスを今すぐ更新する] オプションを選択します。

> ⓘ 注記
>
> どの AD パスワードもユーザエイリアスに保存されません。

9.4.4 SIA 実行のための BI プラットフォームサービスの設定

9.4.4.1 BI プラットフォームサービスアカウントでの SIA の実行

BI プラットフォーム用の AD Kerberos 認証をサポートするには、サービスアカウントに、オペレーティングシステムの一部として機能する権限を付与する必要があります。Central Management Server (CMS) で、Server Intelligence Agent (SIA) を実行している各マシンに、この手順を実行する必要があります。

サービスアカウントで SIA を実行または開始できるようにするには、この節で説明している特定のオペレーティングシステムの設定を行う必要があります。

> ⓘ 注記
>
> データベースにシングルサインオンする必要がある場合は、SIA に次のサーバを含める必要があります。
>
> - Crystal Reports Processing Server
> - Report Application Server
> - Web Intelligence Processing Server

9.4.4.2 サービスアカウントで実行されるように SIA を設定する

BI プラットフォームのサービスアカウントで実行されるように SIA アカウントを構成する前に、次の要件のアクションを完了する必要があります。

- サービスアカウントを BI プラットフォームのドメインコントローラで作成しておきます。
- 必要なサービスプリンシパル名 (SPN) が、サービスアカウントに追加されていることを確認しておきます。
- AD ユーザグループを BI プラットフォームに正常にマップしておきます。

ユーザに特定のアクセス権を付与する場合は、以下の手順を実行します。

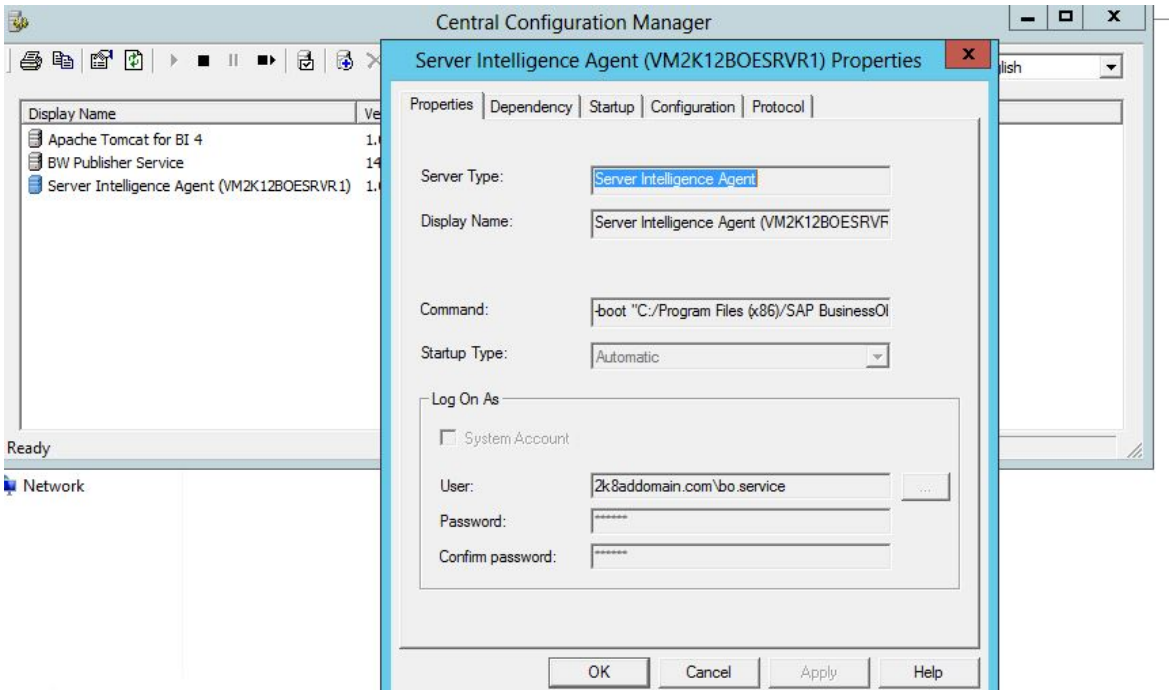
1. *[スタート]>[コントロールパネル]>[管理ツール]>[ローカルセキュリティポリシー]*の順にクリックします。
2. [ローカルポリシー]を展開し、[ユーザ権限の割り当て]をクリックします。
3. *[オペレーティングシステムの一部として機能する]*をダブルクリックします。
4. [追加] をクリックし、作成したサービスアカウントの名前を入力して、[*OK*] をクリックします。

サービスアカウントによって使用されるサービスを実行するすべての Server Intelligence Agent (SIA) で、このタスクを実行します。

1. CCM を起動するには、[プログラム] > [*SAP Business Intelligence*] > [*SAP BusinessObjects BI プラットフォーム 4*] > [セントラル設定マネージャ] を選択します。
   CCM ホームページが開きます。
2. CCM で Server Intelligence Agent (SIA) を右クリックし、[停止] を選択します。

> **注記**
>
> SIA を停止すると、SIA が管理していたすべてのサービスが停止されます。

3. SIA を右クリックして、[プロパティ] を選択します。



4. [システムアカウント] チェックボックスをオフにします。
5. サービスアカウントの認証情報 (`<DOMAINNAME>¥<service name>`) を入力して、[*OK*] をクリックします。

   サービスアカウントには、SIA を実行中のマシンで次の権限が与えられている必要があります。

   - アカウントは、特に“オペレーティングシステムの一部として機能”の権限を持つ必要があります。
   - アカウントは、特に“サービスとしてログオンする”権限を持つ必要があります。
   - BI プラットフォームのインストールフォルダに対するフルコントロール権限。
   - システムレジストリ内の “HKEY_LOCAL_MACHINE¥SOFTWARE¥SAP BusinessObjects” に対するフルコントロール権限。
6. BI プラットフォームサーバを実行する各マシンについて、上記の手順を繰り返します。

> **注記**
>
> [オペレーティングシステムの一部として機能]を選択した後で、実効アクセス権を確認します。通常は、この状態にするためにはサーバを再起動する必要があります。サーバを再起動した後でもこのオプションがオンにならない場合は、[ローカルポリシー]の設定が[ドメインポリシー]の設定によって上書きされています。

7. SIA を再起動します。

8. 必要な場合は、設定する必要があるサービスを実行している各 SIA に対して、手順 1 から 5 までを繰り返します。

AD 認証情報を使用して、CCM にログインできるようになります。

9.4.4.3 CCM で AD 認証情報をテストする

このタスクを実行するには、AD ユーザグループが BI プラットフォームに正常にマップされている必要があります。

1. CCM を開いて、[サーバの管理] アイコンをクリックします。
2. 正しい情報が [システム] フィールドに表示されていることを確認します。
3. 認証オプションのリストから [*Windows AD*] を選択します。
   [ログイン] ダイアログボックスが表示されます。
4. BI プラットフォームにマップされた AD グループから既存の AD アカウントを使用してログオンします。

> ⓘ 注記
>
> デフォルトドメインに存在しない AD アカウントを使用している場合、`domain¥username` としてログインします。

エラーメッセージは表示されません。ユーザは、次の節に進む前に、マップされた AD アカウントを使用する CCM を経由してログインできる必要があります。

> → ヒント
>
> エラーメッセージが表示された場合、▶ *CMC* ▶ 認証 ▶ *Windows AD* ▶ に移動します。[認証のオプション] で、[*Kerberos* 認証を使用する] を [*NTLM* 認証を使用する] に変更し、[更新] をクリックします。上記の手順 1 ～ 4 を繰り返します。これが動作する場合は、Kerberos 設定に問題があります。

9.4.5 AD 認証用の Web アプリケーションサーバの設定

9.4.5.1 Windows AD 認証 (Kerberos) のアプリケーションサーバの準備

Web アプリケーションサーバに Kerberos を設定するプロセスは、指定するアプリケーションサーバに応じて変わります。ただし、Kerberos を設定する一般的なプロセスは、以下の手順になります。

- Kerberos 設定ファイル (`krb5.ini`) の作成。
- JAAS ログイン設定ファイル (`bscLogin.conf`) の作成。

> ⓘ 注記
>
> この手順は、SAP NetWeaver 7.3 Java アプリケーションサーバでは必要ありません。ただし、SAP NetWeaver サーバに LoginModule を追加する必要があります。

- アプリケーションサーバの Java オプションの変更。
- Windows AD 認証用に `BOE.war` ファイルプロパティの上書き。
- Java アプリケーションサーバの再起動。

この節では、次のアプリケーションサーバで使用する Kerberos の設定の詳細について説明します。

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.3

9.4.5.1.1 Kerberos の設定ファイルの作成

9.4.5.1.1.1 Kerberos 設定ファイルを作成する

続行する前に、前提条件となる次のタスクを実行してください。

- サービスアカウントを BI プラットフォームのドメインコントローラで作成しておきます。
- サービスプリンシパル名 (SPN) が、サービスアカウントに追加されていることを確認しておきます。
- AD ユーザグループを BI プラットフォームに正常にマップしておきます。
- CCM で AD 認証情報をテストしておきます。

BI プラットフォームデプロイメントの Web アプリケーションサーバとして、SAP NetWeaver 7.3、Tomcat、Oracle Application Server、WebSphere、または WebLogic を使用している場合は、以下の手順を使用して Kerberos の設定ファイルを作成します。

1. `krb5.ini` ファイルが存在しない場合はこのファイルを作成し、Windows の場合は `C:¥Windows` に保存します。

   > **注記**
   >
   > アプリケーションサーバが Unix にインストールされている場合は、次のディレクトリを使用する必要があります。
   >
   > Solaris: `/etc/krb5/krb5.conf`
   >
   > Linux: `/etc/krb5.conf`

   > **注記**
   >
   > このファイルは別の場所に保存することができます。ただし、Java のオプションでその場所を指定する必要があります。`krb5.ini` の詳細については、http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view を参照してください。

2. Kerberos の設定ファイルに以下の必須情報を追加します。

```
[libdefaults]
default_realm = DOMAIN.COM
```

```
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

ⓘ 注記

重要なパラメータについて、次の表で説明します。

DOMAIN.COM	ドメインの DNS 名で、FQDN 形式で大文字で入力する必要があります。
kdc	ドメインコントローラのホスト名です。
[capath]	別の AD フォレスト内にあるドメイン間の信頼関係を定義します。前述の例では、DOMAIN2.COM が外部フォレスト内のドメインとなり、DOMAIN.COM に対する直接的な双方向の推移的な信頼関係を持っています。
default_realm	複数ドメインの設定では、 [libdefaults] の下の default_realm の値は、任意のソースドメインです。ベストプラクティスとしては、AD アカウントで認証するユーザ数が最大のドメインを使用します。UPN 接尾語がログオン時に指定されなかった場合、デフォルトでは、default_realm の値が使用されます。この値は、CMC の [デフォルトドメイン] 設定と一致している必要があります。すべてのドメインは、上記の例に示すとおり、大文字で指定する必要があります。

9.4.5.1.2 JAAS ログイン設定ファイルの作成

9.4.5.1.2.1 Tomcat または WebLogic の JAAS ログイン設定ファイルを作成する

bscLogin.conf ファイルは、Java ログインモジュールをロードするために使用され、Java Web アプリケーションサーバでの AD Kerberos に必要です。

ファイルのデフォルトの保存場所は、次のとおりです。C:¥Windows

1. bscLogin.conf というファイルが存在しない場合は作成し、C:¥Windows に保存します。

   > ⓘ 注記
   >
   > このファイルは別の場所に保存することができます。ただし、このファイルを別の場所に保存する場合は、Java のオプションでその場所を指定する必要があります。

2. JAAS の bscLogin.conf 設定ファイルに以下のコードを追加します。

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. ファイルを保存して閉じます。

9.4.5.1.2.2 Oracle JAAS ログイン設定ファイルを作成する

1. jazn-data.xml ファイルを検索します。

   > ⓘ 注記
   >
   > このファイルのデフォルトの保存場所は、C:¥OraHome_1¥j2ee¥home¥config です。Oracle Application Server を別の場所にインストールしている場合は、インストールしたシステムでこのファイルを検索します。

2. <jazn-loginconfig> タグの間に、以下の内容を追加します。

```
<application>
<name>com.businessobjects.security.jgss.initiate</name>
<login-modules>
<login-module>
<class>com.sun.security.auth.module.Krb5LoginModule</class>
<control-flag>required</control-flag>
</login-module>
</login-modules>
</application>
```

3. jazn-data.xml ファイルを保存して閉じます。

9.4.5.1.2.3 Websphere JAAS ログイン設定ファイルを作成する

1. bscLogin.conf というファイルが存在しない場合は作成し、デフォルトの保存場所 (C:¥Windows) に保存します。
2. bscLogin.conf 設定ファイルに次のコードを追加します。

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

3. ファイルを保存して閉じます。

9.4.5.1.2.4 SAP NetWeaver AS に LoginModule を追加する

Kerberos と SAP NetWeaver AS 7.3 を使用するには、Tomcat Web アプリケーションサーバを使用しているかのようにシステムを設定します。 `bscLogin.conf` ファイルを作成する必要はありません。

一度この操作を行うと、LoginModule を追加して、SAP NetWeaver AS 7.3 の一部の Java 設定を更新する必要が生じます。

`com.sun.security.auth.module.Krb5LoginModule` を `com.businessobjects.security.jgss.initiate` にマップするには、SAP NetWeaver AS 7.3 に LoginModule を手動で追加する必要があります。

1. Web ブラウザに `http://<machine name>:<port>/nwa` を入力して、SAP NetWeaver Administrator を開きます。
2. *Configuration Management* > *Security* > *Authentication* > *Login Modules* > *Edit* をクリックします。
3. 新しいログインモジュールを次の情報とともに追加します。

表示名	**`Krb5LoginModule`**
クラス名	**`com.sun.security.auth.module.Krb5LoginModule`**

4. 保存をクリックします。
   SAP NetWeaver で新しいモジュールが作成されます。
5. コンポーネント > 編集 の順にクリックします。
6. **`com.businessobjects.security.jgss.initiate`** という新しいポリシーを追加します。
7. *Authentication Stack* で、手順 3 で作成したログインモジュールを追加し、*Required* に設定します。
8. *Options for Selected Login Module* に他のエントリがないことを確認します。 ある場合は、それらを削除します。
9. 保存をクリックします。
10. SAP NetWeaver Administrator からログアウトします。

9.4.5.1.3 設定ファイルをロードするためのアプリケーションサーバ Java 設定の変更

9.4.5.1.3.1 Tomcat 上での Kerberos の Java オプションを変更する

1. *[スタート]*メニューから、*[プログラム]>[Tomcat]>[Tomcat の設定]*の順にクリックします。
2. *[Java]*タブをクリックします。
3. 次のオプションを追加します。

```
-Djava.security.auth.login.config=C:¥XXXX¥bscLogin.conf
-Djava.security.krb5.conf=C:¥XXXX¥krb5.ini
```

   XXXX は、`bscLogin.conf` ファイルの保存場所に置き換えます。

4. Tomcat 設定ファイルを閉じます。
5. Tomcat を再起動します。

9.4.5.1.3.2 SAP NetWeaver AS 7.3 の Java オプションを変更する

1. Java Configuration Tool (デフォルトでは、`C:¥usr¥sap¥<NetWeaver ID>¥<instance>¥j2ee¥configtool¥` にあります) に移動して、`configtool.bat` をダブルクリックします。
   Configuration Tool が開きます。
2. *View* > *Expert Mode* をクリックします。
3. *Cluster-Data* > *Template* を展開します。
4. SAP NetWeaver AS に対応するインスタンス (例: *Instance* - `<system ID><machine name>`) を選択します。
5. [*VM Parameters*] をクリックします。
6. [ベンダ] リストから [*SAP*] を、[プラットフォーム] リストから [*GLOBAL*] を選択します。
7. [*System*] をクリックし、次のカスタムパラメータ情報を追加します。

java.security.krb5.conf	`<ファイル名を含む krb5.ini ファイルへのパス>`
javax.security.auth.useSubjectCredsOnly	false

8. [*Save*] をクリックし、次に [*Configuration Editor*] をクリックします。
9. 設定 > セキュリティ > 設定 > *com.businessobjects.security.jgss.initiate* > セキュリティ > 認証 の順にクリックします。
10. [*Edit Mode*] をクリックします。
11. [認証] ノードを右クリックして、[サブノードの作成] を選択します。
12. 上部のリストから [*Value-Entry*] を選択します。
13. 次を入力します。

名前	create_security_session
値	false

14. [*Create*] をクリックし、ウィンドウを閉じます。
15. [*Config Tool*] をクリックし、次に [*Save*] をクリックします。

設定を更新した場合は、SAP NetWeaver AS を再起動する必要があります。

9.4.5.1.3.3 WebLogic 上での Kerberos の Java オプションを変更する

WebLogic で Kerberos を使用している場合、Java オプションを変更して Kerberos 設定ファイルと Kerberos ログインモジュールの場所を指定する必要があります。

1. BI プラットフォームアプリケーションを実行している WebLogic のドメインを停止します。
2. BI プラットフォームアプリケーションを実行している WebLogic のドメインを開始するスクリプト (Windows の場合は `startWeblogic.cmd`、Unix の場合は `startWebLogic.sh`) を開きます。
3. 次の情報を、ファイルの Java_Options セクションに追加します。

   ```
   set JAVA_OPTIONS=-Djava.security.auth.login.config=C:/XXXX/bscLogin.conf
   -Djava.security.krb5.conf=C:/XXX/krb5.ini
   ```

   XXXX は、ファイルの保存場所に置き換えます。
4. BI プラットフォームアプリケーションを実行している WebLogic のドメインを再起動します。

9.4.5.1.3.4 WebSphere 上での Kerberos の Java オプションを変更する

1. WebSphere の管理コンソールにログオンします。

   IBM WebSphere 5.1 の場合は、「`http://servername:9090/admin`」と入力します。IBM WebSphere 6.0 の場合は、「`http://servername:9060/ibm/console`」と入力します。
2. [サーバ] を展開し、[アプリケーションサーバ] をクリックして、BI プラットフォームを使用して作成したアプリケーションサーバの名前をクリックします。
3. *JVM* ページに移動します。

   WebSphere 5.1 を使用している場合、*JVM* ページに移動するには次の手順を実行します。
   1. [サーバ]ページで、[追加プロパティ]列に[プロセス定義]が表示されるまで下にスクロールします。
   2. *[プロセス定義]*をクリックします。
   3. 下にスクロールして*[Java Virtual Machine]*をクリックします。

   WebSphere 6.0 を使用している場合、*JVM* ページに移動するには次の手順を実行します。
   1. サーバページで*[Java およびプロセス管理]*をクリックします。
   2. *[プロセス定義]*をクリックします。
   3. *[Java 仮想マシン]*をクリックします。
4. [汎用 *JVM* 引数] をクリックした後、`Krb5.ini` と `bscLogin.conf` ファイルの場所を次のように指定します。

   -Djava.security.auth.login.config=C:¥XXXX¥bscLogin.conf

   -Djava.security.krb5.conf=C:¥XXXX¥krb5.ini

   XXXX は、ファイルの保存場所に置き換えます。
5. *[適用]*をクリックして、*[保存]*をクリックします。
6. サーバを停止して再起動します。

9.4.5.1.4 Java が Kerberos チケットを受け取れることを確認する

Java が Kerberos チケットを受け取れるかどうかをテストする前に、次の要件のアクションを完了する必要があります。

- アプリケーションサーバ用に `bscLogin.conf` ファイルを作成します。
- `krb5.ini` ファイルを作成します。

1. コマンドプロンプトを開き、BI プラットフォームインストールの `jdk¥bin` ディレクトリに移動します。

   デフォルトでは、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥jdk¥bin` にあります。
2. `kinit <ユーザ名>` を実行します。
3. Press `Enter`.
4. パスワードを入力します。

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\win64_x64\jdk\bin>kinit sfredell
Password for sfredell@VTIAUTH08.COM: password
New ticket is stored in cache file C:\Users\Administrator\krb5cc_Administrator
```

   `krb5.ini` ファイルが正しく設定されている場合、Java ログインモジュールがロードされ、次のようなメッセージが表示されます。

   新しいチケットがキャッシュファイル `C:¥Users¥Administrator¥krb5cc_Administrator` に保存されました。

Kerberos チケットを正常に受け取れるまで、AD セットアップを続行しないでください。

チケットを受け取れない場合は、次のオプションを検討してください。

- この章の最後のトラブルシューティングの節を参照してください。
- KDC、Kerberos の設定ファイル、およびユーザ認証情報が Kerberos のデータベースで使用できないことに関する問題については、SAP Knowledge Base の記事 KBA 1476374 および KBA 1245178 を参照してください。

9.4.5.1.5 BI 起動パッドを手動 AD ログイン用に設定する

BI プラットフォームアプリケーションを手動 AD ログイン用に設定する前に、前提条件となる次のアクションを完了する必要があります。

- サービスアカウントを BI プラットフォームのドメインコントローラで作成しておきます。
- HTTP サービスプリンシパル名 (SPN) が、サービスアカウントに追加されていることを確認しておきます。
- AD ユーザグループを BI プラットフォームに正常にマップしておきます。
- CCM で AD 認証情報をテストしておきます。
- Web アプリケーションサーバで必要な設定ファイルを作成し、設定およびテストをしておきます。
- 設定ファイルをロードするように、アプリケーションサーバの Java 設定を変更しておきます。

BI 起動パッドの Windows AD 認証オプションを有効化するには、次の手順を実行します。

1. 以下に示す、Web アプリケーションサーバをホストするマシン上の BOE Web アプリケーションのカスタムフォルダにアクセスします。

   `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥`

   変更は、`config¥custom` ディレクトリで行ってください。`config¥default` ディレクトリではありません。そうしないと、将来、パッチをデプロイメントに適用する際に、変更が上書きされます。

   後で、変更した BOE Web アプリケーションを再デプロイする必要があります。
2. 新しいファイルを作成します。

   > **注記**
   >
   > メモ帳などのテキスト編集ユーティリティを使用します。
3. ファイルを `BIlaunchpad.properties` という名前で保存します。
4. 次の情報を入力します。

   ```
   authentication.visible=true
   authentication.default=secWinAD
   ```
5. ファイルを保存して閉じます。
6. Web アプリケーションサーバを再起動します。

これで、手動で BI ラウンチパッドにログインし、いずれかのアプリケーションにアクセスして、認証オプションの一覧から Windows AD を選択できます。

> **注記**
>
> 既存の AD アカウントを使用して、BI 起動パッドに手動でログインできるようになるまで、Windows AD の設定を継続しないでください。

これらの新しいプロパティが有効になるのは、BOE Web アプリケーションが Web アプリケーションサーバを実行しているマシン上に再デプロイされてからです。WDeploy を使用して、Web アプリケーションサーバに BOE を再デプロイします。Wdeploy を使用して Web アプリケーションをアンデプロイする際の詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

> **注記**
>
> デプロイメントでファイアウォールを使用する場合は、必ずすべての必要なポートを開きます。そうしない場合、Web アプリケーションは BI プラットフォームサーバに接続できません。

9.4.6 シングルサインオンの設定

9.4.6.1 AD 認証を使用した BI プラットフォームへの SSO

Windows AD を使用する SSO のオプション

BI プラットフォームで Windows AD 認証のシングルサインオン (SSO) を設定するためにサポートされている方法は、次の 3 つがあります。

- Vintela - このオプションは Kerberos でのみ使用できます。
- SiteMinder - このオプションは Kerberos でのみ使用できます。

データベースへの SSO

データベースへの SSO によって、ログオンしたユーザは、ログオン情報を再度入力しなくてもデータベースアクセスに必要なアクション、特にレポートの表示や最新表示を行うことができます。制限された委任は、AD 認証および Vintela SSO のオプションですが、これは、システムデータベースにシングルサインオンするデプロイメントシナリオで必要です。

エンドツーエンド SSO

BI プラットフォームでは、エンドツーエンド SSO は、Windows AD と Kerberos を通じてサポートされます。このシナリオでは、ユーザが、フロントエンドにある BI プラットフォームへのシングルサインオンアクセス権と、バックエンドにあるデータベースへの SSO アクセス権の両方を持っています。したがって、ユーザはオペレーティングシステムへのログオン時にログオン情報を一度入力するだけで、BI プラットフォームへのアクセス権を持つことができ、さらにデータベースアクセスに必要なレポートの表示などのアクションを実行することができます。

手動および SSO AD 認証設定の比較

BI ラウンチパッドに手動でログインするために AD 認証を有効にできるように、デプロイメントを正常に設定した後で、特定の SSO 要件を有効にするために AD 認証設定を見直す必要があります。要件は、SSO メソッドの選択によって変わります。

9.4.6.2 Vintela SSO の使用

9.4.6.2.1 Vintela SSO 設定のためのチェックリスト

Vintela SSO に対応するように BI プラットフォームを設定するには、次のタスクを完了する必要があります。

1. Vintela SSO 用のサービスアカウントを特別に設定する。
2. 制限された委任を設定する (オプション)。
3. CMC で Windows AD SSO 認証オプションを設定する。
4. 一般プロパティおよび BI ラウンチパッド固有のプロパティを Vintela SSO 用に設定する。
5. Tomcat を Web アプリケーションサーバとしてデプロイメントに使用している場合、ヘッダのサイズ制限を増やす必要があります。
6. Vintela 用にインターネットブラウザを設定する。

9.4.6.2.2 Vintela SSO のサービスアカウントを設定する

`Ktpass` コマンドラインツールでは、Active Directory でホストまたはサービスに対するサーバプリンシパル名を設定し、サービスアカウントの共有シークレットキーを含む Kerberos "keytab" ファイルを生成します。 このツールは、通常、ドメインコントローラ上にあるか、Microsoft のサポートサイト (http://support.microsoft.com/kb/892777) からダウンロードします。

指定した Windows AD グループのユーザが、AD 認証を使用して BI 起動パッドに自動的に認証されるように、サービスアカウントを特別に設定する必要があります。 ドメインコントローラで AD Kerberos 認証用に作成されたサービスアカウントを設定できます。

クライアントが BI ラウンチパッドにログインを試みると、Kerberos チケット生成サーバへのリクエストが開始されます。 このリクエストを円滑に行うには、BI プラットフォーム用に作成されたサービスアカウントが、アプリケーションサーバの URL と一致する SPN を持っている必要があります。 ドメインコントローラをホストするマシン上で、次の手順を実行します。

1. Kerberos Keytab 設定コマンドの `ktpass` を実行して、`keytab` ファイルを作成して設定します。

   次の表に示す `ktpass` パラメータを指定します。

パラメータ	説明
`-out`	生成する Kerberos `Keytab` ファイルの名前を指定します。

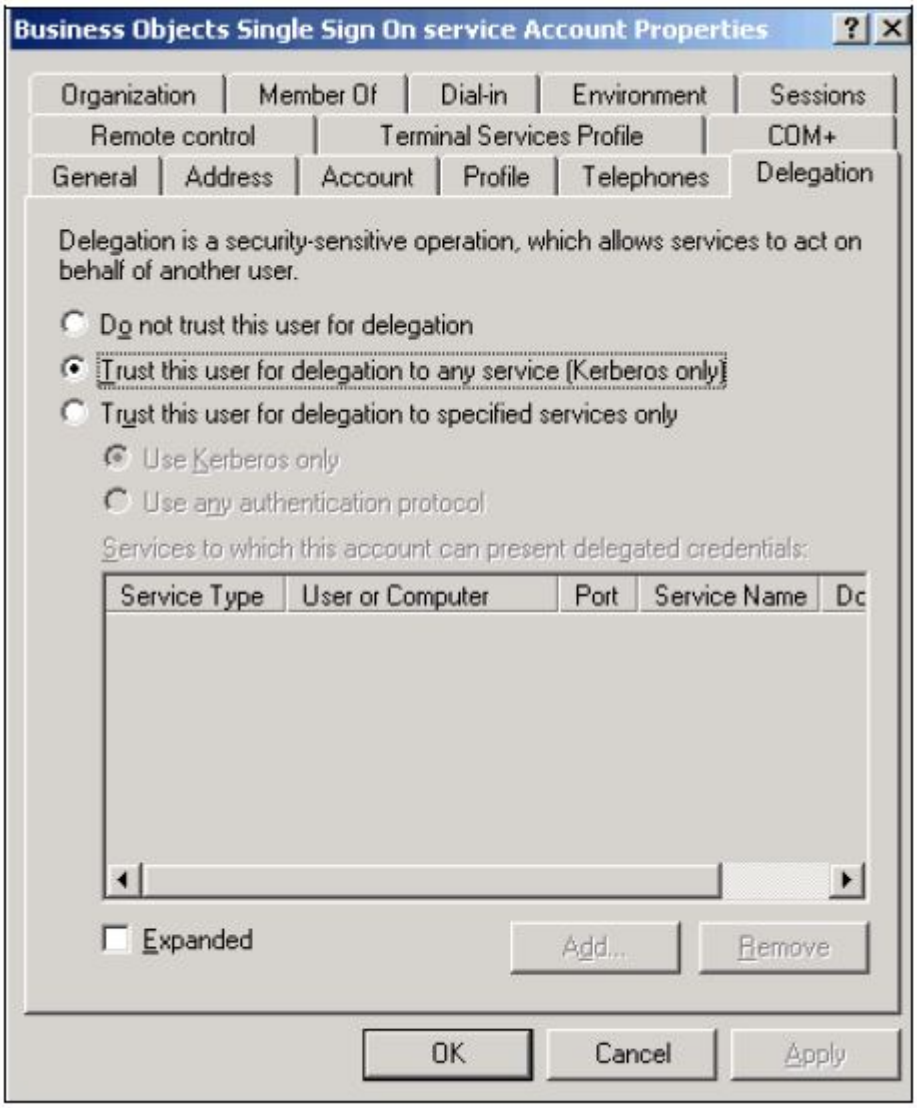
パラメータ	説明
-princ	サービスアカウントに使用されるプリンシパル名を、`< MYSIAMYSERVER>/<sbo.service.domain.com>@<DOMAIN>.COM` の SPN 形式で指定します。ここで、`<MYSIAMYSERVER>` は、セントラル設定マネージャ (CCM) で指定されている Service Intelligence Agent の名前です。 **注記** サービスアカウントの名前は大文字と小文字が区別されます。 SPN には、サービスインスタンスが実行されるホストコンピュータの名前を含めます。 **ヒント** SPN は、登録先のフォレストで一意であることが必要です。 確認するには、Windows サポートツール `Ldp.exe` を使用して SPN を検索します。
-pass	サービスアカウントが使用するパスワードを指定します。
-ptype	主体の種類を指定します。 `-ptype KRB5_NT_PRINCIPAL`
-crypto	サービスアカウントに使用する暗号の種類を指定します。 `-crypto RC4-HMAC-NT`

例:

```
ktpass -out <keytab_filename>.keytab -princ <MYSIAMYSERVER>/
sbo.service.domain.com@DOMAIN.COM
-pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

`ktpass` コマンドの出力で、目標のドメインコントローラと、共有シークレットを含む Kerberos `keytab` ファイルが作成されたことを確認する必要があります。 また、このコマンドで、プリンシパル名が (ローカル) サービスアカウントにマップされます。

2. サービスアカウントを右クリックして、プロパティ > 委任 を選択します。
3. [任意のサービスへの委任でこのユーザを信頼する *(Kerberos のみ)*] をクリックします。



4. [*OK*] をクリックして、設定を保存します。

これで、サービスアカウントには、すべての必要な Vintela SSO 用のサービスプリンシパル名があり、サービスアカウントの暗号化されたパスワードを使用して、keytab ファイルが生成されます。

> ⓘ 注記
>
> エンドツーエンドのシングルサインオンまたは keytab ファイルシナリオを使用したデータベースへのシングルサインオンの場合:
>
> keytab 内の KVNO を変更することによりエラーが解決された場合は、サービスアカウントの KVNO 属性が、keytab の作成で使用された KVNO よりも高い番号である可能性があります。 正しい KV 番号の取得方法については、http://service.sap.com/sap/support/notes/1853668 を参照してください。

9.4.6.2.2.1 Vintela SSO の制限された委任を設定する

制限された委任は、Vintela SSO を設定するためのオプションです。ただし、これはシステムデータベースへの SSO を必要とするデプロイメントで必須です。

1. AD ドメインコントローラマシンで、Active Directory [ユーザーとコンピューター] スナップインを開きます。
2. 前の節で作成したサービスアカウントを右クリックして、プロパティ > 委任 をクリックします。
3. [指定されたサービスへの委任でのみこのユーザを信頼する] を選択します。
4. [*Kerberos のみを使う*] を選択します。
5. 追加 > ユーザまたはコンピューター をクリックします。
6. サービスアカウント名を入力し、[*OK*] をクリックします。
   サービスの一覧が表示されます。
7. 次のサービスを選択してから、[*OK*] をクリックします。
   - HTTP サービス
   - BI プラットフォームをホストするマシンで Service Intelligence Agent (SIA) を実行するのに使用されるサービス

   これらのサービスが、サービスアカウントに委任できるサービスの一覧に追加されます。

Web アプリケーションプロパティを、変更対象のアカウントに変更する必要があります。

9.4.6.2.3 CMC で SSO を設定する

1. CMC の[認証]管理エリアを表示します。
2. [*Windows AD*]をダブルクリックします。
3. [*Windows Active Directory (AD) を有効にする*] チェックボックスがオンになっていることを確認します。
4. [認証のオプション] エリアで [*Kerberos 認証を使用する*] オプションを選択します。
5. データベースへの SSO を設定する場合、[セキュリティコンテキストをキャッシュする] を選択します。
6. [選択した認証モードでのシングルサインオン *(SSO)* を有効にする] を選択します。
7. [更新] をクリックします。

9.4.6.2.4 BI 起動パッドおよび OpenDocument で Vintela シングルサインオンを有効にする

この手順は、BI 起動パッドまたは OpenDocument のいずれかで使用されます。BI プラットフォーム Web アプリケーションへの SSO を有効にするには、Vintela および SSO 固有のプロパティを `BOE.war` ファイルに指定する必要があります。SSO を設定する目的では、その他のアプリケーションの操作以前に、AD アカウント用に BI ラウンチパッドへの SSO を有効化することに注力することをお勧めします。

1. 以下に示す、Web アプリケーションサーバをホストするマシン上の BOE Web アプリケーションのカスタムフォルダにアクセスします。

   ```
   <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥
   ```

変更は、`config¥custom` ディレクトリで行ってください。`config¥default` ディレクトリではありません。そうしないと、将来、パッチをデプロイメントに適用する際に、変更が上書きされます。

後で、変更した BOE Web アプリケーションを再デプロイする必要があります。

2. テキストエディタで新しいファイルを作成します。
3. 次を入力します。

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=DOMAIN.COM
idm.princ=MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.keytab=C:/WIN/filename.keytab
idm.logger.props=error-log.properties
```

> ⓘ 注記
>
> `idm.realm` パラメータと `idm.princ` パラメータには有効な値を設定する必要があります。`idm.realm` は、`krb5.ini` ファイルの `default_realm` を設定したときの設定値と同じになります。値には大文字を使用します。`idm.princ` パラメータは、Vintela SSO 用に作成したサービスアカウントで使用される SPN です。

> ⓘ 注記
>
> キータブファイルの場所を指定するときはスラッシュを使用する必要があります。

Windows AD 認証および Vintela SSO の制限された委任を使用しない場合は、次の手順をスキップします。

4. 制限された委任を使用するには、次を追加します。

```
idm.allowS4U=true
```

5. `global.properties` という名前でファイルを保存し、ファイルを閉じます。

> ⓘ 注記
>
> ファイル名に `.txt` のような拡張子を付けて保存しないように注意してください。

6. 同じディレクトリで別のファイルを作成します。必要に応じて、`OpenDocument.properties` または `BILaunchPad.properties` と名前を付けてファイルを保存します。
7. 次の情報を入力します。

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

例:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

8. ファイルを保存して閉じます。
9. Web アプリケーションサーバを再起動します。

これらの新しいプロパティが有効になるのは、BOE Web アプリケーションが Web アプリケーションサーバを実行しているマシン上に再デプロイされてからです。WDeploy を使用して、Web アプリケーションサーバに BOE

を再デプロイします。Wdeploy を使用して Web アプリケーションをアンデプロイする際の詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

> ⓘ 注記
>
> デプロイメントでファイアウォールを使用する場合は、必ずすべての必要なポートを開きます。そうしない場合、Web アプリケーションは BI プラットフォームサーバに接続できません。

9.4.6.2.5 Web サービスで Vintela シングルサインオンを有効化する

一部のクライアントツールでは、Web サービス経由での認証が必要です。Web サービスでシングルサインオン (SSO) を有効化するには、これらの手順に従います。詳細については、次の関連 SAP ノートを参照してください。 http://service.sap.com/sap/support/notes/1646920

1. ファイル`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥web.xml` をバックアップしてから、開いて編集します。
2. Kerberos Proxy Filter セクションおよび Kerberos Filter セクションをコメント解除し、Windows Active Directory (secWinAD) 認証の Kerberos SSO を有効化します。

```
-->
<!--          top of filter
<filter>
    <filter-name>KerberosFilter</fil
    <filter-class>com.businessobject

    <init-param>
        <param-name>idm.realm</param
        <param-value></param-value>

    <init-param>
        <param-name>idm.
        <param-value>cla
        <description>
            Configures 1
        </description>
    </init-param>
</filter>
-->          bottom of filter
```

```
                filter mapping
<!-- Kerberos Filter
  - This filter mapping must be uncommented to enable Kerberos SSO
  - See above for further instructions
-->
<!--
<filter-mapping>
    <filter-name>KerberosFilter</filter-name>
    <url-pattern>/services/Session</url-pattern>
</filter-mapping>
-->

<!-- Kerberos Filter (for legacy support)
  - This filter mapping must also be uncommented to enable Kerberos SSO for legacy consumers.
-->
<!--
<filter-mapping>
    <filter-name>KerberosFilter</filter-name>
    <url-pattern>/services/session</url-pattern>
</filter-mapping>
-->
```

以下のオプションを指定する必要があります (それ以外は任意です)。

- `idm.realm` (Krb5.ini ファイルで指定されている default_realm と同様)。
- `idm.princ` (`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にある global.properties ファイルの idm.princ で指定されているものと同様)。
- `idm.keytab` (`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にある global.properties ファイルの idm.keytab で指定されているものと同様)。

> ⓘ 注記
>
> ハードコードされたパスワード設定を Tomcat の Java オプションで使用している場合、`web.xml` ファイルの keytab 行を変更しないでください。

3. SSL が Java アプリケーションサーバで使用されていない場合、idm.allowUnsecured パラメータを **`true`** に設定します。

Tomcat SSL の詳細については、ナレッジベースの記事 ID:1484802 を参照してください。

4. ファイル`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥classes¥dsws.properties` をバックアップしてから、開いて編集します。
5. kerberos.sso を **`true`** に設定し、ファイルを保存します。

```
68  allowedOrderBy = SI_CREATION_TIME,SI_KIND,SI_LAST_RUN_TIME,SI_SCHEDULEINFO.SI_SUBMITTER,SI_OWNER
69
70  ##############################
71  # Kerberos SSO Properties #
72  ##############################
73  #Set this value to true and activate the Vintela Authentication Filter (in web.xml) to enable SSO via Kerberos
74  kerberos.sso=true
75
76  #Setting this value to true if user wants trusted authentication
77  trustedAuthentication.enabled = false
```

kerberos SSO setting

6. WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。

   WDeploy の使用については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。
7. Tomcat を再起動します。
8. 設定をテストするには、クライアントツールがインストールされているクライアントマシンで、Query as a Web Service Designer を起動します。
9. 新しいマネージドホストを追加します。
10. アプリケーションサーバ名を入力します。
11. Web サービス URL を次の書式で入力します。`http://<WebAppServer>:<portNumber>/dswsbobje/services/Session`

    例: `http://BI4:8080/dswsbobje/services/Session`
12. CMS ホスト名を入力します。
13. 認証の種類を *Windows AD* に変更します。
14. [*Windows Active Directory シングルサインオンを有効化*] を選択します。
15. ログインプロンプトで、[ユーザ] フィールドおよび [パスワード] フィールドを空白にしたまま、[*OK*] をクリックします。

9.4.6.2.6 RESTful Web サービスで Vintela シングルサインオンを有効化する

一部のクライアントツールでは、RESTful Web サービスによる認証が必要です。Web サービスでシングルサインオン (SSO) を有効化するには、これらの手順に従います。

1. ファイル `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥biprws.properties` を `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps ¥biprws¥WEB-INF¥config¥custom¥biprws.properties` にコピーした後、開いて編集します。
2. Windows Active Directory 用の Kerberos SSO (secWinAD) 認証を有効化するには、`sso.enabled` を `true` に設定します。次のスクリーンショットを参照してください。

```
# ---------------------------------------------------- SSO Related Default Global Core Web Properties ----------------------------------------------------
# Vintela single sign on properties
sso.enabled=
idm.realm=
idm.princ=
idm.keytab=
idm.allowUnsecured=
idm.allowNTLM=
idm.logger.name=
idm.logger.props=
```

以下の必須オプションを指定します。

- `idm.realm` (Krb5.ini ファイルで指定されている default_realm と同様)。
- `idm.princ` (`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にある global.properties ファイルの idm.princ で指定されているものと同様)。
- `idm.keytab` (`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にある global.properties ファイルの idm.keytab で指定されているものと同様)。
- パラメータ `idm.allowUnsecured` は、Java アプリケーションサーバで SSL が使用されていない場合は `true` に設定する必要があります。Tomcat SSL の詳細については、ナレッジベースの記事 *ID:1484802* を参照してください。

3. WDeploy を使用して、Web アプリケーションサーバに WAR ファイルを再デプロイします。WDeploy の使用については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。
4. Tomcat を再起動します。
5. クライアントマシンで設定をテストするには、任意のブラウザを開き、URL: http://<WebAppServer>:<portnumber>/biprws/v1/logon/adsso にアクセスします。
   REST トークンが API への応答として表示されます。

9.4.6.2.7 Tomcat のヘッダサイズ制限を増やす

Active Directory は Kerberos を作成し、これは認証プロセスで使用されます。このトークンは、HTTP ヘッダに格納されます。Java アプリケーションサーバにはデフォルトの HTTP ヘッダサイズがあります。失敗しないために、デフォルトサイズの 16384 バイト以上であることを確認します(デプロイメントによっては、より大きいサイズが必要になります。詳細については、Microsoft のサポートサイト(http://support.microsoft.com/kb/327825)のサイズ設定のガイドラインを参照してください)。

1. Tomcat がインストールされたサーバで、`server.xml` ファイルを開きます。

   Windows では、このファイルは `<TomcatINSTALLDIR>/conf` にあります。

   - Windows で、BI プラットフォームと一緒にインストールされた Tomcat のバージョンを使用しており、デフォルトのインストール場所を変更していない場合、`<TomcatINSTALLDIR>` を `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥` に置き換えます。
   - サポートされるその他の Web アプリケーションサーバを使用している場合は、その Web アプリケーションサーバのマニュアルを参照して、適切なパスかどうか確認してください。
2. 設定したポート番号に対応する `<Connector ...>` タグを見つけます。

   デフォルトポート 8080 を使用している場合は、port="8080" が含まれている `<Connector ...>` タグを見つけます。

   以下はその例です。

```
<Connector URIEncoding="UTF-8" acceptCount="100"
```

```
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="8080" redirectPort="8443"
/>
```

3. `<Connctor ...>` タグ内に、次の値を追加します。

   `maxHttpHeaderSize="16384"`

   以下はその例です。

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" port="8080"
redirectPort="8443" />
```

4. `server.xml` ファイルを保存して閉じます。
5. Tomcat を再起動します。

> **注記**
>
> 他の Java アプリケーションサーバに関しては、その Java アプリケーションサーバのマニュアルを参照してください。

9.4.6.2.8 インターネットブラウザの設定

AD Kerberos 認証用の Vintela SSO をサポートするには、BI プラットフォームクライアントを設定する必要があります。これは、クライアントマシンでの Web ブラウザの設定に関係します。

9.4.6.2.8.1 クライアントマシンの Internet Explorer を設定する

1. クライアントマシンで、IE ブラウザを開きます。
2. 統合 Windows 認証を有効にします。
   a. ［ツール］メニューの［インターネット オプション］をクリックします。
   b. *[詳細]*タブをクリックします。
   c. [セキュリティ]までスクロールし、[統合 *Windows* 認証を使用する]を選択して[適用]をクリックします。
3. Java アプリケーションマシンまたは URL を信頼されているサイトに追加します。サイトの完全なドメイン名を入力できます。
   a. ［ツール］メニューの［インターネット オプション］をクリックします。
   b. *[セキュリティ]* タブをクリックします。
   c. [サイト]をクリックして[詳細設定]をクリックします。
   d. サイトを選択または入力して、[追加] をクリックします。
   e. [*OK*]をクリックすると、[インターネットオプション]ダイアログボックスが閉じます。
4. Internet Explorer ブラウザウィンドウを閉じて再度開くと、これらの変更が有効になります。

5. ここまでの手順を BI プラットフォームクライアントマシンごとに繰り返します。

9.4.6.2.8.2 クライアントマシンに FireFox を設定する

1. *network.negotiate-auth.delegation-uris* を変更します。
   a. クライアントマシンで、Firefox ブラウザを開きます。
   b. URL アドレスフィールドに「**`about:config`**」と入力します。
      設定可能なプロパティの一覧が表示されます。
   c. *network.negotiate-auth.delegation-uris* をダブルクリックしてプロパティを編集します。
   d. BI 起動パッドへのアクセスに使用する URL を入力します。

      たとえば、BI 起動パッドの URL が **`http://<machine.domain.com>:8080/BOE/BI`** の場合は、「**`http://<machine.domain.com>`**」と入力する必要があります。

      > ⓘ 注記
      >
      > 複数の URL を追加するには、それらをカンマで区切ります。たとえば、「**`http://<machine.domain.com>,<machine2.domain.com>`**」と入力します。

   e. [*OK*]をクリックします。
2. *network.negotiate-auth.trusted-uris* を変更します。
   a. クライアントマシンで、Firefox ブラウザを開きます。
   b. URL アドレスフィールドに「**`about:config`**」と入力します。
      設定可能なプロパティの一覧が表示されます。
   c. *network.negotiate-auth.trusted-uris* をダブルクリックしてプロパティを編集します。
   d. BI 起動パッドへのアクセスに使用する URL を入力します。
      たとえば、BI 起動パッドの URL が **`http://<machine.domain.com>:8080/BOE/BI`** の場合は、「**`http://<machine.domain.com>`**」と入力する必要があります。

      > ⓘ 注記
      >
      > 複数の URL を追加するには、それらをカンマで区切ります。たとえば、「**`http://<machine.domain.com>,<machine2.domain.com>`**」と入力します。

   e. [*OK*]をクリックします。
3. Firefox ブラウザウィンドウを閉じて再度開くと、これらの変更が有効になります。
4. ここまでの手順を BI プラットフォームクライアントマシンごとに繰り返します。

9.4.6.2.9 AD Kerberos 認証用に Vintela SSO をテストする。

SSO 設定はクライアントワークステーションからテストする必要があります。クライアントが、BI プラットフォームデプロイメントとして同じドメイン上にあること、およびマップされた AD ユーザとしてワークステーションにログインしていることを確認してください。このユーザアカウントは、手動で BI 起動パッドにログインできるようにする必要があります。

SSO をテストするには、ブラウザを開いて BI 起動パッドの URL を入力します。SSO が正しく設定されている場合、ログオン認証情報について入力を求められることはありません。

→ ヒント

デプロイメント内で、さまざまな AD ユーザシナリオをテストすることをお勧めします。たとえば、ユーザの環境に複数のオペレーティングシステムからのユーザがいる場合、各オペレーティングシステムからのユーザについて、SSO をテストする必要があります。また、組織内でサポートされる可能性のあるすべてのブラウザでも、テストする必要があります。ユーザの環境に複数のフォレストまたはドメインからのユーザがいる場合、各ドメインまたはフォレストからのユーザアカウントについて SSO をテストする必要があります。

9.4.6.2.10 アプリケーションサーバのデータベースへの Kerberos とシングルサインオンの設定

以下のすべての要件を満たすデプロイメントで、データベースへのシングルサインオンがサポートされます。

- BI プラットフォームのデプロイメントが Web アプリケーションサーバにある。
- Web アプリケーションサーバは AD 認証用の Vintela SSO で設定されている。
- SSO が必要なデータベースは SQL Server または Oracle でサポートされるバージョンである。
- データベースに対するアクセス権が必要なグループとユーザに、SQL Server または Oracle 内の権限が付与されている。

最後の手順では、`krb5.ini` ファイルを変更して Web アプリケーションのデータベースへの SSO をサポートするようにします。

9.4.6.2.10.1 Java アプリケーションサーバのデータベースへのシングルサインオンを有効化する

1. BI プラットフォームのデプロイメントで使用される `krb5.ini` ファイルを開きます。

   このファイルのデフォルトの場所は、Web アプリケーションサーバの WIN ディレクトリです。

   ⓘ 注記

   WIN ディレクトリにファイルが見つからない場合は、ファイルの場所に関する次の Java 引数を確認します。

   ```
   -Djava.security.auth.login.config
   ```

   この変数は、Kerberos を使用する AD を Web アプリケーションサーバに設定するときに指定されます。

2. ファイルの `[libdefaults]`セクションに移動します。
3. 次の文字列は、ファイルの `[realms]`セクションの開始位置よりも前に入力してください。

   ```
   forwardable=true
   ```

4. ファイルを保存して閉じます。
5. Web アプリケーションサーバを再起動します。

データベースへのシングルサインオンは、CMC の Windows AD 認証のページで [セキュリティコンテキストをキャッシュする (データベースへの *SSO* に必要)] ボックスをオンにするまで有効になりません。

9.4.6.3 SiteMinder の使用

9.4.6.3.1 Windows AD と SiteMinder の併用

ここでは、AD と SiteMinder の併用方法を説明します。SiteMinder はサードパーティ製のユーザアクセスおよび認証ツールであり、AD セキュリティプラグインとともに使用して BI プラットフォームへのシングルサインオンを作成できます。Kerberos と SiteMinder を併用できます。

Windows AD 認証が SiteMinder に対応するように設定する前に、SiteMinder の ID 管理リソースをインストールして設定してあることを確認します。SiteMinder の詳細とインストール方法については、SiteMinder のマニュアルを参照してください。

SiteMinder と AD シングルサインオンの併用を有効にするには、次の 2 つのタスクを完了する必要があります。

- SiteMinder を使用したシングルサインオン用に AD プラグインを設定する
- BOE Web アプリケーションの SiteMinder プロパティを定義する

> ⓘ 注記
>
> SiteMinder 管理者が 4.x エージェントに対するサポートを有効にしていることを確認してください。これは、使用している SiteMinder のサポートされているバージョンにかかわらず、実行する必要があります。SiteMinder 設定の詳細については、SiteMinder のマニュアルを参照してください。

9.4.6.3.1.1 BI 起動パッド用に SiteMinder プロパティを有効にする

Windows AD セキュリティプラグインの SiteMinder 設定の指定に加えて、BOE war プロパティの SiteMinder 設定も指定する必要があります。

1. BI プラットフォームインストール内にある `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥` ディレクトリを探します。
2. メモ帳などのテキスト編集ユーティリティを使用して、このディレクトリ内に新しいファイルを作成します。
3. 新しいファイルに、次の値を入力します。

   ```
   sso.enabled=true
   siteminder.authentication=secWinAD
   siteminder.enabled=true
   ```

4. `global.properties` という名前でファイルを保存します。

   > ⓘ 注記
   >
   > ファイル名に `.txt` のような拡張子を付けて保存しないように注意してください。

5. 同じディレクトリで別のファイルを作成します。
6. 新しいファイルに、次の値を入力します。

   ```
   authentication.default=secWinAD
   cms.default=[cms name]:[CMS port number]
   ```

次はその例です。

```
authentication.default=LDAP
cms.default=mycms:6400
```

7. `BIlaunchpad.properties` という名前でファイルを保存し、ファイルを閉じます。

これらの新しいプロパティが有効になるのは、BOE.war が Web アプリケーションサーバを実行しているコンピュータ上に再デプロイされてからです。WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。Wdeploy を使用して Web アプリケーションをアンデプロイする際の詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

9.4.6.3.1.2 CMC で SiteMinder を設定する

SiteMinder 用に CMC を設定する前に、次の要件のアクションを完了する必要があります。

- AD ユーザグループを BI プラットフォームに正常にマップしておきます。
- CCM で AD 認証情報をテストしておきます。

1. CMC の認証管理エリアを表示します。
2. *Windows AD* をダブルクリックします。
3. [*Windows Active Directory (AD) を有効にする*] チェックボックスを選択します。
4. [認証のオプション] で、[*NTLM 認証を使用する*] または [*Kerberos 認証を使用する*] を選択します。

   Kerberos と Kerberos を使用する AD 認証に対応して BI プラットフォームを設定するには、サービスアカウントが必要です。新しいドメインアカウントを作成することも、既存のドメインアカウントを使用することもできます。サービスアカウントは、BI プラットフォームサーバの実行に使用されます。

   > → ヒント
   >
   > BI ラウンチパッドに手動でログオンする場合、他のドメインに属するユーザは、ユーザ名の後に大文字のドメイン名を追加する必要があります。たとえば、`user@CHILD.PARENTDOMAIN.COM` では、“CHILD.PARENTDOMAIN.COM” がドメインです。

5. [*Kerberos 認証を使用する*] を選択した場合、次の操作を実行します。
   a. データベースへのシングルサインオンを設定する場合は、[セキュリティコンテキストをキャッシュする] を選択します。
   b. [サービスプリンシパル名] ボックス内の情報を削除します。
6. シングルサインオンを設定する場合は、[*選択した認証モードでのシングルサインオン (SSO) を有効にする*] を選択します。

   また、BOE Web アプリケーションの一般プロパティおよび BI ラウンチパッドプロパティをシングルサインオンが有効になるように設定する必要があります。
7. 認証情報の同期エリアで、いずれかのオプションを選択し、ログオン時に AD ユーザのデータソース認証情報を有効化して更新します。

   このオプションにより、ユーザの現在のログオン認証情報を使用してデータソースが同期化されます。
8. *SiteMinder オプション*エリアで、Kerberos での AD 認証用シングルサインオンオプションとして、SiteMinder を設定します。
   a. 無効をクリックします。

[*Windows Active Directory*] ページが表示されます。

Windows AD プラグインを設定していない場合は、警告が表示されて、続行するかどうかの確認が行われます。*OK* をクリックします。

b. *SiteMinder* シングルサインオンを使用をクリックします。
c. [ポリシーサーバホスト] ボックスに各ポリシーサーバ名を入力し、[追加] をクリックします。
d. それぞれのポリシーサーバホストについて、[アカウントポート]、[認証ポート]、および[承認ポート] ボックスにポート番号を入力します。
e. [エージェント名] に、エージェント名を入力します。
f. [共有シークレット] ボックスに、共有シークレットを入力します。

   使用する SiteMinder のサポートされるバージョンに関わらず、SiteMinder 管理者が 4.x エージェントに対するサポートを有効にしていることを確認してください。SiteMinder およびそのインストール方法の詳細については、SiteMinder のマニュアルを参照してください。
g. [更新] をクリックして保存し、AD 認証のメインページに戻ります。

9. *AD* エイリアスのオプションエリアで、BI プラットフォームでの新しいエイリアスの追加および更新方法を指定します。
   a. 新しいエイリアスのオプションエリアで、Enterprise アカウントに新しいエイリアスをマップするためのオプションを選択します。
      - 同じ名前の既存のユーザアカウントに新しい *AD* エイリアスをそれぞれ割り当てる
        このオプションは、複数のユーザが同じ名前で既存の Enterprise アカウントを持っている場合、つまり AD エイリアスが既存のユーザに割り当てられる (自動エイリアス作成がオンである) 場合に選択します。既存の Enterprise アカウントを持っていないユーザや Enterprise と AD で同じアカウント名を使用していないユーザは、新しいユーザとして追加されます。
      - 新しい *AD* エイリアスごとに新しいユーザアカウントを作成する
        このオプションは、ユーザごとに新しいアカウントを作成する場合に選択します。
   b. エイリアス更新オプションエリアで、Enterprise アカウントのエイリアスの更新を管理するためのオプションを選択します。
      - エイリアスの更新時に新しいエイリアスを作成する
        このオプションを選択すると、BI プラットフォームにマップされた各 AD ユーザに対して、新しいエイリアスを自動的に作成します。新しい AD アカウントが BI プラットフォームアカウントを持たないユーザに対して作成されます。または [新しい *AD* エイリアスごとに新しいユーザアカウントを作成する] を選択し、[更新] をクリックした場合は、新しい AD アカウントがすべてのユーザに対して作成されます。
      - ユーザのログオン時にのみ新しいエイリアスを作成する
        マッピングしている AD ディレクトリに多くのユーザが含まれており、その一部のユーザだけが BI プラットフォームを使用する場合に、このオプションを選択します。BI プラットフォームは、すべてのユーザに対してエイリアスや Enterprise アカウントを自動で作成するわけではありません。代わりに、BI プラットフォームにログオンするユーザだけにエイリアスを (必要な場合は、アカウントも) 作成します。
   c. 新しいユーザのオプションエリアで、次の新しいユーザを作成するためのオプションを選択します。
      - 新しいユーザを登録ユーザとして作成する
        登録ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。指定ユーザライセンスは特定のユーザに関連付けられており、ユーザはそのユーザ名およびパスワードに基づいてシステムにアクセスすることができます。このため、指定ユーザは、システムに接続しているユーザの数に関係なく接続できます。このオプションを使用して作成したユーザアカウントに使用できる登録ユーザライセンスを持っている必要があります。

> **注記**
>
> 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。
>
> ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。

- 新しいユーザを同時接続ユーザとして作成する
  同時接続ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。同時接続ライセンスでは BI プラットフォームに同時接続できるユーザ数が指定されます。この種類のライセンスは、少ないユーザ数の同時接続ライセンスで多数のユーザをサポートできるため、柔軟性に優れています。たとえば、ユーザがシステムにアクセスする頻度と時間の長さによって、100 ユーザ同時接続ライセンスで 250、500、または 700 のユーザをサポートできます。

10. AD エイリアスの更新のスケジュール方法を設定するには、[スケジュール] をクリックします。
    a. [スケジュール] ダイアログボックスで、[オブジェクトの実行] リストから繰り返しを選択します。
    b. 必要に応じて、その他のスケジュールオプションやパラメータを設定します。
    c. スケジュールをクリックします。
       エイリアスの更新が行われると、グループ情報も更新されます。
11. 属性バインディングオプションエリアで、AD プラグインの属性バインディングの優先順位を指定します。
    a. [フルネーム、電子メールアドレス、およびその他の属性のインポート] チェックボックスを選択します。
       AD アカウントで使用するフルネームと説明がインポートされ、ユーザオブジェクトとともに BI プラットフォームに格納されます。
    b. [別の属性バインディングに関連する *AD* 属性バインディングの優先順位を設定する] のオプションを指定します。

       オプションが 1 に設定されていると、AD およびその他のプラグイン (LDAP および SAP) が有効な場合、AD 属性が優先されます。オプションが「3」に設定されている場合は、その他の有効化プラグインの属性が優先されます。バインディングは、異なる値に設定する必要があります。複数の認証プラグインを同じバインディング値に設定すると、予期しない結果が発生します。
12. *AD* グループオプションエリアで、AD グループの更新について設定します。
    a. スケジュールをクリックします。
       スケジュールダイアログボックスが表示されます。
    b. [オブジェクトの実行] リストから繰り返しを選択します。
    c. 必要に応じて、その他のスケジュールオプションやパラメータを設定します。
    d. スケジュールをクリックします。

    更新がスケジュールされ、指定したスケジュールに従って実行されます。AD グループアカウントに対して次にスケジュールされている更新は、*AD* グループオプションに表示されます。
13. オンデマンド *AD* の更新エリアで、更新をクリックしたときに、AD グループまたはユーザのどちら (あるいはどちらでもない) を更新するかを示すオプションを選択します。

    - *AD* グループを今すぐ更新する
      [更新] をクリックしたときに、すべてのスケジュールされている AD グループの更新を開始する場合は、このオプションを選択します。次にスケジュールされている AD グループの更新が *AD* グループオプションにリストされます。
    - *AD* グループとエイリアスを今すぐ更新する

[更新] をクリックしたときに、すべてのスケジュールされている AD グループおよびユーザエイリアスの更新を開始する場合は、このオプションを選択します。次にスケジュールされている更新は、*AD グループオプション*および *AD エイリアスのオプション*にリストされます。

- *AD グループとエイリアスを今すぐ更新しない*
  [更新] をクリックしても、AD グループまたはユーザエイリアスの更新は行われません。

14. [更新] をクリックし、[*OK*] をクリックします。

9.4.6.3.1.3 SiteMinder を無効にする

SiteMinder を設定できないようにする場合、または CMC で設定した後に無効にする場合は、BI 起動パッドの Web 設定ファイルを変更します。

9.4.6.3.1.3.1 Java クライアントの SiteMinder を無効にする

Windows AD セキュリティプラグインの SiteMinder 設定の無効化以外にも、Web アプリケーションサーバの BOE war ファイルの SiteMinder 設定も無効化する必要があります。

1. インストールされている BI プラットフォームの次のディレクトリに移動します。
   `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥`
2. `global.properties` ファイルを開きます。
3. `siteminder.enabled` を false に変更します。

```
siteminder.enabled=false
```

4. 変更を保存し、ファイルを閉じます。

この変更が有効になるのは、`BOE.war` が Web アプリケーションサーバを実行中のマシンに再デプロイされてからです。WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。Wdeploy を使用して Web アプリケーションをアンデプロイする際の詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

9.4.7 Windows AD 認証のトラブルシューティング

9.4.7.1 設定のトラブルシューティング

Kerberos の設定時に問題が起きた場合は、次の手順が有用です。

- ログの有効化
- Java SDK Kerberos 設定のテスト

9.4.7.1.1 ログを有効にする

1. *[スタート]*メニューから、*[プログラム]>[Tomcat]>[Tomcat の設定]*の順にクリックします。
2. *[Java]*タブをクリックします。
3. 次のオプションを追加します。

```
-Dcrystal.enterprise.trace.configuration=verbose
-sun.security.krb5.debug=true
```

これにより、次の場所にログファイルが作成されます。

```
C:¥Documents and Settings¥<user name>¥.businessobjects¥jce_verbose.log
```

9.4.7.1.2 Kerberos 設定をテストする

次のコマンドを実行して、Kerberos の設定をテストします。ここで、`servant` は CMS が実行されているサービスアカウントとドメインで、`password` は、このサービスアカウントに関連付けられているパスワードです。

```
<InstallDirectory>¥SAP BusinessObjects Enterprise XI
4.0¥win64_64¥jdk¥bin¥servact@TESTM03.COM Password
```

例:

```
C:¥Program Files¥SAP BusinessObjects¥
 SAP BusinessObjects Enterprise XI 4.0¥win64_64¥jdk¥bin¥
 servact@TESTM03.COM Password
```

ドメインおよびサービスプリンシパル名は、Active Directory のドメインおよびサービスプリンシパル名と完全に一致している必要があります。 問題が解消されない場合は、同じ名前を入力したかどうかを確認してください。名前では大文字と小文字が区別されます。

9.4.7.1.3 異なる AD UPN および SAM 名によるログオンの失敗

ユーザの Active Directory ID は正常に BI プラットフォームにマップされています。それにもかかわらず、`DOMAIN¥ABC123` という形式で、Windows AD 認証および Kerberos を使用して CMC または BI 起動パッドにログオンすることができません。

この問題は、ユーザが UPN を使用して Active Directory で設定され、SAM 名が同じでない場合に発生する可能性があります。以下のような例の場合に、問題が発生する可能性があります。

- UPN が abc123@company.com だが、SAM 名が DOMAIN¥ABC123 である場合。
- UPN が jsmith@company だが、SAM 名が DOMAIN¥johnsmith である場合。

この問題を解決するには、次の 2 とおりの方法があります。

- ユーザに、SAM 名ではなく UPN 名を使用してログインさせる。
- SAM アカウント名と UPN 名を完全に同じにする。

9.4.7.1.4 事前認証エラー

以前にログオンできたユーザが、正常にログオンできなくなることがあります。ユーザは、"アカウント情報を認識できません。" というエラーを受け取ります。Tomcat エラーログには、"`Pre-authentication information was invalid (24)`" というエラーが記録されます。

これは、Kerberos ユーザデータベースが AD の UPN への変更を取得していないために発生します。これは、Kerberos ユーザデータベースと AD の情報が同期していないことを意味します。

この問題を解決するには、AD でユーザのパスワードをリセットしてください。これにより、変更が正しく伝播されます。

> **注記**
>
> この問題は、J2SE 5.0 によるものではありません。

9.5 SAP 認証

9.5.1 SAP 認証の設定

この節では、SAP 環境に合わせて BI プラットフォームの認証を設定する方法について説明します。

SAP 認証によって、SAP ユーザは自分の SAP ユーザ名とパスワードを使用して、BI プラットフォームにログオンすることができます。パスワードは、BI プラットフォームに保存する必要はありません。また、SAP 認証では、ユーザのロールに関する情報を SAP 内に保持し、このロール情報を BI プラットフォーム内で使用して、管理タスクの実行権限やコンテンツへのアクセス権限を割り当てることもできます。

SAP 認証アプリケーションへのアクセス

SAP システムに関する情報を BI プラットフォームに入力する必要があります。専用の Web アプリケーションには、メインの BI プラットフォーム管理ツールであるセントラル管理コンソール (CMC) を介してアクセスできます。CMC の[ホーム]ページからアクセスするには、[認証]をクリックします。

SAP ユーザの認証

セキュリティプラグインにより、BI プラットフォームがユーザを認証する方法を拡張およびカスタマイズできます。SAP 認証機能には、BI プラットフォームの Central Management Server (CMS) コンポーネントのための SAP セキュリティプラグイン (`secSAPR3.dll`) が含まれます。SAP セキュリティプラグインには、次のような長所があります。

- 認証プロバイダとして動作し、CMS の代わりに SAP システムに対してユーザの認証情報を確認します。BI プラットフォームに直接ログオンする場合は、SAP 認証を選択し、通常の SAP ユーザ名とパスワードを入力

します。BI プラットフォームは、SAP システムに対してエンタープライズポータルのログオンチケットも認証できます。

- SAP から BI プラットフォームユーザグループにロールをマップできるため、アカウントが簡単に作成できます。また、BI プラットフォーム内で一貫した方法でユーザやグループへの権限の割り当てが可能なため、アカウントの管理が容易に行えます。
- SAP のロールリストは動的に維持されます。したがって、SAP のロールを BI プラットフォームにマップすると、そのロールに属するすべてのユーザがシステムにログオンできるようになります。その後、SAP ロールメンバーシップに変更を加えた場合も、BI プラットフォームでリストを更新したり、最新表示したりする必要はありません。
- SAP 認証コンポーネントには、プラグインを設定する Web アプリケーションがあります。このアプリケーションは、セントラル管理コンソール (CMC) の [認証] エリアでアクセスできます。

9.5.2 BI プラットフォームのユーザアカウントの作成

BI プラットフォームシステムには、SAP ロールメンバーシップリストへのアクセスや SAP 認証が許可されている SAP ユーザアカウントが必要です。BI プラットフォームを SAP システムに接続するときに、このアカウントの認証情報が必要になります。SAP ユーザアカウントの作成やロールを介した権限の割り当てに関する一般的な手順については、SAP BW のマニュアルを参照してください。

トランザクション `SU01` を使用して、`CRYSTAL` という名前の新規 SAP ユーザアカウントを作成します。トランザクション `PFCG` を使用して、`CRYSTAL_ENTITLEMENT` という名前の新規ロールを作成します。(これらの名前を推奨しますが、必須ではありません)。以下の権限オブジェクトの値を設定して、新しいロールの権限を変更します。

権限オブジェクト	フィールド	値
ファイルアクセスの認証(S_DATASET)	アクティビティ(ACTVT)	読み取り、書き込み(33、34)
	物理ファイル名(FILENAME)	*(すべてを意味します)
	ABAP プログラム名(PROGRAM)	*
RFC アクセスの認証チェック (S_RFC)	アクティビティ(ACTVT)	16
	保護される RFC の名前 (RFC_NAME)	BDCH、STPA、SUSO、BDL5、SUUS、SU_USER、SYST、SUNI、RFC1、SDIFRUNTIME、PRGN_J2EE、/CRYSTAL/SECURITY
	保護される RFC オブジェクトのタイプ (RFC_TYPE)	プログラムグループ(FUGR)
ユーザマスタメンテナンス: ユーザグループ (S_USER_GRP)	アクティビティ (ACTVT)	作成または生成、および表示(03)

権限オブジェクト	フィールド	値
	ユーザマスタメンテナンスのユーザグループ (CLASS)	* **注記** セキュリティ機能を強化にするために、BI プラットフォームへのアクセスを必要とするメンバーを含むユーザグループを明示的に一覧に示すことができます。

最後に、CRYSTAL ユーザを CRYSTAL_ENTITLEMENT ロールに追加します。

ヒント

システムポリシーによってシステムへの最初のログオン時にユーザによるパスワードの変更が要求される場合、この時点で CRYSTAL ユーザアカウントでログオンし、パスワードを再設定します。

注記

特定のパフォーマンス拡張が ABAP 環境で有効されると、S_RFC オブジェクトの追加権限が必要になる可能性があります。[ロールのインポート] ページでこれらのエラーがレポートされ、権限がない機能が示されます。

例: 汎用モジュール RFC_METADATA_GET の RFC 権限がありません。

権限オブジェクト	フィールド	値
RFC アクセスの認証チェック (S_RFC)	アクティビティ(ACTVT)	16
	保護される RFC の名前 (RFC_NAME)	BDCH、STPA、SUSO、BDL5、SUUS、SU_USER、SYST、SUNI、RFC1、SDIFRUNTIME、PRGN_J2EE、/CRYSTAL/SECURITY、および RFC_METADATA
	保護される RFC オブジェクトのタイプ (RFC_TYPE)	プログラムグループ(FUGR)

9.5.3 SAP 権限認証システムへの接続

BI プラットフォームにロールをインポートするか BW コンテンツを公開する前に、統合する SAP 権限認証システムに関する情報を提供する必要があります。BI プラットフォームは、ロールメンバーシップを特定したり SAP ユーザを認証したりするときに、この情報を使用してターゲットの SAP システムに接続します。

9.5.3.1 SAP 権限認証システムを追加する

1. CMC の [認証] 管理エリアを表示します。
2. [*SAP*]リンクをダブルクリックします。

   権限認証システムの設定が表示されます。

   > → ヒント
   >
   > 権限認証システムが[論理システム名]リストにすでに表示されている場合は、[新規]をクリックします。

3. *[システム]*フィールドに、SAP システムの 3 文字のシステム ID(SID)を入力します。
4. [クライアント] フィールドに、BI プラットフォームがログオンする際に使用する必要のあるクライアント番号を入力します。
   システム情報とクライアント情報が結合され、[論理システム名] リストにエントリが追加されます。
5. [無効] チェックボックスがオフになっていることを確認します。

   > ⓘ 注記
   >
   > [無効] チェックボックスを使用して、特定の SAP システムが一時的に使用不可になっていることを BI プラットフォームに示します。

6. BI プラットフォームが必ずメッセージサーバを介してログオンするように負荷分散を設定している場合は、[メッセージサーバ] フィールドと [ログオングループ] フィールドに適切な値を入力します。

   > ⓘ 注記
   >
   > 特にデプロイメントが 1 つのマシンに限定されていない場合は、負荷分散を有効にするために、BI プラットフォームマシン上の `Services` ファイルに適切なエントリを作成しておく必要があります。つまり、CMS のホストとなっているマシン、Web アプリケーションサーバ、および認証アカウントと認証設定を管理しているすべてのマシンのアカウントを作成しておく必要があります。

7. 負荷分散を設定しなかった場合、または SAP システムに BI プラットフォームを直接ログオンさせる場合、[アプリケーションサーバ] フィールドと [システム番号] フィールドに適切な値を入力します。
8. [ユーザ名] フィールド、[パスワード] フィールド、および [言語] フィールドには、BI プラットフォームが SAP にログオンする際に使用する SAP アカウントのユーザ名、パスワード、および言語コードをそれぞれ入力します。

   > ⓘ 注記
   >
   > これらのログオン情報は、BI プラットフォームに対して作成したユーザアカウントに一致する必要があります。

9. [更新] をクリックします。

複数の権限認証システムを追加する場合、[オプション] タブをクリックし、BI プラットフォームがデフォルトで使用するシステム、すなわち、SAP 認証情報を使用してログオンしようとしているユーザが、特定の SAP システムを指定していない場合にユーザ認証のためにアクセスするシステムを指定します。

9.5.3.2 権限認証システムが正しく追加されているかどうかを確認する

1. [ロールのインポート]タブをクリックします。
2. [論理システム名]リストから該当する権限認証システムの名前を選択します。

   権限認証システムが正しく追加されている場合は、[利用可能なロール]リストに、インポートできるロールのリストが示されます。

   > → ヒント
   >
   > [論理システム名]リストにロールが表示されない場合は、そのページのエラーメッセージを確認してください。このエラーメッセージには、問題を修正するために必要な情報が示される場合があります。

9.5.3.3 SAP 権限認証システムへの接続を一時的に無効にする

CMC では、BI プラットフォームと SAP 権限認証システムとの接続を一時的に無効にすることができます。これは、SAP 権限認証システムの停止が予定されている場合などに、BI プラットフォームの動作を保持する際に便利です。

1. CMC の [認証] 管理エリアを表示します。
2. [*SAP*]リンクをダブルクリックします。
3. *[論理システム名]*リストから、無効にするシステムを選択します。
4. *[無効]*チェックボックスをオンにします。
5. *[更新]*をクリックします。

9.5.4 SAP 認証オプションの設定

SAP 認証には、BI プラットフォームと SAP システムを統合する場合に指定可能な、数多くのオプションがあります。オプションには、次のようなものがあります。

- SAP 認証を有効化または無効化する
- 接続設定を指定する
- インポートされたユーザを BI プラットフォームライセンスモデルにリンクする
- SAP システムへのシングルサインオンの設定

9.5.4.1 SAP 認証オプションを設定する

1. CMC の [認証] 管理エリアに移動します。
2. [*SAP*] リンクをダブルクリックし、[オプション] タブをクリックします。

3. 必要に応じて、以下の設定を確認および変更します。

設定	説明
SAP 認証を有効にする	SAP 認証を無効にするには、このチェックボックスの選択を解除します。 **注記** 特定の SAP システムの SAP 認証を無効にする場合は、[権限認証システム] タブでそのシステムの [無効] チェックボックスをオンにします。
コンテンツフォルダルート	BI プラットフォームが CMC および BI ラウンチパッドで BW フォルダ構造の複製を開始する場所を指定します。 デフォルトでは `/SAP/2.0` に設定されていますが、別のフォルダに変更できます。値を変更する場合は、CMC およびコンテンツ管理ワークベンチの両方で変更する必要があります。
デフォルトシステム	SAP 認証を使用してログオンしようとしているユーザが、特定の SAP システムを指定していない場合にユーザ認証のためにアクセスする BI プラットフォームの SAP 権限認証システムを選択します。 **注記** デフォルトシステムを選択した場合、そのシステムのユーザは、Live Office や Universe Designer などのクライアントツールから SAP 認証を使用して接続するときにシステム ID またはクライアントを入力する必要がありません。たとえば、デフォルトシステムとして SYS~100 が設定されている場合に、SAP 認証が選択されていると、SYS~100/user1 は user1 としてログオンできます。
権限認証システムへのアクセス試行の最大失敗数	BI プラットフォームが認証要求を実行するために SAP システムへのアクセスを再試行する回数を入力します。 値に「-1」を設定すると、プラットフォームは、権限認証システムへのアクセスを何度でも試行できるようになります。値に「0」を設定すると、BI プラットフォームは、権限認証システムに 1 度だけアクセスを試行します。 **注記** この設定を [*権限認証システムを無効な状態で維持 [秒数]*] と使用して、一時的に使用不可になっている SAP 権限認証システムを BI プラットフォームにどのように処理させるかを設定します。2 つのオプションを基に、使用不可になっている SAP システムとの通信を停止/再開するタイミングが決定されます。
権限認証システムを無効な状態で維持 [秒数]	SAP システムに対するユーザ認証を再開するまでの BI プラットフォームの待機時間を秒数で入力します。

設定	説明
	たとえば、[権限認証システムの最大失敗アクセス数] に「3」を入力すると、BI プラットフォームでは、任意の SAP システムに対するユーザ認証の試行失敗が最大 3 回まで許可されます。4 回目の試行失敗で、システムに対するユーザ認証の試行が指定されている時間だけ停止されます。
システムあたりの最大同時接続数	SAP システムに対して同時に開いたままにしておくことのできる接続の最大数を指定します。 たとえば、「2」を入力すると、BI プラットフォームは SAP に対して 2 つの接続を開いたままにします。
1 接続あたりの使用数	接続ごとの SAP システムへの最大オペレーション数を指定します。 たとえば、[システムあたりの最大同時接続数] が「2」に設定されており、[*1* 接続あたりの使用数] が「3」に設定されている場合、1 接続に 3 つのログオンがあると、BI プラットフォーム] はその接続を閉じてから再開します。
同時接続ユーザと登録ユーザ	同時接続ユーザライセンスまたは登録ユーザライセンスのどちらかを使用するように新規のユーザアカウントを設定します。 同時接続ライセンスでは BI プラットフォームに同時接続できるユーザ数が指定されます。この種類のライセンスは、少数の同時接続ライセンスで大規模なユーザベースをサポートできるため、柔軟性に優れています。たとえば、ユーザがシステムにアクセスする頻度と時間の長さによって、100 ユーザ同時接続ライセンスで 250、500、または 700 のユーザをサポートできます。 登録ユーザライセンスはユーザに関連付けられており、ユーザはそのユーザ名およびパスワードに基づいてシステムにアクセスすることができます。このため、登録ユーザは、システムに接続している他のユーザの数に関係なく接続できます。 **注記** 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。 ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。

設定	説明
	注記 ここで選択するオプションは、BI プラットフォームにインストールされたユーザライセンスの数や種類を変更するものではありません。お使いのシステムで適切なライセンスを利用できることが必要です。
フルネーム、電子メールアドレス、およびその他の属性のインポート	SAP 認証プラグインの優先度レベルを指定します。 SAP アカウントで使用するフルネームと説明がインポートされ、ユーザオブジェクトとともに BI プラットフォームに格納されます。
別の属性バインディングに関連する *SAP* 属性バインディングの優先順位を設定する	SAP ユーザ属性 (フルネームと電子メールアドレス) をバインドする優先順位を指定します。 オプションが 1 に設定されている場合は、SAP およびその他のプラグイン (Windows AD および LDAP) が有効なシナリオでは、SAP 属性が優先されます。オプションが 3 に設定されている場合は、その他の有効化プラグインの属性が優先されます。バインディングは、異なる値に設定する必要があります。複数の認証プラグインを同じバインディング値に設定すると、予期しない結果が発生します。

以下のオプションを設定して、SAP シングルサインオンサービスを設定します。

設定	説明
システム *ID*	SAP シングルサインオンサービスを実行したときに、BI プラットフォームが SAP システムに提供するシステム ID です。
参照	クリックして、SAP シングルサインオンを有効化するために生成された `keystore` ファイルをアップロードします。ファイルへの完全パスを手動で入力することもできます。
キーストアパスワード	`keystore` ファイルへのアクセスに必要なパスワードを入力します。
秘密鍵パスワード	`keystore` ファイルに対応する証明書へのアクセスに必要なパスワードを入力します。証明書は、SAP システムに保存されています。
秘密鍵エイリアス	`keystore` ファイルへのアクセスに必要なエイリアスを入力します。

4. 更新をクリックします。

9.5.4.2 コンテンツルートフォルダを変更する

1. CMC の[認証]管理エリアを表示します。

2. [*SAP*]リンクをダブルクリックします。
3. [オプション]をクリックし、[コンテンツフォルダルート]フィールドにフォルダ名を入力します。

   このフィールドに入力するフォルダ名は、BI プラットフォームが BW フォルダ構造の複製を開始するフォルダの名前です。
4. [更新]をクリックします。
5. BW コンテンツ管理ワークベンチで、[*Enterprise* システム]を展開します。
6. [利用可能なシステム] を展開し、BI プラットフォームが接続しているシステムをダブルクリックします。
7. [レイアウト] タブをクリックし、BI プラットフォームでルート SAP フォルダとして使用するフォルダ (*/SAP/2.0/* など) を [コンテンツベースフォルダ] に入力します。

9.5.5 SAP ロールのインポート

SAP のロールを BI プラットフォームにインポートすることで、ロールメンバーが通常の SAP ログオン情報を使用して BI プラットフォームにログオンできるようになります。 また、シングルサインオンを有効にすると、SAP ユーザは SAP GUI または SAP Enterprise Portal 内からレポートにアクセスする際に自動的に BI プラットフォームにログオンできるようになります。

> ⓘ 注記
>
> SSO を使用可能にするためには、通常、多くの要求事項があります。 たとえば、SSO に対応したドライバやアプリケーションの使用や、サーバと Web サーバが同じドメインにあることの確認などがそれに含まれます。

BI プラットフォームはインポートされたロールごとにグループを生成します。 各グループは命名規則「`<SystemID~ClientNumber@NameOfRole>`」に従って命名されます。 CMC の [ユーザとグループ] 管理エリアに新しいグループが表示されます。 また、これらのグループを使用して、BI プラットフォーム内でオブジェクトセキュリティを定義できます。

公開用に BI プラットフォームを設定する場合、およびロールを BI プラットフォームにインポートする場合、次の 3 つの主要ユーザカテゴリについて考えます。

- BI プラットフォーム管理者
  Enterprise 管理者は、SAP からコンテンツを公開できるよう、システムを設定します。 BI プラットフォームで、適切なロールをインポートし、必要なフォルダを作成して、これらのロールやフォルダへの権限の割り当てを行います。
- コンテンツ公開者
  コンテンツ公開者は、コンテンツをロールに公開する権限を持つユーザです。 このユーザカテゴリの目的は、レポートを公開する権限を持つユーザを通常のロールメンバーと区別することです。
- ロールメンバー
  ロールメンバーは、“コンテンツに関連した”ロールに属しているユーザです。 つまり、これらのユーザは、レポートが公開されるロールに属しています。 メンバーになっているロールに公開されたすべてのレポートに対する、表示、オンデマンドでの表示、スケジュールの権限を持ちます。 ただし、通常のロールメンバーは、新しいコンテンツや、コンテンツの更新バージョンを公開することはできません。

最初に公開する前に、コンテンツ公開者ロールとコンテンツ保持ロールのすべてを BI プラットフォームにインポートしておく必要があります。

> ⓘ 注記
>
> 各ロールでの作業は、それぞれ固有にしておくことをお勧めします。 たとえば、管理者ロールからの公開が可能でも、公開はコンテンツ公開者ロールからのみ行うようにします。 ただし、コンテンツ公開者ロールは、

> コンテンツを公開できるユーザを定義することだけが目的です。 そのため、コンテンツ公開者ロールにはコンテンツを含めないようにして、コンテンツ公開者から、通常のロールメンバーがアクセスできる、コンテンツを保持するロールに公開するようにします。

9.5.5.1 SAP ロールをインポートする

1. CMC の[認証]管理エリアを表示します。
2. [*SAP*]リンクをダブルクリックします。
3. [オプション] タブで、使用権許諾契約に応じて、[同時接続ユーザ] または [登録ユーザ] を選択します。

   このオプションは、BI プラットフォームにインストールされたユーザライセンスの数や種類を変更するものではありません。お使いのシステムで適切なライセンスを利用できることが必要です。
4. *[更新]*をクリックします。
5. [ロールのインポート] タブで、[論理システム名] リストから、該当する権限認証システムを選択します。
6. [利用可能なロール] エリアで、インポート対象のロールを選択し、[追加] をクリックします。
7. [更新] をクリックします。

9.5.5.2 ロールとユーザが正しくインポートされているか確認する

このタスクを開始する前に、BI プラットフォームにマップしたロールの 1 つに属している SAP ユーザのユーザ名およびパスワードをメモしておいてください。

1. Java BI ラウンチパッドの場合は、**`http://<webserver>:<portnumber>/BOE/BI`** にアクセスします。

   `<webserver>` を Web サーバの名称に、`<portnumber>` を BI プラットフォームのポート番号に置き換えます。入力する Web サーバ、ポート番号および URL を管理者に確認する必要がある場合があります。
2. [認証の種類] リストで、[*SAP*] を選択します。

   > ⓘ 注記
   >
   > BI ラウンチパッドでは、[認証の種類] 一覧はデフォルトで非表示になっています。一覧が非表示の場合、システム管理者に `BIlaunchpad.properties` ファイル内の [認証の種類] 一覧を有効にするように依頼し、アプリケーションサーバを再起動します。
3. ログオンする SAP システムとシステムクライアントを入力します。
4. マップしたユーザのユーザ名とパスワードを入力します。
5. [ログオン] をクリックします。

   選択したユーザとして BI ラウンチパッドにログオンされます。

9.5.5.3 SAP ロールとユーザの更新

SAP 認証を有効化した後、BI プラットフォームにインポート済みのマップされたロールに対する定期的な更新をスケジュールし、実行する必要があります。このことにより、SAP ロールの情報を、BI プラットフォームに正確に反映できます。

SAP ロールの更新を実行し、スケジュールするためのオプションは 2 つあります。

- ロールのみを更新: このオプションを使用すると、BI プラットフォームにインポート済みの現在マップされているロール間のリンクのみを更新します。頻繁に更新を実行する予定があり、システムリソースの使用状況に懸念がある場合に、このオプションを使用することをお勧めします。SAP ロールを更新するだけでは、新しいユーザアカウントは作成されません。
- ロールとエイリアスを更新: このオプションを使用すると、ロール間のリンクを更新するだけでなく、SAP システムのロールに追加されたユーザエイリアス用の新しいユーザアカウントを BI プラットフォームに作成します。

> ⓘ 注記
>
> SAP 認証を有効化しているときに、更新時にユーザエイリアスを自動で作成するよう指定していない場合は、新しいエイリアスに対してアカウントは作成されません。

9.5.5.3.1 SAP ロールの更新をスケジュールする

BI プラットフォームにロールをマップしたら、ロールの更新方法を指定する必要があります。

1. [ユーザの更新] タブをクリックします。
2. [ロールのみを更新] セクションまたは [ロールとエイリアスを更新] エリアで [スケジュール] をクリックします。

   > → ヒント
   >
   > すぐに更新を実行する場合は、[今すぐ更新] をクリックします。

   > → ヒント
   >
   > 頻繁に更新をするためシステムリソースに懸念がある場合は、[ロールのみを更新] オプションを使用します。ロールとエイリアスの両方を更新するには、より多くの時間がかかります。

   [繰り返し] ダイアログボックスが表示されます。
3. [オブジェクトの実行] リストからオプションを選択し、必要なスケジュール情報を表示されたフィールドにすべて入力します。

   更新をスケジュールする場合、次の表に示した定期スケジュールパターンの中から選択することができます。

定期スケジュールパターン	説明
時間単位	更新は毎時間実行されます。開始時間、開始日、終了日を指定します。

定期スケジュールパターン	説明
日単位	更新は、毎日または <n> 日おきに実行されます (<n> はユーザが指定した日数)。開始時間、開始日、終了日を指定できます。
週単位	更新は、毎週、1 週間に 1 回または 1 週間に数回実行されます。実行日、開始時間、開始日、終了日を指定できます。
月単位	更新は毎月または数カ月ごとに実行されます。開始時間、開始日、終了日を指定できます。
N 日	更新は毎月指定された日付に実行されます。実行する日にち、時間、開始および終了日を指定することができます。
第 *1* 月曜日	更新は毎月第 1 月曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
月末日	オブジェクトは毎月末日に実行されます。実行時刻、開始日および終了日を指定することができます。
第 *N* 週の *X* 日	更新は毎月特定の週の特定の曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
カレンダ	更新は、すでに作成されているカレンダで指定した日付に実行されます。

4. [スケジュール] をクリックします。
   次回のスケジュールされたロールの更新の日付が、[ユーザの更新] タブに表示されます。

> → ヒント
>
> 次回のスケジュールされた更新をキャンセルするには、[ロールのみを更新] エリアまたは [ロールとエイリアスを更新] エリアで [スケジュールされた更新のキャンセル] をクリックします。

9.5.6 セキュアネットワークコミュニケーション (SNC) の設定

この節では、BI プラットフォームへの SAP 認証の設定プロセスの一部として SNC を設定する方法について説明します。

詳細については、SAP ノート 1396213 を参照してください。

SAP システムと BI プラットフォームシステム間で信用を確立するには、SIA が SNC に設定されたアカウントで開始および実行されるように設定されていることを確認する必要があります。SAP システムが BI プラットフォームを信用するように設定する必要もあります。

関連情報

SAP サーバサイドの信頼の概要 [333 ページ]

9.5.6.1 SAP サーバサイドの信頼の概要

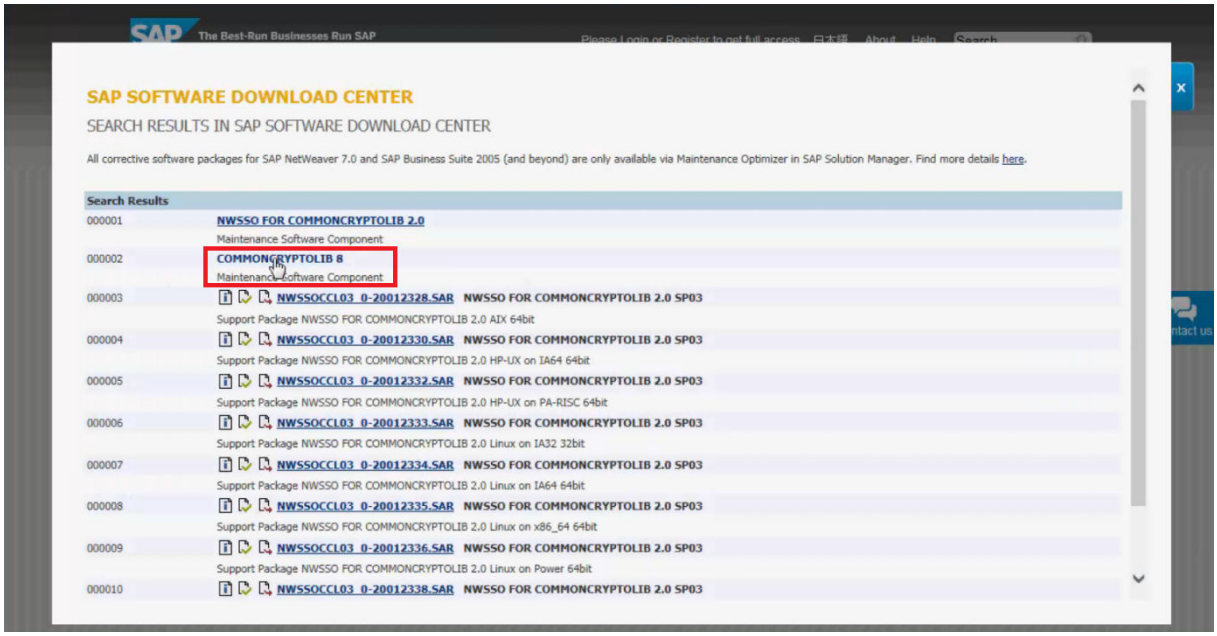
この節では、バージョン 6.20 以降の SAP Web アプリケーションサーバと SAP BusinessObjects Business Intelligence プラットフォームとの間でサーバサイドの信頼を設定する手順を説明します。レポートクエリがユーザのコンテキストに依存するパブリケーションに対してマルチパスのレポートバーストを使用する場合は、サーバサイドの信頼を設定する必要があります。

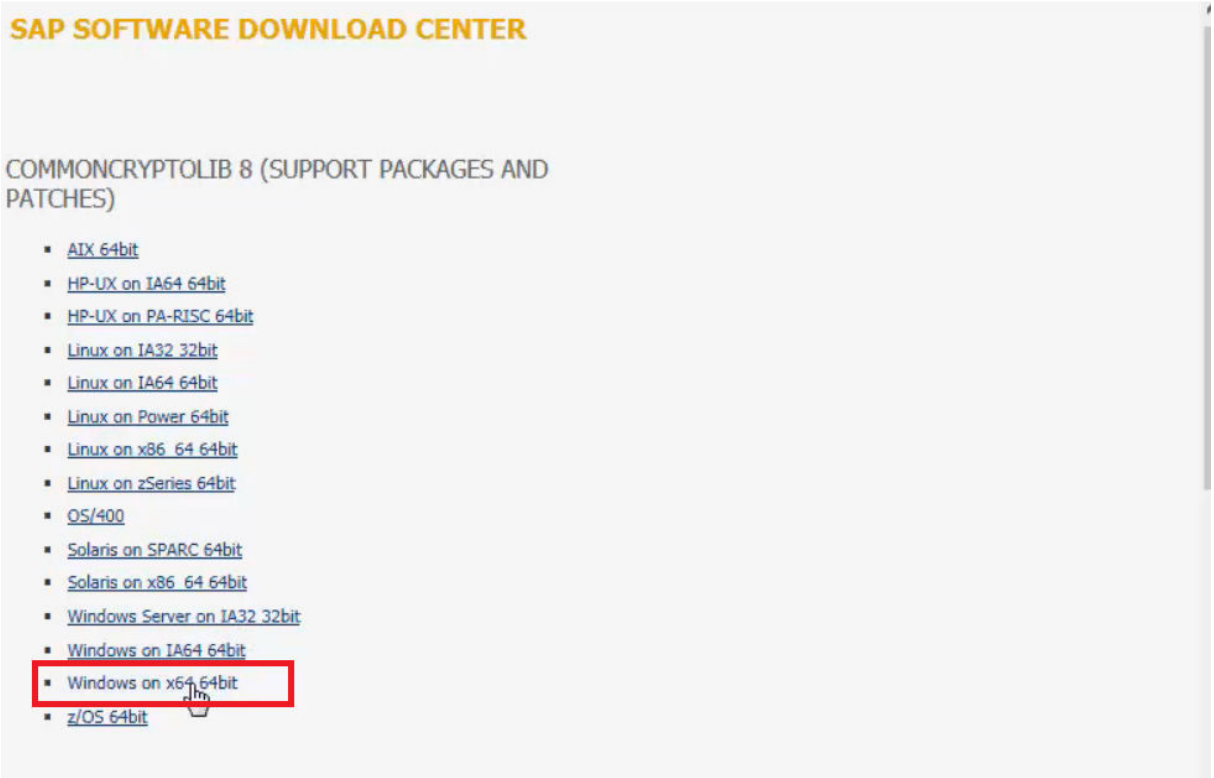
サーバサイドの信頼には、パスワードを使用しない偽装が含まれます。パスワードを指定せずに SAP ユーザを偽装するには、ユーザは、通常のユーザ名とパスワードよりも安全な方法を使用して SAP に識別される必要があります。たとえば、SAP_ALL という認証プロファイルを持つ SAP ユーザは、別の SAP ユーザのパスワードを知らなければそのユーザを偽装することはできません。

SAP 暗号ライブラリを使用したサーバサイドの信頼の有効化

SAP 暗号ライブラリを使用して BI プラットフォームに対するサーバサイドの信頼を有効化するには、登録されている Secure Network Communication (SNC) プロバイダを使用して認証された情報を使って、関連するサーバを実行する必要があります。これらの認証情報は、パスワードなしでユーザの偽装を許可するよう SAP 内部で設定されています。BI プラットフォームの場合、SNC 認証情報下でレポートバーストに含まれるサーバを実行する必要があります。たとえば、Adaptive Job Server などがこれに当たります。

32 ビットプロセスには 32 ビットの SNC バイナリが、64 ビットプロセスには 64 ビットの SNC バイナリが必要です。SAP 暗号ライブラリは、BI プラットフォームとともにインストールされます。SAP 暗号ライブラリは、サーバサイドの信頼を設定する目的以外には使用できないことに注意してください。暗号ライブラリは Windows と UNIX で利用できます。





暗号ライブラリの詳細については、SAP Web サイトで SAP ノート 711093、597059、および 397175 を参照してください。

SAP サーバと BI プラットフォームには、互いを識別するための証明書が割り当てられていることが必要です。各サーバは、独自の証明書と、信頼できるパーティの証明書の一覧を備えています。SAP と BI プラットフォーム間でサーバサイドの信頼を設定するには、Personal Security Environment (PSE) と呼ばれる、パスワード保護された証明書のセットを作成する必要があります。ここでは、PSE を設定して保守する方法、および PSE を BI プラットフォームの処理サーバと安全に関連付ける方法を説明します。

SAP BusinessObjects BI プラットフォームサーバの責任

特定の BI プラットフォームサーバは、シングルサインオン (SSO) の点で SAP Integration と関連しています。以下の表は、これらのサーバとその責任範囲を示しています。

サーバ	責任範囲
Web アプリケーションサーバ	SAP 認証ロールリスト
BW Publisher Service	Crystal Reports 動的パラメータピックリストおよびパーソナライゼーション
CMS	パスワード、チケット、ロールメンバーシップの確認、ユーザリスト
Page Server	オンデマンドの Crystal Reports ビュー
Job Server	Crystal Reports のスケジュール
Web Intelligence Processing Server	Web Intelligence レポートと値の一覧 (LOV) プロンプトの表示とスケジュール
Multi-Dimensional Analysis Service	分析

9.5.6.2 ＳＡＰでのサーバサイドの信頼の設定

サーバサイドの信頼は、ユニバース (`.unv`) に基づく Crystal レポートおよび Web Intelligence レポートにのみ適用されます。BI プラットフォームとともに使用する SNC をセットアップする必要があります。詳細またはトラブルシューティングについては、SAP サーバに付属する SAP のマニュアルを参照してください。

9.5.6.2.1 SAP にサーバ側の信頼を設定する

1. SAP 内および SAP を実行するマシンの SAP 管理者の認証情報、BI プラットフォームおよびこれを実行するマシンの管理者の認証情報を持っていることを確認します。
2. SAP マシンで、Windows の `<DRIVE>:¥usr¥sap¥<SID>¥SYS¥exe¥run¥` ディレクトリに SAP 暗号ライブラリおよび SAPGENPSE ツールが存在することを確認します。
3. ticket ファイルが含まれるディレクトリを指定する **`<SECUDIR>`** 環境変数を作成します。

   > ⓘ 注記
   >
   > この変数は、ユーザからアクセス可能にする必要があります。SAP の *disp+work* プロセスは、この変数の下で実行されます。

4. SAP GUI でトランザクション RZ10 に移動し、拡張メンテナンス モードでインスタンスプロファイルを変更します。
5. プロファイル編集モードで、SAP プロファイル変数を Cryptographic Library に指定し、SAP システムに識別名(DN)を設定します。次の変数は、LDAP 命名規則に従って設定します。

タグ	意味	説明
CN	共通名	証明書所有者の名前。
OU	組織単位	たとえば、製品グループは PG。
O	組織	証明書を発行した組織の名前。
C	国	組織の所在国。

たとえば、R21: **p:CN=R21, OU=PG, O=BOBJ, C=CA** です。

> ⓘ 注記
>
> 前置記号の **p:** は、SAP 暗号ライブラリを表します。この前置記号は、SAP 内で DN を参照するときに必要ですが、STRUST で証明書を確認する場合、または SAPGENPSE を使用する場合には表示されません。

6. 必要に応じて、SAP システムの代わりに次のプロファル値を入力します。

プロファイル変数	値
ssf/name	**SAPSECULIB**
ssf/ssfapi_lib	sapcrypto lib の完全パス
sec/libsapsecu	sapcrypto lib の完全パス
snc/gssapi_lib	sapcrypto lib の完全パス
snc/identity/as	SAP システムの DN

7. SAP インスタンスを再起動します。
8. システムを再実行したらログオンし、トランザクション STRUST に移動します。このトランザクションには、SNC および SSL の追加エントリが含まれています。
9. SNC ノードを右クリックし、[作成]をクリックします。
   RZ10 で指定した ID が表示されます。
10. [*OK*]をクリックします。
11. SNC PSE にパスワードを割り当てるには、ロックアイコンをクリックします。

> ⓘ 注記
>
> このパスワードは、忘れないようにしてください。STRUST では、SNC PSE を表示または編集するたびにこのパスワードを入力するように求められます。

12. 変更を保存します。

> ⓘ 注記
>
> SNC を有効にしていると、変更を保存しない場合はアプリケーションサーバが再起動しません。

13. トランザクション RZ10 に戻り、残りの SNC プロファイルパラメータを追加します。

プロファイル変数	パラメータ
snc/accept_insecure_rfc	**1**
snc/accept_insecure_r3int_rfc	**1**

プロファイル変数	パラメータ
`snc/accept_insecure_gui`	`1`
`snc/accept_insecure_cpic`	`1`
`snc/permit_insecure_start`	`1`
`snc/data_protection/min`	`1`
`snc/data_protection/max`	`3`
`snc/enable`	`1`

最低保護レベルは認証のみの(1)、最大レベルはプライバシーの(3)に設定されます。この場合、`snc/data_protection/use` 値では、認証のみが使用されるように定義されますが、整合性の(2)、プライバシーの(3)、最大の(9)に設定することもできます。`snc/accept_insecure_rfc`、`snc/accept_insecure_r3int_rfc`、`snc/accept_insecure_gui`、`snc/accept_insecure_cpic` の各値が(1)に設定され、安全ではない可能性のある従来の通信方法が今後も許可されるようにします。

14. SAP システムを再起動します。

サーバサイドの信頼のために BI プラットフォームを設定する必要があります。

9.5.6.3 BI プラットフォームでのサーバサイドの信頼の設定

BI プラットフォームでサーバサイドの信頼を設定するには、次の手順を実行する必要があります。これらの手順は Windows ベースですが、SAP ツールはコマンドラインツールであるため、UNIX での手順も非常に似ています。

1. 環境を設定する。
2. パーソナルセキュリティ環境 (PSE) を生成する。
3. BI プラットフォームサーバを設定する。
4. PSE アクセスを設定する。
5. SAP 認証の SNC を設定する。
6. SAP 専用のサーバグループを設定する。

関連情報

環境を設定する [338 ページ]
PSE を生成する [338 ページ]
BI プラットフォームサーバを設定する [340 ページ]
PSE アクセスを設定する [340 ページ]
SAP 認証の SNC を設定する [341 ページ]
サーバグループの使用 [342 ページ]

9.5.6.3.1 環境を設定する

BI プラットフォームにはデフォルトの SAP 暗号ライブラリが含まれます。デフォルトのライブラリを使用する場合に実行する必要があるのは、最後の 2 つの手順 (サブフォルダの作成および環境変数の追加) のみです。そうでない場合、SAP 暗号ライブラリのカスタムコピーを設定するには、すべての手順を実行します。

デフォルトの SAP 暗号ライブラリは次の場所にあります。

- Windows：`<INSTALLDIR>¥sap¥sapcrypto.dll`
- Unix の場合: `<INSTALLDIR>/sap/libsapcrypto.so`

作業を開始する前に、次のことを確認してください。

- SAP 暗号ライブラリが、BI プラットフォーム処理サーバが実行されるホスト上で展開済みである。
- SNC プロバイダとして SAP 暗号ライブラリを使用するために、適切な SAP システムが設定されている。

PSE のメンテナンスを開始する前に、ライブラリ、ツール、および PSE の保存環境を設定する必要があります。

1. BI プラットフォームを実行するマシンのフォルダに PSE メンテナンスツールを含む SAP 暗号ライブラリをコピーします。

   例: `C:¥Program Files¥SAP¥Crypto`.
2. `<PATH>` 環境変数にこのフォルダを追加します。
3. システム全体に適用される `<SNC_LIB>` 環境変数を追加します。この環境変数は、Cryptographic Library を指示します。

   例: `C:¥Program Files¥SAP¥Crypto¥sapcrypto.dll`

   > ⓘ 注記
   >
   > パスの最大長は 100 文字です。
4. **`sec`** という名前のサブフォルダを作成します。

   例: `C:¥Program Files¥SAP¥Crypto¥sec`.
5. システム全体に適用される `<SECUDIR>` 環境変数を追加します。この環境変数は、**`sec`** フォルダを指示します。

関連情報

ＳＡＰでのサーバサイドの信頼の設定 [335 ページ]

9.5.6.3.2 PSE を生成する

関連する BI プラットフォームサーバに PSE が存在し、この PSE が SAP に関連付けられている場合、SAP は BI プラットフォームサーバを信頼できるエンティティとして受け入れます。SAP と BI プラットフォームコンポーネントとの間のこの“信頼”は、相互の公的な証明書を共有することによって確立されます。BI プラットフォームの PSE を生成するための最初の手順は、PSE の証明書を自動生成することです。

1. コマンドプロンプトを開き、暗号ライブラリフォルダから **`sapgenpse.exe gen_pse -a sha256WithRsaEncryption -s 2048 -v -p BOE.pse`** を実行します。

2. BI プラットフォームシステムで使用する PIN および DN を選択します。

   たとえば、**CN=MyBOE01, OU=PG, O=BOBJ, C=CA** です。

   デフォルトの PSE およびその証明書が生成されました。
3. 次のコマンドを使用して、PSE 内の証明書をエクスポートします。

   ```
   sapgenpse.exe export_own_cert -v -p BOE.pse -o <MyBOECert.crt>
   ```
4. SAP GUI でトランザクション STRUST に移動し、SAP システムに関連付けられたシステム PSE を開きます。

   このシステム PSE に割り当て済みのパスワードの入力を求めるメッセージが表示されます。
5. STRUST トランザクション画面の左下にある [<証明書のインポート>] ボタンをクリックし、作成済みの "MyBOECert.crt" ファイルをインポートします。

   SAPGENPSE の証明書は、Base64 でエンコードされています。これらの証明書をインポートするときは、Base64 を選択します。
6. BI プラットフォーム証明書を SAP サーバの PSE 証明書一覧に追加するには、[証明書一覧に追加] ボタンをクリックします。
7. 変更を STRUST に保存します。
8. [エクスポート]ボタンをクリックし、証明書のファイル名を指定します。

   たとえば、**MySAPCert.crt** と指定します。

   > ⓘ 注記
   >
   > 書式は、Base64 のままです。
9. トランザクション SNC0 に移動します。
10. 次のように新エントリを追加します。
    - システム ID は任意ですが、BI プラットフォームシステムを反映します。
    - SNC 名は手順 2 で BI プラットフォーム PSE を作成したときに指定した、先頭に **p:** が付く DN です。
    - [*RFC* 用エントリ有効化] チェックボックスと [外部 *ID* エントリ有効化] チェックボックスの両方を選択します。
11. エクスポートされた証明書を BI プラットフォームの PSE に追加するには、コマンドプロンプトで次のコマンドを実行します。

    ```
    sapgenpse.exe maintain_pk -v -a <MySAPCert.crt> -p BOE.pse
    ```

SAP 暗号ライブラリは、BI プラットフォームマシンにインストールされます。BI プラットフォームサーバを SAP サーバとして識別するために使用される PSE が作成されました。SAP と BI プラットフォームの PSE は、証明書を交換しました。SAP は、BI プラットフォームの PSE へのアクセス権を持つエンティティが、RFC 呼び出しおよびパスワードなしの偽装を実行することを許可します。

関連情報

BI プラットフォームサーバを設定する [340 ページ]

9.5.6.3.3 BI プラットフォームサーバを設定する

BI プラットフォームの PSE を生成したら、SAP 処理用に適切なサーバ構造を設定する必要があります。次の手順を実行すると、SAP 処理サーバのノードが作成され、このノードレベルでオペレーティングシステムの認証情報を設定できます。

> ⓘ 注記
>
> このバージョンの BI プラットフォームでは、サーバがセントラル設定マネージャ (CCM) で設定されなくなりました。その代わりに、Server Intelligence エージェント(ＳＩＡ)を作成する必要があります。

1. CCM で SAP 処理サーバ用の新しいノードを作成します。

   作成したノードに、**SAPProcessor** などの適切な名前を指定します。
2. CMC で、必要な処理サーバを新ノードに追加し、新サーバを起動します。

9.5.6.3.4 PSE アクセスを設定する

BI プラットフォームのノードおよびサーバを設定したら、SAPGENPSE ツールを使用して PSE アクセスを設定する必要があります。

1. コマンドプロンプトで次のコマンドを実行します。

   ```
   sapgenpse.exe seclogin -p SBOE.pse
   ```

   > ⓘ 注記
   >
   > PSE PIN の入力を求める画面が表示されます。BI プラットフォームの SAP 処理サーバで使用する認証情報を使ってツールを実行する場合、ユーザ名を指定する必要はありません。

2. シングルサインオン(SSO)リンクが確立されたことを確認するには、次のコマンドを使用して PSE の内容を一覧表示します。

   ```
   sapgenpse.exe maintain_pk -l
   ```

   結果は、次のようになります。

   ```
   C:¥Documents and Settings¥username¥Desktop¥sapcrypto.x86¥ntintel>sapgenpse.exe
   maintain_pk -l
    maintain_pk for PSE "C:¥Documents and Settings¥username¥My
   Documents¥snc¥sec¥bobjsapproc.pse"
   *** Object <PKList> is of the type <PKList_OID> ***
   1. ---------------------------------------------------------------
               Version:                  0 (X.509v1-1988)
               SubjectName:              CN=R21Again, OU=PG, O=BOBJ, C=CA
               IssuerName:               CN=R21Again, OU=PG, O=BOBJ, C=CA
               SerialNumber:             00
               Validity  -  NotBefore:   Wed Nov 28 16:23:53 2007 (071129002353Z)
                                                                   NotAfter:
   Thu Dec 31 16:00:01 2037 (380101000001Z)
               Public Key Fingerprint:   851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
               SubjectKey:               Algorithm RSA (OID
   1.2.840.113549.1.1.1), NULL
   C:¥Documents and Settings¥username¥Desktop¥sapcrypto.x86¥ntintel>
   ```

   seclogin コマンドが正常に機能した場合、PSE PIN の入力を求める画面が再表示されることはありません。

> ⓘ 注記
>
> PSE へのアクセスに問題が発生した場合は、-O 引数を使用して PSE へのアクセスを指定します。たとえば、PSE へのアクセスを特定ドメインの特定ユーザに付与するには、Windows では次のコマンドを入力します。
>
> ```
> sapgenpse seclogin -p SBOE.pse -O SYSTEM
> ```

9.5.6.3.5 SAP 認証の SNC を設定する

PSE アクセスを設定したら、CMC で SAP 認証を設定する必要があります。

1. CMC の [認証] 管理エリアに移動します。
2. [*SAP*]リンクをダブルクリックします。

   権限認証システムの設定が表示されます。

3. [*SAP* 認証] ページの [*SNC* 設定] タブをクリックします。
4. [論理システム名] リストから該当する権限認証システムを選択します。
5. [基本設定] の [セキュアネットワークコミュニケーション *(SNC)* の有効化] を選択します。
6. [デフォルトを使用する] オプションを選択してライブラリへのデフォルトのパスを使用するか、[カスタムパスを定義] オプションを選択して別の場所を選択します。
7. [保護レベル] で保護のレベルを選択します。

   たとえば、[認証] を選択します。

> ⓘ 注記
>
> SAP システムで設定されている保護レベルを超えないようにしてください。保護のレベルはカスタマイズ可能であるため、組織のニーズと SNC ライブラリの機能に合うように設定できます。
>
> [保護レベル] は、プラットフォーム側の処理のみを指します。たとえば、Web Intelligence dHTML ビューアは指定したレベルに従います。ただし、SAP Business Warehouse (BW) とのクライアント側通信は保護されていないと見なす必要があります。たとえば、Web Intelligence リッチクライアントやインフォメーションデザインツールの通信は常に暗号化されません。

8. [相互認証の設定]に SAP システムの SNC 名を入力します。

   SNC 名の形式は SNC ライブラリに依存します。SAP 暗号ライブラリを使用している場合、識別名は LDAP の命名規則に従い、接頭辞として `p:` を付けることが推奨されます。
9. BI プラットフォームサーバの実行時に使用する認証情報の SNC 名が [*Enterprise システムの SNC 名*] ボックスに表示されていることを確認します。

   複数の SNC 名が設定されている場合は、このフィールドを空白のままにする必要があります。
10. SAP システムおよび BI プラットフォーム PSE の DN を設定します。

9.5.6.3.6 サーバグループの使用

処理 (Crystal Reports または Web Intelligence) サーバが PSE にアクセスできる認証情報の下で実行中でない限り、必須サポートサーバとともにこれらのサーバだけを含む特定のサーバグループを作成する必要があります。さまざまな BI プラットフォームサーバの詳細説明については、「“アーキテクチャ”」の章を参照してください。

SAP コンテンツのコンテンツ処理サーバを設定するときには、3 つのオプションがあります。

1. すべての BI プラットフォームサーバを含む、PSE にアクセスできる認証情報の下で実行中の単一の SIA を維持する。これは、一番単純なオプションです。サーバグループを作成する必要はありません。このアプローチは、不必要な数のサーバが PSE にアクセスできるため、安全性が最も低くなります。
2. PSE にアクセスできる 2 番目の SIA を作成し、それを Crystal Reports または Web Intelligence 処理サーバに追加する。重複したサーバを元の SIA から削除します。サーバグループを作成する必要はありませんが、いくつかのサーバは PSE にアクセスできます。
3. PSE にアクセスできる SAP 用の SIA を排他的に作成する。これを Crystal Reports または Web Intelligence 処理サーバに追加します。このオプションを使用する場合、SAP コンテンツだけがこれらのサーバ上で動作し、より重要なこととして、SAP コンテンツはこれらのサーバ上でのみ動作します。この場合、コンテンツを特定のサーバに送る必要があるため、SIA 用のサーバグループを作成する必要があります。

サーバグループの使用に関するガイドライン

サーバグループは、SAP コンテンツの処理に排他的に使用される SIA を参照する必要があります。さらに、サーバグループは次のサーバを参照する必要があります。

- Adaptive Server
- Adaptive Job Server

すべての SAP コンテンツ、Web Intelligence ドキュメント、および Crystal レポートは、最も厳密な関連付けを使用してサーバグループと関連付け、このグループ内のサーバで必ず実行するようにします。この関連付けをオブ

ジェクトレベルで実行したら、サーバグループ設定を直接スケジュールとパブリケーションの両方の設定に反映する必要があります。

他の (非 SAP) コンテンツが SAP 専用の処理サーバ上で処理されないようにするには、別のサーバグループを作成して、そこに元の SIA の下にあるすべてのサーバを含める必要があります。このコンテンツと非 SAP サーバグループの間に厳密な関連付けを設定することをお勧めします。

9.5.6.4 マルチパスパブリケーションの設定

マルチパスパブリケーションのトラブルシューティング

マルチパスパブリケーションで問題が発生した場合は、Crystal Reports(CR)または SAP 用多次元データアクセス(MDA)ドライバのトレース機能を有効にして、各ジョブや受信者が使用するログオン文字列を調べます。これらのログオン文字列は、次のようになります。

```
 SAP: Successfully logged on to SAP server.
Logon handle: 1. Logon string: CLIENT=800 LANG=en
ASHOST="vanrdw2k107.sap.crystald.net" SYSNR=00 SNC_MODE=1 SNC_QOP=1
SNC_LIB="C:¥WINDOWS¥System32¥sapcrypto.dll"
SNC_PARTNERNAME="p:CN=R21Again, OU=PG, O=BOBJ, C=CA" EXTIDDATA=HENRIKRPT3
EXTIDTYPE=UN
```

ログオン文字列にはユーザ名に適切な **EXTIDTYPE=UN** が含まれており、**EXTIDDATA** は受信者の SAP ユーザ名です。この例では、正常にログオンが行われました。

9.5.6.5 Secure Network Communication との統合のためのワークフロー

BI プラットフォームは SAP コンポーネント間の認証やデータの暗号化のための Secure Network Communication (SNC) を実装する環境をサポートします。 SAP 暗号ライブラリ (または SNC インタフェースを使用するその他の外部セキュリティ製品) を導入した場合、セキュリティ保護された環境内で BI プラットフォームを効果的に統合するために、一部の追加の設定を行う必要があります。

BI プラットフォームを設定して Secure Network Communication を使用するには、次のタスクを完了する必要があります。

1. 適切なユーザアカウントで起動/実行できるよう、BI プラットフォームサーバを設定します。
2. BI プラットフォームシステムを信頼するよう SAP システムを設定します。
3. セントラル管理コンソール内の SNC リンクで SNC を設定します。
4. SAP ロールとユーザを BI プラットフォームにインポートします。

関連情報

SAP ロールのインポート [329 ページ]

9.5.6.6 セントラル管理コンソールで SNC を設定する

SNC を設定する前に、BI プラットフォームに新しい権限認証システムを追加し、SNC ライブラリファイルが指定のディレクトリにあることを確認して、このファイルを指す環境変数 `<RFC_LIB>` を作成する必要があります。

1. [*SAP* 認証] ページの [*SNC* 設定] タブをクリックします。
2. [論理システム名] リストから該当する権限認証システムを選択します。
3. [基本設定] の [セキュアネットワークコミュニケーション *(SNC)* の有効化] を選択します。
4. `.unx` ユニバースまたは OLAP BICS 接続を使用するように SAP 認証を設定しており、STS を使用する予定の場合は、[セキュリティで保護されていない *RFC* 接続の禁止] チェックボックスを選択します。
5. [デフォルトを使用する] オプションを選択してライブラリへのデフォルトのパスを使用するか、[カスタムパスを定義] オプションを選択して別の場所を選択します。

   Web アプリケーションサーバと CMS は同じ OS タイプ上にあり、暗号ライブラリへのパスが同じである必要があります。
6. [保護品質] で保護のレベルを選択します。

   たとえば、[認証] を選択します。

   > ⓘ 注記
   >
   > 保護のレベルはカスタマイズ可能であるため、組織のニーズと SNC ライブラリの機能に合うように設定できます。
7. [相互認証の設定]に SAP システムの SNC 名を入力します。

   SNC 名の形式は SNC ライブラリに依存します。SAP 暗号ライブラリを使用している場合、識別名は LDAP の命名規則に従い、接頭辞として `p:` を付けることが推奨されます。
8. BI プラットフォームサーバの実行時に使用する認証情報の SNC 名が [*Enterprise* システムの *SNC* 名] ボックスに表示されていることを確認します。
9. [更新]をクリックします。

関連情報

SAP 権限認証システムへの接続 [323 ページ]

9.5.6.7 権限認証ユーザを SNC 名に関連付ける

1. SAP BW システムにログオンし、トランザクション `SU01` を実行します。

   [ユーザ管理: 第一画面] が表示されます。
2. [ユーザ] フィールドに、権限認証ユーザとして指定されている SAP アカウント名を入力し、ツールバーの[変更] をクリックします。

   [ユーザ管理]画面が表示されます。
3. [SNC]タブをクリックします。

4. [*SNC 名*] フィールドに、手順 2 で入力した `SNC USER ACCOUNT` を入力します。
5. [保存] をクリックします。

9.5.6.8 システム ID を SNC アクセスコントロールリストに追加する

1. SAP BW システムにログオンし、トランザクション `SNC0` を実行します。

   [ビュー "SNC: システム用アクセスコントロールリスト (ACL)" 変更: 概要] 画面が表示されます。
2. ツールバーの [新規エントリ] をクリックします。

   [新規エントリ: 追加エントリ詳細] 画面が表示されます。
3. [*システム ID*] フィールドに、BI プラットフォームマシンの名前を入力します。
4. [*SNC ユーザ名*] フィールドに「`p:<SNC USER NAME>`」と入力します。`SNC USER NAME` は、BI プラットフォームサーバの設定時に使用したアカウントです。

   > **注記**
   >
   > ご使用の SNC プロバイダが gssapi32.dll の場合は、SNC USER NAME を大文字で表記します。ユーザアカウントの指定には、ドメイン名を含める必要があります。たとえば、domain¥username となります。

5. [*RFC 用エントリ有効化*]および[*外部 ID エントリ有効化*]を選択します。
6. 他のオプションをすべてクリアして、*[保存]*をクリックします。

9.5.7 SAP システムへのシングルサインオンの設定

統合環境では、さまざまな BI プラットフォームクライアントおよびバックエンドサービスが SAP NetWeaver ABAP バックエンドシステムと通信します。BI プラットフォームからこれらの (通常は BW) バックエンドシステムへのシングルサインオンを設定すると便利です。ABAP システムを外部認証システムとして設定した後は、専用形式の SAP トークンを使用して、SAP NetWeaver ABAP システムに接続するすべての BI プラットフォームクライアントおよびサービスのシングルサインオンをサポートするメカニズムを実現します。

詳細については、サポートノート 1670073 を参照してください。

SAP システムへのシングルサインオンを有効にするには、`keystore` ファイルと対応する証明書を作成する必要があります。`keytool` コマンドラインプログラムを使用して、keystore ファイルと証明書を生成します。keytool プログラムは、デフォルトでは各プラットフォームの `sdk/bin` ディレクトリにインストールされています。

証明書は、CMC を使用して、SAP ABAP BW システムと BI プラットフォームに追加しておく必要があります。

> **注記**
>
> SAP BW が使用するデータベースへのシングルサインオンを設定できるようにするには、SAP 認証プラグインを設定する必要があります。

9.5.7.1 キーストアファイルを生成する

このトピックでは、キーストアファイルを生成するために Java Keytool を使用するための指示を記述します。下の表には、Java Keytool のデフォルトの場所が一覧表示されています。

プラットフォーム	デフォルトの場所
Windows	`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥ win64_x64¥sapjvm¥bin`
Linux	`sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool`

1. Java Keytool のデフォルトの場所に移動し、コマンドプロンプトを起動します。
2. キーストアを生成するために Java Keytool を実行します。
   a. <INSTALLDIR>¥ SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥bin に移動します。
   b. 次のコマンドを実行します。
      - Windows: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥bin¥keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`
      - Linux: `*/sap_bobj/enterprise_xi40/java/lib>/sap_bobj/enterprise_xi40/linux_x64/sapjvm/bin/keytool" -genkey -alias mywin -keystore keystore.p12 -storepass admin1 -dname CN=palmtree -validity 365 -keyalg DSA -keysize 1024 -storetype pkcs12`

> → ヒント
>
> デフォルト値を上書きするには、ツールを「-?」パラメータとともに実行します。次のメッセージが表示されます。

> {·} サンプルコード
>
> ```
> Usage: keytool -genkey <options>
>  -keystore <filename(keystore.p12)>
>  -alias <key entry alias(mywin)>
>  -storepass <keystore password (admin1)>
>  -dname <certificate subject DN(CN=palmtree)>
>  -validity <number of days (365)>
>  -cert <filename (cert.der)>
>  (No certificate is generated when importing a keystore)
>  -importkeystore <filename>
> ```

これらのパラメータを使用すると、デフォルト値を上書きできます。

> ⓘ 注記
>
> キーストアを生成するには、Java Keytool を PKCS12 ツールの代替として使用する必要があります。詳細については、2524775 を参照してください。

9.5.7.2 公開鍵証明書をエクスポートする

キーストアファイル用の証明書を作成してエクスポートする必要があります。

1. コマンドプロンプトを起動して、keytool プログラムがあるディレクトリに移動します。
2. キーストアファイルのキー証明書をエクスポートするには、次のコマンドを使用します。

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
-alias <alias>
```

<keystore> をキーストアファイルの名前に置き換えます。
<filename> を証明書の名前に置き換えます。
<alias> をキーストアファイルの作成で使用したエイリアスに置き換えます。

3. 要求されたら、キーストアファイルに設定したパスワードを入力します。

keytool プログラムがあるディレクトリに、キーストアファイルと証明書ができます。

9.5.7.3 ターゲット ABAP SAP システムへの証明書ファイルのインポート

次の操作を実行するには、BI プラットフォームデプロイメント用の、キーストアファイルと関連付けられた証明書が必要です。

> ⓘ 注記
>
> この操作は、ABAP SAP システムでのみ実行できます。

1. SAP GUI を使用して、SAP ABAP BW システムに接続します。

   > ⓘ 注記
   >
   > 管理者権限を持つユーザとして接続する必要があります。

2. SAP GUI で STRUSTSSO2 を実行します。
   証明書ファイルをインポートする準備ができました。
3. [証明書] タブに移動します。
4. [バイナリオプションを使用] チェックボックスが選択されていることを確認します。
5. ファイルパスボタンをクリックして、証明書ファイルがある場所を指定します。
6. 緑色のチェックマークをクリックします。
   証明書ファイルがアップロードされます。
7. [証明書一覧に追加] をクリックします。
   証明書が証明書一覧に表示されます。
8. [*ACL* に追加] をクリックして、システム ID とクライアントを指定します。

   このシステム ID は、SAP BW に対して BI プラットフォームシステムを識別する際に使用するものと同じである必要があります。

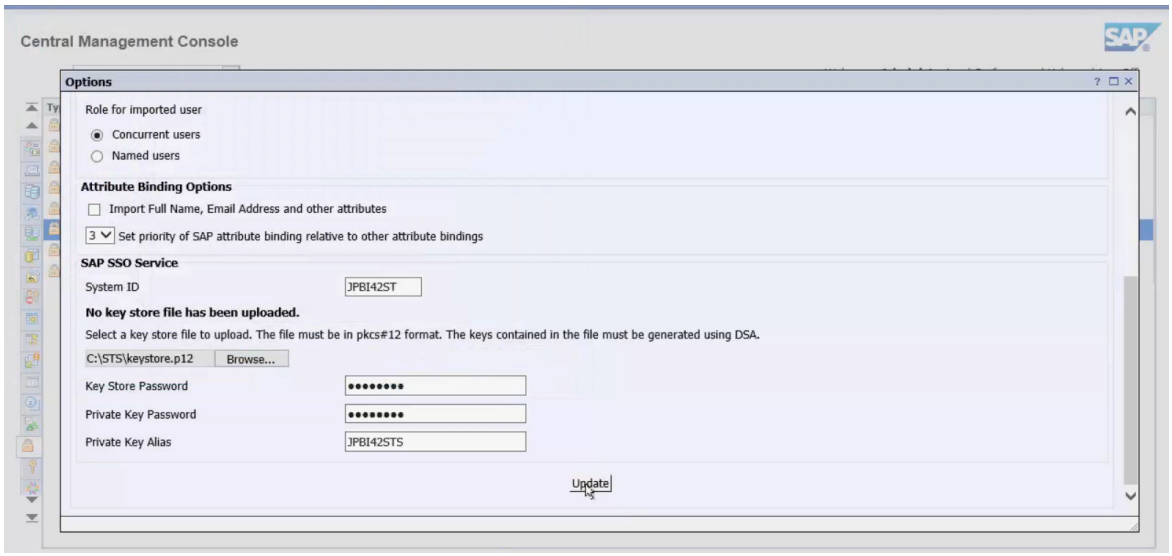
   証明書がアクセスコントロールリスト (ACL) に追加されます。クライアントは「“000”」と指定する必要があります。

9. 変更を保存して終了します。
   変更内容は SAP システムに保存されます。

9.5.7.4 CMC で SAP データベースへのシングルサインオンを設定する

次の手順を実行するには、管理者アカウントを使用して SAP セキュリティプラグインにアクセスする必要があります。

1. CMC の [認証] 管理エリアに移動します。
2. [*SAP*]リンクをダブルクリックし、[オプション]タブをクリックします。



   証明書がインポートされていないと、[*SAP SSO サービス*] セクションに次のメッセージが表示されます。

   キーストアファイルがアップロードされていません。
3. 表示されたフィールドに BI プラットフォームシステムのシステム ID を指定します。

   このシステム ID は、ターゲットの SAP ABAP システムに証明書をインポートするときに使用される値と同じである必要があります。
4. [参照] ボタンをクリックして、キーストアファイルを指定します。
5. 次の必須情報を入力します。

フィールド	必須情報
キーストアパスワード	キーストアファイルへのアクセスに必要なパスワードを入力します。このパスワードは、キーストアファイルを作成したときに指定したものです。
秘密鍵パスワード	キーストアファイルに対応する証明書へのアクセスに必要なパスワードを入力します。このパスワードは、キーストアファイルの証明書を作成したときに指定したものです。

フィールド	必須情報
秘密鍵エイリアス	キーストアファイルへのアクセスに必要なエイリアスを入力します。このパスワードは、キーストアファイルを作成したときに指定したものです。

6. [更新] をクリックして、設定を適用します。
   設定の適用が成功すると、[システム ID] フィールドの下に次のメッセージが表示されます。

   キーストアファイルがアップロードされました。

9.5.7.5 セキュリティトークンサービスを Adaptive Processing Server に追加する

クラスタ化環境では、セキュリティトークンサービスは各 Adaptive Processing Server に個別に追加されます。

1. CMC の[サーバ]管理エリアを表示します。
2. [コアサービス] をダブルクリックします。
   [コアサービス] の下にサーバの一覧が表示されます。
3. Adaptive Processing Server を右クリックして、[サーバの停止] を選択します。

   サーバの状態が [停止] となるまで、次の手順に進まないでください。
4. Adaptive Processing Server を右クリックして、[サービスの選択] を選択します。
   [サービスの選択] ダイアログボックスが表示されます。
5. [追加] ボタンを使用して、セキュリティトークンサービスを [利用可能なサービス] リストから [サービス] リストに移動します。
6. [*OK*] をクリックします。
7. Adaptive Processing Server を再起動します。

9.5.8 SAP Crystal Reports および SAP NetWeaver の SSO の設定

デフォルトで、BI プラットフォームは、SAP Crystal Reports ユーザがシングルサインオン (SSO) を使用して SAP データにアクセスできるよう設定されています。

9.5.8.1 SAP NetWeaver と SAP Crystal Reports の SSO を無効化する

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。
4. 次のドライバのいずれかを選択します。

ドライバ	表示名
オペレーショナルデータストアドライバ	*crdb_ods*
オープン SQL ドライバ	*crdb_opensql*
InfoSet ドライバ	*crdb_infoset*
BW MDX クエリドライバ	*crdb_bwmdx*

5. [削除] をクリックします。
6. [保存して閉じる]をクリックします。
7. SAP Crystal Reports を再起動します。

9.5.8.2 SAP NetWeaver と SAP Crystal Reports の SSO を再有効化する

以下の手順に従って、SAP NetWeaver (ABAP) と SAP Crystal Reports の SSO を再有効化します。

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。
4. [*SSO* コンテキストをデータベースログオンに使用する] で、次の値を入力します。

`crdb_ods`	ODS ドライバをアクティブにする
`crdb_opensql`	オープン SQL ドライバをアクティブにする
`crdb_bwmdx`	SAP BW MDX クエリドライバをアクティブにする
`crdb_infoset`	InfoSet ドライバをアクティブにする

5. [追加] をクリックします。
6. [保存して閉じる]をクリックします。
7. SAP Crystal Reports を再起動します。

9.6 PeopleSoft 認証

9.6.1 概要

BI プラットフォームで PeopleSoft Enterprise データを使用するには、デプロイメントに関する情報をプログラムに設定する必要があります。この情報は、PeopleSoft 認証情報を使用して BI プラットフォームにログオンするユーザをプログラムで認証する際に使用します。

9.6.2 PeopleSoft Enterprise 認証の有効化

BI プラットフォームで PeopleSoft Enterprise 情報を使用できるようにするには、PeopleSoft Enterprise システムへの認証方法に関する情報が BI プラットフォームに必要です。

9.6.2.1 BI プラットフォームで PeopleSoft Enterprise 認証を有効化する

1. セントラル管理コンソールに管理者としてログオンします。
2. [管理]領域で[認証]をクリックします。
3. [*PeopleSoft Enterprise*] をダブルクリックします。
   [*PeopleSoft Enterprise*] ページが表示されます。[オプション]、[ドメイン]、[ロール]、[ユーザの更新] の 4 つのタブがあります。
4. [オプション] タブで、[*PeopleSoft Enterprise* 認証の有効化] チェックボックスをオンにします。
5. BI プラットフォームのデプロイメントに応じて、[新しいエイリアス]、[更新オプション]、および [新しいユーザのオプション] を適切に変更します。

   [更新] をクリックして変更を保存してから、[ドメイン] タブに移動します。
6. [ドメイン] タブをクリックします。
7. [*PeopleSoft Enterprise* システムユーザ] エリアで、BI プラットフォームが PeopleSoft Enterprise データベースにログオンする際に使用する、データベースのユーザ名とパスワードを入力します。
8. [*PeopleSoft Enterprise* ドメイン] 領域で、PeopleSoft Enterprise 環境に接続するのに使用するドメイン名と QAS アドレスを入力して、[追加] をクリックします。

   > ⓘ 注記
   >
   > 複数の PeopleSoft ドメインがある場合は、アクセス対象となる追加のドメインに対してこのステップを繰り返します。最初に入力するドメインがデフォルトドメインになります。
9. [更新]をクリックして、変更内容を保存します。

9.6.3 BI プラットフォームへの PeopleSoft ロールのマップ

BI プラットフォームでは、PeopleSoft ロールをマップするごとに 1 つのグループが自動的に作成されます。同様に、SAP BusinessObjects Enterprise は、マップされた PeopleSoft ロールのメンバーを表すエイリアスを作成します。

作成されたエイリアスごとにユーザアカウントを 1 つ作成できます。

ただし、複数のシステムを実行し、ユーザが複数のシステムのアカウントを持っている場合は、BI プラットフォームでアカウントを作成する前に、同じ名前の 1 つのエイリアスに各ユーザを割り当てることができます。

これを行うことで、BI プラットフォームで同じユーザに対して作成されるアカウントの数を減らすことができます。

たとえば、PeopleSoft HR 8.3 と PeopleSoft Financials 8.4 を実行しているときに、30 人のユーザが両方のシステムへのアクセス権を持っている場合、それらのユーザに対して 30 個のアカウントだけが作成されます。各ユーザ

を同じ名前の 1 つのエイリアスに割り当てない場合は、BI プラットフォーム内の 30 人のユーザに対して 60 個のアカウントが作成されます。

ただし、複数のシステムを実行し、ユーザ名が重なる場合は、作成されるエイリアスごとに新しいメンバーアカウントを作成する必要があります。

たとえば、Russell Aquino のユーザアカウント(ユーザ名は "raquino")を使用して PeopleSoft HR 8.3 を実行し、Raoul Aquino のユーザアカウント(ユーザ名は "raquino")を使用して PeopleSoft Financial 8.4 を実行している場合は、各ユーザのエイリアスに対して個別のアカウントを作成する必要があります。作成しない場合、これらの 2 人のユーザは同じ BI プラットフォームアカウントに追加されます。この 2 人のユーザは、独自の PeopleSoft 認証情報を使用して BI プラットフォームにログオンでき、両方の PeopleSoft システムからデータにアクセスできます。

9.6.3.1 PeopleSoft ロールを BI プラットフォームにマップする

BI プラットフォーム JVM (Java 仮想マシン) に PeopleSoft サーバへの証明書がない場合、以下で説明する主なステップの前に、これらの追加の手順を実行する必要があります。

1. PeopleSoft サーバから .cer ファイルを取得します。
2. .cer ファイルを `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥jre¥lib¥security` にコピーします。
3. security ディレクトリから、以下のコマンドを実行します。`"<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥bin¥keytool.exe" -import -file <peoplesoftserver>.cer -keystore cacerts -alias <peoplesoftserver>`
4. Web アプリケーションサーバを再起動します。

主なステップは、以下のとおりです。

1. セントラル管理コンソールに管理者としてログオンします。
2. [認証] をクリックします。
3. [*PeopleSoft Enterprise*] をダブルクリックします。
4. [ロール] タブの [PeopleSoft Enterprise ドメイン] エリアで、BI プラットフォームにマップするロールに関連付けられたドメインを選択します。
5. 次のいずれかのオプションを使用して、マップするロールを選択します。
   - [*PeopleSoft Enterprise* ロール] エリアのロールの検索ボックスに、BI プラットフォームにマップする検索対象のロールを入力し、[>] をクリックします。
   - [利用可能なロール] 一覧で、BI プラットフォームにマップするロールを選択し、[>] をクリックします。

> **注記**
>
> 特定のユーザまたはロールを検索している場合は、ワイルドカード % を使用できます。たとえば、"A" で始まるすべてのロールを検索する場合は、「*A%*」と入力します。検索では大文字と小文字も区別されます。

> **注記**
>
> ロールを別のドメインからマップする場合は、利用可能なドメインの一覧から、別のドメインのロールと一致する新しいドメインを選択する必要があります。

6. [ユーザの更新] タブに移動し、[更新] ボタンをクリックするか、更新をスケジュールします。
7. [オプション] タブで、[新しいユーザのオプション] エリアに移動し、次のオプションのいずれかを選択します。
   - 追加した各エイリアスを同一名のアカウントに割り当てる
     このオプションは、複数の PeopleSoft Enterprise システムを実行し、ユーザが複数のシステムのアカウントを持っている (および各ユーザがシステムごとに異なるユーザ名を持っている) 場合に選択します。
   - 追加するすべてのエイリアスに新しいアカウントを作成する
     このオプションは、PeopleSoft Enterprise システムを 1 つだけ実行している場合、またはユーザの多くがシステムのいずれか 1 つにアカウントを持っている場合、あるいは、2 つ以上のシステムで異なるユーザに対して同じユーザ名が使用されている場合に選択します。
8. [エイリアス更新オプション] エリアで、次のオプションのいずれかを選択します。
   - エイリアスの更新時に新しいエイリアスを作成する
     このオプションは、BI プラットフォームにマップされるすべてのユーザに新しいエイリアスを作成する場合に選択します。新しいアカウントが BI プラットフォームアカウントを持たないユーザに対して追加されます。または [追加するすべてのエイリアスに新しいアカウントを作成する] オプションを選択した場合は、新しいアカウントがすべてのユーザに対して追加されます。
   - ユーザのログオン時にのみ新しいエイリアスを作成する
     このオプションは、マップするロールに多くのユーザが含まれているが、その一部のユーザのみが BI プラットフォームを使用する場合に選択します。BI プラットフォームは、ユーザに対してエイリアスやアカウントを自動で作成しません。代わりに、BI プラットフォームに初めてログインしたユーザに対してのみエイリアス (必要な場合は、アカウントも) を作成します。これはデフォルトのオプションです。
9. [新しいユーザのオプション] エリアで、新しいユーザを作成する方法を指定します。

   次のいずれかのオプションを選択します。
   - 新しいユーザを登録ユーザとして作成する
     登録ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。登録ユーザライセンスは特定のユーザに関連付けられており、ユーザはそのユーザ名およびパスワードに基づいてシステムにアクセスすることができます。このため、登録ユーザは、システムに接続している他のユーザの数に関係なく接続できます。このオプションを使用して作成したユーザアカウントに使用できる登録ユーザライセンスを持っている必要があります。

     > **注記**
     >
     > 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。
     >
     > ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。
   - 新しいユーザを同時接続ユーザとして作成する
     同時接続ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。同時接続ライセンスでは BI プラットフォームに同時接続できるユーザ数が指定されます。この種類のライセンスは、少ないユーザ数の同時接続ライセンスで多数のユーザをサポートできるため、柔軟性に優れています。たとえば、ユーザが BI プラットフォームにアクセスする頻度と時間の長さによって、100 ユーザ同時接続ライセンスで 250、500、または 700 のユーザをサポートできます。

   選択したロールが BI プラットフォームにグループとして表示されます。

9.6.3.2 再マップの考慮事項

すでに BI プラットフォームにマップされているロールにユーザを追加する場合は、そのロールを再マップして、ユーザを BI プラットフォームに追加する必要があります。ロールを再マップする場合は、ユーザを登録ユーザまたは同時接続ユーザとしてマップするオプションは、ロールに追加した新しいユーザにのみ影響します。

たとえば最初に、[新しいユーザを指定ユーザとして作成する] オプションを選択して、ロールを BI プラットフォームにマップします。後から同じロールにユーザを追加して、[新しいユーザを同時接続ユーザとして作成する] オプションを選択してロールを再マップします。

この場合、ロールの新しいユーザだけが同時接続ユーザとして BI プラットフォームにマップされ、すでにマップされているユーザは登録ユーザのままになります。最初に同時接続ユーザとしてユーザをマップし、その後に設定を変更して新しいユーザを登録ユーザとして再マップした場合も同じです。

9.6.3.3 ロールをマップ解除する

1. セントラル管理コンソールに管理者としてログオンします。
2. [認証]をクリックします。
3. [*PeopleSoft Enterprise*] をクリックします。
4. [ロール] をクリックします。
5. 削除するロールを選択して、[<] をクリックします。
6. *[更新]*をクリックします。

   ロールのメンバーは、他のアカウントまたはエイリアスを持っていない限り、BI プラットフォームにアクセスできなくなります。

   > ⓘ 注記
   >
   > 特定のユーザをログオンさせないようにするために、BI プラットフォームにマップする前に、個々のアカウントを削除するか、ロールからユーザを削除することもできます。

9.6.4 ユーザの更新のスケジュール

ERP システムのユーザデータへの変更が BI プラットフォームユーザデータに確実に反映されるよう、定期的なユーザの更新をスケジュールできます。この更新は、セントラル管理コンソール (CMC) で設定したマッピング設定に従って、ERP ユーザと BI プラットフォームユーザを自動的に同期します。

インポートされたロールの更新を実行し、スケジュールするためのオプションは 2 つあります。

- ロールのみを更新: このオプションを使用すると、BI プラットフォームにインポート済みの現在マップされているロール間のリンクのみを更新します。頻繁に更新を実行する予定があり、システムリソースの使用状況に懸念がある場合は、このオプションを使用します。ロールを更新するだけでは、新しいユーザアカウントは作成されません。
- ロールとエイリアスを更新: このオプションを使用すると、ロール間のリンクを更新するだけでなく、ERP システムに追加された新しいユーザエイリアス用の新しいユーザアカウントを BI プラットフォームに作成します。

> ⓘ 注記
>
> 認証を有効化しているときに、更新時にユーザエイリアスを自動で作成するよう指定していない場合は、新しいエイリアスに対してアカウントは作成されません。

9.6.4.1 ユーザの更新をスケジュールする

BI プラットフォームにロールをマップしたら、これらのロールの更新方法を指定する必要があります。

1. [ユーザの更新] タブをクリックします。
2. [ロールのみを更新] セクションまたは [ロールとエイリアスを更新] セクションのいずれかで、[スケジュール] をクリックします。

   > → ヒント
   >
   > すぐに更新を実行する場合は、[今すぐ更新] をクリックします。

   > → ヒント
   >
   > 頻繁に更新をするためシステムリソースに懸念がある場合は、[ロールのみを更新] オプションを使用します。ロールとエイリアスの両方を更新するには、より多くの時間がかかります。

   [繰り返し] ダイアログボックスが表示されます。
3. [オブジェクトの実行] リストからオプションを選択し、必要なスケジュール情報をすべて入力します。

   更新をスケジュールする場合、次の表に示した定期スケジュールパターンの中から選択することができます。

定期スケジュールパターン	説明
時間単位	更新は毎時間実行されます。開始時間、開始および終了日を指定します。
日単位	更新は毎日または指定した日数ごとに実行されます。実行時刻、開始日および終了日を指定することができます。
週単位	更新は毎週実行されます。1 週間に 1 回または数回実行することができます。実行する曜日、時間、開始および終了日を指定することができます。
月単位	更新は毎月または数カ月ごとに実行されます。実行時刻、開始日および終了日を指定することができます。
N 日	更新は毎月指定された日付に実行されます。実行する日にち、時間、開始および終了日を指定することができます。
第 1 月曜日	更新は毎月第 1 月曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
月末日	オブジェクトは毎月末日に実行されます。実行時刻、開始日および終了日を指定することができます。
第 N 週の X 日	更新は毎月特定の週の特定の曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
カレンダ	更新は、すでに作成されているカレンダで指定した日付に実行されます。

4. スケジュール情報の入力を終了したら、[スケジュール] をクリックします。

次回のスケジュールされたロールの更新の日付が、[ユーザの更新] タブに表示されます。

> ⓘ 注記
>
> [ロールのみを更新] セクションまたは [ロールとエイリアスを更新] セクションのいずれかで、[スケジュールされた更新のキャンセル] をクリックすると、いつでも次回のスケジュールされた更新をキャンセルできます。

9.6.5 PeopleSoft セキュリティブリッジの使用

BI プラットフォームのセキュリティブリッジ機能を使用して、PeopleSoft EPM セキュリティ設定を BI プラットフォームにインポートできます。

セキュリティブリッジは、次の 2 つのモードで動作します。

- 設定モード
  設定モードでは、セキュリティブリッジは応答ファイルを作成するためのインタフェースを提供します。この応答ファイルが、実行モードでのセキュリティブリッジの動作を管理します。
- 実行モード
  応答ファイルで定義したパラメータに基づき、セキュリティブリッジは PeopleSoft EPM のディメンションテーブルのセキュリティ設定を BI プラットフォームのユニバースにインポートします。

9.6.5.1 セキュリティ設定のインポート

セキュリティ設定をインポートするには、次のタスクを順番に実行する必要があります。

- セキュリティブリッジの管理対象となるオブジェクトを定義する。
- 応答ファイルを作成する。
- セキュリティブリッジアプリケーションを実行する。

設定のインポート後のセキュリティ管理については、セキュリティ設定の管理 [360 ページ]を参照してください。

9.6.5.1.1 マネージドオブジェクトの定義

セキュリティブリッジの実行前に、アプリケーションの管理対象となるオブジェクトを決定します。セキュリティブリッジは、1 つまたは複数の PeopleSoft ロール、1 つの BI プラットフォームグループ、および 1 つまたは複数のユニバースを管理します。

- マネージド PeopleSoft ロール
  PeopleSoft システムにはロールが含まれます。これらのロールのメンバーは、PeopleSoft EPM 経由で PeopleSoft データを使用できます。管理者は、BI プラットフォームのマネージドユニバースへのアクセス権限を提供または更新するメンバーを含むロールを選択する必要があります。
  これらのロールのメンバーに定義されるアクセス権限は、PeopleSoft EPM でのそれぞれの権限に基づきます。セキュリティブリッジはこれらのセキュリティ設定を BI プラットフォームにインポートします。

- マネージド BI プラットフォームグループ
  セキュリティブリッジを実行すると、マネージド PeopleSoft ロールの各メンバーに対して BI プラットフォームでのユーザが作成されます。
  ユーザが作成されるグループが、マネージド BI プラットフォームグループです。このグループのメンバーは、それぞれが所有するマネージドユニバースへのアクセス権限がセキュリティブリッジの管理対象となるユーザです。ユーザは 1 つのグループに作成されるため、マネージド BI プラットフォームグループから特定のユーザを削除するだけで、そのユーザに対するセキュリティ設定の更新を停止するようにセキュリティブリッジを設定できます。
  セキュリティブリッジの実行前に、ユーザの作成場所となる BI プラットフォームのグループを選択する必要があります。存在しないグループを指定した場合、セキュリティブリッジは BI プラットフォームでそのグループを作成します。
- マネージドユニバース
  マネージドユニバースは、セキュリティブリッジが PeopleSoft EPM からセキュリティ設定をインポートするユニバースです。BI プラットフォームシステムに保存されているユニバースから、セキュリティブリッジの管理対象となるユニバースを選択する必要があります。マネージド BI プラットフォームグループのメンバーでもあるマネージド PeopleSoft ロールのメンバーは、PeopleSoft EPM からアクセスできないユニバースを経由してデータにアクセスすることはできません。

9.6.5.1.2 応答ファイルを作成する

1. セキュリティブリッジのインストール時に指定したフォルダを開き、`crpsepmsecuritybridge.bat`(Windows)および `crpsempsecuritybridge.sh`(UNIX)ファイルを実行します。

   > ⓘ 注記
   >
   > Windows の場合、デフォルトでは、この場所は `C:¥Program Files¥Business Objects¥BusinessObjects 12.0 Integration Kit for PeopleSoft¥epm` です。

   [PeopleSoft EPM 用セキュリティブリッジ]ダイアログボックスが表示されます。
2. [新規作成]を選択して応答ファイルを作成するか、[開く]、[参照]の順でクリックして、変更する応答ファイルを指定します。ファイルに必要な言語を選択します。
3. [次へ] をクリックします。
4. *PeopleSoft EPM SDK* および *BI プラットフォーム SDK* の保存場所を入力します。

   > ⓘ 注記
   >
   > PeopleSoft EPM SDK は通常、`<PS_HOME>/class/com.peoplesoft.epm.pf.jar` の PeopleSoft サーバに置かれます。

   > ⓘ 注記
   >
   > BI プラットフォーム SDK は通常、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib` に置かれます。

5. [次へ] をクリックします。

   このダイアログボックスでは、PeopleSoft データベースの接続情報とドライバ情報を入力するように指示されます。

6. データベースリストから適切なデータベースの種類を選択し、次のフィールドに情報を入力します。

フィールド	説明
データベース	PeopleSoft データベースの名前
ホスト	データベースがホストされているサーバの名前
ポート番号	サーバにアクセスするためのポート番号
クラスの場所	データベースドライバのクラスファイルの保存場所
ユーザ名	ユーザ名
パスワード	パスワード

7. [次へ] をクリックします。

   セキュリティブリッジが実行に使用するすべてのクラスの一覧が、ダイアログボックスに表示されます。必要な場合は、この一覧へのクラスの追加や、一覧からのクラスの削除を実行できます。

8. [次へ] をクリックします。

   このダイアログボックスでは、BI プラットフォームの接続情報を入力するように指示されます。

9. 次のフィールドに、適切な情報を入力します。

フィールド	説明
サーバ	Central Management Server (CMS) が置かれているサーバ名
ユーザ名	ユーザ名
パスワード	パスワード
認証	使用している認証タイプ

10. [次へ] をクリックします。
11. BI プラットフォームグループを選択して、[次へ] をクリックします。

> ⓘ 注記
>
> このフィールドで指定するグループは、マネージド PeopleSoft ロールのメンバーに対してセキュリティブリッジがユーザを作成するグループです。

> ⓘ 注記
>
> 存在しないグループを指定した場合、セキュリティブリッジはそのグループを作成します。

   PeopleSoft システムのロールの一覧が、ダイアログボックスに表示されます。

12. セキュリティブリッジの管理対象とするロールの [インポート] オプションを選択して、[次へ] をクリックします。

> ⓘ 注記
>
> セキュリティブリッジは、選択したロールの各メンバーについて、マネージド BI プラットフォームグループ (前の手順で指定済み) にユーザを作成します。

   BI プラットフォームのユニバースの一覧が、ダイアログボックスに表示されます。

13. セキュリティブリッジを使用してセキュリティ設定をインポートするユニバースを選択して、[次へ] をクリックします。
14. セキュリティブリッジログファイルの名前と、このログファイルの保存場所を指定します。ログファイルを使用して、セキュリティブリッジによる PeopleSoft EPM からのセキュリティ設定のインポートが正常に実行されたかどうかを判断できます。
15. [次へ] をクリックします。

    実行モードの間、セキュリティブリッジが使用する応答ファイルのプレビューが、ダイアログボックスに表示されます。
16. *[保存]*をクリックし、応答ファイルの保存場所を選択します。
17. [次へ] をクリックします。

    これで、セキュリティブリッジの応答ファイルが正常に作成されました。
18. [終了]をクリックします。

> ⓘ 注記
>
> 応答ファイルは、手動で作成および変更できる Java プロパティファイルです。詳細については、「“PeopleSoft 応答ファイル”」を参照してください。

9.6.5.2 セキュリティ設定の適用

セキュリティ設定を適用するには、`crpsepmsecuritybridge.bat` バッチファイル (Windows) または `crpsempsecuritybridge.sh` ファイル (Unix) を実行し、引数として作成した応答ファイルを使用します。たとえば、**`crpsepmsecuritybridge.bat myresponsefile.properties`** (Windows) または **`crpsempsecuritybridge.sh myresponsefile.properties`** (Unix) と入力します。

セキュリティブリッジアプリケーションが実行されます。このアプリケーションは、応答ファイルで指定した PeopleSoft ロールのメンバーについて、BI プラットフォームユーザを作成し、セキュリティ設定を PeopleSoft EPM から適切なユニバースにインポートします。

9.6.5.2.1 マップの留意点

実行モードの間、セキュリティブリッジはマネージド PeopleSoft ロールの各メンバーに対して BI プラットフォームにユーザを作成します。

作成されるユーザには Enterprise 認証エイリアスのみが付与され、BI プラットフォームはこれらのユーザにランダムパスワードを割り当てます。したがって、管理者が手動で新しいパスワードを割り当てるか、または PeopleSoft セキュリティプラグイン経由で BI プラットフォームにロールをマップすることによってユーザの PeopleSoft 認証によるログオンが可能になるまで、ユーザは BI プラットフォームにログオンできません。

9.6.5.3 セキュリティ設定の管理

セキュリティブリッジの管理対象のオブジェクトを変更することによって、適用済みのセキュリティ設定を管理できます。

9.6.5.3.1 マネージドユーザ

セキュリティブリッジは、次の条件に基づいてユーザを管理します。

- ユーザがマネージド PeopleSoft ロールのメンバーかどうか
- ユーザがマネージド BI プラットフォームグループのメンバーかどうか

BI プラットフォームでユニバース経由での PeopleSoft データへのアクセスをユーザに許可する場合、そのユーザがマネージド PeopleSoft ロールとマネージド BI プラットフォームグループの両方のメンバーであることを確認してください。

- BI プラットフォームにアカウントを持たないマネージド PeopleSoft ロールのメンバーについては、セキュリティブリッジがアカウントを作成してランダムパスワードを割り当てます。ユーザに BI プラットフォームへのログオンを許可する場合、管理者は手動で新しいパスワードを割り当てるか、PeopleSoft セキュリティプラグイン経由で BI プラットフォームにロールをマップするかを決定する必要があります。
- マネージド BI プラットフォームグループのメンバーでもあるマネージド PeopleSoft ロールのメンバーについては、そのユーザに適用されているセキュリティ設定をセキュリティブリッジが更新します。したがってこれらのユーザは、該当するデータへのマネージドユニバースからのアクセス権限を持つことになります。

マネージド PeopleSoft ロールのメンバーが、BI プラットフォームにアカウントを持つものの、マネージド BI プラットフォームグループのメンバーではない場合は、セキュリティブリッジはそのユーザに適用されているセキュリティ設定を更新しません。通常この状況は、セキュリティブリッジが作成したユーザアカウントを、管理者が手動でマネージド BI プラットフォームグループから削除した場合にのみ発生します。

> ⓘ 注記
>
> これは、セキュリティの効果的な管理方法です。マネージド BI プラットフォームグループからユーザを削除することによって、そのユーザに対して PeopleSoft でのセキュリティ設定とは異なる設定を行うことができるからです。

反対に、マネージド BI プラットフォームグループのメンバーが、マネージド PeopleSoft ロールのメンバーではない場合、セキュリティブリッジはそのユーザに対してマネージドユニバースへのアクセス権を付与しません。通常この状況は、セキュリティブリッジが BI プラットフォームにマップしたユーザを、PeopleSoft 管理者がマネージド PeopleSoft ロールから削除した場合にのみ発生します。

> ⓘ 注記
>
> この方法で、セキュリティを管理することもできます。マネージド PeopleSoft ロールからユーザを削除することにより、PeopleSoft からのデータへのアクセス権から確実にそのユーザを除外できます。

9.6.5.3.2 マネージドユニバース

セキュリティブリッジは、制限セットを使用してユニバースを管理します。このセットは、マネージドユーザがマネージドユニバースからアクセスできるデータを制限します。

制限セットとは、制限のグループ(クエリ制御や SQL 生成に対する制限など)です。セキュリティブリッジは、マネージドユニバースに対する行アクセス制限やオブジェクトアクセス制限を適用または更新します。

- セキュリティブリッジは、PeopleSoft EPM で定義されているディメンションテーブルに対し、行アクセス制限を適用します。これらの制限はユーザ固有であり、次のいずれかに設定できます。
  - ユーザは、すべてのデータへのアクセス権を持つ。
  - ユーザは、どのデータに対してもアクセス権を持たない。
  - ユーザは、PeopleSoft での行レベル権限に基づくアクセス権を持つ。この許可は、PeopleSoft EPM で定義されるセキュリティ結合テーブル(SJT)を通じて公開されます。
- セキュリティブリッジは、オブジェクトアクセス制限を適用して、メジャーオブジェクトがアクセスするフィールドに基づき、オブジェクトを評価します。
  PeopleSoft でメトリクスとして定義されるフィールドにメジャーオブジェクトがアクセスする場合、メジャーオブジェクトへのアクセスは、PeopleSoft の参照メトリクスに対するユーザのアクセス権の有無によって、許可または不許可が決定されます。ユーザがこのメトリクスにアクセスできない場合、メジャーオブジェクトへのアクセスは拒否されます。ユーザがすべてのメトリクスにアクセスできる場合は、メジャーオブジェクトへのアクセスが許可されます。

管理者はまた、セキュリティブリッジの管理対象であるユニバース数を制限することによって、ユーザが PeopleSoft システムからアクセスできるデータを制限できます。

9.6.5.4 PeopleSoft 応答ファイル

BI プラットフォームのセキュリティブリッジ機能は、応答ファイルでの設定に基づいて動作します。

通常、応答ファイルは、設定モードでセキュリティブリッジが提供するインタフェースを使用して生成されます。ただし、このファイルは Java プロパティファイルであることから、手動で作成または変更することもできます。

この付録には、応答ファイルを手動で作成する場合に、このファイルに含める必要のあるパラメータについての情報が記載されています。

> ⓘ 注記
>
> 応答ファイルの作成時には、Java プロパティファイルのエスケープ要件(":"を"¥:"でエスケープするなど)に注意する必要があります。

9.6.5.4.1 応答ファイルのパラメータ

次の表は、応答ファイルに含まれるパラメータの説明です。

パラメータ	説明
classpath	必須 .jar ファイルのロードに使用するクラスパス。Windows および UNIX ともに、";"を使用して複数のクラスパスを区切ります。 クラスパスが必要なのは、`com.peoplesoft.epm.pf.jar` ファイルと JDBC ドライバ .jar ファイルです。
db.driver.name	PeopleSoft データベースへの接続に使用される JDBC ドライバ名 (`com.microsoft.jdbc.sqlserver.SQLServerDriver` など)
db.connect.str	PeopleSoft データベースへの接続に使用される JDBC 接続文字列 (`jdbc:microsoft:sqlserver:// vanrdpsft01:1433;DatabaseName=PRDMO` など)
db.user.name	PeopleSoft データベースへのログオンに使用するユーザ名
db.password	PeopleSoft データベースへのログオンに使用するパスワード
db.password.encrypted	このパラメータの値は、応答ファイルに含まれるパスワードパラメータを暗号化するかどうかを決定します。この値は、True または False のいずれかに設定します(値を指定しない場合、この値はデフォルトで False になります)。
enterprise.cms.name	ユニバースが置かれる CMS
enterprise.user.name	CMS へのログオンに使用するユーザ名
enterprise.password	CMS へのログオンに使用するパスワード
enterprise.password.encrypted	このパラメータの値は、応答ファイルに含まれるパスワードパラメータを暗号化するかどうかを決定します。この値は、True または False のいずれかに設定します(値を指定しない場合、この値はデフォルトで False になります)。
enterprise.authMethod	CMS へのログオンに使用する認証メソッド
enterprise.role	マネージド BI プラットフォームグループ。詳細については、マネージドオブジェクトの定義 [356 ページ]を参照してください。
enterprise.license	PeopleSoft からユーザをインポートするときに、ライセンスの種類を制御します。"0" は指定ユーザライセンスを設定します。"1" は同時接続ユーザライセンスを設定します。

パラメータ	説明
peoplesoft.role.n	マネージド PeopleSoft ロールの一覧詳細については、マネージドオブジェクトの定義 [356 ページ]を参照してください。 **<n>** は整数で、各エントリが前置記号 peoplesoft.role を持つ 1 つのプロパティを含みます。 ⓘ 注記 **<n>** は、1 を基本とします。 使用可能なすべての PeopleSoft ロールを示すには、"*"を使用します。たとえば n が 1 の場合は、これが応答ファイルで peoplesoft.role を前置記号として持つ唯一のプロパティです。
mapped.universe.n	セキュリティブリッジを更新するユニバースの一覧詳細については、マネージドオブジェクトの定義 [356 ページ]を参照してください。 **<n>** は整数で、各エントリが前置記号 mapped.universe を持つ 1 つのプロパティを含みます。 ⓘ 注記 **<n>** は、1 を基本とします。 使用可能なすべてのユニバースを示すには、"*"を使用します。たとえば n が 1 の場合には、これが応答ファイルで mapped.universe を前置記号として持つ唯一のプロパティです。
log4j.appender.file.File	セキュリティブリッジによって書き込まれるログファイル

パラメータ	説明
log4j.*	log4j の正常な動作に必要なデフォルトの log4j プロパティは、次のとおりです。 log4j.rootLogger=INFO, file, stdout log4j.appender.file=org.apache.log4j.RollingFile Appender log4j.appender.file.layout=org.apache.log4j.PatternLayout log4j.appender.file.MaxFileSize=5000KB log4j.appender.file.MaxBackupIndex=100 log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n log4j.appender.stdout=org.apache.log4j.ConsoleAppender log4j.appender.stdout.layout=org.apache.log4j.PatternLayout log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n
peoplesoft classpath	PeopleSoft EPM API .jar ファイルへのクラスパス このパラメータは省略できます。
enterprise.classpath	BI プラットフォーム SDK .jar ファイルへのクラスパス このパラメータは省略できます。
db.driver.type	PeopleSoft データベースの種類。このパラメータは、次のいずれか 1 つの値となります。 Microsoft SQL Server 2000 Oracle Database 10.1 DB2 UDB 8.2 Fixpack 7 カスタム Custom は、一般に認知されている種類またはバージョン以外のデータベースの指定に使用できます。 このパラメータは省略できます。
sql.db.class.location sql.db.host sql.db.port sql.db.database	SQL Server JDB ドライバ .jar ファイルの場所、SQL Server のホストマシン、SQL Server のポート、および SQL Server データベース名 これらのパラメータは、db.driver.type が Microsoft SQL Server 2000 の場合にのみ使用できます。 このパラメータは省略できます。

パラメータ	説明
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	Oracle JDBC ドライバ .jar ファイルの場所、Oracle データベースのホストマシン、Oracle データベースのポート、および Oracle データベース SID これらのパラメータは、db.driver.type が Oracle Database 10.1 の場合にのみ使用できます。 このパラメータは省略できます。
db2.db.class.location db2.db.host db2.db.port db2.db.sid	DB2 JDBC ドライバ .jar ファイルの場所、DB2 データベースのホストマシン、DB2 データベースのポート、および DB2 データベース SID これらのパラメータは、db.driver.type が DB2 UDB 8.2 Fixpack 7 の場合にのみ使用できます。 このパラメータは省略できます。
custom.db.class.location custom.db.drivername custom.db.connectStr	カスタム JDBC ドライバの場所、名前、接続文字列 これらのパラメータは、db.driver.type が Custom の場合にのみ使用できます。 このパラメータは省略できます。

9.7 JD Edwards 認証

9.7.1 概要

BI プラットフォームで JD Edwards データを使用するには、JD Edwards デプロイメントに関する情報をシステムに設定する必要があります。この情報を基に BI プラットフォームは、JD Edwards EnterpriseOne 認証情報を使用して BI プラットフォームにログオンするユーザを認証することができます。

9.7.2 JD Edwards EnterpriseOne 認証の有効化

BI プラットフォームで JD Edwards EnterpiseOne 情報を使用できるようにするには、JD Edwards EnterpriseOne システムへの認証方法に関する情報がプラットフォームに必要です。

9.7.2.1 BI プラットフォームで JD Edwards EnterpriseOne 認証を有効化する

1. セントラル管理コンソールに管理者としてログオンします。
2. [管理]領域で[認証]をクリックします。
3. [*JD Edwards EnterpriseOne*] をダブルクリックします。
   [*JD Edwards EnterpriseOne*] ページが表示されます。
4. [オプション] タブで [*JD Edwards EnterpriseOne 認証の有効化*] チェックボックスをオンにします。
5. BI プラットフォームのデプロイメントに応じて、[新しいエイリアス]、[更新オプション]、および [新しいユーザのオプション] を適切に変更します。更新をクリックして変更を保存してから、システムタブに移動します。
6. *[Servers]* タブをクリックします。
7. `jdeutil.jar`、`kernel.jar`、および `log4j.jar` を JD Edwards のインストールから以下の場所にコピーします (Windows の場合): `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib¥jdedwards¥default¥jdedwards¥` and `<INSTALLDIR>¥Tomcat¥lib¥`。
8. Tomcat および Server Intelligence Agent を再起動します。
9. [*JD Edwards EnterpriseOne システムユーザ*] エリアで、JD Edwards EnterpriseOne データベースにログオンするための BI プラットフォームのデータベースユーザ名とパスワードを入力します。
10. [*JD Edwards EnterpriseOne ドメイン*] 領域で、JD Edwards EnterpriseOne 環境に接続するのに使用する名前、ホスト、ポートを入力します。
11. 環境の名前を入力し、[追加] をクリックします。
12. [更新]をクリックして、変更内容を保存します。

9.7.3 BI プラットフォームへの JD Edwards EnterpriseOne ロールのマップ

BI プラットフォームでは、JD Edwards EnterpriseOne ロールをマップするごとに 1 つのグループが自動的に作成されます。同様に、マップされた JD Edwards EnterpriseOne ロールのメンバーを表すエイリアスが作成されます。

作成されたエイリアスごとにユーザアカウントを 1 つ作成できます。

ただし、複数のシステムを実行し、ユーザが複数のシステムのアカウントを持っている場合は、BI プラットフォームでアカウントを作成する前に、同じ名前の 1 つのエイリアスに各ユーザを割り当てることができます。

これを行うことで、BI プラットフォームで同じユーザに対して作成されるアカウントの数を減らすことができます。

たとえば、JD Edwards EnterpriseOne のテスト環境と実稼動環境を実行しており、30 人のユーザが両方のシステムへのアクセス権を持っている場合は、これらのユーザに対してアカウントが 30 個だけ作成されます。各ユーザを同じ名前の 1 つのエイリアスに割り当てない場合は、BI プラットフォーム内の 30 人のユーザに対して 60 個のアカウントが作成されます。

ただし、複数のシステムを実行し、ユーザ名が重なる場合は、作成されるエイリアスごとに新しいメンバーアカウントを作成する必要があります。

たとえば、Russell Aquino のユーザアカウント(ユーザ名は "raquino")でテスト環境を実行しており、Raoul Aquino のユーザアカウント(ユーザ名は "raquino")で実稼動環境を実行している場合は、各ユーザのエイリアスに対して

個別のアカウントを作成する必要があります。作成しない場合、これらの 2 人のユーザは同じ BI プラットフォームアカウントに追加され、それぞれの JD Edwards EnterpriseOne 認証情報を使って BI プラットフォームにログオンできません。

9.7.3.1 JD Edwards EnterpriseOne ロールをマップする

1. セントラル管理コンソールに管理者としてログオンします。
2. [管理] 領域で [認証] をクリックします。
3. [*JD Edwards EnterpriseOne*] をダブルクリックします。
4. [新しいエイリアスのオプション]エリアで、次のオプションのいずれかを選択します。
   - 追加した各エイリアスを同一名のアカウントに割り当てる
     このオプションは、複数の JD Edwards EnterpriseOne Enterprise システムを実行しており、ユーザが複数のシステムのアカウントを持っている (各ユーザがシステムごとに異なるユーザ名を持っている) 場合に選択します。
   - 追加するすべてのエイリアスに新しいアカウントを作成する
     このオプションは、1 つの JD Edwards EnterpriseOne システムしか実行していない場合、大部分のユーザがいずれか 1 つのシステムのアカウントしか持っていない場合、または 2 つ以上のシステムで異なるユーザに対して同じユーザ名が使用されている場合に選択します。
5. [更新オプション] エリアで、次のオプションのいずれかを選択します。
   - 新しいエイリアスを追加して新しいユーザを作成する
     このオプションは、BI プラットフォームにマップされるすべてのユーザに新しいエイリアスを作成する場合に選択します。新しいアカウントが BI プラットフォームアカウントを持たないユーザに対して追加されます。または [追加するすべてのエイリアスに新しいアカウントを作成する] オプションを選択している場合は、新しいアカウントがすべてのユーザに対して追加されます。
   - 新しいエイリアスの追加および新しいユーザの作成を行わない
     このオプションは、マップするロールに多くのユーザが含まれているが、その一部のユーザのみが BI プラットフォームを使用する場合に選択します。システムは、ユーザに対してエイリアスやアカウントを自動で作成しません。代わりに、BI プラットフォームに初めてログインしたユーザに対してのみエイリアス (必要な場合は、アカウントも) を作成します。これはデフォルトのオプションです。
6. [新しいユーザのオプション] エリアで、新しいユーザを作成する方法を指定します。

   次のいずれかのオプションを選択します。
   - 新しいユーザを登録ユーザとして作成する
     登録ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。登録ユーザライセンスは特定のユーザに関連付けられており、ユーザはそのユーザ名およびパスワードに基づいてシステムにアクセスすることができます。このため、登録ユーザは、システムに接続している他のユーザの数に関係なく接続できます。このオプションを使用して作成したユーザアカウントに使用できる登録ユーザライセンスを持っている必要があります。

     > ⓘ 注記
     >
     > 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。
     >
     > ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。

- 新しいユーザを同時接続ユーザとして作成する
  同時接続ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。同時接続ライセンスでは BI プラットフォームに同時接続できるユーザ数が指定されます。この種類のライセンスは、少ないユーザ数の同時接続ライセンスで多数のユーザをサポートできるため、柔軟性に優れています。たとえば、ユーザが BI プラットフォームにアクセスする頻度と時間の長さによって、100 ユーザ同時接続ライセンスで 250、500、または 700 のユーザをサポートできます。

選択したロールが BI プラットフォームにグループとして表示されます。

7. [ロール] タブをクリックします。
8. [ドメイン一覧] で、マップするロールを含む JD Edwards サーバを選択します。
9. [利用可能なロール] で、BI プラットフォームにマップするロールを選択して [<] をクリックします。
10. [更新] をクリックします。
    これらのロールが BI プラットフォームにマップされます。

9.7.3.2 再マップの考慮事項

すでに BI プラットフォームにマップされているロールにユーザを追加する場合は、そのロールを再マップして、ユーザを BI プラットフォームに追加する必要があります。ロールを再マップする場合は、ユーザを登録ユーザまたは同時接続ユーザとしてマップするオプションは、ロールに追加した新しいユーザにのみ影響します。

たとえば最初に、[新しいユーザを指定ユーザとして作成する] オプションを選択して、ロールを BI プラットフォームにマップします。後から同じロールにユーザを追加して、[新しいユーザを同時接続ユーザとして作成する] オプションを選択してロールを再マップします。

この場合、ロールの新しいユーザだけが同時接続ユーザとして BI プラットフォームにマップされ、すでにマップされているユーザは登録ユーザのままになります。最初に同時接続ユーザとしてユーザをマップし、その後に設定を変更して新しいユーザを登録ユーザとして再マップした場合も同じです。

9.7.3.3 ロールをマップ解除する

1. セントラル管理コンソールに管理者としてログオンします。
2. [管理]エリアで、[認証]をクリックします。
3. [*JD Edwards EnterpriseOne*] のタブをクリックします。
4. [ロール]領域で、削除するロールを選択し、[<]をクリックします。
5. *[更新]*をクリックします。

   ロールのメンバーは、他のアカウントまたはエイリアスを持っていない限り、BI プラットフォームにアクセスできなくなります。

   > ⓘ 注記
   >
   > 特定のユーザをログオンさせないようにするために、BI プラットフォームにマップする前に、個々のアカウントを削除するか、ロールからユーザを削除することもできます。

9.7.4 ユーザの更新のスケジュール

ERP システムのユーザデータへの変更が BI プラットフォームユーザデータに確実に反映されるよう、定期的なユーザの更新をスケジュールできます。この更新は、セントラル管理コンソール (CMC) で設定したマッピング設定に従って、ERP ユーザと BI プラットフォームユーザを自動的に同期します。

インポートされたロールの更新を実行し、スケジュールするためのオプションは 2 つあります。

- ロールのみを更新: このオプションを使用すると、BI プラットフォームにインポート済みの現在マップされているロール間のリンクのみを更新します。頻繁に更新を実行する予定があり、システムリソースの使用状況に懸念がある場合は、このオプションを使用します。ロールを更新するだけでは、新しいユーザアカウントは作成されません。
- ロールとエイリアスを更新: このオプションを使用すると、ロール間のリンクを更新するだけでなく、ERP システムに追加された新しいユーザエイリアス用の新しいユーザアカウントを BI プラットフォームに作成します。

> ⓘ 注記
>
> 認証を有効化しているときに、更新時にユーザエイリアスを自動で作成するよう指定していない場合は、新しいエイリアスに対してアカウントは作成されません。

9.7.4.1 ユーザの更新をスケジュールする

BI プラットフォームにロールをマップしたら、これらのロールの更新方法を指定する必要があります。

1. [ユーザの更新] タブをクリックします。
2. [ロールのみを更新] セクションまたは [ロールとエイリアスを更新] セクションのいずれかで、[スケジュール] をクリックします。

   > → ヒント
   >
   > すぐに更新を実行する場合は、[今すぐ更新] をクリックします。

   > → ヒント
   >
   > 頻繁に更新をするためシステムリソースに懸念がある場合は、[ロールのみを更新] オプションを使用します。ロールとエイリアスの両方を更新するには、より多くの時間がかかります。

   [繰り返し] ダイアログボックスが表示されます。
3. [オブジェクトの実行] リストからオプションを選択し、必要なスケジュール情報をすべて入力します。

   更新をスケジュールする場合、次の表に示した定期スケジュールパターンの中から選択することができます。

定期スケジュールパターン	説明
時間単位	更新は毎時間実行されます。開始時間、開始および終了日を指定します。
日単位	更新は毎日または指定した日数ごとに実行されます。実行時刻、開始日および終了日を指定することができます。

定期スケジュールパターン	説明
週単位	更新は毎週実行されます。1 週間に 1 回または数回実行することができます。実行する曜日、時間、開始および終了日を指定することができます。
月単位	更新は毎月または数カ月ごとに実行されます。実行時刻、開始日および終了日を指定することができます。
N 日	更新は毎月指定された日付に実行されます。実行する日にち、時間、開始および終了日を指定することができます。
第 1 月曜日	更新は毎月第 1 月曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
月末日	オブジェクトは毎月末日に実行されます。実行時刻、開始日および終了日を指定することができます。
第 N 週の X 日	更新は毎月特定の週の特定の曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
カレンダ	更新は、すでに作成されているカレンダで指定した日付に実行されます。

4. スケジュール情報の入力を終了したら、[スケジュール] をクリックします。
   次回のスケジュールされたロールの更新の日付が、[ユーザの更新] タブに表示されます。

> ⓘ 注記
>
> [ロールのみを更新] セクションまたは [ロールとエイリアスを更新] セクションのいずれかで、[スケジュールされた更新のキャンセル] をクリックすると、いつでも次回のスケジュールされた更新をキャンセルできます。

9.8 Siebel 認証

9.8.1 Siebel 認証の有効化

BI プラットフォームで Siebel 情報を使用できるようにするには、Siebel システムの認証方法に関する情報が BI プラットフォームに必要です。

9.8.1.1 BI プラットフォームで Siebel 認証を有効化する

1. セントラル管理コンソールに管理者としてログオンします。
2. [管理]領域で[認証]をクリックします。
3. [*Siebel*]をダブルクリックします。
   [*Siebel*] ページが表示されます。[オプション]、[システム]、[職責]、および [ユーザの更新] の 4 つのタブがあります。
4. [オプション] タブで、[*Siebel* 認証を有効にする] チェックボックスをオンにします。

5. BI プラットフォームのデプロイメントに応じて、[新しいエイリアス]、[更新オプション]、および [新しいユーザのオプション] を適切に変更します。[更新]をクリックして変更を保存してから、[システム]タブに移動します。
6. [ドメイン] タブをクリックします。
7. [ドメイン名] フィールドに、接続先の Siebel システムのドメイン名を入力します。
8. [接続] で、そのドメインの接続文字列を入力します。
9. [ユーザ名] エリアで、Siebel データベースへのログオンに使用する BI プラットフォームのデータベースのユーザ名とパスワードを入力します。
10. [パスワード] エリアで、選択したユーザのパスワードを入力します。
11. [追加] をクリックして、[現在のドメイン] リストにシステムの情報を入力します。
12. [更新]をクリックして、変更内容を保存します。

9.8.2 BI プラットフォームへのマッピング

BI プラットフォームでは、Siebel ロールをマップするごとに 1 つのグループが自動的に作成されます。同様に、SAP BusinessObjects Enterprise は、マップされた Siebel ロールのメンバーを表すエイリアスを作成します。

作成されたエイリアスごとにユーザアカウントを 1 つ作成できます。

ただし、複数のシステムを実行し、ユーザが複数のシステムのアカウントを持っている場合は、BI プラットフォームでアカウントを作成する前に、同じ名前の 1 つのエイリアスに各ユーザを割り当てることができます。

これを行うことで、このプログラムで同じユーザに対して作成されるアカウントの数を減らすことができます。

たとえば、Siebel eBusiness のテスト環境と実稼動環境を実行しており、30 人のユーザが両方のシステムへのアクセス権を持っている場合は、これらのユーザに対してアカウントが 30 個だけ作成されます。各ユーザを同じ名前の 1 つのエイリアスに割り当てない場合は、BI プラットフォーム内の 30 人のユーザに対して 60 個のアカウントが作成されます。

ただし、複数のシステムを実行し、ユーザ名が重なる場合は、作成されるエイリアスごとに新しいメンバーアカウントを作成する必要があります。

たとえば、Russell Aquino のユーザアカウント(ユーザ名は "raquino")でテスト環境を実行しており、Raoul Aquino のユーザアカウント(ユーザ名は "raquino")で実稼動環境を実行している場合は、各ユーザのエイリアスに対して個別のアカウントを作成する必要があります。作成しない場合、これらの 2 人のユーザは同じアカウントに追加され、それぞれの Siebel eBusiness 認証情報を使って BI プラットフォームにログオンできません。

9.8.2.1 Siebel eBusiness ロールを BI プラットフォームにマップする

1. セントラル管理コンソールに管理者としてログオンします。
2. [認証] をクリックします。
3. [*Siebel*] をダブルクリックします。
4. [*Siebel* 認証の有効化] チェックボックスを選択します。
5. [新しいエイリアスのオプション] エリアで、次のオプションのいずれかを選択します。

- 追加した各エイリアスを同一名のアカウントに割り当てる
  このオプションは、複数の Siebel eBusiness システムを実行し、ユーザが複数のシステムのアカウントを持っている (および各ユーザがシステムごとに異なるユーザ名を持っている) 場合に選択します。
- 追加するすべてのエイリアスに新しいアカウントを作成する
  このオプションは、Siebel eBusiness システムを 1 つだけ実行している場合、またはユーザの多くがシステムのいずれか 1 つのアカウントを持っている場合、あるいは、2 つ以上のシステムで異なるユーザに対して同じユーザ名が使用されている場合に選択します。

6. [エイリアス更新オプション] エリアで、次のオプションのいずれかを選択します。
   - エイリアスの更新時に新しいエイリアスを作成する
     このオプションは、BI プラットフォームにマップされるすべてのユーザに新しいエイリアスを作成する場合に選択します。新しいアカウントが BI プラットフォームアカウントを持たないユーザに対して追加されます。または [追加するすべてのエイリアスに新しいアカウントを作成する] オプションを選択している場合は、新しいアカウントがすべてのユーザに対して追加されます。
   - ユーザのログオン時にのみ新しいエイリアスを作成する
     このオプションは、マップするロールに多くのユーザが含まれているが、その一部のユーザのみが BI プラットフォームを使用する場合に選択します。プログラムは、ユーザに対してエイリアスやアカウントを自動で作成しません。代わりに、BI プラットフォームに初めてログインしたユーザに対してのみエイリアス (必要な場合は、アカウントも) を作成します。これはデフォルトのオプションです。
7. [新しいユーザのオプション] エリアで、新しいユーザを作成する方法を指定します。

   BI プラットフォームのライセンスがユーザロールに基づいている場合は、次のいずれかのオプションを選択します。

   次のいずれかのオプションを選択します。

   - 新しいユーザを登録ユーザとして作成する
     登録ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。登録ユーザライセンスは特定のユーザに関連付けられており、ユーザはそのユーザ名およびパスワードに基づいてシステムにアクセスすることができます。このため、登録ユーザは、システムに接続している他のユーザの数に関係なく接続できます。このオプションを使用して作成したユーザアカウントに使用できる登録ユーザライセンスを持っている必要があります。

     > **注記**
     >
     > 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。
     >
     > ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。
   - 新しいユーザを同時接続ユーザとして作成する
     同時接続ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。同時接続ライセンスでは BI プラットフォームに同時接続できるユーザ数が指定されます。この種類のライセンスは、少ないユーザ数の同時接続ライセンスで多数のユーザをサポートできるため、柔軟性に優れています。たとえば、ユーザが BI プラットフォームにアクセスする頻度と時間の長さによって、100 ユーザ同時接続ライセンスで 250、500、または 700 のユーザをサポートできます。
8. [ロール] タブをクリックします。
9. ロールをマップする Siebel サーバに対応するドメインを選択します。
10. [利用可能なロール] で、マップするロールを選択して [>] をクリックします。

> ⓘ 注記
>
> ロールが多数ある場合は、[検索ロールの開始] フィールドを使用して、検索を絞り込みます。ロールの最初の文字とそれに続くワイルドカード（%）を入力し、[検索] をクリックします。

> ⓘ 注記
>
> 検索機能が動作するためには、Siebel プラグインの jar ファイルが Tomcat の lib ディレクトリ `<INSTALLDIR>¥tomcat¥webapps¥BOE¥WEB-INF¥lib` および `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib¥siebel¥default¥siebel` にデプロイされている必要があります。次に、Tomcat サーバおよび Server Intelligence Agent を再起動します。

11. [更新] をクリックします。
    これらのロールが BI プラットフォームにマップされます。

9.8.2.2 再マップの考慮事項

BI プラットフォームと Siebel の間でグループとユーザを同期させるには、[ユーザ同期の強制] を設定します。

> ⓘ 注記
>
> [ユーザ同期の強制]を選択するために、[新しいエイリアスを追加して新しいユーザを作成する]を最初に選択する必要があります。

ロールを再マップする場合は、ユーザを登録ユーザまたは同時接続ユーザとしてマップするオプションは、ロールに追加した新しいユーザにのみ影響します。

たとえば最初に、[新しいユーザを指定ユーザとして作成する] オプションを選択して、ロールを BI プラットフォームにマップします。後から同じロールにユーザを追加して、[新しいユーザを同時接続ユーザとして作成する] オプションを選択してロールを再マップします。

この場合、ロールの新しいユーザだけが同時接続ユーザとして BI プラットフォームにマップされ、すでにマップされているユーザは登録ユーザのままになります。最初に同時接続ユーザとしてユーザをマップし、その後に設定を変更して新しいユーザを登録ユーザとして再マップした場合も同じです。

9.8.2.3 ロールをマップ解除する

1. セントラル管理コンソールに管理者としてログオンします。
2. [管理]エリアで、[認証]をクリックします。
3. [*Siebel*]をダブルクリックします。
4. [ドメイン]タブで、マップを解除するロールに対応する Siebel ドメインを選択します。
5. [ロール]タブで、削除するロールを選択し、[<]をクリックします。
6. [更新]をクリックします。

   職責のメンバーは、他のアカウントまたはエイリアスを持っていない限り、BI プラットフォームにアクセスできなくなります。

> ⓘ 注記
>
> 特定のユーザをログオンさせないようにするために、BI プラットフォームにマップする前に、個々のアカウントを削除するか、ロールからユーザを削除することもできます。

9.8.3 ユーザの更新のスケジュール

ERP システムのユーザデータへの変更が BI プラットフォームユーザデータに確実に反映されるよう、定期的なユーザの更新をスケジュールできます。この更新は、セントラル管理コンソール (CMC) で設定したマッピング設定に従って、ERP ユーザと BI プラットフォームユーザを自動的に同期します。

インポートされたロールの更新を実行し、スケジュールするためのオプションは 2 つあります。

- ロールのみを更新: このオプションを使用すると、BI プラットフォームにインポート済みの現在マップされているロール間のリンクのみを更新します。頻繁に更新を実行する予定があり、システムリソースの使用状況に懸念がある場合は、このオプションを使用します。ロールを更新するだけでは、新しいユーザアカウントは作成されません。
- ロールとエイリアスを更新: このオプションを使用すると、ロール間のリンクを更新するだけでなく、ERP システムに追加された新しいユーザエイリアス用の新しいユーザアカウントを BI プラットフォームに作成します。

> ⓘ 注記
>
> 認証を有効化しているときに、更新時にユーザエイリアスを自動で作成するよう指定していない場合は、新しいエイリアスに対してアカウントは作成されません。

9.8.3.1 ユーザの更新をスケジュールする

BI プラットフォームにロールをマップしたら、これらのロールの更新方法を指定する必要があります。

1. [ユーザの更新] タブをクリックします。
2. [ロールのみを更新] セクションまたは [ロールとエイリアスを更新] セクションのいずれかで、[スケジュール] をクリックします。

   > → ヒント
   >
   > すぐに更新を実行する場合は、[今すぐ更新] をクリックします。

   > → ヒント
   >
   > 頻繁に更新をするためシステムリソースに懸念がある場合は、[ロールのみを更新] オプションを使用します。ロールとエイリアスの両方を更新するには、より多くの時間がかかります。

   [繰り返し] ダイアログボックスが表示されます。
3. [オブジェクトの実行] リストからオプションを選択し、必要なスケジュール情報をすべて入力します。

   更新をスケジュールする場合、次の表に示した定期スケジュールパターンの中から選択することができます。

定期スケジュールパターン	説明
時間単位	更新は毎時間実行されます。開始時間、開始および終了日を指定します。
日単位	更新は毎日または指定した日数ごとに実行されます。実行時刻、開始日および終了日を指定することができます。
週単位	更新は毎週実行されます。1 週間に 1 回または数回実行することができます。実行する曜日、時間、開始および終了日を指定することができます。
月単位	更新は毎月または数カ月ごとに実行されます。実行時刻、開始日および終了日を指定することができます。
N 日	更新は毎月指定された日付に実行されます。実行する日にち、時間、開始および終了日を指定することができます。
第 1 月曜日	更新は毎月第 1 月曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
月末日	オブジェクトは毎月末日に実行されます。実行時刻、開始日および終了日を指定することができます。
第 N 週の X 日	更新は毎月特定の週の特定の曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
カレンダ	更新は、すでに作成されているカレンダで指定した日付に実行されます。

4. スケジュール情報の入力を終了したら、[スケジュール] をクリックします。
   次回のスケジュールされたロールの更新の日付が、[ユーザの更新] タブに表示されます。

> ⓘ 注記
>
> [ロールのみを更新] セクションまたは [ロールとエイリアスを更新] セクションのいずれかで、[スケジュールされた更新のキャンセル] をクリックすると、いつでも次回のスケジュールされた更新をキャンセルできます。

9.9 Oracle EBS 認証

9.9.1 Oracle EBS 認証の有効化

BI プラットフォームで Oracle EBS 情報を使用できるようにするには、Oracle EBS システムの認証方法に関する情報が BI プラットフォームに必要です。

9.9.1.1 Oracle E-Business Suite 認証を有効化する

手順を実行する前に、以下の手順に従って、Oracle DLL および JAR ファイルを BI プラットフォーム にデプロイする必要があります。

1. Oracle データベースクライアントアプリケーションから `ojdbc11.dll` をダウンロードします。
2. ファイルを以下の場所にコピーします。

- Windows: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64`
- UNIX: `<INSTALLDIR>/sap_bobj/enterprise_xi40/platform`

3. Oracle データベースクライアントアプリケーションから `ojdbc5.jar` をダウンロードします。
4. ファイルを以下の場所にコピーします。
   - Windows: `<INSTALLDIR>¥Tomcat¥lib`
   - UNIX: `<INSTALLDIR>/sap_bobj/tomcat/lib`

1. セントラル管理コンソールに管理者としてログオンします。
2. [管理]領域で[認証]をクリックします。
3. [*Oracle EBS*]をクリックします。
   [*Oracle EBS*]ページが表示されます。[オプション]、[システム]、[職責]、および [ユーザの更新] の 4 つのタブがあります。
4. [オプション] タブでは、[*Oracle EBS* 認証を有効にする] チェックボックスを選択します。
5. BI プラットフォームのデプロイメントに応じて、[新しいエイリアス]、[更新オプション]、および [新しいユーザのオプション] を適切に変更します。[更新]をクリックして変更を保存してから、[システム]タブに移動します。
6. [システム]タブをクリックします。
7. [*Oracle EBS* システムユーザ] エリアで、BI プラットフォームが Oracle E-Business Suite データベースにログオンするために使用する、データベースのユーザ名とパスワードを入力します。
8. [*Oracle EBS* サービス]領域で、Oracle EBS 環境で使用されるサービス名を入力して、[追加]をクリックします。
9. [更新]をクリックして、変更内容を保存します。

ここで、Oracle EBS ロールをシステムにマップする必要があります。

関連情報

Oracle E-Business Suite ロールをマップする [377 ページ]

9.9.2 BI プラットフォームへの Oracle E-Business Suite ロールのマップ

BI プラットフォームでは、マップするそれぞれの Oracle E-Business Suite (EBS) ロールのグループが自動的に作成されます。また、マップされた Oracle E-Business Suite のロールのメンバーを表すエイリアスも作成されます。

作成されたエイリアスごとにユーザアカウントを 1 つ作成できます。ただし、複数のシステムを実行し、ユーザが複数のシステムのアカウントを持っている場合は、BI プラットフォームでアカウントを作成する前に、同じ名前の 1 つのエイリアスに各ユーザを割り当てることができます。

これを行うことで、システムで同じユーザに対して作成されるアカウントの数を減らすことができます。

たとえば、EBS のテスト環境と実稼動環境を実行しており、30 人のユーザが両方のシステムへのアクセス権を持っている場合は、これらのユーザに対してアカウントが 30 個だけ作成されます。各ユーザを同じ名前の 1 つのエイリアスに割り当てない場合は、BI プラットフォーム内の 30 人のユーザに対して 60 個のアカウントが作成されます。

ただし、複数のシステムを実行し、ユーザ名が重なる場合は、作成されるエイリアスごとに新しいメンバーアカウントを作成する必要があります。

たとえば、Russell Aquino のユーザアカウント(ユーザ名は "raquino")でテスト環境を実行しており、Raoul Aquino のユーザアカウント(ユーザ名は "raquino")で実稼動環境を実行している場合は、各ユーザのエイリアスに対して個別のアカウントを作成する必要があります。作成しない場合、これらの 2 人のユーザは同じ BI プラットフォームアカウントに追加されます。この 2 人のユーザは、独自の Oracle EBS 認証情報を使用してシステムにログオンでき、両方の EBS 環境からデータにアクセスできます。

9.9.2.1 Oracle E-Business Suite ロールをマップする

1. セントラル管理コンソールに管理者としてログオンします。
2. [管理]領域で[認証]をクリックします。
3. [*Oracle EBS*]をクリックします。
   [*Oracle EBS*]ページに[オプション]タブが表示されます。
4. [新しいエイリアスのオプション]エリアで、次のオプションのいずれかを選択します。
   - 追加した各 *Oracle EBS* エイリアスを同一名のアカウントに割り当てる
     このオプションは、複数の Oracle E-Business Suite システムを実行し、ユーザが複数のシステムのアカウントを持っている (および各ユーザがシステムごとに異なるユーザ名を持っている) 場合に選択します。
   - 追加するすべての *Oracle EBS* エイリアスに新しいアカウントを作成する
     このオプションは、Oracle E-Business Suite システムを 1 つだけ実行している場合、またはユーザの多くがシステムのいずれか 1 つのアカウントを持っている場合、あるいは、2 つ以上のシステムで異なるユーザに対して同じユーザ名が使用されている場合に選択します。
5. [更新オプション]エリアで、次のオプションのいずれかを選択します。
   - エイリアスの更新時に新しいエイリアスを作成する
     このオプションは、BI プラットフォームにマップされるすべてのユーザに新しいエイリアスを作成する場合に選択します。新しいアカウントが BI プラットフォームアカウントを持たないユーザに対して追加されます。または [追加するすべての *Oracle EBS* エイリアスに新しいアカウントを作成する] オプションを選択した場合は、新しいアカウントがすべてのユーザに対して追加されます。
   - ユーザのログオン時にのみ新しいエイリアスを作成する
     このオプションは、マップするロールに多くのユーザが含まれているが、その一部のユーザのみが BI プラットフォームを使用する場合に選択します。BI プラットフォームは、ユーザに対してエイリアスやアカウントを自動で作成しません。代わりに、BI プラットフォームに初めてログインしたユーザに対してのみエイリアス (必要な場合は、アカウントも) を作成します。これはデフォルトのオプションです。
6. [新しいユーザのオプション] で、新しいユーザを作成する方法を指定し、[更新] をクリックします。

   次のいずれかのオプションを選択します。

   - 新しいユーザを登録ユーザとして作成する
     登録ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。登録ユーザライセンスは特定のユーザに関連付けられており、ユーザはそのユーザ名およびパスワードに基づいてシステムにアクセスすることができます。このため、登録ユーザは、システムに接続している他のユーザの数に関係なく接続できます。このオプションを使用して作成したユーザアカウントに使用できる登録ユーザライセンスを持っている必要があります。

> ⓘ 注記
>
> 登録ユーザライセンスを使用して作成された登録ユーザの同時ログオンセッション数は、10 に制限されています。このような登録ユーザが 11 番目の同時ログオンセッションにログインしようとすると、該当するエラーメッセージが表示されます。ログインするには、既存のセッションの 1 つをリリースする必要があります。
>
> ただし、プロセッサライセンスおよびパブリックドキュメントライセンスを使用して作成された登録ユーザに対しては、同時ログオンセッションの数に制限はありません。

- 新しいユーザを同時接続ユーザとして作成する
  同時接続ユーザのライセンスを使用するように、新しいユーザアカウントを設定します。同時接続ライセンスでは BI プラットフォームに同時接続できるユーザ数が指定されます。この種類のライセンスは、少ないユーザ数の同時接続ライセンスで多数のユーザをサポートできるため、柔軟性に優れています。たとえば、ユーザがプラットフォームにアクセスする頻度と時間の長さによって、100 ユーザ同時接続ライセンスで 250、500、または 700 のユーザをサポートできます。

選択したロールが BI プラットフォームにグループとして表示されます。

7. [職責]タブをクリックします。
8. [現在の *Oracle EBS* サービス]で、マップするロールを含む Oracle EBS サービスを選択します。
9. [マップされた *Oracle EBS* ロール]で、Oracle EBS ユーザに対してフィルタを指定できます。
   a. [アプリケーション]リストから、新しいロールで使用できるアプリケーションを選択します。
   b. [職責]リストで、ユーザが実行できる Oracle アプリケーション、機能、レポート、同時プログラムを選択します。
   c. [セキュリティグループ] のセキュリティグループで、新しいロールが割り当てられるセキュリティグループを選択します。
   d. [現在のロール] の下にある[追加] ボタンと [削除] ボタンを使用して、ロールに対するセキュリティグループの割り当てを変更します。
10. [更新] をクリックします。
    これらのロールが BI プラットフォームにマップされます。

BI プラットフォームにロールをマップしたら、これらのロールの更新方法を指定する必要があります。

9.9.2.1.1 Oracle EBS ロールとユーザの更新

Oracle EBS 認証を有効化した後、BI プラットフォームにインポート済みのマップされたロールに対する定期的な更新をスケジュールし、実行する必要があります。このことにより、更新された Oracle EBS ロールの情報を、BI プラットフォームに正確に反映できます。

Oracle EBS ロールの更新を実行し、スケジュールするためのオプションは 2 つあります。

- ロールのみを更新: このオプションを使用すると、BI プラットフォームにインポート済みの現在マップされているロール間のリンクのみを更新します。頻繁に更新を実行する予定があり、システムリソースの使用状況に懸念がある場合に、このオプションを使用することをお勧めします。Oracle EBS ロールを更新するだけでは、新しいユーザアカウントは作成されません。
- ロールとエイリアスを更新: このオプションを使用すると、ロール間のリンクを更新するだけでなく、Oracle EBS システムのロールに追加されたユーザエイリアス用の新しいユーザアカウントを BI プラットフォームに作成します。

> ⓘ 注記
>
> Oracle EBS 認証を有効化しているときに、更新時にユーザエイリアスを自動で作成するよう指定していない場合は、新しいエイリアスに対してアカウントは作成されません。

9.9.2.1.2 Oracle EBS ロールの更新をスケジュールする

BI プラットフォームにロールをマップしたら、これらのロールの更新方法を指定する必要があります。

1. [ユーザの更新] タブをクリックします。
2. [ロールのみを更新] セクションまたは [ロールとエイリアスを更新] セクションのいずれかで、[スケジュール] をクリックします。

   > → ヒント
   >
   > すぐに更新を実行する場合は、[今すぐ更新] をクリックします。

   > → ヒント
   >
   > 頻繁に更新をするためシステムリソースに懸念がある場合は、[ロールのみを更新] オプションを使用します。ロールとエイリアスの両方を更新するには、より多くの時間がかかります。

   [繰り返し] ダイアログボックスが表示されます。
3. [オブジェクトの実行] プルダウンリストからオプションを選択し、必要なスケジュール情報を表示されたフィールドにすべて入力します。

   更新をスケジュールする場合、次の表に示した定期スケジュールパターンの中から選択することができます。

定期スケジュールパターン	説明
時間単位	更新は毎時間実行されます。開始時間、開始および終了日を指定します。
日単位	更新は毎日または指定した日数ごとに実行されます。実行時刻、開始日および終了日を指定することができます。
週単位	更新は毎週実行されます。1 週間に 1 回または数回実行することができます。実行する曜日、時間、開始および終了日を指定することができます。
月単位	更新は毎月または数カ月ごとに実行されます。実行時刻、開始日および終了日を指定することができます。
N 日	更新は毎月指定された日付に実行されます。実行する日にち、時間、開始および終了日を指定することができます。
第 1 月曜日	更新は毎月第 1 月曜日に実行されます。実行時刻、開始日および終了日を指定することができます。
月末日	オブジェクトは毎月末日に実行されます。実行時刻、開始日および終了日を指定することができます。
第 N 週の X 日	更新は毎月特定の週の特定の曜日に実行されます。実行時刻、開始日および終了日を指定することができます。

定期スケジュールパターン	説明
カレンダ	更新は、すでに作成されているカレンダで指定した日付に実行されます。

4. スケジュール情報の入力を終了したら、[スケジュール] をクリックします。
   次回のスケジュールされたロールの更新の日付が、[ユーザの更新] タブに表示されます。

> ⓘ 注記
>
> [ロールのみを更新] セクションまたは [ロールとエイリアスを更新] セクションのいずれかで、[スケジュールされた更新のキャンセル] をクリックすると、いつでも次回のスケジュールされた更新をキャンセルできます。

9.9.3 ロールのマップ解除

特定のユーザグループを BI プラットフォームにログオンさせないようにするには、ユーザグループが属しているロールのマップを解除します。

9.9.3.1 ロールをマップ解除する

1. セントラル管理コンソールに管理者としてログオンします。
2. [管理]領域で[認証]をクリックします。
3. ロールをマップ解除する ERP システムの名前をダブルクリックします。
   ERP システムのページに [オプション] タブが表示されます。
4. [職責] タブをクリックします。
5. [現在の *Oracle EBS* サービス] を選択します。
6. [現在のロール] の下でロールを選択し、[削除] ボタンをクリックします。
7. *[更新]*をクリックします。

   ロールのメンバーは、他のアカウントまたはエイリアスを持っていない限り、BI プラットフォームにアクセスできなくなります。

> ⓘ 注記
>
> 特定のユーザをログオンさせないようにするために、BI プラットフォームにマップする前に、個々のアカウントを削除するか、ロールからユーザを削除することもできます。

9.9.4 マップされた Oracle EBS のグループ権限とユーザ権限のカスタマイズ

ロールを BI プラットフォームにマップするときに、作成されたグループとユーザの権限を設定したり、付与することができます。

9.9.4.1 管理権限を割り当てる

ユーザが BI プラットフォームを管理できるようにするには、それらのユーザをデフォルトの Administrators グループのメンバーにする必要があります。このグループのメンバーは、システムのすべての面 (アカウント、サーバ、フォルダ、オブジェクト、設定など) のフルコントロール権を付与されます。

1. セントラル管理コンソールに管理者としてログオンします。
2. [整理] 領域で、[ユーザとグループ] をクリックします。
3. [名前] 列で、[*Administrators*] を右クリックし、[グループにメンバーを追加] をクリックします。

   [利用可能なユーザまたはグループ] ページが表示されます。
4. [ユーザ一覧]または[グループリスト]エリアで、管理権限を割り当てるマップされたロールを選択します。
5. [>]をクリックし、ロールを Administrators グループのサブグループに設定してから、[*OK*]をクリックします。

これで、このロールのメンバーは BI プラットフォームの管理権限を持つことができます。

> **注記**
>
> また、Oracle EBS 内でロールを作成して、適切なユーザをロールに追加し、ロールを BI プラットフォームにマップして、マップしたロールをデフォルトの Administrators グループのサブグループにして、ロールのメンバーが管理権限を取得することもできます。

9.9.4.2 公開権限を割り当てる

組織内でコンテンツ作成者に指定されているユーザがシステムに存在する場合は、それらのユーザに、オブジェクトを BI プラットフォームに公開するための権限を付与できます。

1. セントラル管理コンソールに管理者としてログオンします。
2. [整理]エリアで、[フォルダ]をクリックします。
3. ユーザにオブジェクトの追加を許可するフォルダに移動します。
4. [管理]、[最上位セキュリティ]、[すべてのフォルダ]の順にクリックします。
5. [主体の追加]をクリックします。

   [主体の追加]ページが表示されます。
6. [利用可能なユーザまたはグループ] リストで、公開権限を付与するメンバーを含むグループを選択します。
7. [>] をクリックしてグループがフォルダへアクセスできるようにしてから、[セキュリティを追加して割り当てる] をクリックします。

   [セキュリティの割り当て] ページが表示されます。
8. [利用可能なアクセスレベル] リストで、使用するアクセスレベルを選択し、[>] をクリックしてアクセスレベルを明示的に割り当てます。
9. [親フォルダからの継承] および [親グループからの継承] オプションが選択されている場合は、それらのオプションの選択を解除し、[適用] をクリックします。
10. [*OK*]をクリックします。

これで、ロールのメンバーは、フォルダおよびそのすべてのサブフォルダにオブジェクトを追加する権限を持つことができます。割り当てられた権限を削除するには、グループを選択して [削除] をクリックします。

9.9.5 SAP Crystal Reports および Oracle EBS のシングルサインオン (SSO) の設定

デフォルトで、BI プラットフォームは、SAP Crystal Reports ユーザがシングルサインオン (SSO) を使用して Oracle EBS データにアクセスできるよう設定されています。

9.9.5.1 Oracle EBS および SAP Crystal Reports の SSO を無効化する

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。
4. [*crdb_oraapps*] を選択します。
5. [削除] をクリックします。
6. [保存して閉じる]をクリックします。
7. CMC の [サーバ] ページに移動し、[*Crystal Reports* サービス] を選択します。
8. [サーバの再起動] ボタンをクリックします。

9.9.5.2 Oracle EBS および SAP Crystal Reports の SSO を再有効化する

以下の手順に従って Oracle EBS および SAP Crystal Reports の SSO を再有効化します。

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。
4. [以下のドライバを使用したデータベースログオンに *SSO* コンテキストを使用] で「**`crdb_oraapps`**」と入力します。
5. [追加] をクリックします。
6. [保存して閉じる]をクリックします。
7. CMC の [サーバ] ページに移動し、[*Crystal Reports* サービス] を選択します。
8. [サーバの再起動] ボタンをクリックします。

9.10 X.509 認証

9.10.1 BI ラウンチパッドの X.509 認証

9.10.1.1 証明書およびキーストアの作成および設定

> ⓘ 注記
>
> X.509 認証によるシングルサインオンを達成するためには、BI プラットフォームにユーザが存在している必要があります。

> ⓘ 注記
>
> OpenSSL ツールキットをダウンロードしてインストールし、以下に示す手順を実行します。

> ⓘ 注記
>
> CA 証明書を作成して自己署名する必要がある場合には、以下に示すすべての手順に従ってください。

> ⓘ 注記
>
> 信頼できる CA がある場合は、証明書およびキーストアの作成および設定について、信頼できる CA の使用 [385 ページ]を参照してください。

1. 次のコマンドを実行して、認証機関 (CA) キー (ca.key) ファイルおよび証明書要求 (ca.csr) ファイルを作成します。`Openssl.exe req -newkey rsa:2048 -nodes -out c:¥ssl¥ca.csr -keyout c:¥ssl¥ca.key`
2. 次のコマンドを実行して、署名付き証明書 (ca.pem) を作成します。`Openssl.exe x509 -req -trustout -signkey c:¥ssl¥ca.key -days 365 -in c:¥ssl¥ca.csr -out c:¥ssl¥ca.pem`
3. サーバキーペア、証明書、およびキーストアを作成します。
   a. 次のコードを実行して、CA のシリアル番号を保持するためのファイルを作成します。`Echo 02 >c:¥ssl¥ca.srl`
   b. `C:¥Program Files¥Java¥jre7¥bin` に移動し、keytool.exe を使用してサーバキーストア、証明書、および秘密鍵を作成します。

      > ⓘ 注記
      >
      > Java keytool.exe の場所で、'jre7' は Java のバージョンによって異なる場合があります。

      ```
      Keytool.exe -genkey -alias server -keyalg RSA -keysize 2048 -keystore
      c:¥ssl¥serverkeystore.jks -storetype JKS
      Keytool.exe -certreq -keyalg RSA -alias server -file c:¥ssl¥server.csr -
      keystore c:¥ssl¥serverkeystore.jks
      ```

      > → 注意
      >
      > 証明書の生成時に、指示に従ってサーバマシンのホスト名を入力します。これを入力しないと、接続時にクライアントに証明書エラーが発生します。

c. キーストアパスワードを入力します。

> → 注意
>
> テキストエディタで要求のファイル server.csr を編集し、"New Begin Certificate Request" を "Begin Certificate Request" に、"New End Certificate Request" を "End Certificate Request" に変更する必要があります。

4. 次のコマンドを実行して、署名付き証明書 (server.crt) を作成します。`Openssl.exe x509 -CA c:¥ssl¥ca.pem -cakey c:¥ssl¥ca.key -CAserial c:¥ssl¥ca.srl -req -in c:¥ssl¥server.csr -out c:¥ssl¥server.crt -days 365`
5. 認証機関およびサーバ証明書をサーバキーストアにインポートします。

```
Keytool.exe -import -alias ca -keystore c:¥ssl¥serverkeystore.jks -
trustcacerts -file c:¥ssl¥ca.pem
Keytool.exe -import -alias server -keystore c:¥ssl¥serverkeystore.jks -
trustcacerts -file c:¥ssl¥server.crt
```

6. 次のコマンドを実行して、クライアント証明書 client.req および client.key を作成します。 `Openssl.exe -newkey rsa:2048 -nodes -out c:¥ssl¥client.req -keyout c:¥ssl¥client.key -config c:¥ssl¥sslc.cnf`

> ⓘ 注記
>
> sslc.cnf ファイルを `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86` から C:¥SSL にコピーし、次のパラメータを変更します。
>
> Dir=c:/ssl # あらゆるものの場所
>
> Certificate= $dir/ca.pem # CA 証明書
>
> Private_key= $dir/ca.key # 秘密鍵
>
> RANDFILE= $dir/.rand # 秘密乱数ファイル

7. 次のコマンドを実行して、クライアント証明書に署名します。`Openssl.exe x509 -CA c:¥ssl¥ca.pem -CAkey c:¥ssl¥ca.key -CAserial c:¥ssl¥ca.srl -req -in c:¥ssl¥client.req -out c:¥ssl¥client.pem -days 365`
8. 次に示すコマンドを使用して CA およびクライアント証明書を信頼キーストアにインポートします。このコマンドは、trustkeystore.jks を作成します。

```
Keytool.exe -import -alias ca -keystore c:¥ssl¥trustkeystore.jks -
trustcacerts -file c:¥ssl¥ca.pem
Keytool.exe -import -alias client -keystore c:¥ssl¥trustkeystore.jks -
trustcacerts -file c:¥ssl¥client.pem
```

9. クライアント秘密鍵 PKCS12 形式でクライアント証明書をエクスポートします。`Openssl.exe pkcs12 -export -clcerts -in c:¥ssl¥client.pem -inkey c:¥ssl¥client.key -out c:¥ssl¥client.p12 -name “client certificate”`。このコマンドは、client.p12 ファイルを作成します。
10. 次のコマンドを実行して、CA 証明書をエクスポートし、ca.crt を作成します。`Openssl.exe x509 -in c:¥ssl¥ca.pem -inform PEM -out c:¥ssl¥ca.crt -outform DER`
11. クライアントマシンに .p12 および ca.crt ファイルをコピーして、クライアントおよび CA 証明書をインストールします。

> ⓘ 注記
>
> Mozilla Firefox に証明書をインストールするには、ツール > オプション > 詳細 に移動し、[証明書] タブの [証明書を表示] を選択して、client.p12 ファイルを [あなたの証明書] タブに、ca.crt ファイルを [認証局証明書] タブにインポートします。

9.10.1.1.1 信頼できる CA の使用

1. サーバキーペア、証明書、およびキーストアを作成します。
   a. 次のコードを実行して、CA のシリアル番号を保存するファイルを作成します。`Echo 02 >c:¥ssl¥ca.srl`
   b. `C:¥Program Files¥Java¥jre7¥bin` に移動し、keytool.exe を使用してサーバキーストア、証明書、および秘密鍵を作成します。

   > ⓘ 注記
   >
   > keytool.exe の場所で、'jre7' は Java のバージョンによって異なる場合があります。

   ```
   Keytool.exe -genkey -alias server -keyalg RSA -keysize 2048 -keystore
   c:¥ssl¥serverkeystore.jks -storetype JKS
   Keytool.exe -certreq -keyalg RSA -alias server -file c:¥ssl¥server.csr -
   keystore c:¥ssl¥serverkeystore.jks
   ```

   > → 注意
   >
   > 証明書の生成時に、指示に従ってサーバマシンのホスト名を入力します。これを入力しないと、接続時にクライアントに証明書エラーが発生します。

   c. キーストアパスワードを入力します。

   > → 注意
   >
   > テキストエディタで要求のファイル server.csr を編集し、"New Begin Certificate Request" を "Begin Certificate Request" に、"New End Certificate Request" を "End Certificate Request" に変更する必要があります。

2. 次のコマンドを実行して、署名付き証明書 (server.crt) を作成します。`Openssl.exe x509 -CA c:¥ssl¥ca.pem -cakey c:¥ssl¥ca.key -CAserial c:¥ssl¥ca.srl -req -in c:¥ssl¥server.csr -out c:¥ssl¥server.crt -days 365`
3. サーバ証明書をサーバキーストアにインポートします。

   ```
   Keytool.exe -import -alias server -keystore c:¥ssl¥serverkeystore.jks -
   trustcacerts -file c:¥ssl¥server.crt
   ```

4. 次のコマンドを実行して、クライアント証明書 client.req および client.key を作成します。 `Openssl.exe -newkey rsa:2048 -nodes -out c:¥ssl¥client.req -keyout c:¥ssl¥client.key -config c:¥ssl¥sslc.cnf`

> **注記**
>
> sslc.cnf ファイルを `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86` から C:¥SSL にコピーし、次のパラメータを変更します。
>
> Dir=c:/ssl # あらゆるものの場所
>
> Certificate= $dir/ca.pem # CA 証明書
>
> Private_key= $dir/ca.key # 秘密鍵
>
> RANDFILE= $dir/.rand # 秘密乱数ファイル

5. 次のコマンドを実行して、クライアント証明書に署名します。`Openssl.exe x509 -CA c:¥ssl¥ca.pem -CAkey c:¥ssl¥ca.key -CAserial c:¥ssl¥ca.srl -req -in c:¥ssl¥client.req -out c:¥ssl¥client.pem -days 365`
6. 次に示すコマンドでクライアント証明書を信頼キーストアにインポートします。このコマンドは、trustkeystore.jks を作成します。

```
Keytool.exe -import -alias client -keystore c:¥ssl¥trustkeystore.jks -
trustcacerts -file c:¥ssl¥client.pem
```

7. クライアント秘密鍵 PKCS12 形式でクライアント証明書をエクスポートします。`Openssl.exe pkcs12 -export -clcerts -in c:¥ssl¥client.pem -inkey c:¥ssl¥client.key -out c:¥ssl¥client.p12 -name "client certificate"`。このコマンドは、client.p12 ファイルを作成します。
8. .p12 ファイルをクライアントマシンにコピーしてインストールします。

> **注記**
>
> Mozilla Firefox に証明書をインストールするには、ツール > オプション > 詳細 に移動し、[証明書] タブの [証明書を表示] を選択して、client.p12 ファイルを [あなたの証明書] タブに、ca.crt ファイルを [認証局証明書] タブにインポートします。

9.10.1.2 Tomcat SSL サーバの設定

9.10.1.2.1 一方向 SSL 設定

1. `<INSTALLDIR>¥tomcat¥conf¥server.xml` に移動します。
2. xml タグを編集します。`<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" SSLEnabled="true" scheme="https" secure="true"> <SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></Connector>`

> **注記**
>
> 上記の xml タグで使用されているキーストアファイルのパスワード (Password1) および場所 (C:¥ssl¥serverkeystore.jks) は単なる例です。任意のパスワードと場所を使用できます。

3. ファイルを保存し、Tomcat サーバを再起動します。

9.10.1.2.2 双方向 SSL 設定

次に示す手順に従って、クライアント認証を要求するように Tomcat サーバを設定します。

1. `<INSTALLDIR>¥tomcat¥conf¥server.xml` に移動します。
2. 次に示す xml タグで server.xml を編集します。`<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="200" SSLEnabled="true" scheme="https" secure="true"> <SSLHostConfig protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></Connector>`

   > ⓘ 注記
   >
   > 上記の xml タグで使用されているサーバキーストアおよび信頼キーストアファイルのパスワード (Password1) および場所 (C:¥ssl¥serverkeystore.jks または C:¥ssl¥trustkeystore.jks) は単なる例です。任意のパスワードと場所を使用できます。

3. ファイルを保存し、Tomcat サーバを再起動します。

   > ⓘ 注記
   >
   > Internet Explorer では、インターネット オプション > セキュリティ > ローカル イントラネット > レベルのカスタマイズ > その他 に移動して、オプション [既存のクライアント証明書が 1 つしか存在しない場合の証明書の選択] を無効にしてください。

9.10.1.3 BI 起動パッドの設定

9.10.1.3.1 共有シークレットキーの作成

共有シークレットキーは、クライアントと CMS 間の信頼関係を確立するために使用します。クライアントの前にサーバで [信用できる認証] を設定する必要があります。

1. CMC にログインします。
2. [認証] に移動し、[Enterprise] を選択します。
3. [信用できる認証] を有効にします。
4. [新規共有シークレット] を選択します。

   > ⓘ 注記
   >
   > 共有シークレットキーが生成され、ダウンロードメッセージが表示されます。

5. [共有シークレットのダウンロード] を選択します。

6. ダウンロードダイアログボックスで [保存] を選択し、以下のいずれかのディレクトリを選択します。
   - `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥`
   - `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86¥`

9.10.1.3.2 TrustedPrincipal.conf ファイルを介した共有シークレットキーの受け渡し

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEBINF¥config¥custom¥directory` に新しいテキストファイルを作成します。
2. 新しいファイルで、以下に示すテキストを追加します。

```
sso.enabled=true
        trusted.auth.user.retrieval=WEB_SESSION
        trusted.auth.user.param=MyUser
        trusted.auth.shared.secret=MySecret
```

3. ファイルを保存し、'global.properties' というファイル名にします。

9.10.1.3.3 custom.jsp ファイルの編集

> **注記**
>
> custom.jsp ファイルを編集する前に、ユーザをマシン名とともに CMC に作成します。

1. ジャンプ
   a. 従来の BI ラウンチパッドの場合は *com.businessobjects.webpath.InfoView.jar* の *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *custom.jsp* に移動します。
   b. Fiorified BI ラウンチパッドの場合は *com.businessobjects.webpath.fioriBI.jar* の *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.fioriBI* > *web* > *custom.jsp* に移動します。
2. custom.jsp ファイルを編集します。

```
<¥!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code
request.getSession().setAttribute("MySecret","<Shared_Secret_Key>")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
```

```
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> **注記**
>
> <Shared_Secret_Key> を *TrustedPrincipal.conf* ファイルで使用できる新しいキーに置き換える必要があります。共有シークレットキーを作成する方法については、共有シークレットキーの作成 [387 ページ] を参照してください。

9.10.1.3.4 myScript.js ファイルの作成

1. *<INSTALLDIR>* > *SAP BusinessObjects Enterprise XI 4.0* > *warfiles* > *webapps* > *BOE* > *WEB-INF* > *eclipse* > *plugins* > *webpath.InfoView* > *web* > *noCacheCustomResources* に移動し、myScript.js を作成します。
2. 以下を、myScript.js に追加します。

```
function goToLogonPage()
{
window.location = "logon.jsp";
}
```

3. Tomcat サーバを再起動します。

9.10.1.3.5 BOE の内部およびカスタムのプロパティファイルの設定

1. *<INSTALLDIR>* > *Tomcat* > *webapps* > *BOE* > *WEB-INF* > *internal* に移動します。
2. bilaunchpad.properties ファイルを開き、以下のプロパティを変更します。

```
redirection.iframe.1.incoming.url=property.ref.app.url.name
redirection.iframe.1.application=InfoView
redirection.iframe.1.bundle.path=/InfoView
redirection.iframe.1.redirectto.url=/custom.jsp
redirection.iframe.2.incoming.url=property.ref.app.url.name
redirection.iframe.2.incoming.url.suffix=/index.html
redirection.iframe.2.application=InfoView
redirection.iframe.2.bundle.path=/InfoView
redirection.iframe.2.redirectto.url=/custom.jsp
redirection.iframe.9.incoming.url=/InfoView/index.html
redirection.iframe.9.application=InfoView
redirection.iframe.9.bundle.path=/InfoView
redirection.iframe.9.redirectto.url=/custom.jsp
```

3. Tomcat サーバを再起動します。

9.10.1.3.6 BOE Web.xml ファイルの設定

1. `<INSTALLDIR>¥tomcat¥webapps¥BOE¥WEB-INF` に移動します。
2. この場所にある web.xml ファイルを、以下に示すコードを使用して編集します。

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
value>
</init-param>
```

3. 以下に示す手順に従って、web.xml ファイルにパラメータを追加します。
   a. `<INSTALLDIR>¥tomcat¥webapps¥BOE¥WEB-INF¥eclipse¥plugins¥webpath.BIPCoreWeb¥web¥WEB-INF` に移動します。
   b. 以下に示すパラメータを追加します。

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>New_Shared_Secret_Key</param-value>
</init-param>
```

   c. `<<INSTALLDIR>¥tomcat¥work¥Catalina¥localhost¥BOE¥eclipse¥plugins¥webpath.BIPCoreWeb¥web¥WEB-INF` に移動して手順を繰り返します。

> → ヒント
>
> 信頼できる認証を正しく設定したことを確認するには、URL https://[cmsname]:8443/BOE/BI/logon.jsp を使用して BI ラウンチパッドアプリケーションにアクセスします。[cmsname] は、CMS をホストしているマシンの名前です。

9.10.2 Web サービスの X.509 認証

9.10.2.1 SOAP Web サービス向け

9.10.2.1.1 Tomcat での SSL の設定

Web サービスを使用する場合、SAP Business Intelligence プラットフォームを設定する前に、Tomcat で SSL を設定する必要があります。

> ⓘ 注記
>
> X.509 認証によるシングルサインオンを達成するためには、BI プラットフォームにユーザが存在している必要があります。

1. `<INSTALLDIR>¥tomcat¥conf` に移動します。
2. server.xml を XML エディタで開き、xml タグを次のように編集します。

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="200" SSLEnabled="true" scheme="https" secure="true"> <SSLHostConfig
protocols="TLSv1.2"><Certificate certificateKeystoreFile="C:/SSL/
myserver.keystore" certificateKeystorePassword="mypassword"/></SSLHostConfig></
Connector>
```

3. ファイルを保存します。

> ⓘ 注記
>
> 上記のパスワードとファイルの場所は単なる例です。任意のパスワードと場所を追加できます。

> ⓘ 注記
>
> キーストアファイルの作成の詳細については、証明書およびキーストアの作成および設定 [383 ページ] を参照してください。

9.10.2.1.2 axis2.xml ファイルの設定

> ⓘ 注記
>
> Linux または Unix では、以下の手順を実行する前に、OS BI インストールユーザが `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥dswsbobje` に対して再帰的な 755 権限を持っていることを確認してください。この権限は、`chmod -R 755` コマンドを使用して付与できます。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥conf` に移動します。
2. 任意の XML エディタで axis2.xml ファイルを開きます。
3. セキュリティ保護された接続を許可する新しいポート番号で xml タグを更新します。

```
<transportReceiver name="http"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8080</parameter>
</transportReceiver>
<transportReceiver name="https"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8443</parameter>
</transportReceiver>
```

> ⓘ 注記
>
> デフォルト設定では、AxisServlet は http でのみ要求を受信すると想定しています。https を許可するには、name = "https" として AxisServletListener を設定し、両方のレシーバでポートパラメータを指定する必要があります。また、xml タグを更新して、複数のポート番号を追加または削除できます。

4. axis2.xml を保存します。
5. Tomcat サーバを再起動します。

6. 任意のブラウザを起動し、https://<IP address>:<https port>/dswsbobje/services/listServices に移動して、セキュア接続を検証します。リンクに移動すると、trustedLoginWithX509 が [セッション] タブに表示されます。

9.10.2.1.3 共有シークレットの値の生成

1. セントラル管理コンソールを起動します。
2. 認証 > *Enterprise* に移動します。
3. 信頼できる認証で、信頼できる認証のボックスが有効になっていることを確認します。
4. [新規共有シークレット] を選択します。これにより、共有シークレットキーが生成されます。
5. [共有シークレットのダウンロード] を選択し、[更新] を選択します。
6. ダウンロードしたファイル TrustedPrincipal.conf を、Windows では `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥container¥bin` にコピーします。

> **注記**
>
> 共有シークレットの値を表示するには、任意の XML エディタで TrustedPrincipal.conf を開きます。

9.10.2.1.4 web.xml ファイルの設定

1. `<INSTALLDIR>¥tomcat¥webapps¥dswsbobje¥WEB-INF` に移動します。
2. web.xml を XML エディタで開き、xml タグを CMS ホストマシン名とともに以下のように更新します。

```
<context-param>
        <param-name>cms.default</param-name>
        <param-value>EnterHostMachineName</param-value>
    </context-param>
```

3. 以下に示す xml タグを共有シークレットの値とともに追加します。共有シークレットの値を生成する方法については、共有シークレットの値の生成 [392 ページ] を参照してください。

```
<context-param>
<param-name>trusted.auth.shared.secret</param-name>
<param-value>shared secret value</param-value>
</context-param>
```

4. web.xml ファイルを保存します。

> **注記**
>
> BI 4.2 SP04 より低いバージョンからアップグレードしている場合、axis2.xml ファイルで行った設定内容は破棄されます。

9.10.2.2 RESTful Web サービス向け

> **注記**
>
> X.509 認証によるシングルサインオンを実現するためには、BI プラットフォームにユーザが存在している必要があります。

Business Intelligence プラットフォーム管理者ガイドのトピック「HTTPS/SSL の設定」をチェックして、RESTful Web サービスの信頼された認証を確立します。

X.509 証明書を使用して信頼された認証を確立するには、共有秘密鍵を生成する必要があります。詳細については、*Business Intelligence* プラットフォーム管理者ガイドの「共有シークレットの値の生成」を参照してください。

また、REST SDK エンドポイントの詳細については、*Business Intelligence* プラットフォーム *RESTful Web* サービス開発者ガイドの *API* リファレンス > 認証 > */v1//logon/trustedx509* を参照してください。

9.10.2.2.1 Tomcat での RESTful Web サービスの X.509 認証

公開鍵暗号化において、X.509 は安全なデジタル証明書の要件を定義する標準です。X.509 証明書により、ユーザまたはサービスのアイデンティティによる公開鍵の所持が証明されます。

以下の手順により、Tomcat アプリケーションサーバ上の RESTful Web サービスに対して X.509 認証を有効化できるようになりました。

1. Tomcat で SSL を有効にします。詳細については、Tomcat での SSL の設定 [390 ページ] を参照してください。
2. 共有秘密鍵を生成します。詳細については、共有シークレットの値の生成 [392 ページ] を参照してください。
3. テキストエディタで共有秘密鍵を開きます。
4. 共有秘密鍵をコピーします。
5. ファイル *biprws.properties* を編集します。
   a. `<INSTALLDIR>/tomcat/webapps/biprws/WEB-INF/config/default` に移動します。
   b. ファイル *biprws.properties* をテキストエディタで開きます。
   c. *Trusted_Auth_Shared_Secret=* を検索します。
   d. 値 *Trusted_Auth_Shared_Secret=* に対して共有秘密鍵をペーストします。
   e. ファイル *biprws.properties* を保存します。

9.10.3 CMC の X.509 認証

> **注記**
>
> X.509 認証によるシングルサインオンを実現するためには、BI プラットフォームにユーザが存在している必要があります。

X.509 認証によるシングルサインオンを実現するには、以下の手順を実行します。

1. 証明書およびキーストアの作成および設定 [383 ページ]
2. 一方向 SSL 設定 [386 ページ]
3. 双方向 SSL 設定 [387 ページ]
4. 共有シークレットキーの作成 [387 ページ]
5. TrustedPrincipal.conf ファイルを介した共有シークレットキーの受け渡し [388 ページ]
6. Custom.jsp ファイルの編集 (CMC 向け) [394 ページ]
7. myScript.js ファイルの作成 (CMC 向け) [395 ページ]
8. BOE の内部およびカスタムのプロパティファイルの設定 (CMC 向け) [395 ページ]
9. BOE Web.xml ファイルの設定 (CMC 向け) [395 ページ]

9.10.3.1 Custom.jsp ファイルの編集 (CMC 向け)

> ⓘ 注記
>
> custom.jsp ファイルを編集する前に、ユーザをマシン名とともに CMC に作成します。マシンにユーザが存在する場合、以下の手順を直接開始できます。

1. com.businessobjects.webpath.InfoView.jar で `<INSTALLDIR>¥tomcat¥webapps¥BOE¥WEBINF¥eclipse¥plugins¥webpath.CmcApp¥web¥cutom.jsp` に移動します。
2. custom.jsp ファイルを編集します。

```
<¥!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"  "http://
www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html;charset=utf-8" %>
<% //custom Java code request.getSession().setAttribute("MySecret","Shared
Secret Key")
request.getSession().setAttribute("MyUser", "John Doe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript"src="noCacheCustomResources/myScript.js">
</script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI
launch pad </a>
</body>
</html>
```

> ⓘ 注記
>
> このコードの共有シークレット値を新しいキーに置き換え、ユーザを CMC に作成されたマシン名に置き換える必要があります。

9.10.3.2 myScript.js ファイルの作成 (CMC 向け)

1. `<INSTALLDIR>¥tomcat¥webapps¥BOE¥WEB-INF¥eclipse¥plugins¥webpath.CmcApp¥web¥noCacheCustomResources and create myScript.js` に移動します。
2. 以下を myScript.js に追加します。

```
function goToLogonPage()
{
window.location = "logon.jsp";
}
```

3. Tomcat サーバを再起動します。

9.10.3.3 BOE の内部およびカスタムのプロパティファイルの設定 (CMC 向け)

1. `<INSTALLDIR>¥tomcat¥webapps¥BOE¥WEB-INF¥internal¥CmcApp.properties` に移動します。
2. CmcApp.properties ファイルを開き、以下のパラメータを追加します。

   `sso.supported.types=vintela, trustedIIS, trustedHeader, trustedParameter, trustedCookie, trustedSession, trustedUserPrincipal, trustedVintela, trustedX509, sapSSO, sitemindera`
3. Tomcat サーバを再起動します。

9.10.3.4 BOE Web.xml ファイルの設定 (CMC 向け)

1. `<INSTALLDIR>¥tomcat¥webapps¥BOE¥WEB-INF` に移動します。
2. この場所にある web.xml ファイルを、以下に示すコードを使用して編集します。

```
<init-param>
<param-name>extendedFrameworkExports</param-name>
<param-
value>com.businessobjects.servletbridge.listener,com.businessobjects.servletbr
idge.customconfig,com.businessobjects.servletbridge.external,com.businessobjec
ts.servletbridge.session,com.businessobjects.resource,oracle.jdbc.pool,com.sie
bel.data,com.jdedwards.system.xml,org.ietf.jgss,com.sap.security.api</param-
value>
</init-param>
```

3. 以下に示す手順に従って、web.xml ファイルにパラメータを追加します。
   a. `<INSTALLDIR>¥tomcat¥webapps¥BOE¥WEB-INF¥eclipse¥plugins¥webpath.CmcApp¥web¥WEB-INF¥web.xml` に移動します。
   b. 以下に示すパラメータを追加します。

```
<init-param>
<param-name>trusted.auth.shared.secret</param-name>
```

```
<param-value>Shared_Secret_Key</param-value>
</init-param>
```

c. `<INSTALLDIR>¥tomcat¥work¥Catalina¥localhost¥BOE¥eclipse¥plugins¥webpath.CmcApp¥web¥WEB-INF¥web.xml` に移動して手順を繰り返します。

> **注記**
>
> 信頼できる認証を正しく設定したことを確認するには、URL https://[cmsname]:8443/BOE/BI/logon.jsp を使用して BI ラウンチパッドアプリケーションにアクセスします。[cmsname] は、CMS をホストしているマシンの名前です。

9.11 OpenID 接続認証

OpenID 接続認証を有効化できます。

OpenID 接続認証は、認証サーバ (OAuth) に基づいて機能します。クラウドドライブのサポートと同様に、OpenID 接続認証も認証サーバ設定に依存します。認証サーバ設定の詳細については、認可サーバの設定 [719 ページ]を参照してください。

OpenID 接続認証は、Enterprise 認証に基づいて開発されています。

SAML 認証の場合と同様に、Enterprise ユーザ (secEnterprise) として事前に BI プラットフォームにユーザをインポートする必要があります。

> **注記**
>
> ユーザのインポート時には、ユーザの電子メール ID も含まれていることを確認する必要があります。

SAML 認証とは異なり、OpenID 接続認証には以下が適用されます。

- すべての設定は、アプリケーションサーバレイヤではなく、BI プラットフォームバックエンドで行う必要があります。
- 信頼できる認証には依存しません。

OpenID 接続認証は、BI ラウンチパッドおよび OpenDocument でのみサポートされています。

9.11.1 OpenID 接続認証の有効化

OpenID 接続認証は、BI ラウンチパッドおよび OpenDocument でのみサポートされています。

OpenID 接続認証の詳細については、Enterprise 認証の設定 [229 ページ]を参照してください。バックエンドの Enterprise 認証プラグインで OpenID 接続認証を有効にした後、サポートされるアプリケーションの同じアプリケーション層 (BI ラウンチパッドの場合は `FioriBI.properties` ファイル、OpenDocument アプリケーションの場合は `WEB-INF/config/custom` の下の `OpenDocument.properties` ファイルなど) を有効にする必要があります。

Web SSO 認証ワークフローを有効化するには、`logon.webssoauthentication.framework` を `OpenId` に設定します。

`openid.restful.url` を、ランドスケープの RESTful Web サービス URL に設定します (`https://<server>:8443/biprws` など)。

BI ラウンチパッドには、…`/BO/BI` URL を使用して OpenID でログインできます。ただし、OpenID 接続認証を使用して BI ラウンチパッドにログインすると、プレースホルダのコンテキストパス「WEBSSO」が URL に追加されます。これは、ログアウト後も URL のパスに残ります。同じウィンドウから同じ URL を使用して再ログインする場合は、ブラウザの URL から「WEBSSO」を削除する必要があります。

10 データソース参照

10.1 拡張認証情報マッピング

BI 4.2.X 以前のリリースでは、管理者は CMC でユーザごとにデータベース認証情報のセットを 1 つのみ保存できました。

この機能を利用するには、管理者がすべての異なるデータベースに対して同じ認証情報を維持する必要があります。BI 4.3 以降では、データソース参照を使用して、各ユーザに対して複数のデータベース認証情報のセットを保存できます。

> ⓘ 注記
>
> SAP BusinessObjects Business Intelligence プラットフォーム 4.3 で導入された拡張認証情報マッピング機能は、インフォメーションデザインツールでのみサポートされます。拡張認証情報マッピングは、ユニバースデザインツールではサポートされていません。

CMC でのデータソース参照

CMC では、管理者が BI プラットフォームでデータソース参照を作成します。このデータソース参照は、管理者がデータベース認証情報のセットを 1 つ定義するユーザプロパティで使用されます。このデータソース参照は、接続で使用可能な認証のモードである認証情報マッピングの一部として使用されます。

認証モードとして認証情報マッピングが選択された場合、管理者には、好みのデータソース参照を選択するオプションが提供されます。同様に、管理者は、BI プラットフォームに接続している複数のデータベースがある場合、複数のデータソース参照を作成し、各ユーザに対して一意の認証情報を定義できます。

> ⓘ 注記
>
> CSV ファイルを使用してユーザをインポートする場合は、プロモーションマネジメントツールを使用してユーザを昇格します。または Enterprise、LDAP、Windows AD 認証タイプでログオン時にデータソース認証情報を同期させる場合は、BI プラットフォームによってデータベース認証情報がデフォルトのデータソース参照に割り当てられます。

BI ラウンチパッドでのデータソース参照

データソース参照も BI ラウンチパッドで利用可能になり、ユーザ認証情報を更新およびマップできるようになりました。

> ⓘ 注記
>
> [データソース参照] の詳細を編集することはできません。ただし、[アカウント名、[パスワード]、[パスワードの再確認] の各フィールドは編集することができます。

使用方法について

以下のように仮定します。

- BI プラットフォームでは、2 つのデータソース参照を使用できます (たとえば、販売データベースは DSR1、財務データベースは DSR2)。
- 各データソース参照には、ユーザ A のユーザプロパティで定義されたデータベース認証情報があります。
- 認証モードとして認証情報マッピングを使用するよう設定された 2 つの接続 CN1 と CN2 があります。
- DSR1 は接続 CN1 に関連付けられ、同様に DSR2 は CN2 に関連付けられています。

ここで、ユーザ A が販売データベースへのアクセスを必要とするレポートを最新表示しようとすると、BI プラットフォームはユーザプロパティで DSR1 を検索し、DSR1 に対して定義されたデータベース認証情報を利用して接続を確立します。

データソース参照を使用するには、以下のタスクを完了する必要があります。

1. データソース参照の作成 [399 ページ]
2. CMC におけるユーザのデータソース参照に対するデータベース認証情報の定義 [400 ページ]
3. OLAP 接続へのデータソース参照の関連付け [401 ページ]

> ⓘ 注記
>
> インフォメーションデザインツールで、リレーショナル接続および OLAP 接続の認証情報マッピングを設定することもできます。

10.1.1 データソース参照の作成

データソース参照は、管理者がユーザごとにデータベース認証情報の一意のセットを保存するために BI プラットフォームで作成する変数のように機能します。データソース参照を作成するには、以下の手順に従います。

1. CMC にログインします。
2. [定義] で、[データソース参照] に移動します。
3. アイコン ([新しいデータソース参照の作成]) を選択します。
4. データソース参照のタイトルおよび説明を追加します。
5. [OK] を選択します。

データソース参照が正常に作成されました。

10.1.2 CMC におけるユーザのデータソース参照に対するデータベース認証情報の定義

データソース参照には、ユーザがデータベースに接続できるように、ユーザプロパティで定義されたデータベース認証情報が必要です。以下の手順に従い、CMC でデータベース認証情報を定義します。

1. CMC にログインします。
2. [ユーザとグループ] に移動します。
3. [ユーザ一覧] から、ユーザのコンテキストメニューを開きます。
4. [プロパティ] に移動し、[データソース認証情報] で [追加] を選択します。
5. 優先するデータソース参照を選択します。
6. [アカウント名]、[パスワード]、[パスワードの再確認] の値を入力します。
7. 手順 4 からプロセスを繰り返して、別のデータソース参照を追加します。
8. [保存して閉じる] を選択します。

   データソース参照のデータベース認証情報が正常に定義されました。

10.1.3 BI ラウンチパッドにおけるユーザのデータソース参照に対するデータベース認証情報の定義

データソース参照には、ユーザがデータベースに接続できるように、ユーザプロパティで定義されたデータベース認証情報が必要です。

データソース参照を BI ラウンチパッドで利用可能になり、ユーザ認証情報を更新およびマップできるようになりました。データベース認証情報は、CMC と BI ラウンチパッド間で同期されます。

以下の手順に従い、BI ラウンチパッドでデータベース認証情報を定義します。

1. BI ラウンチパッドにログインします。
2. (ユーザ設定) に移動し、ドロップダウンから (設定) オプションをクリックします。

   [設定] ウィンドウが表示されます。
3. [ユーザアカウント (管理者)] をクリックします。

   [アカウント情報]、[データベース認証情報]、[認可トークン] の 3 つのタブを含む [ユーザアカウント] ページが開きます。
4. [データベース認証情報] をクリックします。

   ユーザの同期ユーザを、ここに表示される CMC から表示できます。

   > **注記**
   >
   > [データソース参照] の詳細は編集できません。
   >
   > ただし、[アカウント名]、[パスワード]、および [パスワードの再確認] の各フィールドは編集することができます。

   パスワードを変更すると、トーストメッセージが [一部の基本設定に対する変更は、ページをリロードした後で有効になります] 画面に表示されます。

5. マッピングされた認証情報の変更を保存するため、[保存] および [閉じる] をクリックします。

10.1.4 グループのデータソース参照に対するデータベース認証情報の定義

データソース参照には、ユーザがデータベースに接続できるように、ユーザプロパティで定義されたデータベース認証情報が必要です。

> **注記**
>
> このタスクでは、サブグループのメンバーのデータソース参照は更新されません。サブグループのメンバーのデータソース参照を更新するには、サブグループに対して同じ手順を繰り返します。

データベース認証情報を定義するには、以下の手順に従ってください。

1. CMC にログインします。
2. [ユーザとグループ] に移動します。
3. ユーザグループのコンテキストメニューを開き、[アカウントマネージャ] を選択します。
4. [データベース認証情報] に対してチェックボックスを選択し、[追加] を選択します。
5. 必須フィールドに値を入力します。
6. [保存して閉じる] を選択します。

ユーザグループのメンバーのデータベース認証情報を使用して、新しいデータソース参照が正常に定義されました。このユーザグループの任意のユーザの [プロパティ] に移動して、更新したデータソース参照をチェックできます。

10.1.5 OLAP 接続へのデータソース参照の関連付け

接続の認証モードとして認証情報マッピングが選択された場合、管理者には、好みのデータソース参照を選択するオプションが提供されます。

データソース参照を接続に関連付けるには、以下の手順に従います。

1. CMC にログインします。
2. [*OLAP* 接続] に移動します。
3. 既存の接続を開くか、新しいセッションを作成します。
4. [認証] フィールドで、[認証情報マッピング] を選択します。
   [データソース参照] フィールドが表示されます。
5. データソース参照を作成します。
6. その他の必要な詳細を入力して [保存] を選択します。

データソース参照が OLAP 接続に正常に関連付けられました。

11　サーバの管理

11.1　CMC の[サーバ]管理エリアの使用

CMC のサーバ管理エリアは、サーバ管理タスクの主要なツールです。この管理エリアには、デプロイメント内のすべてのサーバが一覧表示されます。多くの管理タスクと設定タスクの場合、一覧内のサーバを選択し、[管理]メニューまたは[アクション]メニューからコマンドを選択する必要があります。

ナビゲーションツリーについて

[サーバ]管理エリアの左側にあるナビゲーションツリーではさまざまな方法で[サーバの一覧]を表示できます。ナビゲーションツリーで項目を選択し、[詳細]ウィンドウに表示される情報を変更します。

ナビゲーションツリーのオプション	説明
サーバの一覧	デプロイメント内のすべてのサーバの一覧が表示されます。
サーバグループの一覧	詳細ウィンドウに使用可能なすべてのサーバグループを全レベル表示します。サーバグループの設定またはセキュリティを設定する場合にこのオプションを選択します。
サーバグループ	サーバグループと各サーバグループ内のサーバを一覧表示します。サーバグループを選択すると、そのグループに含まれるサーバとサーバグループが詳細ウィンドウに階層表示で示されます。
ノード	デプロイメント内のノードの一覧を表示します。ノードは、CCM で設定されます。ノードをクリックして選択し、ノードにあるサーバを表示または管理できます。

ナビゲーションツリーのオプション	説明
サービスカテゴリ	デプロイメント内にあるサービスの種類の一覧を示します。サービスカテゴリは、コア BI プラットフォームサービスと、特定の SAP Business Objects コンポーネントに関連付けられているサービスに分類されます。次のサービスカテゴリがあります。 • 接続サービス • コアサービス • *Crystal Reports* サービス • データフェデレーションサービス • プロモーション管理サービス • *Analysis* サービス • *Web Intelligence* サービス ナビゲーションリストでサービスカテゴリを選択し、カテゴリ内のサーバを表示または管理します。 **注記** サーバは、複数のサービスカテゴリに属するサービスをホストすることがあります。このため、1 つのサーバが複数のサービスカテゴリに表示されることがあります。
サーバステータス	サーバは、その現在のステータスに従って表示されます。これは、実行中のサーバと停止しているサーバを確認するのに役立つツールです。たとえば、システムのパフォーマンスが低下している場合は、[サーバステータス]一覧を使用して、異常な状態のサーバがないかすぐに確認できます。サーバの状態は次のとおりです。 • 停止 • 開始中 • 初期化中 • 実行中 • 停止中 • 実行中、エラーあり • 失敗 • リソースの待機中です

詳細ウィンドウについて

ナビゲーションツリーで選択したオプションに応じて、[サーバ]管理エリアの右側にある[詳細]ウィンドウには、サーバ、サーバグループ、状態、カテゴリ、またはノードの一覧が表示されます。次の表で、[詳細]ウィンドウに示されるサーバ情報について説明します。

> **注記**
>
> ノード、サーバグループ、カテゴリ、および状態については、[詳細]ウィンドウに名前と説明が通常表示されます。

詳細ウィンドウの列	説明
サーバ名または名前	サーバの名前を表示します。
状態	サーバの現在の状態を表示します。ナビゲーションツリーの[サーバステータス]一覧を使用して、サーバの状態で並べ替えることができます。サーバの状態は次のとおりです。 • 停止 • 開始中 • 初期化中 • 実行中 • 停止中 • 実行中、エラーあり • 失敗 • リソースの待機中です
有効	サーバが有効かどうかを表示します。
要再起動	サーバに[古い]とマークが付いている場合は、再起動が必要です。たとえば、サーバの[プロパティ]画面で特定のサーバ設定を変更した場合、変更を反映するには、サーバを再起動する必要があります。
種類	サーバの種類を表示します。
ホスト名	サーバのホスト名を表示します。
サーバの状態	サーバの健全性全般を表示します。 サーバの状態は次のとおりです。 • 緑色 (正常) • 黄色 (注意) • 赤色 (危険) サーバのヘルスステータスは、サーバの監視のステータスに直接依存します。たとえば、Central Management Server のヘルスステータスは `<NODENAME>.CentralManagementServer Watch` のステータスによって決まります。 監視の詳細へは CMC の [モニタリング] ページからアクセスできます。[監視リスト] タブで、監視を選択して [編集] をクリックします。監視の注意ルールおよび危険ルールが表示され、それぞれ黄色のヘルスステータスと赤色のヘルスステータスにマップされています。
PID	サーバの固有プロセス ID 番号を表示します。
説明	サーバの説明を表示します。この説明はサーバの[プロパティ]ページで変更できます。
変更した日付	サーバが最後に変更された日付、またはサーバの状態が変更された日付を表示します。この列は、最近変更されたサーバのステータスを確認する場合に役に立ちます。

11.2 Windows でのスクリプトを使用したサーバ管理

ccm.exe 実行可能ファイルを使用すると、コマンドラインを使用して Windows デプロイメント内にあるサーバの起動、停止、再起動、有効化および無効化することができます。

関連情報

ccm.exe [1056 ページ]

11.3 Unix でのサーバ管理

ccm.sh 実行可能ファイルを使用すると、コマンドラインを使用して Unix デプロイメント内にあるサーバを起動、停止、再起動、有効化、および無効化することができます。

関連情報

ccm.sh[ccm.sh] [1049 ページ]

11.4 サーバのステータスの表示および変更

11.4.1 サーバのステータスの表示

サーバのステータスとは、実行中、開始中、停止中、停止、失敗、初期化中、エラーありで開始、リソースの待機などの現在の動作状況を指します。BI プラットフォームリクエストに応答するには、サーバが実行中で、有効な状態にあることが必要です。無効にされたサーバはプロセスとして続けて実行されますが、BI プラットフォームのその他のコンポーネントからのリクエストは受け付けません。停止されたサーバは、プロセスとしての実行も停止します。

この節では、CMC を使用してサーバのステータスを変更する方法を説明します。

関連情報

サーバのステータスを表示する [406 ページ]
サービスの状態を表示する [406 ページ]

サーバの開始、停止、再起動 [407 ページ]
サーバの有効化/無効化 [410 ページ]
Central Management Server の停止 [409 ページ]
サーバを自動的に起動する [408 ページ]

11.4.1.1 サーバのステータスを表示する

1. CMC の [サーバ] 管理エリアを表示します。

   [詳細] ペインに、デプロイメントでのサービスカテゴリが表示されます。
2. ナビゲーションツリーに特定のサーバグループ、ノードまたはサービスカテゴリのサーバ一覧を表示するには、サーバグループ、ノード、カテゴリをクリックします。
   [詳細] ペインに、デプロイメント内のサーバ一覧が表示されます。 [状態] 列には、一覧内の各サーバのステータスが表示されます。
3. 現在特定のステータスになっているすべてのサーバの一覧を表示する場合は、ナビゲーションツリーで[サーバステータス]オプションを展開し、必要なステータスを選択します。

   選択されたステータスのサーバの一覧が詳細ウィンドウに表示されます。

   > ⓘ 注記
   >
   > この機能は、特に、正しく起動していない、または予期せずに停止したサーバの一覧をすばやく参照する必要がある場合に役に立ちます。

11.4.1.2 サービスの状態を表示する

サービスに障害が発生している場合、ホストサーバの状態は [実行中、エラーあり] (少なくとも 1 つのサービスの開始には成功しているという意味) または [失敗] (いずれのサービスの開始にも成功していないという意味) のいずれかに設定されています。CMC および CCM でサーバの状態を表示できます。ただし、CMC のサーバの [プロパティ] ページで、個別のサービスのステータスを表示することもできます。

1. CMC の [サーバ] 管理エリアに移動します。

   [詳細] ペインに、デプロイメントでのサービスカテゴリが表示されます。
2. ナビゲーションツリーに特定のサーバグループ、ノードまたはサービスカテゴリのサーバ一覧を表示するには、サーバグループ、ノード、カテゴリをクリックします。
   [詳細] ペインに、デプロイメント内のサーバ一覧が表示されます。
3. サーバをダブルクリックして、その [プロパティ] ページを開きます。

   [プロパティ] ページには、サーバのプロパティおよびサーバがホストするサービスが表示されます。失敗したサービスの場合、エラーメッセージも表示されます。

関連情報

サーバのステータスの表示 [405 ページ]

11.4.2 サーバの開始、停止、再起動

サーバの開始や停止、再起動は通常、サーバを設定するときや、サーバをオフラインにするときに実行する操作です。たとえば、サーバの名前を変更する場合は、最初にサーバを停止する必要があります。変更を行ったら、サーバを再起動して変更を有効にします。サーバの設定を変更すると、サーバの再起動が必要な場合は CMC にその旨を示すメッセージが表示されます。

この節の残りの部分では、特定の設定を変更する際に、いつサーバを停止または再起動する必要があるかについて説明します。ただし、これらのタスクは頻繁に発生するため、最初に概念と違いについて説明してから、参考として一般的な手順を説明します。

操作	説明
サーバを停止する	BI プラットフォームサーバを停止してから、特定のプロパティと設定を変更する必要があります。
サーバを開始する	サーバを設定するために停止した場合は、サーバを再起動して変更を有効にし、リクエストの処理を再開させる必要があります。
サーバを再起動する	サーバの再起動は、サーバを完全に停止してから再び開始するためのショートカットです。サーバの設定を変更した後にサーバを再起動する必要がある場合は、CMC にメッセージが表示されます。
サーバの自動起動	Server Intelligence Agent が起動するときにサーバも自動的に起動するよう設定することができます。
強制終了	サーバを直ちに停止します。一方、サーバを単に停止すると、現在処理しているアクティビティが完了してから停止します。サーバの停止が失敗した場合、およびサーバを直ちに停止する必要がある場合にのみ、強制的にサーバを終了させます。

→ ヒント

サーバを停止 (または再起動) する場合、サーバのプロセスを終了し、サーバは完全に停止します。サーバを停止する前に、以下を実行することをお勧めします。

- サーバを無効化し、進行中のジョブの処理を終了できるようにする。
- キュー内に残っている監査イベントがないことを確認する。キュー内に残っている監査イベント数を表示するには、サーバの [メトリクス] 画面に移動し、[キュー内の監査イベントの現在の数] メトリクスを表示します。

関連情報

サーバの有効化/無効化 [410 ページ]

11.4.2.1 CMC でサーバを起動、停止、または再起動する

1. CMC の [サーバ] 管理エリアを表示します。

   [詳細] ペインに、デプロイメントでのサービスカテゴリが表示されます。
2. 特定のサーバグループ、ノード、またはサービスカテゴリに含まれるサーバの一覧を表示するには、ナビゲーションペインでグループ、ノード、またはカテゴリを選択します。
   [詳細] ペインに、サーバの一覧が表示されます。
3. 現在特定のステータスになっているすべてのサーバの一覧を表示する場合は、ナビゲーションツリーで[サーバステータス]オプションを展開し、必要なステータスを選択します。

   選択されたステータスのサーバの一覧が [詳細] ペインに表示されます。

   > ⓘ 注記
   >
   > この機能は、特に、正しく起動していない、または予期せずに停止したサーバの一覧をすばやく参照する必要がある場合に役に立ちます。
4. ステータスを変更するサーバを右クリックして、実行する必要のあるアクションに応じて、[サーバの起動]、[サーバの再起動]、[サーバの停止] または [強制終了] をクリックします。

11.4.2.2 CCM を使用して Windows 環境のサーバを開始、停止、または再起動する

1. CCM で、ツールバーの [サーバの管理] ボタンをクリックします。
2. 指示に従って、管理アカウントで CMS にログオンします。
3. [サーバの管理] ダイアログボックスで、開始、停止、または再起動するサーバを選択します。
4. [開始]、[停止]、[再起動] または [強制終了] をクリックします。
5. [閉じる] をクリックして CCM に戻ります。

11.4.2.3 サーバを自動的に起動する

デフォルトでは、Server Intelligence Agent が起動すると、デプロイメント内のサーバが自動的に起動します。このタスクでは、自動起動オプションの設定方法を説明します。

1. CMC の[サーバ]管理エリアを表示します。
2. 自動起動するサーバをダブルクリックします。
   [プロパティ] 画面が表示されます。
3. [共通設定] の下で、[*Server Intelligence Agent* の起動時にこのサーバを自動的に起動します] チェックボックスをオンにし、[保存] または [保存して閉じる] をクリックします。

   > ⓘ 注記
   >
   > クラスタの各 CMS の [*Server Intelligence Agent* の起動時にこのサーバを自動的に起動します] チェックボックスがオフの場合、CCM を使用してシステムを再起動する必要があります。CCM を使用して SIA を停止した後、SIA を右クリックして、[プロパティ] を選択します。[スタートアップ] タブで、[プロパテ

ィ] をクリックして、CMS の [サーバプロパティ] ページを開きます。[自動開始] を選択し [*OK*] をクリックして [サーバプロパティ] ページを閉じ、再度 [*OK*] をクリックします。SIA を再起動します。[自動開始] オプションは、クラスタの各 CMS の [*Server Intelligence Agent の起動時にこのサーバを自動的に起動します*] チェックボックスがオフの場合のみ利用できます。

11.4.3 Central Management Server の停止

BI プラットフォームのインストールに複数の有効な Central Management Server (CMS) がある場合は、データを失うことなく、またはシステム機能に影響を与えることなく単一 CMS をシャットダウンすることができます。この場合、ノード上の別の CMS が、停止したサーバの処理を引き継ぎます。複数の CMS をクラスタ化することにより、BI プラットフォームのサービスを停止せずに、各 Central Management Server のメンテナンスを交代で実行することができます。

ただし、BI プラットフォームデプロイメント内に CMS が 1 つしかない場合、CMS をシャットダウンすると、ユーザはプラットフォームを使用できなくなり、レポートとプログラムの処理が中断します。この問題を回避するために、各ノードの Server Intelligence Agent によって、常に 1 つ以上の CMS が実行されているか確認されます。SIA を停止して CMS も停止することもできますが、SIA を停止する前に、進行中のすべてのジョブが完了してから BI プラットフォームがシャットダウンするように CMC で処理サーバを無効にする必要があります。そうしないと、ノードの他のサーバもすべてシャットダウンしてしまいます。

> ⓘ 注記
>
> CMS が停止し、CCM からシステムを再起動しなければならない場合があります。たとえば、ノードの各 CMS をシャットダウンし、SIA 起動時にクラスタの各 CMS の [*Server Intelligence Agent の起動時にこのサーバを自動的に起動します*] チェックボックスがオフの場合、CCM を使用してシステムを再起動する必要があります。CCM で、SIA を右クリックし、[プロパティ] を選択します。[スタートアップ] タブで、[プロパティ] をクリックして、CMS の [サーバプロパティ] ページを開きます。 [自動開始] を選択し [*OK*] をクリックして [サーバプロパティ] ページを閉じ、再度 [*OK*] をクリックします。 SIA を再起動します。[自動開始] オプションは、クラスタの各 CMS の [*Server Intelligence Agent の起動時にこのサーバを自動的に起動します*] チェックボックスがオフの場合のみ利用できます。

他のサーバを起動および停止しなくても、クラスタ内の Central Management Server を起動および停止できるようにシステムを設定するには、CMS を別のノード上に配置します。新しいノードを作成し、CMS をノードにクローンします。CMS がそれぞれ独自のノードにある場合、他のサーバに影響することなく、ノードを簡単にシャットダウンできます。

関連情報

ノードの使用 [451 ページ]
サーバのクローン [412 ページ]
Central Management Server のクラスタ化 [414 ページ]

11.4.4 サーバの有効化/無効化

BI プラットフォームサーバを無効にすると、新しい BI プラットフォームリクエストの受け付けおよび応答が停止されますが、実際にはサーバプロセスは停止していません。これは、サーバを完全に停止する前に現在の全リクエストの処理を完了する必要がある場合に便利です。

たとえば、Job Server を実行しているマシンを再起動する前に、Job Server を停止するとします。この場合、キューにある未処理のレポートリクエストを完了させるようにするとします。まず、リクエストがこれ以上受け付けられないように、Job Server を無効にします。次に、セントラル管理コンソールでサーバ上の処理中のジョブを監視し、それらが完了するのを待ちます。([サーバ] 管理エリアから、サーバを右クリックして [メトリクス] を選択します。)現在のリクエストの処理が完了したら、サーバを安全に停止できます。

> ⓘ 注記
>
> CMS を実行していなければ、その他のサーバを有効または無効にすることはできません。

> ⓘ 注記
>
> CMS を有効または無効にすることはできません。

11.4.4.1 CMC でサーバを有効/無効にする

1. CMC の [サーバ] 管理エリアを表示します。
2. ステータスを変更するサーバを右クリックして、実行する必要のあるアクションに応じて、[サーバの有効化] または [サーバの無効化] をクリックします。

11.4.4.2 CCM を使用して Windows 環境のサーバを有効/無効にする

1. CCM で [サーバの管理] をクリックします。
2. 指示に従って、BI プラットフォームの管理者権限があるアカウント情報を使用して、CMS にログオンします。
3. [サーバの管理] ダイアログボックスで、有効または無効にするサーバを選択します。
4. [有効] または [無効] をクリックします。
5. [閉じる] をクリックして CCM に戻ります。

11.5 サーバの追加、クローン、または削除

11.5.1 サーバの追加、クローン、および削除

追加された新しいマシンにサーバコンポーネントをインストールして、BI プラットフォームに新しいハードウェアを追加する場合は、それらのマシンで BI プラットフォームインストールプログラムを実行します。 セットアッププログラムでは、カスタムインストールを実行できます。 カスタムインストールでは、既存のデプロイメントの CMS を指定して、ローカルマシンにインストールするコンポーネントを選択します。 カスタムインストールのオプションの詳細については、*SAP BI* プラットフォームインストールガイドを参照してください。

11.5.1.1 サーバの追加

1 つのマシン上で同一の BI プラットフォームサーバの複数のインスタンスを実行できます。 サーバを追加するには、次の操作を行います。

1. CMC の [サーバ] 管理エリアを表示します。
2. [管理] メニューの 新規 > 新しいサーバ をクリックします。
   [新規サーバ名]ダイアログボックスが開きます。
3. [サービスカテゴリ]を選択します。
4. [サービスの選択] 一覧からサービスのタイプを選択し、[次へ] をクリックします。
5. 追加のサービスをサーバに追加するには、[利用可能な追加のサービス]一覧でサービスを選択し、[>]をクリックします。

   > **注記**
   >
   > すべてのタイプのサーバで追加のサービスを利用できるわけではありません。

6. 必要なサービスを追加した後に、[次へ]をクリックします。
7. BI プラットフォームアーキテクチャが複数のノードで構成されている場合は、[ノード] 一覧から新しいサーバを追加するノードを選択します。
8. [サーバ名]ボックスにサーバの名前を入力します。

   システムの各サーバには、一意の名前が必要です。 デフォルトの命名規則は `<NODENAME>.<servertype>` です (同じホストマシン上に同じタイプのサーバが複数ある場合は、名前に数字が付け加えられます)。
9. サーバの説明を含める場合は、[説明]ボックスに説明を入力します。
10. 新しい Central Management Server を追加する場合は、[ネームサーバポート]フィールドでポート番号を指定します。
11. [作成] をクリックします。
    新しいサーバが、CMC の[サーバ]エリアのサーバの一覧に表示されますが、開始されていなくて、有効にもなっていません。
12. 新しいサーバに BI プラットフォームリクエストへの応答を開始させるには、CMC を使用してサーバを開始して有効にします。

11.5.1.2 サーバのクローン

今後は、デプロイメントで新しいサーバインスタンスが必要になった場合は、既存のサーバをクローンできます。クローンされたサーバでは、共通設定とコマンドラインのパラメータを除き、元のサーバの構成設定が維持されます。デプロイメントを拡張していて、既存のサーバとほとんど同じ設定のサーバを使用する新しいサーバインスタンスを作成する必要がある場合に、これは特に便利です。

クローンによって、マシン間でのサーバの移動の処理も簡便になります。既存の CMS を別のノードに移動する場合は、その CMS を新しいノードにクローンします。クローンされた CMS が新しいノードに表示され、共通設定とコマンドラインのパラメータを除いた、元の CMS の構成設定がすべて維持されます。

サーバをクローンするときに、注意しておく点がいくつかあります。いくつかの設定がクローンされない可能性があるため、クローンされたサーバをチェックして要件を満たしていることを確認します。

> ⓘ 注記
>
> サーバをクローンする前に、デプロイメント内のすべてのマシンで BI プラットフォーム (および必要に応じた更新) のバージョンが同じであることを確認します。

> ⓘ 注記
>
> どのマシンからもサーバをクローンできます。ただし、サーバに必要なバイナリがインストールされているマシンにのみサーバをクローンできます。

> ⓘ 注記
>
> サーバをクローンする場合、必ずしも新しいサーバで同じ OS 認証情報を使用する必要はありません。ユーザアカウントは、サーバが実行されている Server Intelligence Agent で制御されます。

11.5.1.2.1 サーバ設定でのプレースホルダの使用

プレースホルダはノードレベルの変数で、ノード上で実行中のサーバによって使用されます。プレースホルダは、セントラル管理コンソール (CMC)の指定ページに一覧表示されています。CMC の[サーバ]にリストされているサーバをダブルクリックすると、“プレースホルダ”の左側のナビゲーションペインにリンクが示されます。[プレースホルダ]ページには、選択したサーバで使用可能なすべてのプレースホルダの名前と関連する値が示されます。プレースホルダには読み取り専用の値が含まれ、プレースホルダ名の前後にはパーセント記号 % が付いています。

> ⓘ 注記
>
> プレースホルダの設定は、CMC サーバの[プロパティ]ページで特定の文字列で常に上書きできます。

例

サーバを複製する場合にプレースホルダが役に立ちます。たとえば、マルチドライブマシン A には、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0` に BI プラットフォ

ームがインストールされています。したがって、%DefaultAuditingDir% プレースホルダは D:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥Auditing¥ です。

別のマシン B には、1 台のディスクドライブしかなく (ドライブ D はありません)、BI プラットフォームは C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0 にインストールされています。この場合、%DefaultAuditingDir% プレースホルダは C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥Auditing¥ です。

Event Server をマシン A からマシン B に複製するには、監査一時ディレクトリにプレースホルダを使用すると、プレースホルダは自身で解決し、Event Server は正しく機能します。プレースホルダを使用しないと、監査一時ディレクトリの設定を手動で上書きしない限り、Event Server は失敗します。

11.5.1.2.2 サーバをクローンする

1. クローンされたサーバを追加するマシンで、CMC の [サーバ] 管理エリアを表示します。
2. クローンするサーバを右クリックし、[クローンサーバ] を選択します。
   [クローンサーバ] ダイアログボックスが開きます。
3. [新しいサーバ名] フィールドに、サーバの名前を入力します (またはデフォルト名を使用します)。
4. Central Management Server をクローンする場合は、[ネームサーバポート] フィールドでポート番号を指定します。
5. [ノードに複製] リストでクローンサーバを追加するノードを選択し、[*OK*] をクリックします。
   CMC の [サーバ] 管理エリアに、新しいサーバが表示されます。

11.5.1.3 サーバの削除

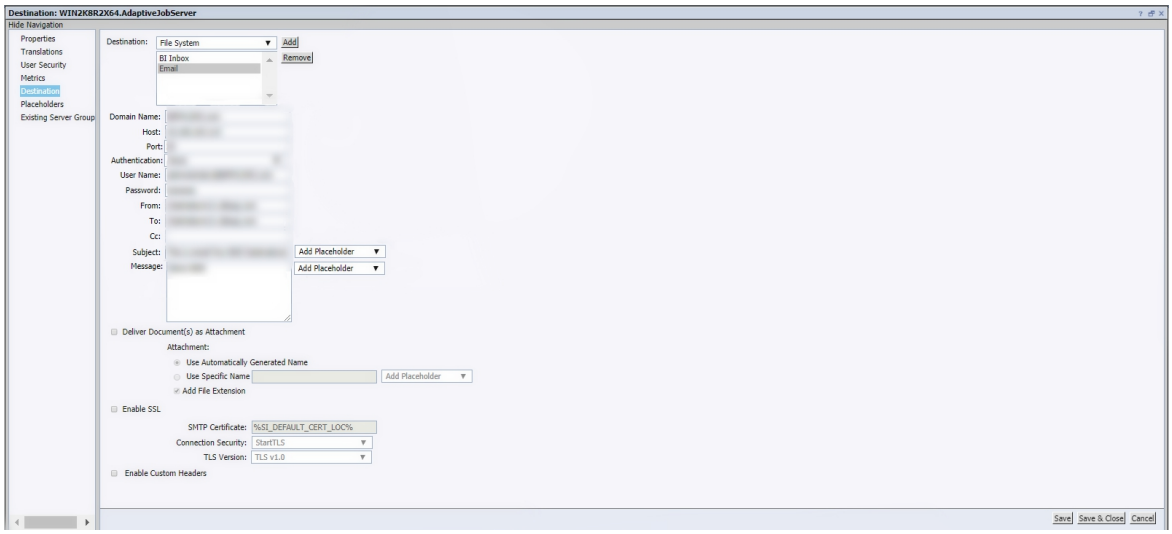
1. CMC の[サーバ]管理エリアを表示します。
2. 削除するサーバを停止します。
3. サーバを右クリックし、[削除]を選択します。
4. 確認を求めるメッセージが表示されたら、[*OK*]をクリックします。

11.6 カスタムインターネットヘッダの追加

電子メールメッセージのインターネットヘッダは、メッセージの作成者、メッセージが通過した電子メールサーバ、およびメッセージの作成に使用されたツールまたはソフトウェアに関する情報で構成されます。SAP BusinessObjects BI プラットフォームから、スケジュールされる電子メールにカスタムインターネットヘッダを追加できるようになりました。以下の手順に従って、カスタムヘッダを追加します。

1. [*CMC*] にログインします。
2. [サーバ]、[サーバの一覧] の順に移動します。
3. [*Adaptive Job Server*] のコンテキストメニューを開き、[出力先] を選択します。

4. [出力先] ウィザードで、[電子メール] を選択し、以下のように各フィールドに必要な詳細を追加します。



5. [カスタムヘッダを有効にする] をオンにし、以下のように空白フィールドにインターネットヘッダを追加します。

6. [保存して終了] を選択します。

スケジュール済みのドキュメントが添付された電子メールに、インターネットヘッダが含まれるようになりました。

> **注記**
>
> - スケジュール時に、[デフォルト設定を使用] を選択して、スケジュールされた電子メールにカスタムインターネットヘッダを追加します。
> - すべての電子メールにカスタムヘッダが追加されるように、すべての [*Adaptive Job Server*] を設定する必要があります。

11.7 Central Management Server のクラスタ化

11.7.1 Central Management Server のクラスタ化

大規模な SAP BusinessObjects Business Intelligence プラットフォームシステムを使用したり、ミッションクリティカルな環境でシステムを使用したりする場合、複数の CMS マシンを 1 つのクラスタとして一度に実行することがあります。 クラスタは、共通する 1 つの CMS システムデータベースに対して同時に動作する 2 つ以上の CMS サーバで構成されます。 1 つの CMS を実行している 1 台のマシンに障害が発生した場合でも、他の CMS が BI プラットフォームのリクエストを処理し続けます。 この "高可用性" 機能により、機器に障害が発生しても BI プラットフォームのユーザは情報にアクセスすることができます。

この節では、すでに実際に稼動している業務用システムに、新しい CMS クラスタメンバーを追加する方法について説明します。 既存のクラスタに新しい CMS を追加する場合は、既存の CMS システムデータベースに接続し

て、既存の CMS マシンと処理の負荷を共有するよう新しい CMS に指示します。 現在の CMS の詳細については、CMC の [サーバ] 管理エリアを表示します。

CMS マシンをクラスタ化する前に、システムにインストールされた各 CMS が、製品出荷マトリックスに概説された、オペレーティングシステム、データベースサーバ、データベースアクセス方式、データベースドライバ、およびデータベースクライアントに関する要件を、(バージョンとパッチレベルも含めて) 正確に満たしていることを確認する必要があります。

さらに、クラスタ化に関する以下の要件を満たす必要があります。

- 最適のパフォーマンスを得るためには、短いクエリを高速に処理可能なデータベースサーバを、システムデータベースのホストサーバとして選択する必要があります。 CMS は、頻繁にシステムデータベースと通信して多数の短いクエリを送信します。 データベースサーバがこれらのリクエストをタイムリーに処理できないと、BI プラットフォームのパフォーマンスが大幅に低下します。
- パフォーマンスを最大にするには、同じメモリ容量と CPU タイプのマシン上で CMS クラスタの各メンバーを実行します。
- 各マシンを同じように設定します。
  - 同じオペレーティングシステムをインストールし、サービスパックやパッチも含めてバージョンを同じにします。
  - 同じバージョンの BI プラットフォーム (パッチがある場合は、パッチも同一のもの) をインストールします。
  - 各 CMS が CMS システムデータベースに同じ方法で接続することを確認します。 ネイティブのドライバまたは ODBC ドライバのどちらを使用するかを確認します。 ドライバが、各マシンで同じであること、およびサポートされるバージョンであることを確認します。
  - 各 CMS が、同じデータベースクライアントを使用してシステムデータベースに接続していること、およびそのクライアントがサポートされているバージョンであることを確認します。
  - 各 CMS が、CMS システムデータベースに接続するために同じデータベースユーザアカウントとパスワードを使用していることを確認します。 このアカウントには、システムデータベースに対する作成、削除、および更新アクセス権が与えられている必要があります。
  - 各 CMS が存在するノードが、同じオペレーティングシステムアカウントで実行されていることを確認します (Windows では、デフォルトはローカルシステムアカウントです)。
  - 各 CMS マシンで、現在の日時が (夏時間設定を含めて) 正確に設定されていることを確認します。
  - クラスタ内のすべてのマシン (CMS をホストしているマシンを含む) が、同じシステム時刻に設定されていることを確認してください。 最善策は、マシンをタイムサーバ (`time.nist.gov` など) と同期するか、中央監視ソリューションを使用することです。
  - クラスタ内のすべての Web アプリケーションサーバに同じ WAR ファイルがインストールされていることを確認します。 WAR ファイルのデプロイメントの詳細については、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドを参照してください。
- クラスタ内の各 CMS が同じ LAN 上に設置されていることを確認します。
- クラスタ化の Ping とクラスタ化の通知には、アウトオブバンドスレッド (-oobthreads) が使用されます。 両方の処理が速い (通知は非同期で実行する) ため、BI プラットフォームで複数の oobthreads は必要なくなり、1 つの -oobthread のみが作成されます。
  クラスタに 9 個以上の CMS クラスタメンバーが含まれている場合、各 CMS のコマンドラインに `-oobthreads <numCMS>` オプションが含まれていることを確認してください。`<numCMS>` はクラスタ内の CMS サーバの数です。 このオプションによって、クラスタは大きな負荷を処理できます。 サーバのコマンドラインの設定の詳細については、*SAP BusinessObjects Business Intelligence* プラットフォーム管理者ガイドのサーバコマンドラインに関する付録を参照してください。
- 単一の CMS そのものに対する監査の有効化は、クラスタ環境での設定として機能します。 CMC における監査設定ページで監査データベース詳細を変更することもできます。 監査データベースの要件は、データベー

スサーバ、クライアント、アクセス方式、ドライバ、ユーザ ID に関してはシステムデータベースの要件と同じです。

> → ヒント
>
> デフォルトで、クラスタ名には最初にインストールされた CMS のマシンホスト名が反映されます。

関連情報

CMS クラスタの名前変更 [417 ページ]

11.7.1.1 クラスタへの CMS の追加

新しい CMS クラスタメンバーを追加するには、いくつか方法があります。該当する手順に従ってください。

- 新しいマシンの CMS に新しいノードをインストールできます。
- CMS バイナリファイルにノードがすでにある場合は、新しい CMS サーバを CMC から追加できます。
- CMS バイナリファイルにノードがすでにある場合も、既存の CMS サーバをクローンして新しい CMS サーバを追加できます。

> ⓘ 注記
>
> 変更を行う前に、現在の CMS システムデータベース、サーバ設定、および Input/Output File Repository のコンテンツをバックアップしておきます。必要に応じて、データベース管理者に連絡してください。

関連情報

クラスタへの新しいノードの追加 [416 ページ]
サーバの追加 [411 ページ]
サーバのクローン [412 ページ]
バックアップと復元の概要 [530 ページ]

11.7.1.2 クラスタへの新しいノードの追加

ノードを追加するとき (ノードは単一の Server Intelligence Agent によって管理される BI プラットフォームサーバのコレクション)、新しい CMS を作成するか、ノードを既存の CMS にクラスタ化するかを尋ねられます。

ノードを既存の CMS にクラスタ化する場合は、インストールセットアッププログラムを使用することもできます。新しい CMS クラスタメンバーをインストールするマシンで、BI プラットフォームインストールおよびセットアッププログラムを実行します。セットアッププログラムでは、カスタムインストールを実行できます。カスタ

ムインストールでは、拡張するシステムの既存の CMS を指定して、ローカルマシンにインストールするコンポーネントを選択します。この場合、既存のシステムを実行している CMS の名前を指定して、ローカルマシンに新しい CMS をインストールするよう選択します。さらに、既存の CMS システムデータベースに接続するために必要な情報をセットアッププログラムで指定します。セットアッププログラムが新しい CMS をローカルマシンにインストールすると、既存のクラスタにサーバが自動的に追加されます。

> ⓘ 注記
>
> 新しいノードを既存の CMS にクラスタ化する前に、新しいノードがまったく新しいサーバの場合は、そのサーバ上の BI プラットフォームのインストールが、既存の BI プラットフォーム環境と同じパッチレベルであることを確認してください。

> ⓘ 注記
>
> Edge BI と Crystal Server のライセンスでは、クラスタリングや複数ノードデプロイメントを実行できません。ただし、Edge BI 4.3 SP2 および Crystal Server 2020 SP2 より、Linux で Edge BI と Crystal Server がデプロイされる場合は、Crystal Reports 2020 サービスを含む 1 つの Windows ノードが許可されます。詳細については、SAP Crystal Reports 2020 サービスを Windows サーバに配布する方法を参照してください。

関連情報

ノードの使用 [451 ページ]

11.7.1.3 Web アプリケーションプロパティファイルへのクラスタの追加

追加の CMS をデプロイメントに追加した場合、その情報は `C:/Users/<you_user>/.businessobjects` にある `clusterinfo.1400.properties` ファイルに取得されます。このファイルは、SIA を再起動すると生成または更新されます。

> ⓘ 注記
>
> スタンドアロンの Tomcat デプロイメントでは、`clusterinfo.1400.properties` ファイルは CMS 名のいずれかでログインしたときにのみ生成されます。クラスタを更新したときに、スタンドアロンの Tomcat デプロイメントのファイルは更新されません。ファイルを CMS から Tomcat マシンにコピーする必要があります。

11.7.1.4 CMS クラスタの名前変更

次の手順を使用すると、すでにインストールされているクラスタの名前を変更できます。 CMS クラスタの名前の変更後、Server Intelligences Agent が自動的に各 SAP Business Objects サーバを再設定して、各サーバが個々の CMS ではなく CMS クラスタに登録されるようにします。

> ⓘ 注記
>
> 経験豊富な BI プラットフォーム管理者の場合、-ns オプションをサーバコマンドラインで使用して、サーバを登録する CMS を設定できなくなった点に注意してください。この作業は現在 SIA で自動的に処理されます。

11.7.1.4.1 Windows 上でクラスタ名を変更する

1. 名前を変更するクラスタのメンバーである CMS を含むノードに対して Server Intelligence Agent を停止するときは、CCM を使用します。
2. Server Intelligence Agent を右クリックし、[プロパティ]を選択します。
3. [プロパティ]ダイアログボックスで[設定]タブをクリックします。
4. *[クラスタ名を変更]*チェックボックスをオンにします。
5. クラスタの新しい名前を入力します。
6. [*OK*]をクリックし、Server Intelligence Agent を再起動します。

   これで CMS クラスタ名が変更されます。残りの CMS クラスタメンバーには、新しいクラスタ名が動的に通知されます。すべてのクラスタメンバーに変更が反映されるには数分かかることがあります。
7. CMC の*[サーバ]*管理エリアを表示して、残りのサーバがすべて有効のままであることを確認します。必要に応じて、変更によって無効になったサーバを有効にします。

11.7.1.4.2 UNIX 上でクラスタ名を変更する

`cmsdbsetup.sh` スクリプトを使用します。 詳細については、*BI プラットフォーム管理者ガイド*のコマンドライン管理の章で、“Unix スクリプト”のトピックを参照してください。

関連情報

Unix スクリプト [1049 ページ]

11.8 サーバグループの管理

サーバグループにより、システムの BI プラットフォームサーバを整理し、その管理を容易にします。 (ユーザではなく) パブリケーション別に特定のサーバまたはサーバグループを選択し、地域またはタイプ別にサーバをグループ化することができます。

デフォルト処理設定、定期スケジュール、およびスケジュールの出力先を、特定の地域オフィスで勤務するユーザに対して容易に設定するために、サーバを地域別にグループ化します。 オブジェクトが常に同じサーバで処理

されるよう、レポートオブジェクト (Crystal レポートや Web Intelligence ドキュメントなど) を単一のサーバグループに関連付けることができます。また、スケジュールされたオブジェクトが適切なプリンタやファイルサーバなどに送信されるよう、スケジュールされたレポートオブジェクトを特定のサーバグループに関連付けることもできます。 複数の場所および複数のタイムゾーンにまたがるシステムの保守を行う場合、サーバグループは特に有用です。

複数の場所および複数のタイムゾーンにまたがるシステムの保守を行う場合、サーバグループは特に有用です。 たとえば、複数の場所および複数のレポートタイプで表示されるレポート向けに BI プラットフォームシステムをカスタマイズする場合に、サーバグループを使用します。 サーバを地域別に整理する場合、サーバグループに対して以下のアクションを実行できます。

- デフォルト処理設定の設定
- 定期スケジュールの設定
- 特定の地域オフィスで勤務するユーザに対するスケジュールの出力先の設定
- オブジェクトが常に同じサーバで処理されるようにするための、レポートオブジェクト (Crystal レポートや Web Intelligence ドキュメントなど) の単一のサーバグループへの関連付け
- スケジュールされたオブジェクトが適切なプリンタやファイルサーバなどに送信されるようにするための、スケジュールされたレポートオブジェクトの特定のサーバグループへの関連付け

これらのオブジェクトに対して最適化されたサーバによって処理されるようオブジェクトを設定する場合に、サーバをタイプ別にグループ化します。

サーバグループを作成した後、レポートのスケジュール、表示、および変更に特定のサーバグループを使用するよう、オブジェクトを設定します。 CMC のサーバ管理エリアのナビゲーションツリーを使用して、サーバグループを表示します。 サーバグループの一覧オプションでは、サーバグループの一覧が詳細ペインに表示され、サーバグループオプションでは、グループ内のサーバを表示できます。

例: 処理サーバのタイプ別グループ化

たとえば、処理サーバは、公開レポートのデータを含むデータベースと頻繁にアクセスする必要があります。 アクセスが必要なデータベースサーバの近くに処理サーバを設置すると、システムのパフォーマンスが向上し、ネットワークトラフィックを最小限に抑えることができます。 そのため、DB2 データベースに対して多数のレポートが実行される場合は、DB2 データベースサーバに対するレポートのみを処理する処理サーバのグループを作成できます。 レポートの表示におけるシステムパフォーマンスを改善するため、表示に常にこの処理サーバグループを使用するようレポートを設定できます。

11.8.1 サーバグループの作成

サーバグループを作成するには、グループの名前と説明を指定した後に、サーバをグループに追加する必要があります。

11.8.1.1 非排他的サーバグループを登録する

非排他的サーバグループには、その他の非排他的サーバグループや一般的なサーバプールの一部であるサーバやサーバグループを含めることができます。

1. CMC の [サーバ] 管理エリアを表示します。
2. 管理 > 新規 > サーバグループの作成 の順にクリックします。

   [サーバグループの作成] ダイアログボックスが表示されます。
3. [名前] フィールドに、新しいサーバグループの名前を入力します。
4. サーバグループに追加情報を含める場合、[説明] フィールドに入力します。
5. [*OK*] をクリックします。
6. [サーバ]管理エリアで、ナビゲーションツリーの[サーバグループ]をクリックして新しいサーバグループを選択します。
7. [アクション] メニューの [メンバーの追加] を選択します。
8. このグループに追加するサーバを選択してから、[>] をクリックします。

   > → ヒント
   >
   > 複数のサーバを選択するには、CTRL + キーを押しながらクリックします。

   > ⓘ 注記
   >
   > 一覧表示されたサーバには、その他の排他的サーバグループの一部ではないサーバのみが含まれます。

9. [*OK*] をクリックします。

   [サーバ] 管理エリアに戻ります。このタブには、グループに追加したすべてのサーバが表示されます。これで、ステータスの変更、サーバメトリクスの表示、グループ内にあるサーバのプロパティの変更ができるようになります。

11.8.1.2 排他的サーバグループを作成する

排他的サーバグループには、その他のサーバグループや一般的なサーバプールの一部ではないサーバまたはサーバグループが含まれます。サーバグループを排他的サーバグループとして登録した場合、このグループに含まれるサーバを他のサーバグループ (排他的または非排他的) に割り当てることはできません。また、排他的サーバグループに追加されたサーバは共通プールから除外されます。これにより、BI システムの全般的な負荷から切り離されたサーバグループを作成することができます。

1. CMC の [サーバ] 管理エリアを表示します。
2. 管理 > 新規 > サーバグループの作成 の順にクリックします。

   [サーバグループの作成] ダイアログボックスが表示されます。
3. [名前] フィールドに、新しいサーバグループの名前を入力します。
4. サーバグループに追加情報を含める場合、[説明] フィールドに入力します。
5. [排他的サーバグループ] チェックボックスを選択します。

> ⓘ 注記
>
> 排他的サーバグループは、ルートレベルでのみ登録することができます。子ノードの場合、ルートまたは親サーバグループが排他である場合にのみ排他的サーバグループを登録することができます。
>
> > 例
> >
> > 次のシナリオについて考えて、排他的サーバグループの理解を深めてください。
> >
> > 2 つの Job Server である JS1 および JS2 は、共通サーバプールに属しています。
> >
> > 排他的サーバグループ SG1 を作成します。
> >
> > JS1 を SG1 に追加します。
> >
> > [選択したグループ内のサーバのみを使用する] を選択して、ドキュメント (D) をスケジュールします。
> >
> > JS1 と JS2 の両方ですでにいくつかのジョブが実行されているとします。
> >
> > 結果: JS1 には、処理が必要ないくつかのジョブがすでにロードされています。ただし、JS1 は現在 SG1 に含まれているため、JS1 は SG1 に割り当てられたワークフローを処理する要求のみを取得します。つまり、JS1 は全般的なシステム負荷から解放されます。

6. [*OK*] をクリックします。
7. [サーバ]管理エリアで、ナビゲーションツリーの[サーバグループ]をクリックして新しいサーバグループを選択します。
8. [アクション] メニューの [メンバーの追加] を選択します。
9. このグループに追加するサーバを選択してから、[>] をクリックします。

> → ヒント
>
> 複数のサーバを選択するには、CTRL + キーを押しながらクリックします。

> ⓘ 注記
>
> ほかのサーバグループや共通サーバプールにまだ属していないサーバのみが一覧表示されます。

10. [*OK*] をクリックします。

    [サーバ] 管理エリアに戻ります。このタブには、グループに追加したすべてのサーバが表示されます。これで、ステータスの変更、サーバメトリクスの表示、グループ内にあるサーバのプロパティの変更ができるようになります。

11.8.2 排他的サーバグループを非排他的サーバグループに変換するおよびその逆も可能です。

11.8.2.1 排他的サーバグループの非排他的サーバグループへの変換

既存の排他的サーバグループを変更して非排他的サーバグループにすることができます。

root レベルの排他的サーバグループを非排他的サーバグループに変換するには、以下を実行します。

1. 変換する排他的サーバグループを右クリックして、ドロップダウンから [プロパティ] を選択します。

   [プロパティ] ダイアログボックスが開きます。[排他的サーバグループ] チェックボックスが選択されていることがわかります。
2. [排他的サーバグループ] チェックボックスを選択解除します。

   警告メッセージが表示されます。
3. [*OK*] を選択して変換を確認します。
4. [保存して閉じる] を選択します。

   排他的サーバグループを非排他的サーバグループに変換しました。

> ⓘ 注記
>
> root レベルの排他的サーバグループのみを非排他的サーバグループに変換することができます。

11.8.2.2 非排他的サーバグループから排他的サーバグループへの変換

既存の非排他的サーバグループを変更して排他的サーバグループにすることができます。

独立したサーバおよびサーバグループを含む非排他的サーバグループを変換するには、以下を実行します。

1. 変換する非排他的サーバグループを右クリックして、ドロップダウンから [プロパティ] を選択します。

   [プロパティ] ダイアログボックスが開きます。[排他的サーバグループ] チェックボックスが選択されていないことがわかります。
2. [排他的サーバグループ] チェックボックスを選択します。

   成功メッセージが表示されます。
3. [*OK*] を選択します。
4. [保存して閉じる] を選択します。

   非排他的サーバグループを排他的サーバグループに変換しました。

> ⓘ 注記
>
> 排他にする独立したサーバおよびサーバグループを含む非排他的サーバグループのみを変換することができます。独立したサーバおよびサーバグループは、ほかのサーバグループに属さないサーバおよびサーバグループです。

11.8.3 サーバサブグループの使用

サーバのサブグループを使用すると、一歩進んだサーバの編成が可能になります。サブグループとは、別のサーバグループに属するサーバグループのことです。

たとえば、地域別および国別にサーバをグループ化する場合、各地域グループは国グループのサブグループとなります。この方法でサーバを編成するには、まず地域ごとにグループを作成し、各地域グループに適切なサーバを追加します。次に、国別にグループを作成し、各地域グループを対応する国グループに追加します。

サブグループの設定には、サーバグループのサブグループを変更する方法と、あるサーバグループを別のサーバグループのメンバーにする方法があります。どちらも結果は同じなので、設定しやすい方法を使用してください。

11.8.3.1 サーバグループにサブグループを追加する

1. CMC の [サーバ] 管理エリアを表示します。
2. ナビゲーションツリーの[サーバグループ]をクリックし、サブグループを追加するサーバグループを選択します。

   このグループは親グループとなります。
3. [アクション] メニューの [メンバーの追加] を選択します。
4. ナビゲーションツリーの [サーバグループ] をクリックし、このグループに追加するサーバグループを選択し、[>] をクリックします。

   > → ヒント
   >
   > 複数のサーバグループを選択するには、Ctrl キーを押しながらクリックします。 +
5. [*OK*] をクリックします。

   [サーバ] 管理エリアに戻ります。このタブには、親グループに追加したすべてのサーバグループが表示されます。

11.8.3.2 サーバグループを他のサーバグループのメンバーにする

1. CMC の [サーバ] 管理エリアを表示します。
2. 他のグループに追加するグループをクリックします。

   > ⓘ 注記
   >
   > root レベルの排他的サーバグループの場合、すべての排他的サーバグループが [利用可能なサーバグループ] に一覧表示されます。排他的サーバグループの親サーバグループは 1 つのみであるため、1 つの排他的サーバグループのみを選択して [サーバグループのメンバー] に移動することができます。
   >
   > 子の排他的サーバグループの親は 1 つのみであるため、子レベルの排他的サーバグループの場合は [利用可能なサーバグループ] にサーバグループは表示されません。
3. [アクション] メニューの [サーバグループに追加] を選択します。

4. [利用可能なサーバグループ] リストで、グループに追加する他のグループを選択し、[>] をクリックします。

> → ヒント
>
> 複数のサーバグループを選択するには、Ctrl キーを押しながらクリックします。 +

5. [*OK*] をクリックします。

11.8.4 サーバのグループメンバーシップの変更

サーバのグループメンバーシップを変更することによって、システム上で作成済みのグループまたはサブグループに対し、サーバを簡単に追加(または削除)できます。

たとえば、多くの地域に対してサーバグループが作成されているとします。複数の地域に 1 つの Central Management Server(CMS)を使用することが必要な場合があります。この場合、各地域のサーバグループに CMS を追加する代わりに、サーバの [所属するグループ] リンクをクリックして、そのサーバを複数の地域に一度に追加できます。

11.8.4.1 サーバのグループメンバーシップを変更する

1. CMC の [サーバ] 管理エリアを表示します。
2. メンバーシップ情報を変更するサーバを右クリックして、[既存のサーバグループ] を選択します。
   詳細パネルの [利用可能なサーバグループ] リストに、サーバを追加できるグループが表示されます。[サーバグループのメンバー]リストに、現在そのサーバが所属するサーバグループのリストが表示されます。

   > ⓘ 注記
   >
   > root レベルのサーバグループの場合、すべての排他的サーバグループが [利用可能なサーバグループ] に一覧表示されます。排他的サーバグループの親サーバグループは 1 つのみであるため、1 つの排他的サーバグループのみを選択して [サーバグループのメンバー] に移動することができます。[利用可能なサーバグループ] から排他的サーバグループを選択して [サーバグループのメンバー] に移動した後、排他的サーバグループは root サーバグループからマップ先の新しいサーバグループに移動されます。
   >
   > 子レベルのサーバグループの場合、既存の親サーバグループは [サーバグループのメンバー] に表示され、その他の排他的サーバグループは [利用可能なサーバグループ] に一覧表示されます。子サーバグループのマッピングを 1 つの排他の親サーバグループから別のサーバグループに変更できます。

3. そのサーバが所属するグループを変更するには、この 2 つのリストの間で矢印キーを使用してサーバグループを移動し、[*OK*]をクリックします。

> ⓘ 注記
>
> [サーバグループから削除] オプションは、子レベルの排他的サーバグループにのみ表示されます。子レベルの排他的サーバグループが親サーバグループから削除されると、排他性を保持したままルートレベルに移動されます。
>
> ユーザセキュリティ権限が特定のサーバグループの CMC の管理者によって付与されている場合は、サーバグループが BI ラウンチパッドに表示されます。

11.8.5 サーバおよびサーバグループへのユーザの管理アクセス

ユーザに管理者権限を付与することで、ユーザがサーバおよびサーバグループタスク (サーバの起動と停止など) を実行できるようにします。

システム設定とセキュリティ上の問題に応じて、サーバ管理を BI プラットフォーム管理者のみに許可することができます。また、該当するサーバを使用するそれ以外のユーザに管理アクセスを許可する必要がある場合もあります。 多くの組織には、サーバ管理を専門に行う IT の専門家グループがいます。 サーバチームが、サーバのシャットダウンと起動を伴うサーバメンテナンス作業を定期的に行う場合は、サーバチームにサーバへの管理者権限を付与する必要があります。 また、BI プラットフォームサーバ管理タスクを別のユーザに委任するか、組織内の一部のグループにそれぞれのサーバ管理を任せることもできます。

> ⓘ 注記
>
> (特定のユーザではなく) パブリケーションに対してサーバまたはサーバグループを選択できます。 ただし、特定のサーバまたはサーバグループについては、ユーザまたはユーザグループに管理者権限を割り当てることができます。

11.8.5.1 サーバまたはサーバグループの管理アクセス権の付与

特定のサーバまたはサーバグループについては、ユーザまたはユーザグループに管理者権限を割り当てることができます。

> ⓘ 注記
>
> (ユーザではなく) パブリケーションに対してサーバまたはサーバグループを選択できます。

1. CMC のサーバ管理エリアを表示します。
2. 管理アクセス権を許可するサーバまたはサーバグループを右クリックして、ユーザセキュリティを選択します。
3. 主体の追加をクリックして、サーバまたはサーバグループへの管理アクセス権を付与するユーザまたはグループを追加します。
4. 主体の追加ダイアログボックスで、サーバまたはサーバグループへの管理アクセス権を付与するユーザまたはグループを選択し、> をクリックします。
5. [セキュリティを追加して割り当てる]をクリックします。
6. セキュリティの割り当て画面で、ユーザまたはグループのセキュリティ設定を選択し、*OK* をクリックします。

関連情報

BI プラットフォームでのアクセス権の動作 [121 ページ]

11.8.5.2 Report Application Server のオブジェクト権限

ユーザが Report Application Server(RAS)を使用して Web でレポートを作成または変更できるように設定するには、そのシステムで使用可能な RAS レポート作成ライセンスを所有している必要があります。また、最低限のオブジェクト権限のセットをユーザに付与する必要があります。ユーザにこれらの権限を付与すると、ユーザは新しいレポートのデータソースとしてレポートを選択したり、レポートを直接変更したりできます。

- オブジェクトを表示する(または、必要に応じて“ドキュメントインスタンスを表示する”)
- オブジェクトを編集する
- レポートのデータを最新表示する
- レポートのデータをエクスポートする

ユーザは、新しいレポートを BI プラットフォームに保存するためには、少なくとも 1 つのフォルダにオブジェクトを追加する権限を持っている必要があります。

ユーザがその他のレポート作業(コピー、スケジュール、印刷など)を継続して実行できるようにするには、まず、適切なアクセスレベルを割り当てて、変更を更新することをお勧めします。次に、アクセスレベルを[詳細]に変更し、まだ付与していない必要なアクセス権を追加します。たとえば、ユーザがすでにレポートオブジェクトへのオンデマンド表示権限を持っている場合、アクセスレベルを[詳細]に変更し、オブジェクトを編集する権限を明示的に追加することによって、ユーザにそのレポートを変更する権限を付与します。

アドバンスト DHTML ビューアおよび RAS を通してユーザがレポートを表示する場合、レポートを表示するには[表示]アクセスレベルで十分ですが、高度な検索機能を実際に使用するにはオンデマンド表示権限が必要です。オブジェクトを編集する権限を追加する必要はありません。

11.8.6 サーバグループへのユーザグループのマップ

新しい [デフォルト設定] オプションを使用して、ユーザグループを特定のサーバグループにマップできるようになりました。

サーバグループにユーザグループをマップするには、以下の手順を実行します。

1. CMC にログオンします。
2. [ユーザとグループ] を選択します。
3. [ユーザとグループ] ページで、サーバグループをマップする必要のあるユーザグループを右クリックします。
4. [デフォルト設定] を選択します。
5. [サーバグループのスケジュール] ページで、ユーザグループをスケジュールするために使用するデフォルトのサーバを設定します。

   次のいずれかのオプションを選択できます。

   - (デフォルト) スケジュール時に最も多くのリソースが空いているサーバでオブジェクトを実行する場合は [最初に見つかった利用可能なサーバを使用する] を選択します。
   - 特定のサーバグループのサーバでオブジェクトを実行する場合は、[選択したグループ内のサーバを優先して使用する] を選択します。次に、特定のサーバグループの基本設定を設定するため、ドロップダウンボックスから必須サーバグループを選択します。選択したサーバグループに使用できるサーバがない場合、オブジェクトは共通サーバプールで次に利用可能なサーバで実行されます。
   - 特定のサーバグループ内のサーバでのみオブジェクトを実行する場合は、[選択したグループ内のサーバのみを使用する] を選択し、ドロップダウンボックスから必須サーバグループを選択して 1 つのサーバグ

ループを排他的に使用します。選択したグループのサーバが使用できない場合、オブジェクトは処理されません。また、ジョブサーバが割り当てられたサーバグループにない場合、ジョブは待機中の状態のままになります。

注記

2 つのラジオボタン[選択したグループ内のサーバを優先して使用する] または [選択したグループ内のサーバのみを使用する] のいずれかを選択することで、排他的または非排他的サーバグループをユーザグループにマップするように選択することができます。

同じく、[デフォルト設定] に移動し、[*Crystal Reports* 処理設定] か [*Web Intelligence* 処理設定] に移動することで、Crystal Reports および Web Intelligence ドキュメントを表示または処理するためのサーバグループを割り当てることができます。

サーバグループを必須として関連付けた場合は、その特定のサーバグループのサーバのみが使用されることになります。共通プールのサーバは使用されません。サーバグループを優先として関連付けると、そのサーバグループ内のサーバがビジー状態である場合に、共通サーバプールのサーバが使用されるようになります。共通サーバプールには、排他的サーバグループに属していないすべてのサーバが含まれます。排他的サーバグループの詳細については、排他的サーバグループを作成する [420 ページ]を参照してください。

1 人のユーザが複数のユーザグループに属している可能性があるため、ユーザグループへのサーバグループの割り当ては複雑です。各ユーザグループをさまざまなサーバグループにマップできます。各サーバグループを必須または優先サーバグループとして割り当てることができます。

例

次のシナリオを考えてください。

ユーザ (U) は UG1 と UG2 という 2 つのユーザグループに属しています。各ユーザグループは、SG1 と SG2 という異なるサーバグループにマップされています。さまざまなシナリオの結果は以下のようになります。

シナリオ	結果
ドキュメント (D) をスケジュールします。 サーバグループ 1 (SG1) は UG1 で設定され、サーバグループ 2 (SG2) は UG2 で設定されています。 SG1 は必須 (R) として設定されています。SG2 も必須 (R) として設定されています。 ドキュメント (D) レベルで割り当てられているサーバグループはありません。	2 つのサーバグループ (SG1 と SG2) の組み合わせは、必須 (R) サーバグループとして機能します。 両方のサーバグループ (SG1 と SG2) が必須として設定されているため、共通プールのサーバは使用されません。
ドキュメント (D) をスケジュールします。 サーバグループ 1 (SG1) は UG1 で設定され、サーバグループ 2 (SG2) は UG2 で設定されます。 SG1 は優先 (P) として設定されています。SG2 も優先 (P) として設定されています。 ドキュメント (D) レベルで割り当てられているサーバグループはありません。	2 つのサーバグループ (SG1 と SG2) の組み合わせは、優先 (P) サーバグループとして機能します。 両方のサーバ (SG1 と SG2) が優先として設定されているため、選択したグループ内に使用可能なサーバがない場合は、共通プールのサーバが使用されます。

シナリオ	結果
ドキュメント (D) をスケジュールします。 サーバグループ 1 (SG1) は UG1 で設定され、サーバグループ 2 (SG2) は UG2 で設定されます。 SG1 は必須 (R) として設定されています。SG2 は優先 (P) として設定されています。 ドキュメント (D) レベルで割り当てられているサーバグループはありません。	2 つのサーバグループ (SG1 と SG2) の組み合わせは、必須 (R) サーバグループとして機能します。 この組み合わせ (SG1 と SG2) は必須サーバグループとして機能するため、共通プールのサーバは使用されません。

6. [保存して閉じる] を選択します。

これで、ユーザグループをサーバグループに正常にマップしました。

注記

- ユーザは 1 つまたは複数のユーザグループに属することができ、これらの各ユーザグループは他のユーザグループに属することができます。ユーザが属するユーザグループ自体に関連付けられたサーバグループがない場合は、次のレベルのユーザグループに関連付けられているサーバグループがあるかどうかがチェックされます。サーバグループが割り当てられているユーザグループが見つかるまで、このプロセスが続きます。ユーザグループレベルで関連付けられたサーバグループが見つかった場合は、その時点でチェックが終了します。ユーザグループレベルで関連付けられているサーバグループが複数ある場合は、上記の表で説明したように、2 つのサーバグループの組み合わせの動作が考慮されます。サーバグループ割り当てを理解するため、以下のシナリオについて考えてみます。

  例

  シナリオ: ドキュメント (D) をスケジュールします。

  ユーザ (U) は UG1 と UG2 という 2 つのユーザグループに属しています。しかし、UG1 と UG2 の両方で割り当てられたサーバグループはありません。

  UG1 はユーザグループ 3 (UG3) に属し、UG2 はユーザグループ 4 (UG4) に属しています。

  サーバグループ 3 (SG3) は UG3 で設定されています。

  SG3 は必須 (R) として設定されています。

  結果: 最初のレベル (UG1 と UG2) で設定されたサーバグループがないため、次のレベル (UG3 と UG4) で設定されたサーバグループがあるかどうかがチェックされます。SG3 が UG3 で設定され、SG3 が必須として設定されているため、SG3 内のサーバのみがオブジェクトの処理に使用され、共通プールのサーバは使用できません。

  これは、サーバグループがユーザグループレベルで設定されていない場合には、その次のレベルでサーバグループが設定されていないかがチェックされることを示しています。サーバグループがいずれかのユーザグループレベルで設定されている場合は、次のレベルにサーバグループがあるかどうかはチェックされなくなります。

- ドキュメントレベルでは、割り当て可能なサーバグループは 1 つのみであり、そのグループは必須 (R) または優先 (P) のいずれかにできます。ただし、ユーザは 1 つまたは複数のユーザグループに属することができるため、複数のサーバが 1 人のユーザに割り当てられる可能性があります。サーバグループがドキュメント (D) レベルとユーザグループ (UG) レベルの両方で設定されている場合は、ドキュ

メントレベルでのサーバグループの関連付けがユーザグループレベルでのサーバグループの関連付けよりも常に優先されます。サーバグループ割り当てを理解するため、以下のシナリオについて考えてみます。

> 例
>
> シナリオ: ドキュメント (D) をスケジュールします。
>
> サーバグループ 1 (SG1) は D で設定され、SG1 は必須に設定されています。
>
> サーバグループ 2 (SG2) は UG で設定され、SG2 は優先に設定されています。
>
> 結果: SG1 が使用されます。SG1 は必須に設定されているため、共通プールのサーバは使用できません。
>
> サーバグループ (SG1) がすでにドキュメント (D) レベルで設定されているため、ユーザグループレベルでのサーバグループ割り当ては無視されます。つまり、ドキュメントレベルでのサーバグループ割り当てがユーザグループレベルよりも優先されます。

- すべての必須サーバがサーバグループに含まれていることを確認する必要があります。
- フォルダおよびユーザグループでのサーバグループ割り当てをさらに詳しく理解するには、https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/ を参照してください。

11.8.7 サーバグループへのフォルダのマップ

新しい [デフォルト設定] オプションを使用して、フォルダを特定のサーバグループにマップできるようになりました。

サーバグループにフォルダをマップするには、以下の手順を実行します。

1. CMC にログオンします。
2. [フォルダ] に移動し、(サーバグループをマップする) 目的のフォルダを右クリックします。
3. [デフォルト設定] を選択します。
4. [サーバグループのスケジュール] ページで、フォルダレベルでスケジュールするために使用するデフォルトのサーバを設定します。

   次のいずれかのオプションを選択できます。

   - (デフォルト) スケジュール時に最も多くのリソースが空いているサーバでオブジェクトを実行する場合は [最初に見つかった利用可能なサーバを使用する] を選択します。
   - 特定のサーバグループのサーバでオブジェクトを実行する場合は、[選択したグループ内のサーバを優先して使用する] を選択します。次に、特定のサーバグループの基本設定を設定するため、ドロップダウンボックスから必須サーバグループを選択します。選択したサーバグループに使用できるサーバがない場合、オブジェクトは共通サーバプールで次に利用可能なサーバで実行されます。
   - 特定のサーバグループ内のサーバでのみオブジェクトを実行する場合は、[選択したグループ内のサーバのみを使用する] を選択し、ドロップダウンボックスから必須サーバグループを選択して 1 つのサーバグループを排他的に使用します。選択したグループのサーバが使用できない場合、オブジェクトは処理されません。

> **注記**
>
> 2 つのラジオボタン[選択したグループ内のサーバを優先して使用する] または [選択したグループ内のサーバのみを使用する] のいずれかを選択することで、排他的または非排他的サーバグループをフォルダにマップすることもできます。
>
> 同じく、[デフォルト設定] に移動し、[*Crystal Reports* 処理設定] か [*Web Intelligence* 処理設定] に移動することで、Crystal Reports および Web Intelligence ドキュメントを表示または処理するためのサーバグループを割り当てることができます。
>
> サーバグループを必須として関連付けた場合は、その特定のサーバグループのサーバのみが使用されることになります。共通プールのサーバは使用されません。サーバグループを優先として関連付けると、そのサーバグループ内のサーバがビジー状態である場合に、共通サーバプールのサーバが使用されるようになります。共通サーバプールには、排他的サーバグループに属していないすべてのサーバが含まれます。排他的サーバグループの詳細については、排他的サーバグループを作成する [420 ページ]を参照してください。

5. [保存して閉じる] を選択します。

これで、フォルダをサーバグループに正常にマップしました。

> **注記**
>
> - フォルダレベルまたはドキュメントレベルでは、割り当て可能な 1 つのサーバグループのみが存在でき、そのグループは必須 (R) または優先 (P) のいずれかにできます。サーバグループをフォルダ (F)、ドキュメント (D)、ユーザグループ (UG) の各レベルで設定した場合は、ドキュメントレベルでのサーバグループ関連付けが常にフォルダレベルでのサーバグループ関連付けよりも優先され、その後にユーザグループレベルでのサーバグループ関連付けが続きます。このため、サーバグループ割り当ての優先順位は以下のようになります。
> ドキュメント > フォルダ > ユーザグループ
> - ドキュメントはフォルダに所属でき、フォルダは別の親フォルダに所属できます。ドキュメントレベルで割り当てられたサーバグループがない場合に、ドキュメントの直属のフォルダにサーバグループが関連付けられていないときは、次の直属の親フォルダにサーバグループが関連付けられているかどうかがチェックされます。サーバグループが割り当てられている親フォルダが見つかるまで、このプロセスが続きます。フォルダレベルでサーバグループ関連付けが見つかった場合は、さらなるチェックが行われます。サーバグループ割り当てを理解するため、以下のシナリオについて考えてみます。
>
> > **例**
> >
> > シナリオ: ドキュメント (D) をスケジュールします。
> >
> > しかし、ドキュメントレベルで割り当てられたサーバグループがありません。
> >
> > ドキュメント (D) は、フォルダ (F) に属します。しかし、F で割り当てられたサーバグループがありません。
> >
> > フォルダ (F) は別のフォルダに属しています。親フォルダ (PF) です。サーバグループ (SG) は PF で設定されています。
> >
> > SG は必須 (R) として設定されています。
> >
> > 結果: ドキュメント (D) で設定されたサーバグループがないため、フォルダレベル (F) で設定されたサーバグループがないかチェックされます。F で設定されたサーバグループもないため、次のレベル、つまり親フォルダ (PF) で設定されたサーバグループがないかチェックされます。SG が PF で設定され、かつ SG が必須として設定されているため、SG 内のサーバのみがオブジェクトの処理に使用され、共通プールのサーバは使用できません。

これは、サーバグループがドキュメントレベルで設定されていない場合には、その直属のフォルダを調べて、サーバグループが設定されていないかチェックされることを示しています。サーバグループがいずれかのフォルダレベルで設定されている場合は、次のレベルにサーバグループがないかチェックされます。

同じく、ドキュメントレベルで設定されたサーバグループがなく、フォルダレベルでも設定されたサーバグループがない場合には、ユーザグループレベルでサーバグループが割り当てられているとみなされます。

- すべての必須サーバがサーバグループに含まれていることを確認する必要があります。
- フォルダおよびユーザグループでのサーバグループ割り当てをさらに詳しく理解するには、https://blogs.sap.com/2016/11/07/servergroup-enhancements-for-scheduling-in-4.2sp03/を参照してください。

11.8.8 サーバグループのアクセス権の管理の理解

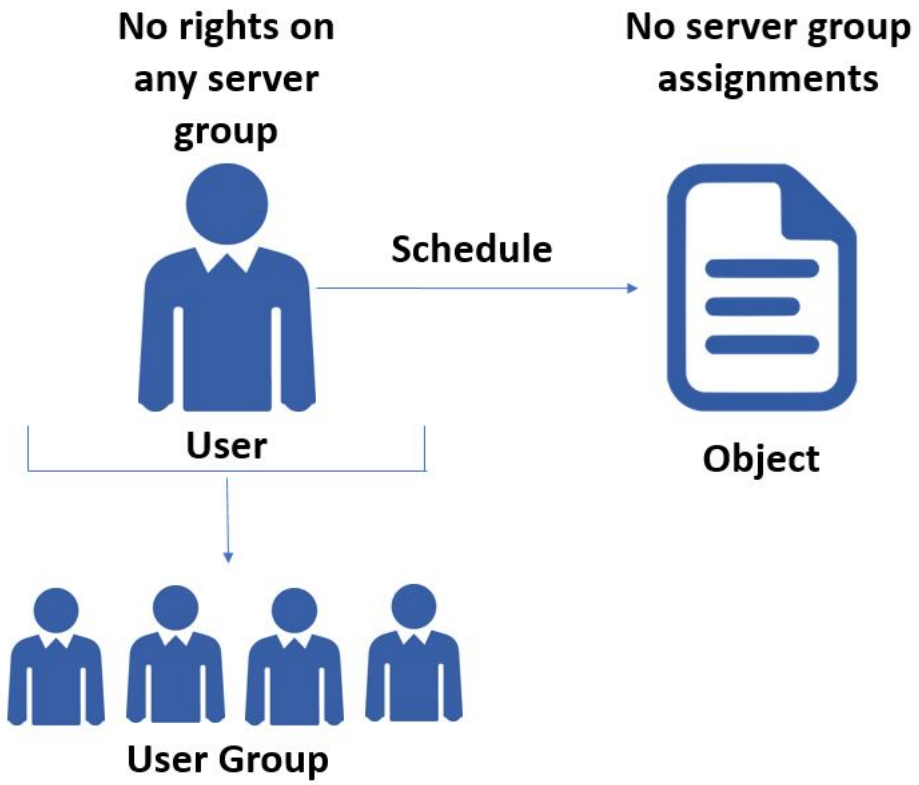
サーバグループのアクセス権をユーザレベルまたはユーザグループレベルで有効にすることができます。つまり、ユーザごとまたはユーザグループごとにサーバグループへのアクセスを制御することができます。

注記

- 以下に示すシナリオでは、サーバグループのアクセス権の管理を説明するためのプロセスとしてスケジュールを使用しています。同様に、表示およびキャッシュに関するサーバグループの権限の管理について理解することができます。
- サーバグループまたはサーバグループの組み合わせでサーバが使用可能になっている場合、オブジェクトを正常にスケジュールすることができます。使用可能なサーバがない場合、スケジュールは失敗します。

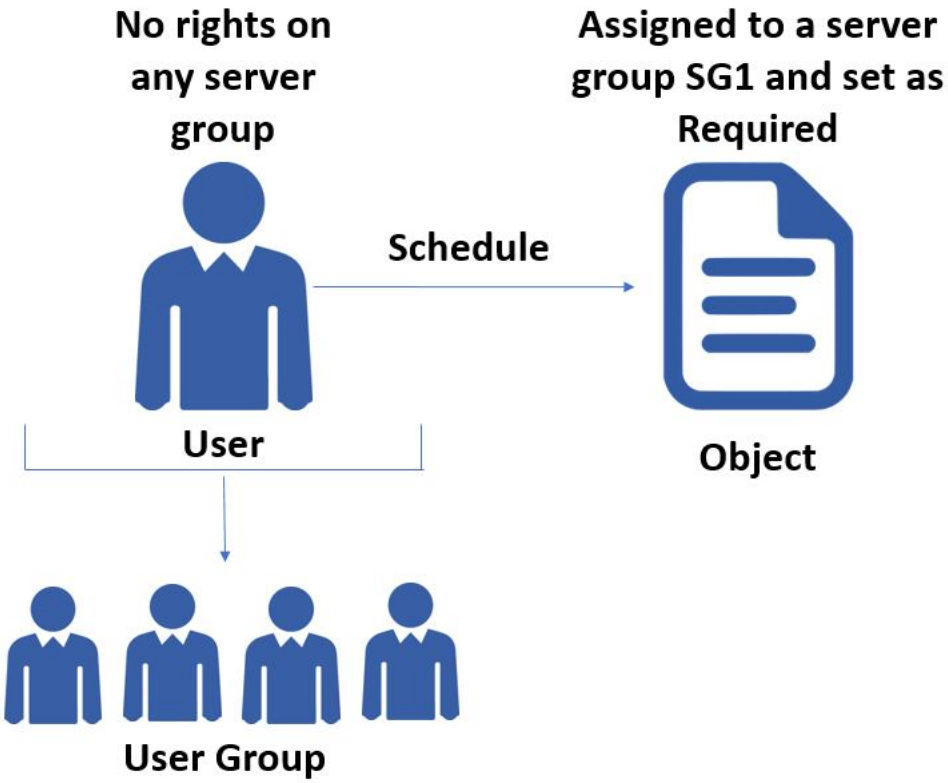
シナリオ 1:

ユーザが Business Intelligence プラットフォームのユーザグループのメンバーあるという理想的なシナリオについて考えてみます。ユーザおよびそれに関連するユーザグループには、いずれのサーバグループの権限もありません。ユーザはいずれのサーバグループにも割り当てられていないオブジェクトをスケジュールすることを考えています。



シナリオ 2:

上記のシナリオを、オブジェクトにサーバグループを割り当てることで変更すると、オブジェクトのスケジュールは失敗します。



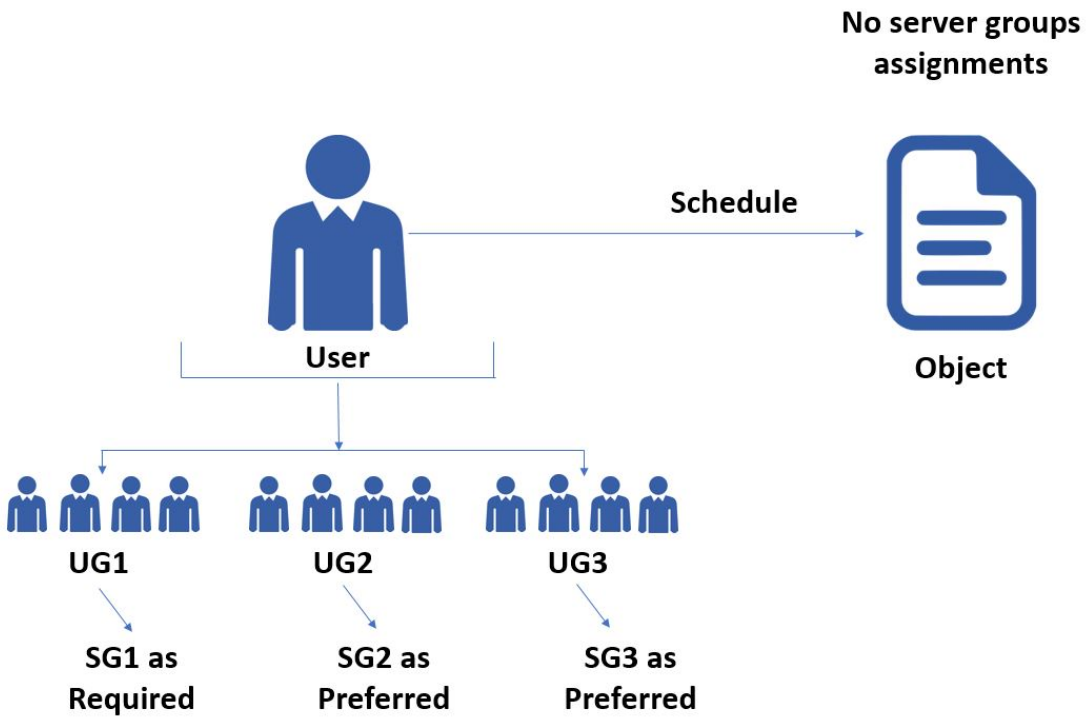
ユーザがオブジェクトをスケジュールすると、オブジェクトに対するサーバグループの割り当てがプラットフォームによってチェックされます。サーバグループがオブジェクトに割り当てられている場合、ユーザにそのサーバグループに対する表示権限があるかどうかがプラットフォームによってチェックされます。

2 つ目のシナリオの場合、ユーザもそのユーザが関連するユーザグループも SG1 に対する権限を持っていません。そのため、スケジューリングジョブは失敗します。このシナリオでユーザが正常にオブジェクトをスケジュールできるようにするには、ユーザまたは関連するユーザグループが SG1 に対する表示権限を持っていることを確実にします。

シナリオ **3:**

> ⓘ 注記
>
> シナリオ 3 および 4 では、ユーザがその関連するユーザグループから権限を継承することを前提としています。

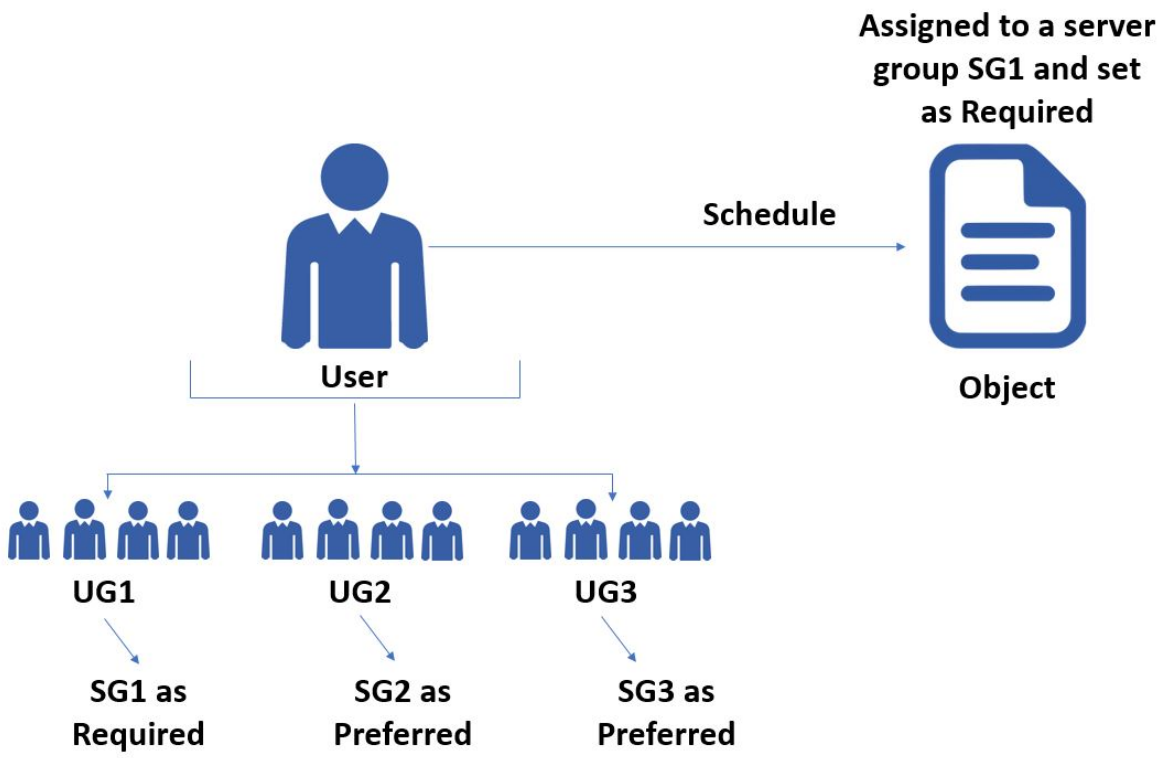
ユーザは UG1、UG2、および UG3 の 3 つのユーザグループのメンバーであり、各ユーザグループは SG1、SG2、および SG3 のサーバグループにそれぞれ割り当て済みです。SG1 は必須サーバグループとして設定されていますが、SG2 および SG3 は優先サーバグループとして設定されています。サーバグループを必須または優先として設定する方法の詳細については、*Business Intelligence* プラットフォーム管理者ガイドのサーバグループへのユーザグループのマッピングを参照してください。



ユーザが複数のユーザグループに関連付けられ、個々のユーザグループがそれぞれ異なるサーバグループにマップされている場合、プラットフォームによって使用可能なサーバグループが計算されます。上記のシナリオの場合、オブジェクトにはサーバグループが割り当てられておらず、オブジェクトのスケジュールに使用可能なサーバグループが SG1、SG2、および SG3 の組み合わせであるため、スケジューリングジョブは成功します。

シナリオ **4**:

シナリオ 3 に加えて、オブジェクトを SG1 に割り当て、SG1 を必須として設定してあります。サーバグループを必須または優先として設定する方法の詳細については、*Business Intelligence* プラットフォーム管理者ガイドのサーバグループへのユーザグループのマッピングを参照してください。



サーバグループがオブジェクトに割り当てられている場合、ユーザにそのサーバグループに対する表示権限が付与されているかどうかがプラットフォームによってチェックされます。このシナリオでは、使用可能なサーバグループはプラットフォームによって計算されません。これは、オブジェクトレベルのサーバグループ割り当てが最も優先順位が高いためです。シナリオ 4 の場合、UG1 に SG1 に対する表示権限があり、ユーザはこれらの権限を UG1 から継承するため、オブジェクトは正常にスケジュールされます。

→ 注意

- オブジェクトをスケジュールする前に、ユーザに関連付けられたすべてのユーザグループに対するサーバグループ割り当てを確認し、使用可能なサーバグループを計算します。
- オブジェクトに割り当てられたサーバグループが、ユーザが使用可能なサーバグループに含まれている場合、スケジューリングジョブは成功します。

以下の表を参照してください。

ⓘ 注記

SG1 および SG2 がユーザグループ UG1 および UG2 にそれぞれ割り当てられているとします。

アクセスレベル	サーバグループの組み合わせ **(SG1 + SG2)**	共通プールのサーバの検索
ユーザはすべてのサーバグループに対して権限を持っています	必須 + 必須	False

アクセスレベル	サーバグループの組み合わせ (SG1 + SG2)	共通プールのサーバの検索
ユーザはすべてのサーバグループに対して権限を持っています	必須 + 優先	False
ユーザはすべてのサーバグループに対して権限を持っています	優先 + 優先	True
ユーザはどのサーバグループに対しても権限を持っていません	必須 + 必須	False
ユーザはどのサーバグループに対しても権限を持っていません	必須 + 優先	False
ユーザはどのサーバグループに対しても権限を持っていません	優先 + 優先	True
ユーザはいくつかのサーバグループに対して権限を持っています	必須 (いいえ) + 必須 (はい)	False
ユーザはいくつかのサーバグループに対して権限を持っています	必須 (いいえ) + 優先 (はい)	False
ユーザはいくつかのサーバグループに対して権限を持っています	必須 (はい) + 優先 (いいえ)	False
ユーザはいくつかのサーバグループに対して権限を持っています	優先 (いいえ) + 優先 (はい)	True

11.9 本稼働システムの Adaptive Processing Server の設定

ホストシステムごとに 1 つの Automated Process Server (APS) がインストールプログラムによりインストールされます。インストールした機能に応じて、この APS はモニタリングサービス、プロモーションマネジメントサービス、多次元分析サービス (MDAS)、公開サービスなど、多くのサービスを提供することができます。

本稼働システムまたはテストシステムでは、追加の APS を作成し、ビジネス要件に合わせて APS を設定するのが最適です。

追加の APS の作成方法には、以下の 2 種類があります。

- システム設定ウィザードを実行する。
  ウィザードは、事前に定義されたデプロイメントテンプレートに従った APS の設定を含む、ユーザの BI プラットフォームシステムの基本設定に役立ちます。ウィザードを使用すると、適切に APS 設定を開始できます。ただし、この場合でもシステムのサイズ設定を実行する必要があります。
- CMC を使用して、追加 APS の作成と設定を手動で実行する。

本稼働システムの Adaptive Processing Server の設定の詳細については、次の場所にある KBA 記事を参照してください。1694041

→ 注意

ウィザードでのデプロイメントテンプレートの選択、または手動での追加 APS の作成で、システムのサイズ設定が置き換わることはありません。http://www.sap.com/bisizing を参照して、サイズ設定が実行されていることを確認してください。

11.10 システムのパフォーマンスの評価

11.10.1 BI プラットフォームの監視

モニタリングアプリケーションは、レポーティングおよび通知について、BI プラットフォームサーバのランタイムメトリクスおよび履歴メトリクスを取得するための機能を提供します。システム管理者は、アプリケーションを使用してサーバが正常に機能しているかどうか、および応答時間が予測どおりかどうかを特定することができます。

関連情報

モニタリング [771 ページ]

11.10.2 サーバメトリクスの分析

セントラル管理コンソール (CMC) では、ユーザのシステム内にあるサーバのメトリクスを表示できます。このメトリクスには、各マシンに関する一般情報と、各タイプのサーバに固有の詳細情報が含まれます。また CMC では、製品バージョン、CMS、現在のシステム利用状況に関する情報などのシステムメトリクスも表示できます。

ⓘ 注記

現在実行中のサーバのメトリクスのみを表示することができます。

11.10.2.1 サーバメトリクスを表示する

1. CMC の[サーバ]管理エリアを表示します。
2. メトリクスを表示するサーバを右クリックし、[メトリクス] を選択します。

[メトリクス] タブに、サーバのメトリクスの一覧が表示されます。

関連情報

サーバのプロパティを変更する [439 ページ]
サーバのメトリクスに関する付録について [1142 ページ]

11.10.3 システムメトリクスの表示

CMC の [設定] 管理エリアには、BI プラットフォームインストール環境についての一般情報を示すシステムメトリクスが表示されます。[プロパティ] セクションには、製品のバージョンとビルドについての情報が含まれます。CMS データベースのデータソース、データベース名、およびデータベースユーザ名も一覧表示されます。[グローバルシステムメトリクスの表示] セクションには、現在のアカウントの利用状況と、現在および処理済みのジョブに関する統計が表示されます。[クラスタ] セクションには、接続している CMS の名前、CMS クラスタの名前、および他のクラスタメンバーの名前が表示されます。

11.10.3.1 システムメトリクスを表示する

1. CMC の[設定]管理エリアを表示します。
2. 矢印をクリックし、[プロパティ]、[グローバルシステムメトリクスの表示]、[クラスタ]、または [ホットバックアップ] 領域を展開して設定を表示します。

11.10.4 サーバの利用状況の記録

BI プラットフォームでは、BI プラットフォームの Web 利用状況に関する特定の情報を記録できます。

- さらに、各 BI プラットフォームサーバは、オペレーティングシステムの標準システムログにメッセージを記録するよう設計されています。
  - Windows では、BI プラットフォームはイベントログサービスに記録します。(アプリケーションログの) イベントビューアを使用して結果を表示できます。
  - UNIX では、BI プラットフォームは syslog デーモンにユーザアプリケーションとして記録します。各サーバは、サーバの名前と PID を記録するメッセージの先頭に挿入します。

各サーバは、製品インストール環境のログディレクトリにアサートメッセージも記録します。これらのファイルに記録されるプログラム情報は通常、SAP BusinessObjects のサポート担当者が高度なデバッグを行う際にのみ役立ちます。これらのログファイルの場所は、使用しているオペレーティングシステムによって異なります。

- Windows では、デフォルトのロギングディレクトリは `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥logging` です。
- UNIX では、デフォルトのロギングディレクトリは `<INSTALLDIR>/sap_bobj/logging` ディレクトリです。

これらのログファイルは自動的にクリーンアップされるため、サーバごとに記録されたデータが 1MB を超えることはありません。

> ⓘ 注記
>
> BI プラットフォームサーバをホストしている UNIX マシンでロギングが機能するようにするには、“info” レベル以上の “user” ファシリティにログが記録されたすべてのメッセージが記録されるようにシステムのロギングを設定する必要があります。リモートロギングを許可するには、SYSLOGD を設定する必要もあります。
>
> セットアップ手順は、システムに応じて異なります。手順については、使用しているオペレーティングシステムのマニュアルを参照してください。

11.11 サーバの設定

この節では、BI プラットフォームサーバの設定変更に関する技術情報と手順を示します。

ここで説明する設定により、BI プラットフォームを現在のハードウェア、ソフトウェア、およびネットワーク構成と効果的に統合できます。最終的にどの設定を選択するかは、各ユーザ必要要件により大きく異なります。

サーバ設定は、セントラル管理コンソール (CMC) を使用して 2 種類の方法で変更できます。

- サーバの [プロパティ] 画面を使用する。
- [共通サービスの編集] 画面を使用する。

すぐに実行されない変更もあるという点に注意する必要することが重要です。設定をすぐに変更できない場合、[プロパティ] および [共通サービスの編集] 画面には現在の設定 (赤のテキスト) および目的の設定の両方が表示されます。[サーバ] 管理エリアに戻ると、サーバには "古い" とマークが付けられます。サーバを再起動すると、サーバは目的の設定を使用し、"古い" フラグはサーバから削除されます。

> ⓘ 注記
>
> この節では、BI プラットフォームアプリケーションを導入するための Web アプリケーションサーバの設定方法については説明しません。このタスクは通常、この製品をインストールするときに実行されます。詳細については、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドを参照してください。

関連情報

ポート番号の設定 [448 ページ]
サーバのプロパティを変更する [439 ページ]
CMS システムデータベースの再作成 [486 ページ]
新規または既存の CMS データベースの選択 [484 ページ]

11.11.1 サーバのプロパティを変更する

1. CMC の [サーバ] 管理エリアを表示します。

2. 設定を変更するサーバをダブルクリックします。
   [プロパティ] 画面が表示されます。
3. 必要な変更を行い、[保存] または [保存して閉じる] をクリックします。

> ⓘ 注記
>
> すぐに実行されない変更もあります。設定をすぐに変更できない場合、[プロパティ]ダイアログボックスには現在の設定(赤のテキスト)および目的の設定の両方が表示されます。[サーバ] 管理エリアに戻ると、サーバには "要再起動" とマークが付けられます。サーバを再起動すると、サーバは [プロパティ] ダイアログボックスの目的の設定を使用し、"要再起動" フラグはサーバから削除されます。

11.11.2 複数のサーバにｻｰ ビス設定を適用する

複数のサーバ上でホストされるサービスに同じ設定を適用できます。

1. CMC の[サーバ]管理エリアを表示します。
2. `Ctrl` キーを押しながら、設定を変更するサービスをホストする各サーバをクリックし、次に右クリックして [共通サービスの編集] を選択します。
   [共通サービスの編集] ダイアログが表示され、選択したサーバ上でホストされた、設定を変更できるサービスの一覧が表示されます。
3. [共通サービスの編集] ダイアログボックスに複数のサービスが一覧表示される場合は、編集するサービスを選択し、[続行] をクリックします。
4. 必要な変更を行い、[*OK*] をクリックします。

> ⓘ 注記
>
> CMC の [サーバ] 管理エリアへリダイレクトします。サーバを再起動する必要がある場合は、"古い" とマーク付けされます。サーバを再起動すると、サーバは新しい設定を使用し、"古い" フラグは削除されます。

11.11.3 設定テンプレートの使用

設定テンプレートを使用すると、サーバの複数のインスタンスを簡単に設定できます。設定テンプレートには、各サービスタイプの設定の一覧が格納されます。この一覧を使用して追加のサーバインスタンスを設定できます。たとえば、同じ設定にする Web Intelligence Processing Server が 12 個ある場合は、それらの 1 つを設定するだけで済みます。その後、設定したサービスを使用して Web Intelligence Processing Server 用の設定テンプレートを定義し、そのテンプレートを他の 11 個のサービスインスタンスに適用できます。

BI プラットフォームサービスの各タイプには、それぞれ独自の設定テンプレートがあります。たとえば、Web Intelligence Processing サービスタイプ用の設定テンプレートや公開サービスタイプ用の設定テンプレートなどがあります。設定テンプレートは、セントラル管理コンソール(CMC)のサーバのプロパティで定義されます。

サーバで設定テンプレートを使用するようにすると、サーバの既存の設定はテンプレートの値で上書きされます。後からテンプレートの使用を停止しても、元の設定は復元されません。また、停止後に設定テンプレートに加えられた設定はサーバに影響しません。

設定テンプレートは次のように使用することをお勧めします。

1. 1 つのサーバに設定テンプレートを設定します。
2. 同じタイプのすべてのサーバに同じ設定を使用する場合は、設定テンプレートを設定したサーバを含め、同じタイプのすべてのサーバで [設定テンプレートの使用] を有効にします。
3. 後からこのタイプのすべてのサービスの設定を変更する場合は、いずれかのサービスのプロパティを表示し、[設定テンプレートの使用] チェックボックスをオフにします。必要な設定を変更し、[設定テンプレートの設定] を選択して [保存] をクリックします。そのタイプのすべてのサービスが更新されます。設定テンプレートとして常に設定されるサーバがない場合は、そのタイプのすべてのサーバの設定を誤って変更しないようにしてください。

関連情報

設定テンプレートを設定する [441 ページ]
設定テンプレートをサーバに適用する [442 ページ]

11.11.3.1 設定テンプレートを設定する

サービスのタイプごとに 1 つの設定テンプレートを設定できます。サービスに複数の設定テンプレートを設定することはできません。サーバの [プロパティ] ページを使用して、サーバでホストされるサービスタイプの設定テンプレートで使用される設定を指定できます。

1. CMC の [サーバ] 管理エリアを表示します。
2. 設定テンプレートを設定するサービスをホストしているサーバをダブルクリックします。
   [プロパティ] 画面が表示されます。
3. テンプレートで使用するサービス設定を設定し、[設定テンプレートの設定] チェックボックスをオンにし、[保存] または [保存して閉じる] をクリックします。

選択したサービスタイプの設定テンプレートは、現在のサーバの設定に従って定義されます。同じサービスをホストしている同じタイプの他のサーバは、そのプロパティで[設定テンプレートの使用]オプションを有効にしている場合、設定テンプレートに合わせて自動的にすぐに再設定されます。

> ⓘ 注記
> 設定テンプレートの設定を明示的に定義していない場合は、サービスのデフォルト設定が使用されます。

関連情報

設定テンプレートをサーバに適用する [442 ページ]

11.11.3.2 設定テンプレートをサーバに適用する

設定テンプレートを適用する前に、テンプレートを適用するサーバのタイプに対して設定テンプレートの設定を定義しているか確認してください。設定テンプレートの設定を明示的に定義していない場合は、サービスのデフォルト設定が使用されます。

> ⓘ 注記
>
> [設定テンプレートの使用] 設定を有効にしていないサーバは、設定テンプレートの設定を変更しても更新されません。

1. CMC の [サーバ] 管理エリアを表示します。
2. 設定テンプレートを適用するサービスをホストしているサーバをダブルクリックします。
   [プロパティ] 画面が表示されます。
3. [設定テンプレートの使用] チェックボックスをオンにし、[保存] または [保存して閉じる] をクリックします。

   > ⓘ 注記
   >
   > 新しい設定を有効にするためにサーバを再起動する必要がある場合は、サーバリストに "要再起動" とマーク付きで表示されます。

適切な設定テンプレートが現在のサーバに適用されます。適用後に設定テンプレートに変更を加えると、設定テンプレートを使用するすべてのサーバの設定が変更されます。

[設定テンプレートの使用]をオフにしても、サーバ設定は、設定テンプレートが適用された時点の値に復元されません。使用停止後に設定テンプレートに加えられた変更は、設定テンプレートを使用しているサーバの設定に影響しません。

関連情報

設定テンプレートを設定する [441 ページ]

11.11.3.3 システムデフォルトを復元する

サーバを誤って設定した場合やパフォーマンスに問題がある場合など、サーバの設定を最初にインストールした設定に戻す必要がある場合があります。

1. CMC の [サーバ] 管理エリアを表示します。
2. システムデフォルトを復元するサービスをホストしているサーバをダブルクリックします。
   [プロパティ] 画面が表示されます。
3. [システムデフォルトの復元] チェックボックスをオンにし、[保存] または [保存して閉じる] をクリックします。
   特定のサービスタイプのデフォルト設定が復元されます。

11.12 サーバネットワークの設定

BI プラットフォームサーバのネットワーク設定は、CMC で管理します。これらの設定は、ポート設定とホスト ID の 2 つのカテゴリに分かれています。

デフォルト設定

インストール時に、サーバのホスト識別子は[自動割り当て]に設定されます。ただし、各サーバに特定の IP アドレスまたはホスト名を割り当てることもできます。CMS のデフォルトのポート番号は 6400 です。他の BI プラットフォームサーバは、動的に使用可能なポートにバインドします。ポート番号は BI プラットフォームで自動的に管理されますが、CMC を使用してポート番号を指定することもできます。

11.12.1 ネットワーク環境オプション

BI プラットフォームでは、インターネットプロトコルバージョン 4 (IPv4)、および IPv4/IPv6 共存ネットワークトラフィックがサポートされます。サーバおよびクライアントコンポーネントは、次のどの環境でも使用できます。

- IPv4 ネットワーク: すべてのサーバおよびクライアントコンポーネントは IPv4 プロトコルでのみ実行されます。
- IPv6 と IPv4 が混在するネットワーク: サーバおよびクライアントコンポーネントは IPv6 プロトコルと IPv4 プロトコルの両方で実行できます。
  例
  - IPv6 のみ (Ipv6 スタックは有効、IPv4 スタックはインストールされているが無効)
  - IPv6/IPv4 共存 (Ipv6 スタックと IPv4 スタックの両方が有効)
  - IPv4 のみ (Ipv4 スタックは有効、IPv6 は無効になっているか、またはアンインストールされている) のホスト

> ⓘ 注記
>
> - ネットワーク設定は、システム管理者とネットワーク管理者が行う必要があります。BI プラットフォームには、ネットワーク環境を指定するメカニズムはありません。CMC を使用して、BI プラットフォームサーバの特定の IPv6 アドレスまたは IPv4 アドレスにバインドすることができます。
> - ピュア Ipv6 スタック (IPV6 のみがインストールされていて有効) はサポートされていません。ただし、共存 Ipv6 ネットワークはサポートされています。

11.12.1.1 IPv6 と IPv4 の混在環境

IPv6 と IPv4 が混在するネットワーク環境では、次の処理が可能です。

- BI プラットフォームサーバは、IPv6/IPv4 の混在モードで実行中の場合、IPv6 と IPv4 のどちらの要求も処理できます。
- クライアントコンポーネントは、IPv4 専用ノード、または IPv6/IPv4 ノードとしてサーバと相互運用できます。

混在モードは、特に次のシナリオで役立ちます。

- IPv4 専用ノードから Ipv6 混在ノードの環境に移行する場合。すべてのクライアントおよびサーバコンポーネントは、移行が完了するまでシームレスに相互運用を続けます。その後、すべてのサーバの IPv4 設定を無効にすることができます。
- IPv6 に対応していないサードパーティソフトウェアを IPv6/IPv4 ノードの環境で引き続き動作させる場合。

11.12.2 サーバホスト ID オプション

ホスト ID オプションは、すべての BI プラットフォームサーバに対して CMC で指定することができます。次の表は、[共通設定] 領域で使用できるオプションをまとめたものです。

オプション	説明
自動割り当て	これはすべてのサーバのデフォルト設定です。このチェックボックスをオンにすると、サーバのリクエストポートがマシン上の最初のネットワークインタフェースに自動的にバインドされます。 **注記** [ホスト名] の [自動割り当て] チェックボックスをオンにすることをお勧めします。ただし、サーバがマルチホームマシンで実行されている場合、またはサーバを特定のファイアウォール設定で運用する必要がある場合などは、特定のホスト名または IP アドレスを使用することを検討する必要があります。*SAP BusinessObjects Business Intelligence* プラットフォーム管理者ガイドにあるマルチホームマシンの設定およびファイアウォールの使用に関する情報を参照してください。
ホスト名	サーバがリクエストを受信待機するネットワークインタフェースのホスト名を指定します。CMS では、この設定により、CMS でネームサーバポートおよびリクエストポートをバインドするネットワークインタフェースのホスト名を指定します。
IP アドレス	サーバがリクエストを受信待機するネットワークインタフェースの IP アドレスを指定します。CMS では、CMS でネームサーバポートをリクエストポートにバインドするのに使用するネットワークインタフェースのアドレスを指定します。すべてのサーバについて、IPv4 アドレスと IPv6 アドレスを指定するための個別のフィールドが用意されています。

> ⚠ 警告
>
> マルチホームマシンで [自動割り当て] チェックボックスをオンにしている場合、CMS では正しくないネットワークインタフェースに自動的にバインドされる場合があります。これを回避するには、(マシンのオペレーティングシステムツールを使用して) ホストマシンのネットワークインタフェースが一覧に正しい順序で指定されていることを確認してください。CMC で CMS のホスト名を指定する必要があります。

> ⓘ 注記
>
> マルチホームマシンまたは一部の NAT ファイアウォール設定を使用している場合は、ホスト名ではなく完全修飾ドメイン名を使用してホスト名を指定する必要がある場合があります。

関連情報

ファイアウォール用にシステムを設定する [197 ページ]
マルチホームマシンの設定 [446 ページ]
複数のネットワークインタフェースをトラブルシューティングする [447 ページ]

11.12.2.1 サーバのホスト ID を変更する

1. CMC の[サーバ]管理エリアを表示します。
2. サーバを選択し、[アクション]メニューの[サーバの停止]を選択します。
3. [管理]メニューの[プロパティ]を選択します。
4. [共通設定]で、次のオプションのいずれかを選択します。

オプション	説明
自動割り当て	サーバは、使用可能なネットワークインタフェースのいずれかにバインドされます。
ホスト名	サーバがリクエストを受信待機するネットワークインタフェースのホスト名を入力します。
IP アドレス	サーバがリクエストを受信待機するネットワークインタフェースの IPv4 IP アドレスまたは IPv6 IP アドレスを、対応するフィールドに入力します。 ⓘ 注記 サーバを IPv4 と IPv6 のデュアルモードのノードとして動作させるには、両方のフィールドに有効な IP アドレスを入力します。

5. [保存]または[保存して閉じる]をクリックします。
   変更が、[プロパティ]タブに表示されるコマンドラインに反映されます。
6. サーバを開始して有効にします。

11.12.3 マルチホームマシンの設定

マルチホームマシンは、複数のネットワークアドレスを持つマシンです。それぞれに 1 つ以上の IP アドレスがある複数のネットワークインタフェース、または複数の IP アドレスが割り当てられた 1 つのネットワークインタフェースを使用して、マルチホームマシンは実現されます。

複数のネットワークインタフェースを使用しており、各インタフェースに単一の IP アドレスが割り当てられている場合、バインド順を変更して、先頭のインタフェースが BI プラットフォームサーバにバインドされるようにします。使用しているインタフェースに複数の IP アドレスが割り当てられている場合は、CMC の [ホスト識別子] オプションを使用して、BI プラットフォームサーバのネットワークインタフェースカードを指定します。ホスト名または IP アドレスで指定できます。[ホスト識別子] 設定の詳細については、「“複数のネットワークインタフェースをトラブルシューティングする”」を参照してください。

> → ヒント
>
> この節では、すべてのサーバを同じネットワークアドレスに限定する方法を示しますが、各サーバを異なるアドレスにバインドすることもできます。たとえば、ユーザのマシンからルーティングできない専用のアドレスに File Repository Server をバインドする場合もあります。このような高度な設定では、すべての BI プラットフォームサーバコンポーネント間の通信を、DNS 設定で効率的にルーティングする必要があります。この例では、DNS は他の BI プラットフォームサーバから、File Repository Server の専用アドレスにルーティングする必要があります。

関連情報

複数のネットワークインタフェースをトラブルシューティングする [447 ページ]

11.12.3.1 ネットワークアドレスにバインドするように CMS を設定する

> ⓘ 注記
>
> マルチホームマシンでは、[ホスト識別子]に、完全修飾ドメイン名、またはサーバがバインドするインタフェースの IP アドレスを設定できます。

1. CMC の[サーバ]管理エリアを表示します。
2. CMS をダブルクリックします。
3. [共通設定]で、次のオプションのいずれかを選択します。
   - ホスト名
   - サーバがバインドするネットワークインタフェースのホスト名を入力します。
   - *IP* アドレス
   - サーバがバインドするネットワークインタフェースの IPv4 IP アドレスまたは IPv6 IP アドレスを対応するフィールドに入力します。

> ⓘ 注記
>
> サーバを IPv4 と IPv6 のデュアルモードのノードとして動作させるには、両方のフィールドに有効な IP アドレスを入力します。

> ⚠ 警告
>
> [自動割り当て]は選択しないでください。

4. [リクエストポート]では、次のいずれかを実行できます。
   - [自動割り当て]オプションを選択します。
   - [リクエストポート]フィールドに有効なポート番号を入力します。
5. [ネームサーバポート]ダイアログボックスでポート番号が指定されているか確認してください。

> ⓘ 注記
>
> デフォルトのポート番号は 6400 です。

11.12.3.2 特定のネットワークアドレスにバインドするための残りのサーバの設定

残りの BI プラットフォームサーバは、デフォルトで動的にそれぞれのポートを選択します。この情報を動的に伝播する [自動割り当て] 設定を無効にする方法については、「“リクエストを受け入れるためにサーバが使用するポートを変更する”」を参照してください。

関連情報

リクエストを受け入れるためにサーバが使用するポートを変更する [451 ページ]

11.12.3.3 複数のネットワークインタフェースをトラブルシューティングする

マルチホームマシンでは、CMS で正しくないネットワークインタフェースに自動的にバインドされる場合があります。このような事態が発生しないようにするには、(マシンの OS ツールを使用して)ホストマシンのネットワークインタフェースが一覧に正しい順序で指定され、CMC で CMS に対して[ホスト名]設定が指定されていることを確認してください。プライマリネットワークインタフェースがルーティングできない場合は、次の手順を使用して、非プライマリのルーティング可能なネットワークインタフェースにバインドするよう BI プラットフォームを設定できます。これらの手順は、ローカルマシンに BI プラットフォームをインストールした直後、および他のマシンに BI プラットフォームをインストールする前に実行します。

1. CCM を開いて、複数のネットワークインタフェースがあるマシンのノードの SIA を停止します。

2. SIA を右クリックし、[プロパティ]を選択します。
3. [プロパティ]ダイアログボックスで[設定]タブをクリックします。
4. SIA を特定のネットワークインタフェースにバインドするには、[ポート] フィールドにターゲットのネットワークインタフェースのポート番号を入力します。
5. [*OK*]をクリックし、[スタートアップ]タブを選択します。
6. [ローカル *CMS* サーバ]一覧から CMS を選択し、[プロパティ]をクリックします。
7. CMS を特定のネットワークインタフェースにバインドするには、[ポート] フィールドにターゲットのネットワークインタフェースのポート番号を入力します。
8. [*OK*]をクリックして、新しい設定を適用します。
9. SIA を起動し、サーバが起動するまで待機します。
10. セントラル管理コンソール(CMC)を起動し、[サーバ]管理エリアを表示します。サーバごとに手順 11 ～ 14 を繰り返します。
11. サーバを選択し、[アクション]メニューの[サーバの停止]を選択します。
12. [管理]メニューの[プロパティ]を選択します。
13. [共通設定]で、次のオプションのいずれかを選択します。
    - ホスト名: サーバがバインドするネットワークインタフェースのホスト名を入力します。
    - IP アドレス: サーバがバインドするネットワークインタフェースの IPv4 IP アドレスまたは IPv6 IP アドレスを対応するフィールドに入力します。

      > ⓘ 注記
      >
      > サーバを IPv4 と IPv6 のデュアルモードのノードとして動作させるには、両方のフィールドに有効な IP アドレスを入力します。

    > ⚠ 警告
    >
    > [自動割り当て]は選択しないでください。

14. [保存]または[保存して閉じる]をクリックします。
15. CCM に戻り、SIA を再起動します。

    SIA は、ノード上のすべてのサーバを起動します。これで、マシンのすべてのサーバは正しいネットワークインタフェースにバインドされます。

11.12.4 ポート番号の設定

CMS はインストール時にデフォルトのポート番号の使用が設定されます。CMS のデフォルトのポート番号は 6400 です。このポートは、SAP BusinessObjects によって予約されているポートの範囲内となります (6400 ～ 6410)。これらのポートを経由した通信は、サードパーティアプリケーションとは競合しません。

起動して有効になると、その他の各 BI プラットフォームサーバは、使用可能なポート (1024 以上) に動的にバインドして、CMS にこのポートを登録し、BI プラットフォームリクエストを受信待機します。必要に応じて、(利用可能なポートを動的に選択するのではなく) 特定のポートで受信待機するよう各サーバコンポーネントに指示することもできます。たとえば、ファイアウォールを通過して通信する必要がある各 BI プラットフォームサーバに、リクエストポートを手動で設定する必要があります。

ポート番号は、CMC の各サーバの[プロパティ]タブで指定できます。次の表に、[共通設定]領域のオプションをまとめます。これらのオプションは、特定のサーバタイプで使用されるポートと関連しています。

設定	CMS	その他のサーバ
リクエストポート	他のサーバからのすべてのリクエスト(ネームサーバのリクエストを除く)を受け入れるために CMS が使用するポートを指定します。ネームサーバポートと同じネットワークインタフェースを使用します。[自動割り当て]をオンにすると、サーバでは、OS で割り当てられたポート番号が自動的に使用されます。	サーバがすべてのリクエストを受信待機するポートを指定します。[自動割り当て]をオンにすると、サーバでは、OS で割り当てられたポート番号が自動的に使用されます。
ネームサーバポート	CMS がネームサービスリクエストを受信待機する BI プラットフォームポートを指定します。デフォルトは 6400 です。	使用できません。

11.12.4.1 CMC でデフォルトの CMS ポートを変更する

クラスタですでに実行されている CMS がある場合は、CMC を使用してデフォルトの CMS ポート番号を変更できます。クラスタで実行されている CMS がない場合は、Windows で CCM を使用するか、UNIX で `serverconfig.sh` を使用してポート番号を変更する必要があります。

> **注記**
>
> CMC では、リクエストポートおよびネームサーバポートに同じネットワークインタフェースカードを使用します。

1. CMC の[サーバ]管理エリアを表示します。
2. サーバリストで CMS をダブルクリックします。
3. [ネームサーバポート]の番号を、CMS で受信待機するポートに置き換えます(デフォルトのポートは 6400 です)。
4. *[保存して閉じる]*をクリックします。
5. CMS を再起動します。

   CMS は指定したポート番号で受信待機を開始します。Server Intelligence Agent は、ノード上の他のすべてのサーバでリクエストポートに対する[自動割り当て]オプションがオンになっている場合、それらのサーバに新しい設定を動的に伝播します。すべてのノードメンバーの[プロパティ]設定に変更が表示されるまで数分かかる場合があります。

   [プロパティ]タブで選択した設定は、サーバのコマンドラインに反映され、[プロパティ]ページにも表示されます。

11.12.4.2 Windows で CCM のデフォルト CMS ポートを変更する

クラスタでアクセス可能な CMS がなく、デプロイメントにおいて 1 つまたは複数の CMS のデフォルト CMS ポートを変更する必要がある場合、CCM を使用して CMS ポート番号を変更する必要があります。

1. CCM を開き、ノードの SIA を停止します。
2. SIA を右クリックし、[プロパティ]を選択します。
3. [プロパティ]ダイアログボックスで[スタートアップ]タブをクリックします。
4. [ローカル *CMS* サーバ]一覧からポート番号を変更する CMS を選択し、[プロパティ]をクリックします。
5. CMS を特定のポートにバインドするには、[ポート] フィールドにポート番号を入力します。
6. [*OK*]をクリックして、新しい設定を適用します。
7. SIA を起動し、サーバが起動するまで待機します。

11.12.4.3 Unix で CCM のデフォルト CMS ポートを変更する

クラスタ上にアクセス可能な CMS がなく、デプロイメントにおいて 1 つまたは複数の CMS のデフォルト CMS ポートを変更する場合は、`serverconfig.sh` スクリプトを使用して CMS ポート番号を変更します。

1. `ccm.sh` スクリプトを使用し、ポート番号を変更する CMS をホストする Server Intelligence Agent (SIA) を停止します。
2. `serverconfig.sh` スクリプトを実行します。

   デフォルトでは、このスクリプトは `<InstallDir>/sap_bobj` ディレクトリにあります。
3. *3 - ノードの変更*を選択し、`Enter` キーを押します。
4. 変更する CMS をホストするノードを選択し、`Enter` キーを押します。
5. *3 - ローカル CMS の変更*を選択し、`Enter` キーを押します。
   ノードでホストされている CMS の一覧が表示されます。
6. 変更する CMS を選択し、`Enter` キーを押します。
7. CMS の新しいポート番号を入力し、`Enter` キーを押します。
8. SIA の起動時に CMS が自動的に起動するかどうかを指定し、`Enter` キーを押します。
9. CMS のコマンドライン引数を入力するか、現在の引数を受け入れ、`Enter` キーを押します。
10. 「**`quit`**」と入力して、スクリプトを終了します。
11. `ccm.sh` を使用して SIA を起動し、サーバが起動するまで待機します。

11.12.4.4 リクエストを受け入れるために CMS が使用するポートを変更する

1. CMC のサーバ管理エリアを表示します。
2. CMS を選択し、管理メニューのプロパティを選択します。
3. 共通設定で、リクエストポートで自動割り当てチェックボックスをオフにしてから、サーバで受信待機するポート番号を入力します。
4. 保存または保存して閉じるをクリックします。
5. CMS を再起動します。

CMS が新しいポートにバインドされ、他のサーバからのリクエストの受信待機を開始します。

11.12.4.5 リクエストを受け入れるためにサーバが使用するポートを変更する

> ⓘ 注記
>
> 以下の手順は、Central Management Server (CMS) のリクエストポートの変更には使用できません。代わりに、「"リクエストを受け入れるために CMS が使用するポートを変更する"」を参照してください。

1. CMC の[サーバ]管理エリアを表示します。
2. サーバを選択し、[アクション]メニューの[サーバの停止]を選択します。
3. サーバをダブルクリックします。
   [プロパティ]画面が表示されます。
4. [共通設定]で、[リクエストポート]で[自動割り当て]チェックボックスをオフにしてから、サーバで受信待機するポート番号を入力します。
5. [保存]または[保存して閉じる]をクリックします。
6. サーバを開始して有効にします。

サーバは新しいポートにバインドされ、CMS に登録されて、新しいポートで BI プラットフォームリクエストの受信待機を開始します。

11.13 ノードの管理

11.13.1 ノードの使用

ノードは、同じホストで実行され、同じ Server Intelligence Agent (SIA) で管理される BI プラットフォームサーバのグループです。 ノード上のサーバはすべて、同じユーザアカウントで実行されます。 1 つのマシンに多数のノードを含めることができるため、異なるユーザアカウントでプロセスを実行できます。 1 つの SIA で、ノード上のすべてのサーバを管理およびモニタリングして、サーバが適切に動作するようにします。

> ⓘ 注記
>
> すべてのノード管理手順を安全に実行するには、Enterprise 認証付きの Administrator アカウントを使用する必要があります。 ただし、サーバ間の SSL 通信が有効になっている場合、ノード管理タスクを実行するには、SSL を無効にする必要があります。

> ⓘ 注記
>
> すべての BI プラットフォームサーバからそれぞれのデータソースに接続するために必要なすべてのデータベースドライバ (たとえば、CMS から CMS データベースに接続するためのドライバ) が存在していることと、正しい環境設定が済んでいること (たとえば、適切な環境変数が設定されていること) を確認します。

11.13.1.1 変数

変数	説明
`<INSTALLDIR>`	SAP BusinessObjects Business Intelligence プラットフォームがインストールされるディレクトリ。 Windows の場合: `C:¥Program Files (x86)¥SAP BusinessObjects`
`<SCRIPTDIR>`	ノード管理スクリプトが配置されるディレクトリ。 • Windows の場合: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥scripts` • Unix の場合: `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts`
`<PLATFORM32>`	Unix オペレーティングシステムの名前。 次の値を指定できます。 • `aix_rs6000` • `linux_x86` • `solaris_sparc` • `win32_x86`
`<PLATFORM64>`	Unix オペレーティングシステムの名前。 次の値を指定できます。 • `aix_rs6000_64` • `linux_x64` • `solaris_sparcv9` • `win64_x64`

11.13.1.2 SQL Anywhere 用に Unix マシンを準備する

Unix マシン上で ODBC データソース として SQL Anywhere を使用するには、`odbc.ini` ファイルを作成し、source コマンドでこのファイルを読み込む必要があります。

> **注記**
>
> BI プラットフォームとともにインストールされるバンドル版の SQL Anywhere を使用する場合、この手順は不要です。

1. `<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>` に `odbc.ini` を作成します。
2. SQL Anywhere のデータベースソース名 (DSN)、データベース名、およびサーバ名と、SQL Anywhere データベースサーバをホストするマシンの IP アドレスおよびポート番号を入力します。

3. odbc.ini を保存します。
4. SQL Anywhere 環境を現在の環境に導入します。

   たとえば、コマンドラインシェルとして Bash を使用している場合は、64 ビット版の sa_config.sh をソースに指定します。
5. odbc.ini ファイルが作成されたディレクトリを示す ODBCINI 環境変数を定義します。

   子プロセスが ODBCINI 環境変数を参照できるように、環境変数を設定します。

例

サンプルの odbc.ini ファイル:

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0
[SampleDatabase]
UID=Administrator
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcpip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

サンプルの source コマンド:

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

関連情報

変数 [452 ページ]

11.13.2 新しいノードの追加

BI プラットフォームを最初にインストールするときに、インストールプログラムによって 1 つのノードが作成されます。

別のユーザアカウントでサーバを実行する場合は、追加のノードが必要になることがあります。

セントラル設定マネージャ (CCM) またはノード管理スクリプトを使用すると、新しいノードを追加できます。ファイアウォールを使用する場合は、Server Intelligence Agent (SIA) および Central Management Server (CMS) のポートが開いていることを確認します。

> **注記**
>
> CCM またはノード管理スクリプトは、ノードを追加するマシン上でを使用します。リモートマシンにノードを追加することはできません。

BI プラットフォームインストールとはインストーラによって 1 つのマシン上に作成される BI プラットフォームファイルの一意のインスタンスです。BI プラットフォームインストールのインスタンスは、単一クラスタ内でのみ使用できます。同一の BI プラットフォームインストールを共有している異なるクラスタに属するノードは、サポートされません。このタイプのデプロイメントではパッチやアップデートの適用ができないためです。同一マシン上で複数のソフトウェアインストールをサポートするのは Unix プラットフォームのみであり、それぞれのインストールが一意のユーザアカウントの下で実行され、インストール間でファイルが共有されないようにフォルダを分けてインストールされている場合のみです。

クラスタ内のすべてのマシンで、バージョンとパッチレベルを同じにする必要があります。

> → 推奨事項
>
> FIPS が有効になっており、CORBA SSL が設定されている BI プラットフォームデプロイメントにノードを追加する場合は、[新規一時 CMS の起動] オプションを使用することをお奨めします。
>
> FIPS が有効になっておらず、CORBA SSL が設定されている BI プラットフォームデプロイメントにノードを追加する場合は、[新規一時 CMS の起動] オプションを使用することをお奨めします。
>
> FIPS が有効になっており、CORBA SSL が設定されていない BI プラットフォームデプロイメントにノードを追加する場合は、既存の CMS を使用することをお奨めします。

11.13.2.1 既存のデプロイメントで新しいマシンにノードを追加する

インストールプログラムを使用して新しいマシンを既存のデプロイメントに追加する際、最初のノードをマシン上に自動作成することができます。

> → ヒント
>
> インストール時に、[展開] をクリックして、既存の Central Management Server を指定します。

追加のノードを作成する場合は、セントラル設定マネージャまたは `serverconfig.sh` スクリプトを使用します。

インストールの詳細については、*SAP BI* プラットフォームインストールガイドを参照してください。

11.13.2.2 Windows 上でノードを追加する

> ⚠ 警告
>
> ノードを追加する前と後に、クラスタ全体のサーバ設定をバックアップします。

1. セントラル設定マネージャ (CCM) のツールバーで、[ノードの追加] をクリックします。
2. ノードの追加ウィザードで、新しい Server Intelligence Agent (SIA) のノード名とポート番号を入力します。
3. 新しいノードにサーバを作成するかどうかを選択します。
   - サーバなしのノードの追加

- *CMS* で使用するノードの追加
- デフォルトサーバで使用するノードの追加
  このオプションを選択すると、このマシンにインストールされているサーバのみが生成されます。使用可能なサーバがすべて含まれるわけではありません。

4. CMS を選択します。
   - デプロイメントが実行中の場合は、[稼働中の既存 *CMS* の使用] を選択し、[次へ] をクリックします。プロンプトが表示されたら、既存の CMS のホスト名とポート番号、管理者認証情報、データソース名、システムデータベースの認証情報、およびクラスタキーを入力します。
   - デプロイメントが停止されている場合は、[新規一時 *CMS* の起動] を選択し、[次へ] をクリックします。プロンプトが表示されたら、一時 CMS のホスト名とポート番号、管理者認証情報、データソース名、システムデータベースの認証情報、およびクラスタキーを入力します。一時 CMS が起動されます。一時 CMS はこのプロセスが終了すると停止されます。

     ⚠ 警告

     一時 CMS の実行中はデプロイメントの使用を控えてください。既存の CMS と新しい CMS が必ず異なるポートを使用するようにします。

5. 確認ページを確認して、[完了] をクリックします。
   CCM によってノードが作成されます。エラーが発生した場合は、ログファイルを確認してください。

これで、CCM を使用して新しいノードを起動できます。

11.13.2.2.1 スクリプトを使用した Windows 上でのノードの追加

⚠ 警告

ノードを追加する前と後に、クラスタ全体のサーバ設定をバックアップします。

`AddNode.bat` を使用して、Windows マシンにノードを追加することができます。 詳細については、「“ノードを追加、再作成、および削除するためのスクリプトパラメータ”」の節を参照してください。

例

コマンドプロンプトの制限により、パラメータ内では、空白を避けるためのキャレット (^)、等号 (=)、およびセミコロン (;) を使用する必要があります。ただし、テキストを引用符で囲む場合はこの限りではありません。

```
<SCRIPTDIR>¥AddNode.bat -name mynode2
  -siaport 6415
      -cms mycms:6400
      -username Administrator
      -password My^ Password
      -cmsport 7400
      -dbdriver mysqldatabasesubsystem
      -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
      -dbkey abc1234
      -noservers
```

```
-createcms
```

> ⓘ 注記
>
> 長い文字列でのキャレットの使用を避けるには、スクリプト名とそのすべてのパラメータを一時 `response.bat` ファイルに書き込んでから、パラメータなしで `response.bat` を実行します。

関連情報

変数 [452 ページ]
ノードを追加、再登録、削除するスクリプトパラメータ [469 ページ]

11.13.2.3 Unix 上でノードを追加する

> ⚠ 警告
>
> ノードを追加する前と後に、クラスタ全体のサーバ設定をバックアップします。

1. `<INSTALLDIR>/sap_bobj/serverconfig.sh` を実行します。
2. [*1 - Add node*]を選択し、`Enter` キーを押します。
3. 新しいノードの名前を入力し、`Enter` キーを押します。
4. 新しい SIA のポート番号を入力し、`Enter` キーを押します。
5. 新しいノードにサーバを作成するかどうかを選択します。
   - *no servers*
     サーバを含まないノードが作成されます。
   - *cms*
     ノード上に CMS が作成されますが、その他のサーバは作成されません。
   - デフォルトサーバ
     このマシンにインストールされているサーバのみが作成されます。使用可能なサーバがすべて含まれるわけではありません。
6. CMS を選択します。
   - デプロイメントが実行中の場合は、[既存] を選択し、`Enter` キーを押します。
     プロンプトが表示されたら、既存の CMS のホスト名とポート番号、管理者認証情報、データベース接続情報とシステムデータベースの認証情報、およびクラスタキーを入力します。
   - デプロイメントが停止されている場合は、[一時] を選択し、`Enter` キーを押します。
     プロンプトが表示されたら、一時 CMS のホスト名とポート番号、管理者認証情報、データベース接続情報とシステムデータベースの認証情報、およびクラスタキーを入力します。一時 CMS が起動されます。一時 CMS はこのプロセスが終了すると停止されます。

     > ⚠ 警告
     >
     > 一時 CMS の実行中はデプロイメントの使用を控えてください。既存の CMS と新しい CMS が必ず異なるポートを使用するようにします。

7. 確認ページを確認して、Enter キーを押します。
   CCM によってノードが作成されます。エラーが発生した場合は、ログファイルを確認してください。

これで、<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName> を実行して新しいノードを起動できます。

11.13.2.3.1 スクリプトを使用した Unix 上でのノードの追加

> ⚠ 警告
>
> ノードを追加する前と後に、クラスタ全体のサーバ設定をバックアップします。

addnode.sh を使用して、Unix マシン上でノードを追加することができます。 詳細については、“ノードを追加、再作成、および削除するためのスクリプトパラメータ”の節を参照してください。

例

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
        -dbkey abc1234
  -noservers
  -createcms
```

関連情報

変数 [452 ページ]
ノードを追加、再登録、削除するスクリプトパラメータ [469 ページ]

11.13.3 ノードの再作成

クラスタ全体のサーバ設定を復元した後、またはデプロイメントをホストするマシンでエラーが発生して損傷を受けた場合、あるいはデプロイメントをホストするマシンのファイルシステムが正しくない場合、セントラル設定マネージャ (CCM) またはノード管理スクリプトを使用することにより、ノードを再作成できます。以下のガイドラインを適用してください。

- 置換マシンに同じインストールオプションとノード名でデプロイメントを再インストールする場合は、ノードを再作成する必要はありません。インストールプログラムによって、自動的にノードが再作成されます。

- ノードの再作成が必要なのは、同じインストールオプションとパッチレベルで既存のデプロイメントが適用されているマシンだけです。
- 再作成する必要があるのは、デプロイメント内のマシンに存在していないノードだけです。他のマシンが同じノードをホストしていないことを確認します。
- デプロイメントでは、別のオペレーティングシステムでノードを実行することができますが、ノードの再作成が必要となるのは、同じオペレーティングシステムを使用するマシンだけです。
- ファイアウォールを使用する場合は、Server Intelligence Agent (SIA) および Central Management Server (CMS) のポートが開いていることを確認します。

> ⓘ 注記
>
> CMS 以外のすべてのサーバが停止した後で、ノードを再作成することができます。

> → 注意
>
> ノードがあるマシンでのみノードを再作成できます。

11.13.3.1 Windows 上でノードを再作成する

1. セントラル設定マネージャ (CCM) のツールバーで、[ノードの追加] をクリックします。
2. ノード追加ウィザードで、再作成された Server Intelligence Agent (SIA) のノード名とポート番号を入力します。

   > ⓘ 注記
   >
   > オリジナルノードの名前と再作成されたノードの名前は同じにする必要があります。

3. [ノードをもう一度作成] を選択し、[次へ] をクリックします。
   - ノードが Central Management Server (CMS) のシステムデータベースに存在する場合、ノードはローカルホストに再作成されます。

     > ⚠ 警告
     >
     > このオプションを使用するのは、ノードがクラスタ内のホストに存在しない場合のみです。

   - ノードが CMS のシステムデータベースに存在しない場合は、デフォルトのサーバを含む新しいノードが追加されます。デフォルトサーバには、ホストにインストールされているすべてのサーバが含まれます。
4. CMS を選択します。
   - CMS が実行中の場合は、[稼働中の既存 *CMS* の使用] を選択し、[次へ] をクリックします。
     プロンプトが表示されたら、既存の CMS のホスト名とポート番号、管理者認証情報、データソース名、システムデータベースの認証情報、およびクラスタキーを入力します。
   - CMS が停止されている場合は、[新規一時 *CMS* の起動] を選択し、[次へ] をクリックします。
     プロンプトが表示されたら、一時 CMS のホスト名、管理者認証情報、データソース名、システムデータベースの認証情報、およびクラスタキーを入力します。一時 CMS が起動されます。一時 CMS はこのプロセスが終了すると停止されます。

     > ⚠ 警告
     >
     > 一時 CMS の実行中はデプロイメントの使用を控えてください。

5. 確認ページを確認して、[完了] をクリックします。
   CCM によってノードが再作成され、ノードに関する情報がローカルマシンに追加されます。エラーが発生した場合は、ログファイルを確認してください。

これで、CCM を使用して再作成されたノードを起動できます。

11.13.3.1.1 スクリプトを使用した Windows 上でのノードの再作成

`AddNode.bat` を使用すると、Windows マシン上でノードを再作成することができます。 詳細については、“ノードを追加、再作成、および削除するためのスクリプトパラメータ”の節を参照してください。

例

コマンドプロンプトの制限により、パラメータ内では、空白を避けるためのキャレット (^)、等号 (=)、およびセミコロン (;) を使用する必要があります。ただし、テキストを引用符で囲む場合はこの限りではありません。

```
<SCRIPTDIR>¥AddNode.bat -name mynode2
  -siaport 6415
        -cms mycms:6400
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
  -adopt
```

> ⓘ 注記
>
> 長い文字列でのキャレットの使用を避けるには、スクリプト名とそのすべてのパラメータを一時 `response.bat` ファイルに書き込んでから、パラメータなしで `response.bat` を実行します。

関連情報

変数 [452 ページ]
ノードを追加、再登録、削除するスクリプトパラメータ [469 ページ]

11.13.3.2 Unix 上でノードを再作成する

1. `<INSTALLDIR>/sap_bobj/serverconfig.sh` を実行します。
2. [*1 - Add node*]を選択し、`Enter` キーを押します。

3. 新しいノードの名前を入力し、Enter キーを押します。

> ⓘ 注記
>
> オリジナルノードの名前と再作成されたノードの名前は同じにする必要があります。

4. 新しい SIA のポート番号を入力し、Enter キーを押します。
5. [ノードをもう一度作成] を選択し、Enter キーを押します。
   - ノードが Central Management Server (CMS) のシステムデータベースに存在する場合、ノードはローカルホストに再作成されます。

     > ⚠ 警告
     >
     > このオプションを使用するのは、ノードがクラスタ内のホストに存在しない場合のみです。

   - ノードが CMS のシステムデータベースに存在しない場合は、デフォルトのサーバを含む新しいノードが追加されます。デフォルトサーバには、ホストにインストールされているすべてのサーバが含まれます。
6. CMS を選択します。
   - デプロイメントが実行中の場合は、[既存] を選択し、Enter キーを押します。
     プロンプトが表示されたら、既存の CMS のホスト名とポート番号、管理者認証情報、データベース接続情報とシステムデータベースの認証情報、およびクラスタキーを入力します。
   - デプロイメントが停止されている場合は、[一時] を選択し、Enter キーを押します。
     プロンプトが表示されたら、一時 CMS のホスト名、管理者認証情報、データベース接続情報とシステムデータベースの認証情報、およびクラスタキーを入力します。一時 CMS が起動されます。一時 CMS はこのプロセスが終了すると停止されます。

     > ⚠ 警告
     >
     > 一時 CMS の実行中はデプロイメントの使用を控えてください。

7. 確認ページを確認して、Enter キーを押します。
   CCM によってノードが再作成され、ノードに関する情報がローカルマシンに追加されます。エラーが発生した場合は、ログファイルを確認してください。

これで `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` を実行して再作成されたノードを起動できます。

11.13.3.2.1 スクリプトを使用した Unix 上でのノードの再作成

`addnode.sh` を使用すると、Unix マシン上でノードを再作成することができます。詳細については、「"ノードを追加、再作成、および削除するためのスクリプトパラメータ"」の節を参照してください。

例

```
<SCRIPTDIR>/addnode.sh -name mynode2
        -siaport 6415
        -cms mycms:6400
```

```
        -username Administrator
        -password Password1
  -cmsport 7400
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=BusinessObjects CMS
140;UID=Administrator;PWD=Password1;HOSTNAME=database;PORT=3306"
        -dbkey abc1234
        -adopt
```

関連情報

変数 [452 ページ]
ノードを追加、再登録、削除するスクリプトパラメータ [469 ページ]

11.13.4 ノードの削除

停止されたノードを削除するには、実行中のセントラル設定マネージャ (CCM) またはノード管理スクリプトを使用します。以下のガイドラインを適用してください。

- ノードを削除すると、ノード上のサーバも完全に削除されます。
- クラスタに複数のマシンが含まれている場合は、ノードを削除した後、クラスタからマシンを削除し、ソフトウェアをアンインストールします。ノードを削除する前にクラスタからマシンを削除する場合、またはマシン上のファイルシステムに不具合が発生した場合は、同じクラスタ内の同じサーバを持つ別のマシンにノードを再作成してからノードを削除する必要があります。

> → 注意
>
> ノードがあるマシンでのみノードを削除できます。

関連情報

ノードの再作成 [457 ページ]

11.13.4.1 Windows 上でノードを削除する

> ⚠ 警告
>
> ノードを削除する前と後に、クラスタ全体のサーバ設定をバックアップします。

1. セントラル設定マネージャ (CCM) を実行します。
2. CCM で、削除するノードを停止します。

3. ノードを選択して、ツールバーの [ノードの削除] をクリックします。
4. プロンプトが表示された場合は、CCM のホスト名、ポート、および管理者認証情報を入力します。

CCM により、ノードとそのノード上のすべてのサーバが削除されます。

> ⓘ 注記
>
> 以下の 2 つの方法を使用すると、新たに追加したノードを SSL 設定の後に削除することができます。
>
> - 新たに作成したノードと接続対象の CMS が実行されている SIA ノードの両方から SSL パラメータを削除します。
> - RemoveNode.bat 内のメインクラス宣言の前に以下の SSL パラメータを追加し、実行します。-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Path to the SSL certificate directory" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.1.1 スクリプトを使用した Windows 上でのノードの削除

> ⚠ 警告
>
> ノードを削除する前と後に、クラスタ全体のサーバ設定をバックアップします。

`RemoveNode.bat` を使用すると、Windows マシン上でノードを削除することができます。詳細については、「“ノードを追加、再作成、および削除するためのスクリプトパラメータ”」の節を参照してください。

例

```
<SCRIPTDIR>¥RemoveNode.bat -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

関連情報

変数 [452 ページ]
ノードを追加、再登録、削除するスクリプトパラメータ [469 ページ]

11.13.4.2 Unix 上でノードを削除する

ノードを削除する前と後に、クラスタ全体のサーバ設定をバックアップします。

1. `<INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>` を実行して、削除するノードを停止します。
2. `<INSTALLDIR>/sap_bobj/serverconfig.sh` を実行します。
3. [2 - ノードの削除] を選択し、`Enter` キーを押します。
4. 削除するノードを選択し、`Enter` キーを押します。
5. プロンプトが表示された場合は、CMS のホスト名、ポート番号、および管理者認証情報を入力します。

ノードとそのノード上のすべてのサーバが削除されます。

> **注記**
>
> 以下の 2 つの方法を使用すると、新たに追加したノードを SSL 設定の後に削除することができます。
>
> - 新たに作成したノードと接続対象の CMS が実行されている SIA ノードの両方から SSL パラメータを削除します。
> - RemoveNode.bat 内のメインクラス宣言の前に以下の SSL パラメータを追加し、実行します。-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=" Path to the SSL certificate directory" -DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key -Dpassphrase=passphrase.txt -Dpsecert=cert.pse

11.13.4.2.1 スクリプトを使用した Unix 上でのノードの削除

> **警告**
>
> ノードを削除する前と後に、クラスタ全体のサーバ設定をバックアップします。

`removenode.sh` を使用すると、Unix マシン上でノードを削除することができます。詳細については、「“ノードを追加、再作成、および削除するためのスクリプトパラメータ”」の節を参照してください。

例

```
<SCRIPTDIR>¥removenode.sh -name mynode2
        -cms mycms:6400
        -username Administrator
        -password Password1
```

関連情報

変数 [452 ページ]
ノードを追加、再登録、削除するスクリプトパラメータ [469 ページ]

11.13.5 ノードの名前の変更

セントラル設定マネージャ (CCM) を使用して、ノードの名前を変更することができます。 ノードの名前を変更するには、新しいノードを新しい名前で作成し、オリジナルノードから新しいノードにサーバをコピーして、オリジナルノードを削除する必要があります。 以下のガイドラインを適用してください。

- ノードが配置されているマシンの名前を変更する場合、ノード名の変更は不要です。 既存のノード名は引き続き使用可能です。
- ファイアウォールを使用する場合は、Server Intelligence Agent (SIA) および Central Management Server (CMS) のポートが開いていることを確認します。

> → 注意
>
> ノードがあるマシンでのみノード名を変更できます。

関連情報

新しいノードの追加 [453 ページ]
ノードの削除 [461 ページ]

11.13.5.1 Windows 上でノードの名前を変更する

> ⚠ 警告
>
> ノードの名前を変更する前と後に、クラスタ全体のサーバ設定をバックアップする必要があります。

1. セントラル設定マネージャ (CCM) を開始します。
2. セントラル設定マネージャ (CCM) のツールバーで、[ノードの追加] をクリックします。
3. ノード追加ウィザードで、新しい Server Intelligence Agent (SIA) のノード名とポート番号、管理者認証情報、データベース接続情報、システムデータベースの認証情報、およびクラスタキーを入力します。
4. [サーバなしのノードの追加] を選択します。
5. ノードが作成されたら、セントラル管理コンソールの [サーバ管理] ページを使用して、すべてのサーバをオリジナルノードから新しいノードにコピーします。

   > ⓘ 注記
   >
   > コピーしたサーバとオリジナルノードのサーバとの間にポートの競合がないことを確認します。

6. CCM で、新しいノードを起動します。
7. 新しいノードを起動してから 5 分経過したら、CCM を使用してオリジナルノードを削除します。

関連情報

新しいノードの追加 [453 ページ]
ノードの削除 [461 ページ]

11.13.5.2 Unix 上でノードの名前を変更する

> ⚠ 警告
>
> ノードの名前を変更する前と後に、クラスタ全体のサーバ設定をバックアップする必要があります。

1. `<INSTALLDIR>/sap_bobj/serverconfig.sh` を実行します。
2. [*1 - Add node*]を選択し、`Enter` キーを押します。
3. 新しいノードの名前を入力し、`Enter` キーを押します。
4. 新しい SIA のポート番号を入力し、`Enter` キーを押します。
5. プロンプトが表示されたら、管理者認証情報、データベース接続情報、システムデータベースの認証情報、およびクラスタキーを入力します。
6. [*no servers*] を選択し、`Enter` キーを押します。
7. ノードが作成されたら、セントラル管理コンソールの [サーバ管理] ページを使用して、すべてのサーバをオリジナルノードから新しいノードにコピーします。

   > ⓘ 注記
   >
   > コピーしたサーバとオリジナルノードのサーバとの間にポートの競合がないことを確認します。

8. `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` を実行して、新しいノードを起動します。
9. 新しいノードを起動してから 5 分経過したら、`serverconfig.sh` を使用してオリジナルノードを削除します。

関連情報

新しいノードの追加 [453 ページ]
サーバのクローン [412 ページ]
ノードの削除 [461 ページ]

11.13.6 ノードの移動

クラスタ間で停止されたノードを移動するには、セントラル設定マネージャ (CCM) またはノード管理スクリプトを使用します。以下のガイドラインを適用してください。

- 出力先クラスタに同じ名前のノードが存在しないことを確認します。

- また、ソースノードが存在するマシンにインストールされているすべてのサーバタイプが、出力先クラスタにもインストールされていることも確認します。
- 新しいマシンを実稼動クラスタに追加する場合、テストが終了するまでマシンを使用不可にしておく場合は、BI プラットフォームをスタンドアロンマシンにインストールし、マシンをテストしてから、ノードを実稼動クラスタに移動します。
- このマシンの BI プラットフォームのバージョンおよびサービスパックレベルは、クラスタ内のほかのマシンと一致している必要があります。

> → 注意
>
> ノードがあるマシンでのみノードを移動できます。

11.13.6.1 Windows 上で既存のノードを移動する

この例では、移動対象のノードがソースシステムにインストールされているとします。当初スタンドアロンであったソースシステムマシンを出力先クラスタに追加します。

> ⚠ 警告
>
> ノードを移動する前と後に、クラスタ全体のサーバ設定をバックアップします。

1. セントラル設定マネージャ (CCM) でノードを停止します。
2. ノードを右クリックして、[移動] を選択します。
3. プロンプトが表示されたら、データソース名を選択し、ホスト名、ポート、データベース接続情報、出力先 CMS の管理者認証情報、およびクラスタキーを入力します。
4. CMS を選択します。
   - ソースデプロイメントが実行中の場合は、[稼働中の既存 *CMS* の使用] を選択し、[次へ] をクリックします。
     プロンプトが表示されたら、ソースシステムの既存の CMS のホスト名とポート番号、および管理者の認証情報を入力します。
   - ソースデプロイメントが停止されている場合は、[新規一時 *CMS* の起動] を選択し、[次へ] をクリックします。
     プロンプトが表示されたら、ソースシステムの一時 CMS のホスト名とポート番号、管理者認証情報、データソース名、ソースシステムデータベースのデータベース認証情報、およびクラスタキーを入力します。一時 CMS が起動されます。一時 CMS はこのプロセスが終了すると停止されます。

     > ⚠ 警告
     >
     > 一時 CMS の実行中はデプロイメントの使用を控えてください。
5. 確認ページを確認して、[完了] をクリックします。
   CCM によって、ソースクラスタのノードと同じ名前および同じサーバで出力先クラスタに新しいノードが作成されます。ノードのコピーはソースクラスタに残ります。ノードのサーバの設定テンプレートは移動されません。エラーが発生した場合は、ログファイルを確認してください。

   > ⚠ 警告
   >
   > ノードの移動後はソースクラスタを使用しないでください。

6. CCM で、移動したノードを起動します。

11.13.6.1.1 スクリプトを使用した Windows 上でのノードの移動

> ⚠ 警告
>
> ノードを移動する前と後に、クラスタ全体のサーバ設定をバックアップします。

`MoveNode.bat` を使用すると、Windows マシン上でノードを移動することができます。詳細については、「“ノードを移動するためのスクリプトパラメータ”」の節を参照してください。

例

コマンドプロンプトの制限により、パラメータ内では、空白を避けるためのキャレット (^)、等号 (=)、およびセミコロン (;) を使用する必要があります。ただし、テキストを引用符で囲む場合はこの限りではありません。

```
<SCRIPTDIR>¥MoveNode.bat -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

> ⓘ 注記
>
> 長い文字列でのキャレットの使用を避けるには、スクリプト名とそのすべてのパラメータを一時 `response.bat` ファイルに書き込んでから、パラメータなしで `response.bat` を実行します。

関連情報

変数 [452 ページ]
ノードを移動するためのスクリプトパラメータ [471 ページ]

11.13.6.2 Unix 上で既存のノードを移動する

この例では、移動対象のノードがソースシステムにインストールされているとします。当初スタンドアロンであったソースシステムマシンを出力先クラスタに追加します。

> ⚠ 警告
>
> ノードを移動する前と後に、クラスタ全体のサーバ設定をバックアップします。

1. `<INSTALLDIR>/sap_bobj/ccm.sh -stop <nodeName>` を実行して、ノードを停止します。
2. `<INSTALLDIR>/sap_bobj/serverconfig.sh` を実行します。
3. [*4 - Move node*] を選択し、`Enter` キーを押します。
4. 移動するノードを選択て、`Enter` キーを押します。
5. プロンプトが表示されたら、システムデータベース接続情報を選択し、ホスト名、ポート、出力先 CMS の管理者認証情報、およびクラスタキーを入力します。
6. CMS を選択します。
   - ソースデプロイメントが実行中の場合は、[既存] を選択し、`Enter` キーを押します。
     プロンプトが表示されたら、ソースシステムの既存の CMS のホスト名とポート番号、および管理者の認証情報を入力します。
   - ソースデプロイメントが停止されている場合は、[一時] を選択し、`Enter` キーを押します。
     プロンプトが表示されたら、ソースシステムの一時 CMS のホスト名とポート、管理者認証情報、データベース接続情報とソースシステムデータベースの認証情報、およびクラスタキーを入力します。一時 CMS が起動されます。一時 CMS はこのプロセスが終了すると停止されます。

     > ⚠ 警告
     >
     > 一時 CMS の実行中はデプロイメントの使用を控えてください。既存の CMS と一時 CMS が必ず異なるポートを使用するようにします。
7. 確認ページを確認して、`Enter` キーを押します。
   CCM によって、ソースクラスタのノードと同じ名前および同じサーバで出力先クラスタに新しいノードが作成されます。ノードのコピーはソースクラスタに残ります。ノードのサーバの設定テンプレートは移動されません。エラーが発生した場合は、ログファイルを確認してください。

   > ⚠ 警告
   >
   > ノードの移動後はソースクラスタを使用しないでください。
8. `<INSTALLDIR>/sap_bobj/ccm.sh -start <nodeName>` を実行して、移動したノードを起動します。

11.13.6.2.1 スクリプトを使用した Unix 上でのノードの移動

> ⚠ 警告
>
> ノードを移動する前と後に、クラスタ全体のサーバ設定をバックアップします。

`movenode.sh` を使用すると、Unix マシン上でノードを移動することができます。詳細については、「“ノードを移動するためのスクリプトパラメータ”」の節を参照してください。

例

```
<SCRIPTDIR>/movenode.sh -cms sourceMachine:6409
        -username Administrator
        -password Password1
        -dbdriver mysqldatabasesubsystem
        -connect "DSN=Source
BOEXI40;UID^=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
        -dbkey abc1234
        -destcms destinationMachine:6401
        -destusername Administrator
        -destpassword Password2
        -destdbdriver sybasedatabasesubsystem
        -destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
        -destdbkey def5678
```

関連情報

変数 [452 ページ]
ノードを移動するためのスクリプトパラメータ [471 ページ]

11.13.7 スクリプトパラメータ

11.13.7.1 ノードを追加、再登録、削除するスクリプトパラメータ

パラメータ	説明	例
-adopt	CMS にすでに存在する場合には、ノードを再作成します。	**-adopt**
-cms	Central Management Server (CMS) の名称およびポート番号。 **⚠ 警告** -usetempcms を使用する場合は、このパラメータは使用しないでください。 **ⓘ 注記** CMS をデフォルト 6400 ポートで実行中でない場合は、ポート番号を指定する必要があります。	**-cms mycms:6409**

パラメータ	説明	例
-cmsport	• 一時 CMS を起動時の CMS のポート番号。 **⚠ 制限** -usetempcms、-dbdriver、-connect、および -dbkey パラメータも使用する必要があります。 • 新しい CMS 作成時の CMS のポート番号。 **⚠ 制限** -dbdriver、-connect、および -dbkey パラメータも使用する必要があります。	**-cmsport 6401**
-connect	CMS (または一時 CMS) システムデータベースの接続文字列。 **ⓘ 注記** DB2、Oracle、SQL Anywhere、SQL Server、または Sybase データベースに接続する場合は、HOSTNAME 属性および PORT 属性は省略します。	**-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"**
-dbdriver	CMS のデータベースドライバ。 設定可能な値は次のとおり。 • **db2databasesubsystem** • **mysqldatabasesubsystem** • **oracledatabasesubsystem** • **sqlanywheredatabasesubsystem** • **sqlserverdatabasesubsystem** • **sybasedatabasesubsystem** • **newdbdatabasesubsystem**	**-dbdriver mysqldatabasesubsystem**
-dbkey	クラスタキー。	**-dbkey abc1234**
-name	ノード名。	**-name mynode2**
-noservers	サーバを含まないノードを作成します。 **ⓘ 注記** 追加 -createcms パラメータにより CMS でノードが作成されますが、その他のサーバでは作成されません。すべてのデフォルトサーバでノードを作成する場合は、これらのパラメータは省略します。	**-noservers**
-password	管理者アカウントのパスワード。	**-password Password1**

パラメータ	説明	例
`-siaport`	ノードの Server Intelligence Agent のポート番号。	**`-siaport 6409`**
`-username`	管理者アカウントのユーザ名。	**`-username Administrator`**
`-usetempcms`	⚠ 警告 `-cms` を使用する場合は、このパラメータは使用しないでください。 一時 CMS を起動して使用します。 ⓘ 注記 デプロイメントを実行中でない場合は、一時 CMS を使用します。	**`-usetempcms`**

関連情報

スクリプトを使用した Windows 上でのノードの追加 [455 ページ]
スクリプトを使用した Unix 上でのノードの追加 [457 ページ]
スクリプトを使用した Windows 上でのノードの再作成 [459 ページ]
スクリプトを使用した Unix 上でのノードの再作成 [460 ページ]
スクリプトを使用した Windows 上でのノードの削除 [462 ページ]
スクリプトを使用した Unix 上でのノードの削除 [463 ページ]

11.13.7.2 ノードを移動するためのスクリプトパラメータ

パラメータ	説明	例
`-cms`	ソース Central Management Server (CMS) の名称。 ⚠ 警告 `-usetempcms` を使用する場合は、このパラメータは使用しないでください。 ⓘ 注記 CMS をデフォルト 6400 ポートで実行中でない場合は、ポート番号を指定する必要があります。	**`-cms sourceMachine:6409`**

パラメータ	説明	例
-cmsport	• 一時 CMS を起動時の CMS のポート番号。 **⚠ 制限** -usetempcms、-dbdriver、-connect、および -dbkey パラメータも使用する必要があります。 • 新しい CMS 作成時の CMS のポート番号。 **⚠ 制限** -dbdriver、-connect、および -dbkey パラメータも使用する必要があります。	**-cmsport 6401**
-connect	ソース CMS (または一時 CMS) システムデータベースの接続文字列。 **ⓘ 注記** DB2、Oracle、SQL Anywhere、SQL Server、または Sybase データベースに接続する場合は、HOSTNAME 属性および PORT 属性は省略します。	**-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"**
-dbdriver	ソース CMS のデータベースドライバ。 設定可能な値は次のとおり。 • **db2databasesubsystem** • **mysqldatabasesubsystem** • **oracledatabasesubsystem** • **sqlanywheredatabasesubsystem** • **sqlserverdatabasesubsystem** • **sybasedatabasesubsystem** • **newdbdatabasesubsystem**	**-dbdriver mysqldatabasesubsystem**
-dbkey	ソースクラスタキー。	**-dbkey abc1234**
-destcms	出力先 CMS の名称。 **ⓘ 注記** CMS をデフォルト 6400 ポートで実行中でない場合は、ポート番号を指定する必要があります。	**-destcms destinationMachine:6401**

パラメータ	説明	例
-destconnect	出力先 CMS システムデータベースの接続文字列。 **注記** DB2、Oracle、SQL Anywhere、SQL Server、または Sybase データベースに接続する場合は、HOSTNAME 属性および PORT 属性は省略します。	**-destconnect "DSN=Destin BOEXI40;UID=username;PWD=passwor d;HOSTNAME=database;PORT=3306"**
-destdbdriver	出力先 CMS のデータベースドライバ。 設定可能な値は次のとおり。 • **db2databasesubsystem** • **mysqldatabasesubsystem** • **oracledatabasesubsystem** • **sqlanywheredatabasesubsystem** • **sybasedatabasesubsystem** • **newdbdatabasesubsystem**	**-destdbdriver sybasedatabasesubsystem**
-destdbkey	出力先クラスタキー。	**-destdbkey def5678**
-destpassword	出力先 CMS の管理者アカウントのパスワード。	**-destpassword Password2**
-destusername	出力先 CMS の管理者アカウントのユーザ名。	**-destusername Administrator**
-password	ソース CMS の管理者アカウントのパスワード。	**-password Password1**
-username	ソース CMS の管理者アカウントのユーザ名。	**-username Administrator**
-usetempcms	**警告** -cms を使用する場合は、このパラメータは使用しないでください。 一時 CMS を起動して使用します。 **注記** デプロイメントを実行中でない場合は、一時 CMS を使用します。	**-usetempcms**

関連情報

スクリプトを使用した Windows 上でのノードの移動 [467 ページ]
スクリプトを使用した Unix 上でのノードの移動 [468 ページ]

11.13.8 Windows サーバ依存関係の追加

Windows 環境の場合、Server Intelligence Agent (SIA) の各インスタンスは、イベントログサービスと Remote Procedure Call (RPC) サービスに依存します。

SIA が正しく動作しない場合は、両方のサービスが SIA の [依存] タブに表示されていることを確認してください。

11.13.8.1 Windows サーバ依存関係を追加する

1. セントラル設定マネージャ (CCM) を使用して、Server Intelligence Agent (SIA) を停止します。
2. SIA を右クリックして、[プロパティ] を選択します。
3. [依存]タブをクリックします。
4. [追加] をクリックします。
   [依存の追加] ダイアログボックスが表示され、使用可能な依存関係がすべて一覧表示されます。
5. 依存関係を選択して、[追加] をクリックします。
6. [*OK*] をクリックします。
7. CCM を使用して SIA を再起動します。

11.13.9 ノードに対するユーザ認証情報の変更

セントラル設定マネージャ (CCM) を使用すると、オペレーティングシステムでパスワードが変更された場合、またはノード上の全サーバを異なるユーザアカウントで実行する場合に、Server Intelligence Agent (SIA) に対するユーザ認証情報を指定または更新することができます。

SIA によって管理されるサーバはすべて、同じアカウントで実行されます。非システムアカウントを使用してサーバを実行するには、アカウントがサーバマシンのローカル Administrators グループのメンバーであり、“プロセスレベルトークンの置き換え”権限を与えられていることを確認します。

> **⚠ 制限**
>
> Unix マシンの場合は、インストール時と同じアカウントを使用して BI プラットフォームを実行する必要があります。別のアカウントを使用するには、別のアカウントを使用してデプロイメントを再インストールする必要があります。

11.13.9.1 Windows 上でノードのユーザ認証情報を変更する

1. セントラル設定マネージャ (CCM) を使用して、Server Intelligence Agent (SIA) を停止します。
2. SIA を右クリックして、[プロパティ] を選択します。
3. [システムアカウント] チェックボックスをオフにします。
4. ユーザ名とパスワードを入力して、[*OK*] をクリックします。

5. CCM を使用して SIA を再起動します。

SIA およびサーバプロセスにより、新しいユーザアカウントを使用してローカルマシンにログオンされます。

11.14 BI プラットフォームデプロイメントでのマシン名の変更

11.14.1 クラスタ名の変更

クラスタの名前変更におけるベストプラクティスは次のようになります。

> ⚠ 警告
>
> 同じ名前で複数のクラスタをデプロイできません。

条件	アクション
クラスタ名を変更する。	ユーザに新しいクラスタ名を通知し、`<hostname>:<port>` 構文を使用して CMS に最初に接続した後に新しいクラスタ名を使用することを依頼します。 Web Tier で、すべての Web アプリケーションサーバのプロパティファイルのクラスタ名を更新します。
以前に CMS を実行していたマシンに異なるバージョンの BI プラットフォームをインストールするか、別のクラスタにそのマシンを追加する。	• 新しい CMS が異なるポートで実行されるようにしてください。 • クラスタごとに異なるパスワードを使用し、ユーザが正しくないクラスタにログインしないようにします。

11.14.2 IP アドレスの変更

マシンの IP アドレスの変更に伴う設定変更を避けるには、CMC の [サーバ] タブで [サーバプロパティ] を選択し、すべてのサーバにホスト名をバインドするか、[自動割り当て] オプションを使用します。さらに、次のベストプラクティスを実践します。

条件	アクション
CMS データベースまたは監査データベースに ODBC を使用している。	DSN が CMS データベースサーバのホスト名を使用するようにします。
CMS データベースまたは監査データベースに別の種類のデータベース接続を使用している。	CCM を使用してデータベースを更新し、データベースサーバのホスト名を使用します。
CMS データベースまたは監査データベースが CMS と同じホストにある。	マシン名に `localhost` を使用します。
ユーザが Web ブラウザでアクセスする BI プラットフォーム Web アプリケーション (CMC など) の URL を使用している。	デフォルト URL に IP アドレスではなくホスト名を使用します。デフォルトビューアの URL を更新するには、選択したアプリケーションで [処理設定] を選択します。

条件	アクション
Web サービス (Crystal Reports for Java や LiveOffice など) に基づく BI プラットフォームクライアントの URL を使用している。	たとえば、OpenDocument では、CMC で [アプリケーション] タブをクリックし、[ドキュメントを開く] を右クリックして、[処理設定] を選択します。
OpenDocument を使用している。	

代替ガイドライン

> **注記**
>
> 上記のベストプラクティスを実践できない場合にのみ、次のガイドラインを参照してください。

サーバをホストするマシン

条件	アクション
ホストに BI プラットフォームサーバが含まれ、サーバを特定の IP アドレスにバインドする必要がある。	CMC の [サーバ] タブで IP アドレスを変更します。ただし、マシン上のすべてが更新されるまで、サーバは再起動しません。次に、個別の BI プラットフォームサーバではなくマシンを再起動します。
データベースに IP アドレスを使用する必要がある。	IP アドレスを変更します。
静的 IP ネットワークで IP アドレスを変更する必要がある。	BI プラットフォームマシンの IP アドレスを変更します。 **ヒント** CMC にログオンして、BI プラットフォームが運用できることを確認します。

> **注意**
>
> アクション実行後はマシンを再起動します。

Web アプリケーションサーバをホストするマシン

条件	アクション
OpenDocument デフォルトビューアの URL に IP アドレスを使用する必要がある。	CMC の [アプリケーション] タブの [処理設定] セクションにある [デフォルトビューアの *URL* の設定] フィールドの IP アドレスを更新します。
ユーザがブラウザで IP アドレスのある URL を使用して BI プラットフォーム Web アプリケーション (CMC など) にアクセスする。	ユーザに新しい IP アドレスを通知します。
Web サービス (Crystal Reports for Java や LiveOffice など) に基づく BI プラットフォームクライアントが IP アドレスを使用する必要がある。	新しい IP アドレスを使用するよう、すべてのクライアントを設定します。

関連情報

新規または既存の CMS データベースの選択 [484 ページ]

11.14.3 マシンの名前変更

BI プラットフォームデプロイメント内のマシンの名前は、マシン上のすべての BI プラットフォームサーバを停止した後にいつでも変更できます。マシンの名前変更におけるベストプラクティスは次のようになります。

条件	アクション
初回のログオンを実行する。	クラスタ名ではなく、CMS マシン名を使用します。
デプロイメントが複数のマシンにある。	名前変更時にすべての他のマシン上のすべての CMS サーバが実行されていることを確認します。

11.14.3.1 サーバ層

> ⓘ 注記
>
> CMS マシンの名前を変更する前に、名前を変更するマシンにあるすべてのサーバの設定を、CMC の [“サーバ管理”] タブで確認します。[ホスト名] プロパティに古い CMS ホスト名が使用されている場合は、新しい CMS ホスト名に更新します。

> → 注意
>
> マシンの名前変更手続きがすべて完了するまでは、サーバを再起動しないでください。

サーバ層のマシンの名前を変更する場合、次の手順に従ってください。

条件	アクション
名前を変更したマシンが CMS をホストし、ユーザはすでに古いマシン名でログインしている。	ユーザに CMS マシン名を通知し、使用を依頼します。

条件	アクション
名前を変更したマシンが CMS をホストし、BI プラットフォーム Web アプリケーションのデフォルトプロパティファイルの `cms.default` プロパティに古い CMS ホスト名が含まれている。	すべての Web Tier マシンのすべてのカスタムプロパティファイルの `cms.default` プロパティで、CMS マシン名を更新します。Tomcat では、作成するプロパティファイルはデフォルトで `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にあります。 **注記** カスタムプロパティファイルがない場合は、新しいカスタムプロパティファイルを作成します。デフォルトのプロパティファイルをカスタムフォルダにコピーし、`cms.default` 行を除くすべてのコンテンツをカスタムプロパティファイルから削除します。
Portal Integration Kits またはカスタムアプリケーションを使用している。	新しい CMS ホスト名を使用するように、Portal Integration Kits またはカスタムアプリケーションを設定します。
デプロイメントが次の条件をすべて満たしている。 • クラスタに複数のノードがある。 • すべての CMS サーバが、名前を変更されたマシンでのみ実行されている。 • 1 つ以上のノードが CMS をホストしていない。 • 1 つ以上のノードがあるマシンの名前を変更する。 • 名前変更中に IP アドレスが変更される。	CCM を使用して、CMS をホストするノードを除くすべてのノードで“ノード再作成”ワークフローを実行し、デプロイメントのすべての BI プラットフォームノードを起動します。詳細については、“ノードの管理”に関する章を参照してください。

→ 注意

アクション実行後、Web アプリケーションまたはアプリケーションサーバを再起動します。

関連情報

ノードの再作成 [457 ページ]

11.14.3.2 Web Tier

BI プラットフォーム Web アプリケーションサーバをホストするマシンの名前を変更する場合、以下の手順に従ってください。

条件	アクション
BI プラットフォーム Web アプリケーションサーバをホストするマシンの名前を変更し、デフォルトの OpenDocument ビューアの URL に Web アプリケーションサーバのホスト名を使用している。	CMC にログオンし、アプリケーション > *CMC* > 処理設置 で、デフォルトビューアの URL を更新します。
BI プラットフォーム Web アプリケーションサーバをホストするマシンの名前を変更し、ユーザが Web アプリケーションサーバのホスト名を含む URL を使用して BI プラットフォーム Web アプリケーションにアクセスしている。	新しい Web アプリケーションサーバのホスト名を含む URL を使用して BI プラットフォーム Web アプリケーションにアクセスすることをユーザに依頼します。
BI プラットフォーム Web アプリケーションサーバをホストするマシンの名前を変更し、Web サービスベースの BI プラットフォームクライアントが URL で Web アプリケーションサーバホスト名を使用している。	新しい Web アプリケーションサーバホスト名を使用するため、Web サービスベースのすべての BI プラットフォームクライアントを再設定します。

11.14.3.3 データベース

CMS システムデータベースまたは監査データベースをホストするマシンの名前を変更する場合、次のベストプラクティスを実践します。

条件	アクション
IP アドレスの更新を回避する。	データソース名 (DSN) に CMS データベースまたは監査データベースのマシン名を使用します。
CMS データベースまたは監査データベースが CMS と同じホストにある。	DSN に `localhost` を使用し、ホスト名変更時の更新を回避します。

CMS システムデータベース

条件	アクション
CMS システムデータベースをホストするマシンの名前を変更し、ODBC を使用している。	CMS データベース DSN を新しいデータベースサーバのホスト名に更新します。
CMS システムデータベースをホストするマシンの名前を変更し、ODBC 以外の接続タイプを使用している。	CCM を使用して、クラスタの全ノードで CMS データベースを新しいデータベースサーバホスト名に更新します。

監査データベース

条件	アクション
監査データベースをホストするマシンの名前を変更し、ODBC を使用している。	監査データベース DSN を更新し、新しいデータベースサーバのホスト名を使用します。

条件	アクション
監査データベースをホストするマシンの名前を変更し、ODBC 以外の接続タイプを使用している。	CMC の [監査] タブで、データベースサーバマシン名を新しいデータベースサーバホスト名に更新します。

11.14.3.4 File Repository Server

FRS ファイルストアをホストするマシンの名前を変更する場合、CMC の [“サーバ管理”] ページで、[*Input File Repository*] サーバと [*Output File Repository*] サーバを更新する必要があります。[ファイル格納ディレクトリ] および [一時ディレクトリ] プロパティで新しいファイル格納パスが使用されていることを確認し、サーバを再起動します。

11.15 32 ビットおよび 64 ビットのサードパーティ製ライブラリの BI プラットフォームでの使用

BI プラットフォームサーバは、32 ビットプロセスと 64 ビットプロセスの組み合わせです。 一部のサーバは、32 ビットおよび 64 ビットの子プロセスを追加で起動します。 サードパーティ製ライブラリの正しいバージョン (32 ビットまたは 64 ビット) を BI プラットフォームプロセスで使用するには、BI プラットフォームをホストするマシンに対して、個別の 32 ビット環境変数および 62 ビット環境変数を設定する必要があります。 次に、追加の環境変数を設定する必要があります。これには、32 ビットおよび 64 ビットバージョンを持つ環境変数のカンマ区切りリストが含まれます。 プロセスが BI プラットフォームによって起動されると、32 ビットまたは 64 ビットプロセスのいずれかに対応して、適切な変数が選択されます。

- `<FIRST_ENV_VAR>` は、64 ビット BI プラットフォームプロセスで使用される値です。
- `<FIRST_ENV_VAR32>` は、32 ビットプロセスで使用される値です。
- `<SECOND_ENV_VAR>` は、64 ビットプロセスで使用される値です。
- `<SECOND_ENV_VAR>` は、32 ビットプロセスで使用される値です。
- BOE_USE_32BIT_ENV_FOR=`<FIRST_ENV_VAR>`,`<SECOND_ENV_VAR>`

たとえば、AIX マシンに BI プラットフォームがインストールされている場合、32 ビットおよび 64 ビット Oracle クライアントと同様に、LIBPATH 変数を設定する必要があります。変数を次のように設定します。

- ORACLE_HOME=`<64 ビットバージョンの Oracle クライアントのホームディレクトリ>`
- ORACLE_HOME32=`<32 ビットバージョンのホームディレクトリ>`
- LIBPATH=`<64 ビットバージョンのライブラリパス>`
- LIBPATH32=`<32 ビットバージョンのライブラリパス>`
- BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH

> **注記**
>
> Linux および Solaris では、BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH を使用して 32 ビットパスと 64 ビットパスを分けないでください。 代わりに、32 ビットパスおよび 64 ビットパスの両方を LD_LIBRARY_PATH に追加します。

11.16 サーバおよびノードのプレースホルダの管理

11.16.1 サーバプレースホルダを表示する

CMC の [サーバ] 管理エリアで、サーバを右クリックして [プレースホルダ] を選択します。
[プレースホルダ] ダイアログに、選択したサーバと同じクラスタ内のすべてのサーバのプレースホルダの一覧が表示されます。プレースホルダの値を変更するには、ノードのプレースホルダを変更します。

関連情報

サーバとノードプレースホルダ [1158 ページ]

11.16.2 ノードのプレースホルダを表示および編集する

1. セントラル管理コンソールの [サーバ] 管理エリアで、プレースホルダを変更するノードを右クリックし、[プレースホルダ] を選択します。
2. プレースホルダの設定を編集するには、適切な変更を行い、[保存] をクリックして続行します。

> **⚠ 警告**
>
> 編集用以外のプレースホルダは、いかなる手段でも変更しないでください。システム管理者は、(ノード管理を目的とする) 管理者グループの適切な担当者のみがノードに対する編集権限を持っていることを確認する必要があります。管理者グループの他のメンバーを含むすべてのユーザは、適切なセキュリティ権限を適用することで、ノードオブジェクトの表示/管理を制限する必要があります。プレースホルダ値のいずれかが誤って破損し、CMS が起動しない場合は、SAP ノート 3269127 を参照してください。

> **ⓘ 注記**
>
> BI ランドスケープへの悪意のある干渉を回避するためにプレースホルダの変更を制限する方法については、以下の SAP Knowledge Base Article 3278916 を参照してください。

関連情報

サーバとノードプレースホルダ [1158 ページ]

12 Central Management Server (CMS) データベースの管理

12.1 CMS システムデータベース接続の管理

ハードウェアやソフトウェアの障害、またはネットワークの問題などで CMS システムデータベースが使用できない場合、CMS は“リソースの待機中です”という状態になります。BI プラットフォームデプロイメントに複数の CMS がある場合、他のサーバのからの以降のリクエストは、システムデータベースとアクティブに接続されているクラスタ内の任意の CMS に移送されます。CMS が“リソースの待機中です”状態である間、データベースアクセスを必要としない現在のリクエストは継続して処理されますが、CMS データベースへのアクセスを必要とするリクエストは失敗します。

デフォルトでは、“リソースの待機中です”状態の CMS は、“必要なシステムデータベース接続”プロパティで指定された接続回数の再確立を定期的に試みます。少なくとも 1 つのデータベース接続が確立されるとすぐに、CMS は、すべての必要なデータを同期化し、“実行中”状態になって、通常の動作を再開します。

CMS でデータベースとの接続が自動的に再確立されないようにする必要がある場合があります。たとえば、データベース接続を再確立する前に、データベースの整合性を検証する必要がある場合です。これを行うには、CMS サーバの [プロパティ] ページで、[システムデータベースへの自動再接続] をオフにします。

関連情報

サーバのプロパティを変更する [439 ページ]

12.1.1 SQL Anywhere を CMS データベースとして選択する

SQL Anywhere を CMS データベースとして使用するには、以下の手順を実行する必要があります。

1. システムですべてのノードを停止します。
2. 適切なアプリケーションを実行します。
   - Unix では、`./cmsdbsetup.sh` を実行します。
   - Windows では、セントラル設定マネージャ (CCM) を開始します。
3. SQL Anywhere をコピー先データベースとして選択し、デフォルトの CMS データベースからデータをコピーします。詳細については、関連するリンク「“CMS データベース間でのデータのコピー”」を参照してください。
4. 複数ノードのデプロイメントでは、データベースのコピー元ノード以外のすべてのノードで CMS データソースを新しい SQL Anywhere データベースに更新します。詳細については、関連するリンク「“新規または既存の CMS データベースの選択”」を参照してください。
5. デプロイメントが稼働していることを確認します (CMC にログインする、レポートを表示するなど)。

関連情報

CMS データベース間でのデータのコピー [488 ページ]
新規または既存の CMS データベースの選択 [484 ページ]

12.1.2 SAP HANA を CMS データベースとして選択する

SAP HANA を CMS データベースとして使用するには、以下の手順を実行する必要があります。

1. BI プラットフォームを、デフォルトの CMS データベースと共にインストールします。
2. SAP HANA クライアントをインストールします。
3. SAP HANA への接続を作成します。
   - Unix 上で、環境変数 `ODBCINI` を確認します。この変数が存在し、既存の `odbc.ini` ファイルを指している場合は、そのファイルに以下の行を追加します。

     ```
     [ODBC Data Sources]
     NewDB=<New_DB_version>
     [NewDB]
     DRIVER=<HANA CLIENT PATH>/libodbcHDB.so
     SERVERNODE=<HANA Server IP address>:<HANA server port #>
     DATABASENAME=<DBNAME>
     DESCRIPTION=<DESCRIPTION>
     ```

     `<New_DB_version>` は SAP HANA バージョン (例: “NewDB 1.0”)、`<HANA Server IP address>` は SAP HANA サーバ IP アドレス、`<HANA server port #>` は SAP HANA サーバポート番号です。`ODBCINI` 環境変数が存在しない場合は、`odbc.ini` ファイルを `<INSTALLDIR>/sap_bobj/enterprise_xi40/` ディレクトリに作成し、そのファイルに上記の行を追加し、以下のように `ODBCINI` 環境変数を設定します。

     ```
     ODBCINI=<INSTALLDIR>/sap_bobj/enterprise_xi40/odbc.ini
     ```

     ODBCINI 環境変数が、BI サーバを起動するユーザのプロファイルで設定されていることを確認します。
   - Windows では、SAP HANA への ODBC 接続を作成します。

     > **注記**
     > ODBC 接続変更の場合、必ず ODBC データソースアドミニストレータの 64 ビットバージョンを実行してください。スタート > コントロール パネル > 管理ツール > データソース *(ODBC)* を選択します。

4. SAP HANA サーバに接続できることを確認します。
   - Unix では、以下のコマンドを実行して、SAP HANA サーバへの接続をテストできます。以下の例の各変数は、SAP HANA インストールを参照するものです。

     ```
     <INSTALLDIR>/odbcreg <SERVER>:<HDBINDEXSERVERPORT> <SYSTEMID>
     <NONADMINUSER> <NONADMINPASSWORD>
     ```

   - Windows では、ODBC データソースアドミニストレータを使用して、SAP HANA ODBC 接続をテストできます。

5. Unix では、`LD_LIBRARY_PATH` または `LIBPATH` 環境変数に `libodbcHDB.so` へのパスが含まれていることを確認します。詳細については、2792543、1886746、および 2721890 を参照してください。
6. ウィザードに従って製品をインストールし、CMS/監査データベースとして SAP HANA を選択します。
7. デプロイメントが稼働していることを確認します (CMC にログインする、レポートを表示するなど)。

> **注記**
>
> 既存のデータベースから SAP HANA データベースへのデータベース移動時には、この手順が適用されません。その場合は、データソースのコピー手順に従います。詳細については、CMS データベース間でのデータのコピー [488 ページ]を参照してください。

関連情報

CMS データベース間でのデータのコピー [488 ページ]
新規または既存の CMS データベースの選択 [484 ページ]

12.2 新規または既存の CMS データベースの選択

CCM または `cmsdbsetup.sh` を使用して、ノードの新しいまたは既存の CMS システムデータベースを指定できます。この手順を実行する状況は 2 ～ 3 の場合に限られます。

- 現在の CMS システムデータベースのパスワードを変更した場合は、この手順によって現在のデータベースから切断して、再び接続できます。指示に従って、CMS に新しいパスワードを指定できます。
- BI プラットフォーム用に空のデータベースを選択して初期化する場合は、この手順によって新しいデータソースを選択できます。
- バックアップから CMS システムデータベースを (標準のデータベース管理ツールおよび手順を使用して) 復元した結果、元のデータベース接続が無効になった場合、復元したデータベースに CMS を再び接続する必要があります(たとえば、新しくインストールしたデータベースサーバに元の CMS データベースを復元した場合)。

> **注記**
>
> IBM DB2 を CMS データベースとして使用しており、9.5 FixPack 5 より前のバージョンから 9.5 FixPack 5 または 9.5 ラインのそれ以降のバージョンにアップグレードする場合、あるいは 9.7 FixPack 1 より前のバージョンから 9.7 FixPack 1 または 9.7 ラインのそれ以降のバージョンにアップグレードする場合は、BI プラットフォームノードまたは CMS の次回の再起動中に、CMS によって CMS データベーススキーマが自動的に更新され、HADR 互換スキーマがサポートされるようになります。
>
> この処理は長くかかる場合があり、その間は BI プラットフォームシステムを使用することはできません。CMS データベースの破損を防ぐために、この更新プロセスを中断しないでください。この操作を実行する前に CMS データベースをバックアップしておくことを強くお勧めします。また、9.5 ラインの 9.5 FixPack 5 より前のバージョン、または 9.7 ラインの 9.7 FixPack 1 より前のバージョンの IBM DB2 CMS データベースでは、IBM HADR を使用しないでください。

> **注記**
>
> システムコピーのワークフローを実行する場合を除き、異なるクラスタに属する CMS システムデータベースを使用するように、BI プラットフォームインストールを設定しないでください。
>
> BI プラットフォームインストールおよび CMS データベースのバージョンまたはパッチレベルが異なる場合、インストールパスが異なる場合、または、インストールされているコンポーネントが異なる場合などには、システム障害が発生する可能性があります。
>
> システム障害を回避するには、BI プラットフォームデプロイメントを、別の BI プラットフォームシステム (特に、異なるバージョンおよびパッチレベルの内の 1 つ) の CMS データベースをポイントすることにより、BI コンテンツを 1 つのシステムから別のシステムに移行しようとしないでください。

> **注記**
>
> Business Intelligence プラットフォームでは、CMS と CMS データベースや監査データベースなどのデータベースの間の SSL 通信がサポートされます。SSL 通信の場合は、以下のようになります。
>
> - SQL Anywhere、SQL Server、および SAP HANA データベースを CMS または監査データベースとして使用し、CMS と安全に通信する必要があります。
> - 各データベースサーバで SSL を有効にする必要があります。使用しているデータベース用のドキュメントを参照してください。
> - ODBC 接続を作成し、その ODBC 接続を介して DB サーバ証明書を渡す必要があります。
> - CMS データベースへの接続と監査データベースへの接続には、同じ ODBC 接続を使用する必要があります。

12.2.1 Windows で新しいまたは既存の CMS データベースを選択する

1. CCM を使用して Server Intelligence Agent (SIA) を停止します。
2. SIA を選択して、[*CMS データソースの指定*] ボタンをクリックします。
3. [データソース設定の更新] を選択して、[*OK*] をクリックします。
4. データベースドライバを選択し、[*OK*] をクリックします。
5. これらの手順は、選択した接続の種類によって異なります。
   - ODBC を選択した場合、Windows の［“データ ソースの選択”］ダイアログ ボックスが表示されます。CMS データベースとして使用する ODBC データソースを選択して、[*OK*] をクリックします。新しい DSN を設定する場合は [新規] をクリックします。指示に従って、データベースの認証情報を入力して［*OK*］をクリックします。
   - ネイティブ ドライバを選択した場合は、データベースのサーバー名、ログイン ID、およびパスワードの入力を要求されます。この情報を入力して、［*OK*］をクリックします。
6. クラスタキーを指定します。
7. Server Intelligence Agent を再起動します。

12.2.2 UNIX で新しいまたは既存の CMS データベースを選択する

`cmsdbsetup.sh` スクリプトを使用します。 詳細については、*BI* プラットフォーム管理者ガイドのコマンドライン管理の章で、“Unix スクリプト”のトピックを参照してください。

1. `cmsdbsetup.sh` スクリプトを実行します (デフォルトで `<INSTALLDIR>/sap_bobj/` に配置されています)。
2. 更新アクション (オプション 6) を選択します。
3. プロンプトが表示されたら、新しい CMS データベースのデータベースタイプを指定します。
4. データベース情報 (ホスト名、ユーザ名、パスワード、クラスタキーなど) を指定します。
   CMS データベースが新しい場所に指定されると、通知メッセージが表示されます。
5. Server Intelligence Agent (SIA) の再ビルドを要求するプロンプトが表示された場合は、管理者パスワードと、CMS で通信に使用するポート番号を指定します。

> **注記**
>
> 空の CMS データベースを指定した場合にのみ、この情報の入力が要求されます。

関連情報

Unix スクリプト [1049 ページ]

12.3 CMS システムデータベースの再作成

この手順では、現在の CMS システムデータベースを作成し直す (初期化し直す) 方法を示します。 このタスクを実行すると、データベースの既存データがすべて削除されます。 この手順は、独自のカスタム Web アプリケーションの設計およびテストを行う開発環境に BI プラットフォームをインストールしている場合などに便利です。 システムのデータをすべてクリアする必要があるたびに、開発環境の CMS システムデータベースを初期化し直すことができます。

> **警告**
>
> このワークフローにまとめられている手順を実装すると、CMS データベース内のすべてのデータに加え、レポートやユーザなどのオブジェクトも削除されます。 実稼動デプロイメントでは、これらの手順を実行しないでください。

CMS システムデータベースを初期化し直す前に、すべてのサーバ設定情報をバックアップすることが非常に重要です。 データベースを再作成するときは、サーバ設定が消去されるため、この情報を復元するにはバックアップが必要になります。

システムデータベースを再作成するときは、既存のライセンスキーがデータベース内に維持される必要があります。 ただし、ライセンスキーの再入力が必要な場合は、デフォルトの Administrator アカウントで CMC にログオンします。 [認証]管理エリアを表示して、[ライセンスキー]タブに情報を入力します。

> ⓘ 注記
>
> CMS システムデータベースを初期化し直すと、現在の CMS システムデータベース内のすべてのデータが破棄されます。 作業を実行する前に、現在のデータベースのバックアップを行うことを検討してください。 必要に応じて、データベース管理者に連絡してください。

関連情報

サーバの設定のバックアップ [537 ページ]

12.3.1 Windows で CMS システムデータベースを作成し直す

1. CCM を使用して Server Intelligence Agent (SIA) を停止します。

   > ⓘ 注記
   >
   > この手順では、CCM をリモートマシンで実行することはできません。CCM は、1 つ以上の有効なノードが存在するマシンで実行する必要があります。また、CMS バイナリもこのマシンにインストールする必要があります。

2. SIA を右クリックし、[プロパティ]を選択します。
3. [プロパティ] ダイアログボックスの [設定] タブで、[指定] をクリックします。
4. [*CMS データベースのセットアップ*]ダイアログボックスで、[現在のデータソースを再作成します]をクリックします。

   > ⓘ 注記
   >
   > 手順 1 で CCM を実行したマシンからサーバとオブジェクトも再作成されます。ただし、すべてのオブジェクトが再作成されるわけではなく、主要なデフォルトオブジェクトのみ再作成されます。たとえば、サンプルレポートは再作成されません。

5. [*OK*]をクリックし、確認を求められたら[はい]をクリックします。
6. CMS システムデータベースのパスワードを指定し、[*OK*] をクリックします。

   > ⓘ 注記
   >
   > 必ず、新しい管理者パスワードを設定してください。デフォルトでは、管理者アカウントにはパスワードがありません。

   CCM により、CMS システムデータベースセットアップの完了が通知されます。
7. [*OK*]をクリックします。

   CCM に戻ります。
8. Server Intelligence Agent を再起動し、サービスを有効にします。

   Server Intelligence Agent の起動中に、それによって CMS が起動されます。CMS は新しく空になったデータソースに必要なシステムデータを書き込みます。

9. デプロイメントに複数のマシンがある場合は、他のマシンでノードを再作成する必要があります。

12.3.2 UNIX 上で CMS システムデータベースを再作成する

`cmsdbsetup.sh` スクリプトを使用します。 詳細については、*BI プラットフォーム管理者ガイド*のコマンドライン管理の章で、“Unix スクリプト”のトピックを参照してください。

1. `cmsdbsetup.sh` を実行します (デフォルトで `<INSTALLDIR>/sap_bobj/` に配置されています)。
2. "再初期化" オプション (オプション 5) を選択し、選択内容を確認します。
   `cmsdbsetup.sh` スクリプトによって、CMS システムデータベースの再作成が開始されます。
3. CMS システムデータベースのパスワードを入力します。
4. データベースの作成が完了したら、`cmsdbsetup.sh` スクリプトを終了します。
5. データベース情報 (ホスト名、ユーザ名、パスワードなど) を指定します。
   CMS データベースが新しい場所に指定されると、通知メッセージが表示されます。
6. Server Intelligence Agent (SIA) の再ビルドを要求するプロンプトが表示された場合は、管理者パスワードと、CMS で通信に使用するポート番号を指定します。

   > ⓘ 注記
   >
   > 空の CMS データベースを指定した場合にのみ、この情報の入力が要求されます。

7. `<INSTALLDIR>/sap_bobj/` ディレクトリで、次のコマンドを使用してノードを起動します。

   ```
   ccm.sh -start <nodename>
   ```

8. サービスを有効にするには、次のコマンドを使用します。

   ```
   ccm.sh -enable all -cms <CMSNAME:PORT> -username administrator -password
   <password>
   ```

   > ⓘ 注記
   >
   > CMS データベースを再作成したばかりであるため、管理者パスワードは空になっています。

関連情報

Unix スクリプト [1049 ページ]

12.4 CMS データベース間でのデータのコピー

セントラル設定マネージャ (CCM) または `cmsdbsetup.sh` を使用して、データベースサーバのシステムデータを別のデータベースサーバにコピーできます。たとえば、データベースをアップグレードするかデータベースの種類を変更するため、別のデータベースで置き換える場合は、既存のデータベースを廃棄する前にそのコンテンツを新しいデータベースにコピーできます。

出力先データベースは、新しいデータがコピーされる前に初期化されるため、出力先データベースの既存の内容は削除され、復元不可能になります。BI プラットフォームテーブルはすべて削除され復元不可能になり、次に再作成されます。データがコピーされると、出力先データベースが CMS の現在のデータベースとして設定されます。

> ⚠ 警告
>
> 他の BI プラットフォームクラスタの CMS データベースを使用しないでください。このワークフローを開始する前に、ソース CMS データベースがこの BI プラットフォームクラスタで使用されていたものであり、他の BI プラットフォームクラスタでは使用されていなかったことを確認してください。

> ⚠ 警告
>
> CMS データベースコピーワークフローを使用してアップグレードを実行しないでください。CMS データベースコピーワークフローは、CMS データベースをあるデータベースサーバから別のデータベースサーバに移動するように設計されています。CMS データベースのアップグレードは対象ではありません。このワークフローを開始する前に、ソース CMS データベースがこの BI プラットフォームクラスタで使用されていたものであり、現在の BI プラットフォームインストールと同じバージョンおよびパッチレベルであることを確認してください。

12.4.1 CMS システムデータベースのコピーの準備

CMS システムデータベースをコピーする前に、すべてのサーバを無効にし、さらに停止することによって、インポート元の環境とインポート先の環境をオフラインにします。両方の CMS データベースをバックアップし、すべての Input File Repository Server と Output File Repository Server によって使用されるルートディレクトリをバックアップします。必要に応じて、データベース管理者またはネットワーク管理者に連絡してください。

ソースデータベースのすべてのデータに対する読み取り権限があるデータベースユーザアカウントと、出力先データベースに対する作成、削除、および更新のアクセス権があるデータベースユーザアカウントを持っていることを確認します。置換するデータベースの CMS マシンから、自分の設定に応じてデータベースクライアントソフトウェアまたは ODBC を使用して、両方のデータベースに接続できることを確認します。

CMS データベースを現在の場所から別のデータベースサーバにコピーする場合、現在の CMS データベースがインポート元の環境ということになります。データベースの内容がコピーされると、出力先データベースが現在の CMS のアクティブなデータベースとして設定されます。この手順は、デフォルトの CMS データベースを、既存のデフォルトデータベースから Microsoft SQL Server、Informix、Oracle、DB2、Sybase などの専用データベースサーバに移動する場合に当てはまります。移動するデータベースが格納されている CMS を実行しているマシンに、管理アカウントでログオンします。

> ⓘ 注記
>
> あるデータベースから別のデータベースにデータをコピーする場合、新しいデータがコピーされる前に、出力先データベースが初期化されます。つまり、出力先のデータベースに BI プラットフォームシステムテーブルが含まれていない場合、それらのテーブルが作成されます。出力先のデータベースに BI プラットフォームシステムテーブルが含まれている場合は、それらのテーブルが完全に削除されてから新しいシステムテーブルが作成され、移行元データベースから新しいテーブルにデータがコピーされます。データベースの他のテーブルは影響を受けません。

> ⓘ 注記
>
> CMS システムデータベースを Windows 上の MaxDB 出力先データベースにコピーする場合は、MaxDB クライアントへのパスが <PATH> 環境変数に追加されていることを確認する必要があります。たとえば、`;C:¥Program Files¥sdb¥MAXDB1¥pgm` です。

12.4.2 Windows で CMS システムデータベースをコピーする

CMS データベースの内容をコピーする前に、テーブルを追加または削除したり、それらのテーブルでデータを追加、削除、変更するための権限を持つアカウントでコピー先のデータベースにログオンできることを確認してください。

1. セントラル設定マネージャ (CCM) を開き、Server Intelligence Agent (SIA) を停止します。
2. SIA を右クリックし、[プロパティ]を選択します。
3. [設定]タブをクリックし、[指定]をクリックします。
4. [コピー]を選択し、[*OK*]をクリックします。
5. コピー元の CMS データベースの種類を選択し、ホスト名、ユーザ名、パスワードを含むデータベース情報を指定します。
6. コピー先の CMS データベースの種類を選択し、ホスト名、ユーザ名、パスワードを含むデータベース情報を指定します。
7. CMS データベースのコピーが完了したら、[*OK*]をクリックします。

12.4.3 UNIX 上の CMS システムデータベースからデータをコピーする

CMS データベースの内容をコピーする前に、テーブルを追加または削除したり、それらのテーブルでデータを追加、削除、変更するための権限を持つアカウントでコピー先のデータベースにログオンできることを確認してください。

> ⓘ 注記
>
> UNIX 上では、CMS データベースへの ODBC 接続を使用している移行元環境から直接移行することはできません。移行元の CMS データベースが ODBC を使用している場合は、まず、そのシステムを、サポートされているネイティブドライバに移行する必要があります。

1. 次のコマンドを入力して、CMS を停止します。

   ```
   /ccm.sh -stop <nodename>
   ```

2. `cmsdbsetup.sh` を実行します (デフォルトで `<INSTALLDIR>/sap_bobj/` に配置されています)。
3. “コピー”オプション (オプション 4) を選択し、選択内容を確認します。
4. コピー元の CMS データベースの種類を選択し、ホスト名、ユーザ名、パスワードを含むデータベース情報を指定します。
5. コピー先の CMS データベースの種類を選択し、ホスト名、ユーザ名、パスワードを含むデータベース情報を指定します。

CMS データベースがコピー先のデータベースにコピーされます。コピーが完了すると、メッセージが表示されます。

12.5 Central Management Server データベースドライバ

既存のプラットフォーム機能 (Connection Server、セマンティックレイヤ、レポートクライアント) を利用するレポート分析のために、BI プラットフォームの CMS リポジトリデータベースにアクセスすることができるようになりました。SAP BusinessObjects データアクセスドライバを使用すると、ユニバースを使用して CMS データベースをクエリすることができます。詳細については、http://scn.sap.com/docs/DOC-74580 を参照してください。

13 Web アプリケーションコンテナサーバ (WACS) の管理

13.1 WACS

13.1.1 Web アプリケーションコンテナサーバ (WACS)

Web アプリケーションコンテナサーバ (WACS) は、SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションをホストするためのプラットフォームです。たとえば、セントラル管理コンソール (CMC)を WACS でホストできます。

WACS を使用すると、以前はアプリケーションサーバの設定や Web アプリケーションのデプロイに必要だったいくつかのワークフローが不要になり、簡略化された一貫性のある管理インタフェイスが提供されるため、システム管理が容易になります。

Web アプリケーションは WACS に自動的にデプロイされます。WACS では、BI プラットフォームや外部 Web アプリケーションの手動デプロイメントまたは WDeploy デプロイメントはサポートされません。

13.1.1.1 WACS の必要性

SAP BusinessObjects Web アプリケーションのホストに Java アプリケーションサーバを使用しない場合、WACS でホストすることができます。

サポートされている Java アプリケーションサーバを使用して BI プラットフォーム Web アプリケーションをデプロイする場合、または UNIX システムに BI プラットフォームをインストールする場合は、WACS をインストールして使用する必要はありません。

13.1.1.2 WACS を使用する利点

WACS を使用して CMC をホストすると、次のような多くの利点があります。

- WACS のインストール、管理、設定は最小限の作業で済みます。
- ホストされているすべてのアプリケーションは WACS に事前にデプロイされるため、追加の手動手順は不要です。
- WACS は、SAP によりサポートされています。
- WACS では、Java アプリケーションサーバの管理および保守に関するスキルは不要です。
- WACS には、他の BI プラットフォームサーバと一貫性のある管理インタフェースが用意されています。

13.1.1.3 共通タスク

タスク	説明	トピック
WACS でホストされている Web アプリケーションまたは Web サービスのパフォーマンスの改善方法	Web アプリケーションまたは Web サービスのパフォーマンスは、複数のマシン上に WACS をインストールすることにより改善できます。	• デプロイメントへの WACS の追加または削除 [494 ページ] • Web アプリケーションコンテナサーバのクローン [496 ページ]
Web Tier の可用性を向上させる	デプロイメントに追加の WACS を作成し、あるサーバでハードウェアまたはソフトウェアの障害が発生した場合に別のサーバが要求の処理を続行できるようにします。	デプロイメントへの WACS の追加または削除 [494 ページ]
誤って設定した CMC から容易に復旧できる環境を構築する	2 つ目の停止状態の WACS を作成し、この WACS を使用して設定テンプレートを定義します。プライマリ WACS を誤って設定した場合に、最初のサーバを設定するか設定テンプレートを最初のサーバに適用するまで 2 つ目の WACS を使用します。	デプロイメントへの WACS の追加または削除 [494 ページ]
クライアントと WACS 間の通信のセキュリティを強化する	WACS の HTTPS を設定します。	• HTTPS/SSL の設定 [499 ページ] • WACS とファイアウォールの併用 [523 ページ]
WACS とデプロイメントの他の BI プラットフォームサーバ間の通信のセキュリティを強化する	WACS とデプロイメントの他の BI プラットフォームサーバ間の SSL 通信を設定します。	• バックエンドサーバの SSL 設定 [174 ページ] • WACS とファイアウォールの併用 [523 ページ]
WACS を HTTPS およびリバースプロキシと併用する	2 つの WACS を作成し、両方のサーバに HTTPS を設定すると、WACS を HTTPS およびリバースプロキシと併用できます。最初の WACS を内部ネットワーク内の通信に使用し、もう一方の WACS をリバースプロキシ経由の外部ネットワークとの通信に使用します。	リバースプロキシを使用した HTTPS をサポートするように WACS を設定する [523 ページ]
WACS を IT 環境に適合させる	WACS は、既存の Web サーバ、ハードウェアロードバランサ、リバースプロキシ、およびファイアウォールを含む IT 環境にデプロイできます。	• WACS と他の Web サーバの併用 [522 ページ] • WACS とロードバランサの併用 [522 ページ] • WACS とリバースプロキシの併用 [522 ページ] • WACS とファイアウォールの併用 [523 ページ]
ロードバランサを含むデプロイメントで WACS を使用する	ハードウェアロードバランサを使用するデプロイメントで WACS を使用でき	WACS とロードバランサの併用 [522 ページ]

タスク	説明	トピック
	ます。WACS 自体をロードバランサとして使用することはできません。	
リバースプロキシを含むデプロイメントで WACS を使用する	リバースプロキシを使用するデプロイメントで WACS を使用できます。WACS 自体をリバースプロキシとして使用することはできません。	WACS とリバースプロキシの併用 [522 ページ]
WACS サーバのトラブルシューティングを行う	WACS のパフォーマンスが低い理由または原因を特定する必要がある場合は、ログファイルを表示したりシステムメトリクスを表示したりできます。	• WACS にトレースを設定する [525 ページ] • サーバメトリクスを表示する [525 ページ]
特定のポートでページが表示されない場合の理由	WACS に接続できない理由はいくつか考えられます。以下を確認してください。 • WACS 用に指定した HTTP、プロキシ経由の HTTP、および HTTPS ポートが他のアプリケーションで使用されていないこと。 • WACS に十分なメモリが割り当てられていること。 • WACS で十分な同時要求を処理できること。 • 必要に応じて、WACS のシステムデフォルトを復元します。	• HTTP ポートの競合を解決する [526 ページ] • メモリ設定を変更する [527 ページ] • 同時要求の数を変更する [528 ページ] • システムデフォルトを復元する [528 ページ]
WACS でホストされている Web アプリケーションのプロパティの設定方法	Web アプリケーションのプロパティの設定手順は、特定のプロパティおよび Web アプリケーションによって異なります。詳細については、章内の「“Web アプリケーションプロパティの設定”」の節を参照してください。	Web アプリケーションプロパティの設定 [524 ページ]
WACS プロパティの一覧を確認できる場所	WACS プロパティの一覧は、このガイドの“サーバのプロパティに関する付録”に記載されています。	コアサービスのプロパティ [1110 ページ]

13.1.2 デプロイメントへの WACS の追加または削除

デプロイメントに WACS を追加すると、次のような利点が得られます。

- 誤って設定したサーバから迅速に復旧できます。
- サーバの可用性が向上します。
- 負荷分散がより適切に行われます。
- 全体のパフォーマンスが向上します。

デプロイメントに WACS を追加するには、次の 3 とおりの方法があります。

- WACS をマシンにインストールします。
- 新しい WACS を作成します。
- WACS をクローンします。

> **注記**
>
> 多くのリソースが消費されるため、WACS は同じマシンで同時に 1 つのみ実行することをお勧めします。ただし、WACS を誤って設定した場合に容易に復旧できるように、同じマシンに複数の WACS をデプロイし、その中の 1 つだけを実行することもできます。

13.1.2.1 WACS のインストール

WACS を別々のマシンにインストールすると、デプロイメントのパフォーマンスが向上し、負荷分散がより適切に行われ、サーバの可用性も向上します。別々のマシンにインストールされた複数の WACS がデプロイメントに含まれている場合は、特定のマシンでハードウェアやソフトウェアの障害が発生しても、他の WACS が CMC サービスを引き継ぐため、Web アプリケーションや Web サービスが利用できなくなることはありません。

Web アプリケーションコンテナサーバをインストールするには、BI プラットフォームインストールプログラムを使用します。WACS のインストールには次の 2 つの方法があります。

- フルインストールの場合、*Java Web アプリケーションサーバの選択*画面で *Web アプリケーションコンテナサーバをインストールし、Web アプリケーションを自動でデプロイします*を選択します。
  新規インストールで Java アプリケーションサーバを選択した場合、WACS はインストールされません。
- カスタムまたは拡張インストールでは、▶ サーバ ▶ *Platform Services* ▶ を選択し、*Web アプリケーションコンテナサーバ*を選択して、機能の選択画面で WACS をインストールするよう選択できます。

WACS をインストールすると、インストール プログラムによって自動的に `<NODE>.WebApplicationContainerServer` という名前のサーバが作成されます。`<NODE>` はノード名です。BI プラットフォーム Web アプリケーションおよび Web サービスがサーバにデプロイされます。CMC をデプロイまたは設定するのに手動による手順は必要ありません。これでシステムを使用できるようになりました。

WACS をインストールするときに、WACS の HTTP ポート番号の入力を求められます。使用されていないポート番号を指定します。デフォルトのポート番号は 6405 です。ユーザにファイアウォールの外部から WACS に接続することを許可する場合は、サーバの HTTP ポートがファイアウォールで開いていることを確認する必要があります。

> **注記**
>
> WACS がホストする Web アプリケーションは、WACS のインストール時、または更新やホットフィックスを WACS や WACS がホストする Web アプリケーションに適用すると自動的にデプロイされます。Web アプリケーションのデプロイには数分かかります。Web アプリケーションのデプロイメントが完了するまで、WACS は“初期化中”状態になります。Web アプリケーションが完全にデプロイされるまで、WACS でホストされている Web アプリケーションにアクセスすることはできません。初期デプロイメントが完了するまで、サーバを停止しないでください。セントラル設定マネージャ(CCM)を通じて、WACS のサーバ状態を表示できます。
>
> この遅延は、WACS のインストール後初めて WACS を起動するとき、または WACS に更新を適用したときにのみ発生します。この遅延は、以降の WACS の再起動では発生しません。
>
> Web アプリケーションは、WACS サーバに手動でデプロイすることはできません。WDeploy を使用して Web アプリケーションを WACS にデプロイすることはできません。

13.1.2.2 新しい Web アプリケーションコンテナサーバの追加

> **注記**
>
> 多くのリソースが消費されるため、WACS は同じマシンで同時に 1 つのみ実行することをお勧めします。ただし、WACS を誤って設定した場合に容易に復旧できるように、同じマシンに複数の WACS をデプロイし、その中の 1 つだけを実行することもできます。

1. CMC の[サーバ]管理エリアを表示します。
2. 管理 > 新規 > 新しいサーバ を選択します。
   [新規サーバ名]画面が表示されます。
3. [サービスカテゴリ]リストから[コアサービス]を選択します。
4. [サービスの選択] リストから、WACS でホストするサービスを選択し、[次へ] をクリックします。
   - WACS で CMC、BI ラウンチパッド、OpenDocument のような Web アプリケーションをホストするには、[*BOE Web アプリケーションサービス*] を選択します。
   - Live Office または Query as a Web Service (QaaWS) などの Web サービスを WACS でホストするには、[*Web サービス SDK および QaaWS サービス*] を選択します。
   - ビジネスプロセス BI Web サービスを WACS でホストするには、[*ビジネスプロセス BI Web サービス*] を選択します。
5. 次の [新規サーバ名] 画面で、WACS でホストする追加のサービスを選択し、[次へ] をクリックします。
6. 次の [サーバの作成] 画面で、サーバを追加するノードを選択し、サーバ名、およびサーバの説明を入力して [作成] をクリックします。

   > **注記**
   >
   > [ノード]リストには、WACS がインストールされているノードだけが表示されます。

7. [サーバ] 画面で、新しい WACS をダブルクリックします。
   [プロパティ] 画面が表示されます。
8. システムの再起動時に WACS が自動的に起動しないようにするには、[共通設定] 枠の [*Server Intelligence Agent の起動時にこのサーバを自動的に起動します*] チェックボックスをオフになっていることを確認します。
9. *[保存して閉じる]*をクリックします。

新しい WACS が作成されます。サーバにはデフォルトの設定とプロパティが適用されます。

13.1.2.3 Web アプリケーションコンテナサーバのクローン

デプロイメントに新しい WACS を追加する代わりに、同じマシンまたは別のマシンに WACS をクローンすることもできます。新しい WACS を追加するとデフォルト設定でサーバが作成されますが、WACS をクローンすると、クローン元の WACS の設定が新しい WACS に適用されます。

サーバは、すでに WACS がインストールされているマシンにのみクローンできます。

> ⓘ 注記
>
> 多くのリソースが消費されるため、WACS は同じマシンで同時に 1 つのみ実行することをお勧めします。ただし、WACS を誤って設定した場合に容易に復旧できるように、同じマシンに複数の WACS をデプロイし、その中の 1 つだけを実行することもできます。

1. CMC の[サーバ]管理エリアを表示します。
2. クローンする WACS を選択し、右クリックして[クローンサーバ]を選択します。

   [クローンサーバ]画面にデプロイメントのノードのリストが表示されます。これらのノードに WACS をクローンできます。[ノードに複製]リストには、WACS がインストールされているノードだけが表示されます。
3. [クローンサーバ]画面で、新しいサーバ名を入力し、サーバをクローンするノードを選択して[*OK*]をクリックします。

新しい WACS が作成されます。新しいサーバには、そのクローン元のサーバと同じサービスが含まれます。新しいサーバとそのサーバがホストするサービスの設定は、サーバ名を除いてクローン元のサーバと同じです。

> ⓘ 注記
>
> WACS を同じマシンにクローンした場合は、クローンに使用した WACS とポートが競合することがあります。その場合は、新しくクローンした WACS インスタンスのポート番号を変更する必要があります。

関連情報

HTTP ポートの競合を解決する [526 ページ]

13.1.2.4 デプロイメントからの WACS の削除

サーバで現在 CMC サービスが実行されていない場合にのみ WACS を削除できます。デプロイメントから WACS を削除する場合は、別の WACS または Java アプリケーションサーバから CMC にログオンする必要があります。現在 CMC サービスを実行している WACS は削除できません。

1. CMC の[サーバ]管理エリアを表示します。
2. 削除するサーバを右クリックし、[サーバの停止]をクリックして、サーバを停止します。
3. サーバを右クリックし、[削除]を選択します。
4. 確認を求めるメッセージが表示されたら、[*OK*]をクリックします。

13.1.3 WACS に対するサービスの追加または削除

13.1.3.1 WACS に Web アプリケーションまたは Web サービスを追加する

BI プラットフォーム Web アプリケーションまたは Web サービスを WACS に追加するには、WACS を停止する必要があります。したがって、サービスを停止し、他の WACS へ追加している間は、BOE Web アプリケーションサービスを提供する、デプロイメントの WACS でホストされている追加の CMC が最低 1 つ必要になります。

WACS にサービスを追加すると、サーバの再起動時にサービスが自動的に WACS にデプロイされます。

1. CMC の[サーバ]管理エリアを表示します。
2. サービスを追加する WACS をダブルクリックし、サーバのプロパティを表示して、追加するサービスがまだ存在しないことを確認します。
3. [キャンセル] をクリックして、[サーバ] 画面に戻ります。
4. サーバを右クリックし、[サーバの停止]をクリックして、サーバを停止します。

   現在 CMC サービスを実行している WACS を停止しようとすると、警告メッセージが表示されます。デプロイメントの他の WACS で少なくとも 1 つの 別の BOE Web アプリケーションサービスが実行されていない場合は、次に進まないでください。別の CMC が実行されている場合は、[*OK*]をクリックし、WACS にログオンして、この手順を最初からやり直します。
5. サーバを右クリックし、[サービスの選択] を選択します。
   [サービスの選択]画面が表示されます。
6. サーバに追加するサービスを選択し、[>]をクリックしてサービスをサーバに追加し、[*OK*]をクリックします。
7. サーバを右クリックし、[サーバの起動]をクリックして、WACS を起動します。

サービスが WACS に追加されます。サービスのデフォルトの設定とプロパティが適用されます。

13.1.3.2 WACS から Web アプリケーションまたは Web サービスを削除する

WACS から Web アプリケーションまたは Web サービスを削除する場合は、別の WACS または Java アプリケーションサーバから CMC にログオンする必要があります。現在 CMC サービスを実行している WACS は停止できません。

WACS から最後の CMC サービスを削除することはできません。したがって、WACS から Web サービスを削除する場合は、サーバが最低 1 つのサービスをホストとしていることを確認する必要があります。

WACS から最後のサービスを削除する場合は、WACS 自身を削除します。

1. CMC の[サーバ]管理エリアを表示します。
2. Web サービスを削除する WACS をダブルクリックし、サーバのプロパティを表示して、削除する Web サービスがまだ存在することを確認します。
3. [キャンセル] をクリックして、[サーバ] 画面に戻ります。
4. サーバを右クリックし、[サーバの停止]をクリックして、WACS を停止します。

   現在 CMC サービスを実行している WACS を停止しようとすると、警告メッセージが表示されます。デプロイメントの他の WACS で少なくとも 1 つの 別の BOE Web アプリケーションサービスが実行されていない場

合は、次に進まないでください。別の CMC が実行されている場合は、[*OK*]をクリックし、WACS にログオンして、この手順を最初からやり直します。

5. WACS を右クリックし、[サービスの選択] を選択します。
   [サービスの選択]画面が表示されます。
6. 削除するサービスを選択し、[<] をクリックしてから、[*OK*] をクリックします。
7. サーバを右クリックし、[サーバの起動]をクリックして、WACS を起動します。

サービスが WACS から削除されます。

13.1.4 HTTPS/SSL の設定

BI プラットフォームデプロイメントのクライアントと WACS の間で行われるネットワーク通信について、Secure Sockets Layer (SSL) プロトコルと HTTP を使用できます。SSL/HTTPS を使用すると、ネットワークトラフィックが暗号化され、セキュリティが強化されます。

SSL には、次の 2 種類があります。

- WACS やデプロイメント内の他の BI プラットフォームサーバなどの、BI プラットフォームサーバ間で使用される SSL。これは、CORBA SSL と呼ばれます。デプロイメントの BI プラットフォームサーバ間での SSL の使用については、*SAP BusinessObjects Business Intelligence* プラットフォーム管理者ガイドの“BI プラットフォームコンポーネント間の通信について”の節を参照してください。
- WACS および WACS と通信するクライアント(ブラウザなど)間で使用される HTTP over SSL。

> ⓘ 注記
>
> プロキシまたはリバースプロキシを含むデプロイメントに WACS をデプロイし、SSL を使用してネットワーク通信を保護する場合は、2 つの WACS を作成する必要があります。詳細については、*WACS とリバースプロキシの併用*を参照してください。

WACS の HTTPS/SSL を設定するには、次の手順を完了する必要があります。

- 証明書と秘密鍵が格納される PKCS12 証明書ストアまたは JKS キーストアを生成するか取得します。Microsoft のインターネットインフォメーションサービス(IIS)と Microsoft 管理コンソール(MMC)を使用して PCKS12 ファイルを生成するか、openssl または Java Keytool コマンドラインツールを使用してキーストアファイルを生成できます。
- 特定のクライアントでのみ WACS に接続する場合は、証明書信頼リストファイルを生成する必要があります。
- 証明書ストアと証明書信頼リストファイル(必要な場合)がある場合は、ファイルを WACS マシンにコピーします。
- WACS の HTTPS を設定します。

関連情報

BI プラットフォームコンポーネント間の通信について [184 ページ]
WACS とリバースプロキシの併用 [522 ページ]

13.1.4.1 PKCS12 証明書ファイルストアを生成する

PKCS12 証明書ファイルストアまたは Java キーストアを生成する方法や使用できるツールは多数あります。生成方法は、使用できるツールや使い慣れたツールによって決まります。

次の例では、Microsoft のインターネットインフォメーションサービス (IIS) と Microsoft 管理コンソール (MMC) を使用して Windows Server 2008 用の PKCS12 ファイルを生成する方法を示します。

1. WACS をホストとしているマシンに Administrator としてログオンします。
2. IIS で、証明機関に証明書を要求します。その方法の詳細については、IIS のヘルプを参照してください。
3. [スタート] > [ファイル名を指定して実行] をクリックし、「`mmc.exe`」と入力して[*OK*]をクリックします。
4. MMC に証明書スナップインを追加します。
   a. [ファイル] メニューの [スナップインの追加と削除] をクリックします。
      [スナップインの追加と削除] 画面が表示されます。
   b. [利用できるスナップイン] リストから [証明書] を選択し、[追加] をクリックします。
   c. [コンピュータアカウント]を選択し、[次へ]をクリックします。
   d. [ローカルコンピュータ]を選択し、[完了]をクリックします。
   e. [*OK*] をクリックします。

   証明書スナップインが MMC に追加されます。
5. MMC で、[証明書]を展開し、使用する証明書を選択します。
6. [操作]メニューの[すべてのタスク] > [エクスポート] を選択します。
   証明書のエクスポートウィザードが開始されます。
7. [次へ]をクリックします。
8. [はい、秘密キーをエクスポートします]を選択し、[次へ]をクリックします。
9. [*Personal Information Exchange - PKCS #12(.PFX)*]を選択し、[次へ]をクリックします。
10. 証明書を作成するときに使用したパスワードを入力し、[次へ]をクリックします。このパスワードは、WACS の HTTPS を設定するときに[秘密鍵のアクセスパスワード]フィールドで指定する必要があります。

PKCS12 証明書ファイルストアが作成されます。

13.1.4.2 証明書信頼リストを生成する

1. WACS をホストとしているマシンに Administrator としてログオンします。
2. Microsoft 管理コンソール(MMC)を起動します。
3. インターネットインフォメーションサービススナップインを追加します。
   a. [ファイル] メニューから [スナップインの追加と削除] を選択します。
   b. [利用できるスナップイン] リストで、[インターネットインフォメーションサービス *(IIS)* マネージャ] を選択し、[追加] をクリックします。
   c. [*OK*] をクリックします。
      IIS スナップインが MMC に追加されます。
4. http://www.iis.net/learn/install/installing-iis-7/compatibility-and-feature-requirements-for-windows-vista#NoWizard に記載されている手順に従い、証明書信頼リストを作成します。

13.1.4.3 HTTPS/SSL を設定する

WACS の HTTPS/SSL を設定する前に、PCKS12 ファイルまたは JKS キーストアが作成され、そのファイルが WACS をホストしているマシンにコピーまたは移動されていることを確認する必要があります。

1. CMC の [サーバ] 管理エリアに移動します。
2. HTTPS を有効にする WACS をダブルクリックします。
   [プロパティ]画面が表示されます。
3. [*HTTPS* 設定] セクションの [*HTTPS* の有効化] チェックボックスをオンにします。
4. [ホスト名または *IP* アドレスに連結]フィールドで、証明書の発行先で WACS をバインドする IP アドレスを指定します。
   HTTPS サービスは、指定した IP アドレスを介して提供されます。
5. [*HTTPS* ポート]フィールドで、WACS が HTTPS サービスの提供に使用するポート番号を指定します。このポートが空いていることを確認する必要があります。ユーザにファイアウォールの外部から WACS に接続することを許可する場合は、このポートがファイアウォールで開いていることも確認する必要があります。
6. リバースプロキシを使用した SSL を設定する場合は、[プロキシホスト名]と[プロキシポート]の各フィールドでプロキシサーバのホスト名とポートを指定します。
7. [プロトコル]リストでプロトコルを選択します。選択可能なオプションは、次のとおりです。
   - *SSL*
     SSL は Secure Sockets Layer の略で、ネットワークトラフィックを暗号化するためのプロトコルです。
   - *TLS*
     TLS は Transport Layer Security の略で、新しい拡張プロトコルです。SSL と TLS の違いはわずかですが、TLS の方が強力な暗号化アルゴリズムを採用しています。
8. [証明書ストアタイプ]フィールドで、証明書のファイルタイプを指定します。選択可能なオプションは、次のとおりです。
   - *PKCS12*
     Microsoft ツールの方が使いやすい場合に選択します。
   - *JKS*
     Java ツールの方が使いやすい場合に選択します。
9. [証明書ストアファイルの場所]フィールドで、証明書ファイルストアまたは Java キーストアファイルをコピーまたは移動したパスを指定します。
10. [秘密鍵のアクセスパスワード]フィールドで、パスワードを指定します。
    PKCS12 証明書ストアと JKS キーストアの秘密鍵は、不正アクセスを防ぐためにパスワードで保護されています。WACS が秘密鍵にアクセスできるように、秘密鍵にアクセスするためのパスワードを指定する必要があります。
11. 1 つの証明書が格納されているか、または使用する証明書が先頭にリストされている証明書ファイルストアまたはキーストアを使用することをお勧めします。ただし、複数の証明書が格納されているか、または証明書が先頭にリストされていない証明書ファイルストアまたはキーストアを使用する場合は、[証明書エイリアス]フィールドで証明書のエイリアスを指定する必要があります。
12. WACS で特定のクライアントからの HTTPS 要求のみ受け付ける場合は、クライアント認証を有効にします。
    クライアント認証はユーザを認証するものではありません。WACS が特定のクライアントに対してのみ HTTPS 要求を処理するようにします。
    a. [クライアント認証を有効にする]チェックボックスをオンにします。
    b. [証明書信頼一覧ファイルの場所] で、信頼一覧ファイルが格納されている PCKS12 ファイルまたは JKS キーストアの場所を指定します。

> **注記**
>
> 証明書信頼リストのタイプは、証明書ストアのタイプと同じにする必要があります。

> **注記**
>
> X.509 証明書を使用した信頼できる認証の確立の詳細については、RESTful Web サービス向け [393 ページ] を参照してください。

> **注記**
>
> 以下のコマンドを実行することにより、ABAP システムの証明書を BI プラットフォームにインポートできます。`keytool -import -trustcacerts -alias <Alias_Name> -file <CA_certificate_path> -keystore <trust_keystore_path>` 。このコマンドを理解するには、次の表を参照してください。
>
> | コマンド | 説明 |
> | --- | --- |
> | -alias | エイリアス名 |
> | -file | ABAP システムの証明書のファイルパス |
> | -keystore | 信頼できるキーストアのファイルパス |

c. [証明書信頼リストの秘密鍵のアクセスパスワード]フィールドに、証明書信頼リストファイルの秘密鍵へのアクセスを保護するパスワードを入力します。

> **注記**
>
> クライアント認証を有効にしてもブラウザまたは Web サービスコンシューマが認証されない場合は、HTTPS 接続が拒否されています。

13. [保存して閉じる] をクリックします。
14. [メトリクス] 画面に移動して、[実行中の *WACS* コネクタの一覧] に HTTPS コネクタが表示されていることを確認します。HTTPS が表示されない場合は、HTTPS コネクタが正しく設定されているかどうかを確認します。

13.1.5 サポートされる認証方法

WACS は、次の認証方法をサポートします。

- Enterprise
- LDAP
- AD Kerberos

WACS は、次の認証方法をサポートしません。

- NT

- AD NTLM
- LDAP とシングルサインオンの併用

13.1.6 WACS への AD Kerberos の設定

WACS に AD Kerberos 認証を設定するには、最初に、AD をサポートするようにマシンを設定する必要があります。次の手順を実行する必要があります。

- Windows AD セキュリティプラグインの有効化
- ユーザとグループのマッピング
- サービスアカウントの設定
- 制限された委任の設定
- WACS に対する Windows AD プラグインでの Kerberos 認証の有効化
- 設定ファイルの作成

WACS をホストしているマシンで AD Kerberos 認証が使用されるように設定したら、セントラル管理コンソール(CMC)で追加の設定手順を実行する必要があります。

Web サービス SDK および QaaWS で AD Kerberos を通じてシングルサインオンを設定している場合は、WACS と WACS をホストしているマシンの両方を設定する必要もあります。

関連情報

Windows AD セキュリティプラグイン [284 ページ]
Windows AD ユーザとグループをマップする [285 ページ]
Kerberos での AD 認証用サービスアカウントの設定 [283 ページ]
BI プラットフォームサービスアカウントでの SIA の実行 [292 ページ]
WACS に対する Windows AD プラグインでの Kerberos 認証の有効化 [503 ページ]
設定ファイルの作成 [505 ページ]
AD Kerberos 用の WACS の設定 [508 ページ]
AD Kerberos シングルサインオンの設定 [510 ページ]

13.1.6.1 WACS に対する Windows AD プラグインでの Kerberos 認証の有効化

Kerberos をサポートするには、Kerberos 認証を使用するように、CMC の Windows AD セキュリティプラグインを設定する必要があります。これには、以下があります。

- Windows AD 認証が有効であることを確認する
- AD Administrator アカウントを入力する

> ⓘ 注記
>
> このアカウントは、Active Directory への読み取りアクセスだけを必要とし、その他のアクセス権は必要としません。

- Kerberos 認証と、シングルサインオンが必要な場合はシングルサインオンを有効にする
- サービスアカウントのサービスプリンシパル名(SPN)を入力する

13.1.6.1.1 前提条件

Kerberos に対して Windows AD セキュリティプラグインを設定する前に、以下のタスクが完了している必要があります。

- Kerberos での AD 認証用サービスアカウントの設定 [283 ページ]
- BI プラットフォームサービスアカウントでの SIA の実行 [292 ページ]
- Windows AD ユーザとグループをマップする [285 ページ]

13.1.6.1.2 Kerberos 用に Windows AD セキュリティプラグインを設定する

1. CMC の[認証]管理エリアを表示します。
2. [*Windows AD*]をダブルクリックします。
3. [*Windows Active Directory (AD) を有効にする*] チェックボックスがオンになっていることを確認します。
4. [認証のオプション] エリアで [*Kerberos 認証を使用する*] をオンにします。
5. データベースへのシングルサインオンを設定する場合には、[セキュリティコンテキストをキャッシュする *(データベースへの SSO に必要)*] チェックボックスをオンにします。
6. [サービスプリンシパル名]フィールドに、サービスアカウントのアカウントとドメイン、またはサービスアカウントへの SPN マッピングを入力します。

   次の形式を使用します。ここで、`<svcacct>` は、以前に作成したサービスアカウント名または SPN で、`<DNS.COM>` は大文字での完全修飾ドメイン名です。たとえば、サービスアカウントは svcacct@DNS.COM になり、SPN は BOBJCentralMS/some_name@DOMAIN.COM となります。

   > ⓘ 注記
   >
   > - デフォルトドメイン以外のドメインのユーザがログオンできるようにする場合は、以前にマップした SPN を指定する必要があります。
   > - サービスアカウントは大文字と小文字を区別します。ここで入力するアカウントの大文字または小文字の区別は、Active Directory ドメインの設定で入力した大文字と小文字の区別と完全に同一でなければなりません。
   > - これは、BI プラットフォームサーバを実行するために使用するアカウントと同じか、このアカウントとマッピングしている SPN にする必要があります。

7. シングルサインオンを設定する場合は、[選択した認証モードでのシングルサインオン*(SSO)*を有効にする]を選択します。

> ⓘ 注記
>
> シングルサインオンを有効にすることを選択した場合、WACS を設定する必要があります。

関連情報

AD Kerberos シングルサインオンの設定 [510 ページ]

13.1.6.2 設定ファイルの作成

アプリケーションサーバに Kerberos を設定する一般的なプロセスは、以下の手順になります。

- Kerberos 設定ファイルの作成。
- JAAS ログイン設定ファイルの作成。

> ⓘ 注記
>
> - デフォルトの Active Directory ドメインには、大文字の DNS 形式を使用します。
> - MIT Kerberos for Windows のダウンロードとインストールは不要です。また、サービスアカウント用の keytab も不要です。

13.1.6.2.1 Kerberos 設定ファイルを作成する

次の手順に従って、Kerberos 設定ファイルを作成します。

1. `krb5.ini` ファイルが存在しない場合はこのファイルを作成し、Windows の場合は `C:¥Windows` に保存します。

   > ⓘ 注記
   >
   > このファイルは別の場所に保存することができます。ただし、別の場所に保存する場合は、CMC で WACS サーバの[プロパティ]ページにある[*Krb5.ini ファイルの場所*]フィールドで場所を指定する必要があります。

2. Kerberos の設定ファイルに以下の必須情報を追加します。

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
```

```
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
}
```

> ⓘ 注記
>
> `DNS.COM` はドメインの DNS 名で、FQDN 形式で大文字で入力する必要があります。

> ⓘ 注記
>
> `kdc` はドメインコントローラのホスト名です。

> ⓘ 注記
>
> ユーザが複数のドメインからログインする場合は、[realms]セクションに複数のドメインエントリを追加できます。複数のドメインエントリを追加したサンプルファイルについては、Krb5.ini のサンプルファイル [507 ページ]を参照してください。

> ⓘ 注記
>
> 複数ドメインの設定では、`[libdefaults]` の下の `default_realm` の値は、任意の対象ドメインです。ベストプラクティスとしては、AD アカウントで認証するユーザ数が最大のドメインを使用します。

13.1.6.2.2 JAAS ログイン設定ファイルを作成する

1. `bscLogin.conf` というファイルが存在しない場合は作成し、デフォルトの保存場所 (`C:¥Windows`) に保存します。

   > ⓘ 注記
   >
   > このファイルは別の場所に保存することができます。別の場所に保存する場合は、CMC で WACS サーバの[プロパティ]ページにある[*bscLogin.conf ファイルの場所*]フィールドで場所を指定する必要があります。

2. JAAS の `bscLogin.conf` 設定ファイルに以下のコードを追加します。

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. ファイルを保存して閉じます。

13.1.6.2.3 Krb5.ini のサンプルファイル

複数ドメイン Krb5.ini ファイルのサンプル

次は、複数のドメインを設定したサンプルファイルです。

```
[domain_realm]
        .domain03.com = DOMAIN03.COM
        domain03.com = DOMAIN03.com
        .child1.domain03.com = CHILD1.DOMAIN03.COM
        child1.domain03.com = CHILD1.DOMAIN03.com
        .child2.domain03.com = CHILD2.DOMAIN03.COM
        child2.domain03.com = CHILD2.DOMAIN03.com
        .domain04.com = DOMAIN04.COM
        domain04.com = DOMAIN04.com
[libdefaults]
        default_realm = DOMAIN03.COM
        dns_lookup_kdc = true
        dns_lookup_realm = true
[realms]
        DOMAIN03.COM = {
         admin_server = testvmw2k07
         kdc = testvmw2k07
         default_domain = domain03.com
        }
     CHILD1.DOMAIN03.COM = {
            admin_server = testvmw2k08
            kdc = testvmw2k08
            default_domain = child1.domain03.com
        }
        CHILD2.DOMAIN03.COM = {
            admin_server = testvmw2k09
            kdc = testvmw2k09
            default_domain = child2.domain03.com
        }
        DOMAIN04.COM = {
            admin_server = testvmw2k011
            kdc = testvmw2k011
            default_domain = domain04.com
        }
```

シングルドメイン Krb5.ini ファイルのサンプル

次は、シングルドメインの krb5.ini ファイルのサンプルです。

```
[libdefaults]
        default_realm = ABCD.MFROOT.ORG
        dns_lookup_kdc = true
        dns_lookup_realm = true
[realms]
        ABCD.MFROOT.ORG = {
            kdc = ABCDIR20.ABCD.MFROOT.ORG
            kdc = ABCDIR21.ABCD.MFROOT.ORG
            kdc = ABCDIR22.ABCD.MFROOT.ORG
            kdc = ABCDIR23.ABCD.MFROOT.ORG
            default_domain = ABCD.MFROOT.ORG
        }
```

13.1.6.3 AD Kerberos 用の WACS の設定

AD Kerberos 認証用の WACS をホストしているマシンを設定したら、セントラル管理コンソール(CMC)で WACS 自身を設定する必要があります。

13.1.6.3.1 AD Kerberos 用の WACS を設定する

1. CMC の[サーバ]管理エリアを表示します。
2. AD を設定する WACS をダブルクリックします。
   [プロパティ]画面が表示されます。
3. [*Krb5.ini ファイルの場所*]フィールドで、`krb5.ini` 設定ファイルへのパスを指定します。
4. [*bscLogin.conf ファイルの場所*]フィールドで、`bscLogin.conf` 設定ファイルへのパスを指定します。
5. [保存して閉じる]をクリックします。
6. WACS を再起動します。

13.1.6.4 Kerberos のトラブルシューティング

Kerberos の設定時に問題が起きた場合は、次の手順が有用です。

- ログの有効化
- Kerberos 設定のテスト

13.1.6.4.1 Kerberos ログを有効にする

1. セントラル設定マネージャ (CCM) を起動し、[サーバの管理] をクリックします。
2. ログオン認証情報を指定します。
3. [サーバの管理]画面で、WACS を停止します。
4. [*Web Tier 設定*] をクリックします。

   > ⓘ 注記
   >
   > [*Web Tier 設定*]アイコンは、停止している WACS を選択した場合にのみ有効になります。

   [*Web Tier 設定*]画面が表示されます。
5. [コマンドラインパラメータ]で、次のテキストをパラメータの終わりにコピーします。

   ```
   “-Dcrystal.enterprise.trace.configuration=verbose
    -Djcsi.Kerberos.debug=true”
   ```
6. [*OK*]をクリックします。
7. [サーバの管理]画面で、WACS を起動します。

13.1.6.4.2 Kerberos 設定をテストする

次のコマンドを実行して、Kerberos の設定をテストします。ここで、servact は CMS が実行されているサービスアカウントとドメインで、password は、このサービスアカウントに関連付けられているパスワードです。

```
<INSTALLDIR>¥Business Objects¥javasdk¥bin¥kinit.exe servact@TESTM03.COM Password
```

以下はその例です。

```
 C:¥Program Files¥Business Objects¥javasdk¥bin¥kinit.exe servact@TESTM03.COM
Password
```

これで問題が解決されない場合には、ドメインとサービスプリンシパル名に入力した大文字または小文字が、Active Directory の設定で入力した大文字または小文字と完全に一致するかどうかを確認してください。

13.1.6.4.3 マップされた AD ユーザが WACS の BI プラットフォームにログオンできない

次の 2 つの問題は、ユーザが BI プラットフォームにマップされているかどうかにかかわらず発生する可能性があります。

13.1.6.4.3.1 異なる AD UPN および SAM 名によるログオンの失敗

ユーザの Active Directory ID は正常に BI プラットフォームにマップされています。それにもかかわらず、次の形式で、AD 認証および Kerberos を使用して CMC にログオンすることができません。DOMAIN¥ABC123

この問題は、ユーザが UPN を使用して Active Directory で設定され、SAM 名の大文字小文字またはそれ以外の部分が異なる場合に発生する可能性があります。次に、問題が発生する原因となる 2 つの例を示します。

- UPN が abc123@company.com だが、SAM 名が DOMAIN¥ABC123 である場合。
- UPN が jsmith@company だが、SAM 名が DOMAIN¥johnsmith である場合。

この問題を解決するには、次の 2 とおりの方法があります。

- ユーザに、SAM 名ではなく UPN 名を使用してログインさせる。
- SAM アカウント名と UPN 名を完全に同じにする。

13.1.6.4.3.2 事前認証エラー

以前にログオンできたユーザが、正常にログオンできなくなることがあります。ユーザは、"アカウント情報を認識できません。" というエラーを受け取ります。WACS のログには、「Pre-authentication information was invalid (24)」というエラーが記録されます。

これは、Kerberos ユーザデータベースが AD の UPN への変更を取得していないために発生します。これは、Kerberos ユーザデータベースと AD の情報が同期していないことを意味します。

この問題を解決するには、AD でユーザのパスワードをリセットしてください。これにより、変更が正しく伝播されます。

13.1.7 AD Kerberos シングルサインオンの設定

BI ラウンチパッドまたは Web サービス SDK および QaaWS に AD Kerberos シングルサインオンを設定する場合は、WACS と AD Kerberos 認証用の WACS をホストするマシンをどちらも設定していることを確認してください。

WACS に AD Kerberos シングルサインオンを設定するには、まず WACS をホストしているマシンを、次に WACS 自体を設定する必要があります。

> ⓘ 注記
>
> リバースプロキシ環境でシングルサインオンを使用する場合は、このガイドのセキュリティ情報に関する記載を参照してください。

関連情報

セキュリティの概要 [147 ページ]
WACS への AD Kerberos の設定 [503 ページ]
AD Kerberos シングルサインオン用のマシン設定 [510 ページ]
AD Kerberos シングルサインオンのための WACS の 設定 [511 ページ]

13.1.7.1 AD Kerberos シングルサインオン用のマシン設定

Web サービス SDK および QaaWS に AD Kerberos シングルサインオンを設定するには、まず WACS をホストしているマシンを設定する必要があります。

- Vintela SSO の制限された委任を設定する [307 ページ]
- Vintela SSO のサービスアカウントを設定する [304 ページ]
- 複数の SPN の設定 [510 ページ]
- WACS のヘッダサイズ制限を増やす [511 ページ]

次の各節で、これらの手順の実行方法を説明しています。

13.1.7.1.1 複数の SPN の設定

複数の SPN の使用はサポートされていません。

13.1.7.1.2 WACS のヘッダサイズ制限を増やす

Active Directory は Kerberos を作成し、これは認証プロセスで使用されます。このトークンは、HTTP ヘッダに格納されます。WACS はほとんどのユーザに十分なデフォルト HTTP ヘッダサイズです。このヘッダサイズは設定可能です。

1. CMC の[サーバ]管理エリアを表示します。
2. HTTP ヘッダサイズを変更する WACS をダブルクリックします。
   [プロパティ] 画面が表示されます。
3. [*HTTP* 設定] の [プロキシ経由の *HTTP* の設定] または [*HTTPS* 設定] セクションで、[最大 *HTTP* ヘッダサイズ *(*バイト*)*] フィールドの値を指定します。
4. [保存して閉じる] をクリックします。
5. サーバを再起動します。

13.1.7.2 AD Kerberos シングルサインオンのための WACS の 設定

Web アプリケーションコンテナサーバで AD Kerberos シングルサインオンが使用されるように設定することができます。AD Kerberos シングルサインオンがサポートされています。AD NTLM はサポートされていません。

WACS を設定する前に、AD Kerberos シングルサインオンを、WACS をホストしているマシンに設定する必要があります。

1. CMC の[サーバ]管理エリアを表示します。
2. 設定する WACS をダブルクリックします。
   [プロパティ]画面が表示されます。
3. [*Kerberos Active Directory* シングルサインオンの有効化] にチェックを入れます。
4. デフォルト AD ドメイン、サービスプリンシパル名、Keytab ファイルプロパティに値を設定し、[保存して閉じる] をクリックします。
5. WACS を再起動します。

Active Directory シングルサインオンを使用する準備ができました。

13.1.7.3 Kerberos とデータベースへのシングルサインオンの設定

以下のすべての要件を満たすデプロイメントで、データベースへのシングルサインオンがサポートされます。

- BI プラットフォームのデプロイメントが WACS 上にある。
- WACS が Kerberos を使用する AD で設定されている。
- シングルサインオンが必要なデータベースは SQL Server または Oracle でサポートされるバージョンである。
- データベースに対するアクセス権が必要なグループとユーザに、SQL Server または Oracle 内の権限が付与されている。
- CMC の[AD 認証]ページの[セキュリティコンテキストをキャッシュする]チェックボックス(データベースへのシングルサインオンに必要)がオンになっている。

最後の手順では、krb5.ini ファイルを変更してデータベースへのシングルサインオンをサポートするようにします。

> ⓘ 注記
>
> 以下の手順は、データベースへのシングルサインオンを設定する方法について説明しています。データベースにエンドツーエンドのシングルサインオンを設定する場合、Vintela シングルサインオンに必要な設定も行う必要があります。詳細については、AD Kerberos シングルサインオンの設定 [510 ページ]を参照してください。

13.1.7.3.1 データベースへのシングルサインオンを有効にする

1. BI プラットフォームのデプロイメントで使用される krb5.ini ファイルを開きます。
   このファイルのデフォルトの場所は、Web アプリケーションサーバの C:¥Windows ディレクトリです。
2. ファイルの [libdefaults]セクションに移動します。
3. 次の文字列は、ファイルの [realms]セクションの開始位置よりも前に入力してください。

   ```
   forwardable = true
   ```

4. ファイルを保存して閉じます。
5. WACS を再起動します。

13.1.8 RESTful Web サービスの設定

Business Intelligence プラットフォーム RESTful Web サービス SDK により、HTTP プロトコルを使用して BI プラットフォームにアクセスできます。 これにより、ユーザは HTTP 要求をサポートするプログラム言語を使用して、BI プラットフォームリポジトリへの移動、およびオブジェクトのスケジュールが可能になります。 RESTful Web サービスは WACS の一部としてインストールされます。

この節では、RESTful Web サービスを管理する方法について説明します。 RESTful Web サービスの詳細については、*Business Intelligence プラットフォーム RESTful Web サービス開発者ガイド*を参照してください。

13.1.8.1 アプリケーション

13.1.8.1.1 RESTful Web サービスのベース URL を設定する

BI プラットフォームデプロイメントがプロキシサーバを使用するか、Web アプリケーションコンテナサーバ (WACS) の複数のインスタンスを含む場合は、RESTful Web サービスで使用できるようにベース URL を設定しなければならないことがあります。ベース URL を設定するには、RESTful Web サービス要求をリスニングするサーバ名とポート番号の情報が必要です。

ベース URL は、各 RESTful Web サービス要求の一部として使用されます。開発者は、プログラムの中でベース URL を検出し、これを使用して RESTful Web サービス要求を正しいサーバとポートに転送します。ベース URL は、他の RESTful リソースへのハイパーリンクを定義するために、RESTful Web サービス応答でも使用されます。

> ⓘ 注記
>
> BI platform のデフォルトインストールでは、ベース URL は `http://<servername>:6405/biprws` と定義されます。`<servername>` は、RESTful Web サービスをホストするサーバーの名前に置き換えてください。

1. セントラル管理コンソール（CMC）に管理者としてログオンします。
2. CMC で［アプリケーション］をクリックします。
   アプリケーションの一覧が表示されます。
3. *RESTful Web サービス* > プロパティ を右クリックします。
   [*プロパティ: RESTful Web サービス*] ページが表示されます。このページに [*相対 URL パスを使用*] チェックボックスが追加されました。これにより、ブラウザの URL を考慮して RESTful Web サービスを起動することができます。詳細については、SAP ノート 3048101 を参照してください。
4. [*アクセス URL*] テキストボックスで、RESTful Web サービスのベース URL の名前を入力します。
   たとえば、`http://<servername>:<portnumber>/biprws` と入力します。`<servername>` と `<portnumber>` は、RESTful Web サービスの要求をリスニングするサーバーとポートの名前に置き換えてください。

   > ⚠ 警告
   >
   > - RESTful Web サービス API については、**Tomcat** サーバ、**WACS** サーバ、**JBoss**、**SAP NetWeaver**、**WebSphere** サーバがサポートされています。
   > - [*アクセス URL*] には、デフォルトでは WACS URL が表示されます。Restful Web サービス API を Tomcat Web サーバで使用する場合は、必要な `<server>` および `<port>` 値を状況に従って必ず修正してください。

5. [保存して終了] をクリックします。

   > ⓘ 注記
   >
   > [*相対 URL パスを使用*] を有効にすると、ブラウザの相対 URL が使用されます。

13.1.8.2 WACS プロパティ

13.1.8.2.1 メソッドとヘッダーのコマンド ライン パラメータを作成する

管理者は、Web アプリケーション コンテナ サービス（WACS）のプロパティの［コマンド ライン パラメータ］に適切なオプションを追加することで、RESTful Web サービスが使用できるメソッドとヘッダーを制限できます。パラメータを変更した後は、WACS サービスを再起動する必要があります。

1. セントラル管理コンソールに管理者ユーザーとしてログオンします。
2. ［サーバー］をクリックし、［サーバーの一覧］をクリックします。
3. `MySIA.WebApplicationContainerServer` などの Web アプリケーション コンテナ サーバー（WACS）を右クリックし、［プロパティ］をクリックします。

WACS サーバーの［プロパティ］タブが表示されます。

4. ［コマンド ライン パラメータ］領域に、許可するメソッドとヘッダーを入力します。

   オプション グループごとに二重引用符で囲みます。GET、HEAD、および POST 以外のメソッドを使用します。PUT や DELETE などのオプション値は、カンマを使用して区切ります。以下に例を示します。

```
"-Dcom.sap.bip.rs.cors.extra.methods= PUT, DELETE"
"-Dcom.sap.bip.rs.cors.extra.headers= X-SAP-LogonToken, X-SAP-PVL, WWW-
Authenticate"
```

> ⓘ 注記
>
> すべてのメソッドとヘッダーを許可するためのデフォルト値は、*（アスタリスク）です。コマンド ライン パラメータ全体を省略しても、同じ効果があります。

5. ［保存して閉じる］をクリックします。
6. WACS サーバー名（MySIA.WebApplicationContainerServer など）を右クリックし、［サーバーの再起動］をクリックしてサービスを再起動します。

13.1.8.2.2 システムプロパティ設定

13.1.8.2.2.1 エラーメッセージスタックを有効にする

管理者は、RESTful Web サービスから返されるエラーメッセージにエラースタックを含めるように構成することができます。エラースタックは、エラーが発生した場所を見つけるために役立つ追加のデバッグ情報を提供します。

> ⓘ 注記
>
> エラースタックは、エンドユーザーに公開することは避けたい BI platform に関する情報を提供する可能性があるため、実稼働シナリオでは有効にしないことをお勧めします。実稼働シナリオでは、デバッグが必要な場合にのみエラースタックを有効にして、不要になったらオフにすることをお勧めします。

1. セントラル管理コンソールに管理者ユーザーとしてログオンします。
2. ［サーバー］をクリックし、［サーバーの一覧］をクリックします。
3. MySIA.WebApplicationContainerServer などの Web アプリケーション コンテナ サーバー（WACS）を右クリックし、［プロパティ］をクリックします。
   WACS サーバーの［プロパティ］タブが表示されます。
4. ［*RESTful Web* サービス］領域で、［エラースタックの表示］を選択します。
5. ［保存して閉じる］をクリックします。

RESTful Web サービスエラーメッセージにエラースタック情報が入りました。

13.1.8.2.2.2 各ページに表示されるデフォルトのエントリ数を設定する

多数のエントリから成るフィードが RESTful Web サービスの応答に含まれる場合は、その応答を複数のページに分割できます。各ページに表示されるデフォルトのエントリ数を構成することができます。開発者は、RESTful Web サービスの要求を行うときに、1 ページに表示するエントリの数を指定できます。ただし、この値を指定しない場合は、デフォルトのページサイズが使用されます。

1. セントラル管理コンソールに administrator としてログオンします。
2. ［サーバー］をクリックし、［サーバーの一覧］をクリックします。
3. `MySIA.WebApplicationContainerServer` などの Web アプリケーション コンテナ サーバー（WACS）を右クリックし、［プロパティ］をクリックします。
   WACS サーバーの［プロパティ］タブが表示されます。
4. ［*RESTful Web サービス*］領域で、［*1 ページあたりのデフォルトオブジェクト数*］テキスト領域にデフォルトのページサイズを入力します。
5. ［保存して閉じる］をクリックします。

13.1.8.2.2.3 ログオントークンのタイムアウト値を設定する

ログオントークンは、一定時間使用されないと、自動的に期限切れになります。未使用のログオントークンが有効な状態を維持する時間を設定できます。

> ⓘ 注記
>
> デフォルトでは、ログオントークンのタイムアウトは 1 時間です。

1. セントラル管理コンソールに administrator としてログオンします。
2. ［サーバー］をクリックし、［サーバーの一覧］をクリックします。
3. `MySIA.WebApplicationContainerServer` などの Web アプリケーション コンテナ サーバー（WACS）を右クリックし、［プロパティ］をクリックします。
   WACS サーバーの［プロパティ］タブが表示されます。
4. ［*RESTful Web サービス*］領域の［*Enterprise セッショントークンのタイムアウト（分単位）*］テキスト領域に、ログオントークンが有効である時間を分数で入力します。
5. ［保存して閉じる］をクリックします。

13.1.8.2.2.4 セッションプールの設定を構成する

セッションプールを使用して、サーバーのパフォーマンスを向上させることができます。セッションプールは、アクティブな RESTful Web サービスセッションをキャッシュします。これにより、ユーザーが HTTP 要求ヘッダーの中で同じログオントークンを使用して別の要求を送信したときに、セッションを再利用できます。セッションプールサイズは、キャッシュされたセッションを一度に格納できる数を定義します。また、セッションタイムアウト値は、セッションをキャッシュしておく時間を制御します。

セッションプールサイズとセッションタイムアウト値を設定するには、次の手順を実行します。

1. セントラル管理コンソール（CMC）に管理者としてログオンします。
2. ［サーバー］をクリックし、［サーバーの一覧］をクリックします。
3. `MySIA.WebApplicationContainerServer` などの Web アプリケーション コンテナ サーバー（WACS）を右クリックし、［プロパティ］をクリックします。
   WACS サーバーの［プロパティ］タブが表示されます。
4. ［*RESTful Web サービス*］領域の［セッションプールサイズ］テキストボックスに、キャッシュするセッションの最大数を入力します。
5. ［*RESTful Web サービス*］領域の［セッションプールタイムアウト（分）］テキストボックスに、セッションプールタイムアウト値を入力します。
6. ［保存して閉じる］をクリックします。
7. `MySIA.WebApplicationContainerServer` などの WACS サーバーを右クリックし、［サーバーの再起動］をクリックします。

13.1.8.2.2.5 HTTP 基本認証を有効化する

HTTP 基本認証を使用すると、ログオントークンを指定しなくても RESTful Web サービス要求を行うことができます。HTTP 基本認証が有効な場合は、ユーザーが初めて RESTful Web サービス要求を行うときに、ユーザー名とパスワードを指定するように求められます。

> **注記**
>
> HTTPS と組み合わせて使用しない限り、HTTP 基本認証のユーザー名とパスワードは安全に転送されません。

HTTP 基本認証を有効にする場合は、デフォルトの HTTP 基本認証タイプとして SAP、Enterprise、LDAP、または WinAD を設定します。ユーザーは、ログオンするときに、デフォルトの HTTP 基本認証タイプ以外を指定して使用することもできます。

HTTP 基本認証を使用した BI platform へのログオンは、ライセンスを 1 つ使用します。セッションプールキャッシュを使用している場合、要求は、キャッシュされたセッションに関連付けられたライセンスを使用します。セッションプールキャッシュを使用していない場合、要求の実行中は 1 つのライセンスが使用され、要求が完了するとそれが解放されます。

1. セントラル管理コンソール（CMC）に管理者としてログオンします。
2. サーバー > サーバーの一覧 をクリックします。
3. `MySIA.WebApplicationContainerServer` などの Web アプリケーション コンテナ サーバー（WACS）を右クリックし、［プロパティ］をクリックします。
   WACS サーバーの［プロパティ］タブが表示されます。
4. ［*RESTful Web サービス*］領域で、［*HTTP Basic 認証を有効にする*］を選択します。
5. （オプション）［*デフォルトの HTTP Basic 用認証スキーマ*］一覧で、デフォルトの HTTP 基本認証タイプを選択します。
6. ［保存して閉じる］をクリックします。

エンドユーザーは、HTTP 基本認証を使用してログオンするときに、使用する認証のタイプを指定できます。Web ブラウザーでは、ユーザー名プロンプトに `<authtype>¥<username>`、パスワードプロンプトに `<password>` と入力します。

プログラムで HTTP 基本認証を使用してログオンするには、HTTP 要求ヘッダーに `Authorization` 属性を追加し、その値を `Basic <authtype>¥<username>:<password>` に設定します。

<authtype> は認証タイプに、<username> はユーザー名に、<password> はパスワードに置き換えてください。認証タイプ、ユーザー名、およびパスワードは、RFC 2617 で定義されている base64 エンコードである必要があります。HTTP 基本認証では、：文字を含むユーザー名を使用できません。

関連情報

セッションプールの設定を構成する [515 ページ]

13.1.8.2.3 クロスオリジンリソース共有

13.1.8.2.3.1 クロスオリジン リソース共有（CORS）を構成する

[クロスオリジン リソース共有設定]（CORS）設定を使用すると、ドメイン名の一覧を追加して、JavaScript ベースの Web ページの複数のソースからデータを取得できます。これは、JavaScript および Ajax 言語でクロスドメイン アクセスを防止するために導入されているセキュリティ ポリシーを回避するために必要です。セキュリティの低下を防止するために、アクセスされる可能性がある Web サイトのみを CMC の［オリジンを許可する］WACS サーバー プロパティに追加します。

[最大期間 (分)] 設定を使用して、キャッシュの有効期限を調整することもできます。この場合はブラウザが HTTP 要求を保持する最大分数を設定します。

> **注記**
> デフォルトでは、*（アスタリスク）によってすべてのドメインへのアクセスが許可されます。

1. セントラル管理コンソールに administrator としてログオンします。
2. ▶ サーバー ▶ サーバーの一覧 ▶をクリックします。
3. `MySIA.WebApplicationContainerServer` などの Web アプリケーション コンテナ サーバー（WACS）を右クリックし、［プロパティ］をクリックします。
   WACS サーバーの［プロパティ］タブが表示されます。
4. ［*RESTful Web* サービス］領域で、［オリジンを許可する:］の隣にある［クロスオリジン リソース共有設定］テキスト ボックスに移動し、*（アスタリスク）をカンマで区切ったドメイン名の一覧で置き換えます。例：`http://origin1.server:8080, http://origin2.server:8080`
5. ［最大期間 (分)］テキスト ボックスに、ブラウザが HTTP 要求をキャッシュする最大分数を入力します。
6. ［保存して閉じる］をクリックします。

13.1.8.2.4 認証

13.1.8.2.4.1 WinAD SSO を有効化するように web.xml を設定する

Windows Active Directory シングル サインオン（WinAD SSO）を認識するように RESTful Web サービスを設定するには、BI platform サーバーにある `web.xml` 構成ファイルを編集する必要があります。詳細については、*Business Intelligence プラットフォーム RESTful Web サービス開発者ガイド*の「SDK の使用」>「認証」>「"Active Directory シングル サインオン（AD SSO）アカウントを使用してログオン トークンを取得する"」を参照してください。

BI platform サーバーでクライアント コンピュータの WinAD SSO ログイン認証情報が認識されるようにするには、`web.xml` の `Kerberos Proxy filter` セクションのコメントを解除し、使用される Active Directory 環境を反映する `idm.realm`、`idm.princ`、および `idm.keytab` の値を更新します。

1. `<boe root>¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥services¥RestWebService¥biprws¥WEB-INF¥` の `web.xml` 設定を特定します。次に、ファイルパスの例を示します。

```
C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI
4.0¥java¥
pjs¥services¥RestWebService¥biprws¥WEB-INF¥web.xml
```

2. `web.xml` ファイルで、`<filter>` タグの前にコメント終了タグ `-->` を追加して Kerberos Proxy Filter セクションのコメントを解除し、コメント終了タグ `-->` を削除します。

```
  <!-- Kerberos Proxy Filter
    - Uncomment this filter and the corresponding filter-mapping to enable
Kerberos SSO
    - for Windows AD (secWinAD) authentication.
    - The following options must be specified (the rest are optional):
    -   idm.realm
    -   idm.princ
    -   idm.keytab (unless using password, see below)
  -->
  <filter>
    <filter-name>WrappedResponseAuthFilter</filter-name>
      .
      .
      .
  </filter>
  <filter-mapping>
    <filter-name>WrappedResponseAuthFilter</filter-name>
    <url-pattern>/logon/adsso</url-pattern>
  </filter-mapping>

</web-app>
```

3. `idm.realm`、`idm.princ`、および `idm.keytab` の各設定の `<param-value>`を Active Directory 環境で使用されているものに更新します。

```
    <init-param>
      <param-name>idm.realm</param-name>
      <param-value>ADDOM.COM</param-value>
      <description>
          Required: Set this value to the Kerberos realm to use.
      </description>
    </init-param>
    <init-param>
```

```
      <param-name>idm.princ</param-name>
      <param-value>BOE120SIAVMBOESRVR/bo.service.addom.com</param-value>
      <description>
          Set this value to the Kerberos service principal to use.
          This will be a name of the form HTTP/fully-qualified-host.
          For example, HTTP/example.vintela.com
          If not set, defaults to the server's hostname and the
          idm.realm  property above.
      </description>
    </init-param>
    <init-param>
      <param-name>idm.kdc</param-name>
      <param-value></param-value>
      <description>
          The KDC against which secondary credentials must be validated
          This can be used for BASIC fallback or credential delegation.
          By default the KDC will be discovered automatically and this
          parameter must only be used if automatic discovery fails, or
          if a different KDC to the one discovered must automatically be used.
      </description>
    </init-param>
    <init-param>
      <param-name>idm.keytab</param-name>
      <param-value>C:/winnt/BOE120SIAVMBOESRVR.keytab</param-value>
      <description>
          The file containing the keytab that Kerberos will use for
          user-to-service authentication. If unspecified, SSO will default
          to using an in-memory keytab with a password specified in the
          com.wedgetail.idm.sso.password environment variable.
      </description>
    </init-param>
```

> **注記**
>
> `idm.keytab` 値は、BI platform サーバー上のファイルパスに対応しています。`idm.realm` および `idm.prince` の値は、セントラル管理コンソールから確認することができます。CMC の［認証］タブで、［*Windows AD*］をダブルクリックします。`idm.realm` の値は、［*AD 設定の概要*］の下にある［デフォルトの *AD* ドメイン］パラメータで設定されます。`idm.prince` の値は、［認証のオプション］の下にある［サービスプリンシパル名］パラメータで設定されます。

4. WACS サービスを再起動して、`web.xml` に加えた変更が認識されるようにします。
5. クライアント マシンを使用して、RESTful Web サービス API を使って AD SSO ログイン トークンを取得できることを確認します（例：`http://<boe host>:6405/biprws/logon/adsso`）。
6. ヘッダーに `X-SAP-LogonToken` を含む `GET` クエリーおよび `/infostore` API を使用して、トークンをテストします。

13.1.8.2.4.2 信用できる認証を有効にして設定する

信用できる認証は、セントラル管理コンソール (CMC) の *[認証] > [Enterprise]* を含む領域で有効化および設定し、ここで有効にします。共有シークレットキーファイルを生成し、*[ユーザとグループ] > [ユーザ一覧]* で信用できるユーザのアカウントを作成します。*[サーバ] > [サーバの一覧] > [WACS] > [プロパティ]* パスで、`/logon/trusted` API ログオントークン要求に対する [取得方法] オプションを選択します。

> **注記**
>
> セキュリティ上の理由から、信用できる認証を HTTPS なしで有効化しないでください。信用できる認証を https なしで有効にすると、URL が認証されていないユーザに公開されるため、セキュリティ侵害とみなされ

ます。セキュリティ侵害を防ぐために、有効な証明書を使用してユーザの情報を検証できます。詳細については、1388240 を参照してください。

1. セントラル管理コンソールに管理者としてログオンします。
2. [認証] > [*Enterprise*] に移動して、[信用できる認証を有効にする] をクリックします。
3. [新規共有シークレット] をクリックし、[共有シークレットのダウンロード] をクリックします。
4. [保存] をクリックし、`TrustedPrincipal.conf` ファイルをデフォルトの場所 (`<EnterpriseDir>¥<platform>`) に保存します。
   例の場所は、次のように表示されます。

   ```
   "C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjectsEnterprise XI 4.0¥win64_x64¥"
   ```

   注記

   `TrustedPrincipal.conf` 共有シークレットファイルのデフォルトの場所を変更するには、CMC の *[サーバ] > [サーバの一覧] > [WACS] > [プロパティ] > [コマンドラインパラメータ]* にコマンドラインエントリを追加して、WACS サービスを再起動します。たとえば、`-Dbobj.trustedauth.home=`、および BI プラットフォームサーバの `C:¥` ドライブのルートに配置されたフォルダ `SharedSecrets` を使用するコマンドラインエントリは、次のようになります。

   ```
   "-Dbobj.trustedauth.home=C:¥SharedSecrets"
   ```

   注記

   オプション [共有シークレット有効期間 (日)] は、デフォルト値の 0 (ゼロ) のままにしておくことができます。こうすると、有効期間が切れることがなくなります。[信用できるログイン要求がタイムアウトするまでの最大時間 *(N ミリ秒) (0 は、制限時間なし)*] オプションは、デフォルト値の 0 (ゼロ) のままにしておくことができます。こうすると、信用できるログオン要求の時間制限がなくなります。

5. [更新] をクリックして変更を保存します。
6. [ユーザとグループ] > [ユーザ一覧] の *[管理] > [新規] > [新しいユーザ]* を使用して、新しいユーザとパスワード (`bob`、`Passw0rd` など) を追加します。[ユーザは次回ログオン時にパスワード変更が必要] チェックボックスをオフにして、[作成して閉じる] をクリックします。

   注記

   [ユーザの新規作成] アイコンをクリックするか、ユーザ名が一覧表示されているウィンドウの空白の領域を右クリックして、[新規] > [新しいユーザ] を選択することで、新しいユーザを作成することもできます。

7. [サーバ] > [コアサービス] > [*WACS*] > [プロパティ] に移動して、[信頼できる認証設定] セクションが表示されるまで下にスクロールし、[取得方法] メニューを使用して、[*HTTP_HEADER*]、[*QUERY_STRING*]、または [*COOKIE*] を選択します。

   注記

   [ユーザ名パラメータ] をデフォルトラベルの `X-SAP-TRUSTED-USER` から、RESTful Web サービスの開発者が使用する任意の実用的なラベル (`UserName`、`bankteller`、`nurse` など) に変更することもできます。

8. WACS サーバ名 (`MySIA.WebApplicationContainerServer` など) を右クリックし、[サーバの再起動] をクリックしてサービスを再起動します。

> ⓘ 注記
>
> ステップ 7 で説明した [取得方法] のオプションを後から変更する場合は、WACS を再起動する必要はありません。

9. ステップ 6 で作成したユーザ名で、`.../biprsw/logon/trusted/` API を使用し、デフォルトのヘッダラベル `X-SAP-TRUSTED-USER` を使用して `GET` 要求を送信することにより、ログオントークンを取得できることを確認します。

13.1.8.2.4.3 `TrustedPrincipal.conf` 共有シークレット構成ファイルを移動するためのコマンド ライン パラメータを構成する

RESTful web サービスには、信頼できる認証 `TrustedPrincipal.conf` ファイルの別の場所を選択するためのコマンド ライン パラメータが含まれています。

`TrustedPrincipal.conf` ファイルには、次の手順で CMC により生成される共有シークレットキーが含まれます。認証をクリックし、エンタープライズをダブルクリックします。 信用できる認証を有効にするを選択し、新規共有シークレットボタンをクリックします。 共有シークレットのダウンロードをクリックしてファイルを保存すると、ファイルはデフォルトの場所に保存されます。

`TrustedPrincipal.conf` ファイルのカスタム パスで Web Application Container Server（WACS）コマンド ラインを更新します。次に例を示します。

1. セントラル管理コンソールに管理者ユーザーとしてログオンします。
2. ［サーバー］をクリックし、［サーバーの一覧］をクリックします。
3. WACS サービス（`MySIA.WebApplicationContainerServer` など）を右クリックし、［プロパティ］をクリックします。
   WACS サーバのプロパティタブが表示されます。
4. ［コマンド ライン パラメータ］領域で、`TrustedPrincipal.conf` ファイルを格納するディレクトリのパスを入力します。

   文字列は二重引用符で囲みます。次に例を示します。

   ```
   "-Dbobj.trustedauth.home=C:¥SharedSecrets"
   ```

   > ⓘ 注記
   >
   > `TrustedPrincipal.conf` ファイルのデフォルトの場所は、`<EnterpriseDir>¥<platform>` です。例の場所は、次のとおりです。
   >
   > ```
   > C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise
   > XI 4.0¥win64_x64
   > "
   > ```

5. ［保存して閉じる］をクリックします。
6. WACS サーバー名（`MySIA.WebApplicationContainerServer` など）を右クリックし、［サーバーの再起動］をクリックしてサービスを再起動します。

13.1.9 WACS と IT 環境

このセクションでは、複雑な環境で WACS を設定する方法について説明します。

13.1.9.1 WACS と他の Web サーバの併用

Web アプリケーションコンテナサーバ(WACS)をインストールすると、特に設定を行わなくても WACS はアプリケーションサーバおよび Web サーバとして動作します。インターネットインフォメーションサービス(IIS)や Apache などのサポートされている Web サーバを、WACS サーバへの URL 転送を行うように設定できます。

> ⓘ 注記
>
> ISAPI フィルタを使用して IIS から WACS に要求を転送することはできません。

WACS は、Web サーバが静的コンテンツをホストして WACS が動的コンテンツをホストするデプロイメントシナリオをサポートしません。静的コンテンツと動的コンテンツは常に WACS 上に存在する必要があります。

13.1.9.2 WACS とロードバランサの併用

ハードウェアロードバランサを含むデプロイメントで WACS を使用するには、IP ルーティングまたはアクティブ cookie を使用するようにロードバランサを設定する必要があります。この場合、ある WACS でユーザのセッションが確立されると、同じユーザによるその後のすべての要求は同じ WACS に送信されます。

WACS はパッシブ cookie を使用したロードバランサではサポートされません。

ハードウェアロードバランサが SSL で暗号化された HTTPS 要求を WACS に転送する場合は、WACS の HTTPS を設定し、すべての WACS に SSL 証明書をインストールする必要があります。

ハードウェアロードバランサが HTTPS トラフィックを復号化し、復号化された HTTP 要求を WACS に転送する場合は、WACS の追加設定は必要ありません。

関連情報

HTTPS/SSL の設定 [499 ページ]

13.1.9.3 WACS とリバースプロキシの併用

フォワードプロキシサーバまたはリバースプロキシサーバを含むデプロイメントで WACS を使用できます。WACS 自体をプロキシサーバとして使用することはできません。

13.1.9.3.1 リバースプロキシを使用した HTTP をサポートするように WACS を設定する

リバースプロキシを含むデプロイメントで WACS を使用するには、ファイアウォール内 (たとえば、セキュリティで保護されたネットワーク上) の通信に HTTP ポートを使用し、ファイアウォールの外部 (たとえば、インターネット) からの通信にプロキシ経由の HTTP ポートを使用するように WACS を設定します。

1. CMC の [サーバ] 管理エリアに移動します。
2. 設定する WACS をダブルクリックします。
   [プロパティ]画面が表示されます。
3. [プロキシ経由の *HTTP* の設定]セクションで、次の操作を行います。
   a. [プロキシ経由の *HTTP* を有効にする]チェックボックスをオンにします。
   b. プロキシ経由の通信に使用する WACS の HTTP ポートを指定します。
   c. プロキシサーバのホスト名とポートを指定します。
4. [保存して閉じる] をクリックします。

13.1.9.3.2 リバースプロキシを使用した HTTPS をサポートするように WACS を設定する

HTTPS トラフィックを復号化し、復号化したトラフィックをアプリケーションサーバに転送するようにロードバランサとリバースプロキシサーバを設定できます。この場合、WACS を、HTTP またはプロキシ経由の HTTP を使用するように設定できます。

ロードバランサまたはリバースプロキシが HTTPS トラフィックを転送する場合に、リバースプロキシを使用した HTTPS を設定するには、2 つの WACS を作成します。1 つの WACS はリバースプロキシ経由の外部トラフィックの HTTPS 用、もう 1 つは内部ネットワーク上のクライアントとの HTTPS 経由の通信用に設定します。

13.1.9.4 WACS とファイアウォールの併用

ファイアウォールが設定された IT 環境に WACS をデプロイできます。

デフォルトでは、WACS は WACS がインストールされているマシン上のすべての IP アドレスにバインドします。クライアントと WACS 間でファイアウォールを使用する場合は、HTTP またはプロキシ経由の HTTP 用に WACS を強制的に特定の IP アドレスにバインドする必要があります。 これを行うには、[すべての *IP* アドレスに連結]チェックボックスをオフにし、バインドするホスト名または IP アドレスを指定します。

WACS サーバとデプロイメントの他の BI プラットフォームサーバ間にファイアウォールを使用する場合は、*SAP BusinessObjects Business Intelligence* プラットフォーム管理者ガイドの “SAP BusinessObjects BI プラットフォームコンポーネント間の通信について”の節を参照してください。

関連情報

BI プラットフォームコンポーネント間の通信について [184 ページ]

13.1.9.5 マルチホームマシンに WACS を設定する

マルチホームマシンは、複数のネットワークアドレスを持つマシンです。デフォルトでは、Web アプリケーションコンテナサーバインスタンスは HTTP ポートをすべての IP アドレスにバインドします。WACS を特定のネットワークインタフェースカード(NIC)にバインドする場合、たとえば WACS の HTTP ポートをある NIC にバインドし、要求ポートを別の NIC にバインドする場合は、次の操作を行います。

1. CMC の[サーバ]管理エリアを表示します。
2. 設定する WACS をダブルクリックします。
   [プロパティ]画面が表示されます。
3. [*Web* アプリケーションコンテナサービス] ペインの [プロキシ経由の *HTTP* の設定] セクションで、[すべての *IP* アドレスに連結] チェックボックスをオフにし、WACS をバインドする IP アドレスを入力します。
4. [*HTTP* 設定] セクションで、[すべての *IP* アドレスに連結] チェックボックスをオフにし、WACS をバインドする IP アドレスまたはホスト名を入力します。
5. [共通設定] の [自動割り当て] の選択を解除し、WACS とデプロイメントのその他の BI プラットフォームサーバ間の通信に使用するホスト名または NIC の IP アドレスを入力します。
6. [保存して閉じる]をクリックします。
7. WACS を再起動します。

13.1.10 Web アプリケーションプロパティの設定

WACS でホストされている Web アプリケーションのプロパティは、次の方法で設定することができます。

- 頻繁に変更されるプロパティは、WACS の設定可能なサービスプロパティとして公開されます。 これらのプロパティを編集するには、セントラル管理コンソール (CMC) で WACS の [プロパティ] ページを開き、適切なプロパティの値を変更して、[保存] をクリックします。
- WACS でホストされる Web アプリケーションのセッションタイムアウトを変更するには、まず、Web アプリケーションに CMC で設定可能なプロパティがあるかどうかを調べます。
  Web アプリケーションに CMC 内で変更できるプロパティがある場合、Web アプリケーションの `web_xml.ino` ファイルを変更します。 ファイルは `<WebAppName>_web_xml.ino` (`<WebAppName>` は Web アプリケーション名) で、`<EnterpriseDirectory>/java/pjs/services/<WebAppName>` ディレクトリ内にあります。
  Web アプリケーションに CMC 内で変更できるプロパティがない場合、Web アプリケーションの `web.xml` ファイルを変更します。 ファイルは `<EnterpriseDirectory>/warfile/webapps/<WebAppName>` にあります。`<WebAppName>` は Web アプリケーション名です。
- セッションタイムアウトまたは CMS 内において WACS の [プロパティ] 画面で表示されるプロパティ以外のプロパティを変更するには、Web アプリケーションの `.properties` ファイルを変更します。 詳細については、*SAP BI* プラットフォーム管理者ガイドの“BOE.war プロパティを介したアプリケーションの管理”の節を参照してください。

> ⓘ 注記
>
> WACS が起動または再起動されるたびに、ユーザの変更が毎回上書きされるため、`<EnterpriseDirectory>/java/pjs/container/work/<ServerFriendlyName>` ディレクトリ内の `web.xml`、`web_xml.ino`、または `.properties` ファイルを変更しないでください。

> ⓘ 注記
>
> WACS のプロパティを変更した後は、常に WACS を再起動する必要があります。

関連情報

サーバのプロパティを変更する [439 ページ]
BOE war ファイル [724 ページ]

13.1.11 トラブルシューティング

13.1.11.1 WACS にトレースを設定する

WACS のトレースを設定するには、コンポーネントのトレースのログ [1026 ページ]を参照してください。

13.1.11.2 サーバメトリクスを表示する

セントラル管理コンソール (CMC) から WACS のサーバメトリクスを表示できます。

1. CMC の[サーバ]管理エリアを表示します。
2. WACS を右クリックし、[メトリクス]をクリックします。

関連情報

Web アプリケーションコンテナサーバのメトリクス [1152 ページ]

13.1.11.3 WACS の状態を表示する

WACS の状態を表示するには、CMC の[サーバ]領域を表示します。[サーバの一覧]には、各サーバの状態を示す[状態]列が含まれています。

WACS には“実行中、エラーあり”というサーバ状態があります。この状態は、WACS が以下のエラー状態が 1 つ以上ある状態で実行されていることを意味します。

- HTTP、プロキシ経由の HTTP、または HTTPS コネクタが間違って設定されている
- トレースログサービスなどの WACS で実行されているサービスが適切に実行されていない
- Web アプリケーションの WACS へのデプロイに失敗した

WACS の [プロパティ] ページを参照して、どのサービスで障害が発生しているか確認してください。

13.1.11.4 ポート競合の解決

特定のポートから CMC にアクセスしようとしてもページが表示されない場合は、WACS 用に指定した HTTP、プロキシ経由の HTTP、または HTTPS のポートを別のアプリケーションが使用していないかどうかを確認してください。

WACS にポート競合があるかどうかを判断する方法は 2 とおりあります。デプロイメントに複数の WACS がある場合は、CMC にログオンし、[実行中の WACS コネクタの一覧] と [WACS コネクタがスタートアップ時に失敗しました] メトリクスを確認します。HTTP、プロキシ経由の HTTP、または HTTP コネクタが [実行中の WACS コネクタの一覧] に表示されない場合は、ポート競合のためにこれらのコネクタを起動できません。

デプロイメントに 1 つの WACS のみ存在する場合、またはどの WACS からも CMC にアクセスできない場合は、netstat などのユーティリティを使用して、別のアプリケーションが WACS ポートを使用していないかどうかを確認します。

13.1.11.4.1 HTTP ポートの競合を解決する

1. セントラル設定マネージャ(CCM)を起動し、[サーバの管理]アイコンをクリックします。
2. ログオン認証情報を指定します。
3. [サーバの管理]画面で、WACS を停止します。
4. [*Web Tier* 設定]アイコンをクリックします。

   > ⓘ 注記
   >
   > [*Web Tier* 設定]アイコンは、停止している WACS を選択した場合にのみ有効になります。

   [*Web Tier* 設定]画面が表示されます。
5. [*HTTP* ポート]フィールドで、Web アプリケーションコンテナサーバで使用する、空いている HTTP ポートを指定し、[*OK*]をクリックします。
6. [サーバの管理]画面で、WACS を起動します。

13.1.11.4.2 プロキシ経由の HTTP ポートまたは HTTPS ポートの競合を解決する

プロキシ経由の HTTP ポートまたは HTTPS ポートから WACS にアクセスできないが、HTTP ポートからセントラル管理コンソール(CMC)に接続できる場合は、CMC からポート番号を変更します。

1. CMC の[サーバ]管理エリアを表示します。
2. 設定する WACS を停止するには、サーバを右クリックし、[サーバの停止]をクリックします。
3. 設定する WACS をダブルクリックします。
   [プロパティ]画面が表示されます。
4. [プロキシ経由の *HTTP* の設定]セクションで、新しい HTTP ポートを指定します。
5. HTTPS ポートを変更するには、[*HTTPS* 設定]セクションの[*HTTPS* ポート]フィールドに新しい値を入力します。
6. [保存して閉じる]をクリックします。
7. WACS を起動するには、サーバを右クリックし、[サーバの起動]をクリックします。

13.1.11.5 メモリ設定を変更する

WACS のサーバパフォーマンスを向上させるには、サーバに割り当てられているメモリの量をセントラル設定マネージャ(CCM)から変更できます。

1. CCM を起動し、[サーバの管理]アイコンをクリックします。
2. CMC のログオン認証情報を指定します。
3. [サーバの管理]画面で、WACS を停止します。
4. [*Web Tier* 設定]アイコンをクリックします。

   > ⓘ 注記
   >
   > [*Web Tier* 設定]アイコンは、停止している WACS を選択した場合にのみ有効になります。

   [*Web Tier* 設定]画面が表示されます。
5. [コマンドラインパラメータ]で、コマンドラインを編集して新しいメモリ値を指定します。
   a. `-Xmx` オプションを探します。通常、このオプションには値が指定されています。
      たとえば、“-Xmx1g”などです。この設定では、1GB のメモリがサーバに割り当てられます。
   b. パラメータの新しい値を指定します。
      - 値を MB 単位で指定するには、“m”を使用します。たとえば、“**`-Xmx640m`**” と指定すると、640MB のメモリが WACS に割り当てられます。
      - 値を GB 単位で指定するには、“g” を使用します。たとえば、“**`-Xmx2g`**” と指定すると、2GB のメモリが WACS に割り当てられます。
   c. [*OK*]をクリックします。
6. [サーバの管理]画面で、WACS を起動します。

13.1.11.6 同時要求の数を変更する

WACS が処理するように設定されている同時 HTTP 要求のデフォルト数は 150 です。この値は、ほとんどのデプロイメントシナリオで使用できます。WACS のパフォーマンスを向上させるために、同時 HTTP 要求の最大数を増やすことができます。同時要求の数を増やすとパフォーマンスは向上しますが、増やしすぎるとパフォーマンスが低下する可能性があります。理想的な設定は、ハードウェア、ソフトウェア、および IT 要件によって決まります。

1. CMC の[サーバ]管理エリアを表示します。
2. 設定する WACS を停止するには、サーバを右クリックし、[サーバの停止]をクリックします。
3. 設定する WACS をダブルクリックします。
   [プロパティ]画面が表示されます。
4. [同時接続の設定 (コネクタ別)]の[最大同時接続要求]フィールドに同時要求の必要数を入力し、[保存して閉じる]をクリックします。
5. WACS を起動するには、サーバを右クリックし、[サーバの起動]をクリックします。

13.1.11.7 システムデフォルトを復元する

WACS を誤って設定した場合は、セントラル設定マネージャ (CCM) を使用してシステムデフォルトを復元できます。

1. CCM を起動し、[サーバの管理]アイコンをクリックします。
2. ログオン認証情報を指定します。
3. [サーバの管理]画面で、WACS を停止します。
4. [*Web Tier* 設定]アイコンをクリックします。

   > ⓘ 注記
   >
   > [*Web Tier* 設定] アイコンは、停止している WACS を選択した場合にのみ有効になります。

   [*Web Tier* 設定]画面が表示されます。
5. [システムデフォルトの復元]をクリックします。
6. 必要に応じて空いている HTTP ポートを指定し、[*OK*]をクリックします。
7. [サーバの管理]画面で、WACS を起動します。

13.1.11.8 ユーザによる HTTP 経由の WACS へのアクセスを禁止する

ユーザに HTTP または HTTPS 経由の WACS への接続をローカルマシンからのみ許可することが必要になる場合があります。たとえば、HTTP ポートを閉じることはできないが、WACS と同じマシンに存在するクライアントからの HTTP 要求のみ受け付けるように WACS を設定する場合などです。このように、WACS と同じマシンからブラウザを使用して WACS の保守または設定を行い、他のユーザにサーバへのアクセスを禁止することができます。

1. CMC の[サーバ]管理エリアを表示します。
2. 変更する WACS をダブルクリックします。
   [プロパティ]画面が表示されます。
3. [*Web* アプリケーションコンテナサービス] セクションで、[すべての *IP* アドレスに連結] チェックボックスをオフにします。
4. [ホスト名または *IP* アドレスに連結] フィールドに「**`127.0.0.1`**」と入力し、[保存して閉じる] をクリックします。
5. WACS を起動するには、サーバを右クリックし、[サーバの起動]をクリックします。
   このように設定した WACS は、ローカルマシンからの接続のみ受け付けます。

13.1.12 WACS プロパティ

WACS に対して設定できる一般プロパティ、HTTP、プロキシ経由の HTTP プロパティ、および HTTPS 設定プロパティについては、“サーバのプロパティに関する付録”の“コアサーバ設定”を参照してください。

関連情報

コアサービスのプロパティ [1110 ページ]

14　システムのバックアップと復元

14.1　バックアップと復元の概要

この章では、BI プラットフォームをバックアップする方法や、ハードウェア障害、ソフトウェア障害、およびデータの損失からシステムを復元する方法について説明します。バックアップおよび回復計画を実行するには、経験豊富な SAP BusinessObjects 専門家、システム管理者、およびデータベース管理者が必要です。

関連情報

システム全体のバックアップ [534 ページ]
BI コンテンツのバックアップ [539 ページ]
Windows 上の CCM でサーバ設定をバックアップする [537 ページ]
Unix のサーバ設定をバックアップする [538 ページ]
システムコピーの概要 [553 ページ]

14.2　用語

用語	定義
データレプリケーション	データレプリケーションとは、1 つ以上のデータのコピーを作成するプロセスのことです。コピーは、ミラーリングされたドライブの使用時などに、リアルタイムに更新されます。これにより、物理的なデータ損傷が発生しないようにリアルタイムにデータが保護されます。しかしドライブは常に更新されるため、データが破損した場合やデータを誤って削除した場合にはシステムを以前の状態に戻すことはできません。
バージョン管理	バージョニングでは、システムの特定のファイルに対して複数のバージョンが作成されます。この場合、システムを以前の状態に戻すことができます。 通常、すべてのデータバージョンが同じホストシステムに保存されます。このシステムが改ざんされたり損傷したりすると、現在のバージョンと以前のバージョンの両方を失うリスクがあります。同様に、復元機能では後で復元できるように "削除した" ファイルのコピーが保持されますが、元のデータと同じホストシステムに保存されることが一般的です。バージョニングでは、データが物理的に損傷 (ディスクの故障など) しないように保護することはできません。

用語	定義
ベアメタルシステムのバックアップ	ベアメタルシステムのバックアップでは、オペレーティングシステムを含めてファイルシステム全体がバックアップされます。ベアメタルシステムのバックアップは、ソフトウェアまたはオペレーティングシステムを含まないハードウェアに、バックアップシステムを復元するために使用します。 ベアメタルシステムのバックアップの場合、障害発生時、同一のハードウェア、または、復元ツールがハードウェア非依存の復元をサポートしている場合は任意のハードウェアに、OS を含むファイルシステム全体が復元されます。
ベアメタルシステムのバックアップとアプリケーションのバックアップの比較	ベアメタルシステムのバックアップでは、オペレーティングシステムを含めてシステム全体のコピーが作成されます。ベアメタルシステムのバックアップにより、システム全体を以前のバージョンに戻すことができます。 アプリケーションのバックアップでは、個々のアプリケーションに関連するファイルをバックアップします。 BI プラットフォームは、ベアメタルシステムのバックアップはサポートしますが、アプリケーションのバックアップはサポートしません。 ベアメタルシステムのバックアップの場合、障害発生時、同一のハードウェア、または、復元ツールがハードウェア非依存の復元をサポートしている場合は任意のハードウェアに、OS を含むファイルシステム全体が復元されます。 BI プラットフォームの完全システムバックアップは、バックアップセットと呼ばれます。
バックアップセット	バックアップセットは、同時に作成される次の個別のバックアップで構成されています。 • CMS システムデータベースのバックアップ • オペレーティングシステムを含めた、BI プラットフォームデプロイメント内のすべてのマシンのファイルシステム全体のベアメタルバックアップです。 • 入力 FRS および出力 FRS ファイルストアのバックアップ (BI プラットフォームファイルシステムに含まれていない場合) • Web Tier コンポーネントのバックアップ (BI プラットフォームファイルシステムの一部として含まれていない場合) • 監査データベースのバックアップ
コールドバックアップとホットバックアップの比較	コールドバックアップは、システムが停止してユーザが利用できないときに実行されます。ホットバックアップは、システムが実行中でユーザが使用できる間に実行されるため、バックアップの実行時にデータが変更される可能性があります。また、ホットバックアップの実行時には、バックアップ手順の順番どおりに実行する必要がありますが、コールドバックアップではこの限りではありません。 BI プラットフォームは、コールドバックアップとホットバックアップの両方をサポートします。 ホットバックアップは、“オンラインバックアップ”とも呼ばれます。

14.3 バックアップおよび復元の使用事例

以下の表で、達成すべき目標と、前提となる現在のリソースを説明し、最も適切なバックアップソリューションへと導きます。

目標	必要なリソース	解決策
目標: システムの復元 1. BI プラットフォームシステムが故障しました。そのため、システムを最後にバックアップした作業状態に復元する必要があります。 2. BI プラットフォームをホストするマシンが壊れました。壊れたマシンを新しいマシンに入れ替える必要があります。	• 同一ハードウェアを使用するターゲットシステムからソースシステム および • ソースシステムのバックアップ	このガイドで説明するシステムバックアップおよび復元ワークフローを使用します。システム全体のバックアップ [534 ページ]の手順を参照してください。ソースシステムのバックアップからターゲットシステムを再作成します。
目標: オブジェクトの復元 誤って削除したドキュメントやその他のオブジェクトを復元します。	• ソースシステムデータベースおよびファイルのバックアップ および • ソースシステムからエクスポートする [557 ページ] で説明している詳細なシステム情報	バックアップを使用し、“BI プラットフォームデプロイメントのコピー”に関する章にあるシステムコピーのワークフローを使用して、別のマシンにシステムのコピーを作成します。次に、プロモーションマネジメントツールを使用して、誤って削除したオブジェクトを新しいシステムから昇格します。システムのコピーの計画 [554 ページ]のシステムコピーワークフローを参照し、この章の残りの手順に従います。 **注記** ターゲットシステムは、同じリリース、サポートパッケージ、およびパッチレベルの既存の BI プラットフォームデプロイメントがインストールされたコンピュータか、BI プラットフォームがインストールされていない "クリーンな" コンピュータに作成できます。
目標: オブジェクトの復元 2 誤って削除したドキュメントやその他のオブジェクトを復元します。	プロモーションマネジメントバージョニングが使用されているシステム	プロモーションマネジメントアプリケーションを使用して、ドキュメントの以前のバージョンを復元します。詳細については、プロモーションマネジメントについての関連トピックを参照してください。

注記

ソフトウェアのアップグレード前後のシステムのバックアップ:

CMS は製品の 'バージョン' に関連付けられています。SAP BusinessObjectsBusiness Intelligence プラットフォームシステムを、異なるバージョンの CMS と FRS とともに使用することはできません。ソフトウェアをアップグレードする前後に必ず CMS と FRS ファイルストアの両方をバックアップしてください。'復元' に

よりソフトウェアのアップグレードをロールバックする場合は、CMS、FRS、およびソフトウェアがすべて同じバージョンに属していることを確認する必要があります。

関連情報

バックアップ [533 ページ]
システムのコピーの計画 [554 ページ]
概要 [564 ページ]

14.4 バックアップ

バックアップおよび回復計画は、自然災害または予期せぬ不具合によるシステム障害が発生したときに備えて実行される手順で構成されます。この計画の目的は、基幹機能を維持し、すばやく再開できるように、災害による日常業務への影響を最小限に抑えることです。

BI プラットフォームデプロイメントをバックアップする際には、次の 3 つのオプションが使用できます。

- システム全体のバックアップ。システム全体を復元することができますが、この場合、システムの一部のみを復元することはできません。バックアップから BI プラットフォームを復元する代わりに再構築する場合は、システムコピーについて説明している関連トピックを参照してください。
- サーバ設定のバックアップ。他のオブジェクトを復元することなくサーバ設定のみを復元でき、システムの BI コンテンツの現在の状態が保持されます。
- BI コンテンツ (ドキュメントなど) のバックアップ。すべてのオブジェクトを復元しなくとも BI コンテンツの一部を選択的に復元できます。

3 種類すべてのバックアップに関する詳細は、関連トピックを参照してください。

→ ヒント

データの損失を防ぐために、定期的にバックアップを実行します。

→ ヒント

BI プラットフォームシステムをバックアップしてから同一または別のホストコンピュータに復元し、システムのコピーを作成できます。

関連情報

システム全体のバックアップ [534 ページ]
サーバの設定のバックアップ [537 ページ]
BI コンテンツのバックアップ [539 ページ]
システムコピーの概要 [553 ページ]

14.4.1 システム全体のバックアップ

コールドバックアップまたはホットバックアップを実行して BI プラットフォームシステム全体をバックアップし、バックアップセットを作成します。さまざまな時点の複数のバックアップセットを保持しておくことで、システム復元時の選択肢が広がります。組織のビジネスニーズに必要な頻度で、システムをバックアップします。

BI プラットフォームシステムを停止してコールドバックアップを実行することも、ホットバックアップを実行することもできます。ホットバックアップでは、システムはバックアップ処理中でも稼動しており、使用可能です。これにはシステムのダウンタイムを回避できるというメリットがあります。

> ⓘ 注記
>
> トランザクションログはメインのデータベースサーバシステム以外のファイルシステムに書き込み、定期的にこのトランザクションログをバックアップして、バックアップ設定内の他のファイルと共に保存することをお勧めします。

> ⓘ 注記
>
> 監査データをバックアップする場合は、バックアップファイルセットに監査データベースのデータベーストランザクションログが含まれていることを確認してください。監査一時ファイルはバックアップに含める必要はありません。

14.4.1.1 ホットバックアップ

ホットバックアップ機能を使用すると、ユーザによるシステムの通常使用を中断することなく BI プラットフォームシステムをバックアップできます。システムのバックアップ中も営業を続ける必要がある場合、セントラル管理コンソールでホットバックアップを有効化して設定します。

[ホットバックアップ最長持続時間] 設定では、バックアップの予測最大時間 (CMS バックアップの開始時間から、FRS バックアップの終了時間まで) を指定します。指定した時間が短すぎると、バックアップによるファイルのコピーが完了する前にファイルが削除される可能性があります。この問題を回避できるように所要時間を多めに見積もっておくと安全です。値が大きいと FRS ファイルストアサイズが若干増大するため、この問題とシステムリソースのバランスを取ってください。

> ⓘ 注記
>
> - ホットバックアップでは、実際にはバックアップは実行されず、ファイルの削除が遅延するだけです。ファイルが編集または更新されると、複数のコピーが保持されます。これは、CMS と FRS が常に正しい関係を保ち、それぞれのバックアップを異なる時間に作成できることを意味します。ただし、これは [ホットバックアップ] ウィンドウ内で行われます。
> - システムをリストアすると、FRS に余分なファイルが多数残ります。これらは、リポジトリ診断ツールで削除する必要があります。
> - CMS バックアップは、常に FRS ファイルストアをバックアップする前に開始してください。
>
> ホットバックアップは、CMC で [ホットバックアップの有効化] チェックボックスが選択されている場合に有効であり、[ホットバックアップ最長持続時間] 設定は、ホットバックアップが有効であるかどうかに影響を与えません。

特定のバックアップ時間にシステムを復元することは非常に簡単です。たとえば、システムバックアップが毎日午前 3 時に実行される場合、CMS システムのバックアップが開始されたときの状態 (選択した日付の午前 3 時) に

システムを簡単に復元できます。CMS データベースまたは監査データベースで障害が発生した場合も、CMS データベースまたは監査データベースでトランザクションロギングを有効にしていれば、システムを障害発生直前の状態に復元できます。

最大限の安全性を確保するため、トランザクションロギングレコードを、プライマリデータベースのバックアップレコードとは異なる場所に保存してください。これにより、データベース障害が発生した場合でも、データベースを障害発生前の状態に復元できます。

> ⓘ 注記
>
> 古いバージョンの IBM DB2 のトランザクションログサイズの制限のため、ホットバックアップおよびトランザクションログ関連のタスクは、CMS システムデータベースが DB2 データベースサーババージョン 9.5 FixPack 5 以上 (9.5 系用)、および 9.7 FixPack 1 以上 (9.7 系用) 上でホストされている場合にのみサポートされます。

> ⓘ 注記
>
> トランザクションログはメインのデータベースサーバシステム以外のファイルシステムに書き込み、定期的にこのトランザクションログをバックアップして、バックアップ設定内の他のファイルと共に保存することをお奨めします。

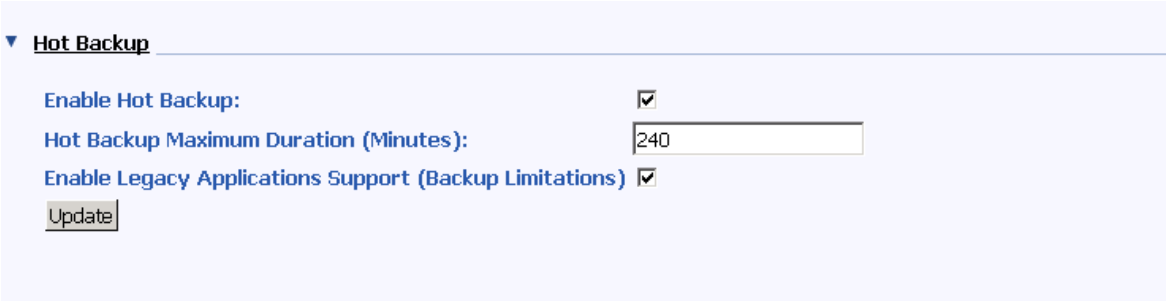
14.4.1.1.1 ホットバックアップを有効にする

1. セントラル管理コンソール (CMC) を開きます。
2. [管理] 領域で、[設定] ページを開きます。
3. [ホットバックアップ] セクションで、[ホットバックアップの有効化] を選択します。
4. [ホットバックアップ最長持続時間 (分)] でバックアップの予測最大時間 (分) を入力します。

   BI プラットフォームホストマシンの CMS データベースとファイルシステムの両方のバックアップに必要な時間を含めるようにします。

   > ⓘ 注記
   >
   > 実際のバックアップ時間がここで入力した上限を超えた場合、バックアップデータに不整合が生じる可能性があります。この問題を回避できるように所要時間を多めに見積もっておくと安全です。

5. [更新] をクリックします。
   ホットバックアップが有効になります。



ホットバックアップのサポートが有効になると、データベースおよびファイルシステムのベンダーのバックアップツールを使用してバックアップを実行できます。

14.4.1.2 システムのホットバックアップまたはコールドバックアップを実行する

ホットバックアップを実行する場合、最初に、ホットバックアップの前提条件および詳細情報に関する関連トピックを参照してください。コールドバックアップを実行する場合は、BI プラットフォームデプロイメント内のすべてのノードを停止します。

> ⚠ 警告
>
> ホットバックアップを有効化せず、またすべてのノードを停止せずにバックアップを実行する場合、CMS データベースと FRS ファイルストア間でのデータの不一致が発生する場合があります。

> ⓘ 注記
>
> ホットバックアップの場合、説明されている順番で手順を開始することが重要です。コールドバックアップの場合、手順はどの順番でも実行可能です。いずれの場合でも、次の手順を開始する前に各バックアップ手順が完了するまで待機する必要はありません。

1. データベースベンダーのツールを使用して、Central Management Server (CMS) システムデータベースをバックアップします。

   > ⓘ 注記
   >
   > ホットバックアップの場合、データベースベンダーのバックアップツールはオンラインのアトミックモードで使用してください。

2. データベースベンダーのツールをオンラインのアトミックモードで使用して、BI プラットフォームの監査データベースをバックアップします。
3. オペレーティングシステムを含めた、BI プラットフォームデプロイメント内のすべてのマシンのファイルシステム全体をバックアップします。Unix マシンの場合、インストールアカウントのインストールディレクトリとホームディレクトリをバックアップします。
   a. 入力および出力 FRS ファイルストアが BI プラットフォームのバックアップに含まれていない場合 (ホストマシンが異なる場合) は、ファイルバックアップツールを使用して、両ファイルのバックアップコピーを作成します。
   b. Web Tier コンポーネントが BI プラットフォームのバックアップに含まれていない場合 (ホストマシンが異なる場合) は、ファイルバックアップツールを使用してバックアップコピーを作成します。

   ホットバックアップの場合は、可能な限りアトミックなファイルバックアップツールを使用してください。

コールドバックアップを実行した場合、すべてのバックアップが完了するまで待機してから BI プラットフォームノードを起動します。

関連情報

ホットバックアップ [534 ページ]

14.4.2 サーバの設定のバックアップ

誤ったサーバの設定からシステムを保護するために、定期的にサーバの設定を BIAR ファイルにバックアップしてください。利用可能なサーバのバックアップを保持することによって、Central Management Server (CMS) システムデータベース、ファイルリポジトリ、または Business Intelligence コンテンツを復元する必要なく、設定を復元できます。

システムのデプロイメントに変更を加える場合は、必ずサーバの設定をバックアップすることが重要です。これには、ノードの作成、ノード名の変更、ノードの移動と削除、およびサーバの作成または削除が含まれます。設定の変更を行う前に、サーバの設定をバックアップし、行った変更を確認した後にもう一度バックアップすることをお勧めします。

> ⓘ 注記
>
> サーバの設定のバックアップは、CMS および FRS ファイルストアのバックアップの追加タスクではありません。つまり、CMS/FRS を復元すると、サーバの設定も復元されます。サーバの設定のバックアップは、CMS データベースの完全なバックアップの一部のサブセットです。CMS を復元している場合は、サーバの設定を復元する必要はありません。

セントラル設定マネージャ (CCM) またはスクリプトを使用して、BI プラットフォームサーバの設定を BIAR ファイルにバックアップし、別のマシンまたは記憶媒体に BIAR ファイルを格納します。

> ⓘ 注記
>
> SSL が有効化されているデプロイメントでサーバ設定をバックアップまたは復元する場合は、まず CCM によって SSL を無効化してから、バックアップまたは復元が完了したら再有効化する必要があります。

Windows では、`BackupCluster.bat` スクリプトはディレクトリ `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥scripts` にあります。

Unix では、`backupcluster.sh` スクリプトは `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts` ディレクトリにあります。

14.4.2.1 Windows 上の CCM でサーバ設定をバックアップする

この手順では、クラスタ全体のサーバの設定をバックアップします。個別のサーバの設定をバックアップすることはできません。

> ⓘ 注記
>
> 一時 CMS を使用している場合は、ローカル CMS のバイナリがインストールされているマシン上で CCM を使用する必要があります。

1. CCM を起動し、ツールバーで [サーバ設定のバックアップ] をクリックします。
   [サーバ設定バックアップウィザード] が表示されます。
2. [次へ] をクリックし、ウィザードを開始します。
3. 既存の CMS を使用したサーバ設定のバックアップ、または一時 CMS の作成のいずれかを指定します。
   - 実行中のシステムからサーバの設定をバックアップするには、[稼働中の既存 *CMS* の使用] を選択し、[次へ] をクリックします。

- 実行中でないシステムからサーバの設定をバックアップするには、[新規一時 *CMS* の起動] を選択し、[次へ] をクリックします。

4. 一時 CMS を使用している場合は、一時 CMS の実行に使用するポート番号を選択し、データベース接続情報を指定します。

   システムの復元中にユーザがシステムにアクセスするリスクを最小限にするには、既存の CMS が使用しているものとは異なるポート番号を指定します。

5. クラスタキーを入力し [次へ] をクリックして続行します。
6. 入力を求められたら、システムと、管理権限のあるアカウントのユーザ名とパスワードを指定して CMS にログオンし、[次へ] をクリックします。
7. サーバ設定のバックアップ先にする BIAR ファイルの場所と名前を指定し、[次へ] をクリックして続行します。
   [確認] ページに入力した情報が表示されます。
8. [確認] ページに表示された情報が正しいことを確認し、[完了] をクリックして続行します。
   CCM によって、指定した BIAR ファイルにクラスタ全体のサーバ設定がバックアップされます。バックアップ手順の詳細は、ログファイルに書き込まれます。ログファイルの名前とパスはダイアログボックスに表示されます。
9. 復元操作が失敗した場合は、ログファイルを確認して原因を特定します。
10. [*OK*] をクリックし、ウィザードを閉じます。

14.4.2.2 Unix のサーバ設定をバックアップする

Unix では、`serverconfig.sh` スクリプトを使用して、デプロイメントのサーバ設定を BIAR ファイルにバックアップします。

1. [*5 - サーバ設定のバックアップ*] を選択し、`Enter` キーを押します。

```
-----------------------------------------------------------

            SAP BusinessObjects

What do you want to do?

1 - Add node
2 - Delete node
3 - Modify node
4 - Move node
5 - Back up server configuration
6 - Restore server configuration
7 - Modify web tier configuration
8 - List all nodes


[quit(0)]
-----------------------------------------------------------

[8]5
```

2. 既存の CMS を使用したサーバ設定のバックアップ、または一時 CMS の作成のいずれかを指定します。

- 稼動中のシステムからサーバ設定をバックアップするには、[既存] を選択して Enter キーを押します。
- 稼動していないシステムからサーバ設定をバックアップする場合、またはサーバ設定を復元する場合は、[一時] を選択して Enter キーを押します。

3. 一時 CMS を使用してサーバ設定をバックアップする場合は、以降の複数の画面で、使用する一時 CMS のポート番号および CMS システムデータベースへの接続情報を選択します。

   システムの復元中にユーザがシステムにアクセスするリスクを最小限にするには、既存の CMS が使用しているものとは異なるポート番号を指定します。
4. 入力を求められたら、システムおよび管理権限のあるアカウントのユーザ名とパスワードを指定して Enter キーを押し、CMS にログオンします。
5. 入力を求められたら、サーバ設定のバックアップ先の BIAR ファイルの場所と名前を指定して Enter キーを押します。
   概要ページに、入力した情報が表示されます。
6. 表示された情報が正しいことを確認し、Enter キーを押して続行します。
   `serverconfig.sh` スクリプトによって、クラスタ全体のサーバ設定が、指定した BIAR ファイルにバックアップされます。バックアップ手順の詳細は、ログファイルに書き込まれます。ログファイルの名前とパスが表示されます。
7. 復元操作が失敗した場合は、ログファイルを確認して原因を特定します。

14.4.2.3 スクリプトを使用してサーバ設定をバックアップする

`BackupCluster.bat` ファイル (Windows の場合)、または `backupcluster.sh` スクリプト (Unix の場合) を実行して、デプロイメントのサーバ設定をバックアップすることができます。

Windows では、`BackupCluster.bat` ファイルは、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥scripts` ディレクトリにあります。

Unix では、`backupcluster.sh` は `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts` ディレクトリにあります。

関連情報

BackupCluster スクリプトおよび RestoreCluster スクリプト [550 ページ]

14.4.3 BI コンテンツのバックアップ

標準のデータベースとファイルバックアップツールと手順を使用して、以下のコンテンツを定期的にバックアップすることをお勧めします。

- CMS データベース
- 入力 FRS および出力 FRS ファイルストア

最新のコンテンツをバックアップすることにより、システム全体またはサーバ設定の復元を行わずに、ビジネスインテリジェンスを復元することが可能になります。

システムのバックアップの詳細については、システムのホットバックアップまたはコールドバックアップを実行する [536 ページ] を参照してください。

14.5 システムの復元

システムが破損している場合は、システム全体を復元することができます。これにより BI プラットフォームが復元されます。システムの状態によっては、完全復元が不要な場合があります。システムは正常に機能しているが、失われたり破損したりしたコンテンツがある場合は、Business Intelligence (BI) コンテンツのみを復元することができます。BI コンテンツは有効だがプラットフォームサーバの設定が適切でなくなった場合は、サーバ設定のみを復元することができます。

手順は、ホットバックアップとコールドバックアップのどちらから復元する場合でも同じです。

関連情報

システム全体の復元 [540 ページ]
サーバ設定の復元[サーバセッテイノフクゲン] [547 ページ]
BI コンテンツの復元 [550 ページ]

14.5.1 システム全体の復元

システム全体を復元する場合は、BI プラットフォームのクラスタも復元されます。システム内の障害の内容によっては、一部の復元しかできない場合があります。

次のコンポーネントのいずれかに障害が発生しているか失われている場合、システム全体を復元する必要があります。

- CMS データベース

  > **注記**
  >
  > データベースサービスがクラッシュした場合は、システム全体を復元することなく単にサービスを再起動することができます。

- FRS ファイルストア
- マシンのファイルシステム

> **注記**
>
> システム全体を復元する場合、ターゲットシステムに BI プラットフォームがすでにインストールされている必要はありません。

監査データベースのみが破損または失われている場合は、システム全体を復元することなく監査データベースを復元することができます。

Web Tier コンテンツが破損または失われている場合は、システム全体を復元することなく Web Tier コンテンツを復元することができます。

関連情報

システム全体を復元する [541 ページ]
監査データベースのみを復元する [543 ページ]
Web Tier コンテンツを復元する [543 ページ]
CMS データベースのみを復元する [543 ページ]

14.5.1.1 システム全体を復元する

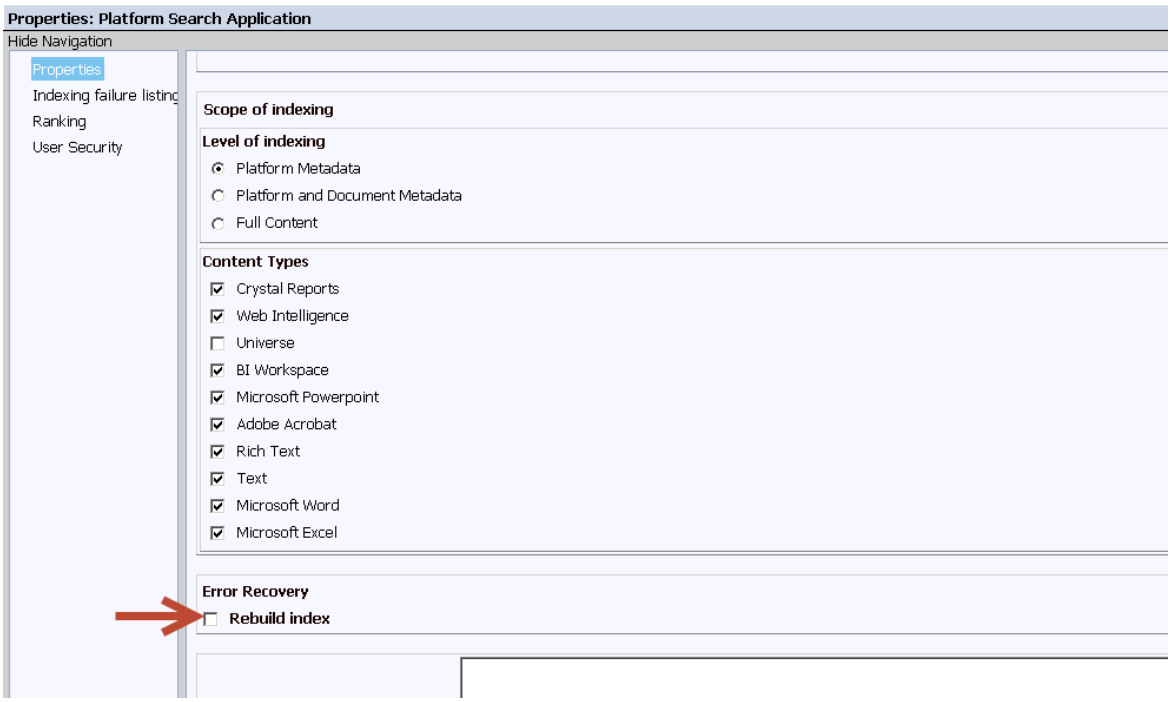
システムを復元する前に、セントラル設定マネージャ (CCM) を使用して、BI プラットフォームデプロイメントのすべてのノードを停止する必要があります。さらに、システムをどの時点に復元するかを選択する必要があります。

> ⓘ 注記
>
> システムを現在の状態に復元する可能性がある場合は、復元する前にシステムをバックアップしてください。

1. 次のバックアップファイルを見つけます。
   - CMS データベースのバックアップ
   - 入力 FRS および出力 FRS ファイルストアのバックアップ
   - BI プラットフォームクラスタ内のすべてのホストマシンのファイルシステムのバックアップ

   > ⓘ 注記
   >
   > - バックアップを確認して、上記すべてのファイルが同じバックアップセットのものであることを確認してください。
   > - バックアップと復元を実行する場合、CMS と FRS は一体として扱われます。一方を復元する場合は、同時にもう一方も復元する必要があります。
   > - バックアップセットがホットバックアップとして取得された場合、CMS データベースのバックアップ開始タイムスタンプが、適合する FRS ファイルストア、Web Tier、およびホストマシンファイルシステムのタイムスタンプよりも早いことを確認してください。障害が発生しているコンポーネントが 1 つのみの場合でも、これらすべてのファイルが必要になります。
2. ファイル復元ツールを使用して、BI プラットフォームクラスタ内のすべてのホストマシンのファイルシステムを復元します。
3. ファイル復元ツールを使用して、入力および出力 FRS ファイルストアを復元します。
4. データベースツールを使用して、CMS データベースを復元します。
5. CMS データベースのバックアップの作成以降にこのデータベースのパスワードを変更した場合は、CCM を使用して、すべてのノードと BI プラットフォームのホストマシンで CMS データベースのパスワードを更新します。
6. 監査機能を使用する場合は、データベースツールを使用して監査データベースを復元します。

7. 次のいずれかのオプションを使用して、検索インデックスを復元します。
   - 検索インデックス復旧スクリプトを実行する場合は、検索インデックス復旧スクリプトを実行する [545 ページ]を参照して、記載されている手順に従います。これにより、フルインデックスがより高速になります。
   - 復旧スクリプトを使用しないで検索インデックスを再構築する場合は、CCM を使用して BI プラットフォームのノードを再起動します。この方が手順としては簡単ですが、インデックスの再構築時は、プラットフォームデータへの部分検索アクセスしか実行できません。



8. システムを起動し、後で必要な手順で使用するために時間を記録してください。
9. システムが正常に機能していることを確認し、サニティテストを実行します。

システムを確認したら、次の操作を実行します。

- リポジトリ診断ツールを実行し、使用されていないすべての一時ファイルを削除してリポジトリの整合性を確認します。このガイドの「リポジトリ診断ツール」の節を参照してください。
- インデックス復元スクリプトを使用しなかった場合は、プラットフォーム検索インデックスを再構築します。
- システムがバックアップされた時点で処理中だったすべての公開ジョブは、失敗と表示されます。これらのインスタンスは再実行せずに、新しい公開ジョブを開始します。
- 監査データベースが復元された場合は、SQL クエリを実行して、データベースの障害発生時と再起動時間 (手順 8 で記録した時間) の範囲内のすべてのイベントを削除する必要があります。例:`delete from [DB_NAME].ADS_EVENT where Start_Time > '<[time of DB failure]>' and Start_Time < '<[time of DB restoration]>'`

関連情報

CMS リポジトリコンテンツのインデックス処理 [909 ページ]

14.5.1.2 監査データベースのみを復元する

監査データベースを復元する前に、セントラル設定マネージャ (CCM) を使用して、BI プラットフォームデプロイメントのすべてのノードを停止します。さらに、データベースをどの時点に復元するかを選択する必要もあります。

> ⓘ 注記
>
> このタスクは、BI プラットフォームの改ざんされたコンポーネントが監査データベースのみである場合に実行してください。その他のコンポーネントが影響を受けている場合は、システム全体を復元する必要があります。

データベースツールを使用して、監査データベースを復元します。

関連情報

システム全体を復元する [541 ページ]

14.5.1.3 Web Tier コンテンツを復元する

Web Tier コンテンツを復元する前に、セントラル設定マネージャ (CCM) を使用して BI プラットフォームデプロイメント内のすべてのノードを停止する必要があります。さらに、Web Tier コンテンツをどの時点に復元するかを決定することも必要です。

システムを現在の状態に戻す場合は、復元する前にシステムのバックアップを実行する必要があります。

Web Tier が破損した場合は、個別に復元することができます。

1. ファイル復元ツールを使用して、Web Tier ホストマシン上の Web Tier フォルダを復元します。
2. CCM を使用して BI プラットフォームデプロイメントのすべてのノードを再起動します。

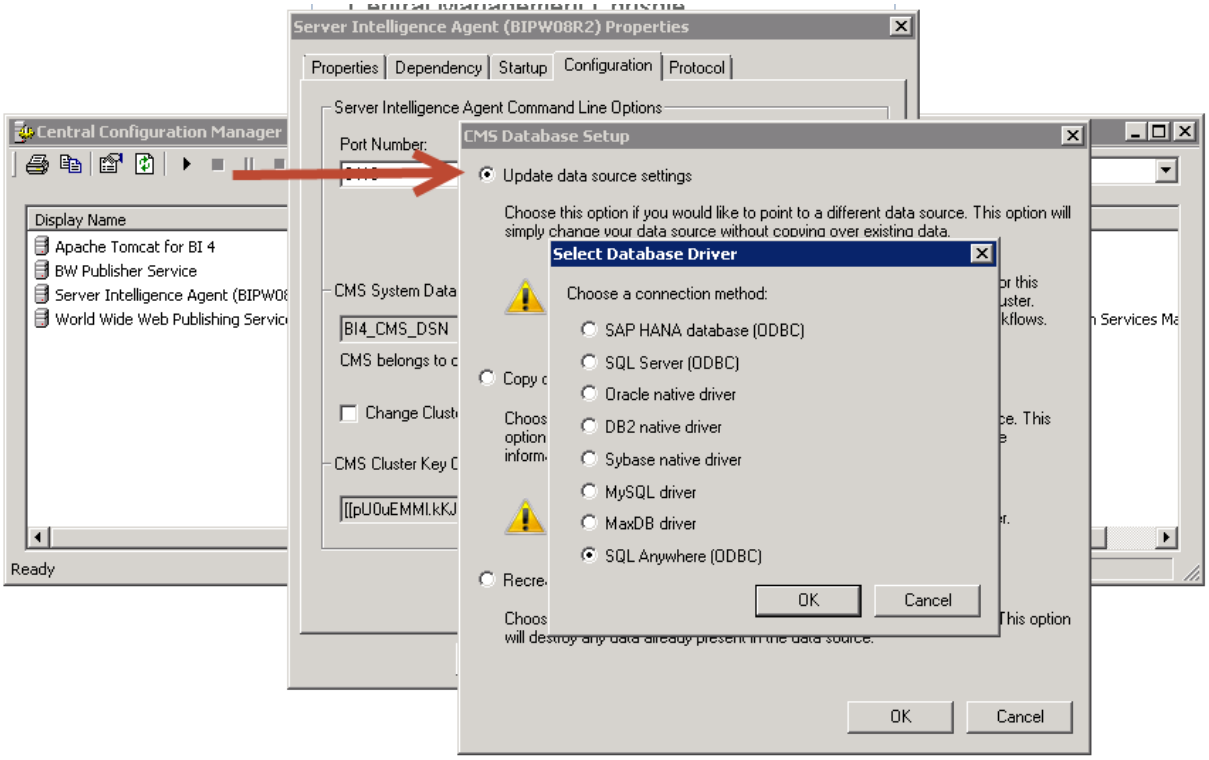
14.5.1.4 CMS データベースのみを復元する

> ⓘ 注記
>
> データベースサービスがクラッシュした場合は、システム全体を復元することなく単にサービスを再起動することができます。CMS データベースが破損した場合、または他のコンポーネントが改ざんされた場合は、システム全体を復元する必要があります。

CMS データベースのホストマシンを修復するか、置き換えます。置き換えた場合は、システム名、ポート設定、およびデータベース認証情報が以前のホストマシンと同じであることを確認します。

> **注記**
>
> 同じ名前と認証情報を使用してマシンを復元できない場合は、CCM を使用して、クラスタ内の各ノードでこのデータベース接続情報を更新し、それらのノードを再起動する必要があります。

Widows の場合:



UNIX の場合:cmsdbsetup.sh を実行し、プロンプトが表示されたらノード名を入力して、オプション 6 `update` を選択します。

```
-------------------------------------------------------

           SAP BusinessObjects


Current CMS Data Source: BI4_CMS_DSN_1381344842

Current cluster name: LRHEL57x64:6400

Current cluster key: [[pU0uEMMl.kKJPezTK002bw]]


update (Update Data Source Settings)
reinitialize (Recreate the current data surce)
copy (Copy data from another Data Source)
change cluster (Change current cluster name)
change cluster key (Change current cluster key)


[update(6)/reinitialize(5)/copy(4)/change cluster(3)/change cluster key(2)/back(1)/quit(0)]
-------------------------------------------------------

[update]6
```

1. CCM を使用して BI プラットフォームのすべてのノードを停止します。
2. データベースツールを使用して、監査データベースを復元します。
3. CCM を使用して BI プラットフォームのノードを起動します。

システムが適切に機能していることを確認したら、次の操作を実行します。

- リポジトリ診断ツールを実行し、使用されていないすべての一時ファイルを削除してリポジトリの整合性を確認します。このガイドの「リポジトリ診断ツール」の節を参照してください。
- システムがバックアップされた時点で処理中だったすべての公開ジョブは、失敗と表示されます。これらのインスタンスは再実行せずに、新しい公開ジョブを開始します。

関連情報

CMS リポジトリコンテンツのインデックス処理 [909 ページ]

14.5.1.5 検索インデックスの復旧

プラットフォーム検索機能では、検索効率が向上するように、システム全体の一連のインデックスと情報ファイルが保持されています。システムを復元する必要がある場合、これらの情報ファイルで不整合が生じている可能性があります。このような不整合を修復するために、インデックス復旧スクリプトまたはインデックスの再構築を行うことができます。

インデックスの再構築は直接的な手法ですが、この処理は大量のリソースを消費し、かつ終了までに時間が掛かります。また、再構築中に行なわれた検索はデータベースの再構築化された部分の結果のみを返します。復旧スクリプトにはより複雑な手順が必要になりますが、完全で実用的なインデックスをより早く取得できます。

複数のコンピュータが含まれるデプロイメントを復元する場合は、検索サービスがホストされているすべてのコンピュータでスクリプトを実行します。クラスタの最初のコンピュータで、`-Both` オプションを使用した後に、`-ContentStore` オプションを使用するクラスタのすべての後続のコンピュータに使用します。

関連情報

CMS リポジトリコンテンツのインデックス処理 [909 ページ]

14.5.1.5.1 検索インデックス復旧スクリプトを実行する

- CMS が実行中であることを確認して、検索サービスがインストールされているすべての Adaptive Processing Server (APS) を停止します。

  > ⓘ 注記
  >
  > ノードの開始後、できるだけ早くこれらの APS を停止する必要があります。

- JAVA_HOME を BI プラットフォームのインストールディレクトリの場所の sapjvm/bin に設定します。
- プラットフォーム検索データのディレクトリは、スクリプトを実行中のマシンからアクセス可能です。

1. CMS ホストマシンまたは APS ホストマシンで、コマンドラインウィンドウを開きます (Windows OS を使用している場合)。
2. ディレクトリを <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib¥ に変更します。

   Unix マシンでは、同様の Unix ファイルパスを使用します。
3. java -jar platformSearchOnlineHotbackupRestore.jar と入力し、*Enter* キーを押します。
4. プロンプトが表示されたら、次の情報を入力して *Enter* キーを押します。
   - BI プラットフォームのインストールの場所 (例: <INSTALLDIR>/SAP businessObjects Enterprise XI 4.0)
   - CMS 名、ユーザ ID、パスワード、および認証の種類を含む、CMS のログオン認証情報認証の種類には、次のオプションがあります。
     - secEnterprise
     - secLDAP
     - secWinAD
     - secSAPR3
5. インデックスの復元の種類を指定するよう求められた場合は、次のいずれかのオプションを入力して *Enter* キーを押します。

値	説明
-Both	これは、単一サーバのデプロイメントに使用されるか、または複数マシンのデプロイメントで検索サービスを含む最初の APS ホストマシンに使用されます。 複数検索 APS を利用するシステムで、スクリプトが最初に実行されるとき、-Both 値を使用します (データベースおよびコンテンツストアを更新)。その他のすべての検索 APS でスクリプトが実行される場合、-ContentStore 値を使用します (コンテンツストアのみを更新)。
-ContentStore	これは、スクリプトが実行されるクラスタの最初のコンピュータではない場合に、検索サービスがインストールされている APS ホストマシンでのスクリプト実行時に使用されます。
-Exit	インデックスの復元を実行せずにスクリプトを終了します。

6. スクリプトの実行が完了したら、コマンドラインウィンドウを閉じます (Windows マシンの場合)。

停止したすべての APS を開始します。

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0
\java\lib>java  -jar platformsearchOnlineHotbackupRestore.jar
Enter the BOE install location :
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0

Enter the CMS Credentials:
CMS NAME: BIPW08R2
USER NAME: Administrator
PASSWORD:
AUTHENTICATION: secEnterprise
BOE Install Location = C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessOb
jects Enterprise XI 4.0 CMS = BIPW08R2  User = Administrator    Authentication =
 secEnterprise

Please verify if the details given above are correct(y/n)...Press 'e' if you wan
t to exit  :y
 What would you like to restore?
 1. Index ?
 2. Content Store ?
 3. Both Index and Content Store (Choose this option only when index and content
 store are present on one node) ?
 4. Exit ?
3_
```

14.5.2 サーバ設定の復元[サーバセッテイノフクゲン]

システムのサーバ設定を BIAR ファイルから復元する必要がある場合は、セントラル設定マネージャ (CCM) または RestoreCluster スクリプトを使用してサーバ設定を復元できます。 BIAR ファイルからサーバコンテンツを復元しても、レポート、ユーザおよびグループ、またはセキュリティ設定などの Business Intelligence コンテンツには影響がありません。

> ⓘ 注記
>
> サーバ設定を復元する場合、クラスタ全体の設定の復元のみがサポートされます。 クラスタ内の一部のサーバのみの設定を復元することはできません。

> ⓘ 注記
>
> SSL が有効化されているデプロイメントでサーバ設定をバックアップまたは復元する場合は、まず CCM によって SSL を無効化してから、バックアップまたは復元が完了したら再有効化する必要があります。

14.5.2.1 Windows 上の CCM を使用してサーバ設定を復元する

セントラル設定マネージャ (CCM) を使用してサーバ設定を復元できます。サーバ設定を復元したら、システムのクラスタにあるすべてのコンピュータ上で、システムのノードを再作成する必要があります。

1. 各ノードで Server Intelligence Agent を停止することによって、サーバ設定を復元するクラスタ内のすべてのコンピュータのすべてのノードを停止します。
2. CMS がインストールされているコンピュータの CCM を起動します。
3. ツールバーから、[サーバ設定の復元] をクリックします。
   [サーバ設定復元ウィザード] が表示されます。
4. [次へ] をクリックし、ウィザードを開始します。

5. 入力画面が表示されたら、一時 Central Management Server (CMS) に使用するポート番号と、CMS システムデータベースに接続するための情報を入力し、[次へ] をクリックして続行します。
6. クラスタキーを入力し [次へ] をクリックして続行します。
7. 入力を求められたら、CMS 名と、管理権限のあるアカウントのユーザ名とパスワードを入力して CMS にログオンし、[次へ] をクリックします。
8. 復元するサーバ設定を含む BIAR ファイルの場所と名前を指定し、[次へ] をクリックして続行します。
   概要ページに BIAR ファイルの内容が表示されます。
9. 続行するには、[次へ] をクリックします。
   概要ページに、入力した情報が表示されます。
10. [完了] をクリックして続行します。
    既存のサーバ設定が BIAR ファイル内の値で上書きされ、続行すれば現在のサーバ設定が失われることを知らせる警告メッセージが表示されます。
11. [はい] をクリックすると、サーバ設定が復元されます。

    CCM は、BIAR ファイルからクラスタ全体のサーバ設定を復元します。復元処理の詳細がログファイルに書き込まれます。ログファイルの名前とパスがダイアログボックスに表示されます。
12. 復元操作が失敗した場合は、原因を特定するためにログファイルを確認してください。
13. [*OK*] をクリックし、ウィザードを閉じます。

BIAR ファイルからサーバ設定がシステムに復元されます。BIAR ファイルに存在するが、復元前にシステムに存在しなかったノードやサーバが作成されます。

> ⓘ 注記
>
> システムに存在するが BIAR ファイルに存在しないノードやサーバは、リポジトリから削除されます。そのようなノードやサーバは CCM には表示されますが、ノードの `dbinfo` ファイルおよび `bootstrap` ファイルを手動で削除できます。

クラスタ内の各コンピュータ上に、システム内のノードを再作成する必要があります。

関連情報

ノードの使用 [451 ページ]

14.5.2.2 Unix のサーバ設定を復元する

Unix マシンでは、`serverconfig.sh` スクリプトを使用して、BIAR ファイルからデプロイメントのサーバ設定を復元します。

1. [*6 - サーバ設定の復元*] を選択し、`Enter` キーを押します。

```
-----------------------------------------------------------

            SAP BusinessObjects

What do you want to do?

1 - Add node
2 - Delete node
3 - Modify node
4 - Move node
5 - Back up server configuration
6 - Restore server configuration
7 - Modify web tier configuration
8 - List all nodes


[quit(0)]
-----------------------------------------------------------

[8]6
```

2. 一時的に使用する Central Management Server (CMS) のポート番号を入力して、`Enter` キーを押します。
3. その後に続く画面で、CMS システムデータベースへの接続情報を指定します。
4. 入力を求められたら、システムおよび管理権限のあるアカウントのユーザ名とパスワードを指定して `Enter` キーを押し、CMS にログオンします。
5. 入力を求められたら、サーバ設定を復元する BIAR ファイルの場所と名前を指定して、`Enter` キーを押します。
   概要画面に、入力した情報が表示されます。
6. 画面に表示された情報が正しいことを確認し、[*Enter*] を押して続行します。
   `serverconfig.sh` スクリプトでは、指定した BIAR ファイルからクラスタ全体のサーバ設定を復元します。復元プロシージャの詳細は、ログファイルに書き込まれます。ログファイルの名前とパスは画面に表示されます。
7. 復元操作が失敗した場合は、原因を特定するためにログファイルを確認してください。

14.5.2.3 スクリプトを使用してサーバ設定を復元する

Windows の場合 `RestoreCluster.bat` スクリプトを、Unix の場合 `restorecluster.sh` スクリプトを実行することにより、デプロイメントのサーバ設定を復元することができます。

Windows では、`RestoreCluster.bat` はディレクトリ `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥scripts` にあります。

UNIX では、`restorecluster.sh` はディレクトリ `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts` にあります。

関連情報

BackupCluster スクリプトおよび RestoreCluster スクリプト [550 ページ]

14.5.3 BI コンテンツの復元

Business Intelligence (BI) コンテンツを LCMBIAR ファイルにバックアップしている場合は、プロモーションマネジメントツールを使用して、システム全体を復元せずに BI コンテンツを復元できます。 詳細については、“プロモーションマネジメント”に関する章を参照してください。

14.6 BackupCluster スクリプトおよび RestoreCluster スクリプト

次の表に、`BackupCluster` スクリプトで使用されるコマンドラインパラメータの説明を示します。

> **注記**
>
> このスクリプトでは、クラスタのサーバ設定のみをバックアップします。その他のデータについては、個別にバックアップする必要があります。

BackupCluster パラメータ

名前	説明	例
`-backup`	復元するシステムのサーバ設定のバックアップ先となる BIAR ファイルの名前およびパス	`-backup "C:¥Users¥Administrator¥Desktop¥my.biar"`
`-cms`	システムの Central Management Server が置かれているコンピュータのホスト名。CMS がデフォルトポートである 6400 以外のポートで実行されている場合は、ポート番号も指定する必要があります。	`-cms mycms:6400`
`-username`	Administrator アカウントのユーザ名	`-username Administrator`
`-password`	Administrator アカウントのパスワード	`-password Password1`

次の表に、`RestoreCluster` スクリプトで使用されるコマンドラインパラメータの説明を示します。

RestoreCluster パラメータ

名前	説明	例
`-restore`	復元するサーバ設定が保存されている BIAR ファイルの名前およびパス	`-restore "C:¥Users¥Administrator¥Desktop¥my.biar"`

名前	説明	例
-username	Administrator アカウントのユーザ名	**-username Administrator**
-password	Administrator アカウントのパスワード	**-password Password1**
-displaycontents	BIAR ファイルに保存されているノードとサーバのリストを表示します。	**-displaycontents "C:¥Users¥Administrator¥Desktop¥my.biar"**

> **注記**
>
> サーバ設定を復元する前に、-displaycontents パラメータを指定して RestoreCluster スクリプトを実行し、BIAR ファイルのコンテンツを表示してください。

稼動していないシステムからサーバ設定をバックアップする場合、またはサーバ設定を復元する場合は、以下のパラメータが必要です。

一時 CMS の使用時に使用されるパラメータ

名前	説明	例
-usetempcms	特定の操作のための一時 CMS を作成します。操作の完了後、一時 CMS は停止します。	**-usetempcms**
-cmsport	一時 CMS のポート番号	**-cmsport 6700**
-dbdriver	CMS システムデータベースのデータベースドライバ指定できる値は次のとおりです。 • **db2databasesubsystem** • **maxdbdatabasesubsystem** • **mysqldatabasesubsystem** • **oracledatabasesubsystem** • **sqlserverdatabasesubsystem** • **sybasedatabasesubsystem** • **sqlanywheredatabasesubsystem** • **newdbdatabasesubsystem** **注記** **newdbdatabasesubsystem** パラメータは SAP HANA データベースを使用します。	**-dbdriver sqlserverdatabasesubsystem**
-connect	CMS システムデータベース接続文字列	**-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"**

名前	説明	例
-dbkey	クラスタキー	**-dbkey abc1234**

例

以下の例では、既存の CMS を使用して、サーバ設定を BIAR ファイルにバックアップする方法を示します。

```
-backup "C:¥Users¥Administrator¥Desktop¥my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

例

以下の例では、BIAR ファイルのコンテンツを表示する方法を示します。

```
-displaycontents "C:¥Users¥Administrator¥Desktop¥mybiar.biar"
```

例

以下の例では、BIAR ファイルから設定を復元する方法を示します。サーバ設定を復元するには、常に一時 CMS を使用する必要があります。

```
-restore "C:¥Users¥Administrator¥Desktop¥my.biar"
-cms mycms:6400
-username Administrator
-password Password1
-usetempcms
-cmsport 6400
-dbdriver sqlserverdatabasesubsystem
-connect "DSN=BusinessObjects CMS
140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
```

15　BI プラットフォームデプロイメントのコピー

15.1　システムコピーの概要

この章では、テスト、スタンバイ、その他の目的で BI プラットフォームデプロイメントの複製を作成する方法について説明します。

詳細については、1275068 を参照してください。

関連情報

バックアップと復元の概要 [530 ページ]

15.2　用語

用語	定義
ソースシステム	元の BI プラットフォームデプロイメント。
ターゲットシステム	作成する新しいデプロイメント。
システムコピー	既存の BI プラットフォームデプロイメントの複製を作成するためのアクション。
同種システムコピー	ソースシステムとターゲットシステムのオペレーティングシステムおよびデータベースが同じタイプとなる複製システムを作成するためのアクション。BI プラットフォームは、同種システムコピーのみをサポートします。
異種システムコピー	ソースシステムとターゲットシステムのオペレーティングシステムまたはデータベースが異なるタイプであるが、同じデータに基づく複製システムを作成するためのアクション。
データベースのコピー	データベースベンダーのツールを使用して、CMS システムデータベースまたは監査データベースの複製を作成するためのアクション。

15.3　システムコピーの使用事例

以下の表で、達成すべき目標と、前提となる現在のリソースを説明し、最も適切なソリューションへと導きます。

目標	必要なリソース	解決策
目標: 同一のコピー 同じハードウェア構成および IP アドレス/マシン名を持つ複製システムを、スタンバイまたはテスト用に作成します。	• 同一ハードウェアを使用するターゲットシステムからソースシステム • ソースシステムのバックアップ、またはバックアップ元のソースシステムへのアクセス	このガイドで説明するシステムバックアップおよび復元ワークフローを使用します。システム全体のバックアップ [534 ページ]の手順を参照してください。ソースシステムのバックアップからターゲットシステムを再作成します。
目標: コピー ソースシステムとは異なるハードウェアおよび IP アドレス/マシン名を持つ複製システムを、スタンバイ、テスト、またはトレーニング用に作成します。	• ソースシステム (実行中または停止状態)、またはソースシステムのデータベースおよびファイルのバックアップ • ソースシステムからエクスポートする [557 ページ]で説明している詳細なシステム情報	システムのコピーの計画 [554 ページ]のシステムコピーワークフローを使用し、この章の残りの手順に従います。 **注記** ターゲットシステムは、同じリリース、サポートパッケージ、およびパッチレベルの既存の BI プラットフォームデプロイメントがインストールされたコンピュータか、BI プラットフォームがインストールされていないクリーンなコンピュータに作成できます。

関連情報

バックアップ [533 ページ]
システムのコピーの計画 [554 ページ]

15.4 システムのコピーの計画

システムコピーでは、現在のシステムを反映する必要はありません。 使用しているシステムのコピーを作成し、ターゲットシステムでコピーを再作成する前にいくらかの時間待つことができます。 または、ソースシステムの以前のバックアップをターゲットシステムのベースとして使用することもできます。 つまり、コピーは、そのコピーの作成時点のシステムのものとなります。 たとえば、1 カ月経過した場合、コピーによって 1 カ月前のシステムが再作成されます。

前の節の使用事例を確認し、ニーズに最も合う事例を決定した後は、システムコピーの計画を作成する必要があります。

システムコピーの計画の作成

システムをコピーする際には、次のことを事前に決めておく必要があります。

- コピーの実行中にソースシステムを停止するかアクティブのままとするか。（どちらの状況でもこの手順を実行可能。）
  - ソースシステムを停止する場合に必要となるダウンタイム。
  - ターゲットシステムの整合性を確保するためのテスト時間の計画。
- データベースのバックアップと復元に使用するデータベースツール。
- ターゲットシステムをデプロイするマシン、および各ノードをホストする場所。
- コピーするオプションのコンポーネント。
- ターゲット CMS データベースに使用するデータベースタイプ、およびコピーするその他のオプションのデータベース。

以下についても考慮する必要があります。

- ソースシステムがインストールされている BI プラットフォームコンポーネント。 インストールプログラムの 追加/削除 > 変更 機能を使用して、現在インストールされているコンポーネントの一覧を表示できます。
- ターゲットシステムがソースシステムとは異なるハードウェアセットアップにインストールされる場合、パフォーマンス向上のためにターゲットシステムを調整する必要がある可能性があります。 システムパフォーマンスの改善に関する情報については、*SAP BusinessObjects Business Intelligence sizing companion guide* を参照してください。
- ターゲットシステムで、ソースシステムのデータベース以外のレポーティングデータベースからレポートする場合。 この場合、レポーティングデータベースのデータベース接続情報を変更する必要があります。 これを実行するには、同じ DSN 名を維持しながら、ターゲットシステム上で DSN を他のデータベースにポイントさせます。

必要なソースシステムのコンポーネント。

- CMS システムデータベース
- FRS ファイルストア
- セマンティックレイヤ設定ファイル
- 監査データベース (オプション)
- モニタリングデータベース (オプション)
- プロモーションマネジメント Subversion データベース (オプション)。

15.5 考慮点および制限

BI プラットフォームデプロイメントのコピーを作成する際には、次の考慮点について注意してください。

領域	考慮点
SAP Business Warehouse 統合	統合した環境で BI プラットフォームおよび SAP ERP または BW を使用している場合は、システムをコピーする前に SAP システムのコピーに関するドキュメントをお読みください。システムのコピーに関するガイドは、http://

領域	考慮点
	www.sdn.sap.com/irj/sdn/systemcopy から取得できます。取得するには、SMP ログインが必要です。SAP NetWeaver のバージョンを選択すると、コピーに関する該当するガイドがインストールガイド用のフォルダにあります。
プログラムのバージョン	ソースシステムとターゲットシステムは、同じバージョン、サポートパッケージ、およびパッチレベルにある必要があります。
内容と設定	ソースシステム全体のみをコピーできます。コンテンツまたはシステム設定を選択的にコピーすることはできません。
インストールパス	ソースおよびターゲットの場所のインストールパスを同一にしてください。たとえば、ソースシステムを `C:¥SAP BusinessObjects Enterprise XI 4.0` にインストールした場合は、ターゲットを `C:¥SAP BusinessObjects Enterprise XI 4.0` にインストールする必要があります。
ホストオペレーティングシステム	ソースおよびターゲットのオペレーティングシステムは同じである必要があります。
CMS データベースのソフトウェアのタイプ	CMS ソースとターゲットデータベースは同じタイプである必要があります。システムをコピーした後、別のサポートされているデータベースタイプに変更を加えるオプションがあります。
監査データベースのソフトウェアのタイプ	監査データをコピーする場合は、ソースとターゲットの監査データベースは同じタイプである必要があります。コピーの作成後は、異なるタイプの新しいデータベースを構築できます。 **注記** 新しいデータベースを構築する場合、既存のイベントはそのデータベースにコピーされず、新しいイベントだけがその新しいデータベースに記録されます。
Web Tier のカスタマイズ	コピー手順では、ソースシステムから Web Tier コンポーネントをコピーすることはできません。Web Tier をカスタマイズした (たとえば、`custom` フォルダの `.properties` ファイルを変更した) 場合、そのカスタマイズをターゲットに手動で適用する必要があります。
この手順で紹介していないトピック	このワークフローは、データベースをエクスポートまたはインポートする方法について説明するものではありません。データベースのコピーと復元には、データベースベンダーのツールを使用してください。

システムのコピー処理時に次のデータがコピーされます。

- CMS リポジトリデータベース。レポート、アナリティクス、フォルダ、権限、ユーザとユーザグループ、サーバ設定、その他の BI コンテンツ、およびシステムコンテンツが含まれます。
- 監査データベース。BI プラットフォームサーバまたはクライアントアプリケーションが起動する監査イベントが含まれます。
- モニタリングデータベース。メトリクス、プローブ、および監視のトレンドデータが含まれます。

- バージョン管理データベース。異なるバージョンのレポート、アナリティクス、その他の BI リソース、およびバージョン情報が含まれます。

> ⓘ 注記
>
> データベースとその内容の説明については、このガイドのデータベース [37 ページ]の節を参照してください。

- セマンティックレイヤ設定ファイル

Web Tier 設定、検索インデックス、および上記に挙げられていないデータはコピーされません。

ファイル復元コピーに関する考慮点

誤って削除してしまったファイルを復元するという目的でシステムをコピーする場合は、さらに次の考慮点にも注意してください。

バックアップを使用して、本稼働システムで「ターゲットシステムにインポートする [561 ページ]」で説明している手順を実行します。

- すべてのノードをインストールせずに、CMS とそのデータベースが含まれる最初のノードだけをインストールします。
- 監査データベース、プロモーションマネジメントデータベース、またはモニタリングデータベースはインストールしないでください。
- 監査データベースまたはレポーティングデータベースへの接続を再作成しないでください。

LCM を使用して、ターゲットシステムからソースシステムに復元するオブジェクトを昇格します。

15.6 システムコピー手順

次の手順では、BI プラットフォームデプロイメントの 2 段階のコピー手順について説明します。

15.6.1 ソースシステムからエクスポートする

ソースシステムの次の情報を書き留めておく必要があります。この情報を記述する場合に利用できるワークシートがシステムコピーワークシート [1178 ページ]にあります。

プロパティ	場所
CMS クラスタキー (レコードのセキュリティを必ず確保してください)。	BI プラットフォームのインストール時にシステム管理者によって作成されます。
ノード名。	CMC の [サーバ] タブに移動し、左側のツリーで [ノード] を展開します。

プロパティ	場所
デプロイメントの各マシンに関するマシン名と BI プラットフォームのインストールフォルダ。	CMC の [サーバ] タブに移動し、CMS を右クリックして [プレースホルダ] を選択します。`%INSTALLROOTDIR%` プレースホルダの値を確認します。
BI プラットフォームの管理者のパスワード (レコードのセキュリティを必ず確保してください)。	BI プラットフォームのインストール時にシステム管理者によって作成されます。
CMS によって使用される可能性のあるすべてのデータベース接続と、それらの接続に関連するユーザ名およびパスワード。監査データベースの情報をコピーする場合は、監査データベースも含まれます。クラスタ内のすべてのマシンについて、この情報を取得してください。 **注記** 監査データベースをコピーする場合は、監査データベースの接続名と認証情報も必要です。	CMC の [サーバ] タブに移動し、CMS を右クリックして [メトリクス] を選択します。 次のメトリクスを確認します。 • システムデータベース接続名 • システムデータベースサーバ名 • システムデータベースユーザ名 • データソース名 • 監査データベースの接続名 (オプション) • 監査データベースのユーザ名 (オプション)
クラスタのすべてのマシンに関する、その他のデータベース接続 (たとえば、ユニバースやレポートが使用するもの) の詳細 (クライアントのタイプ、バージョン)。ユーザ名とパスワードを含めるようにしてください。	データベースから直接レポートする Crystal Reports については、SAP Crystal Reports 2020 または SAP Crystal Reports for Enterprise デザイナを使用して接続情報を確認します。ユニバースの接続情報については、インフォメーションデザインツール (.unx) またはユニバースデザインツール (.unv) を使用します。
ソースシステムのバージョン、サポートパッケージ、およびパッチレベル。	Windows では、プログラムの削除または変更ツールで確認できます。 Unix では、BI プラットフォームのインストールディレクトリにある `modifyOrRemoveProducts.sh` ユーティティを使用できます。
デプロイメント内のすべての Input FRS および Output FRS のファイルストアの場所。	CMC の [サーバ] タブに移動し、Input FRS または Output FRS を右クリックして [プロパティ] を選択します。ファイル格納ディレクトリプロパティを確認します。 **注記** % で始まっている値はプレースホルダです。その場合は、[プレースホルダ] をクリックし、そのプレースホルダの下に表示されるディレクトリを書き留める必要があります。
プロモーションマネジメントのコピーを計画している場合、プロモーションマネジメントデータベースフォルダと Subversion フォルダの場所。	Windows インストールでのプロモーションマネジメントデータベースのデフォルトのフォルダは `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Data¥LCM¥LCMOverride` で

プロパティ	場所
	す。Unix では、<INSTALLDIR>/sap_bobj/data/LCM/LCMOverride です。 Windows インストールでの Subversion ファイルのデフォルトの場所は次のとおりです。 • <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥CheckOut • <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥LCM_Repository また、Unix では次のとおりです。 • <INSTALLDIR>/check_out (このディレクトリは、Subversion を使用してファイルをチェックアウトした後にだけ作成されます)。 • $HOME/LCM_Repository
モニタリングデータベースをコピーする計画がある場合は、モニタリングデータベースフォルダ。	このフォルダは CMC で設定します。CMC のアプリケーション管理エリアに移動し、モニタリングアプリケーション > プロパティ を選択し、トレンドデータベースのバックアップディレクトリを確認します。 Windows インストールでのデフォルトフォルダは <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Data¥TrendingDB です。Unix では <INSTALLDIR>/sap_bobj/Data/TrendingDB です。
セマンティックレイヤフォルダのパス。	Windows インストールでのデフォルトフォルダは、デフォルトで <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥dataAccess¥connectionsServer¥ です。

上記の情報を記録した後で、次の手順を実行します。

1. データベースベンダーのバックアップツールを使用して、次のデータベースのバックアップコピーを作成します。
   - CMS システムデータベース
   - 監査データベース (オプション)
2. ファイルバックアップツールを使用して、次のファイルセットをバックアップします。
   - Input/Output FRS ファイルストア。
   - モニタリングトレンドデータベース (オプション)。これは、ワークシートに記録されたモニタリングフォルダからファイルをバックアップすることによって実現します。デフォルトで、Windows では次のようになります。<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Data¥TrendingDB。Unix の場合: <INSTALLDIR>/sap_bobj/Data/TrendingDB。

- プロモーションマネジメント Subversion データベース (オプション)。これは、ワークシートに記録された Subversion フォルダからファイルをバックアップすることによって実現します。デフォルトでは、Windows の場合次のとおりです。
  - `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥CheckOut`
  - `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥LCM_Repository`.

  また、Unix では次のとおりです。
  - `<INSTALLDIR>/check_out` (このディレクトリは、Subversion を使用してファイルをチェックアウトした後にだけ作成されます)。
  - `$HOME/LCM_Repository`
- セマンティックレイヤフォルダの設定ファイル: `connectionServer` フォルダの `cs.cfg` ファイル、およびそのサブフォルダの `.sbo` ファイルと `.prm` ファイル。

> **注記**
>
> このワークフローの制約と詳細の説明については、ホットバックアップ [534 ページ]の節を参照してください。

3. 次のファイルは、ユーザがカスタマイズ可能です。これらのファイルのいずれかをカスタマイズした場合、ファイルをソースシステムからバックアップし、後で、ターゲットシステムの同じフォルダにそれらのファイルを復元します。
   - `BO_trace.ini` は、次の場所にインストールされます。
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/conf`
   - 以下にインストールされた `clientSDKOptions.xml`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java/lib`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win32_x86`
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/win64_x64`
   - `CRConfig.xml` は次の場所にインストールされます。
     - `[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/java`
   - `mdas.properties` は次の場所にインストールされます。
     - `[INSTALLDIR]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services`
   - WDeploy 設定ファイルは、`[INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf` の次の場所にインストールされます。
     - `config.apache`
     - `config.jboss7`
     - `config.sapappsvr75`
     - `config.tomcat6`
     - `config.tomcat7`
     - `config.weblogic11`
     - `config.websphere7`
     - `config.websphere8`
     - `wdeploy.conf`
4. 次の Web Tier ファイルは、ユーザがカスタマイズ可能です。これらのファイルのいずれかを変更した場合、ファイルをソースシステムからバックアップします。後で、これらのファイルを復元するか、ターゲットシステムに変更を再適用する必要があります。

- 以下にインストールされた BO_trace.ini
  - [INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog
  - [INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf
- clientaccesspolicy.xml は次の場所にインストールされます。
  - [INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT
- 以下にインストールされた clientSDKOptions.xml
  - [INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib
  - [INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib
- crossdomain.xml は次の場所にインストールされます。
  - [INSTALLDIR]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT
  - [INSTALLDIR]tomcat/webapps/ROOT
- config/custom フォルダ内のカスタマイズされたすべてのファイル (Web Tier 内)。ターゲットシステムにカスタマイズを転送するために、これらのファイルをバックアップします。

5. たとえば、パブリケーション拡張やカスタムライブラリなどの、ソースシステムに手動で追加したすべてのカスタム拡張をバックアップします。

上記で記録した情報を、データベースおよびファイルのコピーと共に保存してください。将来のシステムコピーの手順に必要となる、更新可能な 2 つ目のコピーを保存することもできます。

15.6.2 ターゲットシステムにインポートする

この手順は、ユーザがターゲットシステムで使用するソースデプロイメントのデータベースとシステムファイルのバックアップコピーを作成済みであることを想定しています。 すべてのバックアップファイルは同じバックアップセットからのものである必要があります。 また、「“ソースシステムからエクスポートする”」で書き留めた詳細 (クラスタキー、データベース認証情報など) も必要になります。

ターゲットシステムが、ソースシステムのリソースへのアクセスが可能なネットワーク内にある場合は、ターゲットシステムが再設定されるまではターゲットシステムからソースシステムのリソースへのアクセスが試行されないようにする必要があります。 これを実現するには、ターゲットシステムとソースシステムのリソース間にファイアウォールを配置するか、ターゲットシステムを開始している間はソースシステムを停止したままにします。ターゲットシステムを最初に開始した後は、ファイアウォールを解除するか、またはソースシステムを開始することができます。

ターゲットシステムにすでに BI プラットフォームがインストールされている場合は、コピーが作成された時点のソースシステムと同じバージョン、サポートパッケージ、およびパッチレベルであることを確認します。 また、ソースシステムと同じインストールパスを使用していることを確認します。

1. ターゲットシステム上で CMS リポジトリ、監査データベース、およびレポーティングデータベースを配置するデータベースに対する接続を作成します。

> **注記**
>
> 接続では異なるデータベースをポイントすることができますが、ソースシステムと同じ接続名または DSN であり、同じ認証情報を使用する必要があります。

2. データベースツールを使用して、CMS システムデータベースと監査データベース (必要な場合) を、ソースシステムのバックアップからターゲットデータベースへ復元します。

   ターゲットシステム上のユニバースまたはレポートで別のレポーティングデータベースを使用する必要がある場合は、そのデータベースをポイントするようにデータベース接続を変更します。

   この手順について詳細な説明が必要な場合は、システムの復元 [540 ページ]を参照してください。
3. BI プラットフォームがターゲットホストシステムにインストールされている場合は、手順 4 に進みます。BI プラットフォームがインストールされていない場合は、次の手順に注意して、ターゲットホストシステムに BI プラットフォームをインストールします。
   a. ソースシステムと同じプログラムバージョン、サポートパッケージ、およびパッチレベルをインストールします。
   b. ソースシステムと同じインストールパスを使用します。
   c. ソースシステムにインストールされたのと同じコンポーネントを選択します。
   d. インストールプログラムで CMS データベース (および該当する場合は監査データベース) を作成するかどうかを確認されたら、[既存のデータベースの使用] オプションを選択して、手順 1 で設定した接続名と認証情報を入力します。

      > **注記**
      >
      > CMS データベースの再初期化を選択しないでください。

   e. [ノード名] を入力するよう求められたら、ソースシステムと同じ名前、ポート番号、プラットフォーム管理者パスワード、およびクラスタキーを使用します。

      インストール手順の詳細については、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドを参照してください。 システムでインストールが完了したら、手順 6 に進みます。

      > **注記**
      >
      > ソースシステムから監査データをコピーしない場合は、インストール実行中に監査を設定することで、新しい監査データベースを作成できます。

   f. CCM ですべてのノードを停止します。
4. ターゲットシステムに BI プラットフォームがすでにインストールされている場合、CCM ですべてのノードを停止します。 ターゲットシステム CMS ホストコンピュータ上で CCM を開始します。
5. BI プラットフォームがすでにインストールされている場合は、[ノードをもう一度作成] オプションを使用して、新しいノードを追加します。
   a. ソースシステムから [ノード名] および [*SIA* ポート番号] を使用します。
   b. [新規一時 *CMS* の起動] を選択します。
   c. 新しい [*CMS* ポート番号] (未使用のポートを任意に指定可能) と、復元されたデータベースタイプと一致する [*CMS* データベースタイプ] を選択します。
   d. 手順 1 の、CMS データベースの復元先の接続に関する詳細を入力します。
   e. ソースシステムからクラスタキーを入力します。
   f. ソースシステムの管理者パスワードを入力します。
6. Input/Output FRS ファイルストアをターゲットシステムファイルストアに復元します。 ソースシステムで使用されていたのと同じフォルダを使用します。
7. モニタリングデータベースフォルダを (モニタリング情報をコピーする場合) ソースシステムで使用されていたのと同じフォルダに復元します。
8. プロモーションマネジメントデータベースフォルダ (プロモーションマネジメント情報をコピーする場合) を、ソースシステムで使用したフォルダと同じフォルダに復元します。

9. Subversion ファイル (プロモーションマネジメント情報をコピーする場合) を、ソースシステムで使用したフォルダと同じフォルダに復元します。
10. セマンティックレイヤ/接続設定サーバファイルを、ソースシステムで使用されていたのと同じフォルダに復元します。
11. ターゲットシステムのホストコンピュータを再起動します。
12. 手順 3 でターゲットシステムに BI プラットフォームをインストールした場合は、ソースシステムと一致させるために必要となるサポートパッケージまたはパッチを適用します。
13. 複数のホストコンピュータでターゲットシステムを実行する場合は、各ホストコンピュータで手順 1 ～ 11 を繰り返します。

    追加の BI プラットフォームノードをインストールする際には、拡張インストールオプションを使用します。ターゲットシステムの追加ノードには、ソースシステムと同じノード名を使用する必要があります。
14. ターゲットシステムの CMS データベースがソースシステムと異なるデータベースタイプを使用する場合は、そのコピーに使用するデータベースをコピー先として指定し、CCM を使用して、CMS データベース間でのデータのコピー [488 ページ]を実行します。
15. 「"ソースシステムからエクスポートする"」手順の手順 3 でバックアップしたユーザがカスタマイズ可能なすべてのファイルを復元します。
16. 「"ソースシステムからエクスポートする"」手順の手順 4 でバックアップしたすべての Web Tier ファイルを復元します。

    "Web Tier" は、カスタマイズを実行できる WDeploy ステージングエリア、およびアプリケーションサーバにデプロイされる Web Tier コンテンツを参照します。

    ターゲットシステムに変更を適用する場合、変更をアプリケーションサーバディレクトリに適用しないでください。変更は、WDeploy ステージングエリアに適用し、次に、WDeploy を使用して Web Tier をアプリケーションサーバに再デプロイします。

    WDeploy ステージングエリアの場所は、Windows では `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/warfiles` です。
17. 「"ソースシステムからエクスポートする"」手順の手順 5 でバックアップしたすべての拡張を復元します。

BI プラットフォームのシステムコピーを実行後、次の手順を実行します。

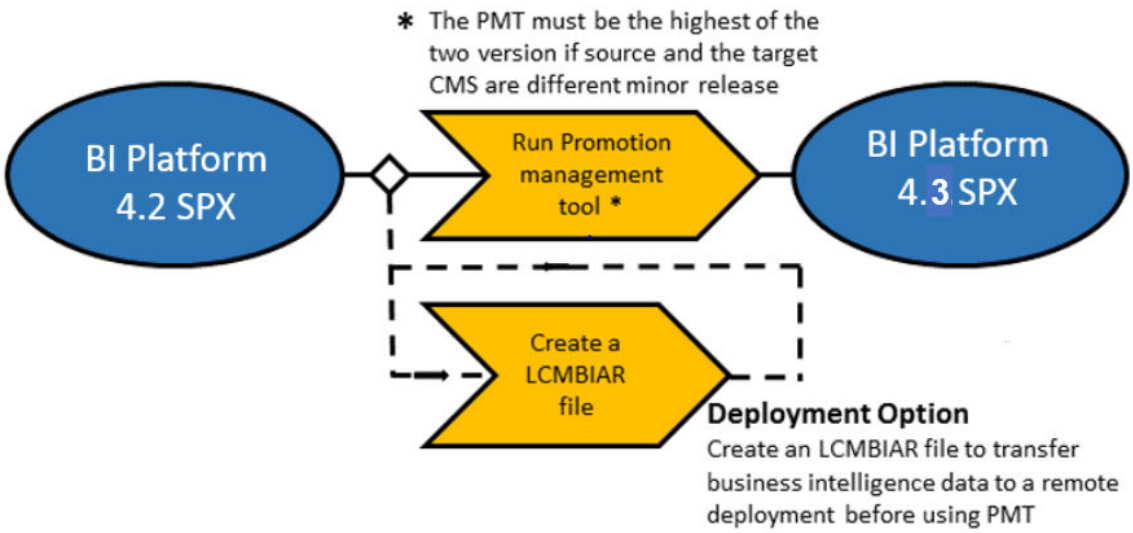
1. ターゲット上の最初のノードのインストールによって、一時 CMS が作成されます。一時 CMS は、インストール終了時に停止されます。 CMC を使用して、[サーバ] ページに移動し、この CMS を削除します。

   > → 注意
   >
   > ソースシステムを削除しない場合 (またはソースシステムをターゲットシステムと同時に使用する場合)、ターゲットシステム上のクラスタの名前を変更することをお勧めします。
2. ターゲット CMS データベースでリポジトリ診断ツールを実行します。
3. 該当する場合、ターゲットシステムで Windows AD シングルサインオン (SSO) を設定します。 AD 認証を使用した BI プラットフォームへの SSO [303 ページ]を参照してください。
4. 該当する場合、ターゲットシステムで SLD を設定します。 詳細については、SAP ノート 1508421: "SAP SLD Data Supplier for Apache Tomcat" を参照してください。
5. ターゲットシステムでサニティチェックを実行し、整合性を確認します。
6. フル検索の再インデックス化を実行します。

16 プロモーション管理

16.1 プロモーションマネジメントへようこそ

16.1.1 概要



プロモーション管理ツールを使用して、以下のことを実行できます。

- リポジトリ間でのビジネスインテリジェンス (BI) リソースの移動または移送。
- リソースの依存関係の管理。
- 必要に応じた、出力先システムでの昇格済みリソースのロールバック。

プロモーション管理ツールでは、同じ BI リソースのさまざまなバージョンの管理もサポートします。

プロモーションマネジメントツールは、セントラル管理コンソールと統合されます。ビジネスインテリジェンスリソースを別のシステムに昇格できるのは、移動元システムと移動先システムの両方に同じバージョンの BI プラットフォームがインストールされている場合だけです。

16.1.2 機能

プロモーションマネジメントツールにより、出力先デプロイメントの InfoObject で次の操作を実行することができます。

- 新しいジョブの作成

- 既存のジョブのコピー
- ジョブの編集
- ジョブの昇格のスケジュール
- ジョブ履歴の表示
- LCMBIAR としてエクスポート
- BIAR/LCMBIAR のインポート

昇格ワークフローには次のタスクも含まれています。

- 依存関係の管理: この機能では、昇格させるジョブの InfoObject の依存関係を選択、フィルタ、および管理できます。
- スケジュール: この機能では、ジョブの作成直後にジョブを昇格するのではなく、ジョブの昇格の時間を指定できます。 1 回または定期的なスケジュールで実行するジョブの昇格を指定できます。
- セキュリティ: この機能では、InfoObject と関連セキュリティ権限を昇格できます。必要であれば、InfoObject をアプリケーション権限とともに昇格できます。.
- 昇格テスト: この機能では、InfoObject を実際に昇格する前に、すべての防止対策が取られているかを確認し昇格をテストできます。.
- ロールバック: この機能では、ジョブの昇格後に出力先システムを以前の状態に復元することができます。 ジョブのすべてまたは一部をロールバックできます。
- 監査: プロモーションマネジメントツールで生成されたイベントは、監査データベースに保存されます。 監査機能では、監査データベースに記録されたイベントをモニタリングできます。
- プロモーションマネジメント上書き設定: この機能では、ジョブの昇格を介して上書きをスキャンおよび昇格できます。

16.1.3 アプリケーションアクセス権

このセクションでは、プロモーションマネジメントツールのアプリケーションアクセス権限について説明します。

- CMC 内でプロモーションマネジメントツールに対するアクセス権限を設定できます。
- プロモーションマネジメントツール内でさまざまな機能に対する詳細なアプリケーション権限を設定できます。

プロモーションマネジメントツールの特定の権限を設定するには、以下の手順に従います。

1. CMC にログオンし、[アプリケーション] を選択します。
2. [プロモーションマネジメント] をダブルクリックします。
3. [ユーザセキュリティ] をクリックし、ユーザを選択します。 ユーザのセキュリティ権限の表示または割り当てを行うことができます。
4. 以下のプロモーションマネジメント固有権限があります。
   - 上書きを編集するためにアクセスを許可
   - セキュリティを含むアクセスを許可
   - 管理へのアクセスを許可
   - [依存関係の管理] ページへのアクセスを許可
   - ジョブの作成
   - ジョブの削除
   - ジョブの編集

- LCMBIAR の編集
- LCMBIAR としてエクスポート
- LCMBIAR のインポート
- ジョブの昇格
- ジョブのロールバック
- BOMM (BusinessObjects Metadata) オブジェクトの表示および選択
- ビジネスビューの表示および選択
- カレンダの表示および選択
- 接続の表示および選択
- プロファイルの表示および選択
- QaaWS の表示および選択
- レポートオブジェクトの表示および選択
- セキュリティ設定の表示および選択
- ユニバースの表示および選択

5. 選択したユーザに権限を割り当てるには、適切な権限を選択し、[セキュリティの割り当て] をクリックします。

プロモーションマネジメントツールのアクセス権限が CMC 内に設定されます。

16.1.4 プロモーションマネジメントでの WinAD のサポート

プロモーションマネジメントツールを正常に動作させるには、以下をすべての Adaptive Job Server のすべての `javaargs` 引数に追加する必要があります。

```
Djava.security.auth.login.config=<path>¥bsclogin.conf,Djava.security.krb5.conf=<path>¥krb5.ini
```

> → 注意
>
> ユーザのデプロイメントで、`bsclogin.conf` および `krb5.ini` への正しいパスを指定します。

16.2 プロモーションマネジメントツールを使用する前に

16.2.1 プロモーションマネジメントツールへのアクセス

プロモーションマネジメントツールにアクセスするには、CMC ホームページから昇格管理を選択します。

昇格ジョブフォルダの表示権限があれば、どのユーザでもプロモーションマネジメントツールを起動することができます。 ただし、ジョブを作成、スケジュール、または昇格するには、管理者から追加権限を得る必要があります。

16.2.2 ユーザインタフェースコンポーネント

この章では、プロモーションマネジメントツールの GUI コンポーネントについて説明します。

- プロモーションマネジメントワークスペースツールバー
- ワークスペースパネル
- ツリーパネル
- 詳細パネル
- ショッピングカートおよびジョブビューアページ

プロモーションマネジメントワークスペースツールバー

次の表は、プロモーションマネジメントワークスペースツールバーのオプションと、それらのオプションを使用して実行できるタスクについての説明の一覧です。

オプション	説明
	新しいフォルダを作成できます。新しいフォルダは [昇格ジョブ] フォルダのサブフォルダとして作成されます。
	選択したジョブまたはフォルダを現在の場所からコピーまたは削除できます。
	ジョブまたはフォルダを現在の場所からコピーできます。
	コピーしたジョブまたはフォルダを新しい場所に貼り付けることができます。
	既存のジョブまたはフォルダを削除できます。
	ジョブまたはフォルダの更新された一覧を取得するために、ホームページを最新表示できます。
プロパティ	選択したジョブのプロパティを変更できます。選択したジョブのタイトル、説明、およびキーワードを変更できます。
履歴	選択したジョブの履歴を表示できます。
新しいジョブ	新しいジョブを作成できます。
インポート	BIAR、LCMBIAR または上書きファイルをインポートできます。
編集	選択したジョブを編集できます。
昇格	選択したジョブを昇格できます。
ロールバック	出力先システムの昇格されたジョブを元に戻すことができます。 **注記** ジョブが出力先にオブジェクトを昇格する場合、これらのオブジェクトはロールバックにより削除されます。ジョブが出力先のオブジェクトを更新する場合、前のバージョンのオブジェクトはロールバックにより復元されます。

オプション	説明
	ジョブ一覧ページ間を移動できます。このオプションでは、1 ページずつ移動するか、あるいは該当するページ番号を入力して特定のページに移動できます。
検索	特定のジョブを検索できます。名前、キーワード、説明、または 3 つのパラメータのすべてからジョブを検索できます。
昇格ジョブ	昇格されたジョブとフォルダを表示できます。
昇格のステータス	昇格されたジョブをステータス(成功、失敗、または一部成功)別に表示します。

ワークスペースパネル

プロモーションマネジメントのホームページのワークスペースパネルには、ジョブの一覧が表示されます。このパネルを使用して、ジョブ、ソースシステムと出力先システム、およびジョブ作成者の名前、ステータス、作成時刻、前回の実行時刻を表示できます。

ツリーパネル

プロモーションマネジメントのホームページのツリーパネルには、[昇格ジョブ] フォルダと [昇格のステータス] フォルダがツリー構造で表示されます。ジョブは、昇格ジョブフォルダの下に階層構造で表示されます。[昇格のステータス]フォルダには、昇格されたジョブがステータス別に表示されます。

ジョブビューアページ

新しいジョブを作成するか既存のジョブを編集すると、“ジョブビューア”ページが表示されます。このページには、動的に生成された昇格対象の InfoObject の一覧および詳細パネルが表示されます。この一覧では、InfoObject はユーザグループ、ユニバースおよび接続に分類されます。詳細パネルでは、この一覧から選択されたノードの内容が表示されます。

16.2.3 設定オプションの使用

ある BI プラットフォームデプロイメントから別の BI プラットフォームデプロイメントおよび SAP デプロイメントへ InfoObject を昇格する前に、設定オプションで設定を行うことができます。 このセクションでは、設定オプションの使用方法について説明します。

[昇格ジョブ] 画面の [設定] ドロップダウンをクリックします。 このドロップダウンには、次のオプションが表示されます。

- システムの管理: このオプションでは、プロモーションマネジメントアクティビティに必要なすべてのシステムを追加できます。

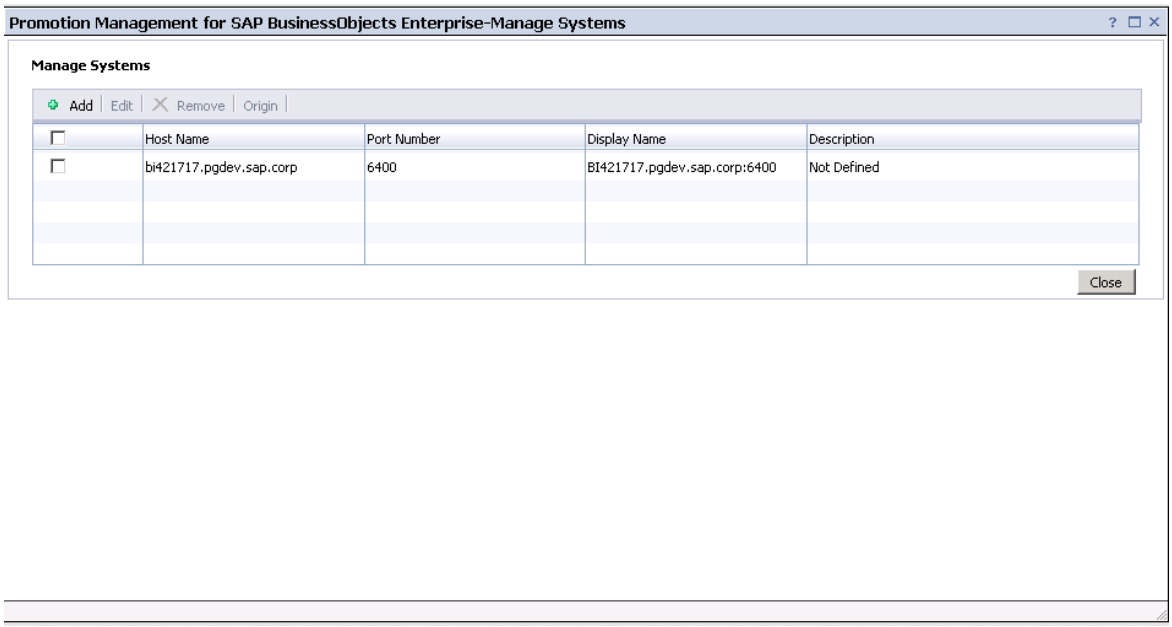
- ロールバック設定: このオプションでは、ロールバックを有効化するシステムを選択できます。
- ジョブ設定: このオプションでは、依存項目ページに完了したインスタンスを表示できるほか、ジョブインスタンスのクリーンアップアクティビティを管理することもできます。 また、ジョブの作成日を指定してフィルタリングすることもできます。
- *CTS* 設定: このオプションでは、拡張移送/修正システムの統合に使用する Web サービスや SAP BW のシステム情報を追加できます。

16.2.3.1 [システムの管理] オプションを使用する

このセクションでは、[システムノ管理]オプションの使用方法について説明します。このオプションを使用してホストシステムを追加または削除できます。

ホストシステムを追加するには、次の手順に従います。

1. プロモーションマネジメントワークスペースツールバーで、設定をクリックしてから、システムの管理をクリックします。
   システムの管理ウィンドウが表示されます。このウィンドウには、ホスト名、ポート番号、表示名、および説明の一覧が表示されます。



2. 追加をクリックします。
   システムの追加ダイアログボックスが表示されます。
3. ホスト名、ポート番号、表示名、および説明を該当するフィールドに追加します。

> ⓘ 注記
>
> ソースにするオプションを選択して、システムをソースシステムとして識別します。ソースシステムは、接続情報の提供元となるシステムです。このオプションは、上書きを使用する場合に便利です。

4. [*OK*] をクリックして、システムに追加します。
   一覧にホストシステムが追加されます。

> ⓘ 注記
>
> ホストシステムを削除または編集するには、ホストシステムを選択して、削除または編集をクリックします。

関連情報

[ロールバック設定] オプションを使用する [570 ページ]
[ジョブ設定] オプションを使用する [570 ページ]

16.2.3.2 [ロールバック設定] オプションを使用する

デフォルトでは、システムレベルでロールバック処理が有効化されています。[ロールバック設定] オプションでは、システムレベルでロールバック処理を無効化できます。

システムレベルでロールバック処理を無効化するには、次の手順に従います。

1. [ロールバック] ウィンドウのホストシステムの一覧から、ロールバックプロセスを無効にするホストシステムを選択します。
2. [保存して閉じる]をクリックして変更を保存します。

関連情報

[ジョブ設定] オプションを使用する [570 ページ]

16.2.3.3 [ジョブ設定] オプションを使用する

ジョブ設定オプションでは、“依存関係の管理”ページに完了したインスタンスを表示するかどうかや、システムに存在できるジョブインスタンスの数を指定できます。 次のオプションのいずれかを指定できます。

- 依存関係の管理ページに完了したインスタンスを表示する: このオプションにより、ジョブに追加することができる“依存関係の管理”ページに、完了したインスタンスを表示することができます。
- ジョブのインスタンスが *N* 個より多い場合はインスタンスを削除する: このオプションにより、システムのジョブ 1 件あたりの最大ジョブインスタンス数を指定することができます。
- ジョブの *N* 日後にインスタンスを削除する: このオプションにより、作成されてから指定日数を経過したジョブインスタンスを削除するように指定することができます。
- 指定した期間中に作成されたジョブを表示するために、次の期間に作成されたジョブを表示リストから時間間隔を選択することができます。

[ジョブ設定]オプションを設定するには、次の手順に従います。

1. オプションを選択し、優先値を入力します。

2. [保存]をクリックして、更新した変更を保存します。

[デフォルト設定]をクリックしてデフォルト値を設定できます。[閉じる]をクリックしてウィンドウを閉じることができます。

> ⓘ 注記
>
> 古いジョブインスタンスは、次回のジョブ実行時に削除されます。

関連情報

バージョン管理システムとして Apache Subversion を使用する [655 ページ]

16.2.3.4 上書き設定オプションの使用

上書き設定オプションにより、ジョブ昇格または LCMBIAR ファイルを使用して上書きを昇格することができます。このオプションにより Crystal Reports 接続およびユニバース接続のデータベース接続情報をスキャン、昇格、編集することができます。また、このオプションを使用して QAAWS URL を編集することもできます。

> ⓘ 注記
>
> 上書き設定オプションを使用するには、Adobe Flash Viewer をインストールする必要があります。

システムという用語は、以下の手順で使用します。システムには、次の 3 種類があります。

- ソース: 接続情報のソースシステムです。
- セントラルプロモーションマネジメント: プロモーションマネジメントツールを実行するシステムです。
- 出力先: BI リソースの昇格先のエンドシステムです。

16.2.3.4.1 上書きを昇格する

上書きを昇格する前にホストシステムを追加してください。ホストシステムの追加についての詳細は、[システムの管理] オプションを使用する [569 ページ] を参照してください。

上書きを昇格するには、次の手順に従います。

1. プロモーションマネジメントワークスペースツールバーで、[上書き設定] オプションをクリックします。[上書き設定] ウィンドウが表示されます。
2. [ソース] ペインで、ドロップダウンメニューから必要なソースシステムを選択します。

   > ⓘ 注記
   >
   > また、[新しいシステム] にログインすることもできます。新しいシステムをソースシステムとして選択するには、以下の手順を実行します。
   >
   > 1. ドロップダウンメニューから [新しいシステム] を選択します。

[ソースログイン] ダイアログボックスが表示されます。
2. [システム]、[ユーザ名]、[パスワード]、および [認証] フィールドに有効な認証情報を入力します。
3. [ログオン] を選択します。

3. [ログイン] を選択します。
4. [今すぐスキャンする] を選択します。

スキャン処理が開始されます。[一意接続の一覧] が表示されます。

> **注記**
>
> 定期的なスキャンをスケジュールするには、[定期的スケジュールの設定] を選択します。

5. 上書き一覧で、各上書きに対応するチェックボックスをオンにして、昇格する上書きを選択します。

> **注記**
>
> 上書きの一覧で上書きを検索するには、上書き名、最終更新日などのキーワードを使用します。
>
> また、次のパラメータによって、上書きをフィルタすることができます。[すべて]、[接続]、[Qwaas]、[Crystal レポート]。
>
> さらに、上書きをアルファベット順に並べ替えることができます。

6. [出力先] ペインで、ドロップダウンメニューから必要な出力先システムを選択します。複数の出力先システムを指定することができます。

> **注記**
>
> また、[新しいシステム] にログインすることもできます。新しいシステムを出力先システムとして選択するには、以下の手順を実行します。
> 1. ドロップダウンメニューから [新しいシステム] を選択します。
> [出力先ログイン] ダイアログボックスが表示されます。
> 2. [システム]、[ユーザ名]、[パスワード]、および [認証] フィールドに有効な認証情報を入力します。
> 3. [ログオン] を選択します。

上書きを LCMBIAR ファイルとしてエクスポートするには、次の手順に従います。
1. ドロップダウンメニューから [LCMBIAR ファイルにエクスポート] を選択します。
2. [エクスポート] を選択します。
[エクスポート設定] ダイアログボックスが開きます。
3. 対応するフィールドに、有効な認証情報を入力します。
4. [完了] を選択します。

7. [昇格] を選択します。

[複数の出力先上書き] ダイアログボックスが表示されます。

> **注記**
>
> デフォルトでは、現在ログインしているすべての出力先システムが選択されます。上書きを特定の出力先システムに選択的に昇格するには、必要な出力先システムに対応するチェックボックスをオンにします。

8. [完了] を選択します。

上書きの昇格が完了します。

9. 有効な認証情報を使用して、いずれかの出力先システムにログインします。

   昇格したすべてのオブジェクトの一覧が一意接続の一覧に表示されます。これらのオブジェクトのステータスは非アクティブです。

10. 編集するオブジェクトの [更新] を選択します。

    [共通接続プロパティの編集] ダイアログボックスが表示されます。

11. 必要な値を更新して、[完了] を選択します。

    編集したオブジェクトのステータスがアクティブになります。

    > ⓘ 注記
    >
    > また、出力先システムで接続を編集せずに、[非アクティブ] を選択して接続をアクティブにすることもできます。

12. [保存] を選択します。

16.2.3.4.2 BIAR ファイルを使用して上書きを昇格する

上書きを昇格する前にホストシステムを追加してください。 ホストシステムの追加についての詳細は、[システムの管理] オプションを使用する [569 ページ]を参照してください。

BIAR ファイルを使用して上書きを昇格するには、次の手順に従います。

1. プロモーションマネジメントワークスペースツールバーで、上書き設定オプションをクリックします。
   上書き設定ウィンドウが表示されます。
2. セントラルプロモーションマネジメントシステムにログオンしている場合、システムからログアウトします。
3. [ログイン] をクリックし、元のシステムに接続します。
   システムにログインウィンドウが表示されます。
4. [上書き設定] 画面で、[ソース] が付いているソースシステムを選択してオブジェクトをスキャンし、有効な認証情報を使用してシステムにログインします。
5. [スキャン] の横にある [開始] ドロップダウンリストで、[開始] オプションを選択します。
   スキャン処理が開始されます。[上書き一覧] が表示されます。

   > ⓘ 注記
   >
   > 定期的なスキャンをスケジュールするには、ドロップダウンリストから定期的スケジュールの設定オプションを選択します。

6. 上書き一覧で、必要なオブジェクトのステータスをアクティブにし、[保存] をクリックします。
7. [上書きの昇格] をクリックします。
   出力先システムの一覧が表示される場所に、上書きの昇格画面が表示されます。
8. パスワードを使用して BIAR ファイルを暗号化するには、[パスワード暗号化] チェックボックスをクリックします。
   [パスワード] と [パスワードの確認] フィールドが有効になります。
9. [パスワード] フィールドにパスワードを入力します。 [パスワードの確認] フィールドに同じパスワードを再入力します。
10. [エクスポート] をクリックし、BIAR ファイルをファイルシステムに上書きします。

11. CMC を使用して出力先システムにログインし、プロモーションマネジメントツールで インポート ファイルの上書き をクリックします。
    LCMBIAR ファイルのインポートウィンドウが表示されます。
12. [参照] をクリックして BIAR ファイルを参照します。
13. [パスワード] フィールドに BIAR ファイルのパスワードを入力します。

    > **注記**
    > パスワードフィールドは、選択した BIAR ファイルがパスワードを使用して暗号化されている場合のみ表示されます。

14. *OK* をクリックします。 上書きの昇格が完了します。
15. 元のシステムからログオフします。
16. [上書き設定] 画面から [ログイン] をクリックします。
    システムにログインウィンドウが表示されます。
17. 有効な認証情報を使用して、出力先システムにログインします。
    インポートされたオブジェクトの一覧が上書き一覧に表示されます。これらのオブジェクトのステータスは非アクティブです。
18. 編集するオブジェクトの [選択] チェックボックスをオンにして、[編集] をクリックします。 編集したオブジェクトにはアイコンが付きます。

    > **注記**
    > アイコンをクリックして、上書きオブジェクトを削除できます。

19. 必要な値を更新して、完了をクリックします。
    編集したオブジェクトのステータスがアクティブになります。
20. 保存をクリックします。

16.2.3.4.3 CTS+ を使用して上書きを昇格する

上書きを昇格する前にホストシステムを追加してください。 ホストシステムの追加についての詳細は、[システムの管理] オプションを使用する [569 ページ]を参照してください。

CTS+ を使用して上書きを昇格するには、次の手順を完了します。

> **注記**
> このオプションを有効にするために、SAP 認証を使用してプロモーションマネジメントツールを起動します。

1. プロモーションマネジメントワークスペースツールバーで、上書き設定オプションをクリックします。
   上書き設定ウィンドウが表示されます。
2. セントラルプロモーションマネジメントシステムにログオンしている場合、システムからログアウトします。
3. [ログイン] をクリックし、元のシステムに接続します。
   システムにログインウィンドウが表示されます。
4. オブジェクトをスキャンするには、[ソース] が付いているソースシステムを選択し、有効な認証情報を使用して、システムにログインします。

5. [スキャン] の横にある [開始] ドロップダウンリストで、[開始] オプションを選択します。
   スキャン処理が開始されます。 上書き一覧が表示されます。

   > ⓘ 注記
   >
   > 定期的なスキャンをスケジュールするには、ドロップダウンリストから定期的スケジュールの設定オプションを選択します。

6. 上書き一覧で、昇格するオブジェクトのステータスをアクティブに変更し、[保存] をクリックします。
7. [上書きの昇格] をクリックします。
   出力先システムの一覧が表示される場所に、上書きの昇格画面が表示されます。
8. [昇格オプション] ドロップダウンリストから、[*CTS+ と昇格*] を選択します。
9. [昇格] をクリックします。
10. 次の手順を完了して、出力先システムに上書きをリリースします。
    a. CTS+ のドメインコントローラにログインして、[移送オーガナイザ] Web UI を開きます。 移送オーガナイザ Web UI の使用方法の詳細については、Transport Organizer Web UI を参照してください。
    b. 要求のステータスが [変更可能] の場合、[リリース] をクリックして上書きの移送要求をリリースします。
       非 ABAP オブジェクトを含む移送要求のリリースの詳細については、Releasing Transport Requests with Non-ABAP Objects を参照してください。
    c. [移送オーガナイザ] Web UI を閉じます。
11. 次の手順を完了して、出力先システムに上書きをインポートします。
    a. CTS+ のドメインコントローラにログインします。
    b. 移送管理システムに入るには、STMS トランザクションを呼び出します。
    c. [インポートの概要] アイコンをクリックします。

       インポートの概要画面が表示され、すべてのシステムから、インポートキューの項目を見ることができます。
    d. 出力先プロモーションマネジメントシステムのシステム ID をクリックします。
       システムにインポートできる移送要求の一覧を確認できます。
    e. [最新表示] をクリックします。
    f. 関連する移送要求をインポートします。 詳細については、Importing Requests ドキュメントを参照してください。
12. 上書きの昇格が完了します。
13. 有効な認証情報を使用して、いずれかの出力先システムにログインします。
    昇格したすべてのオブジェクトの一覧が [上書き一覧] に表示されます。 これらのオブジェクトのステータスは非アクティブです。
14. 編集するオブジェクトの [選択] チェックボックスをオンにして、[編集] をクリックします。
15. 必要な値を更新して、[完了] をクリックします。
    編集したオブジェクトのステータスがアクティブになります。
16. 保存をクリックします。

16.2.3.5 CTS 設定オプションの使用

このオプションを使用して、ランドスケープ内で Web サービスを追加したり BW システムを管理したりすることができます。 CTS 設定オプションの使用、およびプロモーションマネジメントツールとともに使用するための

CTS の設定に関する詳細については、プロモーションマネジメントツールで CTS+ を設定する [629 ページ]セクションを参照してください。

16.3 プロモーションマネジメントツールの使用

プロモーションマネジメントツールを起動すると、デフォルトで昇格ジョブページに移動します。

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454 を参照してください。

[昇格ジョブ]ホームページ画面には、次のタスクを実行できるさまざまなタブが表示されます。

- 新しいジョブをクリックし、新しいジョブを作成します。ホームページ画面を右クリックして、一覧から新しいジョブを選択することもできます。
- ジョブの新規作成手順をすべて実行するのではなく、インポート > ファイルのインポート をクリックして、BIAR ファイルまたは LCMBIAR をファイルシステムから直接インポートします。
- 上書きをインポートするには、インポート > ファイルの上書き をクリックします。
- 一覧で既存のジョブを選択し、編集をクリックして選択した既存のジョブを編集します。
- 一覧で既存のジョブを選択し昇格をクリックして、選択したジョブをソースシステムから出力先システムに昇格するか、または選択したジョブを LCMBIAR ファイルにエクスポートします。
- 一覧から既存の実行済みジョブを選択しロールバックをクリックして、出力先システムから昇格されたオブジェクトを戻します。
- 一覧から既存の実行済みジョブを選択し履歴をクリックして、選択したジョブの以前の昇格インスタンスを表示します。
- 一覧で既存のジョブを選択しプロパティ をクリックして、選択されたジョブのプロパティ (タイトル、ID、ファイル名、説明など) を表示します。

昇格ジョブアプリケーション領域には、システムに存在するジョブおよびフォルダの一覧と、次の各ジョブまたはフォルダの情報が表示されます。

- 名前: 作成されたジョブまたはフォルダの名前が表示されます。
- ステータス: 作成、成功、一部成功、実行中、失敗などのジョブステータスが表示されます。
- 作成日時: ジョブまたはフォルダが作成された日時が表示されます。
- 最終実行日時: ジョブが最後に昇格された日時が表示されます。
- ソースシステム: ジョブの昇格元システムの名前が表示されます。
- 出力先システム: ジョブの昇格先システムの名前が表示されます。
- 作成者: 特定のジョブまたはフォルダを作成したユーザの名前が表示されます。

> ⓘ 注記
>
> プロモーションマネジメントツールではすべての操作に対して BI プラットフォーム SDK を使用します。

16.3.1 フォルダを作成、削除する

このセクションでは、[昇格ジョブ]ホームページでフォルダを作成および削除する方法について説明します。

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

16.3.1.1 フォルダを作成する

このセクションでは、フォルダの作成方法について説明します。

フォルダを作成するには、次の手順に従います。

1. プロモーションマネジメントツールバーの をクリックします。
2. [フォルダの作成]ダイアログボックスで、フォルダ名を入力します。
3. [*OK*]をクリックします。

新しいフォルダが作成されます。

関連情報

ジョブを作成する [578 ページ]
フォルダを削除する [577 ページ]

16.3.1.2 フォルダを削除する

このセクションでは、フォルダの削除方法について説明します。

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

フォルダを削除するには、次の手順に従います。

1. 昇格ジョブホームページでフォルダを選択します。
2. をクリックします。
   確認ダイアログボックスが表示されます。
3. *OK* をクリックします。

選択したフォルダが削除されます。

関連情報

ジョブを作成する [578 ページ]

16.3.2 ジョブを作成する

このセクションでは、プロモーションマネジメントツールを使用してジョブを新規作成する方法について説明します。

次の表では、ジョブの新規作成に使用できる GUI 要素とフィールドについて説明します。

> **注記**
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454 を参照してください。

フィールド	説明
名前	作成するジョブの名前。
説明	作成するジョブの説明。
キーワード	作成するジョブのコンテンツのキーワード。
ジョブの保存場所	選択したデフォルトのフォルダが表示されます。
ソースシステム	ジョブの昇格元となる BI プラットフォームシステムの名前。
出力先システム	ジョブの昇格先となる BI プラットフォームシステムの名前。
ユーザ名	ソースシステムまたは出力先システムへのログインに使用する必要があるログイン ID。
パスワード	ソースシステムまたは出力先システムへのログインに使用する必要があるパスワード。
認証	ソースシステムまたは出力先システムへのログインに使用される認証の種類。 プロモーションマネジメントツールは、次の認証の種類に対応しています。 • Enterprise • Windows AD • LDAP • SAP

> **注記**
>
> ジョブを作成する前に、BI プラットフォームコンテンツが自動的に更新されるように上書き (存在する場合) が出力先システムで編集および更新されていることを確認してください。詳細については、「上書き設定オプションの使用」を参照してください。

プロモーションマネジメントツールを使用してジョブを新規作成するには、以下の手順に従います。

1. プロモーションマネジメントツールを起動します。
2. [昇格ジョブ]ホームページで[新しいジョブ]をクリックします。
3. 適切なフィールドにジョブの名前、説明、およびキーワードを入力します。

   > ⓘ 注記
   >
   > [説明]、[キーワード]、[出力先システム] の各フィールドには情報を任意入力できます。

4. [ジョブの保存場所] フィールドでジョブの保存先となるフォルダを参照および選択します。

   > ⓘ 注記
   >
   > [ジョブの保存場所] フィールドには、 [新しいジョブ] をクリックする前に [フォルダ] ペインで強調表示されていたフォルダの名前がデフォルトで入力されます。

5. 各ドロップダウンリストからソースシステムと出力先システムを選択します。
   ドロップダウンリストにシステム名が含まれていない場合には、[新しい *CMS* へのログイン]オプションをクリックします。新たなウィンドウが起動します。システム名、ユーザ名、およびパスワードを入力します。
6. [作成] をクリックします。
   “オブジェクトの追加”ウィンドウが表示されます。
7. ジョブに追加するソースシステムからオブジェクトを選択し、追加して閉じるをクリックします。
8. 保存をクリックします。

新たに作成されたジョブがソースシステムの CMS リポジトリに保存されます。

> ⓘ 注記
>
> 一次オブジェクトとしてジョブをフォルダとともに作成し、ジョブが定期ジョブである場合、ジョブには次回実行時にフォルダに追加されるすべてのコンテンツが含まれます。

関連情報

上書き設定オプションの使用 [571 ページ]

16.3.2.1 新しい CMS にログインする

このセクションでは、新しい CMS へのログイン方法について説明します。

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

新しい CMS にログインするには、次の手順に従います。

1. プロモーションマネジメントアプリケーションを起動します。
2. 新しいジョブを作成します。
   新しいジョブの作成の詳細については、ジョブを作成する [578 ページ]を参照してください。

3. [ソースシステム]ドロップダウンリストから[新しい *CMS* へのログイン]を選択します。
   システムにログインダイアログボックスが表示されます。
4. ドロップダウンリストからシステムを選択するか、新しいシステム名を入力します。
5. ユーザ認証情報を入力し、適切な認証の種類を選択してから、[ログイン]をクリックします。
6. [出力先システム]ドロップダウンリストから[新しい *CMS* へのログイン]を選択します。
7. ドロップダウンリストからシステムを選択するか、新しいシステム名を入力します。
8. ユーザ認証情報を入力し、適切な認証の種類を選択してから、ログインをクリックします。

関連情報

ジョブを編集する [581 ページ]
ジョブに InfoObject を追加する [582 ページ]
リポジトリに接続しているときのジョブを昇格する [585 ページ]
ジョブの昇格をスケジュールする [591 ページ]

16.3.3 既存ジョブをコピーして新規ジョブを作成する

このセクションでは、既存ジョブをコピーして新しいジョブを作成する方法について説明します。

> **注記**
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

既存ジョブをコピーして新しいジョブを作成するには、次の手順を実行します。

1. プロモーションマネジメントツールを起動します。
2. [昇格ジョブ]ホームページで[新しいジョブ]をクリックします。
3. [既存のジョブのコピー]オプションをクリックします。
   既存のジョブのコピーウィンドウが開き、昇格ジョブフォルダのジョブ一覧が表示されます。
4. 一覧からジョブを選択し、[作成] をクリックします。
   ジョブの名前、キーワード、説明のほか、ジョブの保存場所フィールドおよび出力先フィールドが表示されます。必要に応じてこれらのフィールドを変更できます。
5. [ジョブの保存場所] フィールドでジョブの保存先となるフォルダを参照および選択し、[作成]をクリックします。

新しいジョブが作成され、オブジェクトの追加ウィンドウが表示されます。

関連情報

ジョブに InfoObject を追加する [582 ページ]
ジョブを編集する [581 ページ]

リポジトリに接続しているときのジョブを昇格する [585 ページ]

16.3.4 ジョブを検索する

プロモーションマネジメントツールの検索機能では、リポジトリにあるジョブを検索することができます。

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

ジョブを検索するには、次の手順に従います。

1. ホームページの [検索] フィールドに検索するテキストを入力します。
2. 検索フィールドの横に表示された一覧をクリックして、検索パラメータを指定します。次の検索パラメータを指定できます。
   - タイトルの検索: このオプションでは、ジョブ名からジョブを検索できます。
   - キーワードの検索: このオプションでは、キーワード名からキーワードを検索できます。
   - 説明の検索: このオプションでは、説明からジョブを検索できます。
   - すべてのフィールドの検索: このオプションでは、ジョブのタイトル、キーワード、および説明からジョブを検索できます。
3. [検索] アイコンをクリックします。

関連情報

ジョブに InfoObject を追加する [582 ページ]
ジョブを編集する [581 ページ]

16.3.5 ジョブを編集する

このセクションでは、ジョブの編集方法について説明します。

> ⓘ 注記
>
> - プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。
> - ジョブの編集はジョブの新規作成とは異なります。

ジョブを編集するには、次の手順に従います。

1. プロモーションマネジメントツールを起動します。
2. [昇格ジョブ]ホームページで、編集するジョブを選択します。
3. [編集]をクリックします。

選択したジョブの詳細が表示されます。必要に応じて InfoObject の追加や削除、依存関係の管理、ジョブの昇格を実行できます。

ジョブを編集する時に、ソースシステム名を変更することはできません。

関連情報

ジョブに InfoObject を追加する [582 ページ]
リポジトリに接続しているときのジョブを昇格する [585 ページ]
ジョブの昇格をスケジュールする [591 ページ]

16.3.6 ジョブに InfoObject を追加する

各ジョブには、InfoObject のセットが含まれている必要があります。したがって、ジョブを出力先システムに昇格する前に、ジョブに InfoObject を追加する必要があります。

> ⓘ 注記
>
> - ビジネスビュー InfoObject (データコネクション、データファンデーション、ビジネスエレメント、およびビジネスビュー) に基づく Crystal レポートを昇格する場合、出力先システムでレポート内のデータを表示するために、セキュリティ情報 (データコネクションでのデータアクセス権限および、データファンデーションおよびビジネスエレメントでのデータフィールド表示権限) を含める必要があります。
> - プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454 を参照してください。

ジョブに InfoObject を追加するには、次の手順に従います。

1. プロモーションマネジメントツールを起動します。
2. 新しいジョブを作成するか、既存のジョブを編集します。
   ジョブの新規作成については、ジョブを作成する [578 ページ]およびジョブを編集する [581 ページ]を参照してください。
3. ジョブを編集する場合はオブジェクトの追加をクリックします。

   > ⓘ 注記
   >
   > ジョブを新規作成する場合は、オブジェクトの追加ダイアログボックスが表示されます。

4. InfoObject を選択するフォルダに移動します。
   選択したフォルダ内の InfoObject の一覧が表示されます。
5. ジョブに追加する InfoObject を選択し、追加をクリックします。

   InfoObject を追加して、[“システムからオブジェクトを追加”] を終了する場合は、“<NAME>”ダイアログボックスで、追加して閉じるをクリックします。InfoObject がジョブに追加され、ダイアログボックスが閉じます。

ジョブに InfoObject を追加したら、ジョブビューアページを右クリックし、昇格処理を選択して昇格タスクを続行できます。選択した InfoObject の依存関係を管理するには、ジョブビューアページで依存関係の管理オプションを使用します。

> ⓘ 注記
>
> - ジョブビューアページの左パネルに表示されるショッピングカートには、ジョブとその依存オブジェクトがフラットツリー構造で表示されます。
> - InfoObject を追加したら、[保存]オプションをクリックして変更を保存します。[保存]オプションをクリックしないでこのタブを閉じようとすると、ジョブを保存するオプションを示すプロンプトが表示されます。

ベストプラクティス: SAP Business Objects では、プロモーションマネジメントツールの最適なパフォーマンスを引き出すために、一度に選択する InfoObject の数が 100 件以下となるように設定することを推奨しています。

関連情報

ジョブの依存関係を管理する [583 ページ]
リポジトリに接続しているときのジョブを昇格する [585 ページ]
ジョブの昇格をスケジュールする [591 ページ]

16.3.7 ジョブの依存関係を管理する

このセクションでは、InfoObject の依存オブジェクトを管理する方法について説明します。

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

InfoObject の依存オブジェクトを管理するには、次の手順に従います。

1. プロモーションマネジメントツールを起動します。
2. 新しいジョブを作成するか、既存のジョブを編集します。
   ジョブの新規作成については、ジョブを作成する [578 ページ]およびジョブを編集する [581 ページ]を参照してください。
3. 必要な InfoObject をジョブに追加し、オブジェクトの追加ダイアログを閉じて、ジョブビューアウィンドウに戻ります。
4. [依存関係の管理]をクリックします。
   依存関係の管理ウィンドウが表示されます。このウィンドウには InfoObject とその依存オブジェクトの一覧が表示されます。選択されていない依存オブジェクトのみを表示するには、[選択されていない依存のみを表示します] チェックボックスをオンにします。
5. グループ化した依存オブジェクトをジョブに追加するオプションを依存オブジェクトの選択ドロップダウンリストから選択します。依存オブジェクトがデフォルトで選択されることはないので、昇格する依存オブジェクトを明示的に選択する必要があります。

   たとえば、[依存オブジェクトの選択]ドロップダウンリストから[すべてのユニバース]を選択すると、依存オブジェクトの一覧にあるすべてのユニバースが含まれることになります。依存オブジェクトを個別に選択することもできます。

タイプ をクリックすると、InfoObject のサポートされているフィルタオプションを表示できます。ドロップダウン リストが表示されます。この一覧には、サポートされているフィルタオプションが表示されます。フィルタオプションを選択し、[*OK*]をクリックします。フィルタされた InfoObject が表示されます。

依存オブジェクト列から依存オブジェクトを選択して、変更を適用をクリックすると、それらの依存オブジェクトがジョブ内のオブジェクト列へ自動的に移動します。

[依存オブジェクトの検索] フィールドに依存オブジェクト名を入力して、依存オブジェクトを検索することもできます。

依存オブジェクトの検索の詳細については、依存関係を検索する [584 ページ]を参照してください。

6. [変更を適用]をクリックして依存オブジェクトの一覧を更新し、[変更を適用して閉じる]をクリックして変更を保存します。

依存オブジェクトは、ツールで自動的に計算されます。これらの依存オブジェクトは、InfoObject の関係または InfoObject のプロパティのいずれかに基づいて計算されます。このツールのバージョンでは、それらの基準のどちらにも当てはまらない依存オブジェクトは計算されません。

> ⓘ 注記
>
> 昇格に使用するフォルダを選択すると、選択したフォルダのコンテンツはプライマリリソースであると見なされます。

関連情報

リポジトリに接続しているときのジョブを昇格する [585 ページ]

16.3.8 依存関係を検索する

プロモーションマネジメントツールの高度な検索機能では、リポジトリにある InfoObject の依存オブジェクトを検索することができます。

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454 を参照してください。

InfoObject の依存オブジェクトを検索するには、次の手順に従います。

1. プロモーションマネジメントを起動します。
2. 新しいジョブを作成するか、または既存のジョブを編集します。
   新しいジョブを作成した場合には、そのジョブに InfoObject を追加します。既存のジョブを編集している場合には、必要に応じてオブジェクトを追加します。
3. [依存関係の管理]をクリックします。
4. [依存オブジェクトの検索] フィールドに検索する依存オブジェクトの名前を入力します。
5. [検索] アイコンをクリックします。

関連情報

ジョブの依存関係を管理する [583 ページ]

16.3.9 リポジトリに接続しているときのジョブを昇格する

このセクションでは、ソースシステムと出力先システムが稼働している場合に、ソースシステムから出力先システムにをジョブを昇格する方法について説明します。

> **注記**
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

以下の表は、プロモーション管理ツールを使用して昇格できる InfoObject タイプの一覧です。

カテゴリ	昇格できるオブジェクトタイプ
レポート	Crystal レポート、Web Intelligence、QaaWS、Lumira
サードパーティオブジェクト	リッチテキスト、テキストドキュメント、Microsoft Excel、Microsoft Power Point、Microsoft Word、Flash、Adobe Acrobat
ユーザ	ユーザとユーザグループ
サーバ	サーバグループ
BI プラットフォーム	フォルダ、プログラム、イベント、プロファイル、オブジェクトパッケージ、ハイパーリンク、カテゴリ、受信ボックスドキュメント、個人用フォルダ、お気に入りフォルダ
ユニバース、ワークスペース、セット	ユニバース UNV、接続、セット
EPM ダッシュボード	ユニバース、接続、レポート、およびアナリティクス
BusinessView	DataFoundation
フェデレーション • レプリケーション一覧 • レプリケーションジョブ	レプリケーション一覧では、Flash、.txt、ディスカッション、.pdf、ハイパーリンク、.xls、オブジェクトパッケージ、Crystal Reports、Web Intelligence ドキュメント、ユニバース、プログラム、接続、DataFoundation、ビジネスビュー、.rtf、プロファイル、イベント、ユーザ、およびユーザグループの各オブジェクトを昇格します。レプリケーション接続は、レプリケーションジョブ、リモート接続、パブリケーション、ディスカッション、Pioneer 接続を昇格します。
BI サービス	Web Intelligence ドキュメント、ユニバース、および接続
新しい InfoObject	Crystal レポート (rpt/rptr)、Pioneer、DSL Universe (UNX)、ビジネスレイヤ (BLX)、接続 (CNX)、データファンデーション (DFX)、Webl、Data Federator、Data Steward、BI ワークスペースなど

カテゴリ	昇格できるオブジェクトタイプ
テナント	プロモーション管理は、テナントおよび対応するテナントオブジェクトを選択してジョブに追加するオプションを提供することで、ソースシステムから出力先システムへのテナントおよびその依存関係の昇格をサポートしています。また、テナントおよび対応するテナントオブジェクト間の関係を依存関係として確立します。この機能は、プロモーション管理の GUI および CLI 両方のモードで動作します。

プロモーション管理では BI Commentary がサポートされます。コメント付きドキュメントを昇格させると、ドキュメントのコメントもソースシステムから出力先システムに移行されます (CMS から CMS、CMS から BIAR、BIAR から CMS)。コメント付きドキュメントを昇格させるには、[昇格] > [コメンタリ設定] を選択してから、[コメントを含める] チェックボックスを選択します。

> **注記**
>
> デフォルトでは [コメントを含める] チェックボックスは選択されていません。

複製されたオブジェクトを昇格する場合、オブジェクトに関連付けられたレプリケーション固有の情報もソースシステムから出力先システムに昇格されます (CMS から CMS、CMS から BIAR、BIAR から CMS)。レプリケーション固有の情報がないドキュメントを昇格するには、[昇格] > [フェデレーションジョブ設定] を選択し、[フェデレーションジョブ関係を含める] チェックボックスの選択を解除します。

> **注記**
>
> デフォルトでは [フェデレーションジョブ関係を含める] チェックボックスは選択されています。

ジョブを昇格するには、次の手順に従います。

1. プロモーション管理を起動します。
2. [昇格ジョブ]ホームページで、昇格するジョブを選択します。
   ホームページ画面を右クリックしてから、[昇格]をクリックすることもできます。
3. 出力先システムのリストから、必要に応じて別の出力先システムを選択します。

   > **注記**
   >
   > 昇格処理を始める前に、ソースシステムと出力先システムの両方にログインしておきます。

4. [管理 *ID* の変更] フィールドに適切な値を入力し、[保存] をクリックします。

   > **注記**
   >
   > 管理 ID の変更は、ロギング、監査、ジョブ履歴などに関する情報を取得するために使用されます。プロモーション管理ツールでは、管理 ID の変更に対して、ジョブ作成の各インスタンスをマップすることができます。管理 ID の変更は、新しいジョブを作成する時にジョブの定義でユーザが設定する属性です。ツールでは、各ジョブの ID が自動的に生成されます。

5. 必要に応じて、セキュリティ設定を選択します。次のオプションが表示されます。
   - セキュリティを昇格しない: これはデフォルトオプションです。
   - セキュリティを昇格: ジョブと関連セキュリティ権限を昇格するには、このオプションを使用します。
   - オブジェクトセキュリティの昇格: オブジェクトやフォルダのセキュリティを昇格するには、このオプションを使用します。
   - ユーザセキュリティの昇格: ジョブに含まれているユーザの権限を昇格できます。

- アプリケーションの権限を含める: このオプションはユーザセキュリティの昇格も選択している場合にのみ選択できます。ジョブに含まれているオブジェクトがアプリケーションの権限を継承する場合には、ジョブとともにそれらの権限が昇格されます。
- 最上位セキュリティの昇格: 最上位のセキュリティ権限を昇格するには、このオプションを使用します。

> ⚠ 警告
>
> [最上位の昇格] セキュリティオプションは、ターゲットシステムに定義されている最上位のセキュリティ権限を上書きします。

[セキュリティを表示]をクリックして、ジョブに含まれている InfoObject のセキュリティ依存関係を表示することもできます。

> ⓘ 注記
>
> [セキュリティを表示] ボタンは、新規ジョブを保存するまでは無効です。

6. [保存] をクリックします。

   [セキュリティを表示] ボタンが有効になります。セキュリティ依存性を確認できます。
7. [昇格をテスト]をクリックして、ソースシステムと出力先システムの間で InfoObject の CUID が競合していないことを確認します。昇格の詳細情報は、成功、失敗、および警告のタブに表示されます。最初の列には昇格対象オブジェクトが表示されます。2 番目の列には各 InfoObject の昇格ステータスが表示されます。プロモーション管理ツールでは、選択したオブジェクトがユーザ、グループ、ユニバースなどに分類されます。

   > ⓘ 注記
   >
   > このオプションで対象の InfoObject が実際に昇格されることはありません。

   昇格テストの結果は次のいずれかになります。
   - 上書き: 出力先システムの InfoObject がソースシステムの InfoObject によって上書きされます。
   - コピー済み: ソースシステムの InfoObject が出力先システムにコピーされます。
   - 中断: InfoObject はソースシステムから出力先システムに昇格されません。
   - 警告: 出力先システムの InfoObject の方が新しいバージョンであり、ジョブから InfoObject を削除できます。ただし、InfoObject を昇格することもできます。
   - マップ済み: InfoObject は出力先システムの InfoObject にマップされています。
8. 特定の時間または定期的なスケジュールで昇格を実行する場合は、スケジュールをクリックします。
9. [昇格] をクリックします。
   スケジュールされたジョブが昇格されます。

ジョブを昇格しない場合には、[保存]オプションを使用して、セキュリティ、変更管理 ID、スケジュール設定などの変更を保存できます。

16.3.10 LCMBIAR ファイルを使用したジョブの昇格

昇格とは、リポジトリ間で BI リソースを移動させるアクティビティです。ソースシステムと出力先システムが同じネットワークにある場合、プロモーションマネジメントツールでは WAN または LAN を使用して InfoObject を昇格します。ただし、プロモーションマネジメントツールでは、ソースシステムと出力先システムが同じネットワークにない場合でも、InfoObject を昇格することもできます。

ソースシステムと出力先システムが同じネットワークにないシナリオでは、プロモーションマネジメントツールでソースシステムから LCMBIAR ファイルにジョブをエクスポートしてから、そのジョブを BIAR ファイルから出力先システムにインポートすることにより、ジョブを出力先システムに昇格することができます。

このセクションでは、LCMBIAR ファイルにジョブをエクスポートしてから、そのジョブを BIAR ファイルから出力先システムにインポートする方法について説明します。

> ⓘ 注記
>
> - プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454 を参照してください。
> - プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454 を参照してください。

関連情報

LCMBIAR ファイルへのジョブのエクスポート [588 ページ]
LCMBIAR ファイルからのジョブのインポート [589 ページ]

16.3.10.1 LCMBIAR ファイルへのジョブのエクスポート

この節では、LCMBIAR ファイルにジョブをエクスポートする方法について説明します。

LCMBIAR ファイルにジョブをエクスポートするには、次の手順に従います。

1. プロモーションマネジメントツールを起動し、ジョブを新規作成します。
   ジョブの新規作成の詳細については、次のリンクを参照してください。 ジョブを作成する [578 ページ]
2. 出力先ドロップダウンリストから *LCMBIAR ファイルに出力*オプションを選択し、作成をクリックします。
3. [オブジェクトの追加] をクリックして InfoObject をジョブに追加します。

   選択したジョブの依存を管理するには、[依存関係の管理]オプションを使用します。
4. パスワードを使用して LCMBIAR ファイルを暗号化するには、[パスワード暗号化] チェックボックスをクリックします。
5. [パスワード] フィールドにパスワードを入力します。
6. [パスワードの確認] フィールドにパスワードを再入力します。
7. [昇格] をクリックします。
   昇格ウィンドウが表示されます。
8. 必要に応じてセキュリティオプションを変更し、エクスポートをクリックします。
   LCMBIAR ファイルが作成されます。LCMBIAR ファイルはファイルシステムに保存できます。
9. (オプション) LCMBIAR ファイルを FTP サーバまたは SFTP サーバにエクスポートするには、[*LCMBIAR ファイルの出力先*] をクリックして [*FTP*] または [*SFTP*] を選択します。ホスト名、ポート、ユーザ名、パスワード、ディレクトリ、およびファイル名を入力し、エクスポートをクリックします。

> ⓘ 注記
>
> [*LCMBIAR ファイルの出力先*] として [*SFTP*] を選択した場合、SFTP フィンガープリントを追加で入力する必要があります。

10. [出力先] ドロップダウンリストから [*LCMBIAR ファイルに出力*] を選択し、[*LCMBIAR ファイルの出力先*] をクリックします。

LCMBIAR ファイルへのジョブのエクスポートをスケジュールできます。この詳細については、ジョブの昇格をスケジュールする [591 ページ]の節を参照してください。

関連情報

ジョブに InfoObject を追加する [582 ページ]
ジョブの依存関係を管理する [583 ページ]

16.3.10.2 LCMBIAR ファイルからのジョブのインポート

LCMBIAR ファイルからジョブをインポートできます。LCMBIAR ファイルは保存デバイスから出力先システムにコピーされます。

LCMBIAR ファイルをインポートするには、次の手順に従います。

1. プロモーションマネジメントツールを起動します。
2. 昇格ジョブホームページで、インポート > ファイルのインポート をクリックします。
   ファイルからインポートウィンドウが表示されます。
3. ファイルシステムまたは FTP サーバあるいは SFTP サーバから BIAR ファイルをインポートできます。
   - ファイルシステムから BIAR ファイルをインポートするには、次の手順に従います。
     1. [ファイルシステム] を選択します。
     2. 参照をクリックし、ファイルシステムから LCMBIAR ファイルを選択します。
     3. [パスワード] フィールドに LCMBIAR ファイルのパスワードを入力します。

        > ⓘ 注記
        >
        > パスワードフィールドは、LCMBIAR ファイルがパスワードで暗号化されている場合にのみ表示されます。

     4. [作成] をクリックします。ジョブが作成されます。

        > ⓘ 注記
        >
        > 同じ名前のジョブが存在する場合、保存の確認ポップアップが表示されます。'はい' をクリックすると既存のジョブが上書きされ、'いいえ' をクリックすると新しい名前 (`jobname_copy<CURRENT_DATE_AND_TIME>`) でジョブが作成されます。

   - FTP サーバから LCMBIAR ファイルをインポートするには、次の手順に従います。
     1. [*FTP*] を選択します。

2. [ホスト]、[ポート]、[ユーザ名]、[パスワード]、[ディレクトリ]、および [ファイル名] の各フィールドに適切な詳細情報を入力し、[*OK*] をクリックします。

- SFTP サーバから LCMBIAR ファイルをインポートするには、次の手順に従います。
  1. [*SFTP*] を選択します。
  2. [ホスト]、[ポート]、[ユーザ名]、[パスワード]、[ディレクトリ]、[フィンガープリント] および [ファイル名] の各フィールドに適切な詳細情報を入力し、[*OK*] をクリックします。

4. [昇格] をクリックします。
   昇格 - ジョブ名ウィンドウが表示されます。
5. [出力先] ドロップダウンリストから、出力先システムを選択します。[新しい *CMS* へのログイン] を選択すると、認証情報が要求されます。出力先システムのログイン認証情報を確認します。
6. [昇格]をクリックし、出力先システムにコンテンツを昇格します。

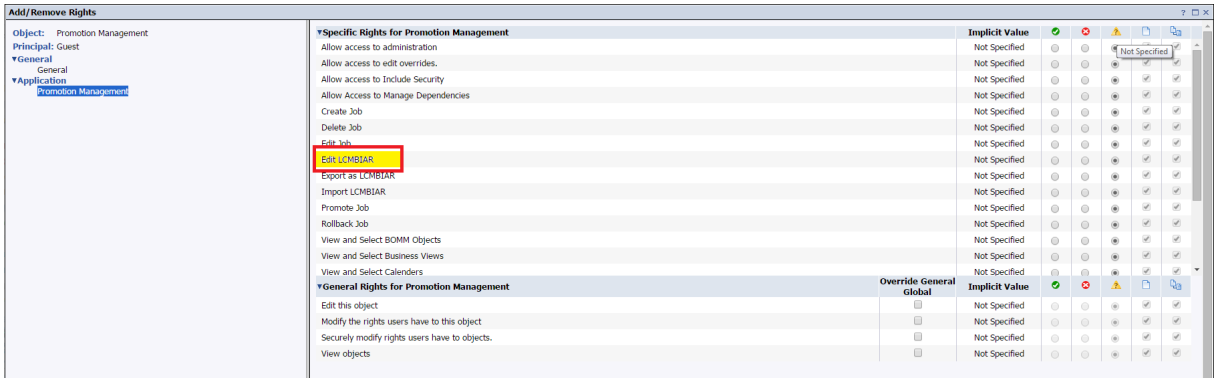
   [昇格をテスト]オプションをクリックして、昇格するオブジェクトと昇格のステータスを表示できます。
7. オプション: カスタマイズを使用する Web Intelligence ドキュメントをインポートする場合は、[ユーザグループ *BI* 基本設定] タブで、[ユーザグループ *BI* 基本設定の上書き] をオンにしてカスタマイズをインポートします。

関連情報

ジョブの依存関係を管理する [583 ページ]

16.3.10.2.1 LCMBIAR ファイルからのオブジェクトの選択的取得

ユーザが LCMBIAR ファイルからオブジェクトを選択的に取得するには、[*LCMBIAR* の編集 権限が必要です。



LCMBIAR ファイルからオブジェクトを選択的に取得するには、次の手順に従います。

1. 該当するオブジェクトを選択します。
2. [昇格] をクリックします。

> ⓘ 注記
>
> - 選択したオブジェクトが含まれる新しいジョブが作成されます。

- コマンドラインツールを使用して、同じ操作を実行することができます。詳細については、コマンドラインツールパラメータ [603 ページ]を参照してください。
- 選択的昇格は、Live から Live のシナリオではサポートされていません。

16.3.11 ジョブの昇格をスケジュールする

この節では、ジョブの昇格をスケジュールする方法について説明します。繰り返しオプションとパラメータを指定する方法についても説明します。

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

ジョブインスタンスの昇格をスケジュールするには、次の手順に従います。

1. [昇格] ダイアログボックスで [スケジュール] オプションをクリックします。
2. 必要なスケジュールオプションを設定し、[スケジュール] をクリックします。

昇格のジョブがスケジュールされた後で、InfoObject をそのジョブを含むフォルダに追加した場合、これらもスケジュールされた時間に出力先に昇格されます。ただし、LCMBIAR ファイルを使用してジョブをスケジュールしようとする場合、LCMBIAR は 'real' 出力先と見なされないため、これは当てはまりません。

> → ヒント
>
> ジョブの昇格が完了したら、そのジョブのインスタンスをすべて表示できます。これを行うには、昇格ジョブページでジョブを選択して、ツールバーで履歴をクリックします。

ジョブの昇格も、イベントトリガに基づいて行われます。

ジョブの昇格のステータス (成功/一部成功/失敗など) に基づいて電子メール通知を選択できます。各種スケジュールオプションおよび通知の設定の詳細については、「スケジュール」の節を参照してください。

関連情報

LCMBIAR ファイルへのジョブのエクスポート [588 ページ]

16.3.11.1 定期および一時停止中のジョブ昇格インスタンスを更新する

プロモーションマネジメントツールでは、定期および待機中のインスタンスオプションを使用して、昇格ジョブインスタンスのステータスを追跡して再スケジュールすることができます。

昇格ジョブインスタンスのステータスを追跡して再スケジュールするには、次の手順に従います。

1. プロモーションマネジメントツールを起動します。
2. [昇格ジョブ]ホームページでジョブを選択します。
3. [履歴] をクリックします。
   ジョブ履歴ウィンドウが表示されます。
4. [定期および一時停止中のインスタンス]をクリックします。
   定期および一時停止中のインスタンスのジョブ履歴ウィンドウが表示されます。 このウィンドウには、定期および待機中の昇格ジョブインスタンスが表示されます。

   必要に応じて、次のオプションを使用できます。
   - 昇格されたジョブインスタンスを表示するには、昇格されたインスタンスをクリックします。
   - 選択した待機中または定期のインスタンスを一時停止するには、一時停止をクリックします。
   - 一時停止中のスケジュールされた昇格ジョブインスタンスの一時停止を解除するには、再開オプションをクリックします。
   - 選択した昇格ジョブインスタンスを再スケジュールするには、再スケジュールオプションをクリックします。
   - スケジュールされた昇格ジョブインスタンスを削除するには、 をクリックします。
   - スケジュールされた昇格ジョブインスタンスのステータスを最新表示するには、 をクリックします。
   - 1 オプションを使用して 1 ページずつ移動するか、あるいは該当するページ番号を入力して特定のページに移動できます。

   > **注記**
   > 定期および一時停止中のインスタンスのジョブ履歴ウィンドウのステータス列には、定期や待機中といった昇格ジョブインスタンスのステータスが表示されます。

関連情報

ジョブをロールバックする [593 ページ]

16.3.12 ジョブ履歴を表示する

このセクションでは、ジョブ履歴の表示方法について説明します。

> **注記**
> ジョブ履歴を表示するには、ジョブが次のいずれかのステータスであることを確認する必要があります。
> - 成功
> - 失敗
> - 一部成功

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

ジョブ履歴を表示するには、次の手順に従います。

1. プロモーションマネジメントツールを起動します。
   昇格ジョブホームページが表示されます。
2. 履歴を表示するジョブを選択し、[履歴] タブをクリックします。

   ジョブインスタンスの日時、ジョブ名、ソースシステム名、出力先システム名、ジョブを昇格させたユーザの ID、およびジョブのステータス (成功、失敗、または一部成功) が表示されます。

   ステータス列に表示されているリンクを使用して、ジョブの詳細ステータスを表示できます。

16.3.13 ジョブをロールバックする

ロールバックオプションでは、ジョブの昇格後に出力先システムを以前の状態に戻すことができます。

> ⓘ 注記
>
> プロモーションマネジメントツールにセキュリティ拡張機能が実装されているため、アクションの実行時に特定の動作が変更されます。詳細については、3350454を参照してください。

ジョブをロールバックするには、次の手順に従います。

1. プロモーションマネジメントツールを起動します。
   昇格ジョブホームページが表示されます。
2. 次の操作を実行できます。

   - ロールバックするジョブを右クリックし、ロールバックを選択します。
   - ロールバックするジョブを選択し、ロールバックタブをクリックします。

   ロールバックウィンドウが表示されます。
3. ロールバックするインスタンスを選択し、完全ロールバックをクリックします。
   インスタンスがロールバックされます。

昇格ジョブの最新インスタンスのみをロールバックできます。同時に複数のジョブインスタンスをロールバックすることはできません。

16.3.13.1 [一部ロールバック] オプションを使用する

プロモーションマネジメントツールでは、ジョブに含まれている InfoObject を出力先システムから完全にまたは一部ロールバックすることができます。

InfoObject を一部ロールバックするには、次の手順に従います。

1. プロモーションマネジメントツールを起動します。
   昇格ジョブホームページが表示されます。

2. 次の操作を実行できます。
   - ロールバックするジョブを右クリックし、[ロールバック] を選択します。
   - ロールバックするジョブを選択し、[ロールバック] タブをクリックします。

   ロールバックウィンドウが表示されます。
3. 一覧からインスタンスを選択し、一部ロールバックをクリックします。

   [ジョブビューア]ページには、選択したジョブの InfoObject 一覧が表示されます。
4. ロールバックする InfoObject を選択し、[ロールバック]をクリックします。

> ⓘ 注記
>
> 次のインスタンスをロールバックする前に、インスタンスに含まれている InfoObject をすべてロールバックしておく必要があります。

> ⚠ 警告
>
> セキュリティとともに昇格されたジョブの場合、InfoObject を一部ロールバックすると、選択した依存 InfoObject のセキュリティが以前の状態にロールバックされないことがあります。

関連情報

異なるバージョンの BI リソースを管理する [653 ページ]

16.3.13.2 パスワード期限切れ後にジョブをロールバックする

このセクションでは、ジョブの昇格に使用されたパスワードの期限切れ後に、ジョブをロールバックする方法について説明します。

パスワードの期限切れ後にジョブをロールバックするには、次の手順に従います。

1. ロールバックするジョブを選択し、[ロールバック]をクリックします。
2. [ロールバック]ウィンドウで[完全ロールバック]を選択します。
   エラーメッセージが表示されます。 このメッセージは、ジョブをロールバックできないことを知らせるものです。 ソースシステムまたは出力先システムへのログインも求められます。
3. 新しいログイン認証情報を入力し、[ログイン]をクリックします。

ロールバック処理が完了したことを知らせるダイアログボックスが表示されます。

> ⓘ 注記
>
> ソースシステムまたは出力先システムの認証情報を使用して昇格されたジョブが自動的に更新されます。

関連情報

パスワード期限切れ後に InfoObject を部分的にロールバックする [595 ページ]
[一部ロールバック] オプションを使用する [593 ページ]

16.3.13.2.1 パスワード期限切れ後に InfoObject を部分的にロールバックする

このセクションでは、ソースシステムまたは出力先システムのパスワードの期限切れ後に InfoObject を部分的にロールバックする方法について説明します。

パスワード期限切れ後に InfoObject を部分的にロールバックするには、次の手順に従います。

1. ロールバックするジョブを選択し、[ロールバック]をクリックします。
   ロールバックウィンドウが表示されます。
2. [一部ロールバック]オプションを選択します。
   エラーメッセージが表示されます。 このメッセージは、InfoObject をロールバックできないことを知らせるものです。 ソースシステムまたは出力先システムへのログインも求められます。
3. 新しいログイン認証情報を入力し、[ログイン]をクリックします。
   ジョブビューアページが表示されます。 このページには InfoObject の一覧が表示されます。
4. 必要な InfoObject を選択し、[ロールバック]をクリックします。

> ⓘ 注記
>
> ソースシステムまたは出力先システムの認証情報を使用して昇格されたジョブが自動的に更新されます。

関連情報

ジョブをロールバックする [593 ページ]
[一部ロールバック] オプションを使用する [593 ページ]
パスワード期限切れ後にジョブをロールバックする [594 ページ]

16.4 プロモーションマネジメントツールを使用するリポジトリのフルコンテンツの昇格

リポジトリのコンテンツを昇格するには、計画、準備を行い、十分な時間をかける必要があります。 この節では、デプロイメント間のコンテンツ昇格に成功するために必要なアクションについて説明します。

16.4.1 ソースシステムおよびターゲットシステムを準備する

ソースシステムおよびターゲットシステムは、コンテンツを昇格する前に最適に設定しておく必要があります。

1. ソースシステムの場合:
   a. リポジトリ診断ツール (RDT) を使用して、ソースシステムをスキャンおよび修正し、リポジトリや FRS の不一致があれば修正します。RDT の詳細については、*Business Intelligence* プラットフォームリポジトリ診断ツールユーザガイドを参照してください。
   b. ソースシステムのシステム使用量を最小限に抑えて、昇格時の変更を最小にします。システムがアクティブな場合、オブジェクトの障害が生じる可能性があります。

   > ⓘ 注記
   >
   > 障害が発生した場合は、ジョブのステータスを確認して、すべての問題を修正します。

2. ターゲットシステムの場合:
   a. ライセンスキーコードを使用して、適切で十分なライセンスをターゲットシステムに確実に設定します。

   > ⓘ 注記
   >
   > 不十分なライセンスが原因のコンテンツ昇格失敗を回避するには、両方のシステムで同一のライセンスを使用します。

   b. サードパーティ認証を使用する場合は、コンテンツを昇格する前に、ターゲットシステムに設定して有効化する必要があります。

   > ⓘ 注記
   >
   > ユーザまたはユーザグループはマップしないでください。マップすると、ターゲットシステムで、異なる CUID を持つユーザまたはユーザグループが作成されます。昇格処理では、CUID を使用して、ソースシステムとターゲットシステム間でオブジェクトを識別しマップします。ユーザおよびユーザグループをマップすると、コンテンツの不一致が生じ、昇格が失敗します。

   c. ソースシステムで必要なすべてのアドオンが、ターゲットシステムにもインストールされているようにします。

   > ⓘ 注記
   >
   > 移行を成功するためには、Analysis や Design Studio などのアドオンをソースシステムにインストールする必要があります。

   d. QaaWS 接続を使用するコンテンツがある場合は、上書きを有効化して、QaaWS 接続が適切な Web サービスをポイントするようにする必要があります。上書きの設定の詳細については、“上書き”の節を参照してください。
   e. スケジュールされ完了したすべてのインスタンスを移行する必要がある場合は、プロモーションマネジメントのジョブ設定で依存関係の管理ページに完了したインスタンスを表示するをクリックする必要があります。
3. セントラルシステムの場合:
   a. ソースシステム、ターゲットシステム、または別のシステムをセントラルシステムとして指定でき、指定したシステムでプロモーションマネジメントジョブが実行されます。リポジトリ全体を昇格する場合は、セントラルシステムで、追加のシステムリソースを必要とする大量のコンテンツを扱います。セントラルシステムをオブジェクト 10,000 個に対応できるよう設定するには、次のサイズ設定を参考にします。

	一時スペースの割り当て	メモリの割り当て	追加設定
`LCM_CLI`	2 GB	2 GB	`LCM_CLI.bat` を更新して、`-Xmx` パラメータを変更します。
プロモーションマネジメント Job Server	3 GB	3 GB	CMC で、`-javaargs Xmx3g` パラメータを追加することで、プロモーションマネジメント Job Server のスタートアッププロパティを更新します。詳細については、SAP ノート 2286419 を参照してください。

たとえば、ジョブに 50,000 個のオブジェクトが含まれると予測される場合は次のとおりとなります。

- メモリ 10 GB を `LCM_CLI` に割り当てます (50,000 ÷ 10,000 × 2)。
- メモリ 15 GB を Job Server に割り当てます (50,000 ÷ 10,000 × 3)。

> **注記**
>
> このサイズ設定ガイドラインはほとんどの環境に適用されます。ただし、リソース要件はドキュメントのサイズに影響を受けることがあります。

16.4.2 移行ストラテジー

- すべてのジョブ昇格で、Web CMC ツールではなくコマンドラインインタフェース (CLI) を使用します。
  - CLI は、1,000 を超えるオブジェクトを含む昇格ジョブで問題となる、20 分という Web セッションの制限を回避します。

    > **注記**
    >
    > オブジェクトの制限は、十分なシステムリソースに依存します。

  - CLI では、クエリ言語を使用して、移行するコンテンツを選択することで、コンテンツの昇格を詳細にコントロールできます。 同じタイプのコンテンツや、同じディレクトリに存在するコンテンツを選択できます。
  - CLI はまとめて実行することができ、他のスクリプトツールで昇格ジョブを初期化できます。
- まず、主体 (ユーザおよびユーザグループ) の昇格によって、セキュリティを確立します。
  - ユーザおよびユーザグループの昇格をはじめに行うと、ターゲットシステムでセキュリティモデルが保持され、その後に行われるユーザの個人用コンテンツ (受信ボックス、お気に入り、個人用カテゴリなど) の移行を成功させることができます。

    > **注記**
    >
    > 最初にこのタスクを実行し、ターゲットシステムのユーザおよびユーザグループの CUID をソースシステムのものと一致させることが重要です。

- 依存関係の計算をオフにします。
  - 依存関係の計算は、ジョブ作成処理で最も負荷が高いタスクの 1 つです。 リポジトリの完全移行中は、すべてのオブジェクトが移行されるため、この計算は必要ありません。

    > ⓘ 注記
    >
    > この機能は、必要な依存オブジェクトがわからない場合にのみ、役立ちます。

- 可能な限り、セキュリティの計算を含めないようにします。
  - セキュリティの計算は、ジョブ作成処理で 2 番目に負荷が高いタスクです。 異なる複数のディレクトリに多くのドキュメントがある場合は、昇格を 2 つのジョブに分割し、セキュリティはディレクトリのみに設定します。 1 つ目のジョブにはセキュリティが有効なオブジェクトのみを含め、2 つ目のジョブにはセキュリティが無効なドキュメントのみを含めます。 こうすることで、ディレクトリのみでセキュリティの計算を実行することができ、すべてのドキュメントでセキュリティを計算せずにすみます。

    > ⓘ 注記
    >
    > オブジェクトのセキュリティは、フォルダのセキュリティから継承されるため、保持されます。

16.5 システム全体の昇格ステップ

システム全体を昇格するには、3 つの別の昇格ジョブを順に実行する必要があり、それぞれで特定のコンテンツタイプを昇格します。複数のオブジェクトを昇格する方法の詳細については、Knowledge Base Article 1969259 を参照してください。

次の表に、各昇格ジョブのコンテンツタイプおよびパラメータ設定の概要を示します。

昇格ジョブ	コンテンツタイプ	`exportDependencies`	`includeSecurity`
1	すべてのユーザとユーザグループ	false	true
2	すべての依存オブジェクト	false	true
3	すべての 1 次オブジェクト	false	true

コマンドラインインタフェース (CLI) を使用して、各ジョブを作成および実行します。CLI の詳細については、コマンドラインオプションの使用 [602 ページ]の節を参照してください。

共通パラメータ

3 つの昇格ジョブすべてで次のパラメータを使用します。

> → 注意
>
> 各パラメータは新しい行に記述してください。

```
action=promote
```

```
Source_CMS=<SourceSystem>
Source_userName=Administrator
Source_password=<AdministratorPassword>
LCM_CMS=<NameOfCentralSystem>
LCM_userName=Administrator
LCM_password=<AdministratorPassword>
Destination_CMS=<TargetSystem>
Destination_userName=Administrator
Destination_password=<AdministratorPassword>
exportDependencies=false
includeSecurity=true
stacktrace=true
consolelog=true
```

16.5.1 ユーザおよびユーザグループを昇格する (ジョブ 1)

ソースシステムとターゲットシステムの間に同一のセキュリティモデルを確立し、ユーザおよびユーザグループオブジェクトの CUID を確実に同一のものとするには、はじめにユーザおよびユーザグループを昇格します。

1. 共通パラメータを使用して usersandgroups.properties ファイルを作成し、すべてのユーザおよびユーザグループを選択するために、このファイルに次のパラメータを追加します。

   ```
   exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
   SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
   (SI_KIND='User' OR SI_KIND='UserGroup') AND NOT (SI_ID in (11,12, 501, 1, 2,
   3))
   ```

2. ジョブを実行するには、<INSTALLDIR>¥win64x64¥scripts ディレクトリに移動して、次のコマンドを実行します。

   ```
   Lcm_cli.bat –lcmproperties=usersandgroups.properties
   ```

16.5.2 依存オブジェクトを昇格する (ジョブ 2)

依存オブジェクトは、パブリックフォルダおよびユーザのお気に入りフォルダの 1 次オブジェクトに依存されます。 他のすべてのジョブで includeDependencies を true に設定しなくてすむよう、2 番目に依存オブジェクトを昇格します。 依存オブジェクトは次のとおりです。

- アクセスレベル
- アプリケーション
- ビジネスビュー
- カレンダ
- カテゴリ
- 接続
- イベント
- OLAP 接続
- プロファイル
- プロジェクト

- QaaWS
- リモート接続
- レプリケーション一覧
- サーバグループ
- ユニバース

1. 共通パラメータを使用して dependencies.properties ファイルを作成し、すべての依存オブジェクトを選択するために、このファイルに次のパラメータを追加します。

```
#total number of queries (if > 1)
exportQueriesTotal=12
#Projects, Universes, Connections, OLAP Connects: SI_ID=95
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (95)")
#QaaWS: SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'
#-need to ensure Overrides are scanned at the source, promoted to the target
and set to active
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='AcTDjF_lm8dElXVCUgHI2Ps'")
#Events: SI_ID=21
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (21)") and
si_specific_kind != 'MON.MonitoringEvent'
#Calendars: SI_ID=22
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (22)")
#Categories: SI_ID=45
exportQuery5=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID IN (45)")
#Access Levels: SI_ID=57
exportQuery6=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (57)")
#Server Groups: SI_ID=17
exportQuery7=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (17)")
#Profiles: SI_ID=50
exportQuery8=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (50)")
#Applications: SI_ID=99
exportQuery9=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (99)")
#Remote Connections:  SI_CUID = 'AVwSekNrtFxGqJ6Jp2rLwrI'
exportQuery10=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID =
'AVwSekNrtFxGqJ6Jp2rLwrI'")
#Replication Lists:  SI_CUID = 'ASOr8wap3MJOgdWV5HLcZ1M'
exportQuery11=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_CUID='ASOr8wap3MJOgdWV5HLcZ1M'")
#BusinessViews: SI_ID=98
exportQuery12=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID IN (98)")
```

2. ジョブを実行するには、<INSTALLDIR>¥win64x64¥scripts ディレクトリに移動して、次のコマンドを実行します。

```
Lcm_cli.bat –lcmproperties=dependencies.properties
```

16.5.3 1 次オブジェクトを昇格する (ジョブ 3)

1 次オブジェクトは、パブリックフォルダおよびユーザのお気に入りフォルダにある中心的な BI ドキュメントです。2 番目の昇格ジョブがすでに実行済みである場合、すべての依存オブジェクトは移行されており、最後に 1 次オブジェクトを昇格すると、1 次オブジェクトと依存オブジェクトの間のリレーションシップが再確立されます。

1. 共通パラメータを使用して primaryobjects.properties ファイルを作成し、すべてのユーザおよびユーザグループを選択するために、このファイルに次のパラメータを追加します。

```
#total number of queries (if > 1)
exportQueriesTotal=4
#All Public Folders
exportQuery1=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)")
#All user collaterals (Inbox, FavoriteFolder, PersonalCategory)
exportQuery2=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='Inbox')")
exportQuery3=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='FavoritesFolder')")
exportQuery4=SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "(SI_KIND='PersonalCategory')")
```

同じジョブを再実行する場合は、以下のクエリを使用して LCM ジョブを除外します。

```
SELECT TOP 100000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER,
SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") and SI_KIND not in
('LCMJob')
```

2. ジョブを実行するには、<INSTALLDIR>¥win64x64¥scripts ディレクトリに移動して、次のコマンドを実行します。

```
Lcm_cli.bat –lcmproperties=primaryobjects.properties
```

> ⓘ 注記
>
> パブリックフォルダまたはユーザのお気に入りフォルダに 50,000 個を超えるオブジェクトがある場合は、この最後のジョブを複数の小さなジョブに分割する必要があることがあります。

> ⓘ 注記
>
> コマンドラインインタフェースのコマンドを実行するマシンとプロモーションマネジメント Job Server の両方が、サイズ設定要件を満たしていることを確認します。詳細については、“サイズ変更”の節を参照してください。

16.5.4 昇格後の作業

プロモーションマネジメントでは、サーバグループのみが昇格され、そのサーバは昇格されません。 サーバが指定されているレポートが引き続き機能するように、サーバを再作成して、適切なサーバグループに割り当てる必要があります。

16.6 コマンドラインオプションの使用

プロモーションマネジメントツールのコマンドラインオプションでは、ある BI プラットフォームデプロイメントから別の BI プラットフォームデプロイメントにオブジェクトを昇格することができます。 複数ジョブのバッチスクリプトを作成することができます。

> → ヒント
>
> 多数のオブジェクトを含むジョブのコマンドラインオプションを使用します。

プロモーションマネジメントツールでは、コマンドラインによる次のジョブの昇格がサポートされています。

- パスワード暗号化を使用した既存の昇格ジョブテンプレートの LCMBIAR へのエクスポート
- パスワード暗号化を使用しない既存の昇格ジョブテンプレートの LCMBIAR へのエクスポート
- 単独/複数のプラットフォームのクエリのエクスポート
- 複数のプラットフォームクエリの昇格
- 既存のジョブテンプレートを使用した昇格
- 既存の LCMBIAR ファイルのインポートおよび昇格
- CMS から CMS への昇格を実行する

16.6.1 Windows でコマンドラインツールを実行する

コマンドラインツールを実行するには、次の手順に従います。

1. コマンドラインウィンドウまたはシェルを起動します。
2. 適切なディレクトリに移動します。

   たとえば、Windows のディレクトリパスは、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib` です。
3. 次のいずれかを実行します。
   - LCMCLI を実行し、プログラムの実行前に Java のパスが設定されていることを確認します。
     コマンド: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <プロパティファイル>`
   - `C:¥Program Files (x86)¥SAP Business Objects¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥scripts¥lcm_cli.bat` から BAT ファイルを実行します。
     コマンド: `lcm_cli.bat -lcmproperty <プロパティファイル>`

> ⓘ 注記
>
> プロンプトが表示されたら、有効なパスワードを入力します。

プロモーションマネジメントコマンドラインツールでは、`<properties>` ファイルをパラメータとして取得します。 `<properties>` ファイルには、実行するアクションに関するプロモーションマネジメントツールと通信するために必要なパラメータ、接続先の BI プラットフォームデプロイメント、接続メソッド、昇格するオブジェクトが含まれています。

ファイルは、`<FILENAME>.properties` の形式で書かれている必要があります。

例: `<Myproperties.properties>`

16.6.2 Unix でコマンドラインツールを実行する

コマンドラインツールを実行するには、次の手順に従います。

1. シェルを起動します。
2. 適切なディレクトリに移動します。

   例: `/usr/u/qaunix/Aurora604/sap_bobj/enterprise_xi40/java/lib`
3. 次のいずれかを実行します。
   - LCMCLI を実行し、プログラムの実行前に Java のパスが設定されていることを確認します。
     コマンド: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <プロパティファイル>`
   - <インストールディレクトリパス>¥sap_bobj¥lcm_cli.sh から BAT ファイルを実行します。
     コマンド: `lcm_cli.sh -lcmproperty <プロパティファイル>`

> ⓘ 注記
>
> プロンプトが表示されたら、有効なパスワードを入力します。

16.6.3 コマンドラインツールパラメータ

プロモーションマネジメントツールのコマンドラインオプションのコマンドラインパラメータは、以下の 3 つの主要なプロモーションタイプに従って編成されています。

- LCMBIAR ファイルからライブ CMS へのオブジェクトの昇格
- ソースライブ CMS からターゲットライブ CMS へのオブジェクトの昇格
- ライブ CMS から LCMBIAR ファイルへのオブジェクトのエクスポート

これら 3 つのプロモーションタイプが関係するパラメータに加えて、すべての昇格シナリオで使用できる一般コマンド用のパラメータもあります。

> → 注意
>
> 引用符で囲んだコマンドラインのパラメータを入れないでください。

> ⓘ 注記
>
> - コマンドラインオプションでは、エクスポート前にジョブが作成されると同様に、その場で一時ジョブが作成されます。作成されるジョブ名は、`Query_<USER>_<Timestamp>` の組み合わせで設定されます。これは `<exportQuery>` にのみ適用されます。
> - ジョブは、プロモーションマネジメントツールからのみロールバックできます。ジョブをロールバックするためのコマンドラインはサポートされていません。
> - 多数のオブジェクトを使用する際は、`LCMCLI` スクリプトの `-Xmx=8g` パラメータを設定して最大 Java ヒープサイズを拡大することをお奨めします。

関連情報

LCMBIAR ファイルをライブ CMS へ [607 ページ]
ソースライブ CMS からターゲットライブ CMS [613 ページ]
ライブ CMS から LCMBIAR ファイル [610 ページ]
すべてのコマンドラインパラメータの一覧 [616 ページ]

16.6.3.1 昇格シナリオごとのコマンドラインパラメータ

コマンドラインパラメータは、各昇格シナリオの推奨順序で示されます。この表は、各昇格シナリオの使用可能なすべてのパラメータとそれらのステータス (必須またはオプション) を示しています。各必須パラメータについては、対応する昇格シナリオに対して説明します。オプションのパラメータについては、すべてのコマンドラインパラメータのセクションの一覧で説明します。シナリオごとのすべてのパラメータ情報および使用可能な追加パラメータについては、関連リンクを参照してください。

パラメータグループ	パラメータ	LCMBIAR からライブ	ライブから LCMBIAR	ライブからライブ	ロールバック
プロパティファイル	`lcmproperty`	オプション	推奨	推奨	推奨
アクションタイプ	`action`	必須 action=promote	必須 action=export	必須 action=promote	必須 action=rollback
LCM ノード	`LCM_CMS`	必須			
	`LCM_userName`	必須			
	`LCM_Password`	必須 空の場合、コンソールで必要になります。			

パラメータグループ	パラメータ	LCMBIAR からライブ	ライブから LCMBIAR	ライブからライブ	ロールバック
	LCM_authentication	オプション: デフォルト = secEnterprise			
	LCM_SystemID	SAP 認証の場合にのみ必須			
	LCM_ClientID	SAP 認証の場合にのみ必須			
ソース (ライブまたは *LCMBIAR*)	importLocation	必須	適用外	適用外	適用外
	lcmbiarpassword	必須 (空にすることができます)	適用外	適用外	適用外
	Source_CMS	適用外	必須	必須	適用外
	Source_UserName	適用外	必須	必須	適用外
	Source_password	適用外	必須 空の場合、コンソールで必要になります。	必須 空の場合、コンソールで必要になります。	適用外
	Source_authentication	適用外	オプション デフォルト = secEnterprise	オプション デフォルト = secEnterprise	適用外
	Source_systemID	適用外	SAP 認証の場合にのみ必須	SAP 認証の場合にのみ必須	適用外
	Source_clientID	適用外	SAP 認証の場合にのみ必須	SAP 認証の場合にのみ必須	適用外
出力先 (ライブまたは *LCMBIAR*)	Destination_CMS	必須	適用外	必須	適用外
	Destination_username	必須	適用外	必須	適用外
	Destination_password	必須	適用外	必須	適用外
	Destination_authentication	オプション デフォルト = secEnterprise	適用外	オプション デフォルト = secEnterprise	適用外
	Destination_systemID	SAP 認証の場合にのみ必須	適用外	SAP 認証の場合にのみ必須	適用外

パラメータグループ	パラメータ	LCMBIAR からライブ	ライブから LCMBIAR	ライブからライブ	ロールバック
	Destination_clientID	SAP 認証の場合にのみ必須	適用外	SAP 認証の場合にのみ必須	適用外
	ExportLocation	適用外	必須	適用外	適用外
	lcmbiarpassword	適用外	必須 (空にすることができます)	適用外	適用外
ジョブ関連	JOB_CUID	適用外	オプション	オプション	必須
	Override	オプション	適用外	適用外	適用外
	forceOverride SP4 で利用可能	オプション	適用外	適用外	適用外
	Timeout SP4 で利用可能	オプション	適用外	オプション	適用外
エクスポート関連	ExportDependencies	適用外	オプション デフォルト = False	オプション デフォルト = False	適用外
	ExportQuery	適用外	必須	必須	適用外
	ExportQueriesTotal	適用外	オプション: 複数のエクスポートクエリがある場合に使用	オプション: 複数のエクスポートクエリがある場合に使用	適用外
	BatchJobQuery	適用外	オプション: Exportquery とともに使用	オプション: Exportquery とともに使用	適用外
	LimitQueryBatchSize	適用外	オプション	オプション	適用外
ログ関連	Consolelog	オプション デフォルト = False	オプション デフォルト = False	オプション デフォルト = False	適用外
	ResultFileName	オプション	オプション	オプション	適用外
	LogFileName SP4 で利用可能	オプション	オプション	オプション	適用外
オブジェクト選択	Selected_CUIDS	オプション	適用外	適用外	適用外
	selectUser SP4 で利用可能	適用外	オプション デフォルト = All	オプション デフォルト = All	適用外

パラメータグループ	パラメータ	LCMBIAR からライブ	ライブから LCMBIAR	ライブからライブ	ロールバック
	selectGroup SP4 で利用可能	適用外	オプション デフォルト = All	オプション デフォルト = All	適用外
セキュリティ	IncludeApplicationSecurity	オプション デフォルト = False	オプション デフォルト = False	オプション デフォルト = False	適用外
	IncludeSecurity	オプション デフォルト = False	オプション デフォルト = False	オプション デフォルト = False	適用外
	IncludeTopLevelSecurity	オプション デフォルト = False	オプション デフォルト = False	オプション デフォルト = False	適用外
コメント	IncludeComments	オプション デフォルト = False	オプション デフォルト = False	オプション デフォルト = False	適用外
フェデレーションジョブ	IncludeFederationJobsRelationship	オプション デフォルト = True	適用外	オプション デフォルト = True	適用外

関連情報

LCMBIAR ファイルをライブ CMS へ [607 ページ]
ライブ CMS から LCMBIAR ファイル [610 ページ]
ソースライブ CMS からターゲットライブ CMS [613 ページ]
すべてのコマンドラインパラメータの一覧 [616 ページ]

16.6.3.2 LCMBIAR ファイルをライブ CMS へ

LCMBIAR ファイルのオブジェクトをライブ CMS に昇格させる場合、コマンドラインから、次のように昇格順序を指定するプロパティファイルを参照します。

- インポートロケーションおよび昇格アクションタイプ
- プロモーションマネジメントツール (以前のライフサイクル管理ツール LCM) をホストする CMS へのログイン認証情報。
- 出力先 CMS のログイン認証情報。
- CMS 昇格に必要なその他のパラメータ。LCMBIAR パスワードや必要に応じて既存のオブジェクトを上書きする設定などが例として挙げられます。

特定の昇格ニーズを指定できるその他のオプションのパラメータを含めることができます。これらのオプションのパラメータについては、すべてのコマンドラインパラメータの一覧 [616 ページ]を参照してください。

コマンドラインでプロパティファイルを使用せずに LCMBIAR ファイルをライブ CMS に昇格させる場合の例を次に示します。

```
Go to
C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI
4.0¥win64_x64¥scripts>
Type
lcm_cli.bat -action promote -LCM_CMS myCMS.mydomain.sap:6400 -LCM_userName
adminLCM -LCM_password my_adminpassword1 -
Destination_CMS myCMS.mydomain.sap:6400 -Destination_userName adminLCM
-Destination_password my_adminpassword1 -
importLocation "C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects
Enterprise XI 4.0¥Samples¥webi¥WebISamples.lcmbiar" -
lcmbiarpassword
```

コマンドラインでプロパティファイルを使用して LCMBIAR ファイルをライブ CMS に昇格させる場合の例を次に示します。

```
Go to
C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI
4.0¥win64_x64¥scripts>
Type
lcm_cli.bat -lcmproperty C:¥LCMTEST¥MyPropertyFile.properties
#
LCM command line property file
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
importLocation=C:¥Backup¥CR.lcmbiar
lcmbiarpassword=validlcmbiarpassword
#
Destination_CMS=myCMS.mydomain.sap:6400
Destination_userName=adminLCM
Destination_password=my_adminpassword1
#
```

次の表は、LCMBIAR ファイルをライブ CMS に昇格させるための適切なプロパティファイルに必要な、必須パラメータを示しています。

パラメータグループ	パラメータ	説明
アクションタイプ	`action`	CLI で実行する必要がある操作。 値: export 例: `action=export`
LCM ノード	`LCM_CMS`	プロモーションマネジメントツールの CMS。 値: 自由形式のテキスト。 例: `LCM_CMS=myCMS.mydomain.sap:6400`

パラメータグループ	パラメータ	説明
	LCM_userName	ツールがプロモーションマネジメントツール CMS への接続時に使用する必要のあるアカウントのユーザ名。 値: 自由形式のテキスト。 例: LCM_userName=adminLCM
	LCM_password	ユーザアカウントのパスワード。 値: 自由形式のテキスト。 例: LCM_password=my_adminpassword1
ソース: LCMBIAR ファイル	importLocation	昇格されるオブジェクトを含む LCMBIAR ファイルの場所。 値: 自由形式のテキスト。拡張子 <.lcmbiar> を付ける必要があります。 例: importLocation=C:¥Backup¥New.lcmbiar
	lcmbiarpassword	パスワードを使用して、BIAR ファイルの暗号化と解読が行えます。 値: 自由形式のテキスト。 例: lcmbiar=validlcmbiarpassword
出力先: ライブ CMS	Destination_CMS	ツールが接続する必要のある CMS。 値: 有効な CMS 名 例: Destination_CMS=myCMS.mydomain.sap:6400
	Destination_username	ツールが BI プラットフォーム CMS に接続する際に使用する必要のあるユーザアカウント。 値: 有効なユーザ名 例: Destination_username=adminLCM

パラメータグループ	パラメータ	説明
	Destination_password	ユーザアカウントの関連パスワード。 値: 有効なパスワード 例: Destination_password=my_adminpassword1

関連情報

ライブ CMS から LCMBIAR ファイル [610 ページ]
ソースライブ CMS からターゲットライブ CMS [613 ページ]
すべてのコマンドラインパラメータの一覧 [616 ページ]

16.6.3.3 ライブ CMS から LCMBIAR ファイル

ライブ CMS から LCMBIAR ファイルにオブジェクトを昇格する場合、コマンドラインから、以下のように昇格順序を指定するプロパティファイルを参照します。

- 昇格アクションタイプ: export
- プロモーションマネジメントツール (以前のライフサイクル管理ツール LCM) をホストする CMS へのログイン認証情報。
- ソース CMS のログイン認証情報。
- LCMBIAR ファイルの出力先ディレクトリ。
- CMS を正常に昇格させるために必要なその他のパラメータ。たとえば、LCMBIAR パスワードやセキュリティ設定。

特定の昇格ニーズを指定できるその他のオプションのパラメータを含めることができます。これらのオプションのパラメータについては、すべてのコマンドラインパラメータの一覧 [616 ページ]を参照してください。

以下の例は、ライブ CMS から LCMBIAR ファイルへの昇格の標準的なプロパティファイルを示しています。

```
Go to
C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI
4.0¥win64_x64¥scripts>
Type
lcm_cli.bat -lcmproperty C:¥LCMTEST¥MyPropertyFile.properties
#
#action=export
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
#
Source_CMS=myCMS.mydomain.sap:6400
Source_userName=adminLCM
Source_password=my_adminpassword1
```

```
#
exportLocation=E:¥LCMTEST¥
lcmbiarpassword=
#
#Queries
#
exportQuery1=SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID,
SI_OWNER, SI_PATH FROM
CI_INFOOBJECTS, CI_APPOBJECTS, CI_SYSTEMOBJECTS WHERE
DESCENDENTS("SI_NAME='Folder Hierarchy'","SI_ID in (23)")
#
#When applicable...
#
exportDependencies=true
includeSecurity=true
#
#Options
#
consolelog=true
```

次の表は、LCMBIAR ファイルをライブ CMS に昇格させるための適切なプロパティファイルに必要な、必須パラメータを示しています。

パラメータグループ	パラメータ	説明
アクションタイプ	`action`	CLI で実行する必要がある操作。 値: export 例: `action=export`
LCM ノード	`LCM_CMS`	プロモーションマネジメントツールの CMS。 値: 自由形式のテキスト。 例: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	ツールがプロモーションマネジメントツール CMS への接続時に使用する必要のあるアカウントのユーザ名。 値: 自由形式のテキスト。 例: `LCM_userName=adminLCM`
	`LCM_password`	ユーザアカウントのパスワード。 値: 自由形式のテキスト。 例: `LCM_password=my_adminpassword1`

パラメータグループ	パラメータ	説明
ソース: ライブ CMS	`Source_CMS`	プロモーションマネジメントツールが接続する必要のある CMS。 値: 自由形式のテキスト。 例: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_userName`	プロモーションマネジメントツールが BI プラットフォーム CMS に接続する際に使用する必要のあるユーザアカウント。 値: 自由形式のテキスト。 例: `Source_username=adminLCM`
	`Source_password`	ユーザアカウントのパスワード。 値: 自由形式のテキスト。 例: `Source_password=my_adminpassword1`
出力先: LCMBIAR ファイル	`exportLocation`	オブジェクトがエクスポートされてパッケージ化された後に LCMBIAR ファイルを配置する場所を指定します。 値: 自由形式のテキスト。拡張子 `<.lcmbiar>` を付ける必要があります。 例: `exportLocation=C:¥Backup¥New.lcmbiar`
	`lcmbiarpassword`	パスワードを使用して、BIAR ファイルの暗号化と解読が行えます。 値: 自由形式のテキスト。 例: `lcmbiarpassword=validlcmbiarpassword`

パラメータグループ	パラメータ	説明
エクスポート関連	`exportQuery`	ソース CMS をクエリして、LCMBIAR ファイルへのエクスポートに必要なオブジェクトを取得します。 値: 自由形式のテキスト。CMS クエリ言語形式を使用します。 例: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **注記** 1 つのプロパティファイルに任意の数のクエリを設定できますが、クエリには、exportQuery1、exportQuery2 と名前を付ける必要があります。

関連情報

LCMBIAR ファイルをライブ CMS へ [607 ページ]
ソースライブ CMS からターゲットライブ CMS [613 ページ]
すべてのコマンドラインパラメータの一覧 [616 ページ]

16.6.3.4 ソースライブ CMS からターゲットライブ CMS

ソースライブ CMS からターゲットライブ CMS にオブジェクトを昇格する場合、コマンドラインから、以下のように昇格順序を指定するプロパティファイルを参照します。

- 昇格アクションタイプ: 昇格
- プロモーションマネジメントツール (以前のライフサイクル管理ツール LCM) をホストする CMS へのログイン認証情報。
- ソース CMS のログイン認証情報。
- 出力先 CMS のログイン認証情報。
- CMS を正常に昇格させるために必要なその他のパラメータ。たとえば、セキュリティまたは依存関係のパラメータ。

特定の昇格ニーズを指定できるその他のオプションのパラメータを含めることができます。これらのオプションのパラメータについては、すべてのコマンドラインパラメータの一覧 [616 ページ]を参照してください。

以下の例は、ソース CMS からターゲット CMS への昇格の標準的なプロパティファイルを示しています。

```
#
action=promote
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
#
Source_CMS=myCMS1:myCMS2
Source_userName=adminLCM
Source_password=my_adminpassword1
Source_authentication=secEnterprise
#
Destination_CMS=myCMS1:myCMS2
Destination_userName=adminLCM
Destination_password=my_adminpassword1
Destination_authentication=secEnterprise
#
exportQuery1select*from CI_INFOOBJECTS where SI_NAME='Charting Samples' and
SI_KIND='Webi'
#
includeSecurity=false
#
exportDependencies=false
#
```

以下の表は、ソース CMS からターゲット CMS への昇格の正常なプロパティファイルに必要な、必須パラメータを示しています。

パラメータグループ	パラメータ	説明
アクションタイプ	`action`	コマンドラインで実行する必要がある操作。 値: promote 例: `action=promote`
LCM ノード	`LCM_CMS`	プロモーションマネジメントツールの CMS。 値: 自由形式のテキスト。 例: `LCM_CMS=myCMS.mydomain.sap:6400`
	`LCM_userName`	ツールがプロモーションマネジメントツール CMS への接続時に使用する必要のあるアカウントのユーザ名。 値: 自由形式のテキスト。 例: `LCM_userName=adminLCM`

パラメータグループ	パラメータ	説明
	LCM_password	ユーザアカウントのパスワード。 値: 自由形式のテキスト。 例: LCM_password=my_adminpassword1
ソース: Live CMS	source_CMS	プロモーションマネジメントツールが接続する必要のある CMS。 値: 自由形式のテキスト。 例: Source_CMS=myCMS.mydomain.sap:6400
	Source_username	プロモーションマネジメントツールが BI プラットフォーム CMS に接続する際に使用する必要のあるユーザアカウント。 値: 自由形式のテキスト。 例: Source_username=adminLCM
	Source_password	ユーザアカウントのパスワード。 値: 自由形式のテキスト。 例: Source_password=my_adminpassword1
出力先: Live CMS	Destination_CMS	ツールが接続する必要のある CMS。 値: 自由形式のテキスト。 例: Destination_CMS=myCMS1:myCMS2
	Destination_username	ツールが BI プラットフォーム CMS に接続する際に使用する必要のあるユーザアカウント。 値: 自由形式のテキスト。 例: Destination_username=adminLCM

パラメータグループ	パラメータ	説明
	`Destination_password`	ユーザアカウントの関連パスワード。 値: 自由形式のテキスト。 例: `Destination_password=my_adminpassword1`
エクスポート関連	`exportQuery`	ターゲット CMS へのエクスポートに必要なオブジェクトを取得するために LCM ツールが実行するクエリ。 値: 自由形式のテキスト。CMS クエリ言語形式を使用します。 例: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **注記** 1 つのプロパティファイルに任意の数のクエリを設定できますが、クエリには、exportQuery1、exportQuery2 と名前を付ける必要があります。

関連情報

LCMBIAR ファイルをライブ CMS へ [607 ページ]
ライブ CMS から LCMBIAR ファイル [610 ページ]
すべてのコマンドラインパラメータの一覧 [616 ページ]

16.6.3.5 すべてのコマンドラインパラメータの一覧

以下の表は、すべてのコマンドラインパラメータを示しています。

> **注記**
>
> コマンドラインで実行する場合、パラメータの構文は -<parameterName><space><parameterValue> です。プロパティファイルでは、パラメータの構文は <parameterName>=<parameterValue> です。

パラメータグループ	パラメータ	説明
プロパティファイル	lcmproperty	ファイルに保存されているコマンドの実行に必要な値を参照します。 値: プロパティファイルが保存されている場所の完全パス。 例: -lcmproperty C:¥MyPropertyFile.properties
アクションタイプ	action	CLI で実行する必要がある操作。 値: promote または export 例: action=promote
LCM ノード	LCM_CMS	プロモーションマネジメントツールの CMS。 値: 自由形式のテキスト。 例: LCM_CMS=myCMS.mydomain.sap:6400
	LCM_userName	ツールがプロモーションマネジメントツール CMS への接続時に使用する必要のあるアカウントのユーザ名。 値: 自由形式のテキスト。 例: LCM_userName=adminLCM
	LCM_Password	ユーザアカウントのパスワード。 空の場合、コンソールで必要になります。 値: 自由形式のテキスト。 例: LCM_password=my_adminpassword1
	LCM_authentication	使用される認証の種類を示します。 値: secEnterprise、secWinAD、secLDAP、secSAPR3。指定していない場合は、secEnterprise が使用されます。 例: LCM_authentication=secEnterprise
	LCM_systemID **注記** SAP 認証の場合は必須。	SAP 認証の場合にのみ必要です。 値: システム ID 例: LCM_systemID=systemID

パラメータグループ	パラメータ	説明
	`LCM_clientID` **注記** SAP 認証の場合は必須。	SAP 認証の場合にのみ必要です。 値: クライアント ID 例: `LCM_clientID=clientID`
ソース: LCMBIAR ファイル	`importLocation`	昇格されるオブジェクトを含む LCMBIAR ファイルの場所。 値: 自由形式のテキスト。拡張子 `<.lcmbiar>` を付ける必要があります。 例: `importLocation=C:¥Backup¥New.lcmbiar`
	`lcmbiarpassword`	パスワードを使用して、BIAR ファイルの暗号化と解読が行えます。 値: 自由形式のテキスト。 例: `lcmbiar=validlcmbiarpassword`
ソース: ライブ CMS	`Source_CMS`	プロモーションマネジメントツールが接続する必要のある CMS。 値: 自由形式のテキスト。 例: `Source_CMS=myCMS.mydomain.sap:6400`
	`Source_UserName`	プロモーションマネジメントツールが BI プラットフォーム CMS に接続する際に使用する必要のあるユーザアカウント。 値: 自由形式のテキスト。 例: `Source_username=adminLCM`
	`Source_password`	ユーザアカウントのパスワード。 値: 自由形式のテキスト。 例: `Source_password=my_adminpassword1`
	`Source_authentication`	使用される認証の種類を示します。 値: secEnterprise、secWinAD、secLDAP、secSAPR3。指定していない場合は、`secEnterprise` が使用されます。 例: `Source_authentication=secEnterprise`
	`Source_systemID` **注記** SAP 認証の場合は必須。	SAP 認証の場合にのみ必要です。 値: システム ID 例: `Source_systemID=systemID`

パラメータグループ	パラメータ	説明
	`Source_clientID` **注記** SAP 認証の場合は必須。	SAP 認証の場合にのみ必要です。 値: システム ID 例: `Source_clientID=clientID`
出力先: *LCMBIAR ファイル*	`exportLocation`	オブジェクトがエクスポートされてパッケージ化された後に LCMBIAR ファイルを配置する場所を指定します。 値: 自由形式のテキスト。拡張子 `<.lcmbiar>` を付ける必要があります。 例: `exportLocation=C:¥Backup¥New.lcmbiar`
	`lcmbiarpassword`	パスワードを使用して、BIAR ファイルの暗号化と解読が行えます。 値: 自由形式のテキスト。 例: `lcmbiarpassword=validlcmbiarpassword`
出力先: *ライブ CMS*	`Destination_CMS`	ツールが接続する必要のある CMS。 値: 有効な CMS 名 例: `Destination_CMS=myCMS.mydomain.sap:6400`
	`Destination_username`	ツールが BI プラットフォーム CMS に接続する際に使用する必要のあるユーザアカウント。 値: 有効なユーザ名 例: `Destination_username=adminLCM`
	`Destination_password`	ユーザアカウントの関連パスワード。 値: 有効なパスワード 例: `Destination_password=my_adminpassword1`
	`Destination_authentication`	使用される認証の種類を示します。 値: secEnterprise、secWinAD、secLDAP、secSAPR3。指定していない場合は、`secEnterprise` が使用されます。 例: `Destination_authentication=secEnterprise`

パラメータグループ	パラメータ	説明
	`Destination_systemID` **注記** SAP 認証の場合は必須。	SAP 認証の場合にのみ必要です。 値: システム ID 例: `Destination_systemID=systemID`
	`Destination_clientID` **注記** SAP 認証の場合は必須。	SAP 認証の場合にのみ必要です。 値: クライアント ID 例: `Destination_clientID=clientID`
ジョブ関連	`JOB_CUID`	ジョブ内のすべてのオブジェクトを LCMBIAR ファイルにエクスポートするようにツールに指示します。 値: 保存されたマネジメントジョブの CUID。
	`Override`	LCMBIAR ファイルからオブジェクトを選択的に昇格するために使用されます。 `true` の場合: ユーザは既存のジョブを上書きすることができます。 `false` の場合: ユーザは `<JOB_NAME>_<TIME_STAMP>` という名前の新しいジョブを作成することができます。 値: true または false 例: `Override=true`
	`forceOverride` SP4 で利用可能	同じ名前だが CUID が異なるジョブを上書きするために使用されます。 値: true または false 例: `forceOverride=true`
	`Timeout` SP4 で利用可能	昇格アクションのタイムアウトを設定します。 値: 時間 (秒) 例: `timeout=30`
エクスポート関連	`ExportDependencies`	ツールがエクスポート対象として収集するオブジェクト依存関係を指定します。`Source_CMS` フラグと一緒に使用する場合にのみ適用可能です。 値: true または false。指定しない場合、デフォルトの `false` が使用されます。 例: `ExportDependencies=false`

パラメータグループ	パラメータ	説明
	`ExportQuery`	ターゲット CMS へのエクスポートに必要なオブジェクトを取得するために LCM ツールが実行するクエリ。 値: 自由形式のテキスト。CMS クエリ言語形式を使用します。 例: `SELECT TOP 3000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE SI_NAME='Xtreme Employees' AND SI_KIND='Webi'` **注記** 1 つのプロパティファイルに任意の数のクエリを設定できますが、クエリには、exportQuery1、exportQuery2 と名前を付ける必要があります。

	`ExportQueriesTotal`	実行するエクスポートクエリの数を指定するために使用されます。x 個のエクスポートクエリがあり、それらをすべて実行する場合は、このパラメータ値に x を指定する必要があります。
		値: 正の整数。指定しない場合、デフォルトの 1 が使用されます。
		例: `ExportQuery1=<your sql statement>`
		`ExportQuery2=<your sql statement>`
		`ExportQueriesTotal=2`

パラメータグループ	パラメータ	説明
	`BatchJobQuery`	`ExportQuery` とともに使用します。ジョブクエリで返される行ごとにジョブを作成および開始します。ジョブエクスポートクエリでは、ジョブクエリで発生したプロパティを参照する "プレースホルダ" を使用することができます。プレースホルダの書式は $b:PPTY$ であり、プロパティ名は大文字と小文字が区別されません。有効な <PPTY>: - "cuid" - "name" - "id" プレースホルダが認識されないかジョブクエリで発生しない場合は、エラーが発生します。 値: 自由形式のテキスト。 例: `batchJobQuery=SELECT si_cuid,si_name FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'", "SI_ID in (23)") AND SI_KIND='Folder' AND SI_NAME LIKE '%sample%' and SI_PARENTID=0` `exportQuery1= SELECT TOP 10000 static, relationships, SI_PARENT_FOLDER_CUID, SI_OWNER, SI_PATH FROM CI_INFOOBJECTS,CI_APPOBJECTS,CI_SYSTEMOBJECTS WHERE DESCENDENTS("SI_NAME='Folder Hierarchy'" ,"SI_CUID='$b:CUID$'")`
	`LimitQueryBatchSize`	デフォルトでは、返されるオブジェクト数は 1,000 に制限されます。このパラメータが false に設定されている場合、すべてのクエリ実行済みオブジェクトが返されます。 **注記** また、`select TOP <number>` を使用して、クエリによって返されるオブジェクト数の新しい制限を明示的に設定することもできます。 値: true または false。指定しない場合、デフォルトの true が使用されます。 例: `LimitQueryBatchSize=true`

パラメータグループ	パラメータ	説明
ログ関連	`consolelog`	コマンドログ内のユーザが実行したコマンドの完全なログを表示するために使用されます。 値: true または false。指定しない場合、デフォルトの `false` が使用されます。 例: `consolelog=true`
	`ResultFileName`	パラメータ `consolelog` が使用された場合、ローカルファイルシステム上のファイルの名前。 値: ジョブ結果のファイルパス 例: `ResultFileName=C:¥Logs¥ResultFile.txt`
	`LogFileName` SP4 で利用可能	ユーザは、ログファイル用に使用する固定パスを指定することができます。 値: ログのファイルパス 例: `LogFileName=C:¥Logs¥LogFile.log`
オブジェクト選択	`Selected_CUIDS`	ユーザは、ファイル全体を昇格せずに、LCMBIAR ファイルのオブジェクト (レポート、ユーザ、ユニバースなど) をその依存関係とともに選択的に昇格することができます。 値: 選択的に昇格される lcmbiar ファイル内のオブジェクトの CUID
	`selectUser` SP4 で利用可能	サードパーティ認証 (LDAP、SAPR3、WindowsAD...) に基づいてユーザをフィルタリングします。 値: all、none、excludeTP、または onlyTP。指定しない場合、デフォルトの `all` が使用されます。 例: `selectUser=excludeTP`
	`selectGroup` SP4 で利用可能	サードパーティ認証 (LDAP、SAPR3、WindowsAD...) に基づいてユーザグループをフィルタリングします。 値: all、none、excludeTP、または onlyTP。指定しない場合、デフォルトの `all` が使用されます。 例: `selectGroup=onlyTP`
セキュリティ	`IncludeApplicationSecurity`	選択したアプリケーションに関連付けられたセキュリティをエクスポートまたはインポートするようにツールに指示します。 値: true または false。指定しない場合、デフォルトの `false` が使用されます。 例: `IncludeApplicationSecurity=true`

パラメータグループ	パラメータ	説明
	`IncludeSecurity`	選択したオブジェクトおよびユーザに関連付けられたセキュリティをエクスポートまたはインポートするようにツールに指示します。アクセスレベルが使用されている場合は、アクセスレベルもエクスポートまたはインポートされます。 値: true または false。指定しない場合、デフォルトの `false` が使用されます。 例: `IncludeSecurity=true`
コメント	`IncludeComments`	選択したオブジェクトに関連付けられたコメントをエクスポートまたはインポートするようにツールに指示します。 値: true または false。指定しない場合、デフォルトの `false` が使用されます。 例: `IncludeComments=true`
フェデレーションジョブ	`IncludeFederationJobsRelationship`	フェデレーションジョブの関係 (レプリケーション一覧およびリモート接続) を維持するようにツールに指示します。false に設定した場合、複製されたオブジェクトが通常のオブジェクトになり、フェデレーションフラグが削除されます。これは、複製されたオブジェクトが使用可能な唯一のオブジェクトであり、ソースオブジェクトがもう使用できなくなっている場合に役立つ可能性があります。 値: true または false。指定しない場合、デフォルトの `true` が使用されます。 例: `IncludeFederationJobsRelationship=false`

16.6.3.6 ロールバック

昇格されたジョブは、プロモーション管理ツールを使用して、出力先システムで元に戻すことができます。

プロモーション管理ツールを使用してジョブを昇格し (BI 4.2 SP07 を BI 4.3 に更新するなど)、後からこの変更を元に戻す場合は、昇格シナリオごとのコマンドラインパラメータ [604 ページ] で定義されたコマンドラインパラメータを使用して、ロールバック操作を実行できます。

ロールバック操作を実行する場合、以下のように昇格順序を指定するプロパティファイルを指定する必要があります。

- 昇格アクションタイプ: ロールバック
- プロモーション管理ツール (以前のライフサイクル管理ツール LCM) をホストする CMS へのログイン認証情報。
- ソース CMS のログイン認証情報。
- 出力先 CMS のログイン認証情報。

- CMS を正常に昇格させるために必要なその他のパラメータ。たとえば、セキュリティまたは依存関係のパラメータ。

特定の昇格ニーズを指定できるその他のオプションのパラメータを含めることができます。これらのオプションのパラメータについては、すべてのコマンドラインパラメータの一覧 [616 ページ]を参照してください。

以下のサンプルプロパティファイルを参照して、ロールバック操作を実行することができます。

```
#
action=rollback
job_cuid=AWWxyVk5fkFKjtQnRAygAYg
#
LCM_CMS=myCMS.mydomain.sap:6400
LCM_userName=adminLCM
LCM_password=my_adminpassword1
LCM_authentication=secEnterprise
```

> **注記**
>
> 昇格されたジョブの `job_cuid` は、*CMC ホーム* > プロモーション管理 > プロパティ にあります。

以下の表は、LCMBIAR ファイルからライブ CMS への昇格の正常なプロパティファイルに必要な、必須パラメータを示しています。

パラメータグループ	パラメータ	説明
アクションタイプ	`action`	CLI で実行する必要がある操作。 値: rollback 例: `action=rollback`
ジョブ関連	`job_cuid`	ジョブ内のすべてのオブジェクトを LCMBIAR ファイルにエクスポートするようにツールに指示します。 値: 保存されたマネジメントジョブの CUID。 例: `job_cuid=AWWxyVk5fkFKjtQnRAygAYg`
LCM ノード	`LCM_CMS`	プロモーションマネジメントツールの CMS。 値: 自由形式のテキスト。 例: `LCM_CMS=myCMS.mydomain.sap:6400`

パラメータグループ	パラメータ	説明
	LCM_userName	ツールがプロモーション管理ツール CMS への接続時に使用する必要のあるアカウントのユーザ名。 値: 自由形式のテキスト。 例: LCM_userName=adminLCM
	LCM_password	ユーザアカウントのパスワード。 値: 自由形式のテキスト。 例: LCM_password=my_adminpassword1
	LCM_authentication	ユーザアカウントの認証の種類。 値: 認証の種類。 例: secEnterprise

16.6.4 サンプルプロパティファイル

以下に、properties ファイルのサンプルを示します。

例

```
importLocation=C:/Backup/CR.lcmbiar
action=promote
LCM_CMS=<CMS 名:ポート番号>
LCM_userName=<ユーザ名>
LCM_password=<パスワード>
LCM_authentication=<認証>
LCM_systemID=<ID>
LCM_clientID=<クライアント ID>
Destination_CMS=<CMS 名:ポート番号>
Destination_userName=<ユーザ名>
Destination_password=<パスワード>
Destination_authentication=<認証>
```

```
Destination_systemID=<ID>

Destination_clientID=<クライアント ID>

lcmbiarpassword=<パスワード>
```

> ⓘ 注記
>
> properties ファイルに個人情報が含まれていない場合、LCM CLI にはコンソールの個人情報を求めるメッセージが表示されます。

16.7 拡張移送/修正システムの使用

移送/修正システム (CTS) は、ABAP ワークベンチで開発プロジェクトを整理、カスタマイズし、システムランドスケープで SAP システム間の変更を移送します。拡張移送/修正システム (CTS+) は、非 ABAP コンテンツを CTS+ 対応の非 ABAP リポジトリ全体にわたって昇格させる CTS のアドオンです。

BI プラットフォーム InfoObject では、データソースとして SAP Business Warehouse コンテンツを使用できます。CTS+ とプロモーションマネジメントツールを統合することで、SAP Business Warehouse (BW) リポジトリと同様に、SAP BI プラットフォームリポジトリを操作できます。これには、CTS 移送要求を使用してジョブを昇格します。CTS+ では、非 SAP オブジェクトをシステムランドスケープ内で移送することもできます。たとえば、開発システムで作成したオブジェクトを移送要求に添付して、ランドスケープ内の他のシステムに移送できます。

移送/修正システムの詳細については、Change and Transport System - Overview (BC-CTS)を参照してください。

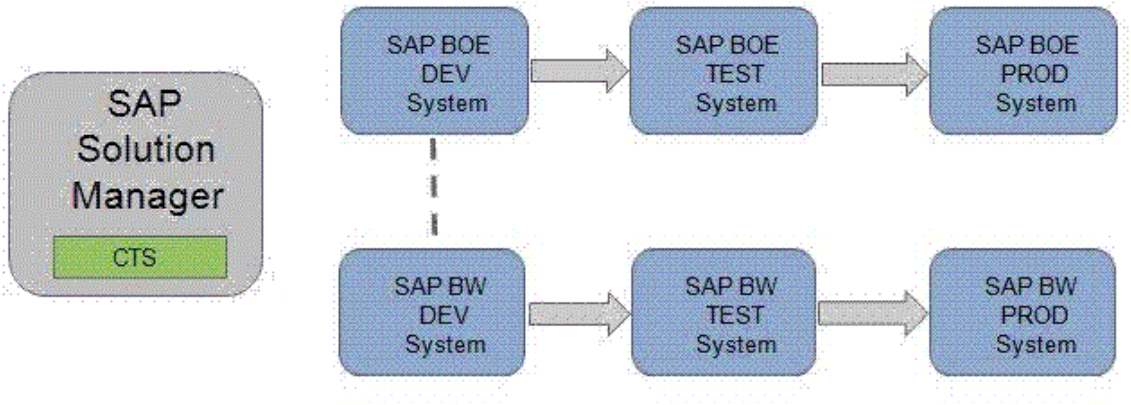
CTS+ および非 ABAP 移送の詳細については、Transporting Non-ABAP Objects in Change and Transport System を参照してください。

16.7.1 前提条件

システム間で CTS+ 経由でビジネスインテリジェンスコンテンツを転送するための前提条件は次のとおりです。

1. BI プラットフォーム 4.0 (以降) がインストールされていること。
2. SAP Solution Manager 7.1 または SAP Solution Manager 7.0 EHP1 (最低でも SP25) がインストールされており、CTS+ のドメインコントローラとして使用されていること (少なくとも SAP BusinessObjects システムの設定に使用されていること)。
   転送ドメインの設定の詳細については、転送ドメインの設定を参照してください。
3. CTS プラグインが SAP Solution Manager にインストールされていること (CTS プラグインは SL Toolset 1.0 SP02 から取得)。最新の利用可能な CTS プラグインを使用することをお勧めします。
   必要な CTS プラグインをインストールする方法については、1533059 を参照してください。
4. *SAP Business Warehouse 7.0* (SPS 24 以上) システムがインストールされていること。詳細については、1369301 を参照してください。
5. SAP Business Warehouse (SAP BW) 転送ランドスケープが、移送/修正システム (CTS) で設定されていること。
6. 1692417 および 1860594 が、CTS デプロイ Web サービスをホストするマシンに適用されていること。

16.7.2 BI プラットフォームと CTS+ との統合を設定する



移送/修正システムの一部である移送管理システム (TMS) は、ランドスケープ内の SAP システム間の変更を転送するのに使用されます。接続されている各種システム、それらのルート、およびそれらのシステムへのインポートを管理します。移送管理システムの詳細については、Transport Management System (BC-CTS-TMS)を参照してください。

CTS+ は、外部からのファイルコレクションと、転送ランドスケープ内でのそれらの配布を有効にします。CTS+ の一部である移送オーガナイザ Web UI は、移送要求とそれに含まれるオブジェクトを管理します。詳細については、Transport Management System (BC-CTS-TMS)を参照してください。

CTS 移送要求を使用して、BI プラットフォームプロモーションマネジメントを CTS+ および SAP BW に統合できます。

> ⓘ 注記
>
> BI プラットフォームと SAP Solution Manager との統合を有効にするには、SAP Solution Manager ランドスケープでアプリケーションの種類を「BOLM」に定義する必要があります。

次の手順を実行し、BI プラットフォームおよび CTS+ を統合します。

1. CTS エクスポート Web サービスを有効にします。
2. プロモーションマネジメントツールで CTS を設定します。
3. SAP Solution Manager で BI プラットフォームインポートシステムを設定します。

関連情報

CTS エクスポート Web サービスを有効にする [629 ページ]
プロモーションマネジメントツールで CTS+ を設定する [629 ページ]
BI プラットフォームと CTS+ との統合を設定する [628 ページ]

16.7.2.1 CTS エクスポート Web サービスを有効にする

BI プラットフォームを設定するには、SOA 管理用の Web ツールで CTS エクスポート Web サービスを有効にする必要があります。

1. アプリケーションを起動するには、SAP Solution Manager でトランザクションコード SOAMANAGER を入力します。
   必要な認証が完了すると、Web ブラウザに SOA 管理コンソールが表示されます。

   SAP Solution Manager 7.0 を使用する SOA の管理およびサービスのエンドポイントの設定に関する詳細については、Configuring a Service Provider を参照してください。 SAP Solution Manager 7.1 についても、Configuring a Service Provider を参照してください。
2. *Application and Scenario Communication* タブで、*Single Service Configuration* をクリックしてください。

   CTS エクスポート Web サービスに、`EXPORT_CTS_WS` と名前を付けます。
3. [*Configuration*] タブで、サービスのエンドポイントを作成または編集します。
4. [*Security*] タブで、転送プロトコルおよび認証方法を設定します。
5. [*Transport Settings* タブで、サービスのエンドポイントに簡単にアクセスできるようにするための代わりのアクセス URL を定義します。

16.7.2.2 プロモーションマネジメントツールで CTS+ を設定する

この節では、プロモーションマネジメントツールとともに使用する CTS+ を設定するため、CMC アプリケーションで実行する設定手順について説明します。

1. [昇格ジョブ] ページで [*CTS 設定*] をクリックし、次に [*BW システム*] をクリックします。
2. [*BW システム*] ページで [追加] をクリックし、BW システムをランドスケープに追加します。
3. [システムの追加] ページで、次の情報を入力します。
   - ホスト *BW SID*: ホスト SAP BW/ABAP マシンのシステム ID (SID) を指定します。
   - ホスト名: ホストマシンの IP アドレスを指定します。
   - システム番号: ホストシステムのシステム番号を入力します。
   - クライアント: クライアントマシンのシステム詳細を参照します。
   - ユーザおよびパスワード: これらのフィールドでは、クライアントマシンのユーザ名とパスワードを指定します。
   - 言語: このフィールドでは、選択する言語を指定します。
4. *OK* をクリックして、システムをランドスケープに追加します。

   > ⓘ 注記
   >
   > BW システムをランドスケープに追加したら、[*BW システム*] ページの [編集] または [削除] を使用して、ランドスケープのシステムを変更できます。

5. [昇格ジョブ] ページで [*CTS 設定*] をクリックし、次に [*Web サービス設定*] をクリックします。
6. [*Web サービス設定*] ページで、Web サービス URL およびユーザ詳細を入力します。

   > ⓘ 注記
   >
   > これらの詳細を把握していない場合は、Solution Manager 管理者に問い合わせます。

7. [保存] および [閉じる] をクリックして、Web サービス設定の追加を完了します。
8. BI プラットフォームプロモーションマネジメント CMS システムのマッピングファイルを作成します。

   BI プラットフォーム開発システムで以下の手順に従い、マッピングを有効化するための接続詳細を含むテキストファイルを作成します。

   a. BI プラットフォームプロモーションマネジメント CMS でルートディレクトリに移動し、パス `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/` に **`LCM`** という名前のフォルダを作成します。
   b. `LCM_SOURCE_CMS_SID_MAPPING.properties` という名前でテキストファイルを作成し、このファイルに次のうちいずれかを入力します。
      - `<ドメイン付き SAP BI プラットフォームソースシステムの完全名>@<CMS ポート番号> = <CTS 設定に使用するソースシステムの論理名 >`
      - `<SAP BI プラットフォームソースシステムの IP 番号>@<CMS ポート番号> = <CTS 設定に使用するソースシステムの論理名 >`

   例:

```
DEWDFTH04171S@6400=WJ3
10.208.112.177@6400=WJ3
DEWDFTH04171S.pgdev.sap.corp@6400=WJ3
```

> ⓘ 注記
>
> クラスタ環境の場合、`LCM_SOURCE_CMS_SID_MAPPING.properties` ファイルを、Adaptive Processing Server が実行中のシステムにコピーしてください。

非 ABAP システムでの設定手順の実行の詳細については、Making Transport Settings in the Application を参照してください。

16.7.2.3 SAP Solution Manager で BI プラットフォームインポートシステムを設定する

1. SAP Solution Manager システムにログオンします。
2. トランザクション `stms` と入力して、`Enter` キーを押します。
3. アプリケーションの種類として BOLM を設定します。
   a. 概要 > システム に移動します。
   b. 追加 > アプリケーションの種類 > 設定 に移動します。
   c. [新規エントリ] を選択します。
   d. [アプリケーションの種類] フィールドに、**`BOLM`** と入力します。
   e. 説明を入力します。
   f. サポートの詳細フィールドに、**`http://service.sap.com (ACH: BOJ-BIP-DEP)`** と入力します。
   g. テーブルビュー > 保存 を選択します。
   h. [はい] を選択して、プロンプトを確認します。
4. 別の言語を扱う場合、次の手順で翻訳されたテキストを管理できます。
   a. ジャンプ > 翻訳 を選択します。
   b. テキストを翻訳する言語を選択します。

c. [説明] および [サポートの詳細] フィールドに翻訳された値を入力します。
d. ダイアログボックスを確認します。
e. [続行] を選択します。
f. テーブルビュー > 保存 を選択します。
g. プロンプトを確認します。

これで、TMS ドメインが、CTS で Business Intelligence コンテンツの使用をサポートする準備ができました。

5. CTS+ で、BI プラットフォームソースシステムをエクスポートシステムとして定義します。

> **注記**
>
> ソースシステムとしての非 ABAP システムの作成の詳細については、Defining and Configuring Non-ABAP Systems を参照してください。

6. 次の手順を完了して、CTS+ で BI プラットフォームインポートシステムを設定します。

> **注記**
>
> BI プラットフォームインポートシステムへの参照として、SID を定義できます。

a. インポートシステムとして非 ABAP システムを作成します。
   詳細については、Defining and Configuring Non-ABAP Systems を参照してください。
b. デプロイメント方法にその他を指定し、他のすべてのオプションを選択解除します。
c. [保存] をクリックします。
d. [ディストリビューション] ダイアログボックスを確認します。
   インポートシステム設定を設定するテーブルビューが表示されます。
e. 編集 > 新規エントリ を選択します。
f. "表示 CTS の変更: アプリケーションの種類の処理のためのシステム詳細" 画面で、次の手順に従います。
   1. [デプロイ方法] フィールドで、[アプリケーション固有のデプロイヤ *(EJB)*] を選択します。
   2. デプロイ *URI* フィールドに次の情報を入力します。 **`http://<BOE web server name>:<Webserver port>/BOE/LCM/CTSServlet?&cmsName=<BOE destination name>:<CMSport>&authType=<BOE authentication type>`**
      パラメータ
      - "BOE web server name" は、BI プラットフォーム Web サーバが実行中のマシン名またはその IP アドレスです。
      - "Web server port" は、BI プラットフォーム Web サーバのポート番号です。
      - "BOE destination name" は、BI プラットフォーム Central Management Server (CMS) が実行中のマシン名です。
      - "CMS port" は、ターゲット CMS のポート番号です。
      - 「BOE authentication type」は、ビジネスインテリジェンスコンテンツをインポートするためのユーザ認証の種類です。 サポートされる認証の種類は、secEnterprise、secLDAP、secWinAD、および secSAPR3 です。
   3. ユーザフィールドに、BI プラットフォームのユーザ名を入力します。
   4. パスワードフィールドに、BI プラットフォームのパスワードを入力します。
   5. [保存] を選択して設定を保存します。

複数のインポートシステムが必要な場合は、上記の手順を繰り返し、必要なすべての出力先システムを作成します。 出力先システムの作成後に、ソースシステムとターゲットシステム間の転送ルートを設定するには、移送ルートの設定を参照してください。

16.7.2.4 SSL を用いて BI プラットフォームから CTS+ へエクスポートする

16.7.2.4.1 CTS+ に対して SSL を設定する

CTS+ に対して SSL を設定するには、アプリケーションサーバ ABAP 上で SSL を設定する必要があります。詳細については、Configuring the SAP Web AS for Supporting SSL を参照してください。

16.7.2.4.2 クライアント側の SSL 証明書を設定する

クライアント側の SSL 証明書を設定するには、サーバ証明書または信頼できる CA 証明書のいずれかを JVM キーストアにインポートします。

1. `cacerts` ファイルを `<INSTALLDIR>¥win64_x64¥sapjvm¥jre¥lib¥security` ディレクトリからバックアップします。
2. 次のパラメータを使用して、`BOE.war` ファイルをホストする Tomcat JVM に証明書をインポートします。

```
<INSTALLDIR>¥win64_x64¥sapjvm¥jre¥bin¥keytool.exe -import -file server.cer
-keystore cacerts
```

3. Tomcat を再起動します。

16.7.2.4.3 CTS+ エクスポート Web サービスを設定する

HTTPS が有効な CTS+ エクスポート Web サービス (`EXPORT_CTS_WS`) を設定するには、新しい HTTPS エンドポイントを作成します。

> ⓘ 注記
>
> または、既存の HTTP エンドポイントを HTTPS を使用するように切り替えることもできます。

1. トランザクションコード **`soamanager`** を使用して、*Provider Security* タブの *Communication Security* で、*SSL over HTTP (Transport Channel Security)*、*Transport Channel Authentication*、*User ID/Password* の順に選択します。
2. *Transport settings* タブの *Transport Binding* で、*Calculated Protocol* の *HTTPS* を選択します。

16.7.2.4.4 SSL 用のプロモーションマネジメントを設定する

> → 注意
>
> サーバ証明書または信頼できる CA 証明書を JVM キーストアにインポートします。

1. CMC で、プロモーションマネジメントタブの 設定 > *CTS 設定* > *Web サービス設定* をクリックします。
2. *Web サービス URL* パラメータに `https://` と上の手順で設定したポート番号が含まれていることを確認します。

> **注記**
>
> 指定した URL にアクセスできない場合は、上書きダイアログボックスのジョブの出力先リストに *CTS 経由の昇格*は表示されません。 プロモーションマネジメントと CTS+ 間の SSL ハンドシェイクが失敗した場合は、CMC ログファイルにエラーが記録されます。

16.7.2.5 SSL を用いて CTS+ から BI プラットフォームへエクスポートする

16.7.2.5.1 BI プラットフォーム Tomcat を設定して HTTPS を使用する

BI プラットフォーム Tomcat を設定して HTTPS を使用するには、BI プラットフォームがインストールされているマシンで次の手順を実行する必要があります。

1. サーバキーペア、証明書、およびキーストアを作成します。
   a. 次のパラメータを使用して、`<INSTALLDIR>¥win64_x64¥sapjvm¥jre¥bin¥keytool.exe` を実行します。

   ```
   keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore
   serverkeystore.jks -storetype JKS
   keytool -certreq -keyalg RSA -alias server -file server.csr -keystore
   serverkeystore.jks
   ```

   b. プロンプトが表示されたら、次の情報を入力します。
      - ユーザの名と姓
      - 部門
      - 組織の名前
      - 市町村または区域名
      - 都道府県または地域名
      - この部門の 2 桁の国コード

      書式設定された文字列が表示されます (`CN=John Smith, OU=Accounting, O=SAP, L=Vancouver, ST=BC, C=CA` など)。**Yes** と入力して Enter キーを押して、確認します。
2. サーバ証明書の要求を認証機関 (CA) に送信します。
3. 次のパラメータを使用して、署名済みサーバ証明書をサーバのキーストアにインポートします。

   ```
   keytool -import -alias server -keystore serverkeystore.jks -trustcacerts
   -file server.crt
   ```

4. HTTPS を有効にして作成したサーバのキーストアを使用するには、Tomcat 設定ファイル `server.xml` を設定します。
5. Tomcat を再起動し、ブラウザで次の URL にアクセスして接続をテストします。`https://<SERVERNAME>:<SSLPORTNUMBER>`

関連情報

CTS+ に対して SSL を設定する [632 ページ]

16.7.2.5.2 SSL に対して CTS+ を設定する

SSL に対して CTS+ を設定するには、SSL クライアント PSE を作成して、証明書をインポートする必要があります。

関連情報

CTS+ に対して SSL を設定する [632 ページ]

16.7.2.5.3 CTS+ のテストシステムおよび本稼働システムを更新して HTTPS を使用する

テストシステムおよび本稼働システムで HTTPS を有効にするには、次の手順に従います。

1. STMS トランザクションコードを使用します。
2. システムの概要をクリックします。
3. テストシステムまたは本稼働システムを選択して、ジャンプ > アプリケーションの種類 > デプロイメント方法 をクリックします。
4. デプロイ *URI* パラメータに `https://` と設定した HTTPS ポート番号が含まれていることを確認します。

16.7.3 CTS を使用してジョブを昇格する

この節では、プロモーションマネジメントツールでサポートされている、BI プラットフォーム Central Management Server (CMS) オブジェクトを、移送/修正システムを使用してソースシステムから出力先システムに昇格するワークフローについて説明します。 CTS を使用してジョブを昇格するには、次の手順を完了します。

1. SAP 認証を使用してプロモーションマネジメントツールを起動し、ジョブを作成します。

   新しいジョブの作成の詳細については、以下の関連リンクの「ジョブの作成」を参照してください。

   > **注記**
   >
   > ソースシステムのログイン画面で、認証の種類として「SAP」を選択してください。

2. 出力先ドロップダウンリストから、*CTS 経由の昇格*オプションを選択します。

3. [作成] をクリックします。
   [システムからオブジェクトを追加] 画面が表示されます。 ツリー構造でフォルダとサブフォルダが表示されます。
4. InfoObject を選択するフォルダに移動します。
5. ジョブに追加する InfoObject を選択し、追加をクリックします。 InfoObject を追加する場合は、オブジェクトの追加画面を終了して、追加して閉じるをクリックします。
   ジョブに InfoObject が追加され、[昇格ジョブ] 画面が表示されます。

   > ⓘ 注記
   >
   > [昇格ジョブ] 画面で、次のことを実行できます。
   > - [オブジェクトの追加] オプションを使用して、ジョブに InfoObject を追加する。 詳細については、「ジョブへの InfoObject の追加」を参照してください。
   > - [依存関係の管理] オプションを使用して、選択した InfoObject の依存関係を管理する。 オブジェクトの SAP BW の依存関係が UI に表示され、ユーザが選択できます。
   > 詳細については、ジョブの依存関係の管理に関するトピックを参照してください。

6. [昇格] をクリックします。
   [昇格] 画面に、ID、所有者、およびデフォルト移送要求の現在の設定に関する簡単な説明が表示されます。
7. [移送要求] ハイパーリンクを使用して、次のことを実行できます。
   - 移送要求の詳細を表示する。
   - デフォルトの移送要求の設定を変更する。
   - 別の移送要求を選択する。
   - 移送要求を作成する。

   1. [移送要求] ハイパーリンクをクリックして、[移送オーガナイザ] Web ユーザインタフェースを開きます。
   2. ログオン認証情報を要求された場合は、有効な CTS ドメインコントローラシステムのユーザ認証情報を使用してログオンします。
   3. [昇格] 画面を最新表示して、更新内容を表示します。

   移送オーガナイザ Web UI の使用の詳細については、Transport Organizer Web UI を参照してください。
8. SAP BW オブジェクトの依存関係の詳細を表示するには、[第 2 レベルの依存オブジェクト] ハイパーリンクをクリックします。

   > ⓘ 注記
   >
   > [第 2 レベルの依存オブジェクト] ハイパーリンクをクリックすると、要求内にロックされているオブジェクトだけが表示されます。 要求がリリース済みの場合は、いずれの依存関係も表示されません。 また、アクティブな第 2 レベルの依存関係がない場合、このハイパーリンクは灰色で表示されます。

9. 昇格をクリックします。
10. ジョブを閉じます。
    プロモーションマネジメントのメイン画面が表示されます。 作成したジョブのステータスは、[*CTS+ にエクスポートしました*] となります。
11. 次の手順を完了して、出力先システムに BI プラットフォームオブジェクトをリリースします。
    a. 昇格するジョブの [ステータス] 列に表示されているリンクをクリックします。
       [昇格のステータス] ウィンドウが表示されます。
    b. [リクエストのステータス] をクリックします。
       [移送オーガナイザ] Web UI が表示されます。
    c. リクエストのステータスが [変更可能] の場合、[リリース] をクリックして BI プラットフォームオブジェクトの移送要求をリリースします。 非 ABAP オブジェクトを含む移送要求のリリースの詳細については、Releasing Transport Requests with Non-ABAP Objects を参照してください。
    d. [移送オーガナイザ] Web UI を閉じます。
12. SAP BW オブジェクトの依存関係を表示するには、[*BW 依存オブジェクトの一覧*] ハイパーリンクをクリックします。

    > **注記**
    >
    > SAP BW 依存関係の更新やこれらのリリースは SAP BW チームによって操作されるため、これらのオブジェクトにアクセスするときには、このチームに確認することをお勧めします。

13. [昇格のステータス] ウィンドウを閉じます。
14. 次の手順を完了して、出力先システムに BI プラットフォームオブジェクトをインポートします。
    a. CTS+ ドメインコントローラにログオンします。
    b. 移送管理システムに入るには、**STMS** トランザクションを呼び出します。
    c. [インポートの概要] アイコンをクリックします。
       [インポートの概要] 画面が表示され、すべてのシステムから、インポートキューのアイテムを見ることができます。
    d. 出力先プロモーションマネジメントシステムのシステム ID を選択します。
       システムにインポートできる移送要求の一覧を確認できます。
    e. [最新表示] をクリックします。
    f. 関連する移送要求をインポートします。 詳細については、依頼のインポートを参照してください。

       BOLM コンテンツを含む移送要求のインポートに関する概要については、Importing Transport Requests with Non-ABAP Objects を参照してください。
15. 選択したオブジェクトに SAP BW 依存関係が含まれる場合、次の手順を実行します。
    a. 次の手順を完了して、出力先システムに SAP BW 依存関係をリリースします。
       1. SAP BW ソースシステムにログオンします。
       2. SE09 トランザクションを呼び出します。 [移送オーガナイザ] 画面が表示されます。
       3. [表示] をクリックします。SAP BW 要求が表示されます。
       4. SAP BW 要求をクリックして展開し、依存関係に作成されたタスクを表示します。
       5. 一次 SAP BW オブジェクトに関連付けられた要求を右クリックして、[直接リリースする] を選択します。 この手順を繰り返して、各依存オブジェクトに関連付けられているすべてのタスクを個別にリリースします。
       6. 一次 BW オブジェクトに関連付けられた要求を右クリックして、[直接リリースする] を選択します。
       7. すべての要求がリリースされるまで、画面を最新表示します。

> **注記**
>
> 要求のログをダブルクリックすると表示できます。

b. 次の手順を完了して、出力先システムに SAP BW 依存関係をインポートします。
   1. SAP BW 出力先システムにログオンします。
   2. 移送管理システムに入るには、STMS トランザクションを呼び出します。
   3. [インポートの概要] アイコンをクリックします。 [インポートの概要] 画面が表示されます。
   4. SAP BW 出力先のシステム ID をダブルクリックします。 システムにインポートできる移送要求の一覧を確認できます。
   5. 関連する移送要求をインポートします。 詳細については、依頼のインポートを参照してください。インポートキューを含む転送の詳細については、インポートキューによる移送を参照してください。

16. 出力先システムにログオンして、昇格したジョブのステータスを表示します。

Generic CTS の詳細については、Configuring Target Systems for Further Applications を参照してください。

関連情報

ジョブを作成する [578 ページ]
ジョブの依存関係を管理する [583 ページ]

16.8 プロモーション管理ウィザードの使用

プロモーション管理ウィザードを使用すると、ビジネスインテリジェンス (BI) リソースを数回のクリックで 1 つのリポジトリから別のリポジトリに簡単にコピーすることができます。

プロモーション管理ウィザードでは、以下の昇格シナリオがサポートされます。

- ソースシステムから LCMBIAR ファイルに BI リソースをエクスポートします。
- ソースシステムから出力先システムに BI リソースを複製します。
- 出力先システムに LCMBIAR ファイルをインポートします。

プロモーション管理ウィザードにより、コマンドラインを使用せずにリポジトリのコンテンツ全体またはリポジトリの選択的コンテンツを昇格できるようになりました。プロモーション管理ウィザードの使いやすいグラフィカルインタフェースによって、管理者の作業が容易になります。

プロモーション管理ウィザードのベストプラクティスに関する詳細については、SAP ノート 2531264 を参照してください。

> **警告**
>
> プロモーション管理ウィザードではロールバックはサポートされていません。つまり、BI リソースの昇格後に出力先システムを前の状態に戻すことはできません。

> ⓘ 注記
>
> オブジェクトの昇格を開始する前に、メモリの値を必ず確認してください。Xms の値は Xmx の値以下である必要があります。

> ⓘ 注記
>
> QaaWs オブジェクトがある場合は、出力先システムを適切に設定する必要があります。

> → ヒント
>
> パフォーマンスを向上させるには、出力先システムの CMC で監査および監視を無効にします。詳細については、『Bsiness Intelligence プラットフォーム管理者ガイド』の「監査」を参照してください。

16.8.1 昇格からオブジェクトを除外する

以下の一覧からオブジェクトを選択して昇格ジョブから除外し、ディスク領域を確保して、移行時間を短縮することができます。

昇格ジョブにより、すべての BI 資産が、ソースシステムから出力先システムに移行されます。その結果、ソースシステムに固有であり、出力先システムで有用でない資産も移行されます。BI 資産を昇格から除外するには、以下の手順に従います。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64` に移動します。
2. テキストエディタで *PromotionManagementWizard.ini* を開きます。
3. 文字列 # 全体エクスポートまたは選択的エクスポートから自動的に除外する種類の一覧を検索して見つけます。
   この文字列の下に、コード `-Dcom.sap.businessobjects.pmw.exclude.kind={}` があります。
4. 以下のオブジェクトの一覧を参照して、除外するオブジェクトを `{}` の間に追加します。
5. ファイルを保存します。

昇格ジョブを実行すると、コードに記載したオブジェクトが除外されます。

昇格ジョブから除外できるオブジェクトの一覧については、以下の表を参照してください。

CustomMapped 属性	DFS.Parameter	ディスカッション	GDPR オブジェクト
LCM ジョブ	LCM 上書き	LCM スキャン履歴	LCM 設定
LANDSCAPE	LANDSCAPE 接続	Live Office	MoN.MBEAN 設定
MON.ManagedEntity ステータス	MON.MonAppDataStore	Mon.Probe	Mon.Subscription
NotificationScheduleObject	上書きエントリ	PlatformSearchApplication ステータス	PlatformSearchContentExtractor
PlatformSearchContentStore	PlatformSearchIndexEngine	PlatformSearchQueue	PlatformSearchScheduling
PlatformSearchSearchAgent	PlatformSearchServiceSession	TaskTemplate	VisualDifferenceComprator

XL.XcelsiusApllication	busobjectreporter	Explorer	Lumira 拡張

16.8.2 プロモーション管理ウィザードを使用する場合

プロモーション管理を使用する際には、複数のオプションが使用可能です。この表は、プロモーション管理ウィザードがニーズに最適なソリューションであるかどうかを判断する際に役立ちます。

プロモーション管理のさまざまなオプション

	プロモーション管理ウィザード	コマンドラインオプションを使用したプロモーション管理	セントラル管理コンソールでのプロモーション管理
目的	1 回限りの昇格	自動化	プロジェクト
昇格の対象範囲	多数の BI リソース	多数の BI リソース	少数の BI リソース
ジョブ	ジョブサーバによって返される可能性のあるジョブは作成不可	ジョブサーバによって実行されるジョブの作成が可能	ジョブサーバによって実行されるジョブの作成が可能

> ⓘ 注記
>
> LCMBIAR ファイルは、選択したプロモーション管理オプションに関係なく、各プロモーション管理オプションと互換性があります。

16.8.2.1 プロモーション管理設定の定義

1. 必要なプロモーション管理設定を指定します。指定に役立つ情報を以下に示します。

設定	説明
一時フォルダ	ⓘ 注記 [一時フォルダ] に必ず十分な空き領域を割り当ててください。空き領域の容量は、必要な領域の容量の 2 倍以上である必要があります。
ログの場所	ログの場所はデフォルトで定義されています。後でログの場所を変更することができます。プロモーション管理設定の変更はすぐに反映されます。
ログレベル	[ログレベル] は以下のレベルに設定することができます。 • デフォルト • 低 • 中

設定	説明
	• 高 変更しない限り、[ログレベル] は [デフォルト] に設定されます。
言語	プロモーション管理ウィザードの言語を希望の言語に設定することができます。

2. [次へ] をクリックします。

16.8.3 シナリオ

プロモーション管理ウィザードでは、3 種類の昇格シナリオがサポートされます。

- ライブシステムから LCMBIAR: ライブ CMS から LCMBIAR ファイルにオブジェクトをコピーします。
- ライブ CMS からライブへの昇格: ライブ CMS ソースシステムからライブ CMS 出力先システムにオブジェクトをコピーします。
- LCMBIAR からライブシステム: LCMBIAR ファイルからライブ CMS 出力先システムにオブジェクトをインポートします。

16.8.3.1 ライブ CMS ソースシステムから LCMBIAR ファイルへのオブジェクトの昇格

ライブ CMS から LCMBIAR ファイルにオブジェクトを昇格するには、以下の手順に従います。

1. [エクスポート] を選択します。
2. ソース CMS を定義するには、以下のいずれかを実行します。
   - セントラル CMS をソース CMS として使用するには、[セントラル *CMS* をソース *CMS* にする] チェックボックスをオンにします。
   - [ソース] セクションで、以下の情報を入力します。
     - CMS 名
     - ユーザ
     - パスワード
     - 認証
3. [出力先] フィールドで [選択] をクリックし、LCMBIAR ファイルの場所を選択します。
4. (オプション) LCMBIAR ファイルを暗号化するためのパスワードを入力します。

   > ⓘ 注記
   > LCMBIAR ファイルを暗号化した場合、昇格処理にかかる時間が長くなります。

5. [次へ] をクリックし、エクスポートするオブジェクトを選択します。

16.8.3.2 ライブ CMS ソースシステムからライブ CMS 出力先システムへのオブジェクトの昇格

ライブ CMS ソースシステムからライブ CMS 出力先システムにオブジェクトを昇格するには、以下の手順に従います。

1. [昇格] を選択します。
2. ソース CMS を定義するには、以下のいずれかを実行します。
   - セントラル CMS をソース CMS として使用するには、[セントラル *CMS* をソース *CMS* にする] チェックボックスをオンにします。
   - [ソース] セクションで、以下の情報を入力します。
     - CMS 名
     - ユーザ
     - パスワード
     - 認証
3. 出力先 CMS を定義するには、以下のいずれかを実行します。
   - セントラル CMS を出力先 CMS として使用するには、[セントラル *CMS* を出力先 *CMS* にする] チェックボックスをオンにします。
   - [出力先] セクションで、以下の情報を入力します。
     - CMS 名
     - ユーザ
     - パスワード
     - 認証
4. [次へ] をクリックし、ソースシステムから出力先システムにコピーするオブジェクトを選択します。

16.8.3.3 LCMBIAR ファイルからライブ CMS 出力先システムへのオブジェクトの昇格

LCMBIAR ファイルからライブ CMS にオブジェクトを昇格するには、以下の手順に従います。

1. [インポート] を選択します。
2. 出力先 CMS を定義するには、以下のいずれかを実行します。
   - [出力先] セクションで、[セントラル *CMS* を出力先 *CMS* にする] チェックボックスをオンにします。
   - [出力先] セクションで、以下の情報を入力します。
     - CMS 名
     - ユーザ
     - パスワード
     - 認証
3. [ソース] セクションで、[選択] をクリックし、インポートする LCMBIAR ファイルを選択します。
4. (オプション) LCMBIAR ファイルを暗号化するためのパスワードを入力します。

> ⓘ 注記
>
> LCMBIAR ファイルを暗号化した場合、昇格処理にかかる時間が長くなります。

5. [次へ] をクリックし、インポートするオブジェクトを選択します。

16.8.4 オブジェクト

プロモーション管理ウィザードでは、2 種類のコンテンツの昇格がサポートされます。

- コンテンツ全体の昇格
- 選択的コンテンツ昇格

それぞれの説明を以下の表に示します。

コンテンツの昇格の種類	昇格されるコンテンツ	コンテンツの依存関係
コンテンツ全体の昇格	ソースシステムから出力先システムに、以下のすべてのコンテンツを昇格します。 • オブジェクト (ユーザ、ドキュメント、ユニバース、接続など) • インスタンス • オブジェクト間の関係 • オブジェクトセキュリティ	すべての関係が保持されるため、依存関係の評価は不要です。現在のオブジェクトステップから概要ステップに直接移動します。
選択的コンテンツ昇格	ソースシステムから出力先システムに、選択したコンテンツを昇格します。選択できるコンテンツは以下のとおりです。 • オブジェクト (ユーザ、ドキュメント、ユニバース、接続など) • インスタンス • オブジェクト間の関係 • オブジェクトセキュリティ	ソースシステムから出力先システムにすべてのコンテンツを昇格するわけではないため、依存関係の評価が必要です。

16.8.4.1 コンテンツ全体の昇格

ソースシステムから出力先システムにコンテンツ全体を昇格するには、以下の手順に従います。

1. [フルコンテンツ昇格] を選択します。

   すべてのオブジェクトが昇格用に選択されます。
2. [次へ] をクリックし、選択したコンテンツを確認します。

16.8.4.2 選択的コンテンツの昇格について

ソースシステムから出力先システムに選択的コンテンツを昇格する前に、エクスポートオプションを定義する必要があります。エクスポートオプションを定義すると、ソースシステムに指定されている設定のうち、出力先システムに昇格する設定を取得できるようになります。

16.8.4.2.1 エクスポートオプションについて

ソースシステムに指定されている設定を取得して、それを出力先システムに昇格する場合は、エクスポートオプションで以下のパラメータを定義する必要があります。

- オブジェクトインスタンス
- オブジェクトの依存関係
- セキュリティ
- Commentary
- フェデレーションジョブ
- 競合する名前の解決

オブジェクトインスタンス

オブジェクトインスタンス	説明
オブジェクトが選択された場合、そのオブジェクトのすべてのインスタンスをエクスポートする	選択したオブジェクトと、そのすべてのインスタンスをエクスポートします。
オブジェクトが選択された場合、そのオブジェクトの定期的なインスタンスのみをエクスポートする	選択したオブジェクトと、その定期的なインスタンスのみをエクスポートします。 たとえば、ドキュメントの週次および月次の最新表示をスケジュールしている場合、このドキュメントとその 2 つの定期的なインスタンスがエクスポート時にエクスポートされます。
オブジェクトインスタンスをエクスポートしない	選択したオブジェクトのみをエクスポートします。そのインスタンスはエクスポートされません。

オブジェクトの依存関係

オブジェクトの依存関係	説明
オブジェクトの選択時に依存関係を含む	選択したオブジェクトと、そのすべての依存関係をエクスポートします。 **注記** このオプションはデフォルトでチェックされています。

オブジェクトの依存関係	説明
オブジェクトの選択時に依存関係を除外する	選択したオブジェクトのみをエクスポートし、その依存関係はエクスポートしません。

セキュリティ

セキュリティ	説明
オブジェクトセキュリティを含める	選択したオブジェクトと、そのオブジェクトセキュリティ設定をエクスポートします。
ユーザセキュリティを含める	選択したオブジェクトと、そのユーザセキュリティ設定をエクスポートします。
アプリケーションセキュリティを含める	選択したオブジェクトと、そのアプリケーションセキュリティ設定をエクスポートします。
最上位セキュリティを含める	ルートフォルダに定義されているセキュリティ設定をエクスポートします。 **⚠ 警告** このオプションは、出力先システムに定義されているセキュリティ設定を上書きします。このオプションは慎重に使用する必要があります。

Commentary

Commentary	説明
コメントを含める	選択したオブジェクトと、そのすべてのコメントをエクスポートします。
ユーザグループの BI ラウンチパッドの基本設定	このチェックボックスを選択すると、ソースシステムの BI ラウンチパッドのユーザグループの基本設定が、出力先システムで設定されます。

ユーザグループ BI 基本設定

ユーザグループ BI 基本設定	説明
ユーザグループ BI 基本設定の上書き	このチェックボックスを選択すると、ソースシステムの BI ラウンチパッドのユーザグループの基本設定が、出力先システムで設定されます。 **注記** BIAR ファイルを使用してカスタマイズを使用する Web Intelligence ドキュメントを昇格する場合は、このオプションを有効にしてカスタマイズをインポートしてください。

フェデレーションジョブ

フェデレーションジョブ	説明
フェデレーションジョブ関係を含める	選択したオブジェクトと、そのフェデレーションジョブの保持されている関係をインポートします。

競合する名前の解決

競合する名前の解決	説明
競合する名前の解決	選択したオブジェクトが出力先システムのオブジェクトと同じ名前で CUID が異なる場合、選択したオブジェクトのコピーが出力先システムに作成されます。 このオプションを有効化しなかった場合、出力先システムのオブジェクトと同じ名前で CUID が異なる選択済みオブジェクトは、出力先システムにコピーされません。

16.8.4.2.2 選択的コンテンツの昇格

ソースシステムから出力先システムに選択的コンテンツを昇格するには、以下の手順に従います。

1. [選択的コンテンツ昇格] を選択します。
2. [エクスポートオプション] を定義するには、[オプション] をクリックします。
3. (オプション) 日時範囲に応じてオブジェクトをフィルタする場合は、[時間フィルタの適用] をオンにします。
4. エクスポートするオブジェクトを選択します。
5. オブジェクトの依存関係を評価するには、依存関係のアイコンの下にある関連するチェックボックスをオンにします。

   注記

   デフォルトでは、依存関係のボックスはすべてオンになっています。オブジェクトの依存関係を評価しない場合は、このボックスをオフにします。

6. [次へ] をクリックし、依存関係を評価します。

16.8.5 依存関係

選択的コンテンツをソースシステムから出力先システムに昇格する場合、選択的コンテンツの依存関係を評価することができます。[依存項目] ステップでは、依存関係として識別された選択オブジェクトの概要が提供されます。

選択オブジェクトの依存関係に関する以下の情報を表示することができます。

- タイトル
- CUID
- 日付

依存関係として識別されたオブジェクトを選択することができます。

1. 表示する詳細のレベルに応じて、以下のいずれかを実行します。
   - 各依存関係の詳細を表示するには、[すべて展開] をクリックします。
   - 依存オブジェクトのみを表示するには、[すべて折りたたむ] をクリックします。
2. 昇格する依存関係を選択します。

   > ⓘ 注記
   >
   > デフォルトでは、依存関係のボックスはすべてオンになっています。オブジェクトの依存関係を昇格しない場合は、このボックスをオフにします。

3. [次へ] をクリックし、昇格のために選択したオブジェクトを確認します。

16.8.6 概要

昇格を実行する前に、昇格用に選択したオブジェクトを確認する必要があります。

各オブジェクトについて以下の情報を表示することができます。

- タイトル
- CUID
- 日付

> ⚠ 警告
>
> コピーするすべてのオブジェクトが含まれていることを確認します。これは、昇格が開始した後で昇格処理をキャンセルすることができないためです。プロモーション管理ウィザードではロールバックはサポートされていません。

以下のようにオブジェクトを確認することができます。

1. 確認する詳細のレベルに応じて、以下のいずれかを実行します。

- 各オブジェクトの詳細を表示するには、[展開] をクリックします。
- 各オブジェクトの親を表示するには、[折りたたむ] をクリックします。

> ⓘ 注記
>
> [展開] を選択したか [折りたたむ] を選択したかに応じて、昇格結果の CSV ファイルに含まれる詳細のレベルが異なります。

2. 昇格に十分な領域がハードドライブにあることを確認するには、[必要な最小一時領域] を確認します。
3. [開始] をクリックし、オブジェクトを昇格します。

   昇格を開始した後でこの処理をキャンセルすることはできません。

16.8.7 (オプション) プロパティファイル

プロモーション管理ウィザードのプロパティファイルに、以下のパラメータを設定することができます。

- SSL 設定
- パラメータ

プロモーション管理ウィザードのプロパティファイルは、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥PromotionManagementWizard` にあります。

16.8.7.1 SSL 設定の指定

SSL を使用する場合、プロモーション管理ウィザードの SSL 設定を以下の場所で定義する必要があります。

`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥PromotionManagementWizard`

1. テキストエディタで `PromotionManagementWizard.ini` を開きます。
2. SSL モードを有効化するには、"-D" で始まる行のコメントを解除します。
3. 各設定の値を入力します。

設定	値
`-Dbusinessobjects.orb.oci.protocol`	値: ssl ⓘ 注記 この値を入力すると、SSL 通信が有効になります。
`-DcertDir`	鍵と証明書の場所
`-DtrustedCert`	信用できる証明書ファイルの名前

設定	値
	注記 複数のファイルを指定する場合は、各ファイルをセミコロンで区切ります (例: fileA; fileB)。
`-DsslCert`	SDK 証明書
`-DsslKey`	SDK 証明書の秘密鍵
`-Dpassphrase`	秘密鍵のパスフレーズを含むファイルの場所
`-Dpsecert`	PSE 証明書ファイル

警告

これ以外の設定や値は、追加または編集しないでください。

4. `PromotionManagementWizard.ini` を保存します。

例: `PromotionManagementWizard.ini` の SSL 設定

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/SSL
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dpsecert=temp.pse
```

16.8.7.2 パラメータの設定

ニーズに応じて、以下の場所にあるプロモーション管理ウィザードのプロパティファイルでオプションを設定することができます。

`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥PromotionManagementWizard`

1. テキストエディタで `PromotionManagementWizard.ini` を開きます。
2. オプションを有効化するには、"-D" で始まる行のコメントを解除します。
3. 各パラメータの値を入力します。

パラメータ	値
`-Dbusinessobjects.connectivity.directory`	接続サーバディレクトリの場所。
`-Dcom.businessobjects.mds.cs.ImplementationID`	`csEX` **注記** この値は変更しないでください。
`-Xms8g`	デフォルトでは、メモリの値は 8 GB に設定されます。 Xms の値は Xmx の値以下である必要があります。
`-Xmx10g`	デフォルトでは、メモリの値は 10 GB に設定されます。 10 GB のメモリは、65 000 オブジェクトのリポジトリに十分な値です。
`-Dbobj.biar.suggestSplit=512`	デフォルト値 (推奨) パラメータ `-Dbobj.biar.suggestSplit` を使用することをお奨めします。 ライブ CMS から LCMBIAR ファイルに昇格する場合、この設定より LCMBIAR ファイルを複数の LCMBIAR ファイルに分割することができます。
`-Dbobj.biar.forceSplit=768`	デフォルト値 (推奨) パラメータ `-Dbobj.biar.suggestSplit` を適用できない場合、パラメータ `-Dbobj.biar.forceSplit` がフォールバックソリューションとして適用されます。
`-Dcom.businessobjects.lcm.commit`	• KEEP_TS: デフォルト値。この値により、ソースの変更日を維持することができます。 • LEGACY: 変更日は出力先システムの実行日に対応します。これは 4.2 SP5 より前の既存の動作です。
`-Dcom.sap.businessobjects.pmw.exclude.list`	このパラメータを使用すると、ソースシステムから出力先システムにオブジェクトを昇格するとき、またはソースシステムから LCMBIAR ファイルにエクスポートするときに、オブジェクトを完全に除外することができます。 値 (CUID) にはオブジェクトを指定することができます (ドキュメント、フォルダなど)。フォルダを指定した場合、そのフォルダのすべての子が除外されます。

4. `PromotionManagementWizard.ini` を保存します。

例: `PromotionManagementWizard.ini` に含まれるプロモーション管理ウィザードのオプション

```
-Dbusinessobjects.connectivity.directory=C:¥Program Files (x86)¥SAP
BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥dataAccess¥connectionServer
-Dcom.businessobjects.mds.cs.ImplementationID=csEX
-Xms2g
-Xmx10g
-Dbobj.biar.suggestSplit=512
-Dcom.businessobjects.lcm.commit=KEEP_TS
-Dcom.sap.businessobjects.pmw.exclude.list="c:/
PromotionManagementWizardExcludedItems.txt"
# Exclusion List AY2ygq4hFJhJmZMQNlQh8OI # Report Samples
AeN4lEu0h_tAtnPEjFYxwi8 # WebIntelligence Samples
```

16.8.8 Linux のプロモーション管理ウィザード

Linux でプロモーション管理ウィザードを実行することができます。

Linux でプロモーション管理ウィザードを起動する前に、`PATH` システム変数に Java ランタイムが設定されていることを確認します。

Linux でプロモーション管理ウィザードを起動するには、以下の手順を実行します。

1. シェルを開き、以下のようなインストールディレクトリに移動します。

   `/usr/sap_bobj/enterprise_xi40`

2. 以下のコマンドを実行します。

   `./PromotionManagementWizard`

   プロモーション管理ウィザードが起動します。

   SSH および X11 リダイレクトの使用方法の詳細については、使用している OS のマニュアルを参照してください。

17 バージョン管理

17.1 InfoObject のさまざまなバージョンを管理する

バージョン管理アプリケーションでは、BI プラットフォームリポジトリに存在する BI リソースのバージョンを管理できます。SubVersion と GIT の両方のバージョン管理システムに対応しています。この節では、プロモーションマネジメントツールのバージョン管理機能の使用方法について説明します。

InfoObject のさまざまなバージョンを作成および管理するには、次の手順に従います。

1. プロモーションマネジメントツールを起動します。
2. ジョブを右クリックして、*VMS アクション*を選択し、*VM に追加*をクリックします(*VMS アクション*タブをクリックしてから *VM に追加*をクリックすることもできます)。

   > ⓘ 注記
   >
   > *VM に追加*をクリックすると、VMS リポジトリにオブジェクトのベースバージョンが作成されます。ベースバージョンは次のチェックインに必要になります。

3. [チェックイン] をクリックして、VMS リポジトリに存在するドキュメントを更新します。
   チェックインコメントダイアログボックスが表示されます。
4. コメントを入力し、[*OK*] をクリックします。
   [VMS]列と[コンテンツ管理システム]列には、選択した InfoObject のバージョン番号の変更が表示されます。
5. VMS からドキュメントの最新バージョンを取得するには、必要な I n foObject を選択し、最新バージョンを取得をクリックします。
6. 最新バージョンのコピーを作成するには、[コピーの作成] をクリックします。
   選択したバージョンのコピーが作成されます。
7. 履歴を選択し、選択したリソースに使用可能なすべてのバージョンを表示します。
   履歴ウィンドウが表示されます。次のオプションが表示されます。
   - バージョンを取得: 複数のバージョンが存在し、BI リソースの特定のバージョンを必要としている場合には、必要なリソースを選択し、[バージョンを取得]をクリックします。
   - バージョンのコピーを取得: このオプションでは、選択したバージョンのコピーを取得できます。
   - バージョンのコピーをエクスポート: このオプションでは、選択したバージョンのコピーを取得し、ローカルシステムに保存できます。

17.1.1 バージョン管理アプリケーションのアクセス権限

このセクションでは、バージョン管理アプリケーションのアプリケーションアクセス権限について説明します。

- CMC 内でバージョン管理アプリケーションに対するアクセス権限を設定できます。
- バージョン管理アプリケーション内でさまざまな機能に対する詳細なアプリケーション権限を設定できます。

バージョン管理アプリケーションの特定の権限を設定するには、以下の手順に従います。

1. CMC にログインし、[アプリケーション] を選択します。
2. [バージョン管理] をダブルクリックします。
3. [ユーザセキュリティ] をクリックし、ユーザを選択します。 選択されたユーザのセキュリティ権限の表示または割り当てを行うことができます。
4. 以下のバージョン管理固有権限があります。
   - チェックインを許可
   - コピーの作成を許可
   - 改訂の削除を許可
   - 改訂の取得を許可
   - ロックおよびロック解除を許可
   - BOMM オブジェクトの表示およびバージョン管理
   - ビジネスビューの表示およびバージョン管理
   - カレンダの表示およびバージョン管理
   - 接続の表示およびバージョン管理
   - プロファイルの表示およびバージョン管理
   - QaaWS の表示およびバージョン管理
   - レポートオブジェクトの表示およびバージョン管理
   - セキュリティオブジェクトの表示およびバージョン管理
   - ユニバースの表示およびバージョン管理
   - 削除済みリソースを表示
5. 選択したユーザに権限を割り当てるには、適切な権限を選択し、[セキュリティの割り当て] をクリックします。

17.1.2 Subversion ファイルのバックアップと復元

この節では、Subversion ファイルのバックアップと復元を実行するための推奨手順について説明します。バックアップおよび復元計画は、自然災害または大惨事によるシステム障害が発生したときに備えて実行される予防措置で構成されます。

17.1.2.1 Subversion ファイルをバックアップする

Subversion ファイルをバックアップするには、次の手順を実行します。

1. Windows で `<INSTALLDIR>¥SAP BusinessObjects Enterprise 4.0¥CheckOut` に移動するか、Unix で `<INSTALLDIR>/sap_bobj/enterprise_40/Subversion/CheckOut` に移動します。
2. `CheckOut` フォルダをコピーして、任意のバックアップデバイスに保存します。
3. `<LCM_Repository>` 全体をコピーして、任意のバックアップデバイスに保存します。

17.1.2.2 Subversion ファイルを復元する

Subversion ファイルを復元するには、次の手順を実行します。

1. 以前バックアップを行った場所から CheckOut フォルダを復元します。

   > ⓘ 注記
   >
   > CMC で [アプリケーション] > [バージョン管理] > [*VMS 設定*] をクリックして、[ワークスペースディレクトリ] フィールドに適切なチェックアウトパスが入力されていることを確認します。

2. 以前バックアップを行った場所から LCM_Repository を復元します。

   > ⓘ 注記
   >
   > CMC で [アプリケーション] > [バージョン管理] > [*VMS 設定*] をクリックして、[インストールパス] フィールドに適切なチェックアウトパスが入力されていることを確認します。

17.2 異なるバージョンの BI リソースを管理する

バージョン管理アプリケーションでは、BI プラットフォームリポジトリに存在する、異なるバージョンの BI リソースを管理できます。この機能を使用するため、ツールには SubVersion バージョン管理システムが含まれています。

異なるバージョンのジョブまたはその他の InfoObject を管理するには、次の手順に従います。

1. CMC アプリケーションにログインし、[バージョン管理] を選択します。
2. バージョン管理ウィンドウの左パネルからフォルダを選択し、バージョンを管理するジョブまたはその他の InfoObject を表示します。
3. InfoObject を選択し、[*VM に追加*] をクリックします。

   > ⓘ 注記
   >
   > [*VM に追加*] をクリックすると、バージョン管理システム(VMS)リポジトリにオブジェクトのベースバージョンが作成されます。ベースバージョンは次のチェックインに必要になります。

4. 次のドキュメントの変更で、追加的に変更されたドキュメントをバージョニングするには、[チェックイン] をクリックします。これにより、VMS リポジトリに存在するドキュメントが更新されます。

   チェックインコメントダイアログボックスが表示されます。

5. コメントを入力し、[*OK*] をクリックします。
   *VMS バージョン*列と *CMS (Central Management Server) バージョン*列には、選択した InfoObject のバージョン番号の変更が表示されます。
6. VMS からドキュメントの最新バージョンを取得するには、必要な InfoObject を選択し、[最新バージョンを取得] をクリックします。
   VMS リポジトリから CMS に最新バージョンがインポートされます。
7. 最新バージョンのコピーを作成するには、[コピーの作成] をクリックします。
   選択したバージョンのコピーが VMS リポジトリおよび CMS リポジトリに作成されます。

8. [履歴] を選択し、選択した InfoObject に使用可能なすべてのバージョンを表示します。
   履歴ウィンドウが表示されます。次のオプションが表示されます。
   - バージョンを取得: 複数のバージョンが存在し、BI リソースの特定のバージョンを必要としている場合には、必要な InfoObject を選択し、[バージョンを取得] をクリックします。
   - バージョンのコピーを取得: このオプションでは、選択したバージョンのコピーを取得できます。
   - バージョンのコピーをエクスポート: このオプションでは、選択したバージョンのコピーを取得し、ローカルシステムに保存できます。
   - 比較: このオプションでは、2 つのバージョンののメタデータ情報を比較できます詳細については、「"同じジョブの異なるバージョンの比較"」を参照してください。
9. InfoObject をロックするには、InfoObject を選択して [ロック] をクリックします。InfoObject のロックを解除するには、[ロック解除] をクリックします。すべてのバージョンのコンテンツを VMS リポジトリから削除するには、[削除] をクリックします。CMS のコンテンツには影響はありません。

   > ⓘ 注記
   >
   > InfoObject をロックすると、InfoObject に対してアクションを実行することはできません。

10. CMS のバージョンが VMS のバージョンよりも新しい場合、更新された InfoObject の隣にインジケータが表示されます。インジケータにカーソルを合わせると、`CMS` 内の方が新しいバージョンですというツールヒントが表示されます。
11. CMS ではなく VMS に存在するチェックイン済みのすべてのリソースの一覧を表示するには、[削除したリソースを表示] をクリックします。
    削除したリソースをクリックし、そのリソースの履歴を表示します。削除したリソースを選択し、[バージョンを取得] をクリックすると、リソースの特定バージョンを表示できます。

    [削除] をクリックすると、VMS リポジトリからもオブジェクトが完全に削除されます。

    > ⓘ 注記
    >
    > バージョンを取得を使用すると、リソースは VMS の見つからないファイル一覧から CMS に移動されます。

12. InfoObject を選択してから をクリックし、InfoObject のプロパティを表示します。

    または、InfoObject を右クリックして、手順 3 ～ 12 を実行することができます。
13. [バージョン管理] アプリケーションで BI アセットを検索することができます。[すべてのフィールドの検索]、[タイトルの検索]、[キーワードの検索]、[説明の検索] などのオプションを使用して、より速く結果を得るために特定の検索を実行することができます。

    > ⓘ 注記
    >
    > バージョン管理アプリケーションの検索機能はコンテキスト依存です。つまり、[監査] などのフォルダを選択して、ドキュメントを検索する文字列を入力すると、BI プラットフォームは [監査] フォルダでのみドキュメントを検索します。同様に、[すべてのフォルダ] を選択して検索を実行すると、BI プラットフォームはすべてのフォルダ内の InfoObject を検索します。

17.3 Unix での Subversion の手動による開始および停止

Unix では、マシンの再起動後、Subversion が自動的に開始されない場合があります。 Subversion は、BI プラットフォーム 4.1 SP2 から `<INSTALLDIR>/svn_startup.sh` を実行して開始し、`<INSTALLDIR>/svn_shutdown.sh` を実行して停止することができます。

> ⓘ 注記
>
> `svn_shutdown.sh` は、`svnserve` が `svn_startup.sh` を使用して開始されている場合にのみ機能します。

> ⚠ 制限
>
> SP2 パッチのインストール前に Subversion プロセスが実行されている場合、パッチのインストール後、`svn_shutdown.sh` は機能しません。 Subversion を再起動するには、手動で `svnserve` プロセスを終了してから `svn_startup.sh` を実行する必要があります。

17.4 Solaris 10 および RedHat Linux 5 の Subversion に必要なファイル

Subversion を実行するには、次のファイルが必要です。

> ⓘ 注記
>
> BI プラットフォーム 4.1 SP1 のインストール前に次のいずれかのバイナリが存在しない場合、バージョン管理を正常に実行するために、`<INSTALLDIR>/sap_bobj/lcm_installer.sh <SUBVERSION_PASSWORD> <CMS_PASSWORD>` を実行してから、Adaptive Processing Server を再起動する必要があります。

- Solaris 10 の場合: `libiconv.so.2` および `libgcc_s.so.1` を含む、`CSWlibiconv2` パッケージおよび `CSWlibgcc-s1` パッケージをインストールする必要があります。

  > → 注意
  >
  > パッケージをインストールした後に、これらのライブラリのパスがユーザの `LD_LIBRARY_PATH` 環境変数に含まれていることを確認してください。

- RedHat Linux 5 の場合: `libexpat.so.1` をデプロイする必要があります。

17.5 バージョン管理システムとして Apache Subversion を使用する

Apache Subversion をバージョン管理システムとして設定し、セントラル管理コンソールで設定を行うことができます。

1. CMC でアプリケーションをクリックします。
2. [*VMS*] をダブルクリックします。
   バージョン管理設定画面が表示されます。
3. [*VMS* 設定] を選択します。
4. バージョン管理システムリストから *SubVersion* を選択します。
   プロモーションマネジメントツールのインストール処理中に入力したサーバポート番号、パスワード、リポジトリ名、サーバ名、ユーザ名、ワークスペースディレクトリ名、およびインストールパス名が該当するフィールドに表示されます。
5. 必要に応じてこれらのフィールドを変更します。

   > ⓘ 注記
   >
   > .exe ファイルを含むインストールパスを入力します。

   Windows の場合: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Subversion`

   Unix の場合: `<INSTALLDIR>/sap_bobj/enterprise_40/subversion/bin`
6. *SVN*、*HTTP*、または *HTTPS* を選択します。

   > ⓘ 注記
   >
   > HTTPS を使用する Suvversion への接続の詳細については、*Apache Subversion* のマニュアルを参照してください。
7. (オプション) *VMS* のテストをクリックして、VMS 設定を確認します。
8. 保存をクリックします。

   > ⓘ 注記
   >
   > - Subversion をデフォルトの VMS にするには、デフォルトの *VMS* として使用を選択します。
   > - フィールドを変更した場合は、Adaptive Processing Server を再起動します。

17.6 バージョン管理システムとして Git を使用する

Git をバージョン管理システムとして設定し、セントラル管理コンソールで設定を行うことができます。

1. CMC のホームページで、[アプリケーション] を選択します。
2. [バージョン管理] をダブルクリックします。
   [バージョン管理設定] 画面の [*VMS* 設定] が表示されます。
3. [バージョン管理システム *(VMS)*] 一覧から [*Git*] を選択します。
   [*Git* 設定] および必要なパラメータが表示されます。
4. プロトコルを選択し、空のフィールドに値を入力します。各フィールドの詳細については、以下の表を参照してください。

UI 用語	説明
プロトコル	Git がローカルシステムにインストールされている場合は [ローカル] を選択し、Git がリモートサーバにインストールされている場合は [HTTP] を選択します。
ユーザ名	Git がインストールされているサーバのユーザ名を入力します。
パスワード	Git がインストールされているサーバにアクセスするためのパスワードを入力します。
サーバ URL	Git がインストールされているサーバへのリンクを入力します。
ワークスペースディレクトリ	ワークスペースを保存するファイルパスを入力します。
サーバリポジトリ名	サーバリポジトリの名前を入力します。
GIT インストールパス	Git のインストールディレクトリを入力します。

> **注記**
>
> Git をデフォルトの VMS にするには、[デフォルトの *VMS* として使用] を選択します。

5. (オプション) [*VMS* のテスト] を選択して、VMS 設定を確認します。
6. [保存] を選択します。
7. サーバ > サーバの一覧 に移動し、[*Adaptive Processing Server*] のコンテキストメニューから [サーバの再起動] を選択します。

Git をバージョン管理システムとして正常に設定しました。

17.7 デフォルトバージョン管理システムの設定

CMS を再初期化すると、すべてのアプリケーション設定が消去されます。 バージョン管理システムのデフォルト設定は次のとおりです。

パラメータ	値
サーバ名	`localhost`
サーバポート	`3690`
ユーザ名	`LCM`
パスワード	インストール中に入力されます。
インストールパス	Windows の場合: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Subversion` Unix の場合: `<INSTALLDIR>/sap_bobj/enterprise_xi40/subversion/bin`

パラメータ	値
リポジトリ名	Windows の場合: `svn_repository` Unix の場合: `LCM_repository`
ワークスペースディレクトリ	Windows の場合: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥CheckOut` Unix の場合: `<INSTALLDIR>/sap_bobj/enterprise_xi40/CheckOut`
プロトコル	`SVN`

17.8 同じジョブの異なるバージョンを比較する

同じジョブの 2 つのバージョンの差分を表示するには、次の手順に従います。

1. CMC アプリケーションにログインします。
2. CMC のホームページから [バージョン管理] を選択します。
3. バージョン管理画面で、バージョンを比較する必要があるジョブを選択します。
4. [履歴] をクリックします。
   [履歴] ページが表示され、選択した InfoObject のすべてのバージョンが表示されます。
5. 比較する 2 つのバージョンを選択します。
6. [比較] をクリックします。
   比較処理が開始されます。差分はオレンジ色で強調表示され、見つからないオブジェクトは赤色で強調表示されます。
7. 差分レポートを保存するには、[保存] をクリックします。

17.9 Subversion コンテンツをアップグレードする

以前のバージョンの BI プラットフォームを使用して作成された古い SubVersion コンテンツがある場合、コンテンツを最新バージョンにアップグレードするには、次の手順に従います。

1. SAP BusinessObjects Enterprise 4.2 マシンの VMS にログオンします。
2. オブジェクトをチェックインします。たとえば、管理者のオブジェクトとゲストのオブジェクトを 2 回チェックインします。
3. CMC で [ユーザ] をクリックし、VMS と CMS のバージョン番号に 2 が表示されていることを確認します。
4. VMS からログオフします。
5. コマンドプロンプトに移動して `C:¥Program Files¥Subversion¥bin` に移動します。次のエクスポートコマンドを実行します。`svnadmin dump c:/LCM_repository/svn_repository > dumrepo`

6. dumrepo ファイルが BI プラットフォームマシンにコピーされます。
7. BI プラットフォームマシンのコマンドプロンプトに移動して C:¥Program Files (x86)¥SAP に移動します。次に、以下のコマンドを実行します。

   ```
   svnadmin.exe load "C:/Program Files (x86)/SAP BusinessObjects/SAPBusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository" < c:/dumrepo
   ```

   ```
   svnadmin.exe upgrade "C:/Program Files (x86)/SAP BusinessObjects/SAP BusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository"
   ```
8. コマンドが正常に実行されたら、SIA を再起動します。
9. CMC にログインして [バージョン管理] をクリックします。
10. [ユーザ] をクリックし、VMS のバージョンが 2 であることを確認します。
11. [管理者] オブジェクトを選択し、[最新バージョンを取得] をクリックします。
12. これで、VMS と CMS のバージョン番号が同じになります。

    Apache Subversion のアップグレードの詳細については、Apache Subversion 1.10 Release Notes を参照してください。

17.10 クラスタ化された Processing Job Server の Subversion の設定

17.10.1 選択肢 A: すべてのバージョン管理システム操作の前にメインの Subversion マシンを設定する

1. 作業コピーディレクトリが <INSTALLDIR>¥CheckOut に作成されていないことを確認します。
2. Subversion 作業コピーファイル用ディレクトリを作成して共有し、このディレクトリを他のマシンから書き込み可能にします。
3. CMC のバージョン管理システム設定ページで、サーバ名を **localhost** からメインマシンのアドレスに変更します。
4. ワークスペースディレクトリを共有した作業コピーに、 ¥¥<HOSTNAME>¥<SHARENAME> の形式で変更します。
5. Server Intelligence Agent (SIA) を停止して、アカウントを LocalSystem からオペレーティングシステムの管理者に変更します。

   > ⓘ 注記
   >
   > LocalSystem には、共有ディレクトリに対するネットワークアクセス権がありません。

6. SIA を開始します。

   > ⓘ 注記
   >
   > SIA がすでに、共有ディレクトリへのネットワークアクセス権を持つアカウントで起動されている場合は、ステップ 3、4 のバージョン管理システムをホストする Processing Job Server すべてを再起動するだけで、効果を得ることができます。

17.10.2 選択肢 B: バージョン管理システムで作業コピーディレクトリを作成した後に Subversion を設定する

1. Subversion が BI プラットフォームの一部としてインストールされていることを確認します。
2. `<INSTALLDIR>¥CheckOut` にある作業コピーディレクトリを共有し、このディレクトリを他のマシンから書き込み可能にします。
3. 次のいずれかの方法で、ワークスペースの名前を指定します。
   - メインマシンを使用してバージョン管理システム (VMS) 操作を実行します。次に、Subversion の作業コピーディレクトリを確認して、ワークスペースの名前を指定します。
   - 記号 @ を削除し、すべてのコロンを文字 *B* で置換することで、ワークスペースの名前を予測します。たとえば、クラスタの名前が `ABCD-LCM:6400` である場合、VMS はワークスペース名として `ABCD-LCMB6400` を使用します。

> **注記**
>
> Subversion は、そのリポジトリを作業コピーディレクトリに格納します。

4. 次のコマンドを実行して、デフォルトの URL を **`localhost`** から、すべてのマシンが使用できるものに変更します。

```
svn switch --relocate svn://localhost:3690/svn_repository svn://
<SUBVERSION_MACHINE>:3690/svn_repository ¥
¥<SUBVERSION_SHARE>¥CheckOut¥<WORKSPACE_NAME>-LCMB6400¥WORKSPACE
```

5. 入力を求められたら、オペレーティングシステムの管理者パスワード、ユーザ、パスワードを入力します。

> **注記**
>
> デフォルトでは、ユーザは LCM、パスワードはインストール中に設定されたものです。

6. CMC のバージョン管理システム設定ページで、サーバ名を **`localhost`** からメインマシンのアドレスに変更します。
7. ワークスペースディレクトリを **`localhost`** から共有した作業コピーの、`¥¥<SUBVERSION_SHARE>¥CheckOut`
8. Server Intelligence Agent (SIA) を停止して、アカウントを LocalSystem からオペレーティングシステムの管理者に変更します。
9. SIA を開始します。

> **注記**
>
> SIA がすでに、共有ディレクトリへのネットワークアクセス権を持つアカウントで起動されている場合は、VMS をホストする Processing Job Server すべてを再起動するだけです。

17.10.3 他の Subversion マシンの設定

他の Subversion マシンを設定するには、Server Intelligence Agent (SIA) を停止して、アカウントを LocalSystem からネットワークアクセス権を持つ別のアカウント (オペレーティングシステムの管理者アカウントなど) に変更し、この Processing Job Server が共有ディレクトリにアクセスできるようにします。次に、SIA を再起動します。

> **注記**
>
> SIA がすでに、共有ディレクトリへのネットワークアクセス権を持つアカウントで起動されている場合は、VMS をホストする Processing Job Server すべてを再起動するだけです。

18 アプリケーションの管理

18.1 GDPR ポップアップメッセージの無効化

SAP BusinessObjects Business Intelligence プラットフォームの 4.2 SP5 リリース以降、GDPR (Global Data Protection Regulation) 免責事項ポップアップメッセージは、すべてのユーザに対して、BI プラットフォーム Web アプリケーションにログインするときに必須になりました。

- BI ラウンチパッド
- CMC
- Fiori BI ラウンチパッド
- OpenDocument

GDPR 免責事項メッセージが必須であることを認識したうえで、このメッセージの表示をオフにすることができます。

> ⚠ 警告
>
> GDPR 免責事項ポップアップメッセージは、無効にしないことをお勧めします。また、事前に無効にすることはできません。EU の GDPR の法律に確実に準拠するために、すべてのユーザが続行前にこのメッセージに積極的に同意する必要があります。

BI ラウンチパッドにログインするユーザに対する GDPR メッセージの無効化

1. デフォルトの Tomcat インストールでは、次のプロパティファイルに移動します。
   `<BOE_HOME>¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥default`
   例: `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥default`
2. `<Infoview.properties>` という名前の新しいファイルを作成し、カスタムパスに `<properties file>` を入力します。
   `<BOE_HOME>¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥custom`
   例: `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥custom`
3. `<disclaimer.enabled>` という新しいプロパティエントリを作成し、`<false>` に設定します。
   `disclaimer.enabled=false`
4. ファイルを保存します。
5. Tomcat を再起動します。

CMC にログインするユーザに対する GDPR メッセージの無効化

1. デフォルトの Tomcat インストールでは、次のプロパティファイルに移動します。
   `<BOE_HOME>¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥default`
   例: `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥custom`
2. `<CMCApp.properties>` という名前の新しいファイルを作成し、カスタムパスに `<properties file>` を入力します。
   `<BOE_HOME>¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥custom`
   例: `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥custom`
3. `<disclaimer.enabled>` という新しいプロパティエントリを作成し、`<false>` に設定します。
   `disclaimer.enabled=false`
4. ファイルを保存します。
5. Tomcat を再起動します。

Fiori BI ラウンチパッドにログインするユーザに対する GDPR メッセージの無効化

1. デフォルトの Tomcat インストールでは、次のプロパティファイルに移動します。
   `<BOE_HOME>¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥default`
   例: `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥default`
2. `<FioriBI.properties>` という名前の新しいファイルを作成し、カスタムパスに `<properties file>` を入力します。
   `<BOE_HOME>¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥custom`
   例: `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥custom`
3. `<disclaimer.enabled>` という新しいプロパティエントリを作成し、`<false>` に設定します。
   `disclaimer.enabled=false`
4. ファイルを保存します。
5. Tomcat を再起動します。

OpenDocument の GDPR メッセージの無効化

1. デフォルトの Tomcat インストールでは、次のプロパティファイルに移動します。
   `<BOE_HOME>¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥default`
   例: `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥default`
2. `<OpenDocument.properties>` という名前の新しいファイルを作成し、カスタムパスに「`<properties file>`」と入力します。
   `<BOE_HOME>¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥custom`
   例: `C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEB-INF¥config¥custom`

3. `<disclaimer.enabled>` という新しいプロパティエントリを作成し、`<false>` に設定します。
   `disclaimer.enabled=false`
4. ファイルを保存します。
5. Tomcat を再起動します。

18.2 CMC を介したアプリケーションの管理

18.2.1 概要

CMC の [アプリケーション] 管理エリアでは、プログラムを作成せずに、CMC や BI ラウンチパッドのような Web アプリケーションの外観や機能を変更できます。各ユーザ、グループ、および管理者に関連付けられたアクセス権を変更することで、ユーザ、グループ、および管理者のアプリケーションへのアクセス権を変更することもできます。

ここでは、さまざまな設定の管理方法についてのコンテキスト情報、手順および指示を説明します。次のアプリケーションには、CMC を介して変更可能な設定があります。

- アラートアプリケーション
- *Analysis edition for OLAP*
- *Analysis Office Runtime*
- 認可サーバの設定
- *BEx Web* アプリケーション
- *BI* 管理者のコックピット
- *BI* ラウンチパッド
- *BI* ワークスペース
- セントラル管理コンソール
- コラボレーション
- *BI* コメンタリアプリケーション
- *Crystal Reports* 設定
- *HANA* 認証
- インフォメーションデザインツール
- *Information Steward* アプリケーション
- *BI* 管理スタジオ
- マルチテナント管理ツール
- *OpenDocument*
- プラットフォーム検索アプリケーション
- プロモーション管理
- リサイクルビンアプリケーション
- *RESTful Web* サービス
- *SAP BusinessObjects Mobile*
- *SAP Analytics Cloud*
- トランスレーションマネジメントツール

- ユニバースデザインツール
- バージョン管理
- バージョン管理
- *Visual Difference*
- *Web Intelligence*
- *Web* サービス
- ワークフローアシスタント

18.2.2 アプリケーションの共通設定

18.2.2.1 アプリケーションに対するユーザアクセス権の設定

権限を使用すると、アプリケーションの特定の機能に対するユーザアクセス権を制御することができます。 CMC の [アプリケーション] エリアを使用すると、アプリケーションのアクセスコントロールリストに主体を割り当てたり、主体が持っている権限を表示したり、主体がアプリケーションに対して持っている権限を変更できます。 権限管理の詳細については、*SAP BI* プラットフォーム管理者ガイドを参照してください。

18.2.2.2 CMC の Web アプリケーショントレースログレベルを設定する

他の Web アプリケーションをトレースするには、対応する `BO_trace.ini` ファイルを手動で設定してください。

1. CMC の [アプリケーション] エリアでアプリケーションを右クリックして、[トレースログ設定] を選択します。

   > **注記**
   >
   > トレースログ設定があるアプリケーションは、Fiorified BI ラウンチパッド、CMC、OpenDocument、プロモーション管理、バージョン管理、Visual Difference、および Web サービスです。

   [トレースログを設定] ダイアログボックスが表示されます。
2. [ログレベル] リストから設定を選択します。
3. [保存して閉じる] をクリックします。
4. Web アプリケーションサーバを再起動します。

新しいトレースログレベルは、Web アプリケーションに次回ログオンしたときに有効になります。

関連情報

トレースログレベル [666 ページ]

18.2.2.2.1 トレースログレベル

BI プラットフォーム のコンポーネントでは、次のトレースログレベルを利用できます。

レベル	説明
未指定	このトレースログレベルは他の方法 (通常は `.ini` ファイル) で指定します。
なし	トレースは発生しません。
低	このトレースログフィルタでは、警告とステータスメッセージを無視しながら、エラーメッセージをログできます。コンポーネントのスタートアップ、シャットダウン、リクエストの開始、リクエストの終了の各メッセージについては、重要ステータスメッセージがログされます。このレベルは、デバッギング目的の場合はお勧めしません。
中	このトレースログフィルタは、エラー、警告、ほとんどのステータスメッセージを含むよう設定されます。あまり重要ではない、または非常に詳細なメッセージはフィルタで除外されます。このレベルは、デバッギング目的には詳細度が足りません。
高	メッセージはフィルタリングされません。このレベルは、デバッギング目的の場合にお勧めします。 ⚠ 警告 このトレースログレベルは、CPU 使用率を上げストレージ容量を消費するため、システムリソースに大きな影響を与えます。

18.2.3 アプリケーション固有の設定

18.2.3.1 CMC アプリケーション設定の管理

18.2.3.1.1 認証およびプログラムオブジェクト

ユーザが実行できるプログラムオブジェクトの種類を制御し、プログラムオブジェクトの実行に必要な認証情報を設定することができます。

プログラムオブジェクトをリポジトリへ追加することに関してはセキュリティ上の危険があることに注意してください。プログラムオブジェクトの実行に使用するアカウントに付与されたファイル権限のレベルによって、ファイルに対してプログラムがどのような変更を行えるかを指定します。

有効または可能にするプログラムオブジェクトの指定

最も初歩的なレベルのセキュリティとして、使用できるプログラムオブジェクトの種類を設定することができます。

すべてのプラットフォームでの認証

CMC の［フォルダ］管理エリアでは、プログラムの実行に使用するアカウントの認証情報を指定します。この機能により、プログラムに特定のユーザアカウントを設定し、そのアカウントでプログラムオブジェクトを実行できる適切なアクセス権をユーザアカウントに割り当てることができます。

また、情報プラットフォームサービスにプログラムオブジェクトを追加するユーザは、固有の認証情報をプログラムオブジェクトに割り当てて、プログラムからシステムにアクセスさせることができます。このように、プログラムはユーザアカウントによって実行され、プログラムのアクセス権はユーザのアクセス権に制限されます。プログラムオブジェクトにユーザアカウントを指定しない場合、プログラムはデフォルトにシステムアカウントで実行されます。このような場合、プログラムのアクセス権は通常ローカルマシンだけにあり、ネットワークに対してはありません。

> ⓘ 注記
>
> デフォルトでは、プログラムオブジェクトをスケジュールしたときに、認証情報が指定されていないと、ジョブが失敗します。デフォルトの認証情報を提供するには、[アプリケーション]管理エリアの[*CMC*]を選択します。[アクション]メニューの[プログラムオブジェクト権限]をクリックします。[次のオペレーティングシステム認証情報を使用してスケジュールを設定する]をクリックして、デフォルトのユーザ名とパスワードを指定します。

Java プログラムの認証

情報プラットフォームサービスでは、あらゆるプログラムオブジェクトのセキュリティを設定することができます。Java プログラムの場合は、情報プラットフォームサービス は Java Policy File を主に使用します。このファイルには、安全でないコードの Java デフォルトに対応したデフォルトの設定です。特殊な要件に合わせるために、Java Policy Tool(Java Development Kit に同梱)を使用して Java Policy File を変更することができます。

Java Policy Tool には コードベースの 2 つのエントリがあります。最初のエントリは、SAP BusinessObjects Enterprise Java SDK にポイントされており、プログラムオブジェクトにすべての SAP BusinessObjects Enterprise JAR ファイルへのフルアクセス権を付与しています。2 つ目のコードベースのエントリは、すべてのローカルファイルに適用されます。安全でないコードの Java デフォルトと同じ安全でないコードのセキュリティ設定を使用します。

> ⓘ 注記
>
> Java Policy の設定は、同じマシンで実行されているすべての Program Job Server で共通です。

> ⓘ 注記
>
> デフォルトでは、Java Policy File は 情報プラットフォームサービスインストールのルートディレクトリにある Java SDK ディレクトリにインストールされます。たとえば、Windows 版インストールの標準の場所は、

C:¥Program Files¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥conf¥crystal-program.policy です。

18.2.3.1.1.1 有効または可能にするプログラムオブジェクトを指定する

1. アプリケーションエリアで、セントラル管理コンソールを選択します。
2. アクション > プログラムオブジェクト権限をクリックします。
   [プログラムオブジェクト権限]ダイアログボックスが表示されます。
3. [ユーザが行える操作]エリアで、ユーザが実行できるようにするプログラムオブジェクトの種類を選択します。

   スクリプト/バイナリの実行と *Java* プログラムの実行のどちらかを選択できます。

   Java プログラムの実行を選択した場合は、偽装の使用チェックボックスをオンまたはオフにできます。このオプションを使用すると、情報プラットフォームサービスにログオンするためのトークンが Java プログラムに提供されます。
4. 保存して閉じるをクリックします。

> **注記**
>
> SAP BusinessObjects Business Intelligence プラットフォーム 4.3 サポートパッケージ 3 にアップグレードすると、すべてのユーザに対するプログラムオブジェクト権限がデフォルトで拒否されます。管理者ユーザ (または管理者グループの任意のユーザ) がこれを有効にすることができます。
>
> *Java* プログラムの実行の下に、偽装の使用チェックボックスがあります。4.3 サポートパッケージ 3 では、偽装の使用チェックボックスが削除されました。

18.2.3.1.2 処理拡張機能のシステムへの登録

> **注記**
>
> この機能は Web Intelligence ドキュメントには適用されません。

処理拡張機能を特定のオブジェクトに適用するには、関連するスケジュールの処理やリクエストの表示を行う各マシンで、コードライブラリを使用できるようにする必要があります。BI プラットフォームのインストール時には、Job Server、Processing Server、Report Application Server (RAS) に処理拡張機能用のデフォルトディレクトリが作成されます。処理拡張機能は、各サーバ上のこのデフォルトディレクトリにコピーすることをお勧めします。Windows の場合、デフォルトディレクトリは、`C:¥Program Files¥SAP Business Objects¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥ProcessExt` です。UNIX の場合、`sap_bobj/ProcessExt` ディレクトリです。

> **→ ヒント**
>
> 処理拡張機能ファイルは、共有することができます。

拡張機能に記述した機能に応じて、次のマシンにライブラリをコピーします。

- 処理拡張機能をスケジュールリクエストだけに対して実行する場合は Adaptive Job Server として起動する各マシンにライブラリをコピーします。
- 処理拡張機能を表示リクエストだけに割り込ませる場合、Crystal Reports Processing Server または RAS として実行されている各マシンにライブラリをコピーします。
- 処理拡張機能をスケジュールリクエストと表示リクエストの両方に割り込ませる場合は、Adaptive Job Server、Crystal Reports Processing Server、または RAS として実行されている各マシンにライブラリをコピーします。

> ⓘ 注記
>
> 処理拡張機能を特定のサーバグループに対して行われるスケジュール/表示リクエストだけに割り込ませる場合、そのグループ内の各処理サーバだけにライブラリをコピーします。

18.2.3.1.2.1 システムに処理拡張機能を登録する

1. CMC の [アプリケーション] 管理エリアを表示します。
2. [セントラル管理コンソール] を選択します。
3. アクション > 処理拡張機能 をクリックします。
   [処理拡張機能: *CMC*] ダイアログボックスが開きます。
4. [名前]フィールドに、処理拡張機能の表示名を入力します。
5. [場所]フィールドに、処理拡張機能のファイル名を追加パス情報と共に入力します。
   - 使用するマシン上のデフォルトのディレクトリに処理拡張機能をコピーした場合は、ファイル名のみを拡張子なしで入力します。
   - デフォルトのディレクトリのサブフォルダに処理拡張機能をコピーした場合は、「`<subfolder>/<filename>`」というように場所を入力します。
6. *[説明]*フィールドを使用して、処理拡張機能に関する情報を追加します。
7. [追加]をクリックします。

   > → ヒント
   >
   > 処理拡張機能を削除するには、[既存の拡張機能]一覧からその機能を選択して、[削除]をクリックします。繰り返して実行されるジョブで、この処理拡張機能を使用していないことを確認してください。この拡張機能を使用したジョブが今後実行されるとエラーになります。

8. [保存して閉じる]をクリックします。
   処理拡張機能は CMC に登録されます。

これで、この処理拡張機能を選択し、そのロジックを特定のオブジェクトに適用できます。

18.2.3.1.2.2 複数のサーバでの処理拡張機能の共有

> ⓘ 注記
>
> この機能は、Web Intelligence ドキュメント、または SAP Crystal Reports for Enterprise で作成したレポートには適用されません。

すべての処理拡張機能を 1 か所に保存する場合は、各 Adaptive Job Server、Crystal Reports Processing Server、および RAS の処理拡張機能のデフォルトディレクトリを変更することができます。最初に、すべてのサーバからアクセス可能なネットワークドライブ上の共有ディレクトリに処理拡張機能をコピーします。各サーバマシンからネットワークドライブをマップ(またはマウント)します。

> ⓘ 注記
>
> Windows のマップされたドライブは、マシンを再起動すると有効になります。

サーバを Windows と UNIX の両方で実行している場合は、すべての処理拡張機能の .dll ファイルと .so ファイルを共有ディレクトリにコピーする必要があります。また、共有ネットワークドライブは Windows マシンと UNIX マシンから(Samba や他のファイル共有システムを介して)認識可能になっている必要があります。

最後に、各サーバのコマンドラインを変更し、デフォルトの処理拡張機能のディレクトリを変更します。コマンドラインを変更するには、CMC の [サーバ] タブに移動し、サーバを選択して、その [プロパティ] ページを開きます。コマンドラインに、`-report_ProcessExtPath <absolute path>` を追加します。サーバが実行されているオペレーティングシステムに応じたパス規則を使用して、<絶対パス> を新しいフォルダのパスで置き換えます(`M:¥code¥extensions`、`/home/shared/code/extensions` など)。

処理拡張機能のデフォルトディレクトリを変更するには、CCM を使用してサーバを停止します。サーバのプロパティを開き、コマンドラインを変更します。完了したら、サーバを再起動します。

18.2.3.1.3 CMC タブアクセスの管理

18.2.3.1.3.1 委任管理および CMC タブへのアクセス

通常、BI プラットフォームシステム管理者は、大量のドキュメント、フォルダ、ユーザ、サーバ、およびその他のオブジェクトを管理します。しかし、大規模な企業の環境では、1 人の管理者のリソースを超える場合があります。優先順位の高いタスクのみに集中したいシステム管理者は、委任管理者を作成して、タスク管理のサブセットを委任管理者に割り当てることができます (部署またはテナントコンテンツの管理など)。システム管理者とは異なり、委任管理者は制限されたタスクセットを実行し、システム内のオブジェクトに対する少数の権限を持っています。

セントラル管理コンソールのデフォルト設定では、ユーザはすべての利用可能な CMC タブにアクセスできます。システム管理者は、主体 (ユーザまたはユーザグループ) に対して表示するタブを制御するために、CMC タブへのアクセスを管理できます。委任管理者のユーザ経験およびワークフローを向上するために、システム管理者は、委任管理者が使用しない見込みの CMC タブを非表示にすることもできます。

> ⚠ 警告
>
> CMC タブのアクセス管理は、CMC ユーザインタフェースの外観のみに影響します。CMC タブを非表示にしてもセキュリティは保障されません。タブ内のオブジェクトの設定または変更のセキュリティ権限を設定し

ていないためです。ユーザが、許可されていないオブジェクトで許可されていない操作を実行できないようにするには (たとえば、セントラル設定マネージャまたは BI プラットフォーム SDK に基づくサードパーティ製ソフトウェアによるサーバの管理など)、適切なセキュリティ権限をオブジェクト (サーバオブジェクトなど) に設定する必要があります。

関連情報

他のユーザに対して CMC タブアクセスを管理する [672 ページ]
他のユーザまたはユーザグループに対して CMC タブへのアクセスを設定する権限を管理する [674 ページ]

18.2.3.1.3.2 CMC タブアクセスの操作

18.2.3.1.3.2.1 他のユーザに対する CMC タブアクセスの管理

システム管理者は、常にすべての CMC タブにアクセスできます。以下のガイドラインを使用して、主体がアクセスできる CMC タブを管理します。

- 管理プロセスを簡素化して、メンテナンスおよびトラブルシューティングの必要性を減らすために、管理者がユーザレベルではなくユーザグループレベルで、CMC タブへのアクセスを管理することをお勧めします。
- 最上位フォルダを持つ CMC タブの場合、管理者はタブへのアクセスを許可し、タブの最上位フォルダで、[表示] 権限を許可する必要があります。以下の CMC タブは最上位フォルダをサポートしています。
  - アクセスレベル
  - カレンダ
  - カテゴリ
  - (ユニバース) 接続
  - 暗号化キー
  - イベント
  - フェデレーション
  - フォルダ
  - 受信ボックス
  - *OLAP* 接続
  - 個人用カテゴリ
  - 個人用フォルダ
  - プロファイル
  - レプリケーション一覧
  - サーバとグループ
  - 一時記憶領域
  - ユニバース
  - ユーザとグループ
  - *Web* サービスクエリ

- システムセキュリティ向上のため、Administrators グループのメンバーのみが以下の CMC タブにアクセスできます。システム管理者などの Administrators グループのメンバーは、CMC タブのアクセス権限に関係なく、すべての CMC タブにアクセスできます。CMC タブのアクセス権限は、委任管理者、すなわち Administrators グループ以外のメンバーに対する CMC タブへのアクセスを制御するように設計されています。
  - 監査
  - 認証
  - 暗号化キー
  - ライセンスキー
  - モニタリング
  - セッション
  - 設定
  - ユーザ属性管理

> ⚠ 警告
>
> CMC タブのアクセス管理は、CMC ユーザインタフェースの外観のみに影響します。CMC タブを非表示にしてもセキュリティは保障されません。タブ内のオブジェクトの設定または変更のセキュリティ権限を設定していないためです。ユーザが、許可されていないオブジェクトで許可されていない操作を実行できないようにするには (たとえば、セントラル設定マネージャまたは BI プラットフォーム SDK に基づくサードパーティ製ソフトウェアによるサーバの管理など)、適切なセキュリティ権限をオブジェクト (サーバオブジェクトなど) に設定する必要があります。

18.2.3.1.3.2.1.1 他のユーザに対して CMC タブアクセスを管理する

1. CMC にログオンします。
2. [ユーザとグループ] タブで主体を右クリックし、[*CMC タブ設定*] を選択します。

   > ⓘ 注記
   >
   > CMC タブへのアクセスが制限されていない場合、以下のメッセージが表示されます。警告: `CMC` タブへのアクセスは現在無制限です。`CMC` へのアクセスを制限するには、[アプリケーション] タブをクリックして [`CMC`] を選択し、`CMC` タブへのアクセスが制限されるように設定します。これらの設定は、`CMC` タブへのアクセスが制限された後に有効になります。CMC タブへのアクセスをここで設定できます。ただし、設定は CMC タブへのアクセスが制限されるまで有効になりません。

   [*CMC タブへのアクセスの設定*] ダイアログボックスに、テーブルが表示されます。
   - □または□は主体がアクセス可能な CMC タブを示します。
   - [継承] は、そのタブへのアクセスが親ユーザグループから継承されたことを示します。
   - [明示] は、そのタブへのアクセスが主体レベルで明示的に指定されていることを示します。
3. CMC タブへのアクセス権限を確認します。アクセス権限を変更するには、ツールバーのボタンを使用します。
   - [許可] をクリックして、タブへのアクセスを明示的に許可します。
   - [拒否] をクリックして、タブへのアクセスを明示的に拒否します。

- [継承] をクリックして、継承されたアクセス権限を使用します。

> ⓘ 注記
>
> ボタンをクリックすると、主体にただちに変更が適用されます。

4. 終了したら、[閉じる] をクリックします。

新しく有効になったタブへのアクセスが、テーブルの [許可] 列に表示されます。

関連情報

CMC タブへのアクセスを制限する [676 ページ]

18.2.3.1.3.2.1.2 CMC タブへのアクセスの継承

CMC タブへのアクセス権限および、他のユーザまたはユーザグループに対して CMC タブへのアクセスを設定する権限は両方とも、他の BI プラットフォームのセキュリティ権限と同じ方法で適用および継承されます。主体が明示的に指定されたタブへのアクセス許可を持っていない場合、主体がメンバーとなっているユーザグループのタブへのアクセス権限を継承します。

ユーザが 2 つのユーザグループのメンバーである場合、タブへのアクセスはその他すべての BI プラットフォームの権限の計算と同じ方法で計算されます。たとえば、CMC タブへのアクセスがグループの 1 つで許可されており、他のグループで拒否されている場合、主体は CMC タブにアクセスすることはできません。

> ⓘ 注記
>
> - ユーザグループの CMC タブへのアクセス権限を変更すると、CMC タブへのアクセスが [継承] に設定されている場合、そのユーザグループから権限を継承するすべてのユーザまたはユーザグループに対して、同じタブへのアクセス権限が変更されます。
> - ユーザレベルでのタブへのアクセス設定は、常にユーザグループから継承されるタブへのアクセスより優先されます。

18.2.3.1.3.2.1.3 委任管理者ユーザグループ

委任管理者ユーザグループを作成して、CMC タブの管理を簡単にすることができます。個別の CMC タブへのアクセス設定を防止するために、既存のユーザまたはユーザグループを委任管理者ユーザグループのメンバーにすることができます。以下は、推奨される設定ですが、特定のビジネスニーズに応じて変更できます。

> ⓘ 注記
>
> 権限が [継承] に設定されている場合、複数のグループ内のメンバーシップが権限の追加となります。

委任管理者ユーザグループ	推奨される権限
システム管理者	すべてのタブへのアクセスを許可します。
ユーザ管理者	[アクセスレベル]、[フォルダ]、[受信ボックス]、[個人用フォルダ]、[個人用カテゴリ]、[クエリ結果]、[セッション]、および [ユーザとグループ] へのアクセスを許可します。その他のすべてのタブを [継承] に設定します。
コンテンツ管理者	[カレンダ]、[カテゴリ]、[イベント]、[フォルダ]、[インスタンスマネージャ]、[個人用カテゴリ]、[個人用フォルダ]、[プロファイル]、[クエリ結果]、および [ユニバース] へのアクセスを許可します。その他のすべてのタブを [継承] に設定します。
サーバ管理者	[サーバ] および [アプリケーション] へのアクセスを許可します。その他のすべてのタブを [継承] に設定します。

18.2.3.1.3.2.1.4 他のユーザまたはユーザグループに対して CMC タブへのアクセスを設定する権限を管理する

大規模な企業の環境では、システム管理者が CMC タブへのアクセス管理を委任管理者に委任する必要がある場合があります。また、複数テナントのシステムでは、その他のユーザおよびユーザグループに対して CMC タブへのアクセスを管理する責任がある委任管理者が各テナントにいます。

1. CMC にログオンします。
2. [ユーザとグループ] タブで主体を右クリックし、[*CMC タブ設定*] を選択します。
   [*CMC タブの設定*] ダイアログボックスに、[*他のユーザまたはユーザグループに対して CMC タブへのアクセスを設定する権限*] が主体に対して表示されます。

   > ⓘ 注記
   >
   > この権限が許可されている場合、主体が [アクセス権を安全に変更する] 権限を持っているユーザに対して、主体は CMC タブ (主体がアクセス権限を持っているタブのみ) へのアクセスを管理できます。また、主体が [アクセス権を安全に変更する] 権限を持っているユーザに、[*他のユーザまたはユーザグループに対して CMC タブへのアクセスを設定する権限*] を許可することにより、主体は他のユーザに CMC タブへのアクセス管理を委任することができます。

   - □または□は、主体が他のユーザまたはユーザグループに対して CMC タブへのアクセスを設定する権限があるかどうかを示します。
   - [継承] は、権限が親ユーザグループから継承されたことを示します。
   - [明示] は、権限が主体レベルで明示的に指定されていることを示します。
3. 他のユーザまたはユーザグループに対して CMC タブへのアクセスを設定する権限を確認します。権限を変更するために、リストから以下の設定のいずれかを選択することができます。
   - [許可] をクリックして、他のユーザまたはユーザグループに対して CMC タブへのアクセスを管理する権限を明示的に許可します。
   - [拒否] をクリックして、他のユーザまたはユーザグループに対して CMC タブへのアクセスを管理する権限を明示的に拒否します。
   - [継承] をクリックして、他のユーザまたはユーザグループに対して 管理された CMC タブへのアクセス権限を継承します。

> ⓘ 注記
>
> リストから設定を選択すると、主体の権限がすぐに変更されます。

4. 終了したら、[閉じる] をクリックします。

新しく有効な許可が表示されます。

関連情報

委任管理および CMC タブへのアクセス [670 ページ]
CMC タブへのアクセスの継承 [673 ページ]

18.2.3.1.3.2.1.5 ユーザまたはユーザグループに [カスタマイズ] タブを追加する

ユーザまたはユーザグループに [カスタマイズ] タブを追加する前に、CMC タブアクセスを ["制限付き"] に設定しておく必要があります。

1. CMC で、[ユーザとグループ] 管理エリアを表示します。
2. ユーザまたはユーザグループを右クリックし、[*CMC タブ設定*] を選択します。

   [*CMC タブの設定*] ダイアログボックスが表示され、各 CMC タブのタイトルと、ユーザグループの場合は権限レベルが一覧表示されます。

   以下の警告メッセージが、ダイアログボックスの最上部に赤で表示されている場合、[カスタマイズ] タブを追加する前に、CMC タブへのアクセスが制限されるように設定する必要があります。

   警告: `CMC` タブへのアクセスは現在無制限です。`CMC` へのアクセスを制限するには、[アプリケーション] タブをクリックして `[CMC]` を選択し、`CMC` タブへのアクセスが制限されるように設定します。これらの設定は、`CMC` タブへのアクセスが制限された後に有効になります。
3. (必要な場合) CMC タブへのアクセスが制限されるように設定するには、次の手順を実行します。
   a. CMC の[アプリケーション] 管理エリアで、[セントラル管理コンソール] を右クリックし [*CMC タブアクセスの設定*] を選択します。
   b. [*CMC タブアクセス*] で、[制限付き] オプションを選択し、[保存して閉じる] をクリックします。
4. ユーザグループの [*CMC タブの設定*] ダイアログボックスで、各 CMC タブに対して、一覧から [許可]、[拒否]、または [継承] を選択します。
   タブに対する権限を変更するたびに、[CMC タブの設定] ダイアログボックスによりユーザグループの権限が更新されるため、その他のユーザまたはユーザグループのタブアクセスを設定できるようになります。
5. [閉じる] をクリックします。

18.2.3.1.3.2.2 CMC タブへのアクセスを制限する

まず、主体の CMC タブへのアクセスを設定してから、CMC タブへのアクセスを制限することをお勧めします。これを設定する前にタブへのアクセスを制限すると、管理者がユーザにアクセスを許可しないと、すべての CMC タブにアクセスできなくなります。

以前のバージョンの BI プラットフォーム との競合を確認するために、BI プラットフォームがインストールされた後で CMC タブへのアクセスは最初に [制限なし] に設定され、CMC にアクセスできるすべてのユーザがすべての使用可能なタブにアクセスできます。アクセス権限のないタブにユーザがアクセスするのを防止するために、システム管理者が CMC タブへのアクセスを制限できます。

緊急の場合、または CMC タブへのアクセス設定問題の解決のために、CMC タブへのアクセス制限を削除できます (たとえば、委任管理者が重要な CMC タブにアクセスできない場合)。

1. CMC にログオンします。
2. [アプリケーション] タブで、[セントラル管理コンソール] を右クリックして [*CMC タブアクセスの設定*] を選択します。
   [*CMC タブアクセス*] ダイアログボックスが表示されます。
3. CMC タブへのアクセスルールを設定します。
   - ユーザが権限を持つタブへのアクセスを制限するには、[制限付き] を選択します。
   - ユーザがすべてのタブにアクセスできるようにするには、[制限なし] を選択します。
4. 作業が完了したら、[保存して閉じる] をクリックします。

CMC タブへのアクセスがシステムに適用されます。

関連情報

CMC タブへのアクセス問題を解決する [676 ページ]

18.2.3.1.3.2.3 CMC タブへのアクセス問題を解決する

許可されていないアクセスを回避したり、CMC タブへのユーザの制限されたアクセスの問題を解決したりするために、ユーザの CMC タブへのアクセス権限の問題を解決できます。

1. 管理者として CMC にログオンします。

   > ⓘ 注記
   >
   > 問題を解決するタブへのアクセス権限があること、ユーザの [アクセス権を安全に変更する] 権限があることを確認します。

2. [ユーザとグループ] タブで主体を右クリックし、[*CMC タブ設定*] を選択します。
   [*CMC タブの設定*] ウィンドウが表示されます。
3. 有効な CMC タブへのアクセスを確認します。利用可能なタブへのアクセスを明示的に許可または拒否できます。

   CMC タブへのアクセスは継承されているが、有効なタブへのアクセスがユーザのニーズに合っていない場合は、以下のとおりです。

a. 選択した主体がメンバーとなっているすべてのユーザグループのリストを収集します。
b. ユーザがタブへのアクセスを継承するすべてのグループに対して、手順 1 ～ 3 を繰り返します。
c. 必要に応じて、主体レベルまたはグループレベルで CMC タブへのアクセスを修正します。

> ⓘ 注記
>
> グループレベルでこのタスクを実行すると、ユーザの CMC タブへのアクセスが [継承] に設定されている限り、このユーザグループのメンバーであるすべてのユーザに対する CMC タブへのアクセスおよび、このグループから継承されたユーザグループのメンバーであるすべてのユーザに影響があります。

4. 終了したら、[閉じる] をクリックします。

関連情報

他のユーザに対して CMC タブアクセスを管理する [672 ページ]
CMC タブへのアクセスの継承 [673 ページ]

18.2.3.2 BI ラウンチパッド設定の管理

ここでは、Fiori 対応 BI ラウンチパッドの以下の設定を管理する詳細な手順について説明します。

- BI ラウンチパッドの表示設定を変更します。
- BI ラウンチパッドへのログオン用に RESTful URL の詳細をセントラル管理コンソールで設定します。
- Fiori 対応 BI ラウンチパッドで [認証] タブおよび CMS の表示を設定します。
- BI ラウンチパッドで [管理者に連絡] オプションの電子メールリンクを設定します。

18.2.3.2.1 Fiori 対応 BI ラウンチパッドへのログオン用の RESTful URL の詳細の CMC での設定

インストールするか BI 4.2 SP4 にアップグレードした後、Fiori 対応 BI ラウンチパッドにユーザがログオンできるように、RESTful Web サービス URL を設定する必要があります。

RESTful Web サービス URL の詳細を CMC で設定するには、以下の手順を実行します。

1. 管理者として CMC にログオンします。
2. 管理 > アプリケーション > *RESTful Web* サービス > プロパティ に移動します。
3. WACS URL (WACS サーバがデプロイされている場所のホスト名または完全修飾名) を入力します。

18.2.3.2.2 Fiori 対応 BI ラウンチパッドで Web アシスタントを有効化するためのプロキシ設定の設定

BI 4.2 SP5 のインストールまたは BI 4.2 SP5 へのアップグレード後、ユーザが Fiori 対応 BI ラウンチパッドのアプリヘルプで Web アシスタントにアクセスできるように、プロキシ設定を設定する必要があります。

Fiori 対応 BI ラウンチパッドの Web アシスタント用のプロキシ設定を行うには、以下の手順を実行します。

前提条件:

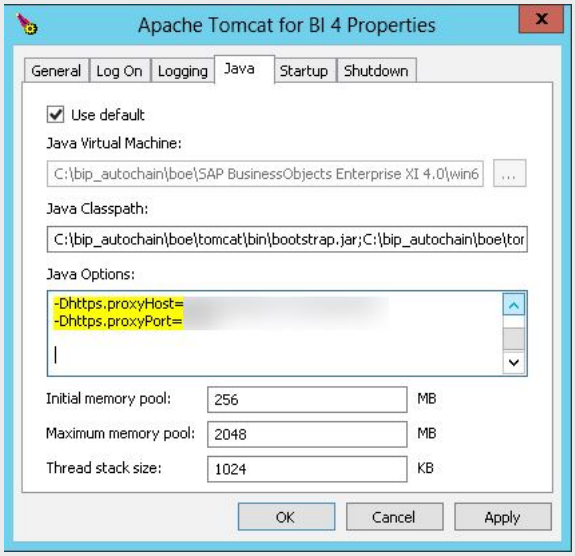
インターネットに接続します。

1. Web サーバのシステムプロパティに移動します。
2. `https.proxyHost` および `https.proxyPort` プロパティを追加します。

例

OS: Windows、Web サーバ: Tomcat 8.5

1. *Windows* > *Tomcat* に移動します。
   [*Apache Tomcat for BI 4 Properties*] ウィンドウが開きます。
2. [*Java*] タブを選択します。
3. Java オプションのフィールドで、以下のプロパティを一覧に追加します。
   ```
   -Dhttps.proxyHost=<proxy_host>
   -Dhttps.proxyPort=<proxy_port>
   ```
4. Tomcat を再起動します。



18.2.3.2.3 Fiori 対応 BI ラウンチパッドでの [管理者に問い合わせる] オプションの電子メールリンクの設定

Fiori 対応 BI ラウンチパッドで [管理者に問い合わせる] オプションの電子メールリンクを設定するには、以下の操作を実行します。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥` に移動します。

   BI プラットフォームに Tomcat バージョンがインストールされている場合は、次の場所にもアクセスできます。`C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEBINF¥config¥custom`
2. メモ帳を使用して新しいファイルを作成し、次の名前でファイルを保存します。FioriBI.properties。
3. ファイル内でプロパティ `admin.user.email=administrator@bilp.com` を変更し、管理者の電子メール ID を含めます。

18.2.3.2.4 Fiori 対応 BI ラウンチパッドでの [認証] タブおよび CMS の表示の設定

Fiori 対応 BI ラウンチパッドで [認証] タブおよび CMS の表示を設定するには、以下の操作を実行します。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom¥` に移動します。

   BI プラットフォームにインストールされた Tomcat を使用する場合は、次の場所にもアクセスできます。`C:¥Program Files (x86)¥SAP BusinessObjects¥Tomcat¥webapps¥BOE¥WEBINF¥config¥custom`
2. メモ帳を使用して新しいファイルを作成し、次の名前でファイルを保存します。FioriBI.properties。
3. BI ラウンチパッドログオン画面に認証オプションを含めるには、次を追加します。`authentication.visible=true`。

   <authentication> をデフォルトの認証タイプである"secEnterprise, secLDAP, secWinAD, secSAPR3" と置き換えます。
4. デフォルトの認証タイプを変更するには、次を追加します。`authentication.default=<authentication>`。
5. BI ラウンチパッドのログオン画面に CMS 名のプロンプトを表示するには、次を追加します。`cms.visible=true`。
6. ファイルを保存して閉じます。
7. Web アプリケーションサーバを再起動します。

18.2.3.2.5 BI ラウンチパッドの表示設定を変更する

1. CMC の [アプリケーション] エリアに移動し、[*BI ラウンチパッド*] をダブルクリックします。[*BI ラウンチパッドのプロパティ*] ダイアログボックスが表示されます。
2. スケジュールのフィルタを有効化するには、[*[スケジュール] ページに [フィルタ] タブを表示する*] チェックボックスを選択します。

   この設定によって、ユーザが Crystal レポートをスケジュールするときに、レコード選択式やグループ選択式を入力できるかどうかを制御できます。
3. 保存して閉じるをクリックします。

18.2.3.3 Web Intelligence の設定の管理

Web Intelligence ドキュメントでユーザがアクセスできる機能を制御するには、Web Intelligence アプリケーションのプロパティを設定します。

18.2.3.3.1 Web Intelligence の表示設定を変更する

1. CMC の [アプリケーション] エリアに移動し、[*Web Intelligence*] を選択します。
2. 管理 > プロパティ をクリックします。
   [プロパティ] ダイアログボックスが表示されます。
3. 次の表示オプションをすべて定義します。

オプション	説明
変更データ表示オプション > ディメンションと詳細	このエリアのオプションを使用して、レポート内での追加されたデータの表示方法を定義します。フォントスタイル、テキスト色、および背景色を変更します。セルのプレビューに変更が自動的に表示されます。完了したら [*OK*] をクリックします。
変更データ表示オプション > 変動値 (数値メジャー)	このエリアのオプションを使用して、ページ見出しの表示を変更および書式設定します。フォントスタイル、テキスト色、および背景色を変更します。セルのプレビューに変更が自動的に表示されます。完了したら [*OK*] をクリックします。
埋め込みイメージのプロパティ	埋め込みイメージの最大サイズを入力します。
地理マップのサポート	Web Intelligence での地理マップのサポートを有効または無効にします。
クイック表示モードのプロパティ	最大垂直レコード、最大水平レコード、ページの最小幅、ページの最小の高さ、右の余白値、および下の余白値を入力します。
自動保存設定	ドキュメントを自動保存する間隔を設定します。この間隔は、ドキュメントが手動または自動で保存されるごとにリセットされます。また、ドキュメントを手動で閉じると、自動保存されたドキュメントも削除されます。
自動更新	Web Intelligence ドキュメントプロパティの [自動最新表示] を選択すると、Web Intelligence ドキュメントの自動最新表示が有効になります。 詳細については、*SAP BusinessObjects Web Intelligence* ユーザガイドを参照してください。
自動結合	Web Intelligence ドキュメントプロパティの [ディメンションの自動結合] を選択すると、ディメンションの自動結合が有効になります。 詳細については、*SAP BusinessObjects Web Intelligence* ユーザガイドを参照してください。
起動時の自動ドキュメント最新表示セキュリティ権限設定	Web Intelligence ドキュメントプロパティで [起動時に最新表示] を有効にせず、Web Intelligence のドキュメントを開く際に自動でドキュメントを最新表示するには、このオプションをクリアします。このオプションを選択すると、セキュリティ権限 [ドキュメント - 起動時の自動最新表示を無効にする] が選択されます。
Smart View	このオプションは、ユーザが Web Intelligence でドキュメントを開く際に、表示するドキュメントバージョンを指定します。

オプション	説明
	• 最新のインスタンスを表示 オブジェクトの最新のインスタンスが開きます。たとえば、ドキュメントが毎時最新表示するようにスケジュールされていて、5 時間前にドキュメントを最終保存して閉じた場合、最新のインスタンスが開きます。 • オブジェクトの表示 スケジュールされた最新表示が実行されているかにかかわらず、ドキュメントが前回保存時と同じ状態で開きます。
JavaScript	ここでの選択は、Web Intelligence ドキュメントの [コンテンツを HTML として表示] または [コンテンツをハイパーリンクとして表示] が指定されているセルのレンダリングを定義します。 • *JavaScript を無効にし、ハイパーリンクと Web Intelligence で使用される HTML エレメントのみを有効にする* このデフォルトのオプションでは、ハイパーリンクおよび Web Intelligence の機能に必要な限定された HTML 要素のセットが有効になります。JavaScript およびその他の HTML 要素はドキュメントから削除されます。 • *[許可される HTML 要素] ページで定義された HTML 要素のみを有効にする* このオプションでは、[*権限のある HTML 要素*] ページで指定した HTML 要素および属性のみが有効になります。 • *JavaScript、HTML 要素、およびハイパーリンクを有効にする* このオプションでは、すべての JavaScript、HTML 要素、およびハイパーリンクが有効になります。 オプションを変更した場合は常に、Web Intelligence での変更を確認するために、アプリケーションからログオフしてからログオンし直してください。 ⚠ 警告 • Web Intelligence では、式の能力によって、ドキュメントセル内の埋め込み JavaScript/HTML コードが有効化されます。 このコードは、セントラル管理コンソールで有効化または無効化できます。ただし、JavaScript、HTML、およびハイパーリンクを承認することで、クロスサイトスクリプティングにさらされるリスクを認識することになります。クロスサイトスクリプティングによって、攻撃者が Web サイトを変更したり、他のシステムでコードを実行したりできるようになります。この脆弱性は、スクリプトの実行時にインターネットブラウザなどの製品に影響します。クロスサイトスクリプティング攻撃の大部分は、ターゲットシステムでの安全でないプログラミングに起因します。 • コードは、*BI 管理スタジオ* > *アプリケーション* > *HTML 要素* で HTML タグと属性を承認することで微調整できます。 ただし、SAP はこのコードの互換性と、考えられる副次的な影響について責任を負いません。たとえば、ブラウザ更新、JavaScript バージョンサポート、または Web ページでコードを動的に埋め込む方法により、コードによっては一部の調整が必要になることがあります。このコードには、新しいコンテキストで実行するために調整が必要になる場合があります。
新しいドキュメントのコンテンツ配置	これらのオプションを使用して、新しいドキュメントのコンテンツを右から左、左から右に配置する必要があるのか、またはユーザの優先表示ロケールと製品ロケールに依存する必要があるのかを定義します。

オプション	説明
フィーチャトグル	このテキストフィールドを使用してトグルを入力し、プレビュー機能を有効にします。これらのトグルを SAP ノートで使用して、デフォルトの動作を変更することもできます。このトグルのリストは、JSON 形式一覧として入力する必要があります。

4. [保存して閉じる] をクリックします。

> ⓘ 注記
>
> デフォルトの表示変数に戻す場合は、[リセット] をクリックします。

18.2.3.3.2 カスタム要素サービス

カスタム要素は、レンダリングが Web Intelligence によってサードパーティサービスに依頼されるビジュアライゼーションです。

Web Intelligence ドキュメントで、カスタム要素は他のレポート要素 (チャート、テーブルなど) と同様に統合および表示されます。エンドユーザが Web Intelligence ドキュメントでカスタム要素を視覚化できるように、カスタム要素サービスを CMC で事前に設定しておく必要があります。

データは BOE サーバとカスタム要素サードパーティサーバ間で転送されるため、カスタム要素サーバをイントラネット上にデプロイすることをお奨めします。それが不可能な場合は、カスタム要素サーバへのアクセスに HTTPS のみを使用することをお奨めします。

> ⚠ 警告
>
> デプロイする [カスタム要素] サービスによってコードが Web Intelligence に追加され、クロスサイトスクリプティングのような潜在的セキュリティ問題の原因となる可能性があります。クロスサイトスクリプティングによって、攻撃者はコードを実行し、スクリプトを他のユーザのコンピュータで実行することができます。[カスタム要素] サービスをデプロイする前に、セキュリティ警告によって明確な同意が求められます。[カスタム要素] サービスをデプロイするには、この同意が必須です。

移行

別の CMS に Web Intelligence ドキュメントを移行する場合は、このドキュメント内のコンテンツの作成に使用されたカスタム要素サービスを新しい CMS に同名で再作成する必要があります。新しい CMS にカスタム要素サービスを (同名で) 再作成しなかった場合、移行後のドキュメント内のカスタム要素は変更不可になります。

18.2.3.3.2.1 カスタム要素サービスを追加する

エンドユーザがカスタム要素を使用できるようにするには、レンダリングを処理するサードパーティサービスを管理者が事前に指定しておく必要があります。デフォルトでは、カスタム要素サービスは有効化されていません。この設定はオプションであり、CMC で有効化する必要があります。

カスタムサービス URL を信頼できる URL の一覧に追加しておきます。まだ追加していない場合は、信頼できる URL を許可された URL の一覧に追加する [688 ページ]の節を確認してください。

1. セントラル管理コンソール (CMC) を開きます。
2. [アプリケーション] をクリックします。
3. [*Web Intelligence*] を右クリックします。
4. [プロパティ] をクリックします。
5. [カスタム要素] をクリックします。
6. [サービスの追加] をクリックします。
7. サービスに名前を付けます。

   ⚠ 警告

   サービスの名称は Web Intelligence クライアントと同じ形式で表示され、一意性を保つ必要があります。既存のサービス名を再利用することはできません。サービス名を変更すると、そのサービスによって Web Intelligence ドキュメントに作成されたカスタム要素を変更できなくなります。

8. ポート番号を含む URL を入力します。
9. [テスト] をクリックします。
10. [メディアタイプ] を選択します。

    Web Intelligence で利用可能なメディアタイプは、HTML またはビットマップのいずれかです。推奨されるメディアタイプは、Web Intelligence クライアントでの対話性と優れたユーザエクスペリエンスを実現する HTML (text/html) です。ビットマップメディアタイプとしては、.PNG (image/png)、.JPG (image/JPG)、または .GIF (image/gif) を指定することができます。

11. [画像 *DPI*] を入力します。

    ⓘ 注記

    これは、サービスによって生成されるビットマップ画像の解像度です。カスタム要素がピクチャとして表される PDF または Excel ファイルとして Web Intelligence レポートを公開する場合は、ビットマップ形式を使用する必要があります。ビットマップ形式を使用せずに公開した場合、必要なカスタム要素ではなく空のブロックが表示されます。

12. [*OK*] をクリックします。

    ⓘ 注記

    同時に複数のカスタム要素サービスを使用することができます。1 つのサービスで複数のカスタム要素を提供することができます。

関連情報

URL の許可 [687 ページ]

18.2.3.3.3 データプロバイダ最新表示の並列処理

データプロバイダ最新表示の並列を使用すると、複数のデータプロバイダを扱う Web Intelligence ドキュメントのデータ最新表示パフォーマンスが向上します。

クエリの最新表示を並列で行う場合、Web Intelligence はすべてのデータプロバイダを複数のスレッドに分散させます。この機能はデフォルトで有効化されており、Web Intelligence は 64 クエリまで並列に最新表示にすることができます。リレーショナル、OLAP、および BICS 接続に基づくデータプロバイダ、さらに個人用データプロバイダがサポートされています (テキストファイル、FHSQL)。

> **⚠ 制限**
>
> Excel データプロバイダはサポートされていません。

Web Intelligence が実行されているハードウェアがこのような負荷に対応できない場合は、セントラル管理コンソールでこの値を小さくすることができます。最適なパフォーマンスを発揮するように、ハードウェアに十分なコアがあることを確認してください。

次の 2 つのグローバルパラメータがセントラル管理コンソールで利用できます。

- ドキュメント別の最大並列クエリ数: Web Intelligence がドキュメントごとに並列に最新表示できるデータプロバイダの最大数を設定します。デフォルト値は 64 に設定されます。
- スケジュールに対して並列クエリを有効にする: ドキュメントのスケジュール時に並列クエリ処理を有効または無効にします。このオプションはデフォルトで有効になっています。

また、並列に実行できるクエリの数を指定するパラメータで各データベース接続を微調整することもお奨めします。最大並列クエリ数と呼ばれるこのパラメータは、次の場所で利用できます。

- OLAP および BICS 接続のセントラル管理コンソールまたはインフォメーションデザインツール
- リレーショナル接続のインフォメーションデザインツールまたはユニバースデザインツール

接続ごとに、並列に最新表示できるデータプロバイダの数はデフォルトで 4 に設定されています。データベース管理者は、データベースのハードウェアに基づいてこの値を変更することができます。ただし、テキストファイルの場合は、デフォルト値は 1 に設定されています。

例

たとえば、デフォルト値がすべて保持されていれば、各接続は最大で 4 つの並列最新表示ジョブをサポートします。

接続	最新表示するデータプロバイダの数
2 OLAP 接続	6 (接続 1 で 5、接続 2 で 1)

接続	最新表示するデータプロバイダの数
1 リレーショナル接続	2
1 BICS 接続	2
個人用データプロバイダからの Excel ファイル	2

データプロバイダ最新表示の並列機能でサポートされていないため、Excel ファイルは両方とも順番に最新表示されます。

最初の OLAP 接続のデータプロバイダのうち 4 つは、スレッド 1、2、3、および 4 で並列に最新表示されます。5 つ目はキューに格納され、(任意の接続の) データプロバイダの 1 つが最新表示された後に処理され、その一方で 2 つ目の OLAP 接続からのものは異なる接続からのものであるためスレッド 5 で最新表示されます。

リレーショナル接続と BICS 接続の両方の 4 つのデータプロバイダは、スレッド 5、6、7、および 8 で並列に最新表示されます。

> ⓘ 注記
>
> 同じタイプのデータプロバイダの数が定義値よりも多い場合は、必ずキューに格納され、その他のデータプロバイダの処理が終了してから処理されます。

関連情報

ドキュメント別に並列に最新表示されるデータプロバイダの数を変更する [685 ページ]
特定の OLAP 接続の並列に最新表示されるデータプロバイダの数を変更する [686 ページ]

18.2.3.3.3.1 ドキュメント別に並列に最新表示されるデータプロバイダの数を変更する

1. CMC ホーム画面で、[サーバ] をクリックします。
2. [*Web Intelligence* サービス] をクリックします。
3. [*Web Intelligence Processing Server*] を右クリックし、[プロパティ] をクリックします。
4. [最大並列クエリ数] 入力項目に数を入力します。
   指定できる値の範囲は、0 ～ 64 です。

   > ⓘ 注記
   >
   > 「0」を入力すると、データプロバイダ最新表示の並列機能は無効になります。

18.2.3.3.3.2 スケジュールに対して並列クエリ処理を無効にする

1. CMC ホーム画面で、[サーバ] をクリックします。
2. [*Web Intelligence* サービス] をクリックします。
3. [*Web Intelligence Processing Server*] を右クリックし、[プロパティ] をクリックします。
4. [スケジュールに対して並列クエリを有効にする] を無効にします。

18.2.3.3.3.3 特定の OLAP 接続の並列に最新表示されるデータプロバイダの数を変更する

1. ホーム画面で、[*OLAP* 接続] をクリックします。
2. 設定する接続を参照して右クリックします。
3. 整理 > 編集 を選択します。
4. [最大並列クエリ数] 入力項目に数を入力します。
   指定できる値の範囲は、1 ～ 64 です。

   > **注記**
   >
   > 「1」を入力すると、データプロバイダは順番に最新表示されます。

18.2.3.3.4 CSV エクスポートに対する保護

Web Intelligence では、ドキュメントから生成された CSV ファイルを Microsoft Excel で開いた際のコマンドインジェクションを防止するためのセキュリティ対策が提供されます。この CSV エクスポートに対する保護を無効にすることができます。

デフォルトでは、Web Intelligence では CSV または CSV アーカイブへのエクスポート時に、以下の文字の前にスペースが追加されます。

- = (等号)
- + (プラス)
- - (マイナス)
- @ (アット)

スペースの追加により、これらの文字を含む値がコマンドとして実行されなくなり、システムでセキュリティに関する問題が発生することを回避できます。

関連情報

CSV エクスポートに対する保護を無効にする [687 ページ]

18.2.3.3.4.1 CSV エクスポートに対する保護を無効にする

Microsoft Excel でエクスポートされた CSV ファイルを開いた際のコマンドインジェクションを防止する、Web Intelligence のデフォルトセキュリティ対策を無効にするには、対応するレジストリキーを変更します。

セキュリティ対策を無効にするには、`EscapeCharactersForCSVExport` レジストリキーの値を false に設定します。デフォルトでは、このレジストリキーは存在せず、その値は true であるため、この値を false に設定するには、このレジストリキーを作成する必要があります。

変更は、Web Intelligence ユーザがアプリケーションを閉じてから再び開いたときに有効になります。

以下のようにレジストリキーを変更します。

- Windows の場合、サーバマシンおよびクライアントマシン上で、次のレジストリキーを false に設定します。`HKEY_LOCAL_MACHINE¥SOFTWARE¥SAP BusinessObjects¥Suite XI 4.0¥default¥WebIntelligence¥EscapeCharactersForCSVExport`。
- UNIX の場合、サーバマシン上の `$installdir/setup/boconfig.cfg` で、レジストリ宣言キー `HKEY_LOCAL_MACHINE¥SOFTWARE¥SAP BusinessObjects¥Suite XI 4.0¥default¥WebIntelligence¥EscapeCharactersForCSVExport` を false に設定します。

18.2.3.3.5 URL の許可

Web Intelligence では、以下について URL が使用されます。

- ドキュメント内のハイパーリンク
- プロンプトのヒントのハイパーリンク
- 背景画像
- OData データソース
- カスタム要素または外部拡張

これらの URL は、セキュリティ上の脅威を発生させる可能性があります。

管理者は、ユーザがセントラル管理コンソールで使用できる信頼できる URL の一覧を作成する必要があります。この一覧は、Web Intelligence でこれらの URL の使用を制御します。

18.2.3.3.5.1 信頼できる URL を許可された URL の一覧に追加する

Web Intelligence で、ドキュメントのハイパーリンクまたはプロンプトのヒント、背景画像、OData データソース、新しいカスタムサービスまたは外部拡張として URL を使用する場合は常に、最初に認証する必要があります。

1. セントラル管理コンソールのホーム画面で、[アプリケーション] をクリックします。
2. [*Web Intelligence*] を選択します。
3. コンテキストメニューで、プロパティを選択します。
4. 許可された *URL* カテゴリセクションを選択します。
5. 新しい *URL* を追加しますボタンをクリックして、信頼できる URL を追加します。
6. 許可された *URL* フィールドで、一意の URL とそのプロトコル、ホスト名、およびポートを指定します。

   > → ヒント
   >
   > * 文字を入力して、ハイパーリンク、背景画像、または OData データソースの任意の URL を認証できます。次に、リスクを受け入れるチェックボックスにチェックを付けて、潜在的なリスクを理解していることを確認し、すべての URL を有効化する必要があります。

7. 入力した URL が、プロキシを介してアクセス可能な拡張またはカスタム要素サービスへの URL である場合、この *URL* がプロキシを必要とするカスタム要素または拡張に使用されている場合は、そのサーバおよびポートを入力してくださいチェックボックスにチェックを付けて、このプロキシサーバとポートを設定できます。
8. [*OK*] をクリックします。

18.2.3.4 Crystal Reports 設定の管理

18.2.3.4.1 Crystal Reports での Smart View の有効化

1. CMC の [アプリケーション] エリアに移動し、[*Crystal Reports*] を選択します。
2. 管理 > プロパティ を選択します。
   [プロパティ] ダイアログボックスが表示されます。
3. [*BI* ラウンチパッド] を選択します。
4. 以下の表示オプションを定義します。

オプション	説明
Smart View	このオプションは、ユーザが Crystal レポートを開く際に、表示するドキュメントバージョンを指定します。 • 最新のインスタンスを表示 オブジェクトの最新の正常なインスタンスが開きます。たとえば、ドキュメントが毎時最新表示するようにスケジュールされていて、5 時間前にドキュメントを最終保存して閉じた場合、最新の正常なインスタンスが開きます。 • オブジェクトの表示 スケジュールされた最新表示が実行されているかにかかわらず、ドキュメントが前回保存時と同じ状態で開きます。

18.2.3.4.2 Crystal Reports for Enterprise に対する Java ユーザ関数ライブラリの有効化

Java ユーザ関数ライブラリ (UFL) が含まれたレポートを表示およびスケジュールすることができます。以下の手順に従います。

1. CMC にログオンします。
2. ドロップダウンリストから [アプリケーション] を選択します。
3. [*Crystal Reports* 設定] を選択します。
4. 左側のパネルの [プロパティ] の下で、[*Crystal Reports for Enterprise*] を選択します。
5. [新規追加] オプションを選択し、次のプロパティを入力します。

プロパティ	値	追加情報
classpath	Java UFL へのクラスパス。	• セミコロンは複数の jar の区切りとして使用します。 • 代わりに、ダブルスラッシュ (¥¥) を使用するか、フォワードスラッシュ (/) を使用する必要があります。 • 例: C:¥¥Program Files (x86)¥¥SAP BusinessObjects¥¥SAP BusinessObjects Enterprise XI 4.0¥¥java¥¥lib¥¥MyFirstUFL.jar
ExternalFunctionLibraryClassNames.classname	UFL の完全修飾名。	例: samples.ufl.InternationalizationLibrary

6. Crystal Reports に関連するサービスを再起動します。
これで、ワークフローの表示とスケジューリングを実行することができます。

18.2.3.4.3 Crystal Reports for Enterprise に対する .NET/COM ユーザ関数ライブラリの有効化

.NET/COM ユーザ関数ライブラリ (UFL) が含まれたレポートを表示およびスケジュールすることができます。以下の手順に従います。

1. 64 ビットバージョンの .Net UFL を `<Install Directory>¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64` にコピーします。

   > ⓘ 注記
   >
   > Crystal Reports for Enterprise デザイナは 64 ビットであるため、64 ビットの .NET UFL を必要とするのに対して、Business Intelligence プラットフォーム上の Crystal Reports for Enterprise サービスは 64 ビットであるため、64 ビットの .NET UFL を必要とします。

2. "regasm <dll>" および "gacutil /if <dll>" を使用して、64 ビットの dll を登録および GAC します。
3. CMC にログオンします。
4. ドロップダウンリストから [アプリケーション] を選択します。
5. [*Crystal Reports* 設定] を選択します。
6. 左側のパネルの [プロパティ] の下で、[*Crystal Reports for Enterprise*] を選択します。
7. [新規追加] オプションを選択し、次のプロパティを入力します。

カテゴリ	プロパティ	値
この列は空白のままにします。	NonJavaExternalFunctionLibraries.managerDirectory	64 ビットの UFL ファイルのパス。 • ダブルスラッシュ (¥¥) を使用するか、代わりにフォワードスラッシュ (/) を使用する必要があります。 • 例: C:¥¥Program Files (x86)¥¥SAP BusinessObjects¥¥SAP BusinessObjects Enterprise XI 4.0¥¥win64_x64).

8. Crystal Reports に関連するサービスを再起動します。
   これで、ワークフローの表示とスケジューリングを実行することができます。

18.2.3.5 アラート設定の管理

*BI プラットフォーム*の CMC の [アプリケーション] エリアで、アラートのシステムレベルの設定を指定できます。

アラート アプリケーションについては、システムユーザがアラートにアクセスする方法を、次の手順を実行して制御および定義できます。

- アラート購読者の [マイアラート] フォルダを有効にする
- 電子メールで送信されるアラートメッセージを有効にして書式設定する
- システムのアラート数の制限を設定する

- アラートメッセージの有効期限の設定

関連情報

アプリケーションに対するユーザアクセス権の設定 [665 ページ]

18.2.3.5.1 アラートの出力先プロパティを変更する

1. CMC の [アプリケーション] エリアで、[アラートアプリケーション] をダブルクリックします。
2. 管理 > プロパティ をクリックします。
   [アラート] ダイアログボックスが表示されます。
3. (必須) 次の操作のいずれかを実行します。
   - アラート購読者が BI ラウンチパッドの [マイアラート] で通知を受信できるようにする場合は、[マイアラートの有効化] を選択します。
   - アラート購読者が電子メールで通知を受信できるようにする場合は、[電子メールを有効にする] を選択します。
     アラートのグローバル電子メールオプションが表示されます。
4. [電子メールを有効にする] を選択した場合は、次の操作を実行します。
   - [差出人] ボックスに、アラート通知の送信元電子メールアドレスを入力します。
     購読者はこの電子メールアドレスからアラート電子メールを受信します。システムが認識している有効な電子メールアドレスを使用します。
   - [宛先] ボックスに、アラート受信者の電子メールアドレスを入力します。
     デフォルトでは、すべてのシステムアラートがこの電子メールアドレスに送信されます。

     > → ヒント
     >
     > 電子メールアドレスまたは受信者を指定しないでください。[*%SI_EMAIL_ADDRESS%*] プレースホルダを使用してください。

   - [*CC*] ボックスに、アラートのカーボンコピーを受信する各受信者の電子メールアドレスを入力します。
   - [件名] ボックスに、アラートを含む電子メールに使用されるデフォルトの表題を入力します。
   - [メッセージ] ボックスに、アラートを含む電子メールに記載されるデフォルトのメッセージを入力します。
   - アラートを含む電子メールにデフォルトでファイルが添付されるようにするには、[添付ファイルの追加] を選択します。
     たとえば、トリガされたアラートに関連付けられた Crystal レポートを含める場合は、このオプションを選択します。
   - [添付ファイルの追加] を選択した場合、[ファイル名] で [自動生成される名前] または [指定の名前] を選択して、電子メールの添付ファイルに名前を付ける方法を指定します。
5. [保存して閉じる] をクリックします。

関連情報

アプリケーションに対するユーザアクセス権の設定 [665 ページ]
アラート設定の管理 [690 ページ]

18.2.3.5.2 アラートのデフォルトプロパティを変更する

1. CMC の [アプリケーション] エリアに移動し、[アラートアプリケーション] を選択します。
2. 管理 > プロパティ > デフォルト設定 をクリックします。
3. 以下のプロパティに適切な値を設定します。

オプション	説明
有効期限	アラートメッセージが削除されるまでにシステムで保持される期間を指定します。
アラートメッセージの最大数	システムでサポートされるアラートメッセージの最大数を指定します。しきい値に達すると、システムによって、アラートメッセージの 20 パーセントが古いメッセージから順に削除されます。

4. [保存して閉じる]をクリックします。

関連情報

アラート設定の管理 [690 ページ]

18.2.3.6 BI Commentary アプリケーション設定の管理

BI Commentary は、CMC に導入されているアプリケーションです。ドキュメントユーザは、指定されたドキュメントで使用できるデータ/統計に関するコメントを作成することによって、相互にコラボレーションすることができます。

BI Commentary で、ユーザはレポート内のデータ/統計に関するコメントを投稿できます。

→ 推奨事項

デフォルトで、BI Commentary のテーブルは監査データベースに作成されて保持されます。

ⓘ 注記

Windows 以外のシステム上で監査データベースで BI Commentary を使用するには、データアクセスガイドを参照して、ODBC ドライバを設定します。

ただし、SAP は BI Commentary アプリケーションのコメントを保存する新しいデータベースを設定することを推奨します。BI Commentary がサポートされているデータベースは、監査がサポートされているデータベ

ースと同じです。BI Commentary がサポートされているデータベースおよび対応する認定済み jdbc.jar には以下を含みます。

- IBM DB2 Workgroup Edition db2jcc4.jar
- Microsoft SQL Server - sqljdbc4.jar
- MySQL - com.mysql.jdbc_5.1.5.jar
- Oracle - ojdbc6.jar
- SAP HANA - ngdbc.jar
- Sybase Adaptive Server Enterprise - jconn4.jar
- Sybase SQL Anywhere - jconn4.jar

> **注記**
>
> 監査データベースまたはその他のサポートされているデータベースで BI Commentary を設定することを選択するかどうかに関わらず、BI Commentary を MySQL データベースで使用するには次の場所に MySQL jdbc jar を置いておく必要があります。`<INSTALL_DIR¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥services¥BICommentaryService¥lib>`.
>
> IBM DB2 で BI Commentary を設定する場合は、システムで一時表スペースのページサイズ、8K、16K、または 32K が必要です。デフォルトでは、ページサイズは、4K です。

注記

デフォルトで監査テーブルが設定/有効化されていない場合、BI Commentary 用の新しいデータベースを手動で設定しない限り、BI Commentary は動作しません。

監査データベースで BI Commentary を設定し、監査データベースを削除した場合、監査データベースに格納されたすべてのコメントも削除されます。

監査データベースは、ODBC またはネイティブデータベースいずれかのドライバタイプを使用します。新しい Commentary データベースを設定するには、JDBC ドライバが必要です。

注記

コメントのサイズは、UTF-8 文字 2000 バイトまたは UTF-16 文字 666 バイトに制限されています。

注記

フェデレーションツールを使用してコメントを移行することはできません。

注記

BI Commentary は MaxDB 接続ではサポートされていません。

注記

ユーザが作成した Commentary のエントリを削除するには、以下のクエリを使用します。

```
DELETE from dba.COMMENTARY_MASTER where UserName ='<User Name>'
```

18.2.3.6.1 新しい BI Commentary データベースの設定

JDBC の接続を作成しておきます。

> ⓘ 注記
>
> 新しい BI Commentary データベースを設定する場合、Adaptive Processing Server に含まれている Commentary サービスにより Commentary 情報がデータベースに書き込まれます。Commentary サービスが実行されているクラスタ内の各マシンで以下の手順を実行してください。

新しい JDBC 接続を作成するには、以下の手順を実行します。

1. 設定するデータベースの JDBC ドライバ jar を以下の場所に配置します。`<INSTALL_DIR¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥services¥BICommentaryService¥lib>`

   > ⓘ 注記
   >
   > SAP BusinessObjects Business Intelligence プラットフォーム 4.2 サポートパッケージ 2 にアップグレードするときに、以前のバージョンの BI Commentary に対する新しいデータベースをすでに設定してある場合には、データベースドライバファイルを `<INSTALL_DIR¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib¥external>` の 'jdbc' フォルダから、`<INSTALL_DIR¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥services¥BICommentaryService¥lib>` に移動する必要があります。

2. SIA を再起動します。

BI Commentary 用の新しいデータベースを設定するには、以下の手順を実行します。

1. CMC にログオンします。
2. CMC のホームページで、ドロップダウンメニューから [アプリケーション] を選択します。
3. アプリケーション名リストから *BI Commentary* アプリケーションを選択します。

   [*BI Commentary*] ポップアップウィンドウが表示されます。デフォルトで、[監査データベースを使用] ラジオボタンが選択されています。
4. [その他のサポートされているデータベースを使用] ラジオボタンを選択します。
5. [*BI Commentary* データベースの設定] ペインに、タイプ、データベース名、ホスト、ポート、ユーザ名、およびパスワードを入力します。
6. [保存して閉じる] を選択します。
7. APS を再起動します。

   BI Commentary データベースの設定に対する変更は、Adaptive Processing Server (APS) の再起動後でのみ有効になります。

   [接続テスト] を選択して、接続を検証できます。

   > ⓘ 注記
   >
   > SAP BusinessObjects Business Intelligence プラットフォーム 4.3 サポートパッケージ 3 にアップグレードし、以前のバージョンの JDBC 向けに BI Commentary のデータベースをすでに設定している場合、[接続テスト]、[保存して閉じる]、または [保存] を選択すると、パスワードフィールドが空になります。

以下よりも古いコメントをすべて削除チェックボックスを有効にし、日数を指定することによって、古いコメントを削除またはクリーンアップすることができます。

> ⓘ 注記
>
> 変更を反映するには、BI Commentary サービスをホストしているすべての APS サーバを再起動する必要があります。

これで、BI Commentary アプリケーションのコメントを保存する新しいデータベースが設定されました。

18.2.3.7 BI 管理スタジオプリケーション設定の管理

> ⓘ 注記
>
> BI 管理スタジオにアクセスするには、管理者グループに属している必要があります。

特定のアクセス権 ([*BI 管理コックピットへのアクセスを許可する*]、[モニタリングへのアクセスを許可する]、[*Visual Difference へのアクセスを許可する*] など) を拒否した場合、BI 管理スタジオの特定のアプリケーションにアクセスできない場合があります。

Specific Rights for BI Admin Studio	Implicit Value					
Allow access to BI Admin Cockpit	Granted					
Allow access to Monitoring	Granted					
Allow access to Visual Difference	Granted					
Visual Difference - Create comparison	Granted					
Visual Difference - Delete comparison	Granted					
Visual Difference - Rerun comparison	Granted					
Visual Difference - View comparison	Granted					

Visual Difference 権限が拒否された場合、VD アプリケーションの使用を制限することもできます。

18.2.3.8 コラボレーションアプリケーション統合の管理

このガイドは、BI プラットフォームと SAP Jam コラボレーションアプリケーションを統合する BI プラットフォーム管理者を対象としています。

BI プラットフォームのセントラル管理コンソール (CMC) のアプリケーション領域を使用して、コラボレーションを有効化して設定できます

コラボレーションアプリケーションのエンタープライズエージェントで、次の追加の設定をする必要があります。

- サービスプロバイダとの HTTPS 接続を確立する
- 認証用の前提条件を満たす

SAP Jam を設定すると、コラボレーションアプリケーションのフィードが BI ラウンチパッドで使用できるようになります。

SAP Jam では、Microsoft Internet Explorer 11 はサポートされていません。

18.2.3.8.1 コラボレーションの前提条件

BI プラットフォームとコラボレーションアプリケーションを統合するには、コラボレーションの前提条件を満たしている必要があります。

- BI プラットフォームに少なくとも 1 つの Central Management Server (CMS) をインストールする必要があります。
- セントラル管理コンソール (CMC) で、コラボレーションアプリケーション (SAP Jam) を設定する必要があります。
- コラボレーションアプリケーション (SAP Jam) のエンタープライズ組織を定義する必要があります。
- SAP Jam のユーザは、エンタープライズ組織に所属する必要があります。
- オンプレミス LDAP/AD ディレクトリサービスを使用するユーザをプロビジョニングするために、SAP Jam エンタープライズエージェントが必要です。

18.2.3.8.2 BI プラットフォーム設定

18.2.3.8.2.1 コラボレーション設定オプション

コラボレーションオプションは、BI プラットフォームのセントラル管理コンソール (CMC) の [プロパティ: コラボレーション] ダイアログボックスに表示されます。

プロパティ: コラボレーションダイアログボックスにアクセスするには、CMC のアプリケーションタブでコラボレーションをクリックして、管理 > プロパティ を選択します。

オプション	説明
コラボレーションを有効にする	このチェックボックスを選択し、[*SAP Jam*] を選択します。
接続 *URL*	コラボレーションアプリケーションへの URL を入力します。
プロバイダ *ID* の一意の *ID*	BI プラットフォームデプロイメントのための一意の値を入力します。 この値は、コラボレーションアプリケーションの管理コンソールで統合を設定するために使用される証明書に関連付ける必要があります。シングルサインオンの ID をアサートするアプリケーションは、管理 OAuth アプリケーションとして設定する必要があります。
ID プロバイダの *Base64* 証明書	生成をクリックすると、このボックスに証明書が作成されます。この証明書をコラボレーションアプリケーションの管理コンソールで使用して、OAuth コンシューマキーを生成します。 この証明書によって、コラボレーションアプリケーションと BI プラットフォームとの信頼関係を確立します。外部 ID プロバイダ自体は、X509 証明書で識別されます。この証明書は、すべての ID アサーションの署名に使用されます。証明書は Base64 でエンコードする必要があります。
OAuth コンシューマキー	コラボレーションアプリケーションの管理コンソールから生成された OAuth コンシューマキーを入力します。

オプション	説明	
プロキシを使用した接続	このチェックボックスを選択してプロキシ経由での接続を有効にし、*HTTP プロキシホスト*ボックスおよびポートボックスにプロキシホストに関する情報を入力します。 コラボレーションアプリケーションのサーバから会社のネットワークへのインバウンド接続を許可するには、DMZ 内にリバースプロキシを設定する必要があります。 SSL 証明書プロバイダの信頼できる証明書をリバースプロキシに追加するには、リバースプロキシのドメイン名またはサブドメイン名を設定する必要があります。	
	HTTP プロキシホスト	リバースプロキシ設定で、コラボレーションアプリケーションにアクセスできる外部アドレスを入力します。たとえば、`https://<ReverseProxy>/` を使用します。ここでの `<ReverseProxy>` は、リバースプロキシのドメイン名またはサブドメイン名です。 コラボレーションアプリケーションはこのアドレスを使用して、BI プラットフォームに情報を送信します。リバースプロキシはこのアドレスを使用して、コラボレーションアプリケーションから取得した情報を、コラボレーションアプリケーションのエンタープライズエージェントを含むマシンにリダイレクトします。
	ポート	コラボレーションアプリケーションのエンタープライズエージェントは、ポート 8443 から受信するように設定します。

18.2.3.8.2.2 CMC でのコラボレーションの有効化と設定

このタスクでは、コラボレーションアプリケーション (SAP Jam) の管理コンソールへの有効な接続が必要です。コンソールのセキュリティ詳細情報を渡したり取得したりする必要があります。

セキュリティ上の理由から、以下のデフォルトアカウントは、SAP Jam へのコンテンツの送信やスケジュールを行うことはできません。

- Guest
- SMAdmin
- Administrator
- WaaWSServletPrincipal

1. BI プラットフォームのセントラル管理コンソール (CMC) で、[アプリケーション] エリアに移動し、[コラボレーション] をダブルクリックします。
2. In the *Properties:*[プロパティ: コラボレーション] ダイアログボックスで、[コラボレーションを有効にする] チェックボックスを選択し、[*SAP Jam*] を選択します。
3. 接続 *URL* ボックスに、コラボレーションアプリケーションの URL を入力します。
4. プロバイダ *ID* の一意の *ID* ボックスに、BI プラットフォームデプロイメントに対して一意である ID プロバイダ値を入力します。

   ID プロバイダ値を書き留めます。後でコラボレーションアプリケーションの設定に使用します。
5. [生成] (または、以前に証明書を作成したことがある場合は [再生成]) をクリックします。
   *ID プロバイダの Base64 証明書*ボックスに証明書が表示されます。コラボレーションアプリケーションの設定に証明書を使用します。

6. *OAuth* コンシューマキーボックスに、有効な OAuth コンシューマキーを入力します。
7. プロキシを経由して SAP Jam を実行しているサーバに接続している場合は、以下のアクションを実行します。
   a. [プロキシを使用した接続] チェックボックスを選択します。
   b. *HTTP* プロキシホストボックスに、サーバのプロキシホスト名を入力します。
   c. ポートボックスに、サーバのポート番号を入力します。
8. 保存して閉じるをクリックします。

18.2.3.8.3 SAP Jam 設定

18.2.3.8.3.1 SAP に対する新しい SAML 信頼済み IDP の登録

BI ラウンチパッド内のユーザの Enterprise 電子メールアドレスに対応する一意の電子メールアドレスとともに、各ユーザを登録する必要があります。 この電子メールアドレスによって、BI プラットフォームと SAP の間がマップされます。

新しい SAML 信頼済み IDP を登録するには、次の条件を満たす必要があります。

- SAP に会社を追加して設定する必要があります。
- SAP 内の会社に関連付けられた有効な SAP ユーザアカウントが必要です。
- SAP 内の会社の会社管理権限と、BI プラットフォームおよび BI ラウンチパッドの完全な管理者権限が必要です。
- BI ラウンチパッドを OAuth クライアントとして登録する必要があります。OAuth クライアントは、SAP 内でラウンチパッドの代表として動作します。

SAP Jam では、Microsoft Internet Explorer 11 はサポートされていません。

1. BI プラットフォームのセントラル管理コンソール (CMC) の右上隅で、管理者を選択し、管理を選択します。
   SAP ライセンスを含む、会社に関する情報が表示されます。 この情報を記録またはメモしてください。
2. 管理メニューで *SAML 信頼済み ID* を選択し、アイデンティティプロバイダの登録をクリックします。
   BI ラウンチパッドで作成した IDP を登録する必要があります。
3. *IDP ID* ボックスに、SAP を BI プラットフォームで設定したときに作成された、一意の ID プロバイダの値を入力します。
   値がない場合は、外部アプリケーション管理者に問い合わせてください。
   たとえば、**`<CompanyName>_<SystemId>_<client>`** を入力します。
4. *Single Sign-On URL* ボックスに、SAP に直接アクセスする URL を入力します。
   SAP では、一意の ID プロバイダとのシングルサインオンに、この URL が使用されます。
5. *Single Log-Out URL* ボックスに、SAP からログオフした後に表示する URL を入力します。
   SAP では、一意の ID プロバイダからのシングルログアウトに、この URL が使用されます。
6. [*Default Name ID Format*] ボックスに、認証要求で使用する名前 ID 形式を入力します。
7. [*Default Name ID Policy SP Name Qualifier*] ボックスに、認証要求で使用する SP 名前修飾子を入力します。
8. *Allowed Assertion Scope* リストで *Users in my company* を選択します。
   このオプションでは、SAP が IDP からのアサーションを受け入れるユーザのセットを指定します。
9. *X509 証明書 (Base64)* ボックスに、SAP を BI プラットフォームで設定したときに生成された、Base64 証明書の値を入力します。

値がない場合は、外部アプリケーション管理者に問い合わせてください。

10. [登録] をクリックします。

18.2.3.8.3.2 SAP Jam に対する OAuth クライアントの作成

OAuth コンシューマキーを作成するには、次の条件を満たす必要があります。

- SAP Jam に会社を追加して設定する必要があります。
- SAP Jam 内の会社に関連付けられた有効な SAP Jam ユーザアカウントが必要です。
- SAP Jam 内の会社の会社管理権限と、BI プラットフォームおよび BI ラウンチパッドの完全な管理者権限が必要です。
- BI ラウンチパッドを SAP Jam に OAuth クライアントとして登録する必要があります。OAuth クライアントは、SAP Jam 内でラウンチパッドの代表として動作します。
- 各ユーザは、BI ラウンチパッド内のユーザの Enterprise 電子メールアドレスに対応する一意の電子メールアドレスとともに、SAP Jam に登録する必要があります。 この電子メールアドレスによって、BI プラットフォームと SAP Jam 間がマップされます。

SAP Jam では、Microsoft Internet Explorer 11 はサポートされていません。

1. SAP Jam で、右上隅の [*Administrator*] メニューから [*Admin*] を選択します。
   SAP Jam ライセンスを含む、会社に関する情報が表示されます。
2. 管理メニューから *OAuth クライアント*を選択し、*OAuth クライアントの追加*をクリックします。
3. [新しい *OAuth クライアントの登録*] ダイアログボックスの [名前] ボックスに、SAP Jam を BI プラットフォームで設定したときに作成された、一意の ID プロバイダを入力します。

   値がない場合は、外部アプリケーション管理者に問い合わせてください。

   ユーザの代わりに処理を行ったときに、SAP Jam に、入力する URL に対するハイパーリンクとしてアプリケーション名が表示されます。

   たとえば、**`<CompanyName>_<SystemId>_<Client>_<Application>`** を入力します。
4. *Integration URL* ボックスに、BI ラウンチパッドの URL を入力します。

   ユーザの代わりに処理を行ったときに、SAP Jam に、この URL に対するハイパーリンクとしてアプリケーション名が表示されます。
5. [*X509 証明書 (Base64)*] ボックスに、SAP Jam を BI プラットフォームで設定したときに生成された、Base64 証明書の値を入力します。

   値がない場合は、外部アプリケーション管理者に問い合わせてください。

   このボックスを空欄のままにすると、SAP Jam によってコンシューマシークレットが設定されます。
6. 保存をクリックします。

OAuth コンシューマキーが生成されます。 BI プラットフォーム管理者が使用できるように、OAuth コンシューマキー値を書きとめます。

18.2.3.9 SAP BusinessObjects Mobile でのプッシュ通知サービスの管理

SAP BusinessObjects Mobile サーバでは、SAP BusinessObjects Mobile アプリケーションユーザの iOS デバイスに通知がプッシュされます。通知は以下のシナリオでプッシュされます。

- ユーザのデバイスにダウンロードされた BI ドキュメントの更新または新しいインスタンスがサーバ上で利用可能になった場合。
- 新しいドキュメントがユーザの BI 受信ボックスに届いた場合。
- BI プラットフォームまたは BOE 管理者がメッセージを配信した場合。

通知は、Mobile サーバから Apple Push Notification Server (APNS) を通してデバイスに自動的にプッシュされます。プッシュ通知を受信するために、ユーザがサーバに接続している必要はありません。システム上でアプリケーションが実行されていない場合でも、ユーザはプッシュ通知を受信することができます。アプリケーションで [通知設定] が有効になっている必要があります。プッシュ通知の設定の詳細については、Mobile サーバ 4.2 の *Mobile* サーバのデプロイメントおよび設定ガイドを参照してください。

> **注記**
>
> Mobile でプッシュ通知を有効にするには、BIMobileService が APS で実行されている必要があります。
>
> BIMobileService はメモリを大量に消費しないため、APS で他のサービスとともに実行することができます。

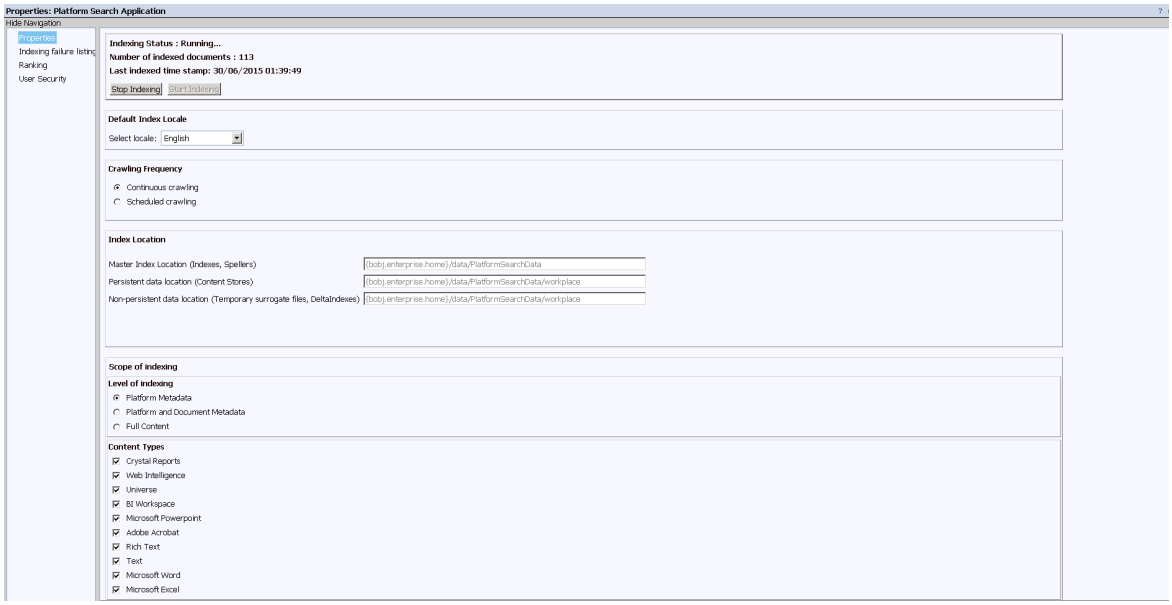
18.2.3.10 プラットフォーム検索設定の管理

BI プラットフォームの CMC の [アプリケーション] エリアで、プラットフォーム検索アプリケーションのシステムレベルの設定を指定できます。

18.2.3.10.1 CMC でのアプリケーションプロパティの設定

プラットフォーム検索アプリケーションプロパティを設定するには、次の手順に従います。

1. CMC の [アプリケーション] エリアを表示します。
2. [プラットフォーム検索アプリケーション] を選択します。
3. 管理 > プロパティ をクリックします。[プラットフォーム検索アプリケーションプロパティ] ダイアログボックスが表示されます。



4. プラットフォーム検索の設定を、以下のとおりに行います。

オプション	説明
検索統計	プラットフォーム検索は、以下の検索統計を提供します。 • インデックス処理のステータス: インデックス処理プロセスのステータスを示します。 • インデックス済みドキュメント数: インデックス処理されたドキュメントの数を表示します。 • 前回インデックス処理タイムスタンプ: ドキュメントが最後にインデックス処理されたときのタイムスタンプを表示します。
インデックス処理の停止/開始	[インデックス処理の開始] または [インデックス処理の停止] オプションにより、継続的クロールからスケジュール済みクロールへ切り替える場合、またはメンテナンス目的で、インデックス処理プロセスを開始または停止することができます。 インデックス処理を停止するには、[インデックス処理の停止] をクリックします。
デフォルトのインデックスロケール	プラットフォーム検索では、CMC で指定したロケールを使用して、すべてのローカライズされていない BI ドキュメントをインデックス処理します。ドキュメントがローカライズされると、対応する言語のアナライザがインデックス処理に使用されます。 検索はクライアントの製品ロケールに基づいて行われます。クライアントの製品ロケールには加重が適用されます。 CMC の設定プロパティでこの加重を設定できます。

オプション	説明
クロール頻度	以下のオプションを使用して、BI プラットフォームリポジトリ全体をインデックス処理することができます。 • 継続的クロール: このオプションを使用すると、インデックス処理は継続的に行われ、オブジェクトが追加、変更、または削除されるたびにリポジトリがインデックス処理されます。これにより、最新の BI プラットフォームコンテンツを表示または処理できます。デフォルトの設定で、リポジトリは、実行するアクションによって継続的クロールにより継続的に更新されます。継続的クロールは、ユーザの操作なしに動作し、ドキュメントのインデックス処理にかかる時間を短縮します。 • スケジュール済みクロール: このオプションを使用すると、インデックス処理は、スケジュールオプションで設定されたスケジュールに基づきます。 オブジェクトをスケジュールする方法については、*SAP BusinessObjects Business Intelligence プラットフォーム CMC* オンラインヘルプのプラットフォーム検索のオブジェクトのスケジュールの節を参照してください。 **注記** • [スケジュール済みクロール] を選択し、[繰り返し] に [今すぐ] 以外のオプションを設定した場合は、ドキュメントの次回のインデックス処理がスケジュールされると、プラットフォーム検索によって日時のタイムスタンプが表示されます。 • [スケジュール済みクロール] を選択した場合は、[インデックス処理の開始] ボタンが有効になり、[インデックス処理の停止] ボタンは無効になります。 • スケジュールの設定が完了すると、[インデックス処理の停止] ボタンは無効になります。

オプション	説明
インデックスの場所	インデックスは、以下の場所にある共有フォルダに格納されます。 • マスタインデックスロケーション (インデックス、スペラ): この場所に保存されているマスタおよびスペラインデックスです。検索中、最初の検索結果はマスタインデックスを使用して取得され、スペラインデックスは提案を取得するために使用されます。クラスタ化された BI プラットフォームデプロイメントでは、この場所は、共有ファイルシステム上にあり、クラスタのすべてのノードからアクセスできる必要があります。 • 永続データロケーション (コンテンツストア): コンテンツストアはこの場所に配置されます。マスタインデックスロケーションから作成され、それとの同期が維持されます。コンテンツストアは、ファセットの生成と、マスタインデックスロケーションから生成された最初の検索結果を処理するために使用されます。クラスタ化された BI プラットフォームデプロイメントでは、コンテンツストアはすべてのノードで生成されます。 永続データロケーションは、コンテンツストアフォルダを含むため、クラスタ環境の影響を受ける唯一のインデックスの場所です。マシンの検索サービスが 1 つである場合、コンテンツストアの場所は 1 つだけになります。たとえば、{bobj.enterprise.home}¥data¥PlatformSearchData¥workspace¥<Server Name>¥ContentStores になります。 ただし、クラスタ環境では、複数の検索サービスがある場合、コンテンツストアの場所は各検索サービスに対して 1 つになります。たとえば、実行中のサーバのインスタンスが 2 つある場合、コンテンツストアの場所は以下のようになります。 1. {bobj.enterprise.home}¥data¥PlatformSearchData¥workspace¥<Server Name>¥ContentStores 2. {bobj.enterprise.home}¥data¥PlatformSearchData¥workspace¥<Server Name 1>¥ContentStores • 非永続データロケーション (一時ファイル、デルタインデックス): この場所には、デルタインデックスが作成され、マスタインデックスと結合される前に一時的に格納されます。インデックスがマスタインデックスに結合されると、この場所から削除されます。また、代理ファイル (エクストラクタからの出力) がこの場所に作成され、デルタインデックスに変換されるまで一時的に格納されます。 **注記** • マスタインデックスロケーションは、共有の場所にする必要があります。 • インデックスの場所を変更するには、[インデックス処理の停止] をクリックする必要があります。 • インデックスの場所を変更する場合は、新しい場所にコンテンツをコピーしないと、既存のインデックス情報が失われます。 • インデックスファイルには、ドキュメントコンテンツをインデックス化するように選択した場合には特に、個人情報や機密情報が保存される可能性があります。データの盗難を防ぐために、共有フォルダへのアクセスをシステムユーザにのみ許可し、共有フォルダを暗号化された環境に保存してください。

オプション	説明

インデックス処理のレベル	インデックス処理のレベルを以下のように設定することにより、検索内容を調整することができます。
	• プラットフォームメタデータ: タイトル、キーワード、ドキュメントの説明などのプラットフォームメタデータ情報に対してのみ、インデックスが作成されます。デフォルトでは、このオプションはオンです。
	• プラットフォームおよびドキュメントのメタデータ: このインデックスには、プラットフォームメタデータとドキュメントメタデータが含まれます。ドキュメントのメタデータには、作成日、変更日、作成者名が含まれます。
	• フルコンテンツ: このインデックスには、プラットフォームメタデータ、ドキュメントメタデータ、および以下のようなその他のコンテンツが含まれます。
	  • ドキュメントの実際のコンテンツ
	  • プロンプトと LOV のコンテンツ
	  • チャート、グラフ、ラベル
	注記
	Analysis Office ドキュメントおよび Lumira ドキュメントでは、フルコンテンツのインデックス処理はサポートされていません。Analysis Office ドキュメントおよび Lumira ドキュメントでは、メタデータのインデックス処理のみがサポートされています。
	注記
	インデックス処理のレベルを変更すると、BI プラットフォームリポジトリ全体に対してインデックス処理が再度初期化されます。

オプション	説明
コンテンツタイプ	インデックス化の目的で次のコンテンツタイプを選択できます。 • Crystal レポート • Web Intelligence • ユニバース • BI ワークスペース • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • リッチテキスト形式 • テキスト • Microsoft Word • Microsoft Excel プラットフォームメタデータのインデックス処理では、コンテンツタイプフィルタは適用されません。プラットフォームメタデータのインデックス処理は、選択したコンテンツタイプに関係なく、すべてのサポートされるオブジェクトタイプに対して実行され、BI ラウンチパッドの検索結果にプラットフォームメタデータに関連するキーワードのすべてのオブジェクトが返されます。 コンテンツタイプフィルタは、ドキュメントメタデータのインデックス処理 (ドキュメント作成者、ドキュメントヘッダ、ドキュメントフッタなど) およびコンテンツのインデックス処理 (レポートのグラフ、チャート、テーブル)に適しています。ドキュメントメタデータおよびコンテンツに関連するキーワードを検索すると、プラットフォーム検索は、選択されたインデックス処理のレベルとコンテンツタイプに基づいて、リポジトリの選択されたオブジェクトタイプのドキュメントメタデータとコンテンツをインデックス処理します。処理されたオブジェクトだけが BI ラウンチパッドの検索結果に表示されます。
インデックスの再構築	このオプションを使用して、既存のインデックスを削除し、リポジトリ全体を再インデックス処理することができます。 インデックス処理が実行中か停止中かに関係なく、[インデックスの再構築] オプションを選択できます。既存のインデックスは、[プロパティ] ページへの変更を保存すると、削除されます。ただし、インデックス処理が現在停止されている場合、インデックス処理を再開するまでインデックスの再構築は開始されません。 プラットフォーム検索でドキュメントの再インデックス処理を行わない場合は、[インデックスの再構築] オプションを選択解除してから、[インデックス処理の開始] をクリックします。

オプション	説明
インデックス処理から除外するドキュメント	[インデックス処理から除外するドキュメント] オプションは、ドキュメントをインデックス処理から除外します。たとえば、レポートアプリケーションサーバのリソースに過負荷がかからないように、サイズが非常に大きい Crystal レポートを検索対象から外す必要がある場合です。または、大量のパーソナライズされたレポートのあるパブリケーションのインデックス処理をしない場合です。 特定のドキュメントを除外することで、プラットフォーム検索でそのドキュメントがアクセスされないように指定できます。このグループに分類される前にドキュメントがインデックス処理されると、そのドキュメントは検索できるので注意してください。[インデックス処理から除外するドキュメント] グループに属するドキュメントが検索されないようにするには、インデックスを再構築する必要があります。 デフォルトでは、[インデックス処理から除外するドキュメント] オプションのフルコントロールを持つのは管理者アカウントのみです。次の権限を持つその他のユーザは、[インデックス処理から除外するドキュメント] グループに対するドキュメントの追加のみを実行できます。 • カテゴリの表示権限および編集権限 • ドキュメントの直接編集
その他の設定 - インスタンスのスキップ	デフォルトでは、ドキュメントのインスタンスが取得されてインデックス処理が行われます。これによって、インデックスサイズが増大し、ディスク容量の消費が増えます。リポジトリ内の膨大な数のインスタンスのインデックス処理のため、PlatformSearchData フォルダ内の "Lucene Index Engine" フォルダのサイズが非常に大きくなります。数百万の (またはそれ以上の) ドキュメントがあり、これらのドキュメントの多くが、システム内にも膨大な数の既存インスタンスを (定期的に生成するスケジュールされたインスタンスとともに) 持つ場合、インデックス処理レベルが "プラットフォームメタデータ" に設定されていたとしても、"Lucene Index Engine" フォルダのサイズは過度に大きくなります。 プラットフォーム検索インスタンスのスキップ機能では、インスタンスのインデックス処理を CMC のプラットフォーム検索アプリケーションプロパティページにある 'その他の設定 - インスタンスのスキップ' チェックボックスで有効化または無効化することによって制御することができます。 ⓘ 注記 • インスタンスのスキップを有効/無効にすると、プラットフォーム検索 Adaptive Processing Server を再開する必要があります。この変更はすべてのインデックス処理レベルに影響します。 • インスタンスのスキップを変更し、この変更をすべての既存のインスタンスに適用する場合 (すなわち、取得してインデックス処理を行う)、インデックスを再構築する必要があります。

オプション	説明
インデックス処理から除外するオブジェクト	[インデックス処理から除外するオブジェクト] オプションは、オブジェクトをインデックス処理から除外します。たとえば、レポートアプリケーションサーバのリソースに過負荷がかからないように、特定のオブジェクトを検索対象から外す必要がある場合です。 特定のオブジェクトを除外することで、プラットフォーム検索でそのドキュメントがアクセスされないように指定できます。このグループに分類される前にオブジェクトがインデックス処理されると、そのオブジェクトは検索可能になるので注意してください。[インデックス処理から除外するオブジェクト] グループに属するドキュメントが検索されないようにするには、インデックスを再構築する必要があります。 インデックスから除外できるオブジェクトの一覧: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • Rtf • Txt • Word • AFDashboardPage • ObjectPackage • QaaWS • プロファイル • イベント • ディスカッション • InformationDesigner • MDAnalysis • パブリケーション • Agnostic • Analytics • Hyperlink • プログラム • pQuery • DSL.MetaDataFile • Shortcut • DataDiscoveryAlbum • AO.Workbook • VISI.Story • VISI.Dataset

オプション	説明
	• VISI.Lums • VISILums • ユーザ • UserGroup

5. [保存して閉じる] をクリックします。

> ⓘ 注記
>
> [インデックスの再構築] オプションを選択せず、インデックス処理のレベルを変更するか、エクストラクタを選択もしくは選択解除した場合は、既存のインデックスは削除されずにインデックスは増分更新されます。

18.2.3.11 BEx Web 統合の設定

BEx Web アプリケーションは、データ分析、レポーティング、および Web 上の分析アプリケーションのための SAP Business Warehouse (BW) の Business Explorer (BEx) に含まれている Web ベースのアプリケーションです。

Business Explorer は、SAP NetWeaver Business Intelligence Suite の一部で、戦略的分析および意思決定をサポートする柔軟性の高いレポーティングおよび分析ツールを提供します。 これらのツールには、クエリ、レポーティング、および分析の機能が含まれます。 アクセス権を持つ従業員は、Web 上および Microsoft Excel にある履歴データまたは現在のデータを、さまざまな詳細レベルそしてさまざまな角度から評価することができます。

ユーザは、SAP NetWeaver Portal、または SAP BI プラットフォームの BI ラウンチパッドからデータにアクセスします。 BEx Web アプリケーションの作成者は、BEx Web Application Designer から直接 BI 起動パッドで Web アプリケーションを実行することができます。

BEx Web アプリケーションを BI プラットフォームに統合するには、以下の設定手順に従います。

1. セントラル管理コンソール (CMC) で BEx Web アプリケーションのサーバを設定する。

   BEx Web アプリケーションには、一般サーバまたはスタンドアロンサーバのどちらでも使用できます。

   > → ヒント
   >
   > 一般サーバは他の多数のサービスによって使用されるため、BEx Web アプリケーション用のスタンドアロンサーバをセットアップすることをお勧めします。

2. サーバを設定する。
3. BW システムへの接続を確認する。
4. 作成者が BEx Web Application Designer から直接 BI 起動パッドで BEx Web アプリケーションを実行できるようにするには、BW システムの [接続済みポータル] テーブル (**RSPOR_T_PORTAL**) で関連の設定を行います。

BI プラットフォームサーバの設定後、ユーザは BI 起動パッドで BEx Web アプリケーションを開くことができます。 ここでデータをナビゲートして、BEx Web アプリケーションをブックマークとして Web ブラウザのお気に入りに保存することができます。

⚠ 制限

統合は次の SAP NetWeaver リリースでサポートされています。

SAP NetWeaver 7.0 拡張パッケージ 1 サポートパッケージスタック 8
SAP NetWeaver 7.3 サポートパッケージスタック 1

SAP NetWeaver Java スタックは、この統合では必要ないため、以下の制約が適用されます。

インフォメーションブロードキャスティングはサポートされていません。
SAP NetWeaver のポータルおよびナレッジマネジメントが必要ないため、BEx Web アプリケーションでは、ドキュメント統合およびポータルモチーフの使用はサポートされていません。
Web 項目の [レポート] はサポートされていません。 書式付きレポートには、SAP Crystal Reports を使用することをお勧めします。
BEx Web アプリケーションの印刷バージョンを作成するには、SAP Business Explorer のエクスポートライブラリを使用します。 Adobe ドキュメントサービス (ADS) は使用できません。
BI プラットフォームに統合されている BEx Web アプリケーションには、BW マスタシステムに保存されているデータソースのみを格納することができます。 システム管理においては、BI プラットフォームで BW マスタシステムとして設定されているシステムを定義します。
BI プラットフォームおよび SAP NetWeaver BW システム間のシングルサインオンは有効化されていません。 BEx Web アプリケーションユーザは、各 BI プラットフォームセッションで、対応する BW マスタシステムへのログオンを要求されます。
BEx Web アプリケーションとのレポート間インタフェースはサポートされていません。 対応するコマンドは実行されません。
BEx クエリまたはクエリビューを基にしたダッシュボード、および SAP BusinessObjects Dashboards で作成されたダッシュボードはサポートされません。

BEx Web アプリケーションの機能の詳細については、SAP Help Portal (http://help.sap.com) で次を参照してください。 *SAP NetWeaver 7.3* > *SAP NetWeaver Library: Function-Oriented View* > *Business Warehouse* > *SAP Business Explorer* > *BEx Web* > *Analysis & Reporting: BEx Web Applications*。

BI 起動パッドでの BEx Web アプリケーションへのアクセスおよび保存の詳細については、*BI 起動パッドユーザガイド* (http://help.sap.com) を参照してください。

関連情報

BEx Web アプリケーション用のサーバの開始 [709 ページ]
BEx Web アプリケーション用のスタンドアロンサーバの開始 [710 ページ]
サーバの設定 [710 ページ]
BW システムへの接続の確認 [711 ページ]
BEx Web Application Designer と BI プラットフォーム間の接続の設定 [711 ページ]

18.2.3.11.1 BEx Web アプリケーション用のサーバの開始

このタスクを実行する前に、Adaptive Processing Server を停止状態にしておく必要があります。

1. セントラル管理コンソール (CMC) にログオンします。
2. [サーバ] を選択します。
3. [サービスカテゴリ] ノードを展開し、[*Analysis* サービス] を選択します。
4. [*Adaptive Processing Server*] を選択し、コンテキストメニューから [サービスの選択] を選択します。
5. [*BEx Web* アプリケーションサービス] を [利用可能なサービス] リストから、右側の [サービス] リストに移動します。
6. Adaptive Processing Server を再起動することにより、BEx Web アプリケーションサービスを再起動します。

18.2.3.11.2 BEx Web アプリケーション用のスタンドアロンサーバの開始

1. セントラル管理コンソール (CMC) にログオンします。
2. [サーバ] を選択します。
3. [サービスカテゴリ] ノードを展開し、[*Analysis* サービス] を選択します。
4. [*Adaptive Processing Server*] を選択し、コンテキストメニューから [クローンサーバ] を選択します。
5. サーバの名前 (**`AdaptiveProcessingServer`** など) を入力して、[ノードに複製] ボックスで必要なノードを選択します。
6. クローンサーバを選択して、コンテキストメニューから [サービスの選択] を選択します。
7. [利用可能なサービス] リストで、[*BEx Web* アプリケーションサービス] を選択して、右側の [サービス] リストに移動します。
8. 新しい Adaptive Processing Server を起動することにより、BEx Web アプリケーションサービスを起動します。

18.2.3.11.3 サーバの設定

1. セントラル管理コンソール (CMC) にログオンします。
2. [サーバ] を選択します。
3. [サービスカテゴリ] ノードを展開し、[*Analysis* サービス] を選択します。
4. BEx Web アプリケーションサービスをホストするサーバを選択して、コンテキストメニューで [プロパティ] を選択します。
5. [*BEx Web* アプリケーションサービス] 領域の [*BEx Web* アプリケーションサービスの設定] の下で、次の設定を行います。
   a. クライアントセッションの最大数を確認し、必要に応じて変更します。
   b. [*SAP BW* マスタシステム] で、 BI プラットフォームで作成した BW システムへの OLAP 接続名を入力します。デフォルト名は [*SAP_BW*] です。
   c. BW システムの [*RFC* 接続の設定] (トランザクションコード **`sm59`**) で入力した [*JCo* サーバ *RFC* 宛先] の名前を入力します。
   d. BW システムの [*RFC* 接続の設定] (トランザクションコード **`sm59`**) で定義した [*JCo* サーバゲートウェイホスト] の名前を入力します。
   e. BW システムの [*RFC* 接続の設定] (トランザクションコード **`sm59`**) で定義した [*JCo* サーバゲートウェイサービス] の名前を入力します。

f. [*JCo サーバ接続数*] を確認し、必要に応じて変更します。

6. [保存して閉じる] を選択します。
7. BEx Web アプリケーションサービスをホストするサーバを選択して、コンテキストメニューで [サーバの再起動] を選択します。

   選択した設定を適用するには、サーバを再起動する必要があります。

   > ⓘ 注記
   >
   > サーバを再起動する前に、ABAP システムに RFC 宛先を作成しておく必要があります。

関連情報

ABAP システムでの RFC 宛先の作成 [712 ページ]

18.2.3.11.4 BW システムへの接続の確認

1. セントラル管理コンソール(CMC)にログオンします。
2. [*OLAP 接続*] を選択します。
3. BW システムへの接続が確立されているかどうかを確認します。確立されていない場合、[新しい接続] ボタンをクリックして接続を設定します。接続のデフォルト名は「**SAP_BW**」です。別の名前を入力することもできます。
4. [認証] で [事前定義済み] を選択していること、およびユーザとパスワードに必要な入力を行っていることを確認します。

   > ⓘ 注記
   >
   > このユーザアカウントは JCo サーバ RFC 宛先に必要です。このアカウントにより、BEx Web Application Designer、BW システム、および BI プラットフォームの統合が許可されます。

   > → ヒント
   >
   > 接続をセキュリティ保護するには、管理者のみがこの接続に対するアクセス権を持つようにします。
   > 1. これを行うには、BW システム (デフォルト名は **SAP_BW**) への接続を右クリックし、コンテキストメニューで [ユーザセキュリティ] を選択します。
   > 2. 必要なセキュリティ設定を行い、可能な場合はアクセス権を管理者のみに付与します。

18.2.3.11.5 BEx Web Application Designer と BI プラットフォーム間の接続の設定

作成者が BEx Web Application Designer から直接 BI 起動パッドで BEx Web アプリケーションを実行できるようにするには、BW システムの [接続済みポータル] テーブル (**RSPOR_T_PORTAL**) で関連の設定を行う必要があります。

1. BW システムで、トランザクション **SM30** を呼び出します ([テーブルビューのメンテナンス])。
2. [テーブル/ビュー] で、「**RSPOR_T_PORTAL**」と入力します。
3. [更新] を選択します。
4. 新しいエントリを作成するには、[新規エントリ] を選択します。
5. 次の設定を行います。
   a. BW システムと BI プラットフォームとを統合するには、トランザクション **SM59** で RFC 宛先を作成する必要があります。[出力先] の下にこの RFC 宛先を入力します。
   b. [標準ポータル] を選択します。これにより、Web Application Designer では Web アプリケーションが常に BI プラットフォームで呼び出されるようになります。
   c. [*URL プレフィックス*] で、BI プラットフォーム Web Application Container Server (WACS) への URL を入力します。URL にはプロトコル、ホスト名、およびポートを含め、たとえば「**http://<wacs><domain>:<port>**」のように入力します。
   d. [プラットフォーム] で、[*BOE*] を選択します。
   e. SAP Business Explorer 用のエクスポートライブラリを有効化する場合は、[*SAP エクスポートライブラリ (PDF) を使用*] を選択し、PDF ファイル、PostScript ファイル、および PCL ファイルを BEx Web アプリケーションからエクスポートできるようにします。
6. 入力内容を保存します。

関連情報

ABAP システムでの RFC 宛先の作成 [712 ページ]

18.2.3.11.5.1 ABAP システムでの RFC 宛先の作成

BW システムと BI プラットフォームとを統合するには、RFC 宛先が必要です。この RFC 宛先により、BW システムと BI プラットフォームが相互通信できるようになります。

1. [*RFC 接続の設定*] (トランザクションコード **SM59**) を呼び出します。
2. [作成] を選択します。
3. RFC 宛先を更新します。
   a. RFC 宛先の名前を入力します。
   b. 接続の種類として [*T (TCP/IP 接続用)*] を選択します。
   c. 説明を入力します。

      RFC 宛先言語の記述は、独立して更新できます。
   d. [技術設定] で、有効化の種類として [登録サーバプログラム] を選択します。
   e. [技術設定] に、プログラム ID を入力します。

      このプログラム ID は、BI プラットフォームサーバでこの BW システム用の宛先を作成したときに指定したプログラム ID (JCo サーバ RFC 宛先) と同じであることが必要です。
   f. [技術設定] の [ゲートウェイオプション] の下に、BI プラットフォームサーバが BW システムとの通信に使用するゲートウェイホストおよびゲートウェイサービスを入力します。
4. [ログオン & セキュリティ] タブページで、[*SAP ログオンチケットの送信*] オプションを有効化します。

5. 入力内容を保存します。

関連情報

サーバの設定 [710 ページ]

18.2.3.12 SAP HANA シングルサインオンの設定

BI プラットフォームの CMC の [アプリケーション] エリアで、SAP HANA データベース接続のシングルサインオン (SSO) を設定できます。SSO は SAML (Security Assertion Markup Language) を使用して実装されます。

BI プラットフォームセッションが確立されると、パスワードを入力せずに SAP HANA にログインして使用できる SAML チケットが生成可能になります。

SAP HANA データソースへの接続における基本ワークフローは次のようになります。

1. 管理者が CMC で SAP HANA と BI プラットフォーム間の信頼を設定します。
2. ユーザがサポートされる認証プロバイダのいずれかを使用して BI プラットフォームにログインします。
3. SAP HANA と BI プラットフォームのユーザ ID が一致する場合、SAP HANA が現在のユーザの接続確立に受け入れ可能な SAML アサーションを BI プラットフォームが生成できるようになります。SAP HANA に渡されるユーザ ID は、ログインしているユーザの BI プラットフォームユーザ ID です。
4. BI プラットフォームクライアントアプリケーションにより SAP HANA 接続が作成されます。

> **注記**
>
> SAP HANA シングルサインオンを SAML で設定する前に、SAP HANA マシンで SSL を設定する必要があります。詳細については、SAP HANA ドキュメントを参照してください。

18.2.3.12.1 SAP HANA 接続設定

SAP HANA 接続を設定するために CMC で使用できる設定について、以下の表にまとめます。

設定	説明
HANA ホスト名	SAP HANA ホストの名前を指定します。
HANA ポート	SAP HANA ホストのポート番号を指定します。
プロバイダ ID の一意の ID	指定された HANA インストール内の一意の名前です。HANA インストールは、このログオン ID プロバイダ名から、正しく署名されたチケットを許可します。
ID プロバイダの Base64 証明書	[生成] をクリックすると、[*ID プロバイダの Base64 証明書*] フィールドに証明書が作成されます。この証明書を SAP HANA デプロイメントの `trust.pem` ファイルにコピーします。この証明書は、SAP HANA と BI プラットフォーム間の信頼関係を確立します。外部 ID プロバイダ自体は、X509 証明書で識別されます。この証明書は、すべての ID アサーションの署名に使用されます。証明書は Base64 でエンコードする必要があります。

設定	説明
HANA インスタンス番号	SAP HANA データベースのインスタンス番号を指定します。
HANA テナントデータベース	SAP HANA テナントデータベースの名前を指定します。

18.2.3.12.2 SAP HANA 接続を作成する

1. 関連する SAP HANA データベースパラメータを取得します。
   a. SAP HANA Studio アプリケーションを開きます。
   b. システムのプロパティページを開き、データベース接続の URL を検索します。
   c. ホストマシン名、ポート番号、インスタンス番号、テナントデータベース名を記録します。

      手順 2 でこの情報が必要になります。
2. BI プラットフォームで SAP HANA 接続を設定します。
   a. CMC の [アプリケーション] エリアに移動し、[*HANA* 認証] をダブルクリックします。
   b. [*HANA*] 認証ダイアログボックスで、[接続を作成します] ボタンをクリックします。
      [*HANA* 認証接続の作成] ダイアログボックスが開きます。
   c. 接続の種類を選択します。

      > ⓘ 注記
      >
      > JDBC 接続の場合は [*SAP HANA*]、HTTP 接続の場合は [*SAP HANA http*] を選択する必要があります。

   d. 手順 1 で記録したポート番号、ホストマシン名、インスタンス番号、テナントデータベース名を入力します。
   e. [プロバイダ *ID* の一意の *ID*] フィールドで、BI プラットフォームデプロイメントで使用する値を指定します。
   f. サービスプロバイダ名を入力します。

      > ⓘ 注記
      >
      > HANA でサービスプロバイダ名の設定を確認するには、`indexserver.ini → Authentication → saml_service_provider_name` に移動します。また、以下に示すコードを入力して、HANA でその値を変更することもできます。`ALTER SYSTEM ALTER CONFIGURATION ('indexserver.ini', 'SYSTEM') SET ('authentication', 'saml_service_provider_name') = 'DEV00' WITH RECONFIGURE;`。このコードで、DEV 00 はサービスプロバイダの名前であり、任意の名前を入力できます。サービスプロバイダの名前を付ける際のベストプラクティスは、システム ID (DEV) とインスタンス番号 (00) を結合することです。

   g. [セキュア接続] を選択します。

      > ⓘ 注記
      >
      > [セキュア接続] を選択して、セキュリティで保護された JDBC または HTTPS 接続を確立する必要があります。
      >
      > - HTTPS 接続を確立するには、[接続の種類] として [*SAP HANA http*] を選択し、[セキュア接続] を選択する必要があります。

> - セキュリティで保護された JDBC 接続を確立するには、[接続の種類] として [*SAP HANA*] を選択し、[セキュア接続] を選択する必要があります。

h. [生成] をクリックします。
[*ID プロバイダの Base64 証明書*] ボックスに証明書が作成されます。

3. SAP HANA デプロイメントを設定します。
   a. HANA システムにログインします。
   b. [*SSL* およびトラスト設定] を展開し、[*PSE* 管理] を選択します。
   c. [*PSE* 管理] に対して、PSE ファイルをドロップダウンから選択します。
   d. [証明書のインポート] を選択します。
   e. BI プラットフォームで以前のステップで生成された証明書をペーストします。
   f. [インポート] を選択します。
   g. SAP HANA Studio を起動します。
   h. [システム] ビューで、SAP HANA システムを展開します。SAP HANA One 管理ガイドを参照してください。
   i. Security フォルダから (セキュリティエディタ) を開きます。
   j. (証明書ファイルの SAML アイデンティティプロバイダをインポート) を選択します。
   k. [*SAML* アイデンティティプロバイダ] 一覧から自分のアイデンティティプロバイダを選択します。
   l. (デプロイ) を選択します。
   m. [システム] ビューで、HANA ユーザにナビゲートします。
   n. [エディタ] 領域で HANA ユーザを開きます。
   o. [ユーザ] タブで、認証として [*SAML*] を選択し、[設定] を選択します。
   p. [外部 *SAML ID* の設定] ウィザードで、[追加] を選択します。
   q. アイデンティティプロバイダを選択します。
   r. [OK] を選択します。
   s. アイデンティティプロバイダを選択し、これに対して HANA ユーザにマッピングされた BI プラットフォームユーザ名を入力します。
   t. [OK] を選択します。
   u. (デプロイ) を選択します。
   v. SAP HANA システムを再起動します。
      1. SAP HANA システムのコンテキストメニューを開きます。
      2. [設定および監視] を選択します。
      3. [システムの再起動] を選択します。

4. SAP HANA 設定をテストします。
   a. CMC の [アプリケーション] エリアに移動し、[*HANA* 認証] をダブルクリックします。
   b. *HANA* 認証ダイアログボックスで、手順 2 で作成した接続を開きます。
   [*HANA* 認証接続の編集] ダイアログボックスが開きます。
   c. [このユーザの接続テスト] の下にユーザ名を入力し、[接続テスト] ボタンをクリックして接続設定が有効になっていることを確認します。

      たとえば、ユーザ名「**`Administrator`**」を入力します。設定が正しくない場合、エラーメッセージが表示されます。以下のトラブルシューティング手順を実行できます。

      - `trust.pem` ファイルにある他の証明書に、同じ CN プロパティ値のサブジェクトまたは発行者が含まれていないことを確認します。証明書のコンポーネントを表示するには、インターネットで「“x509 証明書デコーダ”」を入力して証明書デコーダを検索します。

- HANA 側の設定を確認するには、次のコマンドを実行します。

```
select * from "SAML_PROVIDERS"
select user_name, is_saml_enabled from users where user_name =
'<UserName>'
select * from "PUBLIC"."SAML_USER_MAPPINGS"
```

- SAP HANA への SSO の設定中に SAML 認証エラーが表示された場合は、次の手順を実行します。
  1. `indexserver.ini` ファイルで、`sslCreateSelfSignedCertificate` パラメータを **`false`** に設定します。
  2. 同じファイルで、`sslKeyStore` パラメータおよび `sslTrustStore` パラメータで絶対パスを使用するように設定します。
  3. `key.pem` ファイルおよび `trust.pem` ファイルを再生成します。

`.ssl` ディレクトリに `key.pem` ファイルが存在しない場合、SAP HANA は SSL を使用する設定になっていません。

18.2.3.12.3 SAP HANA HTTPS 接続の設定

SAP HANA HTTPS を設定するときには、HANA サーバおよび HANA サーバ CA 証明書をトラストストアまたは任意の場所に追加します。

> **注記**
>
> SAP HANA サーバ証明書をトラストストアや異なる場所に追加する前に、SAP HANA システムからエクスポートする必要があります。

トラストストアへの証明書の追加

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥jre¥lib¥security` に移動します。
2. 次のコマンドを実行します。`..¥..¥bin¥keytool -importcert -file "<absolute path of the certificate>" -alias CertifcateAliasName -keystore cacerts -storepass changeit`.
3. HANA サーバおよび HANA サーバ CA 証明書がトラストストアに格納されます。

> **注記**
>
> キーストアファイルがデフォルトの場所 `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥jre¥lib¥security` にある場合、キーストアファイルに対する変更内容は、Business Intelligence プラットフォームサポートパッケージ 4 からサポートパッケージ 5 にアップグレードした後に失われます。このため、証明書を別の場所に追加することをお奨めします。

別の場所への証明書の追加

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥jre¥bin` に移動します。
2. 次のコマンドを実行します。`keytool -importcert -file "C:¥certificate¥HANASERVERCertificate " -alias CertificateAliasName -keystore C:¥certificate¥cacerts -storepass changeit`。

   > **注記**
   >
   > 上記で定義した場所は単なる例です。任意の場所を追加することができます。

3. APS サーバがファイルの場所を識別できるように、次のコマンドを実行します。

   ```
   -Djavax.net.ssl.trustStore= cacerts_PATH
   -Djavax.net.ssl.trustStorePassword= Password
   ```

   > **注記**
   >
   > cacerts_PATH および Password は、キーストアパスおよび証明書パスワードの単なる例です。任意のパスおよびパスワードを追加することができます。

18.2.3.13 SAP Lumira の設定の管理

CMC の "アプリケーション" 領域から、各ユーザまたはユーザグループに対して SAP Lumira のデータ取得およびコンテンツ共有機能に関連するアクセス権を管理することができます。

SAP Lumira のアクセス権を管理するには、以下の手順に従います。

1. CMC ホームページで、アプリケーション > *SAP Lumira* > ユーザセキュリティ を選択します。
2. アクセス権を設定するユーザまたはグループを選択します。
3. セキュリティの割り当てを選択します。
4. 詳細を選択します。
5. 権限の追加/削除を選択します。
6. SAP Lumira に対してユーザに必要な権限を定義します。
7. 適用をクリックします。

18.2.3.14 SAP Analytics Cloud 設定の管理

18.2.3.14.1 SAP Analytics Hub への Hub アセットのプッシュ

BI アセットを新しいカテゴリ [*Hub アセット*] に追加し、同じ BI アセットに SAP Analytics Hub からアクセスすることができます。

SAP Analytics Cloud で *OAuth クライアント*を作成し、[*SAP Analytics Cloud テナント URL*]、[*トークン URL*]、[*OAuth クライアント ID*]、[*シークレット*] などのパラメータの値を書き留めます。OAuth クライアントの作成方

法については、SAP Help Portal で SAP Analytics Cloud ヘルプのトピック *OAuth* クライアントの管理を参照してください。

SAP Analytics Hub では、オンプレミスおよびクラウドベースの BI アセットに 1 つのプラットフォームでアクセスできます。BI プラットフォームと SAP Analytics Hub の ID プロバイダとして機能する SAP Analytics Cloud との間にトラストを設定して、BI プラットフォームが BI アセットを SAP Analytics Hub にアップロードできるようにする必要があります。

> **注記**
>
> [*Hub アセット*] カテゴリでは、パブリケーションはサポートされていません。

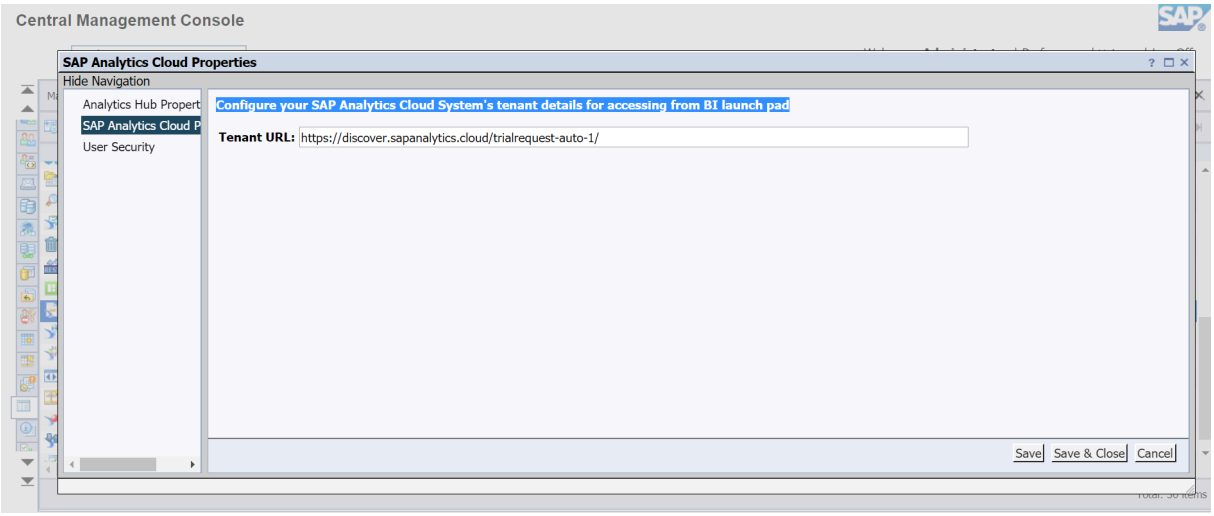
1. CMC にログインし、アプリケーション > *SAP Analytics Cloud* に移動します。
2. [*BI プラットフォームに BI アセットの SAP Analytics Hub へのプッシュを許可*] を選択します。
3. 次のパラメータを入力します。
   - *SAP Analytics Cloud テナント URL*
   - *トークン URL*
   - *OAuth クライアント ID*
   - *シークレット*
4. [*保存して閉じる*] を選択します。

[*Hub アセット*] カテゴリの BI アセットを SAP Analytics Hub にアップロードするための SAP Analytics Cloud の設定が、BI プラットフォームで正常に完了しました。

18.2.3.14.2 SAP Analytics Cloud テナント URL の設定

これで、BI ラウンチパッドアプリケーションの SAC タイルからアクセスできるように、SAP Analytics Cloud システムのテナント詳細を設定できます。

> **注記**
>
> デフォルトでは、URL は SAP Analytics トライアルアカウント URL に設定されています。



18.2.3.15 認可サーバの設定

認可サーバの設定アプリケーションは、認可サーバのメカニズムやプロトコルを介してアクセスするすべてのデータベースリソースに使用されます。

エンドツーエンドの SSO OAuth サポート - 単一および複数 OAuth サーバのサポート

セントラル管理コンソールでは、BI プラットフォームで認可サーバを設定および管理するために、認可サーバの設定アプリケーションを使用できます。このアプリケーションでは、管理者が認可参照オブジェクトを使用して設定を登録および管理します。認可サーバの各設定に対し、認可参照オブジェクトがあります。認可サーバの設定は、その他、Google ドライブ、Microsoft Drive、または OData リソースに対して作成できます。

認可サーバ設定を作成するには、[認可サーバの設定情報入力] の必須フィールドを入力します。

エンドユーザがオンラインまたはオフラインでアクセスできる対象を制御するため、[認可範囲] をニーズに基づいて定義できます。

18.2.3.15.1 認可サーバを設定する

認可サーバを設定することができます。

1. セントラル管理コンソールを起動し、管理者としてログインします。
2. ホームページで、[管理] 列の下にある [アプリケーション] を選択します。
3. [アプリケーション] ページで、[認可サーバの設定] をダブルクリックします。
4. [認可サーバの設定] ダイアログで、以下のいずれかを実行します。
   - 管理 > 新規認可サーバの設定 を選択します。
   - [新規認可サーバの設定の作成] ツールバーアイコンを選択します。
5. [新規認可サーバの設定の作成] ダイアログで、以下のパラメータを入力します。
   - 参照名
     一意のランダム文字列を選択し、同じ文字列を入力して設定を識別し、権限ベースの SSO を実現するためのさまざまなワークフローの設定を認識および選択します。
   - 説明 (オプション)
     説明のための文またはキーワードを入力して、利用可能な設定の一覧から設定を識別します。
   - **OpenID** 接続に固有のフィールド
     以下のフィールドは OpenID 接続の認証に固有であり、権限 SSO には必要ありません。
     - [*OpenID 接続認証に対して有効*] チェックボックス
     - *発行者 URI*
     - *JSON Web キーセット URI (jwks_uri)*
     - *ID トークン署名アルゴリズム*
   - 認可エンドポイント
     権限付与を取得できる、認可サーバの URL を入力します。

- トークンエンドポイント
  権限コードを変更することでアクセストークンを要求できる、認可サーバの URL を入力します。
- クライアント *ID*
  認可サーバでの BI ランドスケープの登録に使用されるアプリケーションの名前を入力します。
- クライアントシークレット
  認可サーバでの BI ランドスケープの登録に使用されるアプリケーションに対応する特定のシークレットコードを入力します。
- リダイレクト *URL*
  権限チェックが成功した後、認可サーバによって認証コードが送信される BI ランドスケープエンドポイントの URL を入力します。
- 失効エンドポイント (オプション)
  認可サーバの URL を入力します。これにより、特定のリフレッシュトークンを使用して、以前に発行されたすべてのアクセストークンの失効をアプリケーションで要求することができます。
- 認可範囲
  認可サーバによってサポートされる認可範囲を入力して、利用可能なさまざまな API リソースへのアプリケーション (BI ランドスケープ) アクセスの制限を定義します。

> ⓘ 注記
>
> OAuth SSO の BI プラットフォーム実装は、オフラインアクセスに基づいています。BI プラットフォームでの認可サーバの設定の目的が、毎回権限チェックを要求されることなくデータをリフレッシュしたりリソースにアクセスしたりすることである場合は、このフィールドを 1 つの必須パラメータ (たとえば、認可サーバのベンダに基づく "refresh_token" または "offline_access") とともに、必要な範囲パラメータで設定する必要があります。

- リソースのタイプ
  BI プラットフォームでサポートされるリソースタイプの利用可能な一覧から、目的のリソースタイプを選択します。以下は、対応する認可サーバを介して設定およびアクセスするために BI プラットフォームでサポートされている現在のリソースタイプの一覧です。
  - その他 (デフォルト値)
    認可サーバによる権限付与が成功してアクセス可能なリソースを示します。ベンダまたはプロトコルに固有ではありません。
  - *Google* ドライブ
    設定が Google 認可サーバであり、さまざまな BI プラットフォームシナリオに対する Google ドライブへのアクセスに使用できることを示します。どの時点でも、システム内に存在できるのは Google ドライブタイプの 1 つの設定のみです。
  - *Microsoft Drive*
    設定が Microsoft 認可サーバであり、さまざまな BI プラットフォームシナリオに対する Microsoft Drive へのアクセスに使用できることを示します。どの時点でも、システムに存在できるのは Microsoft Drive タイプの 1 つの設定のみです。
  - *OData*
    どのベンダにも固有ではありませんが、設定がリソースに関連していることを示します。リソースには、認可サーバによって権限を付与された OData プロトコルを介してアクセスできます。Google ドライブと同様に、どの時点でも、システムに存在できるのは OData タイプの 1 つの設定のみです。

> ⓘ 注記
>
> [リソースのタイプ] パラメータは、OAuth 2.0 標準とは関係ありません。ただし、これは、BI プラットフォームでの特定のリソースの特定におけるあいまいさを回避するために設定で導入されていま

> す。そのため、権限を取得するために、対応する設定を特定のシナリオで簡単に選択して使用することができます。

- アクセスの種類
  このパラメータは、タイプ [*Google ドライブ*] の権限設定に固有です。[リソースのタイプ] フィールドの値が [*Google ドライブ*] の場合は、自動的に入力されます。
- カスタムパラメータ (オプション)
  権限の要求中に送信するために必要なカスタムパラメータを入力します。これは、設定されている認可サーバのカスタム要件 (必要な場合) に基づきます。

> ⓘ 注記
>
> カスタムパラメータの名前は、設定で一意にする必要があります。
>
> どの権限設定でも、最大 5 つのカスタムパラメータを設定できます。

6. 必要なパラメータをすべて入力したら、[*OK*] を選択して詳細をチェックし、設定を保存します。

   設定は、タイプ [権限参照] でシステムオブジェクトとしてリポジトリに保存されます。サポートされているすべてのシナリオの設定を [参照名] で参照することができます。

18.2.3.15.2 認可サーバの設定をテストする

認可サーバの設定をテストできます。

1. 認可サーバの設定が正常に保存されたら、BI ラウンチパッドを起動し、ログインして設定をテストします。

   > ⓘ 注記
   >
   > 現在、CMC から設定をテストすることはできません。
   >
   > 管理者として、または上記で保存した権限設定の使用が制限されていない BI プラットフォームユーザアカウントを使用してログインします。
   >
   > BI ラウンチパッドに設定された現在のログイン方法 (Enterprise や任意の認証方法など) を使用します。

2. ユーザアイコンを選択します。
3. 表示されるドロップダウンメニューで、[設定] を選択します。
4. [設定] ダイアログの [ユーザアカウント] セクションで、[認可トークン] を選択します。
5. [トークンの管理] 列で [生成] を選択します。
6. 組織のポリシーに従い、認可サーバの権限設定に基づいて、システムで設定された証明書に基づいたアカウントチェックが行われるか、設定に基づいてユーザ名、パスワード、多要素認証を使用して身元が確認されます。
7. 認証情報または証明書が正常に検証されると、BI プラットフォームはリフレッシュトークンを受信します。これは、BI プラットフォームリポジトリに安全に保存されます。これが成功すると、[認可トークン] タブに以下の変更が表示されます。
   - [有効期限] 列に、認可サーバによって発行されたトークンの有効期限値が表示されます。認可サーバが期限切れのないトークンを発行した場合、列の値は [期限なし] として更新されます。
   - [トークンの管理] 列で、[生成] ボタンの横に [削除] ボタンが表示されます。

- [削除] ボタンは、認可サーバによって発行されたトークンを削除するためのものです。この削除は、BI プラットフォームリポジトリストレージからのトークンの削除に限定されません。また、設定とサポートに基づいて認可サーバに伝播することもできます。
- オプションの [失効エンドポイント] パラメータに、認可サーバのサポートに基づいて適切な URL が入力されている場合、発行されたトークンは BI プラットフォームリポジトリストレージからクリアされるとともに、認可サーバレベルでも無効化されます。

8. トークンが発行され、発行されたトークンの有効期限に従って [有効期限] 列が更新されると、設定が正常に機能し、BI 開発者と BI エンドユーザが使用できるようになります。

18.2.3.16 情報分類設定

BI プラットフォームでは、組織の Azure Policy サーバを設定して、BI ランドスケープで BI コンテンツを分類できるようにすることができます。これらの分類機能は、組織の Azure Policy サーバ管理者が定義した秘密度ラベルによって適用できます。

> **注記**
>
> Policy サーバを設定するこの統合オプションは、Microsoft Azure Information Protection プラットフォームでのみサポートされています。
>
> SAP BusinessObjects BI 4.3 SP04 リリースには、Microsoft Azure Information Protection プラットフォームの統合オプションが含まれています。ただし、BI プラットフォームで Azure Policy サーバの詳細を設定するアプリケーションはデフォルトでは有効化されずに、非表示機能として出荷されていることに注意してください。この非表示機能を表示するには、3409349 を参照してください。

この機能は、Windows プラットフォームでのみ利用可能です。

18.2.3.16.1 情報分類の設定方法

1. セントラル管理コンソールに管理者としてログインします。
2. アプリケーションに移動します。
3. 情報分類設定アプリケーションを右クリックします。
4. 情報分類の設定を選択します。
5. 情報分類の有効化チェックボックスを選択し、設定およびフィールドを有効化します。
6. 組織の Azure Policy サーバのポリシーサーバ *URL* フィールドのトークン URL を入力します。
   URL 書式は、`https://login.microsoftonline.com/<tenant-id>/oauth2/v2.0/token` である必要があります。
7. Azure のクライアントアプリケーションのクライアント *ID* およびクライアントシークレットの値を入力します。
   これらは、組織の Azure Policy サーバにアクセスする権限のクライアント認証情報フローモードに対して有効化されます。
8. 設定の保存およびテストをクリックして、接続をテストします。
9. 設定テストが成功したら、保存または保存して閉じるをクリックします。

> **注記**
>
> 証明書の認証に対して有効に関連するチェックボックスは、この認証設定のモードがサポートされていないため選択しないでください。

18.3 セマンティックレイヤプロパティを使用したアプリケーションの管理

ディメンションセマンティックレイヤ (DSL) ライブラリの設定オプションを実行時に設定することにより、BI ツール (Web Intelligence、インフォメーションデザインツール、ダッシュボード、Crystal Reports for Enterprise など) 内での BICS 接続を介した HANA ダイレクトアクセスおよび BW ダイレクトアクセスの動作を変更することができます。これらのオプションは、以下の形式の Java コマンドラインオプションで指定されます。

-DoptionName=optionValue

これらの設定の維持および変更では、以下のような課題が生じることがあります。

- DSL を実行しているすべての Java プロセスに、個別にコマンドラインオプションを指定する必要があります。変更を行うための共通の場所はありません。
- 修正された設定を有効にするには、すべての DSL Java プロセスを個別に再起動する必要があります。変更は即時には有効になりません。

DSL-BICS 設定オプションを維持する管理タスクを簡略化するために、オプションをファイルに保存できる新しいメカニズムが導入されました。ファイルを変更すると、このファイルを読み込むすべての DSL プロセスに新しいオプション設定が伝搬されます。

オプション名および値は、http://java.sun.com/dtd/properties.dtd で定義されている java.util.Propertes の有効な XML としてファイルに保存されます。

DSL を実行してこの新しいメカニズムを初めて開始すると、以下の 2 つのファイルが自動的に生成されます。

- DSLBICSConfiguration.xml または DSLConfiguration.xml - このファイルには、すべての使用可能なオプションおよびそのデフォルト値が含まれています。このファイルは変更しないでください。
- DSLBICSConfiguration_custom.xml または DSLConfiguration_custom.xml - このファイルには、すべてのオプションおよび管理者が指定した値が含まれています。

> **注記**
>
> - DSLBICSConfiguration.xml および DSLBICSConfiguration_custom.xml ファイルは、BICS 接続を介した BW ダイレクトアクセスの動作を管理するために使用されます。
> - DSLConfiguration.xml および DSLconfiguration_custom.xml ファイルは、HANA ダイレクトアクセスの動作を管理するために使用されます。

生成された `DSLBICSConfiguration_custom.xml` および `DSLConfiguration_custom.xml` ファイルには、コマンドラインから指定されたすべてのオプション設定、およびその他のオプションのデフォルト設定が含まれています。ファイルの初回生成後は、`DSLBICSConfiguration_custom.xml` または `DSLConfiguration.xml` ファイルを変更してオプション値を追加または変更することができます。このファイルの初回生成後に、メカニズムによってファイルが更新されることはありません。

`DSLBICSConfiguration.xml` ファイルは、新しく使用可能になったオプションによって、またはデフォルト値が変更された場合に、メカニズムにより更新されます。

デフォルトプロパティを変更するには、カスタム設定ファイルを使用して、グローバルプロパティまたはアプリケーション固有のプロパティのいずれかの新しい設定を保存します。デフォルトでは、ディレクトリファイルは `SAP BusinessObjects Enterprise XI 4.0¥java¥lib` にあります。

デフォルト設定ファイルのプロパティは変更しないでください。

18.4 BOE.war プロパティを介したアプリケーションの管理

18.4.1 BOE war ファイル

BOE.war ファイルのデフォルトプロパティを上書きすることにより、BI プラットフォーム Web アプリケーションの設定を変更できます。このファイルは、Web アプリケーションサーバをホストするマシンにデプロイされます。このファイルのデプロイ方法の詳細については、*SAP BusinessObjects Business Intelligence* プラットフォーム *Web* アプリケーションデプロイメントガイドを参照してください。

BOE.war ファイルに含まれるプロパティによって、デフォルトのログイン動作、デフォルトの認証方法、シングルサインオンの設定の指定を制御できます。指定できるプロパティのタイプには 2 つあります。

- グローバルプロパティ - このプロパティは、BOE.war ファイルに含まれているすべての Web アプリケーションに影響を与えます。
- アプリケーション固有のプロパティ - 特有の Web アプリケーションのみに影響を与えるプロパティ設定

デフォルトプロパティを変更するには、カスタム設定ディレクトリを使用して、グローバルプロパティまたはアプリケーション固有のプロパティのいずれかの新しい設定を保存します。デフォルトのディレクトリは、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` にあります。

`config¥default` ディレクトリにあるプロパティは変更しないでください。

> **注記**
>
> BI プラットフォームにバンドルされている Tomcat バージョンなどの Web アプリケーションサーバの一部では、BOE.war に直接アクセスすることができます。このシナリオでは、WAR ファイルをアンデプロイすることなく、カスタム設定を直接設定できます。デプロイされた Web アプリケーションに直接アクセスできないときは、WAR ファイルをアンデプロイし、カスタマイズしてから再度デプロイする必要があります。詳細については、*SAP BusinessObjects Business Intelligence* プラットフォーム *Web* アプリケーションデプロイメントガイドを参照してください。

18.4.1.1 グローバル BOE.war プロパティ

以下の表は、BOE.war のデフォルトの `global.properties` ファイルに含まれている設定です。

これらの設定を上書きするには、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` に新しいファイルを作成します。

設定	デフォルト値	説明
`persistentcookies.enabled`	`persistentcookies.enabled=true`	Web アプリケーションのログオンページの永続 Cookie を有効化または無効化します。
`siteminder.authentication`	`siteminder.authentication=secLDAP`	SiteMinder で使用する認証方法を指定します。オプションは secLDAP および secwinAD のみです。
`siteminder.enabled`	`siteminder.enabled=false`	SiteMinder の認証を有効化または無効化します。
`sso.enabled`	`sso.enabled=false`	BI プラットフォームへのシングルサインオン (SSO) を有効化または無効化します。
`sso.sap.primary`	`sso.sap.primary=false`	SAP SSO をアプリケーションの一次シングルサインオンメカニズムとして使用するには、`true` に設定します。SAP と SiteMinder SSO の両方が使用されている場合にのみ適用されます。
`max.tree.children.threshold`	`max.tree.children.threshold=200`	ツリーリストコントロールですべてのノードを表示せず、代わりに「子供の数が多すぎます」というメッセージを表示するしきい値を指定します。
`trusted.auth.shared.secret`	なし	信用できる認証のシークレットの取得に使用するセッション変数名を指定します。共有シークレットを渡すために Web セッションを使用する場合のみ適用されます。
`trusted.auth.user.param`	なし	信用できる認証のユーザ名の取得に使用する変数を指定し、次のいずれかの値を設定できます。 • `Header` • `URL Parameter` • `Cookie` • `Session`
`trusted.auth.user.retrieval`	なし	信用できる認証のユーザ名の取得に使用するメソッドを指定し、次のいずれかの値を設定できます。 • `"REMOTE_USER"` • `"HTTP_HEADER"` • `"COOKIE"` • `"QUERY_STRING"` • `"WEB_SESSION"` • `"USER_PRINCIPAL"` 信用できる認証を無効化するには、空白を設定します。

設定	デフォルト値	説明
trusted.auth.user.namespace.enabled	trusted.auth.user.namespace.enabled=false	既存のユーザアカウントへのエイリアスの動的バインディングを有効化および無効化します。プロパティが true に設定されている場合は、信用できる認証ではユーザを BI プラットフォームに認証するためにエイリアスバインディングを使用します。エイリアスバインディングを使用すると、アプリケーションサーバは SAML サービスプロバイダとして機能するため、信用できる認証を有効にすると SAML SSO はシステムにシングルサインオンできます。false に設定すると、信用できる認証はユーザ認証に一致する名前を使用します。
vintela.enabled	vintela.enabled=false idm.realm=YOUR_REALM idm.princ=YOUR_PRINCIPAL idm.allowUnsecured=true idm.allowNTLM=false idm.logger.name=simple idm.logger.props=error-log.properties	Windows AD 認証の Vintela 設定を有効または無効にするために使用されます。
pinger.showWarningDialog.cmc	pinger.showWarningDialog.cmc=true	CMC での現在のセッションの有効期限がまもなく切れることを示すメッセージを警告ダイアログに表示するかどうかを指定します。
pinger.showWarningDialog.bilaunchpad	pinger.showWarningDialog.bilaunchpad=true	BI 起動パッドでの現在のセッションの有効期限がまもなく切れることを示すメッセージを警告ダイアログに表示するかどうかを指定します。
pinger.warningPeriod.pingIncrementsInSeconds	pinger.warningPeriod.pingIncrementsInSeconds=15	セッションの有効期限切れの警告メッセージが表示されている間の Web サーバリクエストの送信頻度を指定します。これは、警告ダイアログをアプリケーション全体で同期化するために重要です。
pinger.warningPeriod.lengthInMinutes	pinger.warningPeriod.lengthInMinutes=5	どれぐらい前にセッションの有効期限切れの警告を表示するかを指定します。
logoff.on.websession.expiry	logoff.on.websession.expiry=true	Web セッションの有効期限が切れたときに、すべてのアプリケーションセッションをログオフするかどうかを指定します。
pinger.enabled	pinger.enabled=true	セッションの有効期限切れの警告メッセージメカニズムを有効化または無効化します。
system.com.sap.bip.jcomanager.destinations.maxsize	system.com.sap.bip.jcomanager.destinations.maxsize=1000	キャッシュされた Java 接続の最大数を指定します。
httpproxy.username	httpproxy.username=myusername	HTTP プロキシサーバにログオンするためのユーザ名を指定します。
httpproxy.password	httpproxy.password=mypassword	HTTP プロキシサーバにログオンするためのパスワードを指定します。

設定	デフォルト値	説明
logon.embed.secret	なし	BI プラットフォームアプリケーションを埋め込むポータルと BI プラットフォームアプリケーションサーバ間の共有シークレットです。これは、BI プラットフォームアプリケーションがほかのページに安全に埋め込めるかの判定に使用されます。
logon.embed.timeout	logon.embed.timeout=300	BI ラウンチパッドなどの BI プラットフォームアプリケーションのポータルへの埋め込みが、何秒後に拒否されるかを指定します。BI プラットフォーム Web サーバマシンおよびポータルサーバマシンのシステムのシステムクロックが互いにこの秒数内であることを確認してください。
iview.autologoff	iview.autologoff=true	SAP NetWeaver technology platform の iViews からの即時の自動ログオフを有効にする場合は、true に設定します。
pinger.showWarningDialog	pinger.showWarningDialog=true	現在のセッションの有効期限がまもなく切れることを示すメッセージを警告ダイアログに表示するかどうかを指定します。CMC および BI ラウンチパッドには適用されません。
ure.request.queue.timeout.seconds	ure.request.queue.timeout.seconds=20	前回の要求がタイムアウトするまでに要求で待機する秒数 BI ラウンチパッドのツリーリストコントロールでユーザがナビゲーションまたはフォルダ展開アクションを実行すると、AJAX 要求は、これらアクションの待機状態になります。ユーザインタフェースは、これらの要求が完了するまで待機してから、ユーザにコントロールを渡します。この設定により、バックエンドクエリで予期しない遅延が発生した場合に、ユーザインタフェースが各要求を待機する秒数を指定します。
enable.safe.html	enable.safe.html=true	BI ワークスペースの Web ページモジュール URL で、安全な Web ページ URL を使用できます。
upload.file.maxsize.inMB	upload.file.maxsize.inMB = 0	ファイルをアップロードするための最大ファイルサイズをメガバイト単位で指定します。デフォルト値の 0 を設定した場合は、どのサイズのファイルでもアップロードすることができます。
upload.file.allowed.formats	なし	ファイルのアップロードに使用できるファイル形式を指定します。詳細については、2296060 を参照してください。
upload.file.maxsize.inMB=0	なし	メガバイト単位のローカルドキュメントアップロードの最大ファイルサイズ。整数 (10 など) にする必要があります。

設定	デフォルト値	説明
upload.file.allowed.formats=	なし	このプロパティを使用して、ローカルドキュメントのアップロードで許可される異なるファイルタイプを制御します。サポートされているファイル形式の一覧を取得するには、SAP ノート 2296060 を参照してください。 複数の形式を定義する場合、各ファイル形式をカンマで区切ります (例: txt,doc,xls)。
offlinehelp.enabled=false	なし	offlineHelp フラグを true に設定して、オフラインヘルプを有効にします。この値は、デフォルトでは false に設定されています。
offlinehelp.url=	なし	offlinehelp.url は、ユーザがオフラインフラグを true に設定しているときに使用されます。

18.4.1.2 BI ラウンチパッドのプロパティ

以下の表は、BOE war ファイルのデフォルトの bilaunchpad.properties ファイルに含まれている設定です。これらの設定を上書きするには、C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom に新しいファイルを作成します。

設定	説明
app.name	アプリケーションの表示名を指定します。Web アプリケーションのタイトルページおよびログオン画面に表示される名前。デフォルト: app.name=BI launch pad
app.name.short	アプリケーションの表示名を指定します。Web アプリケーションのタイトルページおよびログオン画面に表示される名前。デフォルト: app.name.short=BI launch pad
app.url.name	先頭に “/” 文字が付いているアプリケーションの URL 名を指定します。デフォルト: app.url.name=/BI
authentication.default	アプリケーションにユーザを認証するために使用されるデフォルトの認証方法を指定します。この設定には以下のいずれかを使用できます。 認証 / 設定値 Enterprise / secEnterprise LDAP / secLDAP Windows AD / secWinAD SAP / secSAPR3 PeopleSoft / secpsenterprise JD Edwards / secPSE1

<table>
<tr><th>設定</th><th>説明</th></tr>
<tr><td></td><td><table><tr><th>認証</th><th>設定値</th></tr><tr><td>Siebel</td><td>secSiebel7</td></tr><tr><td>Oracles EBS</td><td>secOraApps</td></tr></table>デフォルト値: authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>BI ラウンチパッドにログインするユーザに、認証方法を表示し変更するオプションがあるかどうかを指定します。デフォルト: authentication.visible=false</td></tr>
<tr><td>Authentication.VisibleList</td><td>ログイン画面に使用可能な認証タイプの一覧を表示するかどうかを指定します。使用可能な認証タイプの一覧は、次のとおりです。Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7。一覧で、Authentication.VisibleList に対して必要な認証タイプを追加または削除することにより、それらの認証タイプを有効または無効にすることを選択できます。デフォルト: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7</td></tr>
<tr><td>sap.system.client.visible
authentication.sapSystem
authentication.sapClient</td><td>認証タイプとして SAP を選択した場合に、[SAP システム] および [SAP クライアント] フィールドを表示するかどうかを指定します。デフォルト: sap.system.client.visible=true。sap.system.client.visible を sap.system.client.visible=false に設定した場合、authentication.sapSystem および authentication.sapClient パラメータをそれぞれ使用して、プロパティファイルで [SAP システム] と [SAP クライアント] の値を指定することができます。</td></tr>
<tr><td>cms.default</td><td>デフォルトの CMS 名を指定します。デフォルト値: cms.default=[name of host machine]</td></tr>
<tr><td>cms.visible</td><td>BI ラウンチパッドにログインするユーザに、CMS 名を表示し変更するオプションがあるかどうかを指定します。デフォルト: cms.visible=true</td></tr>
<tr><td>dialogue.prompt.enabled</td><td>ダイアログボックスの入力ページから離れたときに、ユーザにプロンプトを表示するかどうかを指定します。デフォルト値: dialogue.prompt.enabled=false</td></tr>
<tr><td>logontoken.enabled</td><td>ユーザが BI ラウンチパッドにログオンした後に、セッションのトークンの作成を有効にするかどうかを指定します。トークンは、Cookie に保存されます。デフォルト: logontoken.enabled=false</td></tr>
</table>

設定	説明
SMTPFrom	オブジェクトを出力先にスケジュールするときの [差出人] フィールドを有効化または無効化します。デフォルト値: SMTPFrom=true 値が false に設定されている場合、[差出人] フィールドは表示されず、システムは [差出人] の電子メール値を次の順で取得しようと試みます。 1. まず、レポートオブジェクトのレポートのデフォルトから取得します。 2. 次に、ログオン中のユーザのユーザプロファイル上にある電子メールアドレスから取得します。 3. 最後に、Job Server のデフォルトから取得します。
url.exit	BI ラウンチパッドセッションの終了後、ユーザをどの URL にリダイレクトするかを指定します。この設定は、外部の認証プロセスを通してアプリケーションにログインしたユーザにのみ適用されます。
disable.locale.preference	BI ラウンチパッドのローカル基本設定のユーザによる編集および表示を有効化または無効化します。デフォルト: disable.locale.preference=false
extlogon.allow.logoff	BI ラウンチパッドセッションを閉じたときのユーザセッションの自動ログオフを有効化または無効化します。ユーザが BI ラウンチパッドをログオフしたときに、ユーザセッションが自動的に終了しないようにするには、false に設定します。デフォルト: extlogon.allow.logoff=true
logon.allowInsecureEmbedding	有効な埋め込みトークンを渡さずにほかのページでこのアプリケーションをフレームとして埋め込めるようにするかを指定します。デフォルト: logon.allowInsecureEmbedding=false
sso.types.and.order	有効にする SSO タイプのカンマ区切りリスト、およびそれらの実行順序を指定します。 空のリストは、レガシーの順序付けが使用されることを意味します。 リストを指定すると、レガシーオプションは無視されます。 有効なオプション: vintela、trustedIIS、trustedHeader、trustedParameter、trustedCookie、trustedSession、trustedUserPrincipal、trustedVintela、trustedX509、sapSSO、および siteminder。 何も指定しない場合は、次のように指定します。none
allowed.cms	安全なログインを保証し、サーバ側要求の偽造を防ぐために、有効な CMS 名または IP とポート番号のホワイトリストを作成することができます。ログイン中に入力した値がホワイト

設定	説明
	リストの値と完全に一致する場合にのみ、アプリケーションにログインできます。 allowed.cms プロパティに、CMS 名または IP とポート番号の一覧を入力します。たとえば、 `allowed.cms =<cms name or IP>:<port number>.` のようにします。接続先の CMS が複数ある場合は、次のように値をカンマで区切って入力します。`allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number>` **注記** • CMS 名または IP のいずれかを使用してログインするには、これら両方を `allowed.cms` プロパティに追加します。 • ポート番号はログイン画面でオプションであるため、ホワイトリストで省略することもできます。この場合は、デフォルトポートにログインします。ただし、ホワイトリストにポート番号が存在して、ログイン中に入力しなかった場合は、ログインは失敗します。 以下に、ホワイトリストを使用する必要のないシナリオを示します。 • `cms.visible` の値が false に設定されていて、`cms.default` に CMS が設定されている場合。 • CMS がクラスタ化されていて、クラスタ名を使用してログインする場合。特定のクラスタ (CMS) にログインしようとしている場合は、`allowed.cms` プロパティにその CMS 名が含まれている必要があります。 • シングルサインオンを使用してログインする場合。

18.4.1.3 Fiori 対応 BI ラウンチパッドのプロパティ

以下の表は、BOE war ファイルのデフォルトの `FioriBI.properties` ファイルに含まれている設定です。これらの設定を上書きするには、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` に新しいファイルを作成します。

注記

BI 4.2 SP5 では、ファイル “Bing.properties” の名前がファイル “FioriBI.properties” に変更されます。任意の古いバージョンから BI 4.2 SP5 に更新またはアップグレードする場合、Fiori 対応 BI ラウンチパッドの既存の

設定を保持するには、Fiori 対応 BI ラウンチパッドのプロパティファイルの名前を “Bing.properties” から “FioriBI.properties” にマニュアルで変更する必要があります。

設定	説明
`app.name`	アプリケーションの表示名を指定します。Web アプリケーションのタイトルページおよびログオン画面に表示される名前。デフォルト: `app.name=BI launch pad`
`app.name.short`	アプリケーションの表示名を指定します。Web アプリケーションのタイトルページおよびログオン画面に表示される名前。デフォルト: `app.name.short=BI launch pad`
`app.url.name`	先頭に “/” 文字が付いているアプリケーションの URL 名を指定します。デフォルト: `app.url.name=/BILaunchpad`
`authentication.default`	アプリケーションにユーザを認証するために使用されるデフォルトの認証方法を指定します。この設定には以下のいずれかを使用できます。 **認証** / **設定値** Enterprise: `secEnterprise` LDAP: `secLDAP` Windows AD: `secWinAD` SAP: `secSAPR3` PeopleSoft: `secpsenterprise` JD Edwards: `secPSE1` Siebel: `secSiebel7` Oracles EBS: `secOraApps` デフォルト: `authentication.default=secEnterprise`
`authentication.visible`	Fiori 対応 BI ラウンチパッドにログインするユーザに、認証方法を表示および変更するオプションがあるかどうかを指定します。デフォルト: `authentication.visible=false`
`Authentication.VisibleList`	ログイン画面に使用可能な認証タイプの一覧を表示するかどうかを指定します。使用可能な認証タイプの一覧は、次のとおりです。`Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`。一覧で、`Authentication.VisibleList` に対して必要な認証タイプを追加または削除することにより、それらの認証タイプを有効または無効にすることを選択できます。デフォルト: `Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7`

設定	説明

`sap.system.client.visible`
 	
`authentication.sapSystem`
 	
`authentication.sapClient`
	認証タイプとして SAP を選択した場合に、[*SAP システム*] および [*SAP クライアント*] フィールドを表示するかどうかを指定します。デフォルト: `sap.system.client.visible=true`。`sap.system.client.visible` を `sap.system.client.visible=false` に設定した場合、`authentication.sapSystem=` および `authentication.sapClient=` パラメータをそれぞれ使用して、プロパティファイルで [SAP システム] と [SAP クライアント] の値を指定することができます。

`cms.default`	デフォルトの CMS 名を指定します。デフォルト: `cms.default=[name of host machine]`
`cms.visible`	Fiori 対応 BI ラウンチパッドにログインするユーザに、CMS 名を表示および変更するオプションがあるかどうかを指定します。デフォルト: `cms.visible=true`
`dialogue.prompt.enabled`	ダイアログボックスの入力ページから離れたときに、ユーザにプロンプトを表示するかどうかを指定します。デフォルト: `dialogue.prompt.enabled=false`
`logontoken.enabled`	ユーザが BI ラウンチパッドにログオンした後に、セッションのトークンの作成を有効にするかどうかを指定します。トークンは、Cookie に保存されます。デフォルト: `logontoken.enabled=false`
`SMTPFrom`	オブジェクトを出力先にスケジュールするときの [差出人] フィールドを有効化または無効化します。デフォルト: `SMTPFrom=true` 値が `false` に設定されている場合、[差出人] フィールドは表示されず、システムは [差出人] の電子メール値を次の順で取得しようと試みます。 1. まず、レポートオブジェクトのレポートのデフォルトから取得します。 2. 次に、ログオン中のユーザのユーザプロファイル上にある電子メールアドレスから取得します。 3. 最後に、Job Server のデフォルトから取得します。
`url.exit`	Fiori 対応 BI ラウンチパッドセッションの終了後、ユーザをどの URL にリダイレクトするかを指定します。この設定は、外部の認証プロセスを通してアプリケーションにログインしたユーザにのみ適用されます。
`disable.locale.preference`	Fiori 対応 BI ラウンチパッドのローカル基本設定のユーザによる編集および表示を有効化または無効化します。デフォルト: `disable.locale.preference=false`
`extlogon.allow.logoff`	Fiori 対応 BI ラウンチパッドセッションを閉じたときのユーザセッションの自動ログオフを有効化または無効化します。ユーザが BI ラウンチパッドをログオフしたときに、ユーザセッションが自動的に終了しないようにするには、false に設定します。デフォルト: `extlogon.allow.logoff=true`

設定	説明
logon.allowInsecureEmbedding	有効な埋め込みトークンを渡さずに他のページでこのアプリケーションをフレームとして埋め込めるようにするかを指定します。デフォルト: logon.allowInsecureEmbedding=false
sso.types.and.order	有効にする SSO タイプのカンマ区切りリスト、およびそれらの実行順序を指定します。 空のリストは、レガシーの順序付けが使用されることを意味します。 リストを指定すると、レガシーオプションは無視されます。 有効なオプション: vintela、trustedIIS、trustedHeader、trustedParameter、trustedCookie、trustedSession、trustedUserPrincipal、trustedVintela、trustedX509、sapSSO、および siteminder。 何も指定しない場合は、none と指定します。
allowed.cms	安全なログインを保証し、サーバ側要求の偽造を防ぐために、有効な CMS 名または IP とポート番号のホワイトリストを作成することができます。ログイン中に入力した値がホワイトリストの値と完全に一致する場合にのみ、アプリケーションにログインできます。 allowed.cms プロパティに、CMS 名または IP とポート番号の一覧を入力します。たとえば、allowed.cms =<cms name or IP>:<port number>. のようにします。接続先の CMS が複数ある場合は、allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number> のように値をカンマで区切って入力します。 **注記** • CMS 名または IP のいずれかを使用してログインするには、これら両方を allowed.cms プロパティに追加します。 • ポート番号はログイン画面でオプションであるため、ホワイトリストで省略することもできます。この場合は、デフォルトポートにログインします。ただし、ホワイトリストにポート番号が存在して、ログイン中に入力しなかった場合は、ログインは失敗します。 以下に、ホワイトリストを使用する必要のないシナリオを示します。

設定	説明
	• `cms.visible` の値が false に設定されていて、`cms.default` に CMS が設定されている場合。 • CMS がクラスタ化されていて、クラスタ名を使用してログインする場合。特定のクラスタ (CMS) にログインしようとしている場合は、`allowed.cms` プロパティにその CMS 名が含まれている必要があります。 • シングルサインオンを使用してログインする場合。
upload.file.maxsize.inMB=0	メガバイト単位のローカルドキュメントアップロードの最大ファイルサイズ。整数にする必要があります (10 など)。
upload.file.allowed.formats=	このプロパティを使用して、ローカルドキュメントのアップロードで許可される異なるファイルタイプを制御します。サポートされているファイル形式の一覧を取得するには、SAP ノート 2296060 を参照してください。 複数の形式を定義する場合、各ファイル形式をカンマで区切ります (例: txt,doc,xls)。
app.custom.banner.message	BI ラウンチパッドでのバナーメッセージを指定します。
logon.webssoauthnetication.framework=None	このプロパティは、Web SSO 認証ワークフローを有効化するために使用されます。使用可能な値は、None、OpenId、および SAML です。
openid.restful.url=	このプロパティは、CMC で提供される Restful URL を設定するために使用されます。例: `http://<hostname>:<portNo>/biprws`

18.4.1.4 OpenDocument プロパティ

以下の表は、BOE war ファイルのデフォルトの `opendocument.properties` ファイルに含まれている設定です。これらの設定を上書きするには、`C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom` に新しいファイルを作成します。

設定	説明
`app.name`	アプリケーションの表示名を指定します。Web アプリケーションのタイトルページおよびログオン画面に表示される名前。デフォルト: `app.name=SAP BusinessObjects OpenDocument`
`app.name.short`	アプリケーションの表示名を指定します。Web アプリケーションのタイトルページおよびログオン画面に表示される名前。デフォルト: `app.name.short=OpenDocument`

<table>
<tr><th>設定</th><th>説明</th></tr>
<tr><td>authentication.default</td><td>アプリケーションにユーザを認証するために使用されるデフォルトの認証方法を指定します。この設定には以下のいずれかを使用できます。
<table><tr><th>認証</th><th>設定値</th></tr><tr><td>Enterprise</td><td>secEnterprise</td></tr><tr><td>LDAP</td><td>secLDAP</td></tr><tr><td>Windows AD</td><td>secWinAD</td></tr><tr><td>SAP</td><td>secSAPR3</td></tr><tr><td>PeopleSoft</td><td>secpsenterprise</td></tr><tr><td>JD Edwards</td><td>secPSE1</td></tr><tr><td>Siebel</td><td>secSiebel7</td></tr><tr><td>Oracles EBS</td><td>secOraApps</td></tr></table>デフォルト値:
authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>OpenDocument にログインするユーザに、認証方法を表示し変更するオプションがあるかどうかを指定します。デフォルト: authentication.visible=false</td></tr>
<tr><td>Authentication.VisibleList</td><td>ログイン画面に使用可能な認証タイプの一覧を表示するかどうかを指定します。使用可能な認証タイプの一覧は、次のとおりです。
Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7。一覧で、Authentication.VisibleList に対して必要な認証タイプを追加または削除することにより、それらの認証タイプを有効または無効にすることを選択できます。デフォルト:
Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7</td></tr>
<tr><td>sap.system.client.visible
authentication.sapSystem
authentication.sapClient</td><td>認証タイプとして SAP を選択した場合に、[SAP システム] および [SAP クライアント] フィールドを表示するかどうかを指定します。デフォルト:
sap.system.client.visible=true。
sap.system.client.visible を sap.system.client.visible=false に設定した場合、authentication.sapSystem= および authentication.sapClient= パラメータをそれぞれ使用して、プロパティファイルで [SAP システム] と [SAP クライアント] の値を指定することができます。</td></tr>
<tr><td>cms.default</td><td>デフォルトの CMS 名を指定します。デフォルト値:
cms.default=[name of host machine]</td></tr>
</table>

設定	説明
cms.visible	OpenDocument にログインするユーザに、CMS 名を表示し変更するオプションがあるかどうかを指定します。デフォルト: cms.visible=true
logontoken.enabled	ユーザが OpenDocument にログオンした後に、セッションのトークンの作成を有効にするかどうかを指定します。トークンは、Cookie に保存されます。デフォルト値: logontoken.enabled=false
extlogon.allow.logoff	OpenDocument セッションを閉じると、ユーザのユーザセッションの自動的なログオフを有効化または無効化します。ユーザが OpenDocument をログオフするときに、ユーザセッションが自動的に終了しないようにするには false を設定します。デフォルト: extlogon.allow.logoff=true
SAPLogonToken.enabled	RESTful Web サービス SAP ログオントークンによる BI プラットフォームへの認証を許可するかどうかを指定します。SAP ログオントークンは、RESTful Web サービス URL を使用したログオンに成功した後、要求ヘッダの X-SAP-LogonToken 値によって指定されます。デフォルト: SAPLogonToken.enabled=true
logon.allowInsecureEmbedding=false	有効な埋め込みトークンを渡さずにほかのページでこのアプリケーションをフレームとして埋め込めるようにするかを指定します。デフォルト: logon.allowInsecureEmbedding=false
sso.types.and.order	有効にする SSO タイプのカンマ区切りリスト、およびそれらの実行順序を指定します。 空のリストは、レガシーの順序付けが使用されることを意味します。 リストを指定すると、レガシーオプションは無視されます。 有効なオプション: serializedSession、sapLogonToken、trustedIIS、trustedHeader、trustedParameter、trustedCookie、trustedSession、trustedUserPrincipal、trustedVintela、vintela、infoview、trustedX509、sapSSO、および siteminder。 何も指定しない場合は、次のように指定します。none
allowed.cms	安全なログインを保証し、サーバ側要求の偽造を防ぐために、有効な CMS 名または IP とポート番号のホワイトリストを作成することができます。ログイン中に入力した値がホワイトリストの値と完全に一致する場合にのみ、アプリケーションにログインできます。 allowed.cms プロパティに、CMS 名または IP とポート番号の一覧を入力します。たとえば、 allowed.cms =<cms name or IP>:<port number>. のようにします。接続先の CMS が複数ある場合は、次のように値をカンマで区切

設定	説明
	って入力します。allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number> **注記** • CMS 名または IP のいずれかを使用してログインするには、これら両方を allowed.cms プロパティに追加します。 • ポート番号はログイン画面でオプションであるため、ホワイトリストで省略することもできます。この場合は、デフォルトポートにログインします。ただし、ホワイトリストにポート番号が存在して、ログイン中に入力しなかった場合は、ログインは失敗します。 以下に、ホワイトリストを使用する必要のないシナリオを示します。 • cms.visible の値が false に設定されていて、cms.default に CMS が設定されている場合。 • CMS がクラスタ化されていて、クラスタ名を使用してログインする場合。特定のクラスタ (CMS) にログインしようとしている場合は、allowed.cms プロパティにその CMS 名が含まれている必要があります。 • シングルサインオンを使用してログインする場合。

18.4.1.5 CMC プロパティ

以下の表は、BOE.war のデフォルトの cmc.properties ファイルに含まれている設定です。これらの設定を上書きするには、C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥config¥custom に新しいファイルを作成します。

設定	説明
app.url.name	先頭に“/” 文字が付いているアプリケーションの URL 名を指定します。デフォルト値: app.url.name=/CMC
authentication.default	アプリケーションにユーザを認証するために使用されるデフォルトの認証方法を指定します。この設定には以下のいずれかを使用できます。 認証 / 設定値 Enterprise / secEnterprise LDAP / secLDAP

設定	説明
	<table><tr><th>認証</th><th>設定値</th></tr><tr><td>Windows AD</td><td>secWinAD</td></tr><tr><td>SAP</td><td>secSAPR3</td></tr><tr><td>PeopleSoft</td><td>secpsenterprise</td></tr><tr><td>JD Edwards</td><td>secPSE1</td></tr><tr><td>Siebel</td><td>secSiebel7</td></tr><tr><td>Oracles EBS</td><td>secOraApps</td></tr></table> デフォルト値: authentication.default=secEnterprise
authentication.visible	CMC にログインするユーザに、認証方法を表示し変更するオプションがあるかどうかを指定します。デフォルト値: authentication.visible=false
Authentication.VisibleList	ログイン画面に使用可能な認証タイプの一覧を表示するかどうかを指定します。使用可能な認証タイプの一覧は、次のとおりです。 Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7。一覧で、Authentication.VisibleList に対して必要な認証タイプを追加または削除することにより、それらの認証タイプを有効または無効にすることを選択できます。デフォルト: Authentication.VisibleList=secEnterprise,secLDAP,secWinAD,secOraApps,secSAPR3,secPSE1,secpsenterprise,secSiebel7
sap.system.client.visible authentication.sapSystem authentication.sapClient	認証タイプとして SAP を選択した場合に、[*SAP システム*] および [*SAP クライアント*] フィールドを表示するかどうかを指定します。デフォルト: sap.system.client.visible=true。 sap.system.client.visible を sap.system.client.visible=false に設定した場合、authentication.sapSystem= および authentication.sapClient= パラメータをそれぞれ使用して、プロパティファイルで [SAP システム] と [SAP クライアント] の値を指定することができます。
cms.default	デフォルトの CMS 名を指定します。デフォルト値: cms.default=[name of host machine]
cms.visible	CMC にログインするユーザに、CMS 名を表示し変更するオプションがあるかどうかを指定します。デフォルト値: cms.visible=true
dialogue.prompt.enabled	ダイアログボックスの入力ページから離れたときに、ユーザにプロンプトを表示するかどうかを指定します。デフォルト値: dialogue.prompt.enabled=false

設定	説明
logontoken.enabled	ユーザが CMC にログオンした後に、セッションのトークンの作成を有効にするかどうかを指定します。トークンは、Cookie に保存されます。デフォルト値: logontoken.enabled=false
SMTPFrom	オブジェクトを出力先にスケジュールするときの [差出人] フィールドを有効化または無効化します。デフォルト値: SMTPFrom=true 値が false に設定されている場合、[差出人] フィールドは表示されず、システムは [差出人] の電子メール値を次の順で取得しようと試みます。 1. まず、レポートオブジェクトのレポートのデフォルトから取得します。 2. 次に、ログオン中のユーザのユーザプロファイル上にある電子メールアドレスから取得します。 3. 最後に、Job Server のデフォルトから取得します。
ulr.exit	CMC セッションの終了後、ユーザをどの URL にリダイレクトするかを指定します。この設定は、外部の認証プロセスを通してアプリケーションにログインしたユーザにのみ適用されます。
allowed.cms	安全なログインを保証し、サーバ側要求の偽造を防ぐために、有効な CMS 名または IP とポート番号のホワイトリストを作成することができます。ログイン中に入力した値がホワイトリストの値と完全に一致する場合にのみ、アプリケーションにログインできます。 allowed.cms プロパティに、CMS 名または IP とポート番号の一覧を入力します。たとえば、 allowed.cms =<cms name or IP>:<port number>. のようにします。接続先の CMS が複数ある場合は、次のように値をカンマで区切って入力します。allowed.cms =<cms name or IP>:<port number>, <cms name or IP>:<port number> **注記** • CMS 名または IP のいずれかを使用してログインするには、これら両方を allowed.cms プロパティに追加します。 • ポート番号はログイン画面でオプションであるため、ホワイトリストで省略することもできます。この場合は、デフォルトポートにログインします。ただし、ホワイトリストにポート番号が存在して、ログイン中に入力しなかった場合は、ログインは失敗します。

設定	説明
	以下に、ホワイトリストを使用する必要のないシナリオを示します。 • `cms.visible` の値が false に設定されていて、`cms.default` に CMS が設定されている場合。 • CMS がクラスタ化されていて、クラスタ名を使用してログインする場合。特定のクラスタ (CMS) にログインしようとしている場合は、`allowed.cms` プロパティにその CMS 名が含まれている必要があります。 • シングルサインオンを使用してログインする場合。

18.5 BI 起動パッドおよび OpenDocument ログオンエントリポイントのカスタマイズ

BI 起動パッドおよび OpenDocument Web アプリケーションのログオンページをカスタマイズできます。たとえば、会社のロゴまたは企業のスタイルシートを使用してログオンページをカスタマイズしたり、信用できる認証を有効化するカスタマイズされたログオンページを作成できます。

ログオンページをカスタマイズするには、BI 起動パッドに保存されている `custom.jsp` ファイルおよび `BOE.war` Web アプリケーションの OpenDocument アプリケーション領域を変更して、`BOE.war` Web アプリケーションを BI プラットフォームシステムに再デプロイします。ユーザは一意の URL に移動することでカスタムログオンエントリポイントにアクセスします。

これらの例を行うためには、BI プラットフォーム Web アプリケーションのデプロイに対する知識が必要です。詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

18.5.1 BI 起動パッドおよび OpenDocument ファイルの場所

BI ラウンチパッドおよび OpenDocument Web アプリケーションは、`BOE.war` Web アーカイブファイル内にパッケージ化されています。`BOE.war` アーカイブの場所は、`BOE.properties` ファイルに定義されています。

Windows システムでは、`BOE.properties` ファイルは、ここに保存されています。

- `<BOE_INSTALL_DIR>¥SAP BusinessObjects Enterprise XI 4.0¥wdeploy¥conf¥apps¥BOE.properties`

UNIX システムでは、`BOE.properties` ファイルは、ここに保存されています。

- `<BOE_INSTALL_DIR>/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties`

以下の表は、BI 起動パッドおよび OpenDocument アプリケーションの両方の `BOE.war` Web アーカイブファイル内の共通ファイルの位置を定義しています。

BI 起動パッドファイルの場所

> ⓘ 注記
>
> BI 起動パッド Web アプリケーションの旧称は、InfoView です。

ファイルの種類	場所
カスタムログオンスクリプト	WEB-INF¥eclipse¥plugins¥webpath.InfoView¥web¥custom.jsp
追加ファイルのディレクトリ	WEB-INF¥eclipse¥plugins¥webpath.InfoView¥web¥noCacheCustomResources
カスタムログオン URL	http://<servername>:<port>/BOE/BI/custom.jsp

OpenDocument ファイルの場所

ファイルの種類	場所
カスタムログオンスクリプト	WEB-INF¥eclipse¥plugins¥webpath.OpenDocument¥web¥opendoc¥custom.jsp
追加ファイルのディレクトリ	WEB-INF¥eclipse¥plugins¥webpath.OpenDocument¥web¥noCacheCustomResources
カスタムログオン URL	http://<servername>:<port>/BOE/OpenDocument/opendoc/custom.jsp

18.5.2 カスタムログオンページを定義する

BI プラットフォームのログオンページへのエントリポイントをカスタマイズできます。 たとえば、会社のロゴを表示して企業のスタイルシートを使用するカスタムログオンページを作成できます。

custom.jsp ファイルを編集して、ユーザのログオンをカスタマイズし、補完するファイルを noCacheCustomResources フォルダに配置します。

この例では、標準ログオンページにユーザをリダイレクトするカスタムログオンページを作成する方法を示します。

1. カスタムログオンコードを含むファイルを作成し、noCacheCustomResources フォルダの custom.js に保存します。

   この例では、標準ログオンページにユーザをリダイレクトする機能である logon.faces を定義します。

   ```
   function load() {window.location =  "logon.faces";}
   ```

2. custom.jsp ファイルを編集してログオンページをカスタマイズします。

   この例では、ようこそメッセージと、custom.js ファイルに定義されている load メソッドを呼び出すハイパーリンクを表示します。

   ```
   <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
    "http://www.w3.org/TR/html4/loose.dtd">
   ```

```
<%@ page language=  "java" contentType=  "text/html;charset=utf-8"%>
<html>
  <head> <title>Welcome</title>
  </head>
  <body>
    <script type=  "text/javascript" src=  "noCacheCustomResources/
custom.js"></script>
    <p>Welcome to ABC corporation.</p>
    <a href= "javascript:load()">Enter</a>
  </body>
</html>
```

3. BOE.war Web アプリケーションを再デプロイし、Web サーバを再起動します。

18.5.3 信用できる認証をログオンに追加する

信用できる認証を有効化するには、信用できるユーザを custom.jsp ファイルのセッション属性として設定し、global.properties ファイルのコピーにある認証設定を変更します。global.properties ファイルのカスタムコピーの値はデフォルト値を上書きします。

> **注記**
>
> セキュリティ上の理由から、信用できる認証を HTTPS なしで有効化しないでください。信用できる認証を https なしで有効にすると、URL が認証されていないユーザに公開されるため、セキュリティ侵害とみなされます。セキュリティ侵害を防ぐために、有効な証明書を使用してユーザーの情報を検証できます。詳細については、1388240 を参照してください。

1. custom.jsp ファイルを編集して、信用できるユーザを定義するセッション属性を設定します。

```
request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
```

2. WEB-INF¥config¥default¥global.properties を WEB-INF¥config¥custom¥global.properties にコピーして、global.properties ファイルのカスタムコピーを作成します。
3. シングルサインオン (SSO) を有効化するには、WEB-INF¥config¥custom¥global.properties を編集します。

```
sso.enabled=true
```

4. 信用できるユーザセッション変数および共有シークレットを含む信用できる認証パラメータを設定するには、WEB-INF¥config¥custom¥global.properties を変更します。

   "..." をシステムの共有シークレットに置き換えます。

```
trusted.auth.user.param=TrustedUserAttribute
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.shared.secret="..."
```

   詳細については、Web アプリケーションの信頼できる認証の設定に関する関連トピックを参照してください。
5. Web アプリケーションを再デプロイして Web サーバを再起動します。
6. CMC で、信頼できる認証を有効にします。

   [認証] タブで、[エンタープライズ] をダブルクリックし、[信頼できる認証を有効にする] チェックボックスを選択します。

関連情報

信用できる認証の有効化 [248 ページ]
Web アプリケーションに対して信用できる認証を設定する [254 ページ]

18.6 アプリケーションユーザインタフェースのカスタマイズ

一部のアプリケーションユーザインタフェースを CMC でカスタマイズできます。

セントラル管理コンソールで、一部のアプリケーションの外観をカスタマイズできます。 たとえば、ユーザインタフェース要素を切り替えることができます。

18.6.1 Web Intelligence

18.6.1.1 ユーザグループおよびフォルダによる Web Intelligence インタフェース要素のカスタマイズ

カスタマイゼーションにより、Web Intelligence ドキュメントを含むユーザグループおよびフォルダに応じて、複数のインタフェース要素を非表示にし、エンドユーザによるアプリケーションとの対話を簡略化することができます。データソースタイプの非表示、編集モードの切り替え、自動リフレッシュ機能の無効化などを行うことができます。

デフォルトでは、すべてのインタフェース要素が有効化されています。これらを非表示にするには、セントラル管理コンソールを使用します。以下の表に、非表示にできるユーザインタフェース要素を示します。

機能一覧	説明
モード	ドロップダウンボタンを使用してユーザがアクセスできる利用可能モードが非表示になります。 • 読み取り ドロップダウンボタンから読み取りモードが非表示になります。 • デザイン ドロップダウンボタンからデザインモードと構造モードの両方が非表示になります。 • データ ドロップダウンボタンからデータモードが非表示になります。 すべてのモードが無効になっている場合、ドキュメントは読み取りモードでのみ開くことができます。

機能一覧	説明
場所	データソースのカテゴリ全体を非表示にします。以下のカテゴリを無効化できます。 • BI プラットフォームリポジトリ • ローカル (リッチクライアントのみで利用可能) • Web サービス • Google ドライブ • Microsoft OneDrive
データソース	デザインモードでは、データソースの選択およびソースの変更ダイアログボックスで使用できるデータソースを制限できます。 無効化できるデータソースは次のとおりです。 • ユニバース • Web Intelligence ドキュメント • Excel ファイル • テキストファイル • SAP BW • SAP HANA ビュー • SQL クエリの直接入力 • OData • Google スプレッドシート
クエリ	• 最新表示 読み取りモードで、ツールバーのデータセクションが非表示になります。デザインモードでは、最新表示ドロップダウンメニュー、すべて最新表示コマンド、実行ボタン、およびそのドロップダウンメニューがクエリパネルで非表示になります。 • 高度な最新表示 デザインモードで、最新表示ドロップダウンメニューの高度な最新表示コマンドが非表示になります。 • 自動最新表示 プレゼンテーションモードで、自動最新表示オプションが非表示になります。 • ソースの変更 デザインモードで、ドキュメントのデータソースを変更する機能が非表示になります。
データ	データモードで、キューブの統合機能が非表示になります。
分析	• ドリル 読み取りモードとデザインモードの両方で、ツールバーの分析セクションでドリルチェックボックスが、フィルタバーでドリルフィルタが非表示になります。また、レポートでは、ドリル可能な値はハイパーリンクとして表示されず、これらの値で使用できるドリルアクションとアイコンは非表示になります。 デザインモードでは、データフィルタの下で、ビルドパネルのドリルフィルタが非表示になります。 • データ変更の追跡 読み取りモードとデザインモードの両方で、ツールバーからデータ変更の追跡と変更の表示が非表示になります。

機能一覧	説明
ドキュメント	• 新規、開く、保存、お気に入り、プレゼンテーションモード。 ツールバーから対応するボタンが非表示になります。 • コメント 読み取りモードとデザインモードの両方で、サイドパネルのコメントタブと、コンテキストメニューのコメントコマンドが非表示になります。 • 共有要素 デザインモードで、サイドパネルの共有要素タブと、ツールバーの挿入セクションに含まれる共有要素コマンドが非表示になります。
エクスポート先	どのモードでも、では、以下にドキュメントレポートおよびキューブをエクスポートする機能が非表示になります。 • Excel • PDF • HTML • TXT • CSV
リンクの生成	デザインモードで、OpenDocument リンクを作成し、クエリと個別のレポート要素を生成するための機能がコンテキストメニューから非表示になります。
スケジュールおよび公開	ドキュメントをスケジュールし、TXT、XLS、PDF、HTML、MHTML、および CSV に公開するための機能が非表示になります。

18.6.1.1.1 カスタマイズインタフェース

カスタマイズによってフォルダに含まれるドキュメントが自動的に活用されるように、個々のフォルダを選択することができます。[カスタマイズされたフォルダ] 領域で 1 つ以上のフォルダを選択し、[機能] タブに移動してカスタマイジングを開始します。デフォルトでは、カスタマイズは選択したフォルダ内のすべてのドキュメントに適用されます。

[機能] タブには、有効化または無効化できるすべての機能が一覧表示されます。専用のチェックボックスを使用して、オンとオフを切り替えます。

18.6.1.1.2 カスタマイズルール

次のルールは、カスタマイズを定義してユーザに適用する際に使用されます。

- ユーザが異なるグループに属する場合、小さい ID を持つグループに定義されたカスタマイズのみが適用されます。このユーザを含む他のグループに定義されたカスタマイズは適用されません。
- ネストされたフォルダ構造の場合、カスタマイズされたフォルダの一覧に追加されたドキュメントの直属の親フォルダは、ユーザインタフェース要素、機能、および拡張機能に関するカスタマイズを定義します。
- デフォルトフォルダに対して定義されたカスタマイズは、個人用ドキュメントおよび受信ボックスに保存されたドキュメントに適用されます。このドキュメントの親フォルダはカスタマイズされません。

- ユーザインタフェース要素に対して定義されたカスタマイズは、機能に対して定義されたカスタマイズに優先されます。機能はすべてのユーザインタフェース要素を有効化するためのショートカットに過ぎないためです。
- シナリオ: カスタマイズ要素がツリー表示で示され、システムでノードを無効化する場合。ここで、このシステムをノードに新しいアイテムがある製品の新しいバージョンにアップグレードすると、これらのアイテムは、上位ノードが無効化されている場合でも、デフォルトで有効化されます。

18.6.1.1.3 Web Intelligence インタフェースの表示をカスタマイズする

選択されたユーザグループとドキュメントフォルダに対してメニュー項目、サブ項目、および機能を非表示にすることで、Web Intelligence ユーザインタフェースの表示をカスタマイズできます。

1. 管理者として CMC にログインします。
2. 整理リストから、ユーザとグループを選択します。
3. グループ階層リストで、ユーザグループを選択します。
4. アクションリストでカスタマイズをクリックします。
5. [カスタマイズされたフォルダ] セクションで、次のいずれかを実行します。

オプション	説明
デフォルトのカスタマイズを定義する	1. [カスタマイズされたフォルダ] 領域で [デフォルトフォルダ] を選択します。
選択したユーザグループにカスタマイズを適用するドキュメントフォルダを追加する	1. [フォルダの追加] をクリックします。 2. フォルダを選択します。 フォルダは [カスタマイズされたフォルダ] 領域に表示されます。
別のフォルダに同じカスタマイズを再定義しないようにする	1. [カスタマイズされたフォルダ] 領域で、カスタマイズをコピーするフォルダを選択します。 2. ドロップダウンリストで [カスタマイズの複製] をクリックします。 3. カスタマイズを定義するフォルダを選択します。 4. [カスタマイズの貼り付け] をクリックします。 5. ステップ 7 に進みます。
特定のフォルダのカスタマイズを削除する	1. [カスタマイズされたフォルダ] 領域で、フォルダを選択します。 2. ドロップダウンリストで [フォルダの削除] をクリックします。 3. ステップ 7 に進みます。 **注記** [デフォルトフォルダ] は削除できません。

6. [機能] タブで項目を選択または選択解除し、Web Intelligence でこの項目の表示または非表示を切り替えます。

親項目のすべての子を選択解除すると、親項目も Web Intelligence で選択解除され非表示になります。詳細については、ユーザグループおよびフォルダによる Web Intelligence インタフェース要素のカスタマイズ [744 ページ]を参照してください。

7. 保存して閉じるをクリックします。

カスタマイズを保存すると、選択されたグループのすべてのユーザで、次回 BI ラウンチパッドにログオンして Web Intelligence を開く際にこれらの変更が反映されます。

> ⓘ 注記
>
> カスタマイズしたグループのユーザとして BI ラウンチパッドにログオンし、Web Intelligence を起動して、インタフェースがカスタマイズ設定に一致していることを確認することをお勧めします。

18.6.1.2 Web Intelligence コンテンツの配置

Web Intelligence ドキュメントを作成するときには、ドキュメントコンテンツの配置方法 (左から右、または右から左) を選択します。

リッチクライアントインタフェースでは、コンテンツの配置は BI ラウンチパッドの基本設定のロケール設定によって決まります。

- 優先表示ロケールと製品ロケールの両方が右から左へ読む言語に設定されている場合のみ、右から左の配置が使用されます。
- その他の場合はすべて、コンテンツの配置は左から右になります。

> ⓘ 注記
>
> ロケールの設定方法の詳細については、*Business Intelligence* ラウンチパッドユーザガイドを参照してください。

> ⓘ 注記
>
> コンテンツの配置は、ドキュメントの作成時にのみ適用され、既存のドキュメントには影響しません。

18.6.1.3 特定のユーザグループに対する Web Intelligence ユーザインタフェース拡張ポイントの有効化

選択したユーザグループにカスタマイズされたインタフェース拡張へのアクセスを許可するよう、Web Intelligence 権限を設定できます。 利用可能な拡張バンドルおよび REST Web サービス API 呼び出しの詳細については、*Web Intelligence* および *BI* セマンティックレイヤ向け *SAP BusinessObjects BI* 開発者ガイドを参照してください。

18.6.1.3.1 Web Intelligence ユーザインタフェース拡張ポイントを有効化する

- インストールに適切な拡張を作成してデプロイしておきます。1 つの拡張機能 (たとえば、カスタムボタンや HTML として保存) に対して 1 つの拡張をデプロイします。
- 信頼できる URL の一覧に拡張を追加しておきます。まだ追加していない場合は、信頼できる URL を許可された URL の一覧に追加する [688 ページ]の節を確認してください。

1. 管理者として CMC にログインします。
2. [整理] リストから、[ユーザとグループ] を選択します。
3. [グループ階層] リストで、ユーザグループを選択します。
4. [アクション] リストで [カスタマイズ] をクリックします。
5. [拡張機能] をクリックして、以下のいずれかを実行します。

オプション	説明
BI プラットフォームとそのアプリケーションサーバにデプロイされた **OSGi** 拡張を追加する	ユーザが使用するカスタム拡張を選択します。

BI プラットフォームアプリケーションサーバまたは外部アプリケーションサーバのどちらかにデプロイされている **OSGi** 拡張を追加する	1. [追加] をクリックします。
	2. 拡張 URL を入力します。
	これが JSON ファイルの URL です。
	注記
	URL のスペースはすべて **%20** で置き換えます。
	例:
	• Apache Tomcat アプリケーションサーバ:
	`http://myserver/webiextension/extension/SAP/RayLight_Embedded/extension.json`
	• 外部アプリケーションサーバ:
	`http://www.mysite.org/documents/web/extension/Custom%20Button/extension.json`
	3. アプリケーションサーバで必要な場合は、[必要な場合はプロキシ情報を設定] を選択し、サーバ名とポート番号を入力します。
	4. アプリケーションサーバで必要な場合は、[認証がありません] または [基本認証] のいずれかを選択し、ユーザ名とパスワードを入力します。
	5. [*OK*] をクリックして拡張を選択します。
	6. [保存] をクリックします。

拡張詳細を変更する	[変更] をクリックします。
CMC から拡張を削除する	[削除] をクリックします。

6. 保存して閉じるをクリックします。

選択されたフォルダにあるドキュメントを開くと、有効な拡張が、選択されたユーザグループに対して使用可能になります。すべての Web Intelligence アプリケーションクライアント (Web、Java アプレット、リッチクライアント) で拡張ポイントを使用できます。

18.6.2 BI ラウンチパッド

18.6.2.1 [スケジュール] ダイアログボックスでプロンプト値のクリアを有効にする

SAP BW プロンプトを含む BEx クエリに基づく Web Intelligence ドキュメントのスケジュール時に、BI ラウンチパッドユーザはプロンプト値をクリアし、ドキュメントの実行時にそれが SAP BW データソース変数によって取得されるようにするか、またはスケジューリングジョブの実行前にプロンプト値を固定することができます。

以下の手順では、ユーザインタフェースに次の 2 つのラジオボタンを表示することができます。

- 動的な値を使用: SAP BW データソースにより値が処理されるようにします。
- 定数値を使用: 固定値を入力します。

1. `<InstallDir>¥<WebAppServer>¥webapps¥BOE¥WEB-INF¥config¥custom` フォルダで、次の操作のいずれかを実行します。
   - `AnalyticalReporting.properties` ファイルがフォルダに格納されている場合、テキストエディタでそのファイルを開く。
   - `AnalyticalReporting.properties` ファイルがフォルダに存在しない場合、このファイル名のファイルを作成し、それをテキストエディタで開く。
2. `AnalyticalReporting.properties` ファイルで、次の操作のいずれかを実行します。
   - ファイルがすでに存在していた場合、ファイルで `bex.dynamic_variable.schedule` プロパティを見つけ、その値を `true` に設定する。
   - `AnalyticalReporting.properties` ファイルを作成した場合、ファイルの末尾に `bex.dynamic_variable.schedule=true` を追加する。
3. ファイルを保存して閉じ、Web アプリケーションサーバを再起動します。

18.7 Web サーバでの BI プラットフォーム RESTful Web サービスの設定

RESTful Web サービスの設定をカスタマイズするには、以下の手順に従います。

1. ファイル: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps ¥biprws¥WEB-INF¥config¥default¥biprws.properties` を `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps ¥biprws¥WEB-INF¥config¥custom¥biprws.properties` にコピーし、編集用に開きます。
   必要に応じてパラメータを変更します。

```
global.properties | bipnws.properties | hosts | bipnws.properties
1  #-----------------------------------------------------Default CMS Configuration-----------------------------------------------------
2  CMS_Default=
3  #-----------------------------------------------------System Property Configuration-------------------------------------------------------
4  Default_Number_Of_Objects_On_One_Page=
5  Enterprise_Session_Token_Timeout_In_Minutes=
6  Session_Pool_Size=
7  Session_Pool_Timeout_In_Minutes=
8  #-----------------------------------------------------Logger properties-----------------------------------------------------
9  LogLevel=
10 #-----------------------------------------------------Trusted Authentication Configuration-----------------------------------------------------
11 Retrieving_Method=
12 User_Name_Parameter=
13 Trusted_Auth_Shared_Secret=
14 # ----------------------------------------------------- SSO Related Default Global Core Web Properties -----------------------------------------------------
15 # Vintela single sign on properties
16 sso.enabled=
17 idm.realm=
18 idm.princ=
19 idm.keytab=
20 idm.allowUnsecured=
21 idm.allowNTLM=
22 idm.logger.name=
23 idm.logger.props=
```

以下の表には、スクリーンショットに示されているプロパティが説明されています。

プロパティ	説明	デフォルト値

`CMS_Default`	ユーザは、CMS の名前とポート番号、またはクラスタ名を指定できます。
	例:
	`CMS_HOST_NAME:CMS_PORT_NUMBER`
	または
	`@CMS_CLUSTER_NAME`
		0

`Default_Number_Of_Objects_On _One_Page`	1 ページにリストされるエントリ数です。この設定は、RESTful Web サービス SDK のパラメータ `&pageSize=<m>` によって上書きできます。	50
`Enterprise_Session_Token_Timeout_In_Minutes)`	ログオントークンが有効のままである有効期限時間です。この時間を超過すると、新しいログオントークンを生成する必要があります。	60
`Session_Pool_Size`	任意の時点で保存可能な、キャッシュされたセッションの数です。セッションプールはアクティブな RESTful Web サービスセッションをキャッシュします。これにより、ユーザは、HTTP 要求ヘッダで同じログオントークンを使用する別の要求を送信する場合にこれらのセッションを再利用できます。	1000
`Session_Pool_Timeout_In_Minutes`	キャッシュされたセッションの有効時間を分単位で表します。	2

プロパティ	説明	デフォルト値
`LogLevel`	ロギングを有効にし、重大度および詳細のレベルを [なし] (重大なイベントのみを記録)、[低] (スタートアップ、シャットダウン、開始と終了の要求メッセージ)、[中] (エラー、警告、およびほとんどのステータスメッセージ)、または [高] (除外なし。これはデバッグでのみ使用されます。CPU 使用量が増加することで、パフォーマンスに影響が及ぶ場合があります) に設定します。 選択可能なメニューは次のとおりです。 • `Unspecified` • `None` • `Low` • `Medium` • `High`	指定なし
Log_Location	BI プラットフォームをホストするマシンの使用ログを記録するログファイルの場所です。 ⓘ 注記 • 存在しないフォルダへのファイルパスを指定すると、新しいフォルダが作成されます。 • ログファイルの場所は、biprws.properties ファイルに指定しない場合、デフォルトの場所に設定されます。	指定なし

プロパティ	説明	デフォルト値
`Retrieving_Method`	RESTful Web サービス API/logon/trusted を使用する場合に、信頼できる認証ログオントークンの取得に使用されるクエリメソッドを指定するメニューです。 • `HTTP_HEADER` は、要求ヘッダ accept=application/xml (または application/json) を使用する GET クエリで使用されます。 • `QUERY_STRING` は、RESTful Web サービス API を使用する URL クエリの末尾にログオン名を追加するために使用します (例: /logon/trusted/?user=johndoe)。 • `COOKIE` は、Web ブラウザの Cookie からログイン名を取得する場合に使用します。ドメイン、名前、値、およびパスは Cookie に保存される必要があります。	`HTTP_HEADER`
`User_Name_Parameter`	ログオントークンを取得する目的で信頼できるユーザを識別するために使用するラベルです。	`X-SAP-TRUSTEDUSER`
`Trusted_Auth_Shared_Secret`	共有シークレットの値の生成 [392 ページ] の節に記載されている手順に従って生成される文字列値です。	指定なし
`Basic_Auth_Supported`	Tomcat Web サーバで基本認証を有効化します。可能な値は `True` または `False` です。	指定なし
`Basic_Auth_Type`	認証を `secEnterprise`、`secLDAP`、`secSAPR3`、または `secWinAD` に設定して、基本認証をサポートします。	`secEnterprise`

2. Tomcat を再起動します。

18.8 ハイブリッドユーザ管理

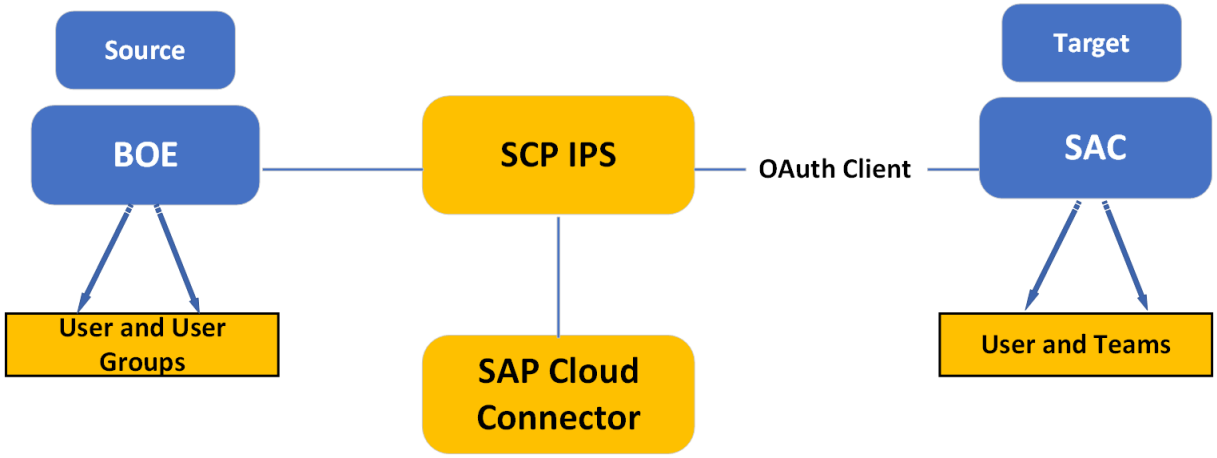
SAP はクラウドファースト戦略に焦点を当てており、お客様もオンプレミス環境とクラウド間でアセットを管理するハイブリッドソリューションに急速に移行しています。これを可能にする SAP BusinessObjects BI プラットフォームからサービスを提供することが不可欠です。

これは、クロスドメイン ID 管理システム (SCIM) ベースのユーザプロビジョニング API (内部) を公開することで実現されます。この API を SAP Cloud Platform Identity Provisioning Service (SCP IPS) で利用して、BI プラット

フォーム Enterprise ユーザを Identity Provisioning Service (IPS) (特に SAP Analytics Cloud) を使用する他のサポートされている SCIM システムにプロビジョニングすることができます。

SCP IPS および SAP BusinessObjects BI プラットフォーム 4.2 SP06 以上を使用して、サポートされている任意の SCIM システムに BI プラットフォーム Enterprise ユーザをプロビジョニングできるようになりました。

次の図は、ハイブリッドシナリオ、およびオンプレミスとクラウド間でサービスを有効化する方法を示しています。



18.9 オンプレミスユーザの SAP Analytics Cloud へのプロビジョニング

エンティティ (ユーザ、グループ、ロール) を企業内で 1 つのシステムから別のシステムにプロビジョニングするには、まずこれらのシステムを Identity Provisioning ユーザインタフェースでソースおよびターゲットシステムとして追加し、設定する必要があります。

SAP Cloud Platform Identity Provisioning Service (SCP IPS) を使用して、いくつかの簡単なステップでオンプレミス (BOE) ユーザを SAP Analytics Cloud にプロビジョニングできます。

1. オンプレミスシステムとクラウド間の接続の確立
2. SAP Analytics Cloud での OAuth クライアント認証情報の作成
3. ソースシステムの設定
4. ターゲットシステムの設定
5. SAP Analytics Cloud へのユーザおよびユーザグループのプロビジョニング
6. プロビジョニングされたユーザおよびユーザグループの表示

18.9.1 オンプレミスシステムとクラウド間の接続の確立

SAP Cloud (IPS システム) Connector を使用して、オンプレミスシステムとクラウド (Identity Provisioning System) 間の接続を確立することができます。

Cloud Connector がインストールされている必要があります。

1. SAP Cloud Connector 管理ページを起動し、`https://<HCC HOST>:8443` にログオンします。

   > ⓘ 注記
   >
   > `<HCC HOST>` を、Cloud Connector がインストールされているシステムのホスト名に置き換えます。

2.
3. ナビゲーションパネルで [*Connector*] を選択し、＋ (*Add Subaccount*) アイコンをクリックします。

   [*Add Subaccount*] ダイアログが表示されます。
4. IPS アカウントに関する以下の情報を入力します。

   > ⓘ 注記
   >
   > IPS でのサブアカウントユーザの [オンプレミス接続の管理] 権限が必要です。[リージョンホスト] および [サブアカウント名] は、IPS の *[サポート] - [アカウント情報]* セクションにあります。

   a. リージョンホスト: 一覧から地域ホストを選択します。
   b. *Subaccount Name*: アカウント名を追加します。例: dd00bb33。
   c. (オプション) *Display Name*: アカウントの名前を追加します。
   d. *Subaccount User*: サブアカウント (S ユーザ) ユーザ名を追加します。
   e. *Password*: S ユーザのパスワードを追加します。
   f. *Location ID*: デフォルトの場所を使用する場合は、空白のままにします。
   g. (オプション) 説明: Cloud Connector の説明を追加します。
5. [*Save*] をクリックします。
6. ナビゲーションパネルの [*DisplayName*] で、[*Cloud to On-Premise*] を選択します。

   [*DisplayName*] は Cloud Connector テナントの名前です。
7. [*Access Control*] タブで、＋ (Add) アイコンをクリックします。

   [*Edit System Mapping*] ダイアログボックスが表示されます。
8. BI プラットフォームシステム、biprws をホストしている Web アプリケーションサーバ (例: Tomcat) の要求されたシステムマッピング情報を追加します。
   a. バックエンドタイプ: ドロップダウンから [その他の SAP システム] を選択します。
   b. *Protocol*: ドロップダウンから [HTTP] を選択します。
   c. (オプション) *Virtual Host*: デフォルトの仮想ホストおよびポートは、内部ホストおよびポートです。ホストおよびポートの名前を変更し、内部ホスト名およびポートが公開されないようにすることができます。
   d. (オプション) *Virtual Port*: これは、仮想ホストで使用されるポート番号です。
   e. *Internal Host*: これは、WAS のホスト名です (例: RESTful Web サービス (biprws) をホストしている Tomcat)。
   f. 内部ポート: これは、内部ホストで使用されるポート番号です。(BIP RESTful Web サービスがデプロイされるポート。たとえば、biprws。)
   g. *SAProuter*: このフィールドは空白のままにします。
   h. *Principal Type*: ドロップダウンから [なし] オプションを選択します。
   i. *SNC Partner Name*: このフィールドは空白のままにします。
   j. (オプション) *Description*: システムの説明を追加します。
9. [*Check internal host*] チェックボックスを選択して、[*Save*] をクリックします。
10. [*Mapping Virtual To Internal System*] リストに追加したシステムを選択します。
11. [*Resources Accessible*] 領域で、＋ (Add) アイコンをクリックします。

[*Add Resource*] ダイアログボックスが表示されます。

12. アカウントに関する以下のリソース情報を追加します。
    a. *URL Path*: /biprws/sbop/internal/v2/scim。
    b. 有効: チェックボックスが選択されていることを確認します。
    c. *Access Policy*: [*Path and all sub-paths*] ラジオボタンを選択します。
    d. (オプション) *Description*: リソースの説明を追加します。
13. [*Save*] をクリックします。

> ⓘ 注記
>
> 仮想ホストの横のステータスが緑色で表示されます。

18.10 SAP Analytics Cloud での OAuth クライアント認証情報の作成

SAP Analytics Cloud で OAuth クライアント認証情報を作成するには、以下の手順に従ってください。

1. SAP Analytics Cloud にログインします。
2. メインメニューから、システム > 管理 > アプリ統合に移動します。
3. [新しい *OAuth* クライアント] をクリックします。
4. 任意の名前を入力します。
5. [目的] として [*API* アクセス] を選択します。
6. [アクセス] で [ユーザプロビジョニング] を選択します。
7. [追加] をクリックします。

   [設定済みクライアント] 一覧で、追加したクライアントを選択します。

> ⓘ 注記
>
> ✎ (編集) アイコンを選択して、生成された OAuth クライアント ID およびシークレットキー (パスワード) を表示します。これらの認証情報は、ターゲットシステムの設定時に必要となります。
>
> OAuth クライアント ID は SCP IPS でのターゲットシステムの設定詳細におけるユーザ名に対応し、シークレットはパスワードに対応します。

18.11 ソースシステムの設定

ユーザおよびユーザグループをプロビジョニングするソースシステムの詳細を SAP Cloud Platform Identity Provisioning Service (SCP IPS) で設定する必要があります。

1. SCP IPS にログインします。
2. ホームページから、[*Source Systems*] タイルを選択します。

3. 左側のパネルの下部にある + (追加) アイコンをクリックします。
4. [*Type*] コンボボックスで、使用するシステムタイプを選択します。
5. システムの名前を追加します。(別のシステムの名前と重複していないことを確認してください。)
6. (オプション) 後で一覧内で簡単に区別できるように、システムの説明を入力します。
7. [*Save*] をクリックします。

   新しいシステムが左側のパネルに表示されます。

   注意: この時点でシステムを保存しない場合、デフォルトの変換およびプロパティは表示されません。
8. 次に、✎ (編集) アイコンをクリックして変換を表示し、設定プロパティを追加します。
9. 次の情報を追加します。
   a. *Authentication*: BasicAuthentication
   b. *Host*: <BOE ホスト名およびポート>
   c. *ips.delta.read*: Enabled
   d. *ips.full.read.force.count*: 2
   e. *ips.trace.failed.entity.content*: true
   f. *Password*: <BOE 管理者ユーザのパスワード>
   g. *Proxy Type*: OnPremise
   h. *scim.group.filter*: <ユーザグループ ID または CUID>

      たとえば、`scim.group.filter: groupId eq "4214"` です。
   i. *scim.user.filter*: <ユーザ ID または CUID>

      たとえば、`scim.filter.filter: userId in "8077"` または `scim.user.filter: userCuid in "AQ.rQ1V1FR9JmQoQa0xYfII"` です。
   j. *Type*: HTTP
   k. *URL*: http://host name: port/biprws/sbop/internal/v2/scim
   l. *User*: Administrator

   > ⓘ 注記
   >
   > - オンプレミスシステムの詳細を最初から入力することも、設定情報を含む既存のファイルをインポートすることもできます。
   > - 変換を介してソースシステムに関する特定の制約または条件を定義することができます。
   > - 接続先を選択する場合、接続先は関連するシステムタイプに準拠している必要があります。接続先では、アイデンティティプロビジョニングシナリオに必要なすべての接続設定を指定する必要があります。
   > - URL フィールドで指定されたホスト名/ポートは、クラウドコネクタで指定された仮想ホスト名/ポートと一致する必要があります。
10. [*Destination Name*] フィールドをスキップした場合は、[*Properties*] タブを開いて、プロビジョニングシナリオに必要なすべての接続および設定プロパティを入力できます。
11. (必要に応じて) デフォルトのシステム変換を変更できます。
12. 変更を保存します。

    > ⓘ 注記
    >
    > Identity Provisioning URL の末尾に、ダッシュで区切られた文字列が表示されます。これは、新しく作成されたシステムの自動的に生成された一意の ID です。

18.12 ターゲットシステムの設定

開始する前に、SAP Analytics Cloud で OAuth クライアント認証情報を作成しておく必要があります。

1. ホームページから [ターゲットシステム] タブをクリックします。
2. [詳細] タブで、SAP Analytics Cloud システムの名前、SAP Analytics Cloud の URL、およびソースシステムを入力します。

   > ⓘ 注記
   >
   > すでに設定されているソースシステムは、デフォルトでここに表示されます。

3. [プロパティ] タブをクリックします。
4. 次の情報を追加します。
   a. 認証: BasicAuthentication
   b. *csrf.token.path*: api/v1/scim/Users?count=1
   c. *ips.trace.failed.entity.content*: True
   d. *OAuth2TokenService URL*: <OAuthClientTokenURL>
   e. パスワード: <OAuthClient の設定時に生成されたシークレット>
   f. *ProxyType*: インターネット
   g. *scim.api.csrf.protection*: 有効
   h. タイプ: HTTP
   i. *URL*: SAP Analytics Cloud の URL
   j. ユーザ: <OAuth クライアント ID>

18.13 SAP Analytics Cloud へのユーザおよびユーザグループのプロビジョニング

SAP Cloud Platform Identity Provision Service を使用してソースシステムとターゲットシステムを設定したら、[ソースシステム詳細] ウィンドウの [ジョブ] タブからプロビジョニングできます。

プロビジョニングされる BI プラットフォームのユーザには、電子メールアドレスが設定されている必要があります。

1. [ソースシステム] タイルをクリックします。
2. [ジョブ] をクリックします。
3. [ジョブ] の [ジョブタイプ]: [ジョブの読込み] で、[直ちに実行] アクションを選択します。

   > ⓘ 注記
   >
   > BOE でユーザまたはユーザグループを変更した場合は、[ジョブを再同期] を選択して、変更が SAP Analytics Cloud で更新されるようにします。

4. 進捗を表示するには、左のパネルから [ジョブログ] を選択し、トリガされたジョブの [ステータス] を表示します。

5. ジョブ実行の詳細を表示するには、対応する行をクリックします。

   [ジョブ実行詳細] ウィンドウが開き、アクションのステータスが表示されます。

18.14 SAP Analytics Cloud でのプロビジョニングされたユーザの表示

1. メインメニュー > セキュリティ > チームに移動します。
2. [チーム] ページに移動します。
3. BOE ユーザグループを選択します。
4. [チームメンバー] をクリックして、BOE から SAP Analytics Cloud にプロビジョニングされたユーザの一覧を表示します。

   > ⓘ 注記
   >
   > [セキュリティ] の [ユーザ] メニューからユーザの一覧を表示することもできます。

18.15 サンプルテンプレート

以下のテンプレートを使用して、ユーザまたはユーザグループをプロビジョニングできます。

サンプルソースシステム設定

```
{ "connectorTypeString": "SCIM", "accessMode": "READ",
"alias": "SBOP_10.47.228.194",
"relatedSystems": [
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
"name": "SBOP_43",
"state": "ENABLED",
"transformation": {
"user": {
"condition": "($.memberOf contains '7741') || ($.memberOf contains '7962') ||
($.id contains '8077') || ($.id contains '8081')",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
```

```
},
{
"targetPath": "$.meta",
"type": "remove"
}
]
},
"group": {
"condition": "$.id contains '7741' || $.id contains '7962'",
"mappings": [
{
"sourcePath": "$",
"targetPath": "$"
},
{
"sourcePath": "$.id",
"targetVariable": "entityIdSourceSystem"
},
{
"targetPath": "$.id",
"type": "remove"
},
{
"targetPath": "$.meta",
"type": "remove"
}
]
}
},
"properties": {
"Type": "HTTP",
"User": "Administrator",
"ips.full.read.force.count": "2",
"Authentication": "BasicAuthentication",
"host": "adept6991435:6400",
"scim.group.filter": "groupId eq ¥"7741,7962¥" or groupCuid eq
¥"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ¥"",
"ProxyType": "OnPremise",
"ips.delta.read": "enabled",
"ips.trace.failed.entity.content": "true",
"URL": "http://adept6991435:6405/biprws/sbop/internal/v2/scim",
"Password": "Password1",
"scim.user.filter": "groupId eq ¥"7741¥" and groupCuid eq
¥"ATKZxWcAGfhOnHwu_A_uyAc,AYIbS.o1pSlDmjcUS107aCQ¥" and userId in ¥"8077¥" or
userCuid in ¥"AQ.rQ1V1FR9JmQoQa0xYfII¥""
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```


サンプル変換


```
{
"connectorTypeString": "SAP_ANALYTICS_CLOUD",
"accessMode": "WRITE",
"destinationName": " ",
"alias": "https://idcsac.jp1.sapanalytics.cloud",
"relatedSystems": [
"SBOP_43"
],
"gitAllowedExpressions": [
],
"gitDisallowedExpressions": [
],
"emailSubscribers": [
],
```

```
"name": "SAC-Machine",
"state": "ENABLED",
"transformation": {
"user": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"sourceVariable": "entityIdTargetSystem",
"targetPath": "$.id"
},
{
"sourcePath": "$.userName",
"targetPath": "$.userName"
},
{
"sourcePath": "$.name",
"targetPath": "$.name"
},
{
"sourcePath": "$.displayName",
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.active",
"optional": true,
"targetPath": "$.active"
},
{
"sourcePath": "$.emails",
"preserveArrayWithSingleElement": true,
"targetPath": "$.emails"
},
{
"condition": "$.emails[0].length() > 0",
"constant": true,
"targetPath": "$.emails[0].primary"
},
{
"constant": [
"PROFILE:sap.epm:BI_Admin"
],
"preserveArrayWithSingleElement": true,
"targetPath": "$.roles"
},
{
"sourcePath": "$.groups",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.groups"
},
{
"sourcePath": "$['urn:ietf:params:scim:schemas:extension:enterprise:2.0:User']
['manager']['value']",
"optional": true,
"targetPath": "$['urn:scim:schemas:extension:enterprise:1.0']['manager']
['managerId']",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
```

```
]
},
"group": {
"mappings": [
{
"sourcePath": "$.schemas",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.schemas"
},
{
"condition": "$.displayName EMPTY false",
"sourcePath": "$.displayName",
"targetPath": "$.id"
},
{
"condition": "$.id EMPTY false",
"sourcePath": "$.id",
"targetPath": "$.id"
},
{
"sourcePath": "$.displayName",
"optional": true,
"targetPath": "$.displayName"
},
{
"sourcePath": "$.roles",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.roles"
},
{
"sourcePath": "$.members[*].value",
"preserveArrayWithSingleElement": true,
"optional": true,
"targetPath": "$.members[?(@.value)]",
"functions": [
{
"type": "resolveEntityIds"
}
]
}
]
}
},
"properties": {
"Type": "HTTP",
"User": "<exampleusername>",
"Authentication": "BasicAuthentication",
"OAuth2TokenServiceURL": "https://oauthasservices-
gf097393f.jp1.hana.ondemand.com/oauth2/api/v1/token",
"csrf.token.path": "/api/v1/scim/Users?count=1",
"ProxyType": "Internet",
"ips.trace.failed.entity.content": "true",
"URL": "https://idcsac.jp1.sapanalytics.cloud",
"scim.api.csrf.protection": "enabled",
"Password": "<examplepassword>"
},
"encryptedProperties": {
},
"gitFetchAllowed": false
}
```

19　接続とユニバースの管理

19.1　接続の管理

接続は、名前の付いたパラメータのセットのことで、1 つまたは複数の SAP BusinessObjects アプリケーションがリレーショナルまたは OLAP データベースにアクセスする方法を定義します。サーバ名、データベース、ユーザ名、およびパスワードなどの接続の詳細情報は、接続フォルダの BI プラットフォームリポジトリに安全に格納できます。

デザイナは接続に基づいてユニバースを定義します。クエリアプリケーション、分析アプリケーション、およびレポーティングアプリケーションのユーザは、データベース内の基となるデータ構造を意識する必要なく、データベースにアクセスします。

次のアプリケーションを使用して、接続を作成できます。

- ユニバースデザインツール: 接続はリポジトリに格納されます。
- インフォメーションデザインツール: 接続はローカルで作成してからリポジトリに公開するか、または直接リポジトリで作成し、編集できます。

> ⓘ 注記
>
> OLAP データソース接続の管理方法については、*SAP BusinessObjects Analysis, edition for OLAP* 管理者ガイドを参照してください。

ユーザが接続を作成、編集、削除できる権限を付与します。

ユーザにユニバース接続へのアクセス権を付与し、ユニバースや接続を使用するドキュメントの作成や表示を許可します。

関連情報

CMC でのオブジェクトのセキュリティ設定の管理 [129 ページ]
接続のアクセス権 [1099 ページ]

19.1.1 ユニバース接続を削除する

> → ヒント
>
> 接続は、ユニバースデザインツールでもインフォメーションデザインツールでも削除できます。

1. [接続]エリアで、一覧からユニバース接続を選択します。

2. 管理 > 削除 をクリックします。

19.2 ユニバースの管理

ユニバースとは、編成されたメタデータオブジェクトのコレクションのことで、これにより、専門用語を使わずに、ビジネスユーザが企業のデータを分析してレポートを作成できます。これらのオブジェクトには、ディメンション、メジャー、階層、属性、定義済みの計算、関数、およびクエリが含まれます。メタデータオブジェクトレイヤは、リレーショナルデータベースのスキーマまたは OLAP キューブ上で構築されるため、オブジェクトは直接データベース構造にマップされます。ユニバースにはデータソースへの接続が含まれているため、クエリツールおよび分析ツールのユーザはユニバースに接続し、クエリを実行し、ユニバースのオブジェクトを使用してレポートを作成できます。その際、ユーザはデータベース内の基となるデータ構造を意識する必要はありません。

次のツールを使用して、ユニバースを作成できます。

- ユニバースデザインツールこのツールを使用して作成したユニバースは、拡張子 .unv で識別可能なため、.unv ユニバースと呼ばれます。.unv ユニバースはセキュリティ接続で定義され、リポジトリのユニバースフォルダに格納されます。
- インフォメーションデザインツールこのツールを使用して作成されたユニバースは、新しいセマンティックレイヤに基づきます。このようなユニバースは、拡張子 .unx で識別可能なため、.unx ユニバースと呼ばれます。.unx ユニバースはローカルで作成してリポジトリのユニバースフォルダに公開できます。デザイナは、インフォメーションデザインツール のセキュリティエディタを使用して、オブジェクトレベルのセキュリティを定義できます。

ユーザにアプリケーションの権限とユニバースの権限を付与し、ユニバースの作成、編集、削除、およびユニバースに対するセキュリティのデザインを許可することができます。

ユーザにユニバースの権限を付与し、ユニバースを使用するドキュメントの作成や表示を許可することができます。

関連情報

CMC でのオブジェクトのセキュリティ設定の管理 [129 ページ]
ユニバースデザインツール [1104 ページ]
ユニバース (.unv) のアクセス権 [1095 ページ]
インフォメーションデザインツール [1104 ページ]
ユニバース (.unx) のアクセス権 [1096 ページ]

19.2.1 ユニバースを削除する

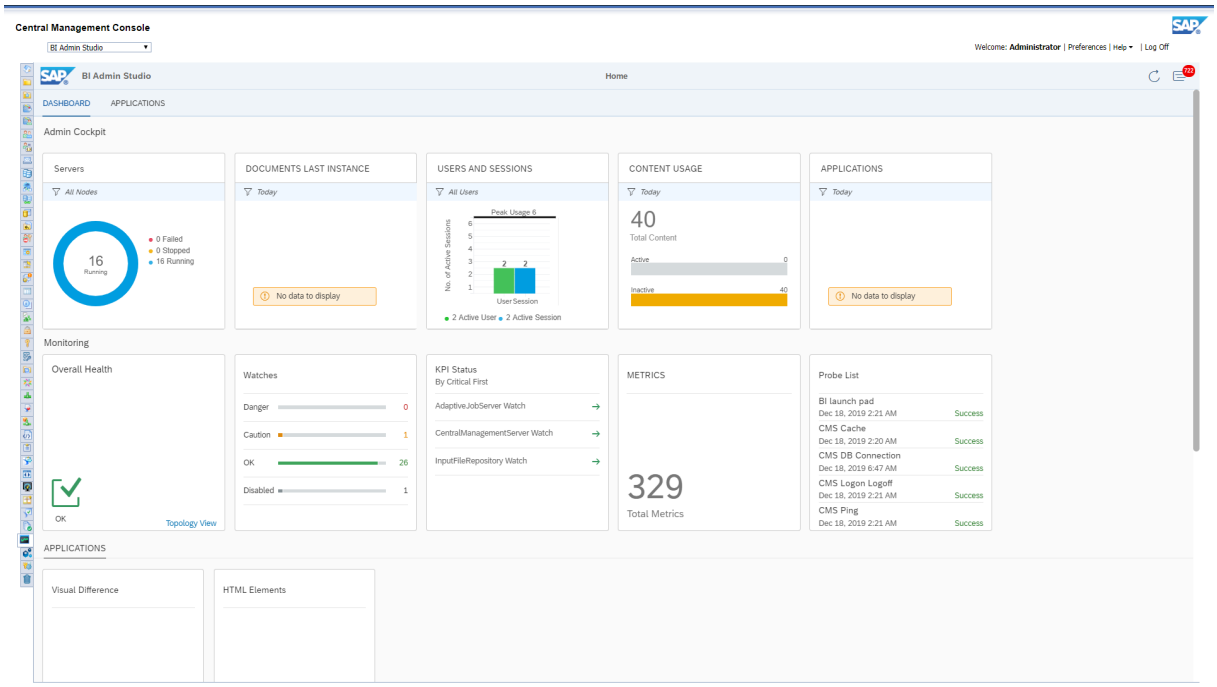
> → ヒント
>
> ユニバースは、インフォメーションデザインツールでも削除できます。

1. CMC の[ユニバース]エリアで、一覧からユニバースを選択します。
2. 管理 > 削除 をクリックします。
3. 確認を求めるメッセージが表示されたら、[*OK*]をクリックします。

20 BI 管理スタジオ

BI 管理スタジオは、モニタリング、アラート、および管理コックピット (以前の名前は BI 管理者のコックピット) を組み合わせた CMC のアプリケーションです。

このアプリケーションは、[ダッシュボード] および [アプリケーション] の 2 つのタブで構成されています。



ダッシュボード

[ダッシュボード] タブには、[管理コックピット] および [モニタリング] で利用可能なダッシュボードの単一のビューがあります。各ダッシュボードをクリックすると、そのダッシュボードに関する詳細情報を確認することができます。たとえば、[サーバ] ダッシュボードを選択すると、[ステータス] が [実行中]、[停止]、および [失敗] であるサーバの一覧を [サーバ名]、[*PID*]、[タイプ] などの詳細とともに表示できます。管理コックピットの詳細については 管理コックピット [767 ページ] を、モニタリングの詳細については モニタリング [771 ページ] を参照してください。

アプリケーション

[アプリケーション] タブから [*Visual Difference*] および [権限のある *HTML* 要素] にアクセスできます。*Visual Difference* の詳細については Visual Difference [794 ページ] を、*HTML* 要素の詳細については HTML 要素の許可 [797 ページ] を参照してください。

アラート

を選択して、アラートの通知ペインにアクセスできます。通知ペインで [アラートページへ] オプションを選択すると、作成したアラートに関する詳細を確認できます。

20.1 管理コックピット

管理コックピットは、CMC に追加された新しいアプリケーションです。このコックピットで、管理者は BI 環境に関する基本データを収集することができます。つまり、BI 環境のデータからビジネスインテリジェンス情報が派生します。管理コックピットを使用して、サーバ、スケジュールされたジョブ、ユーザとセッション、コンテンツの使用状況、およびアプリケーションについての情報を取得することができます。

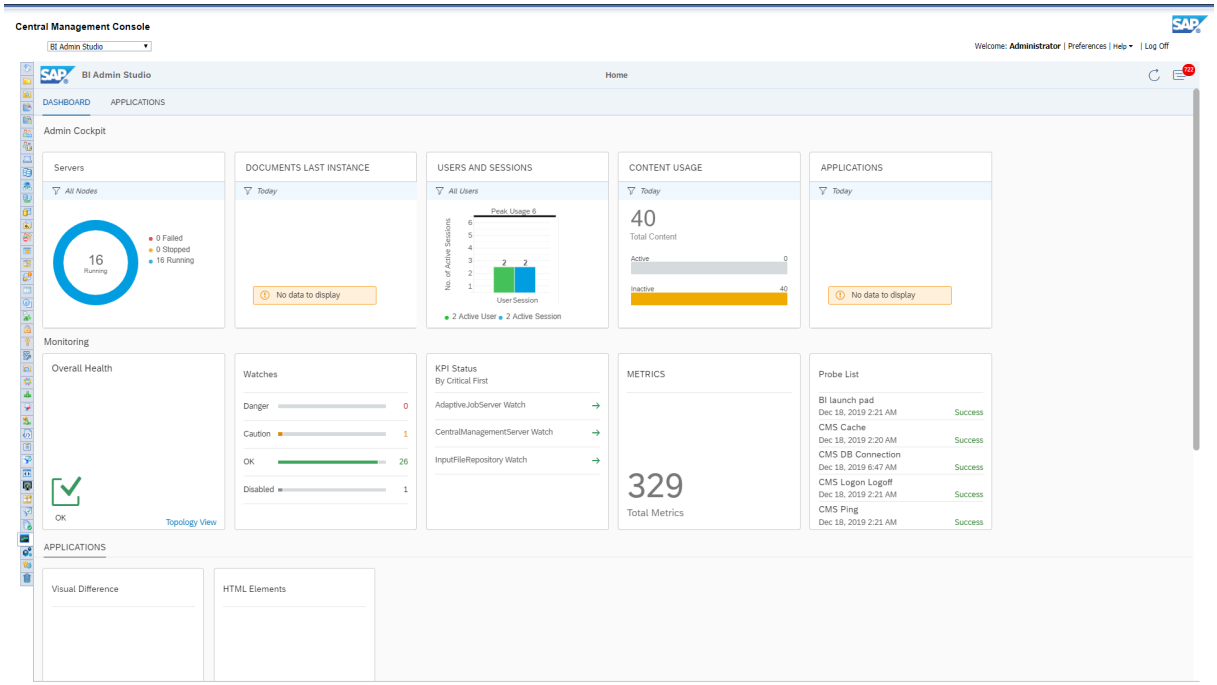
> **注記**
>
> 管理コックピットを正常に使用するには、以下の要件が必要です。
>
> - モニタリングサービスを有効にする必要があります。
> - 正しいデータがフェッチされるように、監査および関連イベントを有効にする必要があります。
> - クライアントによる BI プラットフォーム RESTful Web サービスへのアクセスが可能である必要があります。
> - RESTful Web サービスが Tomcat にデプロイされている場合を除き、WACS が実行されている必要があります。
> - CMC に SSL を設定している場合は、RESTful Web サービスが Tomcat にデプロイされている場合を除き、WACS にも SSL を設定する必要があります。
> - クロスドメインへのアクセスを有効にする必要があります。
> - 管理コックピットにアクセスするには、管理者グループまたはそのサブグループに属している必要があります。

20.1.1 管理コックピット

管理コックピットでは、画像ビジュアライゼーションの以下のコンポーネントに関連するデータを包括的に分析できます。

- サーバ
- ドキュメント最終インスタンス
- ユーザとセッション
- コンテンツの使用
- アプリケーション

> **注記**
>
> コンテンツの使用とアプリケーションに関する分析を表示するには、監査データベースを有効にする必要があります。



ホームページの右上隅にある をクリックすると、管理コックピットの各ページに表示されるデータを最新表示できます。

20.1.2 BI のサーバ

管理コックピットでは、BI 環境におけるすべてのサーバのステータスと関連する詳細のリアルタイムのデータを取得できます。

ホームページには以下の詳細が表示されます。

- サーバの合計数
- エラーがあるサーバの数
- 停止したサーバの数

希望するサーバクラスタを選択して、[サーバ] タイルに表示するデータをフィルタ処理することができます。

[サーバ] タイルをクリックすると、[サーバ] ページが表示されます。このページには、サーバの合計数、エラーが発生したサーバ、および停止したサーバに関する詳細が表示されます。[サーバ] ページには、各エラー発生サーバの [ステータス]、[サーバ名]、[*PID*] (プロセス ID)、[タイプ]、[状態]、および [前回の変更時刻] も表示されます。

[サーバ] ページ内で、希望するサーバクラスタを選択して、特定のサーバクラスタに従ってデータをフィルタ処理することができます。

対応する行を選択すると、エラー発生サーバに関するより詳細な情報を表示することができます。この場合、エラーの理由が詳細に説明された新しいページが表示されます。[開始] を選択すると、ページ内からエラー発生サーバを再起動することができます。

20.1.3 ドキュメントインスタンスに関する BI

管理コックピットを使用して、BI 環境におけるスケジュールされたドキュメントのすべてのインスタンスのステータスと詳細に関するデータを取得できます。

ホームページには以下の情報が表示されます。

- スケジュールされた各ドキュメントの最近のインスタンスの合計数。
- スケジュールされた各ドキュメントの最近の実行中のインスタンスの数。
- スケジュールされた各ドキュメントの最近のエラー発生インスタンスの数。
- スケジュールされた各ドキュメントの最近の待機中のインスタンスの数。

[ドキュメント最終インスタンス] タイルで、ドロップダウンメニューから特定の期間を選択すると、その期間のデータをフィルタリングできます。以下の期間を使用できます。

- 今日
- 最後の 7 日間
- 最後の 30 日間
- 四半期
- 年

[ドキュメント最終インスタンス] タイルをクリックすると、[最終インスタンス] ページが表示されます。このページには、スケジュールされた各ドキュメントの最近のインスタンスの合計数の詳細が状態別に表示されます (実行中、エラー、および待機中)。[統計] タブに詳細が表示され、セクション [インスタンス数が最も多いドキュメント] および [実行時間が最も長いインスタンス] で参照することができます。[ドキュメントのインスタンス] ページには、エラーステータスごとに [インスタンス名]、[ステータス]、[タイプ]、[所有者]、および [終了時刻] も表示されます。

[エクスポート] リンクボタンをクリックして、[最終インスタンス] ページに表示されているデータを .CSV ファイルとしてエクスポートすることができます。対応するチェックボックスを選択し、[エクスポート] ドロップダウンリストから [選択済みエクスポート] を選択して、選択したインスタンスをエクスポートすることもできます。

対応する行を選択すると、エラー発生インスタンスに関するより詳細な情報を表示することができます。[実行] を選択すると、ページ内からジョブを再起動することができます。

[統計] タブで、上位 5、上位 10、上位 15、および上位 20 のドキュメントをフィルタ処理および表示することを可能にする新規チャートフィルタが有効化されます。

20.1.4 BI のユーザとセッション

管理コックピットでは、BI 環境におけるユーザとセッションに関するデータを取得できます。

たとえば、ホームページには以下の詳細が表示されます。

- アクティブユーザの数
- アクティブセッションの数

[ユーザとセッション] タイルで、次のデータをフィルタ処理することができます。

- すべてのユーザ
- 登録ユーザ
- 同時接続ユーザ

[ユーザとセッション] タイルをクリックすると、すべてのユーザ、登録ユーザ、同時接続ユーザの詳細が示されている [ユーザとセッション] ページが表示されます。[統計] タブに、最もアクティブなユーザと最も非アクティブなユーザに関連する詳細が表示されます。

[ユーザとセッション] ページには、[ユーザ名]、[合計セッション]、[最終ログイン時刻]、および [最長の実行中セッション]も表示されます。

対応する行を選択すると、特定のユーザに関するより詳細な情報を表示できます。これによって、その特定のユーザの上位セッションが詳細に説明された新しいページが表示されます。指定するセッションを選択し、[セッション終了] を選択することによって、ページ内からその特定のユーザのどのセッションも終了することができます。

20.1.5 BI におけるコンテンツの使用

管理コックピットでは、BI 環境におけるコンテンツの使用に関するデータを取得できます。

たとえば、ホームページには以下の詳細が表示されます。

- アクティブなドキュメントの数
- 非アクティブなドキュメントの数

[コンテンツの使用状況] タイルで、ドロップダウンリストから特定の期間を選択すると、その期間のデータをフィルタリングできます。

> ⓘ 注記
>
> アクティブなコンテンツを削除しており、特定の期間のデータをフィルタリングする場合、削除したアイテムは、選択した期間においてアクティブであった場合には、まだアクティブなコンテンツとして表示されます。

以下の期間を使用できます。

- 今日
- 最後の 7 日間
- 最後の 30 日間
- 四半期
- 年

[コンテンツの使用状況] タイルをクリックすると、[コンテンツの使用] ページが表示されます。このページには、アクティブなコンテンツ、非アクティブなコンテンツ、および統計に関する詳細が表示されます。[統計] タブに、最大量の非アクティブコンテンツを持つ受信ボックス、最大量のコンテンツを持つユニバース、および最大量のコンテンツを持つフォルダに関する詳細が表示されます。

エクスポートリンクボタンを選択して、csv ファイルの [コンテンツの使用状況] ページに表示するデータをエクスポートすることができます。対応するチェックボックスを選択し、エクスポートドロップダウンから [エクスポートを選択] を選択して、特定のジョブをエクスポートするよう選択することもできます。

[コンテンツの使用] ページには、[コンテンツ名]、[タイプ]、および [実行時刻] も表示されます。

[統計] タブで、上位 5、上位 10、上位 15、および上位 20 のドキュメントをフィルタ処理および表示することを可能にする新規チャートフィルタが有効化されます。

20.1.6 BI のアプリケーション

管理コックピットでは、BI 環境のアプリケーション名で並び替えられたアプリケーションの数に関するデータが表示されます。

[アプリケーション] タイルで、ドロップダウンリストから特定の期間を選択すると、その期間のデータをフィルタリングできます。以下の期間を使用できます。

- 今日
- 最後の 7 日間
- 最後の 30 日間
- 四半期
- 年

[アプリケーション] タイルをクリックすると、[アプリケーション] ページが表示されます。このページには、[すべてのアプリケーション] および [上位アプリケーション] に関連する詳細が表示されます。

[上位アプリケーション] タブに、選択された期間内に最も多くのドキュメントが含まれる上位 5 のアプリケーションが一覧表示されます。[アプリケーション] ページには、[アプリケーション名]、[ユーザの数]、および [アーティファクトの数] も表示されます。

20.2 モニタリング

モニタリングアプリケーションでは、レポーティングおよび通知について、BI プラットフォームサーバのランタイムメトリクスおよび履歴メトリクスを取得できます。システム管理者は、モニタリングアプリケーションを使用してアプリケーションが正常に機能しているかどうか、および応答時間が予測どおりかどうかを特定することができます。キービジネスメトリクスを指定することによって、モニタリングアプリケーションは BI プラットフォームに関する有用な洞察をもたらします。

モニタリングでは、以下のタスクを実行できます。

- 各サーバのパフォーマンスチェック: これは、各サーバのステータスを信号で示す監視を使用することによって可能になります。システム管理者は、これらの監視に対するしきい値を設定し、しきい値の違反が発生したときにアラートを受信して、エラーや機能停止が発生した場合にアクションを実行することができます。

- 重要なシステム KPI (主要業績評価指標) の表示: これは、アクティビティとリソースのモニタリングに役立ちます。これらの KPI は、モニタリングアプリケーションの [ダッシュボード] ページに表示されます。
- サーバグループ、サービスカテゴリ、および Enterprise ノードに基づいて、BI プラットフォームデプロイメント全体を (グラフィック形式と表形式の両方で) 表示します。
- 最近の失敗をダッシュボード画面で表示します。
- システムの可用性および応答時間のチェック: プローブを使用して、BI プラットフォームデプロイメントのサーバとサービスが期待どおりに機能しているかどうかをチェックするため、ワークフローをシミュレーションします。これらのプローブの往復時間を定期的な間隔で分析することにより、システム管理者はシステム使用パターンを評価することができます。
- CMS のピーク負荷およびピーク期間の分析: これにより、システム管理者は追加のライセンスまたはシステムリソースが必要かどうかを決定することができます。
- 他のエンタープライズアプリケーションとの統合: BI プラットフォームモニタリングアプリケーションは、SAP Solution Manager や IBM Tivoli Monitoring など、他のエンタープライズアプリケーションと統合することができます。
- [イベントの設定] が [オフ] (メトリック値 1) に選択されている場合、[*Central Management Server*] で [監査レベル] メトリック値を追跡します。ここで監視リストを作成でき、メトリック値が 1 のときに、テストアラートが監視リストで電子メールアラートとともに送信されます。

プローブと監視の詳細を含むモニタリングアプリケーションの使用に関する詳細については、*SAP BusinessObjects Business Intelligence* プラットフォーム *CMC* オンラインヘルプを参照してください。

関連情報

サーバのメトリクスに関する付録について [1142 ページ]

20.2.1 モニタリング用語

以下の一覧は、モニタリングアプリケーションに関連する用語を提供するものです。

トレンド

トレンドを検索する目的で履歴データを記録または表示します。

ダッシュボード

[ダッシュボード] ページは、システム管理者がすべてのサーバのパフォーマンスをモニタリングするための集中型ビューを提供します。このページでは、システム KPI、最近のアラート、および監視に関するリアルタイムの情報と、監視ステータスに基づく関連グラフが提供されます。

監視

監視は、BI プラットフォーム環境内におけるサーバとワークフローのリアルタイムステータスおよび履歴トレンドを提供します。ユーザは、しきい値とアラートを監視に関連付けることができます。監視は、プローブ、サーバ、SAPOSCOL、または派生メトリクスからのデータを使用して作成することができます。

派生メトリクス

派生メトリクスとは、数学の方程式内に複数の既存のメトリクスを組み合わせて作成するメトリクスです。ユーザの必要性に基づいてメトリクスを作成し、このメトリクスを使用して監視を作成できます。

トポロジメトリクス

トポロジメトリクスは、BI プラットフォーム内の各サービスカテゴリの全体的な状態を示します。たとえば、Crystal Reports サービスは、Crystal Reports サーバに関連するすべての監視のヘルスステータスを組み合わせて表示します。

ヘルスステータス

以下は、ヘルスステータスの値です。

- "0" - "DANGER"
- "1" - "AMBER"
- "2" - "GREEN"

KPI

KPI (主要業績評価指標) は、BI プラットフォームの標準メトリクスです。これらは、スケジュールとログインセッションに関する情報を提供します。たとえば、[実行中のジョブ] の数字が大きい場合は、サーバのパフォーマンスが高いことを示します。または、[一時停止中のジョブ] の数字が大きい場合は、パフォーマンスが低く、システムに対する負荷が高いことを示します。

プローブ

プローブは、各種サービスをモニタリングし、BI プラットフォームコンポーネントの各種機能をシミュレーションします。指定された間隔で実行されるようプローブをスケジュールすることにより、システム管理者は BI プラ

ットフォームによって提供される重要なサービスの可用性とパフォーマンスを追跡することができます。このデータは、キャパシティ計画にも使用することができます。

信号機

信号機は、緑色、黄色、赤色を表示するアイコンで、指定された時間に監視の状態を示します。ユーザは監視のステータスを 2 つにするか 3 つにするかを選択することができます。

トレンドグラフ

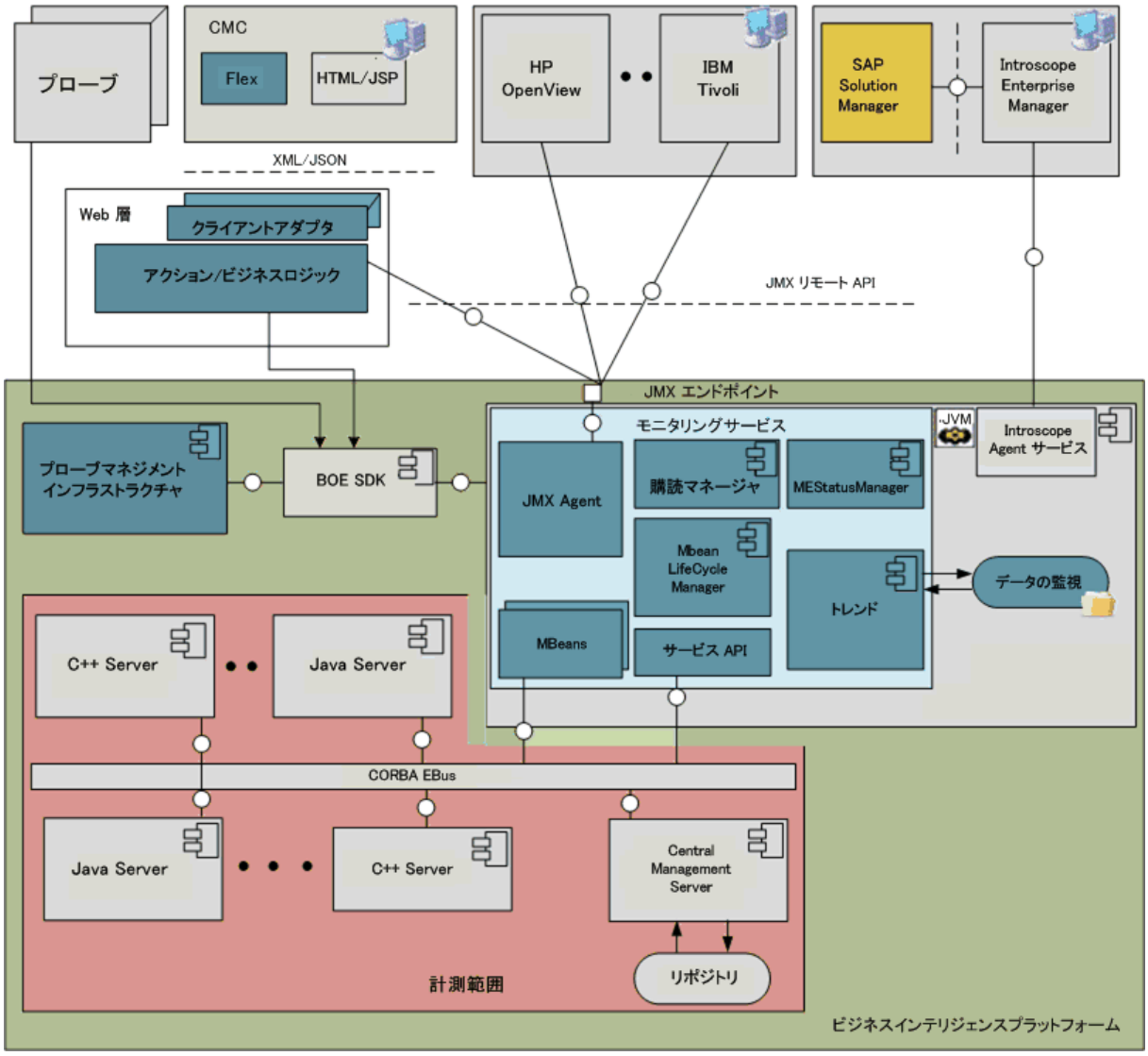
トレンドグラフは、プローブとサーバによって生成された履歴メトリクスデータをグラフィカルに表現したものです。システム管理者は、これを使用してさまざまな間隔でシステムをモニタリングし、システムの使用パターンを評価することができます。

アラート

アラートは、監視に適用される異なるメトリクスに対して設定されたユーザ定義しきい値に違反した場合に、モニタリングアプリケーションによって生成される通知です。アラートは、電子メールまたは [ダッシュボード] ページを介して受信することができます。

20.2.1.1 アーキテクチャ

この節では、モニタリングアーキテクチャの高レベル概要を提供し、コンポーネントが果たす役割を簡潔に説明します。以下は、モニタリングアーキテクチャをグラフィカルに表したものです。



以下は、アーキテクチャの高レベルコンポーネントを一覧にしたものです。

- Adaptive Processing Server (APS)
- Java Management Extensions (JMX) エージェント/サーバ
- MBeans
- JMX クライアント
- 管理コンソール
- トレンドデータベース

モニタリングサービスは、Adaptive Processing Server でホストされます。アプリケーションは、JMX 技術を基盤としています。

モニタリングサービスはモニタリングアプリケーションで利用できるコアサービスを提供します。モニタリングサービスは以下のサービスを提供します。

- JMX エージェントサービスを提供します。
- SAP BusinessObjects サーバに対し、MBeans を動的に作成します。

- MBeans のライフサイクルマネジメントを提供します。
- 新規プローブの登録メカニズムを提供します。
- ユーザが、サーバのメトリクスを使用して複雑なしきい値条件を作成できるようにします。
- しきい値通知メカニズムを提供し、アラートを送信します。
- 履歴データを保存します。

Adaptive Job Server でホストされるプローブスケジュールサービスが、プローブの実行とスケジュールを管理します。このため、Adaptive Job Server は、実行するプローブに対して実行されている必要があります。

モニタリングアプリケーションでは、JMX または Remote Method Invocation (RMI) URL エンドポイントも公開されます。IBM Tivoli Monitoring など、ほかのエンタープライズアプリケーションは、JMX リモート API を使用してモニタリングアプリケーションに接続し、BI プラットフォームメトリクスにアクセスすることができます。モニタリングアプリケーションでは、トレンディングを目的として履歴データを保存するため、監査データストア (ADS) データベースが使用されます。トレンドデータベーススキーマの詳細については、トレンドデータベーススキーマ [1175 ページ]を参照してください。

20.2.2 モニタリング用のデータベースサポートの設定

この節では、モニタリングの設定方法、およびモニタリングデータに対するレポートについて説明します。

> **注記**
>
> [トレンドデータベースへの書き込み] 設定が選択されている監視のみ、トレンドデータベースに監視情報を書き込みます。

監視情報を記録するためのデータベースオプションには、以下の 2 種類があります。監査データストア (ADS) を使用して情報を記録するか、JDBC ドライバを使用してプラットフォームでサポートされている他のデータベースを使用して記録するかのいずれかです。

> **注記**
>
> Apache Derby データベースは、BI 4.3 リリースで非推奨になりました。データの移行およびバックアップの詳細については、2912759 を参照してください。

監査データベースと呼ばれることが多い、デフォルトの監査データストア (ADS) を使用することができます。これは、CMS が監査データを格納するリレーショナルデータベースです。BI プラットフォームに含まれる ADS か、監査データベースとして設定したサポートされている他のデータベースのいずれかを使用できます。

サポートされている他のデータベースは、次のとおりです。

- DB2
- SQL Server
- My SQL
- Oracle
- SAP HANA データベース
- SQL Anywhere
- Sybase

監査データベースを使用することにより、監視情報と一緒に監査データをレポートすることができます。リレーショナルデータベースでデータを取得すると、バックアップおよび復元機能が提供されるほか、リアルタイムでデータを利用できます。

関連情報

監査データベースを使用するための設定 [777 ページ]

20.2.2.1 監査データベースを使用するための設定

モニタリングデータ用に監査データベースを使用する場合、以下の追加設定の手順を実行する必要があります。

- BI 4.3 より前では、Derby トレンドデータベースに既存のデータがある場合、Derby データベースを監査データベースに移行し、監査データベースに監視情報を記録するように BI プラットフォームを設定する必要がありました。これらは、実行する必要のある手順の概要です。詳細については、関連トピックを参照してください。
  1. Derby データベースを移行します。
  2. SBO ファイルを設定し、エイリアス名を追加します。
  3. 監査データベースに切り替えます。
  4. モニタリングサービスをホストする Adaptive Processing Server を再起動します。
  5. モニタリングダッシュボードで、すべてが正常に動作していることを確認します。以下のモニタリングテーブルが、データベース内に作成されていることを確認します。

     MOT_MES_DETAILS
     MOT_MES_METRICS
     MOT_TREND_DATA
     MOT_TREND_DETAILS
- トレンドデータベースにデータがない場合、つまり、新規インストールの場合、データベースを移行する必要はなく、監査データベースに監視情報を記録するように BI プラットフォームを設定する必要があるだけです。これらは、実行する必要のある手順の概要です。詳細については、関連トピックを参照してください。
  1. 監査データベースが正常に動作しており、監査が適切に実行されていることを確認します。
  2. ADS にモニタリングテーブルを作成します。
  3. SBO ファイルを設定し、エイリアス名を追加します。
  4. 監査データベースに切り替えます。
  5. モニタリングサービスをホストする Adaptive Processing Server を再起動します。
  6. モニタリングダッシュボードで、すべてが正常に動作していることを確認します。以下のモニタリングテーブルが、データベース内に作成されていることを確認します。

     MOT_MES_DETAILS
     MOT_MES_METRICS
     MOT_TREND_DATA
     MOT_TREND_DETAILS

> ⓘ 注記
>
> モニタリングデータを監査データベースに記録し、このデータからレポートする場合、カスタムユニバースを作成する必要があります。

関連情報

SBO ファイルの設定 [779 ページ]
SBO ファイルでのエイリアス名の追加 [781 ページ]
監査データベースに切り替える [782 ページ]
ADS にモニタリングテーブルを作成する [778 ページ]

20.2.2.1.1 ADS にモニタリングテーブルを作成する

次の手順に従って、ターゲットとなる監査データベースを準備します。

1. BI プラットフォームのインストール後、サポートされるすべての CMS 監査データベースに関連する DDL が `<Install Dir>¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥Data¥TrendingDB` で使用できるようになります。それぞれのデータベース名に対応する 7 つの異なるファイル (拡張子 .sql) があります。例: Oracle 用 `Oracle.sql`、Sybase ASE Database 用 `Sybase ASE.sql` など。
2. ターゲットデータベースに移動して (この場合のターゲットデータベースは CMS 監査が設定されたデータベース)、.sql ファイルを実行します。`MOT_TREND_DETAILS`、`MOT_TREND_DATA`、`MOT_MES_DETAILS`、および `MOT_MES_METRICS` という 4 つのモニタリングテーブルが作成されます。必要なインデックスもテーブルと一緒に作成されます。

.sql ファイルに記載されたとおりに正しいデータタイプですべてのテーブルが作成されると、モニタリングアプリケーションに必要なデータベーススキーマが作成されます。

20.2.2.1.2 ターゲットデータベースにコンテンツを復元する

コンテンツをターゲットデータベースに復元するには、次の手順を実行する必要があります。

1. ID の挿入の有効化。

   モニタリングテーブルには、多くの IDENTITY 列が含まれています。これは、値を自動生成するための列です。いくつかのデータベース (MS SQL Server や Sybase ASE など) は、これらの列に値を明示的に挿入できません。しかし、データ移行中は、IDENTITY 列値も移行する必要があります。したがって、ユーザはこれらの値を明示的に挿入できるようにする必要があります。そのためには、SQL コマンド `SET IDENTITY_INSERT <TABLE NAME> ON` を使用します。
2. CSV ダンプファイルのターゲットテーブルへのインポート。

   データベースクライアントから提供されるすべてのソフトウェアで、メニューオプションまたはコマンドのいずれかを使用して、CSV からテーブルへデータをインポートできます。ユーザは、このオプションを使用し

て、CSV ファイルから対応するテーブルにデータをインポートする必要があります。以下の順番で、データファイルを新しいテーブルにインポートします。

1. `MOT_TREND_DETAILS`
2. `MOT_TREND_DATA`
3. `MOT_MES_DETAILS`
4. `MOT_MES_METRICS`

3. ID の挿入の無効化。

   データのインポートが終了したら、そのテーブルでの ID の挿入を無効にする必要があります。そのためには、SQL コマンド `SET IDENTITY_INSERT <TABLE NAME> OFF` を使用します。

   次のテーブルで ID の挿入を有効にするために、データのインポート後にテーブルでの ID の挿入を無効にする必要があります。これは、ID の挿入操作は一度に 1 つのテーブルでしか有効にできないためです。

ID の挿入のオン/オフの設定は、MS SQL Server および Sybase ASE にのみ適用されます。Oracle、MaxDb、DB2、MySQL、または SQL Anywhere などのほかのデータベースでは、この設定は必要ありません。テーブルに直接データをインポートできます。

20.2.2.1.3 SBO ファイルの設定

内部的に、モニタリングアプリケーションは Connection Server ライブラリを使用し、Connection Server がデータベースドライバへの接続を確立するのに SBO の設定が必要です。 この接続を確立するには、データベースドライバと SBO ファイル内での場所を指定する必要があります。

> **注記**
>
> モニタリングアプリケーションは監査接続名を参照し、`<hostName>.<Portnum>.<dbName>` が使用される場合は JDBC を、それ以外の場合は ODBC を使用します。 モニタリングアプリケーションを監査データベースに接続するには、Connection Server SBO ファイルを適切に設定する必要があります。

> **注記**
>
> Oracle データベースでは、JDBC 接続のみがサポートされています。

例

- CMC の監査ページで設定した接続名フィールドが `<hostName>.<Portnum>.<dbName>` の場合、ドライバ JAR を設定する必要のあるファイル: `dataAccess¥connectionServer¥jdbc¥<dbType>.sbo`.
- CMC の監査ページで設定した接続名フィールドが ODBC DSN の場合、ドライバを設定する必要があります。`<Install_Dir>¥dataAccess¥connectionServer¥odbc¥<dbType>.sbo`.
- 監査用データベースが MS SQL Server の場合、ドライバの設定が必要とされるファイルはこれです。`<Install_Dir>¥dataAccess¥connectionServer¥odbc¥newdb.sbo`.
- 監査用データベースが MS SQL Server の場合、ドライバの設定が必要とされるファイルはこれです。`<Install_Dir>¥dataAccess¥connectionServer¥odbc¥<dbType>.sbo`.
- 監査用データベースが DB2 サーバの場合、Connection Server にサポートされる `db2iseries.sbo` ファイルは含まれません。

デフォルトでは、監視アプリケーションにより、DB2 監査データベースへの接続に ODBC 接続モードが使用されます。 このモードで作業する場合、監視アプリケーションが実行されているマシンにシステム DSN (DB2 サーバ用) を追加して設定する必要があります。 DB2 の ODBC 接続の追加方法および設定方法の詳細については、以下のリンクを参照してください。

- http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024166.htm
- http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=%2Fcom.ibm.db2.udb.apdv.cli.doc%2Fdoc%2Ft0024200.htm

> **注記**
>
> DB2 のシステム DSN を設定しない場合、モニタリングトレンドが失敗します。

SBO ファイルの設定

通常、ODBC ライブラリは SBO ファイルにすでに設定されているので、エイリアス名だけを追加する必要があります。 そうでない場合、次の例に従って SBO ファイルで設定を実行します。

例

- 監査で使用されるデータベースバージョンが SAP HANA の場合、SBO での設定は次のようになります。

```
<DataBase Active="Yes" Name="SAP HANA database 1.0" Platform="MSWindows">
    <Aliases>
        <Alias>SAP High-Performance Analytic Appliance (SAP HANA) 1.0</Alias>
        <Alias>Hana</Alias>
    </Aliases>
    <Libraries>
        <Library Platform="MSWindows">dbd_wnewdb</Library>
        <Library Platform="MSWindows">dbd_newdb</Library>
    </Libraries>
    <Parameter Name="Driver Name">HDBODBC</Parameter>
</DataBase>
```

- 監査で使用されているデータベースバージョンが MS SQL Server 2008 の場合、SBO での設定は次のようになります。

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
    <Libraries>
        <Library>dbd_wmssql</Library>
        <Library>dbd_mssql</Library>
    </Libraries>
    <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
    <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
    <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
    <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

- id="li_9D4EB94F9752458BB21A940C0A892C6D"> 監査で使用されているデータベースバージョンが MySQL 5 の場合、SBO は次のようなエントリになります。

```
<DataBase Active="Yes" Name="MySQL 5">
```

```
    <JDBCDriver>
        <ClassPath>
            <Path>C:¥mysqljdbcdriver.jar</Path>
              </ClassPath>
        <Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
        <Parameter Name="URL Format">jdbc:mysql://$DATASOURCE$/$DATABASE$</
Parameter>
    </JDBCDriver>
    <Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
    <Parameter Name="Force Execute">Always</Parameter>
    <Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
</DataBase>
```

- 監査で使用されるデータベースバージョンが Oracle の場合、SBO での設定は次のようになります。

```
<DataBase Active="Yes" Name="Oracle 11">
        <Aliases>
           <Alias>Oracle</Alias>
        </Aliases>
      <JDBCDriver>
            <ClassPath>

<Path>C:¥app¥Administrator¥product¥11.2.0¥client_64¥jdbc¥lib¥ojdbc6.jar</Path>
              </ClassPath>
                 <Parameter Name="JDBC Class">oracle.jdbc.OracleDriver</
Parameter>
                 <Parameter Name="URL Format">jdbc:oracle:thin:@//$DATASOURCE$/
$DATABASE$</Parameter>
       </JDBCDriver>
       <Parameter Name="Extensions">oracle11,oracle,jdbc</Parameter>
        <Parameter Name="Escape Character">/</Parameter>
         <Parameter Name="Force Execute">Always</Parameter>
         <Parameter Name="Catalog Separator">.</Parameter>
</DataBase>
```

SBO ファイルでのドライバの設定に関する詳細は、データアクセスガイドを参照してください。

20.2.2.1.4 SBO ファイルでのエイリアス名の追加

ドライバの設定に加えて、SBO にエイリアスを追加する必要もあります。場所は、監査で使用されているデータベースバージョンの下です。以下の表は、指定されたデータベースで使用されるエイリアス名の一覧です。

DB 名	SBO で使用されるエイリアス名
SAP HANA	HANA
Microsoft SQL Server	MS SQL Server
My SQL	MySQL
SAP Max DB	MaxDB
IBM DB2	DB2
Sybase SQL Anywhere	Sybase SQL Anywhere
Sybase Adaptive Server Enterprise	Sybase Adaptive Server Enterprise
Oracle	Oracle

モニタリングアプリケーションが SBO でこれらの名前を検索するため、指定された名前を使用する必要があります。

例

監査に使用されるデータベースが MS SQL Server 2008 の場合、エイリアスを以下に示すように SBO に追加する必要があります。

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
        <Aliases>
        <Alias>MS SQL Server</Alias>
        </Aliases>
            <Libraries>
                <Library>dbd_wmssql</Library>
                <Library>dbd_mssql</Library>
            </Libraries>
            <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
            <Parameter Name="CharSet Table" Platform="Unix">datadirect</
Parameter>
            <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
            <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
   </DataBase>
```

20.2.2.1.5 監査データベースに切り替える

モニタリングトレンド情報が監査データベースに保存されるようにデータベースを切り替えます。

1. CMC ホームページの管理領域で、アプリケーションをクリックします。
2. [*BI* 管理スタジオ] をクリックします。
3. 次に、[モニタリングプロパティ] をクリックします。
4. [モニタリングアプリケーション] をダブルクリックして、その [プロパティ] ページを開きます。
5. トレンドデータベースの設定領域で、監査データベースを使用を選択します。

> **注記**
>
> 監査に Oracle データベースを使用している場合は、CMC の監査ページの [*ADS* データベース接続名] を JDBC 接続として指定する必要があります。接続名を次のように指定します。
> `<server_name>,<port>,<service_name>`

> **注記**
>
> モニタリングテーブルを正しく作成するには、データベースユーザアカウントに以下の権限を付与します。
>
> EXECUTE
> CREATE SEQUENCE
> CREATE TRIGGER

20.2.2.2 JDBC を使用したモニタリングデータベースの設定

JDBC の接続を作成しておきます。新しい JDBC 接続を作成するには、以下の手順を実行します。

1. 設定するデータベースの JDBC ドライバ jar を以下の場所に配置します。`<INSTALL_DIR¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥services¥MON.MonitoringService¥lib>`

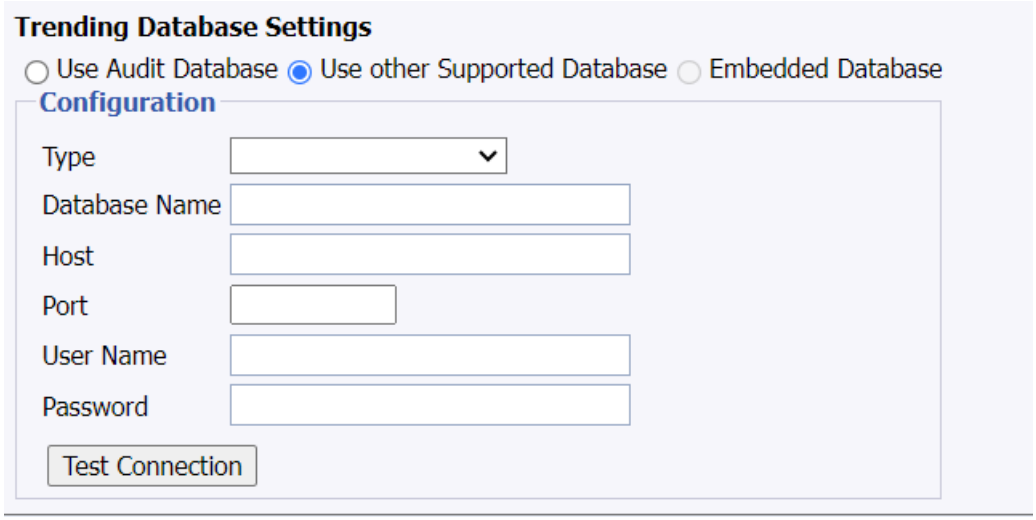
   > **注記**
   >
   > クラスタ化されたデプロイメントでは、モニタリングサービスをホストするシステムに JDBC ドライバをコピーする必要があります。

2. SIA を再起動します。

BI 監視用の新しいデータベースを設定するには、以下の手順を実行します。

1. CMC にログオンします。
2. CMC のホームページで、ドロップダウンメニューから [アプリケーション] を選択します。
3. [*BI* 管理スタジオ] を右クリックして、[モニタリングプロパティ] を選択します。

   [モニタリングアプリケーションのプロパティ] ポップアップウィンドウが表示されます。デフォルトで、[監査データベースを使用] ラジオボタンが選択されています。
4. [その他のサポートされているデータベースを使用] ラジオボタンを選択します。
5. [タイプ]、[データベース名]、[ホスト]、[ポート]、[ユーザ名]、および [パスワード] を入力します。



6. オプション: [*X* 日より古いすべての履歴を削除] プロパティを使用して、プラットフォームでモニタリング履歴データが削除されるまでの日数を追加します。
7. [保存して閉じる] を選択します。
8. Adaptive Processing Server を再起動します。

   [接続テスト] を選択して、接続を検証できます。

   > **注記**
   >
   > 変更を反映するには、BI 監視サービスをホストしているすべての APS サーバを再起動する必要があります。

これで、BI 監視アプリケーションのコメントを保存する新しいデータベースが設定されました。

20.2.3 設定プロパティ

この節では、モニタリングアプリケーションのプロパティとその編集方法について説明します。

モニタリングアプリケーションの設定プロパティを参照するには、以下の手順に従います。

1. CMC のホームページで、[アプリケーション] をクリックします。
2. [*BI* 管理スタジオ] を右クリックして、[モニタリングプロパティ] を選択します。設定可能なプロパティについて、以下で説明します。

セクション	フィールド	説明
	モニタリングアプリケーションを有効にする	モニタリング機能を有効化するには、このオプションを選択します。このオプションの選択を解除した場合、プローブを除くすべてのモニタリング機能が無効化されます。プローブトレンディングも無効化されます。
	デフォルトの *JMX* エージェントエンドポイント *URL (IIOP)*	このフィールドには、IIOP プロトコルを使用するデフォルトの JMX エージェントエンドポイント URL が含まれています。モニタリングを有効にしてからサーバを再起動した場合、この URL は自動的に生成されます。これは、モニタリングサービスのデフォルトプロトコルです。これは読み取り専用のフィールドです。
RMI	*JMX* 用 *RMI* プロトコルを有効にする	デフォルトでは、このオプションは無効になっています。このオプションを有効化するには、RMI ポート番号を指定する必要があります。このポートは、RMI レジストリエントリと RMI コネクタポートの両方に使用されます。このポートは、サービスで利用できるようにする必要があります。利用できない場合、サービスを開始できません。 RMI ポート番号を指定したら、サーバを再起動します。サーバを再起動すると、RMI JMX エージェントのエンドポイント URL が生成されます。これは、RMI プロトコルを使用する JMX エージェントエンドポイント URL を含んだ読み取り専用プロパティです。この URL を使用して、ほかのクライアントからモニタリングに接続します。
ホストメトリクス	ホストメトリクスを有効にする	デフォルトでは、このオプションは無効になっています。このオプションを有効化した場合、SAPOSCOL バイナリのインストールへのパスを指定する必要があります。 ホストメトリクスを有効にするには、SAPOSCOL をインストールする必要があります。 SAPOSCOL のインストール方法に関する詳細については、“SAPOSCOL のインストール”を参照してください。

セクション	フィールド	説明
トレンドデータベースの設定	監査データベースを使用	このオプションを選択すると、監査データストア (ADS) 監査データベースにメトリクスのトレンド履歴を保存できます。 **注記** この処理を実行するには、監査データストアを設定する必要があります。
	他のサポートされているデータベースを使用	このオプションを選択すると、設定したサポートされているデータベースにメトリクス/監視トレンド履歴を保存できます。
	X 日より古いすべての履歴を削除	履歴データを保存する期間 (日数) を指定します。
その他の設定	メトリクスの最新表示間隔 (秒)	設定できる最小の間隔は 15 秒です。間隔によって以下を管理できます。 • 監視の予約計算注意と危険ルールは、指定された時間間隔を使用して継続的に計算されます。 • 監視ステータスの計算監視のイベント設定に以下のオプションが選択されていても、指定された間隔で監視ステータスが継続的に計算されます。注意または危険のルール評価が *true* であるたびに監視ステータスを変更します。. • トレンド期間: 履歴モードのグラフは、指定された間隔で継続的に記録されます。
	UI モニタリングの自動最新表示間隔 (秒)	この間隔は、自動最新表示について、モニタリングユーザインタフェース (ダッシュボード、監視リスト、プローブを含む) で使用されます。最小間隔は 15 秒です。自動最新表示は、ライブモードでのグラフの経過時間 (デフォルトで 15 秒に設定) に影響を与えません。
	警告アラームの頻度 (日)	警告アラームが生成されるまでの日数を指定します。

3. 保存をクリックします。

> **注記**
> モニタリングアプリケーションの有効化と無効化を除くこれらのプロパティを変更する場合、モニタリングサービスをホストする Adaptive Processing Server を再起動する必要があります。

SAPOSCOL のインストール

SAPOSCOL をインストールするには、次の手順を実行します。

1. SAP Service Marketplace (http://service.sap.com) から `SAPHOSTAGENT710_XX.SAR` をダウンロードします。

2. `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR` コマンドを実行して、`SAPHOSTAGENT710_XX.SAR` を抽出します。
3. `saphostexec.exe -install` コマンドを実行して、`saphostexec` をインストールします。saphostexec がサービスとしてインストールされると、SAPOSCOL が起動します。
4. `saposcol -s` コマンドを実行して SAPOSCOL のステータスを確認します。

20.2.3.1 JMX エンドポイント URL

モニタリングアプリケーションでは、ほかのクライアントが JMX リモート API を使用した接続するに利用できる JMX エンドポイント URL が公開されます。デフォルトでは、JMX 接続は IIOP (Internet Inter-Orb Protocol) または CORBA (Common Object Request Broker Architecture) 移送を介して提供されます。この接続 URL は、モニタリングアプリケーションの [プロパティ] ページに表示されます。IIOP を介した接続が可能な場合、ファイアウォールおよびポートの公開に関する心配が不要になります。CORBA ポートは、デフォルトで使用できます。下の表で一覧にされている jar ファイルは、JMX クライアント側での接続に必要です。

Jar ファイル
activation-1.1.jar
axiom-api-1.2.5.jar
axiom-impl-1.2.5.jar
axis2-adb-1.3.jar
axis2-kernel-1.3.jar
cecore.jar
celib.jar
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar
logging.jar
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wsdl4j-1.6.2.jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar

Jar ファイル
aspectjrt.jar

もう 1 つのオプションは、デフォルト RMI ポートを介した接続です。デフォルト RMI ポートを介した接続方法の詳細については、設定プロパティ [784 ページ]を参照してください。

20.2.3.2 JMX SSL 設定

JMX SSL 設定を使用して、JConsole と BOE 間の安全な通信を実行できるようになりました。

1. CMC にログインします。
2. アプリケーション > *BI* 管理スタジオ > モニタリングプロパティ に移動します。
3. [*RMI*] で、[*JMX 用 RMI プロトコルを有効にする*] オプションを有効にします。
4. RMI ポート番号を入力します。

   7777
5. [*JMX 用 RMI プロトコルに対して SSL を有効にする*] オプションを有効にします。
6. [保存] および [閉じる] をクリックします。
7. *Adaptive Processing Server* を再起動します。

> **注記**
>
> モニタリングサービスをホストしているサーバが再起動されます。

20.2.3.2.1 証明書の生成

1. 管理者モードまたはターミナルセッションでコマンドプロンプトを開き、以下の場所に移動します。

   Windows:

   ```
   INSTALLDIR¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥bin
   ```

   Linux/Unix:

   ```
   INSTALLDIR/sap_bobj/enterprise_xi40/<PLATFORM>_x64/sapjvm/bin
   ```
2. 証明書を生成するためのコマンド: `keytool -genkeypair -alias serverkey -keyalg RSA -keysize 2048 -keystore serverkeystore` を実行します。
3. 証明書を作成するために必要な情報をすべて入力します。
4. 4. 実行が成功すると、同じ sapjvm bin ディレクトリ: `serverkeystore` で証明書ファイルが名前別に作成されます。

20.2.3.2.2 証明書ストアファイルのモニタリングサービスへの追加

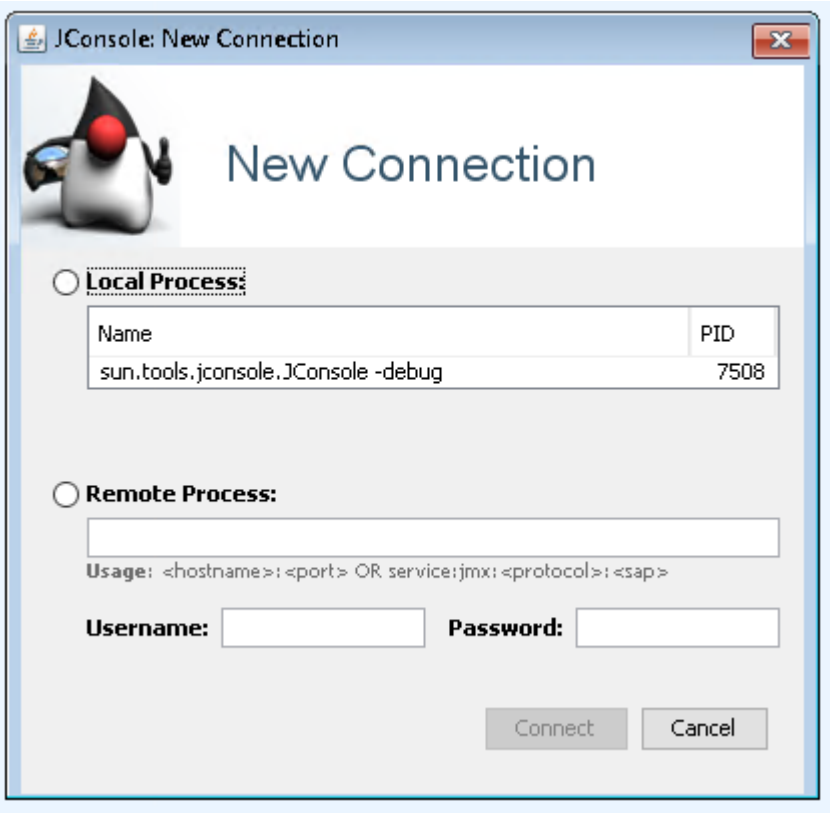
1. CMC で、サーバ > サーバの一覧 に移動します。
2. [*Adaptive Processing Server*] (監視サービスをホストするサーバ) を選択します。
3. [プロパティ] を選択します。
4. [*JMX SSL* 設定] セクションに移動します。
5. [証明書ストアファイルの場所] に、証明書キーストアファイルの場所のパスを入力します。
6. [秘密鍵のアクセス用パスワード] 情報を入力します。

   Password1

20.2.3.2.3 JConsole への接続

1. コマンドプロンプトで、`JCONSOLE.exe` を起動するためのコマンド (`jconsole.exe -J-Djavax.net.ssl.trustStore="<Path of Certificate Keystore file location >" -J-Djavax.net.ssl.trustStorePassword=<PasswordDetail>`) を実行します。

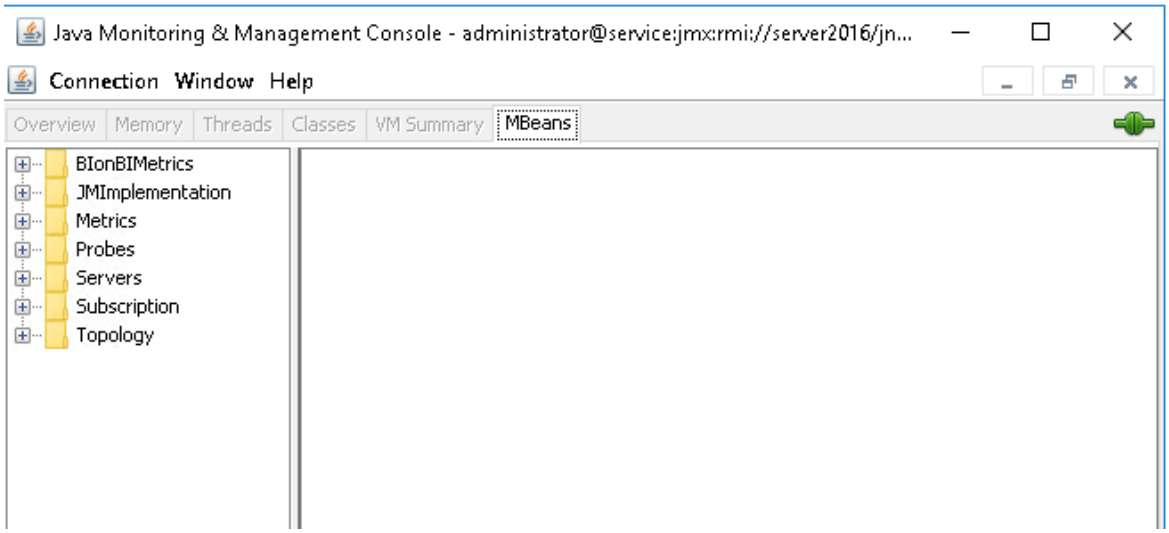
   ```
   jconsole.exe -J-Djavax.net.ssl.trustStore="C:¥Program Files (x86)¥SAP
   BusinessObjects¥SAP BusinessObjects Enterprise XI
   4.0¥win64_x64¥sapjvm¥bin¥serverkeystore" -J-
   Djavax.net.ssl.trustStorePassword=Password1
   ```
2. 上記のコマンドが実行された後、下のように JConsole ビューアが起動します。



3. [リモートプロセス] ラジオボタンをクリックし、フィールドを有効化します。
4. [*RMI JMX エージェントエンドポイント URL*] と、関連する [ユーザ名] および [パスワード] を入力します。

   [*RMI JMX エージェントエンドポイント URL*] の書式は以下のとおりです。 `service:jmx:rmi:// <HostName>/jndi/rmi://<HostName>:<RMI Port Number>/<hostname>:<CMS Port>`.

   `service:jmx:rmi://server2016/jndi/rmi://server2016:7777/server2016:6400`.
5. [接続] をクリックします。
6. JConsole ビューア [*JAVA Monitoring & Management Console*] が起動します。



7. JConsole ビューアでは、関連データを取得するため、各種のセクション ([BIonBIMetrics]、[Metrics]、[Probes]、[Servers]、[Topology] など) に移動できます。

20.2.3.3 プローブの監視のための HTTPS 認証

プローブの監視のための HTTPS サーバ認証がサポートされており、使用する前には、以下の設定が必要です。

1. サーバ証明書をクライアントの truststore にインポートします。これにより、クライアント側 (プローブ) でサーバの ID を検証できます。次のコマンドを実行します。`<INSTALL_ROOT>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥lib> keytool -import -alias ca -keystore "<INSTALL_ROOT>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥jre¥lib¥security¥cacerts" –file ca.cer`
   `ca.cer` は、サーバの自己署名証明書か、サーバの証明書を生成した認証機関 (通常は内部 CA) の証明書のいずれかです。サーバの証明書が既知の CA によって生成され、インポートの必要がない場合、この手順はスキップできます。これは、サーバの証明書が CA で検証され、その公開鍵がデフォルトですでに truststore にあるためです。
2. BI ラウンチパッドのプローブの設定にある [*URL ベース*] を `https://<URL>/BOE/BI` に変更します。
   <URL> は、証明書内で使用されている名前のホストです。

プローブの監視のための HTTPS クライアント認証はサポートされていません。

20.2.3.4 プローブのパスワードの暗号化

プローブを使用する場合、パスワードが暗号化されていることを確認します。コマンドラインを介してプローブを作成する場合は、`true` パラメータを各モニタリングプローブのパスワードパラメータに追加する必要があります。詳細および構文例については、CMC のヘルプのコマンドラインを介したプローブの管理に関するトピックを参照してください。

20.2.4 その他アプリケーションとの統合

IBM Tivoli Monitoring などのエンタープライズソリューションは、JMX エンドポイントの URL を経由して接続する JMX クライアントなどのモニタリングアプリケーションと統合されます。統合後、SAP BusinessObjects メトリクスをクライアントのユーザインタフェースから表示することができます。

20.2.4.1 モニタリングアプリケーションと SAP Solution Manager との統合

モニタリングアプリケーションを SAP Solution Manager と統合するには、Wily Introscope がシステムにインストールされ、実行中である必要があります。SAP Solution Manager を Introscope ワークステーションに対して設定する必要があります。BI プラットフォームインストール中に次の手順を実行します。

1. "Wily Introscope Enterprise Manager への接続の設定"ステップで、ホスト名とポート詳細を指定します。BI プラットフォームのインストール時に、`C:¥Program Files (x86)¥SAP Business Objects¥SAP BusinessObjects Enterprise XI 4.0¥java¥Wily` にインストールされます。
2. Wily Introscope ワークステーションを起動して、[*New Investigator*] をクリックします。設定されたエージェントの JMX セクションに SAP BusinessObjects サーバメトリクスおよびプローブ仮想メトリクスを表示することができます。

> **注記**
>
> Wily Introscope (IS) エージェントは、*CMC* > *Servers* > *Server node* > *Placeholders* の順に選択して設定できます。IS Enterprise Manager のホストおよびポートもここで設定でき、IS エージェントがモニタリングアプリケーションと通信できるようにすることができます。詳細については、CMC ヘルプのサーバの管理を参照してください。
>
> JMX メトリクスを IS で使用できるようにするには、IS エージェントサービスとモニタリングサービスの両方を AdaptiveProcessingServer のインスタンスで使用できるようにします。
>
> IS の計測を有効化すると、コード計測が自動的に有効になります。

20.2.5 モニタリングサーバのクラスタサポート

モニタリングアプリケーションは、フェールオーバー機能を提供するクラスタリングをサポートしています。

クラスタサポートにより、いつでも 1 つのサービスのみがアクティブになり、その他すべてのサービスはパッシブになります。クラスタ環境において、2 つのモニタリングサービス s1 と s2 がある場合、いずれか 1 つのみが使用できます。s1 と s2 の両方がアクティブになろうとしますが、いずれか 1 つがアクティブになると、もう 1 つのサービスは非アクティブになるか、パッシブになります。

パッシブサービスでは、アクティブなサービスが利用可能であることを定期的 (毎分) に確認します。アクティブなサービスが利用できない場合、パッシブなサービスはすぐにアクティブになろうとします。

> **注記**
>
> Adaptive Processing Server (APS) のエラー、またはパフォーマンスの低下を避けるため、独立した APS インスタンス上でモニタリングサービスをホストすることをお勧めします。

20.2.6 トラブルシューティング

ここでは、モニタリングアプリケーションでの操作中に生じる可能性のある広範な問題に対して、解決策を段階的に説明します。

20.2.6.1 ダッシュボード

CMC ページにモニタリングリンクが表示されません。

- ユーザに適切なアクセス権があるかを確認する。
- ユーザがモニタリングユーザグループまたは管理者グループ、またはこれらのグループの一部であるその他のグループに追加されていることを確認する。

モニタリングダッシュボードに事業業績評価指標 (KPI) が表示されません。

- サーバプロパティ > メトリクス の順に選択し、必要なメトリクスが表示されるかを確認します。
- Central Management Server が正常に応答していることを確認する。

20.2.6.2 警告

アラートページでアラートを受け取ることができません。

- アラートアプリケーションのプロパティで [マイアラートの有効化] オプションが選択されているかを確認する。
- アラートを受信するための適切なアクセス権があることを確認する。

- モニタリングダッシュボードに最近のアラートが表示されるかを確認する。

> ⓘ 注記
>
> SMTP が正しく動作しているかをテストするために設定した電子メール ID に Crystal Reports ドキュメントを送信できます。

電子メール通知を受信できません

- アラートアプリケーションのプロパティで [電子メールを有効にする] オプションが選択されているかを確認する。
- 電子メールアラートを受け取るための電子メールアドレス設定が適切であるかを確認する。
- SMTP サーバが機能しているかを確認する。
- Adaptive Job Server インスタンスが有効になっていることを確認する。
- Adaptive Job Server インスタンス出力先の SMTP 設定を確認する。

20.2.6.3 監視リスト

監視の履歴データを受信できません

- モニタリングアプリケーションの [プロパティ] ページでポーリング間隔を確認する。
- ロギングフォルダのトレースファイルを確認する。
- 特定のタイムゾーンのサーバとクライアントのシステム時間が同じであるかを確認する。

同期ライブデータを取得中にエラーが発生しました。

Adaptive Processing Server インスタンスが実行中であるかを確認する。

監視リストタブは無効です

- モニタリングサービスが実行されているかどうかを確認する。
- エラーメッセージのモニタリングサービスログを確認する。
- サーバおよびそのメトリクスに jconsole からアクセスできるかどうかを確認する。

20.2.6.4 プローブ

プローブをスケジュールできません。

- プローブスケジュールサービスをホストする AdaptiveJobServer インスタンスが実行中であるかを確認する。
- Crystal Reports および Web Intelligence ドキュメントに使用するレポート CUID が適切であることを確認する。
- ユーザに管理権限があるか、またはユーザが管理者グループのメンバーであることを確認する。
- ユーザに、対応するプローブに使用する Crystal Reports または Web Intelligence ドキュメントを開く、最新表示する、エクスポートするための適切な権限があるかを確認する。

プローブのスケジュールステータスが **[**保留**]** です。

- ProbeSchedulingService インスタンスがインストールされているかを確認する。
- プローブスケジュールサービスをホストする AdaptiveJobServer インスタンスが実行中であるかを確認する。

データベースからトレンドデータを取得中にエラーが発生しました。

AdaptiveProcessingServer インスタンスが実行中であるかを確認します。

probeRun.bat を実行できません

- `java_home` が設定されているかを確認する。
- コマンドプロンプトに正しいパラメータが入力されているかを確認する。

> **注記**
>
> コマンドプロンプトに「**`probeRun.bat -help`**」と入力し、すべてのパラメータが適切であることを確認します。

20.2.6.5 メトリクス

ホストメトリクスが一覧表示されません。

- SAPOSCOL が実行中であることを確認する。
- モニタリングアプリケーションの [プロパティ] ページで、[ホストメトリクスを有効にする] オプションが選択されていることを確認する。
- AdaptiveProcessingServer インスタンスを再起動して変更を有効にする。
- [*SAPOSCOL バイナリのインストール場所のパス*] が適切であることを確認する。

JMX Client の取得中にエラーが発生しました。

AdaptiveProcessingServer インスタンスが実行中であるかを確認します。

メトリクスページの **SAPOSCOL** メトリクス値がゼロです。

- SAPOSCOL が実行中であることを確認する。
- SAPOSCOL がインストールされているホスト上で、以下を実行します。
  1. `saposcol -s` でステータスをチェック
  2. `saposcol -m` で SAPOSCOL によって収集されたデータのスナップショットを取得

20.2.6.6 チャート

チャートに表示されるライブモードおよび履歴モードの時間が異なります。

特定のタイムゾーンのサーバとクライアントのシステム時間が同じであることを確認します。

20.3 Visual Difference

Visual Difference を用いて、LCMBIAR またはオブジェクト、またはその両方の 2 つのバージョン間の差分を表示することができます。この機能を使用すると、ファイルまたはオブジェクト間の差分を確認し、さまざまな種類のレポートを作成および管理できます。この機能では、比較元バージョンと比較先バージョン間の比較ステータスが提供されます。たとえば、以前のバージョンのユーザレポートが正確で現在のバージョンのユーザレポートは不正確である場合、ファイルを比較および分析して問題点を評価できます。

ホーム ページ

Visual Difference ホームページは、次のタブおよびペインで構成されています。

- 新しい比較 - このタブでは、オブジェクト間の新しい比較を作成できます。
- 比較の検索 - このフィールドでは、すでに比較したオブジェクトを検索できます。
- [比較] ペイン - このペインには、フィルタおよび差分のタブの一覧が表示されます。
- 比較: [差分] ペイン - このペインには、比較されたオブジェクト、比較名、日付/時刻、および差分のステータスが一覧で表示されます。

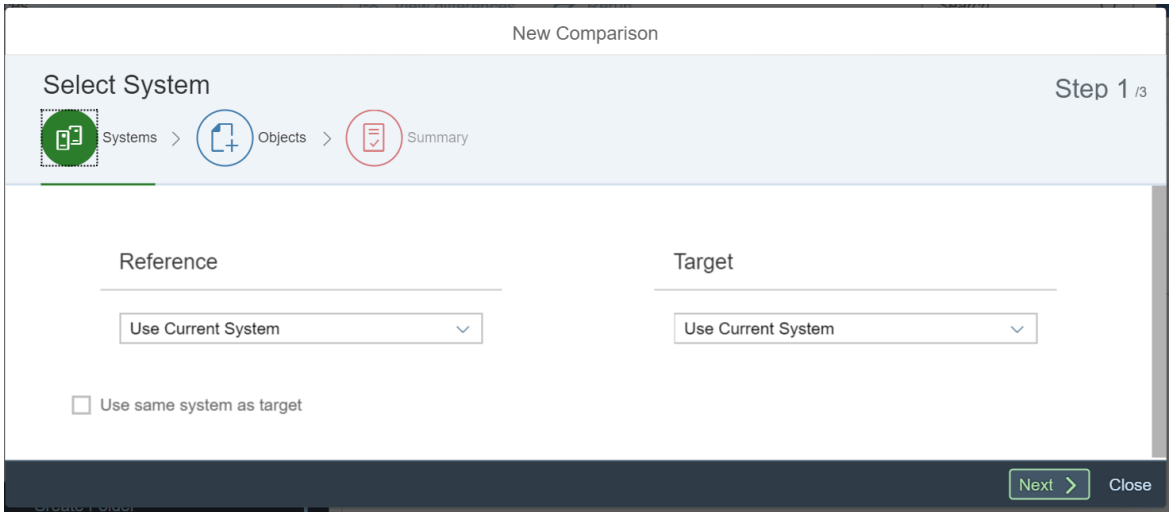
20.3.1 Visual Difference を使用してオブジェクトまたはファイルを比較する

Visual Difference を使用してファイルを比較するには、次の手順に従います。

1. CMC アプリケーションにログインします。
2. CMC ホームページで、管理タブの *Visual Difference* リンクをクリックします。
   Visual Difference ページが表示されます。比較対象のファイルは、"Differences" フォルダまたはユーザが作成したいずれかのサブフォルダに保存されています。

   > **注記**
   >
   > 新しいサブフォルダを作成するには、Create Folder + を選択します。

3. + を選択して、新しい比較を作成します。
   [新しい比較] ウィザードが表示されます。



4. [参照] および [ターゲット] システムをドロップダウンから選択します。
   以下の参照およびターゲットシステムのいずれにも接続できます。

   > **注記**
   >
   > オブジェクトがバージョン管理システム (VMS) に追加されている場合、次のステップでバージョンを選択することができます。

- CMS
- ローカルファイルシステム

5. [オブジェクト選択] 画面で、[参照] および [ターゲット] システムからオブジェクトまたはファイルを検索して選択します。
6. 必要であれば [比較名] を変更します。
7. [比較] を選択して、オブジェクトを比較します。

> ⓘ 注記
>
> - 差異をチェックするには、まず比較を選択し、次に [違いを表示] を選択します。差分はオレンジ色で強調表示され、見つからないオブジェクトは赤色で強調表示されます。
> - 比較を再実行するには、まず比較を選択し、次に [再実行] を選択します。

比較処理はすぐに開始されます。

また、比較したオブジェクトは、フィルタオプションを使用してタイプ別に表示したり、差分または共通の属性と共に表示することもできます。

20.3.2 バージョン管理システムを使用してオブジェクトまたはファイルを比較する

Visual Difference オプションを使用すると、バージョン管理システム内のプロモーションマネジメントジョブまたはフォルダを比較することができます。

バージョン管理システム内のオブジェクトを比較するには、次の手順に従います。

1. CMC アプリケーションにログオンします。
2. CMC ホームページで、管理タブの *Visual Difference* リンクをクリックします。
   Visual Difference ページが表示されます。比較対象のファイルは、"Differences" フォルダまたはユーザが作成したいずれかのサブフォルダに保存されています。

   > ⓘ 注記
   >
   > 新しいサブフォルダを作成するには、フォルダアイコンをクリックします。

3. [新しい比較] をクリックします。
   比較画面が表示されます。
4. [参照] の [システムの選択] から [*VMS にログオン*] を選択します。
5. VMS へのログイン認証情報を入力し、ログオンをクリックします。
   ターゲットシステムの自動選択ダイアログボックスが表示されます。
6. 異なるターゲットシステムを設定する場合は [いいえ] をクリックし、ターゲットシステムを参照システムと同じように設定する場合は、[はい] をクリックします。
7. [参照] をクリックし、参照システムおよびターゲットシステムの両方から、比較するオブジェクトまたはジョブを選択します。
8. 追加をクリックします。
   比較目的で選択されたオブジェクトの一覧が、新しい比較ペインに表示されます。
   ファイルの比較をすぐに行うことも、後で行うようにスケジュールすることもできます。ファイルを比較するには、続けて次の手順に従います。

9. [比較] をクリックして、ジョブまたはフォルダを比較します。
   比較処理はすぐに開始され、差分が存在する場合は [*Visual Difference ビューア*] に表示されます。差分はオレンジ色で強調表示され、見つからないオブジェクトは赤色で強調表示されます。
   また、比較したオブジェクトは、フィルタオプションを使用してタイプ別に表示したり、差分または共通の属性と共に表示することもできます。
10. 差分レポートを保存するには、[保存] をクリックします。
11. レポートを保存する場所を指定して、[*OK*] をクリックします。

20.4 HTML 要素の許可

信頼できる HTML 要素の機能を活用し、その他すべての要素から組織を保護するには、権限のある HTML 要素の一覧を指定します。

Web Intelligence HTML ビューアまたはインタラクティブビューアで、[HTML として読み込む] または [ハイパーリンクとして読み込む] プロパティが設定されたセルを含むドキュメントを開くと、ビューアで HTML が解釈される場合があります。この動作は、Web Intelligence の表示プロパティで定義されているこれらのセルの表示方法と、許可する HTML 要素に応じて決まります。

権限のある HTML 要素が指定されていて、読み取りモードのドキュメントに許可されていない要素が含まれている場合には、その要素のテキストのみが保持され、要素タグまたはその属性は保持されません。ドキュメントに権限のある要素が含まれていて、許可された属性と許可されていない属性の両方がある場合は、その要素と許可された属性のみが保持されます。

特定の HTML 要素のみを許可するには、Web Intelligence の JavaScript 表示プロパティで [*許可された HTML エレメントページに定義されている HTML エレメントのみを有効にする*] を選択し、[*権限のある HTML 要素*] ページで HTML 要素を指定します。

デフォルトでは、Web Intelligence を正常に機能させるために必要な HTML 要素のみが許可されます。デフォルト一覧に対して、要素を追加または削除することができます。

⚠ 警告

- Web Intelligence では、式の能力によって、ドキュメントセル内の埋め込み JavaScript/HTML コードが有効化されます。
  このコードは、セントラル管理コンソールで有効化または無効化できます。ただし、JavaScript、HTML、およびハイパーリンクを承認することで、クロスサイトスクリプティングにさらされるリスクを認識することになります。クロスサイトスクリプティングによって、攻撃者が Web サイトを変更したり、他のシステムでコードを実行したりできるようになります。この脆弱性は、スクリプトの実行時にインターネットブラウザなどの製品に影響します。クロスサイトスクリプティング攻撃の大部分は、ターゲットシステムでの安全でないプログラミングに起因します。
- コードは、権限のある HTML タグおよび属性の一覧を使用して微調整できます。ただし、SAP はこのコードの互換性と、考えられる副次的な影響について責任を負いません。たとえば、ブラウザ更新、JavaScript バージョンサポート、または Web ページでコードを動的に埋め込む方法により、コードによっては一部の調整が必要になることがあります。技術的な観点から、4.3 リリース以降、アプリケーションは単一ページアプリケーションとして実行されます。レポートと Web ページ全体の間の技術的分離はありません。このコードには、新しいコンテキストで実行するために調整が必要になる場合があります
- デフォルト一覧から要素を削除すると Web Intelligence の機能が損なわれるため、削除しないことをお奨めします。

以下のものを許可することができます。

- 参照を追加するために、属性 `href` を持つ要素 `<a>` を許可することができます。
- 要素 * を属性の一覧に関連付けることにより、一覧内のすべての要素について、特定の属性セットを許可することができます。
  1 つの要素に関連付けられたすべての属性を許可することはできません。
- `<script>`、`<onClick>`、`<onMouseEnter>` など、JavaScript を含む可能性のある要素を許可することができます。
  JavaScript キーワードは許可できません。

例

権限のある HTML 要素

要素	属性
*	style、class、id
img	src
link	ref

以下の表に、許可によって Web Intelligence で HTML 要素がどのようにドキュメントに表示されるかを示します。

HTML 要素の許可による影響

元の **HTML**	最終的な **HTML**	説明
`<link title="SAP" ref="www.sap.com">`	`<link ref="www.sap.com">`	`<link>` 要素と `ref` 属性は許可されているため、リンクはドキュメントで有効なリンクとして表示されます。 `title` 属性は許可されていないため、ドキュメントから削除されます。
`<img src="datasource" id="I1">`	`<img src="datasource" id="I1">`	`<img>` 要素および関連する `src` 属性は許可されていて、`id` 属性はすべての要素で許可されているため、元の HTML のままになります。
`<div title="datasource" id="D1">`	削除されます。	`<div>` 要素は許可されていないため、この要素および関連する属性はドキュメントから削除されます。

元の HTML	最終的な HTML	説明
`<p> ...as shown in the picture below: <img src="../picture.jpg" alt="Mountain"> </p>`	`...as shown in the picture below:<img src="../picture.jpg">`	`<p>` 要素は許可されていないため、削除されます。`<p>` 要素に含まれているテキストのみが表示されます。 `<img>` 要素および関連する `src` 属性は許可されているため、表示されます。 `alt` 属性は許可されていないため、ドキュメントから削除されます。

Web Intelligence の表示設定を変更する [680 ページ]権限のある HTML 要素の一覧を変更する [799 ページ]

20.4.1 権限のある HTML 要素の一覧を変更する

権限のある HTML 要素の一覧を変更することにより、許可する信頼性の高い HTML 要素を指定して、悪意のある可能性のある要素から保護します。

Web Intelligence では、Web Intelligence のプロパティで JavaScript 表示プロパティ [*許可された HTML エレメントページに定義されている HTML エレメントのみを有効にする*] が有効になっている場合、[*権限のある HTML 要素*] ページで定義した要素のみが許可されます。

1. CMC に移動し、[*BI 管理スタジオ*] を選択します。
2. セントラル管理コンソールの [ホーム] で、[*HTML 要素*] まで下にスクロールします。
3. 以下の表に示すように、一覧を変更します。

変更	手順
要素を追加する	[新しい要素を追加します] をクリックして、許可する要素と関連する属性を入力します。 **注記** • すべての HTML 要素の特定の属性を許可するには、要素として「*」を入力し、属性を追加します。 • すでに一覧にある HTML 要素を追加しようとした場合は、その要素の新しい属性のみが一覧に追加されます。
要素を編集する	要素をクリックして [選択した要素を編集します] をクリックします。
要素を削除する	要素をクリックして [選択した要素を削除します] をクリックします。
権限のある **HTML** 要素のデフォルト一覧を復元する	[リセット] をクリックします。 デフォルト一覧には、Web Intelligence を正常に機能させるために必要な要素のみが含まれています。

21　CMS レポーティング

21.1　CMS レポーティング

CMS のレポーティングを開始する前に、以下の概念についての基本的な理解が必要です。

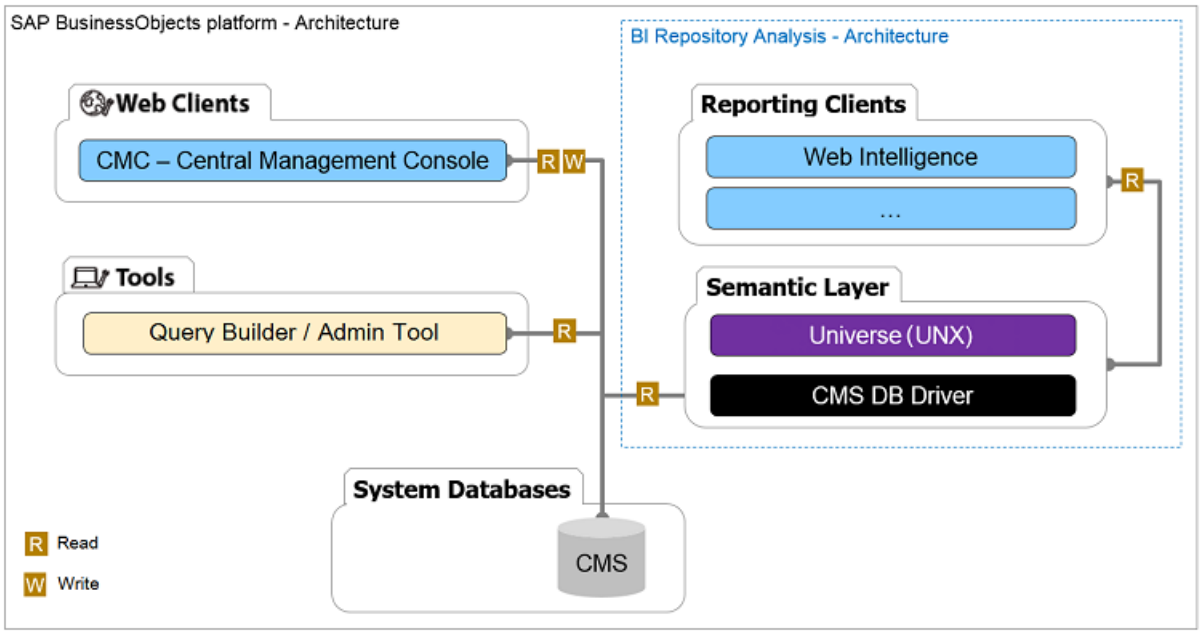
- SAP BusinessObjects プラットフォームのアーキテクチャ
- CMS システムデータベースの構造
- InfoObject プロパティおよび関係

関連情報

SAP BusinessObjects プラットフォームのアーキテクチャ [800 ページ]
CMS システムデータベースの構造 [801 ページ]

21.1.1 SAP BusinessObjects プラットフォームのアーキテクチャ

スキーマは、SAP BusinessObjects プラットフォームのアーキテクチャを理解できるように設計されています。



以下の表に、SAP BusinessObjects プラットフォームのコンポーネントの追加情報を示します。

SAP businessObjects プラットフォームのコンポーネント

コンポーネント	説明
CMC - セントラル管理コンソール	セキュリティの設定および以下の項目の管理に使用する Web ベースのツールです。 • ユーザ • コンテンツ • サーバ
CMS システムデータベース	以下の BI プラットフォーム情報を格納するデータベースです。 • ユーザ • サーバ • ドキュメント • 設定 • 認証 CMS システムデータベースは Central Management Server (CMS) によって保守され、システムリポジトリとして参照することができます。
クエリビルダ (管理ツールとも呼ばれる)	BusinessObjects リポジトリをクエリして、CMC では見つからない必須情報を取得するために使用する Web ベースのツールです。
BI リポジトリ分析	このソリューションでは、BI プラットフォームのセマンティックレイヤ、ユニバース (UNX)、および CMS DB ドライバを使用して、CMS をクエリします。

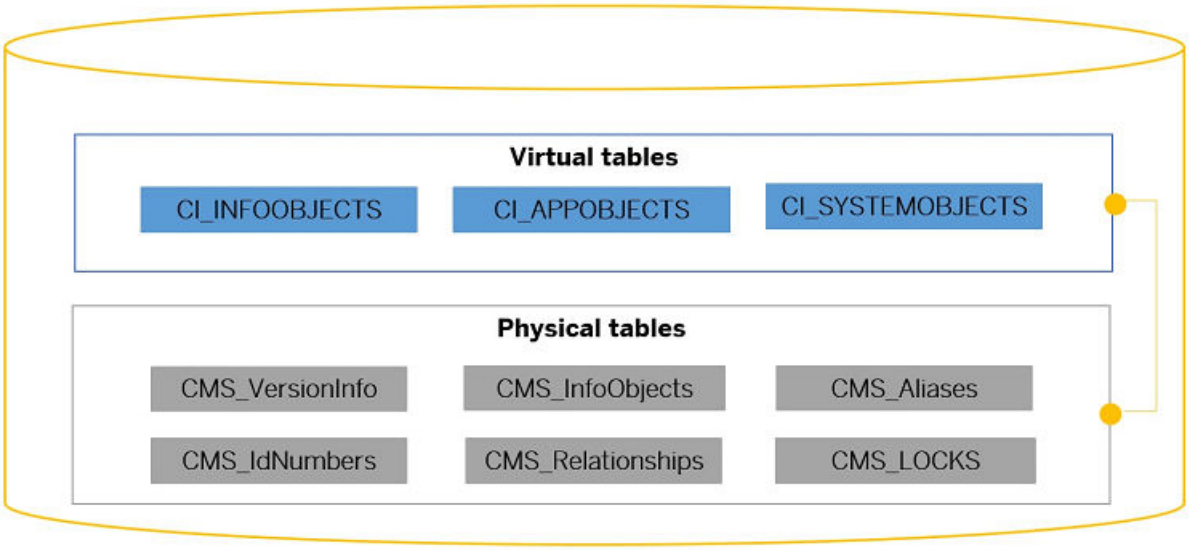
21.1.2 CMS システムデータベースの構造

CMS システムデータベースは Central Management Server (CMS) によって保守され、システムリポジトリとして参照することができます。CMS システムは、BI プラットフォーム情報が InfoObject の形式で格納されるデータベースです。

CMS システムデータベースには、2 種類のテーブルが含まれます。

- 物理データベーステーブル: CMS メタデータは物理データベーステーブルに格納されます。
- 仮想テーブル: CMS サーバは仮想テーブルで InfoObject を参照します。

以下のスキーマは、CMS システムデータベース構造の概要を示します。



CMS システムデータベース構造の詳細については、関連トピックを参照してください。

関連情報

物理データベーステーブル [802 ページ]
仮想テーブル [803 ページ]

21.1.2.1 物理データベーステーブル

CMS メタデータは 6 つの物理データベーステーブルに格納されます。

物理データベーステーブル

物理テーブル	説明
CMS_VersionInfo	BusinessObjects Enterprise (BOE) の現行バージョンが含まれます。
CMS_InfoObjects	システムリポジトリ内のメインテーブル。各行に単一の InfoObject が格納されます。
CMS_Aliases	ユーザエイリアスを対応するユーザ ID にマップします。ユーザがメンバーとなっているセキュリティドメインごとに、ユーザのエイリアスがあります。ただし、ユーザのユーザ ID は 1 つのみです。
CMS_IdNumbers	一意のオブジェクト ID およびタイプ ID を生成します。

物理テーブル	説明
CMS_Relationships	InfoObject 間の関係を格納します。
CMS_LOCKS	CMS_RELATIONS の補助テーブル。

21.1.2.2 仮想テーブル

CMS サーバは 3 つの仮想テーブルで InfoObject を参照します。

仮想テーブル

仮想テーブル	説明
InfoObject テーブル	エンドユーザが表示できる以下のような InfoObject が含まれます。 • レポートドキュメント • プログラム • ショートカット • フォルダ • カテゴリ • 受信ボックス
アプリケーションオブジェクトテーブル	ドキュメントで使用される以下のような InfoObject が含まれます。 • ユニバース • 接続 • オーバーロード
システムオブジェクトテーブル	BI プラットフォームが機能するために使用する以下のような InfoObject が含まれます。 • ユーザ • グループ • ライセンスキー

21.1.3 InfoObject について

InfoObject メタデータをクエリする前に、以下の概念について明確に理解しておく必要があります。

- InfoObject プロパティ
- InfoObject 間の関係

CMS リポジトリでの InfoObject の編成方法を理解したら、簡単にリポジトリを参照したり、CMS リポジトリ関連の問題を修正したりできるようになります。

関連情報

InfoObject プロパティ [804 ページ]
InfoObject 間の関係 [804 ページ]

21.1.3.1 InfoObject プロパティ

以下の表に、InfoObject の最も重要なプロパティとその説明を示します。

InfoObject プロパティ

InfoObject プロパティ	説明
SI_NAME	オブジェクトの名前
SI_KIND	オブジェクトの種類
SI_OWNER	所有者のユーザ名
SI_OWNERID	所有者のユーザ ID
SI_CHILDREN	子の名前
SI_CUID	CUID は InfoObject を一意に識別する Cluster Unique Identifier
SI_UNIVERSE	ドキュメントによって使用されるユニバース (UNV)

21.1.3.2 InfoObject 間の関係

InfoObjecgt は 3 つの階層に編成されます。

- フォルダ階層
- ユーザ/ユーザグループ階層
- サーバ/サーバグループ階層

CMS およびクライアントアプリケーションでは、フォルダ階層を使用して InfoObject 内をナビゲートします。

InfoObject 間の関係の詳細については、関連トピックを参照してください。

関連情報

フォルダ階層 [805 ページ]
ルートフォルダ [805 ページ]

21.1.3.2.1 フォルダ階層

フォルダ階層は InfoObject の親から作成されるフラットリストです。すべての InfoObject には、プロパティ SI_PARENTID で定義されている親が 1 つ必要です。

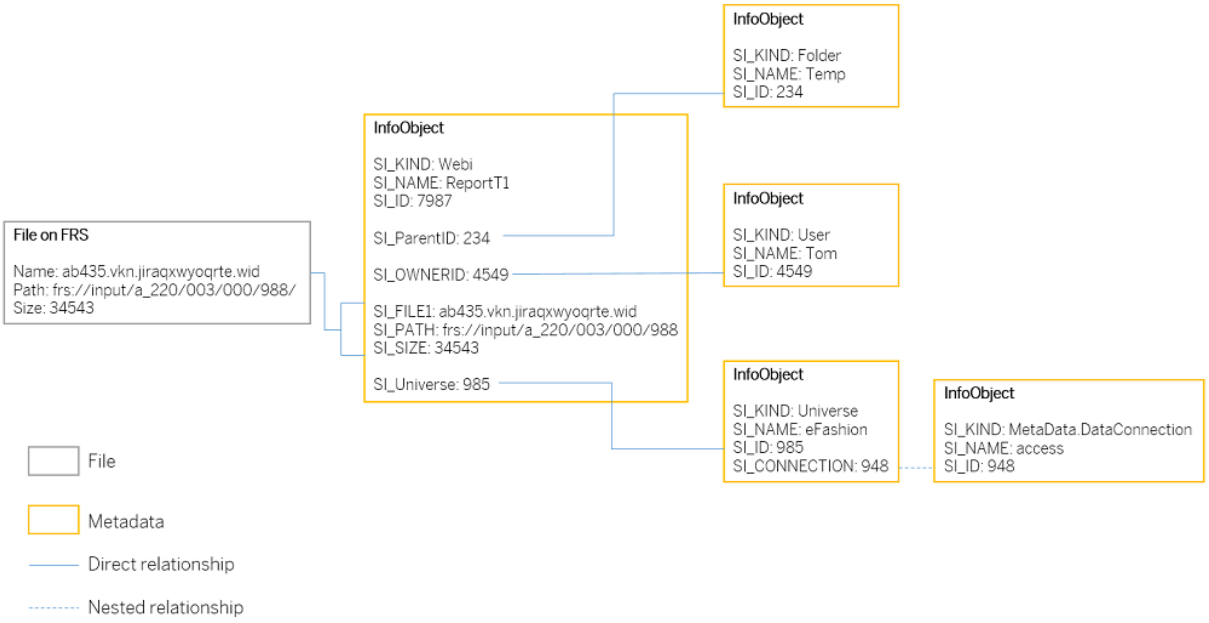
CMS は親 ID のプロパティを使用して、フォルダ階層 (仮想) を作成します。実際には、階層はリポジトリでの InfoObject の格納方法には対応していません。

21.1.3.2.2 ルートフォルダ

CMS リポジトリ階層の最上位フォルダは CMS クラスタフォルダです。ルートフォルダは、CMS クラスタフォルダの下のレベルにあります。ルートフォルダは仮想であり、ファイルシステムに対応するものはありません。

InfoObject は、CMS およびクライアントアプリケーションで簡単に見つけられるように、ルートフォルダに編成されています。たとえば、クライアントアプリケーションは、最初に InfoObject のルートフォルダ、次に親 ID プロパティと子 ID プロパティを使用することによって、InfoObject のコレクション内をナビゲートできます。同じ種類の InfoObject は通常、同じルートフォルダの下で見つけることができます。

以下の図を使用して、InfoObject 間の関係を理解できます。



上で見たように、InfoObject の構造により、InfoObject は無限数の関係とネストされた関係を持つことができます。

21.2 CMS レポーティングの概要

管理者は、Business Intelligence プラットフォームの使用法について理解し、これを最適化する必要があります。CMS レポーティングサンプルキットには CMS データベースドライバが含まれており、これを使用して CMS デー

タベースのメタデータオブジェクトを表示およびレポートすることができます。現在、ユニバースおよびネイティブのレポーティングクライアントを使用して、CMS リポジトリデータベースのメタデータオブジェクトをクエリすることができます。これらのメタデータオブジェクトには、以下のような Business Intelligence プラットフォーム情報が含まれます。

- 接続
- ドキュメント
- スケジュール
- ユニバース
- ユーザ

事前定義済みオブジェクトを含む CMS レポーティングサンプルをインポートして、以下の SAP BusinessObjects データ分析およびレポーティングアプリケーションを使用したレポートとダッシュボードの作成に役立てることができます。

- SAP BusinessObjects Web Intelligence
- SAP Crystal Reports for Enterprise

CMS のレポーティングをすばやく簡単に開始するために、CMS レポーティングサンプルキットを使用することができます。CMS レポート作成の主な段階を以下に示します。

- CMS レポーティングサンプルのインポート: CMC のプロモーションマネジメントを使用して、CMS レポーティングサンプルをインポートします。
- CMS レポートの作成: SAP BusinessObjects Web Intelligence では、CMS サンプルユニバースをデータソースとして使用して CMS レポートを作成することができます。

完全な手順については、作成プロセスのより詳細な概要を示す関連情報を参照してください。

関連情報

CMS レポーティングサンプルキット
CMS レポートの作成
プロモーションマネジメントを使用した CMS レポーティングサンプルキットのインポート [808 ページ]

21.3 CMS データベース接続

CMS データベースドライバを使用して、CMS データベースへのセキュア接続を作成します。CMS レポーティングサンプルにあるデフォルト接続を使用するか、または独自の CMS データベース接続を作成することができます。

CMS データベース接続では、リレーショナル接続を使用する必要があります。以下の表に、リレーショナル接続のパラメータを示します。

リレーショナル接続のパラメータ

パラメータ	説明
認証モード	データソースにアクセスするときに、ユーザの次のログイン認証情報の認証に使用する方法。 • 指定されたユーザ名、パスワード、およびシステム *ID* を使用する: 接続用に定義された [ユーザ名] および [パスワード] パラメータを使用します。オンプレミスシステムまたは遠方のシステムからデータソースにアクセスすることができます。 ⓘ 注記 ユーザにこのセッションのコンテンツを表示する権限があることを確認します。 • セッショントークンの使用: 現在のユーザセッションを使用します。表示および操作が許可されているコンテンツのみ表示することができます。オンプレミスシステムからのみデータソースにアクセスすることができます。 ⓘ 注記 セキュリティの点から、この認証モードをお勧めします。
システム *ID*	[認証モード] が [指定されたユーザ名とパスワードを使用する] の場合、アプリケーションにアクセスするパスワード。
ユーザ名	[認証モード] が [指定されたユーザ名とパスワードを使用する] の場合、データソースにアクセスするユーザ名。
パスワード	[認証モード] が [指定されたユーザ名とパスワードを使用する] の場合、データソースにアクセスするパスワード。

21.4 CMS レポーティングサンプルキット

CMS レポーティングのドキュメントの作成を開始するには、CMS レポーティングサンプルキットを使用する必要があります。Business Intelligence プラットフォームには CMS データベースドライバが組み込まれており、CMS レポーティングサンプルは以下の場所で見つけることができます。

```
<INSTALLDIR>¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥Samples¥BI
on BI.
```

このサンプルには以下が含まれています。

- 接続 (BI platform CMS system database.cns)
- ユニバース (BI platform CMS system database.unx)
- Web Intelligence のサンプル

CMS レポーティングの詳細については、SAP Community Network を参照してください。

関連情報

プロモーションマネジメントを使用した CMS レポーティングサンプルキットのインポート [808 ページ]

21.4.1 プロモーションマネジメントを使用した CMS レポーティングサンプルキットのインポート

開始する前に、以下の場所にある CMS レポーティングサンプルにアクセスできることを確認します。

```
<INSTALLDIR>¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥Samples¥BI
on BI
```

セントラル管理コンソール (CMC) のプロモーションマネジメントツールを使用して、CMS レポーティングサンプルをインポートします。

1. セントラル管理コンソールで、[プロモーションマネジメント] をクリックします。
2. インポート > ファイルのインポート をクリックします。
3. [ファイルシステム] を選択します。
4. [ファイルの選択] をクリックし、サンプルを選択します。
5. [新しいジョブ] ペインで、[出力先] フィールドの [新しい *CMS* へのログイン] を選択します。
6. ログインパラメータを入力し、ログイン > 作成 をクリックします。
7. [昇格ジョブ] ペインでサンプルを右クリックし、[昇格] を選択します。
8. [昇格] ダイアログボックスで [昇格] をクリックします。

CMS レポーティングサンプルの [昇格のステータス] が [成功] の場合は、Business Intelligence 4.2 システムに正常にサンプルがインポートされています。CMS レポーティングのサンプルユニバースを使用するには、関連トピックを参照してください。

関連情報

CMS レポーティングサンプルキット [807 ページ]

21.4.2 CMS サンプルユニバース

CMS サンプルユニバースには、一般的なレポーティングシナリオをサポートする事前定義済みのユニバースが含まれます。分析およびレポーティングのニーズに応じて、事前定義済みのユニバースを編集および拡張することができます。また、[クエリ] ペインで事前定義済みクエリの一覧を参照することもできます。これらのクエリは、ユニバース機能のチュートリアルとして役立ちます。

以下の表に、最も有用なクエリとその内容を示します。

CMS ユニバースで実行する有用なクエリ

クエリ	説明
Sample-User-Relationship-Detail	ユーザが属するグループを参照することができます。
Sample-FolderPath (Universe)	ユニバースの場所を確認することができます。
Sample-ScheduleInfo-Relationships	ユーザによってスケジュールされているアクションを表示することができます。
Sample-QT-Properties with Filter (Server)	InfoObject のプロパティを表示することができます。

21.4.3 CMS サンプルユニバースの拡張

リンクされたユニバースを作成して、CMS サンプルユニバースを拡張することができます。リンクされたユニバースとは、CMS で指定されたコアユニバースにリンクされている .UNX ユニバースです。

このような場合、CMS サンプルユニバースは、リンクされたユニバースで CMS サンプルユニバースのデータファンデーションおよびビジネスレイヤを既成の構成要素として使用できるように、コアユニバースとして機能します。リンクされたユニバースを作成すると、CMS サンプルユニバースから継承したデータファンデーションとビジネスレイヤを、CMS サンプルユニバースに依存しないライフサイクルを持つ新しいファイルとして保存することができます。

CMS サンプルユニバースの CMS データベース接続または CMS データベースと互換性がある別の接続を使用することができます。

テーブルの追加、コアデータファンデーションテーブルを新しいテーブルにリンクする結合の作成、および他のユニバースと同じ方法でのビジネスレイヤへの新しいコンポーネントの追加を行うことができます。コアコンポーネントに加えられた変更は、リンクされたユニバースが CMS にチェックインされるときに、リンクされたユニバースに自動的に反映されます。

21.5 CMS レポートの作成

SAP BusinessObjects Web Intelligence では、CMS サンプルユニバースをデータソースとして使用して CMS レポートを作成することができます。

1. Web Intelligence を開き、[ファイル] ツールバーの [新規作成] アイコンをクリックします。
2. CMS サンプルユニバースを選択します。

   Web Intelligence リッチクライアントを使用している場合は、[選択] をクリックします。

   [クエリパネル] が開きます。
3. クエリに含めるディメンションとメジャーを選択して、[結果オブジェクト] ペインにドラッグします。
4. クエリフィルタを定義するオブジェクトを選択し、[クエリフィルタ] ペインにドラッグします。オブジェクトのクイックフィルタを作成するには、[結果オブジェクト] ペインでオブジェクトを選択し、[結果オブジェクト] ツールバーの [クイックフィルタの追加] アイコンをクリックします。

5. [クエリの実行] をクリックします。

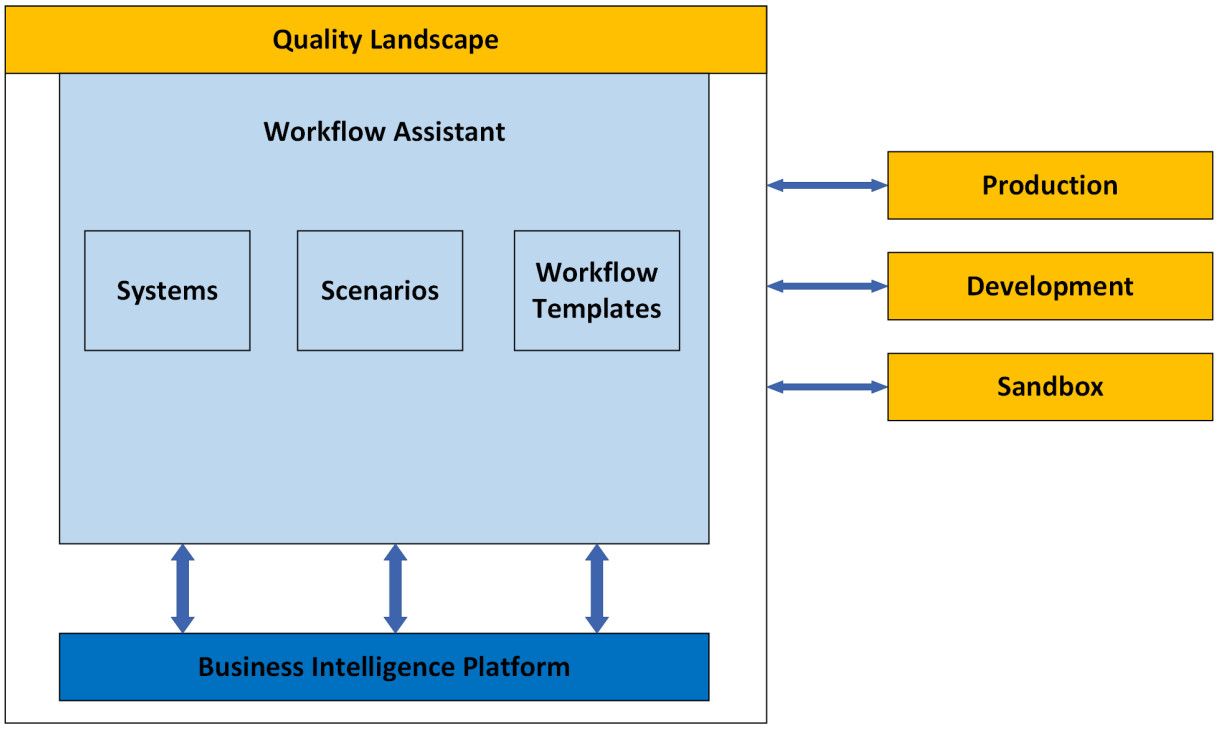
22 ワークフローアシスタント

Automation Framework およびエージェントサービスは、ワークフローアシスタントサービスと呼ばれる 1 つのサービスに結合されました。ワークフローアシスタントは、BI システムの管理および BI タスクの自動化のためのセントラル管理コンソール (CMC) のアプリケーションです。

> **注記**
>
> BI 管理コンソールの Automation Framework 機能は、ワークフローアシスタントによって実現されるようになりました。BI 管理コンソールの URL (`http://<systemName>:<portNo>/BOE/BIAdminConsole`) およびメッセージキューサービスは使用停止になりました。

ワークフローアシスタントでは、コンテンツがタブ ([シナリオ]、[ワークフローテンプレート]、および [システム]) として表示されます。これらのタブから関連セクションにドリルダウンして、詳細情報と機能を確認できます。

ワークフローアシスタントにはロールベースのコンセプトが実装されているため、ユーザは許可されているタブにのみアクセスできます。



システムについて

システムとは、アクセスが許可されている 1 つ以上の BI マシンを指します。システム管理は、使用する BI ランドスケープを集中してアクセスおよび管理できるようにするアプリケーションです。ワークフローアシスタントの

機能を使用するには、まずシステム管理アプリケーションを使用して BI ランドスケープを登録する必要があります。

ワークフローアシスタントについて

ワークフローアシスタントでは、複雑で繰り返される BI タスクを簡素化する機能が提供されます。

> **例**
>
> 以下の BI タスクを順番に実行する必要があるとします。
>
> 1. BI プラットフォームにログインします。
> 2. 特定の Web Intelligence ドキュメントのソースを .unv から .unx に変更します。
> 3. これらの Web Intelligence ドキュメントを最新表示します。
> 4. BI プラットフォームからログアウトします。

ワークフローアシスタントによって手動による作業が削減されます。タスクテンプレートとワークフローテンプレートを使用してシナリオを作成し、このシナリオを保存して、実行し、結果を表示することができます。

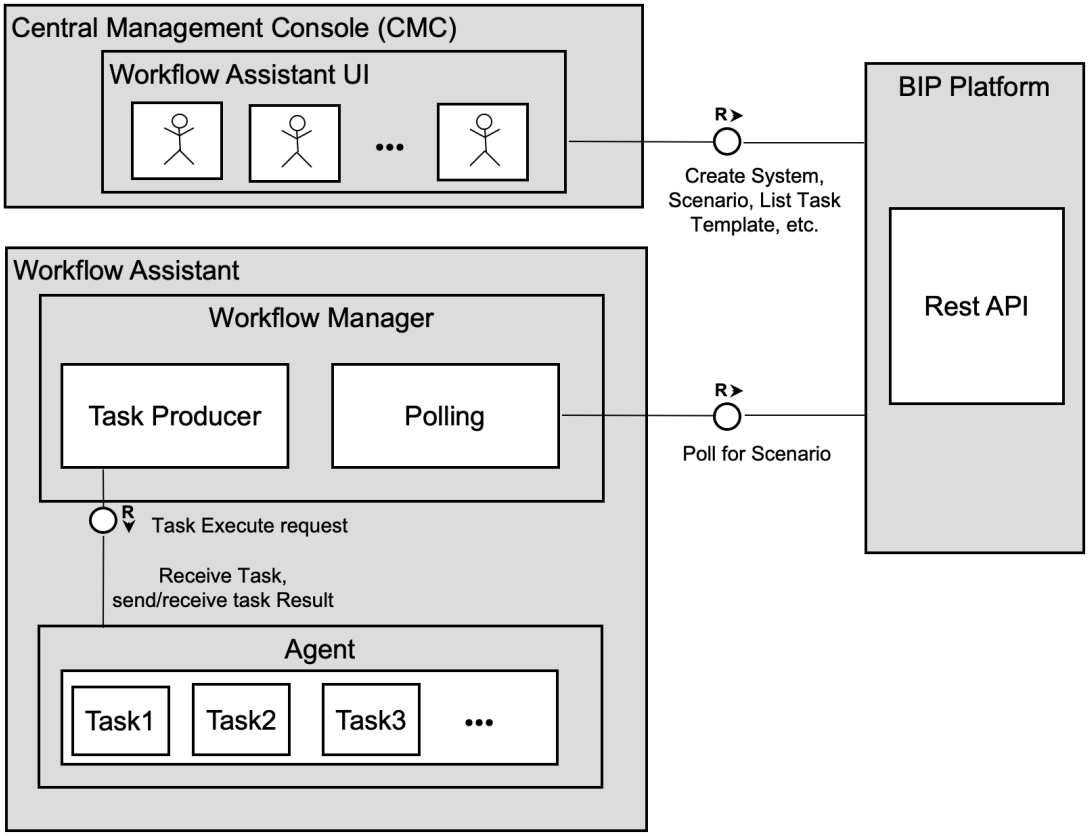
22.1 対象読者

このガイドは、Business Intelligence (BI) プラットフォームの特定のユーザおよび特定の BI プラットフォーム開発者を対象としています。

- このガイドを使用する BI プラットフォームユーザには、セントラル管理コンソール (CMC) およびワークフローアシスタントにアクセスする権限が必要です。これらのユーザには、管理者または委任管理者のロールがあります。
- このガイドを使用する BI プラットフォーム開発者は、Java SDK での作業に精通し、Task Template SDK を使用してカスタム要件の JSON スキーマを作成できる必要があります。

22.2 アーキテクチャの理解

下の図は、ワークフローアシスタントのアーキテクチャとそのコンポーネント間の相互接続を理解するために役立ちます。



上の図で使用されている用語の用語集:

用語	定義
ワークフローアシスタント UI	任意のシステムで実行できるワークフローテンプレートおよびシナリオを作成する UI。
ワークフローマネージャ	ワークフローマネージャは、プラットフォームからシナリオをポーリングし、シナリオの実行を管理し、結果を保存します。
エージェント	シナリオ内でタスクを実行する軽量プロセスです。

22.3 用語集

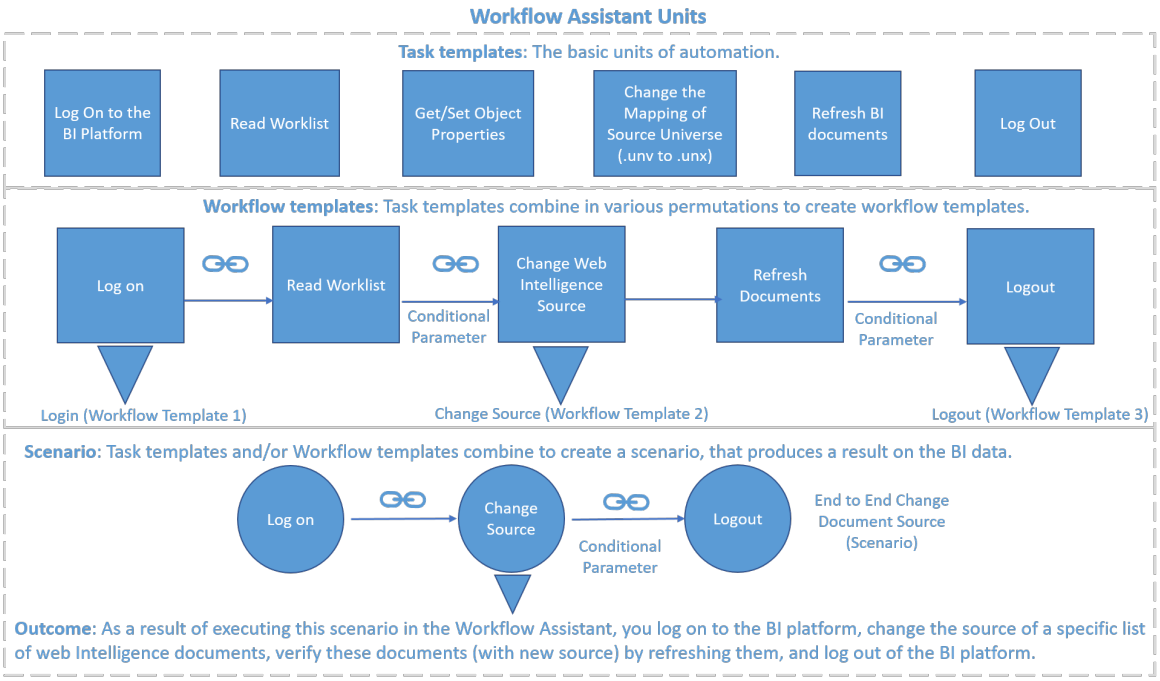
ワークフローアシスタントには、独自の専門用語があります。

ワークフローアシスタントで頻繁に使用される用語

用語	定義
標準タスクテンプレート	アプリケーションでデフォルトで提供される自動化の基本単位。これらの単位は、シナリオまたはワークフローテンプレートで使用できます。 たとえば、BI プラットフォームへのログオン、BI ドキュメントの最新表示、データの読み取り、Web Intelligence ドキュメントのソースユニバースのマッピングの変更 (unv から unx へ)、ランドスケープへのユーザの追加、ログアウトなどの単純なタスクです。
カスタムタスクテンプレート	開発者がカスタム要件に合わせて作成するタスクテンプレート (自動化の基本単位)。 **制限** ワークフローアシスタントの UI を使用してカスタムタスクテンプレートを作成することはできません。Task Template SDK が必要です。
ワークフローテンプレート	ワークフローの結果を達成するために、必要な順序で並べられたタスクテンプレートの論理グループ。
標準ワークフローテンプレート	ワークフローアシスタントですぐに使用できるワークフローテンプレート。管理者は、さまざまな BI 自動化要件のシナリオを作成するときに、標準ワークフローテンプレートをすぐに使用できます。
カスタムワークフローテンプレート	管理者がカスタム要件に合わせて作成するワークフローテンプレート。標準またはカスタムのタスクテンプレートをグループ化することによって、ワークフローアシスタントで作成されます。
シナリオ	必要な順序でタスクテンプレートまたはワークフローテンプレートを使用して作成された実行可能エンティティ。

用語	定義
条件パラメータ	制御フローを指示するタスクテンプレートまたはワークフローテンプレート間の接続リンクは、以下のいずれかの条件に基づきます。 • 続行 (デフォルト) • 成功時 • 失敗時 • 一部成功時 **注記** 条件パラメータを使用すると、[時間遅延] (秒) を挿入して、前のタスク実行が完了した後、特定の経過時間の後にのみ、シナリオの次のタスクが開始されるようにすることもます。 **注意** ワークフローアシスタントでは、条件パラメータ値 [続行] は、前のタスクが [成功]、[一部成功]、または [失敗] の 3 つのステータスのいずれかで完了した場合にのみ考慮されます。前のタスクのステータスが [エラー] または [未実行] である場合、次のノードのステータスは自動的に [未実行] に設定されます。

以下の図は、上記の用語間の相互関係を理解するために役立ちます。



22.4 インストールおよび更新について

新しいインストールを行うか、既存のインストールを更新するかに応じて、バックエンド機能へのアクセスが異なることがあります。

SAP BusinessObjects BI プラットフォーム (デフォルトインストール) の新しいインストールを行うと、BI プラットフォームをインストールおよび設定したマシン上で、ワークフローアシスタントへのフルアクセス権を取得できます。これには、CMC のワークフローアシスタントアプリケーションおよびバックエンド機能 (ワークフローアシスタントサービス) へのアクセスが含まれます。

ただし、BI プラットフォーム SP5 以降から 4.3 に更新すると、ワークフローアシスタントの完全な機能を使用できるようになりますが、「制限事項」で示した SAP ノートを確認する必要があります。更新のインストール後、"変更" インストールワークフローを実行してバックエンドサービスを取得してください。変更インストールの詳細については、Help Portal の SAP Business Intelligence プラットフォームページに提供されているサポートパッケージアップデートガイドを参照してください。

> **注記**
>
> ワークフローアシスタントは、BOE.war ファイルの一部です。BI プラットフォーム 4.2 SP4 以前から 4.2 SP5 以降のバージョンに更新した後、既存のバージョンのインストール時に *Java Web アプリケーション*機能が選択されていた場合にのみ Web アプリケーションがデプロイされます。

> **警告**
>
> ワークフローアシスタントのクラスタリングはサポートされていないため、システム内の複数のマシンにワークフローアシスタントをインストールすることはできません。

ワークフローアシスタントでは、AIX および Solaris オペレーティングシステムがサポートされるようになりました。

> **制限**
>
> - AIX および Solaris プラットフォームの場合、4.2 SP05 以降のバージョンに BI 4.3 バージョンをインストールすると、デフォルトでワークフローアシスタントがインストールされます。ただし、バックエンドサービスを取得するには、修復が必要です。
> - BI プラットフォーム 4.2 SP4 以前から 4.2 SP5 以降に更新すると、一部のフォルダがワークフローアシスタントに表示されません。詳細については、2882649 を参照してください。

22.5 ワークフローアシスタントの設定

BI プラットフォームのインストールの一部としてワークフローアシスタントをインストールすると、セットアップ時にデフォルトでサービスを取得します。

その後、信頼できる認証を設定して、ワークフローアシスタントの使用を開始できます。

22.5.1 基本設定

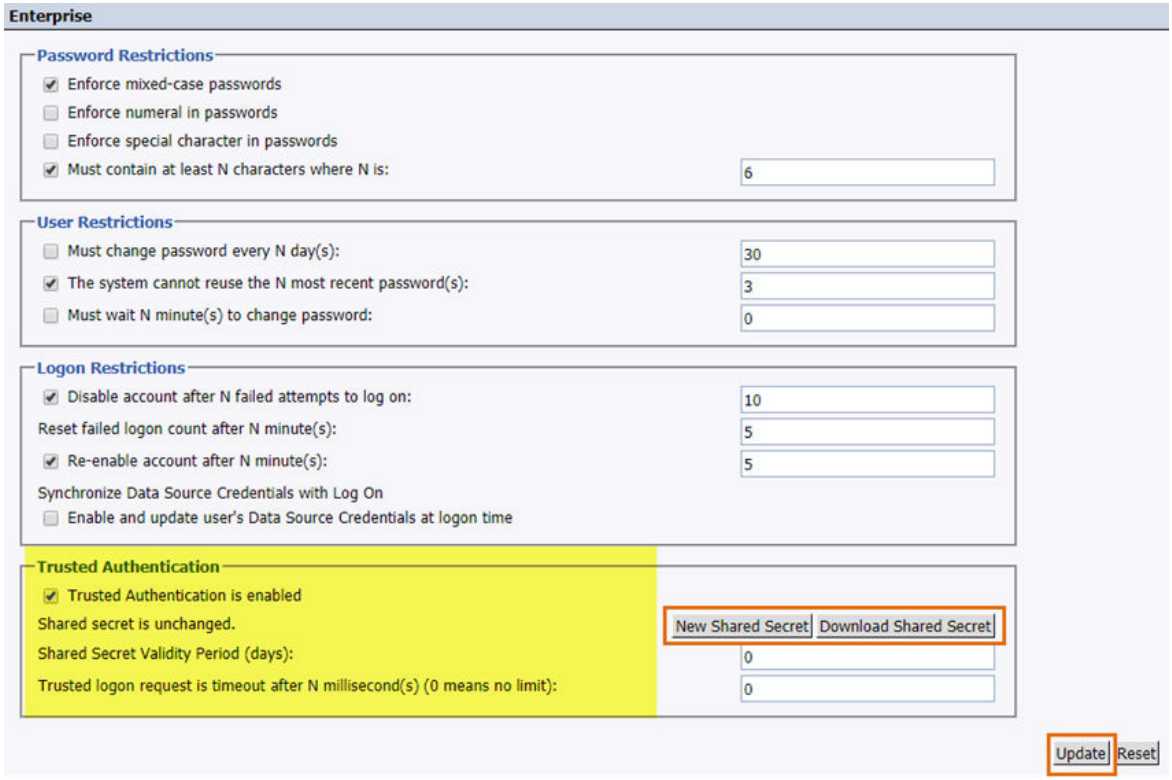
22.5.1.1 ワークフローアシスタントの Enterprise 認証の設定

セットアップで BI プラットフォームインストールの一部としてワークフローアシスタントがインストールされていること。

ワークフローアシスタントの信頼できる (Enterprise) 認証を設定するには、以下の手順に従います。

1. マスタノードの CMS に接続して、セントラル管理コンソール (CMC) にログオンします。
2. ドロップダウンで [認証] を選択し、[*Enterprise*] をダブルクリックします。

   [Enterprise] ダイアログが以下のように表示されます。



3. [信頼できる認証] セクションで、[信頼できる認証] が有効になっていることを確認します。
4. [新規共有シークレット] を選択します。
   共有シークレットキーが生成されます。
5. [共有シークレットのダウンロード] を選択します。
6. [更新] を選択します。
7. 生成された共有シークレットキー (TrustedPrincipal.conf) を以下の場所に保存します。
   a. Windows では、`<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0¥win64_x64/` です。
   b. Linux では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/linux_x64/` です。
   c. AIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/aix_rs6000_64/` です。
   d. Solaris では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/solaris_sparcv9/` です。

> ⓘ 注記
>
> 信頼できる認証証明書を異なるオプションで作成する方法の詳細については、トピック信用できる認証の有効化 [248 ページ]を参照してください。

22.5.1.2 ワークフローアシスタントバックエンドサービスのデフォルトユーザの作成

1. ワークフローアシスタントに **WAUser** という名前で新しいユーザを作成します。
2. `Workflow Assistant` フォルダに移動して **WAUser** アカウントにフルコントロールを付与することで、適切な権限を割り当てます。

   ワークフローアシスタントバックエンドサービスは、**WAUser** アカウントを使用して開始します。

   WAUser アカウントが存在しない場合、ワークフローアシスタントは管理者アカウントを使用して起動します。

   > ⓘ 注記
   >
   > 新しいユーザが管理者ユーザグループに属している必要はありません。

22.5.1.3 ワークフローアシスタントサービスの開始

このトピックでは、ワークフローアシスタントサービスを開始する手順について説明します。

1. ワークフローアシスタントの Enterprise 認証を設定します。詳細については、ワークフローアシスタントの Enterprise 認証の設定 [817 ページ] を参照してください。
2. ワークフローアシスタントサービスを開始するには、以下の手順に従います。
   a. Windows では、セントラル設定マネージャ (CCM) を起動し、ワークフローアシスタントサービスを開始します。
   b. Unix では、`<INSTALLDIR>/AdminConsole/WorkflowAssistant/startWfAssistant.sh` に移動します。

   これで、ワークフローアシスタントを使用してシナリオを実行する準備ができました。

   > ⓘ 注記
   >
   > ワークフローアシスタントが正常に開始されたことを確認するには、`<BOE-Install-Directory>¥AdminConsole¥WorkflowAssistant¥service-logs` で `message.properties` ファイルの内容を確認します。`message.properties` の内容は以下のとおりです。
   >
   > ```
   > STATUS_WFM=success
   >
   > MESSAGE_AGENT=Agent - Started¥!¥!
   >
   > STATUS_AGENT=success
   >
   > MESSAGE_WFM=Workflow Assistant - Started¥!¥!
   > ```

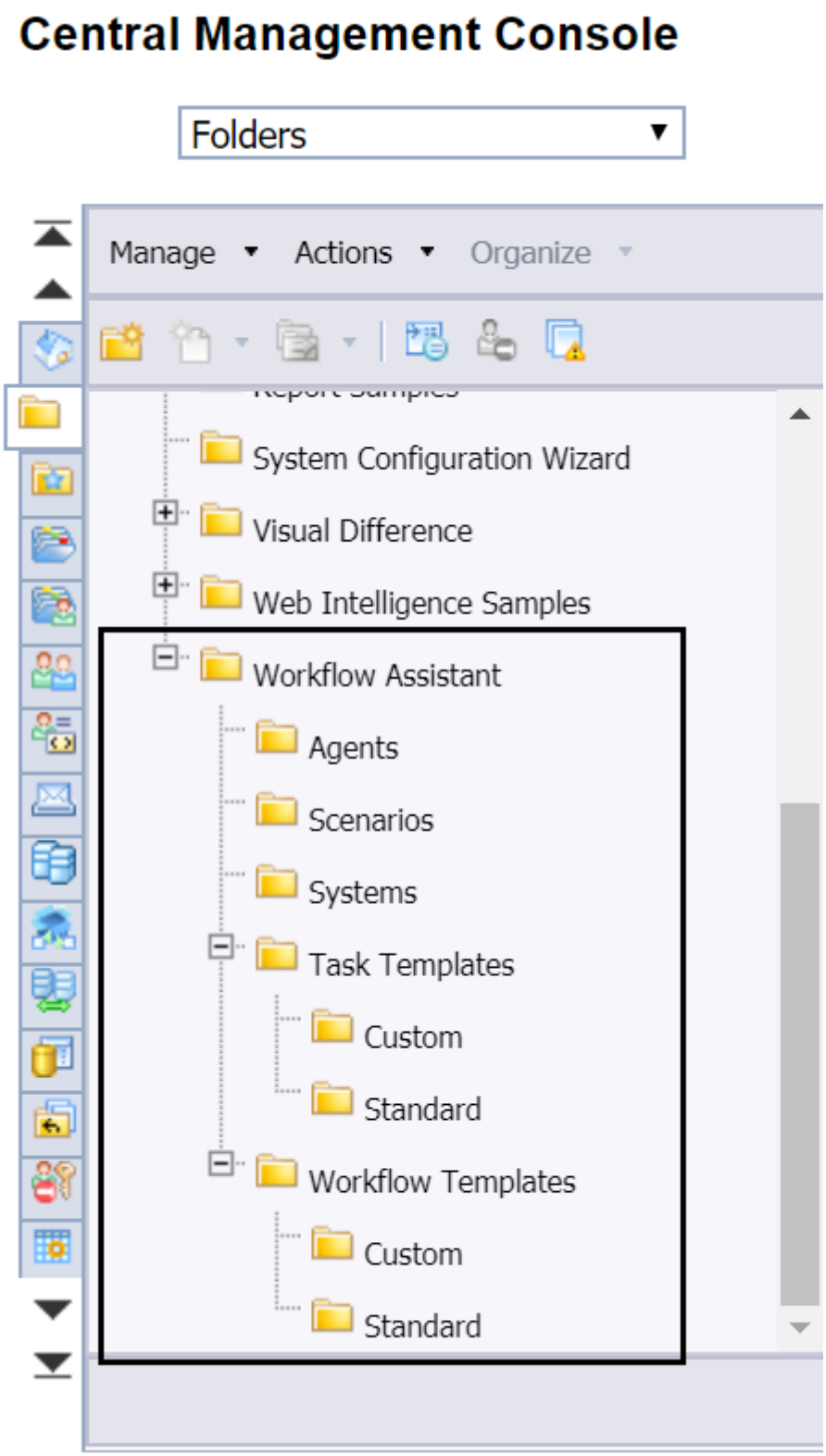
22.6 セントラル管理コンソールでのワークフローアシスタントの権限の管理

セントラル管理コンソールを使用して、ワークフローアシスタントのセキュリティを管理します。

[ワークフローアシスタント] は、[セントラル管理コンソール] の [アプリケーション] に表示されます。

ワークフローアシスタントでは、以下のエンティティのアクセス権と全体的なセキュリティ設定を表示および管理することができます。

- システム
- シナリオ
- タスクテンプレート
- ワークフローテンプレート



CMC でオブジェクトのセキュリティ設定を管理する方法については、トピック CMC でのオブジェクトのセキュリティ設定の管理を参照してください。

ⓘ 注記

- フォルダレベルまたはオブジェクトレベルで権限をユーザに割り当てることで、[システム]、[シナリオ]、[タスクテンプレート]、[ワークフローテンプレート] などのワークフローアシスタントの機能へのアクセスを制御できますが、権限の不足はユーザインタフェースに影響しません。つまり、シナリオを作成するには、*Scenario* フォルダに対する [このフォルダにオブジェクトを追加する] 権限が必要です。
- たとえば、ユーザが CMC の *Scenario* フォルダに対する権限がなくても、ワークフローアシスタントでシナリオを作成するためのオプションが表示されます。ユーザがシナリオを作成して *Scenario* フォルダに保存しようとすると、エラーメッセージが表示されます。

アプリケーションの権限の管理

適切なアプリケーション固有の権限がある場合、ワークフローアシスタントで以下のタスクを拒否または実行することができます。

- [タスクテンプレートの作成] を拒否するには、Task Template フォルダに移動し、[オブジェクトをフォルダに追加する] を拒否します。
- [ワークフローテンプレートの作成] を拒否するには、Workflow Template フォルダに移動し、[オブジェクトをフォルダに追加する] を拒否します。
- [シナリオの作成] を拒否するには、Scenario フォルダに移動し、[オブジェクトをフォルダに追加する] を拒否します。
- [タスクテンプレートの編集] を拒否するには、Task Template フォルダに移動し、[オブジェクトを編集する] を拒否します。
- [ユーザが所有するタスクテンプレートの編集] を拒否するには、Task Template フォルダに移動し、[ユーザが所有するオブジェクトを編集する] を拒否します。
- [ワークフローテンプレートの編集] を拒否するには、Workflow Template フォルダに移動し、[オブジェクトを編集する] を拒否します。
- [ユーザが所有するワークフローテンプレートの編集] を拒否するには、Workflow Template フォルダに移動し、[ユーザが所有するオブジェクトを編集する] を拒否します。
- [シナリオの編集] を拒否するには、Scenario フォルダに移動し、[オブジェクトを編集する] を拒否します。
- [ユーザが所有するシナリオの編集] を拒否するには、Scenario フォルダに移動し、[ユーザが所有するオブジェクトを編集する] を拒否します。
- [タスクテンプレートの表示] を拒否するには、Task Template フォルダに移動し、[オブジェクトを表示する] を拒否します。
- [ユーザが所有するタスクテンプレートの表示] を拒否するには、Task Template フォルダに移動し、[ユーザが所有するオブジェクトを表示する] を拒否します。
- [ワークフローテンプレートの表示] を拒否するには、Workflow Template フォルダに移動し、[オブジェクトを表示する] を拒否します。
- [ユーザが所有するワークフローテンプレートの表示] を拒否するには、Workflow Template フォルダに移動し、[ユーザが所有するオブジェクトを表示する] を拒否します。
- [シナリオの表示] を拒否するには、Scenario フォルダに移動し、[オブジェクトを表示する] を拒否します。
- [ユーザが所有するシナリオの表示] を拒否するには、Scenario フォルダに移動し、[ユーザが所有するオブジェクトを表示する] を拒否します。
- [タスクテンプレートの削除] を拒否するには、Task Template フォルダに移動し、[オブジェクトを削除する] を拒否します。

- [ユーザが所有するタスクテンプレートの削除] を拒否するには、Task Template フォルダに移動し、[ユーザが所有するオブジェクトを削除する] を拒否します。
- [ワークフローテンプレートの削除] を拒否するには、Workflow Template フォルダに移動し、[オブジェクトを削除する] を拒否します。
- [ユーザが所有するワークフローテンプレートの削除] を拒否するには、Workflow Template フォルダに移動し、[ユーザが所有するオブジェクトを削除する] を拒否します。
- [シナリオの削除] を拒否するには、Scenario フォルダに移動し、[オブジェクトを削除する] を拒否します。
- [ユーザが所有するシナリオの削除] を拒否するには、Scenario フォルダに移動し、[ユーザが所有するオブジェクトを削除する] を拒否します。
- [すべての組み合わせでシナリオを実行] を拒否するには、特定のシナリオに移動し、[オブジェクトをフォルダに追加する] を拒否します。
- [すべての組み合わせでユーザが所有するシナリオを実行] を拒否するには、特定のシナリオに移動し、[オブジェクトをユーザが所有するフォルダに追加する] を拒否します。
- [ランドスケープの作成] を拒否するには、Landscape フォルダに移動し、[オブジェクトをフォルダに追加する] を拒否します。
- [ランドスケープの編集および表示] を拒否するには、Landscape フォルダに移動し、[オブジェクトを編集する] および [オブジェクト表示する] を拒否します。
- [ランドスケープの削除] を拒否するには、Landscape フォルダに移動し、[オブジェクトを削除する] を拒否します。
- [ランドスケープでのユーザ認証情報の追加] を拒否するには、Landscape フォルダに移動し、[オブジェクトをフォルダに追加する] を拒否します。

> **注記**
>
> 上記の権限はすべて、個々のタスクテンプレート、ワークフローテンプレート、シナリオに適用することができます。

22.7 ワークフローアシスタントの使用

ワークフローアシスタントは、繰り返される複雑な BI 管理タスクを自動化することができる、CMC のアプリケーションです。以下の節では、BI 管理タスクを自動化する方法を学習します。

22.7.1 標準タスクテンプレートについて

標準タスクテンプレートは、ワークフローアシスタントに組み込まれています (事前設定済み)。シナリオまたはワークフローテンプレートの作成時に、これらのタスクテンプレートを使用することができます。

標準タスクテンプレート	説明
ログオン	ターゲット BI プラットフォームサーバとのセッションを確立します。

標準タスクテンプレート	説明
ドキュメントの最新表示	<今すぐスケジュールする>操作を使用し、提供されたドキュメントのリストを開いて最新表示します。 **注記** プロンプトを含むドキュメントの場合、実行する前にドキュメントにデフォルト値を指定する必要があります。
Web Intelligence ソースの変更	ドキュメント一覧のソースユニバースのマッピングを、.unv から .unx、.unx から .unx、または .unv から .bex に変更します。
ユーザおよびユーザグループの追加/削除	ユーザおよびユーザグループを BI ランドスケープに追加または削除します。 **注記** このタスクテンプレートは、BI プラットフォームの<インポート機能>に対応します。インポート機能の詳細については、トピックユーザまたはユーザグループを一括して追加するを参照してください。
プロパティの取得	クエリが実行された InfoObject の特定のプロパティの値を返します。
プロパティの設定	CMS の特定の InfoObject の特定のプロパティの値を設定します。
ワークリストの読み取り	.CSV ファイルを入力として読み取り、後続のタスクで使用できるカンマ区切り値を返します。このタスクテンプレートは、多数の値 (バルクデータ) をシナリオのワークフローテンプレートで使用する必要があり、ワークフローアシスタントの入力パネルを使用して手動で値を入力できない場合に使用します。
クエリワークリスト	CMS テーブルに対してクエリを実行して、CSV 形式で出力します。
出力の保存	タスクの [出力パラメータ] から取得された値を CMS で CSV ファイルに保存します。
サーバプロパティの設定	特定のサーバの特定のプロパティの値を設定します。
ログアウト	ターゲット BI プラットフォームサーバとのタスクセッションを終了します。

22.7.1.1 ログオン

ログオンタスクテンプレートのパラメータ

入力パラメータ

名前	タイプ	説明
システム	文字列	ワークフローアシスタントに登録されたランドスケープの名前

22.7.1.2 ドキュメントの最新表示

ドキュメントの最新表示のパラメータ

入力パラメータ

名前	タイプ	説明
*ドキュメント	CSV	最新表示する必要があるドキュメントのドキュメント ID (id/cuid)。ユーザは、入力ヘルプを介してリポジトリエクスプローラからドキュメントを選択することもできます。 CSV 形式: id または cuid

出力パラメータ

名前	タイプ	説明
SuccessfullyRefreshedDocuments	CSV	正常に最新表示されたドキュメント。 CSV 形式: id, cuid
UnsuccessfullyRefreshedDocuments	CSV	正常に最新表示されなかったドキュメント。 CSV 形式: id, cuid
すべて	CSV	処理されたドキュメントの一覧。 CSV 形式: id, cuid

22.7.1.3 Web Intelligence ソースの変更

Web Intelligence ソースの変更のパラメータ

入力パラメータ

名前	タイプ	説明
*ドキュメント	CSV	UNV を UNX、UNX を UNX、または UNV を BEx に置き換える Web Intelligence ドキュメントの CUID を指定します。ユーザは、入力ヘルプを介してリポジトリエクスプローラからドキュメントを選択することも、別のタスクへの出力をマッピングすることもできます。 CSV 形式: id または cuid
*ユニバースマッピング	CSV	ID または CUID に基づいてユニバース (UNV、UNX、BEx) をマッピングします。ユーザは、入力ヘルプの [ユニバースマッピング] 画面でユニバースをマッピングすることもできます。 CSV 形式 (UNV-UNX の場合): unv_cuid, unx_cuid または unv_id, unx_id CSV 形式 (UNX-UNX の場合): src_cuid,dest_cuid,type CSV 形式 (UNV-BEx の場合): src_cuid,dest_cuid,type,technical_name
ドキュメントアクション	文字列	ドキュメントを保存せずにソースを変更するには、次の値を割り当てます。'Test' ソースを変更してドキュメントを保存するには、次の値を割り当てます。'Change'

出力パラメータ

名前	タイプ	説明
成功	CSV	ソースが正常に変更された文書。 CSV 形式: id, cuid

名前	タイプ	説明
失敗	CSV	ソースを変更できなかった文書。 CSV 形式: id, cuid
すべて	CSV	入力ドキュメントの一覧。 CSV 形式: id, cuid

⚠ 制限

- .BEx クエリに基づいて作成された .UNV のみを別の .BEx クエリに置き換えることができます。
- プロンプトを含む BEx クエリはサポートされていません。
- マッピングは、ユニバースオブジェクトが BEx クエリオブジェクトと類似のタイプおよび最も近い名前を持つ場合にのみ行われます。
- ラベルで作成されたユニバースオブジェクトはマッピングされません。

22.7.1.4 ユーザおよびユーザグループの追加/削除

ユーザおよびユーザグループの追加/削除のパラメータ

入力パラメータ

名前	タイプ	説明

*データ	CSV	ユーザ固有の情報。
		以下のサンプル CSV データを参照してください。CSV データの詳細については、*Business Intelligence* プラットフォーム管理者ガイドのトピックユーザまたはユーザグループを一括して追加するを参照してください。
		`command,group,user,full-name,password,mail,profileName,profileValue`
		`Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue`

ⓘ 注記

CSV ヘッダなしで CSV ファイルを作成し、シナリオへの入力として使用することもできます。

CSV ファイルで選択されるパスワードは、パスワードポリシーに準拠している必要があります。

→ ヒント

連続するカンマを使用して、入力フィールドをスキップできます。

22.7.1.5 プロパティの取得

プロパティの取得のパラメータ

入力パラメータ

名前	タイプ	説明
*InfoObject	CSV	InfoObject の CSV 値。プロパティを使用するために接頭辞 'si_' は指定できません。 CSV 形式: id または cuid
*プロパティ	CSV	プロパティの CSV 値。プロパティを使用するために接頭辞 'si_' は指定できません。 ユーザの InfoObject の場合、サポートされるプロパティは 'property;data' です。

出力パラメータ

名前	タイプ	説明
成功	CSV	プロパティ値が正常に検索または割り当てられた InfoObject の一覧。 CSV 形式: id または <検索されたプロパティ>
失敗	CSV	プロパティ値を正常に検索または割り当てできなかった InfoObject の一覧。 CSV 形式: id, cuid
すべて	CSV	処理されたすべての InfoObject の一覧。 CSV 形式: id, cuid

22.7.1.6 プロパティの設定

プロパティの設定のパラメータ

入力パラメータ

名前	タイプ	説明
*InfoObject	CSV	InfoObject の CSV 値。プロパティを使用するために接頭辞 'si_' は指定できません。 CSV 形式: id または cuid
*プロパティ	CSV	プロパティの CSV 値。 ユーザの InfoObject の場合、サポートされるプロパティは 'property;data' です。

出力パラメータ

名前	タイプ	説明
成功	CSV	プロパティ値が正常にフェッチまたは設定された InfoObject の一覧。 CSV 形式: id または <検索されたプロパティ>
失敗	CSV	プロパティ値を正常にフェッチまたは設定できなかった InfoObject の一覧。 CSV 形式: id, cuid
すべて	CSV	処理されたすべての InfoObject の一覧。 CSV 形式: id, cuid

22.7.1.7 サーバプロパティの設定

サーバプロパティの設定のパラメータ

入力パラメータ

名前	タイプ	説明
*サーバ	CSV	変更する必要があるサーバの ID (id/cuid)。ユーザは、入力ヘルプを介してリポジトリエクスプローラからサーバを選択することもできます。 CSV 形式: id または cuid
*プロパティ	CSV	プロパティと値を含む CSV 値。例: `hostname;new value` サポートされるプロパティ: hostname

出力パラメータ

名前	タイプ	説明
成功	CSV	プロパティ値が正常に設定されたサーバの一覧。 CSV 形式: id
失敗	CSV	プロパティ値を正常に設定できなかったサーバの一覧。 CSV 形式: id
すべて	CSV	処理されたすべてのサーバの一覧。 CSV 形式: id

22.7.1.8 ワークリストの読み取り

ワークリストの読み取りのパラメータ

入力パラメータ

名前	タイプ	説明
*ファイル	CSV	読み取りに必要なデータを含む CSV ファイル。ユーザは、入力ヘルプを介してリポジトリエクスプローラから CSV ファイルを選択することもできます。 CSV 形式: <Header1>, <Header2>, ..<HeaderN> **注記** データ形式および CSV の区切り文字については、CSV データの使用 [838 ページ]を参照してください。

出力パラメータ

名前	タイプ	説明
値	CSV	カンマ区切り形式で返される、入力ファイルから読み取られた値の一覧。

22.7.1.9 出力の保存

出力保存タスクのパラメータ

入力パラメータ

名前	タイプ	説明
パラメータ	CSV	前のタスクから取得された出力をマッピングします。
*ファイル名	文字列	出力を保存するファイル名を指定します。

名前	タイプ	説明
*出力先フォルダの選択	文字列	ファイルを保存する必要があるフォルダを選択します。
*保存オプション	文字列	同じ名前で存在するファイルを上書きするには、値 [上書き] を選択します。 同じ名前で存在するファイル名を接尾辞 _1、_2 などで変更するには、値 [名前の変更] を選択します。

> ⓘ 注記
>
> 出力パラメータ:
>
> 取得された出力は、CMS のファイルです。そのため、使用できるパラメータはありません。

22.7.1.10 ログアウト

ログアウトタスクのパラメータ

入力パラメータ

名前	タイプ	説明
SessionToken	文字列	セッショントークン (ログオンのために生成)

22.7.2 標準ワークフローテンプレートについて

標準ワークフローテンプレートは、ワークフローアシスタントに組み込まれています (事前設定済み)。シナリオの作成時に、これらのワークフローテンプレートを使用することができます。

ワークフローアシスタントで利用可能な標準ワークフローテンプレート

テンプレート名	説明
ログオン	ターゲット BI プラットフォームサーバとのセッションを確立します。
ドキュメントの最新表示	指定された Web Intelligence ドキュメントの一覧を最新表示します。

テンプレート名	説明
ドキュメント所有者の変更	ドキュメントの所有者に対してクエリを実行し、同じ所有者を別のドキュメントに割り当てます。
ユーザライセンスの種類の変更	ユーザ固有の条件に基づいてユーザ一覧に対してクエリを実行し、ライセンスの種類を変更します。
Web Intelligence ソースの変更およびドキュメントの確認	ソースユニバースのマッピングを .unv から .unx、.unx から .unx、または .unv から .bex に変更し、Web Intelligence ドキュメントのドキュメントを一括で検証します。
ユーザの追加/削除	管理者は、ユーザおよびグループを追加または削除できます。
ログアウト	ターゲット BI プラットフォームサーバとのタスクセッションを終了します。

22.7.3 カスタムタスクテンプレートについて

ワークフローアシスタントの標準タスクテンプレートを使用して、ワークフローテンプレートを設計し、シナリオを実行することができます。標準テンプレートがニーズを満たさない場合は、ワークフローアシスタント用の独自のタスクテンプレートおよびプラグインを開発することができます。

開発者が新しいタスクテンプレートを実装するための API を提供するカスタムタスクテンプレート SDK を使用して、独自のカスタムタスクテンプレートを作成します。詳細については、BI Automation Framework でのカスタムタスクテンプレートの作成方法を参照してください。

22.7.4 ワークフローテンプレートの管理

ワークフローアシスタントからカスタムワークフローテンプレートを作成、編集、および削除することができます。

22.7.4.1 カスタムワークフローテンプレートの作成

標準またはカスタムタスクテンプレートを使用して、カスタムワークフローテンプレートを作成します。

1. ホームページで、[ワークフローアシスタント] を選択します。
2. [ワークフローアシスタント] ページで、[ワークフローテンプレート] タブを選択します。
3. [ワークフローテンプレート] の右上にある + ([追加]) アイコンを選択します。
4. [ワークフローテンプレートの作成] キャンバスで、左側のパネルのタスクテンプレートの [標準] および [カスタム] カテゴリの前に表示される > ([展開]) アイコンを選択します。
5. 必要なタスクテンプレートをページの右側にあるキャンバスにドラッグアンドドロップします。

6. キャンバス内でドロップしたタスクテンプレートの名前を変更します。
7. (オプション) 2 つのタスクテンプレートの間に表示される ([リンク]) アイコンを選択し、表示されるリストで条件パラメータに必要な値を選択します。

   ここでは、必要な <時間遅延> (秒単位) を挿入することもできます。
8. (オプション) 入力パラメータの値を設定すると、シナリオでワークフローテンプレートが使用される際にデフォルト値として使用されます。
9. [保存] を選択します。
10. [ワークフローテンプレートの保存] ダイアログで、ワークフローテンプレートの名前 (必須) を入力し、必要に応じて説明を追加します。
11. [ワークフローテンプレートの保存] ダイアログで [保存] を選択します。

    新しいワークフローテンプレートが、ワークフローアシスタントの [ワークフローテンプレート] ビューに表示されます。

    > **注記**
    >
    > 既存のワークフローテンプレートに対する変更は、既存のシナリオには影響しません。

22.7.4.2 カスタムワークフローテンプレートの編集

ワークフローアシスタントでカスタムワークフローテンプレートを編集します。

1. ワークフローアシスタントの [ワークフローテンプレート] タブで、 ([その他]) を選択し、[編集] を選択します。
2. [ワークフローテンプレートの編集] 画面で、タスクテンプレートの追加/削除、入力パラメータ値の変更、またはタスクテンプレート間の条件パラメータの変更を行って、ワークフローテンプレートに必要な編集を行います。
3. [名前を付けて保存] を選択します。
4. [ワークフローテンプレートの保存] ダイアログで、必要に応じてワークフローテンプレートの名前を変更します。
5. [保存] を選択します。

   ワークフローテンプレートの変更が保存され、ワークフローアシスタントのホームページに戻ります。

22.7.4.3 カスタムワークフローテンプレートの削除

ワークフローアシスタントでカスタムワークフローテンプレートを削除します。

1. ワークフローアシスタントの [ワークフローテンプレート] タブで、 ([その他]) を選択し、[削除] を選択します。
2. 表示される警告で、[削除] を選択します。

   削除されたワークフローテンプレートは、ワークフローアシスタントの [ワークフローテンプレート] タブに表示されなくなります。

22.7.5 シナリオの管理および結果の表示

シナリオは、タスクテンプレートおよびワークフローテンプレートを結合することによって作成されます。ワークフローアシスタントでシナリオを管理し、結果を表示します。

22.7.5.1 シナリオの作成

このトピックでは、ワークフローアシスタントでシナリオを作成する方法について説明します。

1. CMC の [ホーム] ページで、[ワークフローアシスタント] を選択します。

   開いたページに使用可能なシナリオが一覧表示されます。
2. + ([フォルダまたはシナリオの作成]) アイコンをクリックし、[シナリオ] を選択します。
3. [シナリオの作成] ページで、左側のパネルのタスクテンプレートの [標準] および [カスタム] カテゴリの前に表示される > ([展開]) アイコンを選択します。

   > **注記**
   >
   > タスクの説明を確認するには、タスクテンプレートの名前にマウスのポインタを合わせます。
4. 必要なワークフローテンプレートをページの右側にあるキャンバスにドラッグアンドドロップします。
5. (オプション) 2 つのタスクテンプレートの間に表示される (リンク]) アイコンを選択し、表示されるリストで条件パラメータに必要な値を選択します。

   ここでは、必要な <時間遅延> (秒単位) を挿入することもできます。
6. キャンバスでワークフローテンプレートをクリックします。

   入力パネルがページの右側に表示されます。
7. 右側の入力パネルで > ([展開]) を選択して、各タスクテンプレートの入力パラメータフィールドを表示し、フィールドで必要な値を選択します。

   > **警告**
   >
   > - テンプレートパラメータに指定する入力値のいずれにも個人データが含まれておらず、一般データ保護規則 (GDPR) ガイドラインに準拠していることを確認します。GDPR の詳細については、トピック データの保護とプライバシー [170 ページ] を参照してください。

   > **注記**
   >
   > パラメータ情報を参照することで、パラメータに関する詳細情報を取得できます。パラメータ情報の詳細については、[パラメータ情報] について [839 ページ] を参照してください。
8. [保存] を選択します。

   > **注意**
   >
   > シナリオを実行する前に、シナリオの各タスクテンプレートに入力を指定する必要があります。ただし、[パラメータありで実行] オプションを使用して、入力を指定することもできます。
9. [シナリオの保存] ダイアログボックスで、[シナリオの保存] および [電子メール通知] タブで必要な情報を入力します。

a. [シナリオの保存] タブで、シナリオの名前 (必須) を入力し、説明を追加し、シナリオを保存する場所を選択します。
b. [電子メール通知] タブで、切り替えボタンを選択してオンに切り替えます。
次の図に示すオプションが表示されます。

c. 1 つまたは複数のオプションを選択します。この選択は、電子メール通知をトリガする基準です。
d. [デフォルト設定を使用] を使用するか、切り替えボタンを使用してオフに切り替えることができます。これらのデフォルト設定は、CMC で定義されます。電子メールの出力先のデフォルト設定を定義する方法については、*Business Intelligence* 管理者ガイドを参照してください。
e. [デフォルト設定を使用] を選択解除した場合は、[差出人、宛先]、[*Cc*] (オプション) と [*BCC*] (オプション) の電子メールアドレス、[件名]、および [メッセージ] を入力します。各フィールドにプレースホルダを追加することもできます。

10. [保存] または [保存して実行] を選択します。

新しいシナリオは、[ワークフローアシスタント] の [シナリオ] ビューに表示され、[電子メール通知] タブで選択した基準に基づいて、電子メールがトリガされます。

22.7.5.1.1 入力パラメータの指定

ワークフローアシスタントでワークフローテンプレートを作成する際に、設計時と実行時の入力値を追加することができます。つまり、シナリオの作成および実行中に入力値を追加することができます。シナリオに入力値を追加するには、2 つの方法があります。

1. 入力ヘルプ
2. タスクの出力を別のタスクの入力としてマッピングする

入力ヘルプ

[入力ヘルプ] を使用して、リポジトリエクスプローラからドキュメントやワークリストなどのオブジェクトを選択することができます。たとえば、ドキュメントを最新表示するシナリオでは、[ドキュメント] フィールドで [入力ヘルプ] アイコン を選択して、ドキュメントを選択することができます。

タスクの出力を別のタスクの入力としてマッピングする

シナリオの実行時に、最初のタスクの出力を 2 番目のタスクの入力として指定することができます。最初のタスクから取得された値の一覧を表示するには、入力フィールドに @ を入力する必要があります。

- 入力値の形式は、**@<WorkflowTemplate>.<TaskTemplate>.<OutputParameter>** です。
- 入力値の一覧には、最初のタスクから取得された互換性のある値のみが表示されます。たとえば、入力フィールドがデータタイプとして CSV を受け入れる場合、前のタスクの CSV 形式の入力値が表示されます。

> ⓘ 注記
>
> 入力パラメータでは、入力として CSV ファイルがサポートされています。詳細については、CSV データの使用 [838 ページ]を参照してください。

22.7.5.1.2 CSV データの使用

ほとんどの標準タスクテンプレートは、CSV 形式の入力パラメータ値をサポートしています。たとえば、[ドキュメントの最新表示] タスクテンプレートは、入力フィールド [ドキュメント] の CSV 形式をサポートしています。つまり、名前、**cuid**、およびステータスの形式のデータで構成される CSV ファイルを [ドキュメント] の入力として選択できます。

> ⓘ 注記
>
> タスク入力フィールドが **cuid** を受け入れる場合、**cuid** を含む他のパラメータを含む CSV ファイルを選択すると、入力フィールドでは CSV ファイルの **cuid** 列の値のみが使用されます。例については、以下の CSV データを参照してください。
>
> 名前, cuid, ステータス;
>
> Charting, AW4AVT1AUhVAogA6P7OQv9c, success;
>
> SalesReport, BW3AVT1AUhVAogA743QCDsD, success;
>
> この例では、入力フィールドでは AW4AVT1AUhVAogA6P7OQv9c と BW3AVT1AUhVAogA743QCDsD が使用され、他の値は無視されます。

列および行区切り

サポートされている列区切りは , です。行区切りは ; です。入力フィールドの列および行区切りによって、列および行形式のデータが区切られます。例については、以下の CSV データを参照してください。

名前, cuid, ステータス;

Charting, AW4AVT1AUhVAogA6P7OQv9c, success;

SalesReport, BW3AVT1AUhVAogA743QCDsD, success;

ここで、カンマは名前、**cuid**、およびステータスが列であることを示し、セミコロンは行の終わりを示します。

> ⓘ 注記
>
> CSV ファイルが [ワークリストの読み取り] タスクテンプレートの入力である場合、列区切りは , になります。行区切りは ; または新しい行になります。

> ⚠ 警告
>
> CSV データの値にカンマまたはセミコロンを含めることはできません。

22.7.5.1.3 [パラメータ情報] について

シナリオの入力パネルでパラメータを展開して選択すると、[パラメータ情報] が表示されます。たとえば、タスクテンプレート [ドキュメントの最新表示] には、[ドキュメント] 入力フィールドがあります。[ドキュメント] 入力フィールドを選択すると、[パラメータ情報] が表示されます。

[パラメータ情報] は、以下の 2 つのセクションで構成されています。

1.入力パラメータ

2.出力パラメータ

入力パラメータ

入力パラメータでは、選択したフィールドに必要な入力のタイプについて説明します。これは、タスクテンプレート内の入力フィールドに固有です。

出力パラメータ

出力パラメータでは、タスクから取得したさまざまな出力について説明します。これは、1 つの入力フィールドのみではなく、タスク全体に固有です。

22.7.5.2 シナリオの編集

ワークフローアシスタントでシナリオを編集します。

1. ワークフローアシスタントの [シナリオ] タブで、 ([その他]) を選択し、[編集] を選択します。

   [シナリオの編集] 画面が表示されます。
2. [シナリオの編集] 画面で、タスクテンプレートやワークフローテンプレートを追加または削除したり、テンプレートの入力パラメータ値を変更したりして、シナリオに必要な編集を行います。
3. [保存] を選択します。

   [シナリオの保存] ダイアログが表示されます。
4. [シナリオの保存] ダイアログで、必要に応じてシナリオの名前を変更し、[保存] を選択します。

   シナリオの変更が保存され、ワークフローアシスタントのホームページに戻ります。

22.7.5.3 シナリオの削除

ワークフローアシスタントでシナリオを削除します。

1. ワークフローアシスタントの [シナリオ] タブで、 ([その他]) を選択し、[削除] を選択します。
2. 表示される警告で、[削除] を選択します。

   削除されたシナリオは、ワークフローアシスタントの [シナリオ] タブに表示されなくなります。

22.7.5.4 シナリオの実行および結果の表示

BI データでシナリオを実行し、ワークフローアシスタントで結果を表示します。

1. ワークフローアシスタントの [シナリオ] ビューで ([その他]) を選択し、[実行] または [パラメータありで実行] を選択します。

   [パラメータありで実行] では、シナリオのすべての入力パラメータを示すダイアログが開き、値を変更したり、欠損値を設定したりすることができます。

   > ⓘ 注記
   >
   > このパラメータダイアログで設定された値はシナリオとともに保存されず、実行中のインスタンスでのみ使用されます。

   シナリオ (タイルまたは表示されたアイテム) では、新しいステータスが [実行中] または [待機] と表示されます。実行が完了すると、ステータスが更新され、該当する値 (<成功/一部成功/失敗/待機/エラー/実行中、エラーあり>) が表示されます。

2. シナリオの結果を表示するには (実行中、または正常に実行された後)、 ([その他]) を選択し、[結果表示] を選択します。

   > ⓘ 注記
   >
   > [ビューの履歴] オプションを選択して、シナリオの以前の実行結果を確認できます。

3. [結果ページ] で結果を展開して、シナリオの各ワークフローテンプレートおよびタスクテンプレートの実行と完了の詳細を表示します。結果を確認したら、< (戻る) ボタンを使用してメイン画面に戻ることができます。

   > ⓘ 注記
   >
   > [エクスポート] オプションを選択して、シナリオ結果を PDF 形式で保存できます。

   > ⓘ 注記
   >
   > 1.wfmanager_conf.properties ファイルでキー値 task_time_out に対して時間 (秒) を追加することで、タスクがエージェントに応答する最大時間を設定できます。デフォルトでは、キー値 task_time_out は 86400、つまり 1 日に設定されています。
   >
   > 2.task_time_out は、ワークフローアシスタントのすべてのエージェントに対して設定されます。

22.7.5.5 シナリオの停止

タスクの実行がまだ進行中である場合でもシナリオを停止できます。

前提条件:

以下の手順は、シナリオが実行中または待機ステータスの場合にのみ実行できます。

- [シナリオ] ビューで、シナリオの [その他] を選択します。
- [停止] を選択します。

> **注記**
>
> [停止] オプションでは、シナリオはすぐに停止しません。[停止] オプションを選択すると、実行中の現在のタスクが完了してから、シナリオが停止します。つまり、シナリオの保留中のタスクのみが実行されません。

22.7.6 タスクテンプレート、ワークフローテンプレート、およびシナリオのステータスの理解

考えられるアーティファクト (タスクテンプレート/ワークフローテンプレート/シナリオ) のステータスと説明

ステータス	説明
作成済み (C)	アーティファクトが作成されたが、まだ一度も実行されていない場合。
待機 (P)	アーティファクトが実行のためにトリガされ、キューで実行を待機している場合。
実行中 (R)	アーティファクトが実行されている場合。
成功 (S)	すべての処理済みアイテムが正常に実行された場合。たとえば、処理されたドキュメントが、ドキュメントの最新表示タスクの後に正常に最新表示された場合。 **注記** シナリオ内のワークフローテンプレートが 1 つでも正常に実行されなかった場合、シナリオ全体のステータスは '成功' になりません。
一部成功 (PS)	いくつかの処理済みアイテムのみが正常に実行された場合。たとえば、ドキュメントの最新表示タスクの後に、いくつかのドキュメントが最新表示に失敗した場合、ステータスは [一部成功] に変わります。
失敗 (F)	すべてのアイテムが正常に実行されなかった場合。
エラー (E)	実行中にアーティファクトにエラーまたは例外が発生した場合。
実行中、エラーあり (RE)	サーバでアーティファクトにエラーが発生したが、実行が継続された場合。

ステータス	説明
未実行	条件パラメータの設定が原因で、シナリオ内のタスクテンプレートまたはワークフローテンプレートが実行されない場合。 たとえば、管理者が 2 つのワークフローテンプレートの間に<成功時>の条件を設定することを選択した場合、前のワークフローテンプレートが失敗した場合、実行フローは次のワークフローテンプレートに到達しません。このような場合、次および後続のワークフローテンプレートは、[<未実行>] ステータスのままになります。

> **注記**
>
> 表の凡例は以下のとおりです。
>
> - TTS: タスクテンプレートステータス
> - WFTS: ワークフローテンプレートステータス
> - SS: シナリオステータス

ステータスマトリクス: タスクテンプレートのステータスおよび結果のワークフローテンプレートステータス

TTS1	TTS2	TTS3	TTS4	TTS5	WFTS
S	S	S	E	NE	E (エラー)
S	S	S	PS	NE	PS (一部成功)
S	S	PS	F	NE	F (失敗)
S	PS	F	R	NE	R (実行中)
S	E	NE	NE	NE	E (エラー)
S	E	RE	NE	NE	RE (実行中、エラーあり)

以下のマトリクスは、各ワークフローテンプレートのステータスがシナリオの全体的なステータスにどのように影響するかを示しています。

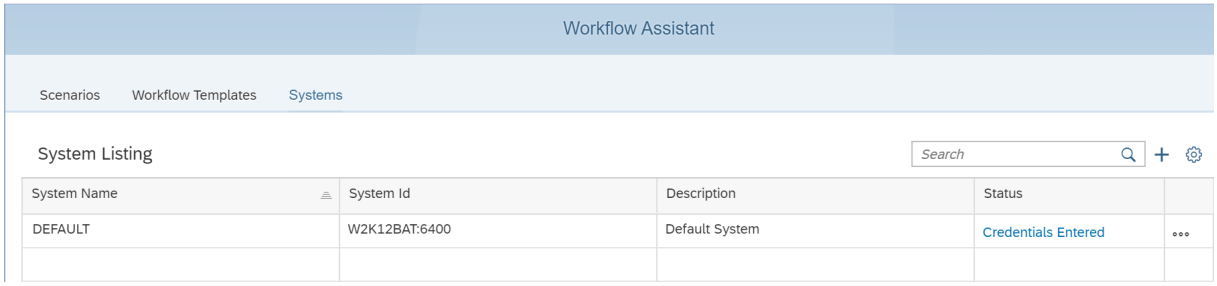
ステータスマトリクス: ワークフローテンプレートのステータスと結果のシナリオステータス

WFTS1	WFTS2	WFTS3	WFTS4	WFTS5	SS
S	S	S	E	NE	E (エラー)
S	S	S	PS	NE	PS (一部成功)
S	S	PS	F	NE	F (失敗)
S	PS	F	R	NE	R (実行中)
S	E	NE	NE	NE	E (エラー)
S	E	RE	NE	NE	RE (実行中、エラーあり)

22.7.7 システムの使用

[システム] タブでは、複数の BI ランドスケープを登録することができます。[システム] では、登録した BI ランドスケープにアクセスできます。

[システム] タブのスナップショット



[システム] タブで、以下のアクションを実行できます。

- 新しいシステムの追加 (登録)

  > → 注意
  >
  > システムを [シナリオ] や [ワークフローテンプレート] などの他のビューで使用できるように、このタブでシステムを登録する必要があります。

- 既存のシステムの変更 (編集または削除)
- 認証情報 (`User Name, Password, Authentication`) を入力してシステムに接続 (または切断) する

  > ⓘ 注記
  >
  > ワークフローアシスタントがインストールされているシステムが、[システム] タブに "デフォルト" システムとして表示されます。ただし、このランドスケープに接続するには、認証情報を入力する必要があります。

- [システム] ビューに表示される列のカスタマイズ

22.7.7.1 新しい BI システムの登録

アクセスが許可されている BI システムに接続してワークフローアシスタント機能を使用するには、最初にワークフローアシスタントで BI システムを登録 (追加) する必要があります。

システムを登録するには、以下の手順に従います。

1. ワークフローアシスタントにログオンします。
2. [ホーム] ページで、[システム] タブに移動します。

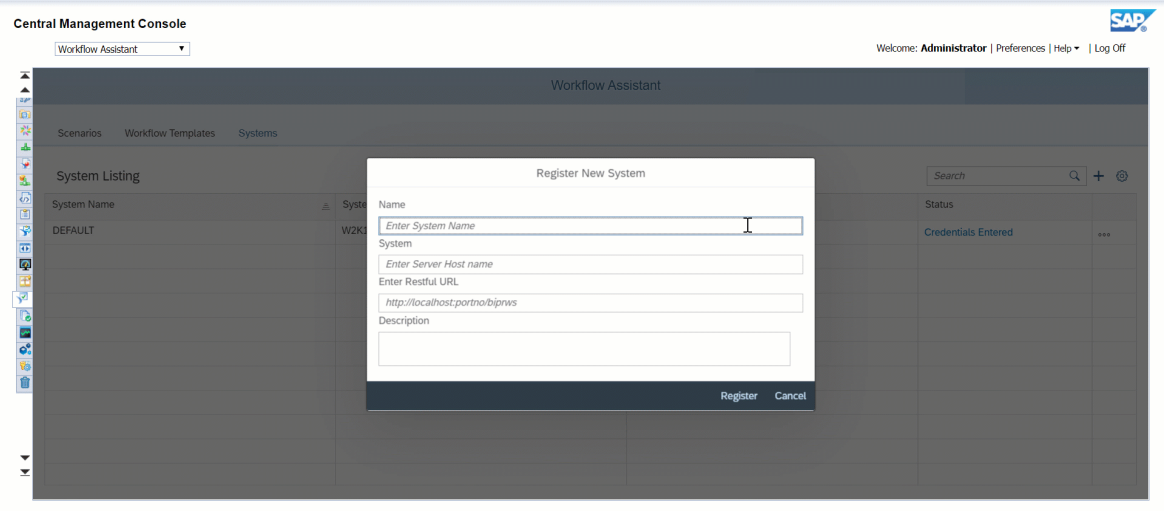
   このビューには、利用可能な登録済みのシステムが一覧表示されます。
3. + ([追加]) アイコンを選択します。

   [新しいシステムの登録] ダイアログが表示されます。
4. [<名前>] に、システムを特定できるエイリアスを入力します。

5. [<システム>] に、マシンまたはマシンのクラスタを識別するサーバホスト名または IP アドレスを入力します。
6. [<RestFul URL>] に、BI プラットフォームサーバの RESTful Web サービス URL を入力します。オプションで、システムの [<説明>] を追加できます。
7. [登録] を選択します。

> **注記**
>
> 同じ BI システムを異なる名前で登録できますが、[システム] ビューで BI システムを一度だけ登録することをお奨めします。

登録したシステムは、[システム一覧] テーブルのシステムの一覧に追加されます。



22.7.7.2 既存の BI システムの変更

[システム] ビューでは、登録したシステムを変更することができます。

既存のシステムを変更するには、以下の手順に従います。

1. ワークフローアシスタントにログオンし、[システム] タブに移動します。
2. [システム] ビューで、変更する一覧表示されたシステムの ([その他]) → [編集] を選択します。

   [システムの編集] ダイアログが表示されます。
3. 要件に応じて、[<名前>] (エイリアス)、[<システム>]、[<RestFul URL>]、または [<説明>] を変更し、[完了] を選択します。

   変更が [システム一覧] テーブルに反映されます。

> **注記**
>
> システムを削除するには、削除する一覧表示されたシステムの [その他] → [削除] を選択し、表示されたダイアログで削除を確認します。

22.7.7.3 登録済み BI システムへの接続

[システム一覧] テーブルの [<ステータス>] フィールドを使用して、登録済みシステムに接続することができます。ワークフローアシスタントのシナリオでシステムを使用するには、BI システムに接続することが不可欠です。

追加した BI システムに接続するには、以下の手順に従います。

1. ワークフローアシスタントにログオンし、[システム] タブに移動します。
2. まだ接続していない登録済みシステムの [<ステータス>] フィールドに、フラグ文字列 ([認証情報未入力]) が表示されます。

   [認証情報の入力] ダイアログが表示されます。
3. (プラットフォーム管理者によって付与された権限に基づいて) BI システムの次の認証情報を入力します。[<ユーザ名>]、[<パスワード>]、および [<認証>]。[保存] を選択します。

   ワークフローアシスタントによって認証情報が検証され、検証が成功した場合、BI ランドスケープの [<ステータス>] が [入力済み認証情報] に更新されます。成功しなかった場合、エラーメッセージが表示され、[<ステータス>] は変更されません。

22.7.7.4 システムビューのカスタマイズ

ビューのフィールド (列) の表示を変更することで、[システム一覧] ビューの外観をカスタマイズすることができます。

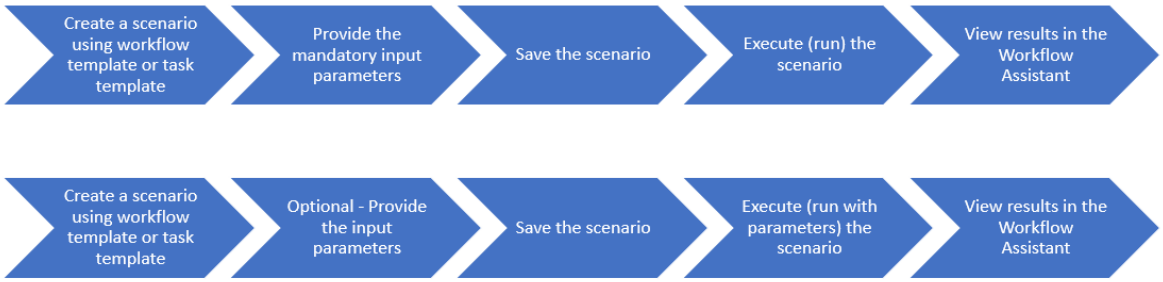
[システム] ビューの特定の列を表示/非表示にするには、以下の手順に従います。

1. ワークフローアシスタントにログオンし、[システム] タブに移動します。
2. ([設定]) を選択し、[システム一覧] テーブルで非表示にする列 (フィールドヘッダ) の選択を解除します。

   選択解除された列は、[システム一覧] テーブルに表示されなくなります。
3. 非表示の列をビューに戻すには、[設定] を選択し、必要なフィールドヘッダを再度選択します。

22.7.8 ワークフローアシスタントのエンドツーエンドのプロセスフロー

視覚的な表示を参照してください。



22.8 ログファイルのチェック

このトピックでは、ワークフローアシスタントのログファイルをチェックする方法について説明します。

ワークフローアシスタント

ワークフローアシスタントの場合、`<INSTALLDIR>¥AdminConsole¥WorkflowAssistant` にある *WorkflowAssistant_Trace.ini* ファイルでトレースレベルを選択する必要があります。トレースファイルは、以下の環境変数を設定して、**_Trace.ini** ファイルを使用して設定することもできます。

- `BO_TRACE_CONFIGDIR`。ログ用に設定ファイルのフォルダ名を設定します。例: `C:¥BOTraces¥config`
- `BO_TRACE_CONFIGFILE`。設定ファイルの名前を設定します。例: `BO_trace.ini`
- `BO_TRACE_LOGDIR`。ログ用にフォルダ名を設定します。例: `C:¥BOTraces`

> **注記**
>
> `INI` ファイル名では大文字と小文字が区別されます。

`BO_trace.ini` 設定ファイルを以下のように作成します。

```
sap_log_level = log_info;
sap_trace_level = trace_debug;
```

デフォルトでは、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥logging` でログをチェックできます。

23 リサイクルビン

23.1 ごみ箱

ごみ箱について

ごみ箱は、CMC の新しいアプリケーションです。ユーザが BOE システムからアイテムを削除すると、そのアイテムはごみ箱に移されて、ごみ箱を空にするまで一時的に保存されます。これにより、ユーザは誤って削除したレポート/フォルダを取り戻して元の場所に復元することができます。

ごみ箱アプリケーションで、管理者は以下の処理を行うことができます。

- 削除されたアイテム (レポートやフォルダなど) の復元を開始する。
- アイテムをごみ箱から完全に削除する。
- ごみ箱の自動クリーンアップを実行する。

ごみ箱が有効になっている場合は、以下のインフォオブジェクトタイプをリサイクルできます。

- 個人用フォルダの内容
- イベント
- カレンダ
- パブリックフォルダの内容
- ユニバース
- 接続
- パブリックカテゴリ
- 個人用カテゴリ
- 受信ボックス
- プロファイル
- カスタムの役割

23.1.1 アイテムをごみ箱から復元する

ごみ箱には削除されたアイテムの一覧が表示されます。アイテムをごみ箱から復元するには、以下の手順を実行します。

1. CMC にログオンします。
2. CMC ホームページの [管理] ペインから、[ごみ箱] を選択します。
3. 復元するアイテムを右クリックして、コンテキストメニューから [復元] を選択します。

4. [*OK*] を選択します。

   復元されたアイテムの場所を参照すると、復元操作を確認できます。

> ⓘ 注記
>
> アイテムをごみ箱から復元するときに、復元場所に同名の別のアイテムがすでに存在する場合、次の名前でアイテムが復元場所に保存されます。"<item name> restored(1, 2, ...)"
>
> ごみ箱内のアイテムの親フォルダが削除された場合、アイテムの復元時にその親フォルダが再作成されます。ただし、この親フォルダには、ごみ箱から復元されたアイテムのみが含まれます。
>
> ごみ箱からアイテムを開くまたは参照することはできません。
>
> アイテムをフォルダから削除した後、そのフォルダの変更権限が管理者によって制限されても、アイテムを元のフォルダに復元しようとした場合、そのアイテムは元のフォルダに復元されます。

これで、ゴミ箱からアイテムが正常に復元されました。

23.1.2 アイテムをごみ箱から完全に削除する

管理者として、ごみ箱から選択したアイテムを完全に削除する、またはゴミ箱を空にする権限があります。

ゴミ箱からアイテムを完全に削除するには、以下の手順を実行します。

1. CMC にログオンします。
2. CMC ホームページの [管理] ペインから、[ごみ箱] を選択します。
3. 削除するアイテムの上で右クリックして、コンテキストメニューから [削除] を選択します。
4. [*OK*] を選択します。

これで、ゴミ箱からアイテムが正常に削除されました。

23.1.3 ごみ箱の自動クリーンアップを有効にする

定期的にゴミ箱の自動クリーンアップを実行することができます。

ゴミ箱の自動クリーンアップを有効にするには、以下の手順を実行します。

1. CMC にログオンします。
2. CMC ホームページの [管理] ペインから、[アプリケーション] を選択します。
3. [アプリケーション] ページで、[リサイクルビン] アプリケーションを選択します。

   プロパティ: [リサイクルビン] ダイアログボックスが表示されます。
4. チェックボックスを選択して、削除されたアイテムが自動クリーンアップされるまでに必要な期間 (何日間) を指定します。
5. [保存して閉じる] を選択します。

これで、ゴミ箱の自動クリーンアップが正常に有効になりました。

24 監査

24.1 概要

監査を使用して、サーバおよびアプリケーションの重要なイベントを記録することができます。このようにして、アクセスされている情報、アクセスと変更の方法、およびそれらの操作の実行者を把握するのに役立てることができます。この情報は、監査データストア (ADS) と呼ばれるデータベースに記録されます。データが ADS に格納されたら、それぞれのニーズに合うようカスタムレポートをデザインすることができます。SAP Community (http://community.sap.com/) でサンプルユニバースとサンプルレポートを検索できます。

この章では、監査実行サーバは、イベントに関する情報を記録または保存するシステムを指します。また、監査対象サーバは、監査可能なイベントを実行するシステムを指します。1 つのシステムが両方の役割を果たす場合もあります。

監査の仕組み

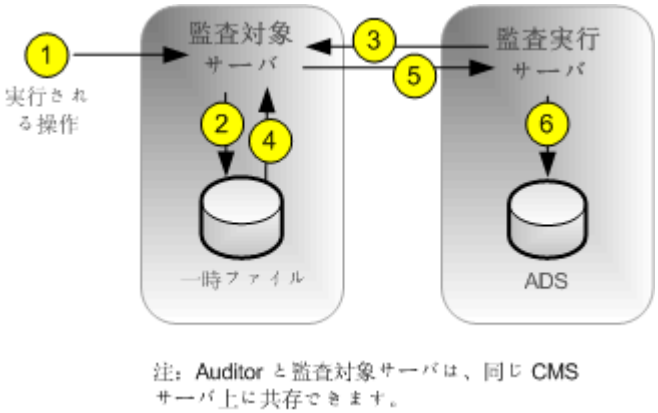
Central Management Server (CMS) はシステム監査実行サーバとして機能し、監査可能なイベントを発生させる各サーバまたはアプリケーションは監査対象サーバとして機能します。監査対象イベントが発生すると、監査対象サーバはレコードを生成してローカルの一時ファイルに格納します。CMS は定期的に監査対象サーバと交信し、これらのレコードを要求し、ADS にデータを書き込みます。

また、CMS は、異なるマシン上で発生する監査対象イベントの同期制御も行います。各監査対象サーバは、記録される監査イベントに、タイムスタンプを付けます。異なるサーバ上で発生するイベントのタイムスタンプの一貫性を保つために、CMS は定期的に、監査対象サーバに対し自分のシステム時間を配信します。監査対象サーバは、この時間をそれぞれの内部クロックと比較します。もし違いがあれば、それ以降の監査イベントに対して記録する時間を修正します。

監査対象サーバの種類に応じて、次のワークフローのいずれかを使用してイベントが記録されます。

サーバ監査

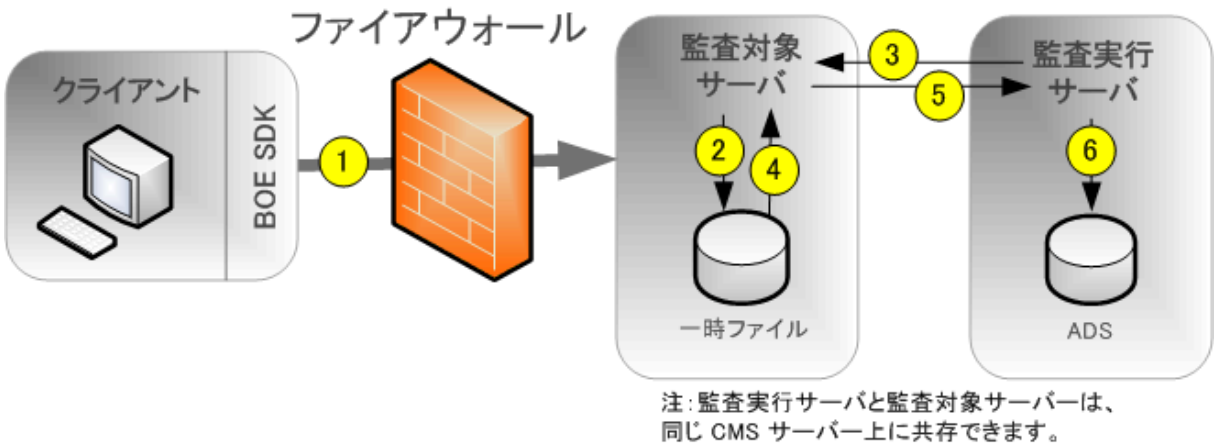
サーバによって生成されたイベントの場合、CMS は監査対象サーバとしても監査実行サーバとしても実行できます。



1. 監査可能なイベントがサーバで実行されます。
2. 監査対象サーバはイベントを一時ファイルに書き込みます。手順 1 および 2 は、手順 3 の前に複数回発生する場合があります。
3. 一定の間隔で、監査実行サーバは監査対象サーバをポーリングし、監査イベントのバッチを要求します。
4. 監査対象サーバは一時ファイルからイベントを取得します。
5. 監査対象サーバはイベントを監査実行サーバに送信します。
6. 監査実行サーバは、ADS にイベントを書き込み、監査対象サーバに一時ファイルからイベントを削除するよう通知します。

CORBA によるクライアント接続のクライアントログオン監査

これには、SAP BusinessObjects Web Intelligence などのアプリケーションが含まれます。



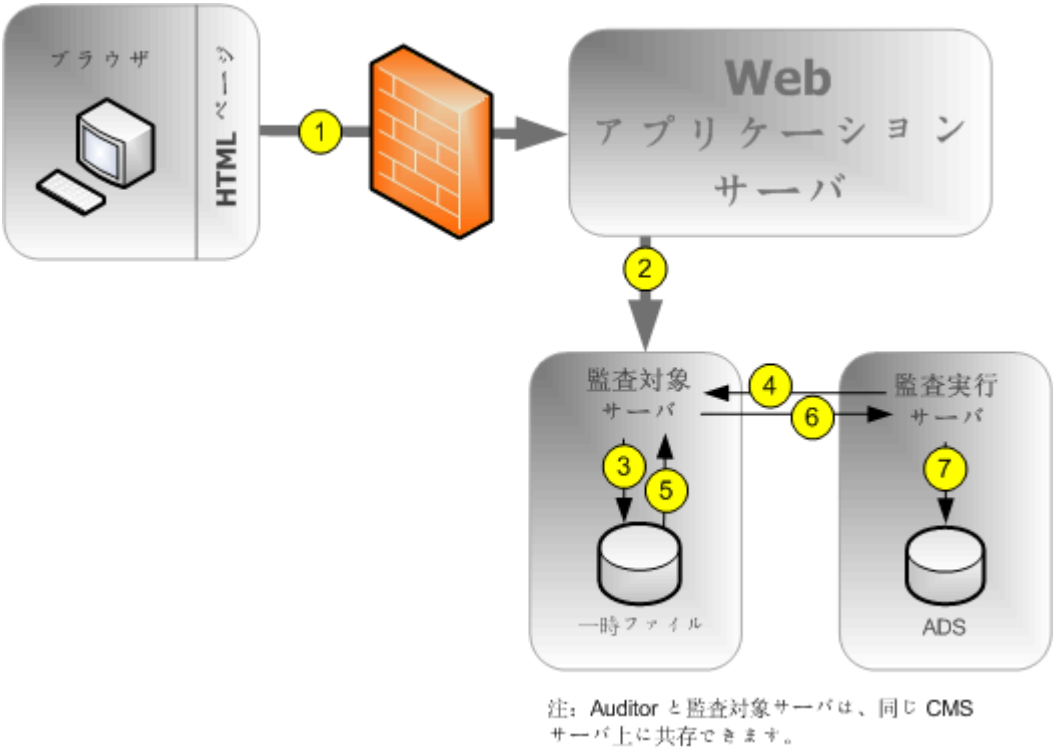
1. クライアントは CMS に接続します。この CMS は監査対象サーバとして機能します。クライアントはその IP アドレスとマシン名を提供し、監査対象サーバがそれを検証します。

> ⓘ 注記
>
> クライアントと CMS 間のファイアウォールでポートを開く必要があります。ファイアウォールの詳細については、*SAP BusinessObjects Enterprise Business Intelligence* プラットフォーム管理者ガイドのセキュリティに関する章を参照してください。

2. 監査対象サーバはイベントを一時ファイルに書き込みます。手順 1 および 2 は、手順 3 の前に複数回発生する場合があります。
3. 一定の間隔で、監査実行サーバは監査対象サーバをポーリングし、監査イベントのバッチを要求します。
4. 監査対象サーバは一時ファイルからイベントを取得します。
5. 監査対象サーバはイベントを監査実行サーバに送信します。
6. 監査実行サーバは、ADS にイベントを書き込み、監査対象サーバに一時ファイルからイベントを削除するよう通知します。

HTTP によるクライアント接続のクライアントログオン監査

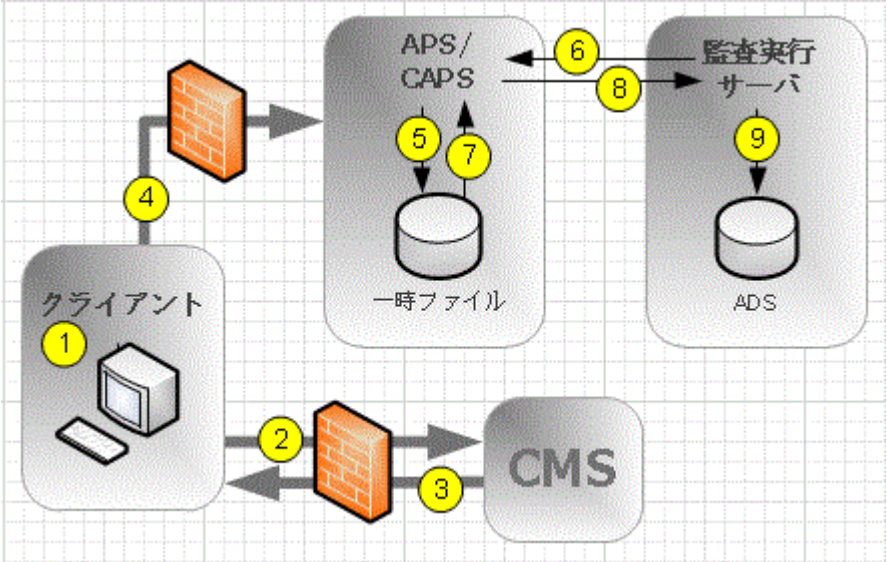
これには、BI ラウンチパッド、セントラル管理コンソール、SAP BusinessObjects Web Intelligence などのオンラインアプリケーションが含まれます。



1. ブラウザが Web アプリケーションサーバに接続し、ログオンデータが Web アプリケーションサーバに送信されます。
2. BI プラットフォーム SDK は、ブラウザマシンの IP アドレスおよび名前とともに、ログオン要求を監査対象サーバ (CMS) に送信します。
3. 監査対象サーバはイベントを一時ファイルに書き込みます。手順 1 および 3 は、手順 4 の前に複数回発生する場合があります。
4. 一定の間隔で、監査実行サーバは監査対象サーバをポーリングし、監査イベントのバッチを要求します。
5. 監査対象サーバは一時ファイルからイベントを取得します。
6. 監査対象サーバはイベントを監査実行サーバに送信します。
7. 監査実行サーバは、ADS にイベントを書き込み、監査対象サーバに一時ファイルからイベントを削除するよう通知します。

CORBA によるクライアント接続のログオンなしの監査

このワークフローは、CORBA による接続時の SAP BusinessObjects Web Intelligence のイベントの監査に適用されます。



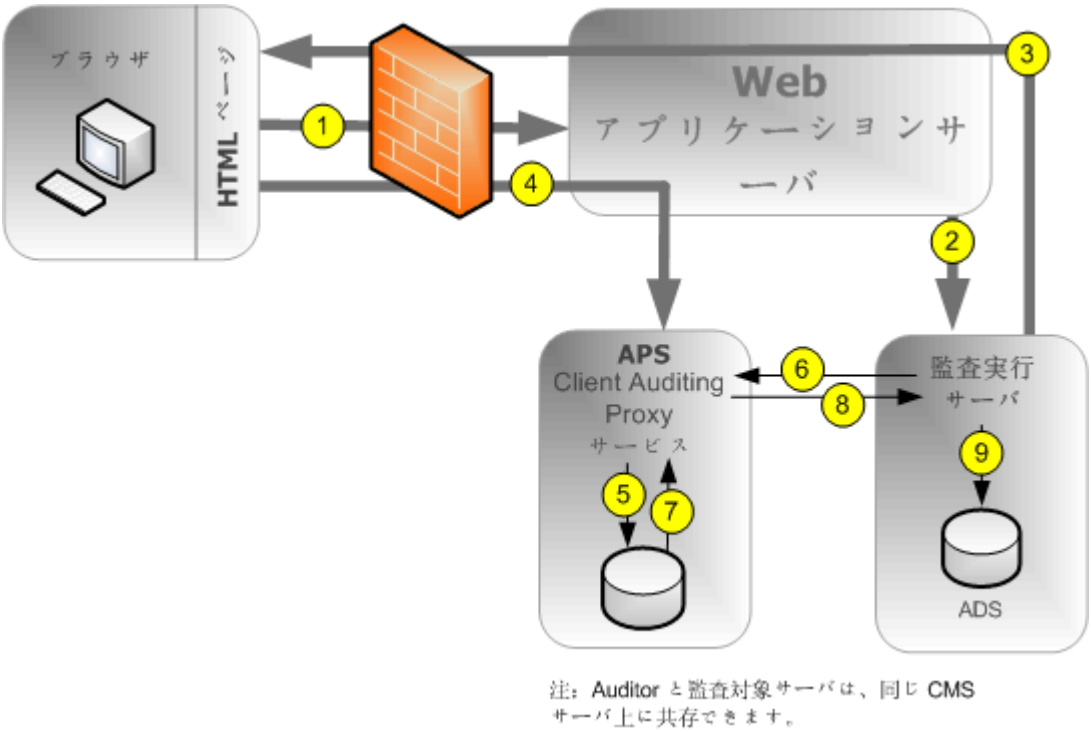
1. ユーザは、監査対象となる動作を実行します。
2. クライアントは CMS に接続し、動作が監査対象として設定されているかどうかを確認します。
3. 動作が監査対象として設定されている場合は、CMS はクライアントにその情報を通知します。
4. クライアントは、Adaptive Processing Server でホストされている クライアント監査プロキシサービス (CAPS)にイベント情報を送信します。

   > ⓘ 注記
   >
   > ファイアウォールのポートは、各クライアントと CAPS をホストするすべての Adaptive Processing Server 間、さらに各クライアントと CMS との間で開かれる必要があります。ファイアウォールの詳細については、*SAP BusinessObjects Enterprise Business Intelligence* プラットフォーム管理者ガイドのセキュリティに関する章を参照してください。

5. CAPS はイベントを一時ファイルに書き込みます。手順 1 および 5 は、手順 6 の前に複数回発生する場合があります。
6. 一定の間隔で、監査実行サーバは CAPS をポーリングし、監査イベントのバッチを要求します。
7. CAPS は一時ファイルからイベントを取得します。
8. CAPS はイベント情報を監査実行サーバに送信します。
9. 監査実行サーバは、ADS にイベントを書き込み、CAPS にイベントを一時ファイルから削除するよう通知します。

HTTP によるクライアント接続のログオンなしの監査

このワークフローは、HTTP による接続時の SAP BusinessObjects Web Intelligence のイベント (ログオンイベントは除く) の監査に適用されます。



1. ユーザは、潜在的に監査可能なイベントを開始します。クライアントアプリケーションは、Web アプリケーションサーバに接続します。
2. Web アプリケーションは、イベントが監査対象として設定されているかどうかを確認します。

   > ⓘ 注記
   >
   > 図では監査実行サーバの CMS が接続されていますが、クラスタ内のどの CMS に接続してもこの情報を得ることができます。

3. CMS は監査設定情報を Web アプリケーションサーバに返し、Web アプリケーションサーバはこの情報をクライアントアプリケーションに渡します。
4. イベントが監査対象として設定されている場合、クライアントはイベント情報を Web アプリケーションサーバに送信し、Web アプリケーションサーバはその情報を、Adaptive Processing Server (APS) でホストされている クライアント監査プロキシサービス (CAPS) に渡します。
5. CAPS はイベントを一時ファイルに書き込みます。手順 1 および 5 は、手順 6 の前に複数回発生する場合があります。
6. 一定の間隔で、監査実行サーバは CAPS をポーリングし、監査イベントのバッチを要求します。
7. CAPS は一時ファイルからイベントを取得します。
8. CAPS はイベント情報を監査実行サーバに送信します。
9. 監査実行サーバは、ADS にイベントを書き込み、CAPS にイベントを一時ファイルから削除するよう通知します。

監査をサポートするクライアント

以下のクライアントアプリケーションが監査をサポートしています。

- Analysis, OLAP エディション (AOLAP)
- BI ラウンチパッド (BILP)
- ビジネスビューマネージャ (BVM)
- セントラル設定マネージャ (CCM)
- セントラル管理コンソール (CMC)
- OpenDocument
- インフォメーションデザインツール (IDT)
- Live Office (LO)
- SAP BusinessObjects Mobile
- トランスレーションマネジメントツール (TMT)
- Web Intelligence リッチクライアント (WIRC)
- Lumira Desktop アプリケーション (Discovery)
- Lumira Designer アプリケーション

> **注記**
>
> 上に一覧表示された監査イベントを収集するには、CAPS のインスタンスを少なくとも 1 つ実行中である必要があります。

上に一覧表示されていないクライアントは直接イベントを生成しませんが、クライアントアプリケーション操作の結果としてサーバによって実行されたアクションの一部は監査できます。

監査の整合性

多くの場合、監査が正しくインストール、設定、保護され、すべてのクライアントアプリケーションの正しいバージョンが使用されている場合、監査機能は指定されたすべてのシステムイベントを正しくかつ一貫して記録します。ただし、特定のシステムおよび環境の条件が監査に悪影響を及ぼす可能性があるので、注意が必要です。

イベントが発生してから ADS に最後の転送が行われるまでの間に常に遅延が発生します。CMS または監査データベースが使用できない、またはネットワークに接続できないといった状況は、このような遅延を長引かせます。

システム管理者は、次の状況をすべて回避する必要があります。これらの状況では、不完全な監査レコードが生成される可能性があります。

- 監査データが格納されているドライブが、最大容量に達している。監査データベースと監査対象サーバの一時ファイルに使用するディスク領域が十分であることを確認する必要があります。
- 監査対象サーバがネットワークから正しく削除されていないため、すべての監査イベントを送信できない。ネットワークからサーバを削除する場合は、監査イベントを監査データベースに送信するための十分な時間を確保する必要があります。
- 監査対象サーバの一時ファイルの削除または変更。
- ハードウェア障害またはディスク障害。
- 監査対象サーバまたは監査実行サーバのホストマシンの物理的な破損。

監査イベントが CMS 監査実行サーバに到達できなくなる条件もいくつかあります。たとえば、次のような条件があります。

- ユーザが、古いクライアントバージョンを使用している。

- 正しく設定されていないファイアウォールによって、監査情報の送信がブロックされる。

> ⓘ 注記
>
> クライアントアプリケーションによって生成されたイベントに、システムの信頼できる領域外であるクライアント側から送信された情報が含まれている。そのため、状況によっては、この情報はシステムのサーバによって記録された情報ほど信頼性が高くない場合があります。

> ⓘ 注記
>
> デプロイメントからサーバを削除する場合は、最初にそのサーバを無効にする必要がありますが、一時ファイル内のすべてのイベントが監査データベースに転送できるようになるまで、サーバをネットワークに接続したまま稼動させておく必要があります。サーバのキュー内の監査イベントの現在の数メトリクスには、転送待ちの監査イベントの数が示されます。このメトリクスが 0 になると、サーバを停止できます。一時ファイルの場所は、そのノードの `%DefaultAuditingDir%` プレースホルダに定義されています。プレースホルダの詳細については、サーバの管理に関する章を参照してください。

> ⓘ 注記
>
> Client Auditing を使用する場合は、Client Auditing Proxy Service 専用の Adaptive Processing Server を作成することをお奨めします。このことによって、最良のシステムパフォーマンスが得られます。システムのフォールトトレランスを向上するには、複数の APS 上で CAPS を実行することも考慮します。

関連リンク

サーバとノードプレースホルダ [1158 ページ]

24.2 CMC 監査ページ

CMC の [監査] ページには、次の領域があります。

- ステータスの概要
- イベントの設定
- イベント詳細の設定
- 設定

24.2.1 監査ステータス

監査の [ステータスの概要] には、監査設定の最適化に有用で、監査データの整合性に影響を与える可能性のある問題を警告する、一連のメトリクスが表示されます。ステータスの概要は、セントラル管理コンソールの [監査] ページの上部にあります。

概要には、次の状況における警告も表示されます。

- 監査データストア (ADS) データベースへの接続は、使用不可能です。
- クライアントイベントが収集されないようにする、実行中または有効化されたクライアント監査プロキシサービスはありません。
- 監査対象には、取得できなかったイベントがあります (サーバまたは影響のあったサーバは特定されます)。通常、これは、サーバが適切に停止またはシャットダウンされなかったこと、および一時ファイルにイベントがまだ存在することを示しています。

> **注記**
>
> ステータスの概要のメトリクスは、緑色、黄色、赤色でマークされ、監査機能の状態を示します。

監査ステータスのメトリクス

メトリクス	詳細
ADS 最終更新日	Auditor CMS が監査イベントの監査対象のポーリングを最後に終了した日付と時刻。
監査スレッド使用率	Auditor CMS が監査対象からのデータ収集に費やすポーリングサイクルの割合、残りは、ポーリング間に存在する時間です。 この値が 100% に達している場合、数値は黄色で表示されます。これは、次のポーリングの開始時に、Auditor がまだ監査対象からのデータ収集を行っていることを意味します。これにより、イベントの ADS への到達が遅れる可能性があります。 この状態が頻繁にまたは永続的に発生する場合は、デプロイメントを更新して ADS データベースにより高い頻度でデータが受信されるようにするか (より迅速なネットワーク接続またはより強力なデータベースハードウェアなど)、システムで追跡される監査イベントの数を減らすことをお奨めします。
最終ポーリングサイクル期間	最終ポーリングサイクル期間 (秒)。これは、以前のポーリングサイクルにおけるイベントデータの ADS への最長到達遅延を示します。 • 20 分 (1200 秒) 未満の場合は、数値は緑色の背景に表示されます。 • 20 分から 2 時間 (7200 秒) の場合は、数値は黄色の背景に表示されます。 • 2 時間を上回る場合は、数値は赤色の背景に表示されます。 この状態が長く続き、遅延が長すぎると考えられる場合は、デプロイメントを更新して ADS データベースにより高い頻度でデータが受信されるようにするか (より迅速なネットワ

メトリクス	詳細
	ーク接続またはより強力なデータベースハードウェアなど)、システムで追跡される監査イベントの数を減らすことをお勧めします。
CMS Auditor	Auditor として現在機能している CMS の名前。
ADS データベース接続名	監査データストア (ADS) に接続するために Auditor CMS により現在使用されているデータベース接続の名前。SQL Anywhere、SQL Server、および HANA サーバの場合、これは ODBC 接続の名前になります。その他の種類のデータベースの場合、データベース名と接続ポートの後にサーバ名が続きます。
ADS データベースのユーザ名	Auditor CMS が ADS データベースにログインするために使用しているユーザ名。

24.2.2 監査イベントの設定

CMC 監査ページは、監査を有効化し、全システムで監査されるイベントを選択するために使用することができます。

特定のイベントまたはイベント詳細に関心がない場合は、選択しないで、システムパフォーマンスを向上させることができます。

> ⓘ 注記
>
> 監査イベントは、一度に 1 つのイベントではなく、バッチモードで監査データベースにプッシュされます。バッチサイズは現在、1000 件の監査イベントに設定されています。

> ⓘ 注記
>
> BI プラットフォームのインストール時に、ADS 接続を設定しないように選択した場合、監査イベントを設定する前にデータベースへの接続を設定する必要があります。接続がなくてもイベントは収集されますが、いったん接続されると、イベントは ADS に書き込まれます。監査をオフにするには、レベルがオフに設定されている必要があります。監査データストア設定を参照してください。

24.2.2.1 監査イベントを設定する

監査イベントを設定するには、次の手順に従います。

1. セントラル管理コンソールで、[監査] タブを選択します。
   [監査] ページが表示されます。
2. [イベントの設定] スライダを目的の監査レベルに設定します。各監査レベルは特定のメトリクス値に対応します。

- オフ - 1
- 最小 - 2
- デフォルト - 3
- 完全 - 4
- カスタム - 0

次のテーブルに、各レベルで取得されたスライダおよびイベントの異なる設定が表示されます。

監査レベル	取得されたイベント
オフ	なし
最小	• ログオン • ログアウト • 権限の変更 • カスタムアクセスレベルの変更 • 監査変更
デフォルト	[最小] イベント、プラス: • 表示 • 最新表示 • プロンプト • 作成 • 削除 • 変更 • 保存 • 検索 • 編集 • 実行 • 配信
完全	[最小] および [デフォルト] イベントプラス: • 呼び出しイベント • 範囲外をドリル • ページの取得 • プロモーションマネジメント設定 • ロールバック • VMS へ追加 • VMS から取得 • VMS へのチェックイン • VMS からチェックアウト • VMS エクスポート • VMS ロック • VMS ロック解除 • VMS 削除 • キューブへの接続 • MDAS セッション

監査レベル	取得されたイベント
	注記 アドオンのインストール時に、より多くのイベントが表示される場合があります。
カスタム	イベントのカスタム設定を選択します。

> **注記**
>
> [イベントの設定] が [デフォルト] に設定されている場合、[監査レベル] の値は 3 です。
>
> [イベントの設定] が [オフ] に設定されている場合、[監査レベル] の値は 3 から 1 に変わります。

3. [カスタム] を選択し、[イベントの設定] スライダの下にある一覧で取得するイベントをクリックします。
4. [イベント詳細の設定] で、イベントと一緒に記録するオプション詳細をクリックします。記録する詳細が少ないほど、システムパフォーマンスが向上します。

詳細	説明
クエリ	設定すると、クエリイベント詳細 (詳細 ID 25) が、データベースをクエリするイベントについて記録されます。
フォルダパス詳細	設定すると、次の詳細が取得されます。 • *オブジェクトフォルダパス (詳細 ID 71)* • *最上位フォルダ名 (詳細 ID 72)* • *コンテナフォルダパス (詳細 ID 64)*
権限詳細	設定すると、次の詳細が取得されます。 • *権限が追加されました (詳細 ID 55)* • *権限が削除されました (詳細 ID 56)* • *権限が変更されました (詳細 ID 57)*
ユーザグループ詳細	設定すると、次の詳細が取得されます。 • *ユーザグループ名 (詳細 ID 16)* • *ユーザグループ ID (詳細 ID 15)*
プロパティ値詳細	設定されると、プロパティ値イベント詳細 (詳細 ID 29) は、オブジェクトのプロパティが更新される際に取得されます。これは、CMC、BI ラウンチパッド、または SharePoint イベントに対してのみ生成されます。

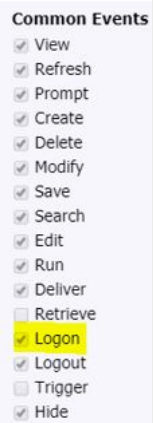
5. [保存] をクリックします。

> **注記**
>
> クライアント監査の場合、システムが新しいイベントのデータの記録を開始する前は、変更が実行された後、最大 2 分かかります。システムの変更を実行する際、この遅延を考慮に入れるようにしてください。

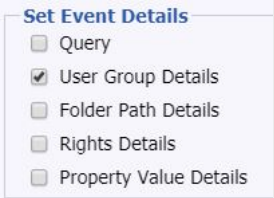
24.2.2.2 監査詳細テーブルの拡張されたイベント詳細記録

ⓘ 注記

- 以下に示す情報を利用するには、CMC 監査ページ [855 ページ]、特に [共通イベント]、[イベント詳細の設定]、[ユーザグループ詳細]、および [ログオン] に関する十分な理解が必要です。
- [ログオン] は、アプリケーションにアクセスするユーザの詳細を提供するイベントです。



- [ユーザグループ詳細] は、イベントごとに、ユーザに関連付けられたユーザグループの情報を提供します。



AUDIT_EVENT_DETAIL テーブルのユーザグループ詳細の記録は、[監査] ページの [共通イベント] および [イベント詳細の設定] で行った選択に部分的に依存します。[監査] ページで [ログオン] を選択し、[ユーザグループ詳細] を選択しなかった場合のシナリオについて考えてみます。このシナリオの場合、[ログオン] イベントのユーザグループ詳細は、引き続き AUDIT_EVENT_DETAIL テーブルに記録されます。BI 4.2 サポートパッケージ 5 の動作を理解するには、以下の表を参照してください。

ログオン	ユーザグループ詳細	動作
選択	選択	[共通イベント] で選択したすべてのイベントに関して、ユーザグループ詳細が記録されます。
選択	未選択	ユーザグループ詳細は、ログオンイベントに関してのみ記録されます。
未選択	未選択	ユーザグループ詳細は記録されません。
未選択	選択	ログオンイベントを除く選択したすべてのイベントに関して、ユーザグループ詳細が記録されます。

24.2.3 監査データストア設定

BI プラットフォームのインストール時に監査データベースを設定しないように選択した場合、またはデータベースの保存場所または設定を変更する場合、次のステップを使用して、ADS への接続を設定することができます。

このステップでは、監査イベントがデータベースに保持される期間を設定することもできます。

SAP BusinessObjects Enterprise XI 3.x の前のバージョンからアップグレードを実行し、Business Objects Metadata Manager (BOMM) をインストールしている場合、ADS を設定して、BOMM と同じデータベースまたはテーブルスペースを使用することをお勧めします。

> **注記**
>
> 既存の DB2 9.7 Workgroup を監査データベースとして使用している場合は、データベースアカウントが 8KB を超えるページサイズを使用できるよう設定されていることを確認してください。

24.2.3.1 監査データストアのデータベース設定を設定する

1. セントラル管理コンソールで、[監査] タブを選択します。
2. 設定エリアの *ADS データベース*見出しの下で、監査データに設定したデータベースタイプを選択します。
3. 接続名で、監査データベースに設定した接続の名前を入力します。

データベースの種類	接続名
IBM DB2	サービス名
Microsoft SQL Server	ODBC DSN
MySQL	`<serverhostname>`、`<port>`、`<databasename>`
Oracle	TNS サービス名
SAP HANA	ODBC DSN
SAP MaxDB	`<serverhostname>`、`<port>`、`<databasename>`
Sybase Adaptive Server Enterprise	サービス名
Sybase SQL Anywhere	ODBC DSN

   a. Windows 認証で Microsoft SQL データベースを使用している場合、[*Windows 認証*] オプションを有効にします。

4. [ユーザ名] フィールドと [パスワード] フィールドに、データベースへのログオン時に Auditor CMS で使用するユーザ名とパスワードを入力します。
5. [(日) より古いイベントを削除する] フィールドで、データベースに情報を残す日数を入力します。(最小値 1、最大値 109,200)

> ⚠ 警告
>
> ここで設定された日数より古いデータは、ADS から完全に削除されます。修復は不可能です。長期のレコードを維持する場合、レコードをアーカイブデータベースに定期的に移動することを考えてください。

6. Auditor-CMS をデータベースにマニュアルで再接続し、[*ADS 自動再接続*] を選択解除する場合、データベース接続はイベントで失われます。

> ⓘ 注記
>
> チェックが解除されている場合、接続が失われると、ADS への接続の再確立が必要になります。この処理は、CMS を再起動するか、または [*ADS 自動再接続*] を有効化することにより実行することができます。イベントは、記録され、ADS が再接続されるまで一時ファイルに保存されます。

7. 保存をクリックします。
8. クラスタ内のすべての CMS を再起動します。

> ⓘ 注記
>
> ページの最上部にあるステータスの概要に現在の ADS 値が表示されますが、これは CMS が再起動されるまで *ADS データベース*セクション内の値と異なる場合があります。

24.3 監査イベント

以下の表では、システム内のすべての監査イベントを示し、各イベントについて簡単に説明します。続いて、それらのイベントを作成するサービスタイプを一覧表示します。

イベント	
監査変更の説明、および各イベントタイプを生成したサーバとクライアント	システムの監査設定が変更されました。 • セントラル管理サービス
作成	新しいオブジェクトがシステムに追加されました。 • BI Commentary サービス • セントラル管理サービス • Crystal Reports 表示および変更サービス • Desktop Intelligence • 情報エンジンサービス • ライフサイクルマネジメント • Web Intelligence • Web Intelligence 共通サービス • 説明、および Web Intelligence コアサービスを生成したサーバとクライアント • Web Intelligence 処理サービス
キューブへの接続	OLAP キューブへの接続操作が実行されました。 • Multi-Dimensional Analysis Service

イベント	
	• 分析アプリケーション
カスタムアクセスレベルの変更	権限に関する情報が変更されました。 • Central Management Service
削除	システムからオブジェクトが削除されました。 • BI Commentary サービス • セントラル管理サービス • ライフサイクルマネジメントサービス
配信	オブジェクトが送信先に送信/配信されました。 • 認証更新スケジュールサービス • セントラル管理サービス • Crystal Reports for Enterprise スケジュールサービス • Crystal Reports スケジュールサービス • Desktop Intelligence • 送信先への配信スケジュールサービス • プラットフォーム検索スケジュールサービス • プローブスケジュールサービス • プログラムスケジュールサービス • セキュリティクエリスケジュールサービス • ユーザとグループのインポートスケジュールサービス • Web Intelligence スケジュールおよび公開サービス
範囲外をドリル	Web Intelligence ドキュメントのユーザが事前ロードしたレポートデータの範囲外の詳細レベルをドリルダウンしました。 • Web Intelligence • Web Intelligence 処理サービス • Web Intelligence 共通サービス • Web Intelligence コアサービス • 情報エンジンサービス
編集	オブジェクトのコンテンツが変更されました。 • BI ワークスペースのアプリケーション • Desktop Intelligence • 情報エンジンサービス • Web Intelligence • Web Intelligence 共通サービス • Web Intelligence コアサービス • Web Intelligence 処理サービス
LCM 設定	ライフサイクルマネジメントコンソール (LCM) の設定の詳細が変更されました。 • ライフサイクルマネジメント

イベント	
ログオン	ユーザがシステムにログオンしました。 • セントラル管理サービス
ログアウト	ユーザがシステムからログアウトしました。 • セントラル管理サービス
変更	オブジェクトのファイルプロパティが変更されました。 • Web Intelligence • ライフサイクルマネジメント • セントラル管理サービス • BI Commentary サービス
MDAS セッション	Multi Dimensional Analysis Service 処理が実行されました。 • Multi-Dimensional Analysis Service
ページの取得	SAP BusinessObjects Web Intelligence クライアントがリポジトリから追加の情報を取得しました。 • Web Intelligence 処理サービス • Web Intelligence 共通サービス • Web Intelligence コアサービス • 情報エンジンサービス
プロンプト	オブジェクトプロンプトに情報が入力されました。 • Crystal Reports キャッシュサービス • Crystal Reports for Enterprise スケジュールサービス • Crystal Reports スケジュールサービス • Desktop Intelligence • 情報エンジンサービス • Live Office • Web Intelligence • Web Intelligence 共通サービス • Web Intelligence コアサービス • Web Intelligence 処理サービス
最新表示	オブジェクトのデータがユーザリクエストによってデータベースから更新されました。 • Crystal Reports キャッシュサービス • Crystal Reports for Enterprise スケジュールサービス • Crystal Reports スケジュールサービス • Desktop Intelligence • 情報エンジンサービス • Live Office • Web Intelligence • Web Intelligence 共通サービス • Web Intelligence コアサービス

イベント	
	• Web Intelligence 処理サービス
取得	オブジェクトがリポジトリから取得されました。 • セントラル管理サービス • Desktop Intelligence
権限の変更	ユーザ、グループ、またはオブジェクトのセキュリティ情報が変更されました。 • セントラル管理サービス
ロールバック	Lifecycle Manager によってオブジェクトが以前のバージョンに戻されました。 • ライフサイクルマネジメント
実行	ジョブが実行されました。 • 認証更新スケジュールサービス • Crystal Reports for Enterprise スケジュールサービス • Crystal Reports スケジュールサービス • Desktop Intelligence • 送信先への配信スケジュールサービス • LCM スケジュールサービス • ライフサイクルマネジメント • プラットフォーム検索スケジュールサービス • プローブスケジュールサービス • プログラムスケジュールサービス • パブリケーションスケジュールサービス • レプリケーションサービス • セキュリティクエリスケジュールサービス • ユーザとグループのインポートスケジュールサービス • Visual Difference スケジュールサービス • Web Intelligence スケジュールおよび公開サービス
保存	オブジェクトが更新または変更された後に保存されました。 • Analysis edition for OLAP • Crystal Reports キャッシュサービス • Crystal Reports for Enterprise スケジュールサービス • Crystal Reports スケジュールサービス • Crystal Reports 表示および変更サービス • Desktop Intelligence • 情報エンジンサービス • ライフサイクルマネジメント • Multi-Dimensional Analysis Service • SAP BusinessObjects Mobile • Web Intelligence • Web Intelligence 共通サービス

イベント	
	• Web Intelligence コアサービス • Web Intelligence 処理サービス
検索	検索が実行されました。 • 検索サービス • Explorer • ライフサイクルマネジメント
トリガ	ファイルイベントが呼び出されました。 • イベントサービス • セントラル管理サービス
表示	オブジェクトが表示されました。 • 分析アプリケーション • Analysis edition for OLAP • BI ラウンチパッド • BI ワークスペースアプリケーション • BI Commentary サービス • CMC • Crystal Reports キャッシュサービス • Crystal Reports 表示および変更サービス • Desktop Intelligence • 情報エンジンサービス • OpenDocument • SAP BusinessObjects Mobile • Web Intelligence • Web Intelligence 共通サービス • Web Intelligence コアサービス • Web Intelligence 処理サービス
VMS へ追加	オブジェクトが LCM バージョン管理システムに追加されました。 • ライフサイクルマネジメント
VMS へのチェックイン	オブジェクトが LCM バージョン管理システムにチェックインされました。 • ライフサイクルマネジメント
VMS からチェックアウト	オブジェクトが LCM バージョン管理システムからチェックアウトされました。 • ライフサイクルマネジメント
VMS エクスポート	リソースが VMS からエクスポートされました。 • ライフサイクルマネジメント
VMS ロック	VMS 内のリソースがロックされました。

イベント	
	• ライフサイクルマネジメント
VMS ロック解除	VMS 内のリソースがロック解除されました。 • ライフサイクルマネジメント
VMS から取得	オブジェクトが LCM バージョン管理システムから取得されました。 • ライフサイクルマネジメント
VMS 削除	オブジェクトが LCM バージョン管理システムから削除されました。 • ライフサイクルマネジメント

イベント (サービスタイプ別)

サービスタイプ	生成されるイベントのタイプ
分析アプリケーション	• 表示 • キューブへの接続
認証更新スケジュールサービス	• 配信 • 実行
Fiorified BI ラウンチパッド	ビュー
BI Commentary サービス	• 作成 • 削除 • ビュー • 変更 • 非表示
セントラル管理サービス	• 監査変更 • 作成 • カスタムアクセスレベルの変更 • 削除 • 配信 • ログオン • ログアウト • 変更 • 取得 • 権限の変更 • 呼び出し
セントラル管理コンソール	表示

サービスタイプ	生成されるイベントのタイプ
Crystal Reports スケジュールサービス	• 配信 • プロンプト • 最新表示 • 実行 • 保存
Crystal Reports キャッシュサービス	• プロンプト • 最新表示 • 保存 • 表示
Crystal Reports for Enterprise スケジュールサービス	• 配信 • プロンプト • 最新表示 • 実行 • 保存
Crystal Reports スケジュールサービス	• 配信 • プロンプト • 最新表示 • 実行 • 保存
Crystal Reports 表示および変更サービス	• 作成 • 保存 • 表示
Desktop Intelligence (クライアント)	• 配信 • プロンプト • 取得 • 実行
Desktop Intelligence スケジュールプロセス	• 配信 • 実行
送信先への配信スケジュールサービス	• 配信 • 実行
イベントサービス	トリガ
情報エンジンサービス	• 作成 • 範囲外のドリル • 編集 • ページの取得 • プロンプト • 最新表示

サービスタイプ	生成されるイベントのタイプ
	• 保存 • 表示
LCM スケジュールサービス	実行
LCM サービス	• 作成 • 削除 • LCM 設定 • 変更 • ロールバック • 実行 • 保存 • VMS へ追加 • VMS へのチェックイン • VMS からチェックアウト • VMS 削除 • VMS エクスポート • VMS ロック • VMS から取得 • VMS ロック解除 • 検索
Live Office	• プロンプト • 最新表示
Multi-Dimensional Analysis Service	• キューブへの接続 • MDAS セッション • 保存
OpenDocument	表示
プラットフォーム検索スケジュールサービス	• 配信 • 実行
プラットフォーム検索サービス	検索
プローブスケジュールサービス	• 配信 • 実行
プログラムスケジュールサービス	• 配信 • 実行
パブリケーションスケジュールサービス	実行
レプリケーションサービス	実行
SAP BusinessObjects Design Studio バージョン 1.3 以降	• ログオン • ログオフ

サービスタイプ	生成されるイベントのタイプ
セキュリティクエリスケジュールサービス	• 実行 • 配信
ユーザとグループのインポートスケジュールサービス	• 実行 • 配信
Visual Difference スケジュールサービス	実行
Web Intelligence アプリケーション	• 作成 • 範囲外のドリル • 編集 • 変更 • プロンプト • 最新表示 • 保存 • 表示
Web Intelligence 共通サービス	• 作成 • 範囲外のドリル • 編集 • ページの取得 • プロンプト • 最新表示 • 保存 • 表示
Web Intelligence コアサービス	• 作成 • 範囲外のドリル • 編集 • ページの取得 • プロンプト • 最新表示 • 保存 • 表示
Web Intelligence 処理サービス	• 作成 • 範囲外をドリル • 編集 • ページの取得 • プロンプト • 最新表示 • 保存 • 表示
Web Intelligence スケジュールおよび公開サービス	• 配信 • 実行

イベントのプロパティと詳細

BI プラットフォームに記録される各イベントには、イベントのプロパティと詳細のセットが含まれています。

イベントプロパティは常にイベントと一緒に生成されますが、その情報が特定のイベントに該当しない場合には、値なしで生成されます。ADS では、イベントプロパティはイベントを保存するテーブルに含まれており、レポート作成時に並べ替えやグループ化のために使用できます。

イベント詳細には、イベントのプロパティには含まれないイベントの追加情報が記録されます。イベント詳細が特定のイベントに該当しない場合、そのイベント詳細は生成されません。すべてのイベントタイプで生成 (該当する場合) される一連の共通イベント詳細があります。また、特定のイベントタイプについて生成される一連の追加イベント詳細もあります。たとえば、プロンプトイベントはプロンプトに入力された値をイベント詳細に記録しますが、他のイベントタイプでは、プロンプト値のイベント詳細は生成されません。ADS では、詳細は、親イベントにリンクしている個別のテーブルに保存されます。

場合によっては、イベントの詳細に複数の値が含まれることがあります。これらの詳細は、束 ID を使用してグループ化できます。束 ID に関する詳細については、関連トピックを参照してください。

多言語データ (オブジェクトやフォルダの名前など) は、監査 CMS のロケールのデフォルト言語で記録されます。

関連情報

Auditing Data Store Tables [1167 ページ]

24.3.1 Audit events and details

The following sections list all of the event types, followed by a description of any properties and event details that are unique to those events. At the beginning of the section is a list of the properties and details that are common to all event types.

> ⓘ 注記
>
> Some client programs do not have their own unique events, and rely on the common and platform events to capture relevant information about their operations.

Universal event Properties and Details

The following tables show what properties and event details are recorded for all events.

> ⓘ 注記
>
> The properties in this table are columns in the ADS_EVENT table in the Auditing Data Store.

Event Property	Description
Event_ID	A unique identifier for the event.
Client_Type_ID	Identifier for the type of application that performed the event
Service_Type_ID	Shows the ID of the type of service or application that triggered the event.
Start_Time	The start date and time when the event started (in GMT).
Duration	Duration of the event in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Session_ID	ID of the session during which the event was triggered.
Event_Type_ID	Type of event (for example, 1002 for view).
Status_ID	Records if the action succeeds or fails ("0" = succeeded, "1" = failed). Some events will have additional status types, these are detailed with the descriptions of those events.
Object_ID	CUID of the object affected (if applicable). CUID of the alerting event for Trigger events. **注記** All objects not saved in the CMS repository will have an ID of 0. These objects could be documents that have not yet been saved to the CMS database, or are stored locally on a client machine for example. You will need to use the Object_Name property to differentiate these objects.
User_ID	CUID of the User that performed the event.
User_Name	The user-name of the user the performed the event.
Object_Name	Name of the affected object (if applicable). Name of the alerting event for Trigger events.
Object_Type_ID	CUID of object type (for example document, folder, and so on).
Object_Folder_Path	Full folder path to where the affected object is located in the CMS repository. For example, `Sales/North America/East Coast`
Folder_ID	The CUID of the folder where the object is stored.
Top_Folder_Name	Name of the top level folder the affected object is stored in. For example, if object is located in `Sales/North America/East Coast` then the value would be `Sales`.
Top_Folder_ID	The CUID of the top level folder where the affected object is located. For example, if object is located in `Sales/North America/East Coast` then the value would be the CUID of the folder `Sales`.

Event Property	Description
Cluster ID	The CUID of the CMS cluster that recorded the event.
Action_ID	A unique identifier that can be used to tie together a sequence of events initiated by a single user action.

> **注記**
>
> The properties in this table are columns in the ADS_EVENT_DETAIL_TYPE_STR table in the Auditing Data Store.

Event Detail	ID	Description
Error	1	Only recorded if the action fails; the text of any error messages that result from the attempt.
Element ID	2	Name of an object that resides in a container object (Live Office document or Dashboard for example).
Element Name	3	ID generated for an object that resides in a container object (Live Office document or Dashboard for example).
Element Type ID	5	The type of object in a container object that is being viewed or modified. Only generated if applicable.
Parent Document ID	12	• For a document instance: the CUID of the parent document. • For parent documents: its own CUID.
Universe ID	13	CUID of the Universe used by the document or object. An event detail will be generated for each Universe if more than one is used.
Universe Name	14	The name of the Universe used by the document/object. An event detail will be generated for each Universe if more than one is used.
User Group Name	15	The user group name that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.
User Group ID	16	The user group ID that the user performing the action belongs to. If the user belongs to multiple groups. An event detail will be generated for each group.

Common Events

The following event types are common to all SAP BusinessObjects servers and clients.

View

User viewed a document / object.

- Event Type ID: 1002

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Container ID	32	The CUID of the container object (a dashboard, for example) that the object resides in (if applicable).
Container Type	33	The application type of the container for the object (if applicable).

> **注記**
>
> If you are using a search service then during document indexing you may notice a large number of View events generated by the "System Account" user. This is caused by the search indexing service opening documents in order to build the search index.

Refresh

An object was refreshed from the database.

- Event Type ID: 1003

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event. **注記** For View on Demand Crystal Reports this will be set to 0.
Number of Rows	63	The number of records the database server returned. **注記** For View on Demand Crystal Reports this will be set to 0.
Query	25	Records the SQL query used to refresh the data (optional, set in CMC).
Universe Object Name	31	The name of the universe the document or object uses. An event detail will be generated for each

Event Detail	ID	Description
		universe accessed by the document or object.
Document Scope	36	Records information on the intended scope of the document from its publishing settings (for example: Country=USA, Role=Manager). Only applicable to publishing workflows.
Publication Instance ID	37	ID of this instance of the publication. Only applicable to publishing workflows.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents.

Prompt

A value was entered for a prompt.

- Event Type ID: 1004

Event Detail	ID	Description
Prompt name	26	The name assigned to the prompt ("Date" for example). A separate detail will be generated for each prompt in a document or object, and they will be grouped.
Prompt value	27	The value entered for a prompt. A separate detail will be generated for each value entered. These can be grouped together and related back to the prompt name.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).
Publication Instance ID	37	ID of this instance of the publication. Only applies to publishing workflows.
Name at Design Time	90	The name of the Dashboards document at the time it was designed. This is only generated for Dashboards refreshes, or a Dashboards or Live Office document that includes a prompt.
Live Office Object Type	10701	Identifies the type of object that is being refreshed in a Live Office document (a Crystal report for example). This will only be generated for Live Office documents where the embedded object includes a prompt.

Create

User created an object.

- Event Type ID: 1005

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Overwrite	21	Records if the document or object is new or overwrites an existing object (0=New document or object, 1=overwrite of existing document or object).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open (0=No refresh, 1=Refresh on open). Only generated if applicable.
Description	24	Records any information in the document or object's description field.

Delete

User deleted an object.

- Event Type ID: 1006

Modify

User modified a file property or the file properties of an object.

- Event Type ID: 1007

Event Detail	ID	Description
Property Name	28	The name of the property that was modified. An event detail will be generated for each modified property.
Property Value	29	The new value for any modified property of the document or object. An event detail will be generated for each modified property.
Old Property Value	120	A user's old email address.
New Property Value	121	The same user's new email address.

Save

Saving or exporting a document or object locally, remotely, or to the CMS repository, in either its existing format or a different format.

- Event Type ID: 1008
- Statuses:
  - "0" indicates the object was successfully saved locally
  - "1" indicates the attempt failed

- "2" indicates the object was successfully saved or exported to a repository
- "3" indicates the object was successfully saved or exported to a new format

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was saved or exported.
File Name	18	The full name the document or object was saved under. If the file is saved locally by a client application, the name will also include the file path.
Overwrite	21	Records if the document or object is new or overwrites an existing file. "0"=New document or object, "1"=overwrite of existing document or object.
Format	22	Specifies the format of the document saved/exported, displayed as the common three-letter file extension ("doc" for a Microsoft Word file, or "pdf" for an Adobe PDF file, for example).
Refresh on Open	23	Records if the document or object is set to be automatically refreshed on open ("0"=No refresh, "1"=Refresh on open). Only recorded if applicable.

Search

A search was conducted.

- Event Type ID: 1009

Event Detail	ID	Description
Keyword	19	The keywords of the conducted search.
Category	20	Category used in the search (if applicable).
Number of Rows	63	The number of rows returned by the search.

Edit

User edited the content of an object.

- Event Type ID: 1010

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that is the subject of the event.
Query	25	If the edit modifies an SQL query, records the new query. (This setting is optional and can be selected in the CMC Auditing page.)

Event Detail	ID	Description
Universe Object Name	31	The name of the universe the document or object uses. A separate detail will be generated for each universe accessed by the document or object.
Container ID	32	The CUID of the container (a dashboard for example) that uses the object (if applicable).
Container Type	34	The application type of the container for the object (if applicable).
Container Folder Path	64	Folder path for the container of the object (if applicable).

Run

A job was run.

- Event Type ID: 1011
- Statuses:
  - "0" indicates the job was successful
  - "1" indicates the job failed
  - "2" indicates the job failed but will be reattempted
  - "3" indicates the job was cancelled

Event Detail	ID	Description
Size	17	Size of the document (in bytes) that was run.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager).

Deliver

An object was delivered.

- Event Type ID: 1012

Event Detail	ID	Description
Size	17	Size of the object (in bytes) that was delivered.
Destination Type	35	The destination of the document or object instance. For example, email, FTP, unmanaged disk, inbox, or printer.
Document Scope	36	Information on the intended scope of the document (for example: Country=USA, Role=Manager)
Publication Instance ID	37	ID of this instance of the document or object.

Event Detail	ID	Description
Domain	38	Records the SMTP server domain name for documents/objects distributed by email (if applicable).
Host Name	39	Records the name of the SMTP or FTP host for documents/objects distributed by email or FTP (if applicable).
Port	40	Records the SMTP or FTP server domain port for documents/objects distributed by email or FTP (if applicable).
From address	41	Records the sender's address for documents/objects distributed by email (if applicable).
To address	42	Records the recipient's address for documents/objects distributed by email (if applicable). Will also specify if the address is included in the To, CC, or BCC fields. An event detail will be generated for each intended recipient.
File Name	18	Records the file name of documents/objects distributed by email or FTP, or written directly to a disk that is not part of the Business Objects deployment.
Account Name	45	This records one of the following: • For *Inbox* delivered objects, a list of BusinessObjects user account names. • For *FTP* delivered objects, the FTP account name. • For *Unmanaged Disk* delivered objects, the login account used. • For *SMTP* delivered objects, the login account used for the SMTP server.
Printer Name	46	The name of the printer the document or object was delivered to (if applicable).
Number of copies	47	The number of copies of the document or object printed (if applicable).
Recipient Name	48	User name or names of the recipient or recipients of the document or object. An event detail will be generated for each intended recipient.
Alerting Event ID	92	The CUID of the Alerting event. This is generated only if the event was prompted by an alert.

Event Detail	ID	Description
Alerting Event Name	93	The name of the alerting event. This is generated only if the event was prompted by an alert.
Delivery Type	75	Indicates how the delivery was initiated: • "0" indicates scheduled • "1" indicates sent to a destination • "2" indicates published • "3" indicates an alert was triggered

Retrieve

An object is retrieved from the CMS.

- Event Type ID: 1013

Logon

A user logs on.

- Event Type ID: 1014
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "1" indicates a failed logon attempt
  - "2" indicates a named-user license logon was successful
  - "3" indicates a non-user (system) login was successful
- Event Type ID: 123
- Statuses:
  - "0" indicates a concurrent-user license logon was successful
  - "2" indicates a named-user license logon was successful

Event Detail	ID	Description
Concurrent User Count	50	The number of users on the system at the time the event was triggered.
Client hostname reported by client	51	Hostname of client as reported by client.
Client hostname resolved by server	52	Hostname of client as resolved by server. If the client hostname cannot be resolved, no value is recorded.
Client IP address reported by client	53	IP address of client as reported by the client.
Client IP address resolved by server	54	IP address of client as resolved by the server. If the client IP cannot be resolved, no value is recorded.
Authentication Type	122	Authentication type is valid for the vlaues secEnterprise, secLDAP, secWinAD, secSAPR3
User Type	123	Type of the user.
Session Count	125	Count of the session is recorded.
Tenant ID	126	The ID of the tenant is recorded.

Event Detail	ID	Description
Concurrent Tenant Session	127	The count of the concurrent session of the tenant is recorded.

Logout

A user logs off.

- Event Type ID: 1015

Event Detail	ID	Description
Concurrent User Count	50	The number of concurrent users on the system at the time the event was triggered.

Trigger

A file event is triggered.

- Event Type ID: 1016

Event Detail	ID	Description
File Name	18	The name of the file that was being monitored and triggered the event.

24.3.1.1 プラットフォームイベント

以下のイベントは BI プラットフォームに特有のイベントです。

権限の変更

オブジェクトの権限が変更されました。

- イベントタイプ ID: 10003

イベントの詳細	ID	説明
追加された権限	55	追加された権限のタイプ、新しい権限の範囲 (対象オブジェクト) およびそれが適用されるオブジェクトタイプ。情報は次の例に従って構造化されます。 `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`
削除された権限	56	削除された権限のタイプ、新しい権限の範囲 (対象オブジェクト) およびそれが適用されるオブジェクトタイプ。情報

イベントの詳細	ID	説明
		は次の例に従って構造化されます。 `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`
変更された権限	57	変更された権限のタイプ、新しい権限の範囲 (対象オブジェクト) およびそれが適用されるオブジェクトタイプ。情報は次の例に従って構造化されます。 `modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`
主体	118	セキュリティ権限を変更されたユーザまたはユーザグループ (主体) の ID
主体名	119	セキュリティ権限を変更されたユーザまたはユーザグループ (主体) の名前

カスタムアクセスレベルの変更

カスタムアクセスレベルが変更されました。

- イベントタイプ ID: 10004

イベントの詳細	ID	説明
追加された権限	55	追加された権限のタイプ、新しい権限の範囲 (対象オブジェクト) およびそれが適用されるオブジェクトタイプ。情報は次の例に従って構造化されます。 `added right=Export; new value=Granted; scope=Current object; applicable object type=all object types`
削除された権限	56	削除された権限のタイプ、新しい権限の範囲 (対象オブジェクト) およびそれが適用されるオブジェクトタイプ。情報は次の例に従って構造化されます。 `removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types`

イベントの詳細	ID	説明
変更された権限	57	変更された権限のタイプ、新しい権限の範囲 (対象オブジェクト) およびそれが適用されるオブジェクトタイプ。情報は次の例に従って構造化されます。`modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types`
主体	118	セキュリティ権限を変更されたユーザまたはユーザグループ (主体) の ID

監査変更

システムの監査設定が変更されました。

- イベントタイプ ID: 10006

イベントの詳細	ID	説明
イベントの種類の ID	58	有効化または無効化された監査イベントタイプの ID を記録します。一度のアクションで複数のイベントタイプが有効化または無効化された場合、イベントの詳細はイベントタイプごとに生成されます。
アクション	59	有効化または無効化された監査イベントを記録します。
新しい監査レベル	60	詳細の監査レベルが変更された場合に、新しいレベル設定 (オフ、最小、またはデフォルトなど) を記録します。
以前の監査レベル	61	詳細の監査レベルが変更された場合に、以前のレベル設定 (オフ、最小、またはデフォルトなど) を記録します。
監査オプション	62	オプショナルの詳細が有効化または無効化された場合に、変更された詳細および有効化または無効化のどちらが実行されたかを記録します。一度のアクションで複数の詳細が有効化または無効化された場合、詳細レコードは変更された詳細ごとに作成されます。
ADS 接続	78	監査データストアへの接続が変更された場合に、次の形式を使用して新しい接続設定を記録します。`DBType=Oracle,DBName=MyADS,Username=USR1,Password="******",SSO=off,DBReconnect=`

イベントの詳細	ID	説明
		on 変更された詳細のみが記録されます。たとえば、ユーザ名のみが更新された場合は、`Username="new"` のみが記録されます。 **注記** データベースでは、パスワード情報は常に * で表示されます。
自動削除間隔	105	この詳細は、CMC の監査ページで [より古いイベントを削除する] フィールドへの変更を記録します。これにより、監査情報を ADS で維持する日数を管理します。

24.3.1.2 Commentary のイベント

次の権限は、Business Intelligence プラットフォームの **BI Commentary** に固有です。

コメントの追加

このイベントは、新しいコメントを追加したとき、コメントを複製したとき、および一括でコメントを作成したときに生成されます。コメントを追加するときには、親ドキュメント ID のみが記録されます。コメントの複製や一括追加の場合は、次の表に示すイベント詳細がすべて記録されます。

イベントタイプ ID: 11001

イベントの詳細	ID	説明
親ドキュメント ID	12	オブジェクトの ID を記録します。
説明	24	イベントの追加情報がある場合はそれを記録します。
サイズ	17	イベントの対象となるオブジェクトのサイズ (バイト)
ファイル名	18	オブジェクトのファイル名を記録します。

コメントの取得

このイベントは、コメントを表示すると生成されます。

イベントタイプ ID: 11002

イベントの詳細	ID	説明
親ドキュメント ID	12	オブジェクトの ID を記録します。
サイズ	17	イベントの対象となるオブジェクトのサイズ (バイト)

コメントの変更

このイベントは、既存のコメントを編集すると生成されます。

イベントタイプ ID: 11003

イベントの詳細	ID	説明
親ドキュメント ID	12	オブジェクトの ID を記録します。

コメント削除

このイベントは、既存のコメントを削除すると生成されます。

イベントタイプ ID: 11004

イベントの詳細	ID	説明
親ドキュメント ID	12	オブジェクトの ID を記録します。

コメントの非表示

このイベントは、コメントを非表示にすると生成されます。

イベントタイプ ID: 11005

イベントの詳細	ID	説明
親ドキュメント ID	12	オブジェクトの ID を記録します。

24.3.1.3 SAP BusinessObjects Web Intelligence のイベント

以下のイベントは、SAP BusinessObjects Web Intelligence コンポーネントに特有のイベントです。

範囲外のドリル

ユーザがレポートの範囲外をドリルしました。

- イベントタイプ ID: 10201

イベントの詳細	ID	説明
オブジェクトインスタンス	11	イベントがスケジュールされた更新の結果であるかユーザによるオブジェクトの表示の結果であるかを記録します ("0" = ユーザによるオブジェクト表示の結果、"1" = スケジュールされたオブジェクトの最新表示の結果)。
行数	63	データベースサーバが返した行数。
クエリ	25	データの最新表示に使用されたクエリを記録します (オプションで CMC に設定)。
ユニバースオブジェクトの名前	31	ドキュメントが使用するユニバースの名前。ドキュメントがアクセスするユニバースごとにインスタンスが記録されます。
ユニバース ID	32	ドキュメントが使用するユニバースの CUID。ドキュメントがアクセスするユニバースごとにインスタンスが記録されます。

ページの取得

Web Intelligence ドキュメントのページが取得されました。

- イベントタイプ ID: 10202

イベントの詳細	ID	説明
WebIntelligence レポート名	10220	表示した WebIntelligence ドキュメントレポートの名前を記録します。
出力タイプ	10221	表示されたドキュメントの出力形式です。例: • `xml.ro` (WebIntelligence) • `pdf` (Adobe Acrobat) • `xls` (Microsoft Excel) • `text/xml` (不明な場合)
ページ番号	10222	表示された WebIntelligence レポートページの番号を記録します。 NB: • "0" は取得できない場合 (例: pdf) • "-1" はエラーの場合

BW 統計

> **注記**
>
> これらの監査イベントは SAP BW に直接送信されます。下で参照用に Web Intelligence イベントとして一覧表示されますが、BI プラットフォームの監査データストアには格納されません。4.2 SP03 以降で利用できます。

オプション	指定できる値	説明

ロングネーム
`sap.sal.bics.postBWstatistics`
ショートネーム
`postBWstatistics`
デフォルト値: `false`
	`true`
	`false`
		以下の BW 統計イベントを有効化します。
		• 20100: BEx の特性メンバーをフェッチします。
		• 20101: BEx クエリの結果をフェッチします。
		• 20102: BEx 変数を送信します。
		• 20103: BICS API を使用して BEx クエリを開きます。
		• 20104: BW と同期化します。
		• 20105: 変数の入力文字列を設定します。

24.3.1.4 SAP BusinessObjects Analysis, edition for OLAP のイベント

MDAS セッション

MDAS セッション操作が実行されます。

- イベントタイプ ID: 10300
- ステータス:
  - "0" = 新しいセッションは正常に開きました。
  - "1" = 新しいセッションは失敗しました。
  - "2" = 既存のセッションは終了しました。

MDAS キューブ接続

キューブ接続操作が実行されます。

- イベントタイプ ID: 10301
- ステータス:
  - "0" = 新しい接続は正常に開きました。
  - "1" = 新しい接続は失敗しました。
  - "2" = 既存の接続は終了しました。

イベントの詳細	ID	説明
接続 ID	94	接続の一意の ID
接続名	95	接続の名前
プロバイダタイプ	96	キューブのプロバイダのタイプ
キューブ名	97	使用されるキューブのフルネーム

24.3.1.5 SAP BusinessObjects プロモーションマネジメントコンソールのイベント

以下は、SAP BusinessObjects プロモーションマネジメントのコンポーネントに固有のイベントです。

SAP BusinessObjects プロモーションマネジメントツールに共通の詳細

すべてのプロモーションマネジメントイベントに、以下のイベント詳細が追加されます。

イベントの詳細	ID	説明
要素クラスタ	6	プロモーションマネジメントツールが複数の異なるクラスタに置かれているオブジェクトに対して操作を実行する場合に影響を受けるクラスタの CUID。影響を受けるクラスタごとにイベントの詳細が生成されます。
要素コメント	7	オブジェクトの追加情報。
プライマリ要素	8	この詳細は、プライマリ要素の場合は "1" に、従属要素の場合は "0" に設定されます。
要素ステータス	9	この詳細は、操作の要素が失敗した場合は "1" に、それ以外の場合は "0" に設定されます。
操作	10	実行される操作のタイプを説明します (追加、削除、変更など)。

SAP BusinessObjects プロモーションマネジメントツールの設定

プロモーションマネジメントの設定が変更されました。

- イベントタイプ ID: 10900

イベントの詳細	ID	説明
設定	100	プロモーションマネジメントツールの設定を表示します。 設定は、カンマ区切りの値のペアとして表示されます。例: ロールバック設定 =enabled, ポート =900
変更前の設定	101	プロモーションマネジメントツールのオブジェクトの設定が変更された場合に、以前の設定を記録します。 設定と同じ形式を使用します。
変更後の設定	102	プロモーションマネジメントツールのオブジェクトの設定が変更された場合に、新しい設定を記録します。 設定と同じ形式を使用します。
VMS タイプ	10900	バージョン管理システムのタイプ

ロールバック

オブジェクトがバージョン管理システム (VMS) の以前のバージョンにロールバックされました。

- イベントタイプ ID: 10901

VMS へ追加

リソースが VMS に追加されました。

- イベントタイプ ID: 10902

イベントの詳細	ID	説明
バージョン	104	バージョン管理システムにドキュメントのバージョン番号を記録します。

VMS から取得

リソースが VMS から取得されました。

- イベントタイプ ID: 10903

イベントの詳細	ID	説明
削除済みオブジェクトの復元	103	取得したオブジェクトがシステムから削除されたかどうかを示します。 "0" はオブジェクトが削除されていないことを示し、"1" はオブジェクトが削除されたことを示します。
バージョン	104	VMS にドキュメントのバージョン番号を記録します。

VMS へのチェックイン

リソースが VMS へチェックインされました。

- イベントタイプ ID: 10904

イベントの詳細	ID	説明
バージョン	104	VMS にドキュメントのバージョン番号を記録します。

VMS からチェックアウト

リソースが VMS からチェックアウトされました。

- イベントタイプ ID: 10905

イベントの詳細	ID	説明
バージョン	104	VMS にドキュメントのバージョン番号を記録します。

VMS エクスポート

リソースが VMS からエクスポートされました。

- イベントタイプ ID: 10906

イベントの詳細	ID	説明
バージョン	104	VMS にドキュメントのバージョン番号を記録します。

VMS ロック

ユーザがリソースを編集できないように、VMS 内でリソースがロックされました。

- イベントタイプ ID: 10907

イベントの詳細	ID	説明
バージョン	104	VMS にドキュメントのバージョン番号を記録します。
ロックしたユーザ	10901	このアクションを実行したユーザの名前。

VMS ロック解除

ユーザがリソースを編集できるように、VMS 内でリソースがロック解除されました。

- イベントタイプ ID: 10908

イベントの詳細	ID	説明
バージョン	104	VMS にドキュメントのバージョン番号を記録します。
ロック解除したユーザ	10902	このアクションを実行したユーザの名前。

VMS 削除

リソースが VMS から削除されました。

- イベントタイプ ID: 10909

イベントの詳細	ID	説明
バージョン	104	バージョン管理システムにドキュメントのバージョン番号を記録します。

25 イベント

25.1 イベントについて

イベントは、サーバ上で発生するイベントやアクションに関する情報を提供するフラグやチェックポイントと似ています。イベントベースのスケジュールを使用すると、オブジェクトのスケジュールをより詳細に制御できます。指定した特定のイベントが発生した後にのみオブジェクトが処理されるように、イベントを設定できます。

CMC で使用できるイベントの一覧は以下のとおりです。

Crystal Report イベント

Crystal Report イベントでは、イベントで待機中のレポートがすでにスケジュールされていて実行可能である場合にのみ、レポート実行がトリガされます。Crystal Report イベントのベースとしてを新しいファイルを使用し、イベントのトリガを待機するようにレポートをスケジュールすることができます。

カスタムイベント

カスタムイベントは、"手動イベント" とも呼ばれます。それぞれのカスタムイベントには、イベント名と対応する説明、の 2 つのプロパティがあります。カスタムイベントは、ユーザの BI 受信ボックスとユーザの電子メール ID へのアラートをトリガするために使用されます。カスタムイベントでは、必要な条件を設定することによって、イベントのトリガに基づいたオブジェクトのスケジュールを作成するオプションも提供されます。

モニタリングイベント

モニタリングイベントは、サービスのヘルスステータスに関連するシステム生成イベントです。モニタリングは、CMC に組み込まれているアプリケーションで、管理者はシステムの健全性をモニタリングできます。モニタンリングの最も重要なアスペクトは、監視とプローブです。

監視では、250 を超えるメトリクスのしきい値をシステム内に設定できます。設定したしきい値を超えると、通知が発行されます。

> 例
>
> Output FRS で消費されるディスク領域をモニタリングする監視がある場合、消費量が指定したディスク領域の値に達すると、通知が発行されます。

システムイベント

システムイベントには、次の 2 種類があります。

- ファイルベースのイベント
  ファイルベースのイベントは、パスの下に置かれている任意のファイルがベースとなります。たとえば、ファイルが複数のサーバパスの 1 つに置かれている場合、そのファイルのパスをベースとしてスケジュールすることによって、レポートを実行できます。ビジネス上の観点から、レポートに必要なテーブルを月次/週次/日次ベースでロードすることを考慮する場合、ロードしたレポートでファイルベースのシステムイベントがトリガされた後で、テキストファイルをパスの下に置きます。
- スケジュールベースのイベント
  スケジュールベースのイベントは、レポートまたは BI オブジェクトを順次的に実行するために使用します。このイベント定義には、成功、失敗、および成功/失敗 の 3 つのアクションが含まれます。これは、指定された時点での実行中オブジェクトのステータスは成功か失敗のいずれかであると考えられるためです。

ユーザ通知

ユーザ通知イベントは、BI ラウンチパッドを使用している BI エンドユーザに重要なイベントに関する通知を発行するために、管理者が使用します。管理者は、スケジュールした時間 (たとえば、システム停止時間) に、選択したユーザに対して、重要なメッセージと他の関連情報を通知することができます。アラートメッセージは、ユーザがログオンすると、通知ポップアップとして BI ラウンチパッド画面に表示されます。

BW イベント

BW システムでは、[*BOE トリガイベント*] という BW プロセスチェーンのプロセスタイプによって、BI プラットフォームの BW イベントがトリガされます。各 BW イベントは、イベント名とその説明で構成されます。BW イベントは、BW データソースに基づくレポートのイベントベースのスケジュールを設定するために使用されます。システム内のデータが変更されたときに、BW システムによって BW イベントがトリガされます。BW イベントで、ユーザの BI 受信ボックスおよび電子メール ID 宛のアラートをトリガすることもできます。

25.1.1 ユーザ通知

管理者は通知機能を使用して、CMC からユーザにアラートメッセージを送信することができます。管理者は、この機能を使用して、(たとえば、システム停止時間) に、選択したユーザに対して、重要なメッセージと他の関連情報を通知することができます。アラートメッセージは、ユーザがログオンすると、通知ポップアップとして BI ラウンチパッド画面の右上隅に表示されます。

25.1.1.1 通知イベントの作成

通知イベントは、スケジュール可能なプラグインです。新しい通知イベントの作成時に、管理者は '開始' と '終了' の日時を指定する必要があります。指定した通知 '開始' 日時になると、スケジュールを担う Adaptive Job Server (AJS) で、スケジュールインスタンスが作成されます。次に、AJS からラウンチパッドのアラート受信ボックスにアラートがプッシュされます。これらの通知は、BI ラウンチパッド画面の右上隅に表示されます。

通知イベントを作成するには、次の手順を実行します。

1. CMC にログオンします。
2. CMC のホームページで、ドロップダウンメニューから [イベント] を選択します。
3. 左側の [イベント] ペインで、[ユーザ通知] を右クリックし、[新規] > [新しい通知] を選択します。

   [新しい通知] ポップアップウィンドウが表示されます。
4. 通知メッセージをスケジュールするには、次の手順を実行します。
   a. [タイムゾーン] ドロップダウンメニューから、該当するタイムゾーンを選択します。
   b. 該当する [開始日時] を設定します。
   c. 該当する [終了日時] を設定します。

   > **注記**
   >
   > - [終了] 時刻を [開始] 時刻より早くすることはできません。
   > - [開始] 時と [終了] 時との差は 14 日間までに制限されています。
   > - 選択したタイムゾーンとは無関係に、[開始] 時刻を CMS サーバ時刻より早くすることはできません。[開始] 時刻が CMS サーバ時刻より早いと、通知はトリガされません。

   d. [通知タイトル] ボックスに、通知のタイトルを入力します。

   > **注記**
   >
   > [通知タイトル] の長さは 256 文字までに制限されています。

   e. [説明] ボックスに、通知に適した説明を入力します。

   > **注記**
   >
   > [説明] の長さは 1024 文字までに制限されています。

   > **注記**
   >
   > 通知がユーザの電子メールに送信されるようにするには、[このメッセージを通知としてユーザ電子メール *ID* に送信] チェックボックスを選択します。
5. [*OK*] を選択します。

これで、通知イベントが正常に作成されました。

> **注記**
>
> [通知プロパティ] ページで、作成時刻および変更時刻は CMS サーバ時刻を反映しています。
>
> 管理者は BI ラウンチパッドでの通知バナーの自動ポップアップを無効にすることができます。これを行うには、`BIlaunchpad.properties` ファイルを修正し、`Notification.enabled` フィールドを `false` に設定

することによってポーリングを無効にします。通知ポーリングをデフォルトで使用するには、`global.properties` ファイルの `pinger.enabled` プロパティを有効にする必要があります。ポーリングと警告が有効ではない場合、通知ポップアップが表示されるのは、ユーザがページを最新表示した場合、初回にログインした場合、または通知が有効であるときに再ログインした場合に限られます。

ポーリングは BI ラウンチパッドで 3 分ごとに行われます。

25.1.1.2 通知対象読者の選択

通知機能によって、作成するすべての通知に対して必要な対象読者を選択することができます。

通知の対象読者を選択するには、以下の手順を実行します。

1. 作成した通知を右クリックし、コンテキストメニューから [購読者の管理] を選択します。

   [購読者の管理] ポップアップウィンドウが表示されます。
2. [受信者一覧] ペインから、[追加] を選択します。

   [購読者の追加] ポップアップウィンドウが表示されます。
3. 通知を送信するユーザ/ユーザグループを選択します。
4. [デフォルト購読の追加] を選択します。

   [購読者の追加] ポップアップウィンドウが表示されなくなります。
5. [購読者の管理] ポップアップウィンドウから、[保存して終了] を選択します。

これで、通知を送信する読者を正常に選択することができました。

> ⓘ 注記
>
> - 通知がトリガされた後は、購読一覧を変更することはできません。
> - 通知を OpenDocument ユーザに送信することが可能になりました。

25.1.1.3 通知イベントの編集

通知イベントを編集するには、次の手順を実行します。

1. CMC にログオンします。
2. CMC のホームページで、ドロップダウンメニューから [イベント] を選択します。
3. 左側の [イベント] ペインで、[ユーザ通知] を選択します。
4. 編集する通知を右クリックして、コンテキストメニューから [イベントの編集] を選択します。

   イベントの編集ダイアログボックスが表示されます。
5. 通知イベントの該当するパラメータを編集します。

   > ⓘ 注記
   >
   > 通知イベントの以下のパラメータを編集することができます。

- タイムゾーン
- 開始日時
- 終了日時
- 通知タイトル
- 説明
- 購読者の管理

6. [*OK*] を選択します。

これで、通知イベントが正常に編集されました。

> **注記**
>
> イベント > ユーザ通知 > プロパティ を選択して通知イベントを編集した場合、[イベントの編集] ページで [*OK*] を選択しない限り、通知はトリガされません。

26 プラットフォーム検索

26.1 プラットフォーム検索について

プラットフォーム検索を使用すると、ユーザは BI プラットフォームリポジトリ内のコンテンツを検索できます。このツールは、検索結果をカテゴリにグループ化し、関連の高い順に順位を付けて、検索結果の絞り込みを行います。

このバージョンの BI プラットフォームのプラットフォーム検索には、以下の機能があります。

- BI プラットフォームコンテンツの検索
- 既存のドキュメントが見つからない場合、ドキュメント作成用のクエリの提案
- 継続的なインデックス処理とスケジュールベースのインデックス処理の両方のサポート
- クラスタ環境におけるインデックス処理のサポート
- インデックス処理のレベルの設定および変更
- 高度な検索設定オプションの提供
- 多言語検索およびインデックス処理のサポート
- 高度な検索構文の提供
- メタデータファセット、コンテンツファセット、動的ファセットのサポート
- システム負荷に応じたセルフヒーリングのサポート

> ⓘ 注記
>
> 旧バージョンから新バージョンに移行する場合、インデックスは移行されません。

26.1.1 プラットフォーム検索 SDK

プラットフォーム検索では、クライアントアプリケーションとプラットフォーム検索間のインタフェースとして機能する、公開 SDK もサポートされています。公開されているこのインタフェースは、検索サービスをカスタマイズしてお使いのアプリケーションと統合するのに役立ちます。

検索要求パラメータがクライアントアプリケーションから SDK レイヤに送信されると、SDK レイヤが要求パラメータを XML にエンコードされた形式に変換し、プラットフォーム検索サービスに渡します。

プラットフォーム検索 API に関する詳細については、*Business Intelligence* プラットフォーム *Java API* リファレンスを参照してください。

26.1.2 クラスタ環境

プラットフォーム検索では、クラスタ環境における複数のノードで負荷を共有できます。クラスタ環境でのデプロイメントにより、システムリソースが最適化され、サーバパフォーマンスが改善します。

プラットフォーム検索は、検索機能とインデックス処理機能の両方について、水平クラスタリングと垂直クラスタリングの両方をサポートしています。クラスタ環境では、検索プロセスとインデックス処理プロセスの両方のパフォーマンスが最適化されます。

クラスタ環境内でプラットフォーム検索インデックスの場所を設定する方法の詳細については、この SAP ノートを確認してください。

負荷分散

プラットフォーム検索は、インデックス処理と検索の両方の負荷分散をサポートします。クラスタ環境では、インデックス処理および検索要求を複数のノードで実行し、負荷を共有することができます。各ノードは独立して機能し、コンテンツのインデックス処理とデルタインデックスの作成を行います。ただし、クラスタ内の 1 つのノードのみがマスタインデックスとして動作し、デルタインデックスをマスタインデックスにマージします。すべてのノードが、マスタインデックスにアクセスできます。これにより、同時検索要求が可能になります。

フェールオーバー

このフェイルオーバーメカニズムにより、ユーザは検索を続行することができ、インデックス操作を中断することなく使用できます。技術的なエラーまたは保守関連アクティビティが原因でクラスタにおける 1 つのノードが利用できなくなると、別のノードが自動的にインデックス処理および検索要求を処理します。

26.2 プラットフォーム検索の設定

26.2.1 OpenSearch のデプロイ

プラットフォーム検索では、OpenSearch 標準がサポートされ、クライアントアプリケーションは OpenSearch 標準またはフォーマットを使用してプラットフォーム検索と通信できます。OpenSearch は、デフォルトでは、SAP BusinessObjects Business Intelligence スイートにはインストールされていないため、ユーザは、個別の WAR ファイル (`opensearch.war`) として Tomcat などのアプリケーションサーバに手動で、または WDeploy ツールを使用してデプロイする必要があります。このファイルは、インストーラによって `<INSTALLDIR>¥warfiles¥OpenSearch` ディレクトリにコピーされます。

> **注記**
>
> クライアントプログラムは、OpenSearch 標準に従ってプラットフォーム検索と通信する必要があります。

> **注記**
>
> BI プラットフォームをインストールすると、デフォルトで Tomcat アプリケーションサーバがインストールされます。

26.2.1.1 手動によるデプロイ

BI プラットフォーム環境に OpenSearch を実装するには、次の手順を実行する必要があります。

1. 以下の場所に移動します。`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥`
2. `<INSTALLDIR>¥tomcat¥webapps¥` に OpenSearch フォルダをコピーします。
3. 以下のように、`¥OpenSearch¥WEB-INF¥config.properties` ファイルの構成パラメータを変更します。
   - CMS: CMS 名とポート番号: `<CMS Name>:<Port Number>`
   - OpenDocURL: OpenDocument アプリケーションの URL: `http://<tomcathost>:<connector port>/BOE/OpenDocument/opendoc/openDocument.jsp`
   - Proxy.rpurl: リバースプロキシを使用する場合は、リバースプロキシサーバの名前が必要です。
   - Proxy.opendoc.rpurl: リバースプロキシを使用する場合は、OpenDoc リバースプロキシサーバの名前が必要です。
4. Tomcat アプリケーションサーバを再起動して OpenSearch をデプロイします。

26.2.1.2 WDeploy を使用したデプロイメント

Windows では、コマンドは `wdeploy.bat <parameters>` と表されます。 UNIX では、コマンドは `wdeploy.sh <parameters>` と表されます。

1. `<InstallDir>¥SAP BusinessObjects Enterprise XI 4.0¥wdeploy¥conf` に格納された `config.<ApplicationServer>` ファイルを、必要な Web アプリケーションサーバパラメータ (インストールディレクトリ、インスタンス名、管理者ポート、管理者ユーザ名、管理者パスワードなど) を使用して更新します。
2. `<InstallDir>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥OpenSearch¥WEB-INF¥config.properties` ファイルの以下のパラメータを変更します。
   a. `CMS` パラメータに対し、`<CMSName>:<Port>` を入力します。
   b. `OpenDocURL` パラメータに対し、OpenDocument アプリケーションの URL を入力します。

      URL は、`http://<WebApplicationServerHost>:<ConnectorPort>/BOE/OpenDocument/opendoc/openDocument.jsp` にする必要があります。
   c. (リバースプロキシに必要) `Proxy.rpurl` パラメータに対し、リバースプロキシサーバ名を入力します。
   d. (リバースプロキシに必要) `Proxy.opendoc.rpurl` パラメータに対し、OpenDocument アプリケーションのリバースプロキシサーバ名を入力します。
3. 以下を実行します。`wdeploy.bat <WebApplicationServer> -Dapp_source_tree=<ParentFolderOpenSearchWebApp> -DAPP=OpenSearch deploy` コマンド (`<InstallDir>¥SAP BusinessObjects Enterprise XI 4.0¥wdeploy` から)
   たとえば、次のコマンドは、WebSphere 7 Web アプリケーションサーバに OpenSearch をデプロイします。

   ```
   wdeploy.bat websphere7 -Dapp_source_tree="<InstallDir>¥SAP BusinessObjects
   Enterprise XI 4.0¥warfiles" -DAPP=OpenSearch deploy
   ```
4. Web アプリケーションサーバを再起動します。

26.2.2 リバースプロキシの設定

リバースプロキシサーバの背後にある Web アプリケーションサーバに Web アプリケーションをデプロイするには、受信 URL リクエストを正しい WAR ファイルにマップするように、リバースプロキシサーバを設定します。

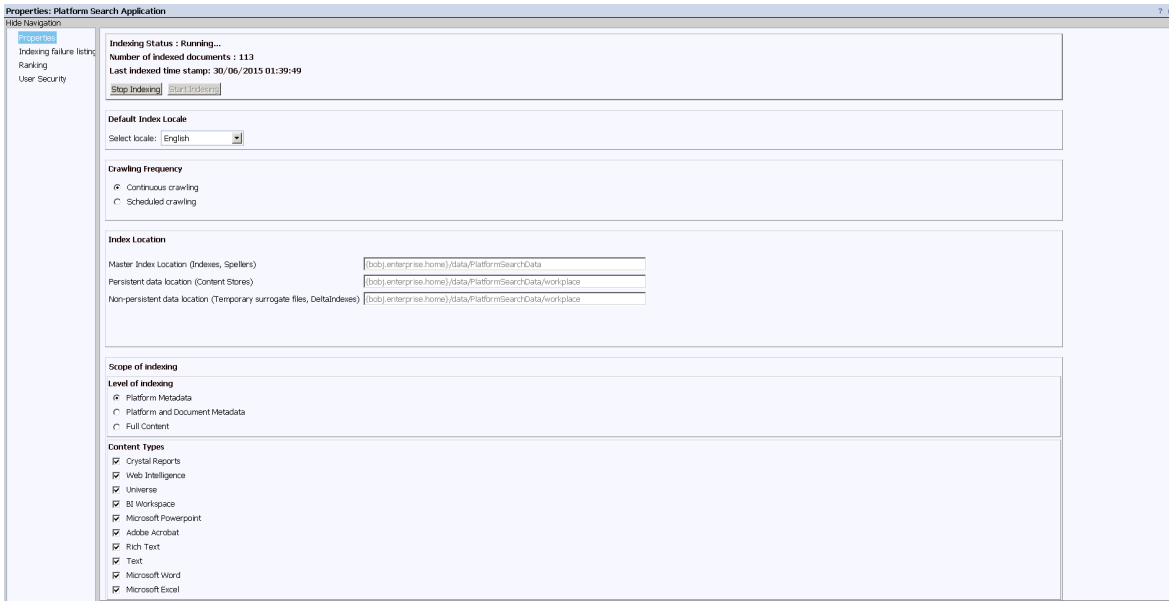
設定の手順を説明するため、ここでは例として Apache 2.2 リバースプロキシサーバを使用します。OpenSearch 用に Apache 2.2 リバースプロキシサーバを設定するには、次の手順を実行します。

1. リバースプロキシをセットアップし、OpenSearch の `WEB-INF¥config.properties` ファイルを変更します。
2. 以下のコンテキストパラメータを有効にし、その値を変更します。
   - `proxy.rpurl`: OpenSearch のリバースプロキシ URL (`http://machineIPAddress/RP/OpenSearch/` など)
   - `proxy.opendoc.rpurl`: Open Doc のリバースプロキシ URL (`http://machineIPAddress/RP/BOE/` など)
3. Apache リバースプロキシインストールフォルダの下にある `httpd.conf` ファイルを、次の設定で更新します。
   - `ProxyPass /RP/BOE/OpenDocument/ http://<Tomcat host>:<Connector Port>/BOE/OpenDocument/`
   - `ProxyPass /RP/OpenSearchRP/ http://<Tomcat host>:<Connector Port>/OpenSearch/`
   - `ProxyPassReverseCookiePath /BOE /RP/BOE`
   - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`
4. Apache 2.2 リバースプロキシサーバを再起動します。

26.2.3 CMC でのアプリケーションプロパティの設定

プラットフォーム検索アプリケーションプロパティを設定するには、次の手順に従います。

1. CMC の [アプリケーション] エリアを表示します。
2. [プラットフォーム検索アプリケーション] を選択します。
3. 管理 > プロパティ をクリックします。[プラットフォーム検索アプリケーションプロパティ] ダイアログボックスが表示されます。



4. プラットフォーム検索の設定を、以下のとおりに行います。

オプション	説明
検索統計	プラットフォーム検索は、以下の検索統計を提供します。 • インデックス処理のステータス: インデックス処理プロセスのステータスを示します。 • インデックス済みドキュメント数: インデックス処理されたドキュメントの数を表示します。 • 前回インデックス処理タイムスタンプ: ドキュメントが最後にインデックス処理されたときのタイムスタンプを表示します。
インデックス処理の停止/開始	[インデックス処理の開始] または [インデックス処理の停止] オプションにより、継続的クロールからスケジュール済みクロールへ切り替える場合、またはメンテナンス目的で、インデックス処理プロセスを開始または停止することができます。 インデックス処理を停止するには、[インデックス処理の停止] をクリックします。
デフォルトのインデックスロケール	プラットフォーム検索では、CMC で指定したロケールを使用して、すべてのローカライズされていない BI ドキュメントをインデックス処理します。ドキュメントがローカライズされると、対応する言語のアナライザがインデックス処理に使用されます。 検索はクライアントの製品ロケールに基づいて行われます。クライアントの製品ロケールには加重が適用されます。 CMC の設定プロパティでこの加重を設定できます。

オプション	説明
クロール頻度	以下のオプションを使用して、BI プラットフォームリポジトリ全体をインデックス処理することができます。 • 継続的クロール: このオプションを使用すると、インデックス処理は継続的に行われ、オブジェクトが追加、変更、または削除されるたびにリポジトリがインデックス処理されます。これにより、最新の BI プラットフォームコンテンツを表示または処理できます。デフォルトの設定で、リポジトリは、実行するアクションによって継続的クロールにより継続的に更新されます。継続的クロールは、ユーザの操作なしに動作し、ドキュメントのインデックス処理にかかる時間を短縮します。 • スケジュール済みクロール: このオプションを使用すると、インデックス処理は、スケジュールオプションで設定されたスケジュールに基づきます。 オブジェクトをスケジュールする方法については、*SAP BusinessObjects Business Intelligence プラットフォーム CMC* オンラインヘルプのプラットフォーム検索のオブジェクトのスケジュールの節を参照してください。 **注記** • [スケジュール済みクロール] を選択し、[繰り返し] に [今すぐ] 以外のオプションを設定した場合は、ドキュメントの次回のインデックス処理がスケジュールされると、プラットフォーム検索によって日時のタイムスタンプが表示されます。 • [スケジュール済みクロール] を選択した場合は、[インデックス処理の開始] ボタンが有効になり、[インデックス処理の停止] ボタンは無効になります。 • スケジュールの設定が完了すると、[インデックス処理の停止] ボタンは無効になります。

オプション	説明
インデックスの場所	インデックスは、以下の場所にある共有フォルダに格納されます。 • マスタインデックスロケーション (インデックス、スペラ): この場所に保存されているマスタおよびスペラインデックスです。検索中、最初の検索結果はマスタインデックスを使用して取得され、スペラインデックスは提案を取得するために使用されます。クラスタ化された BI プラットフォームデプロイメントでは、この場所は、共有ファイルシステム上にあり、クラスタのすべてのノードからアクセスできる必要があります。 • 永続データロケーション (コンテンツストア): コンテンツストアはこの場所に配置されます。マスタインデックスロケーションから作成され、それとの同期が維持されます。コンテンツストアは、ファセットの生成と、マスタインデックスロケーションから生成された最初の検索結果を処理するために使用されます。クラスタ化された BI プラットフォームデプロイメントでは、コンテンツストアはすべてのノードで生成されます。 永続データロケーションは、コンテンツストアフォルダを含むため、クラスタ環境の影響を受ける唯一のインデックスの場所です。マシンの検索サービスが 1 つである場合、コンテンツストアの場所は 1 つだけになります。たとえば、{bobj.enterprise.home}¥data¥PlatformSearchData¥workspace¥<Server Name>¥ContentStores になります。 ただし、クラスタ環境では、複数の検索サービスがある場合、コンテンツストアの場所は各検索サービスに対して 1 つになります。たとえば、実行中のサーバのインスタンスが 2 つある場合、コンテンツストアの場所は以下のようになります。 1. {bobj.enterprise.home}¥data¥PlatformSearchData¥workspace¥<Server Name>¥ContentStores 2. {bobj.enterprise.home}¥data¥PlatformSearchData¥workspace¥<Server Name 1>¥ContentStores • 非永続データロケーション (一時ファイル、デルタインデックス): この場所には、デルタインデックスが作成され、マスタインデックスと結合される前に一時的に格納されます。インデックスがマスタインデックスに結合されると、この場所から削除されます。また、代理ファイル (エクストラクタからの出力) がこの場所に作成され、デルタインデックスに変換されるまで一時的に格納されます。 **注記** • マスタインデックスロケーションは、共有の場所にする必要があります。 • インデックスの場所を変更するには、[インデックス処理の停止] をクリックする必要があります。 • インデックスの場所を変更する場合は、新しい場所にコンテンツをコピーしないと、既存のインデックス情報が失われます。 • インデックスファイルには、ドキュメントコンテンツをインデックス化するように選択した場合には特に、個人情報や機密情報が保存される可能性があります。データの盗難を防ぐために、共有フォルダへのアクセスをシステムユーザにのみ許可し、共有フォルダを暗号化された環境に保存してください。

オプション	説明

インデックス処理のレベル	インデックス処理のレベルを以下のように設定することにより、検索内容を調整することができます。
	• プラットフォームメタデータ: タイトル、キーワード、ドキュメントの説明などのプラットフォームメタデータ情報に対してのみ、インデックスが作成されます。デフォルトでは、このオプションはオンです。
	• プラットフォームおよびドキュメントのメタデータ: このインデックスには、プラットフォームメタデータとドキュメントメタデータが含まれます。ドキュメントのメタデータには、作成日、変更日、作成者名が含まれます。
	• フルコンテンツ: このインデックスには、プラットフォームメタデータ、ドキュメントメタデータ、および以下のようなその他のコンテンツが含まれます。
	  • ドキュメントの実際のコンテンツ
	  • プロンプトと LOV のコンテンツ
	  • チャート、グラフ、ラベル
	注記
	Analysis Office ドキュメントおよび Lumira ドキュメントでは、フルコンテンツのインデックス処理はサポートされていません。Analysis Office ドキュメントおよび Lumira ドキュメントでは、メタデータのインデックス処理のみがサポートされています。
	注記
	インデックス処理のレベルを変更すると、BI プラットフォームリポジトリ全体に対してインデックス処理が再度初期化されます。

オプション	説明
コンテンツタイプ	インデックス化の目的で次のコンテンツタイプを選択できます。 • Crystal レポート • Web Intelligence • ユニバース • BI ワークスペース • Analysis Office • Lumira • Microsoft PowerPoint • Adobe Acrobat • リッチテキスト形式 • テキスト • Microsoft Word • Microsoft Excel プラットフォームメタデータのインデックス処理では、コンテンツタイプフィルタは適用されません。プラットフォームメタデータのインデックス処理は、選択したコンテンツタイプに関係なく、すべてのサポートされるオブジェクトタイプに対して実行され、BI ラウンチパッドの検索結果にプラットフォームメタデータに関連するキーワードのすべてのオブジェクトが返されます。 コンテンツタイプフィルタは、ドキュメントメタデータのインデックス処理 (ドキュメント作成者、ドキュメントヘッダ、ドキュメントフッタなど) およびコンテンツのインデックス処理 (レポートのグラフ、チャート、テーブル)に適しています。ドキュメントメタデータおよびコンテンツに関連するキーワードを検索すると、プラットフォーム検索は、選択されたインデックス処理のレベルとコンテンツタイプに基づいて、リポジトリの選択されたオブジェクトタイプのドキュメントメタデータとコンテンツをインデックス処理します。処理されたオブジェクトだけが BI ラウンチパッドの検索結果に表示されます。
インデックスの再構築	このオプションを使用して、既存のインデックスを削除し、リポジトリ全体を再インデックス処理することができます。 インデックス処理が実行中か停止中かに関係なく、[インデックスの再構築] オプションを選択できます。既存のインデックスは、[プロパティ] ページへの変更を保存すると、削除されます。ただし、インデックス処理が現在停止されている場合、インデックス処理を再開するまでインデックスの再構築は開始されません。 プラットフォーム検索でドキュメントの再インデックス処理を行わない場合は、[インデックスの再構築] オプションを選択解除してから、[インデックス処理の開始] をクリックします。

オプション	説明
インデックス処理から除外するドキュメント	[インデックス処理から除外するドキュメント] オプションは、ドキュメントをインデックス処理から除外します。たとえば、レポートアプリケーションサーバのリソースに過負荷がかからないように、サイズが非常に大きい Crystal レポートを検索対象から外す必要がある場合です。または、大量のパーソナライズされたレポートのあるパブリケーションのインデックス処理をしない場合です。 特定のドキュメントを除外することで、プラットフォーム検索でそのドキュメントがアクセスされないように指定できます。このグループに分類される前にドキュメントがインデックス処理されると、そのドキュメントは検索できるので注意してください。[インデックス処理から除外するドキュメント] グループに属するドキュメントが検索されないようにするには、インデックスを再構築する必要があります。 デフォルトでは、[インデックス処理から除外するドキュメント] オプションのフルコントロールを持つのは管理者アカウントのみです。次の権限を持つその他のユーザは、[インデックス処理から除外するドキュメント] グループに対するドキュメントの追加のみを実行できます。 • カテゴリの表示権限および編集権限 • ドキュメントの直接編集
その他の設定 - インスタンスのスキップ	デフォルトでは、ドキュメントのインスタンスが取得されてインデックス処理が行われます。これによって、インデックスサイズが増大し、ディスク容量の消費が増えます。リポジトリ内の膨大な数のインスタンスのインデックス処理のため、PlatformSearchData フォルダ内の "Lucene Index Engine" フォルダのサイズが非常に大きくなります。数百万の (またはそれ以上の) ドキュメントがあり、これらのドキュメントの多くが、システム内にも膨大な数の既存インスタンスを (定期的に生成するスケジュールされたインスタンスとともに) 持つ場合、インデックス処理レベルが "プラットフォームメタデータ" に設定されていたとしても、"Lucene Index Engine" フォルダのサイズは過度に大きくなります。 プラットフォーム検索インスタンスのスキップ機能では、インスタンスのインデックス処理を CMC のプラットフォーム検索アプリケーションプロパティページにある 'その他の設定 - インスタンスのスキップ' チェックボックスで有効化または無効化することによって制御することができます。 ⓘ 注記 • インスタンスのスキップを有効/無効にすると、プラットフォーム検索 Adaptive Processing Server を再開する必要があります。この変更はすべてのインデックス処理レベルに影響します。 • インスタンスのスキップを変更し、この変更をすべての既存のインスタンスに適用する場合 (すなわち、取得してインデックス処理を行う)、インデックスを再構築する必要があります。

オプション	説明
インデックス処理から除外するオブジェクト	[インデックス処理から除外するオブジェクト] オプションは、オブジェクトをインデックス処理から除外します。たとえば、レポートアプリケーションサーバのリソースに過負荷がかからないように、特定のオブジェクトを検索対象から外す必要がある場合です。 特定のオブジェクトを除外することで、プラットフォーム検索でそのドキュメントがアクセスされないように指定できます。このグループに分類される前にオブジェクトがインデックス処理されると、そのオブジェクトは検索可能になるので注意してください。[インデックス処理から除外するオブジェクト] グループに属するドキュメントが検索されないようにするには、インデックスを再構築する必要があります。 インデックスから除外できるオブジェクトの一覧: • CrystalReport • Webi • LCMJob • Universe • Excel • PDF • PowerPoint • Rtf • Txt • Word • AFDashboardPage • ObjectPackage • QaaWS • プロファイル • イベント • ディスカッション • InformationDesigner • MDAnalysis • パブリケーション • Agnostic • Analytics • Hyperlink • プログラム • pQuery • DSL.MetaDataFile • Shortcut • DataDiscoveryAlbum • AO.Workbook • VISI.Story • VISI.Dataset

オプション	説明
	• VISI.Lums • VISILums • ユーザ • UserGroup

5. [保存して閉じる] をクリックします。

> ⓘ 注記
>
> [インデックスの再構築] オプションを選択せず、インデックス処理のレベルを変更するか、エクストラクタを選択もしくは選択解除した場合は、既存のインデックスは削除されずにインデックスは増分更新されます。

26.3 プラットフォーム検索の使用

26.3.1 CMS リポジトリコンテンツのインデックス処理

インデックス処理は、以下の連続タスクを含む継続的なプロセスです。

1. クロール: クロールは、CMS リポジトリをポーリングし、公開、変更、または削除されたオブジェクトを特定するためのメカニズムです。クロールは、継続クロールとスケジュール済みクロールという 2 つの方法で実行することができます。
   継続クロールとスケジュール済みクロールの詳細については、関連項目のトピックアプリケーションプロパティの設定を参照してください。
2. 抽出: 抽出は、ドキュメントの種類に基づいてエクストラクタを呼び出すためのメカニズムです。リポジトリで使用できるすべてのドキュメントの種類に対し、専用のエクストラクタがあります。新しいエクストラクタプラグインを定義することにより、新しいドキュメントの種類を検索可能にすることができます。これらの各エクストラクタは、多数のレコードを含む大きなドキュメントからコンテンツを抽出できるよう、拡張することができます。
   次のエクストラクタがサポートされています。
   - メタデータエクストラクタ
   - Crystal レポートエクストラクタ
   - Web Intelligence エクストラクタ
   - ユニバースエクストラクタ
   - サードパーティエクストラクタ (MS Office 2003/2007 および PDF ドキュメント)

   検索可能なドキュメントの種類の詳細については、関連項目のトピック検索可能コンテンツタイプを参照してください。
3. インデックス処理: インデックス処理は、抽出されたすべてのコンテンツを、Apache Lucene Engine と呼ばれるサードパーティライブラリを介してインデックス処理するメカニズムです。インデックス処理に必要な時間は、システムにおけるオブジェクト数、文書のサイズと種類によって異なります。
   インデックス処理を正常に実行するには、以下のサーバが実行されており、有効である必要があります。
   - Input File Repository Server (IFRS)
   - Output File Repository Server (OFRS)

- Central Management Server(CMS)
- プラットフォーム検索サービスをホストする Adaptive Processing Server (APS)

オブジェクトタイプが Web Intelligence および Crystal レポートとして選択された場合は、対応する Web Intelligence Processing Server または Crystal Reports Application Server が実行され、選択された各オブジェクトタイプに対して有効化されている必要があります。

4. コンテンツストア: コンテンツストアには、メインインデックスから抽出された ID、CUID、名前、種類、インスタンスなどの情報が、読みやすい形式で含まれています。これにより、検索プロセスが高速化されます。

関連情報

CMC でのアプリケーションプロパティの設定 [901 ページ]
検索可能コンテンツタイプ [911 ページ]

26.3.2 インデックス処理失敗一覧

インデックス処理失敗一覧では、インデックス処理できなかったドキュメントの一覧が表示されます。プラットフォーム検索では、ドキュメントのインデックス処理を 3 回試行します。ドキュメントのインデックス処理に失敗した場合は、そのドキュメントはインデックス処理失敗一覧に表示されます。

インデックス処理失敗一覧を表示するには、次の手順に従います。

1. CMC の [アプリケーション] エリアを表示します。
2. [プラットフォーム検索アプリケーション] を選択します。
3. [アクション] > [インデックス処理失敗一覧] を選択します。

   [プラットフォーム検索アプリケーション] ダイアログボックスが表示され、以下の詳細とともにドキュメントの一覧が表示されます。
   - タイトル: インデックス処理に失敗したドキュメントのタイトルを表示します。
   - タイプ: Crystal Report や Web Intelligence などのドキュメントタイプの名前と、ドキュメントの場所を表示します。
   - エラータイプ: エラーコードとドキュメントのインデックス処理に失敗した理由を表示します。エラーの原因のスタックトレースについて詳細を確認するには、詳細ハイパーリンクをクリックします。
   - 最終指定時刻: ドキュメントのインデックス処理を最後に試行した時点のタイムスタンプを表示します。

26.3.3 検索結果

26.3.3.1 検索前

26.3.3.1.1 クエリの提案

プラットフォーム検索を使用して、特定のオブジェクトを検索するのではなく、特定の質問に対する回答を検索することができます。これらの質問には、BI プラットフォームのリポジトリ内のレポートで回答されている場合と、回答されていない場合があります。

プラットフォーム検索では、リポジトリ内のユニバースの構造と既存のレポートの構造を分析し、この情報をユーザが入力した検索要求と比較して、質問に対する回答を検索する際に役立つ新しい SAP BusinessObjects Web Intelligence クエリを提案します。

潜在的なレポートを作成するために、プラットフォーム検索は、ディメンション、メジャー、条件、およびフィルタ値のすべてのユニバースに含まれている単語を照合します。

プラットフォーム検索は、ユニバースまたは既存の Web Intelligence ドキュメントに関する次の情報で一致する内容を探します。

- 検索入力内の単語と一致するユニバース内のメジャー。
  メジャーが検索語のいずれかに一致すると、そのメジャーは結果の Web Intelligence ドキュメントで使用されます。
- 検索入力内の単語と一致するユニバース内のディメンション名。
  ディメンション名が検索語のいずれかに一致すると、結果の Web Intelligence ドキュメントではこのディメンションの情報が分類されます。
- クエリフィルタを使用して、ドキュメントに表示されるデータを絞ることができます。これらのクエリフィルタは、検索入力を分析して生成されます。
  - ユニバース条件の名前が検索語のいずれかに一致すると、その条件はフィルタとして使用されます。
  - 既存の Web Intelligence ドキュメント内に、名前が検索語に一致するフィールド値がある場合、条件演算子として "等しい" を使用して、一致した値を含む履歴レポートのディメンションからフィルタが作成されます。

プラットフォーム検索で、結果のドキュメントに 2 つの結果フィールドと 1 つのフィルタが含まれる十分な一致項目が作成されると、クエリは実行可能とみなされます。この場合、完了したレポートをクリックして表示できます。

ユニバースとドキュメント間で一致する項目数が不十分な場合、クエリを編集してから実行することができます。

複数のユニバースが検索入力と一致した場合、またはディメンションの名前やフィルタ値などで、同じ単語が 2 つの異なる一致項目に表示される場合、プラットフォーム検索は複数のクエリを提案します。

26.3.3.1.2 検索可能コンテンツタイプ

BI プラットフォームに公開されているコンテンツは、プラットフォーム検索で検索できます。以下は、オブジェクトタイプとそれに対応するインデックス処理されたコンテンツの一覧です。

オブジェクトタイプ	インデックス処理されたコンテンツ
Crystal Reports 2020	タイトル、説明、選択式、保存されたデータ、任意のセクションのテキストフィールド、パラメータ値、およびサブレポート。
Web Intelligence ドキュメント	タイトル、説明、レポートで使用されるユニバースフィルタの名前、保存されたデータ、レポートにローカルに定義されたフィルタ条件の定数、レポートで使用されるユニバースメジャーの名前、レポートで使用されるユニバースオブジェクトの名前、レコードセットのデータ、およびセルの静的テキスト。
Microsoft Excel ドキュメント (2003 および 2007)	空白でないすべてのセルのデータ、ドキュメントプロパティの要約ページのフィールド (タイトル、サブジェクト、作成者、会社、分類、キーワードおよびコメント)、およびドキュメントのヘッダおよびフッタのテキスト。 計算や式を使用するセルでは、評価後の値が検索できます。数値や日時値の場合、生データを検索できます。
Microsoft Word ドキュメント (2003 および 2007)	すべてのパラグラフおよびテーブルのテキスト、ドキュメントプロパティの要約ページのフィールド (タイトル、サブジェクト、作成者、会社名、分類、キーワードおよびコメント)、ドキュメントのヘッダおよびフッタのテキスト、および数値テキスト。
RTF、PDF、PPT、および TXT ファイル	ファイル内のすべてのテキストが検索できます。
LCMJob、オブジェクトパッケージ、Web サービスクエリ (QaaWS)、プロファイル、ディスカッション、インフォメーションデザイナ、SAP BusinessObjects BI プラットフォーム向けウィジェット、MD 分析、パブリケーション、アナリティクス、ハイパーリンク	メタデータコンテンツを検索できます。
イベント	カスタムイベント、システムイベント、Crystal Reports イベント、監視イベントなどのすべてのイベントを検索できます。イベントがソースに関連付けられている場合、プラットフォーム検索ではイベントと共にソースも表示します。 **注記** プラットフォーム検索では、Crystal Reports for Enterprise のイベントがサポートされています。

オブジェクトタイプ	インデックス処理されたコンテンツ

BI ワークスペース	• 次の BI ワークスペースモジュールのタイトル、説明、およびコンテンツがインデックス処理されます。
	  • テキストモジュール
	  • Web ページモジュール
	  • ナビゲーション一覧モジュール
	  • ビューアモジュール
	• 複合モジュールのタイトルと説明がインデックス処理されます。
	• ワークスペーステンプレートモジュールのタイトルのみがインデックス処理されます。
	• グループモジュールの場合は、このモジュール内のタイトルとメタデータがインデックス処理されます。
	• BI ワークスペース内の InfoObject モジュールのタイトル、説明、および CUID がインデックス処理されます。
	  注記
	  埋め込み InfoObject モジュールのタイトルと説明のみがインデックス処理されるため、InfoObject のコンテンツを検索しても、この埋め込みモジュールへの参照は返されません。たとえば Crystal Reports が BI ワークスペースに挿入されている場合、このタイトルと説明はインデックス処理されますが、Crystal Reports のコンテンツを検索しても、埋め込み InfoObject モジュールへの参照は返されません。
	• BI ワークスペースに複数のタブおよびサブタブが含まれている場合、各タブおよびサブタブのタイトルとコンテンツもインデックス処理されます。

次世代 Crystal Reports	タイトル、説明、選択式、保存されたデータ、任意のセクションのテキストフィールド、パラメータ値、およびサブレポート。 次世代 Crystal Reports の次のオブジェクトはサポートされていません。 • クロスタブレポート • チャートデータの抽出 • 画像および関連メタデータの抽出 • 埋め込み OLE (Crystal Reports に埋め込まれた Word ドキュメントなど) また、次世代 Crystal Reports レポートからページごとのデータを読み込むこともできません。

オブジェクトタイプ	インデックス処理されたコンテンツ
ユニバース	データコンテンツを検索できます。 **注記** デフォルトでは、ユニバースのインデックス処理オプションは有効化されています。ユニバースコンテンツのインデックス処理のためにプラットフォーム検索で使用されるクエリの実行に時間がかかり、データベースサーバのパフォーマンスに影響する場合は、セントラル管理コンソール (CMC) のユニバースのインデックス処理オプションを無効化することをお勧めします。ユニバースコンテンツのインデックス処理中にプラットフォーム検索で使用するクエリの例は次のとおりです。`Select distinct SampleColumnName from SampleTableName LIMIT 1000` 次の手順に従って、ユニバースのインデックス処理を無効化します。 1. セントラル管理コンソール (CMC) にログオンします。 2. [アプリケーション] を選択します。 3. プラットフォーム検索アプリケーションに移動し、[プロパティ] を選択します。 4. コンテンツタイプに移動し、[ユニバース] のチェックを外します。 5. [保存して閉じる] を選択します。
Lumira ドキュメント	メタデータコンテンツのみを検索できます。
Analysis Office ドキュメント	メタデータコンテンツのみを検索できます。

注記

サードパーティドキュメント (MS Office 2003/2007 ドキュメントおよび PDF ドキュメント) に対してサポートされる最大サイズは 15 MB です。

26.3.3.2 検索

ユーザが BI ラウンチパッドまたはプラットフォーム検索 SDK を使用するその他のアプリケーションからキーワードを検索すると、検索用語に対してマスタインデックスがチェックされます。ユーザの表示権限に基づき、検索エンジンはユーザがアクセス権を持つドキュメントのみを表示します。

注記

大規模な CMS DB の環境内で CMC で検索を実行すると、検索が失敗する可能性があります。詳細については、SAP ノート 2156647「CMC での検索が遅い、または結果が返されない」を確認してください。

26.3.3.3 検索後

26.3.3.3.1 ファセット

プラットフォーム検索は、検索結果を類似したオブジェクトタイプのカテゴリまたはファセットにグループ化し、検索用語に対して返された結果におけるカテゴリの件数に基づいてそれらに順位を付け、検索結果を絞り込みます。ファセットを使用すると、正確な結果にたどり着くことができます。

プラットフォーム検索では、InfoObject メタデータ、ドキュメントメタデータ、およびドキュメントの内容からファセットが生成されます。指定したクエリに一致するドキュメントが 2 つ以上あるファセットのみが表示されます。ファセットは検索クエリに一致するドキュメントに基づき動的に表示され、ドキュメントカウントでソートされます。

ドキュメントは、以下の一般ファセットまたはカテゴリにグループ化されます。

- パーソナルまたはパブリック (HR、会社、財務など): これは、BI プラットフォームドキュメントカテゴリに基づきます。
- ドキュメントの種類: これは、Web Intelligence、Crystal Reports、Microsoft Word (2003 および 2007)、Microsoft Excel (2003 および 2007) などのドキュメントの種類に基づきます。
- ユニバースおよび接続: これは、コンテンツソースに基づきます。
- 日付: 前回更新日付: (年、四半期および月) を含みます。
- 時間: 過去 24 時間、先週など、最後に更新された時間を含みます。
- 作成者: ドキュメントを作成したユーザの名前です。

> **注記**
>
> ヘブライ語またはアラビア語ロケールを使用している場合、BI ラウンチパッドでコンテンツオブジェクトを検索すると、検索結果にファセットが表示されません。

26.3.3.3.2 検索結果のランクの正規化

プラットフォーム検索では、ドキュメントをランク付けする際、検索用語のオカレンスの場所が考慮されます。コンテンツは、ドキュメントのコンテンツのオカレンスに基づいて以下のカテゴリに分類されます。

1. プラットフォームメタデータ
2. ドキュメントメタデータ
3. コンテンツメタデータ
4. コンテンツ

CMC でこれらのカテゴリの加重を設定できます。

26.3.3.3.2.1 検索結果のランク付けに使用する加重のカスタマイズ

プラットフォーム検索では、ドキュメントのコンテンツのオカレンスに基づいてカテゴリ別に分類されたコンテンツの加重を設定できるため、目的のカテゴリの値を高く設定して、関連する検索結果をより速く取得できます。

加重を設定するには、次の手順に従います。

1. CMC の [管理] エリアで、[アプリケーション] をクリックします。
2. [プラットフォーム検索アプリケーション] を開きます。
3. [ランク] を選択します。

   プラットフォームメタデータ、ドキュメントメタデータ、コンテンツメタデータ、およびコンテンツなどのさまざまなコンテンツカテゴリの加重が表示されます。[ユーザのロケール] は、BI ラウンチパッドの基本設定で設定するロケールです。
4. 必要に応じて加重を設定します。
5. [保存] をクリックします。

アップグレードシナリオでは、すでにインデックス化されているドキュメントにランクを適用する必要がある場合、インデックスを再構築する必要があります。詳細は、CMC でのアプリケーションプロパティの設定 [901 ページ]の節のインデックスの再構築に関する情報を参照してください。

26.3.3.3.3 多言語のサポート

プラットフォーム検索では、コンテンツのインデックス処理、検索結果の取得、希望言語での提案の取得に対する多言語サポートが用意されています。CMC の [デフォルトのインデックスロケール] で設定されたロケールを使用して、ローカライズされていないすべての BI プラットフォームドキュメントがインデックス処理されます。

InfoObject がローカライズされると、プラットフォーム検索は対応する言語のアナライザを使用してドキュメントをインデックス処理します。

検索は、クライアントの製品ロケールとして設定されたロケールに基づいて行われます。プラットフォーム検索では、検索結果を取得するときのクライアントの製品ロケールに対する加重が高くなっています。CMC でこの加重を設定できます。

26.3.3.3.4 提案

プラットフォーム検索には、スペルが正しくない検索クエリに対する提案が用意されています。最初の検索クエリで何も結果が得られない場合、プラットフォーム検索ではインデックス処理されたコンテンツに基づき最も有望な用語が提案されます。

提案は、ハイパーリンク付きのキーワードとして表示されます。元のクエリに一致するキーワードを含むドキュメントのリストを表示するには、そのハイパーリンクをクリックします。これらの提案は、さまざまな客観的要因に基づきアルゴリズム的に決定されます。

元の要求に一致する用語が複数ある場合、プラットフォーム検索では、CMC で [デフォルトのインデックスロケール] として設定された言語で上位 3 つが提案されます。

> ⓘ 注記
>
> 以下の場合、プラットフォーム検索で提案はされません。
>
> - 検索クエリの文字数が 3 文字未満の場合
> - タイプ: Crystal Report など、属性検索の場合
> - ユニバースメタデータおよびコンテンツの場合

- 中国語、日本語、韓国語など、複数バイト言語の場合

26.4 プラットフォーム検索と SAP NetWeaver Enterprise Search の統合

SAP NetWeaver Enterprise Search 7.20 以上では、OpenSearch (RSS および ATOM) に基づく検索サービスが使用できます。 OpenSearch では、検索要求をリモートの検索サービスプロバイダシステムに委任できます。 この場合は、OpenSearch がサービスプロバイダで、SAP NetWeaver Enterprise Search が検索結果のコンシューマで、SAP BusinessObjects のプラットフォーム検索が検索サービスプロバイダです。

ユーザが検索要求を送信すると、SAP NetWeaver Enterprise Search から直接 OpenSearch プロバイダに検索要求が転送されます。 プロバイダは検索要求に応答し、SAP NetWeaver Enterprise Search に応答を返します。 その後、他の検索オブジェクトコネクタから受信した結果が検索結果に結合され、ユーザインタフェースに表示されます。

SAP NetWeaver Enterprise Search とプラットフォーム検索を統合するには、次の手順を実行する必要があります。

1. SAP NetWeaver Enterprise Search にコネクタを作成します。
2. BI プラットフォームにユーザのロールをインポートします。

26.4.1 SAP NetWeaver Enterprise Search でのコネクタの作成

OpenSearch を介して利用可能な検索機能を提供する外部検索プロバイダを統合するのに、OpenSearch タイプの検索オブジェクトコネクタを使用することができます。

SAP NetWeaver Enterprise Search にコネクタを作成するには、次の前提条件が必要です。

1. OpenSearch 記述サービスの URL.。
2. OpenSearch 記述サービスは、RSS または ATOM 形式でのみ使用できる必要があります。

次の手順に従って、SAP NetWeaver Enterprise Search にコネクタを作成します。

1. 管理コックピットを起動して [作成] を選択します。
2. 検索オブジェクトコネクタのタイプとして "OpenSearch" を選択します。
3. [次へ] を選択します。
4. OpenSearch プロバイダの OpenSearch 記述サービスの URL を入力します。
5. 次の認証設定のいずれかを選択して、記述サービスの URL を起動します。
   - 認証なし: 認証は行われません。
   - SAP 認証アサーションチケット: このユーザを使用して、SSO 経由で認証が行われます。
   - ユーザ/パスワード: 定義済みのユーザを使用して認証が行われます。
6. OpenSearch URL 設定から "検索 URL の起動" を選択します。
   その後、適合する検索サービスに対して OpenSearch 記述サービスの検証が行われます。検索 URL テンプレートおよび関係付けられた記述の値がシステムにより自動的に入力されます。

7. 次の認証設定のいずれかを選択して、コネクタを設定します。
   - 認証なし: 認証は行われません。
   - SAP 認証アサーションチケット: このユーザを使用して、SSO 経由で認証が行われます。
   - ユーザ/パスワード: 定義済みのユーザを使用して認証が行われます。
8. [次へ] を選択します。
   この検索オブジェクトコネクタに入力した値を示す概要ダイアログボックスが表示されます。
9. 設定を変更する場合は [戻る] を、入力したデータをすべて破棄する場合は [キャンセル] を選択します。
10. [完了] を選択して設定を保存します。

26.4.2 BI プラットフォームへのユーザのロールのインポート

BI プラットフォームにユーザのロールをインポートするには、次の手順を実行します。

> **注記**
>
> 管理者は、ユーザの詳細、システム情報、およびアプリケーションのホスト情報とユーザ認証情報を把握している必要があります。

1. CMC の[認証]エリアを表示します。
2. [*SAP*] を選択します。
3. [権限認証システム] タブで、次の項目を指定します。
   - システム
   - クライアント
   - アプリケーションサーバ
   - システム番号
   - ユーザ名
   - パスワード
   - Language
4. [更新] を選択します。
5. [ロールのインポート] タブを選択し、ユーザロールをインポートします。
6. [更新] を選択します。
7. CMC で 管理 > ユーザセキュリティ を選択して、適切なユーザの権限を割り当てます。

26.5 SAP NetWeaver Enterprise Search からの検索

SAP NetWeaver Enterprise Search からの結果を検索するには、次の手順を実行します。

1. SAP NetWeaver Enterprise Search アプリケーションにログオンします。
2. [高度な検索] を選択します。
3. プラットフォーム検索用に作成したコネクタを選択します。

4. キーワード検索をします。

   キーワードに一致するものがあれば、キーワードの統合結果にはプラットフォーム検索からの結果が含まれます。

26.6 監査

プラットフォーム検索サービスを使用するクライアントアプリケーションから送信される検索要求のすべてのイベントおよび検索応答が監査されます。プラットフォーム検索の場合、監査はサービスレベルで実行されます。

監査イベントを送信するには、プラットフォーム検索サービスを、同じサーバ上のクライアント監査プロキシサービスを使用して実行する必要があります。

プラットフォーム検索には 1 つのイベントタイプ ID は 1009 があり、以下のような 4 つのプラットフォーム検索固有のイベント詳細タイプ ID があります。

- Keyword searched (ID: 19)
- Number of Search Results (ID: 63)
- Facet Search (ID: 20)
- Search Exception (ID: 1)

上記のイベント詳細の他に、すべての BI プラットフォームモジュールにおけるすべての監査でサポートされている sessionCuid や userCuid などの標準イベント詳細がいくつかあります。

プラットフォーム検索における監査の機能については、以下で例を用いて説明します。

たとえば、キーワード "Sales" を検索する場合、検索結果の合計数は 5 になります。この場合、以下のイベントが監査されます。

- イベントタイプ ID 1009
- 値 Sales のイベント詳細タイプ ID 19
- 値 5 のイベント詳細タイプ ID 63
- セッション CUID
- ユーザ CUID
- 成功ステータスである値 0 のステータス
- 開始時間
- 期間
- サービスサイド監査であるために値が 0 であるオブジェクト ID

ファセットが生成され、1 つ以上のファセットを選択した場合、以下のイベントが監査されます。

- イベントタイプ ID 1009
- 値 Sales のイベント詳細タイプ ID 19
- 値 5 のイベント詳細タイプ ID 63
- ファセットのカンマ区切り文字列を含むイベント詳細タイプ ID 20
- セッション CUID
- ユーザ CUID
- 成功ステータスである値 0 のステータス

- 開始時間
- 期間
- サービスサイド監査であるために値が 0 であるオブジェクト ID

*"a" などの無効なエントリが原因の検索例外が発生した場合、以下のイベント詳細が監査されます。

- イベントタイプ ID 1009
- 値 Sales のイベント詳細タイプ ID 19
- 値 0 のイベント詳細タイプ ID 63
- 例外メッセージを含むイベント詳細タイプ ID 1
- セッション CUID
- ユーザ CUID
- 失敗ステータスである値 1 のステータス
- 開始時間
- 期間
- サービスサイド監査であるために値が 0 であるオブジェクト ID

26.7 トラブルシューティング

26.7.1 セルフヒーリング

プラットフォーム検索は、独自のセルフヒーリングメカニズムを備えています。これによって検索サービスメモリの使用率が継続的に監視され、メモリ使用率がしきい値を超過するとインデックス処理が自動的に停止されます。メモリ使用率が適切な水準に低下すると、インデックス処理は自動的に開始されます。ただし、ユーザはこのプロセス中も検索を続行できますが、特定期間はインデックス処理をすることはできません。デフォルトでは、プラットフォーム検索で、ドキュメントの種類に基づき、任意の瞬間にインデックス処理が可能なドキュメント数が設定されます。インデックス処理は、CPU やメモリなどのシステムリソースに基づいて開始されます。

26.7.2 問題のシナリオ

ここでは、プラットフォーム検索で検索結果を取得する際に生じる可能性のある広範な問題に対して、解決策を段階的に説明します。

新しく追加したドキュメントにはキーワードが含まれているが、そのドキュメントから検索結果を取得できない

- 送信したドキュメントの種類が、プラットフォーム検索でサポートされているかどうかを確認します。ドキュメントの種類がサポートされていない場合、そのドキュメントのインデックス処理は行われません。
  サポートされるドキュメントの種類の詳細については、後述の関連項目のトピック検索可能コンテンツタイプを参照してください。

- [クロール頻度] で選択されているオプションを確認します。[クロール頻度] が [継続的クロール] に設定されている場合、ドキュメントはただちに取得されてインデックス処理が行われます。[クロール頻度] が [スケジュール済みクロール] に設定されている場合、インデックス処理はスケジュールされた期間のみで実行されます。
  クロール頻度の詳細については、後述の関連項目のトピックアプリケーションプロパティの設定を参照してください。
- インデックス処理の失敗一覧を調べて、ドキュメントが正常にインデックス処理されたかどうかを確認します。ドキュメントが失敗一覧に表示されている場合は、プラットフォーム検索でドキュメントのインデックス処理が行われるように、そのドキュメントを変更して再送信する必要があります。

  > ⓘ 注記
  >
  > ドキュメントを変更するには、フィールドを追加または削除して、再度保存します。この操作により、ドキュメントのタイムスタンプが BI プラットフォームリポジトリ内で更新され、ドキュメントのインデックスの再処理が開始されます。

  インデックス処理に失敗したドキュメントの詳細については、後述の関連項目のトピックインデックス処理失敗一覧を参照してください。
- Adaptive Processing Server が、インデックス処理の失敗に関する情報を含む追跡ログを確認します。
  1. .glf という拡張子を持つ APS トレースログが含まれる `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥logging¥` ディレクトリに移動します。
  2. 追跡ログファイルを開き、インデックス処理に必要なドキュメントの SI_ID を検索します。

     > ⓘ 注記
     >
     > ドキュメントの SI_ID はドキュメントプロパティで見つけることができます。

Crystal Reports ドキュメントを取得できない

プラットフォーム検索における Crystal Reports コンテンツのインデックス処理は、Crystal Reports 2020 に対してのみ行われます。Crystal Reports for Enterprise のインデックス処理は行われません。

ただし、Crystal Reports for Enterprise では、ドキュメントプロパティであるタイトル、説明、キーワードなどのドキュメントのメタデータを検索することはできます。

インデックス処理の可能なコンテンツがドキュメントに含まれている場合は、上記の節新しく追加したドキュメントにはキーワードが含まれているが、そのドキュメントから検索結果を取得できないに記述されたのと同じ手順を実行する必要があります。

SAP NetWeaver Enterprise Search アプリケーションで、BI プラットフォームリポジトリからの検索結果を取得できない

- プラットフォーム検索で検索結果を取得するのに BI 起動パッドが使用されていないか確認し、問題の原因がプラットフォーム検索と SAP NetWeaver Enterprise Search の統合にあるかどうかを調査します。

- OpenSearch が Web アプリケーションサーバに正しくデプロイされているかどうか確認します。OpenSearch のデプロイメントの個々の検証手順は、使用している Web アプリケーションサーバの種類に応じて異なります。
- コネクタが正しく作成または設定されているかどうか、SAP NetWeaver Enterprise Search 設定で確認します。プラットフォーム検索からの検索結果を連結するには、SAP NetWeaver Enterprise Search 用の正しいコネクタを使用する必要があります。
- SAP NetWeaver Enterprise Search を実行するマシンと BI プラットフォームを実行するマシンとの間で正しく通信が行われているかどうか確認します。分散環境にネットワークの問題がある場合、SAP NetWeaver Enterprise Search では結果の連結に失敗することがあります。
- SAP NetWeaver Enterprise Search のユーザが適切な権限を持って BI プラットフォームに追加されているかどうか確認します。ユーザの権限を確認するには、CMC の [認証] エリアに移動し、[*SAP*] を選択します。

関連情報

インデックス処理失敗一覧 [910 ページ]
CMC でのアプリケーションプロパティの設定 [901 ページ]
検索可能コンテンツタイプ [911 ページ]

27 フェデレーション

27.1 フェデレーション

フェデレーションは、グローバル環境下での複数の BI プラットフォームデプロイメントで作業する場合の、サイト間レプリケーションツールです。

コンテンツは、BI プラットフォームデプロメイントで作成および管理でき、定期的に地理的に異なるサイト間で他の BI プラットフォームデプロイメントに複製できます。一方向レプリケーションジョブと双方向レプリケーションジョブの両方を実行できます。

フェデレーションの利点は次のとおりです。

- ネットワークトラフィックの削減
- 1 つのサイトからのコンテンツの作成と管理
- エンドユーザに対するパフォーマンスの向上

フェデレーションを使用してコンテンツを複製する場合、次のことを実行できます。

- 複数のデプロイメントの管理ニーズを簡素化
- グローバルな組織の複数のオフィスに一貫したアクセス権ポリシーを提供
- データが存在するリモートサイトでの迅速な情報の取得、およびレポートの処理
- ローカルのデータや分散されているデータを高速に取得して時間を節約
- カスタムコードを記述することなく、複数のデプロイメントのコンテンツを同期

フェデレーションは、個々のセキュリティモデル、ライフサイクル、テストおよびデプロイメントの時間だけでなく、さまざまなビジネスの所有者や管理者を持つことができるツールです。たとえば、管理機能を委任して、販売アプリケーションの管理者が人事アプリケーションを変更しないようにすることができます。

フェデレーションではさまざまなオブジェクトを複製できます。

カテゴリ	複製できるオブジェクトの種類	その他の注意事項
ビジネスビュー	Business View Manager、DataConnection、LOV、データファンデーションなど。	すべてのオブジェクトはサポートされますが、個々のレベルではサポートされません。
レポート	Crystal レポート、Web Intelligence、および Dashboard Design	フルクライアントアドインおよびテンプレートはサポートされます。
サードパーティオブジェクト	Excel、PDF、PowerPoint、Word、テキスト、リッチテキスト、および Shockwave Flash ファイル	
ユーザ	ユーザ、グループ、受信ボックス、お気に入り、個人用カテゴリ	
Business Intelligence プラットフォーム	フォルダ、イベント、カテゴリ、カレンダ、アクセスレベル、ハイパーリンク、ショートカット、プログラム、プロファイル、オブジェクトパッケージ、その他	

カテゴリ	複製できるオブジェクトの種類	その他の注意事項
ユニバース	ユニバース、接続、ユニバースオーバーロード	

次のシナリオでは、組織でフェデレーションを使用する方法を示す 2 つの例を重点的に説明します。

シナリオ **1:** 小売 **(**中央化された設計**)**

ACME ストアでは、一方向レプリケーション方式を使用してさまざまな場所にあるすべての店舗に月間販売レポートを送信する必要があります。レプリケート元サイトの管理者がレポートを作成すると、各レプリケート先サイトの管理者はそのレポートを複製し、その店舗のデータベースに対して実行します。

> → ヒント
>
> ローカライズされたインスタンスをレプリケート元サイトに戻し、各オブジェクトの複製された情報を管理することができます。たとえば、適切なロゴ、データベース接続情報などが適用されます。

シナリオ **2:** リモートスケジュール **(**分散アクセス**)**

データはレプリケート元サイトにあります。一時停止中のレプリケーションジョブは、レプリケート元サイトに送信されて実行されます。その後、完了したレプリケーションジョブは、確認のため、レプリケート先サイトに戻されます。たとえば、レポートのデータがレプリケート先サイトで利用できない場合でも、ユーザはレプリケート元サイトで実行されるようにレポートを設定してから、完了したレポートをレプリケート先サイトに戻すことができます。

27.2 フェデレーションの用語

ここでは、フェデレーションに関連する新しい単語とフレーズを紹介します。これらは、フェデレーションを操作および使用する際に役立ちます。

BI Application	特定の目的や対象者を持つ関連の Business Intelligence(BI)の論理グループ分け。 BI Application はオブジェクトではありません。 1 つの BI プラットフォームデプロイメントで複数の BI Application をホストできます。各 BI Application は、個別のセキュリティモデル、ライフサイクル、テスト、およびデプロイメント時間枠に加え、個別のビジネス所有者や管理者を持つことができます。
レプリケート先サイト	レプリケート元サイトから複製された BI プラットフォームコンテンツを取得する BI プラットフォームシステム。
ローカル	ユーザまたは管理者が接続しているローカルシステム。 たとえば、レプリケート先サイトの管理者は、レプリケート先サイト に対して“ローカル”と見なされます。
ローカルで実行して完了したインスタンス	レプリケート先サイトで処理されて、レプリケート元サイトに戻されるインスタンス。
複数のレプリケート元サイト	複数のサイトをレプリケート元サイトとして使用できます。 たとえば、複数の開発センタには通常複数のレプリケート元サイトがあります。 ただし、1 つのレプリケーションで使用できるのは 1 つのレプリケート元サイトだけです。

一方向レプリケーション	オブジェクトは一方向、つまりレプリケート元サイトからレプリケート先サイトにのみ複製されます。 レプリケート先サイトで行われた更新は、レプリケート先サイトで維持されます。
レプリケート元サイト	コンテンツが作成される BI プラットフォームシステム。
リモート	ユーザにローカルではないシステム。 たとえば、レプリケート元サイトは、レプリケート先サイトのユーザおよび管理者に対して“リモート”であると見なされます。
リモート接続	ユーザ名やパスワード、CMS 名、WebService URL、クリーンアップオプションなど、BI プラットフォームデプロイメントへの接続に使用される情報を含むオブジェクト。
リモートスケジュール	レプリケート先サイトからレプリケート元サイトに戻されるスケジュール要求。 レプリケート先サイトのレポートはリモートでスケジュールすることができ、レポートインスタンスはレプリケート元サイトに戻されて処理されます。 その後、完了したインスタンスがレプリケート先サイトに戻されます。
レプリケーション	ある BI プラットフォームシステムから別のシステムにコンテンツがコピーされるプロセス。
レプリケーションジョブ	レプリケーションスケジュール、複製するコンテンツ、およびコンテンツの複製時に実行する必要がある特殊な条件に関する情報を含むオブジェクト。
レプリケーション一覧	複製されるオブジェクトの一覧。 レプリケーション一覧は、BI プラットフォームデプロイメントに含まれている、まとめて複製されるその他のコンテンツ (ユーザ、グループ、レポートなど) を表します。
レプリケーションオブジェクト	レプリケート元サイトからレプリケート先サイトへ複製されるオブジェクト。 レプリケート先サイトで複製されたすべてのオブジェクトには、レプリケーションアイコンが付けられます。競合が発生すると、オブジェクトには競合アイコンが付けられます。
レプリケーションパッケージ	転送中に作成されるレプリケーションパッケージには、レプリケーションジョブからのオブジェクトが含まれます。 レプリケーションパッケージには、環境が短期間に変化する場合や初期レプリケーション用に、レプリケーション一覧で定義されているすべてのオブジェクトを含むことができます。 または、レプリケーションジョブのスケジュールに比べてオブジェクトの変更頻度が少ない場合は、レプリケーション一覧の小さいサブセットを含むことができます。 レプリケーションパッケージは、BI Application Resource(BIAR)ファイルとして実装されます。
レプリケーションの最新表示	レプリケーション一覧内のすべてのオブジェクトは、最終変更バージョンに関係なく最新表示されます。
双方向レプリケーション	一方向レプリケーションと同様に動作しますが、双方向レプリケーションでは両方向で変更が送信されます。 レプリケート元サイトへの更新は各レプリケート先サイトに複製されます。 レプリケート先サイトでの更新および新しいオブジェクトは、レプリケート元サイトに送信されます。

27.3 セキュリティアクセス権の管理

フェデレーションでは、別個のデプロイメント間でコンテンツを複製し、他の管理者との共同作業が必要になるため、フェデレーションの使用を開始する前にセキュリティについて理解する必要があります。

別個のデプロイメントの管理者が相互に調整した上でフェデレーションを有効にする必要があります。コンテンツが複製されたら、管理者はコンテンツを変更できます。

特定のタスクを実行するには、レプリケート元デプロイメントおよびレプリケート先デプロイメントに対する次のような特定の権限が必要です。

- レプリケート元サイトで必要な権限
- レプリケート先サイトで必要な権限
- フェデレーション固有のオブジェクトに必要な権限
- フェデレーションシナリオ

> → ヒント
>
> この章を読んでからフェデレーションを有効にすることをお勧めします。

27.3.1 レプリケート元サイトで必要な権限

ここでは、レプリケート元サイトで行われるアクションと、レプリケート元サイトに接続しているユーザアカウントに必要な権限について説明します。これは、レプリケート先サイトのリモート接続オブジェクトで入力したアカウントです。

対処方法	説明	必要な権限
一方向レプリケーション	レプリケート元サイトからレプリケート先サイトのみへのレプリケーションを実行します。 ⓘ 注記 “表示”および“複製”権限は、複製中のすべてのオブジェクトに対して必要です。これには、依存関係の計算によって自動的に複製されるオブジェクトも含まれます。	• 複製するすべてのオブジェクトに対する“表示”および“複製”権限 • レプリケーション一覧に対する“表示”権限
双方向レプリケーション	レプリケート元サイトからレプリケート先サイト、およびレプリケート先サイトからレプリケート元サイトへのレプリケーションを実行します。	• 複製するすべてのオブジェクトに対する“表示”および“複製”権限 • レプリケーション一覧に対する“表示”権限 • パスワードを変更するための、ユーザオブジェクトに対する“アクセス権の変更”権限
スケジューリング	レプリケート先サイトからレプリケート元サイトで行われるリモートスケジュールを実行できるようにします。	• リモートでスケジュールするすべてのオブジェクトに対する“スケジュール”権限

関連情報

レプリケート先サイトで必要な権限 [927 ページ]

27.3.2 レプリケート先サイトで必要な権限

ここでは、レプリケート先サイトに適用されるアクションと、レプリケーションジョブを実行しているユーザアカウントに必要な権限について説明します。これは、レプリケーションジョブを作成したユーザのアカウントです。

> **注記**
>
> 他のスケジュール可能なオブジェクトと同様に、別のユーザに代わってレプリケーションジョブをスケジュールできます。

対処方法	説明	必要な権限
全てのオブジェクト	レプリケーションが一方向か双方向かにかかわらず、オブジェクトを複製します。	• すべてのオブジェクトに対する“表示”、“追加”、“編集”、および“アクセス権の変更”権限 • すべてのユーザのオブジェクトに対する“ユーザパスワードの変更”権限
最初のレプリケーション	レプリケーションジョブを初めて実行するときには、オブジェクトはまだレプリケート先サイトに存在しません。したがって、レプリケーションジョブの実行に使用するユーザアカウントには、すべての最上位レベルのフォルダおよびそれらに追加するコンテンツを含むオブジェクトの権限が必要です。	• すべての最上位レベルのフォルダとデフォルトオブジェクトに対する“表示”、“追加”、“編集”、および“アクセス権の変更”権限

関連情報

レプリケート元サイトで必要な権限 [926 ページ]

27.3.3 フェデレーション固有の権限

ここでは、フェデレーションに固有のシナリオについて説明します。

対処方法	説明	必要な権限
オブジェクトのクリーンアップ	オブジェクトのクリーンアップは、レプリケート先サイトのオブジェクトを削除します。	• レプリケーションジョブの実行に使用するアカウントには、削除される可能性のあるすべてのオブジェクトの“削除”権限が必要です。
特定のオブジェクトに対するクリーンアップの無効化	特定のオブジェクトがレプリケート元サイトから複製されるときに、それらのオブジェクトがレプリケート元サイトで削除される場合でも、レプリケート先サイトからは削除したくない場合があります。これは権限を使用して保護できます。たとえば、レプリケート先サイトのユーザがレプリケート元サイトのユーザとは別に、独自にオブジェクトの使用を開始する場合に、このオプションを選択できます。 たとえば、レプリケート先サイトのユーザが独自のローカルレポートを作成するときに使用する複製済みのユニバースがある場合、レプリケート元サイトからそのユニバースが削除されても、レプリケート先サイトではそのユニバースを失いたくはありません。	• 保持するオブジェクトでレプリケーションジョブを実行する場合に使用するユーザアカウントの“削除”の拒否権限
レプリケート元サイトを変更しない、双方向レプリケーション	双方向レプリケーションを選択していても、一部のレプリケート元のオブジェクトを、レプリケート先で変更された場合でも、変更したくない場合があります。この理由としては、オブジェクトが特殊でレプリケート元サイトのユーザのみが変更する必要がある、またはリモートスケジュールを有効にしても変更を戻したくないなどがあります。 **注記** リモートスケジュールの場合は、リモートスケジュール用のオブジェクトだけを処理するジョブを作成できます。ただし、この場合は、レポート、レポートを含むフォルダ、そのフォルダの親フォルダなど、祖先オブジェクトも複製されます。レプリケート先サイトで行った変更はレプリケート元サイトに複製され、レプリケート元サイトで行った変更はレプリケート先サイトに複製されます。	• リモート接続オブジェクトで接続に使用されるユーザアカウントの“編集”の拒否権限

27.3.4 オブジェクトに対するセキュリティの複製

オブジェクトに対するセキュリティ権限を維持するには、オブジェクトおよびそのユーザまたはグループの両方を同時に複製する必要があります。これを行わない場合は、複製先のサイトにそれらがすでに存在するので、各サイトに同一の一意の識別子(CUID)が必要です。

オブジェクトが複製され、ユーザまたはグループが複製されない場合、または複製先のサイトにそれらが存在しない場合、権限は削除されます。

例

Group A と Group B には Object A に対する権限が割り当てられています。Group A には“表示”権限があり、Group B には“表示の拒否”権限があります。レプリケーションジョブで Group A と Object A だけを複製すると、レプリケート先サイトの Object A は、関連付けられている Group A の“表示”権限だけを持つことになります。

オブジェクトを複製するときに、オブジェクトに対する明示的な権限を持つすべてのグループを複製しない場合、潜在的なセキュリティリスクがあります。上記の例は、潜在的なリスクを示しています。User A が Group A と Group B の両方に属している場合、ユーザはレプリケート元サイトに対する Object A の表示権限を持ちません。ただし、User A は両方のグループに属しているため、レプリケート先サイトに複製されます。そこで、Group B が複製されなかったため、User A はレプリケート先サイトで Object A を表示する権限を持ちますが、レプリケート元サイトでは Object A を表示できません。

レプリケーションジョブに含まれていないその他のオブジェクトを参照するオブジェクト、またはすでにレプリケート先サイトに存在しないオブジェクトは、ログファイルに表示されます。ログファイルには、複製されていないオブジェクトを参照したオブジェクトおよび参照が削除されたオブジェクトが記録されています。

特定のユーザまたはグループのオブジェクトのセキュリティは、レプリケート元サイトからレプリケート先サイトにのみ複製されます。レプリケート先サイトで複製したオブジェクトのセキュリティを設定できますが、それらの設定はレプリケート元サイトに複製されません。

27.3.5 アクセスレベルを使用したセキュリティの複製

保持するには、アクセスレベルによってアクセス権を定義する必要があります。オブジェクト、ユーザまたはグループ、およびアクセスレベルを同時に複製するか、それらがレプリケート先のサイトにすでに存在している必要があります。

レプリケーションジョブに含まれていない、またはレプリケート先サイトに存在しないユーザまたはグループに明示的なアクセス権を割り当てるオブジェクトは、そのログファイルに表示されます。ログファイルには、複製されていない割り当て済みのアクセス権や、削除されたアクセス権を持つオブジェクトが表示されます。

また、インポートされたオブジェクトで使用される“アクセスレベル”を自動的に複製することもできます。このオプションは、レプリケーション一覧で使用できます。

> ⓘ 注記
>
> デフォルトのアクセスレベルは複製されませんが、参照は維持されます。

27.4 レプリケーションの種類とモードのオプション

レプリケーションの種類とレプリケーションモードの選択に応じて、次の 4 つのレプリケーションジョブオプションのいずれかを作成します。

- 一方向レプリケーション
- 双方向レプリケーション
- レプリケート元から最新表示
- レプリケート先から最新表示

27.4.1 一方向レプリケーション

[一方向レプリケーション] では、コンテンツを一方向、つまりレプリケート元サイトからレプリケート先サイトへのみ複製できます。レプリケーション一覧内のレプリケート元サイトのオブジェクトに加えられた変更が、レプリケート先サイトに送信されます。ただし、レプリケート先サイトのオブジェクトに加えられた変更は、レプリケート元サイトに戻されません。

[一方向レプリケーション] は、中央の 1 つの BI プラットフォームデプロイメントでオブジェクトが作成、変更、管理されている場合に適しています。他のデプロイメントは、中央のデプロイメントのコンテンツを使用します。

一方向レプリケーションを作成するには、次のオプションを選択します。

- レプリケーションの種類 = 一方向レプリケーション
- レプリケーションモード = 通常のレプリケーション

27.4.2 双方向レプリケーション

[双方向レプリケーション]では、レプリケート元サイトとレプリケート先サイト間で双方向にコンテンツを複製できます。レプリケート元サイトでオブジェクトに加えられた変更はレプリケート先サイトに複製され、レプリケート先サイトで加えられた変更はレプリケート元サイトに複製されます。

> ⓘ 注記
>
> リモートスケジュールを実行したり、ローカルで実行したインスタンスをレプリケート元に戻したりするには、[双方向レプリケーション]モードを選択する必要があります。

コンテンツが作成、変更、管理されている BI プラットフォームデプロイメントが複数あり、両方の場所で使用される場合は、[双方向レプリケーション] が最も効率的なオプションです。またこのモードは、デプロイメントを同期するのにも役立ちます。

双方向レプリケーションを作成するには、次のオプションを選択します。

- レプリケーションの種類 = 双方向レプリケーション
- レプリケーションモード = 通常のレプリケーション

関連情報

リモートスケジュールおよびローカルで実行したインスタンス [955 ページ]

27.4.3 [レプリケート元から最新表示]または[レプリケート先から最新表示]

コンテンツを[一方向レプリケーション]モードまたは[双方向レプリケーション]モードで複製すると、レプリケーション一覧のオブジェクトがレプリケート先サイトに複製されます。ただし、レプリケーションジョブが実行されるたびにすべてのオブジェクトが複製されるわけではありません。

フェデレーションには、レプリケーションジョブを高速で完了することができる最適化エンジンが用意されています。最適化エンジンでは、オブジェクトのバージョンとタイムスタンプを組み合わせて使用して、最後のレプリケーション以降にオブジェクトが変更されているかどうかを確認します。この確認作業は、レプリケーション一覧内で明示的に選択されたオブジェクトおよび依存関係のチェック中に複製されたオブジェクトで実行されます。

ただし、最適化エンジンはオブジェクトを見逃す場合があり、その場合オブジェクトは複製されません。このような場合に、“レプリケート元から最新表示”および“レプリケート先から最新表示”を使用すると、レプリケーションジョブは、タイムスタンプに関係なく、コンテンツおよびそれらの依存関係を複製します。

[レプリケート元から最新表示]では、レプリケート元サイトからレプリケート先サイトへのみコンテンツが送信されます。[レプリケート先から最新表示]では、レプリケート先サイトからレプリケート元サイトへのみコンテンツが送信されます。

例

以下に示す 3 つの例で、“レプリケート元から最新表示”と“レプリケート先から最新表示”を使用している場合に、最適化によって特定のオブジェクトが失われるシナリオを詳しく説明します。

シナリオ **1:** 他のオブジェクトを含むオブジェクトを複製中の領域に追加する場合。

Folder A がレプリケート元サイトからレプリケート先サイトへ複製されます。これで、Folder A は両方のサイトに存在します。ユーザが Report B を含む Folder B を、レプリケート元サイトの Folder A に移動またはコピーします。次のレプリケーション時に、フェデレーションは Folder B のタイムスタンプが変更されていることを確認し、Folder B をレプリケート先サイトに複製します。ただし、Report B のタイムスタンプは変更されていません。したがって、通常の一方向または双方向レプリケーションジョブでは Report B は複製されません。

Folder B のコンテンツを正しく複製するためには、“レプリケート元から最新表示”を使用するレプリケーションジョブを一度だけ使用する必要があります。この後に、通常の一方向または双方向レプリケーションジョブによって Folder B は正しく複製されます。反対に、Folder B をレプリケート先サイトに移動またはコピーする場合は、“レプリケート先から最新表示”を使用します。

シナリオ **2:** LifeCycle Manager または BIAR コマンドラインを使用して新しいオブジェクトを追加する場合。

LifeCycle Manager または BIAR コマンドラインを使用して複製中の領域にオブジェクトを追加する場合、通常の一方向または双方向レプリケーションジョブではオブジェクトは選択されない場合があります。これは、

LifeCycle Manager または BIAR コマンドラインを使用する場合、レプリケート元システムとレプリケート先システムの内部クロックが同期しない場合があるからです。

> ⓘ 注記
>
> レプリケート元サイトで複製中の領域に新しいオブジェクトをインポートした後は、“レプリケート元から最新表示”レプリケーションジョブを実行することをお勧めします。レプリケート先サイトで複製中の領域に新しいオブジェクトをインポートした後は、“レプリケート先から最新表示”レプリケーションジョブを実行することをお勧めします。

シナリオ **3:** スケジュールされたレプリケーション時間の間。

オブジェクトを複製中の領域に追加し、次にスケジュールされているレプリケーション時間まで待てない場合は、“レプリケート元から最新表示”および“レプリケート先から最新表示”レプリケーションジョブを使用できます。オブジェクトが追加された領域を明確に選択することで、コンテンツを迅速に複製できます。

> ⓘ 注記
>
> このシナリオは、大きなレプリケーション一覧に対して実行すると時間がかかるので、頻繁に使用しないことをお勧めします。たとえば、時間単位でスケジュールされた、[レプリケート元から最新表示]モードまたは[レプリケート先から最新表示]モードで実行されるレプリケーションジョブを作成する必要はありません。これらのモードは、“今すぐ実行”する場合か、または頻度の低いスケジュールで使用してください。

> ⓘ 注記
>
> 場合によっては、競合解決を使用できないことがあります。たとえば、“レプリケート元から最新表示”では、レプリケート先サイトが優先されるオプションがブロックされたり、“レプリケート先から最新表示”では、レプリケート元が優先されるオプションがブロックされたりします。

27.5 サードパーティユーザとグループの複製

フェデレーションでは、サードパーティのユーザとグループ、特に Active Directory(AD)および LDAP のユーザおよびグループを複製することができます。

> → ヒント
>
> これらの種類のユーザとグループまたはその個人用コンテンツ(お気に入りフォルダや受信ボックスなど)を複製する場合は、この節を参照してください。

ユーザとグループのマッピング

1. ユーザとグループをレプリケート元サイトでマップしてフェデレーションでユーザとグループを正しく複製します。
2. マップしたユーザとグループをレプリケート先サイトへ複製します。

> ⓘ 注記
>
> レプリケート先サイトではグループとユーザを個別にマップしないでください。 個別にマップすると、それらのグループとユーザはレプリケート先サイトとレプリケート元サイトで異なる一意の識別を持つことになり、フェデレーションはユーザまたはグループを照合できなくなります。

例

管理者は、User A を含む Group A をレプリケート元サイトとレプリケート先サイトでマップします。 Group A と User A の両方が、レプリケート元サイトとレプリケート先サイトで異なる一意の識別子を持つことになります。 レプリケーション中、フェデレーションはそれらを照合できず、Group A と User A はエイリアスが競合しているため複製されません。

> ⓘ 注記
>
> サードパーティユーザまたはグループを複製する前に、レプリケート先サイトは、AD または LDAP 認証を使用するように設定されている必要があります。 ただし、AD または LDAP を使用するようにレプリケート先サイトを設定して、ディレクトリサーバまたはドメインコントローラと通信できるようにする必要もあります。

> ⓘ 注記
>
> AD または LDAP グループを初めて複製した後に、このグループ内のユーザは、AD/LDAP グループチャートが最新表示されるまではログオンできなくなります。 これは、約 15 分ごとに自動的に発生します。 AD/LDAP グループチャートを手動で最新表示するには、CMC の[認証]ページで、[*Windows AD*]または[*LDAP*]をダブルクリックし、[更新]をクリックします。

> ⓘ 注記
>
> サードパーティグループを複製する場合は注意が必要です。 ユーザをディレクトリサーバ内のグループに追加すると、それらのユーザは両方のサイトにログオンできるようになります。 AD 認証または LDAP 認証のこのセキュリティの問題は、フェデレーションとは無関係です。
>
> レプリケート先サイトとレプリケート元サイトに個別にログオンするか、グループメンバーシップが CMC の[認証]ページの[更新]ボタンを使用して両方のサイトで更新されると、両方のサイトでユーザアカウントが作成されます。 アカウントの一意の識別子が異なるため、フェデレーションはそれらを正しく複製できません。
>
> 1 つのサイトでアカウントを作成してから、他のサイトに複製することが重要です。

27.6 ユニバースおよびユニバース接続の複製

BI プラットフォームデプロイメント間でユニバースを複製するためにフェデレーションを使用する場合、事前に計画を立てておくことが重要です。ユニバースオブジェクトは、基になるユニバース接続がないと機能しません。

ユニバース接続オブジェクトには、レポーティングデータベースへの接続に必要な情報が含まれています。正しく機能するためには、ユニバース接続オブジェクトに有効な情報が含まれており、確立されるデータベース接続が許可されている必要があります。

> **注記**
>
> 双方向レプリケーションを使用して、ユニバース接続を含めずにレプリケート元サイトからレプリケート先サイトへユニバースを複製すると、以降のレプリケーションで、レプリケート元サイトのユニバースとレプリケート元サイトのユニバース接続との関係が上書きまたは削除される可能性があります。これを回避するためには、常にユニバース接続をユニバースと共に複製します。

依存するユニバース接続が必ずユニバースと共に複製されるようにするために、ユニバースを含むレプリケーション一覧を作成または変更する際、常に次のオプションを選択します。

- 選択したユニバースで使用される接続を含める
- 選択したユニバースに必要なユニバースを含める

> **注記**
>
> ユニバースとそのユニバース接続との関係が上書きまたは削除されている場合は、Universe Designer でユニバースを開き、ファイル > パラメータ の順に選択して、接続情報を変更します。

次の 2 つの例では、ユニバースとその関連のユニバース接続を複製するプロセスを示します。

例

ユニバースおよびユニバース接続を複製している場合は、レプリケート元サイトの接続環境とレプリケート先サイトの接続環境が一致していることを確認する必要があります。

たとえば、ユニバース接続で “TestODBC” という名前の ODBC 接続を使用している場合は、レプリケート先環境にも “TestODBC” という名前の適切に設定された ODBC 接続が必要です。ODBC 接続は、同じデータベースにも、別のデータベースにも解決できます。この接続を使用するユニバースで接続の問題が発生しないようにするには、データベースのスキーマが同じであることが必要です。

例

レプリケート先サイトに複製したユニバースで、レプリケート元のユニバースが使用しているデータベースと異なるデータベースを使用する場合、ユニバース接続を複製しますが、レプリケート先サイトの接続情報が目的のデータベースを指すようにします。

たとえば、レプリケート元サイトのユニバース接続が “DatabaseA” を指す “Test” という名前の ODBC 接続を使用している場合は、レプリケート先サイトの ODBC 接続が名前は同じ “Test” でも “DatabaseB” を指すようにします。

27.7 レプリケーション一覧の管理

レプリケーション一覧には、BI プラットフォームデプロイメント内にある、一緒に複製することができるユーザ、グループ、レポートなどのコンテンツが含まれます。レプリケーション一覧には、CMC からアクセスします。

複製できるコンテンツタイプを以下の表で説明します。

カテゴリ	サポートされるオブジェクト
リポジトリオブジェクト	ビジネスビュー、DataConnection、LOV、データファンデーションなどを含むオブジェクト。 **注記** すべてのオブジェクトはサポートされますが、個々のレベルではサポートされません。
レポート	Crystal レポート、Web Intelligence ドキュメント、および Dashboards オブジェクト。 **注記** フルクライアントアドインおよびテンプレートはサポートされます。
サードパーティオブジェクト	Excel、PDF、PowerPoint、Word、テキストファイル、リッチテキストファイル、Shockwave ファイル。
ユーザ	ユーザ、グループ、受信ボックス、お気に入り、個人用カテゴリ
BI プラットフォーム	フォルダ、イベント、カテゴリ、カレンダ、カスタムロール、ハイパーリンク、ショートカット、プログラム、プロファイル、オブジェクトパッケージ、その他。
ユニバース	ユニバース、接続、ユニバースオーバーロード

注記

次のオブジェクトをレプリケート元サイトで作成し、レプリケート先サイトに複製する必要があります。レプリケート先サイトでこれらのオブジェクトを作成してから、それらをレプリケート元サイトに複製すると、それらのオブジェクトはレプリケート元サイトで機能しません。

- ビジネスビュー
- ビジネスエレメント
- データファンデーション
- データコネクション
- 値の一覧
- ユニバースオーバーロード

27.7.1 レプリケーション一覧の作成

レプリケーション一覧は、CMC の [レプリケーション一覧] エリアにあります。フォルダやサブフォルダを作成してレプリケーション一覧を整理することができます。

27.7.1.1 [レプリケーション一覧] フォルダを作成する

1. CMC の [レプリケーション一覧] エリアを表示します。
2. [レプリケーション一覧] をクリックします。
3. 管理 > 新規 > フォルダ の順にクリックします。
   [フォルダの作成] ダイアログボックスが表示されます。
4. フォルダ名を入力し、[OK] をクリックします。
   これで、このフォルダ内にレプリケーション一覧を作成できるようになりました。

27.7.1.2 レプリケーション一覧を作成する

1. CMC の [レプリケーション一覧] エリアを表示します。
2. 新しいレプリケーション一覧を保存するフォルダを選択します。
3. 管理 > 新規 > 新しいレプリケーション一覧 をクリックします。
   [新しいレプリケーション一覧] ダイアログボックスが表示されます。
4. レプリケーション一覧のタイトルと説明を入力します。
5. 詳細オプションを指定する場合は、[レプリケーション一覧のプロパティ] リンクをクリックします。

   これにより、レプリケート元サイトからレプリケート先サイトに自動的に複製する依存関係を指定することができます。
6. 以下の表で説明する必要なオプションを選択します。

依存関係オブジェクトオプション	定義
選択したユーザの個人用フォルダを含む	選択したユーザの個人用フォルダとそのコンテンツを複製します。
選択したユーザの個人用カテゴリを含む	選択したユーザの個人用カテゴリを複製します。
選択したレポートのユニバースを含む	選択したレポートオブジェクトが依存するユニバースを複製します。
選択したユーザグループのメンバーを含む	選択したグループ内のユーザを複製します。
選択したユニバースに必要なユニバースを含む	ほかのユニバースに依存するユニバースを複製します。
選択したユーザの受信ボックスを含む	選択したユーザの受信ボックスとそのコンテンツを複製します。
選択したユニバースのユーザグループを含む	ユニバースのオーバーロードに関連付けられたユーザグループを複製します。
選択したオブジェクトに設定されるアクセスレベルを含む	選択したオブジェクトに設定されているアクセスレベルを複製します。
選択したカテゴリのドキュメントを含む	選択したカテゴリに含まれている Word、Excel、PDF などのすべてのドキュメントを複製します。
選択したユーザとユーザグループのプロファイルを含む	選択したユーザまたはグループに関連付けられているプロファイルを複製します。
選択したユニバースによって使用される接続を含む	選択したオブジェクトによって使用されるユニバース接続オブジェクトを複製します。

> ⓘ 注記
>
> BI プラットフォームの一部のオブジェクトは他のオブジェクトに依存しています。たとえば、Web Intelligence ドキュメントは、構造およびコンテンツを基になるユニバースに依存しています。Web Intelligence ドキュメントを複製しても、そのレポートが使用するユニバースを選択しない場合、ユニバースがすでに複製されていない限り、レプリケーションはレプリケート先サイトで機能しません。ただし、選択したレポートのユニバースを含むが有効な場合、フェデレーションによってレポートが依存するユニバースが自動的に複製されます。

7. [次へ] をクリックします。
8. 1 つまたは複数のオブジェクトを選択してレプリケーション一覧に追加します。
   - 矢印ボタンを使用して [利用可能なオブジェクト] フォルダのオブジェクトを追加または削除します。
   - または、[すべてレプリケート] の [リポジトリオブジェクト] をクリックし、すべてのビジネスビュー、ビジネスエレメント、データファンデーション、データ接続、値の一覧、およびリポジトリオブジェクト (レポートイメージや関数を含む) を複製します。

> ⓘ 注記
>
> [使用できるオブジェクト] フォルダにある最上位フォルダを複製することはできません。

9. [保存して閉じる] をクリックします。

27.7.2 レプリケーション一覧の変更

レプリケーション一覧を作成したら、そのプロパティまたはオブジェクトを変更できます。

27.7.2.1 レプリケーション一覧のプロパティを変更する

1. CMC の [レプリケーション一覧] エリアを表示します。
2. 変更するレプリケーション一覧を選択します。
3. 管理 > プロパティ をクリックします。
   [一般プロパティ] ダイアログボックスが表示されます。
4. タイトルと説明を変更します。[一般プロパティ] ダイアログボックスが開いている間は、選択したレプリケーション一覧の他の領域も変更できます。
5. 依存関係オプションを変更するには、ナビゲーション一覧の [レプリケーション一覧のプロパティ] をクリックします。
6. [保存して閉じる]をクリックします。

関連情報

レプリケーション一覧の作成 [935 ページ]

27.7.2.2 レプリケーション一覧でオブジェクトを変更する

1. CMC の [レプリケーション一覧] エリアを表示します。
2. レプリケーション一覧を選択します。
3. アクション > レプリケーション一覧の管理 の順にクリックします。
   [レプリケーション一覧の管理] ダイアログボックスが表示され、レプリケーション一覧に含まれるオブジェクトの一覧が表示されます。
4. 必要に応じてオブジェクトを追加または削除します。
5. [保存して閉じる] をクリックします。

関連情報

レプリケーション一覧の作成 [935 ページ]

27.8 リモート接続の管理

リモート接続オブジェクトには、リモートの BI プラットフォームデプロイメントへの接続に必要な情報が含まれています。

> **注記**
>
> リモート接続オブジェクトは、レプリケート先サイトの BI プラットフォームデプロイメントで作成されます。リモート接続はレプリケート元サイトです。

リモート接続は、CMC の [フェデレーション] エリアで確認できます。

27.8.1 リモート接続の作成

フェデレーションのリモート接続は、リモートの BI プラットフォームデプロイメントに接続します。複製するコンテンツがあるレプリケート元サイトへの接続を確立するには、最初にレプリケート先サイトでリモート接続を作成する必要があります。

リモート接続を整理するために、フォルダおよびサブフォルダを作成できます。

27.8.1.1 リモート接続フォルダを作成する

1. CMC の [フェデレーション] エリアを表示します。
2. [リモート接続] をクリックします。

3. 管理 > 新規 > フォルダ の順にクリックします。
   [フォルダの作成] ダイアログボックスが表示されます。
4. フォルダ名を入力し、[*OK*] をクリックします。
   これで、このフォルダ内にリモート接続を作成できるようになりました。

27.8.1.2 リモート接続を作成する

リモートの BI プラットフォームデプロイメントに接続するには、フェデレーションでリモート接続を作成する必要があります。

1. CMC の[フェデレーション]エリアを表示します。
2. [リモート接続] をクリックします。
3. 管理 > 新規 > 新しいリモート接続 の順にクリックします。
   [新しいリモートシステム接続] ダイアログボックスが表示されます。
4. 必要に応じてタイトル、説明および関連フィールドを入力します。

> **注記**
>
> ["説明"] および ["クリーンアップオブジェクトの数を次に制限します"] 以外のフィールドはすべて必須です。

フィールド	説明
タイトル	リモート接続オブジェクトの名前。
説明	リモート接続オブジェクトの説明。（オプション）
リモートシステム Web サービス URI	Java アプリケーションサーバに自動的にデプロイされるフェデレーション Web サービスへの URL。 BI プラットフォーム では、レプリケート元サイトまたはレプリケート先サイト、あるいは別のデプロイメントのどのフェデレーション Web サービスでも使用できます。 以下の形式を使用します。 **`http://<application_yourserver_machine_name>:<port>/dswsbobje`**. 例: **`http://<mymachine.mydomain.com>:<8080>/dswsbobje`**
リモートシステム CMS	フェデレーション Web サービスでアクセスできる接続先 CMS の名前。 これは、レプリケート元サイトの CMS と見なされます。 形式は **`CMS 名:ポート`** です。 例: **`<mymachine>:6400`** **注記** デフォルトポート 6400 を使用する場合、ポートの指定は省略できます。

フィールド	説明
ユーザ名	レプリケート元サイトに接続する際に使用するユーザ名。 **注記** 使用しているユーザ名に、レプリケート元サイトのデプロイメントでレプリケーション一覧の表示権限があることを確認してください。
パスワード	レプリケート元サイトに接続するユーザアカウントのパスワード。
認証	レプリケート元サイトに接続する際のアカウント認証の種類。 オプションは、Enterprise、AD または LDAP です。
クリーンアップ間隔 (時間)	このリモート接続オブジェクトを使用するレプリケーションジョブでオブジェクトのクリーンアップを行う間隔。 正の整数のみ入力します。 単位は時間数です。 デフォルトは 24 です。
クリーンアップオブジェクトの数を次に制限します	レプリケーションジョブがクリーンアップするオブジェクトの数。 (オプション)

5. [*OK*] をクリックします。

27.8.2 リモート接続の変更

リモート接続を作成したら、そのプロパティとセキュリティのオプションを変更することができます。

リモート接続を変更する

1. CMC の [フェデレーション] エリアを表示します。
2. [リモート接続] をクリックします。
3. 変更するリモート接続をダブルクリックします。
   [リモート接続のプロパティ] ダイアログボックスが表示されます。次のプロパティを変更できます。
   - タイトル
   - 説明
   - リモートシステム *Web* サービス *URI*
   - リモートシステム *CMS*
   - ユーザ名
   - パスワード
   - 認証
   - クリーンアップ間隔 (時間)
   - クリーンアップオブジェクトの数を次に制限します
4. 変更を指定します。
5. [保存して閉じる]をクリックします。

27.9 レプリケーションジョブの管理

レプリケーションジョブはスケジュールに基づいて実行されるオブジェクトの種類で、フェデレーション内の 2 つの BI プラットフォームデプロイメント間でコンテンツを複製するために使用します。

> **注記**
>
> レプリケート先サイトで複製されたオブジェクトには、次の図のようなレプリケーションアイコンが付けられます。 競合が発生すると、次の図のように、オブジェクトには競合アイコンが付けられます。

CMC の [フェデレーション] エリア内の [リモート接続] フォルダで、レプリケーションジョブの一覧を表示できます。

27.9.1 レプリケーションジョブの作成

レプリケーションジョブは、フェデレーション内の 2 つの BI プラットフォームデプロイメント間のコンテンツを複製するために必要です。各レプリケーションジョブには、1 つのリモート接続と 1 つのレプリケーション一覧を関連付ける必要があります。

27.9.1.1 レプリケーションジョブを作成する

1. CMC の[フェデレーション]エリアを表示します。
2. [リモート接続] をクリックします。
3. 新しいレプリケーションジョブを含めるリモート接続を選択します。

   > **警告**
   >
   > CMC はリモート接続 URI の Web サービスに接続して、ウィザードで処理を進めることができるようにする必要があります。

4. 管理 > 新規 > 新しいレプリケーションジョブ の順にクリックします。
   [新しいレプリケーションジョブ] ダイアログボックスが表示されます。
5. レプリケーションジョブのタイトルと説明を入力します。
6. [次へ] をクリックします。
   レプリケート元サイトで使用可能なレプリケーション一覧のリストが表示されます。
7. レプリケーションジョブで使用する [レプリケーション一覧] を選択します。
8. [次へ] をクリックします。
9. 以下の表で説明する設定オプションを選択します。

オプション	説明
レプリケート先でオブジェクトのクリーンアップを有効にする	レプリケート元サイトで作成されているオブジェクトが削除された場合、レプリケーションジョブでレプリケート先サイトの複製オブジェクトをすべて削除します。 **注記** オブジェクトのクリーンアップでは、レプリケーション一覧で選択した依存関係またはオブジェクトを使用して複製されたオブジェクトは削除されません。
一方向レプリケーション	オブジェクトがレプリケート元サイトからレプリケート先サイトにのみ複製されることを指定します。 レプリケーション後にレプリケート元サイトのオブジェクトに行われた変更はレプリケート先サイトに複製されますが、レプリケート先サイトの変更はレプリケート元サイトに複製されません。
双方向レプリケーション	オブジェクトが双方向、つまり、レプリケート元サイトからレプリケート先、およびレプリケート先からレプリケート元サイトへ複製されることを指定します。 レプリケーションの後に一方のサイトでこれらのオブジェクトに行われた変更は、もう一方のサイトに自動的に複製されます。
レプリケート元サイトが優先されます	レプリケート元サイトのオブジェクトとレプリケート先サイトの複製バージョン間で競合が検出された場合、レプリケート元サイトのバージョンが優先されることを指定します。
自動競合解決なし	検出された競合を解決するためのアクションは実行しないことを指定します。
レプリケート先サイトが優先されます (双方向レプリケーションでのみ有効)	レプリケート元サイトのオブジェクトとレプリケート先サイトの複製バージョン間で競合が検出された場合、レプリケート先サイトのバージョンが優先されることを指定します。
通常のレプリケーション	レプリケーションジョブが通常どおり動作することを指定します。
レプリケート元から最新表示	コンテンツが変更されているかどうかに関係なく、レプリケート元サイトからレプリケート先サイトへすべてのコンテンツが複製されます。 レプリケーション一覧全体、またはその一部だけを複製できます。
レプリケート先から最新表示 (双方向レプリケーションでのみ有効)	コンテンツが変更されているかどうかに関係なく、レプリケート先サイトからレプリケート元サイトへすべてのコンテンツが複製されます。 レプリケーション一覧全体、またはその一部だけを複製できます。
すべてのオブジェクトを複製 (双方向レプリケーションでのみ有効)	レプリケーション一覧全体を複製します。 **注記** これは最も完全なオプションですが、最も時間がかかります。
リモートスケジュールを複製 (双方向レプリケーションでのみ有効)	レプリケート先サイトからレプリケート元サイトへ保留中のリモートインスタンスを複製し、レプリケート元サイト

オプション	説明
	からレプリケート先サイトへ完了したインスタンスを複製します。
ドキュメントテンプレートを複製	インスタンスではない (ローカルで実行されるオブジェクトまたはリモートスケジュールのチェック対象となるレポート) オブジェクトをすべて複製します。 これには、ユーザ、グループ、フォルダ、レポートなどが含まれます。
ローカルで実行して完了したインスタンスを複製	完了したインスタンスをレプリケート先サイトからレプリケート元サイトに複製します。

10. [*OK*] をクリックします。

27.9.2 レプリケーションジョブのスケジュール

レプリケーションジョブを作成したら、レポートを 1 回だけまたは定期的に実行するようにスケジュールできます。レプリケート元サイトから、1 つのレプリケート先サイトで複数のレプリケーションジョブをスケジュールすることもできます。

> **注記**
>
> 1 つのレプリケート先サイトで複数のレプリケーションジョブをスケジュールする場合は、一度に 1 つのレプリケーションジョブのみレプリケート元サイトに接続できます。接続しようとしている他のすべてのレプリケーションジョブは、保留状態に移行し、レプリケート元サイトに自動的に接続できるようになるまでそのままになります。

27.9.2.1 レプリケーションジョブをスケジュールする

1. CMC の [フェデレーション] エリアを表示します。
2. スケジュールするレプリケーションジョブを選択します。
3. アクション > スケジュール の順にクリックします。
4. 目的のスケジュールオプションを選択します。

27.9.3 レプリケーションジョブの変更

フェデレーションにレプリケーションジョブを作成したら、そのプロパティを変更することができます。

27.9.3.1 レプリケーションジョブを変更する

1. CMC の [フェデレーション] エリアを表示します。
2. [リモート接続] フォルダをクリックします。
3. 変更するレプリケーションジョブを含むリモート接続オブジェクトを選択します。
4. 変更するレプリケーションジョブを選択します。
5. 管理 > オブジェクトプロパティの管理 をクリックします。
6. 必要に応じて、[プロパティ]、[スケジュール]、[履歴]、[レプリケーション一覧]、および[ユーザセキュリティ]を表示および変更します。

セクション	説明
プロパティ	名前、説明、その他の一般的なプロパティおよびレプリケーションジョブのオプションを変更します。
スケジュール	レプリケーションジョブが定期的なスケジュールで実行されるように設定します。
履歴	レプリケーションジョブのすべてのインスタンスを表示および管理します。
レプリケーション一覧	選択したレプリケーション一覧を変更します。
ユーザセキュリティ	レプリケーションジョブにアクセス権を設定します。

27.9.4 レプリケーションジョブ後のログの表示

レプリケーションジョブを実行するたびに、フェデレーションでは自動的にレプリケート先サイトにログファイルが作成されます。ログファイルでは XML 1.1 標準を使用します。また、XML 1.1 を使用する Web ブラウザが必要です。

レプリケーションログを表示する

1. CMC の[フェデレーション]エリアを表示します。
2. [すべてのレプリケーションジョブ]をクリックします。
3. 一覧から[レプリケーションジョブ]を選択します。
4. [プロパティ]をクリックします。
   選択したレプリケーションジョブの[プロパティ]ページが表示されます。
5. [履歴]をクリックします。
6. ログファイルの[インスタンスの日時]をクリックして成功したレプリケーションジョブを表示するか、[失敗]ステータスをクリックして失敗したレプリケーションジョブのログファイルを表示します。
7. 目的のインスタンスを選択して、ログファイルを表示します。
   ログファイルは XML 形式で生成され、XSL フォームを使用して、情報を書式設定し、HTML ページに表示できるようにします。

   Adaptive Job Server を含む Server Intelligence Agent を実行中のコンピュータから XML ログにアクセスすることができます。ログファイルは次の場所にあります。

   - Windows では、`<InstallDir>¥SAP BusinessObjects XI 4.0¥logging` です。

- Unix では、`<InstallDir>/sap_bobj/logging` です。

27.10 オブジェクトのクリーンアップの管理

フェデレーションでは、レプリケート元サイトから削除したすべてのオブジェクトが、各レプリケート先サイトからも削除されるように、レプリケーションプロセスのライフサイクルを通じてオブジェクトのクリーンアップを実行する必要があります。

オブジェクトのクリーンアップには、リモート接続とレプリケーションジョブの 2 つの要素があります。リモート接続オブジェクトでは一般的なクリーンアップオプションを定義し、レプリケーションジョブでは適切な間隔が経過したときにクリーンアップを実行します。

27.10.1 オブジェクトのクリーンアップ方法

別個のレプリケーションジョブが同じリモート接続を使用する場合、それらのレプリケーションジョブは、オブジェクトのクリーンアップ中に連携して動作します。つまり、レプリケーションジョブによって、そのレプリケーション一覧内のオブジェクトだけでなく、同じリモート接続を使用する他のレプリケーション一覧内のオブジェクトもクリーンアップされます。リモート接続は、レプリケーションジョブの親が同じリモート接続オブジェクトである場合のみ、同じと見なされます。

例

レプリケーションジョブ A と B はオブジェクト A とオブジェクト B を複製します。これらのジョブは、同じレプリケート元サイトから複製され、同じリモート接続を使用します。レプリケート元サイトでオブジェクト B を削除すると、レプリケーションジョブ A はオブジェクト B が削除されたことを確認します。レプリケーションジョブ B がオブジェクト B を複製している場合でも、オブジェクト B はレプリケート先サイトからも削除されます。レプリケーションジョブ B が実行されるときに、オブジェクトのクリーンアップを実行する必要はありません。

> **注記**
>
> オブジェクトのクリーンアップ中は、レプリケート先サイトのオブジェクトだけが削除されます。レプリケーションに含まれるオブジェクトをレプリケート元サイトから削除すると、そのオブジェクトはレプリケート先サイトから削除されます。ただし、オブジェクトがレプリケート先サイトから削除された場合、レプリケーションジョブが双方向レプリケーションモードで実行されている場合でも、そのオブジェクトはオブジェクトのクリーンアップ中にレプリケート元から削除されません。
>
> レプリケーション一覧から削除されたオブジェクトは、レプリケート先サイトから削除されません。レプリケーション一覧で指定されたオブジェクトを正しく削除するには、レプリケート先サイトとレプリケート元サイトの両方でオブジェクトを削除する必要があります。依存関係の計算を通じて複製されたオブジェクトは削除されません。

27.10.2 オブジェクトのクリーンアップの制限

リモート接続オブジェクトで、レプリケーションジョブが一度にクリーンアップするオブジェクトの数を定義できます。フェデレーションでは、クリーンアップジョブが終了した場所が自動的に追跡されます。このように、レプリケーションジョブを次に実行すると、終了した時点の次のクリーンアップジョブが開始されます。

> → ヒント
>
> レプリケーションジョブを高速で実行するには、クリーンアップ対象のオブジェクトの数を制限します。

例

レプリケーションジョブ A と B はオブジェクト A とオブジェクト B を複製しています。両方のオブジェクトは、同じレプリケート元サイトから複製され、同じリモート接続を使用します。

レプリケート元サイトがオブジェクト B を削除すると、オブジェクトの制限が 1 に設定されている場合、次にレプリケーションジョブ A が実行されたときに、レプリケーションジョブ A はオブジェクト A が削除されているかどうか確認します。このように、オブジェクト B の削除はチェックされず、オブジェクト B は削除されません。

次に、レプリケーションジョブ B が実行され、レプリケーションジョブ A が終了した地点からオブジェクトのクリーンアップが開始されます。レプリケーションジョブ B は、オブジェクト B が削除されているかどうか確認し、レプリケート先サイトかオブジェクト B を削除します。このオプションについては、リモート接続オブジェクトのプロパティ [“クリーンアップオブジェクト数を次の数に制限する”] で確認できます。

> ⓘ 注記
>
> このオプションを選択しない場合、このリモート接続を使用するすべてのレプリケーションジョブは、クリーンアップの対象となる可能性のあるすべてのオブジェクトをチェックします。

27.10.3 オブジェクトのクリーンアップ間隔

レプリケーションジョブでオブジェクトのクリーンアップを実行する間隔は、リモート接続の [“クリーンアップ間隔”]フィールドで設定できます。

> ⓘ 注記
>
> 正の整数を入力する必要があります。これは、オブジェクトのクリーンアップ処理間に待機する時間数を表します。

例

レプリケーションジョブ A と B はオブジェクト A とオブジェクト B を複製します。両方のオブジェクトは、同じレプリケート元サイトから複製され、同じリモート接続を使用します。

オブジェクト B がレプリケート元サイトから削除され、次のすべての条件が満たされている場合、レプリケーションジョブはオブジェクト A が削除されているかどうか確認します。

- オブジェクト制限が 1
- クリーンアップ間隔が 150 時間
- 次にレプリケーションジョブ A が実行される

オブジェクト制限が 1 であるため、レプリケーション先サイトのオブジェクト B はチェックまたは削除されません。

レプリケーションジョブ A が初期チェックを実行してから 150 時間後に次のクリーンアップが行われます。レプリケーションジョブ A および B は、制限の 150 時間が経過するまでに何度も実行できますが、オブジェクトのクリーンアップは実行されません。150 時間が経過すると、レプリケーションジョブが実行され、クリーンアップが実行されます。次に、オブジェクト B がレプリケーション元サイトから削除されていることを確認し、レプリケーション先サイトでオブジェクト B を削除します。

有効化/無効化オプション

各レプリケーションジョブを、オブジェクトのクリーンアップに参加させることができます。レプリケーションジョブの [“レプリケート先でオブジェクトのクリーンアップを有効にする”] オプションで、オブジェクトのクリーンアップを実行するかどうかを指定できます。優先度の高いレプリケーションジョブで、オブジェクトのクリーンアップに参加させずに、できるだけ早く実行できるようにする場合は、オブジェクトのクリーンアップを無効にします。

関連情報

オブジェクトのクリーンアップの制限 [946 ページ]

27.11 競合の検出と解決の管理

フェデレーションでは、レプリケート元サイトとレプリケート先サイトの両方でオブジェクトのプロパティが変更されると競合が発生する場合があります。1 つのオブジェクトにつき、最上位プロパティとネストされているプロパティの両方の競合がチェックされます。たとえば、レプリケート元サイトとレプリケート先サイトの両方でレポートまたはレポート名が変更されると競合が発生することがあります。

競合が作成されないインスタンスもあります。たとえば、レプリケート元サイトでレポート名が変更され、レプリケート先サイトで複製バージョンの説明が変更された場合、変更は共にマージされ、競合は発生しません。

27.11.1 一方向レプリケーションの競合の解決

一方向レプリケーションでは、競合解決について次の 2 つの選択肢があります。

レプリケート元サイトが優先されます

一方向レプリケーションで競合が発生すると、レプリケート元サイトのオブジェクトが優先されます。レプリケート先サイトでのオブジェクトの変更は、レプリケート元サイトの情報によって上書きされます。たとえば、レプリケート元サイトとレプリケート先サイトの両方でレポートが変更される場合、レプリケート先サイトでの変更は、次のレプリケーションジョブ実行時にレプリケート元サイトのバージョンによって上書きされます。

> ⓘ 注記
>
> 競合は自動的に解決されるため、ログファイルに競合は記録されず、競合オブジェクトリストにも表示されません。

自動競合解決なし

競合が発生し、“自動競合解決なし”を選択している場合、競合は解決されません。また、ログファイルに競合は記録されず、競合オブジェクトリストにも表示されません。

管理者は、CMC の[フェデレーション]エリアを使用して競合しているすべての複製オブジェクトのリストにアクセスできます。競合しているオブジェクトは、レプリケート元サイトへの接続に使用したリモート接続でグループ化されます。これらのリストにアクセスするには、CMC の[フェデレーション]エリアの[複製エラー]フォルダに移動して、目的のリモート接続を選択します。レプリケート先サイトで複製されたすべてのオブジェクトには、レプリケーションアイコンが付けられます。競合が発生すると、オブジェクトには競合アイコンが付けられます。プロパティページには警告メッセージも表示されます。

> ⓘ 注記
>
> リモート接続を使用するレプリケーションジョブが完了すると、リストが更新されます。リストには、特定のリモート接続を使用するすべてのレプリケーションジョブについて競合しているすべてのオブジェクトが含まれます。

> ⓘ 注記
>
> CMC およびレプリケーションジョブインスタンスへのアクセス権を持つすべてのユーザは、logfile ディレクトリに保存される XML ログにアクセスできます。レプリケート先サイトのオブジェクトのアイコンは、競合を示すアイコンになります。処理中に、競合ログが作成されます。

Abdul がレプリケート元サイトで Report A を変更します。Maria がレプリケート先サイトで複製バージョンを変更します。レポートは、両方のサイトで変更されていて解決されないため、次にレプリケーションジョブを実行したときに競合します。

レプリケート先のレポートは維持され、レプリケート元のレポートの変更は複製されません。以降のレプリケーションジョブは、競合が解決されるまで同様に動作します。レプリケート元サイトの変更は、競合を手動で解決するまで複製されません。

> ⓘ 注記
>
> この場合、オブジェクト全体が複製されません。競合していない他の変更は複製されません。

競合を手動で解決する場合には、次の **3** つのオプションがあります。

1. 競合しているオブジェクトだけを複製するレプリケーションジョブを作成します。この場合、同じリモート接続オブジェクトとレプリケーション一覧を使用します。
   レプリケート元サイトの変更を維持するには、レプリケーションジョブを作成します。次に、[レプリケーションモード]を“レプリケート元から最新表示”に設定し、[自動競合解決]を“レプリケート元サイトが優先されます”に設定します。
   レプリケート先の変更を維持するには、[レプリケーションの種類]を“双方向レプリケーション”、[レプリケーションモード]を“レプリケート先から最新表示”、および[自動競合解決]を“レプリケート先サイトが優先されます”に設定して、レプリケーションジョブを作成します。

   > ⓘ 注記
   >
   > [レプリケーションモード]で、“レプリケート元から最新表示”または“レプリケート先から最新表示”を設定し、レプリケーション一覧で競合しているオブジェクトだけを選択します。この方法では、他のオブジェクトは複製されません。次に、レプリケーションジョブの実行をスケジュールすると、レプリケーションジョブは選択したオブジェクトを複製し、指定されたとおりに競合を解決します。

2. 競合しているオブジェクトだけを複製するレプリケーションジョブを作成します。この場合、同じリモート接続オブジェクトを使用する必要があります。ただし、オプション 1 とは異なり、新しいレプリケーション一覧をレプリケート元サイトで作成できます。競合しているオブジェクトだけを使用し、このフォーカスされているレプリケーション一覧を使用する新しいレプリケーションジョブを作成します。
   レプリケート元サイトの変更を維持するためには、[自動競合解決]を“レプリケート元サイトが優先されます”に設定します。
   レプリケート先サイトの変更を維持するには、[自動競合解決]を“レプリケート先サイトが優先されます”、[レプリケーションの種類]を“双方向レプリケーション”に設定します。
3. 一方向レプリケーションジョブの場合は、レプリケート先サイトのオブジェクトだけを削除できます。レプリケーションジョブを次に実行するときに、レプリケーションジョブはレプリケート元サイトからレプリケート先サイトへオブジェクトを複製します。

   > ⓘ 注記
   >
   > オブジェクトを削除するときは注意が必要です。そのオブジェクトに依存している他のオブジェクトが削除されたり、動作しなくなったり、セキュリティを失うことがあります。オプション 1 と 2 の使用をお勧めします。

27.11.2 双方向レプリケーションの競合の解決

双方向レプリケーションの競合では、競合の検出方法として次の 3 つの方法があります。

- レプリケート元サイトが優先されます
- レプリケート先サイトが優先されます
- 自動競合解決なし

レプリケート元サイトが優先されます

競合が発生すると、レプリケート元サイトが優先され、レプリケート先サイトの変更が上書きされます。

例

Lily はレポートの名前を Report A に変更します。Malik はレプリケート先サイトの複製バージョンの名前を Report B に変更します。次にレプリケーションジョブを実行するときに、レプリケート先サイトの複製バージョンは Report A に戻ります。

この場合、競合はレプリケート元サイトでユーザの指示に従って解決されているため、ログファイルに競合は記録されず、競合オブジェクトリストにも表示されません。

レプリケート先サイトが優先されます

競合が発生すると、レプリケート先サイトでは変更が維持され、その変更がレプリケート元サイトに上書きされます。

例

Kamal はレポートの名前を Report A に変更し、Peter はレプリケート先サイトの複製バージョンの名前を Report B に変更します。レプリケーションジョブを実行すると、競合が検出されます。レプリケート先レポートの名前は Report B のまま変わりません。

また、双方向レプリケーションでは、変更はレプリケート元サイトに戻されます。このシナリオでは、レプリケート元サイトは更新されて、そのレポート名は Report B に変更されます。この場合、競合はユーザの指示に従って解決されているため、ログファイルに競合は記録されず、競合オブジェクトリストにも表示されません。

自動競合解決なし

“自動競合解決なし”を選択すると、競合は解決されません。競合はログファイルに記録され、管理者が手動で解決できます。

> ⓘ 注記
>
> オブジェクトのアイコンは、競合の存在を示すアイコンになります。

> ⓘ 注記
>
> 変更はレプリケート元サイトとレプリケート先サイトに双方向レプリケーションで複製されますが、レプリケート先サイトのバージョンにのみ競合アイコンのフラグが設定されます。

> ⓘ 注記
>
> CMC およびレプリケーションジョブインスタンスへのアクセス権を持つすべてのユーザは、logfile ディレクトリに出力される XML ログにアクセスできます。レプリケート先サイトのオブジェクトのアイコンは、競合を示すアイコンになります。処理中に、競合ログが作成されます。

管理者は、CMC の[フェデレーション]エリアを使用して競合しているすべての複製オブジェクトのリストにアクセスできます。競合しているオブジェクトは、レプリケート元サイトへの接続に使用したリモート接続でグループ化されます。これらのリストにアクセスするには、*CMC* > フェデレーション > 複製エラー > リモート接続 の順に選択します。

> ⓘ 注記
>
> リモート接続を使用するレプリケーションジョブが完了すると、リストが更新されます。リストには、特定のリモート接続を使用するすべてのレプリケーションジョブについて競合しているすべてのオブジェクトが含まれます。レプリケート先サイトで複製されたすべてのオブジェクトには、レプリケーションアイコンが付けられます。競合が発生すると、オブジェクトには競合アイコンが付けられます。

例

Michael がレプリケート元サイトで Report A を変更します。Damien がレプリケート先サイトで複製バージョンを変更します。レポートは、両方のサイトで変更されていて解決されないため、次にレプリケーションジョブを実行したときに競合します。

レプリケート先のレポートは維持され、レプリケート元のレポートの変更は複製されません。以降のレプリケーションジョブは、競合が解決されるまで同様に動作します。レプリケート元サイトの変更は、管理者または委任管理者が競合を手動で解決するまで複製されません。

> ⓘ 注記
>
> この場合、オブジェクト全体が複製されません。競合していない他の変更は複製されません。

> ⓘ 注記
>
> CMC およびレプリケーションジョブインスタンスへのアクセス権を持つすべてのユーザは、logfile ディレクトリに出力される XML ログにアクセスできます。レプリケート先サイトのオブジェクトのアイコンは、競合を示すアイコンになります。処理中に、競合ログが作成されます。

管理者は、CMC のフェデレーションエリアを使用して競合しているすべての複製オブジェクトのリストにアクセスできます。競合しているオブジェクトは、レプリケート元サイトへの接続に使用したリモート接続でグループ化されます。これらのリストにアクセスするには、*CMC* > フェデレーション > 複製エラー > リモート接続 の順に選択します。

> ⓘ 注記
>
> リモート接続を使用するレプリケーションジョブが完了すると、リストが更新されます。リストには、特定のリモート接続を使用するすべてのレプリケーションジョブについて競合しているすべてのオブジェクトが含まれます。レプリケート先サイトで複製されたすべてのオブジェクトには、レプリケーションアイコンが付けられます。競合が発生すると、オブジェクトには競合アイコンが付けられます。

競合を手動で解決する場合には、次の **3** つのオプションがあります。

1. 競合しているオブジェクトだけを複製するレプリケーションジョブを作成します。この場合、同じリモート接続オブジェクトとレプリケーション一覧を使用します。

レプリケート元サイトの変更を維持するには、レプリケーションジョブを作成します。次に、[レプリケーションモード]を“レプリケート元から最新表示”に設定し、[自動競合解決]を“レプリケート元サイトが優先されます”に設定します。
レプリケート先の変更を維持するには、レプリケーションジョブを作成し、[レプリケーションの種類]を“双方向レプリケーション”、[レプリケーションモード]を“レプリケート先から最新表示”、および[自動競合解決]を“レプリケート先サイトが優先されます”に設定します。

> ⓘ 注記
>
> [レプリケーションモード]で、“レプリケート元から最新表示”または“レプリケート先から最新表示”を設定し、レプリケーション一覧で競合しているオブジェクトだけを選択します。この方法では、他のオブジェクトは複製されません。次に、レプリケーションジョブの実行をスケジュールすると、レプリケーションジョブは選択したオブジェクトを複製し、指定されたとおりに競合を解決します。

2. 競合しているオブジェクトだけを複製するレプリケーションジョブを作成します。この場合、同じリモート接続オブジェクトを使用する必要があります。ただし、オプション 1 とは異なり、新しいレプリケーション一覧をレプリケート元サイトで作成できます。競合しているオブジェクトだけを使用し、このフォーカスされているレプリケーション一覧を使用する新しいレプリケーションジョブを作成します。
   レプリケート元サイトの変更を維持するためには、自動競合解決を“レプリケート元サイトが優先されます”に設定します。
   レプリケート先サイトの変更を維持するには、自動競合解決を“レプリケート先サイトが優先されます”、レプリケーションの種類を“双方向レプリケーション”に設定します。
3. 配置しないサイト上のオブジェクトを削除します。

> ⓘ 注記
>
> オブジェクトを削除するときは注意が必要です。そのオブジェクトに依存している他のオブジェクトが削除されたり、動作しなくなったり、セキュリティを失うことがあります。オプション 1 と 2 の使用をお勧めします。

レプリケート先の変更を維持するには、レプリケート元サイトのオブジェクトを削除します。次にレプリケーションジョブを実行すると、オブジェクトはレプリケート先サイトからレプリケート元サイトに複製されます。

> ⓘ 注記
>
> レプリケート元サイトのコピーを削除する場合には注意が必要です。そのオブジェクトを複製している他のレプリケート先サイトが、コピーを複製し直す前にレプリケーションジョブを実行する可能性があります。これにより、他のレプリケート先サイトでコピーが削除され、コピーが戻されるまで使用できなくなります。

レプリケート元サイトの変更を維持するには、レプリケート先サイトでオブジェクトを削除します。

27.12 フェデレーションでの Web サービスの使用

フェデレーションは、Web サービスを使用してオブジェクトおよびその変更をレプリケート元サイトとレプリケート先サイト間で送信します。フェデレーション固有の Web サービスは自動的にインストールされ、BI プラットフォームインストールにデプロイされます。ただし、ここで説明するように、Web サービスでプロパティを変更したり、デプロイメントをカスタマイズする必要がある場合があります。

→ ヒント

ファイル管理や機能を向上させるためには、フェデレーションでファイルのキャッシュを有効にしてください。

27.12.1 セッション変数

1 つのレプリケーションジョブで多くのコンテンツファイルを転送している場合は、フェデレーションの Web サービスのセッションタイムアウト期間を長くすることができます。

このプロパティは、次の場所の `dsws.properties` ファイルにあります。

```
<App Server Installation Directory>¥dswsbobje¥Web-INF¥classes
```

例:

```
C:¥Program Files¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI
4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥classes
```

セッション変数を有効にするには、次のように入力します。

```
session.timeout = x
```

ここで、“x” は目的の時間です。この “x” は秒単位で表されます。指定されない場合、デフォルト値は 1200 秒(20 分)です。

これらの新しいプロパティが有効になるのは、変更された Web アプリケーションが Web アプリケーションサーバを実行しているコンピュータ上に再デプロイされてからです。WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。WDeploy の使用については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

27.12.2 ファイルのキャッシュ

ファイルのキャッシュを使用すると、非常に大きな添付ファイルをメモリにバッファリングしなくても Web サービスで処理できます。大きい転送サイズを使用しているときにこの機能を有効にしないと、Java の仮想マシンのメモリがすべて使用され、レプリケーションは失敗する可能性があります。

ⓘ 注記

Web サービスがメモリではなくファイルに対して処理されるため、ファイルのキャッシュによってパフォーマンスは低下します。両方のオプションを組み合わせて使用し、大きい転送ファイルをファイルに送信し、小さい転送ファイルをメモリに送信することができます。

ファイルのキャッシュを有効にするには、次のディレクトリにある `Axis2.xml` ファイルを変更します。

```
<App Server Installation Directory>¥dswsbobje¥Web-Inf¥conf
```

例:

```
C:¥Program Files¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI
4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥conf
```

次を入力します。

```
<parameter name="cacheAttachments" locked="false">true</parameter>
```

```
<parameter name="attachmentDIR" locked="false">temp directory</parameter>
```

```
<parameter name="sizeThreshold" locked="false">4000</parameter>
```

> ⓘ 注記
>
> しきい値のサイズはバイト単位です。

これらの新しいプロパティが有効になるのは、変更された Web アプリケーションが Web アプリケーションサーバを実行しているコンピュータ上に再デプロイされてからです。WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。WDeploy の使用については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

27.12.3 カスタムデプロイメント

フェデレーション Web サービスは自動的にデプロイすることができますが、“federator”、“biplatform”、および“session”サービスを有効にする必要があります。フェデレーション、またはその他の Web サービスを無効にするには、対応する Web サービス `service.xml` ファイルを変更します。

BI プラットフォームの Web サービスは次の場所にあります。

```
<App Server Installation Directory>¥dswsbobje¥WEB-INF¥services
```

例:

```
C:¥Program Files¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI
4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥services
```

Web サービスを無効にする

- “service.xml”ファイルのサービス名タグに `activate` プロパティを追加し、このプロパティを false に設定します。
- Java アプリケーションサーバを再起動します。

たとえば、フェデレーションを無効にするには、次のようにします。

`services.xml` ファイルは次の場所にあります。

```
C:¥Program Files¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI
4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥services¥federator¥META-INF
```

次のサービス名を変更します。

```
<service name="Federator">
```

変更後

```
<service name="Federator" activate="false">
```

これらの新しいプロパティが有効になるのは、変更された Web アプリケーションが Web アプリケーションサーバを実行しているコンピュータ上に再デプロイされてからです。WDeploy を使用して、Web アプリケーションサーバに BOE war ファイルを再デプロイします。WDeploy の使用については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

27.13 リモートスケジュールおよびローカルで実行したインスタンス

ここでは、リモートスケジュール、ローカルで実行したインスタンス、およびインスタンス共有について説明します。これらの機能を使用すると、データが存在する場所でレポートを実行し、完了したインスタンスを適切な場所に送信できます。

27.13.1 リモートスケジュール

フェデレーションを使用して、レプリケート先サイトでレポートをスケジュールし、それをレプリケート元サイトで処理することができます。完了したインスタンスは、レプリケート先サイトに戻されます。

リモートスケジュールを有効にするには、レポートを通常どおりスケジュールし、“元のサイトで実行”オプションを有効にします。このオプションを有効にするには、スケジュール > サーバグループのスケジュール > 元のサイトで実行 をクリックします。スケジュールされたインスタンスが作成されて、保留状態になります。

リモートスケジュール中、レプリケート先サイトで送信された情報は無視されて、レポートインスタンスは保留状態のままになります。

該当のレポートを管理する次のレプリケーションジョブでリモートスケジュールが有効になっている場合、レプリケーションジョブはインスタンスを、処理を行うレプリケート元サイトにコピーします。スケジューラによって処理されるまでインスタンスは保留状態のままです。その間に、インスタンスを送信したレプリケーションジョブは、前に完了したインスタンスおよびオブジェクトの変更と共に戻ります。

インスタンスがレプリケート元サイトで処理されると、インスタンスは完了状態になります。該当のレポートを管理する次のレプリケーションジョブでリモートスケジュールが有効になっていると、完了したインスタンスを使用してレプリケート先サイトのコピーが更新されます。更新後、レプリケート先サイトのインスタンスは完了します。

> ⓘ 注記
>
> 完了した 1 つのインスタンスを戻すためには、レプリケーションジョブを 2 回実行する必要があります。

例

1. Tom は、Report A をリモートスケジュールにスケジュールします。
2. Report A がレプリケート先サイトで作成されて、保留状態になります。
3. レプリケーションジョブ A が実行されます。1 回目: レプリケート元サイトからレプリケート先サイトに変更 (前に完了したインスタンスを含む) を複製します。2 回目: 保留状態のインスタンスがレプリケート元サイトにコピーされ、さらにレプリケート先サイトからレプリケート元サイトに変更が複製されます。
4. レプリケート元サイトでは、スケジューラが保留状態のインスタンスを選択し、そのインスタンスを、処理を行う適切な Job Server に送信します。インスタンスはレプリケート元サイトで処理され、完了状態になります。

5. レプリケーションジョブ A がもう一度実行されます。レプリケーションジョブ A がレプリケート元サイトからレプリケート先サイトにコンテンツを複製すると、完了したインスタンス Report A が選択されて、変更がレプリケート先のバージョンに適用されます。
6. このタスクが完了すると、レプリケート先のバージョンが完了します。

リモートスケジュールは双方向レプリケーションジョブでのみ使用でき、“リモートスケジュールを複製”を有効にする必要があります。このオプションは、“レプリケーションフィルタ”エリアの[レプリケーションジョブのプロパティ]ページにあります。リモートでスケジュールされているジョブを、レプリケーション一覧の他のオブジェクトよりも頻繁に複製する場合があります。この場合は、2 つのレプリケーションジョブを作成します。1 つは、リモートスケジュールのみに対象を絞ったレプリケーションジョブに対して“リモートスケジュールを複製”を使用して有効にします。もう 1 つは、“ドキュメントテンプレートを複製”または“すべてのオブジェクトを複製(フィルタなし)”で有効にします。

> ⓘ 注記
>
> リモートスケジュールを有効にすると、完了したインスタンスと失敗したインスタンスがレプリケート元サイトとレプリケート先サイトの両方に表示されます。
>
> レプリケート先サイトのユーザがレポートをリモートスケジュール用にスケジュールし、レプリケート元サイトにそのユーザが存在しない場合、インスタンスはレプリケート元サイトで失敗します。失敗したインスタンスの所有者は、レプリケート元に接続する際に使用したリモート接続オブジェクトのユーザアカウントになります。
>
> リモートスケジュールに対して設定できるのは 1 つのレプリケーションジョブだけですが、レプリケーションジョブは、レポートインスタンスの祖先オブジェクトを常に複製します。つまり、レプリケーション間で変更があった場合、実際のレポート、レポートフォルダなどが複製されます。レプリケート先サイトのこれらの変更をレプリケート元サイトに複製しない場合は、セキュリティ権限を使用して、どの変更が複製されるかを制御できます。

関連情報

セキュリティアクセス権の管理 [925 ページ]

27.13.2 ローカルで実行したインスタンス

ローカルで実行したインスタンスは、レプリケート先サイトのレポートから処理されたレポートのインスタンスです。フェデレーションを使用して、完了したインスタンスをレプリケート先サイトからレプリケート元サイトに複製できます。

レプリケーションジョブで、レプリケート先サイトからレプリケート元サイトに完了インスタンスと失敗したインスタンスを複製できるようにするには、レプリケーションジョブのプロパティ > レプリケーションフィルタ > ローカルで実行して完了したインスタンスを複製 を有効にします。

レプリケーションジョブがローカルで実行したインスタンスだけを複製する場合があります。この場合は、“ローカルで実行して完了したインスタンスを複製”を有効にします。

> ⓘ 注記
>
> ローカルで実行したインスタンスがレプリケーションジョブで有効になると、完了したインスタンスと失敗したインスタンスの両方がレプリケート元サイトに複製されます。つまり、レプリケート元サイトとレプリケート先サイトの両方にコピーが存在することになります。
>
> 保留中のインスタンスは複製されません。
>
> ローカルで実行したインスタンスの所有者がレプリケート元サイトに存在しない場合、所有者は、リモート接続オブジェクトで接続に使用したユーザアカウントになります。

27.13.3 インスタンス共有

リモートスケジュールおよびローカルで実行したインスタンスをレプリケーションジョブで有効にすると、1 つのレプリケート元サイトと、同じレポートを複製している複数のレプリケート先サイトが存在する場合、インスタンス共有が発生する可能性があります。

例

Report A はレプリケート元サイトで作成され、レプリケート先サイト A と B の両方がそれを複製しています。次の場合、両方のレプリケート先サイトでインスタンス共有が発生します。

- “リモートスケジュールを複製”または“ローカルで実行して完了したインスタンスを複製”(あるいはその両方)が有効になっているレプリケーションジョブ。上記と同じレプリケーションジョブを使用してレポート A を複製する場合。
- Report A を“レプリケート元サイトで実行”されるようにスケジュールするか、またはローカルで実行されるようにスケジュールする場合。

レプリケート先サイト A および B の両方が Report A を複製し、それらに対応するレプリケーションジョブがリモートスケジュールまたはローカルで実行したインスタンスを複製している場合、レプリケート先サイト A またはレプリケート先サイト A の代わりにレプリケート元サイト(あるいはその両方)で処理されたインスタンスは、レプリケート先サイト B で共有されます。

同様に、レプリケート先サイト B で処理された、またはレプリケート元サイトで処理された(あるいはその両方)インスタンスもレプリケート先サイト A で共有されます。最終的に、レプリケート元サイトとレプリケート先サイト A および B はインスタンスの同じセットを持ちます。

インスタンス共有は多くの場合に適しています。たとえば、他のサイトのユーザが兄弟デプロイメントの情報にアクセスする必要がある場合があります。その場合、インスタンスをローカルサイトにいるユーザが表示しないようにするには、適切なセキュリティアクセス権が設定されているか確認します。たとえば、レポートオブジェクトで、ユーザが自分の所有するインスタンスのみ表示できるようにアクセス権を適用します。

> ⓘ 注記
>
> すべてのオブジェクトは、BI プラットフォームセキュリティルールに従います。ユーザとグループが適用可能なインスタンスのみ表示できるようにするためには、ユーザが所有しているインスタンスだけを表示できるようにアクセス権を設定することをお勧めします。たとえば、レポートオブジェクトで、ユーザが自分の所有するインスタンスのみ表示できるようにアクセス権を適用します。

関連情報

セキュリティアクセス権の管理 [925 ページ]

27.14 複製したコンテンツのインポートと昇格

場合によっては、BI プラットフォームシステムから別のシステムへ複製したコンテンツをインポートまたは昇格することがあります。このセクションでは、フェデレーションのこれらの機能について説明します。

> ⓘ 注記
>
> オブジェクトの移行に最も適しているのは、Administrators グループに属するメンバー、特に Administrator ユーザアカウント内のメンバーです。オブジェクトを移行するためには、多数の関連オブジェクトも移行する必要がある場合があります。すべてのオブジェクトについて必要となるセキュリティ権限を取得することは、場合によっては委任管理者アカウントでは不可能です。

27.14.1 複製したコンテンツのインポート

LifeCycle Manager を使用してコンテンツを BI プラットフォームデプロイメントから別のデプロイメントにインポートする場合、LifeCycle Manager は、インポート中の複製したオブジェクトに関連付けられているレプリケーション固有の情報をインポートしません。つまり、インポート後、オブジェクトは複製されていないものとして動作します。これは、レプリケート先サイトで複製したオブジェクトに固有の動作です。これについて、次のシナリオで説明します。

例

BI プラットフォーム A は、フェデレーションプロセスのレプリケート先サイトです。Report A は、システム A にある複製レポートで、LifeCycle Manager を使用してシステム A から BI プラットフォーム B にインポートされます。

結果: Report A が BI プラットフォーム B にコピーされると、Report A に複製された情報は含まれません。Report A にはレプリケーションアイコンが付きません。BI プラットフォーム A でオブジェクトが競合していた場合でも、そのオブジェクトはシステム B では競合しません。基本的に、オブジェクトはシステム B で生成されたオブジェクトと見なされます。

> ⓘ 注記
>
> LifeCycle Manager で選択したインポートの選択肢に応じて、CUID は同じ場合と異なる場合があります。

27.14.2 複製したコンテンツのインポートとレプリケーションの継続

複製したコンテンツをインポートしたら、インポートしたオブジェクトをフェデレーションプロセスに含めることができます。この場合、インポートしたオブジェクトが存在するシステムをレプリケート元サイトとして扱う、またはレプリケート先サイトとして扱うという 2 つのシナリオがあります。このシステムをレプリケート元サイトとして扱うには、フェデレーションの処理を通常どおり進めます。

システムをレプリケート先サイトとして扱い、レプリケート元サイトからインポートしたオブジェクトを複製するには、次の条件に従う必要があります。

- LifeCycle Manager を使用する場合は、オブジェクトの CUID を保持するようにします。
- 最初のレプリケーションジョブの競合解決が“出力元サイトが優先されます”または“出力先サイトが優先されます”に設定されるようにします。

> → ヒント
>
> あるレプリケート先サイトから別のレプリケート先サイトへ LifeCycle Manager を使用してオブジェクトをインポートするのではなく、フェデレーションのみを使用してオブジェクトを複製する方が効率がよいため、この方法をお勧めします。

例

Report A は BI プラットフォームシステム A で作成されました。システム X ではフェデレーションを使用してシステム A からシステム X へ Report A を複製しました。その後、LifeCycle Manager で Report A をシステム X からシステム Y にインポートしました。

計画: システム Y はフェデレーションをシステム A に設定し、Report A をレプリケーションの一部として維持する必要があります。システム Y はレプリケート先で、システム A はレプリケート元です。

アクション: Report A をシステム X からシステム Y にインポートしている場合、Report A の CUID を保持する必要があります。また、最初のレプリケーションジョブを実行するときに、レプリケーションジョブは Report A を複製しようとします。オブジェクトはすでにシステム Y に存在するため、レプリケーションによって競合が発生します。使用するバージョンを指定するには、競合の解決モードを“出力元サイトが優先されます”または“出力先サイトが優先されます”に設定する必要があります。

> ⓘ 注記
>
> この例では、あるレプリケート先サイトから別のレプリケート先サイトへ LifeCycle Manager を使用してオブジェクトをインポートするのではなく、フェデレーションのみを使用してオブジェクトを複製することをお勧めします。Report A はシステム A からシステム Y に複製されて、LifeCycle Manager を使用してシステム X からシステム Y にインポートする必要はありません。

27.14.3 テスト環境からのコンテンツの昇格

組織では、本稼働用環境に何かを配置する前にテストを行うことがよくあります。通常は、本稼動用マシンでフェデレーションを設定する前に、開発環境またはテスト環境の BI プラットフォームシステム間でフェデレーショ

ンをテストします。テスト環境でレプリケート元サイトとレプリケート先サイトおよびコンテンツを作成したら、次の手順を使用して、この設定を本稼動用マシンに昇格できます。

1. LifeCycle Manager を使用してテスト環境のレプリケート元サイトのコンテンツを、レプリケート元サイトとして動作する本稼動のマシンに昇格します。

   > ⓘ 注記
   >
   > LifeCycle Manager を使用している場合、レプリケーション一覧ブジェクトは選択できません。

2. 本稼動のレプリケート元サイトでレプリケーション一覧を作成し、目的のコンテンツを含めます。
3. 次の 2 つのオプションから選択します。
   - A)リモート接続オブジェクトおよび適切なレプリケーションジョブを、レプリケート先サイトとして動作する本稼動の本稼動用のマシンで作成します。
   - B)LifeCycle Manager を使用してリモート接続およびレプリケーションジョブを Dev/QA のレプリケート先サイトから、レプリケート先サイトとして動作する本稼動用マシンにインポートします。次に、インポートしたリモート接続を編集し、レプリケート元サイトとして動作する本稼動のマシンを指定します。

27.14.4 レプリケート先サイトの再指定

現在のところ、レプリケート元サイトから複製されたオブジェクトは、必ずそのレプリケート元サイトから複製される必要があり、他の BI プラットフォームから複製することはできません。リモート接続オブジェクトを編集して、新しいシステムを指定するようにした場合でも、異なる BI プラットフォームシステムから複製されたオブジェクトを複製しようとすると、リモート接続オブジェクトは複製できません。別のレプリケート元サイトからオブジェクトを複製するには、最初にレプリケート先サイトからオブジェクトを削除します。

> ⓘ 注記
>
> 複製したオブジェクトをコピーすると、コピーの CUID は変更され、コピーには複製された情報は含まれません。

27.15 ベストプラクティス

フェデレーションを使用して、レプリケーションジョブのパフォーマンスを最適化できます。

1 つのレプリケーションジョブに多数のオブジェクトがある場合は、追加の手順を実行すると正しく実行できます。通常は、各レプリケーションジョブで 32,000 個までのオブジェクトを複製できます。ただし、一部のデプロイメントでは、レプリケーションのサイズを増減して設定する必要があります。

1) 専用 **Web** サービスプロバイダの取得

フェデレーションでは、複製されたコンテンツは Web サービスを使用して送信されます。BI プラットフォームのデフォルトのインストールでは、Web サービスはすべて同じ Web サービスプロバイダを使用します。容量の大きいレプリケーションジョブが Web サービスプロバイダを長時間使用していると、ほかの Web サービスリクエストおよびそれに対応するアプリケーションへの応答が遅くなる可能性があります。

一度に多数のオブジェクトを複製する予定がある場合や、複数のレプリケーションジョブを連続して実行する予定がある場合は、独自の Web サービスプロバイダを使用してフェデレーション Web サービスを、独自の Java アプリケーションサーバにデプロイすることができます。

これを行うには、BI プラットフォームインストーラを使用して Web サービスをインストールします。Java アプリケーションサーバがインストール済みであることが必要です。Java アプリケーションサーバがインストールされていない場合は、Web Tier コンポーネントオプション全体をインストールします。これで、Web サービスと Tomcat がインストールされます。

> ⓘ 注記
>
> 既存の CMS の情報 (ホスト名、ポート、管理者パスワードなど) を入力する必要があります。

> ⓘ 注記
>
> この新しい Web サービスプロバイダの URI は、リモート接続の URI フィールドで使用する必要があります。

2) Java アプリケーションサーバの使用可能なメモリ量の増加

1 つのレプリケーションジョブで多くのオブジェクトを複製する場合、または Java アプリケーションサーバを他のアプリケーションと共有している場合は、Java アプリケーションサーバで使用できるメモリの量を増やします。

BI プラットフォームと Tomcat をデプロイしている場合、デフォルトの使用可能メモリ量は 1 GB です。Tomcat の使用可能なメモリ量を増やすには、次の手順を実行します。

Windows の場合

1. [*スタート* > *プログラム* > *Tomcat* > *Tomcat 設定*] の順にクリックします。
2. [*Java*]を選択します。
3. [*Java オプション*] ボックスで、[`-Xmx1024M`] を見つけます。
4. [`-Xmx1024M`]の値を目的のサイズまで増やします。

例

メモリの量を 2 GB まで増やすには、「`-Xmx2048m`」と入力します。

UNIX の場合

1. `<BOE_Install_Dir>/setup/` で、任意のテキストエディタを使用して `env.sh` を開きます。`-Xmx1024m` パラメータを目的のサイズまで増やします。
2. 次の行を探します。

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
 # set the JAVA_OPTS for Tomcat
 JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
 if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" ];
then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxMetaspaceSize=256m"
 fi
 export JAVA_OPTS
 # fi
```

> ⓘ 注記
>
> BI 4.2 サポートパッケージ 5 では、MaxPermSize パラメータではなく、MaxMetaspaceSize パラメータを使用してメタスペースメモリサイズを定義できます。
>
> - BI 4.2 サポートパッケージ 5 より前のバージョンから BI 4.2 サポートパッケージ 5 にアップグレードしている場合は、既存のすべてのサーバについて、パラメータを手動で編集する必要があります。
> - BI 4.2 サポートパッケージ 5 のフレッシュインストールを実行している場合、パラメータはデフォルトで置き換えられます。

3. `-Xmx1024m` パラメータを目的のサイズまで増やします。

例

メモリの量を 2 GB まで増やすには、「`-Xmx2048m`」と入力します。

> → ヒント
>
> 他の Java アプリケーションサーバに関しては、Java アプリケーションサーバのマニュアルを参照して使用可能なメモリの量を増やしてください。

3)作成する **BIAR** ファイルサイズの縮小

フェデレーションは、Web サービスを使用してレプリケート元サイトとレプリケート先サイト間でコンテンツを複製します。効率的な転送を行うために、オブジェクトはグループ化されて BIAR ファイルに圧縮されます。

多数のオブジェクトを複製している場合は、Java アプリケーションサーバを設定してサイズの小さい BIAR ファイルを作成してください。この方法を使用すると、フェデレーションで、複数の小さい BIAR ファイルにオブジェクトがパッケージ化および圧縮されるので、複製するオブジェクトの数は制限されません。

作成する BIAR ファイルのサイズを小さくするには、次の Java パラメータを Java アプリケーションサーバに追加します。

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

`bobj.biar.suggestSplit` を指定すると、BAR ファイルの適切なサイズが提案され、そのサイズへの変更が行われます。提案される新しい値は 90MB です。

`bobj.biar.forceSplit` を指定すると、BIAR ファイルは指定されたサイズで強制的に停止します。提案される新しい値は 100 MB です。

> ⓘ 注記
>
> アプリケーションサーバでメモリ不足が発生しているか、最大ヒープサイズをこれ以上増やすことができない場合を除き、デフォルトの BIAR ファイルのサイズ設定を変更する必要はありません。

Tomcat Windows の場合

1. [*Tomcat 設定*] ツールを開くには、▶ スタート ▶ プログラム ▶ *Tomcat* ▶ *Tomcat 設定* ▶ の順にクリックします。

2. [*Java*] を選択します。
3. [*Java オプション*] ボックスの最後に次の行を追加します。

```
                    -Dbobj.biar.suggestSplit=90
                    -Dbobj.biar.forceSplit=100
```

Tomcat Unix/Linux の場合

1. 任意のテキストエディタで、env.sh を開きます。このファイルは `<BOE_Install_Dir>/setup/` にあります。
2. 次の行を探します。

```
 # if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"
if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" ];
then
JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
 fi
export JAVA_OPTS
 # fi
```

目的の BIAR ファイルサイズパラメータを追加します。

例: `JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m` **-Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"**

他の Java アプリケーションサーバに関しては、Java アプリケーションサーバのマニュアルを参照して、Java システムプロパティを追加してください。

4)ソケットタイムアウトの延長

Adaptive Job Server で、レプリケーションジョブが実行されます。レプリケーションジョブの実行中、Adaptive Job Server はレプリケート元サイトとの接続を確立します。レプリケート元サイトから大量の情報を受け取る場合、Adaptive Job Server が情報の受信に使用するソケットがタイムアウトしないようにすることが重要です。

デフォルト値は 90 分です。必要な場合は、ソケットタイムアウトの値を増やします。

Adaptive Job Server でソケットのタイムアウト値を延長するには、次の手順を実行します。

1. セントラル管理コンソール(CMC)を開きます。
2. [サーバ] セクションで、[*Adaptive Job Server*] を選択します。
3. [プロパティ]をクリックします。
4. 次の行の終わりに、“コマンドラインパラメータ”を追加します。
   - **Windows:**`-javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<timeout in minutes>`
   - **Unix:** `-javaArgs Xmx512m,Dbobj.federation.WSTimeout=<timeout in minutes>`

関連情報

エラーメッセージのトラブルシューティング [965 ページ]
フェデレーションでの Web サービスの使用 [952 ページ]
現在のリリースの制限 [964 ページ]

27.15.1 現在のリリースの制限

フェデレーションは、柔軟性のあるツールですが、実稼動中のパフォーマンスに影響する可能性のある特定の制限があります。ここでは、フェデレーションの運用を最適化するために変更可能な領域について詳しく説明します。

- オブジェクトの最大数
  各レプリケーションジョブは、BI プラットフォームデプロイメント間でオブジェクトを複製します。1 つのレプリケーションジョブで複製する最大オブジェクト数は 100,000 にすることをお勧めします。オブジェクトが 100,000 個を超えてもレプリケーションジョブは機能しますが、フェデレーションでサポートされるのは、100,000 個までのオブジェクトの複製だけです。
- アクセス権
  フェデレーションでは、アクセス権はレプリケート元サイトからレプリケート先サイトにのみ複製されます。両方のデプロイメントに共通するユーザアクセス権をレプリケート元サイトで設定し、双方向レプリケーションを使用してそれらのアクセス権をレプリケート先サイトに複製することをお勧めします。特定のサイトのユーザアクセス権は、ユーザが存在するサイトの BI プラットフォームデプロイメントで通常どおりに管理されます。
- ビジネスビューと関連オブジェクト
  BI プラットフォームには、ビジネスビュー、ビジネスエレメント、データファンデーション、データコネクション、および値の一覧 (LOV) を保存できます。これらのオブジェクトは、Crystal Reports の機能を拡張するために使用します。
  オブジェクトがレプリケート先サイトで最初に作成されてから、双方向レプリケーションを使用してレプリケート元サイトに複製されると、これらのオブジェクトは正しく動作せず、それらのデータは Crystal Reports に表示されない場合があります。
  レプリケート元サイトでビジネスビュー、ビジネスエレメント、データファンデーション、データコネクションおよび LOV を作成してから、それらをレプリケート先サイトに複製することをお勧めします。レプリケート先サイトまたはレプリケート元サイトでオブジェクトを更新すると(アクセス権を許可する)、変更は正しく複製されます。
- ユニバースオーバーロード
  BI プラットフォームにはユニバースオーバーロードを保存できます。ユニバースオーバーロードがレプリケート先サイトで作成されてから、双方向レプリケーションを使用してレプリケート元サイトに複製されると、それらは正しく機能しない場合があります。
  この問題を解決するには、最初にレプリケート元サイトでユニバースオーバーロードを作成してから、レプリケート先サイトに複製します。次に、レプリケート元サイトでユニバースオーバーロードにセキュリティを設定し、レプリケート先サイトに複製します。
- オブジェクトのクリーンアップ
  オブジェクトのクリーンアップによって、一方のサイトで削除されているオブジェクトが削除されます。現在、オブジェクトのクリーンアップは、レプリケート元サイトからレプリケート先サイトにのみ実行されます。
- フェデレーションログファイル
  フェデレーションログファイルは、XML 1.1 標準を使用する XML ファイルに書き込まれます。ブラウザでログファイルを表示するには、ブラウザが XML 1.1 をサポートしている必要があります。

関連情報

オブジェクトのクリーンアップの管理 [945 ページ]

27.15.2 エラーメッセージのトラブルシューティング

ここでは、フェデレーションを使用する際に発生する可能性のあるエラーメッセージについて説明します。これらのメッセージはレプリケーションジョブのログまたはレポートの機能領域に表示されます。

1)無効な GUID

エラーの例: `ERROR 2008-01-10T00:31:08.234Z GUID ASXOOFyvy0FJnRcD0dZNTZg (オブジェクト番号 1285 のプロパティ SI_PARENT_CUID) は有効な GUID ではありません。`

このエラーは、親が一緒に複製されていないオブジェクトやレプリケート先に存在しないオブジェクトを複製していることを意味します。たとえば、オブジェクトが複製されていても、そのオブジェクトを含むフォルダが複製されていない場合があります。オブジェクトを複製しているアカウントが親オブジェクトに対する十分なアクセス権を持っていないために、親オブジェクトは複製されない可能性があります。

2) レプリケート元サイトでデータが表示されない Crystal Reports

このエラーは、最初にレプリケート先サイトで作成されてから、レプリケート元サイトに複製されたビジネスビュー、ビジネスエレメント、データファンデーション、データコネクションまたは値の一覧 (LOV) を Crystal Reports が使用している場合に発生する可能性があります。

3)ユニバースオーバーロードが正しく適用されない

このエラーは、レプリケート先サイトで作成されてから、レプリケート元サイトに複製されたユニバースオーバーロードを含むユニバースをレポートが使用している場合に発生します。

4)Java のメモリ不足

エラー例: `java.lang.OutOfMemoryError`

このエラーは、レプリケーションジョブの処理中に Java アプリケーションサーバのメモリが不足すると発生する可能性があります。レプリケーションジョブのサイズが大きすぎるか、Java アプリケーションサーバに十分なメモリがありません。

フェデレーション Web サービスを専用のマシンに移動して Java アプリケーションサーバの使用可能なメモリ量を増やすか、1 つのレプリケーションジョブで複製されるオブジェクトの量を減らします。

5)ソケットタイムアウト

エラーの例: 元のサイトの通信中にエラーが発生しました。タイムアウトになりました。

レプリケート元サイトからレプリケート先サイトの Adaptive Job Server へ送信される情報が、割り当てられたタイムアウトを超える長さになっています。Adaptive Job Server でソケットのタイムアウト値を延長するか、レプリケーションジョブで複製しているオブジェクトの数を減らしてください。

6)クエリ制限

エラーの例: レプリケート先サイトで SDK エラーが発生しました。有効なクエリでありません。(FWB 00025) ….. . .クエリ文字列がクエリの長さ制限を超えています。

このエラーは、一度に多数のオブジェクトを複製している場合や、フェデレーションが、CMS で処理しきれない大きさのクエリを送信した場合に発生する可能性があります。レプリケート元サイトからのオブジェクトはレプリケート先サイトにコミットされます。ただし、レプリケート元サイトにコミットする必要がある変更はコミットされません。競合は指定されたとおりに解決されますが、オブジェクトには手動による競合解決のフラグは設定されません。レプリケート先サイトでコミットされたオブジェクトは継続して正しく動作します。

この問題を解決するには、1 つのレプリケーションジョブで複製しているオブジェクトの数を減らします。

7)レプリケーションジョブのタイムアウト

エラーの例: 指定の時間間隔内にオブジェクトをスケジュールできませんでした。

このメッセージは、別のレプリケーションジョブの完了を待機している間にレプリケーションジョブがタイムアウトすると表示されます。複数のレプリケーションジョブが 1 つのレプリケート元サイトに同時に接続している場合、このエラーが発生する可能性があります。失敗したレプリケーションジョブは、次のスケジュール時に再実行を試みます。

この問題を解決するには、失敗したレプリケーションジョブを、同じレプリケート元サイトに接続している他のレプリケーションジョブと競合しない時間にスケジュールします。

8)レプリケーションの制限

エラーの例: レプリケート先サイトで SDK エラーが発生しました。データベースアクセスのエラーです。….内部クエリプロセッサのエラーです。クエリの最適化中にクエリプロセッサのスタック領域が足りなくなりました。ExecWithDeadlockHandling でクエリを実行中にエラーが発生しました。

このメッセージは、一度に複製可能な、サポートされるオブジェクトの数を超えると表示される場合があります。この問題を解決するには、レプリケーションジョブで複製しているオブジェクトの数を減らし、再実行してみてください。

9)オブジェクトの削除

エラーの例: 「セキュリティ権限をチェック中にエラーが発生しました。」または「オブジェクトのパック中にエラーが発生しました。」

このメッセージは、オブジェクトがレプリケーションパッケージから削除されると表示される場合があります。これは、権限をチェックしたり、オブジェクトをパックする前に、レプリケーションの必要があるオブジェクトに対してフェデレーションがクエリを実行すると発生する場合があります。

10)Adaptive Processing Server

エラーの例: `Job Processing Server` でエラーが発生しました。

このエラーは、フェデレーションによってロードされるクラスの数が多すぎて、レプリケーションジョブを処理するメモリが足りない場合に発生する可能性があります。

この問題を解決するには、次の両方の手順を実行する必要があります。

1. Adaptive Processing Server のコマンドライン引数に、`-javaArgs "XX:MaxMetaspaceSize=256m"` という行を追加します。

   > **注記**
   >
   > BI 4.2 サポートパッケージ 5 では、MaxPermSize パラメータではなく、MaxMetaspaceSize パラメータを使用してメタスペースメモリサイズを定義できます。
   >
   > - BI 4.2 サポートパッケージ 5 より前のバージョンから BI 4.2 サポートパッケージ 5 にアップグレードしている場合は、既存のすべてのサーバについて、パラメータを手動で編集する必要があります。
   > - BI 4.2 サポートパッケージ 5 のフレッシュインストールを実行している場合、パラメータはデフォルトで置き換えられます。

2. 接続先の Java アプリケーションサーバに次のパラメータを追加して、使用している BIAR ファイルのサイズを縮小します。
   - `-Dbobj.biar.suggestSplit=100m`
   - `-Dbobj.biar.forceSplit=100m`

11) Adaptive Processing Server の調整

新しい Java 引数 `-XX:MetaspaceSize` が APS コマンドラインに追加され、既存の `-XX:MaxMetaspaceSize` との組み合わせによって初期化のエクスペリエンスを改善し、Adaptive Processing Server に関連する Java プロセス内での不要なフルガーベジコレクションを防ぎます。

最小 RAM リソース、デフォルト APS、およびすべてのサービスを含む VM のテストで、MetaSpace および MaxMetaSpace に対してこれらの値を指定すると、APS の起動と初期化が既定の設定よりも若干速くなるようです。'フル GC' はレポートされていません。

Adaptive Processing Server の JAVA オプションの調整による MetaSpace でのフルガーベッジコレクション (フル GC) の回避の詳細については、SAP ノート 3001317 を参照してください。

12) オブジェクトマネージャの領域

エラーの例: プッシュパッケージを構築できませんでした。入力/出力例外が発生しました: "デバイスに領域が残っていません。"

これは、フェデレーションが使用する一時ディレクトリに十分なディスク領域がない場合に発生します。この問題を解決するには、一時ディレクトリに追加の領域を作成するか、一時ディレクトリに別の場所を使用します。

レプリケート元サイトで一時ディレクトリに別の場所を指定するには、Java アプリケーションサーバの設定ファイルに`-Dbobj.tmp.dir=<TempDir>`という行を追加します。

レプリケート元サイトで一時ディレクトリに別の場所を指定するには、Adaptive Processing Server のコマンドライン引数に`-javaArgs “-Dbobj.tmp.dir=<TempDir>”`という行を追加します。

この例で、`<TempDir>`は、使用する一時ディレクトリの場所です。

13) ユニバースエラー

エラーの例: `processDPCommands API` の呼び出し中に内部エラーが発生しました。

このエラーは、複製されたユニバースに、無効なまたは見つからないユニバース間接続のリレーションシップが含まれている場合に発生します。この問題を解決するには、[レプリケート元から最新表示]オプションを選択して、レプリケーションジョブを実行し、ユニバース接続が複製されていることを確認します。

または、Universe Designer でユニバースを開き、ユニバースのユニバース接続を編集して、ユニバースを再コミットします。

関連情報

ベストプラクティス [960 ページ]
現在のリリースの制限 [964 ページ]

28 ERP 環境の追加設定

28.1 SAP NetWeaver 統合の設定

28.1.1 SAP Business Warehouse (BW) との統合

28.1.1.1 概要

この節では、SAP Business Warehouse アプリケーションから BI プラットフォームへのレポートの公開を有効化および管理できるように BW を設定する方法について説明します。

この節を読み始める前に、CMC での SAP 認証プラグインの設定が完了していることを確認してください。

関連情報

SAP 認証の設定 [321 ページ]

28.1.1.1.1 BI プラットフォームでのフォルダとセキュリティの設定

BI プラットフォームで権限認証システムを定義すると、お使いの SAP システムに対応する論理フォルダ構造が作成されます。 ロールをインポートし、コンテンツを BI プラットフォームに公開すると、対応するフォルダが作成されます。 管理者として、これらのフォルダを作成する必要はありません。 これらのフォルダは、SAP 認証プラグイン設定時の権限認証システムの定義や、CMC へのロールのインポート、および BI プラットフォームへのコンテンツの公開といった操作を行うことによって作成されます。

> ⓘ 注記
>
> BI プラットフォーム管理者は、これらのフォルダに対して適切な権限を割り当てる必要があります。
>
> - *SAP 最上位フォルダ*
> Everyone グループのアクセス権が SAP 最上位フォルダに制限されていることを確認してください。
> - *システム ID フォルダ*
> CMC では、プリンシパル公開者に次の権限を割り当てます。
>
> > ⓘ 注記
> >
> > プリンシパル公開者はコンテンツが公開されるまで使用できません。
>
> - オブジェクトをフォルダに追加する
> - オブジェクトを表示する

- オブジェクトを編集する
- オブジェクトに対するユーザの権限を変更する
- オブジェクトを削除する

→ ヒント

権限の管理を容易にするには、これらの権限を含めたカスタマイズした公開者アクセスレベルを作成し、関連するシステム ID フォルダに対してそのアクセスレベルをプリンシパル公開者に付与します。

関連情報

アクセスレベルの使用 [134 ページ]
BI プラットフォームでのアクセス権の動作 [121 ページ]

28.1.1.1.2 デフォルトフォルダセキュリティパターンについて

SAP から BI プラットフォームにコンテンツを公開する場合、ロール、フォルダおよびレポートの残りの階層が自動的に作成されます。システム ID、クライアント番号、ロールの名前に基づいた名前のフォルダに、レポートが配置されます。

- 権限認証システムを定義すると、最上位フォルダ、つまり SAP、2.0 およびシステム (`<SID>`) の各フォルダが作成されます。
- システムは、ロールが BW から公開されたときに、必要に応じてロールフォルダ (グループとして BI プラットフォームにインポート) を作成します。
- システムは、コンテンツが公開されるロールごとに 1 つのコンテンツフォルダを作成します。
- セキュリティは各レポートオブジェクトに設定され、ユーザは自身のロールに属するレポートのみを参照できます。

管理者は、異なるロールのメンバーに権限を割り当てる必要があります。コンテンツ管理ワークベンチを使用して、SAP BW 内からレポート公開機能を管理することができます。特定の BI プラットフォームシステムで SAP BW システムからロールを識別したり、レポートを公開したり、SAP BW および BI プラットフォーム間のデプロイメントでレポートの同期をとったりすることができます。

コンテンツフォルダ

BI プラットフォームは、権限認証システムに追加された各ロールに対し、CMC での定義に従ってグループをインポートします。

コンテンツ保持ロールのすべてのメンバーに対して適切なデフォルト権限を確実に付与するには、コンテンツ管理ワークベンチで、BI プラットフォームで定義されている各権限認証システムに適切な権限を割り当てます。コンテンツ管理ワークベンチを起動するには、トランザクション /CRYSTAL/RPTADMIN を実行します。

1. コンテンツ管理ワークベンチで、[*Enterprise システム*]、[利用可能なシステム] の順に展開します。

2. 目的のシステムをダブルクリックします。
3. [レイアウト]タブをクリックしてください。
4. [レポートのデフォルトセキュリティポリシー]を[表示]に指定します。
5. [ロールフォルダのデフォルトセキュリティポリシー]を[オンデマンド表示]に設定します。
6. [*OK*] をクリックします。

これらの設定は、BI プラットフォームで、すべてのコンテンツロールについて反映されます。コンテンツロールとは、コンテンツを持ち、そのコンテンツの公開先となっているロールです。これらのロールのメンバーは、他のロールに公開されているレポートのスケジュールされたインスタンスを表示できるようになり、メンバーであるロールに公開されているレポートを最新表示することもできるようになります。

> ⓘ 注記
>
> 各ロールでの作業は、それぞれ固有にしておくことをお勧めします。たとえば、管理者ロールからの公開が可能でも、公開は公開者ロールからのみ行うようにします。ただし、公開者ロールは、コンテンツを公開できるユーザを定義することだけが目的です。そのため、公開者ロールにはコンテンツを含めないようにして、公開者は通常のロールメンバーがアクセスできるコンテンツを保持するロールに公開するようにします。

28.1.1.1.3 BW イベントに基づくスケジュール

BI プラットフォームで、BW イベントに基づいてオブジェクトをスケジュールできるようになりました。BW イベントに基づくスケジュールを有効化するには、SAP NetWeaver Business Warehouse (BW) システムと BI プラットフォームの間に信頼できる通信チャネルを確立する必要があります。

28.1.1.1.3.1 BW イベントを作成および設定する

BW イベントを作成するには、以下の手順に従います。

1. CMC にログオンします。
2. イベント > *BW イベント* に移動します。
3. を選択して新しいイベントを作成します。
4. [イベント名] および [説明] を入力します。
5. [作成] を選択します。
   新しい BW イベントが作成されます。

28.1.1.1.3.2 レポートのスケジュール中に BW イベントを追加する

レポートのスケジュール中に BW イベントを追加するには、以下の手順に従います。

1. **CMC** で、[フォルダ] に移動してレポートを選択します。

2. レポートのコンテキストメニューで、[スケジュール] を選択します。
3. ナビゲーションペインで、イベント > *BW イベント* に移動します。
4. [利用可能なイベント] からイベントを選択します。
5. >> を使用して、そのイベントを [待機するイベント] に追加します。
6. ナビゲーションペインで、[繰り返し] に移動します。
7. [オブジェクトの実行]、[可能な再試行回数]、および [再試行間隔 (秒単位)] の各パラメータを指定します。
8. [スケジュール] を選択します。

   イベントがトリガされると、レポートのスケジュールステータスが [待機] から [実行中] に変更されます。

   > **注記**
   >
   > [待機するイベント] で定義されたイベントのいずれか 1 つがトリガされていない場合は、スケジュールステータスは [待機] のままになります。

28.1.1.1.3.3 BI プラットフォームと ABAP システムを統合する

このトピックでは、BW イベントに基づくスケジュールを有効化する方法について説明します。

以下の手順に従います。

1. BI プラットフォームで任意のサポート対象アプリケーションサーバの HTTPS/SSL を設定し、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥container¥bin` に共有シークレットキーを追加します。WACS についてはトピック HTTPS/SSL を設定する [501 ページ] を、Tomcat については Tomcat での SSL の設定 [390 ページ] を参照してください。

   > **注記**
   >
   > サポート対象アプリケーションサーバの詳細については、SAP 製品出荷マトリクス (PAM) を参照できます。

2. BI プラットフォームのサーバ証明書をブラウザからローカルシステムにエクスポートします。以下の手順に従って、証明書を Chrome ブラウザからダウンロードできます。
1. http://<hostname>:<port_number>/biprws に移動します。各アプリケーションに固有なポート番号の詳細については、トピック RESTful Web サービスのベース URL を設定する [512 ページ] を参照してください。
2. F12 を押して、Chrome ブラウザのデベロッパーツールを開きます。
3. [*Security*] タブに移動して、[*View Certificate*] を選択します。
   [証明書] ウィザードが表示されます。
4. [証明書] ウィザードで、[詳細] タブに移動して [ファイルにコピー] を選択します。
   [証明書のエクスポート ウィザード] が表示されます。
5. [次へ] を選択します。
6. [エクスポートファイルの形式] ページで、形式 [*Base 64 encoded X.509 (.CER)*] を選択して [次へ] を選択します。
7. 証明書ファイルの名前を指定して、ローカルに保存します。
3. SAP NetWeaver BW システムの証明書をダウンロードします。
1. SAP NetWeaver BW を起動します。
2. トランザクション *STRUSTSSO2* に移動します。

3. システム *PSE* > サブジェクト > 独自の証明書 に移動します。
4. [ダウンロード] を選択します。
5. ファイルパスを指定し、ファイル形式として [*Base64*] を選択します。
6. を選択します。

SAP NetWeaver BW システムの証明書が指定した場所にダウンロードされます。

4. BI プラットフォームの証明書を SAP NetWeaver BW システムにインポートします。
1. トランザクション *STRUSTSSO2* に移動します。
2. [編集] モードに切り替えます。
3. [*SSL* クライアント (標準)] フォルダを選択します。
4. [インポート] を選択します。
5. SAP NetWeaver BW システムの証明書をアップロードして、[証明書一覧に追加する] を選択します。
   証明書が証明書一覧に追加されます。
6. トランザクションを保存します。
5. SAP NetWeaver BW システムの証明書を BI プラットフォームにインポートします。証明書のインポートの詳細については、トピック HTTPS/SSL を設定する [501 ページ]の手順 12 を参照してください。
6. BI プラットフォームでユーザを作成します。

> **注記**
>
> BI プラットフォームでのユーザ名が SAP NetWeaver BW システムでのユーザ名と同じであることを確認する必要があります。たとえば、SAP NetWeaver BW システム名が MySystem である場合は、BI プラットフォームで MySystem という名称のユーザを作成する必要があります。

7. SAP NetWeaver BW システムで HTTP 宛先を作成します。
1. トランザクション *SM59* に移動します。
2. [外部サーバへの *HTTP* 接続] を選択します。
3. を選択します。
4. [*RFC* 宛先] ウィンドウで、[技術設定] タブに切り替えて、[ホスト]、[ポート]、および [パス接頭辞] をそれぞれ `<hostname>`、`<port_number>`、`/biprws` のように入力します。
5. [ログオンとセキュリティ] タブに切り替えて、[*SSL*] を [有効] に設定します。
6. [*SSL* 証明書] として [デフォルト *SSL* クライアント (標準)] を選択します。
7. [保存] を選択します。
8. テスト接続 Connection Test を選択して、HTTP 宛先への接続をテストします。接続テストの結果が表示され、ステータステキストとして OK が表示されます。

> **注記**
>
> SAP NetWeaver BW と BI プラットフォームの間の HTTP 接続は、下記の条件が満たされないと使用できません。
>
> - BW システムは、TLS 1.1 および TLS 1.2 のバージョンをサポートするように更新される必要があります。
> - BW システムでは、BI プラットフォームでサポートされる同一の暗号スイートがサポートされる必要があります。

9. SAP NetWeaver BW システムでプロセスチェーンを作成します。
1. トランザクション *RSPC* に移動します。

2. [プロセスチェーン] のコンテキストメニューを開き、[表示コンポーネントの作成] を選択します。
3. [グルーピングの作成] ウィンドウで、[アプリケーションコンポーネント] と [テキスト (長)] を指定します。
   SAP NetWeaver BW コンポーネントが作成されます。
4. アプリケーションコンポーネントのコンテキストメニューで、[プロセスチェーンの作成] を選択します。
5. 名称とテキストを指定して、を選択します。
   新しいプロセスチェーンの名称を指定すると、[開始プロセスの挿入] ダイアログが表示されます。ここで、プロセスチェーンの開始プロセスを挿入できます。
6. [プロセスバリアント] および [テキスト (長)] を指定して、を選択します。
   [開始プロセスの更新] ウィンドウが表示されます。
7. [条件の編集] を選択し、[即時] を選択してプロセスチェーンを即時に実行します。
8. [開始時刻] ウィンドウで [保存] を選択します。
9. [開始プロセスの更新] ウィンドウで [保存] を選択します。
10. [開始プロセスの挿入] ウィンドウで、を選択します。
    プロセスチェーンが作成されます。
10. プロセスチェーンのプロセスタイプを設定します。
1. [プロセスチェーン] 列から、前の手順で作成したプロセスチェーンを選択します。
2. [プロセスのロードと後処理] フォルダを展開して、[*BW データ変更用 SAP BOBJ BI プラットフォームのイベントトリガ*] を選択します。
   [BW データ変更用 SAP BOBJ BI プラットフォームのイベントトリガを挿入] ダイアログが表示されます。
3. [*SAP BOBJ BI プラットフォームで BW データ変更のイベントを挿入*] で、を選択します。
4. [プロセスバリアント] と [テキスト (長)] を入力します。
5. を選択します。
   [プロセスの更新] ウィンドウが表示されます。
6. [宛先] でを選択して、宛先を選択します。
7. [イベント] でを選択して、イベントを選択します。
8. 変更を保存します。
9. [SAP BOBJ BI プラットフォームで BW データ変更のイベントを挿入] ダイアログで、を選択します。
   プロセスタイプが作成されます。
11. プロセスチェーンを有効化して実行します。

これにより、プロセスタイプに指定されている BW イベントがトリガされます。

28.1.1.2 BW Publisher の設定

BW Publisher を使用すると、Crystal レポート (.rpt ファイル) を BW から BI プラットフォームへ、個々にまたはまとめて公開できます。

Windows では、BW Publisher を次のいずれかの方法で設定できます。

- BI プラットフォームをホストするマシン上のサービスとして、BW Publisher を開始します。BW Publisher Service が必要に応じて BW Publisher のインスタンスを開始します。
- ローカル SAP ゲートウェイを使用して BW Publisher を起動し、BW Publisher のインスタンスを作成します。

設定方法は、サイトの要件を基に、各方法の有利な点と不利な点を考慮した上で決定する必要があります。BI プラットフォームで BW Publisher を設定したら、コンテンツ管理ワークベンチで公開を設定する必要があります。

28.1.1.3 BW Publisher のサービスとしての設定

ここでは、BW Publisher を 1 つのサービスとして使用し、BW から BI プラットフォームへのレポートの公開を有効にする方法について説明します。

28.1.1.3.1 BW Publisher インストールの分散

この節では、BW Publisher サービスの配布と、他の BI プラットフォームコンポーネントから BW Publisher を分離する方法について説明します。

同じ BI プラットフォームシステム内の 2 台の異なるマシンに BW Publisher Service をインストールして、BW から公開するときの負荷を分散することができます。

BI プラットフォームをホストする 2 台のマシンに BW Publisher をインストールするときに、同じプログラム ID および SAP Gateway ホストと Gateway サービスを使用するようそれぞれの BW Publisher を設定します。このプログラム ID を使用する RFC 宛先を作成すると、BW は BI プラットフォームをホストするマシン間で公開の負荷を分散します。また、一方の BW Publisher が使用できなくなると、BW は引き続き他方の BW Publisher を使用します。

複数の BW アプリケーションサーバが含まれる設定であれば、システム冗長性のレベルを追加することができます。SAP ゲートウェイを実行できるよう、各 BW アプリケーションサーバを設定します。BW アプリケーションサーバごとに、BI プラットフォームをホストするマシンに異なる BW Publisher Service をインストールします。異なる BW アプリケーションサーバの Gateway ホストと Gateway サービスを使用するよう、それぞれの BW Publisher Service を設定します。この設定では、BW Publisher またはアプリケーションサーバのいずれかが失敗しても、BW からの公開を続行できます。

BW Publisher を他の BI プラットフォームコンポーネントと分離する場合は、スタンドアロンの SAP Gateway を使用して BW をインストールします。

この場合は、BW Publisher と同じマシンにローカル SAP Gateway をインストールする必要があります。さらに、BW Publisher は BI プラットフォーム SDK および Crystal Reports Print Engine へのアクセスを必要とします。したがって、専用のマシンに BW Publisher とローカルの SAP Gateway をインストールする場合は、SIA Server もインストールする必要があります。

28.1.1.3.2 BW Publisher の開始: UNIX の場合

BW Publisher スクリプトを実行して、公開要求を処理するための 1 つまたは複数のパブリッシャインスタンスを作成します。最初は 1 つのパブリッシャインスタンスで開始することをお勧めします。

BW Publisher を開始すると、BI プラットフォームインストールプログラムの実行時に指定した SAP Gateway サービスとの接続が確立されます。

28.1.1.3.3 BW Publisher の開始: Windows の場合

Windows では、セントラル設定マネージャ™ (CCM) を使用して BW Publisher Service を開始します。BW Publisher Service を開始すると、BW システムからの公開要求を処理するためのパブリッシャインスタンスが 1 つ

作成されます。公開要求の数が増えると、BW Publisher ではそれらの要求の増加に対応するために追加のパブリッシャが自動的に作成されます。

28.1.1.3.4 BW Publisher Service の宛先の設定

BW Publisher を有効にするには、BW Publisher Service と通信できるよう BW サーバに RFC 宛先を設定します。BW クラスタがある場合は、どの場合でも BW のセントラルインスタンスをゲートウェイホストとして使用して、各サーバに RFC 宛先を設定します。

BW から複数の BI プラットフォームシステムに公開する場合は、BW Publisher Service の RFC 宛先を、BI プラットフォームデプロイメントごとに 1 つずつ作成します。各宛先には一意のプログラム ID を使用する必要がありますが、ゲートウェイホストとゲートウェイサービスは同じです。

28.1.1.3.5 ローカル SAP ゲートウェイを使用した BW Publisher の設定

> ⓘ 注記
>
> BI プラットフォームが UNIX にインストールされている場合は、この設定は使用しないでください。UNIX でこのメソッドを使用すると、システムの予期しない動作を引き起こす場合があります。

ローカル SAP Gateway を使用して、BW から BI プラットフォームへのレポートの公開を有効にするには、次の手順に従います。

- ローカル SAP ゲートウェイのインストール [976 ページ]
- BW Publisher の宛先の設定 [977 ページ]

28.1.1.3.6 ローカル SAP ゲートウェイのインストール

ローカル SAP Gateway は、BW Publisher をインストールしたマシンにインストールする必要があります。 これらの SAP ゲートウェイのインストールのうちの 1 つは、SAP ベーシス管理者が実行することを推奨します。

ローカル SAP ゲートウェイをインストールする最新の手順については、SAP プレゼンテーション CD に含まれる SAP インストールの指示を参照してください。

テスト環境の詳細なリストについては、Product Availability Matrix (PAM) (http://service.sap.com/sap/support/pam?hash=pvnr%3D67837800100900006540) を参照してください。 PAM には、アプリケーションサーバ、オペレーティングシステム、SAP コンポーネントのバージョンや、必要なサービスパックなどが説明されています。

SAP ゲートウェイのインストール後、`regedit` を用いて、`HKEY_CURRENT_USER¥Environment` の下の `TMP` および `TEMP` レジストリの入力値を確認します。 両方のレジストリエントリに保存されている同一の文字列値が、有効な絶対ディレクトリパスである必要があります。 いずれかのエントリの値に `%USERPROFILE%` 変数が含まれる場合は、絶対ディレクトリパスに置き換えます。 通常、両方のレジストリエントリは `C:¥WINDOWS¥TEMP` に設定します。

28.1.1.4 BW Publisher の宛先の設定

BW Publisher を有効にするには、ローカル SAP ゲートウェイと BW Publisher をインストールしたマシンの場所を BW に提供できるよう RFC 宛先を設定する必要があります。

28.1.1.5 コンテンツ管理ワークベンチでの公開の設定

コンテンツ管理ワークベンチを使用して、SAP BW 内からレポート公開機能を管理することができます。特定の BI プラットフォームシステムで SAP BW システムからロールを識別したり、レポートを公開したり、SAP BW および BI プラットフォーム間のデプロイメントでレポートの同期をとったりすることができます。SAP 認証を設定し、BW Publisher を設定したら、この節で概説する機能を実行して公開を有効にします。この指示に従うと、次のことが実行できます。

- コンテンツ管理ワークベンチの各ユーザに対して適切な権限を設定する
- コンテンツを公開する BI プラットフォームへの接続を設定する
- 各 BI プラットフォームに公開できるロールを定義する
- BW から BI プラットフォームへコンテンツを公開する

28.1.1.6 コンテンツ管理ワークベンチにアクセスできるユーザ

コンテンツ管理ワークベンチにアクセスできるユーザには、次の 3 つの種類があります。

- コンテンツ利用者。コンテンツ保持ロールに属し、レポートを表示することができます。このユーザには、レポートの表示以外の操作を行う権限はありません。
- BI プラットフォームコンテンツ公開者。BW からレポートを表示、公開、変更、削除 (オプション) することができます。
- BI プラットフォーム管理者。コンテンツ管理ワークベンチ内のすべてのタスクを実行することができます。これらのタスクには、BI プラットフォームシステムの定義、レポートの公開、およびレポートメンテナンスの実行が含まれます。

28.1.1.7 コンテンツ公開者用ロールの BW での作成

BI プラットフォームと統合させるよう BW を設定する際に、現在のロール構造によって BI プラットフォームシステムのコンテンツ公開者またはシステム管理者として特定の BW ユーザを迅速に指定可能かどうかを判断してください。

新規に作成したすべてのロールについて、説明的な名前を付けることをお勧めします。説明的なロール名の例には、`BOE_CONTENT_PUBLISHERS` や `SBOP_SYSTE _ADMINISTRATORS` などがあります。

> → ヒント
>
> 管理者ユーザにはフルシステム管理者権限またはそれらの権限のサブセットを割り当てることができます。

これらの新しいロールや既存のロールに BI プラットフォームで割り当てられた権限を変更するには、最初に SAP 認証をセットアップし、ロールをインポートします。次に、セントラル管理コンソールを使用し、個々のインポートされたロールの権限を変更できます。

ロールの作成についての詳細は、SAP のマニュアルを参照してください。コンテンツ管理でのロールの使用については、次の節を参照してください。

- SAP ロールのインポート [329 ページ]
- BI プラットフォームでのフォルダとセキュリティの設定 [969 ページ]
- デフォルトフォルダセキュリティパターンについて [970 ページ]

28.1.1.8 コンテンツ管理ワークベンチへのアクセスの設定

コンテンツ管理ワークベンチにアクセスできるユーザのタイプごとに、BW で適切な権限を適用する必要があります。次の表は、権限の一覧です。

管理者ユーザの権限

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
S_TCODE	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	実行 (16)
	TCD	/CRYSTAL/RPTADMIN, RSCR_MAINT_PUBLISH
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	変更、照会 (02、03)
	DICBERCLS	&NC&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
S_RS_ADMWB	ACTVT	実行 (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	新規登録、変更、照会、削除 (01、02、03、06)
ZCNTADMJOB	ACTVT	新規登録、削除 (01、06)
ZCNTADMRPT	ACTVT	照会、削除、有効化、更新、チェック (03、06、07、23、29)

コンテンツ公開者の権限

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	実行 (16)
	TCD	/CRYSTAL/RPTADMIN
S_BTCH_JOB	JOBACTION	DELE, RELE
	JOBGROUP	' '
	ACTVT	実行 (16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	照会 (03)
ZCNTADMJOB	ACTVT	(新規登録、削除) 01、06
ZCNTADMRPT	ACTVT	照会、有効化、更新、チェック (03、07、23、29) 削除 (オプション) (06) 編集 (オプション) (02)

BW コンテンツ管理ワークベンチでのレポートの削除権限は、オプションでコンテンツ公開者に付与することができます。ただし、BW でレポートを削除すると BI プラットフォーム内のレポートも削除されてしまう点に注意してください。公開者がプラットフォーム内のレポートを削除する権限を持っていない場合は、エラーになります。

コンテンツ利用者の権限

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SH3A, SUNI
	ACTVT	実行 (16)
	TCD	/CRYSTAL/RPTADMIN
S_RS_ADMWB	ACTVT	実行 (16)
	RSADMWBOBJ	WORKBENCH

権限オブジェクト	フィールド	値
	ACTVT	照会 (03)

28.1.1.9 BI プラットフォームの定義

レポートを公開する BI プラットフォームシステムごとに、コンテンツ管理ワークベンチ内にシステム定義を作成する必要があります。

28.1.1.9.1 BI プラットフォームシステムを追加する

1. トランザクション `/crystal/rptadmin` を実行して、コンテンツ管理ワークベンチにアクセスします。
2. [オペレーション]パネルから[*Enterprise* システム]を選択します。
3. [新しいシステムの追加]をダブルクリックします。
4. [システム] タブで次を実行します。
   - [エイリアス]フィールドに説明的な名前を入力します。スペースや特殊文字は使用しないでください。エンタープライズポータルの設定時にこれらの文字を使用する場合は、特殊な処理が必要になります。
   - CMS を実行しているマシンの名前を入力します。CMS がデフォルトのポート以外のポートで通信するよう設定している場合、「**`CMSNAME:PORT`**」と入力します。
   - BI プラットフォームシステムに明示的に割り当てられていない任意のロールからこのシステムにレポートを公開する場合は、[既定のシステム] を選択します。デフォルトシステムとして使用できるのは 1 つの BI プラットフォームシステムのみです。
     利用可能なすべてのシステムのリストでは、デフォルトシステムに緑色のチェックマークが付いています。
5. [保存] をクリックします。
6. [*RFC* 宛先] タブで、このシステムに関連付けられた各 RFC 宛先を追加します。

   宛先を追加するには、[行挿入]ボタンをクリックします。表示されたリストで、RFC 宛先の名前をダブルクリックします。

   > ⓘ 注記
   >
   > 1 つの BI プラットフォームシステムに複数の宛先を設定して、システムの冗長性を追加することができます。「“BW Publisher インストールの分散”」を参照してください。

7. 追加した出力先名の横にあるチェックボックスをオンにして、[*BOE* 定義の確認] をクリックします。

   このテストでは、指定した BW Publisher に BW がアクセスできるかどうか、および Crystal 権限認証ユーザアカウントを使用してこのシステムにログオンできるかどうかを確認します。
8. [*HTTP*] タブで次を実行します。
   - [プロトコル] フィールドに「**`http`**」または「**`https`**」(BI プラットフォームに接続されている Web サーバが HTTPS 向けに設定されている場合) と入力します。
   - [*Web* サーバのホストおよびポート] フィールドに、BI ラウンチパッドをホストする Web サーバの完全修飾ドメイン名または IP アドレスを入力します。Java アプリケーションサーバを使用するインストール

の場合は、ポート番号を含めてください。たとえば、「**boserver01.businessobjects.com:8080**」と入力します。

- [パス] フィールドに「**SAP**」と入力します。
  このパスは、Web サーバが BI プラットフォームの Web Content フォルダの sap サブフォルダを参照するときに使用する仮想パスを表します。Web 環境とプラットフォーム Web Content ファイルの場所をカスタマイズした場合のみ、別の値を指定してください。
  エントリの先頭または最後にスラッシュ記号 (/) を含めないようにしてください。
- [ビューアアプリケーション] フィールドにビューアアプリケーションの名前を入力します。
  Java バージョンの BI ラウンチパッドを使用するデフォルトの BI プラットフォームビューアを使用するには、「**openDocument.jsp**」と入力します。
  デフォルトの ASP.NET 設定を使用して Windows に BI プラットフォームをインストールした場合にデフォルトのブラウザを使用するには、「**report/report_view.aspx**」と入力します。

9. [言語] タブで、このシステムに公開するレポートの言語を選択します。
10. [ロール] タブで、この BI プラットフォームシステムと関連付けるコンテンツ保持ロールを追加します。
    「“SAP ロールのインポート”」を参照してください。
11. [行挿入] ボタンをクリックします。

    このシステムに追加する利用可能なロールのリストが表示されます。

    > ⓘ 注記
    >
    > 各ロールは 1 つの BI プラットフォームシステムにのみ公開できます。この BI プラットフォームシステムに追加するロールがリストに表示されない場合は、[キャンセル] をクリックして [ロール] タブに戻り、[ロールの再割当] をクリックします。

12. このシステムに公開するロールを選択し、[*OK*] をクリックします。
13. [レイアウト] タブで、この BI プラットフォームシステムに公開されるレポートとロールフォルダのデフォルトのセキュリティ設定を選択します。

    > ⓘ 注記
    >
    > BI プラットフォームでは、そのシステムに公開されるロールごとに 1 つのフォルダが自動的に作成されます。このフォルダには、そのロールに基づいて公開されるレポートへのショートカットが含まれます。

    > ⓘ 注記
    >
    > BI プラットフォームシステムを設定した後に、ここでデフォルトのセキュリティレベルを変更しても、公開されるロールフォルダやレポートのセキュリティレベルには影響ありません。プラットフォームに公開されるすべてのロールとコンテンツについてデフォルトのセキュリティレベルを変更するには、システム内のロールフォルダとショートカットを削除します。この操作によって、実際のレポートは削除されません。ここでセキュリティ設定を変更し、ロールとレポートを再び公開します。

14. 下部にある [*OK*] をクリックして設定を保存し、コンテンツ管理ワークベンチに BI プラットフォームシステムを登録します。

これで、BW から BI プラットフォームにレポートを公開できるようになります。

関連情報

BW Publisher インストールの分散 [975 ページ]

SAP ロールのインポート [329 ページ]

28.1.1.10 コンテンツ管理ワークベンチを使用したレポートの公開

レポートを BW に保存した後で、コンテンツ管理ワークベンチを使用してそのレポートを公開することができます。コンテンツ管理ワークベンチを使用して個々のレポートを公開することも、特定のロールに保存されているすべてのレポートを公開することもできます。Crystal コンテンツ公開者に付与される権限を持っているユーザ(権限の登録および適用 [997 ページ]を参照)のみが、コンテンツ管理ワークベンチを使用してレポートを公開したり更新したりすることができます。

28.1.1.11 ロールまたはレポートの公開

1. トランザクション `/crystal/rptadmin` を実行して、コンテンツ管理ワークベンチにアクセスします。
2. [オペレーション]パネルの[レポートの公開]を選択します。
3. BW システムに保存されているコンテンツを検索するには、[公開するレポートとロールの選択]をダブルクリックします。
   利用可能なロールとレポートのフィルタを実行できるダイアログボックスが表示されます。
4. リストから、表示するコンテンツを含む 1 つまたは複数のシステムを選択します。

   > **注記**
   >
   > リストには、この BW システムで定義されている利用可能なすべてのシステムが示されます。

5. 次に、結果をフィルタして、表示するレポートとロールの数を制限します。次のオプションを使用します。
   - オブジェクトバージョン
     [A 有効]を選択すると、公開可能なすべてのレポートが表示されます。オプションを選択しない場合、すべてのレポートが表示されます。残りのオプションは SAP の予約語です。
   - オブジェクトステータス
     公開されているレポートだけを表示するには、[ACT 有効、実行可能]を選択します。公開されていないレポートだけを表示するには、[INA 無効、実行不可]を選択します。すべてのレポートを表示するには、フィールドを空白のままにします。残りのオプションは SAP の予約語です。
   - ロールフィルタ
     このボックスにテキストを入力すると、ここで入力した内容と一致するロールだけが表示されます。ワイルドカード文字として * を使用します。たとえば、d という文字から始まるすべてのロールを表示する場合は、「d*」と入力します。
   - レポートの説明
     このボックスにテキストを入力すると、ここで入力した内容と一致する説明を持つレポートだけが表示されます。何文字にでも一致するワイルドカード文字として * を使用します。0 文字 または 1 文字と一致するワイルドカードとして + を使用します。たとえば、revenue という語を含む説明を持つすべてのレポートを表示する場合は、「*revenue*」と入力します。
6. [*OK*]をクリックします。
   条件に一致するレポートのリストが、右側のパネルに表示されます。
   レポートは、階層形式 (BI プラットフォームシステム > そのシステムのロール > ロールに保存されているレポート) で示されます。
   階層内の各項目には、赤色、黄色、緑色の点が付いています。階層内の上位項目には、その下位にある項目のステータスが反映され、階層の最上位には、最も高い条件が示されます。たとえば、ロール内の 1 つのレポー

トが黄色 (アクティブ) で、残りのすべてのレポートが緑 (公開済み) である場合、ロールは黄色 (アクティブ) として示されます。

- 緑: 項目は完全に公開されています。項目が BI プラットフォームシステムまたはロールである場合、その項目のすべてのレポートが公開されます。
- 黄: 項目はアクティブですが、公開されていません。項目がレポートである場合、項目は公開することができます。項目がロールまたは BI プラットフォームシステムである場合、すべてのコンテンツがアクティブになりますが、ロールまたはシステムに含まれる少なくとも 1 つの項目が公開されていません。
- 赤: 項目は SAP コンテンツであるため、コンテンツ管理ワークベンチでは公開できません。BW 管理ワークベンチを使用してコンテンツをアクティブにするまで、このコンテンツを公開することはできません。

7. 公開するレポートを選択します。
   ロール内のすべてのレポートを公開する場合は、そのロールを選択します。BI プラットフォームシステム内のすべてのロールを公開するには、そのシステムを選択します。

   > ⓘ 注記
   >
   > ロール (またはシステム) を選択すると、そのロール (またはシステム) に含まれているすべてのレポートが選択されます。この選択を解除するには、該当のロール (またはシステム) のチェックボックスをオフにして、[最新表示] をクリックします。

8. [公開]をクリックします。

   > ⓘ 注記
   >
   > バックグラウンドで公開されたレポートが処理されると、システムリソースが利用可能になります。このオプションを使用するには、[公開]ではなく、[バックグラウンドで]をクリックします。

9. [最新表示] をクリックして、コンテンツ管理ワークベンチ内の BI プラットフォームシステム、ロール、およびレポートのステータスの表示を更新します。

   > → ヒント
   >
   > レポートを表示するには、レポートを右クリックして[表示]を選択します。レポートで使用されるクエリを確認するには、レポートを右クリックして、[参照クエリ] を選択します。

   > ⓘ 注記
   >
   > BI プラットフォームにレポートを公開した後で、そのレポートを上書きする場合は、[上書き] をクリックします。

関連情報

バックグラウンドでの公開のスケジュール [984 ページ]

28.1.1.12 バックグラウンドでの公開のスケジュール

バックグラウンドで、直ちにまたはスケジュールされたジョブとしてレポートを公開すると、システムリソースを節約することができます。システムの応答性を向上させるために、バックグラウンドでレポートを公開することをお勧めします。

レポートをスケジュールされたジョブとして定期的に公開し、BW と BI プラットフォームデプロイメントの間でレポート情報を同期化できます。すべてのレポート(またはこれらのレポートを含むロール)をスケジュールすることをお勧めします。また、[レポートのメンテナンス]オペレーションの[ステータスの更新]オプションを使用して、ロールとレポートを手動で同期化することもできます。詳細については、レポートのステータスの更新 [984 ページ]を参照してください。

28.1.1.13 公開されたレポートのシステム情報の更新

BW Publisher は、ここで入力した SAP システム情報を使用して、公開されたレポートのデータソースを更新します。ローカルの BW アプリケーションサーバを使用するか、負荷分散設定を使用する場合は BW セントラルインスタンスを使用することができます。

28.1.1.14 レポートの管理

レポート管理タスクには、BI プラットフォームと BW の間でのレポートに関する情報の同期化 ([ステータスの更新])、不要なレポートの削除 ([レポートの削除]) および前のバージョンのプラットフォームから移行されたレポートの更新 ([ポスト移行]) があります。

28.1.1.14.1 レポートのステータスの更新

レポートの公開先のロールを変更した場合など BI プラットフォームシステムで公開されたレポートに変更を加えた場合、その変更は BI プラットフォームと BW を同期化するまで BW には反映されません。公開ジョブをスケジュールして、BI プラットフォームと BW を定期的に同期化する (バックグラウンドでの公開のスケジュール [984 ページ]を参照) か、[レポートのメンテナンス] ツールを使用してレポートのステータスを手動で更新することもできます。

28.1.1.14.2 レポートの削除

コンテンツ管理ワークベンチを使用して、発行されたレポートを BW から削除すると、そのレポートは BI プラットフォームからも削除されます。BW と BI プラットフォームシステムの両方でレポートを削除するために必要な権限を付与されたユーザだけがレポートを削除できます。

> ⓘ 注記
>
> BW でレポートを削除する権限があっても、レポートが公開されている BI プラットフォームシステムで権限がない場合は、エラーが発生する場合があります。

28.1.1.15 SAP http リクエストハンドラの設定

BW でレポートの表示を有効にする場合は、コンテンツ管理ワークベンチの一部として含まれている http リクエストハンドラを使用するよう BW の設定を行う必要があります。これで、BW ユーザが SAPGUI 内から Crystal レポートを開くときに、BW は Web 上で表示要求のルートを適切に選定できます。

BW システムでアクティブな仮想ホストとサービスのリストにアクセスするには、トランザクション SICF を使用します。`default_host` 階層の BW の下に、`ce_url` という名前の新しいロールを登録し、`/CRYSTAL/CL_BW_HTTP_HANDLER` をハンドラリストに追加します。このサービスは、登録後に手動で有効にすることが必要な場合があります。

28.1.1.16 SAP データ処理の設定

28.1.1.16.1 スケジュールしたレポートの SAP のバッチモードでの処理

Windows 版の BI プラットフォームでは、スケジュールしたレポートを SAP のバッチモードを使用して実行できます。特定の環境変数が 1 に設定されている場合、インフォセットドライバやオープン SQL ドライバは SAP のバッチまたはバックグラウンドモードを使用してレポートを実行することができます。関係する環境変数は次のとおりです。

- `CRYSTAL_INFOSET_FORCE_BATCH_MODE`(インフォセットドライバ用)
- `CRYSTAL_OPENSQL_FORCE_BATCH_MODE`(オープン SQL ドライバ用)

ただし、BI プラットフォームの分散インストールを実行している場合にのみ、この機能を使用することをお勧めします。これらの環境変数が 1 に設定されている場合、レポートが実際にどのレポーティングコンポーネントで実行されているかに関わらず、ドライバはレポートを SAP のバッチモードで実行します。このため、BI プラットフォームサーバを組み合わせて実行しているマシン上のシステム環境変数としてこれらの環境変数を作成すると、ドライバは Crystal Reports Processing Server および Report Application Server からのオンデマンドレポート要求を含むすべてのレポートをバッチモードで実行します。

確実に、ドライバがスケジュールしたレポート (Adaptive Job Server が実行するレポート) だけをバッチモードで実行するためには、BI プラットフォームサーバを組み合わせて実行しているマシン上のシステム環境変数として設定しないようにしてください。代わりに、次の手順に従って、各 Adaptive Job Server 用に環境変数をカスタマイズします。

> ⓘ 注記
>
> レポートを BI プラットフォームにスケジュールする SAP ユーザは、追加の SAP 認証が必要となることがあります。

関連情報

バッチモードでのレポートのスケジュール (オープン SQL クエリを使用) [1011 ページ]

28.1.1.16.2 スケジュールしたレポートを SAP のバッチモードで処理する

1. メモ帳のようなテキストエディタで、バッチスクリプト(.bat ファイル)を次の内容で作成します。

```
@echo off
set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
set CRYSTAL_OPENSQL_FORCE_BATCH_MODE=1
%*
```

   このスクリプトは環境変数を 1 に設定し、コマンドラインからスクリプトに渡されたすべてのパラメータを実行します。
2. ファイルを、各 Adaptive Job Server マシンのフォルダに jobserver_batchmode.bat という名前で保存します。
3. セントラル管理コンソール (CMC) にログオンします。
4. [サーバ] を選択します。
5. [サービスカテゴリ] ノードを展開し、[*Analysis* サービス] を選択します。
6. [*Adaptive Processing Server*] を選択し、コンテキストメニューから [プロパティ] を選択します。
   [プロパティ] ページが開きます。
7. [プロパティ] ページで、[コマンドラインパラメータ] フィールドに移動します。

   これは、Adaptive Job Server の起動コマンドです。例:

```
"¥¥SERVER01¥C$¥Program Files¥SAO Business Objects¥SAP BusinessObjects
Enterprise¥win32_x86¥JobServer.exe" -service -name SERVER01.report -ns SERVER01
-objectType BusinessObjects Enterprise.Report -lib procReport -restart
```

8. このデフォルトのコマンドの前に、Adaptive Job Server マシン上に保存した jobserver_batchmode.bat ファイルのフルパスを指定します。

   この例では、バッチファイルは、SERVER01 という名前のマシン上に次の名前で保存されています。

```
C:¥Crystal Scripts¥jobserver_batchmode.bat
```

   この Adaptive Job Server の新しい起動コマンドは、次のようになります。

```
"¥¥SERVER01¥C$¥Crystal Scripts¥jobserver_batchmode.bat" "¥¥SERVER01¥C$
¥Program Files¥SAP Business Objects¥SAP
BusinessObjects Enterprise 12.0¥win32_x86¥JobServer.exe" -service -name
SERVER01.report  -ns SERVER01
-objectType BusinessObjects Enterprise.Report -lib procReport  -restart
```

   新しい起動コマンドは、バッチファイルを最初に起動します。このバッチファイルは、Adaptive Job Server のオリジナルの起動コマンドを実行する前に、必要な環境変数の設定を行います。これにより、Adaptive Job Server が使用する環境変数が、オンデマンドレポーティングに対応しているサーバ (Crystal Reports Processing Server および Report Application Server) に対して有効な環境変数とは異なることが保証されます。

9. [保存して閉じる] をクリックします。
10. Adaptive Job Server を右クリックし、コンテキストメニューから [開始] を選択します。

> ⓘ 注記
>
> Adaptive Job Server の起動に失敗した場合、新しい起動コマンドを確認してください。

28.1.1.17 SAP 移送の設定

28.1.1.17.1 概要

BI プラットフォームには以下の移送が含まれています。

- オープン SQL 接続移送
- インフォセット接続移送
- 行レベルセキュリティ定義移送
- クラスタ定義移送
- コンテンツ管理ワークベンチ移送
- BW クエリパラメータパーソナライゼーション移送
- MDX 移送
- ODS 移送

移送には、Unicode 互換移送および ANSI 移送の 2 つの異なるセットがあります。ベーシスシステムの 6.20 またはそれ以降を実行している場合、Unicode 互換移送を使用します。6.20 以前のベーシスシステムを実行している場合、ANSI 移送を使用します。インストール済みのすべての移送は、製品配布メディアの `¥Collaterals¥Add-Ons¥SAP¥Transports¥` ディレクトリにあります。

> ⓘ 注記
>
> インストールによる競合の可能性をチェックする際には、SAP システムに同一のオブジェクト名が存在しないことを確認します。デフォルトでは、オブジェクトは **`/crystal/`** 名前空間を使用します。したがって、ユーザがこの名前空間を作成する必要はありません。手動で **`/crystal/`** 名前空間を作成すると、アクセスできないライセンス修復キーの入力を求めるメッセージが表示されます。

28.1.1.17.2 移送を設定する

BI プラットフォームの Data Access または BW Publisher のコンポーネントをセットアップするには、適切な移送を SAP システムにインポートする必要があります。これらのコンポーネントは、SAP システムと通信する際にこれらの移送ファイルのコンテンツを使用します。

SAP システム上で必要なインストールと設定手順は、システムの変更および移送を熟知し、SAP システムへの管理者権限を持つ ベーシスの専門家により実行される必要があります。移送ファイルをインポートする細かい手順は、実行している ベーシスのバージョンによって異なります。詳細については、SAP のマニュアルを参照してください。

データアクセスコンポーネントの最初の導入時には、デフォルトですべてのユーザが全 SAP テーブルにアクセス可能です。ユーザがアクセス可能な SAP データを保護するには、セキュリティ定義エディタを使用します。

移送をインポートしたら、適切なユーザアクセスレベルを設定する必要があります。必要な権限を作成し、それを Crystal レポートを作成、実行、スケジュールする SAP ユーザに対して、プロファイルまたはロールを介して適用します。

関連情報

権限の登録および適用 [997 ページ]

28.1.1.17.2.1 移送の種類

移送には、Unicode 互換移送および ANSI 移送の 2 つの異なるセットがあります。ベーシスシステムの 6.20 またはそれ以降を実行している場合、Unicode 互換移送を使用します。6.20 以前のベーシスシステムを実行している場合、ANSI 移送を使用します。インストール済みのすべての移送は、製品配布の `¥Collaterals¥Add-Ons¥SAP¥Transports` ディレクトリにあります。`transports.txt` ファイルには、Unicode 互換移送ファイルおよび ANSI 移送ファイルが一覧にされています。

移送タイプは、次のとおりです。

- オープン SQL 接続移送
  オープン SQL 接続移送により、オープン SQL ドライバは、SAP システムに接続したり、SAP システムからのレポーティングを行ったりすることができます。
- 行レベルセキュリティ定義移送
  この移送は、オープン SQL 接続移送内の /crystal/auth テーブルのグラフィカルなインタフェースとして機能するツールである、セキュリティ定義エディタを提供します。
- クラスタ定義移送
  この移送は、クラスタ定義ツールを提供します。このツールにより、ABAP データクラスタ定義のメタデータリポジトリを作成することができます。これらの定義は、データクラスタによるレポーティングのために必要な情報を、オープン SQL ドライバに提供します。

  > ⓘ 注記
  >
  > ABAP データクラスタは、クラスタテーブルと同じではありません。クラスタテーブルは、すでに DDIC で定義されています。

- インフォセット接続移送
  インフォセット接続移送により、インフォセットドライバはインフォセットおよび SAP クエリにアクセスすることができます。
- コンテンツ管理ワークベンチ移送
  この移送は、コンテンツ管理機能を BW システムに提供します。この移送は、Unicode 互換移送としてのみ利用できます。
- BW クエリパラメータパーソナライゼーション移送
  この移送は、BW クエリを基にしたレポートのパーソナライズパラメータ値とデフォルトパラメータ値のサポートを提供します。

- BW MDX 接続移送
  この移送を使用することにより、MDX クエリドライバが BW キューブおよびクエリにアクセスできるようになります。この移送は BW 3.0B パッチ 27 以降、および BW 3.1C パッチ 21 以降で使用できます。
- ODS 接続移送
  この移送を使用することにより、ODS クエリドライバが ODS データにアクセスできるようになります。この移送は BW 3.0B パッチ 27 以降、および BW 3.1C パッチ 21 以降で使用できます。

28.1.1.17.2.2 競合の確認

移送ファイルの内容は、ファイルをインポートすると、SAP BusinessObjects 名前空間の下に自動的に登録されます。 R/3 および MYSAP ERP の比較的新しいバージョンでは、SAP BusinessObjects の名前空間はこの用途のために予約されています。 ただし、権限オブジェクト、権限クラス、およびレガシーオブジェクトなど、一部のオブジェクトのオブジェクト名には適切な前置記号が含まれていない場合があります。 移送ファイルをインポートする前に、これらのオブジェクトタイプの競合がないかどうかをチェックすることをお勧めします。

汎用プログラムグループ、汎用プログラムモジュール、またはその他のオブジェクトのいずれかがすでに SAP システムに存在している場合、SAP BusinessObjects の移送ファイルをインポートする前に、名前空間の競合を解決する必要があります。 お使いのバージョンの SAP に適した手順については、SAP NetWeaver technology platform のマニュアルを参照してください。

28.1.1.17.2.3 移送ファイルのインポート

製品配布メディアのディレクトリ `¥Collaterals¥Add-Ons¥SAP¥Transports¥` にある、`transports_EN.txt` ファイルを参照してください。このテキストファイルには、各移送を構成するファイルの正確な名前が一覧されます。(`transports` ディレクトリの下の `cofiles` および `data` ディレクトリは、SAP サーバの .../`trans/cofiles` および .../`trans/data` ディレクトリに対応しています)。

行レベルのセキュリティ定義移送またはクラスタ定義移送をインポートする前に、オープン SQL 接続移送をインポートする必要があります。他の移送については、任意の順序でインポートできます。

> **注記**
>
> CD からサーバにファイルをコピーした後、移送をインポートする前に、すべてのファイルが書き込み可能であることを確認してください。インポートファイルが読み取り専用の場合、インポートに失敗します。

> **注記**
>
> 移送はバイナリファイルなので、UNIX インストールでは、ファイルの破損を避けるため FTP によるファイルの追加をバイナリモードで行う必要があります。さらに、UNIX サーバに対する書き込み権限を持っている必要があります。

28.1.1.17.2.4 移送

28.1.1.17.2.4.1 オープン SQL 接続移送

オープン SQL 接続移送により、ドライバは、SAP システムに接続したり、SAP システムからのレポーティングを行ったりすることができます。

オブジェクト	種類	説明
/CRYSTAL/BC	パッケージ	開発クラス
/CRYSTAL/OPENSQL	関数グループ	オープン SQL 関数
/CRYSTAL/OSQL_AUTH_FORMS	プログラム	ヘルパープログラム
/CRYSTAL/OSQL_EXECUTE	プログラム	ヘルパープログラム
/CRYSTAL/OSQL_TYPEPOOLPROG	プログラム	ヘルパープログラム
/CRYSTAL/OSQL_TYPEPOOLS	プログラム	ヘルパープログラム
/CRYSTAL/OSQL_UTILS	プログラム	ヘルパープログラム
ZSSI	権限オブジェクトクラス	レポート権限オブジェクト
ZSEGREPORT	権限オブジェクト	レポート権限オブジェクト
/CRYSTAL/ OSQL_CLU_ACTKEY_ENTRY	テーブル	クラスタメタデータ
/CRYSTAL/OSQL_FCN_PARAM	テーブル	関数メタデータ
/CRYSTAL/OSQL_FCN_PARAM_FIELD	テーブル	関数メタデータ
/CRYSTAL/OSQL_FIELD_ENTRY	テーブル	テーブルのメタデータ
/CRYSTAL/OSQL_OBJECT_ENTRY	テーブル	テーブルのメタデータ
/CRYSTAL/OSQL_RLS_CHK_ENTRY	テーブル	RLS メタデータ
/CRYSTAL/OSQL_RLS_FCN_ENTRY	テーブル	RLS メタデータ
/CRYSTAL/OSQL_RLS_VAL_ENTRY	テーブル	RLS メタデータ
ZCLUSTDATA	テーブル	クラスタメタデータ
ZCLUSTID	テーブル	クラスタメタデータ
ZCLUSTKEY	テーブル	クラスタメタデータ
ZCLUSTKEY2	テーブル	クラスタメタデータ

オブジェクト	種類	説明
/CRYSTAL/AUTHCHK	テーブル	RLS メタデータ
/CRYSTAL/AUTHFCN	テーブル	RLS メタデータ
/CRYSTAL/AUTHKEY	テーブル	RLS メタデータ
/CRYSTAL/AUTHOBJ	テーブル	RLS メタデータ
/CRYSTAL/AUTHREF	テーブル	RLS メタデータ
ZSSAUTHCHK	テーブル	古い RLS メタデータ
ZSSAUTHOBJ	テーブル	古い RLS メタデータ
ZSSAUTHKEY	テーブル	古い RLS メタデータ
ZSSAUTHREF	テーブル	古い RLS メタデータ
ZSSAUTH FCN	テーブル	古い RLS メタデータ

28.1.1.17.2.4.2 インフォセット接続移送

インフォセット接続移送により、インフォセットドライバはインフォセットにアクセスすることができます。この移送は R/3 4.6c 以降のバージョンとの互換性があります。SAP R/3 4.6a 以前のバージョンをご使用の場合は、この移送をインポートしないでください。

オブジェクト	種類	説明
/CRYSTAL/BC	パッケージ	開発クラス
/CRYSTAL/FLAT	関数グループ	インフォセットラッパー関数
/CRYSTAL/QUERY_BATCH	プログラム	バッチモード実行
/CRYSTAL/QUERY_BATCH_STREAM	プログラム	ストリーミングバッチモード実行

28.1.1.17.2.4.3 行レベルセキュリティ定義移送

この移送は、オープン SQL 接続移送内の /CRYSTAL/AUTH テーブルのグラフィカルなインタフェースとして機能するツールである、セキュリティ定義エディタを提供します。

オブジェクト	種類	説明
/CRYSTAL/BC	パッケージ	開発クラス
/CRYSTAL/TABMNT	関数グループ	関数制限のテーブルメンテナンスビューの関数グループ
/CRYSTAL/RLSDEF	プログラム	メインプログラム
/CRYSTAL/RLS_INCLUDE1	プログラム	モジュール定義のあるインクルードプログラム
/CRYSTAL/RLS_INCLUDE2	プログラム	サブルーチン定義のあるインクルードプログラム
TDDAT [/CRYSTAL/AUTHFCN]	テーブルコンテンツ	テーブルメンテナンス定義
TVDIR [/CRYSTAL/AUTHFCN]	テーブルコンテンツ	テーブルメンテナンス定義
/CRYSTAL/AUTHFCNS	移送およびメンテナンスオブジェクトの定義	テーブルメンテナンス定義
/CRYSTAL/RLS	トランザクション	メインプログラムトランザクション
/CRYSTAL/RLSFCN	トランザクション	メインプログラムから内部呼び出しされるヘルパートランザクション

28.1.1.17.2.4.4 クラスタ定義移送

この移送は、クラスタ定義ツールを提供します。このツールにより、ABAP データクラスタ定義のメタデータリポジトリを作成することができます。これらの定義は、データクラスタによるレポーティングのために必要な情報を、オープン SQL ドライバに提供します。

> ⓘ 注記
>
> ABAP データクラスタは、クラスタテーブルと同じではありません。クラスタテーブルは、すでに DDIC で定義されています。

オブジェクト	種類	説明
ZCIMPRBG	プログラム	メインプログラム
ZCRBGTOP	プログラム	インクルードプログラム
ZCDD	トランザクション	メインプログラムトランザクション

28.1.1.17.2.4.5 コンテンツ管理ワークベンチ移送

この移送は、コンテンツ管理機能を BW システムに提供します。この移送は、Unicode 互換移送としてのみ利用できます。

オブジェクト	種類	説明
/CRYSTAL/BC	パッケージ	開発クラス
/CRYSTAL/CL_BW_HTTP_HANDLER	クラス	複数の CE で認識可能な HTTP リクエストハンドラ
/CRYSTAL/OBJECT_STATUS_DOM	ドメイン	レポートアクティビティ
/CRYSTAL/OBJ_POLICY_DOM	ドメイン	CE オブジェクトセキュリティ
/CRYSTAL/OBJECT_STATUS	データ要素	レポートアクティビティ
/CRYSTAL/OBJ_POLICY	データ要素	CE オブジェクトセキュリティ
/CRYSTAL/CE_SYNCH	関数グループ	パブリッシャスタブ
/CRYSTAL/CA_MSG	メッセージクラス	ステータスメッセージ
/CRYSTAL/CE_SYNCH_FORMS	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN_CLASS_D	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN_CLASS_I	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN_CTREE	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN_FORMS	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN_MODULES	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN_PAIS	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN_PBOS	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN_TAB_FRM	プログラム	プログラムコンポーネント
/CRYSTAL/CONTENT_ADMIN_TOP	プログラム	プログラムコンポーネント
/CRYSTAL/PUBLISH_WORKER	プログラム	プログラムコンポーネント

オブジェクト	種類	説明
/CRYSTAL/PUBLISH_WORKER_DISP	プログラム	プログラムコンポーネント
/CRYSTAL/PUBLISH_WORKER_DISP_I	プログラム	プログラムコンポーネント
/CRYSTAL/ PUBLISH_WORKER_FORMS	プログラム	プログラムコンポーネント
/CRYSTAL/PUBLISH_WORKER_PROC	プログラム	プログラムコンポーネント
/CRYSTAL/ PUBLISH_WORKER_PROC_I	プログラム	プログラムコンポーネント
/CRYSTAL/ PUBLISH_WORKER_SCREEN	プログラム	プログラムコンポーネント
/CRYSTAL/CA_DEST	テーブル	アプリケーションステート
/CRYSTAL/CA_JOB	テーブル	アプリケーションステート
/CRYSTAL/CA_JOB2	テーブル	アプリケーションステート
/CRYSTAL/CA_LANG	テーブル	アプリケーションステート
/CRYSTAL/CA_PARM	テーブル	アプリケーションステート
/CRYSTAL/CA_ROLE	テーブル	アプリケーションステート
/CRYSTAL/CA_SYST	テーブル	アプリケーションステート
/CRYSTAL/MENU_TREE_ITEMS	構造	アプリケーションステート
/CRYSTAL/REPORT_ID	テーブル	アプリケーションステート
/CRYSTAL/RPTADMIN	トランザクション	メインプログラムトランザクション
/CRYSTAL/EDIT_REPORT	プログラム	レポート編集用ラッパー
/CRYSTAL/EDIT_REPORT	関数グループ	レポート編集用の機能
ZSSI	権限オブジェクトクラス	Crystal 権限
ZCNTADMCES	権限オブジェクト	CE の処理
ZCNTADMRPT	権限オブジェクト	レポート操作
ZCNTADMJOB	権限オブジェクト	バックグラウンドジョブの処理

28.1.1.17.2.4.6 ODS 接続移送

この移送を使用することにより、ODS クエリドライバが ODS データにアクセスできるようになります。この移送は BW 3.0B パッチ 27 以降、および BW 3.1C パッチ 21 以降で使用できます。

オブジェクト	種類	説明
/CRYSTAL/BC	パッケージ	開発クラス
/CRYSTAL/ODS_REPORT	関数グループ	ODS 関数

28.1.1.17.2.4.7 BW クエリパラメータパーソナライゼーション移送

この移送は、BW クエリを基にしたレポートのパーソナライズパラメータ値とデフォルトパラメータ値のサポートを提供します。

オブジェクト	種類	説明
/CRYSTAL/BC	パッケージ	開発クラス
/CRYSTAL/PERS_VAR	構造	変数の定義
/CRYSTAL/PERS_VALUE	構造	値定義
/CRYSTAL/PERS	関数グループ	パーソナライゼーション関数

28.1.1.17.2.4.8 BW MDX 接続移送

この移送を使用することにより、MDX クエリドライバが BW キューブおよびクエリにアクセスできるようになります。この移送は BW 3.0B パッチ 27 以降、および BW 3.1C パッチ 21 以降で使用できます。

オブジェクト	種類	説明
/CRYSTAL/BC	パッケージ	開発クラス
/CRYSTAL/MDX	関数グループ	MDX 関数
/CRYSTAL/MDX_STREAM_LAYOUT	テーブルの定義	データベース構造
/CRYSTAL/CX_BAPI_ERROR	クラス	例外
/CRYSTAL/CX_METADATA_ERROR	クラス	例外
/CRYSTAL/CX_MISSING_STREAMINFO	クラス	例外

オブジェクト	種類	説明
/CRYSTAL/CX_NO_MORE_CELLS	クラス	例外
/CRYSTAL/CX_NO_MORE_MEMBERS	クラス	例外
/CRYSTAL/CX_NO_MORE_PROPERTIES	クラス	例外
/CRYSTAL/CX_SAVE_SESSION_STATE	クラス	例外
/CRYSTAL/MDX_APPEND_DATA	クラス	データベースプロセッサ
/CRYSTAL/MDX_READER_BASE	クラス	データベースプロセッサ
/CRYSTAL/MDX_READ_DIMENSIONS	クラス	データベースプロセッサ
/CRYSTAL/MDX_READ_MEASURES	クラス	データベースプロセッサ
/CRYSTAL/MDX_READ_PROPERTIES	クラス	データベースプロセッサ
/CRYSTAL/MDX_AXIS_LEVELS	テーブルタイプ	メタデータ構造
/CRYSTAL/MDX_PROPERTY_KEYS	テーブルタイプ	メタデータ構造
/CRYSTAL/MDX_PROPERTY_VALUES	テーブルタイプ	メタデータ構造
/CRYSTAL/MDX_STREAM_LAYOUT_TAB	テーブルタイプ	メタデータ構造

28.1.1.18 権限の概要

この節では、SAP の統合環境で BI プラットフォームの一般的なタスクを実行する際に、必要なことがわかっている、また、テスト環境において必要となった SAP 権限の一覧を提供します。各実装環境によって、追加の権限オブジェクトあるいは権限フィールドが必要な場合があります。

各権限オブジェクトから権限を作成し、適切な項目の値を定義する必要があります。次に、SAP ユーザのプロファイル(またはロール)に対して適切な権限を適用します。次の節では、必要な権限とフィールド値について説明します。SAP の各バージョン固有の手順の詳細は、 SAP のマニュアルを参照してください。

> ⓘ 注記
>
> ここで提供される情報は、あくまでもガイドラインです。

> ⓘ 注記
>
> ZSEGREPORT 権限オブジェクトは ZSSI オブジェクトクラスに属し、オープン SQL クエリのサポートに必要な SAP Integration の移送ファイルのインポート時にインストールされます。

28.1.1.18.1 権限の登録および適用

各ユーザが Desktop Intelligence Integration for SAP を使用して情報にアクセスするために必要な権限を登録、適用する必要があります。 権限の登録、設定、適用の細かな手順は、インストールされている SAP のバージョンによって異なります。この節では、SAP Netweaver ABAP 環境内で統合された BI プラットフォームを使用して共通タスクを実行する場合に必要なことがわかっている、また、テスト環境において必要となった SAP 権限の一覧を提供します。各実装環境によって、追加の権限オブジェクトあるいは権限フィールドが必要な場合があります。

関連情報

コンテンツ管理ワークベンチでの公開の設定 [977 ページ]

28.1.1.19 BW の操作

ここでは、BW のさまざまな操作について説明します。

28.1.1.19.1 Crystal Reports 内のアクション

28.1.1.19.1.1 BW ロールのクエリからの新しいレポートの作成

権限オブジェクト	フィールド	値
S_USER_AGR	ACT_GROUP	**<USER_ROLE>***
	ACTVT	01、02、06
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	RS_PERS_BOD
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****

権限オブジェクト	フィールド	値
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<USER_ROLE>** は、ユーザが属するロールの名前です。このフィールドには、複数の値を入力できます。

QUERY_OWNER <は、クエリの所有者>の名前です。名前を指定した場合、その所有者のクエリからのレポーティングのみが可能となります。すべての所有者のクエリからレポーティングするには、「*」を入力します。

** **< INFO_AREA>**、**<INFO_CUBE>** または **<COMP_ID>** に「*」を入力すると、すべての値になります。特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.1.2 BW ロールから既存のレポートを開く

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SUSO, SUNI.RSCR, SH3A, RFC1, RZX0, RZX2, RS_PERS_BOD, /CRYSTAL/PERS, RSOB
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<QUERY_OWNER>** は、レポートの作成元である所有者の名前です。クエリの所有者を入力すると、この所有者のクエリからしかレポートを作成できません。あらゆるクエリの所有者を指定するには、「*」を入力します。

** **< INFO_AREA>**、**<INFO_CUBE>** または **<COMP_ID>** に「*」を入力すると、すべての値になります。特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.1.3 レポートのプレビューまたは最新表示

権限オブジェクト	フィールド	値
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<QUERY_OWNER>** は、レポートの作成元である所有者の名前です。クエリの所有者を入力すると、この所有者のクエリからしかレポートを作成できません。あらゆるクエリの所有者を指定するには、「*」を入力します。

** **< INFO_AREA>**、**<INFO_CUBE>** または **<COMP_ID>** に「*」を入力すると、すべての値になります。特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.1.4 データベースの検証(レポートでのテーブルの定義の最新表示)

権限オブジェクト	フィールド	値
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****

権限オブジェクト	フィールド	値
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<QUERY_OWNER>** は、レポートの作成元である所有者の名前です。クエリの所有者を入力すると、この所有者のクエリからしかレポートを作成できません。あらゆるクエリの所有者を指定するには、「*」を入力します。

** **< INFO_AREA>**、**<INFO_CUBE>** または **<COMP_ID>** に「*」を入力すると、すべての値になります。特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.1.5 データソースの場所の設定

権限オブジェクト	フィールド	値
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16

* **<QUERY_OWNER>** は、レポートの作成元である所有者の名前です。クエリの所有者を入力すると、この所有者のクエリからしかレポートを作成できません。あらゆるクエリの所有者を指定するには、「*」を入力します。

** **< INFO_AREA>**、**<INFO_CUBE>** または **<COMP_ID>** に「*」を入力すると、すべての値になります。特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.1.6 BW ロールへのレポートの保存

権限オブジェクト	フィールド	値
S_USER_AGR	ACT_GROUP	**<USER_ROLE>** *
	ACTVT	01, 02, 06
S_CTS_ADMI	CTS_ADMFCT	TABL

* **<USER_ROLE>** は、ユーザが属するロールの名前です。 このフィールドには、複数の値を入力できます。

28.1.1.19.1.7 BW への保存時の、レポートの翻訳準備

権限オブジェクト	フィールド	値
S_USER_AGR	ACT_GROUP	**<USER_ROLE>***
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

* **<USER_ROLE>** は、ユーザが属するロールの名前です。このフィールドには、複数の値を入力できます。

28.1.1.19.1.8 レポートの保存と同時の BI プラットフォームへの公開

権限オブジェクト	フィールド	値
S_USER_AGR	ACT_GROUP	**<USER_ROLE>***
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	**<INFO_AREA>** ***
	RSINFOCUBE	**<INFO_CUBE>** ***
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>** ***

権限オブジェクト	フィールド	値
S_RS_COMP1	RSZCOMPID	**<COMP_ID>** ***
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>** **
	ACTVT	16

* **<USER_ROLE>** は、ユーザが属するロールの名前です。このフィールドには、複数の値を入力できます。

** **<QUERY_OWNER>** は、レポートの作成元であるクエリの所有者の名前です。クエリの所有者を入力すると、この所有者のクエリからしかレポートを作成できません。あらゆるクエリの所有者を指定するには、「*」を入力します。

*** **< INFO_AREA>**、**<INFO_CUBE>** または **<COMP_ID>** に「*」を入力すると、すべての値になります。特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.1.9 BEx Query Designer™ の開始

権限オブジェクト	フィールド	値
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

* **<QUERY_OWNER>** は、レポートの作成元であるクエリの所有者の名前です。 クエリの所有者を入力すると、この所有者のクエリからしかレポートを作成できません。 あらゆるクエリの所有者を指定するには、「*」を入力します。

** **<INFO_AREA>**、**<INFO_CUBE>**、または **<COMP_ID>** に * を入力すると、すべての値になります。 特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.2 BI ラウンチパッド内のアクション

28.1.1.19.2.1 SAP 認証情報を使用した BI プラットフォームへのログオン

権限オブジェクト	フィールド	値
S_ADMI_FCD	S_ADMI_FCD	STOR、STOM

28.1.1.19.2.2 オンデマンドでの SAP BW レポートの表示

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>** は、レポートの作成元である所有者の名前です。クエリの所有者を入力すると、この所有者のクエリからしかレポートを作成できません。あらゆるクエリの所有者を指定するには、「*」を入力します。

** **< INFO_AREA>**、**<INFO_CUBE>** または **<COMP_ID>** に「*」を入力すると、すべての値になります。特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.2.3 ビューアからのレポートの最新表示

権限オブジェクト	フィールド	値
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>** は、レポートの作成元であるクエリの所有者の名前です。 クエリの所有者を入力すると、この所有者のクエリからしかレポートを作成できません。 あらゆるクエリの所有者を指定するには、「*」を入力します。

** **<INFO_AREA>**、**<INFO_CUBE>**、または **<COMP_ID>** に * を入力すると、すべての値になります。 特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.2.4 レポートのスケジュール

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR

権限オブジェクト	フィールド	値
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	**<INFO_AREA>****
	RSINFOCUBE	**<INFO_CUBE>****
	RSZCOMPTP	REP
	RSZCOMPID	**<COMP_ID>****
S_RS_COMP1	RSZCOMPID	**<COMP_ID>****
	RSZCOMPTP	REP
	RSZOWNER	**<QUERY_OWNER>***
	ACTVT	16
S_RS_ODSO	RSINFOAREA	**<INFO_AREA>****
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* **<QUERY_OWNER>** は、レポートの作成元である所有者の名前です。クエリの所有者を入力すると、この所有者のクエリからしかレポートを作成できません。あらゆるクエリの所有者を指定するには、「*」を入力します。

** **< INFO_AREA>**、**<INFO_CUBE>** または **<COMP_ID>** に「*」を入力すると、すべての値になります。特定の値を指定すると、その値の ID を持つインフォエリア、キューブ、コンポーネントを含むクエリだけでレポートを実行できます。

28.1.1.19.2.5 レポートパラメータのダイナミックピックリストの読み取り

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

28.1.1.19.3 SAP Netweaver (ABAP) 内のアクション

28.1.1.19.3.1 オープン SQL ドライバを使用して Crystal Reports で

ここでは、Open SQL ドライバを使用した Crystal Reports での SAP NetWeaver (ABAP) のさまざまな操作について説明します。

28.1.1.19.3.2 SAP サーバへのログオン

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.3.3 新しいレポートの作成

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	01

28.1.1.19.3.4 既存のレポートを開くまたはプレビュー

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16

権限オブジェクト	フィールド	値
ZSEGREPORT	ACTVT	02

28.1.1.19.3.5 データベースの検証(レポートでのテーブルの定義の最新表示)

権限オブジェクト	フィールド	値
S_ADMI_FCD	S_ADMI_FCD	ST0R、ST0M
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.3.6 データソースの場所の設定

権限オブジェクト	フィールド	値
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

28.1.1.19.4 インフォセットドライバを使用してインフォセットのレポートを作成する Crystal Reports 内のアクション

28.1.1.19.4.1 SAP サーバへのログオン

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

28.1.1.19.4.2 SAP Netweaver (ABAP) 上のインフォセットからの新しいレポートの作成

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT, SKBW, AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

ⓘ 注記

データ行の表示のために、十分な権限を追加します。たとえば P_ORIG や P_APAP などがあります。

関連情報

データソースの場所の設定 [1009 ページ]

28.1.1.19.4.3 データベースの検証(レポートでのテーブルの定義の最新表示)

権限オブジェクト	フィールド	値
S_ADMI_FCD	S_ADMI_FCD	ST0R、ST0M

28.1.1.19.4.4 データソースの場所の設定

権限オブジェクト	フィールド	値
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

28.1.1.19.5 インフォセットドライバを使用して ABAP クエリのレポートを作成する Crystal Reports 内のアクション

28.1.1.19.5.1 SAP サーバへのログオン

権限オブジェクト	フィールド	値
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

28.1.1.19.5.2 SAP Netweaver 上の ABAP クエリからの新しいレポートの作成

権限オブジェクト	フィールド	値
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP

権限オブジェクト	フィールド	値
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	STOR、STOM
S_TABU_DIS	ACTVT	03
	GROUP	テーブルグループの名前

28.1.1.19.5.3 データベースの検証

権限オブジェクト	フィールド	値
S_ADMI_FCD	S_ADMI_FCD	STOR、STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

28.1.1.19.5.4 データソースの場所の設定

権限オブジェクト	フィールド	値
P_ABAP	REPID	AQTG02==========P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	STOR、STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	テーブルグループの名前

28.1.1.19.6 BI プラットフォーム内のアクション

28.1.1.19.6.1 ダイアログモードでのレポートのスケジュール(オープン SQL クエリを使用)

権限オブジェクト	フィールド	値
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

> ⓘ 注記
>
> CLASS の値は空白です。

28.1.1.19.6.2 バッチモードでのレポートのスケジュール (オープン SQL クエリを使用)

権限オブジェクト	フィールド	値
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPENSQL, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02

権限オブジェクト	フィールド	値
S_BTCH_ADM	BTCADMIN	Y

> **注記**
> CLASS の値は空白です。

28.1.1.19.6.3 Crystal 権限認証システム

権限オブジェクト	フィールド	値
ファイルアクセスの認証(S_DATASET)	アクティビティ(ACTVT)	読み取り、書き込み(33、34)
	物理ファイル名(FILENAME)	*(すべてを意味します)
	ABAP プログラム名(PROGRAM)	*
RFC アクセスの認証チェック(S_RFC)	アクティビティ(ACTVT)	16
	保護される RFC の名前(RFC_NAME)	BDCH、STPA、SUSO、SUUS、SU_USER、SYST、SUNI、PRGN_J2EE、/CRYSTAL/SECURITY
	保護される RFC オブジェクトのタイプ(RFC_TYPE)	プログラムグループ(FUGR)
ユーザマスタメンテナンス: ユーザグループ (S_USER_GRP)	アクティビティ(ACTVT)	作成または生成、および表示(03)
	ユーザマスタメンテナンスのユーザグループ (CLASS)	* **注記** セキュリティ機能を強化にするために、BI プラットフォームへのアクセスを必要とするメンバーを含むユーザグループを明示的に一覧に示すことができます。

28.1.1.19.6.4 BW BEx クエリの実行および設計

BW BEx クエリに基づくユニバースからレポートを作成する際、日付ディメンションが含まれている場合、システム管理者は、ユニバースを設計するユーザおよびレポートを実行するユーザの両方に対して S_RS_IOBJ 権限を付与する必要があります。

権限オブジェクト	フィールド	値
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

28.2 JD Edwards 統合の設定

28.2.1 SAP Crystal Reports のシングルサインオンの設定

デフォルトでは、BI プラットフォームは、SAP Crystal Reports ユーザがシングルサインオン (SSO) を使用して JD Edwards EnterpriseOne のデータにアクセスできるよう設定されています。

28.2.1.1 JD Edwards および SAP Crystal Reports の SSO を無効化する

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。
4. [*crdb_pseone*] を入力します。
5. [削除] をクリックします。
6. [保存して閉じる]をクリックします。
7. CMC の [サーバ] ページで、[*Crystal Reports* サービス] を選択し [サーバの再起動] をクリックします。

28.2.1.2 JD Edwards および SAP Crystal Reports の SSO を有効化する

JD Edwards および SAP Crystal Reports の SSO を無効化している場合は、再有効化します。

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。
4. [以下のドライバを使用したデータベースログオンに *SSO* コンテキストを使用] で「*crdb_pseone*」と入力します。

5. [追加] をクリックします。
6. [保存して閉じる]をクリックします。
7. CMC の [サーバ] ページで、[*Crystal Reports* サービス] を選択し [サーバの再起動] をクリックします。

28.2.2 JD Edwards Integrations のセキュアソケットレイヤの設定

BI プラットフォームおよび JD Edwards EnterpriseOne デプロイメントのクライアントとサーバの間で行われるすべてのネットワーク通信に、Secure Sockets Layer (SSL) プロトコルを使用できます。

BI プラットフォームで JD Edwards EnterpriseOne のデータを使用するには、一部の SSL 設定を変更する必要があります。他の BI プラットフォームサーバおよびクライアントに対する SSL 設定と同様に、BI プラットフォームデプロイメント内のコンピュータからアクセスできる安全な場所 (同じディレクトリ内) に次のキーと証明書ファイルを保存してください。

- 信頼できる証明書ファイル(cacert.der)
- 生成されたサーバ証明書ファイル(servercert.der)
- サーバキーファイル(server.key)
- パスフレーズファイル(passphrase.txt)

28.2.2.1 SSL を使用した JD Edwards EnterpriseOne のデータ接続を有効にする

> ⓘ 注記
>
> 次の手順に記載されている値はすべて大文字と小文字が区別されます。

1. SSL 証明書を `C:¥SSLCert` にコピーします。
2. セントラル設定マネージャ (CCM) を開始します。
3. Server Intelligence Agent(SIA)を停止します。
4. SIA をダブルクリックして [プロパティ] ダイアログボックスを開きます。
5. [プロトコル] タブをクリックします。
6. [*SSL* を有効にする] を選択します。
7. *SSL* 証明書フォルダで、SSL 証明書が含まれるディレクトリ `C:¥SSLCert` を選択します。
8. サーバ *SSL* 証明書ファイルで、`servercert.der` を選択します。
9. 信頼できる *SSL* 証明書ファイルで、`cacert.der` を選択します。
10. *SSL* 秘密鍵ファイルで、`server.key` を選択します。
11. *SSL* 秘密鍵パスフレーズファイルで、`passphrase.txt` を選択します。
12. 適用をクリックします。
13. Server Intelligence Agent を起動します。

これらの変更を有効にする前に、BI プラットフォームレポーティングサーバ (Adaptive Job Server など) を再起動する必要があります。

28.2.2.2 SSL 設定プロパティファイル

`sslconf.properties` プロパティファイルには、BI プラットフォームによって使用される必要な証明書とキーに関するすべての情報が含まれています。例:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

`sslconf.properties` ファイルは、BI プラットフォームがインストールされているフォルダ (デフォルトで `C:¥Program Files¥Business Objects¥BusinessObjects 13.0`) に配置する必要があります。

28.3 PeopleSoft Enterprise 統合の設定

28.3.1 SAP Crystal Reports および PeopleSoft Enterprise のシングルサインオン (SSO) の設定

デフォルトでは、BI プラットフォームは、SAP Crystal Reports ユーザがシングルサインオン (SSO) を使用して PeopleSoft Enterprise のデータにアクセスできるよう設定されています。

28.3.1.1 PeopleSoft Enterprise および SAP Crystal Reports の SSO を無効化する

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。
4. [*crdb_psenterprise*] を選択します。
5. [削除] をクリックします。
6. [保存して閉じる]をクリックします。
7. CMC の [サーバ] ページで、[*Crystal Reports* サービス] を選択し [サーバの再起動] をクリックします。

28.3.1.2 PeopleSoft Enterprise および SAP Crystal Reports の SSO を有効化する

PeopleSoft Enterprise および SAP Crystal Reports の SSO を無効化している場合は、再有効化します。

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。
4. [以下のドライバを使用したデータベースログオンに *SSO* コンテキストを使用] で「*crdb_psenterprise*」と入力します。
5. [追加] をクリックします。
6. [保存して閉じる]をクリックします。
7. CMC の [サーバ] ページで、[*Crystal Reports* サービス] を選択し [サーバの再起動] をクリックします。

28.3.2 Secure Sockets Layer (SSL) 通信の設定

BI プラットフォームデプロイメントのクライアントとサーバの間で行われるすべてのネットワーク通信について、Secure Sockets Layer (SSL) プロトコルを使用できます。

他の BI プラットフォームサーバおよびクライアントに対する SSL 設定と同様に、BI プラットフォームデプロイメント内のマシンからアクセスできる安全な場所 (同じディレクトリ内) に次のキーと証明書ファイルを保存してください。

- 信頼できる証明書ファイル(cacert.der)
- 生成されたサーバ証明書ファイル(servercert.der)
- サーバキーファイル(server.key)
- パスフレーズファイル(passphrase.txt)

28.3.2.1 SSL 設定プロパティファイル

`sslconf.properties` プロパティファイルには、BI プラットフォームコンポーネントによって使用される必要な証明書とキーに関するすべての情報が含まれています。例:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

`sslconf.properties` ファイルは、BI プラットフォームがインストールされているフォルダに配置してください。デフォルトフォルダは、`C:¥Program Files¥Business Objects¥BusinessObjects 12.0 Integration Kit for PeopleSoft¥` です。

28.3.2.2 SSL を使用した PeopleSoft Query Server を有効にする

> ⓘ 注記
>
> 次の手順に記載されている値はすべて大文字と小文字が区別されます。

1. SSL 証明書を `C:¥SSLCert` にコピーします。
2. セントラル設定マネージャ (CCM) を開始します。
3. Server Intelligence Agent(SIA)を停止します。
4. SIA をダブルクリックして [プロパティ] ダイアログボックスを開きます。
5. [プロトコル] タブをクリックします。
6. [*SSL を有効にする*] を選択します。
7. *SSL 証明書フォルダ*で、SSL 証明書が含まれるディレクトリ `C:¥SSLCert` を選択します。
8. サーバ *SSL 証明書ファイル*で、`servercert.der` を選択します。
9. 信頼できる *SSL 証明書ファイル*で、`cacert.der` を選択します。
10. *SSL 秘密鍵ファイル*で、`server.key` を選択します。
11. *SSL 秘密鍵パスフレーズファイル*で、`passphrase.txt` を選択します。
12. 適用をクリックします。
13. Server Intelligence Agent を起動します。

これらの変更を有効にする前に、BI プラットフォームレポーティングサーバ (Adaptive Job Server など) を再起動する必要があります。

28.3.2.3 SSL を使用したセキュリティブリッジを有効にする

> ⓘ 注記
>
> 次の手順に記載されている値はすべて大文字と小文字が区別されます。

1. SSL 証明書を `C:¥SSLCert` にコピーします。
2. セントラル設定マネージャ (CCM) を開始します。
3. Server Intelligence Agent(SIA)を停止します。
4. SIA をダブルクリックして [プロパティ] ダイアログボックスを開きます。
5. [プロトコル] タブをクリックします。
6. [*SSL を有効にする*] を選択します。
7. *SSL 証明書フォルダ*で、SSL 証明書が含まれるディレクトリ `C:¥SSLCert` を選択します。
8. サーバ *SSL 証明書ファイル*で、`servercert.der` を選択します。
9. 信頼できる *SSL 証明書ファイル*で、`cacert.der` を選択します。
10. *SSL 秘密鍵ファイル*で、`server.key` を選択します。
11. *SSL 秘密鍵パスフレーズファイル*で、`passphrase.txt` を選択します。
12. 適用をクリックします。

13. Server Intelligence Agent を起動します。

28.3.3 PeopleSoft システムのパフォーマンスチューニング

PeopleSoft クエリからレポートを作成する場合に最適なパフォーマンスを確保するには、Crystal Reports と BI プラットフォームによるクエリの実行方法を理解しておくことが重要です。

PeopleSoft クエリに基づくレポートを最新表示または実行すると、PeopleSoft サーバに接続が確立されます。

- PeopleSoft Enterprise(PeopleTools 8.46 以降)環境では、*PeopleSoft Analytic Server* に接続が確立されます。
- PeopleSoft Enterprise(PeopleTools 8.21 ～ 8.45)環境では、*PeopleSoft Application Server* に接続が確立されます。

28.3.3.1 推奨事項

最適な導入環境では、レポートリクエストの処理専用に 1 つまたは複数の PeopleSoft Analytic Server または PeopleSoft Application Server がセットアップされます。これらの各サーバで、最小インスタンスおよび最大インスタンスに対する設定によって、同時に処理できるレポート数を制御します。この設定には、次のような長所があります。

- PeopleSoft サーバで、レポートリクエストとその他のトランザクションリクエストが競合しません。
- トランザクションリクエストを処理するサーバを無効にすることなく、レポートリクエストを処理するサーバのメンテナンスを実行できます。

レポートリクエストとトランザクションリクエストの双方が 1 つの PeopleSoft Analytic Server または PeopleSoft Application Server によって処理される環境では、複数のレポートを同時に実行しないように BI プラットフォームを設定する必要があります。この設定を行わないと、すべての PSANALYTICSRV または PSAPPSRV プロセスがレポートの実行に使用された場合、一切のトランザクションリクエストを実行できなくなります。

> ⓘ 注記
>
> スケジュール済みのレポートジョブやオンデマンドレポート表示ジョブのジョブ数を制限する方法については、*SAP BusinessObjects Business Intelligence* プラットフォーム管理者ガイドの「サーバの管理および設定」を参照してください。

> ⓘ 注記
>
> サーバへのアクセスを同時に試行する Crystal Reports ユーザ数をシステムの設定によって制限することはできません。

パフォーマンス上の問題が発生した場合は、Psadmin 設定ツールを使用して、リクエストが待機中になっているかどうかを確認します。同時に、PeopleSoft Analytic Server または PeopleSoft Application Server マシンのシステムリソースを監視します。物理メモリの不足による仮想メモリの使用も、処理スピードの低下を引き起こす場合があります。

28.3.3.2 PeopleSoft サーバ

PeopleSoft Analytic Server では、レポートを最新表示または実行するプロセスは PSANALYTICSRV プロセスです。PeopleSoft Application Server では、レポートを最新表示または実行するプロセスは PSAPPSRV プロセスです。使用可能な PSANALYTICSRV または PSAPPSRV プロセスの数により、同時に実行できるレポート数が決まります。

通常、PeopleSoft Analytic Server または Application Server の構成ファイルには次の情報が含まれています。

```
Min Instances=3
Max Instances=5
```

この例では、常時最低 3 つの PSANALYTICSRV または PSAPPSRV プロセスを使用でき、最大 5 つまでプロセス数を増やすことができます。この設定は、必ずしも 5 つのレポートを常に実行できることを意味しません。このプロセスは、システム内での他のタスクの処理に使用される場合もあります。リクエストの処理に使用できる PSANALYTICSRV または PSAPPSRV プロセスがない場合には、プロセスが使用できるようになるまでそのリクエストは待機状態になります。

> **注記**
>
> 通常は PeopleSoft *Application* Server の構成ファイルにも、`Service Timeout` パラメータが含まれます。これは、待機状態のリクエストが使用可能なプロセスの出現を待つ最長時間を指定するパラメータです。このパラメータに指定された時間内にプロセスが使用可能にならなかった場合は、リクエストがタイムアウトになります。

28.4 Siebel 統合の設定

28.4.1 SAP BI プラットフォームと統合するための Siebel の設定

BI プラットフォーム統合は、SAP BusinessObjects Business Intelligence スイートのコンテンツを Siebel アプリケーションに組み込めるようにする Crystal Reports へのリンクを提供します。 インストールおよび設定ができたら、新しいメニュー項目が表示され、Siebel アプリケーション内から BI 起動パッドを起動することができます。

デフォルトでは、必要なファイルは `C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥Samples¥siebel¥Siebel Files¥` にインストールされます。

28.4.1.1 BI プラットフォーム Siebel 統合プロジェクトをインポートする

1. Siebel Tools を開始します。
2. ▶ ツール ▶ アーカイブからインポート ▶ をクリックします。
3. アーカイブファイルを要求されたら、Integration 製品がインストールされている Siebel Files フォルダを参照します。

デフォルトでは、このフォルダは `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Samples¥siebel¥Siebel Files¥` です。

4. 該当するサブフォルダ (Siebel 7.7 または Siebel 8.0 のいずれか) で、`BusinessObjectsEnterprise.sif` ファイルを選択します。
   インポート ウィザードが表示されます。
5. [リポジトリで定義付きアーカイブ ファイルからオブジェクト定義をマージ] をクリックします。
6. ウィザードの画面を最後まで進めて、統合プロジェクトのインポートを終了します。
   統合プロジェクトがリポジトリに追加されます。
7. *BusinessObjects Integration* プロジェクトについて説明します。

28.4.2 Crystal Reports のメニュー項目の作成

1. Siebel Tools で、[メニュー]プロジェクトをロックします。
2. オブジェクトエクスプローラで、[メニュー項目]オブジェクトを選択します。

   > **注記**
   >
   > メニューオブジェクトがオブジェクトエクスプローラに表示されない場合、Siebel Tools で 表示 > オプション の順にクリックし、[オブジェクトエクスプローラ]タブをクリックして[メニュー]オブジェクトを選択します。

3. [メニュー]リストで、[一般 *Web*]メニューを選択します。
4. [メニュー項目]リストの見出しをクリックします。
5. 編集 > 新しいレコード をクリックします。
6. 新しいメニュー項目を適切に定義します。以下は、推奨される値です。
   - 名前: View - Crystal Reports
   - コマンド: Crystal Reports
   - コメント: SAP BusinessObjects Integrated Report Menu
   - 非アクティブ: False
7. 表示メニューでのメニュー項目の場所を選択するには、位置番号を使用します。

   位置番号を選びやすくするには、メニュー項目を位置で並べ替えます。
8. これで、キャプションを適切にローカライズするためにロケールを追加できます。

Siebel アプリケーションを再コンパイルします。Siebel アプリケーションの再コンパイル [1020 ページ] を参照してください。

28.4.2.1 Siebel アプリケーションの再コンパイル

BI プラットフォームをインストールし、ユーザが Siebel のメニュー項目からコマンドを使用できるようにした場合、次の通常の手順に従って Siebel アプリケーションを再コンパイルする必要があります。詳細は、Siebel Bookshelf を参照してください。

Siebel アプリケーションを再コンパイルする場合、その JavaScript ファイルも再生成してください。Siebel 7.7 およびそれ以降のバージョンでは、再コンパイルプロセスの一環として JavaScript ファイルの再生成を自動で実行することができます。

Siebel リポジトリをコンパイルするために必要な手順は、Siebel Tools ワークステーションで実行されるため、再生成された JavaScript を Siebel Tools ワークステーションから Siebel Server にデプロイする必要があります。通常、Siebel がインストールされている場所に応じて、生成された JavaScript ファイルは次の場所に保存されます。

```
C:¥sea77¥tools¥PUBLIC¥ENU¥<srf1096416329_444>
```

たとえばフォルダ名「**<srf1096416329_444>**」は、Siebel Tools で生成され、リポジトリファイルの結果に一意に対応しています。

JavaScript ファイルは、Siebel Server にデプロイされる必要があり、通常、Siebel ga インストールされている場所に応じて、次の場所に保存されます。

```
C:¥sea77¥SWEApp¥PUBLIC¥ENU¥<srf1096416329_444>
```

フォルダ名は、Siebel Tools で生成された名前のままにしておいてください。

また、サービスを許可するために、Siebel Server マシン上で Siebel 設定ファイルを更新する必要があります。ユーザの Siebel Server マシンで適切な設定ファイルを検索します。たとえば、英語版の Siebel Call Center を実行している場合、`uagent.cfg` を使用します。Siebel 7.7 の場合、このファイルは、デフォルトで `C:¥sea77¥siebsrvr¥bin¥ENU¥uagent.cfg` にあります。

次に、設定ファイルの SWE セクションの最後に、次の行を追加します。

```
ClientBusinessService<NUMBER> = BusinessObjects Integration Service
```

`ClientBusinessService` 番号は連番です。SWE セクションに他の ClientBusinessServices がない場合、**<NUMBER>** を「0」に設定します。それ以外では、**<NUMBER>** を次に大きな数字に設定します。

Siebel 8.x 以降の場合:

1. Siebel Tools にログインして、[*Siebel* ユニバースエージェント]アプリケーションオブジェクトをオブジェクトエクスプローラで検索します。
2. アプリケーションオブジェクトを展開して、[アプリケーションユーザプロパティ]オブジェクトを表示します。
3. 宣言されるように各 Business Service で新しいレコードを作成し、それぞれの名前および値プロパティを次のように設定します。
   - 名前 = ClientBusinessServiceX
   - 値 = BusinessObjects Integration

インポートされた Siebel コマンドを呼び出す Crystal Reports のメニュー項目を作成します。

28.4.3 コンテキスト認識

コンテキスト認識は、ユーザの現在のタスクに関連する可能性のあるレポートをユーザに表示する機能です。この場合、Siebel クライアントアプリケーションから Crystal Reports に直接アクセスするユーザには、Siebel データを組み込むように設計されたレポートが自動的に表示されます。

28.4.3.1 コンテキスト認識を設定する

コンテキストの検出感度を設定する前に、次のことを完了しておいてください。

- Siebel Integration 製品のインストール
- BI プラットフォームと統合するための Siebel の設定

1. セントラル管理コンソール (CMC) を開きます。
2. [認証]をクリックします。
3. [*Siebel*]をダブルクリックします。
   Siebel マッピングインタフェースが表示されます。
4. [ドメイン]をクリックします。
   ドメインマッピングインタフェースが表示されます。
5. 使用する Siebel サーバに対応するドメイン名をメモします。
6. Siebel マッピングインタフェースを閉じます。
7. BI ラウンチパッドを開きます。
8. `PublicFolders¥Siebel` の下に、CMC の Siebel ドメインと同じ名前の新しいフォルダを作成します。
9. Siebel の情報を組み込むように設計されたレポートをこのフォルダに配置します。

28.4.3.2 コンテキストの認識を URL に指定する

1. アプリケーションの JavaScript ファイルを再生成したら、BI プラットフォームの Siebel Files フォルダに移動します。このフォルダは、デフォルトで `C:¥Program Files¥Business Objects¥SAP BusinessObjects Enterprise XI¥Siebel Files¥` です。
2. `BusinessObjectsEnterpriseServer.html` ファイルをコピーします。genbscript プログラムが新しい JavaScript ファイルを生成したパブリックフォルダを特定し、`BusinessObjectsEnterpriseServer.html` のコピーを適切な言語サブフォルダにコピーします。

   たとえば、アプリケーションの JavaScript ファイルを Siebel サーバの `c:¥sea752¥SWEApp¥PUBLIC¥ENU` フォルダに生成した場合は、`BusinessObjectsEnterpriseServer.html` ファイルを `c:¥sea752¥SWEApp¥PUBLIC¥ENU` フォルダにコピーします。
3. パブリックフォルダから `BusinessObjectsEnterpriseServer.html` ファイルを Notepad などのテキストエディタで開き、次の行を記入します。

```
Var userDomain = "SIEB78"

var destAddr = "http://<SAP BusinessObjects server>:8080/BOE/BI/logon/
siebelStart.do"
```

> **注記**
>
> `<userDomain>` または `<destAddr>` 変数を変更した場合は、ブラウザが正しい参照先アドレスを示すように、ブラウザにキャッシュされた Web ページを削除する必要があります。

> **注記**
>
> userDomain では、大文字と小文字が区別されます。

28.4.3.3 コンテキスト認識を確認する

1. Siebel ツールで、デバッグ > 開始 をクリックします。
2. 任意の画面に移動し、[表示]メニューをクリックします。
   新しい Crystal Reports メニュー項目がメニューに表示されます。
3. [*Crystal Reports*]メニュー項目をクリックします。
   BI プラットフォームで [BI ラウンチパッド] ウィンドウが開き、接続のためのユーザ名とパスワードが要求されます。これはセッションタイムアウトの前に、初めてログオンする場合にのみ必要になります。html と Siebel 認証に設定されているドメイン名がすでに入力されています。

> ⓘ 注記
>
> このステップは、この時点までのインストールを確認する場合のみ行います。Siebel 機能を BI プラットフォームにマップするまで、Siebel 認証を使用して BI プラットフォームにログオンできません。

28.4.3.4 BI プラットフォームへのフォルダの追加

BI プラットフォーム Integration for Siebel では、コンテキスト認識機能を完全に有効化するために、BI ラウンチパッドにいくつかのフォルダを追加する必要があります。

関数には、`Public Folders¥Siebel¥<Domain Name>` のような構造のコンテキストフォルダが必要です。`<Domain Name>` サブフォルダに保存され、特定の SAP BusinessObjects ビジネスコンポーネントと関連付けられた Siebel システムで構成されたレポートのみが、コンテキスト認識機能の一部として表示されます。ここで使用される `<Domain Name>` は、認証設定で Siebel 用に設定されたドメイン名と同じで、かつ、Siebel 側の `BusinessObjectsEnterpriseServer.html` ファイルで設定された値と同じである必要があります。

> ⓘ 注記
>
> Siebel Tools では、このセクションの手順を完了する必要があります。

28.4.4 SAP Crystal Reports および Siebel のシングルサインオン (SSO) の設定

デフォルトで、BI プラットフォームは、SAP Crystal Reports ユーザがシングルサインオン (SSO) を使用して Siebel データにアクセスできるよう設定されています。

28.4.4.1 Siebel と SAP Crystal Reports の SSO を無効化する

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。

4. [*crdb_siebel*] を選択します。
5. [削除] をクリックします。
6. [保存して閉じる]をクリックします。
7. SAP Crystal Reports を再起動します。

28.4.4.2 Siebel と SAP Crystal Reports の SSO を有効化する

Siebel と SAP Crystal Reports の SSO を無効にした後で、これを再有効化する場合。

1. セントラル管理コンソール (CMC) で [アプリケーション] をクリックします。
2. [*Crystal Reports* 設定] をダブルクリックします。
3. [シングルサインオンオプション] をクリックします。
4. [*SSO* コンテキストをデータベースログオンに使用する] で、[*crdb_siebel*] と入力します。
5. [追加] をクリックします。
6. [保存して閉じる]をクリックします。
7. SAP Crystal Reports サーバを再起動します。

28.4.5 Secure Sockets Layer (SSL) 通信の設定

Siebel および BI プラットフォームデプロイメントのクライアントとサーバの間で行われるすべてのネットワーク通信について、Secure Sockets Layer (SSL) プロトコルを使用できます。

他の BI プラットフォームサーバおよびクライアントに対する SSL 設定と同様に、Siebel デプロイメント内のマシンからアクセスできる安全なディレクトリ内に次のキーと証明書ファイルを保存してください。

- 信頼できる証明書ファイル(cacert.der)
- 生成されたサーバ証明書ファイル(servercert.der)
- サーバキーファイル(server.key)
- パスフレーズファイル(passphrase.txt)

SSL 設定プロパティファイル

プロパティファイル `sslconf.properties` には、Integration for Siebel コンポーネントに必要な証明書およびキーに関するすべての情報が格納されています。 例:

```
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

sslconf.properties ファイルは、BI プラットフォーム製品がインストールされているフォルダに配置してください。デフォルトフォルダは、C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0 です。

28.4.5.1 SSL を使用した Siebel データ接続を有効にする

> **注記**
>
> 次の手順に記載されている値はすべて大文字と小文字が区別されます。

1. SSL 証明書を C:¥SSLCert にコピーします。
2. セントラル設定マネージャ (CCM) を開始します。
3. Server Intelligence Agent(SIA)を停止します。
4. SIA をダブルクリックして [プロパティ] ダイアログボックスを開きます。
5. [プロトコル] タブをクリックします。
6. [*SSL を有効にする*] を選択します。
7. *SSL 証明書フォルダ*で、SSL 証明書が含まれるディレクトリ C:¥SSLCert を選択します。
8. *サーバ SSL 証明書ファイル*で、servercert.der を選択します。
9. *信頼できる SSL 証明書ファイル*で、cacert.der を選択します。
10. *SSL 秘密鍵ファイル*で、server.key を選択します。
11. *SSL 秘密鍵パスフレーズファイル*で、passphrase.txt を選択します。
12. 適用をクリックします。
13. Server Intelligence Agent を起動します。

これらの変更を有効にする前に、BI プラットフォームレポーティングサーバ (Adaptive Job Server など) を再起動する必要があります。

29 管理および設定ログ

29.1 コンポーネントのトレースのログ

ログ

BI プラットフォームでは、システムレベルのメッセージが生成され、ログファイルに書き込まれます。システム管理者は、このログファイルを使用してパフォーマンスの監視やエラーのデバッグができます。

トレース

BI プラットフォームではトレース (監視対象コンポーネントの運用中に発生したイベントの記録) も生成され、拡張子が `.glf` のログファイルに収集されます。トレースされるイベントは、ステータスメッセージから重大な例外エラーまでさまざまです。SAP のサポート担当者および開発者は、トレースを使用して、BI プラットフォームコンポーネント (サーバおよび Web アプリケーション) のパフォーマンス、および監視対象コンポーネントのアクティビティについてレポートすることができます。

コンポーネントのトレースログレベルを設定する際に、ログファイルに送信する情報のタイプと冗長性を決定します。トレースログレベルとは、指定したしきい値未満のトレースを非表示にするフィルタです。コンポーネントのトレースログを監視することにより、増加した負荷の下で運用するためにコンポーネントの現在のインスタンスまたはその設定を変更する必要があるかどうかを確認できます。

> **注記**
>
> BI プラットフォームのログファイルは任意のテキストエディタを使用して表示できます。

29.2 トレースログレベル

BI プラットフォーム のコンポーネントでは、次のトレースログレベルを利用できます。

レベル	説明
未指定	このトレースログレベルは他の方法 (通常は `.ini` ファイル) で指定します。
なし	トレースは発生しません。
低	このトレースログフィルタでは、警告とステータスメッセージを無視しながら、エラーメッセージをログできます。コンポーネントのスタートアップ、シャットダウン、リクエスト

レベル	説明
	の開始、リクエストの終了の各メッセージについては、重要ステータスメッセージがログされます。このレベルは、デバッギング目的の場合はお勧めしません。
中	このトレースログフィルタは、エラー、警告、ほとんどのステータスメッセージを含むよう設定されます。あまり重要ではない、または非常に詳細なメッセージはフィルタで除外されます。このレベルは、デバッギング目的には詳細度が足りません。
高	メッセージはフィルタリングされません。このレベルは、デバッギング目的の場合にお勧めします。 **⚠ 警告** このトレースログレベルは、CPU 使用率を上げストレージ容量を消費するため、システムリソースに大きな影響を与えます。

29.3 サーバのトレースの設定

ログメッセージとは、ソフトウェアシステムのイベントとステータスの永続記録です。監視対象の BI プラットフォームデプロイメントのトレースは特定の `.glf` ログファイルに書き込まれ、ログディレクトリに格納されます。

- Windows の場合、デフォルトの場所は `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥logging` です。
- Unix の場合、デフォルトの場所は `<INSTALLDIR>/sap_bobj/logging` です。

`.glf` ログファイルの名前には、`aps_mysia.AdaptiveProcessingServer_trace.000012.glf` のように、略称 ID、サーバ名、参照番号が含まれます。ログファイルのサイズが 10 メガバイトのしきい値に達すると、監視対象サーバに新しいトレースログファイルが作成されます。また、同時に 5 つのログファイルが管理されます。新しいログファイルが作成されると、古いログファイルは削除されます。

特定のサーバまたはサーバのグループにトレースログレベルを設定することで、ログファイルに集められたトレースの重大度と重要度を測定することができます。

ⓘ 注記

特定のサーバまたはサーバのグループのトレースログレベルを変更するには、セントラル管理コンソール (CMC) のトレースログサービスを使用します。ほかのパラメータを変更するには、`BO_trace.ini` ファイルのトレースログレベルおよびその他の設定を手動で変更します。

29.3.1 CMC にログレベルを設定する

サーバのトレースログレベルは、他のトレース設定に影響を与えずに調整できます。

1. CMC の [サーバ] エリアで、サーバにアクセスします。
   - 特定のカテゴリからサーバを選択します。
   - ナビゲーションペインの [サーバの一覧] をクリックし、サーバの完全一覧にアクセスし、サーバを選択します。
2. 選択したサーバを右クリックし、[プロパティ] を選択します。
   [プロパティ]ダイアログボックスが表示されます。
3. [トレースログ設定] エリアで、[ログレベル] リストから設定を選択します。
4. [保存して閉じる] をクリックします。

新しいトレースログレベルが直ちに適用されます。

ログファイルに別の出力ディレクトリを指定する場合は、[コマンドラインパラメータ] エリアに `-loggingPath <target_directory>` パラメータを含めます。この設定を有効にするには、コンピュータを再起動します。

関連情報

トレースログレベル [666 ページ]

29.3.2 CMC の複数のサーバにログレベルを設定する

1. CMC の [サーバ] エリアで、複数のサーバにアクセスします。
   - 特定のカテゴリからサーバを選択します。
   - ナビゲーションペインの [サーバの一覧] をクリックし、サーバの完全一覧にアクセスします。`Ctrl` キーを押したまま複数のサーバをクリックして選択します。
2. 選択したサーバを右クリックし、[共通サービスの編集] を選択します。
   [共通サービスの編集] ダイアログボックスが表示されます。
3. [トレースログ設定] エリアで、[ログレベル] リストから設定を選択します。
4. [*OK*] をクリックします。

新しいトレースログレベルが直ちに適用されます。

ログファイルに別の出力ディレクトリを指定する場合は、[コマンドラインパラメータ] エリアに `-loggingPath <target_directory>` パラメータを含めます。この設定を有効にするには、コンピュータを再起動します。

関連情報

トレースログレベル [666 ページ]

29.3.3 BO_trace.ini ファイルを使ってサーバトレースを設定する

BO_trace.ini ファイルには、デフォルトでエラーとアラートのみが記録されます。

1. BO_trace.ini ファイルを開きます。
   - Windows の場合、デフォルトの場所は <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥conf¥ です。
   - Unix の場合、デフォルトの場所は <INSTALLDIR>/sap_bobj/enterprise_xi40/conf/ です。
2. “Trace Syntax and Setting” セクションの行をコメント解除します。
3. サーバトレースパラメータを変更します。サーバトレースの設定には次のパラメータを使用します。

パラメータ	入力される値	説明
sap_log_level	**log_information** **log_warning** **log_error** **log_fatal** **log_none**	ログメッセージの重大度を決定します。デフォルトのログの重大度は **log_error** です。 ログの重大度は、最上位を **log_information**、最下位を **log_none** とする階層になっています。ログの重大度をあるレベルに設定すると、そのレベル以下のすべてのメッセージが表示されます。たとえば、ログの重大度を **log_warning** に設定すると、**log_warning**、**log_error**、および **log_fatal** を含むメッセージがログファイルに書き込まれます。 ⓘ 注記 **log_information** および **log_warning** は **log_info** および **log_warn** に短縮できます。
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	トレースメッセージの重大度を決定します。デフォルトのトレースの重大度は **trace_error** です。 トレースの重大度は、最上位を **trace_debug**、最下位を **trace_none** とする階層になっています。トレースの重大度をあるレベルに設定すると、そのレベル以下のすべてのメッセージが表示されます。たとえば、トレースの重大度を **trace_path** に設定すると、**trace_path**、

パラメータ	入力される値	説明
		trace_information、および **trace_error** を含むメッセージがログファイルに書き込まれます。 ⓘ 注記 **trace_information** は **trace_info** に短縮できます。

4. BO_trace.ini ファイルを保存して閉じます。

BO_trace.ini ファイルは頻繁に読み取られます。BO_trace.ini ファイルに対する変更は、保存してから 5 分以内に有効になります。CMS を再起動すると、BO_trace.ini ファイルに対する変更は直ちに有効になります。

例

BO_trace.ini ファイル

```
sap_log_level=log_warning;
sap_trace_level=trace_path;
```

29.3.3.1 特定のサーバのトレースを設定する

BI プラットフォームサーバのトレースパラメータは BO_trace.ini ファイルで指定します。設定はすべての管理サーバに影響します。管理者は BO_trace.ini ファイルを使用して、指定サーバの特定のトレースパラメータを設定できます。

> ⚠ 警告
>
> 特定のサーバに対して CMC に新たなトレースログレベル設定を指定すると、BO_trace.ini 内の設定はすべて上書きされます。

1. BO_trace.ini ファイルを開きます。
   - Windows の場合、デフォルトの場所は <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥conf¥ です。
   - Unix の場合、デフォルトの場所は <INSTALLDIR>/sap_bobj/enterprise_xi40/conf/ です。
2. 特定のサーバにトレース設定を指定するには if 文を使用します。例:

```
if (process == "aps_MySIA.ProcessingServer") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

> → ヒント
>
> 特定のサーバにトレース設定を適用するには、プロセスを指定する必要があります。

3. BO_trace.ini ファイルを保存して閉じます。

変更した設定は 5 分以内に実装されます。

29.4 Web アプリケーションのトレース設定

監視対象の BI プラットフォームデプロイメントのトレースは、特定の .glf ログファイルに書き込まれ、Web アプリケーションフォルダをホストするマシン上のディレクトリに格納されます。

- Windows の場合、デフォルトの場所は C:¥Windows¥System32¥config¥systemprofile¥SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>¥ です。たとえば、C:¥Windows¥System32¥config¥systemprofile¥SBOPWebapp_BIlaunchpad_192.0.2.0_8080¥ です。
- Unix の場合、デフォルトの場所は $userHome/SBOPWebapp_<APPLICATION>_<IPADDRESS>_<PORT>/ です。たとえば、$userHome/SBOPWebapp_CMC_192.0.2.0_8080/ です。

CMC の Web アプリケーションのトレースログレベルは、デフォルトで [指定なし] に設定されています。トレースログ設定は、CMC 内の次のアプリケーションで使用できます。

- セントラル管理コンソール
- BI ラウンチパッド
- OpenDocument
- Web サービス

> **注記**
>
> 特定のサーバまたはサーバのグループのトレースログレベルを変更するには、セントラル管理コンソール (CMC) のトレースログサービスを使用します。ほかのパラメータを変更するには、BO_trace.ini ファイルのトレースログレベルおよびその他の設定を手動で変更します。このファイルは、BOE.war および dswsbobje.war ファイルとともに、Web アプリケーションサーバ上にデプロイされます。

BO_trace.ini ファイルを設定する前に、WDeploy ツールを使用して Web アプリケーションサーバから既存の Web アプリケーションをアンデプロイする必要があります。BO_trace.ini ファイルを設定したら、Web アプリケーションサーバ上に Web アプリケーションとともに再デプロイする必要があります。WDeploy を使用して Web アプリケーションを準備、デプロイ、アンデプロイする際の詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。

29.4.1 CMC の Web アプリケーショントレースログレベルを設定する

他の Web アプリケーションをトレースするには、対応する BO_trace.ini ファイルを手動で設定してください。

1. CMC の [アプリケーション] エリアでアプリケーションを右クリックして、[トレースログ設定] を選択します。

> ⓘ 注記
>
> トレースログ設定があるアプリケーションは、Fiorified BI ラウンチパッド、CMC、OpenDocument、プロモーション管理、バージョン管理、Visual Difference、および Web サービスです。

[トレースログを設定] ダイアログボックスが表示されます。

2. [ログレベル] リストから設定を選択します。
3. [保存して閉じる] をクリックします。
4. Web アプリケーションサーバを再起動します。

新しいトレースログレベルは、Web アプリケーションに次回ログオンしたときに有効になります。

関連情報

トレースログレベル [666 ページ]

29.4.2 `BO_trace.ini` ファイルを使ってトレース設定を設定する

`BO_trace.ini` ファイルは、`BOE` および `dswsbobje.war` ファイルとともに Web アプリケーションサーバ上にデプロイされます。`BO_trace.ini` を使用して、BI プラットフォーム Web アプリケーションのトレースパラメータを指定できます。このファイルは常にアクセスできるわけではないため、影響を受ける Web アプリケーションを Web アプリケーションサーバからアンデプロイする必要があります。

1. WDeploy を使用して、Web アプリケーションサーバから Web アプリケーションをアンデプロイします。Wdeploy を使用して Web アプリケーションをアンデプロイする際の詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。
   - BI プラットフォームのインストールで提供された Tomcat Web アプリケーションサーバを使用する場合は、Web アプリケーションをアンデプロイする必要はありません。直接ファイルを変更できます。
     - `BOE.war` ファイルのトレース設定ファイルは、`<INSTALLDIR>¥Tomcat¥webapps¥BOE¥WEB-INF¥TraceLog` にあります。
     - `dswsbobje.war` ファイルのトレース設定ファイルは、`<INSTALLDIR>¥Tomcat¥webapps¥dswsbobje¥WEB-INF¥conf` にあります。

> ⓘ 注記
>
> バンドルされた Tomcat Web アプリケーションサーバを使用する場合はステップ 2 をスキップします。

2. `BO_trace.ini` ファイルの事前デプロイ済みバージョンにアクセスします。
   - `BOE.war` ファイルの設定ファイルの事前デプロイ済みバージョンのデフォルトの場所は `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥TraceLog` です。
   - `dswsbobje.war` ファイルの設定ファイルの事前デプロイ済みバージョンのデフォルトの場所は `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥conf` です。
3. `BO_trace.ini` ファイルを開きます。

- Windows の場合、デフォルトの場所は `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥conf¥` です。
- Unix の場合、デフォルトの場所は `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/` です。

4. サーバトレースパラメータを変更します。サーバトレースの設定には次のパラメータを使用します。

パラメータ	入力される値	説明
sap_log_level	**log_information** **log_warning** **log_error** **log_fatal** **log_none**	ログメッセージの重大度を決定します。デフォルトのログの重大度は **log_error** です。 ログの重大度は、最上位を **log_information**、最下位を **log_none** とする階層になっています。 ログの重大度をあるレベルに設定すると、そのレベル以下のすべてのメッセージが表示されます。たとえば、ログの重大度を **log_warning** に設定すると、**log_warning**、**log_error**、および **log_fatal** を含むメッセージがログファイルに書き込まれます。 **注記** **log_information** および **log_warning** は **log_info** および **log_warn** に短縮できます。
sap_trace_level	**trace_debug** **trace_path** **trace_information** **trace_error** **trace_none**	トレースメッセージの重大度を決定します。デフォルトのトレースの重大度は **trace_error** です。 トレースの重大度は、最上位を **trace_debug**、最下位を **trace_none** とする階層になっています。 トレースの重大度をあるレベルに設定すると、そのレベル以下のすべてのメッセージが表示されます。たとえば、トレースの重大度を **trace_path** に設定すると、**trace_path**、**trace_info**、および **trace_error** を含むメッセージがログファイルに書き込まれます。 **注記** **trace_information** は **trace_info** に短縮できます。

5. BO_trace.ini ファイルを保存して閉じます。
6. WDeploy を使用して、Web アプリケーションサーバをホストしているマシン上に .war ファイルをデプロイします。

トレース設定の変更は、Web アプリケーションに次回ログオンしたときに有効になります。

29.4.2.1 特定の Web アプリケーションのトレースを設定する

BO_trace.ini ファイルは BOE および dswsbobje.war ファイルとともに Web アプリケーションサーバ上にデプロイされます。BO_trace.ini を使用して、BI プラットフォーム Web アプリケーションのトレースパラメータを指定できます。このファイルは常にアクセスできるわけではないため、影響を受ける Web アプリケーションを Web アプリケーションサーバからアンデプロイする必要があります。次に示すのが、Web アプリケーションとそれに関連する .war ファイルです。

Web アプリケーション	WAR ファイル	事前デプロイ済みの場所
セントラル管理コンソール	BOE.war	<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥TraceLog
BI ラウンチパッド	BOE.war	<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥TraceLog
OpenDocument	BOE.war	<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥TraceLog
Web サービス	dswsbobje.war	<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥conf

1. WDeploy を使用して、Web アプリケーションサーバから Web アプリケーションをアンデプロイします。Wdeploy を使用して Web アプリケーションをアンデプロイする際の詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム Web アプリケーションデプロイメントガイド*を参照してください。
   - BI プラットフォームのインストールで提供された Tomcat Web アプリケーションサーバを使用する場合は、Web アプリケーションをアンデプロイする必要はありません。直接ファイルを変更できます。
     - BOE.war ファイルのトレース設定ファイルは、<INSTALLDIR>¥Tomcat¥webapps¥BOE¥WEB-INF¥TraceLog にあります。
     - dswsbobje.war ファイルのトレース設定ファイルは、<INSTALLDIR>¥Tomcat¥webapps¥dswsbobje¥WEB-INF¥conf にあります。

> ⓘ 注記
>
> バンドルされた Tomcat Web アプリケーションサーバを使用する場合はステップ 2 をスキップします。

2. BO_trace.ini ファイルの事前デプロイ済みバージョンにアクセスします。
   - BOE.war ファイルの設定ファイルの事前デプロイ済みバージョンのデフォルトの場所は <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥BOE¥WEB-INF¥TraceLog です。
   - dswsbobje.war ファイルの設定ファイルの事前デプロイ済みバージョンのデフォルトの場所は <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps¥dswsbobje¥WEB-INF¥conf です。
3. BO_trace.ini ファイルを開きます。
   - Windows の場合、デフォルトの場所は <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥conf¥ です。
   - Unix の場合、デフォルトの場所は <INSTALLDIR>/sap_bobj/enterprise_xi40/conf/ です。
4. 特定の Web アプリケーションのトレース設定を指定するには if 文を使用します。例:

```
if (device_name == "Webapp_opendocument_trace") {
  sap_log_level=log_warning;
  sap_trace_level=trace_path;
}
```

特定の Web アプリケーションサーバにトレース設定を適用するには、プロセスを指定する必要があります。初期インストール後は、次の Web アプリケーションを利用できます。

Web アプリケーション	デバイス名
BI 起動パッド	**WebApp_BIlaunchpad**
Central Management Server	**WebApp_CMC**
OpenDocument	**WebApp_OpenDocument**

Web アプリケーションサーバのトレースの設定には次のパラメータを使用します。

パラメータ	入力される値	説明
sap_log_level	**log_information** **log_warning** **log_error** **log_fatal** **log_none**	ログメッセージの重大度を決定します。デフォルトのログの重大度は **log_error** です。 ログの重大度は、最上位を **log_information**、最下位を **log_none** とする階層になっています。 ログの重大度をあるレベルに設定すると、そのレベル以下のすべてのメッセージが表示されます。たとえば、ログの重大度を **log_warning** に設定すると、**log_warning**、**log_error**、および **log_fatal** を含むメッセージがログファイルに書き込まれます。

パラメータ	入力される値	説明
		注記 **log_information** および **log_warning** は **log_info** および **log_warn** に短縮できます。
sap_trace_level	**trace_debug trace_path trace_information trace_error trace_none**	トレースメッセージの重大度を決定します。デフォルトのトレースの重大度は **trace_error** です。 トレースの重大度は、最上位を **trace_debug**、最下位を **trace_none** とする階層になっています。 トレースの重大度をあるレベルに設定すると、そのレベル以下のすべてのメッセージが表示されます。たとえば、トレースの重大度を **trace_path** に設定すると、**trace_path**、**trace_info**、および **trace_error** を含むメッセージがログファイルに書き込まれます。 注記 **trace_information** は **trace_info** に短縮できます。

5. BO_trace.ini ファイルを保存して閉じます。
6. WDeploy を使用して、Web アプリケーションサーバをホストしているマシン上に .war ファイルをデプロイします。

29.5 BI プラットフォームクライアントアプリケーションのトレース設定

トレースは、次のクライアントに対して有効化できます。

- ユニバースデザインツール
- インフォメーションデザインツール
- Web Intelligence リッチクライアント

これらのコンポーネントに対してトレースを設定するには、各クライアントタイプの .ini ファイルを編集します。これらの .ini ファイルは、この章で説明している BO_trace.ini ファイルと同様に動作します。.ini ファイルの変更に関する詳細については、BO_trace.ini ファイルを使ってサーバトレースを設定する [1029 ページ]を参照してください。

.ini ファイルは、これらのアプリケーションに対して設定された作業ディレクトリ (デフォルトでは `<INSTALLDIR>¥SAP BusinessObjects`) に存在する必要があります。.ini ファイルがまだ存在していない場合は、新たに作成する必要があります。ファイル名は次のとおりです。

- ユニバースデザインツール: `designer_trace.ini`
- インフォメーションデザインツール: `BO_Trace.ini`
- Web Intelligence リッチクライアント: `WebIRichClient_trace.ini`

詳細については、これらの製品のマニュアルを参照してください。

29.6 拡張エラーメッセージトレーシングの設定

SAP BusinessObjects Web Intelligence など一部のアプリケーションの場合は、トレーシングを有効にすることで、アプリケーションからスローされたエラーメッセージの詳細情報を含むログファイルを生成することができます。

> **注記**
>
> これらのログファイルは SAP Support エンジニアリングで使用されるように設計されています。このログファイルの形式は JSON です。

SAP BusinessObjects BI インストールでエラーメッセージ詳細情報ログファイルを有効にします。それには、ファイル `extended_info.properties` を変更します。

29.7 エラーメッセージ詳細情報ログファイルを有効にする

アプリケーションがスローしたエラーメッセージの詳細情報を取得します。それには、エラーメッセージ詳細情報ログファイルを有効にする必要があります。

> **注記**
>
> SAP BusinessObjects BI Suite バージョン 4.2 SP5 では、SAP BusinessObjects Web Intelligence に対してのみこの機能がサポートされます。

1. SAP BusinessObjects BI インストールでファイル `extended_info.properties` を開きます。

   デフォルトロケーションは次のとおりです。

   - Windows の場合: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥conf¥`
   - UNIX の場合: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`
2. パラメータを適切に設定します。

パラメータ	指定できる値	説明
`output.format`	• Json • none	生成されたファイルの形式を制御します。 **注記** この形式を none に設定すると、ファイルは生成されません。
`output.size`	`<size><unit>` (`<size>` は正の整数、`<unit>` はギガバイトの 'g' またはメガバイトの 'm' になります。) **注記** unit のデフォルト値はキロバイトです。	アプリケーションが生成できるすべてのファイルの合計サイズです。このサイズを超過すると、古いファイルから削除されます。

ログファイルはトレースファイルと同じフォルダに生成されます。デフォルトロケーションは次のとおりです。

- Windows の場合: `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥logging¥`
- UNIX の場合: `<INSTALLDIR>/sap_bobj/logging/`

ファイル名 `<application_name>_<error_id>_exinfo.<format>`

アプリケーション名はエラーをスローしたアプリケーションの名称です。エラー ID はランダムに生成されます。このファイル形式は設定ファイルに指定された形式です。

> **注記**
>
> 適用可能な唯一のファイル拡張子は `.json` です。

特定のアプリケーションがスローしたメッセージごとに個別のログファイルが生成されます。

30 SAP Solution Manager への統合

30.1 統合の概要

SAP Solution Manager への統合を有効にするサポート促進機能が BI プラットフォームに追加されました。次の SAP Solution Manager™ コンポーネントを使用して、BI プラットフォームデプロイメントをサポートすることができます。

- ソリューションランドスケープディレクトリ
- Solution Manager Diagnostics
- CA Wily Introscope
- SAP パスポート

> **注記**
>
> SAP BusinessObjects の SAP サポートポータルにアクセスするには、次を表示してください。 https://support.sap.com/home.html

30.2 SAP Solution Manager の統合のチェックリスト

次の表に、SAP Solution Manager で BI プラットフォームをサポートできるようにするために必要なコンポーネントを示します。

SAP Solution Manager のサポート	BI プラットフォームで必須
SLD 登録	• BI プラットフォームサーバを登録できるようにするには SAPHOSTAGENT をインストールする必要があります。 **注記** SAPHOSTAGENT がすでにインストールされている場合は、BI プラットフォームインストーラにより自動的にサーバが登録されます。 • バックエンドサーバについてレポートするデータサプライヤ用の connect.key ファイルを作成する必要があります。 • (オプション) SLD 登録に WebSphere 6.1 または 7 を使用する場合は、WebSphere の各 Web アプリケーションサーバに SLDREG 登録ツールをインストールする必要があります。詳細については、SAP ノート 1482727 を参照してください。 • (オプション) SLD 登録に SAP NetWeaver 7.2 を使用する場合は、すべての NetWeaver ホストに SLDREG をインストールする必要があります。詳細については、SAP ノート 1018839 を参照してください。 • (オプション) SLD 登録に Apache Tomcat を使用する場合は、各 Tomcat サーバに SLDREG をインストールする必要があります。詳細については、SAP ノート 1508421 を参照してください。
SMD 統合	• SMD エージェント (DIAGNOSTICS.AGENT) をダウンロードして BI プラットフォームサーバのすべてのホストにインストールする必要があります。 • BI プラットフォームの SMAdmin ユーザアカウントが有効になっている必要があります。
パフォーマンス計測	• Introscope エージェントが Enterprise Manager に接続できるように設定する必要があります。BI プラットフォームインストーラまたは CMC のノードプレースホルダを使用して、接続を設定します。 • SMD エージェントをインストールする必要があります。 • BI プラットフォームが SMD エージェントに接続できるように設定する必要があります。BI プラットフォームインストーラまたは CMC のノードプレースホルダを使用して、接続を設定します。
SAP パスポート	• SAP パスポートクライアントツールをダウンロードしてインストールする必要があります。

30.3 システムランドスケープディレクトリ登録の管理

30.3.1 システムランドスケープでの BI プラットフォームの登録

システムランドスケープディレクトリ (SLD) は、ソフトウェアライフサイクルの管理に関連するシステムランドスケープ情報のセントラルリポジトリです。SLD には、システムランドスケープ (現在インストールされているシステムコンポーネントおよびソフトウェアコンポーネント) の説明が含まれます。SLD データサプライヤは SLD サーバにシステムを登録し、情報を最新の状態に維持します。管理アプリケーションおよび業務アプリケーションが、SLD に格納されている情報にアクセスし、協調的なコンピューティング環境でタスクを実行します。

システムランドスケープディレクトリデータサプライヤ (SLD-DS) は、BI プラットフォームサーバを SLD サーバに登録する役割を担うアプリケーションです。プラットフォームのインストール先のそれぞれに固有のデータサプライヤが 1 つ準備され、次のコンポーネントについてレポートします。

- BI プラットフォームサーバ
- WebSphere Web アプリケーションサーバにホストされている Web アプリケーションおよび Web サービス

> ⓘ 注記
>
> SAP NetWeaver には、NetWeaver アプリケーションサーバやホストされている Web アプリケーションと Web サービスを登録する SLD-DS サプライヤが組み込まれています。この SLD-DS は、SAP NetWeaver 環境に統合されている BI プラットフォームデプロイメントに関連しています。

BI プラットフォームサーバについてレポートする SLD-DS には、SLDREG プログラムをインストールして設定しておく必要があります。SLDREG プログラムは、SAPHOSTAGENT ツールのインストール時にインストールされます。SAPHOSTAGENT のアクセスおよびインストール方法についての詳細は、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドの準備に関する節を参照してください。SLDREG のインストールが済んだら、`connect.key` ファイルを作成し、SLD サーバに接続できるようにする必要があります。

WebSphere 用の固有のデータサプライヤの設定方法については、*Web* アプリケーションデプロイメントガイドを参照してください。

BI プラットフォームのインストール中に、BI プラットフォームの登録に必要な情報が設定ファイルに格納されます。このファイルには、SLD-DS が BI プラットフォームデータベースに接続するときに使用する情報が含まれます。

30.3.1.1 SLD データサプライヤの connect.key ファイルを作成する

SLD データサプライヤの `connect.key` ファイルを作成する前に、SAPHOSTAGENT をダウンロードしてインストールする必要があります。詳細は、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドの準備に関する章を参照してください。

> ⓘ 注記
>
> `connect.key` ファイルは、BI プラットフォームサーバについてレポートするデータサプライヤを使用して SLD 登録をする際に必要です。

1. コマンドラインコンソールを開きます。
2. デフォルトの SAPHOSTAGENT インストールパスに移動します。
   - Windows の場合: `Program Files¥SAP¥hostctrl¥exe`
   - Unix の場合: `/usr/sap/hostctrl/exe`
3. 次のコマンドを実行します。

   ```
   sldreg -configure connect.key
   ```
4. 次に示す設定の詳細を入力します。
   - ユーザ名
   - パスワード

- ホスト
- ポート番号
- HTTP の使用を指定

`sldreg` ツールは、SLD サーバに情報をプッシュするときにデータサプライヤで自動的に使用される connect.key ファイルを作成します。

30.3.2 SLD 登録がトリガーされるタイミング

SLD 登録処理は、BI プラットフォームバックエンドサーバについてレポートするデータサプライヤにより次のシナリオで起動されます。

- BI プラットフォームデプロイメント上のサーバノードが再起動される
- 新しいサーバまたはノードがデプロイメントに追加される
- サーバまたはノードが削除される

> **注記**
>
> サーバまたはノードが削除されても、SLD 登録処理では SLD サーバの内容が変更されません。サーバまたはノードを削除するときに SLD サーバを更新するには、SLD からシステムを削除し、BI プラットフォームを再起動して SLD を再送信します。

WebSphere の SLD 登録に使用されるデータサプライヤは、手動で起動したり、指定した間隔 (例: 24 時間ごと) で実行されるように設定することができます。このデータサプライヤの設定についての詳細は、SAP ノート 482727 を参照してください。

30.3.3 パッチインストール前の SLD クリーンアップ

パッチインストール後に以前のバージョンの BI プラットフォームからのデータが SLD サーバに蓄積されるため、SAP Solution Manager を使用した製品の診断が困難になります。この問題を回避するため、パッチインストールを開始する前に、ベースマシンで以下の手順を実行してください。

> **注記**
>
> この機能は、バージョン 4.2 SP3 以上で使用することができます。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib¥bobj-sld-ds` に移動します。
2. クリーンパラメータ (`-clean`) でバッチファイル bobjsldds.bat を実行します。

   > **注記**
   >
   > クリーンアップのために SLD サーバにプッシュされる、事前定義済みのパラメータを含む xml ファイルが作成されます。クリーンアップは、SIA の再起動後にリフレッシュされます。

30.3.4 SLD 接続のログ作成

データサプライヤ設定ファイル

SLD 登録に使用される設定ファイルは、BI プラットフォームデプロイメントに作成されます。ファイル (`sldparserconfig.properties`) は、`<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/` ディレクトリにあります。

SLD 接続のログ作成

SLD サーバと BI プラットフォームデプロイメント上のデータサプライヤとの間の接続は、`sldreg` ツールと `connect.key` ファイルを使用して制御されます。

> **注記**
>
> ログファイルの名前は `sldparserconfig.properties` ファイルでプロパティとして指定されます。

BI プラットフォームバックエンドサーバについてレポートする SLD データサプライヤのログファイルは、デフォルトでは `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log` にあります。このファイルは、データサプライヤが実行されるたびに上書きされます。

`sldreg` のログファイルは、デフォルトでは `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log` にあります。sldreg のログファイル名は変更できず、`sldreg_<Timestamp>.log` という形式が使用されます。

sldreg がデータサプライヤから呼び出されるたびに新しいログファイルが作成されます。

30.3.5 仮想ホスト名

Server Intelligence Agent が再起動されると、各ノードに対してデータサプライヤファイルが生成されます。このファイルはシステムランドスケープディレクトリに保存され、後から SAP Solution Manager によって使用されます。Business Intelligence プラットフォーム 4.2 サポートパッケージ 4 およびそれ以前では、データサプライヤファイルに物理ホスト名が付加されていました。Business Intelligence プラットフォーム 4.2 サポートパッケージ 5 では、*sldparserconfig.properties* ファイルで仮想ホスト名を定義して、データサプライヤファイルで仮想ホスト名が使用されるようにすることができます。

> **注記**
>
> デフォルトでは、データサプライヤファイルは、sldparserconfig.properties ファイルに仮想ホスト名が含まれていない場合に物理ホスト名を取得します。

sldparserconfig.properties に仮想ホスト名を追加するには、以下の手順に従います。

1. `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib¥bobj-sld-ds` に移動します。
2. sldparserconfig.properties ファイルを編集します。

3. パラメータ `virtualHostName = <Virtual Hostname>` を追加します。
4. ファイルを保存します。
5. *Server Intelligence Agent* を再起動して、変更内容がデータサプライヤファイルで使用されるようにします。

> **注記**
>
> 変更内容は、以下のコマンドの実行によっても使用されます。
>
> Windows の場合: `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/` にある `runbobjsldds.bat -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>`
>
> UNIX の場合: `<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bobj-sld-ds` にある `runbobjsldds.sh -config sldparserconfig.properties -name <Node Name> -clusterlist <Cluster Name with Port Number>`

30.4 ソリューション管理診断エージェントの管理

30.4.1 Solution Manager Diagnostics (SMD) の概要

SAP Solution Manager の Solution Manager Diagnostics (SMD) コンポーネントには、システムランドスケープ全体を一元的に分析および監視するためのあらゆる機能が用意されています。SMD エージェントがインストールされていると、SMD サーバを使用して BI プラットフォームを監視することができます。SMD エージェント (`DIAGNOSTICS.AGENT`) により SMD に収集された情報は、根本原因の分析に使用できます。収集されて SMD サーバに送信された情報には、バックエンドサーバの設定情報とサーバのログファイルの位置情報が含まれます。

30.4.2 SMD エージェントの操作

BI プラットフォームは、SMD エージェントをインストールしません。エージェント `DIAGNOSTICS.AGENT` を https://support.sap.com/swdc からダウンロードできます。

このエージェントのインストールおよび設定についての情報は、以下の場所に掲載されています。http://service.sap.com/diagnostics

SMD エージェントの操作のガイドライン

BI プラットフォームの監視に SMD エージェントを使用する際のガイドラインは次のとおりです。

- 監視対象システムとエージェントのインストール順序は重要ではありません。SMD エージェントをインストールするタイミングは、BI プラットフォームのインストールおよびデプロイの前でも後でも構いません。
- SMD エージェントのインストール時に、ホスト名とリスニングポートを記録します。これらは、BI プラットフォームを監視対象システムとして設定するのに不可欠な情報です。監視対象システムより先にエージェントをインストールした場合は、BI プラットフォームのインストール設定時に設定情報を提供することができ

ます。この情報は、デプロイメント内のセントラル管理コンソールでノードのプレースホルダを使用して後から提供することもできます。

- 分散システムにバックエンドサーバがデプロイされている場合は、バックエンドサーバをホストしているすべてのマシンに SMD エージェントをインストールする必要があります。
- Java 以外のサーバのパフォーマンス計測には SMD エージェントが必要です。
- SMD サーバから CMS にアクセスできるようにするには、SMAdmin ユーザアカウントをアクティブにする必要があります。

30.4.3 SMAdmin ユーザアカウント

各 BI プラットフォームデプロイメントには、SMD の統合を円滑にするために作成されたユーザアカウントがあります。この読み取り専用アカウントは、CMS にログインしてサーバの設定やデプロイメントに関するその他の情報を収集する際に SMD サーバで使用されます。

SMAdmin はデフォルトではアクティブになっていません。

30.4.3.1 SMAdmin をアクティブにする

1. CMC の [ユーザとグループ] 管理エリアで、[ユーザー覧] を選択します。
   ユーザの一覧が表示されます。
2. [*SMAdmin*] ユーザアカウントを選択します。
3. 管理 > プロパティ をクリックします。
   [プロパティ]ダイアログボックスが表示されます。
4. [アカウントを無効にする] ボックスをオフにします。
5. [保存して閉じる]をクリックします。

30.5 パフォーマンス計測の管理

30.5.1 BI プラットフォームのパフォーマンス計測

BI プラットフォームパフォーマンス計測の測定用に、SAP Solution Manager の一部として CA Wily Introscope を使用できます。プラットフォームのインストール時に、次のリソースがデプロイメントに準備されます。

- Introscope エージェント: BI プラットフォーム Java バックエンドサーバから、パフォーマンスメトリクスを収集します。エージェントは、周辺のコンピューティング環境からも情報を収集します。その後、Enterprise Manager にこれらのメトリクスをレポートします。
- 計測処理を円滑にするファイル: Java 以外のサーバの計測用に 1 つのファイルセットが準備され、Java サーバ用にもう 1 つのセットが準備されます。 SAP Solution Manager 側には、Enterprise Manager (EM) コンポーネントが必要です。EM は、アプリケーション環境で収集されたすべての Introscope パフォーマンスデータおよびメトリクスのセントラルリポジトリとして動作します。EM はパフォーマンスデータを処理して、ユーザが実稼働環境の監視および診断に使用できるようにします。

30.5.2 BI プラットフォームのパフォーマンス計測の設定

BI プラットフォームバックエンドサーバ上で実行中のワークフローのパフォーマンス計測を設定する方法は 2 つあります。

1. BI プラットフォームのインストール設定時。SMD エージェントのホスト名とリスニングポートを知る必要があります。詳細については、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドを参照してください。このオプションを選択すると、監視対象システムのデプロイが終了したときにデフォルトで計測が実行されます。
2. BI プラットフォームをインストールした後に、セントラル管理コンソール (CMC) のノードプロパティのプレースホルダを使用して、SMD エージェントに設定情報を提供できます。

> **注記**
>
> Java 以外のサーバのワークフローを計測する場合は、SMD エージェント (`DIAGNOSTICS.AGENT`) をインストールしておく必要があります。

関連情報

SMD エージェントの操作 [1044 ページ]

30.5.2.1 計測できるようにノードを設定する

BI プラットフォームのインストール設定時に SMD エージェントおよび Enterprise Manager に設定情報を提供しなかった場合は、次の手順を実行します。

1. CMC の [サーバ] エリアを表示します。
2. ナビゲーションペインで [ノード] をクリックします。
   使用可能なすべてのノードが表示されます。
3. 計測を実行するノードを右クリックして [プレースホルダ] を選択します。
   [プレースホルダ] ダイアログボックスが表示されます。
4. 次のプレースホルダの値を変更します。

プレースホルダ	説明
%IntroscopeAgentEnableInstrumentation%	Java サーバの計測を有効または無効にします。インストール設定時に Enterprise Manager の設定詳細を提供した場合は、"有効" に設定されます。計測を有効にするには TRUE に設定します。
%IntroscopeAgentEnterpriseManagerHost%	Enterprise Manager がインストールされているマシンのホスト名。
%IntroscopeAgentEnterpriseManagerPort%	Enterprise Manager が使用するリスニングポート。

プレースホルダ	説明
%IntroscopeAgentEnterpriseManagerTransport%	Enterprise Manager が使用する通信プロトコル。サポート対象のプロトコルには、TCP、SSL、HTTP トンネル、および HTTPS が含まれます。
%NCSInstrumentLevelThreshold%	Java 以外のサーバの計測レベルを設定するのに使用します。計測をオフにする場合は、“0” に設定します。“0” より大きい値に設定すると、計測がアクティブになります。
%SMDAgentHost%	SMD エージェント (`DIAGNOSTICS.AGENT`) がインストールされているマシンのホスト名。
%SMDAgentPort%	SMD エージェントで使用されるリスニングポート。

5. [保存して閉じる]をクリックします。
6. ノードを再起動します。

ノードを再起動すると、指定された新しい値がすべてのマネージドサーバに反映されます。

30.5.3 Web Tier のパフォーマンス計測

Web Tier のコンポーネントの計測データは BI プラットフォームには含まれません。

30.5.4 計測ログファイル

BI プラットフォームのデプロイメントで計測が実行されるように設定すると、特定の場所にメッセージが記録されます。ログファイルを確認することは、計測ステータスを検証する 1 つの方法です。

Java バックエンドサーバの計測の場合、ログファイルは `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs` ディレクトリにあります。各 java プロセスにつき独立した 1 つの `.log` ファイルが作成されます。このフォルダには、計測のためにロードされたメソッドを特定する `AutoProbe.log` ファイルも含まれます。

Java 以外のバックエンドサーバの計測の場合、ログファイルは `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/logging/` ディレクトリにあります。Unix の場合、ファイルは `<sap_bobj>¥logging¥` ディレクトリにあります。Java 以外のサーバの計測に関連するログファイルは、`.trc` ファイルとして保存されます。

Web アプリケーションサーバの計測の場合、ログファイルは `<INSTALLDIR>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs` ディレクトリにあります。このフォルダには、`Introscope.log` と `Autoprobe.log` の 2 種類のログファイルが表示されます。

30.6 SAP パスポートを使用したトレース

トレースメカニズムは、サーバや Web アプリケーションなどの BI プラットフォームコンポーネントのトレースのほかに、特定のアクションのトレースをサポートできます。エンドツーエンドトレース分析により、単一トラン

ザクションのパフォーマンスが分析されます。特定のアクションのすべてのトレース情報を連結することにより、SAP サポート担当者は他のアクションに関連する情報のトレースの妨害を受けることなく、すべてのトレースデータを確認することができます。

詳細については、1861180 にアクセスしてください。

SAP パスポート

BI プラットフォームのエンドツーエンドトレースをサポートしているメカニズムは、SAP パスポート™というツールです。SAP パスポートクライアントツールにより、一意の ID が特定のワークフローのすべての HTTP 要求に投入され、この ID はワークフローで使用するすべてのサーバに転送されます。SAP サポート担当者は、この一意 ID を使用してワークフローのエンドツーエンドトレースをまとめることができます。

> **注記**
>
> CMC および `BO_trace.ini` 設定ファイルで指定したトレースログレベルのほうが、SAP パスポートクライアントツール (`SAPClientPlugin.exe`) で指定したレベルより高い場合は、前者のトレースレベルが使用されます。

パスポートは、バックエンドサーバのログ、Web アプリケーション、および Web サービスのログで見つけることができます。

SAP パスポートクライアントツールは、BI プラットフォームの一部としてインストールされていません。このツールにアクセスしてダウンロードするには、https://support.sap.com/swdc を表示してください。

31　コマンドライン管理

31.1　Unix スクリプト

この節では、BI プラットフォームの Unix ディストリビューションに付属する各管理ツールとスクリプトについて説明します。これは、主に参照用として提供されるものです。概念と設定手順については、このガイド全体でさらに詳しく説明します。

> ⓘ 注記
>
> BI プラットフォームをインストールしたユーザのみが、BI プラットフォームでシェルスクリプトを実行する権限を持ちます。

BI プラットフォームの Unix ディストリビューションに付属している多くのスクリプトによって、セントラル設定マネージャ (CCM) の Windows 版で使用できるすべての設定オプションが提供されます。その他にも数多くのスクリプトがあり、Unix 特有のオプションとして、あるいはユーザ独自のスクリプトに使用するテンプレートとして機能します。また、BI プラットフォームで使用する二次的スクリプトもいくつか用意されています。この節では、各スクリプトについて説明し、適用されるコマンドラインオプションも紹介します。

> ⓘ 注記
>
> Unix コマンドラインのパラメータを指定するときは、特定のシェル文字を単独でエスケープまたは複数文字エスケープする必要があります。たとえば、パスワードで感嘆符 “!” を使用している場合は、感嘆符を次のようにエスケープする必要があります。`./ccm.sh -display -username Administrator -password Abc¥!defgh123 -cms cmsname`

31.1.1 スクリプトユーティリティ

この節では、UNIX 上の BI プラットフォームで作業する際に役立つ管理スクリプトについて説明します。 この節では、これらのスクリプトを使って実行できる各タスクの概念が適切な箇所で説明されています。 この参照用セクションでは、主要なコマンドラインオプションとそれらの引数を紹介します。

31.1.1.1 ccm.sh[ccm.sh]

`ccm.sh` スクリプトは、インストール先の `<INSTALLDIR>/sap_bobj` ディレクトリにインストールされます。このスクリプトによって、セントラル設定マネージャのコマンドラインバージョンが使用できます。 この節では、コマンドラインオプションの一覧を紹介し、いくつかの例を示します。

> ⓘ 注記
>
> 角かっこ([])で囲まれた引数はオプションです。

> ⓘ 注記
>
> Server Intelligence Agent の名称が不確かな場合は、`ccm.config` ファイル内のコマンドプロパティを検索し、`-name` オプションの後ろに表示される値を使用します。

> ⓘ 注記
>
> `ccm.sh` スクリプトは、BI プラットフォームのインストールを実行したユーザのみが起動できます。

- [**<その他の認証情報>**] と記されている引数は 2 番目の表に説明があります。

CCM オプション	有効な引数	説明
`-help`	該当せず	コマンドラインヘルプを表示します。
`-start`	`all` または **<sianame>**	各 Server Intelligence Agent をプロセスとして起動します。 `all` オプションにより、異なるクラスタに属するノードを含め、マシン上のすべてのノードが起動します。
`-stop`	`all` または **<sianame>**	プロセス ID を終了して各 Server Intelligence Agent を停止します。`all` オプションにより、異なるクラスタに属するノードを含め、マシン上のすべてのノードが起動します。
`-restart`	`all` または **<sianame>**	プロセス ID を終了して各 Server Intelligence Agent を停止した後、各 Server Intelligence Agent を起動します。 `all` オプションにより、異なるクラスタに属するノードを含め、マシン上のすべてのノードが起動します。
`-managedstart`	**<fully qualified server name><[other authentication information]>**	サーバを起動します。
`-managedstop`	**<fully qualified server name><[other authentication information]>**	サーバを停止します。
`-managedrestart`	**<fully qualified server name><[other authentication information]>**	サーバを停止してから、起動します。

CCM オプション	有効な引数	説明
-managedforceterminate	**<fully qualified server name><[other authentication information]>**	現在の処理要求を実行せずにサーバを直ちに停止します。
-enable	**<fully qualified server name><[other authentication information]>**	起動したサーバを有効にして、サーバをシステムに登録し、適切なポートで受信待機を開始します。 サーバ名は完全な形式で指定します。
-disable	**<fully qualified server name><[other authentication information]>**	サーバを無効にして、プロセスとして起動した状態のまま、BI プラットフォームのリクエストに対する応答を停止します。 サーバ名は完全な形式で指定します。
-display	**< [other authentication information]>**	サーバ名、ホスト名、プロセス ID、説明、実行中かどうか、有効か無効かなど、クラスタ内のすべてのサーバの現在のステータスがレポートされます。

次の表に、**<[other authentication information]>** と記された引数を構成するオプションを示します。

> ⓘ 注記
>
> セキュリティを強化するために、常に Enterprise 認証を使用してアカウントの認証情報を提供する必要があります。 他の種類の認証はサポートされていません。

認証オプション	有効な引数	説明
-cms	**<cmsname:port#>**	ログオンする CMS を指定します。 指定しない場合、CCM のデフォルト設定はローカルマシンとデフォルトポート(6400)になります。
-username	**<username>**	BI プラットフォームに対する管理者権限を付与するアカウントを指定します。 指定しない場合、デフォルトの Administrator アカウントが使用されます。

認証オプション	有効な引数	説明
-password	**<password>**	適切なパスワードを指定します。 指定しない場合、空のパスワードが使用されます。 **注記** メモ: -password 引数を指定する場合は、必ず、-username 引数も指定する必要があります。

CCM は ccm.config ファイルから起動文字列とその他の設定値を読み取ります。

関連情報

ccm.config [1053 ページ]

31.1.1.1.1 例

以下の 2 つのコマンドは、すべての BI プラットフォームサーバを起動および有効化します。Central Management Server (CMS) はローカルマシンとデフォルトポート (6400) で起動します。

```
ccm.sh -start all
ccm.sh -enable all
```

以下の 2 つのコマンドは、すべての BI プラットフォームサーバを起動および有効化します。CCM はクラスタ内のすべてのサーバを有効化します。CMS は MACHINE01 とポート 6701 で起動します。

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

以下の 2 つのコマンドは、SysAdmin という指定された管理アカウントと入力されたパスワードで、すべての BI プラットフォームサーバを起動および有効化します。

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

以下のコマンドは、指定された管理アカウントでログオンし、2 番目のマシンで実行中の Adaptive Job Server を無効にします。

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

31.1.1.1.2 ccm.config

この設定ファイルは、コマンド実行時に CCM が使用する起動文字列とその他の値を設定します。このファイルは、CCM とその他の BI プラットフォームスクリプトユーティリティで管理されます。通常は、Server Intelligence Agent のコマンドラインを変更する必要がある場合にのみ、このファイルを編集します。手動で編集する前に、このファイルをバックアップすることを強くお勧めします。

関連情報

コマンドラインの概要 [1059 ページ]

31.1.1.2 cmsdbsetup.sh

`cmsdbsetup.sh` スクリプトは、インストール先の `<sap_bobj>` ディレクトリにインストールされます。 このスクリプトは、以下のタスクを実行できるテキストベースのプログラムを提供します。

- CMS システムデータベースの設定
- CMS システムデータベースの再初期化
- 別のデータソースからのデータのコピー
- クラスタキーの変更
- クラスタ名の変更

> **注記**
>
> このスクリプトを実行する前に、現在の CMS システムデータベースと入力ファイルおよび出力ファイルリポジトリのコンテンツをバックアップします。 詳細については、「"システムのバックアップと復元"」を参照してください。 SAP BI プラットフォーム

スクリプトは Server Intelligence Agent(SIA)名の入力を要求します SIA の名前を確認するには、`ccm.config` ファイルで SIA の "コマンド" プロパティを表示します。 SIA の現在の名称は、`-name` オプションの後に表示されます。 または、オプション 8 を `serverconfig.sh` ファイルとともに使用することもできます。

関連情報

Central Management Server のクラスタ化 [414 ページ]
バックアップと復元の概要 [530 ページ]

31.1.1.3 serverconfig.sh

`serverconfig.sh` スクリプトは、インストール先の `<sap_bobj>` ディレクトリにインストールされます。このスクリプトは、以下の作業を実行できるテキストベースのプログラムを提供します。

- ノードの追加
- ノードの削除
- ノードの修正
- ノードの移動
- サーバ設定のバックアップ
- サーバ設定の復元
- Web Tier 設定の修正
- 全ノードの一覧表示

31.1.1.3.1 UNIX 上のノードを追加、削除、修正、一覧表示する

1. インストールしたシステムの `<INSTALLDIR>/sap_bobj` ディレクトリに移動します。
2. 次のコマンドを発行します。

   ```
   ./serverconfig.sh
   ```

   このスクリプトにより、オプションの一覧が表示されます。

   1. ノードの追加
   2. ノードの削除
   3. ノードの修正
   4. ノードの移動
   5. サーバ設定のバックアップ
   6. サーバ設定の復元
   7. Web Tier 設定の修正
   8. 全ノードの一覧表示
3. 実行する操作に対応する数値を入力します。
4. サーバを追加、削除、修正する場合は、スクリプトが要求する情報を入力します。

31.1.2 スクリプトテンプレート

31.1.2.1 startservers

`startservers` スクリプトは、インストール先の `<INSTALLDIR>/sap_bobj` ディレクトリにインストールされます。このスクリプトは、CCM コマンドを実行して BI プラットフォームサーバを起動するユーザ独自のスクリプトの設定方法を示す例として提供されていますので、独自のスクリプト用のテンプレートとしてご使用いただけます。使用しているサーバの CCM コマンドの記述についての詳細は、ccm.sh[ccm.sh] [1049 ページ]を参照してください。

31.1.2.2 stopservers

stopservers スクリプトは、インストール先の <INSTALLDIR>/sap_bobj ディレクトリにインストールされます。このスクリプトは、CCM コマンドを実行して BI プラットフォームサーバを停止するユーザスクリプトの設定方法を示す例として提供されていますので、独自のスクリプト用のテンプレートとしてご使用いただけます。使用しているサーバの CCM コマンドの記述についての詳細は、ccm.sh[ccm.sh] [1049 ページ]を参照してください。

31.1.3 BI プラットフォームによって使用されるスクリプト

以下の二次的なスクリプトは、主要な BI プラットフォームスクリプトユーティリティの実行時にバックグラウンドで実行される場合がありますが、ユーザが実行する必要はありません。

bobjrestart.sh

このスクリプトは、CCM が Server Intelligence Agent ノードを管理する際に内部的に実行されます。このスクリプトは各自で実行しないでください。

env.sh

env.sh スクリプトは、インストール先の <sap_bobj/setup> ディレクトリにインストールされます。このスクリプトで、ほかの一部のスクリプトで必要な BI プラットフォーム環境変数が設定されます。BI プラットフォームスクリプトは、必要に応じて env.sh を実行します。詳細については、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドを参照してください。

env-locale.sh

env-locale.sh スクリプトは、スクリプトの言語文字列を各種エンコード方式 (例: UTF8、EUC、Shift-JIS など) 間で変換するために使用されます。このスクリプトは、必要に応じて env.sh によって実行されます。

initlaunch.sh

initlaunch.sh スクリプトは env.sh を実行して BI プラットフォーム環境変数を設定してから、スクリプトのコマンドライン引数として追加したすべてのコマンドを実行します。このスクリプトは、主に SAP BusinessObjects のデバッグ用ツールとして開発されたものです。

postinstall.sh

postinstall.sh スクリプトは、インストール先の <SCRIPTDIR> ディレクトリにインストールされます。このスクリプトをユーザ自身が実行する必要はありません。

setup.sh

setup.sh スクリプトは、インストールしたルートディレクトリにインストールされます。このスクリプトは、BI プラットフォームインストールをセットアップする、テキストベースのプログラムを提供します。このスクリプトは、BI プラットフォームをインストールすると自動的に実行されます。このスクリプトにより、初回の BI プラットフォームのセットアップに必要な情報の入力を求めるプロンプトが表示されます。

BI プラットフォームインストール時のセットアップスクリプトに対する応答の詳細については、*SAP BusinessObjects Business Intelligence* プラットフォームインストールガイドを参照してください。

setupinit.sh

setupinit.sh スクリプトは、インストール先の <sap_bobj/init> ディレクトリにインストールされます。このスクリプトは、自動起動用の rc#ディレクトリに実行制御スクリプトをコピーします。インストール先のマシンで BI プラットフォームサーバを起動したり停止したりする場合は、setup.sh スクリプトが完了した後にこのスクリプトを実行します。

> **注記**
>
> このスクリプトを実行するには root 権限が必要です。

31.2 Windows スクリプト

この節では、BI プラットフォームの Windows ディストリビューションに付属する各管理ツールとスクリプトについて説明します。これは、主に参照用として提供されるものです。概念と設定手順については、このガイド全体でさらに詳しく説明します。

BI プラットフォームの Windows ディストリビューションには、セントラル設定マネージャ (CCM) の Windows バージョンが含まれています。GUI を使用して対話する方法のほかに、オプションを付けて CCM 実行可能ファイルをコマンドラインから実行して、サーバを管理する方法も選択できます。

31.2.1 ccm.exe

ccm.exe 実行可能ファイルは、インストール先の <INSTALLDIR>¥SAP BusinessObjects Business Intelligence platform 4.0¥win64_x64 ディレクトリにインストールされます。実行可能ファイルをコマ

ンドラインから直接実行して、特定の操作を実行することができます。この節では、コマンドラインオプションの一覧を紹介し、いくつかの例を示します。

> ⓘ 注記
>
> Server Intelligence Agent (SIA) および Central Management Server (CMS) が実行されていなければ、`ccm.exe` のコマンドラインオプションを使用して個別のサーバと対話することはできません。

> ⓘ 注記
>
> 角かっこ([])で囲まれた引数はオプションです。

> ⓘ 注記
>
> [**<その他の認証情報>**] と記されている引数は 2 番目の表に説明があります。

CCM オプション	有効な引数	説明
`-help`	該当せず	コマンドラインヘルプを表示します。
`-managedstart`	`all` または**<完全修飾サーバ名> <[その他の認証情報]>**	サーバを起動します。
`-managedstop`	`all` または**<完全修飾サーバ名> <[その他の認証情報]>**	サーバを停止します。
`-managedrestart`	`all` または**<完全修飾サーバ名> <[その他の認証情報]>**	サーバを停止してから、起動します。
`-managedforceterminate`	`all` または**<完全修飾サーバ名> <[その他の認証情報]>**	現在の処理要求を実行せずにサーバを直ちに停止します。
`-enable`	`all` または**<完全修飾サーバ名> <[その他の認証情報]>**	起動したサーバを有効にして、サーバをシステムに登録し、適切なポートで受信待機を開始します。
`-disable`	`all` または**<完全修飾サーバ名> <[その他の認証情報]>**	サーバを無効にして、プロセスとして起動した状態のまま、BI プラットフォームのリクエストに対する応答を停止します。
`-display`	**< [他の認証情報]>**	サーバ名、ホスト名、プロセス ID、説明、実行中かどうか、有効か無効かなど、クラスタ内のすべてのサーバの現在のステータスがレポートされます。

次の表に、**<[その他の認証情報]>**と記された引数を構成するオプションを示します。

> ⓘ 注記
>
> Enterprise 認証とともに、アカウントの認証を常に提供する必要があります。

認証オプション	有効な引数	説明
-cms	**<cmsname:port#>**	ログオンする CMS を指定します。指定しない場合、CCM のデフォルト設定はローカルマシンとデフォルトポート (6400)になります。
-username	**<username>**	BI プラットフォームに対する管理権限を付与するアカウントを指定します。指定しない場合、デフォルトの Administrator アカウントが使用されます。
-password	**<password>**	適切なパスワードを指定します。指定しない場合、空のパスワードが使用されます。 **注記** メモ: -password 引数を指定する場合は、必ず、-username 引数も指定する必要があります。
-authentication	**<認証の種類>**	認証の種類を指定します。**secEnterprise** のみがサポートされています。

CCM は ccm.config ファイルから起動文字列とその他の設定値を取得します。

31.2.1.1 例

次の例は、Server Intelligence Agent (SIA) と Central Management Server (CMS) が起動されて実行中であることを前提としています。ccm.exe のコマンドラインオプションを使用して個別のサーバと対話する前に、次の Windows コマンドを使用して SIA サービスを起動することができます。

```
net start "Server Intelligence Agent (NODENAME)"
```

SIA は、net stop "Server Intelligence Agent (NODENAME)" を使用して停止することもできます。

このコマンドはすべての BI プラットフォームサーバを起動します。

```
ccm.exe -managedstart all
```

このコマンドは Adaptive Job Server を起動します。CMS は、デフォルトポートではなくポート 6701 で起動します。

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

このコマンドは、SysAdmin という名前の指定された管理アカウントを使用して Adaptive Job Server を有効にします。

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

このコマンドは、指定された管理アカウントでログオンし、2 番目のマシンで実行中の Adaptive Job Server を無効にします。

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username
SysAdmin -password 35%bC5@5
```

31.3 サーバコマンドライン

31.3.1 コマンドラインの概要

この節では、各 BI プラットフォームサーバの動作を制御するコマンドラインオプションを紹介します。

セントラル管理コンソール (CMC) を経由してサーバの開始や設定を行う場合、サーバは、一般的なオプションと値を含むデフォルトのコマンドラインを使用して、開始または再起動されます。通常はデフォルトのコマンドラインを直接変更する必要はありません。また、CMC のさまざまなサーバ設定画面を使用して、最も一般的な設定を行うこともできます。この節では、参考までに各サーバで使用可能なすべてのコマンドラインオプションを説明します。BI プラットフォームの動作をさらにカスタマイズする必要がある場合には、各サーバのコマンドラインを直接変更することができます。

この節では、角かっこ([])で囲まれている値はオプションであることを示しています。

> **注記**
>
> 次の表は、サポートされているコマンドラインオプションを示しています。BI プラットフォームサーバでは、これらの表に記載されていない多数の内部オプションが使用されます。これらの内部オプションは変更しないでください。

31.3.1.1 サーバのコマンドラインを表示、変更する

1. セントラル管理コンソール (CMC) を使用してサーバを停止します。
2. サーバを右クリックし、[プロパティ] を選択します。
3. [プロパティ] 画面で、サーバのコマンドラインを変更し、[保存して閉じる] をクリックします。
4. サーバを開始します。

31.3.2 すべてのサーバに使用できる標準オプション

これらのコマンドラインオプションは、特に指定のない限り、すべての BI プラットフォームサーバに適用されます。 各サーバタイプに固有のオプションについては、この節で後述される説明を参照してください。

オプション	有効な引数	動作
-requestPort	<port >	サーバが受信待機するポートを指定します。 サーバはこのポートを CMS に登録します。 指定しない場合、サーバは 1024 以上の任意の空のポートを選択します。 **注記** このポートは、別のサーバにより別の目的で使用されます。 変更する前に、*BI プラットフォーム管理者ガイド*のデフォルトサーバポート番号の変更に関するセクションを参照してください。
-loggingPath	<absolute path>	ログファイルを作成するパスを指定します。

31.3.2.1 UNIX のシグナルハンドリング

UNIX では、BI プラットフォームのデーモンは以下のシグナルを処理します。

- SIGTERM を使用すると、サーバを正常に終了させることができます(終了コード = 0)。
- SIGSEGV、SIGBUS、SIGSYS、SIGFPE、および SIGILL を使用すると、サーバを高速に終了させることができます(終了コード = 1)。

31.3.3 Central Management Server

この節では、CMS に固有のコマンドラインオプションの一覧を記載しています。 Windows 上のサーバへのデフォルトパスは、<INSTALLDIR>¥BusinessObjects Enterprise XI 4.0¥win64_x64¥CMS.exe です。

UNIX 上のサーバへのデフォルトパスは、<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_cmsd です。

オプション	有効な引数	動作
-threads	**<NUMBER>**	CMS が初期化して使用するワーキングスレッドの数を指定します。 12 から 150 までの値を指定でき、デフォルトで 50 に設定されます。
-reinitializedb		CMS がシステムデータベースを削除し、デフォルトのシステムオブジェクトのみを使用してシステムデータベースを再作成するようにします。 再作成すると、データベース内に存在するすべてのデータが失われます。
-quit		-reinitializedb オプションを処理した後、強制的に CMS を終了します。
-receiverPool	**<number>**	クライアントリクエストを受信するために CMS が作成するスレッドの数を指定します。 クライアントは、別の SAP BusinessObjects サーバ、レポート公開ウィザード、Crystal Reports、または作成したカスタムクライアントアプリケーションになります。 デフォルト値は 5 です。通常、多くのクライアントを持つカスタムアプリケーションを作成するのでなければ、この値を増やす必要はありません。
-maxobjectsincache	**<number>**	CMS がメモリキャッシュに格納するオブジェクトの最大数を指定します。 オブジェクトの数を増やすと、必要となるデータベース呼び出しの数が減り、CMS パフォーマンスが大幅に向上します。 しかし、メモリ内にオブジェクトを多く配置しすぎると、クエリ処理のために CMS に割り当てるメモリが非常に少なくなります。 デフォルト値は 100000 です。
-ndbqthreads	**<number>**	データベースにリクエストを送信する CMS ワーカースレッドの数を指定します。 どのスレッドもデータベースに接続するため、データベース容量を超えないように注意する必要があります。 ほとんどの場合、指定すべき最大値は 20 です。

オプション	有効な引数	動作
-oobthreads	**<number>**	クラスタに 9 個以上の CMS クラスタメンバーが含まれている場合、各 CMS のコマンドラインにこのオプションが含まれていることを確認してください。 クラスタの CMS サービスの数を指定します。 このオプションによって、クラスタは大きな負荷に対応できます。

関連情報

すべてのサーバに使用できる標準オプション [1060 ページ]

31.3.4 Crystal Reports Processing Server と Crystal Reports Cache Server

Crystal Reports Processing Server と Crystal Reports Cache Server は、ほぼ同じ方法でコマンドラインから制御されます。 コマンドラインオプションで、サーバを Processing Server として起動するか、Cache Server として起動するか、またはその両方として起動するかを決定します。 以下に、1 つのサーバタイプのみに適用されるオプションを示します。

Windows 上のサーバのデフォルトパスは以下のとおりです。

- <INSTALLDIR>¥SAP BusinessObjects Business Intelligence platform 4.0¥win64_x64¥cacheserver.exe.
- <INSTALLDIR>¥BusinessObjects Business Intelligence platform XI 4.0¥win64_x64¥pageserver.exe.

UNIX 上のサーバへのデフォルトパスは以下のとおりです。

- <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_cachesd.
- <INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_procd.

オプション	有効な引数	動作
-cache		Cache Server の機能を有効にします。
-deleteCache		サーバが開始、停止するたびにキャッシュディレクトリを削除します。
-report_ProcessExtPath	**<absolutepath>**	処理拡張機能のデフォルトディレクトリを指定します。

関連情報

すべてのサーバに使用できる標準オプション [1060 ページ]

31.3.5 Job Server

この節では、Adaptive Job Server に固有のコマンドラインオプションについて説明します。

Windows 上のサーバへのデフォルトパスは、`<INSTALLDIR>¥SAP BusinessObjects Business Intelligence platform 4.0¥win64_x64¥JobServer.exe` です。

UNIX 上のサーバへのデフォルトパスは、`<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/boe_jobsd` です。

オプション	有効な引数	動作
`-dir`	**`<absolutepath>`**	Job Server のデータディレクトリを指定します。
`-maxJobs`	**`<数値>`**	サーバが同時に処理するジョブの最大数を設定します。デフォルトは 5 です。
`-requestJSChildPorts`	**`<lowerbound-upperbound>`**	子プロセスがファイアウォール環境で使用するポートの範囲を指定します。たとえば、`6800-6805` を指定すると、子プロセスを 6 つのポートに限定します。 **注記** このオプションを有効にするには、`-requestPort` 設定も指定する必要があります。
`-report_ProcessExtPath`	**`<absolutepath>`**	処理拡張機能のデフォルトディレクトリを指定します。詳細については、*SAP BusinessObjects Business Intelligence プラットフォーム管理者ガイド*を参照してください。

関連情報

すべてのサーバに使用できる標準オプション [1060 ページ]

31.3.6 Adaptive Processing Server

Adaptive Processing Server では、SAP Java 仮想マシン (SAP JVM) 用に定義されたパラメータを使用します。詳細は、SAP JVM に関する文書を参照してください。

31.3.7 Report Application Server

この節では、Report Application Server に固有のコマンドラインオプションについて説明します。

Windows 上のサーバへのデフォルトパスは、`<INSTALLDIR>¥SAP BusinessObjects Business Intelligence platform 4.0¥win32_x86¥crystalras.exe` です。

UNIX 上のサーバへのデフォルトパスは、`<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/ras/boe_crystalrasd` です。

オプション	有効な引数	動作
`-ipport`	**`<port>`**	スタンドアロンモード (BI プラットフォーム外) で実行中の場合は、TCP/IP 要求を受信するポート番号を指定します。
`-report_ProcessExtPath`	**`<absolutepath>`**	処理拡張機能のデフォルトディレクトリを指定します。詳細については、*SAP BusinessObjects Business Intelligence* プラットフォーム管理者ガイドを参照してください。

オプション	有効な引数	動作
-ProcessAffinityMask	**<mask>**	マスクを使用して、マルチプロセッサマシンで RAS が実行するときに使用する CPU を正しく指定します。 マスクは、0xffffffff の形式で表します。ここで、f は、各プロセッサを表し、プロセッサのリストは右から左へ読まれます (つまり、最後の f が最初のプロセッサを表します)。各 f は、0 (CPU 使用不可) または 1 (CPU 使用可) で置き換えます。 たとえば、4 基のプロセッサを搭載したマシンで RAS を実行し、3 つ目と 4 つ目のプロセッサを使用する場合、マスクを 0x1100 とします。2 つ目と 3 つ目のプロセッサを使用する場合は、0x0110 となります。 **注記** RAS は、文字列の中で最初に許可したプロセッサから、ライセンスによって指定された最大数のプロセッサまで使用します。2 基のプロセッサのライセンスを持っている場合、0x1110 と 0x0110 の指定はまったく同じです。 **注記** マスクのデフォルト値である -1 は、0x1111 という形式と同じ意味を表します。

関連情報

すべてのサーバに使用できる標準オプション [1060 ページ]

31.3.8 Web Intelligence Processing Server

この節では、Web Intelligence Processing Server に固有のコマンドラインオプションについて説明します。

Windows 上のサーバへのデフォルトパスは、<INSTALLDIR>¥SAP BusinessObjects Business Intelligence platform 4.0¥win64_x64¥WIReportServer.exe です。

UNIX 上のサーバへのデフォルトパスは、<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/WIReportServer です。

オプション	有効な引数	動作
-ConnectionTimeoutMinutes	**<分>**	サーバがタイムアウトになるまでの時間を分単位の数値で指定します。
-MaxConnections	**<数値>**	サーバが一度に許可する最大同時接続数を指定します。
-DocExpressEnable		Web Intelligence ドキュメントを表示する場合に、ドキュメントのキャッシュを有効にします。
-DocExpressRealTimeCachingEnable		Web Intelligence ドキュメントのリアルタイムキャッシュを有効にします。
-DocExpressCacheDurationMinutes	**<分>**	コンテンツがキャッシュに格納されている時間(分単位)を指定します。
-DocExpressMaxCacheSizeKB	**<kilobytes>**	ドキュメントキャッシュのサイズを指定します。
-EnableListOfValuesCache		値の一覧のユーザセッションごとのキャッシュを有効にします。
-ListOfValuesBatchSize	**<数値>**	バッチ単位の値の一覧ごとに返すことができる値の最大数を指定します。
-UniverseMaxCacheSize	**<数値>**	キャッシュされるユニバースの数を指定します。
-WIDMaxCacheSize	**<数値>**	キャッシュに格納できる Web Intelligence ドキュメントの最大数を指定します。

関連情報

すべてのサーバに使用できる標準オプション [1060 ページ]

31.3.9 Input/Output File Repository Server

この節では、Input File Repository Server と Output File Repository Server に固有のコマンドラインオプションについて説明します。

Windows 上のサーバへのデフォルトパスは、`<INSTALLDIR>¥SAP BusinessObjects Business Intelligence platform 4.0¥win64_x64¥fileserver.exe` です。

UNIX 上でこの 2 つのサーバをインストールするプログラムのデフォルトパスは、以下のとおりです。`<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_filesd`.デフォルトでは、Server Intelligence Agent は、Input File Repository Server 用に `boe_filesd` の 1 インスタンス、Output File Repository Server 用に 1 インスタンスを起動します。

オプション	有効な引数	動作
`-rootDir`	**`<absolutepath>`**	サーバが管理するさまざまなサブフォルダとファイルのルートディレクトリを設定します。File Repository Server でファイルを参照するために使用するファイルパスは、このルートディレクトリに対して相対的に解釈されます。 **注記** Input File Repository Server はすべて同じルートディレクトリを共有し、Output File Repository Server もすべて同じルートディレクトリを共有する必要があります。このようにしなければ、一貫性のないインスタンスが生成されます。また、input ルートディレクトリを output ルートディレクトリと同じにすることはできません。RAID 配列、または代わりのハードウェアソリューションを使用して、ルートディレクトリの複製を行うことをお勧めします。

オプション	有効な引数	動作
-tempDir	**<absolutepath>**	FRS がファイル転送に使用する一時ディレクトリの場所を設定します。FRS の一時ディレクトリの場所を制御する場合や、FRS によって生成されたデフォルトの一時ディレクトリの名前がファイルシステムパスの制限を超え、FRS を起動できない場合に、このコマンドラインオプションを使用します。 **注記** このオプションに既存のディレクトリは指定しないでください。指定したディレクトリは、FRS の起動時に空にされ、FRS のシャットダウン時に削除されます。既存のディレクトリを使用すると、そのディレクトリが空にされ、削除されてしまいます。
-maxidle	**<minutes>**	アイドルセッションがクリーンアップされるまでの時間を分単位の数値で指定します。
-legacymode		下位バージョンの SDK、または 4.0 リリースよりも前のクライアントで BI プラットフォームに完全にアクセスすることができます。
-vsaFileLoc	**<absolutepath>**	ウィルススキャンアダプタライブラリファイルへの絶対パスを設定します。 **注記** Input File Repository Server はすべて同じルートディレクトリを共有し、Output File Repository Server もすべて同じルートディレクトリを共有する必要があります。このようにしなければ、一貫性のないインスタンスが生成されます。

関連情報

すべてのサーバに使用できる標準オプション [1060 ページ]

31.3.10 Event Server

この節では、Event Server に固有のコマンドラインオプションについて説明します。

Windows 上のサーバへのデフォルトパスは、`<INSTALLDIR>¥SAP BusinessObjects Business Intelligence platform 4.0¥win64_x64¥EventServer.exe` です。

Unix 上のサーバへのデフォルトパスは、`<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_eventsd` です。

オプション	有効な引数	動作
`-cleanup`	**<分数>**	サーバがリスナープロキシをクリーンアップする頻度を分単位で指定します。この値は、2 つのクリーンアップの実行にかかる時間を表します。たとえば、値に 10 を指定すると、プロキシは 5 分ごとにクリーンアップされます。

関連情報

すべてのサーバに使用できる標準オプション [1060 ページ]

32 リポジトリ診断ツール

32.1 リポジトリ診断ツールの概要

リポジトリ診断ツール (RDT) は、Central Management Server (CMS) システムデータベースと File Repository Server (FRS) ファイルストアの間に生じるおそれのある不整合、または CMS データベースに保存されている InfoObject のメタデータで生じるおそれのある不整合のスキャン、診断、および修復を行うコマンドラインツールです。

通常の操作では、CMS システムデータベースに不整合が発生することはありません。しかし、災害復旧、バックアップの復元、ネットワーク障害などの予期されないイベント中に、不整合が発生することがあります。このような場合、タスクの実行中に、CMS システムデータベースが中断されることがあります。これによって、CMS システムデータベースのオブジェクトに不整合が生じる可能性があります。

RDT は、CMS システムデータベースをスキャンし、レポート、ユーザ、ユーザグループ、フォルダ、サーバ、ユニバース、ユニバース接続などのオブジェクトおよびその他のオブジェクトの不整合を識別します。

RDT では、3 種類の不整合がスキャンされます。

- オブジェクトからファイルへの不整合。
  これらは、CMS データベース内の InfoObject とファイルリポジトリ内の対応するファイル間で生じるおそれのある不整合です。たとえば、FRS に格納されたファイルに対応するオブジェクトが CMS システムデータベースに存在しないなどです。
- InfoObject メタデータの不整合。
  これらは、CMS データベースの InfoObject のオブジェクト定義(メタデータ)に存在する可能性のある不整合です。たとえば、InfoObject は、CMS データベースに存在しない別の InfoObject を参照する場合があります。
- 関係の不整合。
  2 つの InfoObject 間に関係が存在する場合に、そのうちの 1 つが削除されると、不整合が発生します。EnterpriseNode - サーバ、サービス - サーバ、ServiceContainer - サーバという関係のみが処理されます。

RDT は、ツールの実行時に指定したパラメータに応じて 2 つの機能を実行します。

- CMS システムデータベースおよび FRS ファイルストアをスキャンし、不整合をレポートします。また、XML 形式のログファイルを出力し、不整合を修復するためのアクションも提示します。
- CMS システムデータベースおよび FRS 内の識別された不整合をスキャンおよび修復し、実行したすべてのアクションと変更を XML 形式でレポートします。

32.2 リポジトリ診断ツールの使用

リポジトリ診断ツール(RDT)は、セントラル設定マネージャ(CCM)がインストールされている任意のマシンで使用できます。 このコマンドラインツールは、Central Management Server (CMS) システムデータベースと File Repository Server (FRS) ファイルストアの間に生じるおそれのある不整合、または InfoObject のメタデータで生じるおそれのある不整合のスキャン、診断、および修復を行います。

CMS データベースと FRS ファイルストアをバックアップし、BI プラットフォームサービスがダウンしている間にバックアップしたバージョンに対して RDT を実行することをお勧めします。 これを実行できない場合は、アクティブなデータベースで RDT を実行することができます。

アクティブなデータベースで RDT を実行する場合は、以下の事項に留意してください。

- RDT は実行中、データベース接続を 1 つ使用します。
- RDT は、実行開始時点までのデータベースの整合性のみをチェックします。 RDT の実行中に発生した整合性は記録および修正されません。
- RDT を実行するホストマシンには、RDT トランザクションを処理するためのシステムの通常の推奨容量を上回るメモリを搭載することをお勧めします。
  - InfoObject が 50,000 未満のデータベースには、処理用にさらに 350 MB 必要です。
  - InfoObject が 50,000 ～ 400,000 のデータベースには、処理用にさらに 1.7 GB 必要です。
  - InfoObject が 400,000 ～ 1,000,000 のデータベースには、処理用にさらに 4 GB 必要です。
- RDT は CMS サーバから実行する必要はありません。 別のマシンで実行することにより、システムパフォーマンスへの影響を軽減できます。
- このツールは実行中、データベースのパフォーマンスにやや影響を与える場合があります。

RDT を実行するために CMS サービスを実行する必要はありません。RDT は CMS データベースに対して直接実行されます。

32.2.1 リポジトリ診断ツールを使用する

1. Windows コンピュータでリポジトリ診断ツールを実行する場合は、コマンドウィンドウを開き、次のコマンドを実行します。

   `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥reposcan.exe <arguments>`。ここで、`<arguments>` は指定するパラメータの一覧です。

2. Unix コンピュータでリポジトリ診断ツールを実行する場合は、/usr/bin/sh 互換シェルを開き、次のコマンドを実行します。

   `.<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/boe_reposcan.sh <arguments>`。ここで、`<platform>` は “linux64_x64”、“solaris_sparcv9”、“hpux_ia64”、または “aix_rs6000_64” のいずれか、`<arguments>` は指定するパラメータの一覧です。

   > ⓘ 注記
   >
   > Unix コマンドラインのパラメータを指定するときは、特定のシェル文字を単独でエスケープまたは複数文字エスケープする必要があります。たとえば、パスワードで感嘆符 “!” を使用している場合は、感嘆符を次のようにエスケープする必要があります。`./ccm.sh -display -username Administrator -password Abc¥!defgh123 -cms cmsname`

リポジトリ診断ツールでは、リポジトリをスキャンして、不整合を検出します。指定するパラメータに応じて、不整合を診断してログに記録するか、不整合を修正して実行するアクションをログに記録します。

`Repo_Scan_yyyy_mm_dd_hh_mm_ss.xml` には、このツールで検出された不整合が一覧表示されます。このツールで検出された不一致を修正した場合は、`Repo_Repair_yyyy_mm_dd_hh_mm_ss.xml` ファイルも作成されます。このファイルには、修正されたオブジェクト、および削除されたすべての孤立ファイルについて詳細が記録されます。修正できない不整合がある場合は、その情報も含まれます。

ログファイルのパスは、outputdir パラメータで指定できます。このパラメータが指定されていない場合、ログファイルのデフォルトディレクトリは、Windows の場合は <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥reposcan、Unix の場合は ./sap_bobj/enterprise_xi40/reposcan です。

> ⓘ 注記
>
> このアプリケーションは、XML ファイルと共に使用して HTML ページを生成する、既定の XSL ファイルも提供します。この XSL ファイルは、Windows の場合は <INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥reposcan、Unix の場合は ./sap_bobj/enterprise_xi40/reposcan に保存されています。

不整合が検出された場合の警告メッセージおよび RDT で実行される推奨アクションの一覧については、*CMS メタデータの不整合および CMS と FRS 間の不整合*を参照してください。

関連情報

CMS メタデータの不整合 [1080 ページ]
CMS と FRS 間の不整合 [1079 ページ]

32.2.2 リポジトリ診断ツールのパラメータ

RDT は、次の表に示すパラメータを受け入れます。

> ⓘ 注記
>
> 実行するときには、コマンドライン引数によってパラメータファイルのエントリが上書きされます。

> ⓘ 注記
>
> SAP HANA データベースパラメータのオプションについては、SAP ノート 1916845 を参照してください。

一般のパラメータ

パラメータ	オプション/必須	説明
dbdriver	必須	CMS データベースへの接続に使用するドライバの種類。指定できる値は次のとおりです。 • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem • sqlanywheredatabasesubsystem

パラメータ	オプション/必須	説明
connect	必須	CMS データベースへの接続に使用する接続の詳細。 例: -connect "UID=root;PWD=<password>;DSN=<dsn>;HOSTNAME=<hostname>;PORT=<portnumber>"
dbkey	必須	BI プラットフォームデプロイメントのクラスタキーを入力します。 クラスタキーがわからない場合は、次の手順に従ってクラスタキーをリセットします。 **注記** マシンがクラスタ内にある場合は、この手順をすべてのクラスタメンバーに行う必要があります。続行する前に、CMS データベースおよびファイルストアのバックアップを行ってください。 1. セントラル設定マネージャ (CCM) を起動します。 2. CCM で Server Intelligence Agent (SIA) を右クリックし、停止を選択します。SIA ステータスが"停止"と表示されるまで、手順 3 に進まないでください。 3. SIA を右クリックし、プロパティ を選択します。 4. 設定タブで、*CMS クラスタキー設定*の次の変更をクリックします。 5. 警告メッセージが表示されます。はいをクリックして続行します。 6. クラスタキーの変更ダイアログボックスで、新規クラスタキー と 新規クラスタキーの確認フィールドに同じ 8 文字のキーを入力します。 **注記** dbkey パラメータが省略されている場合、またはクラスタキーが間違っている場合は RDT は実行できません。 **注記** CCM に表示されたクラスタキーが暗号化されており、dbkey パラメータ内で使用することができません。 クラスタキーの詳細については、*SAP BusinessObjects Business Intelligence* プラットフォーム管理者ガイドの「"BI プラットフォームのセキュリティ確保"」を参照してください。

パラメータ	オプション/必須	説明
`inputfrsdir`	必須	Input File Repository Server のファイルパス。 **注記** ログオンに使用するユーザアカウントは、コマンドラインツールの実行にも使用されます。そのファイルの場所に対して、フルコントロールを持つ必要があります。
`outputfrsdir`	必須	Output File Repository Server のファイルパス。 **注記** ログオンに使用するユーザアカウントは、コマンドラインツールの実行にも使用されます。そのファイルの場所に対して、フルコントロールを持つ必要があります。
`outputdir`	オプション	RDT でログファイルを書き込むファイルパス。 デフォルト値は、Windows の場合は `<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥reposcan`、Unix の場合は `./sap_bobj/enterprise_xi40/reposcan` です。
`count`	オプション	スキャンするエラー(疑わしいものを含む)の数。これにより、パフォーマンスが最適化されます。最大数は 2e31 - 1 です。値 0 は、リポジトリ全体と解釈されます。 デフォルト値は 1000 です。
`repair`	オプション	RDT で検出されたすべての不整合を修正します。デフォルトの動作は、不整合を報告するだけで修復は実行しません。`-repair` パラメータがコマンドラインに存在する場合、RDT はすべての不整合をレポートして修復します。 **警告** このプロセスで、リポジトリデータベース内の孤立したオブジェクトまたはファイルが削除されます。
`scanfrs`	オプション	RDT で CMS と FRS の不整合をスキャンするかどうかを指定します。
`scancms`	オプション	RDT で InfoObject 間の不整合について CMS をスキャンするかどうかを指定します。

パラメータ	オプション/必須	説明
submitterid	オプション	スケジュールされたオブジェクトの見つからない ID または無効な ID を置き換えるユーザ ID を指定します。値を指定しない場合、RDT では無効な ID を置き換えません。提供されているユーザ ID が CMS に存在しない場合、有効な ID の入力が要求されます。 このパラメータは、RDT が修正モードで動作している場合にのみ使用されます。
startid	オプション	スキャンを開始する CMS データベース内のオブジェクトを指定します。たとえば、リポジトリ内の最初の 500 個のオブジェクトをすでにスキャンしている場合は、**-startid=501** を設定して、新しいスキャンが 501 番目のオブジェクトから開始されるようにできます。 デフォルト値は **1** です。
optionsfile	オプション	パラメータファイルへのファイルパスを指定します。パラメータファイルは、各コマンドラインオプションとその値を示すテキストファイルです。このファイルには、1 行ごとに 1 つのパラメータが必要です。 **注記** このオプションを使用して、テキストファイル内のすべてのパラメータを上記で説明したとおりに設定できます。このオプションを使用すると、コマンドラインにパラメータを入力せずにパラメータファイルを指定することができます。
syscopy	オプション	このパラメータは、リポジトリデータベースをコピーする際に使用されます。新しく作成したコピー上でツールを実行する必要があります。これにより、コピーが更新されて、ソースシステムサーバでクラスタリングされなくなります。コピーとソースシステムが通信できなくなる場合、これは必要ありません。このパラメータは、このリストにある他のオプションパラメータと組み合わせずに必須パラメータとだけ併用するようにしてください。 **注記** ソースシステム内の syscopy パラメータで RDT を実行しないように注意してください。
trace	オプション	パラメータではトレース (監視対象コンポーネントの運用中に発生したイベントの記録) が生成され、その場所の拡張子が .glf のログファイルに収集されます。 `<SAP_BOBJ_INST_DIR>¥SAP BusinessObjects¥SAP BusinessObjects Enterprise XI 4.0¥logging`

パラメータ	オプション/必須	説明
`scankind`	オプション	不整合をスキャンする InfoObject の種類を入力します。 例 SI_KIND: Web Intelligence レポート、Crystal レポート 不整合をスキャンできる、サポートされている InfoObject の一覧は以下のとおりです。 • folder • crystalreport • shortcut • user • usergroup • calendar • connection • category • objectpackage • publication • pdf • rtf • txt • note • word • excel • tenant • profile • program • agnostic • universe • hyperlink • fullclient • powerpoint • scopebatch • metadata.dataconnection • webi • qaaws • lcmjob • overload • xcelsius

パラメータ	オプション/必須	説明
		• biwidgets • mon.probe • liveoffice • mdanalysis • visualdiff • ao.workbook • dsl.metadatafile • afdashboardpage • ao.presentation • ccis.dataconnection • platformsearchqueue • metadata.businessview • platformsearchindex • platformsearchcontentstore • platformsearchcontentsurrogate **注記** scankind の XML 出力には、InfoObject に関して不整合の一覧が表示されます。つまり、影響を受けるファイルオブジェクトは一覧表示されません。
scandays	オプション	RepoScan で不整合をチェックする日数を入力します。 **例** 0 以外の任意の実数です。 **注記** このオプションは、現在のシステム時間に基づいて機能します。

部分的なスキャン中、リレーションシップはスキャンされません。部分的なスキャンは、以下の 3 つのオプションのいずれかが使用されている場合に行われます。

- startid
- scankind
- scandays

リレーションシップの不整合

警告メッセージ	不整合	提案	アクション
Relation '<Name>' from object ID <ID> has an invalid target (Object ID = <ID>)	リレーションシップの境界は存在しなくなりました。	アプリケーションにより、リレーションシップを削除できます。	リレーションシップが削除されます。

次のパラメータは、リポジトリ診断ツールがクラスタ化された有効な CMS データベース上で稼働している場合に使用します。

クラスタ化された CMS に対する RDT の使用

パラメータ	オプション/必須	説明
requestport	オプション	RDT が CMS と通信する際に使用するポート番号。正の整数を指定します。デフォルトでは、RDT が実行されているマシンのオペレーティングシステムの値が使用されます。
numericip	オプション	RDT が、CMS と RDT を実行するマシンとの間の通信にホスト名ではなく数値の IP アドレスを使用するかどうかを指定します。指定できる値は、**True** と **False** です。 デフォルト値は **False** です。
ipv6	オプション	RDT が実行されているマシンの ipv6 名。文字列を指定します。 デフォルト値は、RDT が実行されているマシンのホスト名です。
port	オプション	RDT が実行されているマシンの ipv4 名。文字列を指定します。 デフォルト値は、RDT が実行されているマシンのホスト名です。
threads	オプション	使用するスレッドの数。正の整数を指定します。 デフォルト値は **12** です。

次のパラメータは、RDT が SSL を使用してスキャン対象の CMS データベースと通信する際に使用します。

SSL を使用する RDT の使用

パラメータ	オプション/必須	説明
protocol	オプション	ツールを SSL モードで実行するかどうかを指定します。 指定できる値は、**ssl** だけです。
ssl_certdir	オプション	SSL 証明書を含むディレクトリ。
ssl_trustedcertificate	オプション	証明書のファイル名。

パラメータ	オプション/必須	説明
ssl_mycertificate	オプション	署名付き証明書のファイル名。
ssl_mykey	オプション	SSL プライベートキーを含むファイルのファイル名。
ssl_mykey_passphrase	オプション	SSL パスフレーズを含むファイルのファイル名。

例

次の Windows の例では、CMS と FRS をスキャンして、両方の種類の不整合を検出し、検出された不整合を修正します。

```
reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect “UID=root;PWD=<Password1>;DSN=<myDsn>;HOSTNAME=<myHostname>;PORT=<3306>”
-inputfrsdir “C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects
Enterprise XI 4.0¥FileStore¥Input”
-outputfrsdir    “C:¥Program Files (x86)¥SAP BusinessObjects¥SAP BusinessObjects
Enterprise XI 4.0¥FileStore¥Output”
-dbkey <cluster key>
-repair
```

例

Unix の例。

```
./boe_reposcan.sh
-dbdriver oracledatabasesubsystem
-connect "UID=<bi_admin>;PWD=<Password1>;DSN=<myDsn>;PORT=<6400>"
-inputfrsdir /apps/frs/bi/frsinput
-outputfrsdir /apps/frs/bi/frsoutput
-dbkey <cluster key>
```

32.3 CMS と FRS 間の不整合

次の表に、Central Management Server (CMS) データベースと File Repository Server (FRS) 間で生じるおそれがあり、リポジトリ診断ツール (RDT) で認識できる不整合についての説明を示します。

- 警告メッセージ
  スキャンログファイルおよび修正ログファイルに書き込まれる警告メッセージ。
- 不整合
  RDT がオブジェクトで検出した不整合の説明。
- 提案
  RDT が不整合を検出したときに提案するアクション。 これは、スキャンログファイルに記録されます。

- アクション
  不整合を修正するために RDT が実行するアクション。 これは、修正ログファイルに記録されます。

警告メッセージ	不整合	提案	アクション
<Object Name> オブジェクト <Object Type> (オブジェクト ID = <ID>) は FRS (<File Name>) 内に存在しないファイルを参照しています。	オブジェクトは CMS データベースに存在しますが、対応するファイルが FRS にありません。	アプリケーションにより、このオブジェクトを削除できます。 このオブジェクトの子孫のオブジェクトもすべて削除されます。	リポジトリからこのオブジェクトを削除しました。
ファイル <File Name> は Input FRS または Output FRS に存在しますが、リポジトリには対応する InfoObject がありません。	ファイルは FRS に存在しますが、CMS データベースに対応するファイルがありません。	アプリケーションにより、リンクされていないファイルを削除できます。	操作は実行されません。
<Object Type> オブジェクト <Object Name> (オブジェクト ID = <ID>) にファイル <File Name> があります。 保存されたファイルサイズは <Size> バイトで、実際のファイルサイズである <Size> バイトと一致しません。	ファイルのサイズが、インフォオブジェクトのファイルサイズと一致しません。	アプリケーションにより、オブジェクトを正しいファイルサイズで更新できます。	ファイルサイズが正しくなるようオブジェクトを更新しました。
このディレクトリにはファイルがありません。	FRS フォルダが空です。	アプリケーションにより、ディレクトリを削除できます。	空のフォルダを削除しました。

32.4 CMS メタデータの不整合

次の表で、Central Management Server (CMS) システムデータベース内のオブジェクトのメタデータで発生する可能性があり、リポジトリ診断ツール (RDT) で認識される不整合について説明します。

- 警告メッセージ
  スキャンログファイルおよび修正ログファイルに書き込まれる警告メッセージ。
- 不整合
  RDT がオブジェクトで検出した不整合の説明。
- 提案
  RDT が不整合を検出したときに提案するアクション。 これは、スキャンログファイルに記録されます。
- アクション
  不整合を修正するために RDT が実行するアクション。 これは、修正ログファイルに記録されます。

警告メッセージ	不整合	提案	アクション
<Object Type> オブジェクト <Object Name> (オブジェクト ID = <ID>) の親オブジェクトが見つかりません (親オブジェクト ID = <ID>)。	オブジェクトの親オブジェクト ID が見つからないか、無効です。	アプリケーションにより、オブジェクトを "BOE 修復" フォルダへ移動できます。	オブジェクトとその子オブジェクトを "BOE 修復" フォルダに移動しました。

警告メッセージ	不整合	提案	アクション
`<Object Type>` オブジェクト `<Object Name>` (オブジェクト ID = `<ID>`) 所有者オブジェクトが見つかりません (所有者オブジェクト ID = `<ID>`)。	オブジェクトの所有者オブジェクト ID が見つからないか、無効です。	アプリケーションにより、オブジェクトを管理者へ割り当てることができます。	オブジェクトを管理者に割り当てました。
`<Object Type>` オブジェクト `<Object Name>` (オブジェクト ID = `<ID>`) 送信元オブジェクトが見つかりません (送信元オブジェクト ID = `<ID>`)。	オブジェクトの送信者オブジェクト ID が見つからないか、無効です。	RDT に表示される推奨事項は、`-submitterid` パラメータに値を指定したかどうかで異なります。 • このパラメータを指定する場合、[“アプリケーションにより、オブジェクトを正しいファイルサイズで更新できます。”]オプションが推奨です。 • このパラメータを指定しない場合、[“オブジェクトを再スケジュールするか、-submitterid コマンドラインを使用して、無効な送信元 ID を置き換えます。”] オプションが推奨です。	`-submitterid` パラメータの値を指定すると、RDT はオブジェクトの送信元 ID の値を適用します。 このパラメータの値を指定しない場合、RDT は何も実行しません。 オブジェクトを再スケジュールすると、CMS によって新しい ID が適用されます。
`<Object Type>` オブジェクト '`<Object Name>`' (オブジェクト ID = `<ID>`) の最後に成功したインスタンスのプロパティは、見つからないオブジェクト (最後に成功したインスタンスオブジェクト ID = `<ID>`) を参照しています。	オブジェクトの最後に成功したインスタンスが見つからないか、無効です。	アプリケーションにより、プロパティを再計算できます。	プロパティを再計算しました。
`<Object Type>` オブジェクト '`<Object Name>`' (オブジェクト ID = `<ID>`) のカレンダオブジェクトが見つかりません (カレンダオブジェクト ID = `<ID>`)。	オブジェクトは、存在していないカレンダを参照しています。	既存のカレンダを持つオブジェクトを再計算します。 このアプリケーションによる操作は実行されません。	操作は実行されません。
`<Object Type>` オブジェクト '`<Object Name>`' (オブジェクト ID = `<ID>`) に必要なスケジュールサーバグループが見つかりません (サーバグループオブジェクト ID = `<ID>`)。	必要なサーバが存在しません。	オブジェクトを再スケジュールし、既存のサーバグループを選択します。 このアプリケーションによる操作は実行されません。	操作は実行されません。

警告メッセージ	不整合	提案	アクション
<Object Type> オブジェクト '<Object Name>' (オブジェクト ID = <ID>) の待機中イベントのリストには、見つからないオブジェクト (複数可) (イベントオブジェクト ID = <ID>) が含まれています。	このオブジェクトが待機している 1 つまたは複数のイベントが存在していません。	既存のイベントオブジェクトを待つようオブジェクトを再スケジュールします。 このアプリケーションによる操作は実行されません。	操作は実行されません。
<Object Type> オブジェクト '<Object Name>' (オブジェクト ID = <ID>) のトリガするイベントのリストには、見つからないオブジェクト (複数可) (イベントオブジェクト ID = <ID>) が含まれています。	このオブジェクトは、存在していないイベントをトリガしています。	アプリケーションにより、見つからないイベントをオブジェクトがトリガするイベントリストから削除できます。	オブジェクトがトリガするイベントのリストから、見つからないイベントを削除しました。
<Object Type> オブジェクト '<Object Name>' (オブジェクト ID = <ID>) のアクセスコントロールリストは、見つからない主体 (主体オブジェクト ID = <ID>) を参照します。	アクセスコントロールエントリが孤立しています。	アプリケーションにより、見つからない主体をオブジェクトのアクセスコントロールリストから削除できます	オブジェクトのアクセスコントロールリストから、見つからない主体を削除しました。
<Object Type> オブジェクト '<Object Name>' (オブジェクト ID = <ID>) のアクセスコントロールリストは、見つからないアクセスレベル (アクセルレベルオブジェクト ID = <ID>) を参照します。	アクセスコントロールエントリが孤立しています。	アプリケーションにより、オブジェクトのアクセスコントロールリストから、見つからないアクセスレベルを削除できます。	オブジェクトのアクセスコントロールリストから、見つからないアクセルレベルを削除しました。
<Object Type> オブジェクト <Object Name> (オブジェクト ID = <ID>) には、お気に入りフォルダが複数あります。	特定のユーザアカウントに複数のお気に入りフォルダがあります。	アプリケーションにより、複数のフォルダを 1 つのお気に入りフォルダに統合できます。	すべてのお気に入りフォルダが 1 つのお気に入りフォルダに統合されています。
<Object Type> オブジェクト <Object Name> (オブジェクト ID = <ID>) に無効な入力ファイルエントリ (<Files>) が含まれています。	オブジェクトには、その入力ファイルリストに無効なエントリが含まれています。	ツールにより、入力ファイルリストからオブジェクトの無効なエントリを削除できます。	オブジェクトの入力ファイルリストから無効なエントリを削除しました。
<Object Type> オブジェクト <Object Name> (オブジェクト ID = <ID>) に無効な出力ファイルエントリ (<Files>) が含まれています。	オブジェクトには、その出力ファイルリストに無効なエントリが含まれています。	ツールにより、出力ファイルリストからオブジェクトの無効なエントリを削除できます。	オブジェクトの出力ファイルリストから無効なエントリを削除しました。
<Object Type> オブジェクト '<Object Name>' (オブジェクト ID = <ID>) に必要なキャッシュサーバグループが	オブジェクトに必要なキャッシュサーバグループが見つかりません。	オブジェクトを再スケジュールし、既存のサーバグループを選択します。	操作は実行されません。

警告メッセージ	不整合	提案	アクション
見つかりません (サーバグループオブジェクト ID = `<ID>`)。			
`<Object Type>` オブジェクト '`<Object Name>`' (オブジェクト ID = `<ID>`) に必要な処理サーバグループが見つかりません (サーバグループオブジェクト ID = `<ID>`)。	オブジェクトに必要な処理サーバグループが見つかりません。	オブジェクトを再スケジュールし、既存のサーバグループを選択します。	操作は実行されません。
`<Object Type>` オブジェクト `<Object Name>` (オブジェクト ID = `<ID>`) のプロファイルのリストに見つからないオブジェクト (複数可) (プロファイルオブジェクト ID = `<ID>`) が含まれています。	オブジェクトには、オブジェクトのプロファイルのリストに見つからないオブジェクトが含まれています。	既存のプロファイルでパブリケーションを更新してください。 このアプリケーションによる操作は実行されません。	操作は実行されません。

32.5 BOE WebApp 内の Restful SDK の管理

4.3 SP03 で BOE Webapp の BIPRWS WebApp 部分を有効化するには、以下の場所でフラグを *true* に設定します。

```
<BOE_INST_DIR>¥SAP BusinessObjects¥tomcat¥webapps¥BOE¥WEB-INF¥internal¥Global.properties
```

`use.boe.internal.biprws=true` を設定します。

フラグを true に設定すると、内部アプリケーションは Restful アプリケーション URL または CMC で設定された相対パスフラグに依存しなくなります。

この機能は、以下の回避に役立つため、有用です。

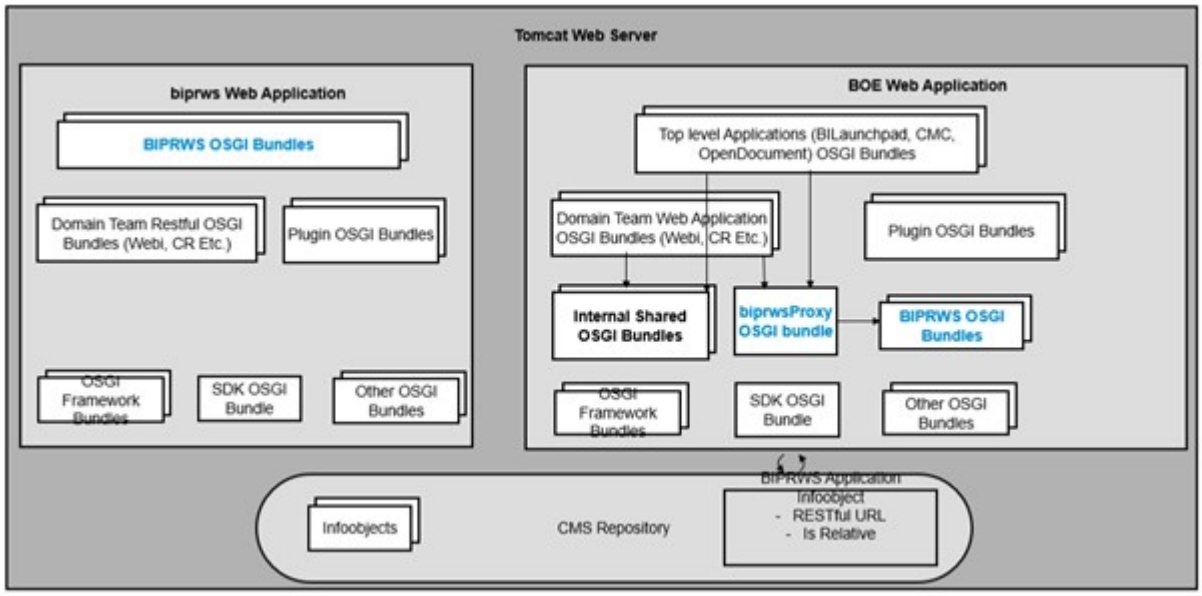
- CORS (クロスオリジンリソース共有)
- 内部および外部システムの接続の問題
- セッションを有効に維持するための BOE WebApp に対する ping の実行
- BIPRWS と BOE に個別の設定がないことによるプロキシ関連の問題の発生
- Web アプリケーションのクラスタ関連の問題

BOE WebApp による既存のデプロイメントは、アップグレード後にシームレスに機能します。

ログ:

BIPRWS が BOE WebApp にマージされると、BI ラウンチパッドまたは CMC アプリケーションのログの場所の一部としてログが生成されます。

アーキテクチャ:


Tomcat Web Server
biprws Web Application
BIPRWS OSGI Bundles
Domain Team Restful OSGI Bundles (Webi, CR Etc.)
Plugin OSGI Bundles
OSGI Framework Bundles
SDK OSGI Bundle
Other OSGI Bundles
BOE Web Application
Top level Applications (BILaunchpad, CMC, OpenDocument) OSGI Bundles
Domain Team Web Application OSGI Bundles (Webi, CR Etc.)
Plugin OSGI Bundles
Internal Shared OSGI Bundles
biprwsProxy OSGI bundle
BIPRWS OSGI Bundles
OSGI Framework Bundles
SDK OSGI Bundle
Other OSGI Bundles
Infoobjects
CMS Repository
BIPRWS Application Infoobject
- RESTful URL
- Is Relative

33 HTTP Strict Transport Security (HSTS)

33.1 HTTP Strict Transport Security (HSTS) の設定

HTTP Strict Transport Security (HSTS) は、プロトコルダウングレード攻撃や Cookie のハイジャックなどの中間者攻撃から Web サイトを保護するためのポリシーメカニズムです。

これにより、Web サーバは、Web ブラウザ (または他の準拠しているユーザエージェント) が HTTPS 接続のみを使用して自動的に通信することを宣言できます。これにより、安全でない HTTP の使用とは異なり、TLS (Transport Layer Security) が提供されます。

HSTS は IETF 標準化過程にあるプロトコルであり、RFC 6797 で規定されています。

HSTS ポリシーは、HTTP 応答ヘッダフィールド "Strict-Transport-Security" を介してサーバからユーザエージェントに伝達されます。

1. このポリシーでは、ユーザエージェントが安全な方法でのみサーバにアクセスする期間を指定します。
2. HSTS を使用する Web サイトでは、HTTP を介した接続を拒否したり、HTTPS にユーザを体系的にリダイレクトしたりして、クリアテキスト HTTP を受け入れないことがよくあります (ただし、これは仕様では必要ありません)。
   これは、TLS を実行できないユーザエージェントがサイトに接続できないことを確認するためです。
3. この保護は、初回利用での信頼の原則に基づきユーザが 1 回以上サイトにアクセスした後にのみ適用されます。

動作

ユーザが HTTP を指定するサイトの URL を入力または選択すると、その URL は HTTP 要求を行わずに HTTPS に自動的にアップグレードされます。これにより、HTTP 中間者攻撃が発生しなくなります。

4.3 SP03 では、SAP BOE で HSTS 契約がサポートされます。

HSTS を設定する前に、SSL を使用してアプリケーションサーバを設定する必要があります。

HSTS サポートを有効化するには、以下の手順を実行します。

1. Tomcat を停止します。
2. `E:¥Program Files (x86)¥SAP BusinessObjects¥tomcat¥webapps¥BOE¥WEB-INF¥config¥default` に移動します。
3. Global.properties ファイルを開き、以下のパラメータを設定します。
   1. `hsts.enabled` True/False。デフォルト値は false に設定されています。
   2. `hsts.Include.SubDomains` True/False。ドメイン名のすべてのサブドメインに影響します。
   3. `hsts.MaxAge.Seconds` = 31536000。
   4. デフォルトは 365 日です。
4. 変更を保存します。

34 アクセス権に関する付録

34.1 付録 - 権限について

このアクセス権に関する付録では、BI プラットフォームシステムのさまざまなオブジェクトに対して設定できる権限の多くをその説明とともに示しています。 オブジェクトに対してタスクを実行するために複数の権限が必要な場合は、他に必要になる権限とその対象になるオブジェクトについての情報も示しています。 アクセス権の設定の詳細については、*SAP BI* プラットフォーム管理者ガイドのアクセス権の設定の章を参照してください。

34.2 全般の権限

このセクションの権限は、複数の種類のオブジェクトに適用されます。これらの権限の多くには、それと等価な所有者権限があります。所有者権限は、アクセス権がチェックされるオブジェクトの所有者にのみ適用されるアクセス権です。

次の権限は、スケジュール可能なオブジェクトのみに適用されます。

- ドキュメントの実行をスケジュールする権限
- 他のユーザの代理としてスケジュール権限
- 別の出力先へスケジュールする権限
- ドキュメントのインスタンスを表示する権限
- インスタンスを削除する権限
- ドキュメントのインスタンスを一時停止して再開する権限
- インスタンスの再スケジュール権限

権限	説明
オブジェクトを表示する	オブジェクトとそのプロパティを表示できるようにします。オブジェクトに対してこの権限がない場合、そのオブジェクトは BI プラットフォームシステムでは非表示になります。この権限は、すべてのタスクに必要な基本的な権限です。
オブジェクトをフォルダに追加する	フォルダにオブジェクトを追加できるようにします。この権限は、フォルダのように動作するオブジェクト (受信ボックス、[お気に入り] フォルダ、オブジェクトパッケージなど) にも適用できます。
オブジェクトを編集する	オブジェクトコンテンツ、およびオブジェクトやフォルダのプロパティを編集できるようにします。

権限	説明
オブジェクトに対するユーザの権限を変更する	オブジェクトのセキュリティ設定を変更できるようにします。
ユーザがオブジェクトに対して持っているアクセス権を安全に変更する	オブジェクトに対してすでに持っている権限またはアクセスレベルを他のユーザに許可できるようにします。これには、相手のユーザとそのオブジェクトに対して、この権限を持っている必要があります。この権限の詳細については、*SAP BusinessObjects Business Intelligence* プラットフォーム管理者ガイドの“アクセス権の設定”の章を参照してください。
ジョブを処理するサーバグループを定義する	オブジェクトを処理するときに使用するサーバグループを指定できるようにします。この権限は、その処理を実行するサーバを指定できるオブジェクトのみに適用されます。 サーバグループを指定するには、そのオブジェクトに対する [オブジェクトを編集する] 権限も必要になります。
オブジェクトを削除する	オブジェクトとそのインスタンスを削除できるようにします。
オブジェクトを別のフォルダにコピーする	CMS の他のフォルダにオブジェクトのコピーを作成できるようにします。そのためには、そのドキュメントフォルダに対する [オブジェクトをフォルダに追加する] 権限も必要になります。 **注記** オブジェクトがコピーされても、オブジェクトの明示的なセキュリティはコピーされません。新しいオブジェクトはコピー先のフォルダからセキュリティ設定を継承しますが、明示的なセキュリティをリセットする必要があります。
内容の複製	フェデレートしたデプロイメント内の別のシステムにオブジェクトを複製できるようにします。
ドキュメントの実行をスケジュールする	オブジェクトをスケジュールできるようにします。
他のユーザの代理としてスケジュール	他のユーザまたはグループのためにオブジェクトをスケジュールできるようにします。代理としてオブジェクトをスケジュールするユーザまたはグループは、そのオブジェクトインスタンスの所有者になります。 他のユーザまたはグループのためにオブジェクトをスケジュールするには、次の権限も必要になります。 • この権限は、ユーザまたはグループに対するものです。 • オブジェクトに対する [ドキュメントの実行をスケジュールする] 権限

権限	説明
別の出力先へスケジュールする	[別の出力先へスケジュールする] は、*[FTP へのスケジュール]*、*[SMTP へのスケジュール]*、*[BI 受信ボックスへのスケジュール]*、*[SFTP へのスケジュール]*、および [ファイルシステムへのスケジュール] の親権限です。オブジェクトを特定の出力先にスケジュールするには、[別の出力先へスケジュールする] 権限を特定の子権限と組み合わせて選択してください。たとえば、オブジェクトを　FTP 出力先にスケジュールするには、[別の出力先へスケジュールする] 権限と [*FTP へのスケジュール*] 権限を選択してください。BI ランドスケープを BI 4.2 SP04 以前から BI 4.2 SP05 以降に更新中の場合、トラブルシューティングの詳細については 2675734、2642221、2626550 を参照してください。 オブジェクトを出力先にスケジュールするには、次の権限も必要になります。 • スケジュールするオブジェクトに対する [ドキュメントの実行をスケジュールする] 権限 • 受信者の受信ボックスに対する [オブジェクトをフォルダに追加する] 権限 (受信ボックスを出力先としてスケジュールする場合) • スケジュールするオブジェクトに対する [オブジェクトを別のフォルダにコピーする] 権限 (受信ボックスを出力先としてショートカットではなくコピーを送信する場合) **注記** BI 4.2 SP04 以前で [別の出力先へスケジュールする] 権限が [フルコントロール] や [スケジュール] ロールなどの [アクセスレベル] を介して割り当てられている場合、BI 4.2 SP05 パッチ 03 以降に更新した後は、*[FTP へのスケジュール]*、*[SMTP へのスケジュール]*、*[SFTP へのスケジュール]*、*[BI 受信ボックスへのスケジュール]*、および [ファイルシステムへのスケジュール] などの子出力先権限も許可されます。BI 4.2 SP04 以前での [オンデマンド表示] や [カスタム] ロールなどの [アクセスレベル] の場合は、BI 4.2 SP05 パッチ 03 以降に更新した後、子出力先権限はデフォルトでは許可されません。権限をマニュアルで許可する必要があります。したがって、BI 4.2 SP04 以前で作成した定期的なスケジュールジョブによって、BI 4.2 SP05 パッチ 03 以降でオブジェクトが正常にスケジュールされます。
FTP へのスケジュール	FTP 出力先へのオブジェクトをスケジュールすることができます。
SFTP へのスケジュール	SFTP 出力先へのオブジェクトをスケジュールすることができます。
SMTP へのスケジュール	SMTP 出力先へのオブジェクトをスケジュールすることができます。

権限	説明
ファイルシステムへのスケジュール	ファイルシステム出力先へのオブジェクトをスケジュールすることができます。
受信ボックスへのスケジュール	BI 受信ボックス出力先へのオブジェクトをスケジュールすることができます。
ドキュメントのインスタンスを表示する	オブジェクトインスタンスを表示できるようにします。この権限は、オブジェクトインスタンスに対して実行するすべてのタスクに必要な基本的な権限です。
インスタンスを削除する	オブジェクトのインスタンスのみを削除できるようにします。[オブジェクトを削除する] 権限がある場合は、インスタンスを削除する権限は必要ありません。
ドキュメントのインスタンスを一時停止して再開する	実行中のオブジェクトインスタンスを一時停止または再開できるようにします。
インスタンスの再スケジュール	オブジェクトインスタンスを再スケジュールできるようにします。
コメントの追加 - *BI Commentary*	ユーザが BI Commentary を使用してドキュメントにコメントを追加できるようにします。
コメントの削除 - *BI Commentary*	ユーザが BI Commentary を使用してドキュメントからコメントを削除できるようにします。
ユーザが作成したコメントの削除 - *BI Commentary*	ユーザが BI Commentary を使用してドキュメントから作成したコメントを削除できるようにします。
コメントの変更 - *BI Commentary*	ユーザが BI Commentary を使用してドキュメントのコメントを変更できるようにします。
ユーザが作成したコメントの変更 - *BI Commentary*	ユーザが BI Commentary を使用してドキュメントの作成したコメントを変更できるようにします。
コメントの表示 - *BI Commentary*	ユーザが BI Commentary を使用してドキュメントのコメントを表示できるようにします。
ユーザが作成したコメントの表示 - *BI Commentary*	ユーザが BI Commentary を使用してドキュメントの作成したコメントを表示できるようにします。
コメントの非表示 - *BI Commentary*	ユーザが BI Commentary を使用してドキュメントのコメントを非表示にできるようにします。

権限	説明
ユーザが作成したコメントの非表示 - *BI Commentary*	ユーザが BI Commentary を使用してドキュメントの作成したコメントを非表示にできるようにします。
コメントの一括追加 - *BI Commentary*	ユーザがドキュメントと一緒にコメントを移行できます。

34.2.1 出力先権限

各出力先は、特定の出力先権限に関連付けられます。BOE 管理者は、ユーザに目的の出力先権限を割り当てる必要があります。

以前は、[別の出力先へスケジュールする] 権限を持っている場合、ユーザは使用可能なすべての出力先に対してスケジュールできました。SP05 リリース以降、[別の出力先へスケジュールする] が [デフォルトの *Enterprise* の場所] のみに対応しているユーザに個別の出力先権限が付与されました。

各出力先の全般の権限に新しい権限が導入されました。

- ファイルシステムへのスケジュール
- FTP へのスケジュール
- 受信ボックスへのスケジュール
- SFTP へのスケジュール
- SMTP へのスケジュール
- Google ドライブへのスケジュール

全般の権限の詳細については、全般の権限 [1086 ページ]を参照してください。

スケジュール中にこれらの出力先オプションを提供するには、管理者は個々の出力先権限を付与する必要があります。2621878 を参照してください。ユーザが [別の出力先へスケジュールする] に対する権限のみを持っている場合、ユーザは FTP、受信ボックス、SFTP、SMTP、およびファイルシステムの出力先にスケジュールすることはできません。

以前のバージョンで [別の出力先へスケジュールする] 権限が [フルコントロール] や [スケジュール] ロールなどのアクセスレベルを介して割り当てられている場合、4.2 SP05 へのアップグレード後、追加の (新しく導入された) 権限も付与されます。したがって、どの宛先へのスケジュールも正常に実行されます。

この権限が [オンデマンド表示] アクセスレベルまたはいずれかのカスタムロールを介して割り当てられているか、直接割り当てられている (ロールによるものではなく、個別の権限) 場合、[デフォルトの *Enterprise* の場所] へのスケジュールのみが成功し、他の出力先へのスケジュールは失敗します。

詳細については、出力先オプションおよび電子メールの出力先のプロパティを参照してください。

34.3 特定のオブジェクトの種類のアクセス権

34.3.1 フォルダのアクセス権

権限の管理を簡単にするために、フォルダに権限を設定してそれに含まれるものが権限設定を継承するようにすることをお勧めします。 フォルダには、次のような権限があります。

- フォルダオブジェクトに適用される一般的な権限
- フォルダのコンテンツに対する種類固有アクセス権(Crystal レポートに対する[レポートのデータを出力する]権限など)

34.3.2 カテゴリ

このセクションの権限は、パブリックカテゴリおよび個人用カテゴリのコンテキストで固有の意味を持つ、一般的な権限です。

> ⓘ 注記
>
> カテゴリのオブジェクトは、そのカテゴリに設定されている権限を継承しません。

権限	説明
オブジェクトをフォルダに追加する	カテゴリ内に新しいカテゴリを作成できるようにします。 この権限は、カテゴリにオブジェクトを追加するときには必要ありません。
オブジェクトを編集する	次の操作を実行できるようにします。 • カテゴリのプロパティを修正する。 • カテゴリを他のカテゴリの中に移動してサブカテゴリにする。 • オブジェクトをカテゴリに追加する。 • カテゴリからオブジェクトを削除する。 カテゴリを他のカテゴリの中に移動してサブカテゴリにする場合は、次の権限も必要です。 • 元のカテゴリに対するオブジェクトを削除する権限 • 移動先のカテゴリに対するオブジェクトをフォルダに追加する権限
オブジェクトを削除する	カテゴリを削除できるようにします。

34.3.3 Crystal レポート

このセクションの権限は、Crystal レポートのみに適用されます。

> **注記**
>
> これらの権限は、Crystal レポートが BI プラットフォーム環境に含まれている場合にのみ適用されます。Crystal レポートをローカルディスクにダウンロードした場合は、これらの権限は無効になります。 このような事態を避けるには、Crystal レポートに対してオブジェクトに関連するファイルをダウンロード権限を拒否します。

権限	説明
レポートのデータを出力する	レポートを印刷できるようにします。
レポートのデータを最新表示する	レポートのデータを最新表示できるようにします。
レポートのデータをエクスポートする	Crystal Reports ビューアでレポートをオンライン表示するときに、任意の形式でエクスポートできるようにします。 レポートデータを RPT 形式でエクスポートするには、オブジェクトに関連するファイルをダウンロード権限も持つ必要があります。
オブジェクトに関連するファイルをダウンロード	この権限によって、次の操作が実行できるようになります。 • RPT 形式でレポートをエクスポートする。 • Crystal Reports Designer でレポートを開く。 • 外部の出力先に向けて RPT 形式のレポート出力をスケジュールする。

34.3.4 Web Intelligence ドキュメント

このセクションの権限は、Web Intelligence ドキュメントのみに適用されます。

権限	説明
値の一覧の使用	値の一覧を使用できるようにします。
レポートのデータをエクスポートする	レポートのデータをテキスト、CSV、Excel、PDF、または HTML 形式にエクスポートできます。また、このコマンドでは、印刷可能な PDF ファイルを生成する印刷コマンドを使用することもできます。
クエリスクリプト - 表示の有効化 *(SQL、MDX...)*	クエリスクリプトを表示できるようにします (SQL および MDX)。
クエリスクリプト - 編集の有効化 *(SQL、MDX...)*	クエリスクリプト (SQL および MDX) を編集できます。SQL 文の直接入力 (FHSQL) データソースを編集することもできます。
レポートのデータを最新表示する	ドキュメントのデータを最新表示できるようにします。
クエリの編集	ドキュメントのクエリを編集できるようにします。

権限	説明
値の一覧の最新表示	プロンプトを作成したとき、またはドキュメントを表示したときに、プロンプトの値の一覧を最新表示できるようにします。そのためには、そのドキュメントに対する [値の一覧の使用] 権限も必要になります。
送信先	ドキュメントをスケジューラまたは BI プラットフォーム受信トレイに送信するか、電子メールでハイパーリンクとして送信できるようになります。また、この権限により、Web Intelligence リッチクライアントユーザがドキュメントを電子メールの添付文書として送信することもできるようになります。

34.3.5 ユーザとグループ

BI プラットフォーム環境内の他のオブジェクトに対してと同様、ユーザとグループに対しても権限を設定できます。このセクションの権限は、ユーザとグループオブジェクトのみに適用されるタイプ固有権限、またはユーザとグループのコンテキストで固有の意味を持つ一般的な権限です。

> ⓘ 注記
>
> ユーザとサブグループは、グループメンバーシップの権限を継承できます。

> ⓘ 注記
>
> ユーザアカウントの作成者は、そのアカウントの所有者と見なされます。ただし、ユーザアカウントが作成された後は、そのアカウントが作成されたユーザも所有者と見なされます。

権限	説明
オブジェクトを編集する	次の操作を実行できるようにします。 • ユーザまたはグループのプロパティを編集する。 • グループメンバーシップを管理する。 ユーザまたはグループを別のグループに追加するには、そのユーザまたはグループと追加先のグループに対して、この権限を持つ必要があります。
ユーザパスワードの変更	次の操作を実行できるようにします。 • ユーザアカウントのパスワードを変更します。そのためには、ユーザアカウントに対する [オブジェクトを編集する] 権限も必要になります。 • 別のユーザアカウントのパスワードを変更します。この場合、そのユーザアカウントに対する [オブジェクトを編集する] 権限と [オブジェクトに対するユーザの権限を変更する] 権限が必要です。

権限	説明
	注記 この権限は、次のユーザパスワード設定には影響しません。 パスワードを無期限にする ユーザは次回ログオン時にパスワード変更が必要 ユーザはパスワードを変更できない **注記** この権限は、SAP BusinessObjects ユニバースのデータソース認証情報には適用されません。
パブリケーションの購読	パブリケーションに受信者としてユーザを追加できるようにします。
他のユーザの代理としてスケジュール	ユーザに代わってオブジェクトをスケジュールし、そのユーザがそのオブジェクトインスタンスの所有者になるようにします。そのためには、そのオブジェクトに対する [他のユーザの代理としてスケジュール] 権限も必要になります。
ユーザ属性の追加または編集	ユーザの電子メールアドレスまたはカスタムユーザ属性の値を変更できるようにします。 この権限は、ユーザに適用できます。
ユーザ属性の追加または編集 (所有者の権限)	ユーザの電子メールアドレスまたはカスタムユーザ属性の値を、ユーザオブジェクトの所有者が変更できるようにします。 この権限は、ユーザに適用できます。
ユーザが所有するオブジェクトの基本設定の変更	アプリケーションオブジェクトの [基本設定] メニューを表示します。 このアクセス権がないと、ユーザはどのアプリケーションでも個人用の基本設定を設定できず、[基本設定] メニューがアプリケーションに表示されません。たとえば、この権限がないと、ユーザは Web Intelligence または BI ラウンチパッドアプリケーションのレポートで使用する測定単位 (インチまたはミリメートル) を選択できません。

34.3.6 アクセスレベル

このセクションの権限は、アクセスレベルのみに適用されます。

権限	説明
セキュリティ割り当てにアクセスレベルを使用する	オブジェクトのアクセス制御リストに主体を追加するときに、アクセスレベルを割り当てられるようにします。この場合、プリンシパルおよびオブジェクトに対してオブジェクトに対するユーザの権限を変更するまたはユーザがオブジェクトに対して持っているアクセス権を安全に変更する権限も必要になります。オブジェクトに対して持っているアクセス権を安全に変更する権限が許可されている場合、オブジェクトで自分に対して同じアクセスレベルを許可する必要があります。

34.3.7 ユニバース (.unv) のアクセス権

このセクションの権限は、ユニバースデザインツールまたは.unv ユニバースを使用して作成したユニバースに適用されます。 ここに挙げられている権限は、ユニバースのみに適用される種類固有の権限、またはユニバースのコンテキストで固有の意味を持つ一般的な権限です。

> ⓘ 注記
>
> ユニバースのアクセス権は、ユニバースデザインツールアプリケーションの CMS からユニバースをインポートしたときにのみ適用されます。 これらの権限は、ユニバースがローカルディスクに保存されているときには適用されません。

権限	説明
オブジェクトをフォルダに追加する	ユニバースに制限セットまたはオブジェクトを追加できるようにします。 そのためには、アクセス制限の編集権限も必要になります。
オブジェクトを表示する	ユニバースのアクセスおよび表示ができるようにします。
オブジェクトを編集する	この権限によって、次の操作が実行できるようになります。 • CMC またはユニバースデザインツールでユニバースを編集します。 • ユニバースをロックまたはロック解除する。 ユニバースのロックを解除するには、ユニバースのロック解除権限も必要になります。
オブジェクトを削除する	ユニバースを削除できるようにします。
オブジェクトの翻訳	トランスレーションマネジメントツールを使用して、翻訳されたユニバースオブジェクト名を保存できるようにします。

権限	説明
	注記 オブジェクトの編集権限が明示的に付与され、オブジェクトの翻訳権限が明示的に拒否されていない場合、翻訳を保存できます。
値の一覧の新規作成	この権限によって、次の操作が実行できるようになります。 • 新しい値の一覧をオブジェクトと関連付ける。 • 既存の値の一覧を編集する。 **注記** この権限では、カスケード値の一覧の作成は制限されません。
ユニバースの印刷	ユニバースを印刷できるようにします。
テーブル、オブジェクト値の表示	ユニバースのテーブルまたはオブジェクトと関連付けられた値を表示できるようにします。
アクセス制限の編集	ユニバースに対するアクセス制限(オーバーロード)を編集できるようにします。
ユニバースのロック解除	次の操作を実行できるようにします。 • ユニバースが他のユーザによってロックされている場合にそれを解除する。 • CMS からユニバースをエクスポートする。 ユニバースのロックを解除するには、オブジェクトを編集する権限も必要になります。
データアクセス	ユニバースからデータを取得して、ユニバースに基づいてドキュメントを最新表示できるようにします。 そのためには、ユニバースデザインツールアプリケーション、ドキュメント、ユニバース接続に対するこの権限も必要になります。
ユニバースに基づいたクエリの作成と編集	ユニバースに基づいて、ドキュメントを作成し、クエリを編集できるようにします。

34.3.8 ユニバース (.unx) のアクセス権

このセクションの権限は、インフォメーションデザインツールまたは.unv ユニバースを使用して作成したユニバースに適用されます。 ここに挙げられている権限は、ユニバースのみに適用される種類固有の権限、またはユニバースのコンテキストで固有の意味を持つ一般的な権限です。

> **注記**
>
> ユニバースのアクセス権は、リポジトリに対し公開されたユニバースにのみ適用されます。 これらの権限は、ユニバースがローカルフォルダに保存されているときには適用されません。

権限	説明
オブジェクトを表示する	ユニバースのアクセスおよび表示ができるようにします。
オブジェクトを編集する	ユニバースを再公開できるようにします。
オブジェクトを削除する	ユニバースを削除できるようにします。
ユニバースの取得	インフォメーションデザインツールで公開されたユニバースを取得したり、基になるリソース (ビジネスレイヤおよびデータファンデーション) を編集できるようにします。 **注記** インフォメーションデザインツールアプリケーションのユニバースの取得権限も付与されている必要があります。
セキュリティプロファイルの編集	インフォメーションデザインツールセキュリティエディタで、ユニバースのセキュリティプロファイルを挿入、編集、削除できるようにします。 **注記** この権限は、セキュリティプロファイルの表示やセキュリティプロファイルの集計オプションの変更には必要ありません。
セキュリティプロファイルの割当	インフォメーションデザインツールセキュリティエディタで、ユーザおよびグループにセキュリティプロファイルを割り当てたり、割当を解除できるようにします。
データアクセス	ユニバースからデータを取得して、ユニバースに基づいてドキュメントを最新表示できるようにします。 インフォメーションデザインツールでは、この権限で、クエリパネルの結果セットをプレビューできるようになります。
ユニバースに基づくクエリの作成と編集	ユニバースに基づいて、クエリを作成、編集できるようにします。 インフォメーションデザインツールでは、この権限でクエリパネルを開き、ユニバースにクエリを実行できるようになります。
すべてのユーザ用に保存	すべてのユーザ用にユニバースを保存できるようにします。

権限	説明
	ⓘ 注記 インフォメーションデザインツールアプリケーションのすべてのユーザ用に保存権限も付与されている必要があります。

34.3.9 ユニバースオブジェクトのアクセスレベル

デザイナがユニバースデザインツールを使用してユニバースを作成する場合、または、インフォメーションデザインツールを使用してビジネスレイヤを作成する場合、デザイナは、ユニバースのすべてのオブジェクトにオブジェクトのアクセスレベルを割り当てます。オブジェクトのアクセスレベルは次のとおりです。

パブリック (デフォルト)
コントロール
リストリクト
コンフィデンシャル
プライベート

ユニバースをリポジトリで公開したら、アプリケーションで割り当てられたオブジェクトのアクセスレベルに基づいてユニバースオブジェクトへのアクセス権を付与できます。たとえば、Everyone グループにパブリックアクセス権を付与できます。これにより、Everyone グループにいるユーザは、パブリックと指定されたユニバース内のオブジェクトを表示できます。

各オブジェクトのアクセスレベルは、オブジェクトに対して以前よりも多くのアクセスを許可します。パブリックは最低レベルです。パブリックアクセスが付与された主体は、パブリックと指定されたオブジェクトしか表示できません。コントロールアクセスを付与された主体は、パブリックおよびコントロールに指定されたオブジェクトを表示できます。プライベートは、最高レベルの設定で、すべてのオブジェクトアクセスレベル、つまりユニバースのすべてのオブジェクトへのアクセス権を主体に付与します。

> ⓘ 注記
> オブジェクトのアクセスレベルのセキュリティ設定は、ユニバースが継承したすべてのセキュリティ設定より優先されます。

> ⓘ 注記
> .unx ユニバースでは、オブジェクトアクセスレベルセキュリティ設定が、セキュリティプロファイルによって定義されたオブジェクトセキュリティの考慮に入れられます。セキュリティプロファイルの詳細については、インフォメーションデザインツールユーザガイドを参照してください。

関連情報

ユニバースオブジェクトのアクセスレベルの割当 [1099 ページ]

34.3.9.1 ユニバースオブジェクトのアクセスレベルの割当

ユニバースオブジェクトのアクセスレベルのセキュリティを設定するには、そのユニバースに対する [オブジェクトに対するユーザの権限を変更する] 権限が必要になります。

1. CMS の [ユニバース] 領域で、ユニバースを選択します。
2. アクション > ユニバースセキュリティ をクリックします。
3. [ユニバースセキュリティ] ダイアログボックスの [オブジェクトレベルセキュリティ] リストでユーザまたはグループに対するオブジェクトアクセスレベルを選択します。

34.3.10 接続のアクセス権

このセクションの権限は、ユニバース接続に適用される種類固有の権限、またはユニバース接続のコンテキストで固有の意味を持つ一般的な権限です。これらの権限は、リポジトリで公開されている接続に適用されます。

リレーショナル接続のアクセス権

権限	説明
オブジェクトを表示する	接続を表示できるようにします。
オブジェクトを編集する	接続パラメータを編集できるようにします。
接続をローカルにダウンロード	Web Intelligence リッチクライアント内の接続で作成されたユニバースを、オフラインモードで使用できるようにします。 インフォメーションデザインツールで、ローカルのミドルウェアドライバを使用できるようにします。これを行うには、インフォメーションデザインツールの基本設定でローカルミドルウェアオプションを選択します。選択しない場合は、データベースに対するクエリでサーバのミドルウェアが使用されます。 この権限は、インフォメーションデザインツールでセキュリティ保護された接続を編集する場合にも必要です。
オブジェクトを削除する	接続を削除できるようにします。
オブジェクトを別のフォルダにコピーする	あるフォルダから他のフォルダに接続をコピーできるようにします。
データアクセス	接続に対して指定されたデータベースからコンテンツを取得できるようにします。 インフォメーションデザインツールでは、この権限で、接続およびデータファンデーションエディタからテーブルデータ

権限	説明
	を参照できるようになります。また、クエリパネルの結果セットをプレビューすることもできます。
ストアドプロシージャの接続を使用	ユニバース接続に対して指定されたデータベースでストアドプロシージャを使用できるようになります。 **注記** この権限は、.unv ユニバースのみに適用されます。
SQL 文の直接入力の接続を使用	接続で SQL スクリプトを実行できるようにします。

OLAP 接続のアクセス権

権限	説明
オブジェクトを表示する	接続を表示できるようにします。
オブジェクトを編集する	インフォメーションデザインツール接続エディタで接続パラメータを編集できるようにします。
オブジェクトを削除する	接続を削除できるようにします。
オブジェクトを別のフォルダにコピーする	あるフォルダから他のフォルダに接続をコピーできるようにします。
接続をローカルにダウンロード	Web Intelligence リッチクライアント内の接続で作成されたユニバースを、オフラインモードで使用できるようにします。

34.3.11 アプリケーション

34.3.11.1 CMC

権限	説明
CMC にログオンしてこのオブジェクトを *CMC* で参照する	CMC にログオンできるようにします
インスタンスマネージャへのアクセスを許可する	インスタンスマネージャにアクセスできるようにします
関係クエリへのアクセスを許可する	CMC で関係クエリを実行できるようにします
セキュリティクエリへのアクセスを許可する	CMC でセキュリティクエリを実行できるようにします

34.3.11.2 Fiori 対応 BI ラウンチパッド

権限	説明
新しい Fiori 対応 BI ラウンチパッドへのログオン	Fiori 対応 BI ラウンチパッドにログオンできるようにします。
整理	オブジェクトの移動とコピー、`Favorites` フォルダへのオブジェクトの追加、およびオブジェクトのショートカット作成を実行できるようにします。
BusinessObjects 受信ボックスに送信	受信者の BI 受信ボックスにオブジェクトを送信できるようにします。
電子メールの出力先に送信	電子メールで受信者にオブジェクトを送信できるようにします。
ファイルの場所に送信	ファイルの場所にオブジェクトを送信できるようにします。
FTP の場所に送信	FTP の場所にオブジェクトを送信できるようにします。
SFTP の場所に送信	SFTP の場所にオブジェクトを送信できるようにします。 SFTP 出力先のプロパティは、FTP 出力先ページに似ていますが、ユーザによる入力が必要な追加フィンガープリントオプションがあります。各 SFTP サーバのプロパティにはフィンガープリントオプションがあります。フィンガープリントの一致/検証は、CMS によってバックエンドで実行されます。

34.3.11.2.1 コラボレーションアプリケーションのアクセス権

これらのアクセス権は、アプリケーションが BI プラットフォームで設定されるときに、SAP Jam に適用されます。

権限	説明
ユーザが所有するドキュメントのコメント	自分の所有するドキュメントおよびインスタンスにコメントできるようにします
ユーザが所有するドキュメントのコメントを表示	自分の所有するドキュメントおよびインスタンスのコメントを表示できるようにします
ユーザが所有するオブジェクトの基本設定の変更	アプリケーションオブジェクトの [基本設定] メニューを表示します。 このアクセス権がないと、ユーザはどのアプリケーションでも個人用の基本設定を設定できず、基本設定メニューがアプリケーションに表示されません。たとえば、この権限がない

権限	説明
	と、ユーザはアプリケーションのレポートで使用する測定単位 (インチまたはミリメートル) を選択できません。

34.3.11.3 BI ワークスペース

権限	説明
BI ワークスペースの作成および編集	新しい BI ワークスペースを作成でき、既存の BI ワークスペースを編集できるようにします
モジュールの作成と編集	新しいモジュールを作成でき、既存のモジュールを編集できるようにします
BI ワークスペースの編集	既存の BI ワークスペースを編集できるようにします (ただしワークスペースを新規作成できるようにはしません)
ユーザが所有するオブジェクトの基本設定の変更	アプリケーションオブジェクトの基本設定メニューを表示します このアクセス権がないと、ユーザはどのアプリケーションでも個人用の基本設定を設定できず、基本設定メニューがアプリケーションに表示されません。 たとえば、この権限がないと、ユーザは Web Intelligence または BI ラウンチパッドアプリケーションのレポートで使用する測定単位 (インチまたはミリメートル) を選択できません。

34.3.11.4 Web Intelligence

このセクションのアクセス権は、リッチクライアントを含む Web Intelligence アプリケーションに適用され、このアプリケーションのビューアとクエリパネルに影響することがあります。

権限	説明
データ: データ追跡の有効化	変更されたデータを追跡できるようにします。
データ: 変更済みデータの書式設定有効化	変更されたデータの書式設定を選択できるようにします。
全般:デスクトップクライアントアクセスの有効化	Web Intelligence デスクトップ (リッチクライアント) を使用できるようにします。
デスクトップ: ドキュメントのエクスポート	Web Intelligence リッチクライアントで、ユーザは BI プラットフォームリポジトリにドキュメントをエクスポートできます。

権限	説明
デスクトップ: すべてのユーザ用にドキュメントを保存	Web Intelligence リッチクライアントにおいて、ユーザはセキュリティなしでドキュメントをローカルに保存することができます。
ドキュメント: 起動時の自動最新表示を無効にする	ドキュメントを開いたときに自動更新されないようにします。
ドキュメント: 自動保存の有効化	管理者が CMC で自動保存を有効にしている場合、ドキュメントが自動的に保存されるようにします。
ドキュメント: 作成の有効化	新しいドキュメントを作成できるようにします。
一般: Web Intelligence 基本設定の編集	BI ラウンチパッドで Web Intelligence の基本設定を変更できるようにします。
一般: Web クライアントアクセスの有効化	Web Intelligence Web クライアントを使用できるようにします。
クエリ: ユニバースから生成されたスクリプトの編集	クエリパネルで、ユニバースから生成された SQL または MDX クエリスクリプトを編集できるようにします。
クエリ: SQL スクリプトの直接入力編集	直接入力の SQL クエリスクリプトを編集できるようにします。
クエリ: クエリ: ユニバースから生成されたスクリプトの表示	クエリパネルで、ユニバースから生成された SQL または MDX クエリスクリプトを表示できます。
クエリ: SQL の直接入力表示	直接入力の SQL クエリスクリプトを表示できます。
レポーティング: ブレークの作成と編集	ブレークを作成および編集できるようにします。
レポーティング: 条件付き書式設定ルールの作成と編集	条件付き書式設定ルールを作成および編集できるようにします。
レポーティング: 定義済みの計算の作成と編集	定義済みの計算を作成および編集できるようにします。
レポーティング: 入力コントロールおよびグループの作成と編集	入力コントロールを作成および編集できるようにします。
レポーティング: フィルタの作成と編集および入力コントロールの使用	レポートフィルタを作成および編集できるようにします。また、入力コントロールを使用できるようにします。
レポーティング: 並べ替えおよびランキングの作成と編集	並べ替えとランキングを作成および編集できるようにします。
レポーティング: 式、変数、グループ、および参照の作成	式、変数、グループ、および参照を作成できるようにします。
レポーティング: ドキュメント変更を有効にする	レポートの書式設定を編集できるようにします。このアクセス権がないと、デザインモードは使用できません。
レポーティング: オブジェクトのマージ	レポートおよびデータマネージャで、結合ディメンションを使用してデータを同期化できるようにします。
レポーティング: レポート、テーブル、チャート、セルの作成と編集	• レポート、テーブル、チャート、セルを挿入および削除できるようにします。 • ワークフローを複製 (コピー/貼り付け) できるようにします。

34.3.11.5 ユニバースデザインツール

権限	説明
ユニバースの整合性をチェック	ユニバースの整合性をチェックできるようにします
構造ウィンドウの最新表示	構造ウィンドウを最新表示できるようにします
テーブル参照の使用	テーブル参照を使用してデータベースのデータを表示できるようにします
ユニバース制約の適用	インポートしたユニバースのユーザに事前定義されたユニバース制約を適用できるようにします
ユニバースのリンク	2 つのユニバースをリンクしてコンポーネントを共有できるようにします
接続の作成、変更、または削除	BI プラットフォームリポジトリに格納されているか、個人用接続または共有接続として格納されているユニバース接続を作成、変更、削除できるようにします。
ユーザが所有するオブジェクトの基本設定の変更	アプリケーションオブジェクトの基本設定メニューを表示します このアクセス権がないと、ユーザはどのアプリケーションでも個人用の基本設定を設定できず、基本設定メニューがアプリケーションに表示されません。 たとえば、この権限がないと、ユーザは Web Intelligence または BI ラウンチパッドアプリケーションのレポートで使用する測定単位 (インチまたはミリメートル) を選択できません。

34.3.11.6 インフォメーションデザインツール

権限	説明
セキュリティプロファイルの管理	セキュリティエディタを開けるようにします セキュリティプロファイルを操作するには、ユニバースに対する権限も必要です。
プロジェクトの共有	ローカルプロジェクトを共有して、共有プロジェクトとローカルプロジェクトを同期化できるようにします
接続の作成、変更、または削除	• 公開済みリソースビューからセキュリティ接続を作成および削除できるようにします • 接続エディタで接続を編集できるようにします • 接続をリポジトリに公開できるようにします

権限	説明
ユニバースの公開	ユニバースをリポジトリに公開できるようにします
ユニバースの取得	公開済みのユニバースを、編集予定のローカルプロジェクトに取得できるようにします
すべてのユーザ用に保存	ユニバースの取得時に、すべてのユーザ用に保存できるようにします
統計の計算	統計を計算して公開するテーブルと列を選択できるようにします
ユーザが所有するオブジェクトの基本設定の変更	アプリケーションオブジェクトの基本設定メニューを表示します このアクセス権がないと、ユーザはどのアプリケーションでも個人用の基本設定を設定できず、基本設定メニューがアプリケーションに表示されません。 たとえば、この権限がないと、ユーザは Web Intelligence または BI ラウンチパッドアプリケーションのレポートで使用する測定単位 (インチまたはミリメートル) を選択できません。

34.3.11.7 アラート

権限	説明
アラートのトリガ	アラートイベントをトリガできるようにします。 ドキュメントに対してアラートをトリガするには、次の追加権限が必要です。 • ドキュメントに対する "表示" および "スケジュール" 権限 • 関連イベントに対する "表示" および "トリガ" 権限
オブジェクトの購読	アラートイベントを購読できるようにします。 イベントを購読するには、次の追加権限が必要です。 • 関連イベントに対する "表示" 権限 • ユーザ自身のアカウントに対する "購読" 権限 ドキュメントのアラートを購読するには、次の追加権限が必要です。 • ドキュメントに対する "表示" 権限 • ドキュメントに対する "インスタンスの表示" 権限 • 関連イベントに対する "表示" 権限 • ユーザ自身のアカウントに対する "購読" 権限

権限	説明
ユーザが所有するオブジェクトの基本設定の変更	アプリケーションオブジェクトの基本設定メニューを表示します このアクセス権がないと、ユーザはどのアプリケーションでも個人用の基本設定を設定できず、基本設定メニューがアプリケーションに表示されません。 たとえば、この権限がないと、ユーザは Web Intelligence または BI ラウンチパッドアプリケーションのレポートで使用する測定単位 (インチまたはミリメートル) を選択できません。

34.3.11.8 SAP BusinessObjects Mobile

権限	説明
SAP BusinessObjects Mobile アプリケーションへのログオン	モバイルアプリケーションから BI プラットフォームにログオンして、ドキュメントを表示できるようにします
ドキュメントアラートの購読	ドキュメントおよび繰り返されるインスタンスのアラートを購読できるようにします 過去にこの権限を許可されたことがあるユーザは、現在は許可されていなくても、購読されたアラートを引き続き受信できます。 アラートの受信を希望しない場合は、明示的にアラートを購読解除する必要があります。 スケジュールに対するドキュメントアラートおよび繰り返しインスタンスを購読するには、CMC のイベントの下の `System Events` フォルダへの "フルコントロール" アクセス権が必要です。
デバイスのローカルストアへのドキュメントの保存	モバイルデバイスにドキュメントを保存できるようにします 過去に "デバイスでのドキュメントのローカル保存" 権限を許可されていて (現在は許可されていなくても)、モバイルデバイスにドキュメントを保存したことがあり、そのドキュメントがまだデバイス上に存在していても、そのドキュメントは同期プロセスで同期化されません。
デバイスからドキュメントを電子メールとして送信	電子メールメッセージでレポートを送信できるようにします
ユーザが所有するオブジェクトの基本設定の変更	アプリケーションオブジェクトの基本設定メニューを表示します このアクセス権がないと、ユーザはどのアプリケーションでも個人用の基本設定を設定できず、基本設定メニューがアプリケーションに表示されません。 たとえば、この権限がない

権限	説明
	と、ユーザは Web Intelligence または BI ラウンチパッドアプリケーションのレポートで使用する測定単位 (インチまたはミリメートル) を選択できません。

詳細については、*SAP BusinessObjects Mobile* のインストールとデプロイメントガイドを参照してください。

34.3.11.9 BI 管理コックピット

権限	説明
BI 管理コックピットへのアクセスを許可する	CMC の BI 管理コックピットにアクセスできます。
モニタリングへのアクセスを許可する	BI 管理コックピットでモニタリングにアクセスできます。
Visual Difference へのアクセスを許可する	BI 管理コックピットで Visual Difference にアクセスできます。
Visual Difference - 比較の作成	Visual Difference で情報オブジェクト間の新しい比較を作成できます。
Visual Difference - 比較の削除	Visual Difference で前の比較を削除できます。
Visual Difference - 比較の再実行	Visual Difference で以前に作成した比較を再度実行できます。
Visual Difference - 比較の表示	Visual Difference で比較を表示できます。

35 サーバのプロパティに関する付録

35.1 サーバのプロパティに関する付録について

このサーバのプロパティに関する付録では、各 BI プラットフォームサーバに設定可能なプロパティをその説明とともに示しています。

35.1.1 共通サーバのプロパティ

この節で説明するサーバプロパティは、すべての種類のサーバに適用されます。

リクエストポートのプロパティ

プロパティ	説明	デフォルト値
サーバ名	サーバの名前です。	デフォルト値は、サーバが存在しているノードの名前にサーバの名前を追加したものです。
ID、*CUID*	サーバの短い ID とクラスタの一意の ID です。 読み取り専用。	これらの値は自動生成されます。
ノード	サーバが配置されているノードの名前。	この値は、インストール時に指定します。
説明	サーバの説明。	デフォルト値はサーバの名前です。
コマンドラインパラメータ	サーバ用のコマンドラインパラメータです。	デフォルト値はサーバの種類によって異なります。
リクエストポート	サーバがリクエストを受信するポートを指定します。 ファイアウォールを使用する環境では、サーバがファイアウォールで開かれているポートでのみリクエストを受信待機するように設定します。 サーバにポートを指定する場合は、ポートがすでに他のプロセスによって使用されていないことを確認してください。 **注記** [自動割り当て] が選択されている場合、サーバは動的に割り当てられたポートにバインドされます。 これは、サーバが再起動するたびにランダムなポート番号がサーバに割り当てられることを意味しています。	デフォルトでは、[自動割り当て]は{**TRUE**}に設定され、[リクエストポート]は空になります。

プロパティ	説明	デフォルト値
自動割り当て	サーバが再起動するたびに、動的に割り当てられたポートにサーバをバインドするかどうかを指定します。 サーバを特定のポートにバインドする場合は、[自動割り当て]を「**FALSE**」に設定し、有効な [リクエストポート] を指定します。	デフォルト値は「**TRUE**」です。

自動起動プロパティ

プロパティ	説明	デフォルト値
Server Intelligence Agent の起動時にこのサーバを自動的に起動します	Server Intelligence Agent(SIA)が起動または再起動したときに、サーバも自動的に起動するようにするかどうかを指定します。 この値を「**FALSE**」に設定して SIA を起動または再起動すると、サーバは停止した状態のままになります。	デフォルト値は「**TRUE**」です。

ホスト識別子のプロパティ

プロパティ	説明	デフォルト値
自動割り当て	自動的に割り当てられたネットワークインタフェースにサーバをバインドするかどうかを指定します。 「**FALSE**」に設定すると、サーバは特定のネットワークインタフェースにバインドされます。「**TRUE**」に設定すると、サーバは使用可能な最初の IP アドレスのリクエストを受け入れます。 マルチホームマシンでは、この値を「**FALSE**」に設定し、有効なホスト名または IP アドレスを指定することで、バインドする特定のネットワークインタフェースを指定できます。	デフォルト値は{**TRUE**}です。
ホスト名	サーバのバインド先のネットワークインタフェースのホスト名。ホスト名が指定されると、サーバは、ホスト名に関連付けられたすべての IP アドレスでリクエストを受け入れます。	デフォルトでは、[自動割り当て] は「**TRUE**」に設定され、[ホスト名] は空になります。
IP アドレス	サーバのバインド先のネットワークインタフェースの IP アドレス。 IPv4 および IPv6 の両方のプロトコルがサポートされます。IP アドレスが指定されている場合、サーバは、その IP アドレスのみでリクエストを受け入れます。	デフォルトでは、[自動割り当て] は **TRUE** に設定され、[*IP* アドレス] は空になります。

設定テンプレートのプロパティ

プロパティ	説明	デフォルト値
設定テンプレートの使用	設定テンプレートを使用するかどうかを指定します。	デフォルト値は、「**FALSE**」です。
システムデフォルトの復元	このサーバに対して元のデフォルト設定を復元するかどうかを指定します。	デフォルト値は「**FALSE**」です。
設定テンプレートの設定	同じ種類のすべてのサービスに対する設定テンプレートとして現在のサーバの設定を使用するかどうかを指定します。 「**TRUE**」に設定すると、[設定テンプレートの使用]で指定した同じ種類のすべてのサービスが、現在のサービスの設定を使用するようにすぐに再設定されます。	デフォルト値は「**FALSE**」です。

トレースログサービスのプロパティ

プロパティ	説明	デフォルト値
ログレベル	記録されるメッセージの重大度の下限を指定し、サーバのログファイルに記録する情報量を決定します。 使用できるログしきい値レベルは、次のとおりです。 • 指定なし • なし • 低 • 中 • 高	デフォルト値は「**指定なし**」です。

35.1.2 コアサービスのプロパティ

コアサービスカテゴリには、次のサーバが含まれます。

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Event Server
- Input File Repository Server
- Output File Repository Server
- Web アプリケーションコンテナサーバ

Adaptive Job Server のプロパティ

一般プロパティ

プロパティ	説明	デフォルト値
一時ディレクトリ	必要な場合に一時ファイルが作成されるディレクトリを指定します。このディレクトリに十分なディスク領域がない場合、パフォーマンスの問題が発生する場合があります。パフォーマンスを改善するには、このディレクトリがローカルディスクにあることを確認してください。 **注記** 変更を有効にするには、サーバを再起動する必要があります。	%DefaultDataDir%

Adaptive Job Server は、多くの異なるサービスをホストできます。各サービスには次のプロパティがあります。

サービスプロパティ

プロパティ	説明	デフォルト値
同時に実行可能なジョブの最大数	サーバが許可する同時に実行可能な独立したプロセス(子プロセス)の数を指定します。レポーティング環境に応じて、ジョブの最大数を調節できます。 デフォルト設定は、ほとんどのレポーティングシナリオで使用できます。各ユーザのレポーティング環境に最適な設定は、ハードウェア構成、データベースソフトウェア、およびレポート要件によって異なります。	5
子の要求の最大数	子が再起動前に処理するジョブ数を示します。	100

Adaptive Processing Server のプロパティ

一般プロパティ

プロパティ	説明	デフォルト値
サービスの起動のタイムアウト(秒単位)	サーバがサービスの開始を待機する時間を秒単位で指定します。 指定された時間内にサービスが開始できない場合、2 つの理由が考えられます。 • サービスが失敗した場合。データベースなどの必要なリソースが見つからなかったり、サービスでポートの競合が発生するなどの原因が考えられます。 • サービスが指定された時間内に開始されなかった場合。システムの速度が遅すぎるなどの原因が考えられます。 理由を特定するためには、サーバのログファイルを確認してください。サービスが指定された時間内に開始されなかった場合は、この値を増やすことを検討してください。	1200

クライアント監査プロキシサービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

セキュリティトークンサービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

Insight to Action サービスのプロパティ

メトリクス	説明	
各ユーザセッションのアクティブな接続の最大数	指定された時間にユーザが使用可能な SAP サーバとの接続の最大数。ユーザが RRI 可能なレポートまたはダッシュボードを開くと、使用可能な RRI ターゲットを決定するために SAP サーバとの接続が確立されます。	20
各ユーザセッションのアイドル接続の最大数	後続の RRI 要求用に開放して再使用するアイドル接続の数。この設定を増やすと、システムリソースが追加で割り当てられます。	20
最大接続待機時間 (秒単位)	Insight to Action フレームワークの合計時間は、タイムアウト (秒単位) する前に SAP Server からの応答を待つ必要があります。	30

公開サービスのプロパティ

プロパティ	説明	デフォルト値
スレッドプールサイズ	同時に実行できるスコープバッチの処理スレッド数を指定します。プロパティの値が “0” に設定されている場合、スレッドプールサイズは、現在のマシン内の CPU コア数に基づく式を使用して決定されます。	0

翻訳サービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

モニタリングサービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

プラットフォーム検索サービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

パブリッシングポスト処理サービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

Central Management Server のプロパティ

> **注記**
>
> これらのサーバのプロパティのいずれかを変更する場合、変更を有効にするにはサーバを再起動する必要があります。

Central Management Service のプロパティ

プロパティ	説明	デフォルト値
ネームサーバポート	CMS が最初のネームサービスリクエストを受信待機するポートを指定します。	6400
要求されたシステムデータベース接続	CMS が確立を試みる CMS システムデータベースへの接続数を指定します。リクエストされたすべてのデータベース接続をサーバが確立できない場合、CMS は機能し続けますが、同時に処理できるリクエスト数が減るため、パフォーマンスは低下します。CMS は、リクエストされた接続数に達するまで、追加の接続を確立しようとします。 CMS の [確立されたシステムデータベース接続] メトリクスは、現在の確立された接続数を示します。	14
システムデータベースへの自動再接続	サービスが中断された場合に、CMS が CMS データベースとの接続を自動的に再確立するかどうかを指定します。この値を **FALSE** に設定すると、処理を再開する前に CMS データベースの整合性を確認できます。データベース接続を再確立するには、CMS を再起動する必要があります。	**TRUE**

シングルサインオンサービスのプロパティ

プロパティ	説明	デフォルト値
シングルサインオンの有効期限 (秒単位)	有効期限までのデータソースへの SSO 接続の有効時間 (秒単位) を指定します。これは、データソースへの Windows AD SSO に対して設定されたレポートを実行する、Windows AD ユーザに適用されます。	86400

Event Server のプロパティ

イベントサービスのプロパティ

プロパティ	説明	デフォルト値
イベントポーリング間隔 (秒単位)	イベントを生成するファイルに対してサーバでポーリングを行う頻度を秒単位で指定します。	10 許可される値の範囲は 1 ～ 1200 秒です。
クリーンアップ間隔 (分単位)	クリーンアップユーティリティの実行頻度を分単位で指定します。	20

Input File Repository Server のプロパティ

Input Filestore サービスのプロパティ

プロパティ	説明	デフォルト値
ファイル格納ディレクトリ	リポジトリオブジェクトが保存されるディレクトリを指定します。 **注記** このディレクトリに十分なディスク領域がない場合、パフォーマンスの問題が発生する場合があります。	%DefaultInputFRSDir/%
一時ディレクトリ	必要な場合に一時ファイルが作成されるディレクトリを指定します。 **注記** このディレクトリに十分なディスク領域がない場合、パフォーマンスの問題が発生する場合があります。よりよいパフォーマンスのために、[一時ディレクトリ] の場所は [ファイル格納ディレクトリ] と同じファイルシステムにすることをお推めします。	%DefaultInputFRSDir/temp%
最大アイドル時間 (分)	サーバが非アクティブな接続を閉じるまでに待機する時間の長さを指定します。設定値が短すぎると、ユーザのリクエストが途中で終了する場合があります。設定値が長すぎると、処理時間やディスク領域などのシステムリソースが過剰に消費される場合があります。	10
ファイルアクセスの最大試行回数	サーバがファイルへのアクセスを試行する回数を指定します。	1
ウィルススキャンアダプタファイルの場所	ウィルススキャンアダプタファイルの場所の絶対パスを指定します。	

Output File Repository Server のプロパティ

Output Filestore サービスのプロパティ

プロパティ	説明	デフォルト値
ファイル格納ディレクトリ	リポジトリオブジェクトが保存されるディレクトリを指定します。 **注記** このディレクトリに十分なディスク領域がない場合、パフォーマンスの問題が発生する場合があります。	%DefaultOutputFRSDir/%

プロパティ	説明	デフォルト値
一時ディレクトリ	必要な場合に一時ファイルが作成されるディレクトリを指定します。 **注記** このディレクトリに十分なディスク領域がない場合、パフォーマンスの問題が発生する場合があります。	%DefaultOutputFRSDir/temp%
最大アイドル時間 (分)	サーバが非アクティブな接続を閉じるまでに待機する時間の長さを指定します。設定値が短すぎると、ユーザのリクエストが途中で終了する場合があります。設定値が長すぎると、処理時間やディスク領域などのシステムリソースが過剰に消費される場合があります。	10
ファイルアクセスの最大試行回数	サーバがファイルへのアクセスを試行する回数を指定します。	1

Web アプリケーションコンテナサーバのプロパティ

一般プロパティ

プロパティ	説明	デフォルト値
サービスの起動のタイムアウト(秒単位)	WACS がホストしているサービスの起動をタイムアウトまで待機する時間の長さを指定します。タイムアウトが経過すると、WACS は開始されていないサービスを提供しません。低速のマシンでは、大きな値を指定することをお勧めします。 指定した時間が短すぎて、WACS がタイムアウトまでに起動しない場合は、セントラル設定マネージャ(CCM)を通じて WACS のデフォルト設定を復元します。	1200

トレースログサービスのプロパティ

プロパティ	説明	デフォルト値
ログレベル	ロギングを有効にし、重大度および詳細のレベルを [なし] (重大なイベントのみを記録)、[低] (スタートアップ、シャットダウン、開始と終了の要求メッセージ)、[中] (エラー、警告、およびほとんどのステータスメッセージ)、または [高] (除外なし。デバッギングでのみ使用します。CPU 使用量が増加し、パフォーマンスに影響が及ぶ場合があります) に設定します。 選択可能なメニューは次のとおりです。 • 指定なし • なし • 低 • 中 • 高	指定なし

ビジネスプロセス BI サービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

クエリビルダサービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

RESTful Web サービス - システムプロパティ設定プロパティ

プロパティ	説明	デフォルト値
エラースタックの表示	このプロパティを有効にすると、エラーログにデバッグ用の RESTful Web サービスエラーメッセージが含まれます。デバッグ以外の目的では使用しないようにしてください。また、BI プラットフォームの詳細が表示されるなどのセキュリティの問題がある場合にも使用しないようにしてください。	未選択
1 ページあたりのデフォルトオブジェクト数	1 ページにリストされるエントリ数です。開発者は、RESTful Web サービス SDK の &pageSize=<m> パラメータを使用してこの設定を上書きできます。	50
Enterprise セッショントークンのタイムアウト *(*分単位*)*	ログオントークンが有効状態を維持する時間です。この時間を過ぎると、新しいログイントークンを生成する必要があります。	60
セッションプールサイズ	サーバパフォーマンスの向上のために使用される、キャッシュされたセッションを一度に格納できる数です。セッションプールはアクティブな RESTful Web サービスセッションをキャッシュします。これにより、ユーザは、HTTP 要求ヘッダで同じログオントークンを使用する別の要求を送信する場合にこれらのセッションを再利用できます。	1000
セッションプールタイムアウト *(*分*)*	キャッシュされたセッションの有効時間を分単位で表します。	2
HTTP Basic 認証を有効にする	この設定を有効にしない場合、RESTful Web サービス要求ではログオントークンを使用する必要があります。この設定を有効にする場合、ユーザは最初に RESTful Web サービス要求を実行するときにユーザ名およびパスワードを入力する必要があります。有効にすると、[デフォルトの *HTTP Basic* 用認証スキーマ] ドロップダウンメニューが表示されます。	未選択

プロパティ	説明	デフォルト値
デフォルトの *HTTP Basic* 用認証スキーマ	[*HTTP Basic* 認証を有効にする] を選択すると、4 つの認証タイプのいずれかを選択できます。HTTPS オプションを使用している場合を除き、名前およびパスワードはプレーンテキストで送信されます。 指定できる値は次のとおりです。 • *secEnterprise* • *secDAP* • *SAPR3* • *secWinAD*	空白。ただし、[*HTTP Basic* 認証を有効にする] が選択されている場合は、デフォルトで [*secEnterprise*] になります。

RESTful Web サービス - クロスオリジンリソース共有設定プロパティ

プロパティ	説明	デフォルト値
オリジンを許可する	この設定を有効にすると、CORS 対応ブラウザを使用しているユーザは、複数のドメイン名にアクセスする必要のある Java スクリプトページにアクセスできるようになります。各ドメイン名をカンマで区切って追加します。たとえば、http://origin1.server.com:8080, http://origin2.server.com:8080 のようにします。デフォルトで、ブラウザはすべてのドメインへのアクセスが許可されています (*)。	* (アスタリスク)
最大期間 (分)	ブラウザが HTTP 要求をキャッシュできる最大時間です。	1440

RESTful Web サービス - 信頼できる認証設定プロパティ

プロパティ	説明	デフォルト値
取得方法	これは、RESTful Web サービス API `/logon/trusted` を使用する場合に、信頼できる認証ログオントークンを取得するために使用するクエリメソッドを設定するメニューです。 • [*HTTP_HEADER*] は、要求ヘッダ accept=application/xml (または application/json) を使用する GET クエリで使用されます。 • [*QUERY_STRING*] は、RESTful Web サービス API を使用する URL クエリの末尾にログオン名を追加するのに使用します (例: /logon/trusted/?user=johndoe)。 • [*COOKIE*] は、Web ブラウザの Cookie からログイン名を取得する場合に使用します。ドメイン、名前、値、およびパスは Cookie に保存されている必要があります。	**HTTP_HEADER**
ユーザ名パラメータ	これは、ログオントークンを取得する目的で信頼できるユーザを識別するために使用するラベルです。	**X-SAP-TRUSTED-USER**

BOE Web アプリケーションサービスのプロパティ

プロパティの種類	説明	デフォルト値
認証の種類	BI ラウンチパッドにログオンするユーザの認証に使用される認証の種類。 指定できる値は次のとおりです。 • *AD Kerberos* • *AD Kerberos SSO* • *Enterprise* • *LDAP*	*Enterprise*
デフォルトの *AD* ドメイン	デフォルトの AD ドメインが使用されていると、ユーザはログインするときにドメインを指定する必要がありません。たとえば、デフォルトのドメインが “mydomain” に設定されている場合に、ユーザがユーザ名 “user” でログオンすると、Active Directory ログオン認証機関によって “user@mydomain.com” の認証が試行されます。	空白
サービスプリンシパル名	サービスプリンシパル名 (SPN) は、クライアントがサービスのインスタンスを一意に識別するために使用されます。Kerberos 認証サービスでは、SPN を使用してサービスを認証します。	空白
Keytab ファイル	Keytab ファイルへの完全パス。keytab ファイルを使用すると、Web アプリケーションマシンのユーザアカウントのパスワードが露出しないように Kerberos フィルタを設定できます。	空白

Web サービス SDK および QaaWS のプロパティ

プロパティ	説明	デフォルト値
Kerberos Active Directory のシングルサインオンの有効化	Web Services SDK および QaaWS で、Kerberos AD シングルサインオンを有効にするかどうかを指定します。	**FALSE**
デフォルトの *AD* ドメイン	デフォルトの Active Directory ドメインを使用すると、ユーザはドメインを指定しなくてもログインできます。	空白
サービスプリンシパル名	サービスプリンシパル名 (SPN) は、クライアントがサービスのインスタンスを一意に識別するために使用されます。Kerberos 認証サービスでは、SPN を使用してサービスを認証します。	空白
Keytab ファイル	Keytab ファイルへの完全パス。keytab ファイルを使用すると、Web アプリケーションマシンのユーザアカウントのパスワードが露出しないように Kerberos フィルタを設定できます。	空白

HTTP 設定プロパティ

プロパティ	説明	デフォルト値
すべての *IP* アドレスに連結	すべてのネットワークインタフェースに連結するかどうかを指定します。サーバに複数の NIC がある場合に特定のネットワークインタフェースにバインドするには、このプロパティをオフにします。	**TRUE**
ホスト名または *IP* アドレスに連結	HTTP サービスが提供されるネットワークインタフェース(IP アドレスまたはホスト名)を指定します。[すべての *IP* アドレスに連結]をオフにした場合にのみ値を指定できます。	`localhost`

プロパティ	説明	デフォルト値
HTTP ポート	HTTP サービスが提供されるポートを指定します。	6405 許可される値の範囲は 1 ～ 65535 です。
最大 *HTTP* ヘッダサイズ	要求および応答 HTTP ヘッダの最大許容サイズ (バイト単位)。	32768

プロキシプロパティ経由の HTTP の設定

プロパティ	説明	デフォルト値
プロキシ経由の *HTTP* の有効化	プロキシ経由の HTTP コネクタを WACS で有効にするかどうかを示します。通常、リバースプロキシを使用するデプロイメントでは有効化されます。	**FALSE**
すべての *IP* アドレスに連結	プロキシ経由の HTTP ポートをすべてのネットワークインタフェースにバインドするかどうかを示します。	**TRUE**
ホスト名または *IP* アドレスに連結	プロキシ経由の HTTP サービスが提供されるネットワークインタフェース(IP アドレスまたはホスト名)を指定します。[すべての *IP* アドレスに連結] をオフにした場合にのみ値を指定できます。	`localhost`
HTTP ポート	リバースプロキシデプロイメントで HTTP サービスが提供されるポートを指定します。[プロキシ経由の *HTTP* を有効にする]をオンにした場合にのみ値を指定できます。	6406 許可される値の範囲は 1 ～ 65535 です。
プロキシホスト名	IPv4 アドレス、IPv6 アドレス、ホスト名、またはプロキシサーバの完全修飾ドメイン名を指定します。[プロキシ経由の *HTTP* の有効化] をオンにした場合にのみ値を指定できます。	空白
プロキシポート	フォワードまたはリバースプロキシサーバのポート。[プロキシ経由の *HTTP* の有効化] をオンにした場合にのみ値を指定できます。	0 許可される値の範囲は 1 ～ 65535 です。
最大 *HTTP* ヘッダサイズ	要求および応答 HTTP ヘッダの最大許容サイズ (バイト単位)。	32768

HTTPS 設定プロパティ

プロパティ	説明	デフォルト値
HTTPS の有効化	HTTPS/SSL 通信を有効にするかどうかを示します。	**FALSE**
ホスト名または *IP* アドレスに連結	HTTPS サービスが提供されるネットワークインタフェース(IP アドレスまたはホスト名)を指定します。[*HTTPS* の有効化] をオンにした場合にのみ値を指定できます。	`localhost`
HTTPS ポート	HTTPS サービスが提供されるポートを指定します。[*HTTPS* の有効化] をオンにした場合にのみ値を指定できます。	443 許可される値の範囲は 1 ～ 65535 です。
プロキシホスト名	IPv4 アドレス、IPv6 アドレス、ホスト名、またはプロキシサーバの完全修飾ドメイン名を指定します。[*HTTPS* の有効化] をオンにした場合にのみ値を指定できます。	空白
プロキシポート	フォワードまたはリバースプロキシサーバのポート。[*HTTPS* の有効化] をオンにした場合にのみ値を指定できます。	0 許可される値の範囲は 1 ～ 65535 です。

プロパティ	説明	デフォルト値
プロトコル	使用する暗号化プロトコルを指定します。[*HTTPS の有効化*] をオンにした場合にのみ値を指定できます。	TLS 許可される値は TLS または SSL です。
証明書ストアのタイプ	証明書と秘密鍵が格納される証明書ストアのタイプです。多くの場合は、[*PCKS12*] になります。[*HTTPS の有効化*] をオンにした場合にのみ値を指定できます。	PKCS12 許可される値は PKCS12 または JKS です。
証明書ストアのファイルの場所	証明書ファイルの完全パス。[*HTTPS の有効化*] をオンにした場合にのみ値を指定できます。	空白
秘密鍵のアクセス用パスワード	PKCS12 証明書ストアと JKS キーストアの秘密鍵は、不正アクセスまたは盗用を防ぐためにパスワードで保護されています。WACS が証明書ストアの秘密鍵にアクセスできるように、証明書ストアを生成したときに指定したパスワードをここに入力します。[*HTTPS の有効化*] をオンにした場合にのみ値を指定できます。	空白
証明書のエイリアス	証明書ストア内の証明書のエイリアスです。この値を指定しなければ、複数の証明書が格納された証明書ストアを使用する場合に、ストア内の最初の証明書が使用されます。多くの場合、値を指定する必要はありません。[*HTTPS の有効化*] をオンにした場合にのみ値を指定できます。	空白
クライアント認証の有効化	クライアント認証を有効にすると、証明書信頼リストファイルに鍵が格納されているクライアントだけが WACS サービスを利用できます。その他のクライアントは拒否されます。クライアント認証は、[*HTTPS の有効化*] をオンにした場合にのみ有効にすることができます。	**FALSE**
証明書信頼一覧ファイルの場所	証明書信頼リストファイルのフルパス。[*HTTPS の有効化*] と [クライアント認証の有効化] をオンにした場合にのみ値を指定できます。	空白
証明書信頼一覧の秘密鍵のアクセス用パスワード	証明書信頼リストファイルの秘密鍵へのアクセスを保護するパスワードです。[*HTTPS の有効化*] と [クライアント認証の有効化] をオンにした場合にのみ値を指定できます。	空白
最大 *HTTP* ヘッダサイズ	要求および応答 HTTP ヘッダの最大許容サイズ (バイト単位)。	32768

同時接続のプロパティ (コネクタ別)

プロパティ	説明	デフォルト値
最大同時接続要求	各コネクタ(HTTP、プロキシ経由の HTTP、HTTPS)が同時に処理できる同時接続 HTTP または HTTPS 要求の数を指定します。	**150** 許可される値の範囲は 1 ～ 1000 です。

Active Directory の設定プロパティ

プロパティ	説明	デフォルト値
Krb5.ini ファイルの場所	Kerberos 設定プロパティを保存する `krb5.ini` ファイルの完全パスです。	空白
bscLogin.conf ファイルの場所	`bscLogin.conf` ファイルの完全パスです。	空白

35.1.3 接続サービスのプロパティ

接続サービスカテゴリには、次のサービスが含まれます。

- ネイティブ接続サービス(スタンドアロンサーバでのホスト)
- ネイティブ接続サービス(スタンドアロンサーバでの 32 ビットホスト)
- Adaptive Connectivity サービス (APS でのホスト)

すべてのサービスが同じ設定を共有します。

Excel データアクセスサービスのプロパティ

プロパティ	説明	デフォルト値
Excel データアクセスクリーンアップタイムアウト (秒)	クライアントのセッションのクリーンアップを実行する前に、非アクティブなクライアントをサービスが待機する時間を秒単位で指定します。	デフォルト値は 1200 秒です。
Excel データアクセススワップタイムアウト (秒)	クライアントのセッションをハードディスクにスワップする前に、非アクティブなクライアントをサービスが待機する時間を秒単位で指定します。 [*Excel データアクセスクリーンアップタイムアウト (秒)*] プロパティの値より低い値を指定することをお勧めします。	デフォルト値は 600 秒です。

サービス処理プロパティ

プロパティ	説明	デフォルト値
→ 注意 以下のサービス処理プロパティの変更後に、サーバを再起動する必要はありません。		
接続プール	接続プールを有効または無効にします。 次のいずれかの値です。 • 有効 - タイムアウトあり • 有効 - タイムアウトなし • 無効 ⓘ 注記 接続プールは、サーバパフォーマンスを改善するため、接続を再利用可能な状態で保持するキャッシュ機能です。	有効 - タイムアウトあり

プロパティ	説明	デフォルト値
接続プールのタイムアウト	プールにおける接続の最大アイドル時間を分単位で指定します。 **注記** このプロパティは、`cs.cfg` ファイルの `cs.cfg` パラメータと同じ意味を持ちます。 プールを無効にすることは、`Max Pool Time` を `0` に設定するのと同じ意味を持ちます。 タイムアウトなしでプールを有効にすることは、`Max Pool Time` を `-1` に設定するのと同じ意味を持ちます。 詳細については、データアクセスガイドを参照してください。	**60**
一時オブジェクトアイドル時間のタイムアウト	使用されない一時オブジェクトをサーバに保持する時間を分単位で指定します。 この時間が経過した後、オブジェクトは削除され、そのリソースが回収されます。	**60**
一時オブジェクトタイマーの間隔	使用状況チェックの間隔を分単位で指定します。 決められた間隔で、サーバが削除候補のオブジェクトを検索します。	**5**
HTTP チャンキングを有効にする	HTTP チャンキングを有効または無効にします。 **注記** HTTP チャンキングは、3-tier デプロイメントのみに関連します。 これは、ドキュメントを開くかまたは最新表示する際のパフォーマンスに影響します。応答時間が長引くと、サイズの大きなドキュメントのフェッチ時のラウンドトリップが減ることになるためです。 HTTP チャンキングを無効にすることは、[*HTTP* チャンクサイズ]を **0** に設定するのと同じ意味を持ちます。	有効
HTTP チャンクサイズ	サーバから送信される HTTP 応答のサイズをキロバイト単位で指定します。	**64**

下位レベルトレースプロパティ

プロパティ	説明	デフォルト値
	注意 以下の下位レベルトレースプロパティの変更後に、サーバを再起動する必要はありません。	
ジョブのトレースを有効にする	Connection Server ジョブのトレースを有効にします。 **注記** そのためには、[ログレベル]プロパティを[高]に設定する必要があります。	無効

プロパティ	説明	デフォルト値
ミドルウェアのトレースを有効にする	すべてのミドルウェアのトレースを有効にします。 特定のミドルウェアをトレースするには、`cs.cfg` ファイルを設定し、サーバを再起動する必要があります。 **注記** そのためには、ログレベルプロパティを高に設定する必要があります。	無効

有効データソースプロパティ

プロパティ	説明	デフォルト値
	警告 以下の有効データソースプロパティの変更後には、サーバを再起動する必要があります。	
データソースを有効にする	接続が必要なデータソースを選択することができます。 このプロパティは、ドライバのフィルタとして機能します。 使用するドライバをロードするための有効なデータソースを指定します。 **警告** デフォルトのサーバ動作では、利用可能なすべてのドライバがロードされます。 この設定を使用して、サーバの役割を特化します。 これは、ネットワーク上に複数の CORBA サーバをデプロイする場合に特に役立ちます。 **注意** 選択したデータソースのドライバのみがロードされます。 その他すべてのドライバは無視されます。 データソースを選択しなかった場合、サーバは利用可能なすべてのドライバをロードします。 **注記** サーバメトリクスで、選択したデータソースが有効にされていることを確認します。 ネットワークレイヤおよびデータベースは、接続サービスメトリクスに表示されます。	チェックなし
ネットワークレイヤ	接続で使用されるネットワークレイヤを指定します。 **注記** ローカライズされていない名前のみが考慮されます。 使用可能なネットワークレイヤの一覧は、`driver.cfg` ファイルで確認できます。このファイルは `<connectionserver-install-dir>¥connectionServer¥` ディレクトリにあります。	• ネイティブ CORBA サーバは ODBC • Adaptive CORBA サーバは JDBC

プロパティ	説明	デフォルト値
データベース	接続で使用されるデータベースを指定します。 **注記** ローカライズされていない名前のみが考慮されます。 データベース名が ASCII 文字列のみで構成される場合、正規表現を使用することができます。 パターンでは GNU regexp 構文が使用されます。 `.*` パターンを使用して、任意の文字に一致させます。 たとえば、`MS SQL Server.*$` という表現は、すべての MS SQL Server データベースが使用されることを意味します。 正規表現については、PERL Web サイト (http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions) を参照してください。	このフィールドは、データベース名を入力するまでは空白のままです。

カスタムデータアクセスサービスのプロパティ

プロパティ	説明	デフォルト値
カスタムデータアクセスクリーンアップタイムアウト (秒)	クライアントのセッションのクリーンアップを実行する前に、非アクティブなクライアントをサービスが待機する時間を秒単位で指定します。	デフォルト値は 1200 秒です。
カスタムデータアクセススワップタイムアウト (秒)	クライアントのセッションをハードディスクにスワップする前に、非アクティブなクライアントをサービスが待機する時間を秒単位で指定します。 [カスタムデータアクセスクリーンアップタイムアウト (秒)] プロパティの値より低い値を指定することをお勧めします。	デフォルト値は 600 秒です。

シングルサインオンサービスのプロパティ

プロパティ	説明	デフォルト値
シングルサインオンの有効期限(秒)	SSO 接続が有効となる有効期限までの時間(秒単位)を指定します。	デフォルト値は 86400 秒です。

プロモーションマネジメントサービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

プロモーションマネジメント ClearCase サービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

Visual Difference サービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

関連情報

共通サーバのプロパティ [1108 ページ]

35.1.4 Crystal Reports サービスのプロパティ

Crystal Reports サービスカテゴリには、次のサーバが含まれます。

- Crystal Reports Cache Server
- Crystal Reports Processing Server
- Crystal Reports 2020 Report Application Server のプロパティ
- Crystal Reports 2020 Processing Server

Crystal Reports Cache Server のプロパティ

Crystal Reports Cache Server と Crystal Reports Processing Serve の両方に適用されるすべてのプロパティに同じ値を設定する必要があります。たとえば、Cache Server で[ビューアを最新表示すると、常に最新データが表示される]の設定を **TRUE** に設定した場合、Processing Server でも同じプロパティの値を **TRUE** に設定する必要があります。

> **注記**
>
> これらのサーバのプロパティのいずれかを変更する場合、変更を有効にするにはサーバを再起動する必要があります。

Crystal Reports キャッシュサービスのプロパティ

プロパティ	説明	デフォルト値
ビューアを最新表示すると、常に最新データが表示される	ユーザがレポートを明示的に最新表示するときに、キャッシュされたすべてのページを無視して新しいデータをデータベースから直接取得するかどうかを指定します。 **注記** このプロパティはレポートオブジェクトそのものに設定でき、レポートごとに異なる場合があります。レポートオブジェクトに指定された値によって、サーバ設定は上書きされます。レポートオブジェクトに値を指定するには、CMC でレポートを選択し、デフォルト設定 > サーバグループの表示 をクリックします。	デフォルト値は「**FALSE**」です。

プロパティ	説明	デフォルト値
クライアント間でレポートデータを共有する	複数のクライアント間でレポートデータを共有するかどうかを指定します。 **注記** このプロパティはレポートオブジェクトそのものに設定でき、レポートごとに異なる場合があります。レポートオブジェクトに指定された値によって、サーバ設定は上書きされます。	デフォルト値は **TRUE** です。
アイドル状態の接続のタイムアウト (分)	Crystal Reports Cache Server がアイドル状態にある接続からのリクエストを待機する時間を分単位で指定します。通常はデフォルト値を変更する必要はありません。	デフォルト値は 20 分です。
セキュリティキャッシュのタイムアウト (分単位)	CMS をクエリする前に、リクエストを処理するためにサーバがキャッシュ済みログオン認証情報、レポートパラメータ、およびデータベース接続情報を使用する時間を分単位で指定します。	デフォルト値は 20 分です。
クライアントに提供する最も古いオンデマンドデータ (秒単位)	サーバがキャッシュされたデータを使用してオンデマンドレポートからのリクエストに応答する時間を秒単位で指定します。 サーバが受け取ったリクエストに対して、以前のリクエストのために生成されたデータを使用して応答することができ、かつ、そのデータが生成されてからの経過時間がこの設定値未満である場合、サーバは受け取ったリクエストへの応答としてこのデータを再利用します。複数のユーザが同じ情報を必要としている場合、このようにデータを再利用することによってシステムパフォーマンスが大幅に向上します。 この値を設定するときは、ユーザに最新のデータを提供することがどの程度重要かを検討してください。頻繁に変更される重要なデータの場合など、すべてのユーザに最新のデータを提供することがとても重要な場合は、この値を 0 に設定してこのようなデータ再利用が行われないようにします。 **注記** このプロパティはレポートオブジェクトそのものに設定でき、レポートごとに異なる場合があります。レポートオブジェクトに指定された値によって、サーバ設定は上書きされます。	デフォルト値は 0 秒です。
最大キャッシュサイズ (KB)	レポートのキャッシュに使用されるハードディスク領域 (KB) の量を指定します。サーバが多数のレポートを処理する場合や特に複雑なレポートを処理する場合は、キャッシュサイズを大きくする必要があります。	デフォルト値は 256000 KB です。
キャッシュファイルディレクトリ	キャッシュファイルディレクトリの場所を指定します。	`%DefaultDataDir%/CrystalReportsCachingServer/temp`
Java 仮想マシンの引数	JVM に提供できるコマンドライン引数を指定します。	デフォルト値は空です。

プロパティ	説明	デフォルト値
DLL 名	現在ロードされているドキュメントタイプのプラグインの名前を指定します。 このプロパティは読み取り専用です。	rasprocReport

Crystal Reports Processing Server のプロパティ

Crystal Reports Cache Server と Crystal Reports Processing Serve の両方に適用されるすべてのプロパティに同じ値を設定する必要があります。たとえば、Cache Server で[ビューアを最新表示すると、常に最新データが表示される]の設定を **TRUE** に設定した場合、Processing Server でも同じプロパティの値を **TRUE** に設定する必要があります。

> ⓘ 注記
>
> これらのサーバのプロパティのいずれかを変更する場合、変更を有効にするにはサーバを再起動する必要があります。

Crystal Reports 処理サービスのプロパティ

プロパティ	説明	デフォルト値
アイドルジョブのタイムアウト (分単位)	Crystal Reports Processing Server が特定のジョブのリクエストを待機する間隔の長さを分単位で指定します。	デフォルト値は 20 分です。
最大終生ジョブ数 (子単位)	各子プロセスで終生ごとに管理できるジョブの最大数を指定します。	デフォルト値は 1000 です。
ビューアを最新表示すると、常に最新データが表示される	ユーザがレポートを明示的に最新表示するときに、キャッシュされたすべてのページを無視して新しいデータをデータベースから直接取得するかどうかを指定します。複数のクライアント間でレポートデータを共有するかどうかを指定します。 ⓘ 注記 このプロパティはレポートオブジェクトそのものに設定でき、レポートごとに異なる場合があります。レポートオブジェクトに指定された値によって、サーバ設定は上書きされます。レポートオブジェクトに値を指定するには、CMC でレポートを選択し、デフォルト設定 > サーバグループの表示 をクリックします。	デフォルト値は「**FALSE**」です。

プロパティ	説明	デフォルト値
クライアント間でレポートデータを共有する	複数のクライアント間でレポートデータを共有するかどうかを指定します。複数のクライアント間でレポートデータを共有するかどうかを指定します。 **注記** このプロパティはレポートオブジェクトそのものに設定でき、レポートごとに異なる場合があります。レポートオブジェクトに指定された値によって、サーバ設定は上書きされます。	デフォルト値は **TRUE** です。
アイドル状態の接続のタイムアウト (分)	Crystal Reports Processing Server がアイドル状態にある接続からのリクエストを待機する時間を分単位で指定します。通常はデフォルト値を変更する必要はありません。	デフォルト値は 20 分です。
同時実行ジョブの最大数 (0 は自動)	Crystal Reports Processing Server で同時に実行できる独立したジョブの最大数を指定します。このプロパティの値を “0” に設定すると、サーバが実行されているマシンの CPU とメモリに基づいて適切な値が適用されます。	デフォルト値は 0 です。
クライアントに提供する最も古いオンデマンドデータ (秒単位)	サーバがキャッシュされたデータを使用してオンデマンドレポートからのリクエストに応答する時間を秒単位で指定します。 サーバが受け取ったリクエストに対して、以前のリクエストのために生成されたデータを使用して応答することができ、かつ、そのデータが生成されてからの経過時間がこの設定値未満である場合、サーバは受け取ったリクエストへの応答としてこのデータを再利用します。複数のユーザが同じ情報を必要としている場合、このようにデータを再利用することによってシステムパフォーマンスが大幅に向上します。 この値を設定するときは、ユーザに最新のデータを提供することがどの程度重要かを検討してください。頻繁に変更される重要なデータの場合など、すべてのユーザに最新のデータを提供することがとても重要な場合は、この値を 0 に設定してこのようなデータ再利用が行われないようにします。 **注記** このプロパティはレポートオブジェクトそのものに設定でき、レポートごとに異なる場合があります。レポートオブジェクトに指定された値によって、サーバ設定は上書きされます。	デフォルト値は 0 です。
事前開始された最大子プロセス数	サーバで許可される事前開始された子プロセスの最大数を指定します。値が小さすぎると、リクエストが作成されるとすぐにサーバによって子プロセスが作成され、ユーザが遅延する可能性があります。値が大きすぎると、アイドル状態にある子プロセスによってシステムリソースが浪費される可能性があります。	デフォルト値は 1 です。

プロパティ	説明	デフォルト値
一時ディレクトリ	必要な場合に一時ファイルが作成されるディレクトリを指定します。 **注記** このディレクトリに十分なディスク領域がない場合、パフォーマンスの問題が発生する場合があります。	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Java のクラスパス	サーバで必要な Java のクラス名とパス。	%CommonJavaLibDir%/procCR.jar
Java 子仮想マシンの引数	サーバによって作成された子プロセスに提供されるコマンドライン引数を指定します。	Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%,Dcom.businessobjects.mds.cs.ImplementationID=csEX

シングルサインオンサービスのプロパティ

プロパティ	説明	デフォルト値
シングルサインオンの有効期限 (秒単位)	SSO 接続が有効となる、有効期限までの時間 (秒単位) を指定します。	デフォルト値は 86400 秒です。

Crystal Reports 2020 Report Application Server のプロパティ

注記

これらのプロパティのいずれかを変更する場合、変更を有効にするにはサーバを再起動する必要があります。

Crystal Reports 2020 表示および変更サービスのプロパティ

プロパティ	説明	デフォルト値
レポートジョブが閉じるまで、レポートジョブをデータベースに接続したままにしておきますか?	プロセスが実行されるまで、レポートジョブをデータベースに接続したままにするかどうかを指定します。	デフォルト値は、**FALSE** です。
参照データのサイズ (レコード数)	特定のフィールドの値を使って参照するときに、データベースから返される固有レコードの数を指定します。データは、まずクライアントのキャッシュが使用可能であればそこから取得され、次にサーバのキャッシュから取得されます。いずれのキャッシュにもデータがない場合、データベースから取得されます。	デフォルト値は 100 レコードです。

プロパティ	説明	デフォルト値
アイドル状態の接続のタイムアウト (分)	Report Application Server (RAS) が、タイムアウトまでアイドル状態のクライアントからのリクエストを待機する時間を分単位で指定します。 値が小さすぎるとユーザのリクエストが途中で終了する可能性があり、また、大きすぎるとサーバのスケーラビリティに悪影響を及ぼす可能性があります (たとえば、`ReportClientDocument` オブジェクトが明示的に閉じられない場合、サーバはアイドル状態にあるジョブが閉じられるのを不必要に待機します)。	デフォルト値は 30 分です。
バッチサイズ (レコード数)	各データ転送中にデータベースから返される結果セットの行数を指定します。 たとえば、500 個のレコードがリクエストされ、バッチサイズのプロパティが 100 レコードに設定されている場合、データは 100 行の 5 つのバッチで返されます。RAS のパフォーマンスを向上させるには、ネットワーク環境、データベース、および適切なバッチサイズを設定するためのリクエストの種類を理解する必要があります。	デフォルト値は 100 レコードです。
レポートをプレビューまたは最新表示するときに読み込まれるデータベースレコードの数 (無制限の場合は -1)	レポートのプレビューまたは最新表示時に読み取るデータベースレコード数を指定します。この設定では、ユーザがクエリまたはレポートを実行したときにサーバによりデータベースから取得されるレコード数が制限されます。この設定は、極端に大量のレコードセットを返すオンデマンドレポートを、ユーザが実行できないようにするときに便利です。 そのようなレポートは、スケジュール設定して実行すれば、より短時間でレポートをユーザに提供でき、また、それらのクエリによるデータベースの負荷を軽減できます。	デフォルト値は 20000 レコードです。
レポートジョブの最大同時実行数 (無制限の場合は 0)	RAS で同時に実行できる独立したジョブの最大数を指定します。	デフォルト値は 75 個のジョブです。
クライアントに提供する最も古いオンデマンドデータ (分単位)	オンデマンドレポートがキャッシュされたレポートデータを処理する時間を分単位で指定します。	デフォルト値は 20 分です。
一時ディレクトリ	必要な場合に一時ファイルが作成されるディレクトリを指定します。 **注記** このディレクトリに十分なディスク領域がない場合、パフォーマンスの問題が発生する場合があります。	`%DefaultDataDir%/CrystalReportsRasServer/temp`

シングルサインオンサービスのプロパティ

プロパティ	説明	デフォルト値
シングルサインオンの有効期限 (秒単位)	SSO 接続が有効となる、有効期限までの時間 (秒単位) を指定します。	デフォルト値は 86400 秒です。

Crystal Reports 2020 Processing Server のプロパティ

> **注記**
>
> これらのプロパティのいずれかを変更する場合、変更を有効にするにはサーバを再起動する必要があります。

Crystal Reports 2020 処理サービスのプロパティ

プロパティ	説明	デフォルト値
アイドルジョブのタイムアウト (分単位)	Crystal Reports Processing Server が特定のジョブのリクエストを待機する間隔の長さを分単位で指定します。	デフォルト値は 20 分です。
最大終生ジョブ数 (子単位)	各子プロセスで終生ごとに管理できるジョブの最大数を指定します。	デフォルト値は 1000 です。
ビューアを最新表示すると、常に最新データが表示される	ユーザがレポートを明示的に最新表示するときに、キャッシュされたすべてのページを無視して新しいデータをデータベースから直接取得するかどうかを指定します。複数のクライアント間でレポートデータを共有するかどうかを指定します。 **注記** このプロパティはレポートオブジェクトそのものに設定でき、レポートごとに異なる場合があります。レポートオブジェクトに指定された値によって、サーバ設定は上書きされます。レポートオブジェクトに値を指定するには、CMC でレポートを選択し、デフォルト設定 > サーバグループの表示 をクリックします。	デフォルト値は「**FALSE**」です。
クライアント間でレポートデータを共有する	複数のクライアント間でレポートデータを共有するかどうかを指定します。複数のクライアント間でレポートデータを共有するかどうかを指定します。 **注記** このプロパティはレポートオブジェクトそのものに設定でき、レポートごとに異なる場合があります。レポートオブジェクトに指定された値によって、サーバ設定は上書きされます。	デフォルト値は **TRUE** です。
アイドル状態の接続のタイムアウト (分)	Crystal Reports Processing Server がアイドル状態にある接続からのリクエストを待機する時間を分単位で指定します。通常はデフォルト値を変更する必要はありません。	デフォルト値は 20 分です。
同時実行ジョブの最大数 (0 は自動)	Crystal Reports Processing Server で同時に実行できる独立したジョブの最大数を指定します。このプロパティの値を “0” に設定すると、サーバが実行されているマシンの CPU とメモリに基づいて適切な値が適用されます。	デフォルト値は 0 です。

プロパティ	説明	デフォルト値
クライアントに提供する最も古いオンデマンドデータ (秒単位)	サーバがキャッシュされたデータを使用してオンデマンドレポートからのリクエストに応答する時間を秒単位で指定します。 サーバが受け取ったリクエストに対して、以前のリクエストのために生成されたデータを使用して応答することができ、かつ、そのデータが生成されてからの経過時間がこの設定値未満である場合、サーバは受け取ったリクエストへの応答としてこのデータを再利用します。複数のユーザが同じ情報を必要としている場合、このようにデータを再利用することによってシステムパフォーマンスが大幅に向上します。 この値を設定するときは、ユーザに最新のデータを提供することがどの程度重要かを検討してください。頻繁に変更される重要なデータの場合など、すべてのユーザに最新のデータを提供することがとても重要な場合は、この値を 0 に設定してこのようなデータ再利用が行われないようにします。 **注記** このプロパティはレポートオブジェクトそのものに設定でき、レポートごとに異なる場合があります。レポートオブジェクトに指定された値によって、サーバ設定は上書きされます。	デフォルト値は 0 です。
事前開始された最大子プロセス数	サーバで許可される事前開始された子プロセスの最大数を指定します。値が小さすぎると、リクエストが作成されるとすぐにサーバによって子プロセスが作成され、ユーザが遅延する可能性があります。値が大きすぎると、アイドル状態にある子プロセスによってシステムリソースが浪費される可能性があります。	デフォルト値は 1 です。
一時ディレクトリ	必要な場合に一時ファイルが作成されるディレクトリを指定します。 **注記** このディレクトリに十分なディスク領域がない場合、パフォーマンスの問題が発生する場合があります。	%DefaultDataDir%/CrystalReports2020ProcessingServer/temp
レポートジョブが閉じるまで、レポートジョブをデータベースに接続したままにしておきますか?	レポートジョブが閉じるまでそのジョブをデータベースに接続したままにするかどうかを指定します。	デフォルト値は FALSE です。
レビューまたは最新表示時に読み取るデータベースレコード数 (無制限の場合は 0)	レポートのプレビューまたは最新表示時に読み取るデータベースレコード数を指定します。この設定では、ユーザがクエリまたはレポートを実行したときにサーバによりデータベースから取得されるレコード数が制限されます。この設定は、極端に大量のレコードセットを返すオンデマンドレポートを、ユーザが実行できないようにするときに便利です。 そのようなレポートは、スケジュール設定して実行すれば、より短時間でレポートをユーザに提供でき、また、それらのクエリによるデータベースの負荷を軽減できます。	デフォルト値は 20000 です。

シングルサインオンサービスのプロパティ

プロパティ	説明	デフォルト値
シングルサインオンの有効期限 (秒単位)	SSO 接続が有効となる、有効期限までの時間 (秒単位) を指定します。	デフォルト値は 86400 秒です。

35.1.5 Analysis サービスのプロパティ

Analysis サービスカテゴリには、Adaptive Processing Server が含まれます。

Multi-Dimensional Analysis Service のプロパティ

プロパティ	説明	デフォルト値
最大クライアントセッション数	サーバで同時に開くことができる MDAS セッションの最大数を指定します。 開いているセッション数がこの値に達した場合、さらに別の MDAS セッションを開始しようとすると、“サーバの使用不可”エラーメッセージが表示されます。この値を変更すると、自身のニーズと使用可能なハードウェアに応じて MDAS のパフォーマンスを最適化できます。ただし、この値を増やすと、MDAS とデータベースの両方でパフォーマンスに問題が生じる場合があります。デフォルト値の 15 セッションは、控えめな値です。ユーザクエリの数が少ないインストールでは、この値を大幅に増やし、ユーザのクエリ数が多いインストールでは、この値を小さくする必要があります。	デフォルト値は 15 に設定されます。有効な範囲は 1 ～ 100 です。
クエリから返される最大セル数	1 つのクエリでユーザに返されるセルの数を指定します。ユーザは、大量のセルを返したりメモリを大量に消費するクエリを実行できなくなります。ユーザのクエリがこのセル限界を超えると、ユーザがエラーメッセージを受信します。	デフォルト値は 100000 セルです。
フィルタ処理時に返される最大メンバー数	メンバー別のフィルタ処理時に取得されるメンバー数を指定します。取得メンバー数が非常に多い場合は、メモリを大量に消費します。	デフォルト値は 100000 メンバーです。

BEx Web アプリケーションサービスのプロパティ

プロパティ	説明	デフォルト値
最大クライアントセッション数	サービスで許可される最大クライアントセッション数。	デフォルト値は 15 セッションです。
SAP BW マスタシステム	BI プラットフォームで作成した BW システムへの OLAP 接続名。	デフォルト値は SAP_BW です。
JCo サーバ *RFC* 宛先	BW システムで入力した JCo サーバ RFS 宛先の名前。	デフォルトでは、この値は空になっています。
JCo サーバゲートウェイホスト	BW システムで定義した JCo サーバゲートウェイホストの名前。	デフォルトでは、この値は空になっています。
JCo サーバゲートウェイサービス	BW システムで定義した JCo サーバゲートウェイサービスの名前。	デフォルトでは、この値は空になっています。

プロパティ	説明	デフォルト値
JCo サーバ接続カウント	自動的に作成されるプログラム数を指定します。このプログラムは、サービス用に ABAP から Java への呼び出しを処理する際に使用できます。	デフォルト値は 3 接続です。

35.1.6 データフェデレーションサービスのプロパティ

データフェデレーションサービスカテゴリには、Adaptive Processing Server が含まれます。

データフェデレーションサービスプロパティ

プロパティ	説明	デフォルト値
最大接続数	サーバで許可される最大接続数を指定します。	デフォルト値は 32767 です。
実行のスレッドプールのサイズ	特定の時点で並行して実行できる最大クエリ数を指定します。	デフォルト値は 10 です。
接続アイドル時間のタイムアウト	非アクティブな接続が閉じられるまでの時間を秒単位で指定します。	デフォルト値は 10800 秒です。
ステートメントアイドル時間のタイムアウト	非アクティブなクエリ文が閉じられるまでの時間を秒単位で指定します。	デフォルト値は 600 秒です。

35.1.7 Web Intelligence サービスのプロパティ

Web Intelligence サービスカテゴリには、次のサーバが含まれます。

- Adaptive Processing Server
- Web Intelligence Processing Server

Adaptive Processing Server の設定

コマンドラインパラメータ

プロパティ	説明	デフォルト値
レベルへの展開	BEx クエリから取得するデータのレベルを指定します。 デフォルトで、階層が所定のレベルに展開されることはありません。デフォルトレベルは常にレベル 00 です。次のパラメータをコマンドラインに追加することで、この動作を変更することができますが、設定する値が大きすぎると、Web Intelligence ですべての階層データを取得することになり、システムのパフォーマンスおよび安定性に影響を及ぼす可能性があります。	`-Dsap.sl.bics.expandToLevel=n` n は 0 ～ 99 の間の整数です。n=0 の場合、またはこのパラメータを指定しない場合は、階層でレベルへの展開パラメータは使用されません。

プロパティ	説明	デフォルト値
選択オプションの変数選択	変数選択の選択オプションを指定します。 このプロパティを interval に設定した場合、テキストボックスは使用できません。プロンプトダイアログボックスに開始値と終了値のみを入力できます。 このプロパティを multivalue に設定した場合は、"値の入力" テキストボックスを使用して、BW 選択オプション変数に値を入力できます。 **注記** このプロパティによって、Web Intelligence リッチクライアントのローカルインストールが更新されることはありません。このようなインストールのローカルレジストリ更新の詳細については、"Web Intelligence リッチクライアントインストールガイド" を参照してください。	**`-Dsap.sl.bics.variableComplexSelectionMapping=n`** n は interval または multivalue です。 **注記** BI 4.1 SP05 より前では、このオプションのデフォルト値は interval でした。このプロパティを Adaptive Processing Server 設定に追加し、multivalue に設定する場合は、既存のドキュメントで次のアクションを行う必要があります。 • ドキュメントを消去する必要があります。 • 複数値選択と互換性を持つように、クエリプロンプトのデフォルト値を変更する必要があります。

Web Intelligence モニタリングサービスのプロパティ

プロパティ	説明	デフォルト値
モニタリングを有効にする	サービスのモニタリングを有効にするかどうかを指定します。	**TRUE**
モニタリングスレッドループの遅延 (秒)	サービスからクライアントに ping 送信を試行する間隔を秒単位で指定します。	300
監視中のリソースのデフォルトクリーンアップタイムアウト (秒)	クライアントのセッションのクリーンアップを実行する前に、非アクティブなクライアントをサービスが待機する時間を秒単位で指定します。	1200
監視中のリソースのデフォルトスワップタイムアウト (秒)	クライアントのセッションをハードディスクにスワップする前に、非アクティブなクライアントをサービスが待機する時間を秒単位で指定します。監視中のリソースのデフォルトクリーンアップタイムアウトプロパティの値より小さい値を指定することをお勧めします。	600
サービスプロファイリングの有効化		**TRUE**
サービスアクティビティ監視の有効化		**TRUE**

ビジュアライゼーションサービスのプロパティ

プロパティ	説明	デフォルト値
ビジュアライゼーションエンジンクリーンアップタイムアウト (秒)	クライアントのセッションのクリーンアップを実行する前に、非アクティブなクライアントをサービスが待機する時間を秒単位で指定します。	1200

プロパティ	説明	デフォルト値
ビジュアライゼーションエンジンスワップタイムアウト (秒)	クライアントのセッションをハードディスクにスワップする前に、非アクティブなクライアントをサービスが待機する時間を秒単位で指定します。ビジュアライゼーションエンジンクリーンアップタイムアウト (秒) プロパティの値より小さい値を指定することをお勧めします。	600

Rebean サービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

ドキュメントリカバリサービスのプロパティ

プロパティ	説明	デフォルト値
設定プロパティはありません。		

DSL ブリッジサービスのプロパティ

プロパティ	説明	デフォルト値
DSL ブリッジエンジンクリーンアップタイムアウト (秒)	クライアントのセッションのクリーンアップを実行する前に、非アクティブなクライアントをサービスが待機する時間を秒単位で指定します。	1200

Web Intelligence Processing Server のプロパティ

Web Intelligence Processing Server のプロパティは、次のサービスに分類されます。

- 情報エンジン
- Web Intelligence コア
- Web Intelligence 処理
- Web Intelligence 共通

しきい値の設定について、各表で説明します。

情報エンジンサービスのプロパティ

プロパティ	説明	デフォルト値
値の一覧キャッシュ有効化	Web Intelligence Processing Server で値の一覧のキャッシュを有効にするかどうかを指定します。	**TRUE**
値の一覧のバッチサイズ (項目数)	値の一覧のバッチごとのエントリ (値) の最大数を指定します。	1000
最大並べ替え (カスタム) サイズ (項目数)	カスタムの並べ替えの最大エントリ数を指定します。	100
ユニバースキャッシュの最大サイズ (ユニバース数)	Web Intelligence Processing Server にキャッシュされるユニバースの数を指定します。	20
値の一覧の最大サイズ (項目数)	各値の一覧のエントリ (値) の最大数を指定します。	50000

Web Intelligence コアサービスのプロパティ

プロパティ	説明	デフォルト値
リサイクルまでのタイムアウト (秒数)	処理済みドキュメントの合計数がリサイクルまでの最大ドキュメント数プロパティで指定された値を上回った場合に、Server Intelligence Agent (SIA) がサーバを停止して再起動するまでサーバがアイドル状態になる時間を秒単位で指定します。	1200
アイドル状態のドキュメントのタイムアウト (秒)	Web Intelligence Processing Server セッションがスワップされるまでの時間を秒単位で指定します。この期間にクライアントがリクエストを生成しない場合、セッションはハードディスクにスワップされて、アクティブなセッションのリソースが解放されます。	300 有効な範囲は 100 ～ 10000 秒です。
サーバポーリング間隔 (秒)	サーバが新しいスレッドリクエストをポーリングする間隔を秒単位で指定します。サーバは、ポーリングフェーズ中、未使用ドキュメントのスワップなどのクリーンアップアクションを実行して、サーバのメモリがメモリの上限のしきい値を超えないようにします。	120
ユーザあたりの最大ドキュメント数	いつでもユーザに関連付けることができるアクティブセッション (Web Intelligence ドキュメント) の最大数を指定します。したがって、5 の場合、ユーザは、一度に最大 5 つのアクティブセッションを使用できます。	5 有効な範囲は 1 ～ 20 です。
リサイクルまでの最大ドキュメント数	サーバがリサイクル対象と見なすまで処理可能な Web Intelligence ドキュメントの数を指定します。処理済みのドキュメントの数に到達し、サーバがアイドル状態の場合、サーバは閉じて、Server Intelligence Agent (SIA) がサーバの新しいインスタンスを起動します。ただし、サーバの新しいインスタンスが起動されるまでに遅延が発生します。遅延時間はリサイクルまでのタイムアウトプロパティで定義されます。	50
ドキュメントマップ最大サイズエラーの許可	<最大接続数>プロパティが制限されるかどうかを指定します。このプロパティが有効な場合は、<最大接続数>プロパティに設定された値がサーバで認識されます。無効な場合、最大接続数プロパティは無視されます。	**TRUE**
アイドル状態の接続のタイムアウト (分)	サーバがアイドル状態にある接続からのリクエストを待機する時間を分単位で指定します。設定値が短すぎると、リクエストが途中で終了する場合があります。設定値が長すぎると、アイドル状態のリクエストが終了するまでサーバが待機している間に、リクエストがキューに入れられる可能性があります。	20
最大接続数	一度に開くことができる最大同時セッション数を指定します。これは概算数です。この設定では、スワップされる非アクティブセッション、またはセッション数の分析のために作成されるセッションはカウントされません。この制限に達し、リクエストを処理できる他のサーバがない場合、ユーザはエラーメッセージを受け取ります。 **注記** このプロパティがサーバで認識されるためには、<ドキュメントマップ最大サイズエラーの許可>プロパティを有効にする必要があります。	200 有効な範囲は 5 ～ 65535 です。

プロパティ	説明	デフォルト値
メモリ分析有効化	メモリの分析を有効にするかどうかを指定します。このプロパティが有効な場合、次のプロパティがアクティブになり、サーバによって認識されます。 • <メモリの最大しきい値> • <メモリの上位しきい値> • <メモリの下位しきい値> サーバのプロセスメモリが<メモリの上位しきい値>を上回ると、ドキュメントの保存アクションのみが許可されます。プロセスメモリが<メモリの最大しきい値>を上回ると、すべてのアクションは停止し、失敗します。	**TRUE**
メモリの下位しきい値 *(MB)*	メモリ使用量の下位しきい値を指定します。	**3500**
メモリの上位しきい値 *(MB)*	メモリ使用量の上位しきい値を指定します。	**4500**
メモリの最大しきい値 *(MB)*	メモリ使用量の最大しきい値を指定します。	**6000**
APS サービスモニタリングを有効にする	Adaptive Processing Server でホストされる APS サービスによる、サーバのモニタリングを有効にします。	**TRUE**
APS サービスの *Ping* 失敗の再試行数	APS サービスに到達できないと決定するまでに、サーバが到達を試行する回数を指定します。	3
APS サービスモニタリングスレッドの期間	APS サービスへの到達を試行する間隔の遅延期間を示します。	300
現利用状況ログを有効にする	サーバのログファイルに完全なトレースを生成するかどうかを指定します。 **注記** このプロパティは、トラブルシューティング時のデバッグを目的とする場合のみ有効にします。通常操作時は、**FALSE** に設定します。	**FALSE**

Web Intelligence 処理サービスのプロパティ

プロパティ	説明	デフォルト値
HTTP URL 使用有効化	リモートに保存されているファイルにサーバがアクセスできるかどうかを指定します。	**TRUE**
プロキシ値	ネットワークのプロキシサーバのアドレスを指定します。ネットワークにプロキシサーバがあり、リモートに保存されているファイルにアクセスしようとしている場合にのみ値を指定する必要があります。	空白

Web Intelligence 共通サービスのプロパティ

プロパティ	説明	デフォルト値
キャッシュのタイムアウト (分)	ドキュメントのキャッシュの内容がクリアされるまでの時間を分単位で指定します。タイムアウトは、各ドキュメントの最新アクセス日付によって異なります。	4370
ドキュメントキャッシュクリーンアップ間隔 (分)	ドキュメントキャッシュがスキャンされて、<最大ドキュメントキャッシュサイズ>、<ドキュメントキャッシュの最大縮小領域>、および<キャッシュの最大ドキュメント数>設定に対してチェックされる間隔を分単位で指定します。	120
キャッシュ共有禁止	キャッシュ共有を禁止するかどうかを指定します。デフォルトでは、キャッシュ共有は有効になっています。つまり、すべての Web Intelligence Processing Server インスタンスで同じキャッシュを共有します。ただし、Web Intelligence Processing Server のインスタンスごとに 1 つのキャッシュを使用する場合は、このプロパティを有効にする必要があります。	**FALSE**
ドキュメントキャッシュ有効化	ドキュメントキャッシュを有効にするかどうかを指定します。このプロパティが有効な場合、キャッシュは、スケジュールされた Web Intelligence ドキュメントと共に事前ロードできます。	**TRUE**
リアルタイムキャッシュ有効化	リアルタイムキャッシュを有効にするかどうかを指定します。このプロパティが有効な場合、キャッシュを動的にロードできます。したがって、Web Intelligence Processing Server は、Web Intelligence ドキュメントを表示時にキャッシュします。また、ドキュメントでプリキャッシュが有効な場合、サーバはドキュメントがスケジュールされたジョブとして実行された場合にもそのドキュメントをキャッシュします。	**TRUE**
最大ドキュメントキャッシュサイズ (KB)	ドキュメントキャッシュの最大サイズを指定します。この制限に達すると、ドキュメントキャッシュは<ドキュメントキャッシュの最大縮小領域>プロパティに基づいてクリアされます。	1000000
ドキュメントキャッシュの最大縮小領域 (%%)	新しいアクションの実行を可能にし、キャッシュ内に結果を保存するために空にするキャッシュの割合を指定します。“最終アクセス時刻”が最も古いドキュメントから消去されます。	70
最大文字ストリームサイズ (MB)	Web Intelligence クライアントに送信される最大文字ストリームサイズを指定します。 **注記** 最大文字ストリームサイズプロパティを超えると、Web Intelligence ドキュメントは作成されず、クライアントはエラーメッセージを受け取ります。	5 有効な範囲は 1 ～ 4095 MB です。
バイナリストリーム最大サイズ (MB)	Web Intelligence クライアントに送信されるバイナリストリームの最大サイズを MB 単位で指定します。 **注記** バイナリストリーム最大サイズプロパティを超えると、Web Intelligence ドキュメントは作成されず、クライアントはエラーメッセージを受け取ります。	50 有効な範囲は 1 ～ 4095 MB です。
イメージディレクトリ	イメージディレクトリの場所を指定します。	空白

プロパティ	説明	デフォルト値
アウトプットキャッシュディレクトリ	キャッシュの場所を指定します。	空白

一般プロパティ

プロパティ	説明	デフォルト値
シングルサインオンの有効期限 (秒単位)	SSO 接続が有効となる、有効期限までの時間 (秒単位) を指定します。	86400

関連情報

Web Intelligence サーバのメモリしきい値の設定 [1140 ページ]

35.1.7.1 Web Intelligence サーバのメモリしきい値の設定

以下の節では、[メモリの最大しきい値]、[メモリの上位しきい値]、または[メモリの下位しきい値] の値を超えた場合の、Web Intelligence サーバの動作について説明します。

メモリの下位しきい値

`<Memory Lower Threshold>` の制限に達すると、サーバは非アクティブなドキュメントをハードディスクに交換し、アクティブなドキュメントを保存するための追加メモリを割り当てます。 各ユーザには、`<Maximum Documents per User>` ではなく、1 つのアクティブなドキュメントのみが許可されます。

メモリの上位しきい値

この `<Memory Upper Threshold>` に達すると、リソースを解放してサーバを保護するために、次のようなサーバアクションが実行されます。

- サーバは新しい接続と新しいクライアント呼び出しを拒否します。 Web Intelligence ドキュメントの [保存] オプションのみ許可されます。 アクションをリクエストしたユーザには、「サーバ使用中」メッセージが表示され、保留中の変更を保存する必要があることが知らされます。
- サーバは十分なリソースを解放するためにシステムのクリーンアップを有効にして、割り当てられたメモリの量が `<Memory Upper Threshold>` プロパティで設定された制限を下回るようにします。
- サーバは、読み取り専用ドキュメントを閉じようとします。
- システムのクリーンアップ中に十分な量のメモリが解放されなかった場合、サーバは [編集] モードのドキュメントを閉じる処理を開始します。 サーバは、LIFO プロトコルに基づいてドキュメントを閉じる処理を開始します。この場合、最初に最新のアクティブなドキュメントがメモリから消去されます。 サーバは安全なレベルに到達するまで、ドキュメントを閉じる処理を継続します。このレベルは、`<Memory Upper`

Threshold> - (20%*(<Memory Upper Threshold>)) という計算に基づいています。 たとえば、[メモリの上位しきい値] プロパティが 4500 MB に設定されている場合、安全なレベルは次のようになります。

```
4500MB - .20*4500MB = 3600MB
```

クライアント呼び出しが実行されているときに、サーバはドキュメントを閉じることができません。 サーバがこのしきい値に達すると、最新表示されたドキュメント、別の形式にエクスポートされたドキュメント、時間のかかるその他の操作は、終了されません。 サーバが、十分なメモリを回復できず、<Memory Upper Threshold> をまだ超えている場合には、サーバは再起動します。

メモリの最大しきい値

<Memory Maximum Threshold> の制限に達すると、現在の操作が中断します。 すべてのクライアント呼び出しは終了されます。 呼び出し終了後に、対応するドキュメントが閉じられます。

36 サーバのメトリクスに関する付録

36.1 サーバのメトリクスに関する付録について

この付録では、特別な記載がないかぎり、サーバという用語は SAP BusinessObjects サーバを意味し、BI プラットフォームがインストールされていたり、稼働したりしているマシンは指しません。

サーバのメトリクスは、稼働していないサーバでは使用できません。

付録に記載されているメトリクスに加えて、モニタリングアプリケーションでは、以下のサーバのステータスを監視できます。

サーバの状態	説明
ヘルスステータス	ヘルスステータスは、サーバの健全性全般を表示します。以下は、可能な値です。 • 0 = 赤色 (危険) • 1 = 黄色 (注意) • 2 = 緑色 (正常)
サーバの有効ステータス	このステータスでは、サーバが有効かどうかを表示します。可能な値は以下のとおりです。 • 0 = 無効 • 1 = 有効
サーバ実行中ステータス	このステータスでは、サーバの実行状態を表示します。可能な値は以下のとおりです。 • 0 = 停止 • 1 = 開始 • 2 = 初期化中 • 3 = 実行中 • 4 = 停止中 • 5 = 失敗 • 6 = エラー有りで実行中 • 7 = 警告有りで実行中

36.1.1 一般的なサーバのメトリクス

以下のメトリクスは、指定されたサーバが稼働しているマシンを示すものです。

マシン固有メトリクス

メトリクス	説明
マシン名	サーバが稼働しているマシンのホスト名。
オペレーティングシステム	サーバが稼働しているマシンのオペレーティングシステム。
CPU の種類	サーバが稼働しているマシンの中央処理装置の種類。このメトリクスは、Adaptive Processing Server または Web アプリケーションコンテナサーバ (WACS) では使用できません。
CPU	サーバで利用できる CPU の数。マルチコアハードウェアの場合、このメトリクスは物理プロセッサの数ではなく論理 CPU の数を示す可能性があります。このメトリクスは、Adaptive Processing Server または Web アプリケーションコンテナサーバ (WACS) では使用できません。
コアの数	BI プラットフォームサーバがホストされているマシン内のコアの数を表示します。
RAM (MB)	サーバが稼働しているマシンで利用できるメガバイト単位のメモリ量。このメトリクスは、Adaptive Processing Server または Web アプリケーションコンテナサーバ (WACS) では使用できません。
ローカル時刻	ローカル時刻。
ディスクサイズ *(GB)*	BI プラットフォームがインストールされているディスクのサイズ (ギガバイト)。このメトリクスは、Adaptive Processing Server または Web アプリケーションコンテナサーバ (WACS) では使用できません。
使用ディスク領域 *(GB)*	BI プラットフォームがインストールされているディスクの使用領域 (ギガバイト)。これには、BI プラットフォームだけでなく、マシンの別のプログラムによって使用されている領域が含まれます。このメトリクスは、Adaptive Processing Server または Web アプリケーションコンテナサーバ (WACS) では使用できません。

以下のメトリクスは、指定された SAP BusinessObjects サーバについて説明しています。

サーバ固有メトリクス

メトリクス	説明
ネームサーバ	このサーバがアドレスを公開する CMS サーバの名前とポート番号。
登録名	サーバの内部名。これは、CMC の[サーバ]画面に表示される名前ではありません。
バージョン	サーバのバージョン。
開始時刻	サーバが最後に起動された時刻。
PID	サーバの固有プロセス ID 番号。サーバが稼働しているマシンのオペレーティングシステムにより、PID が生成されます。PID を使用して、特定のサーバを識別することができます。
ホスト名	サーバで現在使用中のホスト名のカンマ区切りリスト。
ホスト *IP* アドレス	サーバがリクエストを受信待機する IP アドレスのカンマ区切りリスト。
リクエストポート	サーバが他のサーバからのリクエストを受信待機するポート。サーバが複数の IP アドレスでリクエストを受信待機している場合、サーバのリクエストポートは常に同じになります。他のプロセスでリクエストポートが使用される場合、サーバは起動されません。このポートが他のプロセスで使用されていないことを確認します。

メトリクス	説明
使用中のサーバスレッド	現在、リクエストを処理中のサーバスレッドの数。この数がサーバのスレッドプールの最大サイズと同じ場合、追加のリクエストを並行して処理できず、新規リクエストは使用中のスレッドが利用可能になるまで待機する必要がある可能性があることを示しています。

監査メトリクス

メトリクス	説明
キュー内の監査イベントの現在の数	監査対象で記録されたものの、CMS Auditor によって取得されていない監査イベントの数。この数が際限なく増加する場合、監査の設定が正しくないか、システムに対する負荷が非常に大きくなり、Auditor が取得できる以上の速さで監査イベントが生成されていることを示している可能性があります。 **注記** サーバを停止する場合、まずサーバを無効にし、このメトリクスが “0” になるまで待機します。待機しない場合、サーバが再起動して CMS がポーリングするまでキュー内に残り、監査データストアに到達しない監査イベントが発生する場合があります。

サービスメトリクスのロギング

メトリクス	説明
ロギングディレクトリ	この場所に、サーバのログファイルがあります。

36.1.2 Central Management Server のメトリクス

次の表は、Central Management Server(CMS)の[メトリクス]画面に表示されるサーバのメトリクスの説明を示します。

Central Management Server のメトリクス

メトリクス	説明
監査データベースへの接続確立	CMS から監査データベースへの正常な接続が確立されているかどうかを示します。値が “1” の場合は、接続が確立されていることを示します。値が “0” の場合は、監査データベースへの接続が確立されていないことを示します。CMS が Auditor であれば、この値は “1” です。値が “0” の場合は、監査データベースへの接続が確立できない理由を調査してください。
CMS Auditor	CMS が Auditor として機能しているかどうかを示します。値が “1” の場合は、CMS が Auditor として機能していることを示します。値が “0” の場合は、CMS が Auditor として機能していないことを示します。
監査データベースの接続名	監査データベース接続の名前。必ずしも監査データベース自体の名前ではありません。このメトリクスが空の場合は、監査データベースへの接続が確立できないことを示します。
監査データベースのユーザ名	監査データベースへの接続に使用されるユーザアカウントの名前。

メトリクス	説明
監査データベースの最終更新日	CMS が監査対象からイベントを取得し始めた直近の日付と時刻。CMS が Auditor の場合、このメトリクスには [“メトリクス”] 画面がロードされた時刻に近い時刻が表示されるはずです。この値が、画面がロードされた時刻の 2 時間前より前であれば、監査が適切に動作していないことを示している可能性があります。
監査スレッドの最終ポーリングサイクル期間 (秒)	最終ポーリングサイクルの秒単位の時間。これは、以前のポーリングサイクルにおけるイベントデータの監査データベースへの最長到達遅延を示します。 • 値が 20 分未満の場合は、システムが正常であることを示します。 • 値が 20 分から 2 時間までの場合は、システムがビジー状態にあることを示します。 • 値が 2 時間を越える場合は、システムが非常にビジー状態にあることを示します。この状態が長く続き、遅延が長すぎると判断した場合、すべての監査データベースに対するデプロイメントを更新してデータをより高い頻度で受信するか、システムで追跡される監査イベントの数を減らすことをお勧めします。
監査スレッド使用率	Auditor CMS が監査対象からのデータ収集に費やすポーリングサイクルの割合。残りの時間は、ポーリング間の間隔です。 この値が 100% に達している場合は、次のポーリングの開始予定時に、Auditor が監査対象からデータをまだ収集していることを意味します。これにより、イベントの監査データベースへの到達が遅れる可能性があります。スレッド使用率が頻繁に 100% に達し、数日間 100% のままである場合は、デプロイメントを更新して監査データベースにより高い頻度でデータが送られるようにするか、システムで追跡される監査イベントの数を減らすことをお勧めします。
クラスタ化 *CMS* サーバ	クラスタ内で実行中の Central Management Server のホスト名とポート番号のセミコロン区切りリスト。
同時接続ユーザによって確立されたセッション数	同時接続ライセンスを持つユーザの合計セッション数。
登録ユーザによって確立されたセッション数	指定ライセンスを持つユーザの合計セッション数。
起動後のユーザセッションのピーク数	CMS の起動後に処理された同時接続ユーザセッションのピーク数。
サーバによって確立されたセッション数	BI プラットフォームサーバで CMS を使用して確立された同時接続セッション数。この数が 250 を超える場合、追加の CMS を作成します。
全ユーザによって確立されたセッション数	[メトリクス] 画面のロード時に CMS によって処理される同時接続ユーザセッション数。この数が大きいほど、システムを使用しているユーザの数が多いことになります。この数が 250 を超える場合、追加の CMS を作成します。
失敗したジョブ	システム内の失敗したジョブ数。
一時停止中のジョブ	スケジュールされているが、スケジュール時間またはイベントが来ていないため、実行の準備ができていないジョブの数。
実行中のジョブ	現在実行されているジョブ数。
完了したジョブ	システム内の完了したジョブ数。
待機中のジョブ	リソースが空くのを待機しているスケジュール済みのシステム内のジョブ数。
同時接続ユーザライセンス	キーコードによって示される同時接続ユーザライセンスの数。
登録ユーザライセンス	キーコードによって示される登録ユーザライセンスの数。

メトリクス	説明
ビルド日付	CMS のビルド日付。
システムデータベース接続名	CMS システムデータベース接続の名前。必ずしも CMS データベース自体の名前ではありません。
システムデータベースサーバ名	CMS システムデータベースが稼働しているサーバの名前。必ずしも CMS データベース自体の名前ではありません。
システムデータベースユーザ名	CMS データベースへの接続に使用されるユーザアカウントの名前。
データソース名	CMS システムデータベース接続の名前。
ビルド番号	CMS のビルド番号。この番号を使用して、インストールした SAP BusinessObjects Business Intelligence プラットフォームのバージョンを特定することができます。
製品バージョン	CMS の製品バージョン。
リソースバージョン	CMS のリソースバージョン。
起動後の平均コミット応答時間 (ミリ秒)	サーバ起動後の CMS でのコミット操作の実行に要したミリ秒単位の平均時間。応答時間が 1000 ミリ秒を超える場合、CMS または CMS システムデータベースの調整が必要である可能性を示しています。
起動後の平均クエリ応答時間 (ミリ秒)	サーバ起動後の CMS でのクエリ操作の実行に要したミリ秒単位の平均時間。応答時間が 1000 ミリ秒を超える場合、CMS または CMS システムデータベースの調整が必要である可能性を示しています。
起動後の最長コミット応答時間 (ミリ秒)	サーバ起動後の CMS でのコミット操作の実行に要したミリ秒単位の最長時間。応答時間が 10000 ミリ秒を超える場合、CMS または CMS システムデータベースの調整が必要である可能性を示しています。
起動後の最長クエリ応答時間 (ミリ秒)	サーバ起動後の CMS でのクエリ操作の実行に要したミリ秒単位の最長時間。応答時間が 10000 ミリ秒を超える場合、CMS または CMS システムデータベースの調整が必要である可能性を示しています。
起動後のコミット数	サーバ起動後の CMS システムデータベースに対するコミット数。
起動後のクエリ数	サーバ起動後のデータベースクエリの合計数。この数が大きい場合、システムにおける処理量または負荷が大きいことを示している可能性があります。
起動後のユーザログオン数	サーバ起動後のユーザログオン数。この数が大きい場合、システムにおける処理量または負荷が大きいことを示している可能性があります。
確立されたシステムデータベース接続	CMS が確立された CMS システムデータベースへの接続数。CMS データベース接続が失われると、CMS は再接続を試みます。確立されたデータベース接続の数が [要求されたシステムデータベース接続] プロパティ ([プロパティ] 画面の [*Central Management Service*] エリア) で指定されたシステムデータベース接続の数を常に下回っている場合、CMS が追加接続を取得できず、システムが最適に機能していないことを示している可能性があります。考えられる解決策は、CMS でより多くのデータベース接続を使用できるようデータベースサーバを設定することです。
現在使用しているシステムデータベース接続	CMS で現在使用されている CMS システムデータベースへの接続数。現在使用されている接続数は、確立されたシステムデータベース接続数より少ないか、同じである場合があります。確立された接続数と使用されている接続数が一定時間同じである場合、ボトルネックの発生を示している可能性があります。[プロパティ]画面の[要求されたシステムデータベース接続]プロパティの値を増やすと、CMS のパフォーマンスが改善される可能性があります。また、CMS システムデータベースの調整によってもパフォーマンスが改善される可能性があります。

メトリクス	説明
保留中のシステムデータベース要求	利用可能な接続を待機中の CMS システムデータベースに対する要求数。この数が大きい場合、[要求されたシステムデータベース接続] プロパティの値を増やすことを検討します。また、CMS システムデータベースの調整によってもパフォーマンスが改善される可能性があります。
CMS システムキャッシュ内のオブジェクト数	CMS システムキャッシュ内で現在使用されているオブジェクトの合計数。
CMS システム DB 内のオブジェクト数	CMS システムデータベース内にある、現在のオブジェクトの合計数。
既存の同時接続ユーザアカウント	クラスタ内で同時接続ライセンスを持つ既存ユーザの合計数。
既存の登録ユーザアカウント	クラスタ内で指定ライセンスを持つ既存ユーザの合計数。

36.1.3 Connection Server のメトリクス

以下のメトリクスは、Connection Server 固有のメトリクスです。

接続サービスメトリクス

メトリクス	説明
データソース	[プロパティ] ページで有効にされたデータソースをテーブルに一覧にします。各ネットワークレイヤとデータベースのペアについて以下の情報を表示します。 • [ステータス] ([ロード済] または [失敗]): ドライバの現在のステータス • 使用できる接続: 使用できるプール接続数 • *ジョブ (CORBA): 処理されているジョブ数 (2 層デプロイメント)* • *ジョブ (HTTP): 処理されているジョブ数 (Web Tier デプロイメント)* **注記** 接続プールの詳細については、データアクセスガイドを参照してください。

36.1.4 Event Server のメトリクス

次の表は、Event Server の[メトリクス]画面に表示されるサーバのメトリクスの説明を示します。

イベントサービスのメトリクス

メトリクス	説明
モニタリング中のファイルの一覧	Event Server によってモニタリングされているファイルを一覧表示する表。“ファイル名”の列には、ファイルの名前とパスが表示されます。“最終通知時刻”の列には、サーバが最後にポーリングし、ファイルの存在を確認した最新の使用日時が表示されます。
モニタリング中のファイル	Event Server によってモニタリングされているファイルの合計数。

36.1.5 File Repository Server のメトリクス

次の表は、Input/Output File Repository Server の[メトリクス]画面に表示されるサーバのメトリクスの説明を示します。

ファイルストアサービスのメトリクス

メトリクス	説明
作業中のファイル	現在アクセス中の File Repository Server のファイル数。
書き込み済みデータ *(MB)*	サーバのファイルに書き込まれた合計メガバイト数。
送信済みデータ *(MB)*	サーバ上のファイルから読み込まれた合計メガバイト数。
作業中のファイルの一覧	現在アクセス中の File Repository Server のファイルを表示する表。
アクティブな接続	クライアントから他のサーバへのアクティブな接続の合計数。
ルートディレクトリの利用可能なディスク領域 *(GB)*	サーバの実行可能ファイルを含むディスクの利用可能領域の合計 (ギガバイト)。
ルートディレクトリの空きディスク領域 *(GB)*	サーバの実行可能ファイルを含むディスクの空き領域の合計 (ギガバイト)。
ルートディレクトリの合計ディスク領域 *(GB)*	サーバの実行可能ファイルを含むディスクの合計ディスク領域 (ギガバイト)。
ルートディレクトリの利用可能なディスク領域 *(%)*	サーバの実行可能ファイルを含むディスクの利用可能なディスク領域の合計 (パーセント)。

36.1.6 Adaptive Processing Server のメトリクス

次の表は、Adaptive Processing Server の [メトリクス] 画面に表示されるサーバのメトリクスの説明を示します。

Adaptive Processing Server のメトリクス

メトリクス	説明
トランスポート層のスレッド	トランスポート層のすべてのスレッドプールにおけるスレッドの合計数。
トランスポート層のスレッドプールサイズ	共有トランスポート層スレッドの合計数。これらのスレッドは、Adaptive Processing Server のホストされたサービスのすべてで使用することができます。
利用可能なプロセッサ	サーバが実行されている Java Virtual Machine (JVM) 上で使用できるプロセッサの数。
最大メモリ *(MB)*	Java 仮想マシンが使用するメガバイト単位の最大メモリ量。
空きメモリ *(MB)*	新規オブジェクトの割り当てのため、JVM で利用できるメガバイト単位のメモリ量。
合計メモリ *(MB)*	Java 仮想マシンのメガバイト単位の総メモリ量。この値は、ホスト環境に応じて時間の経過とともに変化する可能性があります。

メトリクス	説明
CPU 使用率 *(*最後 *5* 分間*)*	直近 5 分間におけるサーバで費やされた合計 CPU 時間の割合。たとえば、単一スレッドが 4 CPU システムにおいて 1 つの CPU を完全に使用する場合、使用率は 25% になります。JVM に割り当てられたすべてのプロセッサが考慮されます。値が 80 % を超える場合は、CPU のボトルネックが考えられます。
CPU 使用率 *(*最後 *15* 分間*)*	直近 15 分間におけるサーバで費やされた合計 CPU 時間の割合。たとえば、単一スレッドが 4 CPU システムにおいて 1 つの CPU を完全に使用する場合、使用率は 25% になります。JVM に割り当てられたすべてのプロセッサが考慮されます。値が 70 % を超える場合は、CPU のボトルネックが考えられます。
GC 中の停止システムの割合 *(*最後 *5* 分間*)*	ガーベジコレクション(GC) の実行中、最後の 5 分間に停止したシステムの割合。この状態では、すべての APS サービスが実行停止し、仮想マシンによって排他的アクセスが必要とされるクリティカルな段階のガーベジコレクションが実行されます。 一般的には、負荷が発生している場合でも 1 桁の小さな数が標準的な値となるべきです。値が長期間 2 桁になっている場合、低スループットの問題が発生しており、調査が必要であることを示している可能性があります。
GC 中の停止システムの割合 *(*最後 *15* 分間*)*	ガーベジコレクション(GC)の実行中、最後の 15 分間に停止したシステムの割合。この状態では、すべての APS サービスが実行停止し、仮想マシンによって排他的アクセスが必要とされるクリティカルな段階のガーベジコレクションが実行されます。 一般的には、負荷が発生している場合でも 1 桁の小さな数が標準的な値となるべきです。値が長期間 2 桁になっている場合、低スループットの問題が発生しており、調査が必要であることを示している可能性があります。
GC 中のページフォルト数 *(*最後 *5* 分間*)*	ガーベジコレクション (GC) の実行中、最後の 5 分間に発生したページフォルトの数。この値が 0 よりも大きい場合、システムに対する負荷が大きくなっており、空きメモリの量が少ない状況を示しています。
GC 中のページフォルト数 *(*最後 *15* 分間*)*	ガーベジコレクション (GC) の実行中、最後の 15 分間に発生したページフォルトの数。この値が 0 よりも大きい場合、システムに対する負荷が大きくなっており、空きメモリの量が少ない状況を示しています。
フル *GC* の数	サーバ起動後のフルガーベジコレクションの数。この値が急激に増加している場合、システムの空きメモリの量が少ない状況を示しています。
JVM ロック競合数	アクセス待機中のスレッドを含む同期されたオブジェクトの数。この値が 0 よりも大きい場合、再実行されないスレッドが存在することを示している可能性があります。問題の原因に関する詳細を取得するには、スレッドダンプを開始します。
JVM デバッグ情報	ステータス、ポート、および存在する場合は接続されたクライアントを含む、SAP Java 仮想マシンに関するデバッグ情報。
JVM バージョン情報	SAP Java 仮想マシンに関するバージョン情報。
JVM デッドロックスレッドカウンタ	デッドロック状態のスレッドの数。この値が 0 よりも大きい場合、再実行されないスレッドが存在することを示します。問題の原因に関する詳細を取得するには、スレッドダンプを開始します。
JVM トレースフラグ	現在 JVM に対して有効化されているトレースフラグ。これは、JVM のトレースレベルを示します。
サービス	サーバがホストするサービスのカンマ区切りリスト。

DSL ブリッジサービスのメトリクス

メトリクス	説明
DSLServiceMetrics.queryCount	クライアントとサービスの間で開いているデータリクエストの数。
DSLServiceMetrics.activeConnectionCount	クライアントとサービスの間で現在開いている接続数。
DSLServiceMetrics.activeSessionCount	クライアントとサービスの間で現在開いているセッション数。
DSLServiceMetrics.activeOLAPConnection Count	OLAP クライアントとサービスの間で現在開いている接続数。

クライアント監査プロキシサービスのメトリクス

メトリクス	説明
サーバ起動後に受け取った監査イベント数	サービス起動後にサービスが受信したクライアント監査イベントの数。このメトリクスを使用して、クライアント監査が正しく設定されていることを確認することができます。値が “0” を超える場合は、クライアントからの監査イベントが、このクライアント監査サービスを通して問題なく転送されたことを示します。

プラットフォーム検索サービスのメトリクス

メトリクス	説明
サービス開始後の成功した抽出試行数	プラットフォーム検索サービスの開始後、ドキュメントの抽出に成功した数。
最終インデックス更新タイムスタンプ	インデックスが最後に更新された日付と時刻。
最終コンテンツストア生成タイムスタンプ	最終コンテンツストアが生成された日付と時刻。
サービス開始後の失敗した抽出試行数	プラットフォーム検索サービスの開始後、ドキュメントの抽出に失敗した数。
サービスは利用可能	サービスが利用可能な場合は [TRUE]。そうでない場合は、[FALSE] になります。
インデックスは実行中	インデックス化を実行中の場合は [TRUE]。そうでない場合は、[FALSE] になります。
インデックス処理済みドキュメント数	サービス開始後、インデックス化されたドキュメントの数を表示します。

Multi-Dimensional Analysis Service のメトリクス

メトリクス	説明
セッション数	MDAS クライアントからサーバへの現在の接続数。
キューブ数	タイムアウトしていない接続にデータを提供するために使用されているデータソースの数。
クエリ数	MDAS クライアントとサーバの間で開いているデータリクエストの数。

データフェデレーションサービスのメトリクス

メトリクス	説明
実行中のクエリの数	実行中のクエリの総数 (メモリを消費しているかどうかにかかわらず)。
接続数	データフェデレーションクエリエンジンへのユーザ接続の総数。
データソースから転送された総バイト数	データソースから読み込まれたデータ数 (バイト)。
データソースから転送されたレコードの総数	データソースから読み込まれた行の総数。
クエリの実行により作成された総バイト数	クエリの出力として作成されたデータ数 (バイト)。

メトリクス	説明
クエリの実行により作成されたレコードの総数	クエリの出力として作成された総行数。
メモリを消費しているクエリの数	メモリを消費しているクエリの総数。
クエリの実行に使用されたメモリの総バイト数	クエリの実行に現在使用されているメモリ数 (バイト)。
クエリの実行に使用されたディスクの総バイト数	クエリの実行に現在使用されているディスク数 (バイト)。
ディスクを使用しているクエリの数	ディスクを使用している実行中のクエリの総数。
リソース待機中のクエリの数	現在実行待機中の実行中のクエリの総数。
アクティブなスレッドの数	リクエストの実行に使用されるアクティブなスレッドの総数。
メタデータキャッシュに使用されたメモリの総バイト数	メタデータ、統計、およびコネクタ設定のキャッシュに使用されたメモリの総数 (バイト)。
失敗したクエリの数	失敗したクエリの総数 (例外の発生)。
クエリ分析ステップのクエリの数	分析ステップで現在実行中のクエリの総数。
クエリ最適化ステップのクエリの数	最適化ステップで現在実行中のクエリの総数。
クエリ実行ステップのクエリの数	実行ステップで現在実行中のクエリの総数。
ロードしたコネクタの数	サービスでロードしたコネクタの総数。
ロードしたコネクタへのアクティブな接続数	サービスでロードしたコネクタへのアクティブな接続の総数。
データフェデレーションサービスは利用可能です	サービスが利用可能な場合は [*TRUE*]。そうでない場合は、[*FALSE*]になります。

接続サービスメトリクス

メトリクス	説明
データソース	[プロパティ] ページで有効にされたデータソースをテーブルに一覧にします。各ネットワークレイヤとデータベースのペアについて以下の情報を表示します。 • ステータス (["ロード済み"] または ["失敗"]): ドライバの現在のステータス • 使用できる接続: 使用できるプール接続数 • ジョブ (CORBA): 処理されているジョブ数 (2 層デプロイメント) • ジョブ (HTTP): 処理されているジョブ数 (Web Tier デプロイメント) 接続プールの詳細については、データアクセスガイドを参照してください。

モニタリングサービスメトリクス

メトリクス	説明
最終 *15* サイクルの平均監視ステータス計算時間 *(*ミリ秒*)*	このモニタリングサービスインスタンスで、最終 15 サイクルの監視ステータスを計算するのに必要な平均時間。
ユーザが作成したメトリクスの数	すべてのユーザに対して、クラスタ内でユーザが作成したメトリクスの合計数。
監視回数	無効化された監視および有効化された監視の両方を含む、クラスタ内の監視回数。

メトリクス	説明
serviceBean.monitoringAppPropEnabled	モニタリングアプリケーションが有効化されている場合は [TRUE] になります。そうでない場合は、[FALSE] になります。このメトリクスは、CMC の [モニタリングアプリケーションのプロパティ] ページの設定と一致します。
監視メトリクスの更新間隔 (秒)	このモニタリングサービスインスタンスで現在使用されている更新間隔。サービスの開始時に、このメトリクスは、その時点の CMC の [モニタリングアプリケーションのプロパティ] ページの設定に初期化されるため、それ以外のときには、メトリクスが CMC ページの現在の設定と異なる場合があります。
サービスは利用可能	このモニタリングサービスが有効化されている場合は [TRUE] になります。そうでない場合は、[FALSE] になります。クラスタ内でアクティブなモニタリングサービスは 1 つのみです。
トレンド化されたメトリクスの数	モニタリングデータベースに現在記録されているメトリクスの合計数。

BEx Web アプリケーションサービスのメトリクス

メトリクス	説明
セッション数	BEx Web アプリケーションサービス内のアクティブなセッションの合計数。

36.1.7 Web アプリケーションコンテナサーバのメトリクス

次の表は、Web アプリケーションコンテナサーバの[メトリクス]画面に表示されるサーバのメトリクスの説明を示します。

> **注記**
>
> Web アプリケーションコンテナサーバには、Adaptive Processing Server のメトリクスセクションで示したすべてのメトリクスもあります。

Web アプリケーションコンテナサーバ のメトリクス

メトリクス	説明
実行中の *WACS* コネクタの一覧	サーバで実行中のすべてのコネクタの一覧。すべてのコネクタ(HTTP、HTTPS、プロキシ経由の HTTP)が表示されない場合、コネクタが有効化されていないか、スタートアップ時に失敗したことを示しています。
WACS コネクタがスタートアップ時に失敗しました	失敗したコネクタがあるかどうかを示します。true の場合、1 つ以上のコネクタが起動に失敗しています。false の場合、すべてのコネクタが実行中です。接続に失敗したコネクタが 1 つ以上ある場合は、サーバを実行しないでください。サーバのトラブルシューティングをして、すべてのコネクタが正しく起動されるようにする必要があります。

関連情報

Adaptive Processing Server のメトリクス [1148 ページ]

36.1.8 Adaptive Job Server のメトリクス

Job Server のメトリクス

メトリクス	説明
受信したジョブリクエスト	サーバで実行される必要があったジョブの数。
同時に実行可能なジョブ	サーバで現在実行中のジョブの数。この数が多い場合、サーバは混み合っています。
ピークジョブ	サーバで同時に実行された同時実行ジョブの最大数。この数は、サーバが再起動されるまで減少することはありません。
作成に失敗したジョブ	サーバで失敗したジョブの数。
一時ディレクトリ	一時ファイルが作成されるディレクトリ。これは、サーバの[プロパティ]画面で指定することができます。 このディレクトリに十分なディスク領域がない場合、問題が発生する場合があります。
ファイルシステム出力先のデフォルト設定が有効	サーバの [出力先] 画面で指定されたファイルシステム出力先にサーバがドキュメントを送信できる場合、[*TRUE*] になります。そうでない場合は、[*FALSE*] になります。
FTP 出力先のデフォルト設定が有効	サーバの [出力先] 画面で指定された FTP サーバ出力先にサーバがドキュメントを送信できる場合、[*TRUE*] になります。そうでない場合は、[*FALSE*] になります。
SFTP 出力先のデフォルト設定が有効	サーバの [出力先] 画面で指定された SFTP サーバ出力先にサーバがドキュメントを送信できる場合、[*TRUE*] になります。そうでない場合は、[*FALSE*] になります。 フィンガープリントが SFTP サーバと正確に一致しない場合、問題が発生することがあります。
受信トレイ送信先のデフォルト設定が有効	サーバの [出力先] 画面で指定された受信ボックス送信先にサーバがドキュメントを送信できる場合、[*TRUE*] になります。そうでない場合は、[*FALSE*] になります。
電子メール送信先のデフォルト設定が有効	サーバの [出力先] 画面で指定された電子メール送信先にサーバがドキュメントを送信できる場合、[*TRUE*] になります。そうでない場合は、[*FALSE*] になります。
スケジュールサービス	サーバで実行中のサービスを表示する表。
子	サーバで実行中の子プロセスを表示する表。

次の表は、サーバで実行中の各スケジュールサービスのメトリクスの説明を示します。

スケジューリングサービスのメトリクス

メトリクス	説明
スケジュールサービス	サービス名。
受信したジョブリクエスト	サービスで実行される必要があったジョブの数。
同時に実行可能なジョブ	サービスで現在実行中の同時に実行可能なジョブの数。この数が多い場合、サービスは混み合っています。

メトリクス	説明
ピークジョブ	サービスで同時に実行された同時実行ジョブの最大数。
同時実行ジョブの最大数	サーバが許可する同時に実行可能な独立したプロセス(子プロセス)の数。 これは、サーバの [プロパティ] 画面で指定することができます。
作成に失敗したジョブ	サービスで失敗したジョブの数。

次の表は、サーバで実行中の各子プロセスのメトリクスの説明を示します。

子メトリクス

メトリクス	説明
スケジュールサービス	子プロセスの名前。
PID	子プロセスの ID。
受信したジョブリクエスト	子プロセスで実行される必要があったジョブの数。
同時に実行可能なジョブ	子プロセスで現在実行中の同時に実行可能なジョブの数。通常、この数は “1” である必要があります。
ピークジョブ	子プロセスで同時に実行された同時実行ジョブの最大数。
最大ジョブ数	子プロセスが許可する同時実行ジョブの数。
Comm. 失敗	親 Adaptive Job Server との間で発生した通信エラーの数。この数が多い場合、子プロセスは再起動されます。
初期化中	子プロセスが初期化中である場合は、[*TRUE*] になります。そうでない場合は、[*FALSE*] になります。
シャットダウン中	子プロセスがシャットダウン中である場合、[*TRUE*] になります。そうでない場合は、[*FALSE*] になります。

36.1.9 Crystal Reports Server のメトリクス

次の表は、Crystal Reports Processing および Crystal Reports 2020 Processing Server の [メトリクス] 画面に表示されるサーバのメトリクスの説明を示しています。

Crystal Reports Processing Server のメトリクス

メトリクス	説明
開いているジョブ	現在サーバ上で実行中のジョブを表示する表。表には、ドキュメントの ID と名前、ジョブを実行しているユーザの名前、ドキュメントが最後にアクセスされた日付、ジョブの実行経過時間が含まれています。
処理されたリクエスト数	サーバ起動後にサーバが処理したリクエストの合計数。
開いているジョブ数	サーバとその子プロセスが現在処理しているジョブの数。
オブジェクトの種類	サーバが主に処理する InfoObject の種類。このメトリクスの値は変わりません。

メトリクス	説明
平均処理時間 (ミリ秒)	サーバが受け取った直近の 500 リクエストの処理に費やした平均時間 (ミリ秒)。この数字が、常に高く、増加する場合は、他のマシンに追加サーバを構築することを検討してください。
最大処理時間 (ミリ秒単位)	サーバが直近 500 リクエストの 1 つの処理に費やした最大時間 (ミリ秒)。この数字が、常に高く、増加する場合は、他のマシンに追加サーバを構築することを検討してください。
最小処理時間 (ミリ秒)	サーバが直近 500 リクエストの 1 つの処理に費やした最小時間 (ミリ秒)。この数字が、常に高く、増加する場合は、他のマシンに追加サーバを構築することを検討してください。
キュー内のリクエスト数	処理待機中、または処理中のリクエストの数。この数字が、常に高く、増加する場合は、他のマシンに追加サーバを構築することを検討してください。
オブジェクト *DLL* 名	サーバのプラグインの処理名。このメトリクスの値は変わりません。
開いている接続数	サーバとクライアント間で現在開いている接続数。
リクエスト失敗率	サーバが受信した直近 500 リクエストに対して、サーバが処理に失敗したリクエスト数。
データ転送 *(KB)*	サーバ起動後にクライアントに転送されるデータの合計数 (キロバイト)。
失敗したリクエスト数	サーバ起動後にサーバが完了できなかったリクエストの数。
子プロセスの最大数	サーバで許可される同時実行子プロセスの最大数を示します。

次の表は、Crystal Reports Cache Server の [メトリクス] 画面に表示されるサーバのメトリクスの説明を示します。

Crystal Reports Cache Server のメトリクス

メトリクス	説明
キャッシュヒット率 *(%)*	キャッシュされたデータを使って処理された、直近の 500 リクエストに対するリクエストの割合。
接続済み処理サーバ	デプロイメント内の Crystal Reports Processing Server を表示する表。この表は、サーバ名と、サーバで現在開いている接続数を示します。
処理されたリクエスト数	サーバ起動後にサーバが処理したリクエストの合計数。
オブジェクトの種類	サーバが主に処理する InfoObject の種類。このメトリクスの値は変わりません。
平均処理時間 (ミリ秒)	サーバが受け取った直近の 500 リクエストの処理に費やした平均時間 (ミリ秒)。この数字が、常に高く、増加する場合は、他のマシンに追加サーバを構築することを検討してください。
最大処理時間 (ミリ秒)	サーバが直近 500 リクエストの 1 つの処理に費やした最大時間 (ミリ秒)。この数字が、常に高く、増加する場合は、他のマシンに追加サーバを構築することを検討してください。
最小処理時間 (ミリ秒)	サーバが直近 500 リクエストの 1 つの処理に費やした最小時間 (ミリ秒)。この数字が、常に高く、増加する場合は、他のマシンに追加サーバを構築することを検討してください。
キュー内のリクエスト数	処理待機中、または処理中のリクエストの数。この数字が、常に高く、増加する場合は、他のマシンに追加サーバを構築することを検討してください。
オブジェクト *DLL* 名	サーバのプラグインの処理名。このメトリクスの値は変わりません。

メトリクス	説明
キャッシュサイズ	サーバで現在ディスクにキャッシュされているデータの合計数 (キロバイト)。
開いている接続数	サーバとクライアント間で現在開いている接続数。
データ転送 *(KB)*	サーバ起動後にクライアントに転送されるデータの合計数 (キロバイト)。

次の表は、Crystal Reports 2020 Report Application Server の [メトリクス] 画面に表示されるサーバのメトリクスの説明を示しています。

Crystal Reports 2020 Report Application Server のメトリクス

メトリクス	説明
metric_currentdoccount **注記** このメトリクスは、CMC の [モニタリング] ページに “document_s_” として表示されます。	サーバで現在処理中のドキュメントの数。
metric_totaldoccount **注記** このメトリクスは、CMC の [モニタリング] ページに “document_s_” として表示されます。	サーバ起動後にサーバで処理されたドキュメントの数。
metric_currentagentthreadcount **注記** このメトリクスは、CMC の [モニタリング] ページに “agent thread_s_” として表示されます。	サーバで現在処理中のスレッドの数。
metric_totalagentthreadcount **注記** このメトリクスは、CMC の [モニタリング] ページに “agent thread_s_” として表示されます。	サーバ起動後にサーバで処理されたスレッドの数。

36.1.10 Web Intelligence サーバのメトリクス

Web Intelligence 処理サービスのメトリクス

メトリクス	説明
キャッシュサイズ *(Kb)*	キャッシュに保存されている現在のデータ数 (KB)。

メトリクス	説明
キャッシュ内の古いドキュメントの数	サーバ起動後に古すぎたためにキャッシュから削除されたドキュメントの数。
キャッシュが最大サイズに達した回数	サーバ起動後にキャッシュが許容最大サイズに達した回数。
CPU 使用率 *(%)*	サーバ起動後にサーバによって費やされた合計 CPU 時間の割合。
合計 *CPU* 時間 *(秒)*	サーバ起動後にサーバによって費やされた合計 CPU 時間 (秒)。
メモリ高しきい値数	サーバ起動後にサーバで高メモリしきい値に達した回数。
メモリの最大しきい値数	サーバ起動後にサーバで最大メモリしきい値に達した回数。
仮想メモリサイズ *(Mb)*	サーバに割り当てられた総メモリ量 (MB)。
現在のクライアント呼び出し数	サーバが現在処理している CORBA 呼び出し数。
リモート拡張エラー数	サーバが、Adaptive Processing Server がホストするリモート拡張サービスに接続できなかった回数。
現在のタスク数	サーバで現在実行されているタスク数。
合計クライアント呼び出し数	サーバ起動後にサーバが受信した CORBA 呼び出しの総数。
合計タスク数	サーバ起動後にサーバで実行されたタスクの総数。
アイドル時間 *(秒)*	サーバがクライアントから最後のリクエストを受信してからの経過時間 (秒)。
現在のアクティブセッション数	現在クライアントからのリクエストを受け付けられるセッションの数。
キャッシュから開いたドキュメントの数	最後のリクエスト結果がキャッシュから直接読み込まれたドキュメントの数。
ドキュメント数	サーバで現在開いているドキュメントの数。
現在のセッション数	サーバで現在作成されているセッション数。
ドキュメント交換の数	クリーンアップスレッドにスケジュールされたスワップリクエストがあるドキュメントの数。
交換されたドキュメントの数	スワップリクエストによってスワップされたドキュメントの数。
セッションタイムアウト数	サーバ起動後にタイムアウトしたセッション数。
合計セッション数	サーバ起動後にサーバ上に作成されたセッション数。
ユーザ数	サーバに接続したユーザの総数。
アクティブなスレッドの数	サーバが受け取ったリクエストを処理するスレッドの数 (非同期性スレッドプール)。
合計スレッド数	サーバ起動後に作成されたスレッド総数 (非同期性スレッドプール)。

37 サーバおよびノードのプレースホルダに関する付録

37.1 サーバとノードプレースホルダ

%SERVER_FRIENDLY_NAME% および *%SERVER_NAME%* を除き、次のプレースホルダは、同じノード上のすべてのサーバに適用されます。

> **注記**
>
> 以下のプレースホルダはノードレベルで編集できます。説明とデフォルト値は、上記の表に記載されています。この一覧にないプレースホルダは、読み取り専用です。
>
> - *%DefaultAuditingDir%*
> - *%DefaultDataDir%*
> - *%DefaultLoggingDir%*
> - *%IntroscopeAgentEnableInstrumentation%*
> - *%IntroscopeAgentEnterpriseManagerHost%*
> - *%IntroscopeAgentEnterpriseManagerPort%*
> - *%IntroscopeAgentEnterpriseManagerTransport%*
> - *%NCSInstrumentLevelThreshold%*
> - *%SMDAgentHost%*
> - *%SMDAgentPort%*

> **警告**
>
> 編集用以外のプレースホルダは、いかなる手段でも変更しないでください。システム管理者は、(ノード管理を目的とする) 管理者グループの適切な担当者のみがノードに対する編集権限を持っていることを確認する必要があります。管理者グループの他のメンバーを含むすべてのユーザは、適切なセキュリティ権限を適用することで、ノードオブジェクトの表示/管理を制限する必要があります。プレースホルダ値のいずれかが誤って破損し、CMS が起動しない場合は、SAP ノート 3269127 を参照してください。

> **注記**
>
> BI ランドスケープへの悪意のある干渉を回避するためにプレースホルダの変更を制限する方法については、以下の SAP Knowledge Base Article 3278916 を参照してください。

プレースホルダ

プレースホルダ	説明	デフォルト値
%AuditingDatabaseConnection%	CMS によって使用される監査データベース接続。	この値は、インストール時に指定されます。

プレースホルダ	説明	デフォルト値
%AuditingDatabaseDriver%	監査データベースへの接続に使用されるデータベースドライバの種類。	Windows では、デフォルト値は sqlserverauditdbss です。
%BINDIR%	SAP BusinessObjects Business Intelligence プラットフォームの 64 ビットバイナリが格納されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/` です。
%BINDIR32%	SAP BusinessObjects Business Intelligence プラットフォームの 32 ビットバイナリが格納されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>/` です。
%CACHESERVER_EXE%	Crystal Reports Cache Server の実行可能ファイル名。	Windows では、`crcache.exe` です。UNIX では、`boe_crcached.bin` です。
%CMS_EXE%	Central Management Server の実行可能ファイル名。	Windows では、`cms.exe` です。UNIX では、`boe_cmsd` です。
%CONNECTIONSERVER32_EXE%	32 ビット Connection Server の実行可能ファイル名。	Windows では、`ConnectionServer32.exe` です。UNIX では、`ConnectionServer32` です。
%CONNECTIONSERVER_DIR%	Connection Server のルートフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥dataAccess¥connectionServer` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer` です。
%CONNECTIONSERVER_EXE%	64 ビット Connection Server の実行可能ファイル名。	Windows では、`ConnectionServer.exe` です。UNIX では、`ConnectionServer` です。
%CRCPP_BINDIR%	Crystal Reports C++ サーババイナリが保存されるディレクトリ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjectsEnterprise XI 4.0¥win32_x86` です。UNIX では、ディレクトリは次のようになります。`<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`。

プレースホルダ	説明	デフォルト値
%CRCPP_DefaultWorkingDir%	Crystal Reports C++ サーバのデフォルトの作業ディレクトリ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjectsEnterprise XI 4.0¥win32_x86` です。UNIX では、ディレクトリは次のようになります。`<INSTALLDIR>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9`。
%CRYSTALRAS_EXE%	Report Application Server の実行可能ファイル名。	Windows では、`crystalras.exe` です。UNIX では、`boe_crystalrasd` です。
%CR_ODBCINI%	`.odbc.ini` ファイルの名前とパスが保存されます。	UNIX では、`<INSTALLDIR>/bobje/odbc.ini` です。Windows では、これは空の文字列です。
%CommonJavaBundlesDir%	共有 OSGI バンドルが保存されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib¥bundles` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/bundles` です。
%CommonJavaLibDir%	共通 Java ライブラリが保存されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib` です。
%DLLEXT%	`.dll` または `.so` ファイルのデフォルトの拡張子。	Windows では、`.dll` です。UNIX では、`.so` です。
%DLLPATH%	インタプリタが実行可能ファイルを検索するディレクトリを指定する、SAP BusinessObjects Business Intelligence プラットフォームがインストールされたコンピュータの環境変数の名前。	Windows では、“Path” です。UNIX では、“LD_LIBRARY_PATH” です。
%DLLPATH32%	Solaris 32 ビットシステムで、インタプリタが実行可能ファイルを検索するディレクトリを指定する、SAP BusinessObjects Business Intelligence プラットフォームがインストールされたコンピュータの環境変数の名前。	Solaris マシンでは、“LD_LIBRARY_PATH_32” です。他のオペレーティングシステムでは、このプレースホルダは空の文字列です。
%DLLPATH64%	Solaris 64 ビットシステムで、インタプリタが実行可能ファイルを検索するディレクトリを指定する、SAP BusinessObjects Business Intelligence プラットフォームがインストールされたコンピュータの環境変数の名前。	Solaris マシンでは、“LD_LIBRARY_PATH_64” です。他のオペレーティングシステムでは、このプレースホルダは空の文字列です。

プレースホルダ	説明	デフォルト値
%DLLPREFIX%	`.dll` または `.so` ファイルのデフォルトのプレフィックスです。	UNIX では、“lib” です。このプレースホルダは、Windows マシンでは空の文字列です。
%DLLPRELOAD%	プラットフォーム向けの LD_PRELOAD 環境変数名。	UNIX では、*LD_PRELOAD* です。このプレースホルダは、Windows マシンでは空の文字列です。
%DLLPRELOAD32%	32 ビット AIX システム向けの LD_PRELOAD 環境変数名。	AIX では、*LDR_PRELOAD* です。このプレースホルダは、他のマシンでは空の文字列です。
%DLLPRELOAD64%	64 ビット AIX システム向けの LD_PRELOAD 環境変数名。	AIX では、*LDR_PRELOAD64* です。このプレースホルダは、他のマシンでは空の文字列です。
%DP%	パスの区切り記号。	Windows では、“;” です。UNIX では、“:” です。
%DefaultAuditingDir%	監査一時ファイルが書き込まれるディレクトリ。最適なパフォーマンスのため、この場所はサーバのローカルドライブにある必要があります。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Auditing` です。UNIX では、`<INSTALLDIR>/sap_bobj/data/Auditing/` です。
%DefaultDataDir%	Job Server で使用される一時ディレクトリ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Data` です。UNIX では、`<INSTALLDIR>/sap_bobj/data/` です。
%DefaultInputFRSDir%	Input File Repository Server のルートフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥FileStore¥Input` です。UNIX では、`<INSTALLDIR>/sap_bobj/data/frsinput` です。
%DefaultLoggingDir%	ログファイルの保存場所。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥logging` です。UNIX では、`<INSTALLDIR>/sap_bobj/logging` です。
%DefaultOutputFRSDir%	Output File Repository Server のルートフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥FileStore¥Output` です。UNIX では、`<INSTALLDIR>/sap_bobj/data/frsoutput` です。
%DefaultWorkingDir%	64 ビットサーバの作業ディレクトリ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>` です。

プレースホルダ	説明	デフォルト値
%DefaultWorkingDir32%	32 ビットサーバの作業ディレクトリ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform>` です。
%EPM_LD_PRELOAD_ONCE%	プラットフォーム向けの LD_PRELOAD_ONCE 環境変数名。	$LD_PRELOAD_ONCE$
%EVENTSERVER_EXE%	Event Server の実行可能ファイル名。	Windows では、`EventServer.exe` です。UNIX では、`boe_eventsd` です。
%EXEEXT%	実行可能ファイルのデフォルトの拡張子。	Windows では、`.exe` です。このプレースホルダは、UNIX では使用できません。
%EXEPATH%	インタプリタが実行可能ファイルを検索するディレクトリを指定する、SAP BusinessObjects Business Intelligence プラットフォームがインストールされたコンピュータの環境変数の名前。	Windows では、“Path” です。UNIX では、“PATH” です。
%EnterpriseDir%	64 ビットの SAP BusinessObjects Business Intelligence プラットフォームがインストールされる場所。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40` です。
%EnterpriseDir32%	32 ビットの SAP BusinessObjects Business Intelligence プラットフォームがインストールされる場所。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40` です。
%ExternalJavaLibDir%	外部のサードパーティ Java ライブラリが保存されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥lib¥external` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/java/lib/external` です。
%FILESERVER_EXE%	File Server の実行可能ファイル名。	Windows では、`fileserver.exe` です。UNIX では、`boe_filesd` です。
%HOARD_PATH%	メモリマネージャの場所。	デフォルトでは、この値は空になっています。
%HOARD_PRELOAD%	メモリマネージャを事前にロードするかどうかを指定します。	デフォルトでは、この値は空になっています。
%INSTALLROOTDIR%	64 ビットの SAP BusinessObjects Business Intelligence プラットフォームがインストールされるフォルダ。	この値は、インストール時に指定されます。

プレースホルダ	説明	デフォルト値
%INSTALLROOTDIR32%	32 ビットの SAP BusinessObjects Business Intelligence プラットフォームがインストールされるフォルダ。	この値は、インストール時に指定されます。
%IntroscopeAgentEnableInstrumentation%	Introscope Agent Enterprise Manager を使用した Java サーバの計測が有効化されているかどうかを示します。	可能な値は、SAP BusinessObjects Business Intelligence プラットフォームがインストールされたときに Introscope Agent Enterprise Manager が有効化されたかどうかによって、TRUE または FALSE に設定されます。
%IntroscopeAgentEnterpriseManagerHost%	計測データが送信される Introscope Agent Enterprise Manager ホスト名。	この値は、インストール時に指定されます。
%IntroscopeAgentEnterpriseManagerPort%	計測データが送信される Introscope Agent Enterprise Manager ポート。	この値は、インストール時に指定されます。
%IntroscopeAgentEnterpriseManagerTransport%	Introscope Agent Enterprise Manager への計測データの送信時に使用されるトランスポート。可能な値は次のとおりです。 • TCP • HTTP • HTTPS • SSL	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	Introscope Agent Enterprise Manager に HTTP 経由で計測データの送信時に使用されるクラス。	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	Introscope Agent Enterprise Manager に HTTPS 経由で計測データの送信時に使用されるクラス。	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportSSL%	Introscope Agent Enterprise Manager に SSL 経由で計測データの送信時に使用されるクラス。	com.wily.isengard.postofficehub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	Introscope Agent Enterprise Manager に TCP 経由で計測データの送信時に使用されるクラス。	com.wily.isengard.postofficehub.link.net.DefaultSocketFactory
%IntroscopeDir%	Introscope Agent Enterprise Manager がインストールされたフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥wily` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/java/wily` です。
%JAVAW_EXE%	コンソールウィンドウのない Java 仮想マシン (JVM) の実行可能ファイル名。	Windows では、`javaw.exe` です。UNIX では、`java` です。
%JAVA_EXE%	Java 仮想マシン (JVM) の実行可能ファイル名。	Windows では、`java.exe` です。UNIX では、`java` です。

プレースホルダ	説明	デフォルト値
%JOBSERVERCHILD_EXE%	Adaptive Job Server の子の実行可能ファイル名。	Windows では、`JobServerChild.exe` です。UNIX では、`boe_jobcd` です。
%JOBSERVER_EXE%	Adaptive Job Server の実行可能ファイル名。	Windows では、`JobServer.exe` です。UNIX では、`boe_jobsd` です。
%JdkBinDir%	JDK バイナリが保存されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥bin` です。UNIX では、`<INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/bin` です。
%JreBinDir%	JRE バイナリが保存されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win64_x64¥sapjvm¥jre¥bin` です。UNIX では、`<INSTALLDIR>/sap_bobj/<PLATFORM>/sapjvm/jre/bin` です。
%JVM_ARCH_ENVIRONMENT%	マシンが 32 ビットと 64 ビットのどちらの JVM で実行されているかを示します。	32 ビット UNIX マシンの場合、デフォルト値は “-d32” です。64 ビットマシンの場合、デフォルト値は “-d64” です。Windows マシンでは、これは空の文字列です。
%JVM_HEADLESS_MODE%	JVM がヘッドレスモードで機能するかどうかを指定するコマンドライン引数。	Windows では、-Djava.awt.headless=false です。UNIX では、-Djava.awt.headless=true です。
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	メモリ不足エラーが発生した場合の JVM の動作を指定するコマンドラインパラメータ。	"-XX:+HeapDumpOnOutOfMemoryError" "-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"
%JVM_SHARED_MEMORY_SEGMENT%	JVM 拡張を有効にし、JVM のインスタンス数を設定するコマンドラインパラメータ。	デフォルトでは、このプレースホルダは空白になっています。
%LANGUAGEPACKSDIR%	デプロイメントの言語パックがインストールされるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Languages` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/` です。

プレースホルダ	説明	デフォルト値
%LANGUAGEPACKSDIR32%	32 ビットシステムで、デプロイメントの言語パックがインストールされるフォルダ。	.Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥Languages` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/Languages/` です。
%LSTDir%	LST 設定ファイルが保存されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥conf¥lst` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/lst` です。
%MDAS_JVM_OS_STACK_SIZE%	多次元分析サービスの JVM スタックサイズを指定します。	デフォルトでは、このプレースホルダは空になっています。
%NCSInstrumentLevelThreshold%	NCS ライブラリのトレースロギングのしきい値レベル。	デフォルトでは、この値は 0 になっています。
%PAGESERVER_EXE%	Crystal Reports 2020 Processing Server の実行可能ファイル名。	Windows では、`crproc.exe` です。UNIX では、`boe_crprocd.bin` です。
%PJSContainerDir%	APS コンテナ JAR が保存されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥container` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/container` です。
%PJSServicesDir%	APS サービス JAR が保存されるフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥java¥pjs¥services` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/java/pjs/services` です。
%Platform%	SAP BI プラットフォームが稼働しているマシンのオペレーティングシステム。	SAP BI プラットフォームが稼働しているマシンのオペレーティングシステム。
%Platform32%	32 ビットの SAP BI プラットフォームが稼働しているマシンのオペレーティングシステム。	SAP BI プラットフォームが稼働しているマシンのオペレーティングシステム。
%RasBinDir%	Report Application Server のルートフォルダ。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥win32_x86` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/<PLATFORM>/ras` です。
%SERVER_FRIENDLY_NAME%	サーバのフルネーム。	サーバのフルネーム。
%SERVER_NAME%	サーバのフルネーム。	サーバのフルネーム。

プレースホルダ	説明	デフォルト値
%SMDAgentHost%	計測データが送信される SMD Agent ホスト名。	この値は、インストール時に指定されます。
%SMDAgentPort%	計測データが送信される SMD Agent ポート。	この値は、インストール時に指定されます。
%TRACE_CONFIGFILE_INI%	`BO_Trace.ini` ファイルの名前とパス。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥conf¥BO_trace.ini` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/BO-trace.ini` です。
%WarFilesDir%	Web アプリケーションファイルの場所。	Windows では、`<INSTALLDIR>¥SAP BusinessObjects Enterprise XI 4.0¥warfiles¥webapps` です。UNIX では、`<INSTALLDIR>/sap_bobj/enterprise_xi40/warfiles/webapps` です。
%WEBI_LD_PRELOAD%	プラットフォーム向けの LD_PRELOAD 環境変数名。	$LD_PRELOAD$
%WEBISERVER_EXE%	Web Intelligence Processing Server の実行可能ファイル名。	Windows では、`wireportserver.exe` です。UNIX では、`WIReportServer` です。
%WEBI_LD_PRELOAD_ONCE%	プラットフォーム向けの LD_PRELOAD_ONCE 環境変数名。	$LD_PRELOAD_ONCE$

関連情報

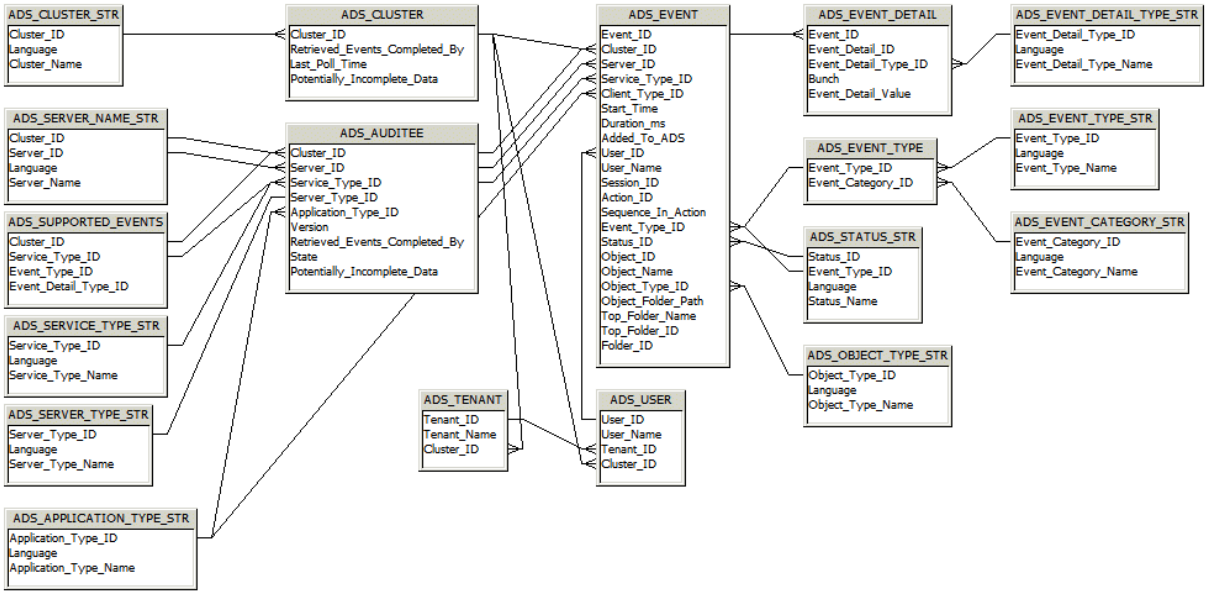
ノードのプレースホルダを表示および編集する [481 ページ]

38 監査データストアスキーマに関する付録

38.1 概要

この付録は、監査データストアテーブルにアクセスしてレポートを作成するレポート作成者向けのリファレンスです。以下の図およびテーブルの説明は、監査データが記録されるテーブル、およびそれらのテーブルの関連性を示しています。

38.2 スキーマ図



38.3 Auditing Data Store Tables

ADS_APPLICATION_TYPE_STR table

This table provides a multilingual dictionary of client application-type names.

Column Name	Type	Description
Application_Type_ID	Character (64)	The application-type CUID for the application.
Language	Character (10)	Code for the language in which the application type is recorded; for example `<EN>`, or `<DE>`.
Application_Type_Name	Character (255)	The text name of the application type; Crystal Reports or Web Intelligence for example.

ADS_AUDITEE table

This table records property information for all auditee servers that are part of the deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID for the cluster the auditee belongs to.
Server_ID	Character (64)	CUID of the server that triggered the event. If the event is client-triggered, will record the CUID of the adaptive processing server that processed the event.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. Client-triggered events will record an application-type CUID.
Server_Type_ID	Character (64)	The server-type CUID for the server that triggered the event.
Application_Type_ID	Character (64)	The application-type CUID for the client that triggered the event. For server events, the ID of the service-type will be recorded.
Version	Character (64)	The version of the server or client that triggered the event at the time it was recorded.
Retrieved_Events_Completed_By	Datetime	The last time the Auditor CMS polled this auditee for its temporary files. This indicates that all events from this auditee competed prior to this date/time are in the ADS.
State	Integer	The state (Running, Not Running, Deleted) that the auditee was in.
Potentially_Incomplete_Data	Integer	Shows if this auditee may have events that were not transferred to the ADS.

ADS_CLUSTER table

This table records information on any clusters that contain Auditees.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.

Column Name	Type	Description
Retrieved_Events_Completed_By	Datetime	Shows how current the auditing information in the database for that cluster is. Records the oldest retrieved auditing timestamp for all currently running auditee servers at any given moment. This indicates all events completed prior to this date are in the ADS.
Last_Poll_Time	Datetime	The last time the auditor CMS polled the auditees in this cluster.
Potentially_Incomplete_Data	Integer	Indicates potentially incomplete audit information within the cluster: "0" = all servers have transferred data normally; and "1" = at least one running or non-running server in the cluster has its *Potentially Incomplete Data* flag set, meaning that one auditee has events that haven't transferred to the ADS.

ADS_CLUSTER_STR table

This table provides a reference record of the different clusters in your deployment.

Column Name	Type	Description
Cluster_ID	Character (64)	A unique ID of the cluster.
Language	Character (10)	Code for the language setting for the cluster, for example, `<EN>`, or `<DE>`.
Cluster_Name	Character (255)	The name of the cluster.

ADS_EVENT table

This table records the basic properties for each event, and is the central linking point for other tables in the schema.

Column Name	Type	Description
Event_ID	Character (64)	A unique ID generated for the event.
Cluster_ID	Character (64)	The GUID of the auditee's cluster. This is recorded because multiple clusters may use the same ADS.
Server_ID	Character (64)	The CUID of the server that triggered the event.
Service_Type_ID	Character (64)	• The CUID of the service-type that triggered the event. Services on a server will record their service-type CUID. • Client applications (BI launch pad or Web Intelligence for example) will record their application-type CUID.
Client_Type_ID	Character (64)	Records the Client Type ID of the client that established the session.

Column Name	Type	Description
Start_Time	Datetime	The date and time (UTC) when the event operation started (including milliseconds).
Duration_ms	Integer	Duration of operation in milliseconds. Value may be zero (0) for certain events. For Example: with View event type, if the document gets loaded quickly, the value will be `0`.
Added_to_ADS	Datetime	The date and time (UTC) when the event was recorded in the ADS.
User_ID	Character (64)	The CUID of the user who performed the action.
User_Name	Character (255)	The name associated with the ID of the user who performed the action. Recorded in the Auditor CMS's default language.
Session_ID	Character (64)	GUID of the session during which the event was triggered. If there is no associated session, the field will be null.
Action_ID	Character (64)	ID of the user action that triggered the event. Used to group events that result from a single user action.
Sequence_In_Action	Integer	For multi-server (or client and multi-server) events, the server or client application in the sequence that triggered the event. In all scheduling workflows the sequence ID will always be 0.
Event_Type_ID	Integer	Type of event (View or Save, for example).
Status_ID	Integer	Status of the operation (for example, "0" = succeeded, "1" = failed).
Object_ID	Character (64)	CUID of the object that the operation was performed on.
Object_Name	Character (255)	The name of the object the operation was performed on. Recorded in the Auditor CMS's default language.
Object_Type_ID	Character (64)	CUID of object-type that the operation was performed on.
Object_Folder_Path	Character (255)	The full folder path (for example `Country/Region/City`) for the object the operation was performed on. Recorded in the Auditor CMS's default language. If the folder path cannot be determined this, value will be set to null.
Folder_ID	Character (64)	The CUID of the folder for the object the operation was performed.
Top_Folder_Name	Character (255)	Name of top level folder for the object. For example, if the object is located in `Country/Region/City` then `Country` will be recorded.
Top_Folder_ID	Character (64)	The CUID of the top-level folder where the object resides. For example, if object is located in `Country/Region/City` then the CUID of the `Country` folder will be recorded.

ADS_EVENT_CATEGORY_STR Table

This table provides a multilingual dictionary of event category names.

Column Name	Type	Description
Event_Category_ID	Integer	The event-category ID.
Language	Character (10)	Code for the language that the event category name is recorded in; for example `<EN>`, or `<DE>`.
Event_Category_Name	Character (255)	The name of the event category.

ADS_EVENT_DELETES

Do not use or report off of this table. It is intended for internal system use, and may be removed in future releases.

ADS_EVENT_DETAIL table

This table records event detail properties.

Column Name	Type	Description
Event_Detail_ID	Integer	GUID for the event detail.
Event_ID	Character (64)	Parent event GUID.
Event_Detail_Type_ID	Integer	Type of event detail.
Bunch	Integer	If the detail is part of a series, this is used to tie them together. For example, if a report had prompts for State and Country, a user may enter "USA" for the Country prompt, and "California" and "Nevada" for the State prompt. This would produce event details with two bunches. Bunch 1 would consist of: • Prompt Name: Country • Prompt Value: USA Bunch 2 would consist of: • Prompt Name: State • Prompt Value: California • Prompt Value: Nevada
Event_Detail_Value	Character (longtext)	The value of the event detail.

ADS_EVENT_DETAIL_TYPE_STR table

This table provides a multilingual dictionary of event detail type names.

Column Name	Type	Description
Event_Detail_ID	Integer	The event detail-type ID for the event detail.
Language	Character (10)	Code for the language that the event detail name is recorded in; for example `<EN>`, or `<DE>`.
Event_Detail_Type_Name	Character (255)	The text name of the event detail type.

ADS_EVENT_TYPE table

This table provides a reference record for the different categories of events.

Column Name	Type	Description
Event_Type_ID	Integer	The unique identifier for the type of event.
Event_Category_ID	Integer	Category of event. For example, common, Web Intelligence, or Life-Cycle Management.

ADS_EVENT_TYPE_STR Table

This table provides a multilingual dictionary of event type names.

Column Name	Type	Description
Event_Type_ID	Integer	The event-type ID for the event.
Language	Character (10)	Code for the language that the event category name is recorded in; for example `<EN>`, or `<DE>`.
Event_Type_Name	Character (255)	The text name of the event type; View or Logon for example.

ADS_OBJECT_TYPE_STR Table

This table provides a multilingual dictionary of event object names.

Column Name	Type	Description
Object_Type_ID	Character (64)	Object-type CUID of the object
Language	Character (10)	Code for the language that the object type name is recorded in; for example `<EN>`, or `<DE>`.
Object_Type_Name	Character (255)	Name of the object type.

ADS_SERVER_NAME_STR table

This table provides a multilingual dictionary of server names. Values will be updated when servers are renamed.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster that the server belongs to.
Server_ID	Character (64)	The CUID of the server.
Language	Character (10)	Code for the language of the server name; for example `<EN>`, or `<DE>`.
Server_Name	Character (255)	The name of the server.

ADS_SERVICE_TYPE_STR table

This table provides a multilingual dictionary of service-type names.

Column Name	Type	Description
Service_Type_ID	Character (64)	The service-type or service-category CUID for the service.
Language	Character (10)	Code for the language the service-type name is recorded in, for example `<EN>`, or `<DE>`.
Service_Type_Name	Character (255)	The name of the service-type.

ADS_STATUS_STR Table

This table provides a multilingual dictionary of event status names.

Column Name	Type	Description
Status_ID	Integer	The numerical representation of the operation's status.
Event_Type_ID	Integer	ID of the event's event-type. For example, 1002 for View.
Language	Character (10)	Code for the language that the event status is recorded in; for example `<EN>`, or `<DE>`.
Status_Name	Character (255)	A text description of the event's status; Succeeded or Failed, for example.

ADS_SUPPORTED_EVENTS table

This table records a list of supported events and associated event details for each type of service or client application.

Column Name	Type	Description
Cluster_ID	Character (64)	The cluster GUID that the service belongs to.
Service_Type_ID	Character (64)	Service-type CUID of the service that triggered the event. If the event is triggered by a client application, then an application-type CUID is recorded.
Event_Type_ID	Integer	ID for the type of event recorded (ID of Save, for example).
Event_Detail_Type_ID	Integer	CUID that identifies the type of event detail captured for that event (File Path, for example).

ADS_TENANT Table

This table records the relationship between tenant names and tenant IDs.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
Tenant_ID	Character (64)	The CUID of the tenant.
Tenant_Name	Character (255)	The name of the tenant.

ADS_USER Table

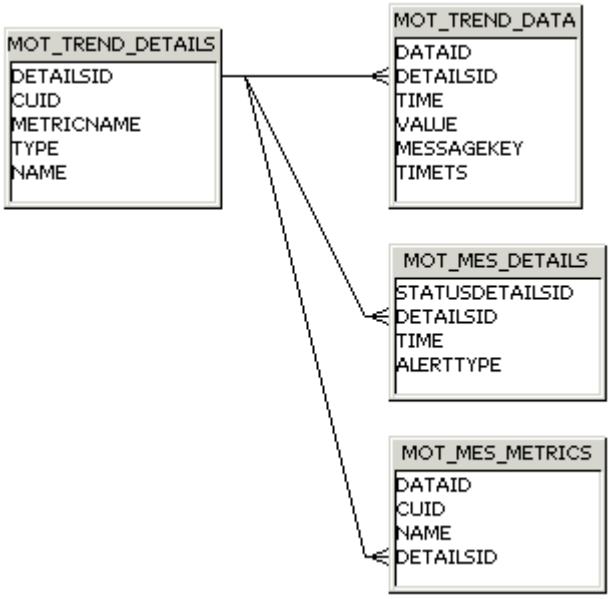
This table records the relationship between users and tenants.

Column Name	Type	Description
Cluster_ID	Character (64)	The GUID of the cluster.
User_ID	Character (64)	The CUID of the user.
User_Name	Character (255)	The name of the user.
Tenant_ID	Character (64)	The CUID of the tenant.

39 モニタリングデータベーススキーマに関する付録

39.1 トレンドデータベーススキーマ

以下のトレンドデータベース図およびテーブルの説明は、メトリクス、プローブ、および監視データが記録される場所、およびそれらのテーブルの関連性を示しています。



MOT_TREND_DETAILS

このテーブルには、管理されたエンティティ、プローブ、および監視に関する情報が記録されます。それには、CUID やメトリクス名などが含まれます。

列名	型	キー	説明
DetailsId	INTEGER	1 次キー Autogenerated	
CUID	VARCHAR(64)	該当せず	メトリクスを公開する、またはメトリクスに関連する InfoObject の CUID
MetricName	VARCHAR(255)	該当せず	メトリックの名前

列名	型	キー	説明
Type	VARCHAR(32)	該当せず	"購読"、"ManagedEntityStatus"、または "プローブ" のいずれか
名前	VARCHAR(255)	該当せず	タイプが "ManagedEntityStatus" の場合の監視の名前。それ以外の場合は、すべてが大文字 (たとえば "PROBE" または "SUBSCRIPTION") の場合を除いて、[タイプ] と同じ文字列がデフォルトになります。

MOT_TREND_DATA

このテーブルには、メトリクス、監視、およびプローブからのトレンディングデータが記録されます。それには、メトリクス値や時間などが含まれます。

列名	型	キー	説明
DataId	INTEGER	1 次キー Autogenerated	
DetailsId	INTEGER	外部キー (MOT_TREND_DETAILS)	
Time または TimeT	BIGINT、NUMBER、または FIXED Unix エポックの日付	該当せず	データが収集された時刻
Value	FLOAT、DOUBLE、または NUMBER	該当せず	メトリクス/購読の値
MessageKey	VARCHAR(32)	該当せず	エラーメッセージキーまたは、成功した場合 null。監視の場合、"watchEnabled" または "watchDisabled" のいずれかになる場合もあります。UI を表示する前に、ローカライズされたメッセージを取得するのに最終的に使用されるため、"キー" になります。
Ts	DATETIME または TIMESTAMP	該当せず	データがデータベースに書き込まれる時間。

MOT_MES_DETAILS

このテーブルには、購読違反に関する情報およびアラート配信情報が記録されます。それには、違反時刻やアラート配信時刻などが含まれます。

列名	型	キー	説明
StatusDetailsId	INTEGER	1 次キー Autogenerated	
DetailsId	INTEGER	外部キー (MOT_TREND_DETAILS)	
Time	BIGINT または NUMBER Unix エポックの日付	該当せず	データが収集された時刻
AlertType	SMALLINT または NUMBER	該当せず	購読通知配信の種類 (電子メールなど)

MOT_MES_METRICS

このテーブルには、監視式に属する監視とメトリクスに関する情報が記録されます。監視に属するすべてのメトリクスのエントリがこのテーブルに 1 つずつ保存されます。

列名	型	キー	説明
DataId	INTEGER	1 次キー Autogenerated	
DetailsId	INTEGER	外部キー (MOT_TREND_DETAILS)	
CUID	VARCHAR(64)	該当せず	監視の CUID
名前	VARCHAR(255)	該当せず	監視の名前

40 システムコピーワークシートに関する付録

40.1 システムコピーワークシート

プロパティ	値
クラスタキー。	
ノード名。	
デプロイメントの各マシンに関するマシン名と BI プラットフォームのインストールフォルダ。	
BI プラットフォームの管理者パスワード。	
デプロイメントの各マシンについて、これらの接続に関連する CMS データベースの接続、ユーザ名、およびパスワード。	
デプロイメントの各マシンについて、これらの接続に関連する監査データベースの接続、ユーザ名、およびパスワード。	
デプロイメントの各マシンについて、ユニバースおよびレポートで使用されるソースシステムの各マシンに関する、その他のデータベースクライアント接続の詳細。	
デプロイメントの各マシンについて、データベースクライアントのタイプとバージョン。	
バージョン、サポートパッケージ、およびパッチレベル。	
デプロイメント内のすべての Input FRS および Output FRS のファイルストアの場所。	
プロモーションマネジメントのコピーを計画している場合、プロモーションマネジメントデータベースフォルダと Subversion フォルダの場所。	
モニタリングデータベースをコピーする計画がある場合は、モニタリングデータベースフォルダ。	
セマンティックレイヤフォルダのパス。	

重要免責事項および法的情報

ハイパーリンク

リンクの一部は、アイコンやマウスオーバーテキストで分類されています。これらのリンクから、追加の情報を得ることができます。
アイコンについて。

- このアイコンが付いたリンク: SAP がホストしているものではない Web サイトに移動します。これらのリンクを使用することで、お客様は (お客様と SAP との契約書に別段の明示的な記載がない限り) 以下のことに同意することになります。
  - リンク先のサイトのコンテンツが SAP のドキュメンテーションではないこと。お客様は、この情報に基づいて SAP に対する製品クレームを推断することはできません。
  - SAP が、リンク先のサイトのコンテンツについて同意することも反対することもなく、また SAP がその利用可能性や正確性について保証しないこと。SAP は、かかるコンテンツの使用により発生した損害が、SAP の重大な過失又は意図的な違法行為が原因で発生したものでない限り、その損害に対して一切責任を負いません。
- このアイコンが付いたリンク: 当該の特定の SAP 製品又はサービスのドキュメンテーションから離れ、SAP がホストしている Web サイトに移動します。これらのリンクを使用することで、お客様は (お客様と SAP との契約書に別段の明示的な記載がない限り)、この情報に基づいて SAP に対する製品クレームを推断することはできないことに同意します。

外部プラットフォームでホストされているビデオ

一部のビデオは、サードパーティのビデオホスティングプラットフォームに置かれている場合があります。SAP では、これらのプラットフォームに保存されているビデオが将来にわたって利用できると保証することはできません。また、これらのプラットフォームにホストされている、いかなる広告またはその他のコンテンツ (関連ビデオまたは同じサイトでホストされている別のビデオに移動する場合など) については、SAP の管理外であり責任を負いません。

ベータおよびその他の試験的機能

試験的機能は、SAP が将来のリリースを保証する正式に提供される機能の範囲外です。これは、試験的機能は、SAP により通知なく理由の如何を問わず随時変更される場合があることを意味します。試験的機能は、本稼働使用のためのものではありません。お客様は、試験的機能を実際の運用環境で、又は十分なバックアップがとられていないデータとともに、デモンストレーション、テスト、試験、評価その他の方法で使用してはなりません。
試験的機能の目的は、早期にフィードバックを得ることで、それに応じて顧客の皆様やパートナーが将来の製品に影響を与えることを可能にすることです。SAP コミュニティなどにおいてフィードバックを提供することで、お客様は、投稿物や二次的著作物の知的財産権が SAP の独占的所有物であり続けることを承認することになります。

コード例

ソフトウェアのコーディングやコードスニペットはすべて、例です。それらは、本稼働使用のためのものではありません。コード例は、構文や表現規則を分かりやすく説明し視覚化することのみを目的としています。SAP は、コード例の正確性や完全性について保証しません。SAP は、コード例の使用により発生した過誤や損害が、SAP の重大な過失又は意図的な違法行為が原因で発生したものでない限り、損害に対して一切責任を負いません。

偏見のない表現

SAP は、ダイバーシティ & インクルージョンの文化を支持しています。SAP の文書では、可能な限り、文化、民族性、ジェンダー、および障がいの有無を問わず、すべての人々に対する偏見を伴わない表現を採用します。

www.sap.com/contactsap

© 2024 SAP SE or an SAP affiliate company. All rights reserved.

本書のいかなる部分も、SAP SE 又は SAP の関連会社の明示的な許可なくして、いかなる形式でも、いかなる目的にも複製又は伝送することはできません。本書に記載された情報は、予告なしに変更されることがあります。

SAP SE 及びその頒布業者によって販売される一部のソフトウェア製品には、他のソフトウェアベンダーの専有ソフトウェアコンポーネントが含まれています。製品仕様は、国ごとに変わる場合があります。

これらの文書は、いかなる種類の表明又は保証もなしで、情報提供のみを目的として、SAP SE 又はその関連会社によって提供され、SAP 又はその関連会社は、これら文書に関する誤記脱落等の過失に対する責任を負うものではありません。SAP 又はその関連会社の製品及びサービスに対する唯一の保証は、当該製品及びサービスに伴う明示的保証がある場合に、これに規定されたものに限られます。本書のいかなる記述も、追加の保証となるものではありません。

本書に記載される SAP 及びその他の SAP の製品やサービス、並びにそれらの個々のロゴは、ドイツ及びその他の国における SAP SE （又は SAP の関連会社）の商標若しくは登録商標です。本書に記載されたその他すべての製品およびサービス名は、それぞれの企業の商標です。

商標に関する詳細の情報や通知については、https://www.sap.com/japan/about/legal/trademark.html をご覧ください。

THE BEST RUN SAP