

SAP BusinessObjects Business Intelligence プラットフォーム
Document Version: 4.0 Support Package 6 - 2013-09-02

Business Intelligence プラットフォーム管理者ガイド

目次

1	ドキュメント履歴.....	18
2	はじめに.....	20
2.1	このヘルプについて.....	20
2.1.1	このヘルプの対象読者.....	20
2.1.2	SAP BusinessObjects Business Intelligence プラットフォームについて.....	20
2.1.3	変数.....	20
2.2	開始前の準備.....	21
2.2.1	基本概念.....	21
2.2.2	主な管理ツール.....	23
2.2.3	主要タスク.....	25
3	アーキテクチャ.....	27
3.1	アーキテクチャの概要.....	27
3.1.1	アーキテクチャ図.....	28
3.1.2	アーキテクチャの各層.....	29
3.1.3	データベース.....	31
3.1.4	サーバ.....	32
3.1.5	Web アプリケーションサーバ.....	32
3.1.6	ソフトウェア開発キット.....	33
3.1.7	データソース.....	35
3.1.8	認証とシングルサインオン.....	36
3.1.9	SAP 統合.....	38
3.1.10	プロモーションマネジメント.....	38
3.1.11	統合バージョン管理.....	39
3.1.12	アップグレードパス.....	39
3.2	サービスおよびサーバ.....	39
3.2.1	XI 3.1 からのサーバの変更点.....	41
3.2.2	サービス.....	42
3.2.3	サービスカテゴリ.....	48
3.2.4	サーバタイプ.....	51
3.2.5	サーバ.....	53
3.3	クライアントアプリケーション.....	55
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共にインストール.....	56
3.3.2	SAP BusinessObjects Business Intelligence プラットフォームと共にインストール.....	60
3.3.3	個別入手可能.....	61
3.3.4	Web アプリケーションクライアント.....	62

3.4	プロセスのワークフロー	65
3.4.1	起動と認証	66
3.4.2	プログラムオブジェクト	67
3.4.3	Crystal Reports	68
3.4.4	Web Intelligence	72
3.4.5	分析	74
4	ライセンスの管理	76
4.1	ライセンスキーの管理	76
4.1.1	ライセンス情報を表示する	76
4.1.2	ライセンスキーを追加する	76
4.1.3	現在のアカウントの利用状況を表示する	77
5	ユーザとグループの管理	78
5.1	アカウント管理の概要	78
5.1.1	ユーザ管理	78
5.1.2	グループ管理	79
5.1.3	利用可能な認証タイプ	80
5.2	Enterprise および通常のアカウントの管理	81
5.2.1	ユーザアカウントを作成する	81
5.2.2	ユーザアカウントを変更する	82
5.2.3	ユーザアカウントを削除する	83
5.2.4	新規グループを作成する	83
5.2.5	グループのプロパティを変更する	83
5.2.6	グループメンバーを表示する	84
5.2.7	サブグループを追加する	84
5.2.8	グループメンバーシップを指定する	85
5.2.9	グループを削除する	85
5.2.10	ユーザまたはユーザグループを一括して追加する	86
5.2.11	Guest アカウントを有効にする	86
5.2.12	グループへのユーザの追加	87
5.2.13	パスワード設定を変更する	88
5.2.14	ユーザおよびグループへのアクセスの許可	89
5.2.15	ユーザの受信ボックスへのアクセスの制御	90
5.2.16	BI 起動パッドのオプションの設定	90
5.2.17	システムユーザの属性の管理	93
5.2.18	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	94
5.2.19	新しいユーザ属性を追加する	94
5.2.20	拡張ユーザ属性を編集する	95
5.3	エイリアスの管理	96

5.3.1	ユーザを作成しサードパーティエイリアスを追加する.	96
5.3.2	既存のユーザの新しいエイリアスを作成する.	97
5.3.3	別のユーザのエイリアスを割り当てる.	98
5.3.4	エイリアスを削除する.	98
5.3.5	エイリアスを無効化する.	99
6	アクセス権の設定.	100
6.1	BI プラットフォームでのアクセス権の動作.	100
6.1.1	アクセスレベル.	100
6.1.2	詳細アクセス権の設定.	101
6.1.3	継承.	101
6.1.4	種類固有アクセス権.	106
6.1.5	実効アクセス権の決定.	108
6.2	CMC でのオブジェクトのセキュリティ設定の管理.	108
6.2.1	オブジェクトの主体のセキュリティを表示する.	109
6.2.2	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.	109
6.2.3	オブジェクトの主体のセキュリティを変更する.	110
6.2.4	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.	110
6.2.5	主体のセキュリティ設定の確認.	111
6.3	アクセスレベルの使用.	113
6.3.1	表示およびオンデマンド表示アクセスレベルの選択.	115
6.3.2	既存のアクセスレベルをコピーする.	116
6.3.3	新しいアクセスレベルを作成する.	116
6.3.4	アクセスレベルの名前を変更する.	116
6.3.5	アクセスレベルを削除する.	117
6.3.6	アクセスレベルの権限を変更する.	117
6.3.7	アクセスレベルとオブジェクト間の関係のトレース.	118
6.3.8	サイト間でのアクセスレベルの管理.	118
6.4	継承の破棄.	119
6.4.1	継承を無効にする.	120
6.5	アクセス権の使用による管理の委任.	121
6.5.1	“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.	122
6.5.2	オーナー権限.	124
6.6	アクセス権管理の推奨事項のまとめ.	124
7	BI プラットフォームのセキュリティ確保.	125
7.1	セキュリティの概要.	125
7.2	障害復旧計画.	125
7.3	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.	126
7.4	同梱されたサードパーティサーバのセキュリティ設定.	127

7.5	アクティブな信頼関係	127
7.5.1	ログオントークン	127
7.5.2	分散セキュリティのチケットメカニズム	128
7.6	セッションとセッショントラッキング	128
7.6.1	CMS セッショントラッキング	129
7.7	環境の保護	129
7.7.1	Web ブラウザから Web サーバへ	129
7.7.2	BI プラットフォームを対象とする Web サーバ	130
7.8	監査セキュリティ設定の変更	130
7.9	Web 利用状況の監査	130
7.9.1	悪意あるログオンに対する保護	131
7.9.2	パスワード制限	131
7.9.3	ログオンの制限	131
7.9.4	ユーザ制限	131
7.9.5	guest アカウントの制限	132
7.10	処理拡張機能	132
7.11	BI プラットフォームのデータセキュリティの概要	133
7.11.1	データ処理セキュリティモード	133
7.12	BI プラットフォームでの暗号化	135
7.12.1	クラスタキーの操作	136
7.12.2	暗号管理者	138
7.12.3	CMC での暗号化キーの管理	139
7.13	サーバの SSL 設定	143
7.13.1	キーファイルと証明書ファイルの作成	143
7.13.2	SSL プロトコルの設定	145
7.14	BI プラットフォームコンポーネント間の通信について	149
7.14.1	BI プラットフォームサーバと通信ポートの概要	150
7.14.2	BI プラットフォームコンポーネント間の通信	152
7.15	ファイアウォール用の BI プラットフォームの設定	157
7.15.1	ファイアウォール用にシステムを設定する	158
7.15.2	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	160
7.16	一般的なファイアウォールシナリオの例	162
7.16.1	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	162
7.16.2	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	164
7.17	統合環境でのファイアウォールの設定	166
7.17.1	SAP 統合に固有のファイアウォールガイドライン	167
7.17.2	JD Edwards EnterpriseOne 統合向けのファイアウォール設定	168
7.17.3	Oracle EBS に固有のファイアウォールガイドライン	170

7.17.4	PeopleSoft Enterprise 統合向けのファイアウォール設定	170
7.17.5	Siebel 統合向けのファイアウォール設定	172
7.18	BI プラットフォームおよびリバースプロキシサーバ	173
7.18.1	サポートされるリバースプロキシサーバ	174
7.18.2	Web アプリケーションのデプロイ方法について	174
7.19	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	174
7.19.1	リバースプロキシサーバの設定の詳細な手順	175
7.19.2	リバースプロキシサーバを設定する	176
7.19.3	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	176
7.19.4	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	176
7.19.5	BI プラットフォーム用に Microsoft ISA 2006 を設定する	177
7.20	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	179
7.20.1	Web サービスのリバースプロキシの有効化	179
7.20.2	ISA 2006 に対するセッション cookie のルートパスの有効化	181
7.20.3	SAP BusinessObjects Live Office に対するリバースプロキシの有効化	183
8	認証	185
8.1	BI プラットフォーム内の認証オプション	185
8.1.1	一次認証	185
8.1.2	セキュリティプラグイン	186
8.1.3	BI プラットフォームへのシングルサインオン	187
8.2	Enterprise 認証	189
8.2.1	Enterprise 認証の概要	189
8.2.2	Enterprise 認証の設定	190
8.2.3	Enterprise 設定を変更する	190
8.2.4	信用できる認証の有効化	191
8.2.5	Web アプリケーションに対する信用できる認証の設定	193
8.3	LDAP 認証	202
8.3.1	LDAP 認証の使用	202
8.3.2	LDAP 認証の設定	203
8.3.3	LDAP グループのマッピング	213
8.4	Windows AD 認証	222
8.4.1	Windows AD 認証の使用	222
8.4.2	ドメインコントローラの準備	223
8.4.3	CMC での AD 認証の設定	224
8.4.4	SIA 実行のための BI プラットフォームサービスの設定	230
8.4.5	AD 認証用の Web アプリケーションサーバの設定	232
8.4.6	シングルサインオンの設定	240
8.4.7	Windows AD 認証のトラブルシューティング	253

8.5	SAP 認証	254
8.5.1	SAP 認証の設定	254
8.5.2	BI プラットフォームのユーザアカウントの作成	255
8.5.3	SAP 権限認証システムへの接続	256
8.5.4	SAP 認証オプションの設定	258
8.5.5	SAP ロールのインポート	261
8.5.6	セキュアネットワークコミュニケーション (SNC) の設定	264
8.5.7	SAP システムへのシングルサインオンの設定	276
8.5.8	SAP Crystal Reports および SAP NetWeaver の SSO の設定	280
8.6	PeopleSoft 認証	281
8.6.1	概要	281
8.6.2	PeopleSoft Enterprise 認証の有効化	281
8.6.3	BI プラットフォームへの PeopleSoft ロールのマップ	282
8.6.4	ユーザの更新のスケジュール	285
8.6.5	PeopleSoft セキュリティブリッジの使用	286
8.7	JD Edwards 認証	295
8.7.1	概要	295
8.7.2	JD Edwards EnterpriseOne 認証の有効化	295
8.7.3	BI プラットフォームへの JD Edwards EnterpriseOne ロールのマップ	296
8.7.4	ユーザの更新のスケジュール	298
8.8	Siebel 認証	300
8.8.1	Siebel 認証の有効化	300
8.8.2	BI プラットフォームへのロールのマップ	301
8.8.3	ユーザの更新のスケジュール	303
8.9	Oracle EBS 認証	305
8.9.1	Oracle EBS 認証の有効化	305
8.9.2	BI プラットフォームへの Oracle E-Business Suite ロールのマップ	305
8.9.3	ロールのマップ解除	309
8.9.4	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	309
8.9.5	SAP Crystal Reports および Oracle EBS のシングルサインオン (SSO) の設定	311
9	サーバの管理	312
9.1	CMC の[サーバ]管理エリアの使用	312
9.2	Windows でのスクリプトを使用したサーバ管理	314
9.3	Unix でのサーバ管理	315
9.4	ライセンスキーの管理	315
9.4.1	ライセンス情報を表示する	315
9.4.2	ライセンスキーを追加する	315
9.4.3	現在のアカウントの利用状況を表示する	316

9.5	サーバのステータスの表示および変更	316
9.5.1	サーバのステータスの表示	316
9.5.2	サーバの開始、停止、再起動	317
9.5.3	Central Management Server の停止	319
9.5.4	サーバの有効化/無効化	320
9.6	サーバの追加、クローン、または削除	321
9.6.1	サーバの追加、クローン、および削除	321
9.7	Central Management Server のクラスタ化	324
9.7.1	Central Management Server のクラスタ化	324
9.8	サーバグループの管理	328
9.8.1	サーバグループの作成	329
9.8.2	サーバサブグループの使用	329
9.8.3	サーバのグループメンバーシップの変更	330
9.8.4	サーバおよびサーバグループへのユーザアクセス権	331
9.9	システムのパフォーマンスの評価	332
9.9.1	SAP BusinessObjects Business Intelligence プラットフォームサーバのモニタリング	332
9.9.2	サーバメトリクスの分析	332
9.9.3	システムメトリクスの表示	333
9.9.4	サーバの利用状況の記録	333
9.10	サーバの設定	334
9.10.1	サーバのプロパティを変更する	335
9.10.2	複数のサーバにサービス設定を適用する	335
9.10.3	設定テンプレートの使用	335
9.11	サーバネットワークの設定	337
9.11.1	ネットワーク環境オプション	338
9.11.2	サーバホスト ID オプション	339
9.11.3	マルチホームマシンの設定	340
9.11.4	ポート番号の設定	343
9.12	ノードの管理	345
9.12.1	ノードの使用	345
9.12.2	新しいノードの追加	347
9.12.3	ノードの再作成	351
9.12.4	ノードの削除	354
9.12.5	ノードの名前の変更	356
9.12.6	ノードの移動	358
9.12.7	スクリプトパラメータ	362
9.12.8	Windows サーバ依存関係の追加	367
9.12.9	ノードに対するユーザ認証情報の変更	367
9.13	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	368

9.13.1	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	368
9.14	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	373
9.15	サーバおよびノードのプレースホルダの管理	374
9.15.1	サーバプレースホルダを表示する	374
9.15.2	ノードのプレースホルダを表示および編集する	374
10	Central Management Server (CMS) データベースの管理	375
10.1	CMS システムデータベース接続の管理	375
10.1.1	SQL Anywhere を CMS データベースとして選択する	375
10.1.2	SAP HANA を CMS データベースとして選択する	376
10.2	新規または既存の CMS データベースの選択	377
10.2.1	Windows で新しいまたは既存の CMS データベースを選択する	377
10.2.2	Unix で新しいまたは既存の CMS データベースを選択する	378
10.3	CMS システムデータベースの再作成	378
10.3.1	Windows で CMS システムデータベースを作成し直す	379
10.3.2	Unix 上で CMS システムデータベースを再作成する	380
10.4	CMS データベース間でのデータのコピー	380
10.4.1	CMS システムデータベースのコピーの準備	381
10.4.2	Windows で CMS システムデータベースをコピーする	382
10.4.3	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	382
11	Web アプリケーションコンテナサーバ (WACS) の管理	383
11.1	WACS	383
11.1.1	Web アプリケーションコンテナサーバ (WACS)	383
11.1.2	デプロイメントへの WACS の追加または削除	385
11.1.3	WACS に対するサービスの追加または削除	388
11.1.4	HTTPS/SSL の設定	390
11.1.5	サポートされる認証方法	393
11.1.6	WACS への AD Kerberos の設定	393
11.1.7	AD Kerberos シングルサインオンの設定	400
11.1.8	RESTful Web サービスの設定	403
11.1.9	WACS と IT 環境	406
11.1.10	Web アプリケーションプロパティの設定	409
11.1.11	トラブルシューティング	409
11.1.12	WACS プロパティ	413
12	バックアップと復元	414
12.1	システムのバックアップと復元	414
12.1.1	バックアップ	415
12.1.2	システムの復元	421

12.1.3	BackupCluster スクリプトおよび RestoreCluster スクリプト	428
13	デプロイメントのコピー	431
13.1	システムコピーの概要	431
13.2	用語	431
13.3	使用事例	431
13.4	システムのコピーの計画	432
13.5	考慮点および制限	433
13.6	システムコピー手順	435
13.6.1	ソースシステムからシステムコピーのエクスポートを実行する	435
13.6.2	ターゲットシステムに対してシステムコピーのインポートを実行する	438
14	バージョン管理	441
14.1	BI リソースのさまざまなバージョンの管理	441
14.2	[VMS 設定] オプションの使用	442
14.2.1	Windows での ClearCase バージョン管理システム (VMS) の設定	443
14.2.2	Unix での ClearCase バージョン管理 (VMS) システムの設定	443
14.3	同じジョブの異なるバージョンの比較	443
14.4	Subversion コンテンツのアップグレード	444
15	プロモーションマネジメント	445
15.1	プロモーションマネジメントへようこそ	445
15.1.1	プロモーションマネジメントの概要	445
15.1.2	プロモーションマネジメントの機能	445
15.1.3	アプリケーションアクセス権	446
15.2	プロモーションマネジメントツールを使用する前に	447
15.2.1	プロモーションマネジメントアプリケーションへのアクセス	447
15.2.2	ユーザインタフェースコンポーネント	447
15.2.3	設定オプションの使用	449
15.3	プロモーションマネジメントツールの使用	455
15.3.1	フォルダの作成と削除	456
15.3.2	ジョブの作成	457
15.3.3	既存ジョブのコピーによるジョブの新規作成	459
15.3.4	ジョブの検索	459
15.3.5	ジョブの編集	460
15.3.6	プロモーションマネジメントでの InfoObject の追加	460
15.3.7	プロモーションマネジメントでの依存関係の管理	461
15.3.8	依存オブジェクトの検索	462
15.3.9	リポジトリに接続している時のジョブの昇格	462
15.3.10	BIAR ファイルを使用したジョブの昇格	464

15.3.11	ジョブの昇格のスケジュール.	467
15.3.12	ジョブ履歴の表示.	468
15.3.13	ジョブのロールバック.	468
15.4	InfoObject のさまざまなバージョンの管理.	471
15.4.1	バージョン管理アプリケーションのアクセス権限.	472
15.4.2	サブバージョンファイルのバックアップと復元.	473
15.5	コマンドラインオプションの使用.	474
15.5.1	Windows でのコマンドラインオプションの実行.	474
15.5.2	UNIX でのコマンドラインオプションの実行.	475
15.5.3	コマンドラインオプションのパラメータ.	475
15.5.4	サンプルプロパティファイル.	480
15.6	拡張移送/修正システムの使用.	481
15.6.1	前提条件.	481
15.6.2	Business Intelligence プラットフォームと CTS+ との統合の設定.	482
15.6.3	CTS を使用したジョブの昇格.	486
16	差分の視覚化.	490
16.1	プロモーションマネジメントツールの Visual Difference.	490
16.1.1	Visual Difference を使用してのオブジェクトまたはファイルの比較.	491
16.1.2	バージョン管理システム内のオブジェクトまたはファイルの比較.	492
16.1.3	比較のスケジュール.	493
17	アプリケーションの管理.	494
17.1	CMC を介したアプリケーションの管理.	494
17.1.1	概要.	494
17.1.2	アプリケーションの共通設定.	495
17.1.3	アプリケーション固有の設定.	496
17.2	BOE.war プロパティを介したアプリケーションの管理.	522
17.2.1	BOE war ファイル.	522
17.3	BI 起動パッドおよび OpenDocument ログオンエントリーポイントのカスタマイズ.	529
17.3.1	BI 起動パッドおよび OpenDocument ファイルの場所.	529
17.3.2	カスタムログオンページを定義する.	530
17.3.3	信用できる認証をログオンに追加する.	531
18	接続とユニバースの管理.	532
18.1	接続の管理.	532
18.1.1	ユニバース接続を削除する.	532
18.2	ユニバースの管理.	532
18.2.1	ユニバースを削除する.	533

19	モニタリング	534
19.1	モニタリングについて	534
19.2	モニタリング用語	534
19.2.1	アーキテクチャ	536
19.3	モニタリングに対するデータベースサポートの設定	538
19.3.1	Derby データベースを使用するための設定	539
19.3.2	監査データベースを使用するための設定	540
19.4	設定プロパティ	546
19.4.1	JMX エンドポイント URL	549
19.4.2	プローブのモニタリングに使用する HTTPS 認証	550
19.4.3	プローブのパスワード暗号化	550
19.5	その他アプリケーションとの統合	550
19.5.1	モニタリングアプリケーションと IBM Tivoli との統合	550
19.5.2	モニタリングアプリケーションと SAP Solution Manager との統合	553
19.6	モニタリングサーバのクラスタサポート	554
19.7	トラブルシューティング	554
19.7.1	ダッシュボード	554
19.7.2	警告	555
19.7.3	監視リスト	555
19.7.4	プローブ	556
19.7.5	メトリクス	557
19.7.6	チャート	557
20	監査	558
20.1	概要	558
20.2	CMC 監査ページ	564
20.2.1	ステータスの概要	564
20.2.2	監査イベントの設定	566
20.2.3	監査データストア設定	568
20.3	監査イベント	569
20.3.1	監査イベントおよび詳細	577
21	プラットフォーム検索	596
21.1	プラットフォーム検索について	596
21.1.1	プラットフォーム検索 SDK	596
21.1.2	クラスタ環境	596
21.2	プラットフォーム検索の設定	597
21.2.1	OpenSearch のデプロイ	597
21.2.2	リバースプロキシの設定	599
21.2.3	CMC でのアプリケーションプロパティの設定	599

21.3	プラットフォーム検索の使用	604
21.3.1	CMS リポジトリコンテンツのインデックス処理	604
21.3.2	インデックス処理失敗一覧	605
21.3.3	検索結果	605
21.4	プラットフォーム検索と SAP NetWeaver Enterprise Search の統合	611
21.4.1	SAP NetWeaver Enterprise Search でのコネクタの作成	612
21.4.2	SAP BusinessObjects Business Intelligence 認証へのユーザロールのインポート	612
21.5	NetWeaver Enterprise Search からの検索	613
21.6	監査	613
21.7	トラブルシューティング	615
21.7.1	セルフヒーリング	615
21.7.2	問題のシナリオ	615
22	フェデレーション	618
22.1	フェデレーション	618
22.2	フェデレーションの用語	619
22.3	セキュリティアクセス権の管理	620
22.3.1	レプリケート元サイトで必要な権限	621
22.3.2	レプリケート先サイトで必要な権限	621
22.3.3	フェデレーション固有の権限	622
22.3.4	オブジェクトに対するセキュリティの複製	623
22.3.5	アクセスレベルを使用したセキュリティの複製	624
22.4	レプリケーションの種類とモードのオプション	624
22.4.1	一方向レプリケーション	624
22.4.2	双方向レプリケーション	625
22.4.3	[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]	625
22.5	サードパーティユーザとグループの複製	626
22.6	ユニバースおよびユニバース接続の複製	628
22.7	レプリケーション一覧の管理	629
22.7.1	レプリケーション一覧の作成	630
22.7.2	レプリケーション一覧の変更	631
22.8	リモート接続の管理	632
22.8.1	リモート接続の作成	633
22.8.2	リモート接続の変更	634
22.9	レプリケーションジョブの管理	635
22.9.1	レプリケーションジョブの作成	635
22.9.2	レプリケーションジョブのスケジュール	637
22.9.3	レプリケーションジョブの変更	638
22.9.4	レプリケーションジョブ後のログの表示	638

22.10	オブジェクトのクリーンアップの管理	639
22.10.1	オブジェクトのクリーンアップ方法	639
22.10.2	オブジェクトのクリーンアップの制限	640
22.10.3	オブジェクトのクリーンアップ間隔	640
22.11	競合の検出と解決の管理	641
22.11.1	一方向レプリケーションの競合の解決	641
22.11.2	双方向レプリケーションの競合の解決	643
22.12	フェデレーションでの Web サービスの使用	646
22.12.1	セッション変数	646
22.12.2	ファイルのキャッシュ	647
22.12.3	カスタムデプロイメント	647
22.13	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	648
22.13.1	リモートスケジュール	648
22.13.2	ローカルで実行したインスタンス	650
22.13.3	インスタンス共有	650
22.14	複製したコンテンツのインポートと昇格	651
22.14.1	複製したコンテンツのインポート	651
22.14.2	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	652
22.14.3	テスト環境からのコンテンツの昇格	652
22.14.4	レプリケート先サイトの再指定	653
22.15	ベストプラクティス	653
22.15.1	現在のリリースの制限	656
22.15.2	エラーメッセージのトラブルシューティング	657
23	ERP 環境の追加設定	661
23.1	SAP NetWeaver 統合の設定	661
23.1.1	SAP Netweaver Business Warehouse (BW) との統合	661
23.2	JD Edwards 統合の設定	700
23.2.1	SAP Crystal Reports のシングルサインオンの設定	700
23.2.2	JD Edwards Integrations のセキュアソケットレイヤの設定	701
23.3	PeopleSoft Enterprise 統合の設定	702
23.3.1	SAP Crystal Reports および PeopleSoft Enterprise のシングルサインオン (SSO) の設定	702
23.3.2	セキュアソケットレイヤ通信の設定	703
23.3.3	PeopleSoft システムのパフォーマンスチューニング	705
23.4	Siebel 統合の設定	707
23.4.1	SAP BusinessObjects Business Intelligence プラットフォームと統合するための Siebel の設定	707
23.4.2	Crystal Reports のメニュー項目の作成	707
23.4.3	コンテキスト認識	709
23.4.4	SAP Crystal Reports および Siebel のシングルサインオン (SSO) の設定	711

23.4.5	Secure Sockets Layer (SSL) 通信の設定	712
24	管理および設定ログ	713
24.1	コンポーネントからのログのトレース	713
24.2	トレースログレベル	713
24.3	サーバのトレースの設定	714
24.3.1	CMC にサーバトレースログレベルを設定する	715
24.3.2	CMC で管理されている複数のサーバにトレースログレベルを設定する	715
24.3.3	BO_trace.ini ファイルを使ってサーバトレースを設定する	716
24.4	Web アプリケーションのトレース設定	718
24.4.1	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	719
24.4.2	BO_trace.ini ファイルを使用してトレース設定を手動で変更する	719
24.5	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	723
24.6	アップグレードマネジメントツールのトレース設定	724
24.6.1	アップグレードマネジメントツールをトレース設定する	724
25	SAP Solution Manager への統合	726
25.1	統合の概要	726
25.2	SAP Solution Manager の統合のチェックリスト	726
25.3	システムランドスケープディレクトリ登録の管理	727
25.3.1	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	727
25.3.2	SLD 登録がトリガーされるタイミング	729
25.3.3	SLD 接続のログ作成	729
25.4	ソリューション管理診断エージェントの管理	730
25.4.1	Solution Manager Diagnostics (SMD) の概要	730
25.4.2	SMD エージェントの操作	730
25.4.3	SMAAdmin ユーザアカウント	731
25.5	パフォーマンス機器の管理	731
25.5.1	BI プラットフォームのパフォーマンス計測	731
25.5.2	BI プラットフォームのパフォーマンス計測の設定	731
25.5.3	Web 層のパフォーマンス計測	733
25.5.4	計測ログファイル	733
25.6	SAP パスポートを使用したトレース	733
26	コマンドライン管理	735
26.1	Unix スクリプト	735
26.1.1	スクリプトユーティリティ	735
26.1.2	スクリプトテンプレート	740
26.1.3	SAP BusinessObjects Business Intelligence プラットフォームで使用されるスクリプト	740
26.2	Windows スクリプト	742

26.2.1	ccm.exe.	742
26.3	サーバコマンドライン.	745
26.3.1	コマンドラインの概要.	745
26.3.2	すべてのサーバに使用できる標準オプション.	745
26.3.3	Central Management Server.	746
26.3.4	Crystal Reports Processing Server と Crystal Reports Cache Server.	747
26.3.5	Dashboards Processing Server と Dashboards Cache Server.	748
26.3.6	Job Server.	749
26.3.7	Adaptive Processing Server.	750
26.3.8	Report Application Server.	750
26.3.9	Web Intelligence Processing Server.	752
26.3.10	Input/Output File Repository Server.	753
26.3.11	Event Server.	753
26.3.12	Dashboard および Dashboard Analytics Server.	754
27	アクセス権に関する付録.	755
27.1	付録 - 権限について.	755
27.2	全般の権限.	755
27.3	特定のオブジェクトの種類のアクセス権.	757
27.3.1	フォルダのアクセス権.	757
27.3.2	カテゴリ.	758
27.3.3	注.	758
27.3.4	Crystal レポート.	759
27.3.5	Web Intelligence ドキュメント.	759
27.3.6	ユーザとグループ.	760
27.3.7	アクセスレベル.	762
27.3.8	ユニバース (.unv) のアクセス権.	762
27.3.9	ユニバース (.unx) のアクセス権.	764
27.3.10	ユニバースオブジェクトのアクセスレベル.	765
27.3.11	接続のアクセス権.	766
27.3.12	アプリケーション.	767
28	サーバのプロパティに関する付録.	777
28.1	サーバのプロパティに関する付録について.	777
28.1.1	共通サーバのプロパティ.	777
28.1.2	コアサービスのプロパティ.	779
28.1.3	接続サービスのプロパティ.	791
28.1.4	Crystal Reports サービスのプロパティ.	795
28.1.5	Analysis サービスのプロパティ.	803
28.1.6	データフェデレーションサービスのプロパティ.	804

28.1.7	Web Intelligence サービスのプロパティ	805
28.1.8	Dashboards サービスのプロパティ	813
29	サーバのメトリクスに関する付録	816
29.1	サーバのメトリクスに関する付録について	816
29.1.1	一般的なサーバのメトリクス	816
29.1.2	Central Management Server のメトリクス	818
29.1.3	Connection Server のメトリクス	821
29.1.4	Event Server のメトリクス	822
29.1.5	File Repository Server のメトリクス	822
29.1.6	Adaptive Processing Server のメトリクス	823
29.1.7	Web アプリケーションコンテナサーバのメトリクス	827
29.1.8	Adaptive Job Server のメトリクス	828
29.1.9	Crystal Reports Server のメトリクス	829
29.1.10	Web Intelligence サーバのメトリクス	832
29.1.11	Dashboards Server のメトリクス	833
30	サーバおよびノードのプレースホルダに関する付録	835
30.1	サーバとノードプレースホルダ	835
31	監査データストアスキーマに関する付録	847
31.1	概要	847
31.2	スキーマ図	848
31.3	監査データストアテーブル	849
32	モニタリングデータベーススキーマに関する付録	857
32.1	トレンドデータベーススキーマ	857
33	システムコピーワークシート	860
33.1	システムコピーワークシート	860

1 ドキュメント履歴

以下の表は、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 4.0	2011 年 11 月	このドキュメントの初版です。
SAP BusinessObjects Business Intelligence プラットフォーム 4.0 機能パック 3	2012 年 3 月	<p>このリリースの追加機能:</p> <ul style="list-style-type: none">• CCM を使用したユーザおよびグループの一括インポート• インポートされたユーザアカウントと Enterprise ユーザアカウントの両方に対する属性の拡張• LDAP プラグインを使用した、JDBC を経由する SAP HANA データベースへのシングルサインオンの設定• ODBC データソースとしての SQL Anywhere。Unix マシンでの SQL Anywhere を使用したノード管理については、「SQL Anywhere 用に Unix マシンを準備する」を参照してください。• マシン名、IP アドレス、クラスタ名、サーバ名の変更によって発生する可能性がある問題を防ぐことを目的としたベストプラクティス• BI プラットフォームの初期インストール後に、CMS データベースとして SAP HANA を選択する• WACS サーバでホストされる RESTful Web サービスを設定する• "ホットバックアップ" を実行する (サーバを停止せずにバックアップコピーを作成する)• テストやスタンバイなどの目的で、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• SAP StreamWork アプリケーションの統合詳細を有効化および設定する• タスクを作成し、委任管理者に割り当てる• プラットフォーム検索のセルフヒーリングメカニズム <p>また、ロールベースライセンス、BI アナリストユーザアカウント、および BI ビューアユーザアカウントに対するすべての参照が削除されました。</p>
SAP BusinessObjects Business Intelligence プラットフォーム 4.0 サポートパッケージ 5	2012 年 11 月	<p>このリリースでの追加と変更:</p> <ul style="list-style-type: none">• SAP BusinessObjects アプリケーションを Windows スタートメニューから起動する方法を指定した指示が更新されました。• 節 クラスタへの新しいノードの追加 [ページ 326]が更新されました。
SAP BusinessObjects Business Intelligence プラットフォーム 4.0 サポートパッケージ 6	2013 年 4 月	<p>このリリースでの追加と変更:</p> <ul style="list-style-type: none">• 「監査」の章が更新されました。• 「モニタリング」の章が更新されました。• 『リポジトリ診断ツールガイド』がこのガイドに統合されました。• サーバのメトリクスに関する付録が更新されました。

関連リンク

[To add users or user groups in bulk](#) [ページ 86]

[Managing attributes for system users](#) [ページ 93]

[Using the LDAP plugin to configure SSO to the SAP HANA database](#) [ページ 216]

[To prepare a Unix machine for SQL Anywhere.](#) [ページ 346]

[To select SAP HANA as a CMS database](#) [ページ 375]

[Configuring RESTful web services](#) [ページ 403]

[Hot backups](#) [ページ 417]

[Overview of system copying](#) [ページ 431]

[Managing SAP StreamWork](#) [ページ 516]

[Delegated administration and CMC tab access](#) [ページ 500]

[Self Healing](#) [ページ 615]

2 はじめに

2.1 このヘルプについて

このヘルプでは、BI プラットフォームシステムのデプロイメントおよび設定に関する情報および手順について説明します。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 このヘルプの対象読者

このヘルプでは、デプロイメントおよび設定タスクについて説明します。次の作業を行うユーザは、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

このヘルプは、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、このヘルプでは、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 SAP BusinessObjects Business Intelligence プラットフォームについて

BI プラットフォームは、信頼性に優れた柔軟でスケーラブルなレポート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、エンドユーザへのパワフルな対話型レポートの配布を実現します。BI プラットフォームは、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、または企業ポータルへの重要情報の統合などのどの目的で使用しても、組織内だけでなくその範囲を越えて利益をもたらします。レポートिंग、データ分析、および情報配信のための統合スイートであるプラットフォームは、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。

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
<<INSTALLEDIR>>	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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • Windows の場合: <<INSTALLEDIR>>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts • Unix の場合: <<INSTALLEDIR>>/sap_bobj/enterprise_xi40/<<PLATFORM64DIR>>/scripts

2.2 開始前の準備

2.2.1 基本概念

2.2.1.1 サービスおよびサーバ

BI プラットフォームでは、サービスおよびサーバ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。

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 で実行されるサブシステムです。

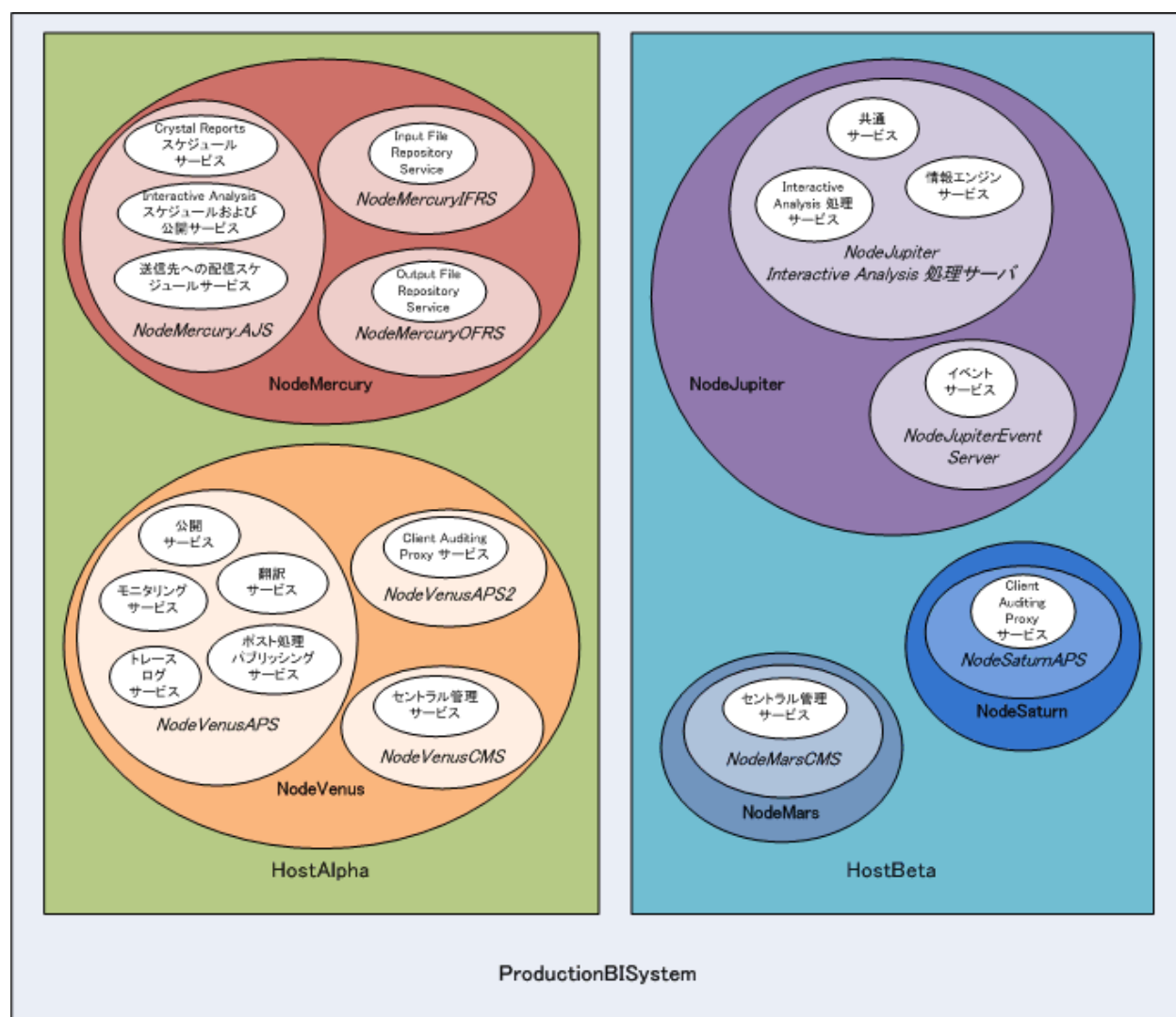
サーバは、1 つまたは複数のサービスをホストするオペレーティングシステムレベルのプロセスです (システムによってはデーモンと呼ばれます)。たとえば、Central Management Server (CMS) と Adaptive Processing Server はサーバです。サーバは、特定のオペレーティングシステムアカウントで実行され、独自の PID を持ちます。

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マシンに分散するか、広域ネットワーク (WAN) を介して分散することができます。

サービス、サーバ、ノード、およびホスト

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。サービス、サーバ、ノード、ホストの数、およびサービスとサーバの種類は実際のインストールによって異なります。



ProductionBI System というクラスターが、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 には、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.WebIntelligence)、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。

関連リンク

[サーバの管理](#)

2.2.1.2 Server Intelligence

Server Intelligence は、Business Intelligence 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、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、また、管理者によるノードの管理にも使用されます。

CMS は、サーバ情報を CMS システムデータベースにアーカイブするため、デフォルトのサーバ設定を簡単に復元したり、同じ設定を持つサーバプロセスの冗長性インスタンスを作成したりできます。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。

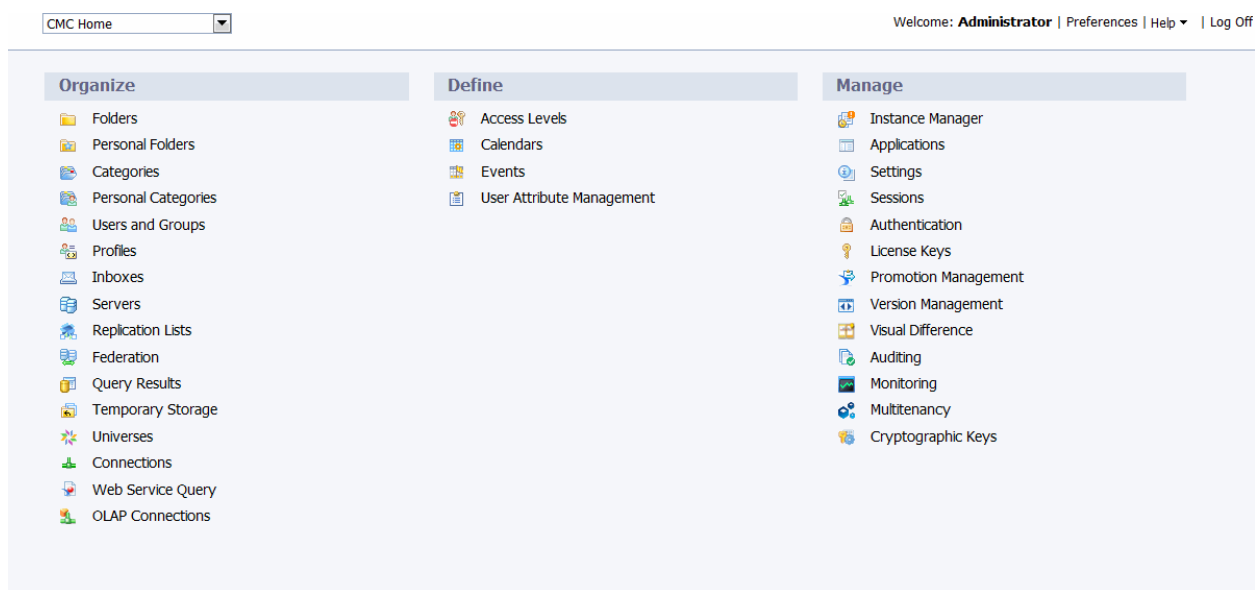
i 注記

1 つのコンピュータに複数のノードを含めることができます。また、ノードは同じ BI プラットフォームクラスタまたは異なるクラスタに存在することができます。

2.2.2 主な管理ツール

2.2.2.1 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。



すべてのユーザは CMC にログオンして、各自の基本設定を変更できます。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。

2.2.2.2 セントラル設定マネージャ

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。Windows では、CCM を使用して、CCM ユーザインタフェース (UI) またはコマンドラインでローカルサーバとリモートサーバを管理します。Unix 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します。

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 (デフォルトで付属する Tomcat Web アプリケーションサーバの場合) を起動または停止したりできます。Windows では、CCM を使用して、Secure Socket 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。

i 注記

サーバ管理タスクの大半は、CCM ではなく CMC で処理されます。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。

2.2.2.3 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。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。

2.2.2.4 アップグレードマネジメントツール

アップグレードマネジメントツール (旧インポートウィザード) は、SAP BusinessObjects Business Intelligence プラットフォームの一部としてインストールされ、管理者が SAP BusinessObjects Business Intelligence プラットフォームの旧バージョンからユーザ、グループ、およびフォルダをインポートするプロセスをサポートします。また、オブジェクト、イベント、サーバグループ、リポジトリオブジェクト、およびカレンダーをインポートおよびアップグレードすることもできます。

SAP BusinessObjects Business Intelligence プラットフォームの旧バージョンからのアップグレードの詳細については、*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、このヘルプ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。

関連リンク

[初めてのデプロイメントの計画または実行](#) [ページ 25]

[デプロイメントの設定](#) [ページ 26]

[システムのパフォーマンスの改善](#) [ページ 26]

[セントラル管理コンソール\(CMC\)](#) [ページ 23]

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、次のタスクを実行し、推奨するトピックを参照してください。

- “アーキテクチャの概要”
- “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”
- “BI プラットフォーム内の認証オプション” (サードパーティ認証を使用する予定がある場合)
- “サーバの管理” (インストール後)

この製品のインストールの詳細については、*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、デプロイメントのアーキテクチャを設計するには、*Business Intelligence* プラットフォーム計画ガイドを参照してください。

関連リンク

[アーキテクチャの概要](#) [ページ 27]

[BI プラットフォームコンポーネント間の通信について](#) [ページ 149]

[セキュリティの概要](#) [ページ 125]

[BI プラットフォーム内の認証オプション](#) [ページ 185]

[サーバの管理](#)

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。

関連リンク

[サーバの管理](#)

[BI プラットフォームコンポーネント間の通信](#) [ページ 152]

[セキュリティの概要](#) [ページ 125]

[モニタリングについて](#) [ページ 534]

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、次の節を参照することをお勧めします。

- 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、サーバメンテナンスに関する情報を参照してください。

関連リンク

[モニタリングについて](#) [ページ 534]

[サーバの管理](#)

2.2.3.4 CMC でのオブジェクトの使用

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、「“BusinessObjects Enterprise 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。

関連リンク

[アカウント管理の概要](#) [ページ 78]

[BI プラットフォームでのアクセス権の動作](#) [ページ 100]

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。

i 注記

このリリースで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、およびその他のシステムの一覧は、SAP サポートポータル (<https://service.sap.com/bosap-support>) の SAP BusinessObjects セクションにある製品出荷マトリックス (サポートされているプラットフォーム/PAR) を参照してください。

SAP BusinessObjects Business Intelligence 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。たとえば、専門のプラットフォームサービスで、オンデマンドのデータアクセスとレポート生成、あるいは時間ベースまたはイベントベースのレポートスケジュールを処理します。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、SAP BusinessObjects Business Intelligence プラットフォームを組織のほか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。

- 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
 - レポート変換ツール
 - 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ナツール (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)
 - ウィジェット (旧 BI ウィジェット)
- 個別入手可能クライアント:
 - SAP Crystal Reports
 - SAP BusinessObjects Dashboards (旧 Xcelsius)
 - 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
- アップグレードマネジメントツール (旧インポートウィザード)
- 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、SAP BusinessObjects Business Intelligence 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。バージョンが異なる 2 つの Business Intelligence 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、またはテスト目的にのみ推奨されます。

サーバプロセスを垂直方向に拡張して (1 台のコンピュータで複数、またはすべてのサーバ側プロセスを実行する) コストを削減したり、水平方向に拡張して (複数のプロセスを 2 台以上のネットワーク化されたマシンに分散する) 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。

i 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で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で使用しないことをお勧めします。

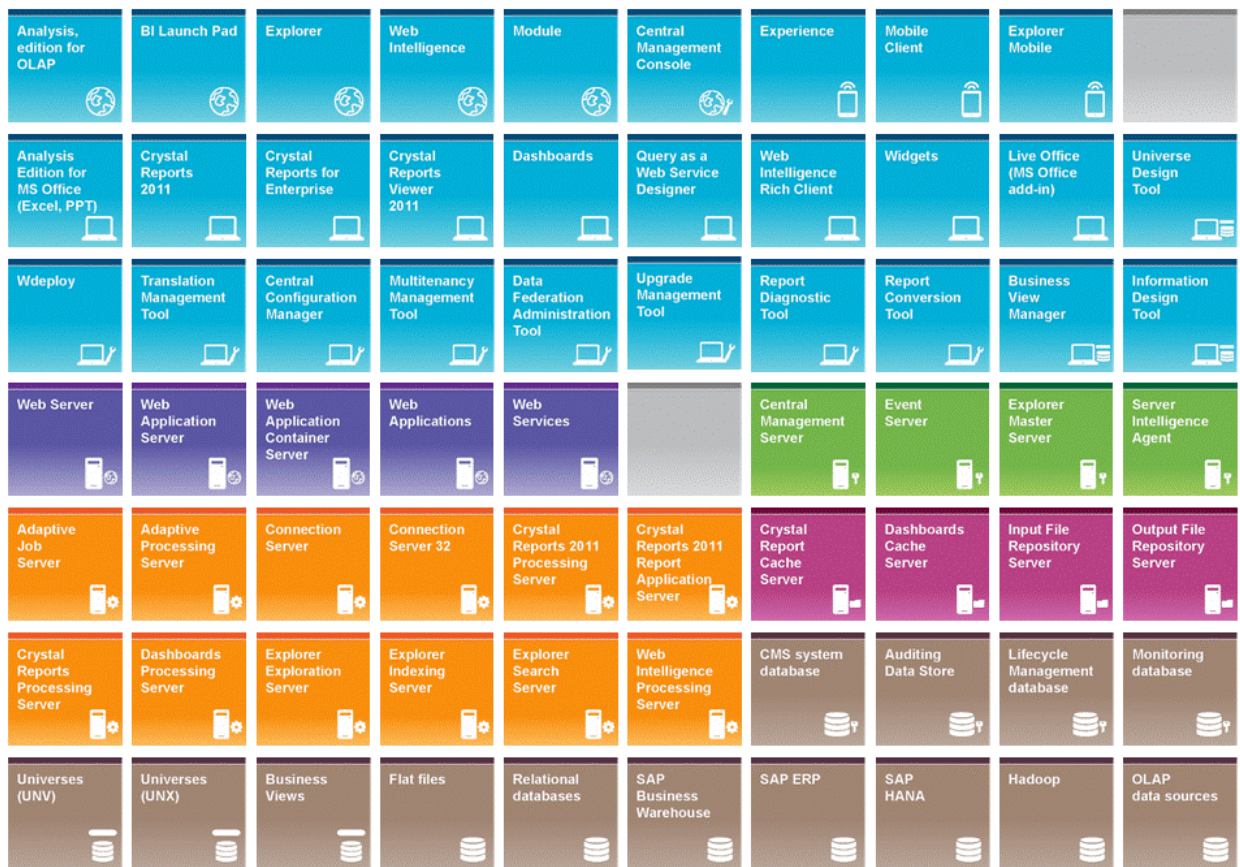
3.1.1 アーキテクチャ図

SAP BusinessObjects Business Intelligence プラットフォームは、エンタープライズレベルの分析およびレポート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。以下の図は、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。

➡ ヒント

SAP Community Network の <http://scn.sap.com/docs/DOC-26788> を使用して、すべての BI プラットフォームコンポーネントおよびサーバのより詳細なビューを操作できます。

SAP BusinessObjects Business Intelligence Platform 4.0



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働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ー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、SAP BusinessObjects Business Intelligence プラットフォームとやりとりして、さまざまなレポート、アナリティクス、管理機能を提供する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 2011 (別個に利用およびインストールが可能) などがあります。

Web 層

Web 層には、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 SAP BusinessObjects Business Intelligence 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 層には、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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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、レポートで使用す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 などのファイルタイプ) を管理します。

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 (32 ビットと 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

データ層には実際のレポートとシステムデータが含まれます。たとえば、リレーショナルデータベースのレポートデータ、OLAP データソース、および実際のユニバースファイル (.unx および .unv) があります。CMS、監査データストア、プロモーション マネジメント、バージョン管理、モニタリングアプリケーションのシステムデータベースなどもデータ層に含まれます。

3.1.3 データベース

SAP BusinessObjects Business Intelligence 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
組織の情報を参照します。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情報となります。通常、この情報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、認証詳細などの SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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。
- バージョン管理データベース
バージョン管理データベースは、SAP BusinessObjects Business Intelligence プラットフォームインストールおよび更新に関連する設定とバージョン情報を追跡します。
- モニタリングデータベース
モニタリングでは、Java Derby 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。

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、SAP BusinessObjects Business Intelligence 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勧めします。

3.1.4 サーバ

SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence プラットフォームサーバホストを 1 つのクラスター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 ユーザーが存在する場合は、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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence プラットフォームサーバホストは、単一の SAP BusinessObjects Business Intelligence プラットフォームサーバホストより迅速にレポート情報のキューを処理することができます。
- 負荷分散
あるサーバがクラスター内のほかのサーバより高負荷になると、CMS は自動的に新規作業をよりリソースが多い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 SAP BusinessObjects Business Intelligence 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。

サポートされている Web アプリケーションサーバの詳細な一覧については、製品出荷マトリックス (<http://service.sap.com/bosap-support/>) を参照してください。

SAP BusinessObjects Business Intelligence 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 6 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。

i 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 SAP BusinessObjects Business Intelligence 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 Web アプリケーションコンテナサービス (WACS)

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 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 SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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ビス (WACS) をインストールできます。

WACS は、SAP BusinessObjects Business Intelligence 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 起動パッド、および Web サービスなどの SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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。

i 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、以下の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、SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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。

SAP BusinessObjects Business Intelligence 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。

i 注記

SAP BusinessObjects Business Intelligence 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。

次の SDK が SAP BusinessObjects Business Intelligence プラットフォームでサポートされています。

- SAP BusinessObjects Business Intelligence プラットフォームの Java SDK および .NET SDK
SAP BusinessObjects Business Intelligence 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。

i 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。

- SAP BusinessObjects Business Intelligence プラットフォーム RESTful Web サービス SDK
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。
- SAP BusinessObjects 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。
SAP BusinessObjects Business Intelligence プラットフォームの Web サービスでは、XML、SOAP、AXIS 2.0、WSDL などの標準が使用されます。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。

i 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

i 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、SAP BusinessObjects Business Intelligence プラットフォームが OEM として統合されている Business Intelligence 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、およびフィールド) を表示する機能を提供します。
- Report Engine Java 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。これらの SDK で作成されたアプリケーションでは、さまざまな SAP BusinessObjects 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、<http://help.sap.com> 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きます。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 および Crystal Reports 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 SAP BusinessObjects Business Intelligence 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ツールでシステムにアクセスしユニバースを作成するためには、SAP BusinessObjects Business Intelligence プラットフォームにログインする必要があります。ユニバースアクセスと行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、SAP BusinessObjects Web Intelligence で、Online Analytical Processing (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、SAP BusinessObjects Business Intelligence プラットフォームで完全にサポートされます。

SAP BusinessObjects Business Intelligence プラットフォームには、分散管理機能のためのパスワード管理、サーバメトリクス、およびユーザアクセス制御など、一連の事前に設定された専用プラットフォーム管理サービスが含まれます。

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、SAP BusinessObjects Business Intelligence 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)、サードパーティ認証に対する信用できる認証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 データに対してレポート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、ユーザアカウントをサードパーティシステムから Business Intelligence (BI) プラットフォームにマップできるため、アカウントの作成および管理を自動で行うことができます。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。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。SAP BusinessObjects Business Intelligence 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 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

i 注記

ユーザは、CMC を介して SAP BusinessObjects Business Intelligence 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 起動パッドは、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 起動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。SAP BusinessObjects Business Intelligence プラットフォームでは、複数の ERP システムからのシングルサインオンとレポートングをサポートします。SAP BusinessObjects BI 4.0 製品出荷マトリックス (PAM) を参照してください (<http://service.sap.com/pam>)。

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。他の ERP システムのサポートは、デフォルトでインストールされていません。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。

ERP 統合の設定については、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。

3.1.9 SAP 統合

SAP BusinessObjects Business Intelligence 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。
SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence プラットフォーム管理者ガイドの「システムランドスケープでの SAP BusinessObjects Business Intelligence 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。
- CTS 移送 (CTS+)
移送/修正システム (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、本稼働の 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 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アプリケーションは、BI オブジェクトの依存関係に影響を及ぼすことなく、システム間で BI オブジェクトを移動できます。また、このツールでは、さまざまなバージョンの管理、依存関係の管理、または昇格したオブジェクトを元の状態にロールバックすることもできます。

BI オブジェクト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アプリケーションがインストールされている場合だけです。

詳細については、このガイドのプロモーションマネジメントを参照してください。

3.1.11 統合バージョン管理

サーバスシステムで SAP BusinessObjects Business Intelligence 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。

3.1.12 アップグレードパス

以前のリリースの SAP BusinessObjects Enterprise (たとえば XI 3.x) からのアップグレードは可能ですが、最初に SAP BusinessObjects Business Intelligence プラットフォーム 4.x をインストールし、次にアップグレードマネジメントツールを使用して既存のシステムから設定とデータを移行する必要があります。

旧バージョンからのアップグレード方法については、*SAP BusinessObjects 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。

3.2 サービスおよびサーバ

BI プラットフォームでは、サービスおよびサーバ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。

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 で実行されるサブシステムです。

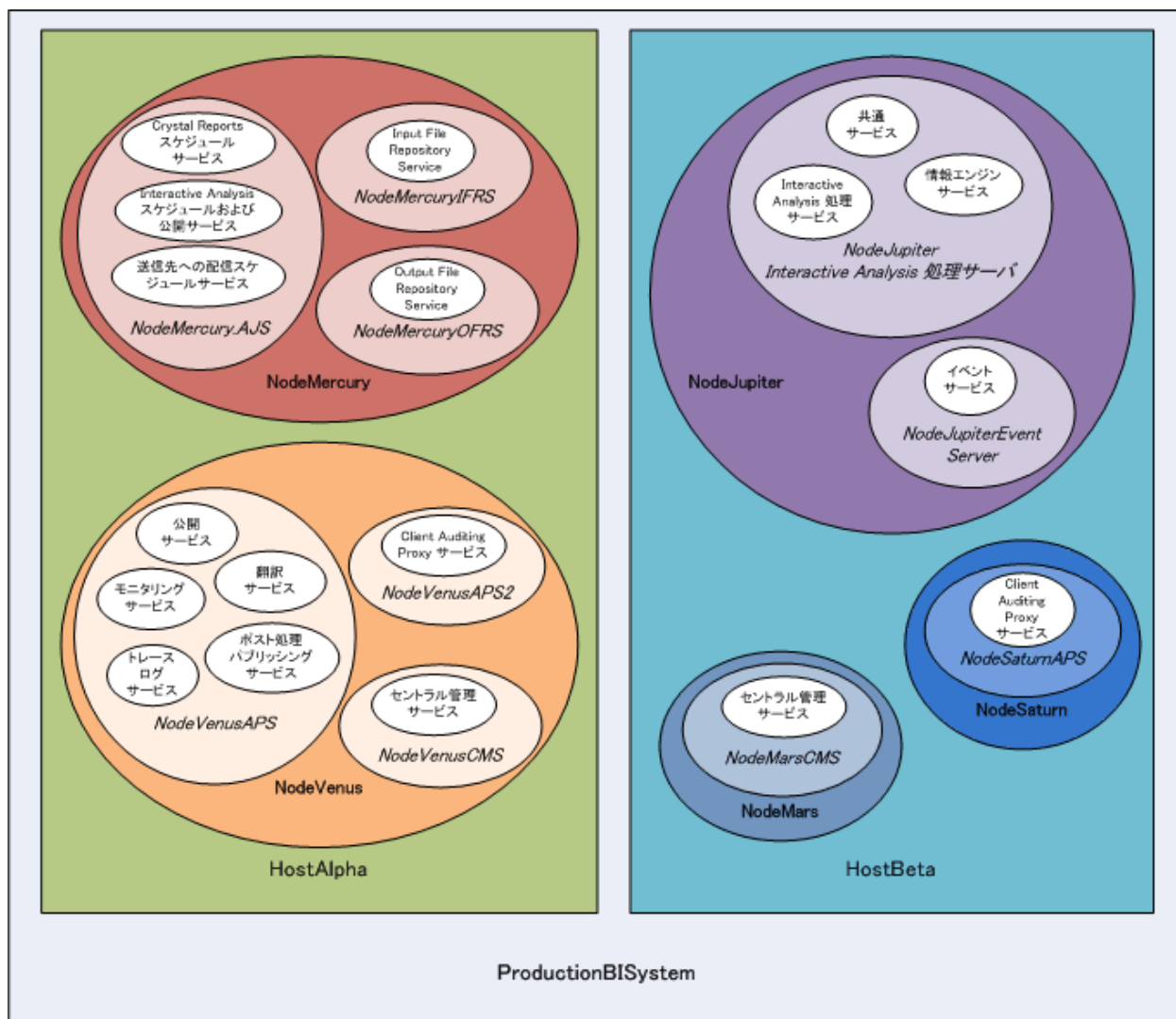
サーバは、1 つまたは複数のサービスをホストするオペレーティングシステムレベルのプロセスです (システムによってはデーモンと呼ばれます)。たとえば、Central Management Server (CMS) と Adaptive Processing Server はサーバです。サーバは、特定のオペレーティングシステムアカウントで実行され、独自の PID を持ちます。

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マシンに分散するか、広域ネットワーク (WAN) を介して分散することができます。

サービス、サーバ、ノード、およびホスト

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。サービス、サーバ、ノード、ホストの数、およびサービスとサーバの種類は実際のインストールによって異なります。



ProductionBI System というクラスターが、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 には、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.WebIntelligence)、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。

関連リンク

[サーバの管理](#)

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 では Adaptive Job Server に移行されました。
- 新しく導入されたサーバ

表 1: サーバの変更点

XI 3.1	4.0	4.0 Feature Pack 3
Connection Server [1]	Connection Server Connection Server 32	Connection Server Connection Server 32
Crystal Reports 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)
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
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
Desktop Intelligence Cache Server [3]	4.0 以降は利用不可	4.0 以降は利用不可

XI 3.1	4.0	4.0 Feature Pack 3
Desktop Intelligence Job Server [3]	4.0 以降は利用不可	4.0 以降は利用不可
Desktop Intelligence Processing Server [3]	4.0 以降は利用不可	4.0 以降は利用不可
Destination Job Server	Adaptive Job Server	Adaptive Job Server
値の一覧サーバ (LOV)	Web Intelligence Processing Server	Web Intelligence Processing Server
Multi-Dimensional Analysis Services	Adaptive Processing Server	Adaptive Processing Server
Program 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)
Web Intelligence Job Server	Adaptive Job Server	Adaptive Job Server
Xcelsius Cache Server [4]	Dashboard Design Cache Server (Xcelsius) [5]	Dashboards Cache Server (Xcelsius)
Xcelsius Processing Server [4]	Dashboard Design Processing Server (Xcelsius) [5]	Dashboards Processing Server (Xcelsius)

- [1] 4.0 では、Connection Server 32 は 32 ビットであり、特に 64 ビットのマドルウェアを処理でき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 以降は利用不可になりました。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 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。

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 (送信先への配信スケジュールサービスなど) を含める必要があります。

i 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 ベースドライバに対する接続サービスを提供します。
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 起動パッドの統合を提供します
BOE Web アプリケーションサービス	コアサービス	Web アプリケーションコンテナサーバ	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
ビジネスプロセス BI 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 向けのビジネスプロセス BI Web サービスを提供します。これにより、Web アプリケーションに BI テクノロジーを組み込むことができます。ビジネスプロセス BI サービスは、現在は使用できません。
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
Crystal Reports 2011 処理サービス	Crystal Reports サービス	Crystal Reports Processing Server	Crystal Reports 2011 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

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
			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 2011 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 2011 表示および変更サービス	Crystal Reports サービス	Report Application Server (RAS)	
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
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。
Dashboards キャッシュサービス	Dashboards サービス	Dashboards Cache Server	レポートのキャッシュを管理することで、Dashboards 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

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
Dashboards 処理サービス	Dashboards サービス	Dashboards Processing Server	Dashboards 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
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	
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	<p>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、電子メール、ユーザの受信ボックスなど）に公開します</p> <div> <p>i 注記</p> <p>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。</p> </div>
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
Excel データアクセスサービス	Web Intelligence サービス	Adaptive Processing Server	Business Intelligence 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。

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
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
ライフサイクルマネジメント ClearCase サービス	ライフサイクルマネジメント サービス	Adaptive Processing Server	LCM のための ClearCase サポートを提供します
ライフサイクルマネジメント スケジュールサービス	ライフサイクルマネジメント サービス	Adaptive Job Server	スケジュールされたライフサイクルマネジメントジョブを実行します
ライフサイクルマネジメント サービス	ライフサイクルマネジメント サービス	Adaptive Processing Server	ライフサイクルマネジメント 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
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

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
			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	指定した時間に行う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、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 シングルサインオンのサポート

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
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
Visual Difference スケジュールサービス	ライフサイクルマネジメントサービス	Adaptive Job Server	スケジュールされた Visual Difference (ライフサイクルマネジメント) 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	ライフサイクル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ライフサイクル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
Web Services SDK および QaaWs	コアサービス	Web アプリケーションコンテナサーバ	WACS 上の Web サービス

3.2.3 サービスカテゴリ

i 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

サービスカテゴリ	サービス	サーバタイプ
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	認証更新スケジュールサービス	Adaptive Job Server
コアサービス	セントラル管理サービス	Central Management Server
コアサービス	クライアント監査プロキシサービス	Adaptive Processing Server
コアサービス	ダッシュボードサービス	Dashboard 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	インプットファイルストアサービス	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	アウトプットファイルストアサービス	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	レプリケーションサービス	Adaptive Job 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	セキュリティエリススケジュールサービス	Adaptive Job Server
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	翻訳サービス	Adaptive Processing Server
Crystal Reports サービス	Crystal Reports 2011 処理サービス	Crystal Reports Processing Server
Crystal Reports サービス	Crystal Reports 2011 スケジュールサービス	Adaptive Job Server
Crystal Reports サービス	Crystal Reports 2011 表示および変更サービス	Report Application Server (RAS)

サービスカテゴリ	サービス	サーバタイプ
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
Dashboards サービス	Dashboards キャッシュサービス	Dashboards Cache Server
Dashboards サービス	Dashboards 処理サービス	Dashboards 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
ライフサイクルマネジメントサービス	ライフサイクルマネジメント 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	ライフサイクル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	ライフサイクル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	ドキュメント回復サービス	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
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 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

関連リンク

[サービス](#) [ページ 42]

[サーバタイプ](#) [ページ 51]

3.2.4 サーバタイプ

i 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
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 2011 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	ライフサイクルマネジメントスケジュールサービス	ライフサイクル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	セキュリティエリス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	ライフサイクル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

サーバタイプ	サービス	サービスカテゴリ
Adaptive Processing Server	ライフサイクルマネジメント ClearCase サービス	ライフサイクル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	ライフサイクル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	ライフサイクル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 2011 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
Dashboards Cache Server	Dashboards キャッシュサービス	Dashboards サービス
Dashboards Processing Server	Dashboards 処理サービス	Dashboards サービス
Dashboard Server	ダッシュボードサービス	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 2011 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

関連リンク

[サービス](#) [ページ 42]

[サービスカテゴリ](#) [ページ 48]

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標準サーバ。SAP BusinessObjects Business Intelligence 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 <div><p>i 注記</p><p>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。</p><p>実稼働環境にインストールしている場合は、デフォルトの APS を使用しないでください。代わりに、インストール手順が完了した後にシステムサイジングを実行して、次のものを決定することを強くお勧めします。</p><ul style="list-style-type: none">• APS サービスのタイプと数• 複数の APS サーバへのサービスの分散• 最適な APS サーバ数 (複数の APS サーバにより、冗長性、よりよいパフォーマンス、およびより高い信頼性が提供されます)• 複数ノードへの APS サーバの分散<p>サイジング処理での決定に従って、新しい APS サーバインスタンスを作成します。</p><p>たとえば、サイジングの結果、サービスカテゴリごとに 1 つの APS を作成することが提案されている場合は、8 つの APS サーバが最終的に作成されます。Analysis サービス、接続サービス、コアサービス、Crystal Reports サービス、Dashboards サービス</p></div>

サーバ	説明
	ービス、データフェデレーションサービス、ライフサイクルマネジメントサービス、および Web Intelligence サービスの各サービスカテゴリに 1 つずつです。
Central Management Server (CMS)	Business Intelligence 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。
Dashboards Cache Server	クライアントから Dashboard 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 Dashboard Server に渡し、Dashboard 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。
Dashboards Processing Server	レポートを処理し、Encapsulated Page Format (EPF) ページを生成して、Dashboards 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。

サーバ	説明
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	アドホックレポート機能があり、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、SAP BusinessObjects Business Intelligence 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。

i 注記

SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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、SAP Crystal Reports 2011 および Live Office があります。

i 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 SAP BusinessObjects Business Intelligence 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、SSL 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共にインストール

3.3.1.1 Web Intelligence デスクトップ

Web Intelligence デスクトップは、SAP BusinessObjects Business Intelligence 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トングツールです。

これにより、ドラッグアンドドロップインタフェースで使い慣れたビジネス用語を使用して、リレーショナルソース、Online Analytical Processing (OLAP) ソース、スプレッドシートソース、またはテキストファイルソースからのデータにアクセスし、それらを結合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 デスクトップユーザは、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。

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。

デザイナーは、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

レポート変換ツールは、レポートを Web Intelligence 形式に変換し、変換したレポートを Central Management Server (CMS) に公開します。

レポートは、CMS フォルダ [パブリック]、[お気に入り]、または [受信ボックス] から取得することができます。変換が完了したレポートは、元の Web Intelligence レポートと同じフォルダまたは異なるフォルダに公開されます。このツールでは、Web Intelligence のすべての機能やレポートが変換されるわけではありません。変換のレベルは、元のレポートの機能によって変わります。特定の機能を含むレポートは変換されない場合があります。その他の機能は、変換中にレポート変換ツールによって変更、再実装または削除されます。

レポート変換ツールを使用して、変換されたレポートを監査することもできます。このツールは、レポート変換ツールで完全に変換できないレポートを識別するのに役立ち、その理由を説明します。

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ー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、このインター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 Query as a Web Service

Query as a Web Service は、クエリを Web サービスとして作成し、Web 対応アプリケーションと統合するためのウィザードベースのアプリケーションです。クエリを保存して標準クエリのカタログを作成し、アプリケーション作成者はそのカタログから必要に応じてクエリを選択できます。

ビジネスインテリジェンス (BI) コンテンツは、通常、BI ツールの特定のユーザインターフェースにバインドされます。Query as a Web Service ではこれを変更し、Web サービスを処理できる任意のユーザインターフェースに BI コンテンツを配布します。

Query as a Web Service は、他の Web サービスと同様に Microsoft Windows アプリケーション上で動作します。Query as a Web Service は、W3C Web サービス仕様の SOAP、SDL、および XML に基づいています。また、次の 2 つの主要コンポーネントがあります。

- サーバコンポーネント
サーバコンポーネント (Business Intelligence プラットフォームに付属) は、Query as a Web Service カタログを保存し、公開された Web サービスを管理します。
- クライアントツール
クライアントツールは、ビジネスユーザがサーバで Query as a Web Service を作成して公開するために使用します。クライアントツールを複数のコンピュータにインストールし、サーバに保存されている共通のカタログへのアクセスとカタログの共有ができます。クライアントツールは、Web サービス経由でサーバコンポーネントと通信します。

Query as a Web Service を使用すると、Web クエリをクライアント側ソリューションの一部として使用することができます。

- Microsoft Office、Excel、および InfoPath
- SAP NetWeaver
- OpenOffice
- ビジネスルールおよびプロセス管理のアプリケーション
- エンタープライズサービスバスプラットフォーム

3.3.1.6 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ー) は、SAP BusinessObjects のメタデータデザイン環境で、デザイナーが 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します。

3.3.1.7 トランスレーションマネジメントツール

SAP BusinessObjects Business Intelligence 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。ユーザーは、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ー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。
- ユーザーインターフェースを介して、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。

3.3.1.8 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。

SAP BusinessObjects Business Intelligence 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に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。

3.3.1.9 SAP BusinessObjects Business Intelligence プラットフォーム向けウィジェット

ウィジェットとは、頻繁に使用される機能に簡単に素早くアクセスすることができ、デスクトップからビジュアルな情報を得られるようにするミニアプリケーションです。SAP BusinessObjects Business Intelligence プラットフォーム (旧 BI ウィジェット) 向けウィジェットを使用すると、組織は SAP BusinessObjects Business Intelligence プラットフォーム上の既存のビジネスインテリジェンス (BI) コンテンツへのアクセスを提供したり、デスクトップウィジェットとして SAP NetWeaver Application Server 上で XBCML (拡張ビジネスクライアントマークアップ言語) ウィジェットとして登録される Web Dynpro アプリケーションを追加したりできます。

ユーザのデスクトップ上に XBCML ウィジェットを表示するには、SAP Web Dynpro Flex クライアントが使用されます。SAP Web Dynpro Flex クライアントは、ウィジェットのレンダリングに使用する Adobe Flex に基づくレンダリングエンジンです。Web Dynpro アプリケーションの設定方法の詳細については、SAP BusinessObjects ウィジェットユーザガイドの SAP NetWeaver アプリケーションサーバ上でウィジェットを有効化するのトピックを参照してください。

i 注記

SAP Web Dynpro Flex クライアントは、リリース 7.0 EhP2 SP3 以降で XBCML ウィジェットをサポートしています。Flex クライアントキューのサポートは、これらの指定リリースの XBCML ウィジェットにある Flex クライアントの問題に限定されています。

SAP BusinessObjects Business Intelligence プラットフォーム向けウィジェットを使用して、Web Intelligence ドキュメント、Dashboards モデルおよび Web Dynpro アプリケーションなどの既存のコンテンツを検索または参照し、必要なときにすぐに利用できるように、デスクトップに情報を貼り付けます。

ウィジェットとして、コンテンツはウィジェットフレームワークから次の機能を取得します。

- ユーザが制御するサイズと位置設定
- 自動最新表示
- 上部のアプリケーションウィンドウとしてのオプション設定
- 完全な SAP BusinessObjects Business Intelligence プラットフォームセキュリティ (Web Intelligence レポートパーツおよび Dashboards モデルのみ)
- 表示の保存
- データコンテキストステータスの保存 (Web Intelligence レポートパーツのみ)
- 詳細なレポートへの Web Intelligence OpenDocument リンク (Web Intelligence ドキュメントのみ)
- タブ付きビュー (Dashboards モデルのみ)

3.3.2 SAP BusinessObjects Business Intelligence プラットフォームと共にインストール

3.3.2.1 セントラル設定マネージャ

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。Windows では、CCM を使用して、CCM ユーザインタフェース (UI) またはコマンドラインでローカルサーバとリモートサーバを管理します。Unix 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します。

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 (デフォルトで付属する Tomcat Web アプリケーションサーバの場合) を起動または停止したりできます。Windows では、CCM を使用して、Secure Socket 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。

i 注記

サーバ管理タスクの大半は、CCM ではなく CMC で処理されます。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

アップグレードマネジメントツール (旧インポートウィザード) は、SAP BusinessObjects Business Intelligence プラットフォームの一部としてインストールされ、管理者が SAP BusinessObjects Business Intelligence プラットフォームの旧バージョンからユーザ、グループ、およびフォルダをインポートするプロセスをサポートします。また、オブジェクト、イベント、サーバグループ、リポジトリオブジェクト、およびカレンダーをインポートおよびアップグレードすることもできます。

SAP BusinessObjects Business Intelligence プラットフォームの旧バージョンからのアップグレードの詳細については、*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。

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) は、Central Management Server (CMS) システムデータベースと File Repository Server (FRS) のファイルストアの間の不整合をスキャン、診断、および修復した後、修復ステータスと完了した操作をレポートします。

ユーザがホットバックアップからシステムを復元した後、または原状回復後 (Business Intelligence プラットフォームサービスの開始前)、RDT を使用してシステムおよびデータベースを同期させることができます。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、簡単に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 BusinessObjects Dashboards

SAP BusinessObjects Dashboards (旧 Xcelsius) は、データビジュアライゼーションおよび動的な対話型ダッシュボードの作成に使用できるツールです。データと式は、埋め込まれた Excel スプレッドシートにインポートするか、直接入力することができます。Flash インタフェースは多様なアナリティクスとダッシュボードを表示できるキャンバスを提供します。

データは SAP BusinessObjects Business Intelligence プラットフォームから動的に更新し、PowerPoint、PDF、Flash など、標準形式のデータコンシューマで表示できるさまざまな形式にエクスポートすることができます。

3.3.3.4 SAP BusinessObjects Explorer

SAP BusinessObjects Explorer とは、強力な検索機能を使用して、ビジネスの疑問に対する回答を会社のデータから迅速かつ直接的に取得できるデータ発見アプリケーションです。

SAP BusinessObjects Explorer をインストールすると、SAP BusinessObjects Business Intelligence プラットフォームセントラル設定マネージャ (CCM) とセントラル管理コンソール (CMC) に次のサーバが追加されます。

- Explorer マスタサーバ: Explorer サーバすべてを管理します。

- Explorer インデックス化サーバ: 情報スペースのデータおよびメタデータをインデックス化し、管理します。
- Explorer 検索サーバ: 検索クエリを処理し、検索結果を戻します。
- Explorer 閲覧サーバ: データの検索、フィルタリング、および集計を含む情報スペースの閲覧と分析の機能を提供し、管理します。

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、SAP BusinessObjects Business Intelligence 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。

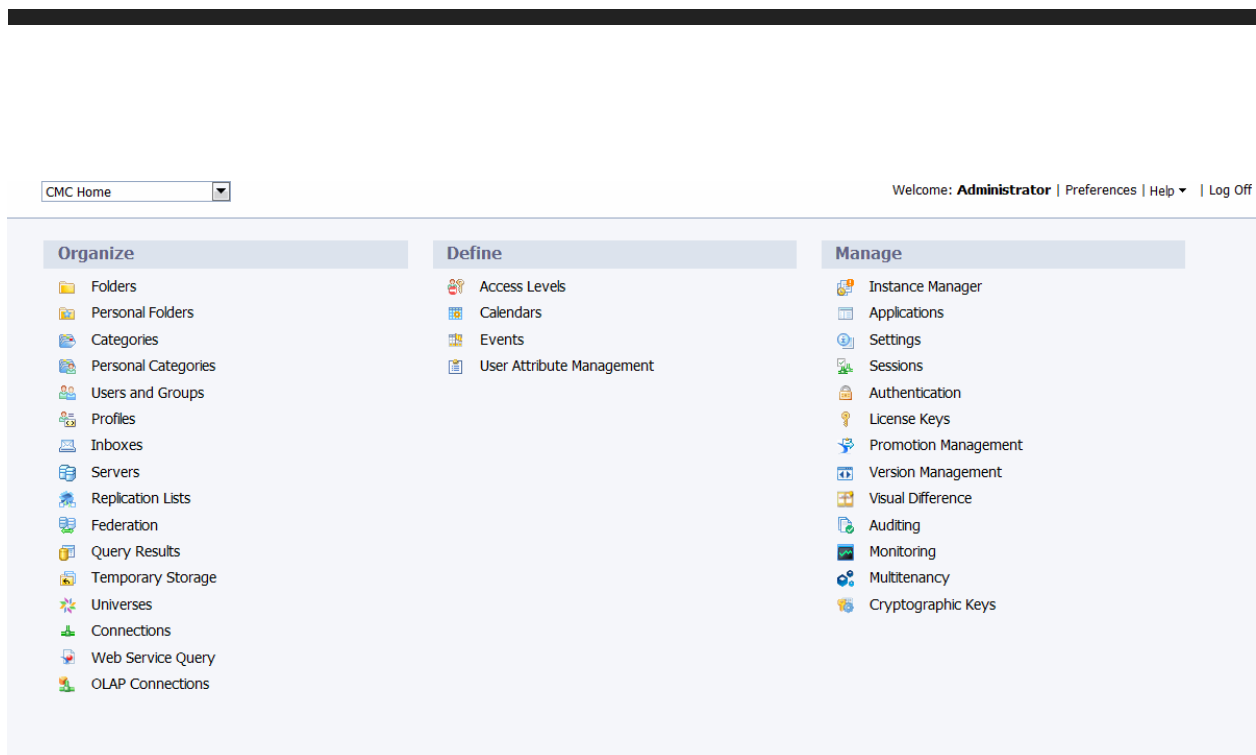
付属の WDeploy コマンドラインツールを使用して、初期インストールの後に Java Web アプリケーションを再設定またはデプロイすることもできます。このツールを使用して、Web アプリケーションを 2 つの方法で Web アプリケーションサーバにデプロイすることができます。

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。



すべてのユーザは CMC にログインして、各自の基本設定を変更できます。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 BI 起動パッド

BI 起動パッド (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 起動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。BI 起動パッドを使用して、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。

BI 起動パッドでは、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 (旧ダッシュボードビルダ) 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、条件の変化に応じてビジネスルールを調整するために必要な情報を提供します。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

- ページ作成: BI ワークスペースおよびモジュールの管理
- 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

i 注記

BI ワークスペースは、BI 起動パッドアプリケーションに不可欠な部分です。したがって、BI ワークスペースの機能を使用するには、契約の一部として BI 起動パッドを含む SAP BusinessObjects Business Intelligence プラットフォームライセンスを購入する必要があります。

3.3.4.4 レポートビューア

各レポートビューアは異なるプラットフォームおよびブラウザをサポートします。ビューアには、次の 2 つのカテゴリがあります。

- クライアント側のレポートビューア (Active X ビューアと Java ビューア)
クライアント側のレポートビューアは、ユーザのブラウザにダウンロードおよびインストールされます。ユーザがレポートを要求すると、アプリケーションサーバはそのリクエストを処理し、SAP BusinessObjects Business Intelligence プラットフォームからレポートページを取得します。そして Web アプリケーションサーバはレポートページをクライアント側のビューアに渡し、そこでレポートページが処理され、Web ブラウザに表示されます。クライアント側のレポートビューアを選択するには、**基本設定** > [Crystal Reports](#) > [Web ActiveX \(ActiveX が必要\)](#) または [[Web Java \(Java が必要\)](#)] を選択します。
- ゼロクライアントレポートビューア (DHTML ビューア)
ゼロクライアントレポートビューアは、Web アプリケーションサーバ上に存在します。ユーザがレポートを要求すると、Web アプリケーションサーバは Business Intelligence プラットフォームからレポートページを取得し、ブラウザで表示される DHTML ページを作成します。ゼロクライアントレポート (DHTML) ビューアを選択するには、**基本設定** > [Crystal Reports](#) > [Web \(ダウンロードは不要\)](#) を選択します。

すべてのレポートビューアがレポートリクエストを処理し、ブラウザに表示されるレポートページを提供します。

各レポートビューアがサポートする特定の機能、またはプラットフォームについては、*BI 起動パッドユーザガイド*、*Report Application Server .NET SDK 開発者ガイド*、またはビューア *Java SDK 開発者ガイド*を参照してください。

3.3.4.5 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、レポートインク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。

3.3.4.6 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で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。

i 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。

3.3.4.7 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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。

i 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して自動的に停止するか、または、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、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、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プロセスについて説明します。

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。

3.4.2.2 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。

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。

i 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。

i 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 2011 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 2011 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 2011 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。

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、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 2011 Processing Server に送信します。
8. Crystal Reports 2011 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) に照会します。Output FRS は、リクエストされたレポートインスタンスを Crystal Reports 2011 Processing Server に送信します。

i 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 2011 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 2011 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 2011 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 2011 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オンデマンドで SAP Crystal Reports 2011 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。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します。

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 2011 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 2011 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 2011 Processing Server に送信します。

i 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 2011 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 2011 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 2011 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 2011 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 2011 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 2011 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 2011 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 2011 スケジュールサービスに送信します。
3. Crystal Reports 2011 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。

i 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 2011 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 2011 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 2011 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 2011 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、`crxpdf.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。

i 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 2011 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 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。たとえば、BI 起動パッドの Web Intelligence ビューアから表示します。

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。

i 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 メタレイアウト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。

i 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 は、メモリ内のドキュメントを開きます。QT.dll は、ドキュメントのベースとなるユニバースから 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。

i 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、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 Analysis, OLAP edition 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 起動パッドから SAP Analysis, OLAP edition 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。

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)テクノロジーを使用して、Web アプリケーションサーバと通信します。AJAX テクノロジー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 Advanced Analyzer 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。

4 ライセンスの管理

4.1 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。

関連リンク

[ライセンス情報を表示する](#) [ページ 76]

[ライセンスキーを追加する](#) [ページ 76]

[現在のアカウントの利用状況を表示する](#) [ページ 77]

4.1.1 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。

関連リンク

[ライセンスキーの管理](#) [ページ 76]

[ライセンスキーを追加する](#) [ページ 76]

[現在のアカウントの利用状況を表示する](#) [ページ 77]

4.1.2 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。

i 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。

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。

関連リンク

[ライセンス情報を表示する](#) [ページ 76]

[現在のアカウントの利用状況を表示する](#) [ページ 77]

4.1.3 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。

関連リンク

[ライセンスキーの管理](#) [ページ 76]

[ライセンスキーを追加する](#) [ページ 76]

[ライセンス情報を表示する](#) [ページ 76]

5 ユーザとグループの管理

5.1 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。

5.1.1 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。

表 2: 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。
SMAAdmin	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。

i 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。

5.1.2 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。

表 3: 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 グループデザイナー	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。

関連リンク

[BI プラットフォームでのアクセス権の動作](#) [ページ 100]

[ユーザおよびグループへのアクセスの許可](#) [ページ 89]

5.1.3 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。

表 4: 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。

認証の種類	説明
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。

5.2 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。

i 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。

5.2.1 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. 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
 - a) [認証の種類]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) パスワードの情報と設定を指定します。
- 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。
 - SAP BusinessObjects Business Intelligence プラットフォーム使用許諾契約で規定されたオプションに基づき、ユーザアカウントの指定方法を指定します。
 - ユーザを、使用許諾契約で同時にアクセスすることが許されるユーザ数に含める場合は、[[同時接続ユーザ](#)]を選択します。
 - 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許諾契約に属する場合は、[[指定ユーザ](#)]を選択します。指定ユーザライセンスは、現在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。
 - [[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 のエイリアスとともに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。

関連リンク

[BI プラットフォームでのアクセス権の動作](#) [ページ 100]

5.2.2 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。

i 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。

- CMC の[[ユーザとグループ](#)]管理エリアを表示します。
- プロパティを変更するユーザを選択します。
- [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。
- 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。

i 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。

- [[保存して閉じる](#)]をクリックします。

関連リンク

[既存のユーザの新しいエイリアスを作成する](#) [ページ 97]

5.2.3 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。変更はすぐに有効になり、変更時にそのユーザがログオンしていた場合、ユーザにエラーメッセージが表示されます。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、個人用力カテゴリー、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。

i 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。
ユーザアカウントが削除されます。

関連リンク

[ユーザアカウントを変更する](#) [ページ 82]

[ユーザアカウントを削除する](#) [ページ 83]

[エイリアスを無効化する](#) [ページ 99]

5.2.4 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。

5.2.5 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。

i 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。

5.2.6 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。

i 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。

5.2.7 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。

i 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。

関連リンク

[グループメンバーシップを指定する](#) [ページ 85]

5.2.8 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。

5.2.9 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。

5.2.10 ユーザまたはユーザグループを一括して追加する

CSV (カンマ区切り値) ファイルを使用して、ユーザまたはユーザグループを一括して CMC に追加することができます。

1. CMC にログインします。
2. [ユーザとグループ] タブで、**管理** > **ユーザグループのインポート** > **ユーザ/グループ/データベース認証** の順にクリックします。
[ユーザ/グループ/データベース認証] ウィンドウが表示されます。
3. [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。データが正しく書式設定されている場合は、[インポート] ボタンが有効になります。
4. [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。



例

サンプルの CSV ファイル

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

➡ 注意

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。

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] タブで、**管理** > **ユーザグループのインポート** > **履歴** の順にクリックします。

5.2.11 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インできません。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 起動パッドにアクセスできなくなります。




ユーザが BI 起動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 パネルの[ユーザー一覧]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。

5.2.12 グループへのユーザの追加

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。

次の手順では、次の方法でユーザをグループに追加する方法を説明します。

関連リンク

[グループメンバーシップを指定する](#) [ページ 85]

5.2.12.1 1 人のユーザを 1 つまたは複数のグループに追加する

1. CMC の[\[ユーザとグループ\]](#)管理エリアを表示します。
2. グループに追加するユーザを選択します。
3. [▶ アクション ▶ グループを結合](#)  をクリックします。

i 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。

[\[グループを結合\]](#)ダイアログボックスが表示されます。


4. ユーザ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。

➡ 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。

5. [\[OK\]](#)をクリックします。

5.2.12.2 1 人または複数のユーザを 1 つのグループに追加する

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. [▶ 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. [\[ユーザー一覧\]](#)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]一覧からグループに追加するユーザを、[選択されたユーザ/グループ]一覧に移動します。

➡ 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。

➡ 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。

➡ ヒント

システムに多数のユーザが存在する場合は、[戻る]および[次へ]ボタンをクリックしてユーザのリスト内を移動します。

5. [OK]をクリックします。

5.2.13 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。

5.2.13.1 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。

5.2.13.2 一般的なパスワード設定を変更する

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. 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。

表 5: パスワード設定

パスワード設定	最小値	推奨される最大値
大文字と小文字を含むパスワードを要求する	該当なし	該当なし
少なくとも N 文字以上のパスワードを要求する	0 文字	64 文字(全角 32 文字)
N 日ごとにパスワードの変更を要求する	1 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	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	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	1 回	100 回
ログオン失敗回数を N 分後にリセットする	1 分後	100 分
N 分後に再びアカウントを有効にする	0 分	100 分

4. [更新] をクリックします。

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。

5.2.14 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。

関連リンク

[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](#) [ページ 109]

5.2.15 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。

関連リンク

[CMC でのオブジェクトのセキュリティ設定の管理](#) [ページ 108]

5.2.16 BI 起動パッドのオプションの設定

管理者はユーザが BI 起動パッドアプリケーションにアクセスする方法を設定できます。BOE war ファイルにプロパティを設定することで、ユーザのログオン画面で利用できる情報を指定できます。CMC を使用して、特定のグループの優先 BI 起動パッドを設定することもできます。

5.2.16.1 BI 起動パッドログオン画面の設定

デフォルトでは、BI 起動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 BI 起動パッドプロパティを編集する必要があります。

5.2.16.1.1 BI 起動パッドログオン画面を設定する

BI 起動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 BI 起動パッド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。

BIlaunchpad.properties

4. BI 起動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. BI 起動パッドのログオン画面でユーザに CMS 名の入力を要求するには、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。

5.2.16.2 BI 起動パッドのグループの基本設定

管理者は、特定のユーザグループの BI 起動パッドの基本設定を設定できます。これらの基本設定は、グループ内のすべてのユーザの BI 起動パッドのデフォルトの基本設定として適用されます。

i 注記

ユーザが独自の基本設定を設定した場合、BI 起動パッドのビューに、管理者が定義した設定は反映されません。ユーザは、独自の基本設定から管理者定義の基本設定にいつでも切り替えて、更新された設定を使用できます。

デフォルトでは、BI 起動パッド基本設定は、どのユーザグループにも設定されていません。管理者は、次の項目に対して基本設定を指定できます。

- ホームタブ
- ドキュメント - 開始場所
- フォルダ
- カテゴリ
- 1 ページあたりのオブジェクト数
- [ドキュメント] タブに表示される列
- BI 起動パッドにタブまたは新しいウィンドウによりドキュメントを表示する方法

5.2.16.2.1 グループの BI 起動パッドの基本設定を設定する

1. CMC の[ユーザとグループ]管理エリアを表示します。
2. グループ一覧からグループを選択します。
3. ► **アクション** ► **BI 起動パッドの基本設定** ► をクリックします。

[BI 起動パッドの基本設定] ダイアログボックスが表示されます。

4. [基本設定が定義されていません] を選択解除します。
5. ユーザの初期ビューを設定する
 - ユーザが最初にログインしたときに **ホーム** タブを表示するには、[ホームタブ] をクリックして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
[デフォルトのホーム] タブ	BI プラットフォームのデフォルトの ホーム タブが使用されます。
[ホーム] タブの選択	<p>特定の Web サイトをホームタブとして表示します。</p> <p>[ホーム] タブを参照] をクリックします。[カスタムホーム] タブを選択] ウィンドウで、リポジトリオブジェクトを選択し、[開く] をクリックします。</p> <div style="background-color: #fff9c4; padding: 10px; margin-top: 10px;"> <p>i 注記</p> <p>リポジトリにすでに追加されているオブジェクトのみを選択できます。</p> </div>

- ユーザが最初にログインしたときに **ドキュメント** タブを表示するには、[ドキュメント] をクリックして、デフォルトで開かれるドロワおよびノードを指定します。以下から選択できます。

ドロワ	ノードオプション
マイドキュメント	<p>以下から、ドキュメント タブに表示する項目を選択します。</p> <ul style="list-style-type: none"> ○ お気に入り ○ 個人用カテゴリ ○ マイ受信ボックス
フォルダ	<p>以下のいずれかを選択します。</p> <ul style="list-style-type: none"> ○ パブリックフォルダ: これは、ドキュメント タブにパブリックフォルダを表示します。 ○ パブリックフォルダの選択 <p>[フォルダの参照] をクリックして、[ドキュメント] タブに表示する特定のパブリックフォルダを選択します。</p>
カテゴリ	<p>以下のいずれかを選択します。</p> <ul style="list-style-type: none"> ○ 会社用カテゴリ: これは、ドキュメント タブに会社用カテゴリを表示します。 ○ 会社用カテゴリの選択 <p>[フォルダの参照] をクリックして、[ドキュメント] タブに表示する特定の会社用カテゴリを選択します。</p>

たとえば、最初にログオンしたときに BI 受信ボックスに [**マイドキュメント**] ドロワを開く場合は、[**マイドキュメント**] をクリックしてから、[**マイ受信ボックス**] をクリックします。

6. [**ドキュメント**] タブに表示される列を選択します] で、ユーザの一覧パネルで各オブジェクトについて表示する概要情報を以下から選択します。
 - **型**
 - **最終実行日時**
 - **インスタンス**

- 説明
- 作成者
- 作成日
- 場所 (カテゴリ)
- 受信日 (受信ボックス)
- 差出人 (受信ボックス)

7. [ドキュメントの表示場所の設定] で、ユーザに対するドキュメントの表示方法を選択します。

ユーザは BI 起動パッド内の新しいタブ、または新しい Web ブラウザウィンドウでドキュメントを開いて表示できます。

8. [ページあたりのオブジェクト数 (最大) の設定] フィールドに数値を入力して、ユーザがオブジェクトの一覧を表示するときに 1 ページに表示するオブジェクトの最大数を指定します。

9. [保存して閉じる] をクリックします。

指定した基本設定は、手順 2 で選択したグループのユーザのデフォルトとして適用されます。ただし、自分の基本設定を設定する権限がある場合は、ユーザは独自の BI 起動パッド基本設定を作成できます。ユーザが基本設定を変更できないようにするには、基本設定を設定する権限をユーザに付与しないでください。

5.2.17 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。

i 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。詳細については、SAP のマニュアルを参照してください。

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。

5.2.18 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。

関連リンク

[LDAP ホストを設定する](#) [ページ 204]

[SAP ロールをインポートする](#) [ページ 262]

[AD ユーザーとグループをマップする](#) [ページ 225]

5.2.19 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。

i 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. 必要の場合は、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。

5.2.20 拡張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

i 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。

5.3 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。

5.3.1 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。

i 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。

5.3.2 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。

i 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。

5.3.3 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。

i 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。

5.3.4 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。

i 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。

5.3.5 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。

i 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。

関連リンク

[エイリアスを削除する](#) [ページ 98]

6 アクセス権の設定

6.1 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。

関連リンク

[権限の上書き](#) [ページ 104]

6.1.1 アクセスレベル

アクセスレベルは、ユーザが頻繁に必要な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ります。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。

関連リンク

[アクセスレベルの使用](#) [ページ 113]

6.1.2 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。

表 6: 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。
	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。

関連リンク

[種類固有アクセス権](#) [ページ 106]

6.1.3 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。

6.1.3.1 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。

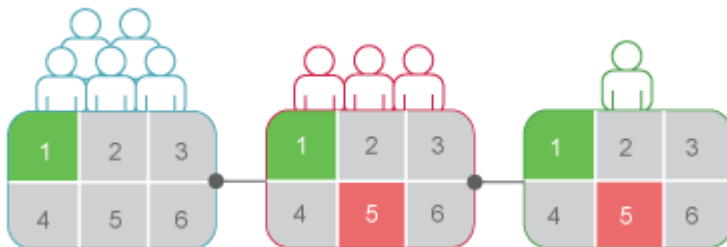


図 1: グループ継承の例 1

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。

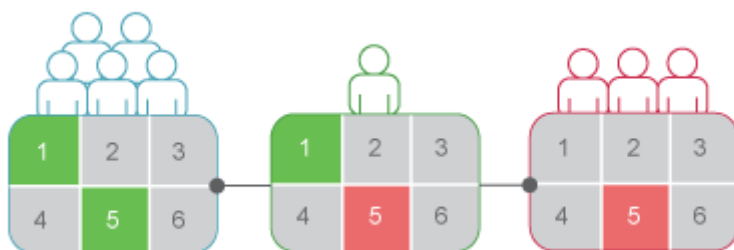


図 2: グループ継承の例 2

関連リンク

[権限の上書き](#) [ページ 104]

6.1.3.2 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。

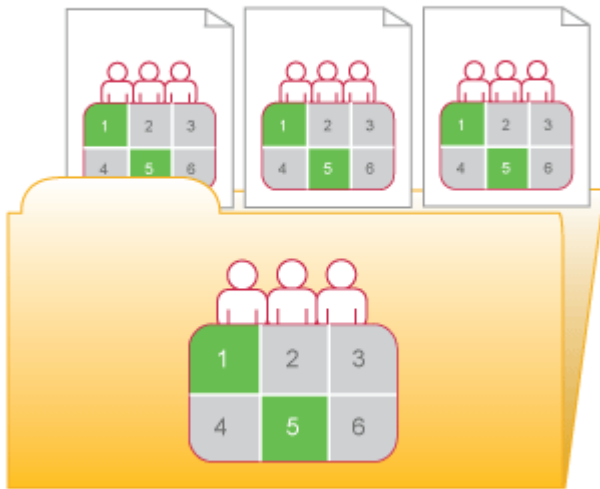


図 3: フォルダ継承の例

関連リンク

[権限の上書き](#) [ページ 104]

6.1.3.3 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ー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。青のユーザーが受け取った、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。

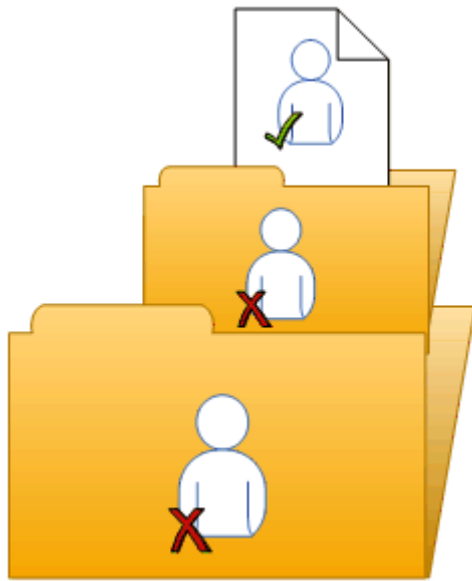


図 4: 権限の上書きの例 1

“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。

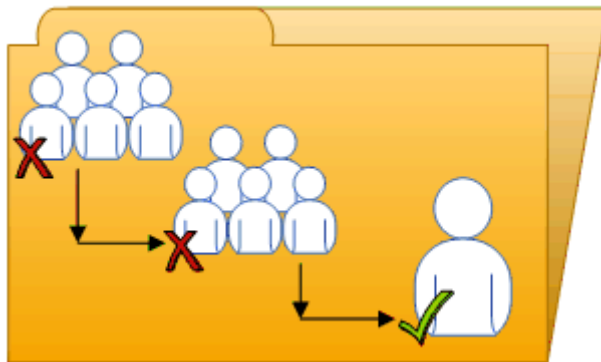


図 5: 権限の上書きの例 2

“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。

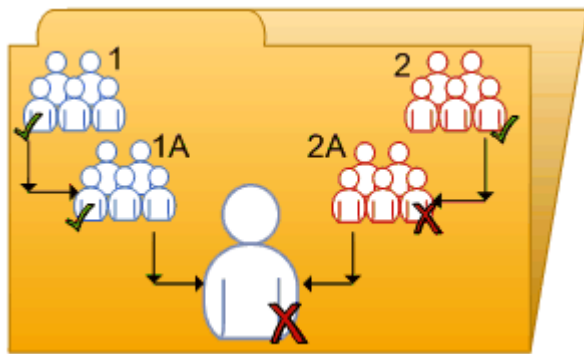


図 6: 複雑な権限の上書き

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。

6.1.3.4 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。

6.1.4 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。

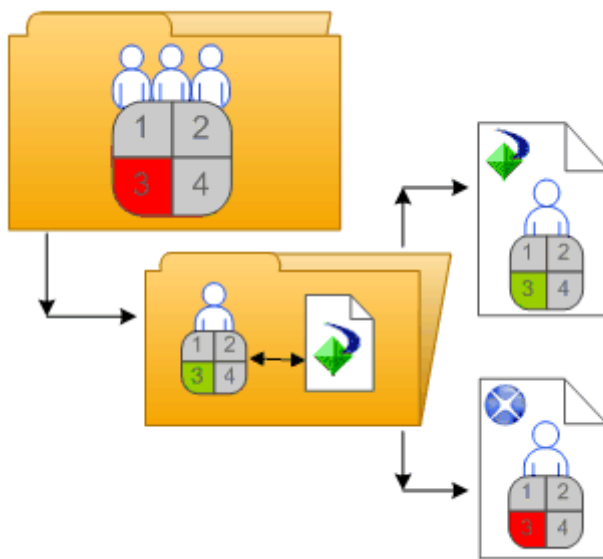


図 7: 種類固有アクセス権の例

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、カレンダー、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。

6.1.5 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。

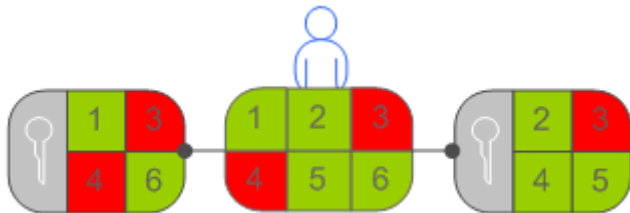


図 8: 複数アクセスレベル

- 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。

6.2 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。

6.2.1 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。
 - 割り当てられているアクセス権
 - 許可されているアクセス権
 - 割り当てられていないアクセス権
 - アクセスレベル
 - オブジェクトの種類
 - アクセス権の名前
- 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
 - 種類
 - アクセス権の名前
 - アクセス権のステータス(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。

6.2.2 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。

関連リンク

[オブジェクトの主体のセキュリティを変更する](#) [ページ 110]

6.2.3 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。

関連リンク

[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](#) [ページ 109]

6.2.4 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。

i 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。

関連リンク

[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](#) [ページ 109]

[オブジェクトの主体のセキュリティを変更する](#) [ページ 110]

6.2.5 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。

6.2.5.1 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。

コレクション	種類	権限名	
全般	全般	オブジェクトをフォルダに追加する	✓
全般	全般	ユーザーが所有するフォルダにオブジェクトを追加する	✓

[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、[ユーザー一覧]または[グループ一覧]を展開し、主体を探るか、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。

- 一覧の横にあるチェックボックスをオンにします。
- 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。

i 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。

6.3 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。

表 7: 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。	<ul style="list-style-type: none"> • 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

アクセスレベル	説明	関連するアクセス権
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。	<p>[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。</p> <ul style="list-style-type: none"> 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。	<p>[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。</p> <ul style="list-style-type: none"> レポートのデータを最新表示する
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。	<p>次のようなすべてのアクセス権を利用できます。</p> <ul style="list-style-type: none"> 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	<p>アクセスレベルに対する表示権限</p> <p>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</p> <p>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</p>

アクセスレベルのタスク	必要な権限
	i 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

6.3.1 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、ライブレポート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。

6.3.2 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。

6.3.3 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。

6.3.4 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。

6.3.5 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。

i 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。

6.3.6 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。

権限のコレクション	▼一般的なグローバル権限	✓	✗	⚠	📄	📁
▼全般	アクセス権の継承設定を安全に変更する	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
全般	インスタンスの再スケジュール	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
コンテンツ	インスタンスを削除する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
アプリケーション	オブジェクトに対するユーザーの権限を変更する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
システム	オブジェクトをフォルダに追加する	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	オブジェクトを別のフォルダにコピーする	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	オブジェクトを削除する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	オブジェクトを編集する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	オブジェクトを表示する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	ジョブを処理するサーバー グループを定義する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	セキュリティ割り当てにアクセス レベルを使用する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	ドキュメントのインスタンスを一時停止して再開する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	ドキュメントのインスタンスを表示する	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[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。

関連リンク

[CMC でのオブジェクトのセキュリティ設定の管理](#) [ページ 108]

[種類固有アクセス権](#) [ページ 106]

6.3.7 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。

i 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。

i 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。

6.3.8 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。

i 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。

i 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

i 注記

これは、一方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。

関連リンク

[フェデレーション](#) [ページ 618]

[アクセスレベルとオブジェクト間の関係のトレース](#) [ページ 118]

6.4 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。

i 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無効です。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。

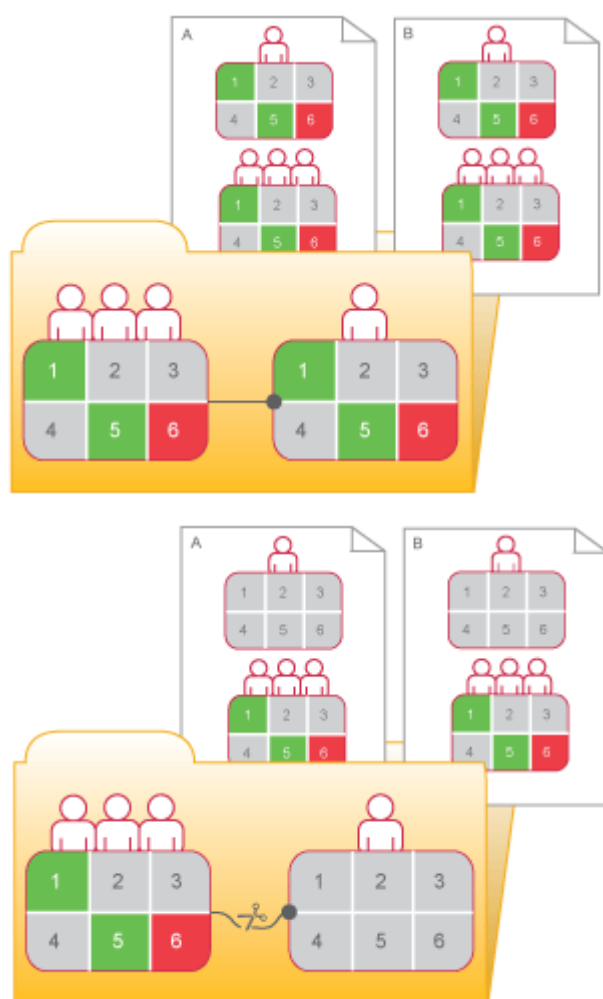


図 9: 継承の破棄

6.4.1 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。

6.5 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。

i 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。

表 8: 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 <div> <i>i</i> 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。 </div>
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 <div> <i>i</i> 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。 </div>

6.5.1 “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。[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。

6.5.2 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。

6.6 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。

7 BI プラットフォームのセキュリティ確保

7.1 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に設計されています。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。

7.2 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。

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。

7.3 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。オペレーティングシステム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。

i 注記

BI プラットフォームでは SFTP をサポートしていません。SFTP 機能が必要な場合は、SAP ノート 1556571 を参照するか、SAP パートナーのソリューションの利用を検討してください。

- 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。
- このプラットフォームには、デフォルトの Web アプリケーションサーバとして Apache Tomcat が含まれています。このサーバの利用を計画する場合は、セキュリティ更新のため、定期的に Apache サイトを参照してください。場合によっては、Tomcat のバージョンを手動で更新して、セキュリティの最新修正プログラムをインストールする必要があります。Web アプリケーションサーバを実行する場合の Apache Tomcat のセキュリティに関する推奨事項を参照してください。
- 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ります。
- 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。

関連リンク

[SSL プロトコルの設定](#) [ページ 145]

パスワード制限 [ページ 131]

同梱されたサードパーティサーバのセキュリティ設定 [ページ 127]

7.4 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、以下の同梱コンポーネントの文書にアクセスし、レビューすることをお勧めします。

- Microsoft SQL Server 2008 Express Edition™: Windows プラットフォーム用のこのシステムデータベースのセキュリティ確保の詳細については、<http://msdn.microsoft.com/en-us/library/bb283235%28v=sql.100%29.aspx> を参照してください。
- IBM DB2 Workgroup Edition™: UNIX プラットフォーム用のこのシステムデータベースのセキュリティ確保の詳細については、<http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/topic/com.ibm.db2.luw.container.doc/doc/c0052964.html> を参照してください。
- Apache Tomcat 6.0™: この Web アプリケーションサーバのセキュリティ確保の詳細については、<http://tomcat.apache.org/tomcat-6.0-doc/index.html> を参照してください。

7.5 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正確に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。

7.5.1 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。

i 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 起動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。

7.5.2 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わ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。

7.6 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。

i 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。

7.6.1 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。

7.7 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と、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。

7.7.1 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

i 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、Secure Sockets Layer(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。

7.7.2 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。

7.8 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。

7.9 Web 利用状況の監査

BI プラットフォームでは Web の利用状況を記録し、詳細情報を検査および監視できます。これにより、システムの実際状況を得ることができます。Web アプリケーションサーバでは、記録する時刻、日付、IP アドレス、ポート番号などの Web の属性を選択できます。監査データはディスク上に記録されてカンマ区切りテキストファイルに保存されるので、データから簡単にレポートを作成したり、データを他のアプリケーションにインポートできます。

7.9.1 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。

7.9.2 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。

- 大文字と小文字を含むパスワードを要求する
パスワードに、大文字、小文字、数字および句読点の文字形式から、少なくとも 2 つの形式の文字を使用するよう強制できます。
- 少なくとも N 文字以上のパスワードを要求する
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。

7.9.3 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った攻撃方法)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

7.9.4 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りません。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。

7.9.5 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。

7.10 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。

➡ ヒント

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でき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。

7.11 BI プラットフォームのデータセキュリティの概要

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。

7.11.1 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に作られています。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に作られています。SAP BusinessObjects Business Intelligence プラットフォーム 4.0 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。

- SAP BusinessObjects Business Intelligence プラットフォーム 4.0 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用して設定されます。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。

7.11.1.1 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. 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]** 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。
[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]** をクリックします。
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。

7.11.1.2 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. Unix マシンにインストールされている BI プラットフォームのディレクトリに移動します。
2. `sap_bobj` ディレクトリに変更します。
3. **「ccm.config」**と入力して **Enter** キーを押します。
`ccm.config` ファイルがロードされます。
4. 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 **[<ノード名> Launch]** のように表示されます。
5. 変更を保存し、**[終了]** します。
6. 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。

7.11.1.3 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。

7.12 BI プラットフォームでの暗号化

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。

7.12.1 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プログラムの実行中、Server Intelligence Agent 用に 6 文字のクラスタキーが指定されます。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。デフォルトの Windows のインストールでは、このファイルはディレクトリ C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64 に格納されます。Unix システムでは、このファイルは <INSTALLEDIR>/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	パス
AIX	<INSTALLEDIR>/sap_bobj/enterprise_xi40/ aix_rs6000_64 /
Solaris	<INSTALLEDIR>/sap_bobj/enterprise_xi40/ solaris_sparcv9/
Linux	<INSTALLEDIR>/sap_bobj/enterprise_xi40/ linux_x64/

ファイル名は次の規則に基づきます: _boe_<sia_name>.dbinfo。<sia_name> にはクラスタの Server Intelligence Agent の名前が入ります。

i 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、デプロイしたすべてのノードに対して 6 文字の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。

7.12.1.1 Windows 上でクラスタキーをリセットする

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。

ノードのクラスタキーをリセットするには、次の手順に従います。

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** 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]** と表示されるまで、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、**[プロパティ]** タブが開きます。

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る場合は、次に進む前に、警告メッセージが示すすべての要件が満たされていることを確認します。
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] フィールドと [新規クラスタキーの確認] フィールドの両方に同じ 6 文字のキーを入力します。

i 注記

Windows プラットフォームでは、クラスタキーに小文字、大文字、数字、句読点のうち 2 つの文字タイプが含まれている必要があります。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。

7.12.1.2 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. Unix マシンにインストールされている BI プラットフォームのディレクトリに移動します。
2. ディレクトリ名を `sap bobj` に変更します。
3. 「`cmsdbsetup.sh`」と入力して **Enter** キーを押します。
[CMS データベースのセットアップ] 画面が表示されます。
4. ノードの名前を入力し、**Enter** キーを押します。
5. 「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。
6. [はい] を選択して続行します。
7. 指定されたフィールドに、8 文字の新しいクラスタキーを入力し、**Enter** キーを押します。

i 注記

Unix プラットフォームでは、有効なクラスタキーは 8 文字の任意の組み合わせで構成されます。制限事項はありません。

8. 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。
9. 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。

7.12.2 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。

i 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。

7.12.2.1 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。

i 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. [\[ユーザー一覧\]](#) 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、暗号管理者グループに追加するユーザを、[\[選択されたユーザ/グループ\]](#) 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きます。

7.12.2.2 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 ▶](#) に移動します。
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。

関連リンク

[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](#) [ページ 140]

7.12.3 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

関連リンク

[暗号化キーのステータス](#) [ページ 139]

[新しい暗号化キーを作成する](#) [ページ 141]

[システムから暗号化キーを削除する](#) [ページ 142]

[暗号化キーを無効化する](#) [ページ 142]

[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](#) [ページ 140]

[暗号化キーを改ざんありにする](#) [ページ 141]

7.12.3.1 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 [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。

ステータス	説明
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: 交換が一時停止	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。

7.12.3.2 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

- CMC の [暗号化キー] 管理エリアでキーを選択します。
- 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。
- [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。

7.12.3.3 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。

7.12.3.4 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。

i 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。

i 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。

関連リンク

[暗号化キーを無効化する](#) [ページ 142]

[暗号化キーのステータス](#) [ページ 139]

[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](#) [ページ 140]

7.12.3.5 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。
[\[暗号化キーの無効化\]](#) ダイアログボックスが開き、警告メッセージが表示されます。
3. [\[OK\]](#) をクリックして、暗号化キーを無効化します。
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。

7.12.3.6 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。
[\[暗号化キーの削除\]](#) 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。

i 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。

関連リンク

[暗号化キーを無効化する](#) [ページ 142]

[暗号化キーのステータス](#) [ページ 139]

7.13 サーバの SSL 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。

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。

i 注記

Crystal Reports または Designer などのシッククライアントを使用していて、これらのシッククライアントから 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。

7.13.1 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、SSLC 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。

i 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、証明書とキーを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。

i 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。

i 注記

旧バージョンの BI プラットフォームに作成した証明書は、SAP BusinessObjects Business Intelligence プラットフォーム 4.0 には機能しません。これらの証明書は再作成する必要があります。

7.13.1.1 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

1. `SSLC.exe` コマンドライン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共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)。

2. 次のコマンドを入力します。

```
sslsc req -config sslc.cnf -new -out cacert.req
```

このコマンドは、認証機関 (CA) 証明書要求 (cacert.req) と秘密鍵 (privkey.pem) の 2 つのファイルを作成します。

3. 秘密鍵を復号化するには、次のコマンドを入力します。

```
sslsc rsa -in privkey.pem -out cakey.pem
```

このコマンドは、復号化された鍵 (cakey.pem) を作成します。

4. CA 証明書に署名するには、次のコマンドを入力します。

```
sslsc x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days 365
```

このコマンドは、自己署名証明書 (cacert.pem) を作成します。この証明書の有効期間は 365 日です。セキュリティの必要に応じて、日数を選択します。

5. テキストエディタを使用して、SSLc コマンドラインツールと同じフォルダに格納されている sslc.cnf ファイルを開きます。

i 注記

Windows Explorer は .cnf 拡張子を正しく認識してファイルを表示できない可能性があるため、テキストエディタの使用をお勧めします。

6. sslc.cnf ファイルの設定に基づいて、次の手順を実行します。

- sslc.cnf ファイルの certificate オプションと private_key のオプションで指定されたディレクトリに、cakey.pem ファイルと cacert.pem ファイルを配置します。

デフォルトでは、sslc.cnf ファイルの設定は、次のようになっています。

```
certificate = $dir/cacert.pem
private_key = $dir/private/cakey.pem
```

- sslc.cnf ファイルの database 設定で指定した名前でファイルを作成します。

i 注記

デフォルトでは、このファイルは \$dir/index.txt です。ファイルの中身は空である必要があります。

- sslc.cnf ファイルの serial 設定で指定した名前でファイルを作成します。
このファイルにオクテット文字列のシリアル番号(16 進形式)が指定されていることを確認します。

i 注記

さらに証明書を作成し、署名できるようにするには、11111111111111111111111111111111 などの大きな偶数桁の 16 進数を指定します。

- sslc.cnf ファイルの new_certs_dir 設定で指定されたディレクトリを作成します。

7. 証明書リクエストと秘密鍵を作成するには、次のコマンドを入力します。

```
sslsc req -config sslc.cnf -new -out servercert.req
```

生成された証明書とキーファイルは、現在の作業フォルダの下に配置されます。

8. 以下のコマンドを実行し、privkey.pem ファイルのキーを復号化します。


```
sslc rsa -in privkey.pem -out server.key
```

9. CA 証明書を使って証明書に署名するには、次のコマンドを入力します。

```
sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
```

このコマンドは、servercert.pem ファイルを作成します。このファイルには、署名された証明書が含まれています。

10. 次のコマンドを使用すると、証明書を DER エンコードされた証明書に変換できます。

```
sslc x509 -in cacert.pem -out cacert.der -outform DER
```

```
sslc x509 -in servercert.pem -out servercert.der -outform DER
```

注記

CA 証明書 (cacert.der) とそれに対応する秘密鍵 (cakey.pem) は、デプロイメントごとに 1 回だけ生成する必要があります。同じデプロイメント内のすべてのマシンは同じ CA 証明書を共有する必要があります。他のすべての証明書は、任意の CA 証明書の秘密鍵で署名する必要があります。

11. 生成された秘密キーの復号化に使用するプレーンテキスト passphrase を格納するテキストファイル (passphrase.txt) を作成します。
12. BI プラットフォームでマシンがアクセスできる安全な場所 ((d:/ssl) と同じディレクトリの下) に次のキーファイルと証明書ファイルを格納します。
- トラストド証明書ファイル (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

この場所は、CCM と Web アプリケーションサーバ用に SSL を設定するときに使用されます。

7.13.2 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。

7.13.2.1 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。たとえば、d:\ssl です。
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
信頼された SSL 証明書ファイル	信頼された SSL 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。

注記

ディレクトリはサーバが稼働中のマシンに対して指定する必要があります。

7.13.2.2 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] オプションを選択します。
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 クラスタの場合は、それぞれの SIA について手順 1 ～ 6 を繰り返します。
8. ccm.sh スクリプトを使用して SIA を起動し、サーバが起動するまで待機します。

7.13.2.3 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。以下はその例です。

```
-Dbusinessobjects.orb.ocj.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
<code><DcertDir> =d:\ssl</code>	すべての証明書と鍵を格納するディレクトリ。
<code><DtrustedCert> =cacert.der</code>	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。
<code><DsslCert> =clientcert.der</code>	SDK によって使用される証明書。
<code><DsslKey> =client.key</code>	SDK 証明書の秘密鍵。
<code><Dpassphrase> =passphrase.txt</code>	秘密鍵のパスフレーズを格納するファイル。

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。

7.13.2.4 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	<code>d:\ssl</code>
サーバ SSL 証明書ファイル名	<code>servercert.der</code>
信頼されている SSL 証明書またはルート証明書ファイル名	<code>cacert.der</code>
SSL 秘密キーファイル名	<code>server.key</code>
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	<code>passphrase.txt</code>

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) やアップグレードマネジメントツール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。

i 注記

ディレクトリはサーバが稼働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。

SSLC ツールは、BI プラットフォームソフトウェアと共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 -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。

関連リンク

[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 \[ページ 143\]](#)

7.13.2.4.1 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。

7.13.2.4.2 レポート変換ツールに対して SSL 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。さらに、レポート変換ツールは BI プラットフォームデプロイメントの一部としてインストールする必要があります。

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
信頼されている 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 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

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、レポート変換ツールで動作する SSL を設定できるようになります。

1. レポート変換ツールをホストするマシンで、Windows の環境変数 <BOBJ_MIGRATION> を作成します。

➡ ヒント

変数には、任意の値を設定することができます。

2. テキストエディタを使用して、以下のディレクトリに保存されている migration.bat を開きます。

```
<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\scripts\.
```

3. 次の行を探します。

```
start "" "%JRE%\bin\javaw" -Xmx512m -Xss10m -jar "%SHAREDIR%\lib\migration.jar"
```

4. -Xss10m パラメータの後に、以下を追加します。

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/ssl
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dbusinessobjects.migration
```

i 注記

各パラメータ間に、1 個のスペースがあることを確認します。

5. 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 を使用してレポート変換ツールにアクセスすることができます。

関連リンク

[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 \[ページ 143\]](#)

7.14 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。

関連リンク

[ファイアウォール用の BI プラットフォームの設定](#) [ページ 157]

[一般的なファイアウォールシナリオの例](#) [ページ 162]

7.14.1 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。

7.14.1.1 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。

7.14.1.2 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

7.14.1.3 CMS で使用する 2 つのポート

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回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。

7.14.1.4 登録したサービスの Central Management Server ディレクトリ

Central Management Server (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。

i 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。

関連リンク

[BI プラットフォームコンポーネント間の通信](#) [ページ 152]

7.14.1.5 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。

7.14.1.6 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。

関連リンク

[コマンドラインの概要](#) [ページ 745]

7.14.2 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。

7.14.2.1 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. CMS™ は 2 つのポートを使用します。BI プラットフォームサーバ、リッチクライアント、および 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 Central Management Server (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。

i 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 <<port range>>` 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、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。

関連リンク

[BI プラットフォームのポート要件](#) [ページ 153]

7.14.2.2 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。

7.14.2.2.1 BI プラットフォームアプリケーションのポート要件

構文

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	サーバのポートの要件
Crystal Reports	SAP Crystal Reports 2011 designer	CMS Input File Repository Server(FRS) Output File Repository Server(FRS) Crystal Reports 2011 Report Application Server (RAS) Crystal Reports 2011 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 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 Crystal Reports 2011 Report Application Server リクエストポート Crystal Reports 2011 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 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 Crystal Reports Processing Server 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	サーバのポートの要件
			Crystal Reports Cache Server リクエストポート
ダッシュボード	SAP BusinessObjects Dashboards	CMS Input File Repository Server(FRS) Output File Repository Server(FRS) 特定のデータソース接続に必要な Dashboards、Live Office、および QaaWS 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)	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 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 HTTP ポート(デフォルトは 80)
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)
BI プラットフォーム	SAP BusinessObjects Web Intelligence デスクトップ	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 File Repository Server(FRS)リクエストポート
BI プラットフォーム	ユニバースデザイナツール	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 File Repository Server(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 File Repository Server(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。

製品	クライアントアプリケーション	関連するサーバ	サーバのポートの要件
			<p>CMS ネームサーバポート (デフォルトでは 6400)</p> <p>CMS リクエストポート</p> <p>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。</p> <p>Microsoft Directory Services(TCP ポート 445)</p> <p>NetBIOS Session Service(TCP ポート 139)</p> <p>NetBIOS Datagram Service(UDP ポート 138)</p> <p>NetBIOS Name Service(UDP ポート 137)</p> <p>DNS(TCP/UDP ポート 53)</p> <p>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。</p>
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	<p>SIA リクエストポート (デフォルトでは 6410)</p> <p>CMS ネームサーバポート (デフォルトでは 6400)</p> <p>CMS リクエストポート</p>
BI プラットフォーム	レポート変換ツール	CMS Input File Repository Server (FRS)	<p>CMS ネームサーバポート (デフォルトでは 6400)</p> <p>CMS リクエストポート</p> <p>Input File Repository Server(FRS)リクエストポート</p>
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)	<p>CMS ネームサーバポート (デフォルトでは 6400)</p> <p>CMS リクエストポート</p> <p>Input File Repository Server(FRS)リクエストポート</p> <p>Output File Repository Server(FRS)リクエストポート</p>
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	デPLOY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。	<p>CMS ネームサーバポート (デフォルトでは 6400)</p> <p>CMS リクエストポート</p>

製品	クライアントアプリケーション	関連するサーバ	サーバのポートの要件
	プラットフォーム SDK	たとえば、SDK が CMS からの Crystal レポートを受信しこれと通信するには、Crystal Reports 2011 Processing Server リクエストポートを使った通信が必要です。	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 2011 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 File Repository Server(FRS)リクエストポート

7.14.2.2.2 サードパーティアプリケーションのポートの要件

構文

次の表に、SAP Business Objects 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 Business Objects 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。

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 Business Objects 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 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 起動パッドおよび CMC を含むすべての SAP Business Objects 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。
電子メールサーバ	すべての Job Server	SMTP(ポート 25)	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。
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 Idap.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。

7.15 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。

7.15.1 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通過して通信する必要がある Job Server の子のポートの範囲を設定します。
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。

関連リンク

[Communication between BusinessObjects Enterprise components](#) [ページ 152]

[Changing the default server port numbers](#) [ページ 343]

[コマンドラインの概要](#) [ページ 745]

[Specifying the firewall rules](#) [ページ 158]

[Configure the hosts files](#) [ページ 159]

7.15.1.1 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。

サーバの [ポート] ボックスで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 Business Objects サーバは、複数のポートを使用します。

i 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。

i 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 [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

関連リンク

[BI プラットフォームコンポーネント間の通信](#) [ページ 152]

7.15.1.2 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。

i 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。

7.15.1.2.1 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、`\WINNT\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。

7.15.1.2.2 UNIX で `hosts` ファイルを設定する

i 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、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。

7.15.2 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
```

7.15.2.1 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。

関連リンク

[ポート番号の設定](#) [ページ 343]

7.16 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。

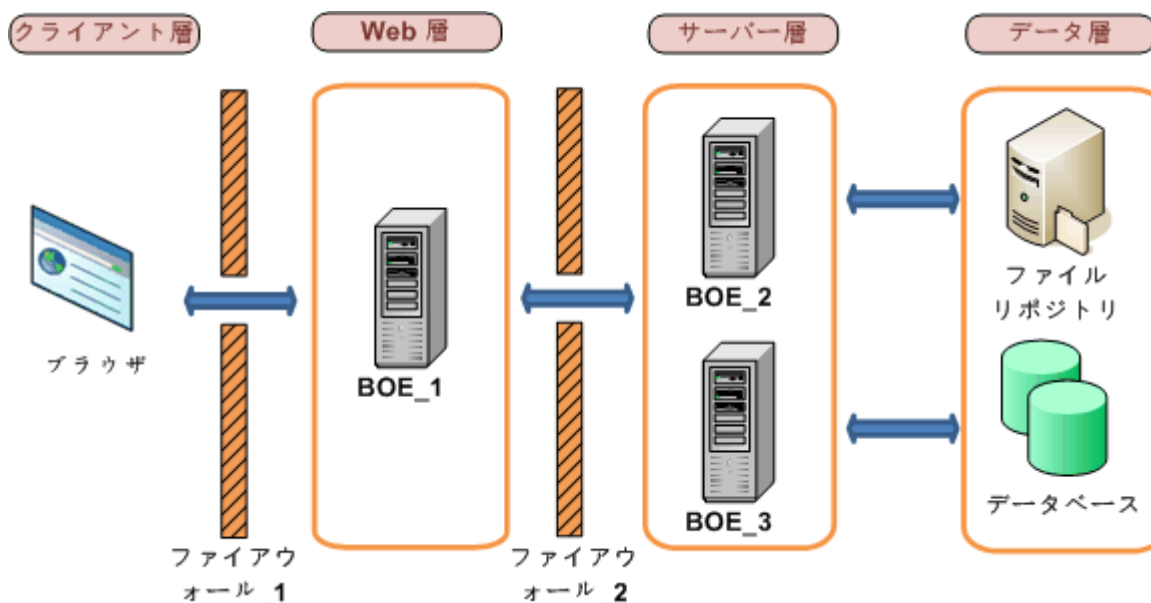
7.16.1 例: 別のネットワークにデプロイされたアプリケーション層

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。

図 10: 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



7.16.1.1 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。

- 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。
- 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

- 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。

表 9: 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

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	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。

関連リンク

[ポート番号の設定](#) [ページ 343]

[BI プラットフォームコンポーネント間の通信について](#) [ページ 149]

7.16.2 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。

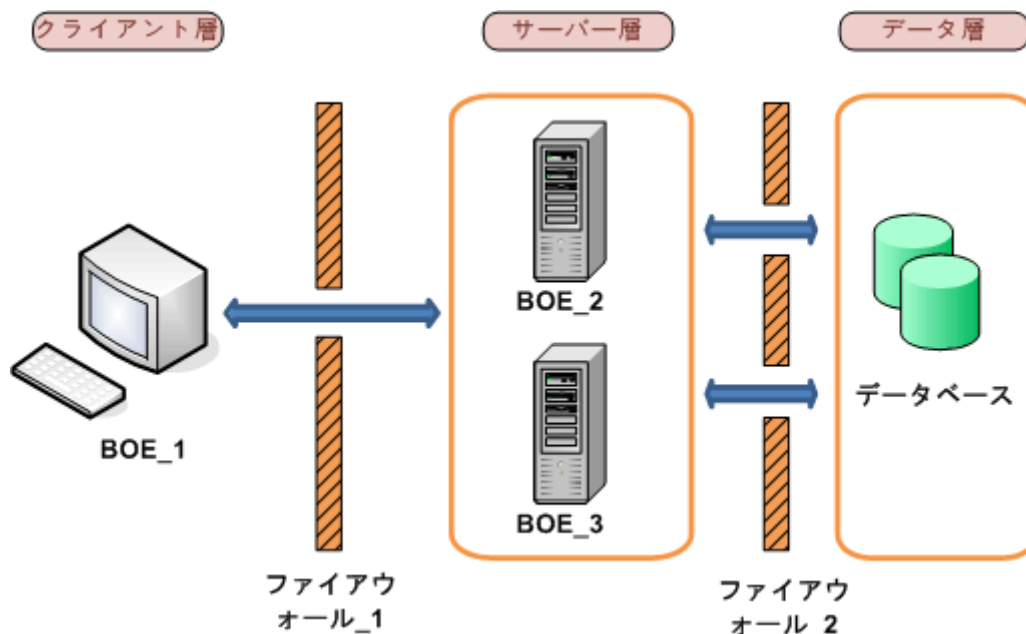
- 1 つのファイアウォールでシッククライアントが BI プラットフォームサーバから隔てられています。
- 1 つのファイアウォールで BI プラットフォームサーバがデータベース層から隔てられています。

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。

図 11: 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



7.16.2.1 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。

- 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。
- 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

- 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ます。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する必要があります。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。

関連リンク

[BI プラットフォームコンポーネント間の通信について](#) [ページ 149]

[ファイアウォール用の BI プラットフォームの設定](#) [ページ 157]

7.17 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

7.17.1 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。

i 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。

関連リンク

[ローカル SAP ゲートウェイのインストール](#) [ページ 665]

7.17.1.1 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 (ABAP) 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
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

7.17.2 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 EnterpriseOne 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	<ul style="list-style-type: none"> 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。

表 10: 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

7.17.3 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)

i 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。

7.17.3.1 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

7.17.4 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 BusinessObjects Business Intelligence プラットフォーム	<ul style="list-style-type: none"> 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。

表 11: 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

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

7.17.5 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。
 - Echo(TCP)ポート 7。Sign-on Server へのアクセスを確認します。
 - 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。
 - 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 (たとえば 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 (たとえば 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。

表 12: 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
Business Intelligence プラットフォーム	<ul style="list-style-type: none"> BI プラットフォーム Sign-on Server のポート

表 13: 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	BI プラットフォーム Sign-on Server for Siebel	任意	許可
CMS	任意	BI プラットフォーム Sign-on Server for Siebel	任意	許可
BI プラットフォーム Sign-on Server for Siebel	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

7.18 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。

7.18.1 サポートされるリバースプロキシサーバ

BI プラットフォームは、次のリバースプロキシサーバをサポートします。

- IBM Tivoli Access Manager WebSEAL 6
- Apache 2.2
- Microsoft ISA 2006

7.18.2 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 2 つの特定の 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 起動パッド、OpenDocument を含みます。
- `dswsboobje`: 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。

7.19 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。

7.19.1 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 dswebobje 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。

i 注記

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。

i 注記

BI プラットフォームにバンドルされている Tomcat パージョンなどの 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。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、カスタム設定を定義できます。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。

/ 文字の一貫した使用

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「/」を入れます。

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、/ (スラッシュ) を一貫して使用します。ソース URL の最後に / (スラッシュ) 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。

7.19.2 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PLOYされた場合に、固有の設定が必要になります。

7.19.3 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PLOYされている各 WAR ファイルに対して、ProxyPass を設定します。
4. リバースプロキシサーバの背後にデPLOY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。次はその例です。

```
ProxyPass /C1/BOE/ http://<<appservername>>:80/BOE/  
ProxyPassReverseCookiePath / /C1/BOE  
ProxyPassReverse /C1/BOE/ http://<<appservername>>:80/BOE/  
ProxyPass /C1/explorer/ http://<<appservername>>:80/explorer/  
ProxyPassReverseCookiePath / /C1/explorer  
ProxyPassReverse /C1/explorer/ http://<<appservername>>:80/explorer/
```

7.19.4 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PLOYすることは、可能ですが推奨はされません。このデPLOY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
```

7.19.5 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。

i 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 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 リスト 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**

i 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。

7.20 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。

7.20.1 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。

7.20.1.1 Tomcat 6 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 を設定したり、新しい proxyName を追加するなどの変更が必要です。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 の場合、server.xml は C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\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。

```
<!-- 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"
    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. 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"
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 Business Objects™ 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。

7.20.1.2 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。

7.20.2 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。

7.20.2.1 Apache Tomcat 6 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" maxSpareThreads="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。

7.20.2.2 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。

7.20.2.3 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インします。
 - 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。

7.20.2.4 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]` をクリックします。
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。

7.20.3 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。

i 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。

7.20.3.1 CMC でデフォルトビューアの URL を調整する

1. CMC にログインします。
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] フィールドにデフォルトビューアの URL を入力して、[URL を設定] をクリックします。
たとえば、「`http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?sIDType=CUID&iDocID=%SI_CUID%`」と入力します。ここで、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。

8 認証

8.1 BI プラットフォーム内の認証オプション

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。

関連リンク

[Enterprise 認証の概要](#) [ページ 189]

[SAP 認証の設定](#) [ページ 254]

[LDAP 認証の使用](#) [ページ 202]

[Windows AD サポート要件と初期設定](#) [ページ 222]

[JD Edwards EnterpriseOne 認証の有効化](#) [ページ 295]

[Oracle EBS 認証の有効化](#) [ページ 305]

[PeopleSoft Enterprise 認証の有効化](#) [ページ 281]

[Siebel 認証の有効化](#) [ページ 300]

8.1.1 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。
- 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 起動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、クラスタ化された CMS がある場合、または BI 起動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、フェールオーバー目的でのみ使用されます。

注記

ログオントークンを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、フェールオーバーも無効になります。

8.1.2 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、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に対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。

i 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。

8.1.3 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。

8.1.3.1 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 起動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されるか、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

i 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、追加設定をせずに利用できます。
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、追加設定をせずに利用できます。BI 起動パッドおよび 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、追加設定をせずに利用できます。BI 起動パッドおよび CMC に対する Enterprise 認証による SSO には、信用できる認証が必要です。

- [BI プラットフォームへのシングルサインオン](#) [ページ 187]
- [データベースへのシングルサインオン](#) [ページ 189]
- [エンドツーエンドシングルサインオン](#) [ページ 189]

8.1.3.2 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。

8.1.3.3 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。

8.2 Enterprise 認証

8.2.1 Enterprise 認証の概要

Enterprise 認証とは、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したときに自動的に有効になり、無効にできません。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 設定は、セントラル管理コンソール (CMC) を使用する場合にのみ変更できます。

8.2.2 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	パスワードに、大文字、小文字、数字および句読点の文字形式から、少なくとも 2 つの形式の文字を使用するよう強制できます。
パスワード制限	少なくとも N 文字以上のパスワードを要求する	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。
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。
ユーザ制限	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。
ユーザ制限	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。
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。
ログオン制限	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。
ログオン制限	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	信用できる認証を有効化します。

関連リンク

[信用できる認証の有効化](#) [ページ 191]

8.2.3 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。

8.2.3.1 一般的なパスワード設定を変更する

i 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オプションのチェックボックスをクリックして、必要であれば値を入力します。

オプション	最小値	推奨する最大値
大文字と小文字を含むパスワードを要求する	該当なし	該当なし
少なくとも N 文字以上のパスワードを要求する	0 文字	64 文字(全角 32 文字)
N 日ごとにパスワードの変更を要求する	1 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	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	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	1 回	100 回
ログオン失敗回数を N 分後にリセットする	1 分後	100 分
N 分後に再びアカウントを有効にする	0 分	100 分

4. [更新] をクリックします。

8.2.4 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ーの 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、ユーザーの 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。

i 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がある、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。
- BI 起動パッドのシングルサインオン URL は、`http://server:port/BOE/BI` です。

関連リンク

[信用できる認証を使用するサーバを設定する](#) [ページ 192]

[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](#) [ページ 196]

8.2.4.1 信用できる認証を使用するサーバを設定する

信用できる認証を使用するには、BI プラットフォームにサインオンする必要がある、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。

- CMC にログオンします。
- [認証] 管理エリアで、[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。
- [信用できる認証] を探し、次の操作を実行します。
 - [信用できる認証を有効にする] をクリックします。
 - [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。
 - [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、クライアントコンピュータおよび CMS が信用を確立するために使用されます。信用できる認証は、サーバとクライアントコンピュータの両方で設定する必要があります。クライアントコンピュータは、アプリケーションサーバのことです。
[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
 - [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。
 - <<INSTALLDIR>>\SAP BusinessObjects Enterprise XI 4.0\win32_x86
 - <<INSTALLDIR>>\SAP BusinessObjects Enterprise XI 4.0\win64_x64
 - [共有シークレット有効期間] ボックスに、共有シークレットが有効となる日数を入力します。
 - 信用できる認証リクエストのタイムアウト値を指定します。

i 注記

タイムアウト値は、クライアントのクロックと CMS のクロックの許容できる最大時間差(ミリ秒)です。0 を入力すると、2 つのクロックの時間差は無制限になります。脆弱性が増して攻撃が繰り返される可能性があるため、この値を 0 に設定することはお勧めしません。

4. **[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、クライアントコンピュータおよび CMS が信用を確立するために使用されます。信用できる認証のクライアントを設定する必要があります。

8.2.5 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 起動パッドおよび 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。

8.2.5.1 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。

i 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。

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。

i 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。

8.2.5.2 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 のデフォルト `global.properties` ファイルに含まれる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。

プロパティ	デフォルト値	説明
<code>sso.enabled=true</code>	<code>sso.enabled=false</code>	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。信用できる認証を有効にするには、このプロパティを <code>true</code> に設定する必要があります。
<code>trusted.auth.shared.secret</code>	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。
<code>trusted.auth.user.param</code>	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。
<code>trusted.auth.user.retrieval</code>	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。次のいずれかが設定できます。 <ul style="list-style-type: none">• <code>REMOTE_USER</code>• <code>HTTP_HEADER</code>• <code>COOKIE</code>• <code>QUERY_STRING</code>• <code>WEB_SESSION</code>• <code>USER_PRINCIPAL</code> 信用できる認証を無効にするには、空白のままにします。
<code>trusted.auth.user.namespace.enabled</code>	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。プロパティが <code>true</code> 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ーは 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。プロパティが空白の場合は、信用できる

プロパティ	デフォルト値	説明
		認証はユーザ認証時に一致する名前を使用します。

8.2.5.3 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	<ul style="list-style-type: none"> <<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/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 起動パッドおよび 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。

i 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。

- 次に示す、Web アプリケーションをホストするコンピュータの 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。

- 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。
- 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=<Variable>
trusted.auth.shared.secret=<WEB_SESSION>
```

`trusted.auth.shared.secret` 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、 <code>trusted.auth.user.param</code> プロパティに指定します。
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、 <code>trusted.auth.user.param</code> 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、 <code>trusted.auth.user.param</code> 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、 <code>global.properties</code> の <code>trusted.auth.user.param</code> プロパティに指定します。
REMOTE_USER	ユーザ名は <code>HttpServletRequest.getRemoteUser()</code> 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 <code>HttpServletRequest</code> オブジェクトで <code>getUserPrincipal().getName()</code> を呼び出して取得されます。

i 注記

一部の Web アプリケーションサーバでは、環境変数 `REMOTE_USER` をサーバ上で `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。

i 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。WDDeploy 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。

8.2.5.3.1 サンプル設定

TrustedPrincipal.conf ファイル経由で共有シークレットを渡す

以下のサンプル設定では、ユーザ <JohnDoe> 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、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\win32_x86 ディレクトリに保存されています。Tomcat 6 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. 新しいファイルに、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=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=
```

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\webpath.InfoView\web\custom.jsp ファイルを探します。
5. custom.jsp ファイルに、次のプロパティを入力します。

```
<!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("MyUser", "JohnDoe");
%>
<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>
```

6. C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources に、myScript.js ファイルを作成します。

7. myScript.js ファイルに、次のプロパティを入力します。

```
function goToLogonPage() {  
    window.location = "logon.jsp";  
}
```

8. Web アプリケーションサーバを再起動します。
9. 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。

信用できる認証が適切に設定されていることを確認するには、URL `http://<[cmsname]>:8080/BOE/BI/custom.jsp` を使用して BI 起動パッドアプリケーションにアクセスします。ここで、`<[cmsname]>` は CMS をホストするマシン名です。[\[Click this to go to the logon page of BI launch pad\]](#) リンクが表示されます。

Web セッション変数経由で共有シークレットを渡す

以下のサンプル設定では、ユーザ `<JohnDoe>` 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 Web セッション経由で格納および渡されるのに対して、共有シークレットは Web セッション変数経由で渡されます。このファイルは、ディレクトリ `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` にあることが前提です。ファイルを開き、コンテンツを記録しておきます。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。

```
9ecb0778edcfff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773  
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

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. 新しいファイルを作成します。

i 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. 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。

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\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。

```
<!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", "9ecb0778edcfff048edae0fcdde1a5db8211
2934
86774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b6a3f1345
285b55a0a7"
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<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>
```

7. 次のディレクトリに、myScript.js ファイルを作成します。

C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web
\noCacheCustomResources

8. 以下を、myScript.js に追加します。

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

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。

信用できる認証が適切に設定されていることを確認するには、URL: `http://[cmsname]:8080/BOE/BI/custom.jsp`
を使用して BI 起動パッドアプリケーションにアクセスします。ここで、[cmsname] は CMS をホストするマシン名です。以下
のリンクが表示されます。

このリンクをクリックし、BI 起動パッドのログオンページに移動します。

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 6 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。

i 注記

Web アプリケーションサーバ設定は、REMOTE_USER の方法と USER_PRINCIPAL の方法で同じです。

1. Tomcat サーバを停止します。
2. デフォルトで C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\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、これを次の値に変更します。
`<Realm className="org.apache.catalina.realm.MemoryRealm" ... />`
4. デフォルトで C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\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>` タグを探し、次の値を入力します。

```
<user name=<FirstnameLastname> password=<password>
roles=<onjavauser>/>
```

6. web.xml ファイルを C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\ ディレクトリで開きます。
7. `</web-app>` タグの前に、次のタグを挿入します。

```
<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>
```

i 注記

`<url-pattern></url-pattern>` タグにページを追加する必要があります。通常、このページは BI 起動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 ファイルを開き、次の値を入力します。

```
trusted.auth.user.retrieval=USER_PRINCIPAL
trusted.auth.user.namespace.enabled=true
```

i 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 BOE 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。

信用できる認証を適切に設定したことを確認するには、[http://\[<cmsname>\]:8080/BOE/BI](http://[<cmsname>]:8080/BOE/BI) に移動して、BI 起動パッドにアクセスします。ここで [\[<cmsname>\]](#) は CMS をホストするマシンの名前です。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。

8.3 LDAP 認証

8.3.1 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 の代替プロトコルと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。

関連リンク

[LDAP 認証の設定](#) [ページ 203]

[LDAP グループのマッピング](#) [ページ 213]

8.3.1.1 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イ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。

関連リンク

[LDAP サーバまたは相互認証の SSL 設定](#) [ページ 207]

[Windows AD に対する LDAP のマッピング](#) [ページ 215]

[SiteMinder での LDAP プラグインの設定](#) [ページ 211]

8.3.2 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イ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)

i 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。

8.3.2.1 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する必要があります。

1. CMC の [認証] 管理エリアで、[LDAP] をダブルクリックします。

i 注記

[認証] 管理エリアに移動するには、ナビゲーションリストで [認証] をクリックします。

2. [LDAP ホストの追加 (ホスト名:ポート)] ボックスに 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] をクリックして、[OK] 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。

3. [LDAP サーバの種類] リストからサーバの種類を選択します。

i 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。

4. [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。

5. [次へ] をクリックします。
6. [ベース LDAP 識別名] ボックスに、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。
7. [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。

i 注記

管理者認証情報は不要です。

i 注記

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。

8. 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] に認証情報を入力し、[紹介のホップ最大数] ボックスに紹介ホップの数を入力します。

i 注記

[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。
- 紹介されるホストが、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。

i 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。

i 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。

9. [次へ] をクリックして、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。
10. [次へ] をクリックし、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。
11. [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] リストで、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。
 - 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] リストで、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、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) BI プラットフォームサービスライセンスがユーザロールに基づいていない場合は、**[新しいユーザのオプション]** リストで、新しいユーザの作成方法を指定するためのオプションを選択します。
- **新しいユーザを指定ユーザとして作成する**
指定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指定ユーザライセンスを持っている必要があります。
 - **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 プラットフォームサービス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、ユーザが情報プラットフォームサービス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。

12. **[属性バインディングオプション]** の下で、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。

i 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。

13. **[完了]** をクリックします。

関連リンク

[LDAP サーバまたは相互認証の SSL 設定](#) [ページ 207]

[SiteMinder での LDAP プラグインの設定](#) [ページ 211]

8.3.2.2 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。

i 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。

i 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）。

関連リンク

[LDAP 認証の設定](#) [ページ 203]

8.3.2.3 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。

関連リンク

[LDAP ホストを設定する](#) [ページ 204]

8.3.2.3.1 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	<p>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。</p> <ol style="list-style-type: none">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。 <p>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。</p>
サーバ証明書	<p>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。</p> <ol style="list-style-type: none">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	<p>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。</p> <ol style="list-style-type: none">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 ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_6_RTM/ 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。<pre>certutil -N -d .</pre>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。<pre>certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer</pre>5. Business Intelligence (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	<p>このファイルは、BI 起動パッドのような Java アプリケーションの SSL を用いるサーバ認証または相互認証に必要です。</p> <ol style="list-style-type: none">1. Javabin 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。<pre>keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore</pre>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。

リソース	このタスクを開始する前に実行する操作
クライアント証明書	<ol style="list-style-type: none"> <p>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。</p> <ul style="list-style-type: none"> 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。 <pre>certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .</pre> <p><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。</p> <p>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。</p> <pre>certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name></pre> <p>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。</p> <ul style="list-style-type: none"> 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。 <pre>keytool -genkey -keystore .keystore</pre> <p>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。</p> <pre>keytool -certreq -file <certificate_request_name> -keystore .keystore</pre> <p>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。</p> <pre>keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore</pre> <p>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。</p> <pre>keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore</pre>

リソース	このタスクを開始する前に実行する操作
	7. BI プラットフォームをホストするコンピュータの <code>cert7.db</code> または <code>cert8.db</code> ファイル、および <code>cacerts</code> ファイルと同じディレクトリに <code>.keystore</code> 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。

- **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する必要があります (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。

i 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。

i 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。

i 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。

関連リンク

[SiteMinder での LDAP プラグインの設定](#) [ページ 211]

8.3.2.4 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、[\[LDAP サーバの設定の概要\]](#) ページを使用して 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、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できます。[\[マップされた LDAP メンバーグループ\]](#) エリアも変更できます。

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。
4. 接続設定を変更し、[\[更新\]](#) をクリックします。
5. [\[エイリアス\]](#) と [\[新しいユーザ\]](#) 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。

8.3.2.5 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 か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

i 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。

関連リンク

[LDAP ホストを設定する](#) [ページ 204]

8.3.2.5.1 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]リンクを選択します。
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。

8.3.2.5.2 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および BOE war ファイルプロパティの SiteMinder 設定を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。

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

4. [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。
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=LDAP
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、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。

8.3.3 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。

i 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。

i 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。

関連リンク

[Windows AD に対する LDAP のマッピング](#) [ページ 215]

8.3.3.1 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](#)] 管理エリアで、[[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。
2. [[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 \(cn または dn ごと\)](#)] ボックスで LDAP グループを共通名 (cn) または識別名 (dn) で入力して、[[追加](#)] をクリックします。

複数の LDAP グループを追加できます。

➡ ヒント

グループを削除するには、LDAP グループを選択して **[削除]** をクリックします。

3. **[新しいエイリアスのオプション]** リストを使用して、Enterprise アカウントに LDAP 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。
 - **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 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選択します。
4. **[エイリアス更新オプション]** リストで、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**
 - **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**
5. **[新しいユーザのオプション]** リストからオプションを選択し、LDAP アカウントをマップするために作成される新しい Enterprise アカウントのプロパティを指定します。
 - **新しいユーザを指定ユーザとして作成する**
このオプションは、新しいユーザアカウントを指定ユーザのライセンスを使用するように設定する場合に選択します。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指定ユーザライセンスを持っている必要があります。
 - **新しいユーザを同時接続ユーザとして作成する**
このオプションは、新しいユーザアカウントを同時接続ユーザのライセンスを使用するように設定する場合に選択します。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。
6. **[更新]** をクリックします。

8.3.3.2 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。

i 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。

8.3.3.3 Windows AD に対する LDAP のマッピング

Windows 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必要があります。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	<p>次ではマッピングでできます。</p> <ul style="list-style-type: none">○ 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 <p>次ではマップできません。</p> <ul style="list-style-type: none">○ 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 <p>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</p>

状況	留意点
	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る場合、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。

8.3.3.4 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。

i 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。 <div> <div>i 注記</div> <p>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。</p> </div>

コンポーネント	要件
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。

8.3.3.4.1 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。

i 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
```

i 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 <code><sianame></code> 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。 <code>-ptype KRB5_NT_PRINCIPAL</code>
-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。 <code>-crypto RC4-HMAC-NT</code>

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。

8.3.3.4.2 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/krb5-1.9.1/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。

i 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/krb5.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
    }
```

i 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。

8.3.3.4.3 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 上にデプロイされた BI プラットフォームから 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] をクリックします。

i 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なになります。

- 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。

<code><sianame></code>	SIA の名前
<code><service ></code>	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) [デフォルトドメイン] 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。

関連リンク

[LDAP 認証の設定](#) [ページ 203]

8.3.3.4.4 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。

i 注記

このファイルを別の場所に保存することもできますが、その場合には 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>";
};
```

i 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。

8.3.3.5 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。

関連リンク

[LDAP 認証の設定](#) [ページ 203]

[LDAP グループのマッピング](#) [ページ 213]

8.4 Windows AD 認証

8.4.1 Windows AD 認証の使用

8.4.1.1 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。実行する必要が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。

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。
- Windows 2003、および Windows 2008 は Kerberos と NTLM 認証の両方をサポートするプラットフォームですが、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だけ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

i 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。

8.4.2 ドメインコントローラの準備

8.4.2.1 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。

i 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。

8.4.2.1.1 Windows 2003 または 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 -a` 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 起動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 -a BICMS/service_account_name.domain.com serviceaccountname
setspn -a HTTP/<servername> <servicename>
setspn -a HTTP/<servername.domain.com> <servicename>
setspn -a HTTP/<ip address of server> <servicename>
```

BICMS は SIA が実行中のマシンの名前、`<servername>` は BI 起動パッドがデプロイされるサーバの名前、`<servername.domain.com>` 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>.DOMAIN.com
HTTP/<servername>
<servername>/<servicename>DOMAIN.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.domain.com
HTTP/Tomcat6 HTTP/Tomcat6.domain.com
HTTP/Load_Balancer.domain.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。

8.4.3 CMC での AD 認証の設定

8.4.3.1 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 (2003 および 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。

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 2003 および 2008 ドメインの両方に対応しています。

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のみ機能します。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。
- 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。

8.4.3.2 AD ユーザー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。

i 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. [\[AD 設定の概要\]](#) エリアで、[\[AD 管理名\]](#) の横にあるリンクをクリックします。

i 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。

i 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)

i 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 起動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. [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。

i 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。

10. [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を正常にマッピングしていて、AD 認証オプションまたは AD グループ更新を設定しない場合は、手順 12 ~ 19 をスキップします。これらのオプションの設定は、手動 AD Kerberos 認証を正常に設定した後で、設定できます。

11. 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。

12. 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。

13. [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。

14. [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ピング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ピングされた各 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 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、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。
- **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。

15. 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。

16. **[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。

17. **[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。

18. **[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。

19. [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。

関連リンク

[To create a Kerberos configuration file for SAP NetWeaver, Tomcat, WebLogic, SAP NetWeaver or Oracle](#) [ページ 233]

8.4.3.3 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。

i 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。
毎月	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。
カレンダー	更新は、すでに作成されているカレンダー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 プラットフォーム内で作成、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。

- ユーザがログオンすると、その AD エイリアスが更新されます。
- 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。

i 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。

8.4.4 SIA 実行のための BI プラットフォームサービスの設定

8.4.4.1 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。

i 注記

データベースにシングルサインオンが必要がある場合は、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

8.4.4.2 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 ユーザグループが BI プラットフォーム に正常にマップされました。

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。

i 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. **[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。
7. **[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。
8. **[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。
9. **[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。
10. 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。

i 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。

11. SIA を再起動します。
12. 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。

8.4.4.3 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。

i 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する必要があります。

➡ 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。

8.4.5 AD 認証用の Web アプリケーションサーバの設定

8.4.5.1 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。

i 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

8.4.5.1.1 Kerberos の設定ファイルの作成

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 6、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。

i 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

i 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。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 =
}
```

i 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。

8.4.5.1.2 JAAS ログイン設定ファイルの作成

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。

i 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。

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。

i 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。

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。

SAP NetWeaver に `LoginModule` を追加する

Kerberos と SAP NetWeaver 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 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、Netweaver 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://<<マシン名>>:<<ポート>>/nwa`」と入力して、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。
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. NetWeaver Administrator からログアウトします。

8.4.5.13 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

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。

SAP NetWeaver 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. NetWeaver サーバに対応するインスタンス (たとえば [*Instance* - <<システム ID>><マシン名>>]) 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、NetWeaver サーバを再起動する必要があります。

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。

Oracle Application Server 上での Kerberos の Java オプションを変更する

Oracle Application Server で Kerberos を使用している場合、Java オプションを変更して Kerberos 設定ファイルの場所を指定する必要があります。

1. Oracle Application Server の管理コンソールにログインします。
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 OC4J インスタンス名をクリックします。
3. [\[サーバのプロパティ\]](#) を選択します。
4. 複数 VM の設定セクションまで下にスクロールします。
5. [\[コマンドラインオプション\]](#) で、[\[Java オプション\]](#) テキストフィールドの最後に、`-Djava.security.krb5.conf=C:/XXXX/krb5.ini` の行を追加します。XXXX は、ファイルの保存場所に置き換えます。
6. OC4J インスタンスを再起動します。

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インします。
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。

8.4.5.1.4 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. `[Enter]` キーを押します。
- 4. パスワードを入力します。
`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。

8.4.5.1.5 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 ユーザグループが BI プラットフォーム に正常にマップされました。
- 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. Web アプリケーション サーバをホストしているマシン上の 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。

i 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 起動パッドにログインできるようになります。いずれかのアプリケーションにアクセスし、認証オプションのリストから Windows AD を選択します。

i 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。

i 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。

8.4.6 シングルサインオンの設定

8.4.6.1 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 2 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 起動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。

8.4.6.2 Vintela SSO の使用

8.4.6.2.1 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. BOE 一般プロパティおよび BI 起動パッド固有のプロパティを Vintela SSO 用に設定する。
5. Tomcat 6 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。

8.4.6.2.2 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 起動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。
-princ	サービスアカウントに使用されるプリンシパル名を、次の SPN 形式で指定します: <code><MYSIAMYSERVER>/<sbo.service.domain.com>@<DOMAIN>.COM</code> 。 <code><MYSIAMYSERVER></code> 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。 i 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必要があります。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。 <code>-ptype KRB5_NT_PRINCIPAL</code>
-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。 <code>-crypto RC4-HMAC-NT</code>

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。

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。

8.4.6.2.3 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. 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。
5. **[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。
6. **[更新]** をクリックします。

8.4.6.2.4 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 起動パッドへの SSO を有効化することに注力することをお勧めします。

1. Web アプリケーション サーバをホストしているマシン上の 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。

i 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. 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
```

i 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。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。バックスラッシュを使用すると、SSO が中断されます。

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。

i 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。

i 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。

8.4.6.2.5 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とも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は、
`<TomcatINSTALLDIR>` を `C:\Program Files (x86)\SAP BusinessObjects\Tomcat6\` 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. <Connector ...> 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。

i 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。

8.4.6.2.6 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 Internet Explorer (IE) ブラウザの設定に関係します。

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せん。
 - 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。

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。

i 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。

i 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。

8.4.6.2.7 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。

8.4.6.2.8 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。

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 WIN ディレクトリです。

i 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。

8.4.6.3 SiteMinder の使用

8.4.6.3.1 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

i 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。

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。

i 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。

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 ユーザグループが BI プラットフォーム に正常にマップされました。
 - 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. [[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。
 5. 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 起動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。
 6. [[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。
 7. [[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。

8. **[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。

- **新しいユーザを指定ユーザとして作成する**

指定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指定ユーザライセンスを持っている必要があります。

- **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。

9. 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。

10. **[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。
11. [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。
12. [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。
13. [更新] をクリックし、[OK] をクリックします。

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。

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。

8.4.7 Windows AD 認証のトラブルシューティング

8.4.7.1 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

8.4.7.1.1 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
```

8.4.7.1.2 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
```

次はその例です。

```
C:\Program Files\SAP BusinessObjects\  
SAP Business Objects 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。

8.4.7.1.3 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。

8.4.7.1.4 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。

i 注記

この問題は、J2SE 5.0 によるものではありません。

8.5 SAP 認証

8.5.1 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。これらのパスワードは、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のため、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。

8.5.2 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)

権限オブジェクト	フィールド	値
	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)
	ユーザマスタメンテナンスのユーザグループ (CLASS)	<div> <div></div> <div>注記</div> </div> <p>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。</p>

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。

8.5.3 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、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。

8.5.3.1 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。

i 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。

i 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。

i 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。

関連リンク

[BI プラットフォームのユーザアカウントの作成](#) [ページ 255]

8.5.3.2 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表示されます。

➡ 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。

8.5.3.3 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。

8.5.4 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

8.5.4.1 SAP 認証オプションを設定する

1. CMC の [認証] 管理エリアで、[SAP] リンクをダブルクリックして [オプション] タブをクリックします。
2. 必要に応じて次の設定を確認し、内容を変更します。

設定	説明
SAP 認証を有効にする	SAP 認証を完全に無効にする場合は、このチェックボックスをオフにします。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。
コンテンツルートフォルダ	BI プラットフォームが CMC および BI 起動パッドで 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。この値を変更するには、CMC とコンテンツ管理ワークベンチの両方で値を変更する必要があります。
デフォルトシステム	<p>BI プラットフォームがデフォルトで使用する SAP 権限認証システム (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) を選択します。</p> <div> <p>i 注記</p> <p>デフォルトシステムを指定した場合、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 とクライアントを入力する必要があります。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。</p> </div>
権限認証システムへのアクセス試行の最大失敗数	<p>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、BI プラットフォームは、権限認証システムへのアクセスを無限回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。</p> <div> <p>i 注記</p> <p>この設定を [権限認証システムを無効な状態で維持 [秒数]] と併用して、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。これらの設定を基に、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。</p> </div>
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。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、特定の 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 回失敗すると、BI プラットフォームはそのシステムに対するユーザ認証の試行を指定された時間停止します。
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、このフィールドに「2」を入

設定	説明
	力すると、BI プラットフォームは SAP に対して 2 つの別個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]に「2」を指定し、[1 接続あたりの使用数]に「3」を指定した場合、1 つの接続でのログオン数が 3 になると、BI プラットフォームはその接続を閉じて再開します。
同時接続ユーザと指定ユーザ	<p>同時接続ユーザライセンスまたは指定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。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せん。このため、指定ユーザは、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。</p> <p>i 注記</p> <p>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することが必要です。</p>
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する場合に選択します。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。

以下のオプションを使用して、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	このボタンを使用して、生成されたキーストアファイルをアップロードし、SAP シングルサインオンを有効にします。表示されているフィールドにファイルへのフル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	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。

設定	説明
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。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	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。

3. [\[更新\]](#) をクリックします。

関連リンク

[SAP 認証の設定](#) [ページ 254]

8.5.4.2 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。

8.5.5 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。

i 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。各グループの命名規則は、[<SystemID~ClientNumber@NameOfRole>](#) です。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。

i 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。

関連リンク

[BI プラットフォームでのアクセス権の動作](#) [ページ 100]

[CMC でのオブジェクトのセキュリティ設定の管理](#) [ページ 108]

8.5.5.1 SAP ロールをインポートする

1. CMC の [\[認証\]](#) 管理エリアで、[\[SAP\]](#) リンクをダブルクリックします。
2. [\[オプション\]](#) タブで、使用許諾契約に応じて、[\[同時接続ユーザ\]](#) または [\[指定ユーザ\]](#) を選択します。
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ないことに注意してください。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。
3. [\[更新\]](#) をクリックします。
4. [\[ロールのインポート\]](#) タブで [\[論理システム名\]](#) リストから、権限認証システムを選択します。
5. [\[利用可能なロール\]](#) 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。
6. [\[更新\]](#) をクリックします。

8.5.5.2 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

1. 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 ユーザのユーザ名とパスワードを確認用に用意しておきます。
2. Java BI 起動パッドの場合は、<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 プラットフォームに設定したポート番号に置き換えます。入力に必要な Web サーバ名、ポート番号および正確な URL を管理者に確認する必要がある場合があります。

3. [認証の種類] 一覧で、[SAP] を選択します。

i 注記

BI 起動パッドでは、[認証の種類] 一覧はデフォルトで非表示になっています。管理者は、BILaunchpad.properties ファイルでこの一覧を有効にして、Web アプリケーションサーバを再起動する必要があります。

4. 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。
5. 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。
6. [ログオン] をクリックします。

選択したユーザとして BI 起動パッドにログオンされます。

8.5.5.3 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。

i 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。

8.5.5.3.1 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、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] 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] 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

頻繁に更新をする場合または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](#)]を選択します。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、必要に応じてスケジュール情報を入力してください。

次の定期スケジュールパターンを使用できます。

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。
カレンダー	更新は、すでに作成されているカレンダー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。

i 注記

今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](#)] 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。

8.5.6 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。

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があります。このガイドの ERP 環境の追加設定の章の SAP サーバサイドの信頼の設定の節で説明する手順に従うことをお勧めします。

8.5.6.1 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、および SAP BusinessObjects Enterprise 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。

無料の 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

無料の SAP 暗号ライブラリを使用して SAP BusinessObjects Enterprise に対するサーバサイドの信頼を有効化するには、登録されているセキュアネットワークコミュニケーション (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 により設定されています。SAP BusinessObjects Enterprise 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。

また、サーバサイドの信頼を設定するための 32 ビット SNC 暗号ライブラリも必要です。SAP Cryptographic Library (Windows および Unix 用) は、SAP の Web サイトからダウンロードできます。SAP Cryptographic Library 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ません。Cryptographic Library 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 SAP BusinessObjects Enterprise 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必要があります。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 SAP BusinessObjects Enterprise 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。本書では、PSE を設定して保守する方法、および PSE を SAP BusinessObjects Enterprise Processing Server と安全に関連付ける方法を説明します。

クライアント SNC とサーバ SNC

クライアント SNC では、SNC 名の識別子は、SU01にある1つ(または複数)の SAP ユーザ名にマップされます。ログオン要求が送信されると、SNC 名は SAP 名とともに SAP システムへ渡されますが、パスワードは送信されません。SNC 名が指定された SAP 名にマップされている場合、ログオンが許可されます。アプリケーションのホストへの直接ログオンに対するクライアントサイドのログオン文字列を以下に示します。

```
ASHOST=myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN USER=USER123
SNC_MODE=1 SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US"
```

このログオン処理が成功するには、SAP ユーザ USER123 は p:CN=TheUser, O=TheCompany, C=US in SU01 にマップされている必要があります。一方、サーバ SNC では、SNC 名の識別子と SAP ユーザ名との間に明示的なマップは必要あ

りません。代わりに、SNC 名は“任意の”ユーザがパスワードを入力しなくても偽装ログオンを実行できるように、トランザクション SNC0 で設定されます。たとえば、次のようになります。

```
ASHOST =myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN SNC_MODE=1
SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US" EXTIDTYPE=UN EXTIDDATA=USER123
```

サーバ SNC 偽装ログオンまたは外部 ID を介したログオンは、クライアント側で行う場合よりも非常に強力です。このログオンにより、システム内の任意の SAP ユーザアカウントにアクセスできます。他の外部 ID ログオンオプションには、ログオンチケットと X.509 クライアント認証があります。

SAP BusinessObjects Enterprise サーバの責任

特定の SAP BusinessObjects Enterprise 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。次の表は、これらのサーバと、特定の責任範囲に対して必要な SNC の種類の一覧です。

サーバ	SNC の種類	責任範囲
Web アプリケーションサーバ	クライアント	SAP 認証ロールリスト
	サーバ	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	クライアント	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	サーバ	オンデマンドの Crystal Reports ビュー
Job Server	サーバ	Crystal Reports のスケジュール
Web Intelligence Processing Server	サーバ	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	サーバ	分析

i 注記

Web アプリケーションサーバと CMS はクライアント SNC を使用するため、SNC 名と SAP ユーザ名の明示的なマップが必要です。これは、テーブル USRACL に対してトランザクション SU01 または SM30 で指定します。

8.5.6.2 SAP でのサーバサイドの信頼の設定

SAP BusinessObjects Enterprise 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。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。

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。

8.5.6.2.1 SAP にサーバ側の信頼を設定する

1. SAP マーケットプレイスから、すべての関連プラットフォームで使用する SAP 暗号ライブラリをダウンロードします。

i 注記

Cryptographic Library 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。

2. SAP 内および SAP を実行するマシンの SAP 管理者の認証情報、SAP BusinessObjects Enterprise およびそれを実行するマシンの管理者の認証情報があることを確認します。
3. 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 ツールをコピーします。
4. SAP 暗号ライブラリと共にインストールされる "ticket" という名前のファイルを検索し、Windows の <DRIVE>:\usr\sap\<<SID>>\<instance>\sec\ ディレクトリにコピーします。
5. 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。

i 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。

6. 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。
7. 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。

i 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。

8. 必要に応じて、SAP システムの代わりに次のプロファイル値を入力します。

プロファイル変数	値
ssf/name	SAPSECULIB

プロファイル変数	値
<code>ssf/ssfapi_lib</code>	sapcrypto lib の完全パス
<code>sec/libsapsecu</code>	sapcrypto lib の完全パス
<code>snc/gssapi_lib</code>	sapcrypto lib の完全パス
<code>snc/identity/as</code>	SAP システムの DN

9. SAP インスタンスを再起動します。
10. 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。
11. 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。
12. [OK]をクリックします。
13. 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。

14. 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。

15. 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
<code>snc/accept_insecure_rfc</code>	1
<code>snc/accept_insecure_r3int_rfc</code>	1
<code>snc/accept_insecure_gui</code>	1
<code>snc/accept_insecure_cplic</code>	1
<code>snc/permit_insecure_start</code>	1
<code>snc/data_protection/min</code>	1
<code>snc/data_protection/max</code>	3
<code>snc/enable</code>	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_cplic` 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。

16. SAP システムを再起動します。

サーバ側の信頼のために、SAP BusinessObjects Enterprise を設定する必要があります。

8.5.6.3 SAP BusinessObjects Enterprise でのサーバサイドの信頼の設定

SAP BusinessObjects Enterprise 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. SAP BusinessObjects Enterprise 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。

関連リンク

[環境を設定する](#) [ページ 269]

[PSE を生成する](#) [ページ 270]

[SAP BusinessObjects Enterprise サーバを設定する](#) [ページ 271]

[PSE アクセスを設定する](#) [ページ 271]

[SAP 認証の SNC を設定する](#)。[ページ 272]

[サーバグループの使用](#) [ページ 273]

8.5.6.3.1 環境を設定する

作業を開始する前に、次のことを確認してください。

- SAP 暗号ライブラリがダウンロードされ、SAP BusinessObjects Enterprise 処理サーバが実行されるホスト上に展開されている。
- 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. SAP 暗号ライブラリ (PSE メンテナンスツールを含む) を、SAP BusinessObjects Enterprise を実行中のマシンのフォルダにコピーします。
たとえば、C:\Program Files\SAP\Crypto です。
2. Add the folder to the `<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。

たとえば、C:\Program Files\SAP\Crypto\sapcrypto.dll です。

4. **sec** という名前のサブフォルダを作成します。

たとえば、C:\Program Files\SAP\Crypto\sec です。

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。
6. SAP 暗号ライブラリから **sec** フォルダに **ticket** ファイルをコピーします。

関連リンク

[SAPでのサーバサイドの信頼の設定](#) [ページ 266]

8.5.6.3.2 PSE を生成する

関連する SAP BusinessObjects Enterprise サーバに、SAP に関連付けられた PSE がある場合、SAP は SAP BusinessObjects Enterprise 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 SAP BusinessObjects Enterprise コンポーネント間のこの“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。最初の手順は、証明書を自動生成する SAP BusinessObjects Enterprise の PSE の生成です。

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 -v -p BOE.pse** を実行します。
2. SAP BusinessObjects Enterprise システム用の PIN および識別名を選択します。

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、SNC PSE を開きます。

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. 先ほど作成した **<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. SAP BusinessObjects Enterprise 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. SAP の証明書を SAP BusinessObjects Enterprise の PSE に追加するには、SAP 証明書をダブルクリックします。
8. 変更を STRUST に保存します。
9. **[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。

1 注記

書式は、Base64 のままです。

10. トランザクション SNC0 に移動します。
11. 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、SAP BusinessObjects Enterprise システムを反映します。

- SNC 名は、手順 2 で SAP BusinessObjects Enterprise PSE を作成したときに指定した、先頭に **p:** が付く識別名である必要があります。
- [\[RFC 用エントリ有効化\]](#) 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。

12. エクスポートされた証明書を SAP BusinessObjects Enterprise 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、SAP BusinessObjects Enterprise マシンにインストールされます。SAP BusinessObjects Enterprise サーバで使用され、SAP サーバとして認識される PSE が作成されました。SAP および SAP BusinessObjects Enterprise PSE は証明書を交換しました。SAP は、SAP BusinessObjects Enterprise PSE へのアクセス権があるエンティティが、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。

関連リンク

[SAP BusinessObjects Enterprise サーバを設定する](#) [ページ 271]

8.5.6.3.3 SAP BusinessObjects Enterprise サーバを設定する

SAP BusinessObjects Enterprise の PSE を生成後、SAP 処理用の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。

i 注記

このバージョンの SAP BusinessObjects Enterprise では、サーバは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。

8.5.6.3.4 PSE アクセスを設定する

SAP BusinessObjects Enterprise 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
```

i 注記

PSE PIN の入力を求める画面が表示されます。SAP BusinessObjects Enterprise の SAP 処理サーバと同じ認証情報で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\hareskoug\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
maintain_pk -l
maintain_pk for PSE "C:\Documents and Settings\hareskoug\My Documents\snc\sec
\bojsapproc.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\hareskoug\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。

i 注記

PSE へのアクセスに問題が発生した場合は、-O 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、次のように入力します。

```
sapgenpse seclogin -p SBOE.pse -O <<domain\user>>
```

8.5.6.3.5 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。
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[Secure Network Communication(SNC)の有効化]を選択します。
6. [SNC ライブラリパス] ボックスで、SNC ライブラリ設定のパスを入力します。

i 注記

この手順は、ライブラリが <SNC_LIB> 環境変数ですでに指定されている場合でも必要です。

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。

i 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ます。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。

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 ライブラリによって異なります。SAP 暗号化ライブラリを使用している場合は、LDAP 命名規則に従った識別名にすることをお勧めします。識別名の先頭に前置記号 "p:" を付ける必要があります。

9. Enterprise 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] フィールド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します。

10. SAP システムおよび SAP BusinessObjects Enterprise PSE の DN を指定します。

8.5.6.3.6 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。SAP BusinessObjects Enterprise サーバの詳細説明については、このガイドの「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 SAP BusinessObjects Enterprise 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 レポートまたは Interactive 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 Report または Web Intelligence 処理サーバに追加します。このアプローチでは、SPA 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

サーバグループは次を参照する必要があります。

- SAP コンテンツの処理のみに使用される SIA
- Adaptive Job Server
- Adaptive Processing 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。

8.5.6.4 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.crystal.d.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。

8.5.6.5 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。

関連リンク

[SAP ロールのインポート](#) [ページ 261]

[SAP でのサーバサイドの信頼の設定](#) [ページ 266]

[SAP BusinessObjects Enterprise でのサーバサイドの信頼の設定](#) [ページ 269]

8.5.6.6 CMC で SNC を設定する

SNC を設定する前に、新規の権限認証システムを BI プラットフォームに追加する必要があります。また、SNC ライブラリファイルを既知のディレクトリにコピーし、このファイルを示す環境変数 `<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 [Secure Network Communication(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. [SNC ライブラリパス] に SNC ライブラリ設定のパスを入力します。

i 注記

アプリケーションサーバと CMS は同じ種類のオペレーティングシステム上にインストールされており、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。

i 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 ライブラリによって異なります。SAP 暗号化ライブラリを使用している場合は、LDAP 命名規則に従った識別名にすることをお勧めします。識別名の前に前置記号 `p:` を付ける必要があります。
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。

複数の SNC 名が設定されている場合は、このボックスを空白のままにしてください。
9. [更新] をクリックします。
10. [SAP 認証] ページにある [権限認証システム] タブをクリックします。
[SNC 名] フィールドが [言語] フィールドの下に表示されます。
11. オプションの [SNC 名] フィールドに、SAP BW サーバで設定した SNC 名を入力します。この名前は、BI プラットフォームを信頼するように SAP システムを設定するときに使用した名前と同じにする必要があります。

i 注記

Insight to Action フレームワークを使用してレポート間のインタフェースを有効化している場合は、SNC が有効化されるまで、または SNC の設定が有効になるまでに最大 10 分かかる場合があります。直ちに更新されるようにするには、Insight to Action サービスを実行している Adaptive Processing Server を再起動します。

関連リンク

[SAP 権限認証システムへの接続](#) [ページ 256]

8.5.6.7 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 4 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。

8.5.6.8 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。

i 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。

8.5.7 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 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、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。

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 `jdk/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。

i 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。

8.5.7.1 キーストアファイルを生成する

PKCS12Tool プログラムは、SAP データベースへのシングルサインオン設定に必要な証明書およびキーストアファイルの生成に使用されます。次の表に、サポートされている各プラットフォームにおける PKCS12Tool.jar のデフォルトの場所を示します。

プラットフォーム	デフォルトの場所
Windows	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\java\lib
UNIX	sap_bobj/enterprise_xi40/java/lib

1. コマンドプロンプトを起動して、PKCS12Tool 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をデフォルト設定で生成するには、次のコマンドを実行します。

```
java -jar PKCS12Tool.jar
```

cert.der ファイルおよび keystore.p12 ファイルは同じディレクトリに生成されます。これらのファイルには、次のデフォルト値が含まれています。

パラメータ	デフォルト
-keystore	keystore.p12
-alias	myalias
-storepass	123456
-dname	CN=CA
-validity	365
-cert	cert.der

➡ ヒント

デフォルト値を上書きするには、-? パラメータを使用してこのツールプログラムを実行します。次のメッセージが表示されます。

```
Usage: PKCS12Tool <options>
  -keystore <filename(keystore.p12)>
  -alias <key entry alias(myalias)>
  -storepass <keystore password(123456)>
  -dname <certificate subject DN(CN=CA)>
  -validity <number of days(365)>
  -cert <filename (cert.der)>
  (No certificate is generated when importing a keystore)
```

```
-disablefips
-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。

8.5.7.2 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。

8.5.7.3 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。

i 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。

i 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。

8.5.7.4 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]管理エリアを表示します。
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。
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。

8.5.7.5 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. セキュリティトークンサービスを [利用可能なサービス] 一覧から [サービス] 一覧に移動します。
[追加] ボタンを使用して、選択項目を移動します。
6. [OK] をクリックします。
7. Adaptive Processing Server を再起動します。

8.5.8 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。

8.5.8.1 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	<i>crdb_ods</i>
オープン SQL ドライバ	<i>crdb_opensql</i>
InfoSet ドライバ	<i>crdb_infoset</i>
BW MDX クエリドライバ	<i>crdb_bwmdx</i>

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。

8.5.8.2 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。

<code>crdb_ods</code>	ODS ドライバをアクティブにする
<code>crdb_opensql</code>	オープン SQL ドライバをアクティブにする
<code>crdb_bwmdx</code>	SAP BW MDX クエリドライバをアクティブにする
<code>crdb_infoaset</code>	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。

8.6 PeopleSoft 認証

8.6.1 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。

8.6.2 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。

8.6.2.1 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、[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. [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。

i 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。

8.6.3 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。

8.6.3.1 PeopleSoft 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. [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] リストで、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。

i 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。

i 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. BI プラットフォームと PeopleSoft の間でグループとユーザを強制的に同期させるには、[ユーザ同期の強制] チェックボックスをオンにします。すでにインポートした PeopleSoft グループを BI プラットフォームから削除するには、[ユーザ同期の強制] チェックボックスをオフにします。
7. [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 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. [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。
 - **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。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。

- **新しいユーザを指定ユーザとして作成する**
指定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指定ユーザライセンスを持っている必要があります。
- **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。

8.6.3.2 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、ユーザを指定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指定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指定ユーザとして再マップした場合も同じです。

8.6.3.3 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。

i 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。

8.6.4 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。

i 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。

8.6.4.1 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。
毎月	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。
カレンダー	更新は、すでに作成されているカレンダー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。

i 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、いつでも次のスケジュールされた更新をキャンセルできます。

8.6.5 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。

8.6.5.1 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。

設定をインポートした後のセキュリティ管理の情報については、「セキュリティ設定の管理」を参照してください。

8.6.5.1.1 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。

8.6.5.1.2 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。

i 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

フィールド	説明
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。

i 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。

i 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。

i 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。

i 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。

8.6.5.2 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` ファイル (Windows) または `crpsepmsecuritybridge.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(Windows)または
crpsepmsecuritybridge.sh(unix)myresponsefile.properties 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。

8.6.5.2.1 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。

8.6.5.3 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。

8.6.5.3.1 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。

i 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ます。

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。

i 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。

8.6.5.3.2 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。

8.6.5.4 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。

i 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。

8.6.5.4.1 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

パラメータ	説明
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 [ページ 287]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。
peoplesoft.role.n	<p>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 [ページ 287]を参照してください。</p> <p><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。</p> <div style="background-color: #fff9c4; padding: 10px; margin: 10px 0;"> <p>i 注記</p> <p><n> は、1 を基本とします。</p> </div> <p>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。</p>
mapped.universe.n	<p>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 [ページ 287]を参照してください。</p> <p><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。</p> <div style="background-color: #fff9c4; padding: 10px; margin: 10px 0;"> <p>i 注記</p> <p><n> は、1 を基本とします。</p> </div> <p>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。</p>
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.*	<p>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。</p> <p>log4j.rootLogger=INFO, file, stdout</p> <p>log4j.appender.file=org.apache.log4j.RollingFileAppender</p> <p>log4j.appender.file.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.file.MaxFileSize=5000KB</p> <p>log4j.appender.file.MaxBackupIndex=100</p> <p>log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n</p> <p>log4j.appender.stdout=org.apache.log4j.ConsoleAppender</p> <p>log4j.appender.stdout.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n</p>
peoplesoft classpath	<p>PeopleSoft EPM API .jar ファイルへのクラスパス</p> <p>このパラメータは省略できます。</p>
enterprise.classpath	<p>BI プラットフォーム SDK .jar ファイルへのクラスパス</p> <p>このパラメータは省略できます。</p>
db.driver.type	<p>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。</p> <p>Microsoft SQL Server 2000</p> <p>Oracle Database 10.1</p> <p>DB2 UDB 8.2 Fixpack 7</p> <p>カスタム</p> <p>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。</p> <p>このパラメータは省略できます。</p>
sql.db.class.location sql.db.host sql.db.port	<p>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</p>

パラメータ	説明
sql.db.database	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。
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.drivename 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。

8.7 JD Edwards 認証

8.7.1 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インするユーザを認証することができます。

8.7.2 JD Edwards EnterpriseOne 認証の有効化

BI プラットフォームで JD Edwards EnterpriseOne 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 Enterprise に必要です。

8.7.2.1 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。[オプション]、[サーバ]、[ロール]、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 [JD Edwards EnterpriseOne 認証の有効化] チェックボックスをクリックします。
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. [JD Edwards EnterpriseOne システムユーザ] エリアで、BI プラットフォームが JD Edwards EnterpriseOne 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. [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、環境の名前を入力して、[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。

8.7.3 BI プラットフォームへの JD Edwards EnterpriseOne ロールのマッピング

BI プラットフォームでは、JD Edwards EnterpriseOne ロールをマッピングすることに 1 つのグループが自動的に作成されます。同様に、マッピングされた 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。

8.7.3.1 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]エリアで、[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 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。

 - **新しいユーザを指定ユーザとして作成する**
指定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指定ユーザライセンスを持っている必要があります。
 - **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. [サーバを選択] で、マップするロールを含む JD Edwards サーバを選択します。
9. [インポートされたロール] 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。

8.7.3.2 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、ユーザを指定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指定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指定ユーザとして再マップした場合も同じです。

8.7.3.3 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。

i 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。

8.7.4 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。

i 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。

8.7.4.1 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。
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。
毎月	更新は毎月または数か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
カレンダー	更新は、すでに作成されているカレンダーで指定した日付に実行されます。

- 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、いつでも次のスケジュールされた更新をキャンセルできます。

8.8 Siebel 認証

8.8.1 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。

8.8.1.1 BI プラットフォームで Siebel 認証を有効化する

- 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。
- [管理] 領域で [認証] をクリックします。
- [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。
- [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。
- 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。
- [ドメイン] タブをクリックします。
- [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。
- [接続] で、そのドメインの接続文字列を入力します。
- [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。
- [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。
- [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。
- [更新] をクリックして、変更内容を保存します。

8.8.2 BI プラットフォームへのロールのマッピング

BI プラットフォームでは、Siebel ロールをマッピングするごとに 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、マッピングされた 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働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")で実稼働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インできません。

8.8.2.1 Siebel eBusiness ロールを BI プラットフォームにマッピングする

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. [\[認証\]](#)をクリックします。
3. [\[Siebel eBusiness\]](#) 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 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。
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ピング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、マッピング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。

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。

- **新しいユーザを指定ユーザとして作成する**
指定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指定ユーザライセンスを持っている必要があります。
- **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。

7. **[ロール]** タブをクリックします。

8. 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。

9. **[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。

i 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。

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。

8.8.2.2 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。

i 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、ユーザを指定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指定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指定ユーザとして再マップした場合も同じです。

8.8.2.3 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。

i 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。

8.8.3 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。

i 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。

8.8.3.1 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。
毎月	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。
カレンダー	更新は、すでに作成されているカレンダー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。

i 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、いつでも次のスケジュールされた更新をキャンセルできます。

8.9 Oracle EBS 認証

8.9.1 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。

8.9.1.1 Oracle E-Business Suite 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. [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 環境で使用す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。

関連リンク

[Oracle E-Business Suite ロールをマップする](#) [ページ 306]

8.9.2 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。

8.9.2.1 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。
 - [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 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。
 - [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。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。
 - [新しいユーザを指定ユーザとして作成する](#)
指定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指定ユーザライセンスを持っている必要があります。

- **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. [職責]タブの[更新]をクリックした後に Oracle EBS ユーザアカウント情報を同期する場合は、[ユーザ認証を強制する]を選択します。
9. [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。
10. [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。
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。

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。

8.9.2.1.1 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。

i 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。

8.9.2.1.2 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。
毎月	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。
カレンダー	更新は、すでに作成されているカレンダー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。

i 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。

8.9.3 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。

8.9.3.1 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](#)] または [[ロール](#)] タブをクリックします。
5. [[インポートされたロール](#)] エリアから目的のロールを選択し、[<] または [[削除](#)] をクリックして、ロールを削除します。
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。

i 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。

8.9.4 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。

8.9.4.1 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 Administrator 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]をクリックします。
3. [名前]列で、[Administrators]をクリックします。
4. [グループリスト]をクリックし、[アクション]リストで[追加]をクリックします。

[利用可能なユーザ/グループ]ページが表示されます。

5. [ユーザー一覧]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。
6. [>]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。

i 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 Administrator の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。

8.9.4.2 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/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。割り当てた権限を削除するには、[\[アクセス権の削除\]](#)をクリックします。

8.9.5 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 にアクセスできるよう設定されています。

8.9.5.1 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. SAP Crystal Reports を再起動します。

8.9.5.2 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. [\[SSO コンテキストをデータベースログオンに使用する\]](#) で [\[crdb_oraapps\]](#) 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. SAP Crystal Reports を再起動します。

9 サーバの管理

9.1 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。
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 SAP BusinessObjects Business Intelligence 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。 <ul style="list-style-type: none">• 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• ライフサイクルマネジメントサービス• Analysis サービス• Web Intelligence サービス• Dashboard Design サービス

ナビゲーションツリーのオプション	説明
	<p>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。</p> <div> i 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。 </div>
サーバステータス	<p>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。</p> <ul style="list-style-type: none"> 停止 開始中 初期化中 実行中 停止中 エラー有りで開始 失敗 待機

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。

i 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	<p>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。</p> <ul style="list-style-type: none"> 停止

詳細ウィンドウの列	説明
	<ul style="list-style-type: none"> 開始中 初期化中 実行中 停止中 エラー有りで開始 失敗 待機
有効	サーバが有効かどうかを表示します。
古い	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。
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。

関連リンク

[サーバグループの管理](#) [ページ 328]

[ノードの使用](#) [ページ 345]

[サーバのステータスの表示](#) [ページ 316]

[サーバの開始、停止、再起動](#) [ページ 317]

[サーバのプロパティを変更する](#) [ページ 335]

9.2 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。

関連リンク

[ccm.exe](#) [ページ 742]

9.3 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。

関連リンク

[ccm.sh\[ccm.sh\]](#) [ページ 735]

9.4 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。

関連リンク

[ライセンス情報を表示する](#) [ページ 76]

[ライセンスキーを追加する](#) [ページ 76]

[現在のアカウントの利用状況を表示する](#) [ページ 77]

9.4.1 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。

関連リンク

[ライセンスキーの管理](#) [ページ 76]

[ライセンスキーを追加する](#) [ページ 76]

[現在のアカウントの利用状況を表示する](#) [ページ 77]

9.4.2 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。

i 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。

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。

関連リンク

[ライセンス情報を表示する](#) [ページ 76]

[現在のアカウントの利用状況を表示する](#) [ページ 77]

9.4.3 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。

関連リンク

[ライセンスキーの管理](#) [ページ 76]

[ライセンスキーを追加する](#) [ページ 76]

[ライセンス情報を表示する](#) [ページ 76]

9.5 サーバのステータスの表示および変更

9.5.1 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。SAP BusinessObjects Business Intelligence プラットフォーム要求に応答するには、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、SAP BusinessObjects Business Intelligence 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。

関連リンク

[サーバのステータスを表示する](#) [ページ 317]

[サーバの開始、停止、再起動](#) [ページ 317]

[サーバの有効化/無効化](#) [ページ 320]

[Central Management Server の停止](#) [ページ 319]

9.5.1.1 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。

i 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。

9.5.2 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	SAP BusinessObjects Business Intelligence 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

操作	説明
	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。

関連リンク

[サーバの有効化/無効化](#) [ページ 320]

9.5.2.1 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。

i 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、実行する必要が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。

関連リンク

9.5.2.2 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 にログインします。
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。

9.5.2.3 サーバを自動的に起動する

既定では、Server Intelligence Agent (SIA) 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。この手順では、このオプションを設定する場所を説明します。

1. CMC の [\[サーバ\]](#) 管理エリアで、自動的に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。
2. [\[共通設定\]](#) 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。

i 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。[\[起動\]](#) タブで、[\[自動開始\]](#) を [\[はい\]](#) に設定し、[\[保存\]](#) 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。

9.5.3 Central Management Server の停止

SAP BusinessObjects Business Intelligence 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、Business Intelligence 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、Business Intelligence 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 Business Intelligence 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。

i 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。[起動] タブで、[自動開始] を [はい] に設定し、[保存] 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。

関連リンク

[ノードの使用](#) [ページ 345]

[サーバのクローン](#) [ページ 322]

[Central Management Server のクラスタ化](#) [ページ 324]

9.5.4 サーバの有効化/無効化

SAP BusinessObjects Business Intelligence プラットフォームサーバを無効にすると、新しい SAP BusinessObjects Business Intelligence プラットフォーム要求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。

i 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。

i 注記

CMS を有効または無効にすることはできません。

9.5.4.1 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、実行する必要が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。

9.5.4.2 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、SAP BusinessObjects Business Intelligence 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 にログインします。
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。



9.6 サーバの追加、クローン、または削除

9.6.1 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、SAP BusinessObjects Business Intelligence 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、製品と共に提供される SAP BusinessObjects Business Intelligence 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 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。

9.6.1.1 サーバの追加

1つのマシン上で、同一の SAP BusinessObjects Business Intelligence 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. SAP BusinessObjects Business Intelligence 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>> です。<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 SAP BusinessObjects Business Intelligence 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。

関連リンク

[サービスおよびサーバ](#) [ページ 21]

[サーバの設定](#) [ページ 334]

[ポート番号の設定](#) [ページ 343]

[サーバのステータスの表示](#) [ページ 316]

9.6.1.2 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、元のサーバの構成設定が保持されます。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、元の CMS の構成設定のすべてが維持されます。

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。たとえば、同じマシンに CMS をクローンしている場合、ポート番号の設定を変更して、それが元の CMS からクローン先の CMS にコピーされたことを確認します。

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 SAP BusinessObjects Business Intelligence プラットフォーム (および必要に応じたパッチ) 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。

9.6.1.2.1 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変更できます。

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 SAP BusinessObjects Enterprise 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)、SAP BusinessObjects Enterprise 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書きしない限り、Event Server は失敗します。

9.6.1.2.2 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。

i 注記

ポート番号の設定もクローンされます。CMS のクローンなど、多くの場合、ポート番号を変更して元のサーバとそのクローン間でポートの競合が生じないようにします。

9.6.1.3 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。

9.7 Central Management Server のクラスタ化

9.7.1 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 Business Intelligence 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 Business Intelligence 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、すでに実際に稼働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、製品出荷マトリクスに記載されている、データベースサーバ、データベースアクセス方法、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 (バージョンレベルとパッチレベルを含む) を満たすオペレーティングシステムに、各 CMS をインストールしていることを確認してください。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、Business Intelligence 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 Business Intelligence 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。
 - ネイティブドライバと ODBC ドライバのどちらのドライバを使用している場合でも、各 CMS が同じ方法で CMS システムデータベースに接続していることを確認します。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。
- 監査を有効にする場合は、使用する監査データベースおよび監査データベースへの接続方法をすべての CMS で一致させる必要があります。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。

関連リンク

[CMS クラスタの名前変更](#) [ページ 327]

9.7.1.1 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。

i 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。

関連リンク

[クラスタへの新しいノードの追加](#) [ページ 326]

[サーバの追加](#) [ページ 321]

[サーバのクローン](#) [ページ 322]

[システムのバックアップと復元](#) [ページ 414]

9.7.1.2 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できます。新しい CMS クラスターメンバーをインストールするマシンで、SAP BusinessObjects Business Intelligence 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。このインストールで、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。

i 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。

関連リンク

[ノードの使用](#) [ページ 345]

9.7.1.3 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

デプロイメントに追加の CMS を加え、Java アプリケーションサーバを使用している場合は、Web アプリケーションデプロイメントの `\webapps\BOE\WEB-INF\config\custom` ディレクトリにある `PlatformServices.properties` ファイルを変更する必要があります。

9.7.1.3.1 BOE Web アプリケーションのクラスタプロパティを定義する

1. 次に示す、Web アプリケーションをホストするコンピュータの 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 Business Intelligence platform 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. 新しいファイルを作成します。
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. デプロイメントの各クラスタに対して、CMS クラスタのプロパティを指定します。

各クラスタ名の先頭に @ 記号を置き、それぞれの CMS 名をカンマ (,) で区切ります。ポート番号と CMS 名は、コロン (:) で区切られます。指定しない場合は、ポート番号は 6400 と見なされます。

cms.clusters プロパティを使用して、デプロイメント内の各クラスタを指定します。たとえば、
cms.clusters=@samplecluster,@samplecluster2, @samplecluster3 のようになります。
cms.clusters.<[cluster name]> プロパティを使用して、クラスタの各 CMS を指定します。次はその例です。

```
cms.clusters=@samplecluster,@samplecluster2, @samplecluster3  
cms.clusters.samplecluster=cmstwo:6400,cmstwo  
cms.clusters.samplecluster2=cms3,cms4, cms5  
cms.clusters.samplecluster3=aps05
```

4. PlatformServices.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。

9.7.1.4 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。

i 注記

経験豊富な SAP Business Objects Business Intelligence 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。

9.7.1.4.1 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。

9.7.1.4.2 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、SAP BusinessObjects Business Intelligence プラットフォーム管理者ガイドの UNIX ツールに関する章を参照してください。

9.8 サーバグループの管理

サーバグループを使用すると、SAP BusinessObjects Business Intelligence プラットフォームサーバをグループに編成して、管理しやすくなることができます。つまり、サーバをグループ単位で管理すると、システムにあるすべてのサーバのサブセットのみを確認すればよいことになります。さらに重要なことは、サーバグループを使用して SAP BusinessObjects Business Intelligence プラットフォームをカスタマイズすることで、異なる場所にいるユーザやさまざまなタイプのオブジェクトに対してシステムを最適化させることができます。

地域別にサーバをグループ化すると、特定地域のユーザに適したデフォルトの処理設定や定期スケジュール、出力先などを簡単に設定できます。オブジェクトが常に同じサーバで処理されるよう、オブジェクト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に送信されるよう、特定のサーバグループに関連付けることもできます。したがって、複数の場所、複数のタイムゾーンにまたがるシステムの保守を行う際にサーバグループを使用すると、非常に便利です。

サーバをタイプごとにグループ化すると、オブジェクトに最適化されたサーバによって処理されるオブジェクトを構成することができます。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。したがって、DB2 データベースに対して実行されたレポートが沢山あるような場合は、DB2 データベースサーバに対するレポートだけを処理する Processing Server のグループを作成します。該当するレポートを設定して、レポート表示に Processing Server を常に使用するようにすれば、レポート表示のシステムパフォーマンスを改善することができます。

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、および変更特定のサーバグループを使用するように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ウィンドウに表示され、[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。

9.8.1 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。

9.8.1.1 サーバグループを作成する

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。| + |

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、サーバマトリクスの表示、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。

関連リンク

[サーバのステータスの表示](#) [ページ 316]

9.8.2 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。

9.8.2.1 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。

9.8.2.2 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。
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。

9.8.3 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。

9.8.3.1 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、このサーバに追加した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。
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。

9.8.4 サーバおよびサーバグループへのユーザアクセス権

アクセス権を使用して、サーバおよびサーバグループへのアクセスを人々に許可し、彼らがサーバの起動や停止などのタスクを実行できるようにします。

システム構成およびセキュリティ上の懸念に応じて、サーバ管理を SAP BusinessObjects Business Intelligence プラットフォームの管理者だけに制限することができます。しかし、これらのサーバを使用する管理者以外の人々にもアクセスを認める必要がある場合があります。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アクセス権を付与する必要があります。SAP BusinessObjects Business Intelligence プラットフォームサーバの管理タスクをほかの担当者委任することもできます。また、組織内のさまざまなグループに、そのグループのサーバを管理させることもできます。

9.8.4.1 サーバまたはサーバグループに対するアクセス権を付与する

1. CMC の [\[サーバ\]](#) 管理エリアを表示します。
2. 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、選択したサーバまたはサーバグループへの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。
[\[主体の追加\]](#) ダイアログボックスが表示されます。
4. 指定のサーバまたはサーバグループへの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に必要なセキュリティ設定を選択し、[\[OK\]](#) をクリックします。
権限の割り当ての詳細については、「[アクセス権の設定](#)」に関する章を参照してください。

9.8.4.2 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する必要があります。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

新しいレポートを SAP BusinessObjects Business Intelligence プラットフォームに保存するには、ユーザには少なくとも 1 つのフォルダにオブジェクトを追加する権限も必要です。

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。

アドバンスド 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。

9.9 システムのパフォーマンスの評価

9.9.1 SAP BusinessObjects Business Intelligence プラットフォームサーバのモニタリング

モニタリングアプリケーションは、レポーティングと通知について、SAP BusinessObjects Business Intelligence 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。

関連リンク

[モニタリングについて](#) [ページ 534]

9.9.2 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。

i 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。

9.9.2.1 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。

関連リンク

[サーバのプロパティを変更する](#) [ページ 335]

[サーバのメトリクスに関する付録について](#) [ページ 816]

9.9.3 システムメトリクスの表示

CMC の [設定] 管理エリアには、SAP BusinessObjects Business Intelligence 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。

9.9.3.1 システムメトリクスを表示する

CMC の [設定] 管理エリアで矢印をクリックして、[プロパティ]、[グローバルシステムメトリクスの表示]、および [クラスタ] と [ホットバックアップ] のエリアの設定を展開、表示します。

9.9.4 サーバの利用状況の記録

SAP BusinessObjects Business Intelligence プラットフォームでは SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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 Business Objects 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。

i 注記

SAP BusinessObjects Business Intelligence 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。

9.10 サーバの設定

この節では、SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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があります。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。

i 注記

この節では、SAP BusinessObjects Business Intelligence 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。

関連リンク

[ポート番号の設定](#) [ページ 343]

[サーバのプロパティを変更する](#) [ページ 335]

[CMS システムデータベースの再作成](#) [ページ 378]

[新規または既存の CMS データベースの選択](#) [ページ 377]

9.10.1 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。

i 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。

9.10.2 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. サービスに変更を行い、[OK] をクリックします。

i 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。

9.10.3 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。

SAP BusinessObjects Business Intelligence プラットフォームサービスの各タイプには、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。

関連リンク

[設定テンプレートを設定する](#) [ページ 336]

[設定テンプレートをサーバに適用する](#) [ページ 336]

9.10.3.1 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す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。

i 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。

関連リンク

[設定テンプレートをサーバに適用する](#) [ページ 336]

9.10.3.2 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。

i 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。

i 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。

関連リンク

[設定テンプレートを設定する](#) [ページ 336]

9.10.3.3 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。

9.11 サーバネットワークの設定

SAP BusinessObjects Business Intelligence プラットフォームサーバのネットワーク設定は、CMC で管理されます。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 SAP BusinessObjects Business

Intelligence プラットフォームサーバは、使用可能なポートに動的にバインドします。ポート番号は SAP BusinessObjects Business Intelligence プラットフォームによって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。

9.11.1 ネットワーク環境オプション

SAP BusinessObjects Business Intelligence プラットフォームは、Internet Protocol 6 (IPv6) と Internet Protocol バージョン 4 (IPv4) の両方のネットワークトラフィックをサポートしています。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 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 IPv6 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。

i 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。SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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。

9.11.1.1 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。

- SAP BusinessObjects Business Intelligence 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、IPv6 専用ノード、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 専用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。

i 注記

IPv6 専用ノードを Windows 2003 で使用する場合、DNS 名は正しく解決されません。IPv4 スタックを Windows 2003 で無効にする場合は、デプロイメントを IPv6 と IPv4 の両方で実行することをお勧めします。

9.11.2 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 SAP BusinessObjects Business Intelligence 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	<p>これはすべてのサーバのデフォルト設定です。[自動割り当て]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。</p> <div><p>i 注記</p><p>[ホスト名] 設定の [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。</p></div>
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、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] を指定している場合、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ていることを確認してください。また、CMC で CMS の [ホスト名] 設定も指定する必要があります。

i 注記

マルチホームマシンまたは特定の NAT ファイアウォール環境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しなければならない場合があります。

関連リンク

[ファイアウォール用にシステムを設定する \[ページ 158\]](#)

[マルチホームマシンの設定 \[ページ 340\]](#)

[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 \[ページ 342\]](#)

9.11.2.1 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。 <div><p>i 注記</p><p>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。</p></div>

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。

9.11.3 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、先頭のネットワークインタフェースが SAP BusinessObjects Business Intelligence 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 [ホスト名] オプションを使用して、Business Intelligence (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。[ホスト名] の値の設定については、「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。

関連リンク

[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](#) [ページ 342]

9.11.3.1 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

i 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。

i 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。

i 注記

デフォルトのポート番号は 6400 です。

9.11.3.2 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 SAP BusinessObjects Business Intelligence プラットフォームサーバは、デフォルトでそれぞれのポートを動的に選択します。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。

関連リンク

[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](#) [ページ 345]

9.11.3.3 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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]フィールドに次のいずれかを入力します。
 - ターゲットネットワークインタフェースのホスト名とポート番号(<ホスト名>:<ポート番号>の形式)
 - ターゲットネットワークインタフェースの IP アドレスとポート番号(<IP アドレス>:<ポート番号>の形式)
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 NIC にバインドするには、[ポート]フィールドに次のいずれかを入力します。
 - ターゲットネットワークインタフェースのホスト名とポート番号(<ホスト名>:<ポート番号>の形式)
 - ターゲットネットワークインタフェースの IP アドレスとポート番号(<IP アドレス>:<ポート番号>の形式)
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。

i 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。

9.11.4 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 Business Objects 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 (1025 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対して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 SAP BusinessObjects Business Intelligence 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。

9.11.4.1 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` スクリプトを使用して、ポート番号を変更する必要があります。

i 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。

9.11.4.2 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]フィールドに次のいずれかを入力します。
 - ポート番号
 - ホスト名およびポート番号 (<ホスト名>:<ポート番号>の形式)
 - IP アドレスとポート番号 (<IP アドレス>:<ポート番号>の形式)
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。

9.11.4.3 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 ポート番号を変更する必要があります。

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. [4 - ローカル CMS の変更]を選択し、Enter キーを押します。
ノードで現在ホストされている 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。

9.11.4.4 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

i 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 SAP BusinessObjects Business Intelligence プラットフォームリクエストの受信待機を開始します。

9.12 ノードの管理

9.12.1 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、SAP BusinessObjects Business Intelligence 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。

i 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は、[[SSL を有効にする](#)]チェックボックスをオフにすることによって SSL を無効にしてからノード管理手順を実行する必要があります。詳細については、このガイドの「CCM で SSL プロトコルを設定する」を参照してください。

警告

BI プラットフォームでは、ODBC データソースとして SQL Anywhere データベースがサポートされています。UNIX マシンで SQL Anywhere を使用してノード管理操作を実行する前に、`odbc.ini` ファイルを作成してソースとして指定する必要があります。

関連リンク

[SQL Anywhere 用に Unix マシンを準備する](#) [ページ 346]

[CCM で SSL プロトコルを設定する](#) [ページ 145]

9.12.1.1 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 では、 <code>C:\Program Files (x86)\SAP BusinessObjects</code> です。
<<SCRIPTDIR>>	ノード管理スクリプトが配置されるディレクトリ。 <ul style="list-style-type: none">Windows では、<<INSTALLDIR>>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts です。Unix の場合: <<INSTALLDIR>>/sap_bobj/enterprise_xi40/<<PLATFORM64>>/scripts です。
<<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。 <ul style="list-style-type: none"><code>aix_rs6000</code><code>linux_x86</code><code>solaris_sparc</code><code>win32_x86</code>
<<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。 <ul style="list-style-type: none"><code>aix_rs6000_64</code><code>linux_x64</code><code>solaris_sparcv9</code><code>win64_x64</code>

9.12.1.2 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。

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)、ユーザ名、パスワード、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. ノード管理操作を実行するマシンで、odbc.ini および SQL Anywhere データベースのクライアント環境をソースに指定します。

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=tcipip(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/aurora41_pi_bip_37/sap_bobj/enterprise_xi40/linux_x64/
odbc.ini;export ODBCINI
```

関連リンク

[変数](#) [ページ 346]

9.12.2 新しいノードの追加

インストールプログラムにより、SAP BusinessObjects Business Intelligence プラットフォーム Error in tm type. の初回インストール時に単一ノードが作成されます。

異なるユーザアカウントでサーバを実行する場合、追加ノードが必要になる可能性があります。

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

ノードを追加するマシンで、CCM またはノード管理スクリプトを使用します。リモートマシンではノードを追加できません。

BI プラットフォームインストールは、マシンでインストーラによって作成される 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、単一クラスタ内のみで使用できます。同じ BI プラットフォームインストールを共有す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には、パッチまたはアップデートを適用できないためです。Unix プラットフォームのみが、同じマシンでのソフトウェアの複数インストールをサポートしま

す。各インストールが独自のユーザアカウントで実行され、インストール間でファイルが共有されないよう、異なるフォルダにインストールされる必要があります。

クラスタに含まれるすべてのマシンのバージョンおよびパッチレベルが同じである必要があることに注意してください。

9.12.2.1 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 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。

9.12.2.2 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 と一時 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。

9.12.2.2.1 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」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、-connect 文字列では、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。

```
<<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
  -noservers
  -createsms
```

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。

関連リンク

[変数](#) [ページ 346]

[ノードを追加、再登録、削除するスクリプトパラメータ](#) [ページ 362]

9.12.2.3 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。

9.12.2.3.1 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
```

関連リンク

[変数 \[ページ 346\]](#)

[ノードを追加、再登録、削除するスクリプトパラメータ \[ページ 362\]](#)

9.12.3 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。

➔ 注意

ノードがあるマシンでのみノードを再作成できます。

9.12.3.1 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 と一時 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。

9.12.3.1.1 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、-connect 文字列では、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。

```
<<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
```

i 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。

関連リンク

[変数 \[ページ 346\]](#)

[ノードを追加、再登録、削除するスクリプトパラメータ \[ページ 362\]](#)

9.12.3.2 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。

i 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。

9.12.3.2.1 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
```

関連リンク

[変数 \[ページ 346\]](#)

[ノードを追加、再登録、削除するスクリプトパラメータ \[ページ 362\]](#)

9.12.4 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。

関連リンク

[ノードの再作成](#) [ページ 351]

9.12.4.1 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ら、ホスト名、ポート番号、および CMS の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。

9.12.4.1.1 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
```

関連リンク

[変数](#) [ページ 346]

[ノードを追加、再登録、削除するスクリプトパラメータ](#) [ページ 362]

9.12.4.2 Unix 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. `<<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 - Delete node] 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ら、ホスト名、ポート番号、および CMS の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。

9.12.4.2.1 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
```

関連リンク

[変数](#) [ページ 346]

[ノードを追加、再登録、削除するスクリプトパラメータ](#) [ページ 362]

9.12.5 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。

関連リンク

[新しいノードの追加](#) [ページ 347]

[サーバのクローン](#) [ページ 322]

[ノードの削除](#) [ページ 354]

9.12.5.1 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。

i 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。

関連リンク

[新しいノードの追加](#) [ページ 347]

[サーバのクローン](#) [ページ 322]

[ノードの削除](#) [ページ 354]

9.12.5.2 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。

関連リンク

[新しいノードの追加](#) [ページ 347]

[サーバのクローン](#) [ページ 322]

[ノードの削除](#) [ページ 354]

9.12.6 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。
- 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、実稼働クラスタにもインストールされていることを確認します。
- 新しいマシンを実稼働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きたいときは、SAP BusinessObjects Business Intelligence 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、ノードを実稼働クラスタに移動します。

注意

ノードがあるマシンでのみノードを移動できます。

9.12.6.1 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インストールであったソースシステムコンピュータ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、ソースクラスタおよび出力先クラスタ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、および出力先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的 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。

⚠ 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。

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。

9.12.6.1.1 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、-connect 文字列では、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。

```
<<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
```

i 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。

関連リンク

[変数](#) [ページ 346]

[ノードを移動するためのスクリプトパラメータ](#) [ページ 364]

9.12.6.2 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クラスタに含まれていたソースシステムコンピュータ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、および出力先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、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、およびソース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。

9.12.6.2.1 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
```

関連リンク

[変数 \[ページ 346\]](#)

[ノードを移動するためのスクリプトパラメータ \[ページ 364\]](#)

9.12.7 スクリプトパラメータ

9.12.7.1 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。	<code>-adopt</code>
-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。	<code>-cms mycms:6409</code>
-cmsport	<ul style="list-style-type: none">一時 CMS を起動時の CMS のポート番号。  制約 -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。  制約 -dbdriver、-connect、および -dbkey パラメータも使用する必要があります。	<code>-cmsport 6401</code>
-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。	<code>-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"</code>

パラメータ	説明	例
-dbdriver	<p>CMS のデータベースドライバ。</p> <p>設定可能な値は次のとおり。</p> <ul style="list-style-type: none"> • <code>db2databasesubsystem</code> • <code>maxdbdatabasesubsystem</code> • <code>mysqldatabasesubsystem</code> • <code>oracledatabasesubsystem</code> • <code>sqlanywheredatabasesubsystem</code> • <code>sqlserverdatabasesubsystem</code> • <code>sybasedatabasesubsystem</code> 	<code>-dbdriver mysqldatabasesubsystem</code>
-dbkey	クラスタキー	<code>-dbkey abc1234</code>
-name	ノード名。	<code>-name mynode2</code>
-noservers	<p>サーバを含まないノードを作成します。</p> <div> <p>i 注記</p> <p>追加 <code>-createcms</code> 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。</p> </div>	<code>-noservers</code>
-password	管理者アカウントのパスワード。	<code>-password Password1</code>
-siaport	ノードの Server Intelligence Agent のポート番号。	<code>-siaport 6409</code>
-username	管理者アカウントのユーザ名。	<code>-username Administrator</code>
-usetempcms	<div> <p>⚠ 警告</p> <p><code>-cms</code> 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。</p> <p>一時 CMS を起動して使用します。</p> </div> <div> <p>i 注記</p> <p>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。</p> </div>	<code>-usetempcms</code>

関連リンク

[スクリプトを使用した Windows 上でのノードの追加 \[ページ 349\]](#)

[スクリプトを使用した Unix 上でのノードの追加 \[ページ 350\]](#)

[スクリプトを使用した Windows 上でのノードの再作成 \[ページ 352\]](#)

スクリプトを使用した *Unix* 上でのノードの再作成 [ページ 354]

スクリプトを使用した *Windows* 上でのノードの削除 [ページ 355]

スクリプトを使用した *Unix* 上でのノードの削除 [ページ 356]

9.12.7.2 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	<p>ソース Central Management Server (CMS) の名称。</p> <div> 警告</div> <p>-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。</p> <div> 注記</div> <p>CMS をデフォルト 6400 ポートで実行中ではない場合は、ポート番号を指定する必要があります。</p>	<pre>-cms sourceMachine:6409</pre>
-cmsport	<ul style="list-style-type: none">一時 CMS を起動時の CMS のポート番号。 <div> 制約</div> <p>-usetempcms、-dbdriver、-connect、および -dbkey パラメータも使用する必要があります。</p> <ul style="list-style-type: none">新しい CMS 作成時の CMS のポート番号。 <div> 制約</div> <p>-dbdriver、-connect、および -dbkey パラメータも使用する必要があります。</p>	<pre>-cmsport 6401</pre>
-connect	<p>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。</p>	<pre>-connect "DSN=Source BOEXI40;UID=username;PWD=password ;HOSTNAME=database;PORT=3306"</pre>

パラメータ	説明	例
	<p>i 注記</p> <p>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。</p>	
-dbdriver	<p>ソース CMS のデータベースドライバ。</p> <p>設定可能な値は次のとおり。</p> <ul style="list-style-type: none"> • <code>db2databasesubsystem</code> • <code>maxdbdatabasesubsystem</code> • <code>mysqldatabasesubsystem</code> • <code>newdbdatabasesubsystem</code> • <code>oracledatabasesubsystem</code> • <code>sqlanywheredatabasesubsystem</code> • <code>sqlserverdatabasesubsystem</code> • <code>sybasedatabasesubsystem</code> <p>i 注記</p> <p>sqlserverdatabase は Unix ではサポートされていません。</p>	<code>-dbdriver mysqldatabasesubsystem</code>
-dbkey	ソースクラスタキー。	<code>-dbkey abc1234</code>
-destcms	<p>出力先 CMS の名称。</p> <p>i 注記</p> <p>CMS をデフォルト 6400 ポートで実行中ではない場合は、ポート番号を指定する必要があります。</p>	<code>-destcms destinationMachine:6401</code>
-destconnect	<p>出力先 CMS システムデータベースの接続文字列。</p> <p>i 注記</p> <p>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。</p>	<code>-destconnect "DSN=Destin BOEXI40;UID=username;PWD=password ;HOSTNAME=database;PORT=3306"</code>
-destdbdriver	出力先 CMS のデータベースドライバ。	<code>-destdbdriver sybasedatabasesubsystem</code>

パラメータ	説明	例
	<p>設定可能な値は次のとおり。</p> <ul style="list-style-type: none"> • <code>db2databasesubsystem</code> • <code>maxdbdatabasesubsystem</code> • <code>mysqldatabasesubsystem</code> • <code>newdbdatabasesubsystem</code> • <code>oracledatabasesubsystem</code> • <code>sqlanywheredatabasesubsystem</code> • <code>sqlserverdatabasesubsystem</code> • <code>sybasedatabasesubsystem</code> <p>i 注記</p> <p>sqlserverdatabase は Unix ではサポートされていません。</p>	
<code>-destdbkey</code>	出力先クラスタキー。	<code>-destdbkey def5678</code>
<code>-destpassword</code>	出力先 CMS の管理者アカウントのパスワード。	<code>-destpassword Password2</code>
<code>-destusername</code>	出力先 CMS の管理者アカウントのユーザ名。	<code>-destusername Administrator</code>
<code>-password</code>	ソース CMS の管理者アカウントのパスワード。	<code>-password Password1</code>
<code>-username</code>	ソース CMS の管理者アカウントのユーザ名。	<code>-username Administrator</code>
<code>-usetempcms</code>	<p>⚠ 警告</p> <p><code>-cms</code> 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。</p> <p>一時 CMS を起動して使用します。</p> <p>i 注記</p> <p>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。</p>	<code>-usetempcms</code>

関連リンク

[スクリプトを使用した Windows 上でのノードの移動 \[ページ 359\]](#)

[スクリプトを使用した Unix 上でのノードの移動 \[ページ 361\]](#)

9.12.8 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。

9.12.8.1 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。

9.12.9 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。

制約

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 SAP BusinessObjects Business Intelligence 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。

9.12.9.1 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。

9.13 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

9.13.1 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

9.13.1.1 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 SBOP 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。	<ul style="list-style-type: none">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。

9.13.1.2 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。

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、CMC の [アプリケーション] タブで [処理設定] を選択します。
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の URL を使用している。	
OpenDocument を使用している。	

代替ガイドライン

i 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。

表 14: 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、サーバは再起動しません。
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 にログインして、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。

表 15: 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。

条件	アクション
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。

関連リンク

[新規または既存の CMS データベースの選択](#) [ページ 377]

9.13.1.3 マシンの名前変更

SAP BusinessObjects Business Intelligence 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。

9.13.1.3.1 サーバ層

i 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。	<p>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 6 では、作成した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 に格納されます。</p> <div> <p>i 注記</p> <p>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。</p> </div>
名前を変更したマシンが CMS をホストし、SAP BusinessObjects Explorer がクラスタのいずれかのマシンにインストールされている。	<p>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で、default.settings.properties ファイルに含まれる default.cms.name プロパティの、古い CMS ホスト名を新しいホスト名に置き換えます。デフォルトでは、Tomcat 6 では default.settings.properties ファイルが <<INSTALLDIR>>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\explorer\WEB-INF\classes\ に格納されます。</p> <div> <p>➡ 注意</p> <p>アクション実行後、Explorer 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。</p> </div>
Explorer で SSO を使用している。	cms の値を jsp-sso-provider.jsp で更新し、sso.global.cms および sso.trusted.auth.x509.cms の値を sso.properties で新しい CMS ホスト名に更新します。
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。
<p>デプロイメントが次の条件をすべて満たしている。</p> <ul style="list-style-type: none"> 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。

関連リンク

[Recreating a node](#) [ページ 351]

9.13.1.3.2 Web 層

SAP BusinessObjects 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 サービススペースの 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 サービススペースのすべての BI プラットフォームクライアントを再設定します。

9.13.1.3.3 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 <code>localhost</code> 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、他のタイプの接続を使用している。	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。
監査データベースをホストするマシンの名前を変更し、他のタイプの接続を使用している。	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。

9.13.1.3.4 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。

9.14 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

SAP BusinessObjects Business Intelligence 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 Business Intelligence (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コンピュータの各バージョンに対して、別々に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_VAR32>>` は、32 ビットプロセスで使用する値です。
- `BOE_USE_32BIT_ENV_FOR=<<FIRST_ENV_VAR>>,<<SECOND_ENV_VAR>>`

たとえば、AIX コンピュータに 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>>`
- `ORACLE_HOME32=<<32 ビットバージョン>>`
- `LIBPATH=<<64 ビットバージョン>>`
- `LIBPATH32=<<32 ビットバージョン>>`
- `BOE_USE_32BIT_ENV_FOR=ORACLE_HOME,LIBPATH`

i 注記

Linux および Solaris では、32 ビットと 64 ビットパスを区切るのに `BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH` を使用しないでください。代わりに、32 ビットおよび 64 ビットパス両方を `LD_LIBRARY_PATH` に追加してください。

9.15 サーバおよびノードのプレースホルダの管理

9.15.1 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。

[\[プレースホルダ\]](#) ダイアログボックスに、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。

関連リンク

[サーバとノードプレースホルダ](#) [ページ 835]

9.15.2 ノードのプレースホルダを表示および編集する

i 注記

すべてのプレースホルダの設定を編集できるわけではありません。たとえば、`%INSTALLROOTDIR%` は自動入力されるため、読み取り専用です。

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. 必要に応じてプレースホルダの設定を編集し、[\[OK\]](#) をクリックします。

関連リンク

[サーバとノードプレースホルダ](#) [ページ 835]

10 Central Management Server (CMS) データベースの管理

10.1 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。SAP BusinessObjects Business Intelligence 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。

関連リンク

[サーバのプロパティを変更する](#) [ページ 335]

10.1.1 SQL Anywhere を CMS データベースとして選択する

初期インストール時に、BI プラットフォームでは、さまざまなデータベースの選択がサポートされます。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. セントラル設定マネージャを開始します。
 - Unix では、`./cmsdbsetup.sh` を実行します。
 - Windows では、CCM を開始します。
2. 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、「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。
3. 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、「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。
4. 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)。

関連リンク

[CMS データベース間でのデータのコピー](#) [ページ 380]

[新規または既存の CMS データベースの選択](#) [ページ 377]

10.1.2 SAP HANA を CMS データベースとして選択する

初期インストール時に、BI プラットフォームでは、さまざまなデータベースの選択がサポートされます。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. HANA クライアントをインストールします。
3. 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]
SERVERNODE=<HANA Server IP address>:<HANA server port #>
```

<New_DB_version> は HANA のバージョン (例、“NewDB 1.0”)、<HANA Server IP address> は HANA サーバの IP アドレス、および <HANA server port #> は HANA サーバのポート番号です。

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
```

- Windows では、HANA への ODBC 接続を作成します。
4. 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、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、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、HANA ODBC 接続をテストできます。
5. Unix では、HANA インストールディレクトリから <<INSTALLDIR>>/sap_bobj/enterprise_xi40/<<PLATFORM>> に、libodbcHDB.so をコピーします。
 6. セントラル設定マネージャを開始します。
 - Unix では、./cmsdbsetup.sh を実行します。
 - Windows では、CCM を開始します。
 7. HANA 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、「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。
 8. 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 HANA データベースに更新します。詳細については、「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。
 9. 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)。

関連リンク

[CMS データベース間でのデータのコピー](#) [ページ 380]

[新規または既存の CMS データベースの選択](#) [ページ 377]

10.2 新規または既存の CMS データベースの選択

CCMを使用して、CMSを含むノードの新規または既存の 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。
- SAP BusinessObjects Business Intelligence 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)。

i 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。

i 注記

システムコピーワークフローを実行している場合を除き、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 BI プラットフォーム `Error in tm type` を設定しないでください。

BI プラットフォーム `Error in tm type` インストールと CMS データベースのバージョンおよびパッチレベル、インストールパス、インストールされたコンポーネントなどが異なる場合、システムが破損する可能性があります。

破損を防ぐため、BI プラットフォーム `Error in tm type` デプロイメントを別の BI プラットフォーム `Error in tm type` システムの CMS データベース (特にバージョンおよびパッチレベルが異なる CMS データベース) にポイントして、BI コンテンツのシステム間移行を行わないでください。

10.2.1 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、ツールバーの [\[CMS データソースの指定\]](#) をクリックします。
3. [\[データソース設定の更新\]](#) を選択します。
4. 残りの手順は、選択した接続の種類によって異なります。

- ODBC を選択した場合は、[データソースの選択] ダイアログボックスで、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、[OK] 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とクラスタキーを入力して [OK] をクリックします。

➡ ヒント

新しい DSN を設定する場合は、[新規] 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、指示に従って、データベースのサーバ名、ログイン ID、パスワード、およびクラスタキーを入力し、[OK] をクリックします。
5. クラスタキーを入力します。
CCM により、CMS データベースセットアップの完了が通知されます。
 6. [プロパティ] ダイアログボックスで、[OK] をクリックします。
 7. Server Intelligence Agent を再起動します。

10.2.2 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、Unix ツールに関する章を参照してください。

i 注記

空の CMS データベースをポイントする場合は、cmsdbsetup.sh スクリプトを再度使用して、データベースの再初期化 (再作成) を実行する必要があります (オプション 5)。

1. cmsdbsetup.sh スクリプトを実行します (デフォルトで <<InstallDirectory>>/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. 「yes」と入力し、データソースにこのクラスタのデプロイメント情報が含まれており、クラスタリングの目的ではこの機能を使用しないことを確認します。
4. 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入力します。
5. データベース情報 (ホスト名、ユーザ名、パスワードなど) とクラスタキーを入力します。
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。

関連リンク

[CMS システムデータベースの再作成](#) [ページ 378]

10.3 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 SAP BusinessObjects Business Intelligence 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。[\[ライセンスキー\]](#) エリアを表示します。

i 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。

関連リンク

[サーバの設定のバックアップ](#) [ページ 419]

10.3.1 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。

i 注記

この手順では、CCM をリモートコンピュータ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コンピュータで実行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で、[\[設定\]](#) タブをクリックし、[\[指定\]](#) 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、[\[現在のデータソースをもう一度作成\]](#) をクリックします。

i 注記

手順 1 で CCM を実行したコンピュータからすべてのサーバとオブジェクトも再作成されます。

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。
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コンピュータがある場合は、他のコンピュータでノードを再作成する必要があります。

関連リンク

[Windows 上でノードを再作成する](#) [ページ 351]

10.3.2 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、SAP BusinessObjects Business Intelligence プラットフォーム 管理者ガイドの Unix ツールに関する情報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. ノード名を入力します。
3. [再初期化] (オプション 5) を選択し、選択内容を確認します。
4. CMS システムデータベースのパスワードを入力します。
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。データベースの作成が完了したら、cmsdbsetup.sh スクリプトは自動的に終了します。
5. <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>>
```

6. 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>>
```

i 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。

10.4 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) 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中、またはデータベースタイプをあるデータベースから別のデータベースに移動中のため、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。

i 注記

BI プラットフォームによって DB2 がデフォルトデータベースとしてインストールされている場合は、空白のパスワードを入力します。

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 (SAP BusinessObjects Business Intelligence 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。

i 注記

ユーザ、グループ、フォルダ、およびレポートを以前のバージョンの SAP BusinessObjects Business Intelligence プラットフォームから現在のバージョンにインポートする場合は、SAP BusinessObjects Business Intelligence プラットフォームアップグレードマネジメントツールを使用します。詳細については、*SAP BusinessObjects 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。

10.4.1 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。このタスクは、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、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実行します。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。

i 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 SAP BusinessObjects Business Intelligence 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 Business Intelligence 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。

i 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。

i 注記

SQL Anywhere を CMS データベースとして使用する場合は、DSN 設定で **[パスワードの暗号化]** をクリックしないでください。

10.4.2 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. [別のデータソースからデータをコピー] を選択して、[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、入力を求められたら、ホスト名、ユーザ名、パスワード、およびコピー元クラスタキー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、入力を求められたら、ホスト名、ユーザ名、パスワード、およびコピー先クラスタキーを含むデータベース情報を指定します。
コピー先のデータベースが空の場合は、新しいクラスタキーを入力できます。コピー先のデータベースにクラスタに関する既存のデプロイメント情報が含まれる場合は、そのクラスタのクラスタキーを入力する必要があります。
7. コピー先のデータベースの Business Intelligence プラットフォームテーブルを削除することを確認します。
8. 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。

10.4.3 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。

i 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. <<InstallDirectory>>/sap_bobj/ (デフォルトの場所) から、cmsdbsetup.sh を実行します。
3. ノード名を入力します。
4. [コピー] (オプション 4) を選択し、選択内容を確認します。
5. コピー先の CMS データベースの種類を選択し、入力を求められたら、ホスト名、ユーザ名、パスワード、およびコピー先クラスタキーを指定します。
コピー先のデータベースが空の場合は、新しいクラスタキーを入力します。コピー先のデータベースにクラスタに関する既存のデプロイメント情報が含まれる場合は、そのクラスタのクラスタキーを入力する必要があります。
6. コピー元の CMS データベースの種類を選択し、入力を求められたら、ホスト名、ユーザ名、パスワード、およびコピー元クラスタキーを指定します。
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。

11 Web アプリケーションコンテナサーバ (WACS) の管理

11.1 WACS

11.1.1 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ー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、SAP BusinessObjects Business Intelligence 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。

11.1.1.1 WACS の必要性

SAP Business Objects 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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。

11.1.1.2 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 SAP BusinessObjects Business Intelligence 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。

11.1.1.3 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。	<ul style="list-style-type: none"> 新しい Web アプリケーションコンテナサーバの追加 [ページ 387] Web アプリケーションコンテナサーバのクローン [ページ 387]
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 [ページ 385]
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 [ページ 385]
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。	<ul style="list-style-type: none"> HTTPS/SSL の設定 [ページ 390] WACS とファイアウォールの併用 [ページ 408]
WACS とデプロイメントの他の Business Objects 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 SAP BusinessObjects Business Intelligence プラットフォームサーバ間の SSL 通信を設定します。	<ul style="list-style-type: none"> サーバの SSL 設定 [ページ 143] WACS とファイアウォールの併用 [ページ 408]
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 [ページ 408]
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。	<ul style="list-style-type: none"> WACS と他の Web サーバの併用 [ページ 406] WACS とロードバランサの併用 [ページ 407] WACS とリバースプロキシの併用 [ページ 407] WACS とファイアウォールの併用 [ページ 408]
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。	WACS とロードバランサの併用 [ページ 407]

タスク	説明	トピック
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 [ページ 407]
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。	<ul style="list-style-type: none"> • WACS にトレースを設定する [ページ 409] • サーバメトリクスを表示する [ページ 410]
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。 <ul style="list-style-type: none"> • 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。 	<ul style="list-style-type: none"> • ポート競合の解決 [ページ 410] • メモリ設定を変更する [ページ 411] • 同時要求の数を変更する [ページ 412] • システムデフォルトを復元する [ページ 412]
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 [ページ 409]
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。	WACS プロパティ [ページ 413]

11.1.2 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。

i 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。

11.1.2.1 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、SAP BusinessObjects Business Intelligence 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 アプリケーションおよびサービスを自動的にデプロイする] 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。SAP BusinessObjects Business Intelligence 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。

WACS は Windows オペレーティングシステムでのみサポートされています。

i 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。

11.1.2.2 新しい Web アプリケーションコンテナサーバの追加

i 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。

i 注記

TraceLog サービス (サーバのトレース) は、WACS の新規作成時に自動的に作成されます。

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 起動パッド、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 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 [新規サーバ名] 画面で [次へ]をクリックします。
7. 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。

i 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。

8. [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。
9. 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。
10. [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。

11.1.2.3 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。

i 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。

i 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。

関連リンク

[ポート競合の解決](#) [ページ 410]

11.1.2.4 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。

11.1.3 WACS に対するサービスの追加または削除

11.1.3.1 WACS に Web アプリケーションまたは Web サービスを追加する

SAP BusinessObjects Business Intelligence 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、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。

11.1.3.2 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、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。

11.1.4 HTTPS/SSL の設定

SAP BusinessObjects Business Intelligence プラットフォームデプロイメントのクライアントと WACS 間のネットワーク通信に、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 やデプロイメントの他の SAP BusinessObjects Business Intelligence プラットフォームサーバなどの、SAP BusinessObjects Business Intelligence プラットフォームサーバ間で使用される CorbaSSL。デプロイメントの SAP BusinessObjects Business Intelligence プラットフォームサーバ間での SSL の使用については、このガイドの、ファイアウォールでの BI プラットフォームコンポーネント間の通信に関する情報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

i 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 を作成します。このガイドの、WACS とリバースプロキシの併用に関する情報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 PKCS12 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。

関連リンク

[ファイアウォール用にシステムを設定する](#) [ページ 158]

[BI プラットフォームコンポーネント間の通信について](#) [ページ 149]

[WACS とリバースプロキシの併用](#) [ページ 407]

11.1.4.1 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 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。
- b) [追加]をクリックします。
- c) [スタンドアロンスナップインの追加] ダイアログボックスで、[証明書] を選択し、[追加] をクリックします。
- d) [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。
- e) [ローカルコンピュータ]を選択し、[完了]をクリックします。
- f) [閉じる]をクリックし、[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 ► [証明書のエクスポートウィザード]を開始されます。
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。

11.1.4.2 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]メニューの[スナップインの追加と削除]を選択し、[追加]をクリックします。
 - b) [スタンドアロンスナップインの追加]ダイアログボックスで、[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) [閉じる]をクリックし、[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. MMC の左ペインで、証明書信頼リストを作成する Web サイトを探します。
5. Web サイトを右クリックし、[プロパティ]を選択します。
6. [ディレクトリセキュリティ]タブで、[セキュリティで保護された通信]の[編集]をクリックします。
7. [証明書信頼リストを有効にする]をクリックし、[新規作成]をクリックします。
証明書信頼リストウィザードが開始されます。
8. [次へ]をクリックします。
9. [ストアから追加]または[ファイルから追加]をクリックし、証明書信頼リストに追加する証明書を選択します。次に、[OK]をクリックし、[次へ]をクリックします。
10. 証明書信頼リストの名前と説明を入力し、[次へ]をクリックします。
11. [完了]をクリックし、[OK]をクリックします。
[現在の CTL]フィールドに証明書信頼リストが表示されます。
12. 証明書信頼リストを選択し、[編集]をクリックします。
証明書信頼リストウィザードが開始されます。

13. [次へ]をクリックします。
14. [現在の CTL 証明書]リストで、信頼リストを選択し、[証明書の表示]をクリックします。
15. [詳細]タブで、[ファイルにコピー]をクリックします。
証明書のエクスポートウィザードが開始されます。
16. [次へ]をクリックします。
17. [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。
18. [Personal Information Exchange - PKCS #12(.PFX)]を選択し、[次へ]をクリックします。
19. 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[証明書信頼リストの秘密鍵のアクセス用パスワード]フィールドで指定する必要があります。

11.1.4.3 HTTPS/SSL を設定する

WACS の HTTPS/SSL を設定する前に、PKCS12 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]管理エリアを表示します。
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) [証明書信頼リストファイルの場所]で、信頼リストファイルが格納されている PKCS12 ファイルまたは JKS キーストアの場所を指定します。

i 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。

- 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。

i 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]画面を表示し、[実行中の WACS コネクタリスト]に HTTPS コネクタが表示され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。

11.1.5 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

11.1.6 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。

関連リンク

[Windows AD セキュリティプラグイン](#) [ページ 224]

[AD ユーザーとグループをマップする](#) [ページ 225]

[Kerberos での AD 認証用サービスアカウントの設定](#) [ページ 223]

[Vintela SSO の制限された委任を設定する](#) [ページ 243]

[Kerberos での AD 認証用サービスアカウントの設定](#) [ページ 223]

[WACS に対する Windows AD プラグインでの Kerberos 認証の有効化](#) [ページ 394]

[設定ファイルの作成](#) [ページ 395]

[AD Kerberos 用の WACS の設定](#) [ページ 398]

[AD Kerberos シングルサインオンの設定](#) [ページ 400]

11.1.6.1 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

i 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。

-
- 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

11.1.6.1.1 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。

- サービスアカウントの設定
- サービスアカウントに権限を付与する

- Kerberos での Windows AD サーバを設定する
- AD ユーザとグループをマップして、Windows AD セキュリティプラグインを設定する

関連リンク

[Kerberos での AD 認証用サービスアカウントの設定](#) [ページ 223]

[BI プラットフォームサービスアカウントでの SIA の実行](#) [ページ 230]

[AD ユーザーとグループをマップする](#) [ページ 225]

11.1.6.1.2 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 認証を有効にする](#)]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. [[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。

i 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。
- このアカウントは、SAP BusinessObjects Business Intelligence プラットフォームサーバの実行に使用するアカウント、またはこのアカウントにマッピングする SPN と同じである必要があります。

関連リンク

[AD Kerberos シングルサインオンの設定](#) [ページ 400]

11.1.6.2 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。

i 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。

11.1.6.2.1 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:\WINNT に保存します。

i 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 =
}
```

i 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。

i 注記

kdc はドメインコントローラのホスト名です。

i 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](#) [ページ 397]を参照してください。

i 注記

複数ドメインの設定では、[libdefaults]の下で 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。

11.1.6.2.2 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:\WINNT)に保存します。

i 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。

11.1.6.2.3 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
    }

```

11.1.6.3 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。

11.1.6.3.1 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。

11.1.6.4 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

11.1.6.4.1 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。

i 注記

[\[Web Tier 設定\]](#) アイコンは、停止している WACS を選択している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。

11.1.6.4.2 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。

```
<Install Directory>\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。

11.1.6.4.3 マップされた AD ユーザが WACS の BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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。

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 SAP BusinessObjects Business Intelligence 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、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。

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。

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。

11.1.7 AD Kerberos シングルサインオンの設定

BI 起動パッドまたは 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。

i 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に関する節を参照してください。

関連リンク

[AD Kerberos シングルサインオンのための WACS の 設定](#) [ページ 402]

[AD Kerberos シングルサインオン用のマシン設定](#) [ページ 401]

[AD Kerberos シングルサインオンのための WACS の 設定](#) [ページ 402]

[セキュリティの概要](#) [ページ 125]

11.1.7.1 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](#) [ページ 243]
- [Vintela SSO のサービスアカウントを設定する](#) [ページ 242]
- [複数の SPN の設定](#) [ページ 401]
- [WACS のヘッダサイズ制限を増やす](#) [ページ 401]

次の各節で、これらの手順の実行方法を説明しています。

11.1.7.1.1 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。

11.1.7.1.2 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。

11.1.7.2 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。

11.1.7.3 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。

- SAP BusinessObjects Business Intelligence プラットフォームが WACS にデプロイされている。
- 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な)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。

i 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](#) [ページ 400]を参照してください。

11.1.7.3.1 データベースへのシングルサインオンを有効にする

1. SAP BusinessObjects Business Intelligence 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 WINNT 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。

11.1.8 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。


11.1.8.1 RESTful Web サービスのベース URL を構成する

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 サービスでできるようにベース URL を構成しなければならないことがあります。ベース URL を構成するには、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。

i 注記

BI プラットフォーム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]を選択します。
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** を右クリックして選択します。
[プロパティ]ダイアログボックスが表示されます。
4. [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とポートの名前に置き換えてください。
5. [保存して閉じる]をクリックします。

11.1.8.2 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。

i 注記

エラースタックは、エンドユーザに公開することは避けたい BI プラットフォーム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としてログインします。
2. [\[サーバ\]](#)をクリックし、[\[サーバの一覧\]](#)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(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。

11.1.8.3 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 としてログインします。
2. [\[サーバ\]](#)をクリックし、[\[サーバの一覧\]](#)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(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。

11.1.8.4 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。

i 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]をクリックし、[サーバの一覧]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(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。

11.1.8.5 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、ユーザが HTTP 要求ヘッダ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]をクリックし、[サーバの一覧]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(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 サーバを右クリックし、[サーバの再起動]をクリックします。

11.1.8.6 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、ユーザが初めて RESTful Web サービス要求を行うときに、ユーザ名とパスワードを指定するように求められます。

i 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 プラットフォームへのログオンは、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** > **サーバの一覧**  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(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、: 文字を含むユーザ名を使用できません。

関連リンク

[セッションプールの設定を構成する \[ページ 405\]](#)

11.1.9 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。

11.1.9.1 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。

i 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。

11.1.9.2 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。

関連リンク

[HTTPS/SSL を設定する](#) [ページ 392]

11.1.9.3 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。

11.1.9.3.1 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. [\[プロキシ経由の HTTP の設定\]](#)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。

11.1.9.3.2 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。

11.1.9.4 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 SAP BusinessObjects Business Intelligence 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 Business Intelligence 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。

関連リンク

[BI プラットフォームコンポーネント間の通信について](#) [ページ 149]

11.1.9.5 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 ポートのある 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 とデプロイメント内のその他の Business Intelligence プラットフォームサーバ間の通信に使用する NIC のホスト名または 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。

11.1.10 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 [\[プロパティ\]](#) 画面を開き、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。このガイドの、BOE.war プロパティを介したアプリケーションの管理に関する情報を参照してください。

i 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。

i 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。

関連リンク

[サーバのプロパティを変更する](#) [ページ 335]

[BOE war ファイル](#) [ページ 522]

11.1.11 トラブルシューティング

11.1.11.1 WACS にトレースを設定する

WACS のトレースを設定するには、[コンポーネントからのログのトレース](#) [ページ 713]を参照してください。

11.1.11.2 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。

関連リンク

[Web アプリケーションコンテナサーバのメトリクス](#) [ページ 827]

11.1.11.3 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“エラー有りで開始”という新しいサーバ状態があります。この状態の WACS は実行中ですが、少なくとも 1 つの HTTP、プロキシ経由の HTTP、または HTTPS コネクタの設定に誤りがあります。

WACS が“エラー有りで開始”状態の場合は、[メトリクス] ページにアクセスして [実行中の WACS コネクタの一覧] メトリクスを確認してください。有効なコネクタが一覧に表示されない場合は、コネクタが正しく設定されていません。

11.1.11.4 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]メトリクスと[WACS 起動エラー]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]リスト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 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。

11.1.11.4.1 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。

i 注記

[[Web Tier 設定](#)] アイコンは、停止している WACS を選択している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。

11.1.11.4.2 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。

11.1.11.5 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 のログイ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。

i 注記

[[Web Tier 設定](#)] アイコンは、停止している WACS を選択している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。

11.1.11.6 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。

11.1.11.7 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。

i 注記

[Web Tier 設定]アイコンは、停止している WACS を選択している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。

11.1.11.8 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、[OK] 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] を選択します。
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。

11.1.12 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。

関連リンク

[コアサービスのプロパティ](#) [ページ 779]

12 バックアップと復元

12.1 システムのバックアップと復元

この章では、Business Intelligence プラットフォームシステムおよびデータファイル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 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。

警告

データの損失を防ぐには、BI プラットフォームの次のコンポーネントを定期的にバックアップしてください。

- すべての環境
- BI プラットフォームシステム
- レポート、ユーザ、権限を含む Business Intelligence コンテンツ

バックアップと回復のプロセスは、開発、テスト、実稼動のすべての環境で同様です。

ヒント

Business Intelligence Suite 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。

バックアップおよび回復計画は、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。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。

コールドバックアップとホットバックアップ

BI プラットフォームシステムに障害が発生した場合は、利用可能なバックアップからシステムを復元する必要があります。

コールドバックアップは、システムがオフラインでユーザが利用できないときに実行します。ホットバックアップは、システムの使用中に実行するため、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。

BI プラットフォームシステムの復元および BI コンテンツとサーバ設定の回復

CMS システムデータベース、監査データベース、Input File Repository、Output File Repository、またはファイルシステムの損失、損傷、破損が発生した場合は、BI コンテンツとサーバ設定を復元する必要があります。

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 BI コンテンツをバックアップし、コンテンツを Business Intelligence Archive (LCMBIAR) ファイルにエクスポートします。コンテンツが破損している、または存在しない場合、システム全体を復元することなく後でそのコンテンツを復元することができます。プロモーションマネジメントアプリケーションの使用に関する詳細については、このガイドのプロモーションマネジメントを参照してください。

関連リンク

[完全システムバックアップの実行](#) [ページ 416]

[BI コンテンツのバックアップ](#) [ページ 421]

[Windows 上の CCM でサーバ設定をバックアップする](#) [ページ 419]

[Unix のサーバ設定をバックアップする](#) [ページ 420]

[システムコピーの概要](#) [ページ 431]

12.1.1 バックアップ

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、システムの一部のみを復元することはできません。
- 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。

用語

バックアップは、SAP BusinessObjects データのコピーで、特に運用データベースが損傷した場合にシステムを復元するために作成されます。さまざまな方法でデータをコピーまたは複製できるため、"バックアップ" や "バックアップコピー" という用語が使用されている場合は、何について説明されているのかを理解することが重要です。

データレプリケーションでは、ミラードライブなどのリアルタイムで更新されるデータのコピーが作成されます。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はできますが、データのバージョンングでは、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。バージョンングでは、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。

システムバックアップとアプリケーションバックアップでは、データの復元時に使用できる粒度のレベルが異なります。システムバックアップでは、システム全体のコピーが作成されます。これにより、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。アプリケーションバックアップでは、該当のアプリケーションに関連するすべてのファイルが個別にバックアップされます。これにより、システム全体を復元することなく、個々のファイルを選択して以前のバージョンに復元できます。

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利用できるときに実行されます。

12.1.1.1 完全システムバックアップの実行

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は、同時に作成される次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
- BI プラットフォームファイルシステムのバックアップ
- 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

バックアップファイルをセットとして使用することにより、CMS データベースのバックアップ開始時点の状態に復元することができます。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。

監査データベースに必要なのは最新のバックアップのみです。監査データベースの以前のバックアップはすべて、新しいバックアップの作成時に削除することができます。

i 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。

i 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。

システムをバックアップする頻度は、組織のビジネスのニーズによって異なります。

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働しており、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。

12.1.1.1.1 バックアップを実行する

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。

i 注記

記載されている順番で手順を開始することは重要ですが、次の手順を開始する前に各バックアップが完了するまで待機する必要はありません。この順序はホットバックアップ時にのみ重要です。コールドバックアップでは同じファイルセットを作成する必要がありますが、任意の順序で実行することができます。

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。

i 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。SAP BusinessObjects Business Intelligence 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されたデータベースには、データベースバックアップ用のツールは含まれていません。

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. BI プラットフォームがインストールされているすべてのホストマシンのファイルシステム全体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再起動します。

12.1.1.1.2 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 Business Intelligence プラットフォームシステムをバックアップできます。

前提条件

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、データベースに障害が発生した場合でも、ロールフォワード操作を実行することができます。

i 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。

i 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。

ホットバックアップの有効化

システムのバックアップ中もビジネスの運用を継続する必要がある場合は、ホットバックアップを有効にし、設定する必要があります。ホットバックアップ機能を有効にする場合、以下の事項に留意してください。

- **[ホットバックアップ最長持続時間]** の時間が、バックアップ操作の予測最大時間よりも長くなるようにします。この時間は、CMS バックアップの開始から FRS バックアップの終了までです。この時間が短すぎると、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。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。
- 4.0 FP3 より前の Crystal Reports 2011 Designer クライアント、Web Intelligence リッチクライアント、およびユニバーサルデザインツールクライアント、および SDK に対してコンパイルされた 4.0 FP3 より前のカスタム開発シックスクライアントアプリケーションは、ホットバックアップ時のファイル変更に対応しない可能性があります。バックアップ時に、これらのクライアントアプリケーションから BI コンテンツが変更された場合、バックアップ中に変更されたデータの品質が損なわれる可能性があります。クライアントアプリケーションからのドキュメントの変更を防ぐことで、バックアップデータの整合性を確保できます。クライアントアプリケーションは、可能な限り 4.0 FP3 に更新してください。更新できない場合にも、次善策を検討することはできます。たとえば、クライアントアプリケーションのユーザに対し、オブジェクトを変更するのではなく、既存のオブジェクトを削除して新しいバージョンを保存するように助言できます。

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. **[設定]** ページに移動します。
3. **[ホットバックアップの有効化]** をクリックします。
4. **[ホットバックアップ最長持続時間]** 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。

i 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. 以前の (4.0 FP3 より前の) Web Intelligence リッチクライアント、Crystal Reports Designer、またはカスタム SDK シックスクライアントのアプリケーションでシステム上のドキュメントを変更できるようにするには、**[レガシーアプリケーションのサポート (バックアップ制限) の有効化]** チェックボックスをオンにします。

i 注記

バックアップ処理中に、以前のクライアントアプリケーションでドキュメントを変更できるようにした場合、バックアップ時に変更されたドキュメント内で不整合が生じる可能性があります。バックアップの制限事項については、ホットバックアップの有効化に関する節を参照してください。

6. **[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。

関連リンク

[ホットバックアップの有効化](#) [ページ 418]

[バックアップを実行する](#) [ページ 416]

12.1.1.2 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。

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。設定を変更する場合は、サーバの設定を必ずバックアップすることをお勧めします。

i 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。

関連リンク

[SSL プロトコルの設定](#) [ページ 145]

12.1.1.2.1 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。

i 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。

システムのバックアップ中または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. クラスターキーを入力し [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 BAR 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。

12.1.1.2.2 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。
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。
 - 稼働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。
 - 稼働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。

システムのバックアップ中または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。

12.1.1.2.3 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 スクリプト (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 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。

関連リンク

[BackupCluster スクリプト](#)および [RestoreCluster スクリプト](#) [ページ 428]

12.1.1.3 BI コンテンツのバックアップ

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、レポート、ユーザとグループ、ユニバースなどの Business Intelligence コンテンツを定期的にバックアップすることができます。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。

プロモーションマネジメントアプリケーションの使用に関する詳細については、このガイドのプロモーションマネジメントを参照してください。

Subversion を使用している場合は、Subversion ファイルのバックアップについて、このガイドのバージョン管理を参照してください。

12.1.2 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。

関連リンク

[システム全体の復元](#) [ページ 421]

[サーバ設定の復元\[サーバセッティノフクゲン\]](#) [ページ 426]

[BI コンテンツの復元](#) [ページ 428]

12.1.2.1 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
- FRS ファイルストア
- BI プラットフォームがインストールされているファイルシステム

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。

CMS データベースがクラッシュしているが BI プラットフォームの残りの機能は正常に動作している場合は、システム全体を復元することなく CMS データベースを復元することができます。

関連リンク

[システム全体を復元する](#) [ページ 422]

[監査データベースのみを復元する](#) [ページ 423]

[Web Tier コンテンツを復元する](#) [ページ 424]

[CMS データベースのみを復元する](#) [ページ 424]

12.1.2.1.1 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で復元するかを選択する必要があります。

i 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

i 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。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. 監査機能を使用している場合は、次の操作を実行します。
 - a) 監査データベースの最新のバックアップとトランザクションログを探します。
 - b) 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。
 - c) 監査データベースでロールフォワードを実行し、トランザクションログを再現します。
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](#) [ページ 425]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。

注記

システムを起動した時間を記録します。

8. 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。
SAP BusinessObjects 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。
- 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改ざんされた場合は、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 7 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]>'`

関連リンク

[CMS リポジトリコンテンツのインデックス処理](#) [ページ 604]

12.1.2.1.2 監査データベースのみを復元する

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します。さらに、システムをどの時点で復元するかを選択する必要があります。

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。

1. 監査データベースの最新のバックアップとトランザクションログを探します。
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. 監査データベースでロールフォワードを実行し、トランザクションログを再現します。

関連リンク

12.1.2.1.3 Web Tier コンテンツを復元する

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内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で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。

12.1.2.1.4 CMS データベースのみを復元する

i 注記

この手順は、CMS データベースがクラッシュした場合にのみ実行してください。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。

i 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。

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. CMS データベースの最新のバックアップセットを探します。
3. 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。
4. CMS データベースの最新のトランザクションログ、つまり最新のバックアップ後に実行されたトランザクションが含まれているログを探します。
5. CMS データベースのトランザクションログ全体を再現します。
6. 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。
SAP BusinessObjects 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。
- 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。

関連リンク

[CMS リポジトリコンテンツのインデックス処理](#) [ページ 604]

12.1.2.1.5 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。

関連リンク

[CMS リポトリコンテンツのインデックス処理](#) [ページ 604]

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。

i 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 `<<install_dir>>\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`」と入力して [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: `<<install_dir>>/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各クラスタにインストールされた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。
-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。

12.1.2.2 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。

i 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。

i 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。

関連リンク

[サーバの SSL 設定](#) [ページ 143]

12.1.2.2.1 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、ログファイルを確認して原因を特定してください。
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。

i 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。

関連リンク

[ノードの使用](#) [ページ 345]

12.1.2.2.2 Unix で CCM を使用して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。
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。復元プロセスの詳細は、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。

12.1.2.2.3 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 `/<<INSTALLDIR>>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts` ディレクトリにあります。

関連リンク

[BackupCluster スクリプト](#) および [RestoreCluster スクリプト](#) [ページ 428]

12.1.2.3 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アプリケーションを使用して、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。

12.1.3 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。

i 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。

表 16: BackupCluster パラメータ

名前	説明	例
<code>-backup</code>	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	<code>-backup "C:\Users\Administrator\Desktop\my.biar"</code>
<code>-cms</code>	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。	<code>-cms mycms:6400</code>
<code>-username</code>	Administrator アカウントのユーザ名	<code>-username Administrator</code>
<code>-password</code>	Administrator アカウントのパスワード	<code>-password Password1</code>

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。

表 17: 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	<code>-restore "C:\Users\Administrator\Desktop\my.biar"</code>
-username	Administrator アカウントのユーザ名	<code>-username Administrator</code>
-password	Administrator アカウントのパスワード	<code>-password Password1</code>
-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。	<code>-displaycontents "C:\Users\Administrator\Desktop\my.biar"</code>

i 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。

表 18: 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。	<code>-usetempcms</code>
-cmsport	一時 CMS のポート番号	<code>-cmsport 6400</code>
-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。 <ul style="list-style-type: none"> <code>db2databasesubsystem</code> <code>maxdbdatabasesubsystem</code> <code>mysqldatabasesubsystem</code> <code>oracledatabasesubsystem</code> <code>sqlserverdatabasesubsystem</code> <code>sybasedatabasesubsystem</code> <code>sqlanywheredatabasesubsystem</code> <code>newdbdatabasesubsystem</code> 	<code>-dbdriver sqlserverdatabasesubsystem</code>

名前	説明	例
	<p>i 注記</p> <p>newdbdatabasesubsystem パラメータは SAP HANA データベースを使用します。</p>	
-connect	CMS システムデータベース接続文字列	<pre>-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"</pre>
-dbkey	クラスタキー	<pre>-dbkey abc1234</pre>

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
```

13 デプロイメントのコピー

13.1 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。

13.2 用語

- **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コピー。
- **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コピー。
- **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コピー。
- **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コピー。

13.3 使用事例

システムのコピーを作成する理由はいくつかあります。以下の表に、達成すべき目標と、前提となる現在のリソースを一覧に挙げ、最も適切なワークフローへの参照を示します。

目標	利用できるリソース	解決策
デプロイメント間でオブジェクトのセット (最大 1,000 個) をコピーする	LCM 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を使用してシステム間でオブジェクトを昇格します。このガイドのプロモーションマネジメントを参照してください。
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する	LCM バージョニングが使用されているシステム	バージョン管理を使用して、ドキュメントの以前のバージョンを復元します。このガイドのバージョン管理を参照してください。
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する	<ul style="list-style-type: none">• 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 AND• コピー手順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 [ページ 432] のシステムコピー手順ワークフローを使用し、この章の残りの手順に従います。

目標	利用できるリソース	解決策
		<p>i 注記</p> <p>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。</p>
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する	<ul style="list-style-type: none"> ソースシステムを再作成するための同じハードウェア AND 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 	<p>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。完全システムバックアップの実行 [ページ 416] 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。</p>
ソースシステムのハードウェアおよび IP アドレス/マシン名と全く一致する必要はない複製システムを、スタンバイ、テスト、またはトレーニング用に作成する	<ul style="list-style-type: none"> 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 AND コピー手順で説明している詳細なシステム情報 	<p>システムのコピーの計画 [ページ 432] のシステムコピー手順ワークフローを使用し、この章の残りの手順に従います。</p> <p>i 注記</p> <p>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。</p>

13.4 システムのコピーの計画

システムをコピーするには、次の 2 つの段階があります。

1. ソースシステムのコピーの作成
2. ターゲット環境でのコピーの再作成

これらの手順は、それぞれを実行した直後に実行する必要はありません。コピーを作成して、ターゲットシステムでのコピーの再作成に進むまでに時間が経過していてもかまいません。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には、次の詳細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なダウンタイム
 - ターゲットシステムの整合性を確保するためのテストの計画時間
- 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

次のトピック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をソースシステムと異なるハードウェアにインストールする場合は、ターゲットシステムのパフォーマンスを改善するためのチューニングが必要になる場合があります。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は、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ファイル

- 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)
- ライフサイクルマネジメント Subversion データベース (オプション)

13.5 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

領域	考慮点
	<p>するガイドは、http://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。</p>
プログラムのバージョン	<p>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。</p>
内容と設定	<p>ソースシステム全体がコピーされます。内容やシステム設定を選択してコピーすることはできません。</p>
インストールパス	<p>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:\BusinessObjects にインストールした場合は、ターゲットを C:\BusinessObjects にインストールする必要があります。</p>
ホストオペレーティングシステム	<p>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。</p>
CMS データベースのソフトウェアのタイプ	<p>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。</p>
監査データベースのソフトウェアのタイプ	<p>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。</p> <div style="background-color: #fff9c4; padding: 10px; margin-top: 10px;"> <p>i 注記</p> <p>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。</p> </div>
Web Tier のカスタマイズ	<p>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場合（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。</p>
この手順で紹介していないピック	<p>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。</p>

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。
- ライフサイクルマネジメントデータベース。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。

i 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](#) [ページ 31]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対してシステムコピーのインポートを実行する](#) [ページ 438]」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、LCM 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。

13.6 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。

13.6.1 ソースシステムからシステムコピーのエクスポートを実行する

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](#)にあります。

プロパティ	場所
CMS クラスターキー (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。
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 [ブレースホルダ] を選択します。%INSTALLROOTDIR% ブレースホルダの値を確認します。

プロパティ	場所
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。
<p>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。</p> <p>i 注記</p> <p>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。</p>	<p>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。</p> <p>次のメトリクスを確認します。</p> <ul style="list-style-type: none"> 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 2011 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。	<p>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。</p> <p>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 <code>AddOrRemoveProducts.sh</code> ユーティリティを使用できます。</p>
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。	<p>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。</p> <p>i 注記</p> <p>% 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。</p>
ライフサイクルマネジメント (LCM) のコピーを計画している場合、LCM データベースフォルダと LCM Subversion フォルダの場所	<p>Windows インストールでの LCM データベースのデフォルトフォルダは、<code><<INSTALLDIR>>\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOverride</code> です。</p> <p>Windows インストールでの LCM Subversion ファイルのデフォルトの場所は次のとおりです。</p> <ul style="list-style-type: none"> <code><<INSTALLDIR>>\SAP BusinessObjects Enterprise XI 4.0\CheckOut</code>

プロパティ	場所
	<ul style="list-style-type: none"> • <<INSTALLDIR>>\SAP BusinessObjects Enterprise XI 4.0\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。	<p>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。</p> <p>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\Data\TrendingDB です。</p>
セマンティックレイヤフォルダのパス。	<p>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 <<install_dir>>\SAP BusinessObjects Enterprise XI 4.0\dataAccess \connectionsServer\ です。</p>

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。
 - FRS 入力および出力ファイルストア
 - モニタリングトレンドデータベース (オプション)。ワークシートに記録されているモニタリングフォルダからファイルをバックアップします。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
 - ライフサイクルマネジメントデータベース (オプション)。これは、ワークシートに記録されているデータベースフォルダからファイルをバックアップすることで作成できます。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\LCM\LCMOverride
 - ライフサイクルマネジメント 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ている Subversion フォルダからファイルをバックアップすることで作成できます。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\CheckOut
 - **<<INSTALLDIR>>**\SAP BusinessObjects Enterprise XI 4.0\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、およびそのいずれかのサブフォルダにある .sbo および .prm ファイル。

i 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**の節を参照してください。

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な、更新可能な 2 つ目のコピーを保存することもできます。

13.6.2 ターゲットシステムに対してシステムコピーのインポートを実行する

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システムコピーのエクスポートを実行する”」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。

i 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](#)トピック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。

i 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したフォルダ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 (モニタリング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。
8. LCM データベースフォルダ (LCM 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. LCM Subversion ファイル (LCM 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したフォルダ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](#)を実行します。

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. 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。
 4. フル検索の再インデックス化を実行します。

14 バージョン管理

14.1 BI リソースのさまざまなバージョンの管理

プロモーションマネジメントアプリケーションでは、SAP BusinessObjects Business Intelligence プラットフォームリポジトリに存在する BI リソースのさまざまなバージョンを管理することができます。この機能のために、ツールには SubVersion バージョン管理システムと ClearCase バージョン管理システムがあります。

ジョブまたは InfoObject のさまざまなバージョンを管理するには、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 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。

i 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ンングするには、[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。
[バージョン管理システム] 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。
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 リポジトリに作成されます。
8. [履歴] を選択し、選択した InfoObject の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 つのバージョンのコンテンツのメタデータ情報を比較できます。
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。

i 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。そのインジケータにカーソルを合わせると、CMS の InfoObject が更新されたことを示す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。[バージョンのコピーを取得] をクリックすると、選択したリソースのコピーを取得できます。

[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。

i 注記

[バージョンを取得] または [バージョンのコピーを取得] のいずれかを使用すると、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 4 ~ 16 を実行することができます。

14.2 [VMS 設定]オプションの使用

セントラル管理コンソールからバージョン管理システムを設定できます。SubVersion および ClearCase のパラメータを設定できます。

SubVersion の管理システムを設定するには、次の手順に従います。

1. CMC のホームページから [アプリケーション] を選択します。
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] ドロップダウンリストから [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ディレクトリ名が該当するフィールドに表示されます。
5. 必要であればフィールドを変更します。
<.exe> ファイルを含む完全なインストールパスを入力します。Windows の場合は、<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\subversion を入力し、Unix の場合は、<INSTALLDIR>/sap_bobj/enterprise_40/subversion/bin を入力します。
6. HTTP ラジオボタンまたは SVN ラジオボタンをクリックすると、それぞれ HTTP プロトコルまたは SVN プロトコルを使用して、SubVersion リポジトリにアクセスできます。
7. [VMS のテスト] をクリックして、入力した VMS 設定を検証できます。
8. [保存] をクリックします。

i 注記

- SubVersion をデフォルトの VMS として使用するには、[デフォルトの VMS として使用]を選択します。
- 手順 3 によりフィールドを変更した場合、Server Intelligence Agent を再起動します。

14.2.1 Windows での ClearCase バージョン管理システム (VMS) の設定

Windows に ClearCase のバージョン管理システムを設定するには、次の手順に従います。

1. [管理オプション] ウィンドウで [VMS 設定] をクリックします。
2. [バージョン管理システム] ドロップダウンリストから [ClearCase] を選択します。
3. 次の詳細情報を入力します。
 - ClearCase マップドライブ: ドライブ名を入力します。デフォルトでは M ドライブです。例: M:
 - VOB タグ名: Versioned Object Base (VOB) の名前を入力します。例: FridayVB
 - ビュー格納域のディレクトリ: 共有フォルダへのパスを入力します。例: \\HostName\FolderName

i 注記

ホスト名として「localhost」を入力することはできません。

4. [保存] をクリックします。

14.2.2 Unix での ClearCase バージョン管理 (VMS) システムの設定

Unix に ClearCase のバージョン管理システムを設定するには、次の手順に従います。

1. [管理オプション] ウィンドウで [VMS 設定] をクリックします。
2. [バージョン管理システム] ドロップダウンリストから [ClearCase] を選択します。
3. 次の詳細情報を入力します。
 - ClearCase マップドライブ: MVFS を含むフォルダの名前を入力します。デフォルトは /view です。
 - VOB タグ名: VOB 名、および VOB を含むフォルダを入力します。例: VobFolder/VobName
 - ビュー格納域ディレクトリ: ビューが作成されたディレクトリのパスを入力します。

ClearCase をデフォルトバージョン管理システムとして使用する場合には、[デフォルトの VMS として使用] を選択できます。

14.3 同じジョブの異なるバージョンの比較

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 InfoObject 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。

14.4 Subversion コンテンツのアップグレード

以前のバージョンの SAP BusinessObjects 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 3.x マシンの VMS にログインします。
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。次に、`svnadmin dump c:/LCM_repository/svn_repository > dumrepo` というエクスポートコマンドを実行します。
6. `dumrepo` ファイルを SAP BusinessObjects BI プラットフォームマシンにコピーします。
7. SAP BusinessObjects 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。

15 プロモーションマネジメント

15.1 プロモーションマネジメントへようこそ

15.1.1 プロモーションマネジメントの概要

プロモーションマネジメントアプリケーションは、ビジネスインテリジェンス (BI) リソースのリポジトリ間の移動、リソースの依存関係の管理を可能にし、必要に応じて出力先システムで昇格されたリソースのロールバックも行います。同一 BI リソースのバージョン管理もサポートします。

プロモーションマネジメントアプリケーションは、セントラル管理コンソールと統合されます。BI リソースを別のシステムに昇格できるのは、ソースシステムと移動先システムの両方に同じバージョンの SAP BusinessObjects Business Intelligence platform アプリケーションがインストールされている場合だけです。

15.1.2 プロモーションマネジメントの機能

プロモーションマネジメントアプリケーションは、以下の機能に対応しています。

- 昇格: この機能では、出力先システムの InfoObject を作成または更新できます。InfoObject の昇格とは別に、この機能では次のタスクを実行できます。
 - 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
- 依存関係の管理: この機能では、昇格させるジョブの InfoObject の依存オブジェクトを選択、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。[毎時]、[毎日]、[毎週]、または [毎月] のいずれかのパラメータを使用して、ジョブを昇格させる時期を指定できます。
- 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戻すことができます。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。
- 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。

15.1.3 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 内でプロモーションマネジメント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。
- プロモーションマネジメント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。

プロモーションマネジメント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
 - LCM 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アプリケーションのアクセス権限が CMC 内に設定されます。

15.2 プロモーションマネジメントツールを使用する前に

15.2.1 プロモーションマネジメントアプリケーションへのアクセス

プロモーションマネジメントアプリケーション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アプリケーション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。







15.2.2 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。
	既存のジョブを削除できます。
	昇格できる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。

オプション	説明
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 ファイルや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	出力先システムから昇格されたジョブを取得できます。
	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、新たに作成されたジョブの一覧が表示されます。このパネルを使用して、ジョブ名、ジョブのステータス、ジョブ作成情報、昇格の概要、昇格テストの概要、依存関係管理画面、出力先システム情報を表示できます。

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。新たに作成されたジョブは、[\[昇格ジョブ\]](#) 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。

詳細パネル

このパネルには [\[基本設定\]](#) リンクも表示されます。管理者とユーザはこのリンクを使用してツールの基本設定を行うことができます。[\[ヘルプ\]](#) リンクおよび [\[バージョン情報\]](#) リンクを使用して、プロモーションマネジメントツールの使用に関する詳細情報を取得することができます。

ショッピングカートおよびジョブビューアページ

ショッピングカートは動的に生成されるツリー表示であり、昇格対象 InfoObject が表示されます。InfoObject はユーザグループ、ユニバース、接続などに分類されます。ジョブビューアページでは、ジョブに追加された InfoObject を表示できます。

15.2.3 設定オプションの使用

ある SAP BusinessObjects Business Intelligence プラットフォームデプロイメントから別の SAP BusinessObjects Business Intelligence 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、完了したインスタンスが [依存項目] ページに表示されるように選択できます。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。
- **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。
- **上書き設定**: このオプションでは、Crystal Reports とユニバースの接続に使用するデータベース接続情報をスキャン、昇格、および編集できます。ここでは、QAAWA URL を編集することもできます。

15.2.3.1 [システムの管理]オプションの使用

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っ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. [管理オプション]ウィンドウで[システムの管理]オプションをクリックします。
[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。

i 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特定します。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。

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。

i 注記

ホストシステムを削除するには、削除するホストシステムを選択してから[削除]をクリックします。

関連リンク

[\[ロールバック設定\]オプションの使用](#) [ページ 450]

[\[ジョブ設定\]オプションの使用](#) [ページ 450]

15.2.3.2 [ロールバック設定]オプションの使用

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。

関連リンク

[\[ジョブ設定\]オプションの使用](#) [ページ 450]

15.2.3.3 [ジョブ設定]オプションの使用

[ジョブ設定]オプションでは、システムに存在可能なジョブインスタンス数を指定できます。次のオプションのいずれかを指定できます。

- 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、システムに存在可能なジョブ 1 件あたりの最大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すべてのジョブインスタンスを削除する必要があることを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、[表示するジョブの作成期間] ドロップダウンリストから時間間隔を選択します。

[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。

i 注記

古いジョブインスタンスは、次のジョブ実行時に削除されます。

関連リンク

[\[VMS 設定\]オプションの使用](#) [ページ 442]

15.2.3.4 上書き設定オプションの使用

上書き設定オプションを使用すると、ジョブの昇格または BIAR ファイルを介して、上書きを昇格できます。

i 注記

システムという用語は、以下の手順で使用されます。システムには、次の 3 種類があります。

- ソース: 接続情報の提供元システムとして機能するソースシステムです。
- セントラル LCM: デフォルトで接続されるシステムです。
- 出力先: BI リソースが昇格されているエンドシステムです。

15.2.3.4.1 上書きの昇格

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、[\[システムの管理\]オプションの使用](#) [ページ 449]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. [\[管理オプション\]](#) ウィンドウで [\[上書き設定\]](#) 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。[\[固有の接続の一覧\]](#) が表示されます。

i 注記

ユーザの基本設定に応じて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. [\[ログイン\]](#) をクリックして、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。
複数の出力先システムを指定することができます。
9. [\[昇格\]](#) をクリックします。
上書きの昇格が完了します。

i 注記

出力先システムで InfoObject の昇格時に上書きが失敗すると、システムによってジョブステータスが [\[一部成功\]](#) に設定されます。また、[\[上書き失敗\]](#) の警告ステータスがオブジェクトに設定されます。

10. 元のシステムからログオフします。
11. [\[上書き設定\]](#) 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。
12. 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。
13. 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。
14. 必要な値を更新して、[\[完了\]](#) をクリックします。
15. オブジェクトの状態をアクティブに変更し、[\[保存\]](#) をクリックします。

15.2.3.4.2 BIAR ファイルを使用した上書きの昇格

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、[\[システムの管理\] オプションの使用](#) [ページ 449] 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. [\[管理オプション\]](#) ウィンドウで [\[上書き設定\]](#) 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 LCM 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。

i 注記

ユーザの基本設定に応じて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. LCM ツールを使用して出力先システムにログインし、[インポート](#) [ファイルの上書き](#) をクリックします。
[\[LCMBIAR のインポート\]](#) 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。

i 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ます。

i 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。
20. 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。

15.2.3.4.3 CTS+ を使用した上書きの昇格

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] オプションの使用 [ページ 449] 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。

i 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. [管理オプション] ウィンドウで [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 LCM 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。

i 注記

ユーザの基本設定に応じて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 の使用の詳細については、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/b5/6d03660d3745938cd46d6f5f9cef2e/frameset.htm 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/55/07c497db8140ef8176715d4728eec1/frameset.htm 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アイテムを見ることができます。
 - d) 出力先 LCM 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm 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。
16. オブジェクトの状態をアクティブに変更し、[保存] をクリックします。

15.2.3.4.4 クラスタ環境における上書きの昇格

InfoObject を上書きする場合に、上書き情報はデフォルトで derby データベース (セントラル LCM) に保存されます。クラスタ環境では、各 BI プラットフォームに独自の derby データベースがあります。上書きを昇格するには、BI プラットフォームシステムの 1 つの derby データベースを共有し、そのデータベースをすべてのクラスタ化システム用の共有セントラルデータベースとして使用する必要があります。

たとえば、3 つのクラスタ化システム A、B、C があるとします。まず、A システムの derby データベースを共有する必要があります。この A システムの derby データベースがセントラルデータベースとなります。B システムおよび C システムの上書き設定で、A システムによって共有されている derby セントラルデータベースの場所を指定する必要があります。

1. CMC にログインします。
2. [\[アプリケーション\]](#)に移動します。
3. [\[プロモーションマネジメント\]](#)を選択します。
4. [\[LCM 上書き設定\]](#)を選択します。
5. derby センtralデータベースの場所を入力します。

たとえば、センtralデータベースをホストしているシステムの場合は、derby 共有データベースの実際のパス (<BI_PLATFORM_INST_DIR>/SAP BusinessObjects Enterprise XI 4.0/Data/) を指定します。他のクラスタ化システムのすべてで、derby 共有データベースの場所 (\\SYSTEM_A_HOSTNAME\Data\) を指定します。

6. [\[保存\]](#) をクリックします。
7. [APS](#) を再起動します。

15.2.3.5 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アプリケーション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の CTS+ の設定](#) [ページ 483]セクションを参照してください。

15.3 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アプリケーションを起動すると、デフォルトで [\[昇格ジョブ\]](#) ページに移動します。

[\[昇格ジョブ\]](#) 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。

- ジョブ関連処理を選択するには、[\[新しいジョブ\]](#)を選択します。ホームページ画面を右クリックして、一覧からジョブ関連処理を選択することもできます。
- 新しいジョブの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](#) を選択して、BIAR または LCMBIAR ファイル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](#) を選択します。
- 既存のジョブを変更するには、[\[編集\]](#)を選択します。
- ソースシステムから出力先システムにジョブを昇格する、あるいは BIAR ファイルにジョブをエクスポートするには、[\[昇格\]](#)を選択します。
- 出力先システムから昇格されたジョブを復元するには、[\[ロールバック\]](#)を選択します。
- ジョブの以前の昇格インスタンスを表示するには、[\[履歴\]](#)を選択します。
- タイトル、ID、ファイル名、説明など、選択したジョブインスタンスのプロパティを表示するには、[\[プロパティ\]](#)を選択します。

[\[昇格ジョブ\]](#) アプリケーション領域には、システムに存在するジョブの一覧と、次のような各ジョブの情報が表示されます。

- [\[名前\]](#): 作成したジョブ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。
- [\[作成者\]](#): ジョブ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アプリケーションでは、すべてのアクティビティに SAP BusinessObjects Business Intelligence プラットフォーム SDK が使用されます。


15.3.1 フォルダの作成と削除

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。

15.3.1.1 フォルダの作成

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。

関連リンク


[ジョブの作成](#) [ページ 457]

[フォルダの削除](#) [ページ 456]

15.3.1.2 フォルダの削除

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。

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またはジョブを選択します。
2.  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。
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。

関連リンク

15.3.2 ジョブの作成

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。

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 SAP BusinessObjects Business Intelligence platform システムの名前。
出力先システム	ジョブの昇格先となる SAP BusinessObjects Business Intelligence platform 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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> Enterprise Windows AD LDAP SAP

i 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]タ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. ジョブに依存オブジェクトを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。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表示されます。その後依存オブジェクトを個別に選択することができます。
6. 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。
7. [作成] 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。

関連リンク

[上書き設定オプションの使用](#) [ページ 451]

15.3.2.1 新しい CMS へのログイン

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。

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、[ジョブの作成](#) [ページ 457]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. 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。
5. [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。
6. 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。

関連リンク

[ジョブの編集](#) [ページ 460]

[プロモーションマネジメントでの InfoObject の追加](#) [ページ 460]

[リポジトリに接続している時のジョブの昇格](#) [ページ 462]

[ジョブの昇格のスケジュール](#) [ページ 467]

15.3.3 既存ジョブのコピーによるジョブの新規作成

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。

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アプリケーションを起動します。
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。
[\[既存のジョブのコピー\]](#) ウィンドウに[\[昇格ジョブ\]](#) 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、および説明が表示されます。必要に応じてこれらのフィールドを変更できます。ただし、ソースシステム名を変更することはできません。
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、[\[オブジェクトの追加 - ジョブ名\]](#) ページが表示されます。

関連リンク

[プロモーションマネジメントでの InfoObject の追加](#) [ページ 460]

[ジョブの編集](#) [ページ 460]

[リポジトリに接続している時のジョブの昇格](#) [ページ 462]

15.3.4 ジョブの検索

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。

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、キーワードからジョブを検索できます。
 - 説明の検索: このオプションでは、ジョブの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。

関連リンク

[プロモーションマネジメントでの InfoObject の追加](#) [ページ 460]

[ジョブの編集](#) [ページ 460]

15.3.5 ジョブの編集

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。

i 注記

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アプリケーションを起動します。
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。

関連リンク

[プロモーションマネジメントでの InfoObject の追加](#) [ページ 460]

[リポジトリに接続している時のジョブの昇格](#) [ページ 462]

[ジョブの昇格のスケジュール](#) [ページ 467]

15.3.6 プロモーションマネジメントでの InfoObject の追加

各ジョブには InfoObject とその依存オブジェク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。

i 注記

ジョブに InfoObject を追加する際には、出力先システムにログインする必要があります。

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します。
ジョブの新規作成については、[ジョブの作成](#) [ページ 457]を参照してください。
3. [\[オブジェクトの追加\]](#) をクリックします。
[\[オブジェクトの追加\]](#) ダイアログボックスが表示され、オブジェクトの一覧が表示されます。
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 を追加してから[\[オブジェクトの追加 - ソースシステム名\]](#)ダイアログボックスを終了するには、[\[追加して閉じる\]](#) をクリックします。ジョブに InfoObject が追加され、[\[オブジェクトの追加 - ソースシステム名\]](#)ダイアログボックスが終了します。

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、ジョブ関連プロセスを選択して昇格タスクを続行します。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、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 件未満となるように設定することを推奨しています。

関連リンク

[プロモーションマネジメントでの依存関係の管理](#) [ページ 461]

[リポトリに接続している時のジョブの昇格](#) [ページ 462]


[ジョブの昇格のスケジュール](#) [ページ 467]

15.3.7 プロモーションマネジメントでの依存関係の管理

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。

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します。
新しいジョブ作成に関する情報については、[ジョブの作成](#) [ページ 457]を参照してください。
3. 必要な InfoObject を新しいジョブに追加します。
[昇格ジョブ](#) 画面が表示されます。
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. ジョブに依存オブジェクトを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、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、[[選択されていない依存オブジェクトのみを表示](#)]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、[依存オブジェクトの検索](#) [ページ 462]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。

i 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。

関連リンク

[リポジトリに接続している時のジョブの昇格](#) [ページ 462]

15.3.8 依存オブジェクトの検索

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。

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。

関連リンク

[プロモーションマネジメントでの依存関係の管理](#) [ページ 461]

15.3.9 リポジトリに接続している時のジョブの昇格

このセクションでは、リポジトリに接続している場合にソースシステムから出力先システムをジョブを昇格する方法について説明します。

以下の表は、プロモーションマネジメント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、Dashboards、QaaWS、Explorer

カテゴリ	昇格できるオブジェクトタイプ
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、アラート、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	ユニバース UNV、接続
EPM ダッシュボード	ユニバース、接続、レポート、ダッシュボード、およびアナリティクス
BusinessView	DataFoundation
フェデレーション <ul style="list-style-type: none"> 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、Dashboards、.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、Dashboard Design、DSL Universe (UNX)、WEBI、エクスプローラ、Data Federator、Data Steward、BI ワークスペースなど

ジョブを昇格するには、次の手順に従います。

1. プロモーションマネジメントを起動します。
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. [\[ソース\]](#) システムと [\[出力先\]](#) システムの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。

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

[\[外部変更管理 ID\]](#) 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。プロモーションマネジメントツールでは、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。変更管理 ID 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 **[セキュリティを昇格]** を選択した場合にのみ有効になります。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。

[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。

6. **[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。プロモーションマネジメントツールでは、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。

i 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: 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。

7. ジョブインスタンスの昇格をスケジュールするには、**[ジョブをスケジュール]**をクリックします。

8. **[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。

15.3.10 BIAR 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接続されている場合には、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接続されていない場合でも、InfoObject を昇格することができます。

ソースシステムと出力先システムが接続されていないシナリオでは、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 BIAR 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、BIAR 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。

i 注記

インポートウィザードツールで作成された BIAR ファイルを使用することはできません。

関連リンク

[BIAR ファイルへのジョブのエクスポート](#) [ページ 465]

[BIAR ファイルからのジョブのインポート](#) [ページ 466]

15.3.10.1 BIAR ファイルへのジョブのエクスポート

このセクションでは、BIAR ファイルへジョブをエクスポートする方法について説明します。

BIAR ファイルへ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、[ジョブの作成](#) [ページ 457]を参照してください。
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. **[昇格]** をクリックします。
[昇格] ウィンドウが表示されます。
5. 必要に応じてオプションを変更し、**[エクスポート]** をクリックします。
BIAR ファイルが作成されます。BIAR ファイルをファイルシステムまたは FTP の場所に保存できます。
6. **[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 ファイルの出力先] ペインが表示されます。
7. 以下のいずれかのステップを実行します。
 - **[ファイルシステム]** を選択します。
 - **[FTP]** を選択し、**[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ます。
8. 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。
9. **[パスワード]** フィールドにパスワードを入力します。
10. **[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。
11. **[エクスポート]** をクリックします。
ステップ 7 で選択したオプションに応じて、BIAR ファイルが、ファイルシステムまたは FTP にエクスポートされます。
12. BIAR 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、[ジョブの昇格のスケジュール](#) [ページ 467]の節を参照してください。

関連リンク

[プロモーションマネジメントでの InfoObject の追加](#) [ページ 460]

[プロモーションマネジメントでの依存関係の管理](#) [ページ 461]

15.3.10.2 BIAR ファイルからのジョブのインポート

従来の BIAR ファイルまたは LCMBIAR ファイルからジョブをインポートできます。BIAR 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。

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. 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. [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. ローカルマシンまたは他のソースマシンから BIAR ファイルをインポートできます。
 - ローカルマシンから 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 BIAR ファイルを選択します。

i 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 CUID と名前 (**Jobname_copy**) でジョブが作成されます。

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。

i 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。
 - FTP が有効化されているソースマシンから 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. [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。

i 注記

LCMBIAR またはアップグレード BIAR ファイルのみをインポートできます。

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。

関連リンク

[プロモーションマネジメントでの依存関係の管理](#) [ページ 461]

15.3.11 ジョブの昇格のスケジュール

このセクションでは、ジョブインスタンス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。

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 を既存の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。

出力先へのスケジュールは、BIAR ファイルへのジョブのエクスポート中に行うことができます。

➡ ヒント

InfoObject の昇格が完了したら、InfoObject の実行中のインスタンスをすべて表示できます。これを行うには、InfoObject を右クリックして **[履歴]** を選択します。

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。

関連リンク

[BIAR ファイルへのジョブのエクスポート](#) [ページ 465]

15.3.11.1 定期および一時停止中のジョブ昇格インスタンスの更新




プロモーションマネジメントツールでは、**[定期的スケジュールのジョブ履歴および待機中のインスタンス]** オプションを使用し、スケジュールされているジョブインスタンスの昇格のステータスを追跡および更新することができます。

スケジュールされているジョブの昇格インスタンスを追跡および更新するには、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、定期および一時停止中のジョブの昇格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。

- スケジュールされたジョブの昇格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。
- スケジュールされた昇格を一時停止するには、**[一時停止]** オプションをクリックします。
- スケジュールされたジョブの昇格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。
- ジョブの昇格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ジョブの昇格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ジョブの昇格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。
-  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。

i 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、定期や一時停止中といったジョブインスタンスの昇格のステータスが表示されます。

関連リンク

[ジョブのロールバック](#) [ページ 468]

15.3.12 ジョブ履歴の表示

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。

i 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

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. 次の操作を実行できます。
 - 履歴を表示するジョブを右クリックし、[履歴] をクリックします。
 - 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。

ジョブのインスタンス、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、ジョブのステータスを表示できます。

15.3.13 ジョブのロールバック

[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。

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. ロールバックするジョブを選択し、[完全ロールバック] をクリックします。
ジョブがロールバックされます。

ジョブの昇格の最新インスタンスのみをロールバックできます。2 つのジョブインスタンスを同時にロールバックすることはできません。

15.3.13.1 [一部ロールバック]オプションの使用

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. 一覧からジョブを選択し、[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。

i 注記

次のジョブをロールバックする前に、ジョブに含まれている InfoObject をすべてロールバックしておく必要があります。

重要: 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。

関連リンク

[BI リソースのさまざまなバージョンの管理](#) [ページ 441]

15.3.13.2 パスワード期限切れ後のジョブのロールバック

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。

関連リンク

[パスワード期限切れ後の InfoObject のロールバック](#) [ページ 470]

[\[一部ロールバック\]オプションの使用](#) [ページ 469]

15.3.13.2.1 パスワード期限切れ後の InfoObject のロールバック

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 InfoObject 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。
[[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。

関連リンク

[ジョブのロールバック](#) [ページ 468]

[\[一部ロールバック\]オプションの使用](#) [ページ 469]

[パスワード期限切れ後のジョブのロールバック](#) [ページ 469]

15.4 InfoObject のさまざまなバージョンの管理


バージョン管理アプリケーションでは、SAP BusinessObjects Business Intelligence 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。LifeCycle Manager ツールは、SubVersion と ClearCase 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コンソール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アプリケーションを起動します。
2. ホームページで、ドロップダウンリストから [\[バージョン管理\]](#) 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。
3. ログイン認証情報を入力し、[\[ログイン\]](#) をクリックします。
[\[バージョン管理\]](#) ウィンドウが表示されます。

i 注記

バージョン管理システム (VMS) には、バージョン管理システムの設定が済んでいる場合に限りログインできます。

4. ホストシステムを変更するには、 をクリックします。
[\[システムにログイン\]](#) ダイアログボックスが表示されます。
5. ユーザ認証情報を入力し、[\[ログイン\]](#) をクリックします。
6. [\[バージョン管理\]](#) 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 InfoObject を表示します。
7. InfoObject を選択し、[\[VM に追加\]](#) をクリックします。

i 注記

[\[バージョン管理に追加\]](#) 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。

8. [\[チェックイン\]](#) 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。
9. 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。
10. 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。
11. 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。
12. [\[履歴\]](#) を選択し、選択したリソースの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。

13. 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。


i 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。

14. CMS と VMS の同期: InfoObject の CMS バージョンが更新されると、更新された InfoObject の横にインジケータが表示されます。そのインジケータにカーソルを合わせると、CMS の InfoObject が更新されたことを示すツールヒントが表示されます。
15. 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。**[バージョンのコピーを取得]** をクリックすると、選択したリソースのコピーを取得できます。

i 注記

[バージョンを取得] または **[バージョンのコピーを取得]** オプションのいずれかを使用すると、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。

16. リソースを選択してから  をクリックし、リソース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 4 ~ 16 を実行することができます。

15.4.1 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。選択し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。

15.4.2 サブバージョンファイルのバックアップと復元

この節では、サブバージョン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。

15.4.2.1 サブバージョンファイルのバックアップ

サブバージョンファイルをバックアップするには、次の手順を完了します。

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。

15.4.2.2 サブバージョンファイルの復元

サブバージョンファイルを復元するには、次の手順を完了します。

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。

i 注記

▶ LCM ▶ 管理オプション ▶ VMS 設定 ▶ サブバージョン ▶ で、[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。

i 注記

▶ LCM ▶ 管理オプション ▶ VMS 設定 ▶ サブバージョン ▶ で、[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。

15.5 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を使用すると、SAP BusinessObjects Business Intelligence プラットフォームデプロイメントからコマンドラインの入力を介して、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できます。

プロモーションマネジメントツールでは、コマンドラインオプションを介して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 LCM 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 LCM ジョブテンプレートの LCMBIAR へのエクスポート
- 既存のジョブテンプレートを使用した昇格
- 既存の LCMBIAR のインポートおよび昇格
- 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
- Live-to-Live 昇格の実行

15.5.1 Windows でのコマンドラインオプションの実行

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. 次のいずれかの操作を行います。
 - 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>`

i 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 SAP BusinessObjects Business Intelligence 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などが含まれています。

ファイルは、<ファイル名>.properties の形式で書かれている必要があります。

例: **<Myproperties.properties>**

15.5.2 UNIX でのコマンドラインオプションの実行

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_40/java/lib

3. 次のいずれかの操作を行います。

- 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>

i 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。

15.5.3 コマンドラインオプションのパラメータ

次の表に、プロモーションマネジメントアプリケーションのコマンドラインオプションのパラメータと、指定可能な値を示します。

パラメータ	指定可能な値	説明	必須またはオプション
action	Export、Promote 例: action=export	<p>このオプションでは、CLI で実行する必要のある操作を指定できます。この操作では、次の操作を実行できます。</p> <ul style="list-style-type: none">● オブジェクトを、LCMBIAR ファイルまたはプロモーションマネジメントジョブから SAP BusinessObjects Business Intelligence プラットフォームシステムに昇格します。● オブジェクトを SAP BusinessObjects Business Intelligence platform システムから LCMBIAR ファイルにエクスポートします。	必須

パラメータ	指定可能な値	説明	必須またはオプション
exportLocation	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	このパラメータでは、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できます。	action=export の場合は必須
importLocation	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	このパラメータでは、昇格されるオブジェクトを含む LCMBIAR ファイルの場所を指定できます。	action=promote の場合は必須
LCM_CMS	自由形式のテキスト。 例: LCM_CMS=<CMS 名:ポート番号>	このパラメータでは、プロモーションマネジメントアプリケーションの CMC を指定できます。	action=promote または export の場合は必須
LCM_userName	自由形式のテキスト。 例: LCM_userName=<ユーザ名>	このパラメータでは、ツールがプロモーションマネジメントアプリケーション CMS に接続する際に使用する必要のあるアカウントのユーザ名を指定できます。 i 注記 委任管理者がサポートされています。	action=promote または export の場合は必須
LCM_password	自由形式のテキスト。 例: LCM_password=<パスワード>	このパラメータでは、ユーザアカウントのパスワードを指定できます。	action=promote または export の場合は必須
LCM_authentication	secEnterprise、secWinAD、secLDAP、secSAPR3 例: LCM_authentication=<認証>	このパラメータは、使用される認証の種類を示します。	オプション。認証の種類を指定しない場合は、secEnterprise が使用されます。
LCM_systemID	システム ID	このパラメータは SAP 認証に使用されます。	SAP 認証の場合は必須

パラメータ	指定可能な値	説明	必須またはオプション
	例: LCM_systemID=<システム ID>		
LCM_clientID	クライアント ID 例: LCM_clientID=<クライアント ID>	このパラメータは SAP 認証に使用されます。	SAP 認証の場合は必須
Source_CMS	自由形式のテキスト。 例: Source_CMS=<CMS 名:ポート番号>	このパラメータでは、ツールが接続する必要がある CMC を指定できます。	action=export の場合は必須
Source_userName	自由形式のテキスト。 例: Source_username=<ユーザ名>	このパラメータでは、ツールが SAP BusinessObjects Business Intelligence platform CMS に接続する際に使用する必要があるユーザアカウントを指定します。 i 注記 委任管理者がサポートされています。	action=export の場合は必須
Source_password	自由形式のテキスト。 例: Source_password=<パスワード>	このパラメータでは、関連するユーザアカウントのパスワードを指定します。	action=export の場合は必須
Source_authentication	secEnterprise、secWinAD、secLDAP、secSAPR3 例: Source_authentication=<認証>	このパラメータは、使用される認証の種類を示します。	オプション。認証の種類を指定しない場合は、secEnterprise が使用されます。
Source_systemID	SAP システム ID 例: Source_systemID=<システム ID>	このパラメータは SAP 認証用にのみ使用されます。	SAP 認証の場合は必須
Source_clientID	SAP クライアント ID 例: Source_clientID=<クライアント ID>	このパラメータは SAP 認証用にのみ使用されます。	SAP 認証の場合は必須

パラメータ	指定可能な値	説明	必須またはオプション
Destination_userName	自由形式のテキスト。 例: Destination_username= <ユーザ名>	このパラメータでは、ツールが SAP BusinessObjects Business Intelligence Platform 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を指定します。 i 注記 委任管理者がサポートされています。	action=promote の場合は必須
Destination_password	自由形式のテキスト。 例: Destination_password= <パスワード>	このパラメータでは、関連するユーザアカウントのパスワードを指定します。	action=promote の場合は必須
Destination_authentication	secEnterprise、secWinAD、secLDAP、secSAPR3 例: Destination_authentication=<認証>	このパラメータは、使用される認証の種類を示します。	オプション。認証の種類を指定しない場合は、secEnterprise が使用されます。
Destination_systemID	システム ID 例: Destination_systemID= <システム ID>	このパラメータは SAP 認証用にのみ使用されます。	SAP 認証の場合は必須
Destination_clientID	クライアント ID 例: Destination_clientID= <クライアント ID>	このパラメータは SAP 認証用にのみ使用されます。	SAP 認証の場合は必須
includeSecurity	false、true 例: includeSecurity=<true または false>	このパラメータでは、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。	オプション。指定しない場合は、デフォルトの false が使用されます。 action=promote または export の場

パラメータ	指定可能な値	説明	必須またはオプション
			合に使用されます。
JOB_CUID	保存された LCM ジョブの CUID	このパラメータでは、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。	オプション。 action=export または promote の場合に使用されます。
exportQuery	<p>自由形式のテキスト。CMS クエリ言語形式を使用します。</p> <p>例:</p> <pre>exportQuery1=select*from ci_infoobjects where si_name='Xtreme Employees' and si_kind='Webi'</pre> <div> <p>i 注記</p> <p>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 などの名前を付ける必要があります。</p> </div>	エクスポート対象のオブジェクトを収集するためにツールで実行するクエリです。	オプション。 action=export の場合に使用されます。
exportQueriesTotal	<p>正の整数。</p> <p>exportQueriesTotal=<整数></p>	このパラメータでは、実行するエクスポートクエリの数を指定できます。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。	オプション。 action=export の場合に使用されます。 指定しない場合は、デフォルトの 1 が使用されます。
stacktrace	<p>true または false</p> <p>例: stacktrace=<true または false></p>	このパラメータにより、すべての呼び出しを追跡できます。	オプション。指定しない場合は、デフォルトの false が使用されます。
lcmbiarpassword	自由形式のテキスト。	このパラメータでは、パスワードを使用して、BIAR ファイ	オプション。指定しない場合、

パラメータ	指定可能な値	説明	必須またはオプション
	例: java -jar upgradeManagementTool .jar -mode livetobiar -biarfile "C:\TEMP \abc.biar" - lcmbiarpassword "testpassword"	ルの暗号化と解読が行えます。	または文字列が空の場合、暗号化されなことを意味します。
lcmproperty	プロパティファイルが保存されている場所の完全パス。 lcm_cli.bat - lcmproperty <プロパティファイルのファイルパス>	このパラメータは、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。	必須
consolelog	true または false	このパラメータは、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。	オプション

i 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_<ユーザ>_<タイムスタンプ> 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。
- LCMBIAR ファイル名が **<exportLocation>** ファイルに指定されていない場合、エクスポートされた LCMBIAR ファイルの命名規則は、<ジョブ名>_<タイムスタンプ>.lcmbiar という一意の組み合わせになります。
- ジョブは、プロモーションマネジメントアプリケーション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。

15.5.4 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>
lcmbiarppassword=<パスワード>
```

i 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。

15.6 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。

SAP BusinessObjects Business Intelligence platform (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 BusinessObjects Business Intelligence 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/3b/dfba3692dc635ce10000009b38f839/frameset.htm を参照してください。

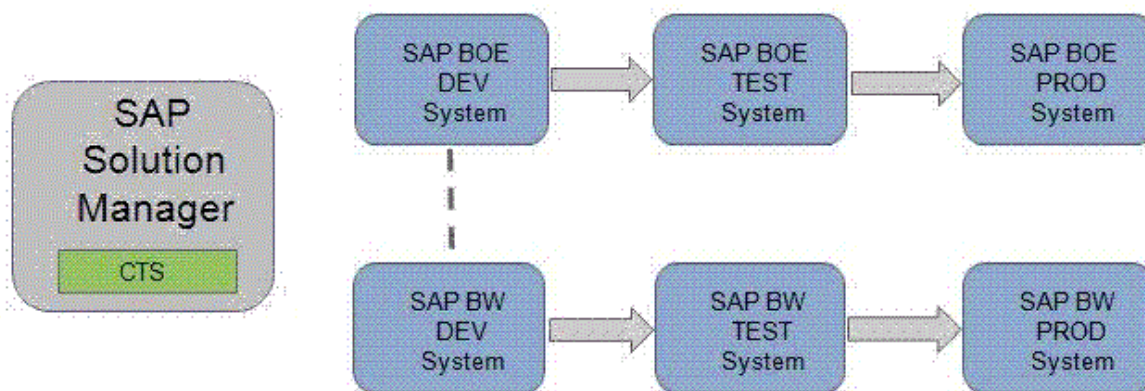
CTS+ および非 ABAP 移送の詳細については、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bb/6fab6036a146baa58e42fac032ab7b/frameset.htm を参照してください。

15.6.1 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. SAP BusinessObjects Business Intelligence プラットフォーム 4.0 (BI プラットフォーム) 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0a77acc11d1899e0000e829fbbd/frameset.htm 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、SAP ノート (<https://service.sap.com/sap/support/notes/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、SAP ノート (<https://service.sap.com/sap/support/notes/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。

15.6.2 Business Intelligence プラットフォームと CTS+ との統合の設定



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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0137acc11d1899e0000e829fbbd/frameset.htm 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0137acc11d1899e0000e829fbbd/frameset.htm を参照してください。

CTS 移送要求を使用して、SAP BusinessObjects Business Intelligence 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。

i 注記

Business Intelligence 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。

関連リンク

[CTS エクスポート Web サービスの有効化](#) [ページ 483]

[プロモーションマネジメントツールでの CTS+ の設定](#) [ページ 483]

[Business Intelligence プラットフォームと CTS+ との統合の設定](#) [ページ 482]

15.6.2.1 CTS エクスポート Web サービスの有効化

BI プラットフォームシステムを設定するには、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。
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、SAP ヘルプポータルにある http://help.sap.com/saphelp_nw70ehp1/helpdata/en/33/06820d9d174c2884576bd78ac5629d/frameset.htm を参照してください。
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。
2. [\[Service Administration\]](#) タブで、[\[Single Service Configuration\]](#) を選択します。
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替のアクセス URL を定義します。

15.6.2.2 プロモーションマネジメントツールでの CTS+ の設定

この節では、CTS+ を設定するために CMC アプリケーションで実行する設定手順（プロモーションマネジメントツールの用法）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. **[保存]** 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。

i 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。

i 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 ソースシステムで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 <SAP BusinessObjects Business Intelligence プラットフォームインストールパス>/SAP BusinessObjects Business Intelligence プラットフォーム 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 BusinessObjects Business Intelligence platform 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 BusinessObjects Business Intelligence platform 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>**

次はその例です。

DEWDFTH04171S@6400=WJ3

10.208.112.177@6400=WJ3

DEWDFTH04171S.pgdev.sap.corp@6400=WJ3

i 注記

クラスタ環境の場合、LCM_SOURCE_CMS_SID_MAPPING.properties ファイルと LCM_SID_RFC_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、http://help.sap.com/saphelp_nw70/helpdata/en/d4/3bab83106941f08ad1f2e1ec14375e/frameset.htm を参照してください。

15.6.2.3 SAP Solution Manager での Business Intelligence プラットフォームインポートシステムの設定

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 `sstms` 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、SAP BusinessObjects Business Intelligence platform 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。

i 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm (http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm) を参照してください。

6. 次の手順を完了して、CTS+ で SAP BusinessObjects Business Intelligence platform インポートシステムを設定します。

i 注記

SAP BusinessObjects Business Intelligence 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm (http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm) 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 URI を入力します。`http://<BOE (http://%3cboe/) web server name>:<Webserver port>/BOE/LCM/CTSServlet?&cmsName=<BOE destination name>:<CMSport>&authType=<BOE authentication type>`
それぞれの項目の意味は次のとおりです。
 - 「BOE web server name」は、Business Intelligence 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、Business Intelligence プラットフォームアプリケーションサーバのポート番号です。
 - 「BOE destination name」は、Business Intelligence 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、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、Business Intelligence 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、Business Intelligence 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a1df7acc11d1899e0000e829fbbd/frameset.htm を参照してください。

15.6.3 CTS を使用したジョブの昇格

この節では、プロモーションマネジメントアプリケーションでサポートされている、SAP BusinessObjects Business Intelligence 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アプリケーションを起動し、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。

i 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+ と昇格] 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 を選択してから、[追加] をクリックします。InfoObject を 1 つ追加して [オブジェクトの追加] 画面を終了するには、[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。

i 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. ログイ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インします。
 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/b5/6d03660d3745938cd46d6f5f9cef2e/frameset.htm 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。

i 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 SAP BusinessObjects Business Intelligence platform 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 SAP BusinessObjects Business Intelligence 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/55/07c497db8140ef8176715d4728eec1/frameset.htm 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。

i 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 SAP BusinessObjects Business Intelligence platform 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 LCM 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm 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一般的な情報については、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/09/ca0f3a878f46e9a5a32e666131d2ba/frameset.htm 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インします。
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。

i 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インします。
2. 移送管理システムに入るには、SIMS 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm 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、http://help.sap.com/saphelp_nw70ehp1/helpdata/en/65/8a99386185c064e10000009b38f8cf/frameset.htm を参照してください。

16. 出力先システムにログインして、昇格したジョブのステータスを表示します。

Generic CTS のオンラインマニュアルについては、http://help.sap.com/saphelp_ctsplug100/helpdata/en/52/700dbe608e4752a8e2e96a1876f865/frameset.htm を参照してください。

関連リンク

[ジョブの作成](#) [ページ 457]

[プロモーションマネジメントでの依存関係の管理](#) [ページ 461]

16 差分の視覚化

16.1 プロモーションマネジメントツールの Visual Difference

Visual Difference では、サポートされるファイルタイプ (LCM BIAR) またはサポートされるオブジェクトタイプ (LCM ジョブ) またはその両方で 2 つのバージョン間の差分を表示できます。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的確に評価できます。

Visual Difference では、ファイルまたはオブジェクトをから次の 3 種類の差分を検出できます。

- 削除済み - どちらかのバージョンのファイルに要素が見つからない場合、この種の差分はレポートに削除済みと表示されます。たとえば、行、セクションのインスタンス、またはブロックなどの要素が見つからない場合があります。
- 変更済み - 比較元バージョンと比較先バージョン間で異なる値が存在する場合、この種の差分はレポートに変更済みと表示されます。たとえば、セルの内容やローカル変数の結果などの値が異なる場合があります。
- 挿入済み - 比較先バージョンに存在する要素が比較元バージョンに存在しない場合、この種の差分はレポートに挿入済みと表示されます。

Visual Difference がサポートされるオブジェクトタイプは次のとおりです。

- LCMBIAR
- LCM ジョブ

比較は次の組み合わせで行うことができます。

- LCM ジョブと別の LCM ジョブ
- LCM ジョブと LCMBIAR ファイル
- LCMBIAR ファイルと別の LCMBIAR ファイル
- LCMBIAR ファイルと LCM ジョブ

基本設定

Visual Difference ホームページでは、製品ロケール、優先表示ロケール、ページごとの最大オブジェクト数、タイムゾーン、保存されていないデータを確認するかどうかなどの基本設定を選択できます。

ホーム ページ

Visual Difference ホームページは、次のタブおよび枠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] 枠 - この枠には、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] 枠 - この枠には、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。

16.1.1 Visual Difference を使用してのオブジェクトまたはファイルの比較

Visual Difference オプションを使用して、BIAR ファイルとオブジェクトを比較することができます。

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 ページが開きます。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いずれかのサブフォルダに保存されています。

i 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] 内の [システムの選択] から、参照システムを選択します。
以下の参照システムのいずれかに接続できます。
 - CMS
 - VMS
 - ローカルファイルシステム
5. [参照] をクリックして、比較するローカルシステムからオブジェクトまたはファイルを選択します。
6. ターゲットの下にある [システムの選択] からターゲットシステムを選択します。
以下の参照システムのいずれかに接続できます。
 - CMS
 - VMS
 - ローカルファイルシステム

i 注記

CMS または VMS にログインすると、参照システム内の選択したオブジェクトを、参照システム内の同じ名前を持つオブジェクトと自動的にマッチングすることもできます。

7. [参照] をクリックして、比較するローカルシステムから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。
比較のために選択されたオブジェクトが、ショッピングカートに追加されます。

ショッピングカートに複数のオブジェクトペアが追加された場合は、後でオブジェクトを比較するようスケジュールできます。ただし、ショッピングカートにオブジェクトが 1 ペアしかない場合も、これらのオブジェクトを比較できます。

ファイルを比較するには、続けて次の手順に従います。比較をスケジュールするには、[比較のスケジュール](#) [ページ 493]を参照してください。

9. [\[比較\]](#) をクリックして、オブジェクトまたはフォルダを比較します。

i 注記

LCMBIAR/LCM ジョブファイルでは次のような比較が行われます。

- LCMBIAR メタデータ: 名前、作成者、時刻など、ジョブの詳細の比較。
- 一次オブジェクト: 明示的に選択された LCMBIAR ファイル内の各オブジェクトと、CUID で指定されたターゲットの LCMBIAR ファイル内の類似オブジェクトとの比較。
- 依存オブジェクト: ファイル内の選択された依存オブジェクトと、CUID で指定されたターゲットファイル内の類似オブジェクトとの比較。

LCMBIAR または LCM ジョブ以外のオブジェクトが選択された場合は、「プラグインが見つかりません。」というエラーメッセージが表示されます。

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。

16.1.2 バージョン管理システム内のオブジェクトまたはファイルの比較

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オブジェクトまたはファイル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 ページが開きます。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いずれかのサブフォルダに保存されています。

i 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、**新しい比較枠**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。比較をスケジュールするには、[比較のスケジュール](#) [ページ 493]を参照してください。
9. [\[比較\]](#) をクリックして、オブジェクト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。

16.1.3 比較のスケジュール

ファイルまたはオブジェクトの比較をスケジュールするには、次の手順に従います。

1. [\[スケジュール\]](#) をクリックします。
[\[スケジュール\]](#) ウィンドウが表示されます。
2. [\[比較の実行\]](#) リストから比較スケジュールの間隔を選択します。
3. 可能な再試行回数、および対応するフィールドでの試行間隔を指定します。

i 注記

再試行回数を指定する場合のみ、試行間隔を指定することができます。

4. レポート名を指定し、[\[参照\]](#) をクリックしてレポートを保存する場所を探します。
[\[ジョブの保存場所\]](#) ウィンドウが表示されます。
5. レポートを保存する必要なフォルダを選択し、[\[OK\]](#) をクリックします。

i 注記

[\[比較の実行\]](#) リストから選択するオプションに応じて、比較の日時をそれぞれ指定する必要があります。

6. [\[スケジュール\]](#) をクリックします。
ユーザは後で、Visual Difference ビューアに比較オブジェクトまたは相違レポートを表示することができます。[\[比較済み: 差\]](#) ページに、フォルダおよびファイルの一覧または比較レポートが表示されます。
[\[比較後の相違点\]](#) ページには、次のオプションも含まれます。
 - **履歴:** [\[履歴\]](#) オプションでは比較の履歴を表示することができます。
 - **再実行:** [\[再実行\]](#) オプションは比較を再度実行します。
 - **スケジュール:** [\[スケジュール\]](#) オプションでは比較をスケジュールすることができます。

17 アプリケーションの管理

17.1 CMC を介したアプリケーションの管理

17.1.1 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 起動パッドのような 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。

- Analysis edition for OLAP
- アラートアプリケーション
- BI 起動パッド
- BI ワークスペース
- セントラル管理コンソール
- Crystal Reports 設定
- ダッシュボード
- ディスカッション
- インフォメーションデザイナー
- Web Intelligence
- プロモーションマネジメント
- モニタリングアプリケーション
- OpenDocument
- プラットフォーム検索アプリケーション
- レポート変換ツール
- SAP BusinessObjects Mobile
- SAP StreamWork
- 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
- アップグレードマネジメントツール
- 差分の視覚化
- Web サービス
- ウィジェット

17.1.2 アプリケーションの共通設定

17.1.2.1 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 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。

17.1.2.2 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

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 起動パッド
- OpenDocument
- Web サービス
- プロモーションマネジメント
- バージョン管理
- 差分の視覚化

他のすべての Web アプリケーションをトレースするには、手動の方法を使用して対応する BO_trace ファイルを設定してください。

1. CMC の [\[アプリケーション\]](#) 管理エリアを表示します。
[\[アプリケーション\]](#) ダイアログボックスが表示されます。
2. 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。
[\[トレースログを設定\]](#) ダイアログボックスが表示されます。
3. [\[ログレベル\]](#) リストから必要な設定を選択します。
4. [\[保存して閉じる\]](#) をクリックして、トレースログレベルを送信します。

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。

関連リンク

[トレースログレベル](#) [ページ 495]

17.1.2.2.1 トレースログレベル

次の表では、BI プラットフォームコンポーネントに対し使用できるトレースログレベルを説明します。

レベル	説明
未指定	トレースログレベルは他のメカニズム (通常は .ini ファイル) を介して指定されます。
なし	<p>トレースログレベルが [なし] に設定されている場合、指定した重要度レベルを下回るトレースをオプションとして抑制するフィルタが無効になります。</p> <p>i 注記</p> <p>[なし] トレースログレベルは、トレース機能がオフになっているという意味ではありません。システムリソースのモニタリングは続けられ、アサーションの失敗など発生頻度の低い重要なイベントに対してはトレースが記録されます。</p>
低	<p>エラーメッセージは記録するが、警告やステータスメッセージの多くを無視するようトレースログフィルタが設定されます。ただし、非常に重要なステータスメッセージは、コンポーネントの起動、シャットダウン、またはリクエストメッセージの開始や終了時にも記録されます。</p> <p>i 注記</p> <p>このレベルは、デバッグ目的の場合はお勧めしません。</p>
中	<p>エラー、警告、ステータスメッセージの多くをログ出力に含めるよう、トレースログフィルタが設定されます。重要性が最小、または詳細度が高いステータスメッセージは除外されます。このレベルは、デバッグ目的には詳細度が足りません。</p>
高	<p>フィルタによって除外されるメッセージはありません。このレベルは、デバッグ目的の場合にお勧めします。</p> <p>i 注記</p> <p>トレースログレベルを [高] にすると、システムリソースに悪影響を与えることがあります。CPU 利用率やファイルシステム内の保存スペースが増加することがあります。</p>

17.1.3 アプリケーション固有の設定

17.1.3.1 CMC アプリケーション設定の管理

17.1.3.1.1 認証およびプログラムオブジェクト

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。

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。

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、BI プラットフォーム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。

i 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 [\[セントラル管理コンソール\]](#) 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入力します。

Java プログラムの認証

BI プラットフォームでは、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、BI プラットフォームは 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が含まれています。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、BI プラットフォーム 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 BI プラットフォーム .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。

i 注記

Java Policy の設定は、同じコンピュータで実行されているすべての Adaptive Job Server で共通です。

i 注記

デフォルトでは、Java Policy File は BI プラットフォーム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ています。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。

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、Business Intelligence プラットフォーム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。

17.1.3.1.2 処理拡張機能のシステムへの登録

i 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\win32_x86\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。

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>/<file_name>」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、そのロジックをオブジェクトに適用できます。

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

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。これを行うには、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。

17.1.3.1.3 CMC タブアクセスの管理

委任管理および CMC タブへのアクセス

通常、Business Intelligence 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。

関連リンク

[他のユーザに対して CMC タブアクセスを管理する \[ページ 501\]](#)

[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 \[ページ 503\]](#)

CMC タブアクセスの操作

他のユーザに対して CMC タブアクセスを管理する

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。次の CMC タブで、最上位フォルダがサポートされます。[アクセスレベル](#)、[カレンダー](#)、[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](#)、[プロフィール](#)、[レプリケーション一覧](#)、[サーバ](#)、[一時記憶領域](#)、[ユニバース](#)、[ユーザとグループ](#)、および [Web サービスクエリ](#)
- システムセキュリティを改善するため、CMC タブ [\[監査\]](#)、[\[認証\]](#)、[\[暗号化キー\]](#)、[\[ライセンスキー\]](#)、[\[モニタリング\]](#)、[\[セッション\]](#)、[\[設定\]](#)、および [\[ユーザ属性管理\]](#) には、管理者グループのメンバーのみがアクセスできます。管理者グループのメンバーは、システム管理者として、CMC タブのアクセス権に関係なくすべての CMC タブにアクセスできます。CMC タブのアクセス権は、代理の管理者に対して CMC タブへのアクセスを管理することを目的としています。代理の管理者とは、管理者グループのメンバー以外のユーザです。

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。

1. CMC にログインします。
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無制限です。以下の設定は、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 へのアクセスを制限するには、[\[アプリケーション\]](#) タブに移動して [\[CMC\]](#) 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。

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。

i 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。

関連リンク

[To restrict CMC tab access](#) [ページ 503]

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 Business Intelligence 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。

i 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。

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。

i 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	[カレンダー] 、 [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] 、 [プロフィール] 、 [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。

委任管理者ユーザグループ	推奨される権限
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。

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 Business Intelligence 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 にログインします。
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。

関連リンク

[CMC タブへのアクセス問題を解決する](#) [ページ 504]

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 にログインします。
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 タブへのアクセスの設定] 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。

i 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。

関連リンク

[委任管理および CMC タブへのアクセス](#) [ページ 500]

[CMC タブへのアクセスの継承](#) [ページ 502]

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. システム管理者として 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。
[\[CMC タブへのアクセスの設定\]](#) 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。

関連リンク

[他のユーザに対して CMC タブアクセスを管理する](#) [ページ 501]

[CMC タブへのアクセスの継承](#) [ページ 502]

17.1.3.2 ディスカッション設定の管理

BI プラットフォームの CMC の [\[アプリケーション\]](#) エリアで、ディスカッションスレッドのシステムレベルの設定を指定できます。

[ディスカッション](#) アプリケーションでは、以下のいくつかの方法でディスカッションスレッドを管理し、ディスカッションスレッドを操作できます。

- 指定した検索条件に従ってディスカッションスレッドを検索する
- ディスカッションスレッドの検索結果を並べ替える
- ディスカッションスレッドを削除する

i 注記

ユーザのアクセス権の設定は、ディスカッションアプリケーションでは使用できません。ただし、個々のレポートに対するアクセス権は設定できます。

17.1.3.2.1 ディスカッションスレッドを検索する

デフォルトでは、[\[ディスカッション\]](#) ページにすべてのディスカッションスレッドのタイトルが表示されます。ルートレベルのスレッドだけが表示され、

ディスカッションスレッドのリスト内のページを移動するには、[\[戻る\]](#) ボタンおよび [\[次へ\]](#) ボタンをクリックします。特定のスレッドまたはスレッドのグループを検索することもできます。

1. CMC の [\[アプリケーション\]](#) エリアに移動し、[\[ディスカッション\]](#) を選択します。
2. [管理 > スレッドの管理](#) をクリックします。
[\[メモの管理\]](#) ダイアログボックスが表示されます。
3. [\[フィールド名\]](#) リストからオプションを選択します。

オプション	説明
スレッドタイトル	スレッドタイトルを指定して検索します
作成日	作成日を指定して検索します
最終更新日	最終更新日を指定して検索します
作成者	作成者を指定して検索します

4. 2 つ目のリストで、検索対象を絞ります。

i 注記

検索では大文字と小文字が区別されません。

- [スレッドタイトル]または[作成者]を選択した場合は、2 つ目のフィールドで次のオプションを選択します。

オプション	説明
である	スレッドタイトルまたは作成者名が、3 つ目のフィールドに入力したテキストと正確に一致するディスカッションスレッドを検索します
でない	スレッドタイトルまたは作成者名が、3 つ目のフィールドに入力したテキストと正確に一致しないディスカッションスレッドを検索します
を含む	スレッドタイトルまたは作成者名の一部に検索対象のテキスト文字列が含まれるディスカッションスレッドを検索します
を含まない	スレッドタイトルの一部に検索対象のテキスト文字列が含まれないディスカッションスレッドを検索します


- [作成日]または[最終更新日]で検索する場合は、次のオプションの中から選択し、日付を指定します。

オプション	説明
以前	検索日より前に作成または変更されたディスカッションスレッドを検索します
以降	検索日より後に作成または変更されたディスカッションスレッドを検索します
の間	2 つの検索日の間に作成または変更されたディスカッションスレッドを検索します

5. 検索対象をさらに絞るには、3 つ目のテキストフィールドを使用します。
 - 最初の 2 つのフィールドでテキストベースの検索を選択した場合は、テキスト文字列を入力します。
 - 日付ベースの検索を選択した場合は、該当フィールドに 1 つまたは複数の日付を入力します。
6. [検索]をクリックします。

17.1.3.2.2 ディスカッションスレッドの検索結果を並べ替える

ディスカッションスレッドを検索する場合は、検索結果を表示する方法を選択できます。たとえば、検索結果を昇順のアルファベット順で表示したり、1 ページに表示する結果の数を選択できます。

1. CMC の[アプリケーション]エリアに移動し、[ディスカッション]を選択します。
2.  **管理** > **プロパティ** をクリックします。
[メモの管理] ダイアログボックスが表示されます。
3. [並べ替え基準]リストから並べ替えオプションを選択します。

オプション	説明
スレッドタイトル	ディスカッションスレッドのタイトル別に並べ替えます。
作成日	スレッドの作成日別に並べ替えます。
最終更新日	ディスカッションスレッドが最後に更新された日付に基づいて並べ替えます。

オプション	説明
作成者	特定のディスカッションスレッドの作成者別に並べ替えます。

- 2 つ目のリストで、レコードを昇順と降順のどちらで表示するか選択します。
- 3 つ目のテキストフィールドに、1 ページに表示するディスカッションスレッドの結果の数を入力します。
デフォルトは、1 ページにつき 10 の結果です。
- [検索]をクリックします。

17.1.3.2.3 ディスカッションスレッドを削除する

ディスカッションスレッドは、BI プラットフォームの CMC の [アプリケーション] エリアで削除できます。

- CMC の [アプリケーション] エリアに移動し、[ディスカッション] を選択します。
- ▶ 管理 ▶ スレッドの管理 ▶ をクリックします。
[メモの管理] ダイアログボックスが表示されます。
- 結果リストで、削除するディスカッションスレッドを探して選択します。
- [削除] をクリックします。

17.1.3.3 BI 起動パッド設定の管理

BI プラットフォームの CMC の [アプリケーション] エリアで、▶ 管理 ▶ プロパティ ▶ を選択して BI 起動パッドの表示オプションを変更できます。

BI 起動パッドでは、ユーザまたはグループに以下の操作を許可することができます。



- 基本設定を変更する
- フォルダを整理する
- 検索
- オブジェクトタイプに従ってオブジェクトのリストをフィルタリングする
- [お気に入り]フォルダを表示する

たとえば、標準的な命名規約に従ってすでにユーザのフォルダを作成している場合は、ユーザが自分たちのフォルダを編成することを禁止することができます。

i 注記

デフォルトでは、すべてのユーザがこれらの機能にアクセスすることができます。



17.1.3.3.1 BI 起動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 起動パッド] を選択します。
2.  **管理** > **プロパティ**  をクリックします。
[BI 起動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。
3. BI 起動パッドのユーザに対してディスカッションを有効化するには、[ディスカッションの有効化] を選択します。
4. スケジュールのフィルタ機能を有効化するには、[[スケジュール] ページに [フィルタ] タブを表示する] 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。
5. [保存して閉じる] をクリックします。

17.1.3.4 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。

17.1.3.4.1 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
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。
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。

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。

17.1.3.5 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

関連リンク

[アプリケーションに対するユーザアクセス権の設定](#) [ページ 495]

[アラート設定の管理](#) [ページ 509]

17.1.3.5.1 アラートの出力先プロパティを変更する

1. CMC の [\[アプリケーション\]](#) エリアに移動し、[\[アラートアプリケーション\]](#) を選択します。
2.  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. 適切なオプションを設定します。

オプション	説明
[マイアラートの有効化]	アラート購読者が BI 起動パッドの [マイアラート] セクションで通知を受信できるようにする場合は、このオプションを選択します。
電子メールを有効にする	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、このオプションを選択します。このオプションを選択すると、アラートのグローバル電子メール設定が表示されます。

注記

上記の出力先オプションのうち、いずれかまたは両方を指定する必要があります。

[\[電子メールを有効にする\]](#) を選択した場合は、次のグローバル設定を変更できます。

オプション	説明
差出人	アラート通知の送信元の電子メールアドレスを指定します。購読者は指定した送信者からの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することをお勧めします。
宛先	アラート購読者の電子メールアドレスを指定します。

オプション	説明
	<p>➡ ヒント</p> <p>この設定の %SI_EMAIL_ADDRESS% プレースホルダを保持しておくことをお勧めします。特定の電子メールアドレスや受信者を指定すると、デフォルトではすべてのシステムアラートが指定した電子メールアドレスに送信されます。</p>
CC	電子メールで送信されるアラートのカーボンコピーの受信者を指定します。
件名	システムアラートを含む電子メールで使用される、デフォルトの件名の見出しを指定します。
メッセージ	システム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指定します。
添付ファイルの追加	システム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、このオプションを選択します。このオプションは通常、発生したアラートに関連する Crystal Reports をデフォルトで含める場合に使用されます。
ファイル名	[添付ファイルの追加]オプションを選択した場合は、[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の名前の付け方を指定します。

4. [保存して閉じる]をクリックします。

関連リンク

[アプリケーションに対するユーザアクセス権の設定](#) [ページ 495]

[アラート設定の管理](#) [ページ 509]

17.1.3.5.2 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 ▸ をクリックします。
[プロパティ] ページが開きます。
3. [デフォルト設定] をクリックします。
4. 次のプロパティの値を設定します。

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。

5. [保存して閉じる]をクリックします。

関連リンク

[CMC でのオブジェクトのセキュリティ設定の管理](#) [ページ 108]

[アラート設定の管理](#) [ページ 509]

17.1.3.6 ウィジェット設定の管理

SAP BusinessObjects 向けウィジェットは、ユーザがデスクトップにミニアプリケーションを追加するために使用できるデスクトップアプリケーションです。ユーザは、SAP NetWeaver Application Server の BI プラットフォームおよび Web Dynpro アプリケーションにある企業のビジネスインテリジェンスコンテンツに容易にアクセスできるようになります。

CMC の [アプリケーション] エリアでは、ユーザのデスクトップでウィジェットを作成したり、使用したりするためのユーザアクセス権と、デスクトップ上のウィジェットアプリケーションから BI プラットフォームリポジトリを検索する操作を制御できます。

ユーザまたはグループに以下の操作を許可することができます。

- ウィジェットを使用する
- ウィジェットで作成したオブジェクトを編集する
- オブジェクトにアクセスするためのユーザ権限を変更する

i 注記

デフォルトでは、すべての一般ユーザがこうした機能にアクセスできます。

関連リンク

[CMC でのオブジェクトのセキュリティ設定の管理](#) [ページ 108]



17.1.3.7 SAP BusinessObjects Explorer 設定の管理

SAP BusinessObjects Explorer でユーザがアクセスできる機能を定義するには、CMC の [アプリケーション] エリアで SAP BusinessObjects Explorer のセキュリティ権限を設定します。

関連リンク

[CMC でのオブジェクトのセキュリティ設定の管理](#) [ページ 108]

17.1.3.7.1 SAP BusinessObjects Explorer アプリケーションプロパティを修正する

1. CMC の[アプリケーション]エリアを表示します。
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 SAP BusinessObjects Explorer 設定を定義します。
 - デフォルトのインデックスフォルダの場所
 - スレッド数
 - ブックマークの有効性
4. [\[保存して閉じる\]](#) をクリックします。

17.1.3.8 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。

関連リンク

[インデックス処理失敗一覧](#)

[CMC でのアプリケーションプロパティの設定](#) [ページ 512]

17.1.3.8.1 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。[\[プロパティ\]](#) ダイアログボックスが表示されます。
4. 必要なプラットフォーム検索の設定を行います。
次の表で、設定可能なプロパティについて説明します。

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。 <ul style="list-style-type: none">○ 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、確認のダイアログボックスで [OK] 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] ページで指定したロケールを使用して、すべてのデフォルトの 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。
クロール頻度	以下のオプションを使用して、SAP BusinessObjects 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できます。

オプション	説明
	<ul style="list-style-type: none"> 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、継続的クロールでは SAP BusinessObjects BI プラットフォームリポトリは実行するアクションによって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。 <div data-bbox="638 786 1473 1173"> <p>i 注記</p> <ul style="list-style-type: none"> [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。 </div>
インデックスの場所	<p>インデックス処理されたドキュメントは、以下の場所にある共有フォルダに格納されます。</p> <ul style="list-style-type: none"> 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。ワークフローの検索中、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 SAP BusinessObjects 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。 <p>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、<code>{bobj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores</code> になります。</p>

オプション	説明
	<p>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になります。</p> <ol style="list-style-type: none"> 1. {boj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores 2. {boj.enterprise.home}\data\PlatformSearchData\workspace\Server1\ContentStores <ul style="list-style-type: none"> ○ 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。インデックス処理済されたドキュメント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。 <div data-bbox="496 815 1342 1061"> <p>i 注記</p> <ul style="list-style-type: none"> ○ すべてのインデックスの場所は、共有ロケーションである必要があります。 ○ 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。 </div>
インデックス処理のレベル	<p>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。</p> <ul style="list-style-type: none"> ○ 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。 ○ 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。 <ul style="list-style-type: none"> ○ 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 <div data-bbox="496 1621 1342 1767"> <p>i 注記</p> <p>インデックス処理のレベルを変更すると、SAP BusinessObjects 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。</p> </div>
コンテンツタイプ	<p>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。</p> <ul style="list-style-type: none"> ○ Microsoft Word ○ Microsoft Excel ○ Microsoft PowerPoint

オプション	説明
	<ul style="list-style-type: none"> ○ テキスト ○ Adobe Acrobat ○ リッチテキスト形式 ○ Crystal Reports ○ ユニバース ○ Web Intelligence
インデックスの再構築	<p>このオプションを使用して、インデックス処理されたすべての既存コンテンツを削除し、ドキュメント全体を初めから再インデックス処理することができます。</p> <p>インデックス処理のステータスに関係なく、[インデックスの再構築] オプションを選択できます。ただし、インデックス処理が停止している場合、[インデックスの再構築] オプションは機能しない可能性があります。[インデックスの再構築] を選択し、プラットフォーム検索アプリケーションを保存してから閉じてください。</p> <p>インデックス処理が停止していて [インデックスの再構築] を選択した場合は、プラットフォーム検索アプリケーションを保存し、閉じてから、設定ページを再度開き、[インデックス処理の開始] をクリックすると、保存された [インデックスの再構築] オプションによって、自動的にドキュメント全体が再インデックス処理される可能性があります。</p> <p>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] をクリックする必要があります。</p>
インデックス処理から除外するドキュメント	<p>[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。</p> <p>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。</p> <p>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] 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。</p> <ul style="list-style-type: none"> ○ 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

5. [\[保存して閉じる\]](#) をクリックします。

i 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初めから増分更新されます。

17.1.3.9 SAP StreamWork 統合の管理

BI プラットフォーム の CMC の [アプリケーション](#) エリアで、SAP StreamWork アプリケーションの統合の詳細情報を有効化および設定できます。SAP StreamWork Enterprise Agent に追加の設定を行う必要があります。詳細については、*Integrating SAP StreamWork with SAP BusinessObjects Business Intelligence Platform* を参照してください。

アプリケーションを適切に設定したら、BI 起動パッドで SAP StreamWork フィードを使用できるようになります。

17.1.3.9.1 SAP StreamWork 統合設定

SAP StreamWork 統合アプリケーションを設定するために 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
StreamWork 統合の有効化	このボックスをチェックすると、SAP StreamWork 統合アプリケーションが有効になります。
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に使用する値を入力します。この値は、SAP StreamWork 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られます。 i 注記 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、[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。SAP StreamWork 管理コンソールでこの証明書を使用して OAuth コンシューマキーを生成します。この証明書は、SAP StreamWork 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。
OAuth コンシューマキー	このフィールドを使用して、SAP StreamWork 管理コンソールで生成する有効な OAuth コンシューマキーを入力します。 i 注記 コンシューマキーの作成については、 <i>Integrating SAP StreamWork with SAP BusinessObjects Business Intelligence Platform</i> を参照してください。
プロキシを使用した接続	このボックスをチェックすると、プロキシ経由での接続が有効になります。[HTTP プロキシホスト] および [ポート] フィールドにプロキシホストに関する情報を指定する必要があります。 ➡ ヒント SAP StreamWork 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。

設定	説明
	<p>i 注記</p> <p>SSL 証明書プロバイダのトラステッド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。</p>
HTTP プロキシホスト	<p>リバースプロキシ設定では、SAP StreamWork からアクセス可能な外部アドレスを含める必要があります。たとえば、次のようなアドレスを使用できます。</p> <p><code>https://<ReverseProxy>/</code></p> <p>ここで、<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。</p> <p>SAP StreamWork ではこのアドレスを使用して、情報を BI プラットフォームに送信します。リバースプロキシはこのアドレスを使用して、SAP StreamWork から取得した情報を、SAP StreamWork Enterprise Agent を含むマシンにリダイレクトします。</p>
ポート	<p>SAP StreamWork Enterprise Agent は、ポート 8443 から受信するように設定されます。</p>

17.1.3.10 BEx Web 統合の設定

BEx Web アプリケーションは、データ分析、レポートティング、および Web 上の分析アプリケーションのための SAP NetWeaver 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ト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、レポートティング、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 BusinessObjects Business Intelligence プラットフォームの BI 起動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 SAP BusinessObjects Business Intelligence 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。

SAP BusinessObjects Business Intelligence 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保存することができます。

制約

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ト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。

SAP BusinessObjects Business Intelligence 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、BusinessObjects Business Intelligence 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。

SAP BusinessObjects Business Intelligence 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 BusinessObjects Business Intelligence 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>) ▶ [SAP NetWeaver 7.3](#) ▶ [SAP NetWeaver Library: Function-Oriented View](#) ▶ [Business Warehouse](#) ▶ [SAP Business Explorer](#) ▶ [BEx Web](#) ▶ [Analysis & Reporting: BEx Web Applications](#) ▶ を参照してください。

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。

関連リンク

[BEx Web アプリケーション用のサーバの開始](#) [ページ 519]

[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](#) [ページ 519]

[サーバの設定](#) [ページ 519]

[BW システムへの接続の確認](#) [ページ 520]

17.1.3.10.1 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) にログインします。
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. [BExWebApplicationsService] を [利用可能なサービス] 一覧から [AdaptiveProcessingServerServices] 一覧に移動します。
6. コンテキストメニューを使用して、BEx Web アプリケーションサービスを有効化し開始します。

17.1.3.10.2 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)にログインします。
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] ボックスで必要なサーバを選択します。
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] 一覧で、[BExWebApplicationsService] を選択して、[AdaptiveProcessingServerServices] 一覧に移動します。
8. コンテキストメニューを使用して、BEx Web アプリケーションサービスを有効化し開始します。

17.1.3.10.3 サーバの設定

1. セントラル管理コンソール(CMC)にログインします。
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、SAP BusinessObjects Business Intelligence 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。

関連リンク

[ABAP システムでの RFC 宛先の作成](#) [ページ 521]

17.1.3.10.4 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は、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 BusinessObjects Business Intelligence 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。

17.1.3.10.5 BEx Web Application Designer と BusinessObjects Business Intelligence 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 BusinessObjects Business Intelligence プラットフォームを統合するには、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 BusinessObjects Business Intelligence 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、BusinessObjects Business Intelligence 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、[[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。

関連リンク

[ABAP システムでの RFC 宛先の作成](#) [ページ 521]

ABAP システムでの RFC 宛先の作成

BW システムと BusinessObjects Business Intelligence 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 BusinessObjects Business Intelligence 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、BusinessObjects Business Intelligence 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 [ゲートウェイオブション] の下に、BusinessObjects Business Intelligence 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。

関連リンク

[サーバの設定](#) [ページ 519]

17.2 BOE.war プロパティを介したアプリケーションの管理

17.2.1 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。

i 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 ディレクトリ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。

17.2.1.1 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。
tree.pagesize	tree.pagesize=100	Web アプリケーションのナビゲーション枠に表示できるエントリの最大数を指定します。
trusted.auth.shared.secret		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		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。次のいずれかが設定できます。 <ul style="list-style-type: none">• Header• URL Parameter• Cookie• Session
trusted.auth.user.retrieval		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ます。次のいずれかが設定できます。 <ul style="list-style-type: none">• "REMOTE_USER"• "HTTP_HEADER"• "COOKIE"• "QUERY_STRING"• "WEB_SESSION"• "USER_PRINCIPAL"

設定	デフォルト値	説明
		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		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 <code>true</code> 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ーは 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。 <code>false</code> 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	<pre>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</pre>	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	<code>pinger.showWarningDialog.cmc=true</code>	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ボックスに表示するかどうかを指定します。
pinger.showWarningDialog.bi-launchpad	<code>pinger.showWarningDialog.bi-launchpad=true</code>	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ボックスに表示するかどうかを指定します。
pinger.warningPeriod.pingIncrementsInSeconds	<code>pinger.warningPeriod.pingIncrementsInSeconds=15</code>	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	<code>pinger.warningPeriod.lengthInMinutes=5</code>	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	<code>logoff.on.websession.expiry=true</code>	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	<code>pinger.enabled=true</code>	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	<code>system.com.sap.bip.jcomanager.destinations.maxsize=1000</code>	キャッシュされた Java 接続の最大数を指定します。

設定	デフォルト値	説明
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。

17.2.1.2 BI 起動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。この名前は、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ます。																		
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	アプリケーションの URL 名を、先頭に / (スラッシュ) 文字を付けて指定します。デフォルト: app.url.name=/BI																		
authentication.default	<p>アプリケーションで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。</p> <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> <p>デフォルト: authentication.default=secEnterprise</p>	認証	設定値	Enterprise	SecEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpsenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
認証	設定値																		
Enterprise	SecEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpsenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	BI 起動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																		

設定	説明
cms.default	デフォルトの CMS 名を指定します。デフォルト: cms.default=[ホストマシン名]
cms.visible	BI 起動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
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 起動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	BI 起動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 起動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 起動パッド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 BI 起動パッド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
enforceTopLevelFrame.enabled	BI 起動パッドのログオンページで、クロスサイトフレームのセキュリティの脆弱性を防ぐためにフレームの破棄を有効にするかどうかを指定します。有効にするには、true に設定します。デフォルト: enforceTopLevelFrame.enabled=true

17.2.1.3 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=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																		
authentication.default	<p>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。</p> <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>secpseenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel17</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </table> <p>デフォルト: authentication.default=secEnterprise</p>	認証	設定値	Enterprise	SecEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpseenterprise	JD Edwards	secPSE1	Siebel	secSiebel17	Oracles EBS	secOraApps
認証	設定値																		
Enterprise	SecEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpseenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel17																		
Oracles EBS	secOraApps																		
authentication.visible	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																		
cms.default	デフォルトの CMS 名を指定します。デフォルト: cms.default=[ホストマシン名]																		
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=false																		
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: logontoken.enabled=true																		
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																		

設定	説明
	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: <code>SAPLogonToken.enabled=true</code>

17.2.1.4 CMC プロパティ

以下の表は、BOE.war のデフォルトの `CmcApp.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																		
<code>app.url.name</code>	アプリケーションの URL 名を、先頭に / (スラッシュ) 文字を付けて指定します。デフォルト: <code>app.url.name=/CMC</code>																		
<code>authentication.default</code>	<p>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。</p> <table> <tr> <th>認証</th><th>設定値</th></tr> <tr> <td>Enterprise</td><td><code>SecEnterprise</code></td></tr> <tr> <td>LDAP</td><td><code>secLDAP</code></td></tr> <tr> <td>Windows AD</td><td><code>secWinAD</code></td></tr> <tr> <td>SAP</td><td><code>secSAPR3</code></td></tr> <tr> <td>PeopleSoft</td><td><code>secpsenterprise</code></td></tr> <tr> <td>JD Edwards</td><td><code>secPSE1</code></td></tr> <tr> <td>Siebel</td><td><code>secSiebel7</code></td></tr> <tr> <td>Oracles EBS</td><td><code>secOraApps</code></td></tr> </table> <p>デフォルト: <code>authentication.default=secEnterprise</code></p>	認証	設定値	Enterprise	<code>SecEnterprise</code>	LDAP	<code>secLDAP</code>	Windows AD	<code>secWinAD</code>	SAP	<code>secSAPR3</code>	PeopleSoft	<code>secpsenterprise</code>	JD Edwards	<code>secPSE1</code>	Siebel	<code>secSiebel7</code>	Oracles EBS	<code>secOraApps</code>
認証	設定値																		
Enterprise	<code>SecEnterprise</code>																		
LDAP	<code>secLDAP</code>																		
Windows AD	<code>secWinAD</code>																		
SAP	<code>secSAPR3</code>																		
PeopleSoft	<code>secpsenterprise</code>																		
JD Edwards	<code>secPSE1</code>																		
Siebel	<code>secSiebel7</code>																		
Oracles EBS	<code>secOraApps</code>																		
<code>authentication.visible</code>	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: <code>authentication.visible=true</code>																		
<code>cms.default</code>	デフォルトの CMS 名を指定します。デフォルト: <code>cms.default=[ホストマシン名]</code>																		
<code>cms.visible</code>	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: <code>cms.visible=true</code>																		
<code>dialogue.prompt.enabled</code>	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: <code>dialogue.prompt.enabled=false</code>																		

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: logontoken.enabled=false
SMTPFrom	<p>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</p> <p>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。</p> <ol style="list-style-type: none"> 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。

17.3 BI 起動パッドおよび OpenDocument ログオンエントリー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ー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。

17.3.1 BI 起動パッドおよび OpenDocument ファイルの場所

BI 起動パッド 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。

表 19: BI 起動パッドファイルの場所

i 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

表 20: 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

17.3.2 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.jsp を定義します。

```
function load() {window.location = "logon.jsp";}
```

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。

17.3.3 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。

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="..."
```

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。

関連リンク

[信用できる認証の有効化 \[ページ 191\]](#)

18 接続とユニバースの管理

18.1 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。

デザイナー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、リポジトリに保存されます。
- 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。

i 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。

関連リンク

[CMC でのオブジェクトのセキュリティ設定の管理](#) [ページ 108]

[接続のアクセス権](#) [ページ 766]

18.1.1 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。

18.2 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。

関連リンク

[CMC でのオブジェクトのセキュリティ設定の管理](#) [ページ 108]

[ユニバースデザインツール権限](#) [ページ 771]

[ユニバース \(.unv\) のアクセス権](#) [ページ 762]



[インフォメーションデザインツールの権限](#) [ページ 772]

[ユニバース \(.unx\) のアクセス権](#) [ページ 764]

18.2.1 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](#)  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。

19 モニタリング

19.1 モニタリングについて

モニタリングを使用すると、レポートिंगと通知について、SAP BusinessObjects Business Intelligence 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 Business Intelligence (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、次の操作を実行できます。

- 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場合にアラートを受信することができます。これにより、エラーや機能停止が発生する状況で事前対応型の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、グラフィック形式と表形式で BI プラットフォームデプロイメントの全体を表示できます。
- 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: Business Intelligence 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。

関連リンク

[サーバのメトリクスに関する付録について](#) [ページ 816]

19.2 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

トレンドを把握する目的で、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 Error in tm type 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

派生メトリクスは、既存の 2 つ以上のメトリクスを数式中で組み合わせて作成できるメトリクスです。ユーザの要件に基づいてメトリクスを作成してから、このメトリクスを使用して監視を作成することができます。

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 Error in tm type 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

次のリストは、値と対応するヘルスステータスを示します。

- "0" - メトリクスのヘルスステータスが低下したことを示します。
- "1" - メトリクスのヘルスステータスが低下しており、即時の注意が必要であることを示します。
- "2" - メトリクスのヘルスステータスが良好であることを示します。

KPI

KPI (主要業績評価指標) は、SAP BusinessObjects Enterprise デプロイメントの標準メトリクスです。これらは、スケジュールとログオ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 Error in tm type. 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 Error in tm type. 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

信号は、特定の時点での監視のステータスを示すため、緑、黄色、赤で表示されるアイコンです。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

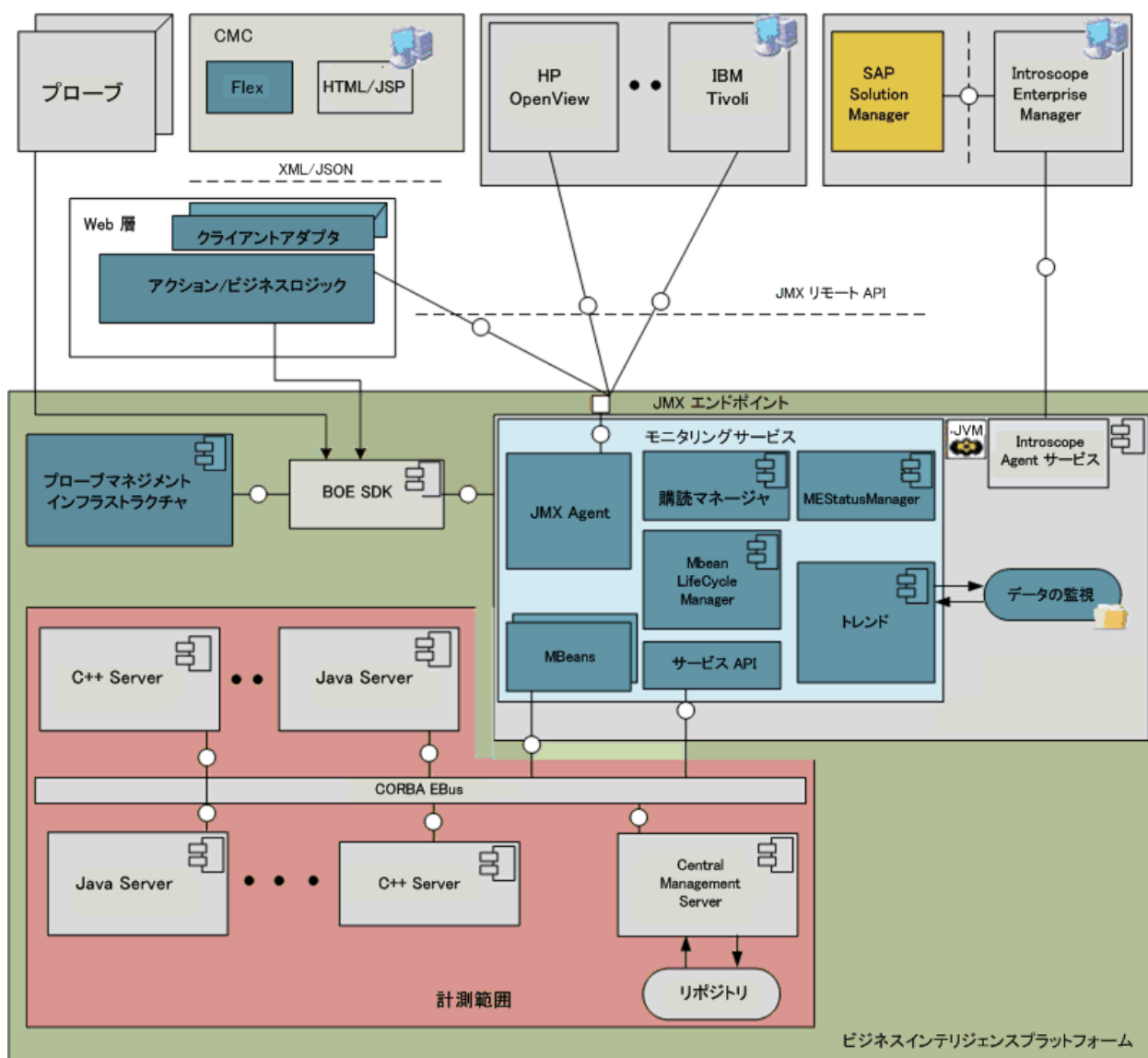
トレンドグラフは、プローブとサーバによって生成された履歴メトリクスデータをグラフィカルに表現したものです。システム管理者は、これを使用してさまざまな間隔でシステムをモニタリングし、システムの使用パターンを評価することができます。

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。

19.2.1 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、他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 Error in tm type. 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、トレンドングを目的として履歴データを保存するため、専用の Derby 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](#)を参照してください。

19.3 モニタリングに対する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の方法について説明します。

i 注記

設定 [[トレンドデータベースへの書き込み](#)] が選択されている監視のみによって、モニタリング情報がトレンドデータベースに書き込まれます。

モニタリング情報の記録には、以下の 2 つのデータベースオプションがあります。

- 埋め込み Derby データベースへの情報の記録 (デフォルトオプション)
モニタリングアプリケーションには、埋め込み Apache Derby データベースが含まれます。このデータベースは、“トレンドデータベース”と呼ばれることが多く、デフォルトでモニタリング情報が保存されます。ユーザは、Derby データベースからレポートを実行できます。ただし、Derby データベースでは、フェールオーバーや従来型のリレーショナルデータベースバックアップおよびリカバリツールは提供されません。また、最新情報が返されるようにするには、Derby データベースを手動で最新表示する必要があります。
- 監査データベース (CMS によって監査データが保存されるリレーショナルデータベース) への情報の記録
デフォルトの Derby データベースを使用する代わりに、監査データベースを使用できます。監査データベースは、監査データストアや ADS と呼ばれることが多いです。BI プラットフォーム Error in tm type. に含まれる監査データベースか、または監査データベースとして設定したそれ以外のサポートされているデータベースを使用できます。監査データベースを使用することで、ユーザは監査データとモニタリング情報からのレポートを同時に行うことができます。リレーショナルデータベースのデータを取得することで、バックアップおよびリカバリ機能と、データのリアルタイムの可用性が実現します。

関連リンク

[Derby データベースを使用するための設定](#) [ページ 539]

[監査データベースを使用するための設定](#) [ページ 540]

19.3.1 Derby データベースを使用するための設定

ユーザが Derby データベースからのレポートを実行する前に、以下のような設定タスクを実行する必要があります。

- [Derby データベースに切り替える](#) [ページ 539]
- [Derby データベースに対するユニバースの作成](#) [ページ 539]

19.3.1.1 Derby データベースに切り替える

モニタリングアプリケーションでは、デフォルトでモニタリングデータが埋め込み Derby データベースに保存されます。過去にモニタリングデータの保存先を監査データベースに切り替えていて、保存先を Derby データベースに戻す場合は、CMC でデータベース設定を変更する必要があります。

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. [監視アプリケーション] をダブルクリックしてプロパティページを開きます。
3. [トレンドデータベースの設定] 領域で、[埋め込みデータベースを使用] を選択します。

19.3.1.2 Derby データベースに対するユニバースの作成

Derby データベースでクエリを実行し、レポートを作成してデータ分析を実行する前に、Derby データベースに対してユニバースを作成する必要があります。CMC の [ユニバース](#) > [Monitoring TrendData Universes](#) において、ユニバースがすでに BI プラットフォーム Error in tm type. のデプロイメントと共にインストールされている可能性があります。

上記のユニバースが存在しない場合、以下の手順に従ってユニバースを作成します。ユニバースの作成に関する詳細については、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。

i 注記

ユニバースは、必ずデータベースに対するバックアップタスクを実行した後に作成します。データベースのバックアップタスクの詳細については、関連項目の設定プロパティを参照してください。

1. インフォメーションデザインツールを起動します。Windows では、[スタート](#) > [すべてのプログラム](#) > [SAP Business Intelligence](#) > [SAP BusinessObjects BI プラットフォーム 4 クライアントツール](#) > [インフォメーションデザインツール](#) の順にクリックします。
2. ユニバースリソースを保存するために新しいプロジェクトを作成します。
3. 新しいリレーショナル接続を作成し、リソース名を入力して、[次へ] をクリックします。
4. [データベースミドルウェアドライバの選択] ページで、[一般設定](#) > [汎用 JDBC データソース](#) > [JDBC ドライバ](#) の順に選択し、[次へ] をクリックします。
5. JDBC 接続の詳細を入力します。
 - a) [JDBC URL] フィールドに「jdbc:derby:<C:\DerbyDBBackup>;create=false」を入力します。<C:\DerbyDBBackup> は、トレンドデータベースのバックアップディレクトリです。
 - b) [JDBC クラス] フィールドに「org.apache.derby.jdbc.EmbeddedDriver」を入力します。

6. [\[接続テスト\]](#) をクリックして接続をテストします。

7. データファンデーションおよびビジネスレイヤを作成します。

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」の節を参照してください。

関連リンク

[Configuration Properties](#) [ページ 546]

[トレンドデータベーススキーマ](#) [ページ 857]

19.3.2 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に監査データベースを使用する場合、以下のような追加の設定手順を実行する必要があります。

- Derbyトレンドデータベースに既存データがある場合、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モニタリング情報を記録するよう BI プラットフォーム `Error in tm type` を設定する必要があります。従う必要があるステップの概要は以下のとおりです。詳細については、関連トピックを参照してください。

- Derby データベースを移行します。
- SBO ファイルを設定し、エイリアス名を追加します。
- 監査データベースに切り替えます。
- 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。
- モニタリングダッシュボードで、すべての機能が想定どおりに機能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で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 (フレッシュインストールの場合)、データベースを移行する必要はありません。モニタリング情報を監査データベースに記録するように BI プラットフォーム `Error in tm type` を設定することのみが必要です。従う必要があるステップの概要は以下のとおりです。詳細については、関連トピックを参照してください。

- 監査データベースが機能しており、監査が正常に実行されていることを確認します。
- ADS でモニタリングテーブルを作成します。
- SBO ファイルを設定し、エイリアス名を追加します。
- 監査データベースに切り替えます。
- 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。
- モニタリングダッシュボードで、すべての機能が想定どおりに機能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で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

i 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を実行する場合、カスタムユニバースを開発する必要があります。BI プラットフォーム Error in tm type.に含まれるユニバースは、埋め込み Derby データベースでの使用のみを想定しています。

関連リンク

[Derby データベースの監査データベースへの移行](#) [ページ 541]

[SBO ファイルの設定](#) [ページ 543]

[SBO ファイルでのエイリアス名の追加](#) [ページ 545]

[監査データベースに切り替える](#) [ページ 545]

[ADS でモニタリングテーブルを作成する](#) [ページ 542]

19.3.2.1 Derby データベースの監査データベースへの移行

モニタリングデータに監査データベースを使用し、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する必要があります。

データの移行を開始する前に、以下の前提条件を確認してください。

- 監査データベースが機能しており、監査が正常に実行されていること。
- 新しいテーブルの作成、CSV ダンプのインポートなどのための十分な権限とデータベースクライアントアプリケーションがターゲットデータベースにあること。
- 監査データベースが、カンマ区切り値 (CSV) ファイルのインポートをサポートしていること。

以下の手順に従い、データベース移行を実行します。

1. [Derby データベースをバックアップする](#) [ページ 541]
2. [データを CSV ファイルにエクスポートする](#) [ページ 542]
3. [ADS でモニタリングテーブルを作成する](#) [ページ 542]
4. [コンテンツをターゲットデータベースに復元する](#) [ページ 542]

i 注記

クラスタ化されたシナリオでは、ユーザはすべてのモニタリングインスタンスで Derby データベースの同じインスタンスを使用することになっています。クラスタ化のシナリオで、Derby データベースインスタンスが 2 つ以上ある場合、ユーザは 1 つの Derby インスタンスからのみデータをインポートする必要があります。複数の Derby インスタンスからデータをインポートすると、データの不整合が発生するため、お勧めできません。

19.3.2.1.1 Derby データベースをバックアップする

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. [監視アプリケーション] をダブルクリックしてプロパティページを開きます。

3. [トレンドデータベースの設定] 領域で、Derbyトレンドデータベースをバックアップするファイルの場所を入力し、[保存] をクリックします。
4. [データベースのバックアップタスクの実行] の隣に表示される [今すぐ] をクリックします。
データベースバックアップが成功した場合、確認メッセージが表示されます。バックアップ場所に対して入力したフォルダの場所もチェックし、バックアップファイルがそこに格納されていることを確認します。

19.3.2.1.2 データを CSV ファイルにエクスポートする

この節では、移行に必要な CSV ダンプファイルの生成方法について説明します。CSV ファイルには、埋め込みの Derby データベースデータコンテンツのカンマ区切りの値が含まれます。

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. [監視アプリケーション] をダブルクリックしてプロパティページを開きます。
3. [トレンドデータベースの設定] 領域の [埋め込みデータベースからのデータを CSV ファイルとしてエクスポートする] の隣にある [エクスポート] をクリックします。

以下の 4 つの CSV ファイルが、デフォルトのトレンドデータベースの場所 (< BOE_Install_Dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB) に生成されます。

- Mot_Mes_Details.csv
- Mot_Trend_Data.csv
- Mot_Trend_Details.csv
- Mot_Mes_Metrics.csv

19.3.2.1.3 ADS でモニタリングテーブルを作成する

以下の手順に従って、ターゲット監査データベースを準備します。

1. BI プラットフォーム `Error in tm type.` をインストールした後、サポートされているすべての CMS 監査データベースに関連する DDL は、<Install Dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB で提供されます。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。

19.3.2.1.4 コンテンツをターゲットデータベースに復元する

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 の挿入を有効化します。

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 ダンプファイルをターゲットテーブルにインポートします。

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 からテーブルヘ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。以下の順序で、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 の挿入を無効化します。

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。

注記

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、SQL Anywhere などの他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。

19.3.2.2 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。

例

- 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 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.`
- 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 を設定する必要があるファイル: `dataAccess\connectionServer\jdbc<dbType>.sbo.`

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

- 監査で使用す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>
```

- 監査で使用するデータベースバージョンが DB2 の場合、SBO での設定は次のようになります。

```
<DataBase Active="Yes" Name="DB2 UDB for iSeries v5">
  <!-- You can add an alias here if you are using some connections that are
defined with an older database engine -->
  <Alias>DB2/400 V5</Alias>
  <Alias>DB2/400 V4</Alias>
  <Alias>DB2 for iSeries v4</Alias>
  <Alias>DB2</Alias>
</Aliases>"
```

- 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>
```

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。

19.3.2.3 SBO ファイルでのエイリアス名の追加

ドライバの設定と共に、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>
```

19.3.2.4 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、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. [監視アプリケーション] をダブルクリックしてプロパティページを開きます。
3. [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。

19.4 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 [アプリケーション] タブに移動します。
2. [監視アプリケーション] を右クリックし、[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] ウィンドウが表示されます。次の表で、設定可能なプロパティについて説明します。

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。トレンドのプローブも無効化されます。
	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 レジストリエンドポイントと 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。

セクション	フィールド	説明
ホストメトリクス	ホストメトリクスを有効にする	<p>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。</p> <p>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。</p>
トレンドデータベースの設定	監査データベースを使用	<p>このオプションを選択すると、CMS 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。</p> <div> <p>i 注記</p> <p>この処理を実行するには、CMS 監査を設定する必要があります。</p> </div>
	埋め込みデータベースを使用	<p>このオプションを選択すると、モニタリングアプリケーションに同梱されている埋め込みデータベースに、メトリクス/監視トレンド履歴を保存できます。</p>
その他の設定	メトリクスの最新表示間隔 (秒)	<p>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。</p> <ul style="list-style-type: none"> 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。
	データベースが次のサイズ (MB) 以上になったら古いデータを削除します。	<p>データベースが指定されたサイズを超過した場合に、トレンドデータベースのデータがクリーンアップされます。データベースに対し、30% のバッファが作成されます。たとえば、このプロパティを 100 MB に設定し、チェック時にデータベースサイズが 100 MB を超過していた場合、データはデータベースが 70 MB になるまでクリーンアップされます。</p>
	UI モニタリングの自動最新表示間隔 (秒)	<p>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</p>

セクション	フィールド	説明
		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。
	データベースのクリーンアップタスクを毎日次の時間に実行する	データベースクリーンアップタスクが、指定された時刻に開始されます。データベースは、データベースが指定された最大サイズを超過するとクリーンアップされます。
	トレンドデータベースのバックアップ	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と、トレンドデータベースのバックアップタスクが、指定された時刻に開始されます。
	トレンドデータベースのバックアップディレクトリ	デフォルトでは、場所が指定されていません。場所を指定できますが、その場合は絶対パスではなく絶対パスを指定します。共有の場所の場合、共有の場所にアクセスするための権限を付与する必要があります。
	データベースのバックアップタスクの実行	このオプションをクリックすると、データベースのバックアップタスクが開始されます。データベースバックアップのディレクトリの場所を指定してから、このオプションを選択してください。
	トレンドデータベースの場所	デフォルトでは、トレンドデータベースの場所は BOE_Install_Dir\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB です。異なる場所を指定することもできますが、その場合は絶対パスではなく絶対パスを指定します。クラスタ環境の場合、場所を共有にし、共有の場所にアクセスするための権限を付与する必要があります。

3. [保存] をクリックします。

i 注記

これらのうち、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いずれか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. SPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR コマンドを実行して、SAPHOSTAGENT710_XX.SAR を解凍します。

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. `saposccl -s` コマンドを実行して、`SAPOSCOL` のステータスを確認します。

19.4.1 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
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](#) [ページ 546]を参照してください。

19.4.2 プローブのモニタリングに使用する HTTPS 認証

プローブのモニタリングに使用する HTTPS サーバ認証がサポートされています。これを使用するには、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 を確認できるようになります。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、またはサーバの証明書を生成した認証機関 (通常は内部 CA) の証明書です。サーバの証明書が広く知られている CA によって生成されており、それをインポートする必要がある場合は、このステップをスキップできます。これは、サーバの証明書が CA によって確認され、その公開鍵がすでにデフォルトで truststore に含まれているためです。
2. BI 起動パッドのプローブの設定で、[\[URL ベース\]](#) を `https://<URL>/BOE/BI` に変更します。<URL> は、証明書で使用する名前のホストを指します。

プローブのモニタリングに使用する HTTPS クライアント認証はサポートされていません。

19.4.3 プローブのパスワード暗号化

パスワードが暗号化されるようプローブを使用する場合、コマンドラインを使用したプローブの作成時に、すべてのモニタリングプローブのパスワードパラメータに `true` パラメータを追加する必要があります。この処理は、セントラル管理コンソールの [\[モニタリング\]](#) タブで実行されます。詳細および構文の例については、CMC ヘルプのコマンドラインによるプローブの管理を参照してください。

19.5 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。

19.5.1 モニタリングアプリケーションと IBM Tivoli との統合

モニタリングアプリケーションと IBM Tivoli とを統合するには、IBM Tivoli Monitoring Agent を作成、インストール、および設定する必要があります。IBM Tivoli Monitoring Agent を作成するには、以下の手順に従います。

1. IBM Tivoli Monitoring Agent ビルダバージョン 6.2.1 ソフトウェアをインストールします。
2. 新規エージェントを作成します。新規エージェントの作成方法に関する詳細については、『IBM Tivoli Monitoring Agent ユーザガイド』を参照してください。
3. データモニタリングタイプの定義ステップでは、[データカテゴリのモニタリング] エリアでサーバからのデータを選択し、[データソース] 領域で JMX を選択します。
4. [次へ] をクリックします。
5. [JMX 情報] ウィンドウで [参照] をクリックし、MBean サーバのすべての JMX MBeans を表示します。

i 注記

ブラウザを始めて実行する場合、新規接続を追加する必要があります。

6. [Java Management Extensions (JMX) ブラウザ] ウィンドウで [接続名] の隣にある + をクリックし、新規接続を追加します。
7. [MBean サーバ接続ウィザード] ウィンドウで標準 JMX 接続 (JSR-160) を選択します。
8. [接続プロパティ] ウィンドウに、次の情報を指定します。

フィールド	説明
接続名	JSR-160 標準サーバ
ユーザ ID	SAP BusinessObjects BI プラットフォーム <small>Error in tm type.</small> へのログインに使用されるユーザ名
パスワード	SAP BusinessObjects BI プラットフォーム <small>Error in tm type.</small> へのログインに使用されるパスワード
サービス URL	JMX エンドポイント URL を指定します。

9. [完了] をクリックします。
10. [MBean キープロパティ] エリアでドメインおよび種類を選択します。
すべての MBeans が下のテキストフィールドに表示されます。
11. すべてのドメイン登録された MBeans をサーバとして選択します。属性が一覧にされるよう、MBean を 1 つずつ選択します。同じタイプの MBeans が複数になる可能性がある場合、キー属性を選択します。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、各インスタンスの PID がキー属性になり得ます。
12. サーバを選択し、[JMX Agent-Wide オプション] ウィンドウで JMX 属性グループのオプションを選択します。
13. [データソース定義] ウィンドウで、追加したエージェントを選択し、[選択に追加] をクリックします。それによってエージェント作成サイクルの最初に戻るので、モニタする別のサーバを追加するには上記のステップを繰り返す必要があります。
14. エージェントの作成後、エージェントをインストールする必要があります。エージェントのインストール方法に関する詳細については、『IBM Tivoli Monitoring Agent ユーザガイド』の図番号 154 以降を参照してください。この節では、エージェントのローカルでのインストール、およびエージェントのインストール可能ソリューションの作成に関する情報を提供します。

i 注記

エージェントビルダを使用して SAP BusinessObjects BI プラットフォーム Error in tm type.のエージェントを作成する場合、SAP BusinessObjects BI プラットフォームが同じシステムにインストールされている必要があります。ただし、すでに作成されているエージェントをそのインストーラファイルを使用してインストールする場合、設定時に JMX エンドポイントを含むすべてのシステムの詳細を指定することができるため、BI プラットフォーム Error in tm type.モニタリングをインストールする必要はありません。

インストール済みエージェントの設定を行うには、以下の手順に従います。

1. [\[Tivoli Enterprise Monitoring Service の管理\]](#) を TEMS モードで開きます。インストールされたエージェントが表示されます。
2. エージェントテンプレートを右クリックし、[\[デフォルトを使用して構成\]](#) を選択します。
3. インスタンス名を選択します。
エージェントは、RMI と BOEIIOP という 2 つの異なるプロトコルを使用して設定することができます。
RMI プロトコルを使用するには、以下の手順に従います。

[\[次へ\]](#) をクリックします。Java パラメータは変更しません。

JMX 認証情報の値を指定します。これには、ユーザ ID、パスワード、サービス URL などが含まれます。詳細については、関連項目の設定プロパティを参照してください。

[\[OK\]](#) をクリックします。

BOEIIOP プロトコルを使用するには、以下の手順に従います。

%InstallDir%\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib
の bcm.jar および cryptojFIPS.jar ファイルをシステムのフォルダにコピーします。

下の表の jar ファイルを別のフォルダにコピーします。

Java パラメータで、JVM 引数を bcm.jar および cryptojFIPS.jar ファイルをコピーしたフォルダの場所 -
Djmx.remote.protocol.provider.pkgs = com.businessobjects.sdk.monitoring および -
Djmx.boeiiop.bcm.dir=< に設定します。

[\[次へ\]](#) をクリックします。

JMX 認証情報の値を指定します。これには、ユーザ ID、パスワード、サービス URL などが含まれます。詳細については、関連項目の設定プロパティを参照してください。

表で提供されている jar ファイルの一覧をコピーしたフォルダの場所として、**<Jar ディレクトリ>** 値を設定します。

[\[OK\]](#) をクリックします。

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

Jar ファイル
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
aspectjrt.jar

4. エージェントを右クリックし、[*Manage Tivoli Enterprise Monitoring Services*] ウィンドウで [開始] を選択します。
5. IBM Tivoli Enterprise Portal Desktop/Browser Client を開きます。[ナビゲータ] ウィンドウにボタンが表示されます。
6. [ナビゲータ] ボタンをクリックします。
エージェントがナビゲータに追加されます。

関連リンク

[Configuration Properties](#) [ページ 546]

19.5.2 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。SAP BusinessObjects 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. 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。SAP BusinessObjects BI プラットフォームのインストール時に、Introscope Agent が C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wiley にインストールされます。
2. Introscope ワークステーションを起動して、[新規 *Investigator* の作成] 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。

i 注記

Introscope (IS) エージェントは、**CMC > サーバ > サーバノード > プレースホルダ** 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、「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。

19.6 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では、フェイルオーバー機能が提供されるクラスタリングがサポートされます。

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、そのうち 1 つのみを使用できます。s1 と s2 の両方がアクティブになろうとしますが、どちらかがアクティブになると、もう 1 つのサービスが無効またはパッシブになります。

パッシブなサービスでは、アクティブなサービスの利用可能性が定期的 (1 分ごと) にチェックされます。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。

i 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。

19.7 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。

19.7.1 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。

-  **CMS サーバプロパティ**  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。

モニタリングアプリケーションを起動できません。

最新の Flash Player (10.5.x) をダウンロードして、インストールします。

19.7.2 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。

- [通知] 設定で、[アラート通知を有効にする] 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。

i 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 CR 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

- SMTP サーバが機能し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に設定された電子メール ID が適切であることを確認する。
- AdaptiveJobServer インスタンスが有効になっていることを確認する。
- AdaptiveJobServer インスタンス出力先の SMTP 設定を確認する。

19.7.3 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。
- CMC の [アプリケーション] ページで [トレンドデータベースの場所] が指定されているかを確認する。クラスタ化環境の場合は、ユーザに共有場所にアクセスする権限があることを確認します。詳細については、関連項目の設定プロパティを参照してください。
- 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。

AdaptiveProcessingServer インスタンスが実行中であることを確認します。

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。

関連リンク

[Configuration Properties](#) [ページ 546]

19.7.4 プローブ

プローブをスケジュールできません。

- AdaptiveJobServer インスタンスが実行中であることを確認する。
- Crystal レポートおよび 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どうかを確認する。

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どうかを確認する。
- AdaptiveJobServer インスタンスが実行中であることを確認する。

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ことを確認します。

probeRun.bat を実行できません

- java_home が設定されているかどうかを確認する。
- 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どうかを確認する。

i 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。

19.7.5 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します。
- 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します。
- 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ことを確認します。

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します。
- 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. `saposc -s` でステータスをチェックします。
 2. `saposc -m` で SAPOSCOL により収集されたデータのスナップショットを取得します。

19.7.6 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。

クラスタシナリオの履歴モードにチャートデータが表示されません。

すべての AdaptiveProcessingServer インスタンスが同じ Derby データベースの場所をポイントしていることを確認します。

20 監査

20.1 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。<http://www.businessobjects.com/jpl/default.asp?destination=auditreports> 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

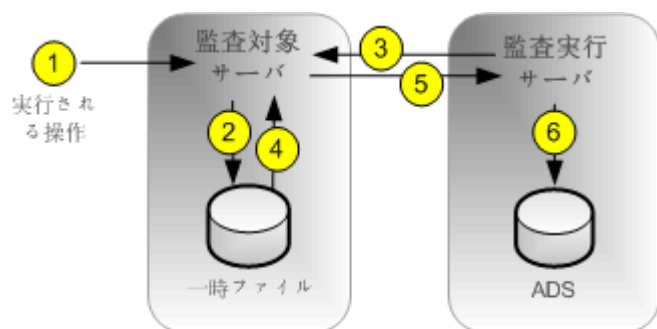
Central Management Server (CMS) はシステム監査実行サーバとして機能し、監査可能なイベントを発生させる各サーバまたはアプリケーションは監査対象サーバとして機能します。監査対象イベントが発生すると、監査対象サーバはレコードを生成してローカルの一時ファイルに格納します。CMS は定期的に監査対象サーバと通信し、これらのレコードを要求し、ADS にデータを書き込みます。

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。

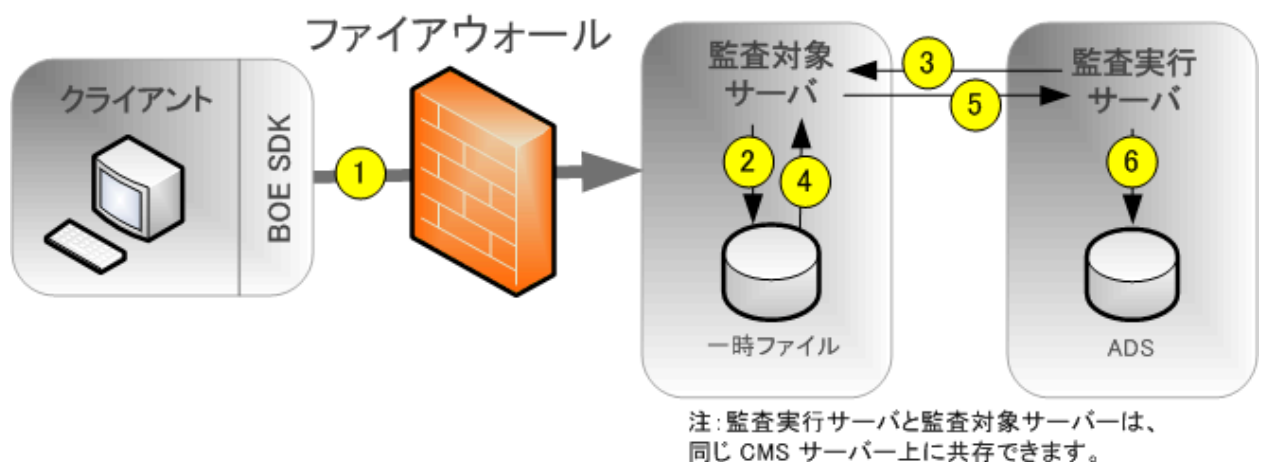


注: Auditor と監査対象サーバは、同じ CMS サーバ上に共存できます。

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。
3. 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。

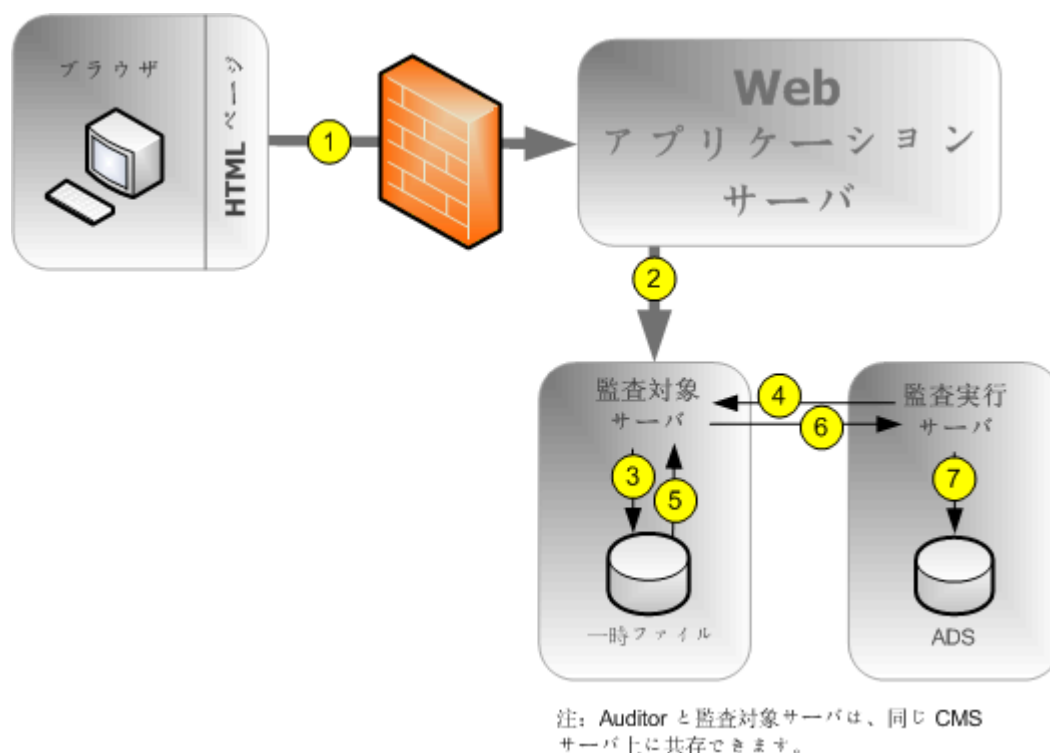
i 注記

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。
3. 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

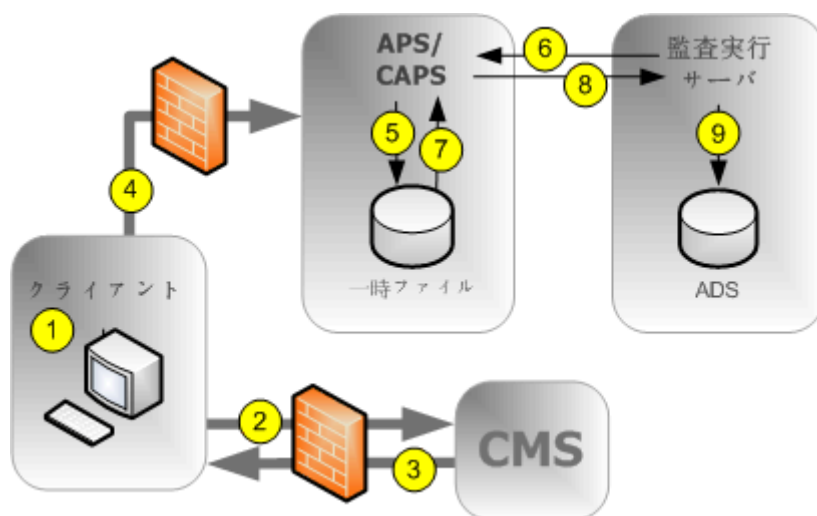
これには、BI 起動パッド、セントラル管理コンソール、SAP BusinessObjects Web Intelligence などのオンラインアプリケーションが含まれます。



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。
4. 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。

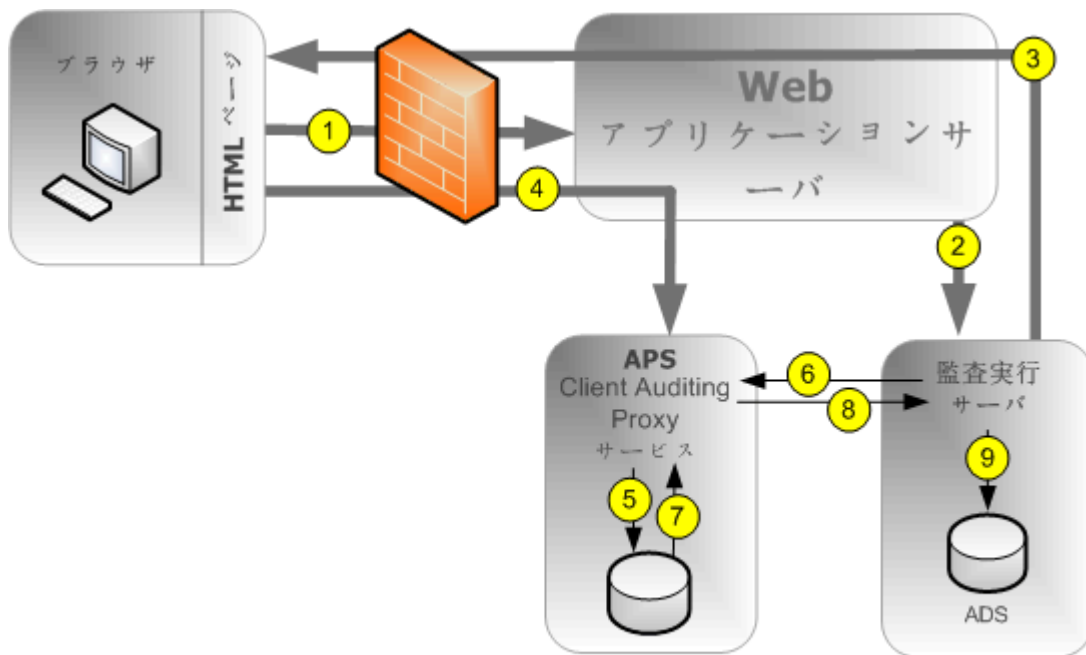
i 注記

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。
6. 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。



注: Auditor と監査対象サーバは、同じ CMS サーバ上に共存できます。

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。

i 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。
6. 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。

- セントラル管理コンソール (CMC)

- BI 起動パッド
- OpenDocument
- 分析
- Live Office Web サービスプロバイダ
- Web Intelligence デスクトップ
- Mobile
- Dashboard Design および Presentation Design
- Dashboard Manager

i 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ため、注意が必要です。

イベントが発生してから監査実行データベース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。

i 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。

i 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働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。この数字が 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 [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。

i 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](#) [ページ 835]

20.2 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](#)

20.2.1 ステータスの概要

[[監査ステータス](#)] 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。

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開始した日付と時刻。
監査スレッド利用率	<p>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。</p> <p>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。</p> <p>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勧めします。</p>
最終ポーリングサイクル期間	<p>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。</p> <ul style="list-style-type: none"> 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。 <p>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。</p>
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	<p>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 および HANA サーバの場合、これは ODBC 接続の名前になります。</p> <p>その他のデータベースの場合、これはサーバ名、接続ポート、およびデータベース名になります。</p>
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。

20.2.2 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。

i 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。監査データストア設定を参照してください。

20.2.2.1 監査イベントを設定する

1. セントラル管理コンソールで、[\[監査\]](#) タブを選択します。
[\[監査\]](#) ページが表示されます。
2. [\[イベントの設定\]](#) スライダを目的のレベルに設定します。

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 4 つ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	<ul style="list-style-type: none">○ ログオン○ ログアウト○ アクセス権の変更回数○ カスタムアクセスレベルの変更○ 監査変更
デフォルト	<p>[最小] イベント、プラス:</p> <ul style="list-style-type: none">○ 表示○ 最新表示○ プロンプト○ 作成○ 削除○ 修正○ 保存○ 検索○ 編集○ 実行○ 配信
完全	<p>[最小] および [デフォルト] イベントプラス:</p> <ul style="list-style-type: none">○ 取得○ 呼び出しイベント○ 範囲外をドリル

監査レベル	取得されたイベント
	<ul style="list-style-type: none"> ○ ページの取得 ○ LCM 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
カスタム	イベントのカスタム設定を選択します。

3. [カスタム] を選択した場合、[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。詳細をより少なく記録すると、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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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。 <ul style="list-style-type: none"> ○ 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 起動パッド、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。

i 注記

クライアント監査の場合、システムが新規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 分かかることがあります。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。

20.2.3 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。

i 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に設定されていることを確認してください。

20.2.3.1 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. [\[設定\]](#) 見出しで、[\[種類\]](#) をクリックします。
サポートされているデータベースタイプの一覧が表示されます。
3. 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。
4. [\[接続名\]](#) 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。

データベースタイプ	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。
5. [\[ユーザ名\]](#) 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。
IBM DB2 が BI プラットフォームによってデフォルトデータベースとしてインストールされている場合、[\[ユーザ名\]](#) および [\[パスワード\]](#) フィールドを空白のままにします。
 6. [\[\(日\) 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 109,500)

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。

7. 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。

8. [保存] をクリックします。
9. CMS を再起動します。

20.3 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	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
監査変更	システムの監査設定が変更されました。 <ul style="list-style-type: none">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。 <ul style="list-style-type: none">Web Intelligence 処理サービスCrystal Reports 表示および変更サービスセントラル管理サービスWeb Intelligenceライフサイクルマネジメント
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。 <ul style="list-style-type: none">Multi-Dimensional Analysis Service
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。 <ul style="list-style-type: none">セントラル管理サービス
削除	システムからオブジェクトが削除されました。 <ul style="list-style-type: none">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。 <ul style="list-style-type: none">送信先への配信スケジュールサービス

イベント	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
	<ul style="list-style-type: none"> Crystal Reports スケジュールサービス Crystal Reports for Enterprise スケジュールサービス Web Intelligence 公開およびスケジュールサービス セントラル管理サービス 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 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
範囲外をドリル	<p>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。</p> <ul style="list-style-type: none"> 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 Web Intelligence エンジンサービス
編集	<p>オブジェクトのコンテンツが変更されました。</p> <ul style="list-style-type: none"> Web Intelligence 処理サービス ダッシュボードサービス Web Intelligence Web Intelligence 共通サービス Web Intelligence コアサービス Web Intelligence エンジンサービス
LCM 設定	<p>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。</p> <ul style="list-style-type: none"> ライフサイクルマネジメント
ログオン	<p>ユーザがシステムにログオンしました。</p> <ul style="list-style-type: none"> セントラル管理サービス
ログアウト	<p>ユーザがシステムからログアウトしました。</p> <ul style="list-style-type: none"> セントラル管理サービス
修正	<p>オブジェクトのファイルプロパティが変更されました。</p> <ul style="list-style-type: none"> 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
MDAS セッション	<p>Multi Dimensional Analysis Service 処理が実行されました。</p> <ul style="list-style-type: none"> Multi-Dimensional Analysis Service
ページの取得	<p>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。</p> <ul style="list-style-type: none"> Web Intelligence 処理サービス Web Intelligence 共通サービス

イベント	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
	<ul style="list-style-type: none"> Web Intelligence コアサービス Web Intelligence エンジンサービス
プロンプト	<p>オブジェクトプロンプトに情報が入力されました。</p> <ul style="list-style-type: none"> Dashboards キャッシュサービス Live Office Crystal Reports スケジュールサービス Crystal Reports for Enterprise Crystal Reports キャッシュサービス Web Intelligence 処理サービス Web Intelligence Web Intelligence 共通サービス Web Intelligence コアサービス Web Intelligence エンジンサービス
最新表示	<p>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。</p> <ul style="list-style-type: none"> Dashboards キャッシュサービス Live Office Crystal Reports for Enterprise スケジュールサービス Crystal Reports キャッシュサービス Crystal Reports スケジュールサービス Web Intelligence 処理サービス Web Intelligence Web Intelligence 共通サービス Web Intelligence コアサービス Web Intelligence エンジンサービス
取得	<p>オブジェクトがリポジトリから取得されました。</p> <ul style="list-style-type: none"> セントラル管理サービス
権限の変更	<p>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。</p> <ul style="list-style-type: none"> セントラル管理サービス
ロールバック	<p>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。</p> <ul style="list-style-type: none"> ライフサイクルマネジメント
実行	<p>ジョブが実行されました。</p> <ul style="list-style-type: none"> ライフサイクルマネジメントスケジュールサービス 送信先への配信スケジュールサービス レプリケーションサービス Crystal Reports スケジュールサービス Crystal Reports for Enterprise 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

イベント	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
	<ul style="list-style-type: none"> パブリケーション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 ライフサイクルマネジメント セキュリティエリススケジュールサービス Visual Difference 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 Explorer
保存	<p>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。</p> <ul style="list-style-type: none"> Crystal Reports for Enterprise スケジュールサービス Crystal Reports キャッシュサービス Multi-Dimensional Analysis Service ライフサイクルマネジメントサービス Web Intelligence 処理サービス Crystal Reports 表示および変更サービス Crystal Reports スケジュールサービス SAP BusinessObjects Mobile Analysis Edition for OLAP イベント Web Intelligence 共通サービス Web Intelligence コアサービス Web Intelligence エンジンサービス
検索	<p>検索が実行されました。</p> <ul style="list-style-type: none"> 検索サービス Explorer
呼び出しイベント	<p>ファイルイベントが呼び出されました。</p> <ul style="list-style-type: none"> イベントサービス セントラル管理サービス
表示	<p>オブジェクトが表示されました。</p> <ul style="list-style-type: none"> Web Intelligence Web Intelligence 処理サービス セントラル管理コンソール BI 起動パッド Dashboards キャッシュサービス Crystal Reports キャッシュサービス Crystal Reports 表示および変更サービス ダッシュボードサービス ドキュメントを開く Explorer SAP BusinessObjects Mobile Analysis Edition for OLAP 情報エンジンサービス

イベント	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
	<ul style="list-style-type: none"> Web Intelligence 共通サービス Web Intelligence コアサービス Web Intelligence エンジンサービス
VMS へ追加	<p>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。</p> <ul style="list-style-type: none"> ライフサイクルマネジメント
VMS へのチェックイン	<p>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。</p> <ul style="list-style-type: none"> ライフサイクルマネジメント
VMS からチェックアウト	<p>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。</p> <ul style="list-style-type: none"> ライフサイクルマネジメント
VMS エクスポート	<p>リソースが VMS からエクスポートされました。</p> <ul style="list-style-type: none"> ライフサイクルマネジメント
VMS ロック	<p>VMS 内のリソースがロックされました。</p> <ul style="list-style-type: none"> ライフサイクルマネジメント
VMS ロック解除	<p>VMS 内のリソースがロック解除されました。</p> <ul style="list-style-type: none"> ライフサイクルマネジメント
VMS から取得	<p>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。</p> <ul style="list-style-type: none"> ライフサイクルマネジメント
VMS 削除	<p>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。</p> <ul style="list-style-type: none"> 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
認証更新スケジュールサービス	<ul style="list-style-type: none"> 配信 実行
BI 起動パッド	表示
セントラル管理サービス	<ul style="list-style-type: none"> 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

サービスタイプ	生成されるイベントのタイプ
	<ul style="list-style-type: none"> ログアウト 修正 取得 権限の変更 呼び出しイベント
セントラル管理コンソール	表示
Crystal Reports 2011 スケジュールサービス	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 作成 保存 表示
Dashboards キャッシュサービス	<ul style="list-style-type: none"> プロンプト 最新表示 表示
ダッシュボードアプリケーション	<ul style="list-style-type: none"> 編集 表示
送信先への配信スケジュールサービス	<ul style="list-style-type: none"> 配信 実行
イベントサービス	呼び出しイベント
情報エンジンサービス	<ul style="list-style-type: none"> 作成 範囲外をドリル

サービスタイプ	生成されるイベントのタイプ	
	<ul style="list-style-type: none"> 編集 ページの取得 プロンプト 最新表示 保存 表示 	
LCM スケジュールサービス	実行	
LCM サービス	<ul style="list-style-type: none"> 作成 削除 LCM コンソールの設定 修正 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 	
Live Office	<ul style="list-style-type: none"> プロンプト 最新表示 	
Multi-Dimensional Analysis Service	<ul style="list-style-type: none"> MDAS キューブ接続 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 配信 実行 	
プログラムスケジュールサービス	<ul style="list-style-type: none"> 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	
セキュリティエリススケジュールサービス	<ul style="list-style-type: none"> 実行 配信 	

サービスタイプ	生成されるイベントのタイプ
ユーザとグループのインポートスケジュールサービス	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 作成 ● 範囲外をドリル ● 編集 ● 修正 ● ページの取得 ● プロンプト ● 最新表示 ● 保存 ● 表示
Web Intelligence 共通サービス	<ul style="list-style-type: none"> ● 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 コアサービス	<ul style="list-style-type: none"> ● 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 処理サービス	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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。

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。

20.3.1 監査イベントおよび詳細

以下の節では、すべてのイベントタイプとそれらのイベントに固有のプロパティおよびイベント詳細の説明を一覧表示します。節の最初に、すべてのイベントタイプに共通のプロパティと詳細の一覧を示します。

i 注記

一部のクライアントプログラムは、固有のイベントを持たず、共通イベントおよびプラットフォームイベントからそれぞれの実行に必要な情報を取得します。

ユニバーサルイベントのプロパティおよび詳細

以下の表に、すべてのイベントで記録されるプロパティおよびイベント詳細を示します。

イベントプロパティ	説明
Event_ID	イベントの一意の ID
Client_Type_ID	イベントを実行したアプリケーションのタイプを示す ID
Service_Type_ID	イベントを呼び出したサービスまたはアプリケーションのタイプを示す ID
Start_Time	イベントが開始された日付と時刻 (GMT)
Duration	イベントの存続時間 (ミリ秒)
Session_ID	イベントの呼び出し時に実行されていたセッションの ID
Event_Type_ID	イベントのタイプ (たとえば、表示の場合は 1002)

イベントプロパティ	説明
Status_ID	アクションの成功または失敗の記録 ("0" = 成功, "1" = 失敗)。一部のイベントには追加のステータスタイプがあり、それらの詳細はイベントの説明に記載されます。
Object_ID	<p>影響を受けるオブジェクトの CUID (該当する場合)。呼び出しイベントの場合は、アラートイベントの CUID。</p> <div> <p>i 注記</p> <p>CMS リポジトリに保存されていないオブジェクトの ID はすべて 0 になります。そのようなオブジェクトの例としては、CMS データベースにまだ保存されていないドキュメントやクライアントマシンにローカルに保存されているドキュメントなどがあります。これらのオブジェクトを区別するには、Object_Name プロパティを使用する必要があります。</p> </div>
User_ID	イベントを実行したユーザの CUID
User_Name	イベントを実行したユーザのユーザ名
Object_Name	影響を受けるオブジェクトの名前 (該当する場合)。呼び出しイベントの場合は、アラートイベントの名前。
Object_Type_ID	オブジェクトタイプの CUID (ドキュメント、フォルダなど)
Object_Folder_Path	影響を受けるオブジェクトが保存されている CMS リポジトリ内のフォルダへの完全パス。例: Sales/North America/East Coast
Folder_ID	オブジェクトが保存されているフォルダの CUID
Top_Folder_Name	影響を受けるオブジェクトの保存場所のトップレベルフォルダの名前。たとえば、オブジェクトが Sales/North America/East Coast に保存されている場合、この値は Sales になります。
Top_Folder_ID	影響を受けるオブジェクトの保存場所のトップレベルフォルダの CUID。たとえば、オブジェクトが Sales/North America/East Coast に保存されている場合、この値はフォルダ Sales の CUID になります。
Cluster ID	イベントを記録した CMS クラスタの CUID
Action_ID	単一のユーザアクションによって開始された一連のイベントをまとめるために使用する一意の ID

イベントの詳細	ID	説明
エラー	1	(アクションが失敗した場合にのみ記録される) 実行の結果として生成されるエラーメッセージのテキスト
要素 ID	2	コンテナオブジェクト (Live Office ドキュメント、ダッシュボードなど) に配置されているオブジェクトの名前

イベントの詳細	ID	説明
要素名	3	コンテナオブジェクト (Live Office ドキュメント、ダッシュボードなど) に配置されているオブジェクトに対して生成される ID
要素タイプ ID	5	表示中または変更中のコンテナオブジェクトに入っているオブジェクトのタイプ。該当する場合にのみ生成されます。
親ドキュメント ID	12	<ul style="list-style-type: none"> ドキュメントインスタンスの場合: 親ドキュメントの CUID 親ドキュメントの場合: 自身の CUID
ユニバース ID	13	ドキュメントまたはオブジェクトによって使用されるユニバースの CUID。複数のユニバースが使用される場合は、ユニバースごとにイベント詳細が生成されます。
ユニバース名	14	ドキュメント/オブジェクトによって使用されるユニバースの名前。複数のユニバースが使用される場合は、ユニバースごとにイベント詳細が生成されます。
ユーザグループ名	15	アクションを実行しているユーザが属しているユーザグループ名。ユーザが複数のグループに属している場合は、グループごとにイベント詳細が生成されます。
ユーザグループ ID	16	アクションを実行しているユーザが属しているユーザグループの ID。ユーザが複数のグループに属している場合は、グループごとにイベント詳細が生成されます。

共通イベント

以下のイベントタイプは、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で共通です。

表示

ユーザがドキュメント/オブジェクトを表示しました。

- イベントタイプ ID: 1002

イベントの詳細	ID	説明
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)

イベントの詳細	ID	説明
コンテナ ID	32	オブジェクトが配置されているコンテナオブジェクト (ダッシュボードなど) の CUID (該当する場合)
コンテナタイプ	33	オブジェクトのコンテナのアプリケーションタイプ (該当する場合)

i 注記

検索サービスを使用している場合は、ドキュメントのインデックス化時に、"システムアカウント" ユーザによって多数の表示イベントが生成される場合があります。これは、検索インデックス化サービスにより、検索インデックスを作成するためにドキュメントが開かれることが原因です。

最新表示

データベースからオブジェクトが最新表示されました。

- イベントタイプ ID: 1003

イベントの詳細	ID	説明
サイズ	17	<p>イベントの対象となるオブジェクトのサイズ (バイト)</p> <p>i 注記 Crystal Reports のオンデマンド表示の場合、この値は 0 に設定されます。</p>
行数	63	<p>データベースサーバによって返されたレコードの数</p> <p>i 注記 Crystal Reports のオンデマンド表示の場合、この値は 0 に設定されます。</p>
クエリ	25	データの最新表示に使用された SQL 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	ドキュメントまたはオブジェクトが使用するユニバースの名前。ドキュメントまたはオブジェクトがアクセスするユニバースごとにイベント詳細が生成されます。
ドキュメント範囲	36	公開設定で対象とするドキュメント範囲に関する情報を記録します (例: 国 = 米国、ロール = マネージャ)。公開ワークフローにのみ適用されます。

イベントの詳細	ID	説明
パブリケーションインスタンス ID	37	パブリケーションのインスタンスの ID。公開ワークフローにのみ適用されます。
Live Office オブジェクトタイプ	10701	Live Office ドキュメント内で最新表示中のオブジェクトのタイプを特定します (Crystal レポートなど)。この値は、Live Office ドキュメントでのみ生成されます。

プロンプト

プロンプトに値が入力されました。

- イベントタイプ ID: 1004

イベントの詳細	ID	説明
プロンプト名	26	プロンプトに割り当てられた名前 ("日付"など)。ドキュメントまたはオブジェクトのプロンプトごとに個別の詳細が生成されてから、グループ化されます。
プロンプト値	27	プロンプトに入力された値。入力された値ごとに個別の詳細が生成されます。これらの値は、グループ化してプロンプト名に関連付けることができます。
ドキュメント範囲	36	対象とするドキュメント範囲に関する情報 (例: 国 = 米国、ロール = マネージャ)
パブリケーションインスタンス ID	37	パブリケーションのインスタンスの ID。公開ワークフローにのみ適用されます。
デザイン時の名前	90	Dashboards ドキュメントのデザイン時の名前。この値は、Dashboards の最新表示、またはプロンプトを含む Dashboards/Live Office ドキュメントの場合にのみ生成されます。
Live Office オブジェクトタイプ	10701	Live Office ドキュメント内で最新表示中のオブジェクトのタイプを特定します (Crystal レポートなど)。この値は、埋め込みオブジェクトにプロンプトが含まれる Live Office ドキュメントの場合にのみ生成されます。

作成

ユーザがオブジェクトを作成しました。

- イベントタイプ ID: 1005

イベントの詳細	ID	説明
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)
上書き	21	ドキュメントまたはオブジェクトが新規に作成されたものか、既存のオブジェクトに上書きしたものかを記録します (0 = 新規のドキュメントまたはオブジェクト、1 = 既存のドキュメントまたはオブジェクトの上書き)。
起動時に最新表示	23	ドキュメントまたはオブジェクトが起動時に自動的に最新表示されるように設定されているかどうかを記録します (0 = 最新表示しない、1 = 起動時に最新表示)。該当する場合にのみ生成されます。
説明	24	ドキュメントまたはオブジェクトの説明フィールドのすべての情報を記録します。

削除

ユーザがオブジェクトを削除しました。

- イベントタイプ ID: 1006

修正

ユーザがオブジェクトのファイルプロパティを変更しました。

- イベントタイプ ID: 1007

イベントの詳細	ID	説明
プロパティ名	28	変更されたプロパティの名前。変更されたプロパティごとにイベント詳細が生成されます。
プロパティ値	29	ドキュメントまたはオブジェクトで変更されたプロパティの新しい値。変更されたプロパティごとにイベント詳細が生成されます。

保存

ドキュメントまたはオブジェクトを、既存のあるいは異なる形式で、ローカル、リモート、または CMS リポジトリに保存またはエクスポートします。

- イベントタイプ ID: 1008

- ステータス:

- "0" は、オブジェクトが正常にローカル保存されたことを示します。
- "1" は、保存に失敗したことを示します。
- "2" は、オブジェクトが正常にリポジトリに保存またはエクスポートされたことを示します。
- "3" は、オブジェクトが正常に新しい形式で保存またはエクスポートされたことを示します。

イベントの詳細	ID	説明
サイズ	17	保存またはエクスポートされたオブジェクトのサイズ (バイト)
ファイル名	18	ドキュメントまたはオブジェクトを保存した完全名。ファイルがクライアントアプリケーションによってローカルに保存された場合、この名前にはファイルパスも含まれます。
上書き	21	ドキュメントまたはオブジェクトが新規に作成されたものか、既存のファイルに上書きしたものを記録します。"0" = 新規のドキュメントまたはオブジェクト、"1" = 既存のドキュメントまたはオブジェクトの上書き。
形式	22	保存/エクスポートされたドキュメントの形式を一般的な 3 文字の拡張子で指定します (例: Microsoft Word 文書の場合は "doc"、Adobe PDF ファイルの場合は "pdf")。
起動時に最新表示	23	ドキュメントまたはオブジェクトが起動時に自動的に最新表示されるように設定されているかどうかを記録します ("0" = 最新表示しない、"1" = 起動時に最新表示)。該当する場合にのみ記録されます。

検索

検索が実行されました。

- イベントタイプ ID: 1009

イベントの詳細	ID	説明
キーワード	19	実行された検索のキーワード
カテゴリ	20	検索に使用されたカテゴリ (該当する場合)
行数	63	検索によって返された行数

編集

ユーザがオブジェクトのコンテンツを編集しました。

- イベントタイプ ID: 1010

イベントの詳細	ID	説明
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)
クエリ	25	編集によって SQL クエリが変更された場合は、新しいクエリを記録します。これはオプションの設定で、CMC 監査ページで選択できます。
ユニバースオブジェクトの名前	31	ドキュメントまたはオブジェクトが使用するユニバースの名前。ドキュメントまたはオブジェクトがアクセスするユニバースごとに個別の詳細が生成されます。
コンテナ ID	32	オブジェクトを使用するコンテナ (ダッシュボードなど) の CUID (該当する場合)
コンテナタイプ	34	オブジェクトのコンテナのアプリケーションタイプ (該当する場合)
コンテナフォルダパス	64	オブジェクトのコンテナのフォルダパス (該当する場合)

実行

ジョブが実行されました。

- イベントタイプ ID: 1011
- ステータス:
 - "0" は、ジョブが成功したことを示します。
 - "1" は、ジョブが失敗したことを示します。
 - "2" は、ジョブは失敗したが、再試行されることを示します。
 - "3" は、ジョブがキャンセルされたことを示します。

イベントの詳細	ID	説明
サイズ	17	実行されたドキュメントのサイズ (バイト)
ドキュメント範囲	36	対象とするドキュメント範囲に関する情報 (例: 国 = 米国、ロール = マネージャ)

配信

オブジェクトが配信されました。

- イベントタイプ ID: 1012

イベントの詳細	ID	説明
サイズ	17	配信されたオブジェクトのサイズ (バイト)
出力先タイプ	35	ドキュメントまたはオブジェクトのインスタンスの出力先。たとえば、電子メール、FTP、アンマネージドディスク、受信ボックス、またはプリンタ。
ドキュメント範囲	36	対象とするドキュメント範囲に関する情報 (例: 国 = 米国、ロール = マネージャ)
パブリケーションインスタンス ID	37	ドキュメントまたはオブジェクトのインスタンスの ID
ドメイン	38	電子メールによって配信されるドキュメント/オブジェクトの SMTP サーバドメイン名を記録します (該当する場合)。
ホスト名	39	電子メールまたは FTP によって配信されるドキュメント/オブジェクトの SMTP または FTP のホスト名を記録します (該当する場合)。
ポート	40	電子メールまたは FTP によって配信されるドキュメント/オブジェクトの SMTP または FTP のサーバドメインポートを記録します (該当する場合)。
送信元アドレス	41	電子メールによって配信されるドキュメント/オブジェクトの送信者のアドレスを記録します (該当する場合)。
送信先アドレス	42	電子メールによって配信されるドキュメント/オブジェクトの受信者のアドレスを記録します (該当する場合)。アドレスが、[To]、[CC]、または [BCC] フィールドのどれに含まれるかも指定します。受信者ごとにイベント詳細が生成されます。
ファイル名	18	電子メール、FTP、または BusinessObjects デプロイメントに含まれないディスクに直接書き込まれたドキュメント/オブジェクトのファイル名を記録します。
アカウント名	45	以下のいずれかを記録します。 <ul style="list-style-type: none"> ● 受信ボックス によって配信されるオブジェクトの場合は、BusinessObjects ユーザアカウント名の一覧。 ● FTP によって配信されるオブジェクトの場合は、FTP アカウント名。 ● アンマネージドディスクによって配信されるオブジェクトの場合は、使用されたログインアカウント。 ● SMTP によって配信されるオブジェクトの場合は、SMTP サーバで使用されたログインアカウント。

イベントの詳細	ID	説明
プリンタ名	46	ドキュメントまたはオブジェクトの配信先となるプリンタの名前 (該当する場合)
部数	47	ドキュメントまたはオブジェクトの印刷部数 (該当する場合)
受信者名	48	ドキュメントまたはオブジェクトを受信するユーザの名前 (複数可)。受信者ごとにイベント詳細が生成されます。
アラートイベント ID	92	アラートイベントの CUID。この値は、イベントがアラートによって呼び出された場合にのみ生成されます。
アラートイベント名	93	アラートイベントの名前。この値は、イベントがアラートによって呼び出された場合にのみ生成されます。
配信タイプ	35	配信がどのように開始されたかを示します。 <ul style="list-style-type: none"> "0" は、スケジュールを示します。 "1" は、出力先への送信を示します。 "2" は、公開を示します。 "3" は、アラートが呼び出されたことを示します。

取得

オブジェクトが CMS から取得されました。

- イベントタイプ ID: 1013

ログオン

ユーザのログオン。

- イベントタイプ ID: 1014
- ステータス:
 - "0" は、同時ユーザライセンスログオンに成功したことを示します。
 - "1" は、ログオンの試行に失敗したことを示します。
 - "2" は、指定ユーザライセンスログオンに成功したことを示します。
 - "3" は、非ユーザ (システム) ログインに成功したことを示します。

イベントの詳細	ID	説明
同時接続ユーザ数	50	イベントの呼び出し時にシステム内に存在していたユーザの数

イベントの詳細	ID	説明
クライアントから報告されたホスト名	51	クライアントから報告されたクライアントのホスト名
サーバで解決されたホスト名	52	サーバで解決されたクライアントのホスト名。クライアントのホスト名が解決されない場合、値は記録されません。
クライアントから報告された IP アドレス	53	クライアントから報告されたクライアントの IP アドレス
サーバで解決された IP アドレス	54	サーバで解決されたクライアントの IP アドレス。クライアントの IP が解決されない場合、値は記録されません。

ログアウト

ユーザのログオフ。

- イベントタイプ ID: 1015

イベントの詳細	ID	説明
同時接続ユーザ数	50	イベントの呼び出し時にシステム内に存在していた同時接続ユーザの数

呼び出しイベント

ファイルイベントが呼び出されました。

- イベントタイプ ID: 10016

イベントの詳細	ID	説明
ファイル名	17	モニタリングの対象であり、イベントを呼び出したファイルの名前

20.3.1.1 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。

- イベントの種類 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	セキュリティ権限が変更されたユーザまたはユーザグループ (主体) の ID

カスタムアクセスレベル変更

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: 1000410004

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

イベントの詳細	ID	説明
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。 <code>removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types.</code>
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。 <code>modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types.</code>
主体	118	セキュリティ権限が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: 1000610006

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	オプション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

イベントの詳細	ID	説明
		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	70	<p>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。</p> <pre>DBType=Oracle,DBName=MyADS, Username=USR1,Password="****",SSO=off,DBReconnect=on</pre> <p>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。</p> <div> <p>i 注記</p> <p>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。</p> </div>
自動削除間隔	105	この詳細は、CMC の監査ページで [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。

20.3.1.2 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)。

イベントの詳細	ID	説明
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

20.3.1.3 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

20.3.1.4 ライフサイクルマネジメントのイベント

以下は、SAP BusinessObjects ライフサイクルマネジメントのコンポーネントに固有のイベントです。

共通の詳細

すべてのライフサイクル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	ライフサイクルマネジメントコンソ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)。

設定

ライフサイクル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	ライフサイクルマネジメントコンソ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 settings=enabled, port=900
変更前の設定	101	ライフサイクルマネジメントコンソ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	ライフサイクルマネジメントコンソ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。

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 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	10901	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。

21 プラットフォーム検索

21.1 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence では、プラットフォーム検索が以下の機能によって拡張されました。

- BOE コンテンツと Explorer コンテンツの両方の検索
- 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

i 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。

21.1.1 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、*SAP BusinessObjects Enterprise Java API* リファレンスを参照してください。

21.1.2 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。

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

このフェー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、インデックス操作が中断されることがなくなります。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。

21.2 プラットフォーム検索の設定

21.2.1 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 SAP BusinessObjects Business Intelligence で使用される 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 {BOE_INSTALL_DIR} \warfiles\OpenSearch ディレクトリにコピーされます。

i 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。
- SAP BusinessObjects Business Intelligence 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。

21.2.1.1 手動によるデプロイ

SAP BusinessObjects Business Intelligence 環境に OpenSearch をデプロイするには、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 4.0\warfiles\
2. {INSTALLDIR}\Tomcat6\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 (例 <CMS Name>:<Port Number>)
 - OpenDocURL: OpenDocument アプリケーションの URL (例: 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。

21.2.1.2 WDeploy を使用したデプロイメント

WDeploy を使用して OpenSearch を実装するには、次の手順に従います。

i 注記

Windows コマンドおよび Unix コマンドは、それぞれ wdeploy.bat <parameters> および wdeploy.sh <parameters> として示します。

1. <BOE_Install_Dir>\<Enterprise_DIR>\wdeploy\conf の下にある config.<app server server> ファイルを、インスタンス名、管理ポート、管理ユーザ名、管理パスワードなどの必要な Web アプリケーションサーバパラメータを使用して更新します。
2. 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 (例 <CMS Name>:<Port Number>)
 - OpenDocURL: OpenDocument アプリケーションの URL (例: http://<Web Application Server Host>:<connectorport>/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。
3. <BOE_Install_Dir>\<Enterprise_DIR>\wdeploy の位置から wdeploy.bat <WEB_APPLICATION_SERVER> -Dapp_source_dir=<LOCATION_OF_OpenSearch_Webapp> -DAPP=OpenSearch deploy コマンドを実行します。
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=<BOE_Install_Dir>\<Enterprise_DIR>\warfiles" -DAPP=OpenSearch deploy
```

4. アプリケーションサーバを再起動します。

21.2.2 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 Business Intelligence 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。

21.2.3 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] を選択します。[プラットフォーム検索アプリケーションプロパティ] が表示されます。
4. 必要なプラットフォーム設定を行います。

次の表で、設定可能なプロパティについて説明します。

オプション	説明
検索統計	<p>プラットフォーム検索は、以下の検索統計を提供します。</p> <ul style="list-style-type: none">○ 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。

オプション	説明
インデックス処理の停止/開始	<p>[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。</p> <p>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、確認のダイアログボックスで [OK] をクリックします。</p>
デフォルトのインデックスロケール	<p>プラットフォーム検索では、[CMC] ページで指定したロケールを使用して、すべてのデフォルトの 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。</p> <p>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。</p> <p>CMC の設定プロパティでこの加重を設定できます。</p>
クロール頻度	<p>以下のオプションを使用して、SAP BusinessObjects 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できます。</p> <ul style="list-style-type: none"> 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、継続的クロールでは SAP BusinessObjects BI プラットフォームリポジトリは実行するアクションによって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。 <p>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。</p> <div data-bbox="794 1608 1359 1852"> <p>i 注記</p> <ul style="list-style-type: none"> [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。 </div>

オプション	説明
	<ul style="list-style-type: none"> ○ [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。
インデックスの場所	<p>インデックス処理されたドキュメントは、以下の場所にある共有フォルダに格納されます。</p> <ul style="list-style-type: none"> ○ 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。ワークフローの検索中、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 SAP BusinessObjects 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。 <p>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\ContentStores になります。</p> <p>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ようになります。</p> <p>a. {bobj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores</p> <p>b. {bobj.enterprise.home}\data\PlatformSearchData\workspace\Server1\ContentStores</p> <ul style="list-style-type: none"> ○ 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。インデックス処理されたドキュメントがマスタインデックスに結合さ

オプション	説明
	<p>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。</p> <div data-bbox="815 461 1359 801"> <p>i 注記</p> <ul style="list-style-type: none"> すべてのインデックスの場所は、共有ロケーションである必要があります。 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。 </div>
インデックス処理のレベル	<p>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。</p> <ul style="list-style-type: none"> 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。 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。 <ul style="list-style-type: none"> 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 <div data-bbox="772 1420 1359 1624"> <p>i 注記</p> <p>インデックス処理のレベルを変更すると、SAP BusinessObjects 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。</p> </div>
コンテンツタイプ	<p>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。</p> <ul style="list-style-type: none"> Microsoft Word Microsoft Excel Microsoft PowerPoint テキスト Adobe Acrobat リッチテキスト形式

オプション	説明
	<ul style="list-style-type: none"> ○ Crystal Reports ○ ユニバース ○ Web Intelligence
インデックスの再構築	<p>このオプションを使用して、インデックス処理されたすべての既存コンテンツを削除し、ドキュメント全体を初めから再インデックス処理することができます。</p> <p>インデックス処理のステータスに関係なく、[インデックスの再構築] オプションを選択できます。ただし、インデックス処理が停止している場合、[インデックスの再構築] オプションは機能しない可能性があります。[インデックスの再構築] を選択し、プラットフォーム検索アプリケーションを保存してから閉じてください。</p> <p>インデックス処理が停止していて [インデックスの再構築] を選択した場合は、プラットフォーム検索アプリケーションを保存し、閉じてから、設定ページを再度開き、[インデックス処理の開始] をクリックすると、保存された [インデックスの再構築] オプションによって、自動的にドキュメント全体が再インデックス処理される可能性があります。</p> <p>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] をクリックする必要があります。</p>
インデックス処理から除外するドキュメント	<p>[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。</p> <p>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。</p> <p>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] 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。</p> <ul style="list-style-type: none"> ○ 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

5. [保存して閉じる] を選択します。

i 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初めから増分更新されます。

21.3 プラットフォーム検索の使用

21.3.1 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。

検索インデックスはファイルの指定された場所に保存され、インデックス化されたドキュメントの検索可能コンテンツがすべて含まれます。

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)
- 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 Report 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、および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。

関連リンク

21.3.2 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。

21.3.3 検索結果

21.3.3.1 検索前

21.3.3.1.1 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、SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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 AP BusinessObjects 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 SAP BusinessObjects 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 SAP BusinessObjects 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。

21.3.3.1.2 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 (2008 および 2011)	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、レポートで使用す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、レポートで使用するユニバースメジャーの名前、レポートで使用す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。

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
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、AF ダッシュボードページ、Dashboards、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ン、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、Flash、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	<p>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。</p> <div data-bbox="863 797 1471 965"> <p>i 注記</p> <p>プラットフォーム検索では、Crystal Reports for Enterprise のイベントはサポートされていません。</p> </div>
BI ワークスペース	<ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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。 <div data-bbox="906 1559 1471 1939"> <p>i 注記</p> <p>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。</p> </div>

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
	<ul style="list-style-type: none"> 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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 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) Flash オブジェクトの抽出 <p>また、次世代 Crystal Reports レポートのページごとの読み込みデータもサポートされません。</p>
ユニバース	<p>データコンテンツを検索できます。</p> <div data-bbox="762 1070 1359 1503"> <p>i 注記</p> <p>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するクエリの実行時間が長く、DB サーバのパフォーマンスに影響を及ぼしうる場合は、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。<i>Select distinct SampleColumnName from SampleTableName LIMIT 1000</i></p> </div> <p>ユニバースのインデックス処理を無効化するには、次の手順を実行します。</p> <ul style="list-style-type: none"> セントラル管理コンソール (CMC) にログインします。 [アプリケーション] を選択します。 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。 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。 [保存して閉じる] を選択します。

i 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。

21.3.3.2 検索

ユーザが BI 起動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。

21.3.3.3 検索後

21.3.3.3.1 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。

SAP BusinessObjects Business Intelligence プラットフォームドキュメントは、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)、および Dashboards など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。

21.3.3.3.2 検索結果のランクの正規化

プラットフォーム検索では、ドキュメントのランク付けに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 のページで上記のカテゴリの加重を設定できます。

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 [\[アプリケーション\]](#) 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. [\[ランク\]](#) を選択します。[\[ランク: プラットフォーム検索アプリケーション\]](#) ダイアログボックスが表示されます。このダイアログボックスには、プラットフォームメタデータ、ドキュメントメタデータ、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。要件に合わせて加重を変更できます。
ユーザのロケールは、BI 起動パッドアプリケーションの基本設定のロケールで設定するロケールです。
4. [\[保存\]](#) 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](#) [ページ 512] 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。

21.3.3.3.3 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 アプリケーションの [\[デフォルトのインデックスロケール\]](#) で設定されたロケールを使用して、すべての SAP BusinessObjects Business Intelligence 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 の設定ページでこの加重を設定できます。

21.3.3.3.4 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 アプリケーションで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。

i 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

21.3.3.5 SAP BusinessObjects Explorer からの検索結果の連結

プラットフォーム検索では、SAP BusinessObjects Explorer からの検索要求が連結され、情報スペースと SAP BusinessObjects Business Intelligence のコンテンツが表示されます。

SAP BusinessObjects Explorer からの検索結果は、メタデータのカテゴリ別にグループ化されます。サポートされる情報スペース用のファセットには、種類、場所、および更新時間が含まれます。

SAP BusinessObjects Explorer は、検索クエリ内の検索用語ごとに、用語の頻度をプラットフォーム検索に送信します。プラットフォーム検索は、用語の頻度の平方根を合計した数を使用して関係性を計算します。結果として生じた値は、各情報スペースにスコアとして割り当てられます。その後、結果はスコア順に並べ替えられ、クライアントに送信されます。

21.4 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、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. SAP BusinessObjects BI プラットフォーム認証セクションにユーザのロールをインポートします。

21.4.1 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。

21.4.2 SAP BusinessObjects Business Intelligence 認証へのユーザロールのインポート

SAP BusinessObjects Business Intelligence 認証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。

i 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。

21.5 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。

21.6 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。

プラットフォーム検索のイベント ID は 1009 で、以下のような 4 つのプラットフォーム検索固有イベント詳細があります。

- 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 BOE 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 ID 1009
- 値 Sales のイベント詳細 ID 19
- 値 5 のイベント詳細 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
- オブジェクト
- サービスサイド監査であるために値が 0 である 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 ID 1009
- 値 Sales のイベント詳細 ID 19
- 値 5 のイベント詳細 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 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 ID 1009
- 値 Sales のイベント詳細 ID 19
- 値 0 のイベント詳細 ID 63
- 例外メッセージを含むイベント詳細 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

21.7 トラブルシューティング

21.7.1 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。

21.7.2 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。

i 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 SAP BusinessObjects Business Intelligence 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. ファイルシステムで、拡張子が .gif の APS 追跡ログが格納されている {BOE Install Dir}\logging\ 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。

i 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 Report コンテンツのインデックス処理は、バージョン 2008 および 2011 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の一部であるタイトル、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。

BI 起動パッドに製品ロケールとして設定されている言語で検索結果を取得できない

プラットフォーム検索では、CMC に設定されているインデックスロケールに基づいて BI プラットフォームリポジトリのコンテンツを検索し、インデックス処理します。BI 起動パッドに設定されている製品ロケールが CMC に設定されているロケールと異なる場合、プラットフォーム検索は結果を取得しません。

インデックスロケールの設定方法の詳細については、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。

SAP BusinessObjects Explorer の情報スペースを取得できない

SAP BusinessObjects Explorer サーバが停止しているか無効になっていないかを確認します。SAP BusinessObjects Explorer から検索結果を取得するには、プラットフォーム検索用のサーバを有効にします。

SAP NetWeaver Enterprise Search で、SAP BusinessObjects Business Intelligence 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。

関連リンク

[インデックス処理失敗一覧](#)

[CMC でのアプリケーションプロパティの設定](#) [ページ 512]

[検索可能コンテンツタイプ](#) [ページ 606]

22 フェデレーション

22.1 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 Business Intelligence 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イメ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、Flash、Word、テキストファイル、リッチテキストファイル、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	
BI プラットフォーム	フォルダ、イベント、カテゴリ、カレンダー、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	
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。

22.2 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。

22.3 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。

22.3.1 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。 i 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。	<ul style="list-style-type: none">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。	<ul style="list-style-type: none">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。	<ul style="list-style-type: none">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

関連リンク

[レプリケート先サイトで必要な権限](#) [ページ 621]

22.3.2 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。

i 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にかかわらず、オブジェクトを複製します。	<ul style="list-style-type: none">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

対処方法	説明	必要な権限
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。	<ul style="list-style-type: none"> 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

関連リンク

[レプリケート元サイトで必要な権限](#) [ページ 621]

22.3.3 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。	<ul style="list-style-type: none"> 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	<p>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。</p> <p>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。</p>	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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

対処方法	説明	必要な権限
	<p>i 注記</p> <p>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。</p>	

22.3.4 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。

22.3.5 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する“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。

i 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。

22.4 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

22.4.1 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

22.4.2 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。

i 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

関連リンク

[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](#) [ページ 648]

22.4.3 [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ます、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、通常の一方または双方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、通常の一方または双方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、通常の一方または双方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。

i 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。

i 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。

i 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。

22.5 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。

i 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子を持つことになり、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。

i 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があります。

i 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。

i 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。

注記

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。

22.6 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。

22.7 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。 i 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。 i 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、Flash、Word、テキストファイル、リッチテキストファイル、Shockwave フラッシュファイル
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、カレンダー、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

i 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

22.7.1 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。

22.7.1.1 [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。

22.7.1.2 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 ▶ の順にクリックします。
[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。

依存関係オブジェクトオプション	定義
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よって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 Flash オブジェクトのサポートされている依存項目を含む	Flash オブジェクトが依存する Crystal レポート、ハイパーリンク、Web Intelligence ドキュメントまたはユニバースを複製します。
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。

i 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。

i 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。

22.7.2 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。

22.7.2.1 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。

関連リンク

[レプリケーション一覧の作成](#) [ページ 630]

22.7.2.2 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。

関連リンク

[レプリケーション一覧の作成](#) [ページ 630]

22.8 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。

i 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。

22.8.1 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。

22.8.1.1 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。

22.8.1.2 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。

i 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。次の形式を使用します。 <code>http://<application_yourserver_machine_name>:<port>/dswsbobje</code> 例: <code>http://<mymachine.mydomain.com>:<8080>/dswsbobje</code>

フィールド	説明
リモートシステム CMS	<p>フェデレーション Web サービスを通じてアクセス可能な、接続先の 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。"CMS 名: ポート" という形式を使用します。たとえば、mymachine:6400 とします。</p> <p>i 注記</p> <p>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。</p>
ユーザ名	<p>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。</p> <p>i 注記</p> <p>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。</p>
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。

関連リンク

[オブジェクトのクリーンアップの管理](#) [ページ 639]

22.8.2 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

- CMC の [フェデレーション] エリアを表示します。
- [リモート接続] をクリックします。
- 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。

22.9 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。

i 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。

22.9.1 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。

22.9.1.1 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	<p>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。</p> <div style="background-color: #fff9c4; padding: 10px; margin-top: 10px;"> <p>i 注記</p> <p>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。</p> </div>
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。

オプション	説明
	i 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。

関連リンク

[オブジェクトのクリーンアップの管理](#) [ページ 639]

[競合の検出と解決の管理](#) [ページ 641]

[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](#) [ページ 648]

22.9.2 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行う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。

i 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。

22.9.2.1 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。

22.9.3 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。

22.9.3.1 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。
Schedule	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。

22.9.4 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。

22.10 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。

22.10.1 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。

22.10.2 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行うと、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を確認します。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を確認し、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。

i 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。

22.10.3 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。

i 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を確認します。

- 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。

関連リンク

[オブジェクトのクリーンアップの制限](#) [ページ 640]

22.11 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。

22.11.1 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。

i 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。

i 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。

i 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。

i 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。

i 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

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。

- 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。
- 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。

22.11.2 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。

i 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。

i 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。

i 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。

i 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。

i 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。

i 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。

i 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。

i 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。

i 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。

i 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。

22.12 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。

22.12.1 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化するには、次を入力します。

`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。

22.12.2 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。

i 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、次の場所にある Axis2.xml ファイルを変更します。

```
<<App Server Installation Directory>\dswsbobje\Web-Inf\conf>
```

たとえば、次のようになります。

```
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>
```

i 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。

22.12.3 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 サービスを無効化する:

- “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`

サービス名の変更前:

`<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。

22.13 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へ送信できます。

22.13.1 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に変更があった場合、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。

関連リンク

[セキュリティアクセス権の管理](#) [ページ 620]

22.13.2 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。

i 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。

22.13.3 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。

関連リンク

[セキュリティアクセス権の管理](#) [ページ 620]

22.14 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。

22.14.1 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。

22.14.2 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。

i 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。

22.14.3 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、本稼働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、この設定を本稼働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。

i 注記

LifeCycle Manager を使用している場合、レプリケーション一覧プロ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。

22.14.4 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。

i 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、コピーにはレプリケーション情報は含まれません。

22.15 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に長時間接続していると、他の 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利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 "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for Tomcat
JAVA_OPTS="-Dboj.enterprise.home=${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
```

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、BIAR 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 90 MB 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。

i 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>`

関連リンク

[エラーメッセージのトラブルシューティング](#) [ページ 657]

[フェデレーションでの Web サービスの使用](#) [ページ 646]

[現在のリリースの制限](#) [ページ 656]

22.15.1 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。

関連リンク

[オブジェクトのクリーンアップの管理](#) [ページ 639]

22.15.2 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 ASX00Fyvy0FJnRcD0dZNTZg (オブジェクト番号 1285 のプロパティ SI_PARENT_GUID) は有効な GUID ではありません。

このエラーは、親と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。有効なクエリではありません。(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エラー: クエリプロセッサでクエリの最適化中に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:MaxPermSize=256m"` という行を追加します。
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)オブジェクトマネージャの領域

エラー例: 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。

レプリケート先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>>"` 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。

12)ユニバースエラー

エラー例: `processDPCommands` API を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。

関連リンク

[ベストプラクティス](#) [ページ 653]

[現在のリリースの制限](#) [ページ 656]

23 ERP 環境の追加設定

23.1 SAP NetWeaver 統合の設定

23.1.1 SAP Netweaver Business Warehouse (BW) との統合

23.1.1.1 概要

この節では、SAP NetWeaver Business Warehouse 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。

関連リンク

[SAP 認証の設定](#) [ページ 254]

23.1.1.1.1 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。

i 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。
 - 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。

関連リンク

[アクセスレベルの使用](#) [ページ 113]

[BI プラットフォームでのアクセス権の動作](#) [ページ 100]

23.1.1.1.2 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。

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。

i 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。

23.1.1.2 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。

23.1.1.3 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。

23.1.1.3.1 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 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。

23.1.1.3.2 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。

23.1.1.3.3 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。

23.1.1.3.4 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。

23.1.1.3.5 ローカル SAP ゲートウェイを使用した BW Publisher の設定

i 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](#) [ページ 665]
- [BW Publisher の宛先の設定](#) [ページ 665]

23.1.1.3.6 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。

BusinessObjects XI Integration for SAP™ のテスト済みの環境の一覧は、製品メディアに収録の `platforms_JP.txt` ファイルを参照してください。このファイルには、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。

23.1.1.4 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。

23.1.1.5 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

23.1.1.6 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。

23.1.1.7 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 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](#) [ページ 261]
- [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](#) [ページ 661]
- [デフォルトフォルダセキュリティパターンについて](#) [ページ 662]

23.1.1.8 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。

表 21: 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 S_TCODE	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	実行 (16)

権限オブジェクト	フィールド	値
	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)

表 22: 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

権限オブジェクト	フィールド	値
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
	ACTVT	照会 (03)

23.1.1.9 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。

23.1.1.9.1 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。

- a) [エイリアス] ボックスに記述名を入力します。スペースや特殊文字は使用しないでください。
スペースや特殊文字を使用すると、エイリアス名を使用してエンタープライズポータルを設定する際に特殊な処理が必要になります。
- b) BusinessObjects Enterprise CMS を実行しているマシンの名前を入力します。

i 注記

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。

- c) 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。

デフォルトシステムは、使用可能なシステムの一覧で緑色のチェックマークで示されます。

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。

i 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。詳細については「BW Publisher インストールの配布」を参照してください。

7. 追加した宛先を選択し、宛先名の左側にあるグレーのボックスをクリックして宛先をテストします。

8. [CE 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。

9. [HTTP] タブで次を実行します。

- a) [プロトコル] ボックスに「http」と入力します。
BI プラットフォームに接続された Web サーバが https を使用するように設定されている場合は、「https」と入力します。
- b) [Web サーバのホストおよびポート] ボックスに、BI 起動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、たとえば「boserver01.businessobjects.com:8080」のようにポート番号を含めてください。
- c) [パス] ボックスに「sap」と入力します。最初と最後にフォワードスラッシュは使用しないでください。
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。
- d) [ビューアプリケーション] ボックスにビュー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 起動パッドを使用する BI プラットフォーム用のデフォルトビューを使用するには、「openDocument.jsp」と入力します。
BI プラットフォームがデフォルトの ASP.NET 設定を使用して Windows にインストールされている場合は、「report/report_view.aspx」と入力してデフォルトのブラウザを使用します。

10. [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。

11. **[ルール]** タブを使用して、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ルールを追加します。

詳細については、「SAP ロールのインポート」を参照してください。

12. **[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ルールのリストが表示されます。

i 注記

各ルールは 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ル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 **[ルール]** タブに戻り、**[ルールの再割当]** をクリックします。

13. このシステムに公開するルールを選択し、**[OK]** をクリックします。

14. この BI プラットフォームシステムに公開されるコンテンツのデフォルトのセキュリティ設定を設定するには、**[レイアウト]** タブをクリックし、レポートおよびルールフォルダでデフォルトで使用するセキュリティ設定を選択します。

i 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ルールごとに 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、そのル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。

i 注記

BI プラットフォームシステムを設定した後に、デフォルトのセキュリティレベルを変更しても、公開されたル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。BI プラットフォームに公開されたすべてのル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、システム内のルールフォルダとショートカットを削除し、セキュリティ設定を変更し、ルールとレポートを再公開します。ルールフォルダとショートカットを削除してもレポートは削除されません。

15. **[OK]** をクリックし、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。

BW から BI プラットフォームにレポートを公開できます。

関連リンク

[BW Publisher インストールの分散](#) [ページ 663]

[SAP ロールのインポート](#) [ページ 261]

23.1.1.10 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、特定のル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](#) [ページ 685]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。

23.1.1.11 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。

i 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。

関連リンク

[バックグラウンドでの公開のスケジュール](#) [ページ 672]

23.1.1.12 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](#) [ページ 673] を参照してください。

23.1.1.13 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。

23.1.1.14 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。

23.1.1.14.1 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](#) [ページ 672]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。

23.1.1.14.2 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。

i 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。

23.1.1.15 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。

23.1.1.16 SAP データ処理の設定

23.1.1.16.1 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_OPENSQLE_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にかかわらず、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 Adaptive 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 (すなわち、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。

i 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。

関連リンク

[バッチモードでのレポートのスケジュール \(オープン SQL クエリを使用\)](#) [ページ 699]

23.1.1.16.2 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_OPENSQLE_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) にログインします。
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作成されています。

```
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ト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。

i 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。

23.1.1.17 SAP 移送の設定

23.1.1.17.1 概要

SAP BusinessObjects Enterprise には、Open 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、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、および ODS 移送の 8 つの移送があります。

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。

i 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。

23.1.1.17.2 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。

関連リンク

[権限の登録および適用](#) [ページ 685]

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。

各移送タイプを以下で説明します。

- **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ト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ー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ト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。

i 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。

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 Business Objects 名前空間の下に自動的に登録されます。R/3 および MY SAP ERP の比較的新しいバージョンでは、SAP Business Objects 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 Business Objects 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 のマニュアルを参照してください。

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 ディレクトリの下に `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。

i 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。

i 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。

移送

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ト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/OPENSQ	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

オブジェクト	種類	説明
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
/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

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

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

オブジェクト	種類	説明
/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

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。

i 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

コンテンツ管理ワークベンチ

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

オブジェクト	種類	説明
/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

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

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

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
/CRYSTAL/CX_NO_MORE_CELLS	クラス	例外
/CRYSTAL/ CX_NO_MORE_MEMBERS	クラス	例外

オブジェクト	種類	説明
/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

23.1.1.18 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。お手持ちの SAP のバージョンにおける手順の詳細については、SAP のマニュアルを参照してください。

i 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。

i 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 BusinessObjects XI Integration for SAP 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。

23.1.1.18.1 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。

関連リンク

[コンテンツ管理ワークベンチでの公開の設定](#) [ページ 665]

23.1.1.19 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。

23.1.1.19.1 Crystal Reports 内のアクション

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>**
S_RS_COMP1	RSZCOMPID	<COMP_ID>**

権限オブジェクト	フィールド	値
	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。

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。

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。

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>**
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。

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。

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。

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。

レポートの保存と同時の BusinessObjects Enterprise 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> ***
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。

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。

23.1.1.19.2 BI 起動パッド内のアクション

SAP 認証情報を使用した BusinessObjects Enterprise 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

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

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	OCRM_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。

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>**

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
S_RS_ODSO	RSINFOAREA	<INFO_AREA>**
	RSODSOBJ	OCRM_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。

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
	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>*

権限オブジェクト	フィールド	値
	ACTVT	16
S_RS_ODSO	RSINFOAREA	<INFO_AREA>**
	RSODSOBJ	OCRM_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。

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

23.1.1.19.3 SAP Netweaver (ABAP) 内のアクション

オープン SQL ドライバを使用して *Crystal Reports* で

ここでは、Open SWL 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。

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

権限オブジェクト	フィールド	値
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16

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/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	01

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/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	02

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	STOR、STOM
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR

権限オブジェクト	フィールド	値
	RFC_NAME	/CRYSTAL/OPENSQ
	ACTVT	16

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/OPENSQ
	ACTVT	16

23.1.1.19.4 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

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

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

権限オブジェクト	フィールド	値
	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。

関連リンク

[データソースの場所の設定](#) [ページ 696]

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	STOR、STOM

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

23.1.1.19.5 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

SAP サーバへのログイン

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
	ACTVT	16

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
	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

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

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

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_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

23.1.1.19.6 BI プラットフォーム内のアクション

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

i 注記

CLASS の値は空白です。

パ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/OPENSQ, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

i 注記

CLASS の値は空白です。

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)

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: 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)	* <div> i 注記 セキュリティ機能を強化するために、SAP BusinessObjects Enterprise 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表示できます。 </div>

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	

23.2 JD Edwards 統合の設定

23.2.1 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。

23.2.1.1 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. SAP Crystal Reports を再起動します。

23.2.1.2 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. [\[SSO コンテキストをデータベースログオンに使用する\]](#) に [\[crdb_pseone\]](#) 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. Crystal Reports サーバを再起動します。

23.2.2 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)

23.2.2.1 SSL を使用した JD Edwards EnterpriseOne のデータ接続を有効にする

i 注記

このタスク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。

次のレジストリ キーの下に 2 つのレジストリ値を設定します。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Business  
Objects\Suite 12.0\Integration Kit for  
PeopleSoft EnterpriseOne\QRY\Instances\noname]  
"CommunicationProtocol"="ssl"  
"SSL Configuration File"="C:\Program  
Files\Business Objects\BusinessObjects XI 13.0\sslconf.properties"
```

変更を有効にするには、BI プラットフォームレポーティングサービス (Adaptive Job Server など) を再起動する必要があります。

23.2.2.2 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。次はその例です。

```
[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。

23.3 PeopleSoft Enterprise 統合の設定

23.3.1 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。

23.3.1.1 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. SAP Crystal Reports を再起動します。

23.3.1.2 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. [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_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. SAP Crystal Reports を再起動します。

23.3.2 セキュアソケットレイヤ通信の設定

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)

23.3.2.1 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、SAP 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。次はその例です。

```
[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\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\ です。

23.3.2.2 SSL を使用した PeopleSoft Query Server を有効にする

i 注記

このタスク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。

次のように、クエリサーバごとにレジストリキーの下に 2 つのレジストリ値を設定します。

次はその例です。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Business
Objects\Suite 12.0\Integration Kit for
PeopleSoft\QRY\Instances\noname]
"CommunicationProtocol"="ssl"
"SSL Configuration File"="C:\Program
Files\Business Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\sslconf.properties"
```

これらの変更を有効にするには、BusinessObjects レポートینگサーバ (Adaptive Job Server など) を再起動する必要があります。

23.3.2.3 SSL を使用したセキュリティブリッジを有効にする

i 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。

crpsepmsecuritybridge.bat に次の引数を追加して、この .bat ファイルを実行します。

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir="d:\ssl"
-DtrustedCert=cacert.der
```



```
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
```

.bat ファイル内の適切な位置、すなわち java.exe のすぐ後で、-jar 引数の前に引数を追加していることを確認してください。以下はその例です。

```
@ECHO OFF
SETLOCAL
SET PATH=%PATH%;C:\Program Files\Business
Objects\BusinessObjects Enterprise 12.0\win32_x86\;C:\Program
Files\Business Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\epm;
"C:\Program Files\Business Objects\javasdk\bin\java.exe" -
Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir="C:\!test" -DtrustedCert=cacert.der
-DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar "C:\Program Files\Business
Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\epm\crpsepmsecuritybridge.jar" %1 "language"
"C:\Program Files\Business
Objects\LanguagePacks.xml\LanguagePacks.xml"
```

次の表は、これらの例に対応する説明を示しています。

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。

23.3.3 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。

23.3.3.1 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として 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。

i 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。

i 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。

23.3.3.2 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。

i 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。

23.4 Siebel 統合の設定

23.4.1 SAP BusinessObjects Business Intelligence 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、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れば、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。

i 注記

Siebel 7.7 および Siebel 8.0 の各サブフォルダには、Siebel のバージョン 7.7 および 8.0 で使用するさまざまなファイルが含まれます。



23.4.1.1 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 <<install directory>>\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. [SAP BusinessObjects Integration] プロジェクトをクリックします。

23.4.2 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**  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**  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
 - キャプション: 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](#) [ページ 708] を参照してください。

23.4.2.1 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\agent.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。

23.4.3 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。

23.4.3.1 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. BI プラットフォームのセントラル管理コンソール (CMC) を表示します。
 2. [認証]をクリックします。
 3. [Siebel]をダブルクリックします。
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 起動パッドを開きます。

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。

23.4.3.2 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\WEApp\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"
```

i 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。

i 注記

userDomain では、大文字と小文字が区別されます。

23.4.3.3 コンテキスト認識を確認する

1. 変更された汎用 Web メニューを使用した Siebel アプリケーションにログオンします。
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 起動パッド] 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、セッションがタイムアウトする前に、最初にログオンするときのみ必要です。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。

i 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インできません。

23.4.3.4 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 起動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、`<Root Dir>\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 Business Objects ビジネスコンポーネントと関連付けられた Siebel 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。

i 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。

23.4.4 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。

23.4.4.1 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。

23.4.4.2 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。

23.4.5 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、BusinessObjects XI 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\Business Objects\SAP BusinessObjects Enterprise XI\` です。

24 管理および設定ログ

24.1 コンポーネントからのログのトレース

システム管理者およびサポート担当者は、トレースにより 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内で発生するアクティビティについてレポートすることができます。

BI プラットフォームサーバによって生成されるシステムレベルのメッセージがトレースされ、ログファイルに書き込まれます。これらのログファイルは、システム管理者がパフォーマンスの監視またはデバッグ用に使用します。トレースとは、監視対象コンポーネントの操作中に発生するイベントの記録です。トレース済みイベントには、一方のエンドの重大な例外エラーから他エンドの単純なステータスメッセージが含まれます。

トレースログ

トレースメッセージは、ジェネリックログファイル（.glf）拡張子の下に保存されるログファイルに収集されます。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、実際には指定した重要度レベル未満のトレースを削除するフィルタです。削除されたトレースは出力ログファイルに書き込まれません。コンポーネントのトレースログを監視することにより、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して増えた負荷を処理する必要があるかどうか、または増えた負荷がパフォーマンスに重大な影響を与えることがないかどうかを確認できます。

24.2 トレースログレベル

次の表では、BI プラットフォームコンポーネントに対し使用できるトレースログレベルを説明します。

レベル	説明
未指定	トレースログレベルは他のメカニズム（通常は .ini ファイル）を介して指定されます。
なし	<p>トレースログレベルが [なし] に設定されている場合、指定した重要度レベルを下回るトレースをオプションとして抑制するフィルタが無効になります。</p> <div><p>i 注記</p><p>[なし] トレースログレベルは、トレース機能がオフになっているという意味ではありません。システムリソースのモニタリングは続けられ、アサーションの失敗など発生頻度の低い重要なイベントに対してはトレースが記録されます。</p></div>
低	エラーメッセージは記録するが、警告やステータスメッセージの多くを無視するようトレースログフィルタが設定されます。ただし、非常

レベル	説明
	<p>に重要なステータスメッセージは、コンポーネントの起動、シャットダウン、またはリクエストメッセージの開始や終了時にも記録されます。</p> <p>i 注記 このレベルは、デバッグ目的の場合はお勧めしません。</p>
中	<p>エラー、警告、ステータスメッセージの多くをログ出力に含めるよう、トレースログフィルタが設定されます。重要性が最小、または詳細度が高いステータスメッセージは除外されます。このレベルは、デバッグ目的には詳細度が足りません。</p>
高	<p>フィルタによって除外されるメッセージはありません。このレベルは、デバッグ目的の場合にお勧めします。</p> <p>i 注記 トレースログレベルを [高] にすると、システムリソースに悪影響を与えることがあります。CPU 利用率やファイルシステム内の保存スペースが増加することがあります。</p>

24.3 サーバのトレースの設定

監視対象の BI プラットフォームサーバのトレースは特定のログファイル (.glf) に書き込まれ、ログフォルダまたはディレクトリに格納されます。Windows プラットフォームでは、Logging ディレクトリはデフォルトでは Program Files <INSTALLDIR>\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\logging にあります。Unix の場合、このディレクトリは <INSTALLDIR>/sap_bobj/logging にあります。

i 注記

.glf ファイル名は、略称 ID、サーバ名、参照番号の組み合わせとしてフォーマット化されています。たとえば、aps_mysia.AdaptiveProcessingServer_trace.000012.glf です。一度ログファイルのサイズが 1 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。

管理者は、特定のサーバまたはサーバのコレクション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。トレースログレベルは、以下の推奨方法で変更することができます。

- セントラル管理コンソール (CMC) の特定のサーバまたはサーバグループに対する [トレースログサービス] を使用する。
- 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マニュアルで変更する。

特定のサーバのトレースログレベルのみを変更する場合は、CMC の [トレースログサービス] の使用をお勧めします。その他のトレースパラメータを変更するには、BO_trace.ini ファイルを再設定する必要があります。

24.3.1 CMC にサーバトレースログレベルを設定する

サーバのトレースレベルは他のトレース設定に影響を与えないで調整できます。次の手順に従って、トレースログレベルを調整します。

1. CMC の[[サーバ](#)]管理エリアを表示します。
2. トレースログレベルを変更するサーバにアクセスします。
 - a) サーバカテゴリをクリックし、特定のサーバ“カテゴリ”からサーバにアクセスします。
 - b) 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。
3. 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。
4. [[トレースログ設定](#)] エリアで、[[ログレベル](#)] リストから該当する設定を選択します。
5. [[保存して閉じる](#)] をクリックし、変更したトレースログレベルを提出します。

新しいトレースログレベルが 1 分以内に有効になります。

ログファイルに別のディレクトリを指定する場合は、`-loggingPath` パラメータと[[コマンドラインパラメータ](#)] エリアのターゲットディレクトリへのパスを使用します。この変更は、サーバを再起動するまで有効になりません。

関連リンク

[トレースログレベル](#) [ページ 495]

24.3.2 CMC で管理されている複数のサーバにトレースログレベルを設定する

1. CMC の[[サーバ](#)]管理エリアを表示します。
使用可能なサービスカテゴリは、[[サーバ](#)] ページに表示されます。
2. トレースログレベルをリセットするサーバにアクセスします。
 - a) サーバカテゴリをクリックし、特定のサーバカテゴリからサーバにアクセスします。
 - b) ナビゲーションペインの [[サーバ一覧](#)] をクリックし、サーバの完全一覧にアクセスします。
3. サーバを選択します。
複数のサーバを選択するには、[Ctrl](#) キーを押しながら選択します。
4. 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](#)] 画面が表示されます。
5. [[トレースログ設定](#)] エリアで、[[ログレベル](#)] リストから該当する設定を選択します。
6. [[OK](#)] をクリックし、変更したトレースログレベルを提出します。

新しいトレースログレベルが 1 分以内に有効になります。

ログファイルに別のディレクトリを指定する場合は、`-loggingPath` パラメータと[[コマンドラインパラメータ](#)] エリアのターゲットディレクトリへのパスを使用します。この変更は、サーバ (複数) を再起動するまで有効になりません。

関連リンク

[トレースログレベル](#) [ページ 495]

24.3.3 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 ファイルは毎分読み取られ、デフォルトでは、トレースが無効になるように設定されています。BO_trace.ini ファイルを使ってトレースをアクティブにして設定するには、次の手順を実行します。

1. BO_trace.ini ファイルを開きます。
 - Windows のデフォルトの場所は、<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\ です。
 - Unix のデフォルトの場所は、<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/ です。
2. *Trace Syntax and Setting* セクションで必要な行をコメント解除します。
3. 必要に応じて、サーバトレースパラメータを変更します。

次の表に、サーバトレースの設定に使用する一般的なパラメータの一覧を示します。

パラメータ	入力される値	説明
active	false, true	true に設定すると、importance パラメータで設定したしきい値を満たすトレースメッセージがトレースされます。false に設定すると、トレースメッセージは "importance" のレベルに基づいてトレースされません。デフォルト値は false です。
importance	'<<','<=','==','>=','>>','xs','s','m','l','xl' i 注記 importance = xs または importance = << は最も冗長な オプションで、importance = xl または importance = >> は最も 冗長性のないオプションです。	トレースメッセージのしきい値を指定します。しきい値を超えたすべてのメッセージがトレースされます。デフォルト値は m (中) です。
alert	false, true	true に設定すると、severity パラメータで設定したしきい値を満たすトレースメッセージがトレースされます。false に設定すると、トレースメッセージは "severity" のレベルに基づいてトレースされません。デフォルト値は true です。
severity	「S」、「W」、「E」、「A」、「F」。	メッセージをトレースできるしきい値の重大度を指定します。表示される severity の下にあるすべての情報が記録されます。そのため、「E」設定ではエラー、アサート、致命的の各トレースがログに記録されます。「S」はディスク領域を最も消費します。デフォルト値は 'E' です。 <ul style="list-style-type: none">○ S = 成功○ W = 警告

パラメータ	入力される値	説明
		<ul style="list-style-type: none"> ○ E = エラー ○ A = アサート ○ F = 致命的
size	指定可能な値は、1000 以上の整数です。	新しいトレースログファイルが作成されるまでの、トレースログファイルに含まれるメッセージの数を指定します。デフォルト値は 100000 です。
keep_num	指定可能な値は、1000 以上の整数です。	保持するログの数を指定します。
administrator	文字列または整数	<p>出力ログファイルで使用する注釈を指定します。次はその例です。</p> <pre>administrator = "hello"</pre> <p>この文字列がログファイルに挿入されます。</p>
log_dir		出力ログファイルディレクトリを指定します。デフォルトでは、ログファイルは、Logging フォルダに保存されます。
always_close	on, off	トレースがログファイルに書き込まれた後にログファイルを閉じるかどうかを指定します。デフォルト値は off です。

4. BO_trace.ini ファイルを保存して閉じます。

この設定変更は、すべてのサーバを再起動するまで有効になりません。

例

```
active=false;
severity='E';
importance=='';
size=1000000;
keep_num=437;
```

24.3.3.1 サーバごとのトレースを設定する

BO_trace.ini ファイルを使用して BI プラットフォームサーバのトレースパラメータを指定します。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。

1. BO_trace.ini ファイルを開きます。

- Windows のデフォルト場所は、<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf/ です。
- Unix のデフォルトの場所は、<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/ です。

2. [Trace Syntax and Setting](#) セクションで必要な行をコメント解除します。

3. 特定のサーバにトレース設定を指定するには、以下の例に示すように、IF ステートメントを使用します。

```
if (process == "aps_MySIA.ProcessingServer")
{
    active = true;
    importance = '<<' ;
    alert = true;
    severity = ' ';
    keep_num = 487;
    size = 100 * 1000;
}
```

4. BO_trace.ini ファイルを保存して閉じます。

変更した設定が実装されます。新規設定により、特定のサーバに CMC で指定されたトレースログレベルがすべて上書きされます。

24.4 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 Web アプリケーションのトレースは、ログファイル (.glf) 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フォルダに格納されます。トレースログファイルは、デフォルトでは \$userHome/SBOPWebapp_\$application_\$IPAddress_\$port/ ディレクトリにあります。

i 注記

Windows で Tomcat は、デフォルトでローカルシステムアカウントで実行されるようにインストールおよび設定されるため、UserHome は Windows ドライブのルート (つまり、C:\) になります。

管理者は、特定の Web アプリケーションまたは Web アプリケーションのコレクション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。トレースログレベルは、以下の推奨方法で変更することができます。

- セントラル管理コンソール (CMC) で、[\[トレースログ\]](#) アプリケーション設定を使用する。
- BO_trace.ini のトレースログレベルおよびその他のすべてのトレース設定をマニュアルで再設定する。このファイルは、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。

BOE Web アプリケーションのトレースログレベルのみを変更する場合は、CMC オプションの使用を強くお勧めします。すべてのトレースパラメータを変更するには、BO_trace.ini ファイルを再設定する必要があります。

i 注記

BO_trace.ini ファイルを再設定する前に、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 を再設定したら、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。

24.4.1 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

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 起動パッド
- OpenDocument
- Web サービス
- プロモーションマネジメント
- バージョン管理
- 差分の視覚化

他のすべての Web アプリケーションをトレースするには、手動の方法を使用して対応する `BO_trace` ファイルを設定してください。

1. CMC の **[アプリケーション]** 管理エリアを表示します。
[アプリケーション] ダイアログボックスが表示されます。
2. 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。
[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。
3. **[ログレベル]** リストから必要な設定を選択します。
4. **[保存して閉じる]** をクリックして、トレースログレベルを送信します。

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。

関連リンク

[トレースログレベル](#) [ページ 495]

24.4.2 BO_trace.ini ファイルを使用してトレース設定を手動で変更する

`BO_trace.ini` ファイルは、`BOE` ファイルおよび `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。このファイルは、常に Web アプリケーションサーバ上でアクセスできるわけではありません。以下の、事前ステップを実行する必要があります。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しておく必要があります。

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。

i 注記

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中の場合は、`BO_trace.ini` ファイルへは以下のディレクトリでアクセスできます。Web アプリケーションをアンデプロイし、直接ファイルを変更する必要はありません。

- `BOE.war` ファイルのトレース設定ファイルは、`<INSTALLDIR>\Tomcat6\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>\Tomcat6\webapps\dswsbobje\WEB-INF\conf にあります。

バンドルされた Tomcat Web アプリケーションサーバを使用中の場合は、ステップ 3 にスキップします。

- BOE ファイルまたは dswsbobje.war ファイルの 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。
 - デフォルトで、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は、ディレクトリ <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog にあります。
 - デフォルトで、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は、ディレクトリ <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf にあります。
- BO_trace.ini ファイルを開きます。
 - Windows のデフォルトの場所は、<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf です。
 - Unix のデフォルトの場所は、<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/ です。
- Trace Syntax and Setting* セクションで必要な行をコメント解除します。
- 必要に応じて、サーバトレースパラメータを変更します。
次の表に、サーバトレースの設定に使用できるすべてのパラメータを示します。

パラメータ	入力される値	説明
active	false, true	true に設定した場合、現在のプロセスまたはサーバのトレースが有効になります。デフォルト値は false です。
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl <div> i 注記 importance = xs は最も冗長なオプションで、importance = xl は最も冗長性のないオプションです。 </div>	トレースメッセージのしきい値を指定します。しきい値を超えたすべてのメッセージがトレースされます。デフォルト値は m(中) です。
alert	false, true	重大なシステムイベントに対するトレースを自動的に有効にするかどうかを指定します。デフォルト値は true です。
severity	'S', 'W', 'E', 'A', 'F', success, warning, error, assert, fatal	メッセージをトレースできるしきい値の重大度を指定します。'S' はディスク領域を最も消費します。デフォルト値は 'E' です。
size	指定可能な値は、1000 以上の整数です。	新しいトレースログファイルが作成されるまでの、トレースログファイルに含まれるメッセージの数を指定します。デフォルト値は 100000 です。

パラメータ	入力される値	説明
keep	false 、 true	新しいファイルが作成された後に古いログファイルを保持するかどうかを指定します。デフォルト値は false です。
administrator	文字列または整数	出力ログファイルで使用する注釈を指定します。次はその例です。 <pre>administrator = "hello"</pre> この文字列はログファイルに挿入されます。
log_dir		出力ログファイルディレクトリを指定します。デフォルトでは、ログファイルは、Logging フォルダに保存されます。
always_close	on 、 off	トレースがログファイルに書き込まれた後にログファイルを閉じるかどうかを指定します。デフォルト値は off です。

```
active=false;
severity='E';
importance='==';
size=1000000;
keep=false;
```

6. BO_trace.ini ファイルを保存して閉じます。
 7. 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。
- 変更済みトレース設定は、次回 Web アプリケーションにログオンすると有効になります。

24.4.2.1 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します。設定は、デプロイされた WAR ファイルに関連付けられたすべてのアプリケーションに影響します。管理者は BO_trace.ini ファイルを使用して、指定した Web アプリケーションに特定のトレースパラメータを設定することもできます。

BI プラットフォームの現行リリースに関して、以下の表は Web アプリケーションとその関連 WAR ファイルを一覧表示したものです。

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	<INSTALLEDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE \WEB-INF\TraceLog
BI 起動パッド	BOE.war	<INSTALLEDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE \WEB-INF\TraceLog

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
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。

i 注記

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中の場合は、BO_trace.ini ファイルへは以下のディレクトリでアクセスできます。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>\Tomcat6\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>\Tomcat6\webapps\dsbobje\WEB-INF\conf にあります。

バンドルされた Tomcat Web アプリケーションサーバを使用中の場合は、ステップ 3 にスキップします。

2. BOE ファイルまたは dswsbobje war ファイルの 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。
 - デフォルトで、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は、ディレクトリ <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog にあります。
 - デフォルトで、dsbobje.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は、ディレクトリ <INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dsbobje\WEB-INF\conf にあります。
3. BO_trace.ini ファイルを開きます。
4. [Trace Syntax and Setting](#) セクションで必要な行をコメント解除します。
5. 特定の Web アプリケーションにトレース設定を指定するには、以下の例に示すように、IF ステートメントを使用します。

```
if (device_name == "Webapp_opendocument_trace")
{
active = true;
importance = '<<' ;
alert = true;
severity = ' ';
keep_num = 332;
log_dir = 'C:\SAP\SAP BusinessObjects Enterprise XI 4.0\logging'
size = 100 * 1000;
}
```

次の表に、Web アプリケーショントレースの設定に使用できるすべてのパラメータを示します。

パラメータ	入力される値	説明
active	false 、 true	true に設定した場合、現在のプロセスまたはサーバのトレースが有効になります。デフォルト値は false です。
importance	'<<','<','=','>','=','>>',' xs 、 s 、 m 、 l 、 xl i 注記 importance = xs は最も冗長なオプションで、importance = xl は最も冗長性のないオプションです。	トレースメッセージのしきい値を指定します。しきい値を超えたすべてのメッセージがトレースされます。デフォルト値は m (中) です。
alert	false 、 true	重大なシステムイベントに対するトレースを自動的に有効にするかどうかを指定します。デフォルト値は true です。
severity	' S ',' W ',' E ',' A ',' F ',' success 、 warning 、 error 、 assert 、 fatal	メッセージをトレースできるしきい値の重大度を指定します。' S ' はディスク領域を最も消費します。デフォルト値は ' E ' です。
size	指定可能な値は、1000 以上の整数です。	新しいトレースログファイルが作成されるまでの、トレースログファイルに含まれるメッセージの数を指定します。デフォルト値は 100000 です。
keep	false 、 true	新しいファイルが作成された後に古いログファイルを保持するかどうかを指定します。デフォルト値は false です。
administrator	文字列または整数	出力ログファイルで使用する注釈を指定します。次はその例です。 <pre>administrator = "hello"</pre> この文字列はログファイルに挿入されます。
log_dir		出力ログファイルディレクトリを指定します。デフォルトでは、ログファイルは、Logging フォルダに保存されます。
always_close	on 、 off	トレースがログファイルに書き込まれた後にログファイルを閉じるかどうかを指定します。デフォルト値は off です。

6. BO_trace.ini ファイルを保存して閉じます。
7. 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。

24.5 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](#) [ページ 716]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) にある必要があります。.ini ファイルがすでに存在しない場合は、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

24.6 アップグレードマネジメントツールのトレース設定

アップグレードマネジメントツールのトレースは、BO_trace.ini 設定ファイルによって行われます。

Windows のデフォルトの場所は、<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\ です。

Unix のデフォルトの場所は、<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/ です。

i 注記

他の BI プラットフォームコンポーネントと異なり、アップグレードマネジメントツールのトレース設定は CMC で実行することはできません。

24.6.1 アップグレードマネジメントツールをトレース設定する

1. BO_trace.ini ファイルを開きます。
 - Windows のデフォルトの場所は、<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\ です。
 - Unix のデフォルトの場所は、<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/ です。
2. *Trace Syntax and Setting* セクションで必要な行をコメント解除します。
3. 特定のサーバにトレース設定を指定するには、以下の例に示すように、IF ステートメントを使用します。

```
if (process == "upgrademanagementtool")
{
  active = true;
  importance = '<<' ;
  alert = true;
  severity = ' ';
  keep = false;
```

```
size = 100 * 1000;  
}
```

➡ ヒント

プロセスをトレース設定の `upgrademanagementtool` として指定し、アップグレードマネジメントツールに適用する必要があります。

4. `BO_trace.ini` ファイルを保存して閉じます。

変更した設定が実装されます。

25 SAP Solution Manager への統合

25.1 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

i 注記

SAP BusinessObjects の SAP サポートポータルにアクセスするには、<https://websmp205.sap-ag.de/bosap-support> を表示してください。

25.2 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 プラットフォームに必要なコンポーネント
SLD 登録	<ul style="list-style-type: none">• 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。 <div>i 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。</div> <ul style="list-style-type: none">• 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。

SAP Solution Manager のサポート	BI プラットフォームに必要なコンポーネント
	<ul style="list-style-type: none"> • (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 6.0 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	<ul style="list-style-type: none"> • 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 SMAAdmin 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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。

25.3 システムランドスケープディレクトリ登録の管理

25.3.1 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

i 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。

25.3.1.1 SLD データサプライヤの `connect.key` ファイルを作成する

BI プラットフォーム

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。

i 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. 次を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。

25.3.2 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

i 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。

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。

25.3.3 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。

i 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、sldrg_<<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。

25.4 ソリューション管理診断エージェントの管理

25.4.1 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。

25.4.2 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。SMD エージェント (DIAGNOSTICS.AGENT) は (<http://service.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、(<http://service.sap.com/diagnostics>) を参照してください。

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、SMAAdmin ユーザーアカウントをアクティブにする必要があります。

25.4.3 SMAAdmin 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。

SMAAdmin はデフォルトではアクティブになっていません。

25.4.3.1 SMAAdmin 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、[ユーザー一覧] を選択します。
ユーザの一覧が表示されます。
2. [SMAAdmin] 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。

25.5 パフォーマンス機器の管理

25.5.1 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。

25.5.2 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。

i 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。

関連リンク

[SMD エージェントの操作](#) [ページ 730]

25.5.2.1 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。
%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す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。

25.5.3 Web 層のパフォーマンス計測

Web 層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。

25.5.4 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。

25.6 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。

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。

i 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 (`SAPIEPlugin.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、<http://service.sap.com/swdc> を表示してください。

26 コマンドライン管理

26.1 Unix スクリプト

この節では、SAP BusinessObjects Business Intelligence 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。

SAP BusinessObjects Business Intelligence 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 版で利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、SAP BusinessObjects Business Intelligence 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。

26.1.1 スクリプトユーティリティ

この節では、Unix 上の SAP BusinessObjects Business Intelligence 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。このヘルプでは、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。

26.1.1.1 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、CCM 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。

i 注記

角かっこ([])で囲まれた引数はオプションです。

i 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。

i 注記

ccm.sh スクリプトは、Business Intelligence 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	<<完全修飾サーバ名>> <[他の認証情報]>	サーバを起動します。
-managedstop	<<完全修飾サーバ名>> <[他の認証情報]>	サーバを停止します。
-managedrestart	<<完全修飾サーバ名>> <[他の認証情報]>	サーバを停止してから、起動します。
-managedforceterminate	<<完全修飾サーバ名>> <[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	<<完全修飾サーバ名>> <[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。サーバ名は完全な形式で指定します。
-disable	<<完全修飾サーバ名>> <[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、BusinessObjects Business Intelligence 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	< [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

CCM オプション	有効な引数	説明
		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。

i 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>	BusinessObjects Business Intelligence プラットフォームの管理者権限を与え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。 <div> <div>i 注記</div> <div>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。</div> </div>

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。

関連リンク

[ccm.config](#) [ページ 738]

26.1.1.1.1 例

以下の 2 つのコマンドは、すべての Business Intelligence 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) はローカルコンピュータ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 Business Intelligence (BI) プラットフォームサーバを起動および有効化します。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.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

以下の 2 つのコマンドは、SysAdmin という名前の指定された管理アカウントですべての BI プラットフォームサーバを起動し、有効にします。

```
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、“NodeA” で実行中の Adaptive Job Server を無効にします。

```
ccm.sh -disable NodeA.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

26.1.1.1.2 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 およびその他の SAP BusinessObjects Business Intelligence 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。

関連リンク

[コマンドラインの概要](#) [ページ 745]

26.1.1.2 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設定の更新
- 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

i 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および Input/Output File Repository のコンテンツをバックアップします。システムのバックアップと復元、Central Management Server のクラスタリング、および CMS データベースの設定と管理については、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。

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、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。

関連リンク

[Central Management Server のクラスタ化](#) [ページ 324]

[システムのバックアップと復元](#) [ページ 414]

26.1.1.3 configpatch.sh

configpatch.sh スクリプトは、インストール先の sap_bobj/enterprise/generic ディレクトリにインストールされます。この configpatch.sh スクリプトは、システム設定値の更新を必要とするパッチをインストールするときに使用します。パッチをインストールした後に、適切な .cf ファイルの名前を引数に指定して configpatch.sh を実行します。configpatch.sh を実行するタイミング、および使用する .cf ファイルの名前については、BusinessObjects Business Intelligence プラットフォームパッチに付属の readme.txt を参照してください。

26.1.1.4 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
- ノードの一覧表示
- Web Tier 設定の修正

26.1.1.4.1 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 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
 - 7 - config ファイルのすべてのノードを一覧表示
3. 実行する操作に対応する数値を入力します。

4. ノードを追加、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。

26.1.2 スクリプトテンプレート

通常、これらのスクリプトは、ユーザが独自で作成する自動化スクリプトの基礎にするテンプレートとして使用されます。

26.1.2.1 startservers

`startservers` 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、一連の CCM コマンドを実行して Business Intelligence 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るため、独自のスクリプト用のテンプレートとして使用できます。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\[ccm.sh\]](#) [ページ 735]を参照してください。

26.1.2.2 stopservers

`stopservers` 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、一連の CCM コマンドを実行して Business Intelligence プラットフォームサーバを停止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るため、独自のスクリプト用のテンプレートとして使用できます。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\[ccm.sh\]](#) [ページ 735]を参照してください。

26.1.3 SAP BusinessObjects Business Intelligence プラットフォームで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 SAP BusinessObjects Business Intelligence プラットフォームスクリプトユーティリティを実行時に、バックグラウンドで実行される場合があります。このようなスクリプトをユーザ自身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 SAP BusinessObjects Business Intelligence プラットフォームサーバコンポーネントを起動時に、内部的に実行されます。通常の終了コードを返さずにサーバプロセスが異常終了した場合、このスクリプトは新しいサーバプロセスを自動的に再開します。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、他の一部のスクリプトに必要な SAP BusinessObjects Business Intelligence プラットフォーム環境変数が設定されます。SAP BusinessObjects Business Intelligence プラットフォームは必要に応じて env.sh を実行します。SAP BusinessObjects Business Intelligence プラットフォームを UNIX にインストールする場合は、起動時にこのスクリプトが使用されるように Java アプリケーションサーバを設定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 SAP BusinessObjects Business Intelligence 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 Business Objects 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。このスクリプトはインストールスクリプトの最後に自動的に実行され、setup.sh スクリプトを起動します。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、SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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。

SAP BusinessObjects Business Intelligence 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、システムインストール時に、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。システムインストールを実行すると、setup.sh スクリプトの完了後にこのスクリプトを実行するよう指示されます。

i 注記

このスクリプトを実行するには root 権限が必要です。

26.2 Windows スクリプト

この節では、SAP BusinessObjects Business Intelligence 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。

Business Intelligence 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。

26.2.1 ccm.exe

ccm.exe 実行可能ファイルは、インストール先の `<<INSTALLDIR>\SAP BusinessObjects Enterprise XI 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。

i 注記

Server Intelligence Agent (SIA) および Central Management Server (CMS) が実行されていない場合は、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。

i 注記

角かっこ([])で囲まれた引数はオプションです。

i 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、BusinessObjects Business Intelligence 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、有効が無効かなど、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>	Business Intelligence プラットフォームの管理者権限を与えるアカウントを指定します。指定しない場合、デフォルト

認証オプション	有効な引数	説明
		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。 <div> i 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。 </div>
-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。

関連リンク

[ccm.config](#) [ページ 738]

26.2.1.1 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 (NODE01)"
```

SIA は、`net stop "Server Intelligence Agent (NODE01)"` 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 Business Intelligence 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 NODE01.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 NODE01.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、リモートマシンで実行可能なノード上で実行されている Adaptive Job Server を無効にします。

```
ccm.exe -disable NODE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

26.3 サーバコマンドライン

26.3.1 コマンドラインの概要

この節では、各 Business Intelligence 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) を経由してサーバを開始する場合、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変更する必要はありません。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。Business Intelligence 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は、CMC で各サーバのコマンドラインを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。

i 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。Business Intelligence 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。

26.3.1.1 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。

26.3.2 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 Business Intelligence 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>	<p>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。</p> <div> <p>i 注記</p> <p>このポート設定の変更は、CMC で、サーバの [プロパティ] ページの [共通設定] にある [リクエストポート] フィールドを変更することと同じです。</p> </div> <div> <p>i 注記</p> <p>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、<i>SAP BusinessObjects Business Intelligence</i> 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節を参照してください。</p> </div>
-loggingPath	<absolute path>	ログファイルを作成するパスを指定します。

26.3.2.1 Unix のシグナルハンドリング

Unix では、SAP BusinessObjects Business Intelligence プラットフォーム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)。

26.3.3 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/<<PLATFORM64>>/boe_cmdsd です。

オプション	有効な引数	動作
-threads	<数値>	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。
-receiverPool	<数値>	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 Business Objects 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あれば、この値を増やす必要はありません。
-maxobjectsincache	<数値>	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。上限は 100000 です。

関連リンク

[すべてのサーバに使用できる標準オプション](#) [ページ 745]

26.3.4 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 つのサーバタイプだけ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 Enterprise XI 4.0\win64_x64\crcode.exe`
- `<<INSTALLDIR>>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\crproc.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/<PLATFORM64>/boe_crcached.bin`
- `<<INSTALLDIR>>/sap_bobj/enterprise_xi40/<PLATFORM64>/boe_crprocd.bin`

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	<code><absolutePath></code>	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、 <i>SAP BusinessObjects Business Intelligence プラットフォーム管理者ガイド</i> を参照してください。

関連リンク

[すべてのサーバに使用できる標準オプション](#) [ページ 745]

26.3.5 Dashboards Processing Server と Dashboards Cache Server

Dashboards Processing Server と Dashboards Cache Server の制御は、ほぼ同じ方法でコマンドラインから行います。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\SAP BusinessObjects Enterprise XI 4.0\win64_x64\xccache.exe`
- `<<INSTALLDIR>>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\xcproc.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/<PLATFORM64>/boe_xccached`
- `<<INSTALLDIR>>/sap_bobj/enterprise_xi40/<PLATFORM64>/boe_xcprocd`

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。

オプション	有効な引数	動作
-dir	<absolutepath>	Cache Server のキャッシュディレクトリと Processing Server の一時ディレクトリを指定します。作成されるディレクトリは、absolutepath/cache と absolutepath/temp です。
-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。
-psdir	<absolutepath>	Processing Server の一時ディレクトリを指定します。このオプションは、-dir オプションより優先されます。
-refresh	<分>	指定した時間(分単位)が経過する間、キャッシュされたページを共有します。
-auditMaxEventsPerFile	<数値>	Cache Server で、監査ログファイルに記録される監査対象動作の最大数を指定します。デフォルトの値は 500 です。この最大レコード数を超過した場合は、サーバが新しいログファイルを開きます。

関連リンク

[すべてのサーバに使用できる標準オプション](#) [ページ 745]

26.3.6 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 Enterprise XI 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/<<PLATFORM64>>/boe_jobstd です。

i 注記

コマンドラインパラメータを使用して Adaptive Job Server のプロパティを設定しないでください。代わりに、CMC で、サーバプロパティとしてパラメータを設定します。

オプション	有効な引数	動作
-dir	<absolute path>	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>	<p>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。</p> <div> i 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。 </div>
-report_ProcessExtPath	<absolute path>	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。

関連リンク

[すべてのサーバに使用できる標準オプション](#) [ページ 745]

26.3.7 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。

26.3.8 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 Enterprise XI 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/<PLATFORM32>/ras/boe_crystalras 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 (Business Intelligence 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。
-ProcessAffinityMask	<mask>	<p>マスクを使用して、マルチプロセッサコンピュータで RAS が実行するときに使用する CPU を正しく指定します。</p> <p>マスクは、0xf f f f f f f f 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。</p> <p>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、0x0110 となります。</p> <div> <p>i 注記</p> <p>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。</p> </div> <div> <p>i 注記</p> <p>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。</p> </div>

関連リンク

[すべてのサーバに使用できる標準オプション](#) [ページ 745]

26.3.9 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 Enterprise XI 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/<PLATFORM64>/WIReportServer です。

オプション	有効な引数	動作
-ConnectionTimeout Minutes	<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。
-DocExpressRealTime CachingEnable		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。
-DocExpressCache DurationMinutes	<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。
-DocExpressMaxCache SizeKB	<kilobytes>	ドキュメントキャッシュのサイズを指定します。
-EnableListOfValues Cache		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。

関連リンク

[すべてのサーバに使用できる標準オプション](#) [ページ 745]

26.3.10 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 Enterprise XI 4.0\win64_x64\fileserver.exe です。

Unix で両方のサーバを提供するプログラムへのデフォルトパスは、<<INSTALLDIR>>/sap_bobj/enterprise_xi40/<PLATFORM64>/boe_filesd です。

i 注記

コマンドラインパラメータを使用して Input File Repository Server および Output File Repository Server のプロパティを設定しないでください。代わりに、CMC で、サーバプロパティとしてパラメータを設定します。

関連リンク

[すべてのサーバに使用できる標準オプション](#) [ページ 745]

26.3.11 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 Enterprise XI 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_<PLATFORM64>/boe_eventsd です。

i 注記

コマンドラインパラメータを使用して Event Server のプロパティを設定しないでください。代わりに、CMC で、サーバプロパティとしてパラメータを設定します。

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。

関連リンク

[すべてのサーバに使用できる標準オプション](#) [ページ 745]

26.3.12 Dashboard および Dashboard Analytics Server

Dashboard と Dashboard Analytics Server には、コマンドライン管理用のコマンドライン固有のパラメータがありません。

27 アクセス権に関する付録

27.1 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 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。

27.2 全般の権限

構文

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。

注記

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。

注記

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。

権限	説明
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。
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、 <i>SAP BusinessObjects Business Intelligence</i> 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	<p>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。</p> <p>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。</p>
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	<p>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。</p> <div> <p>i 注記</p> <p>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。</p> </div>
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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> この権限は、ユーザまたはグループに対するものです。

権限	説明
	<ul style="list-style-type: none"> 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
別の出力先へスケジュールする	<p>次の操作を実行できるようにします。</p> <ul style="list-style-type: none"> デフォルトの Enterprise ロケーション以外の出力先に対してオブジェクトをスケジュールする。 スケジュールに対して指定されるデフォルトの出力先を変更する。 <p>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。</p> <ul style="list-style-type: none"> 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(ショートカットではなく受信ボックスを出力先としてコピーを送信する場合)。
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すべてのタスクを実行するときに必要になる基本的な権限です。
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。

関連リンク

[オーナー権限](#) [ページ 124]

[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](#) [ページ 122]

27.3 特定のオブジェクトの種類のアクセス権

27.3.1 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)

関連リンク

種類固有アクセス権 [ページ 106]

27.3.2 カテゴリ

構文

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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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。

27.3.3 注

構文

メモを使用すると、ディスカッションアプリケーションを使用して他のオブジェクトにコメントできます。メモはディスカッションスレッドで互いにリンクし、それらのディスカッションスレッドはディスカッション中のオブジェクトの子オブジェクトと見なされます。ディスカッションスレッドの使用方法を制御するには、オブジェクトレベルまたはフォルダレベルで権限を設定できます。

このセクションの権限は、メモのみに適用されます。

権限	説明
ディスカッションスレッドを認める	<p>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。</p> <ul style="list-style-type: none"> ディスカッションスレッドの開始および返信する。 ディスカッションスレッドに対するメモを表示する。 投稿したメモを修正または削除する。

27.3.4 Crystal レポート

構文

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。

i 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	<p>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。</p> <p>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。</p>
オブジェクトに関連するファイルをダウンロード	<p>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。</p> <ul style="list-style-type: none"> 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。

27.3.5 Web Intelligence ドキュメント

構文

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。

Right	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	ドキュメントのデータを Excel、PDF、CSV の各形式にエクスポートできるようにします。この権限がない場合は、[CSV として保存]、[Excel ファイルとして保存]、または[PDF として保存]の権限が必要になります。これらの権限があると、指定した形式にのみエクスポートできます。
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)。
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。
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[値の一覧を使用]権限も必要になります。
CSV として保存	CSV ファイルとしてのみドキュメントをエクスポートできるようにします。そのドキュメントに対してすでに[レポートのデータをエクスポートする]権限がある場合は、この権限は必要ありません。
Excel ファイルとして保存	Excel ファイルとしてのみドキュメントをエクスポートできるようにします。そのドキュメントに対してすでに[レポートのデータをエクスポートする]権限がある場合は、この権限は必要ありません。
PDF として保存	PDF ファイルとしてのみドキュメントをエクスポートできるようにします。そのドキュメントに対してすでに[レポートのデータをエクスポートする]権限がある場合は、この権限は必要ありません。
[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 デスクトップ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。

27.3.6 ユーザとグループ

構文

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種類固有の権限、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。

i 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。

i 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。しかし、ユーザアカウントが作成された後は、そのアカウントの使用者であるユーザが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	<p>次の操作を実行できるようにします。</p> <ul style="list-style-type: none">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。 <p>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。</p>
ユーザパスワードの変更	<p>次の操作を実行できるようにします。</p> <ul style="list-style-type: none">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[オブジェクトの編集]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。 <div><p>i 注記</p><p>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。</p><p>パスワードを無期限にする ユーザは次回ログイ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</p></div> <div><p>i 注記</p><p>この権限は、Business Objects 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。</p></div>
パブリケーションを購読	<p>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。</p>
他のユーザの代理としてスケジュール	<p>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。</p>

27.3.7 アクセスレベル

構文

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。

関連リンク

[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](#) [ページ 122]

27.3.8 ユニバース (.unv) のアクセス権

構文

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。

i 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。 <ul style="list-style-type: none">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。

権限	説明
	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	<p>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。</p> <p>i 注記</p> <p>[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。</p>
値の一覧の新規作成	<p>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。</p> <ul style="list-style-type: none"> 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。 <p>i 注記</p> <p>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。</p>
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	<p>次の操作を実行できるようにします。</p> <ul style="list-style-type: none"> 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。 <p>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。</p>
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。

27.3.9 ユニバース (.unx) のアクセス権

構文

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。

i 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。

Right	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	<p>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。</p> <p>i 注記</p> <p>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。</p>
セキュリティプロファイルの編集	<p>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。</p> <p>i 注記</p> <p>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。</p>
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	<p>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。</p> <p>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。</p>

Right	説明
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。 <div> i 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。 </div>

27.3.10 ユニバースオブジェクトのアクセスレベル

デザイナー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、デザイナーは、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が付与された主体は、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。

i 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。

i 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。

関連リンク

[ユニバースオブジェクトのアクセスレベルの割当](#) [ページ 766]

27.3.10.1 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。

27.3.11 接続のアクセス権

構文

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

Right	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する	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。

Right	説明
	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。
ストアードプロシージャの接続を使用	<p>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ードプロシージャを使用できるようになります。</p> <div> i 注記 この権限は、.unv ユニバースのみに適用されます。 </div>

OLAP 接続のアクセス権

Right	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。

27.3.12 アプリケーション

27.3.12.1 CMC

構文

このセクションの権限は、CMC のみに適用されます。

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。
インスタスマネージャへのアクセスを許可する	インスタ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。

権限	説明
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。

27.3.12.2 BI 起動パッド

構文

このセクションの権限は、BI 起動パッドのみに適用されます。

Right	説明
整理	次の操作を実行できるようにします。 <ul style="list-style-type: none"> オブジェクトを移動またはコピーする。 [お気に入り]フォルダにオブジェクトを追加する。 オブジェクトへのショートカットを作成する。
<i>BusinessObjects</i> 受信ボックスに送信	オブジェクトを BI 受信ボックスに送信できるようにします。
電子メールの出力先に送信	オブジェクトを BI 受信ボックスに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保存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保存できるようにします。

27.3.12.3 BI ワークスペース

構文

このセクションの権限は、BI ワークスペースのみに適用されます。

Right	説明
BI ワークスペースの作成および編集	ユーザに、新しい BI ワークスペースの作成と既存の BI ワークスペースの編集を許可します。
モジュールの作成と編集	ユーザに、新しいモジュールの作成と既存モジュールの編集を許可します。
BI ワークスペースの編集	既存の BI ワークスペースの編集をユーザに許可します。ユーザは、新しい BI ワークスペースは作成できません。

27.3.12.4 Web Intelligence

構文

このセクションの権限は、デスクトップインタフェースを含む SAP BusinessObjects Web Intelligence のみに適用され、これら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。

Right	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を選択できます。
デスクトップインタフェース - Web Intelligence デスクトップの有効化	デスクトップインタフェースを使用できます。
デスクトップインタフェース - ローカルデータプロバイダの有効化	デスクトップインタフェースで個人用データプロバイダを使用できます。
デスクトップインタフェース - ドキュメントのエクスポート	デスクトップインタフェースでドキュメントを CMS にエクスポートできます。
デスクトップインタフェース - ドキュメントのインポート	デスクトップインタフェースでドキュメントを CMS からインポートできます。
デスクトップインタフェース - BI 起動パッドからのインストール	BI 起動パッドからデスクトップインタフェースをダウンロードできます。
デスクトップインタフェース - ドキュメントを印刷する	デスクトップインタフェースからドキュメントを印刷できます。
デスクトップインタフェース - ドキュメントセキュリティの削除	デスクトップインタフェースからドキュメントセキュリティを削除できます。
デスクトップインタフェース - ドキュメントを全ユーザ用に保存	デスクトップインタフェースからすべてのユーザ用にドキュメントを保存できます。
デスクトップインタフェース - ドキュメントのローカル保存	デスクトップインタフェースでドキュメントをローカルディスクに保存できます。
デスクトップインタフェース - メールで送信	デスクトップインタフェースでドキュメントを電子メールで送信できます。
デスクトップインタフェース - ローカルデータプロバイダの有効化	デスクトップインタフェースで個人用データプロバイダを使用できます。
ドキュメント - 開いたときの自動更新を無効化	ドキュメントを開いたときに自動的に最新表示されなくなります。
ドキュメント - 自動保存の有効化	ドキュメントを自動保存できます (管理者によって CMC で自動保存が有効に設定されている場合)。
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ます。

Right	説明
ドキュメント - コンテンツの公開と管理の有効化	CMS でドキュメントを公開できます。
アラータの作成と編集	対話型ビューアでアラートを作成および編集できます。
インタフェース - リッチインターネットアプリケーションの有効化	リッチインターネットアプリケーションの使用とインタフェース (旧リリースの Java レポートパネル) での表示と編集ができます。
インタフェース - Web 表示インタフェースの有効化	Web 表示インタフェース (旧リリースの DHTML ビューア) を使用できます。
インタフェース - Web クエリパネルの有効化	Web クエリパネル (旧リリースのクエリ - HTML) を使用できます。
全般 - [個人用設定] の編集	BI 起動パッドで個人用設定を編集できます。
全般 - 右クリックメニューの有効化	右クリックメニューを使用できます。
左枠 - ドキュメントの概要を有効化	左枠でドキュメントの概要を表示できます。
左枠 - ドキュメント構造とフィルタを有効化	左枠でドキュメントの構造とフィルタを表示できます。
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。
クエリスクリプト - 表示の有効化 (SQL、MDX...)	クエリスクリプト (SQL および MDX) 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	条件付き書式ルールを作成および編集できます。
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ます。
レポーティング - 入力コントロールの作成と編集	入力コントロールを作成および編集できます。
レポーティング - レポートフィルタの作成と編集および入力コントロールの使用	レポートフィルタおよび入力コントロールを作成および編集できます。(左枠の入力コントロール枠は、無効化されていると表示されません)
レポーティング - 並べ替えの作成と編集	ソートを作成および編集できます。
レポーティング - 式および変数の作成	数式と変数を作成できます。
レポーティング - 書式設定の有効化	レポートの書式設定を編集できます。この権限が拒否されると、ユーザはデザインモードおよびデータモードを使用できなくなります (無効化)。
レポーティング - 結合ディメンションの有効化	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ます。ワークフローの重複 (コピー/貼り付け) も制御します。

27.3.12.5 ストラテジービルダ

構文

ストラテジービルダは、パフォーマンスマネジメントに関連するツールです。このセクションの権限はストラテジービルダのみに適用され、Performance Manager での目標管理、またはストラテジービルダ固有の機能に影響します。

権限	説明
目標の作成、変更、削除	Performance Manager で目標を追加、編集、削除できるようにします。
目標の表示	目標を含むアナリティック内の目標を表示できるようにします。
目標管理へのアクセス	<i>Performance Manager</i> の[目標管理]ページに目標を表示できるようにします。
目標の公開	Performance Manager で目標を公開できるようにします。
ストラテジービルダへのアクセス	Performance Manager でストラテジービルダツールにアクセスできるようにします。
ロールの作成、変更、削除	ストラテジービルダで目標またはメトリックを特定の対象ユーザに公開するために使用するロールを管理できるようにします。
ストラテジーの作成、変更、削除	ストラテジービルダで、ロールとリンクしたストラテジを作成し、目標およびメトリックを公開できるようにします。

27.3.12.6 ユニバースデザインツール権限

構文

このセクションの権限は、ユニバースデザインツールアプリケーションに適用されます。

Right	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検査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	リポジトリに格納された、または個人用接続または共有接続として格納されたユニバース接続を作成、変更、削除できるようにします。

27.3.12.7 インフォメーションデザインツールの権限

構文

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アプリケーションに適用されます。

Right	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なります。 i 注記 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が必要です。
プロジェクトの共有	ローカルプロジェクトを共有し、[プロジェクトの同期] ビューを開いて、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	次の操作を実行できるようにします。 <ul style="list-style-type: none">• [公開済みリソース] ビューからのセキュリティ接続の作成および削除• 接続エディタでの接続の編集• リポジトリに対する接続の公開
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ローカルプロジェクトに取得して編集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] オプションを使用できるようにします。
統計の計算	統計を計算し公開するテーブルおよび列を選択できるようにします。

27.3.12.8 SAP BusinessObjects Business Intelligence プラットフォーム向けウィジェット

構文

このセクションの権限は、SAP BusinessObjects Business Intelligence プラットフォーム向けウィジェットのアプリケーションのみに適用されます。

Right	説明
エクスプローラを使用	ユーザは、ドキュメント一覧エクスプローラを使用して、接続しているすべての BI プラットフォームサーバのコンテンツを参照できます。
警告受信ボックスを使用	(使用停止) アラート受信ボックスを使用できるようにします。
検索を使用	ユーザは、コンテンツ検索機能を使用して、接続しているすべての BI プラットフォームリポジトリを検索できます。

27.3.12.9 アラート

構文

このセクションの権限は、アラートアプリケーションのみに適用されます。

Right	説明
[アラートをトリガする]	<p>アラートイベントをトリガすることができます。</p> <p>ドキュメントに対してアラートをトリガするには、以下の権限が必要になります。</p> <ul style="list-style-type: none"> 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
[オブジェクトを購読する]	<p>アラートイベントを購読することができます。</p> <p>イベントを購読するには、以下の権限が必要です。</p> <ul style="list-style-type: none"> 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 <p>ドキュメントのアラートを購読するには、以下の権限が必要になります。</p> <ul style="list-style-type: none"> 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

27.3.12.10 Explorer

このセクションの権限は、Explorer のみに適用されます。

Right	説明
Explorer にログインして、このオブジェクトを CMC で表示	Explorer にログインできます。この権限は、Explorer で他のタスクを実行する場合に必要です。
情報スペースの閲覧	<p>情報スペースを調査できます。</p> <p>このタスクを実行するには、[Explorer にログインして、このオブジェクトを CMC で表示] 権限も必要です。</p>
情報スペースの閲覧: ブックマーク/電子メールへのエクスポート	<p>ブックマークを付け、ブックマークを電子メールで送信できます。</p> <p>このタスクを実行するには、次の権限も必要です。</p> <ul style="list-style-type: none"> Explorer にログインして、このオブジェクトを CMC で表示 情報スペースの閲覧
情報スペースの閲覧: CSV へのエクスポート	<p>調査の結果を CSV または Excel ファイルにエクスポートできます。</p> <p>このタスクを実行するには、次の権限も必要です。</p> <ul style="list-style-type: none"> Explorer にログインして、このオブジェクトを CMC で表示 情報スペースの閲覧
情報スペースの閲覧: イメージへのエクスポート	<p>調査の結果をイメージとしてエクスポートできます。</p> <p>このタスクを実行するには、次の権限も必要です。</p> <ul style="list-style-type: none"> Explorer にログインして、このオブジェクトを CMC で表示 情報スペースの閲覧
情報スペースの閲覧: Web Intelligence へのエクスポート	<p>調査の結果をクエリにエクスポートできます。</p> <p>このタスクを実行するには、次の権限も必要です。</p> <ul style="list-style-type: none"> Explorer にログインして、このオブジェクトを CMC で表示 情報スペースの閲覧
情報スペースの管理	<p>[スペースの管理]メニューにアクセスして、関連のタスクを実行できます。</p> <p>このタスクを実行するには、[Explorer にログインして、このオブジェクトを CMC で表示] 権限も必要です。</p>
情報スペースの管理: 新しいスペースの作成	<p>新しい情報スペースを作成できます。</p> <p>このタスクを実行するには、次の権限も必要です。</p> <ul style="list-style-type: none"> Explorer にログインして、このオブジェクトを CMC で表示 情報スペースの管理
情報スペースの管理: スペースの変更	<p>情報スペースを変更または削除できます。</p> <p>このタスクを実行するには、次の権限も必要です。</p> <ul style="list-style-type: none"> Explorer にログインして、このオブジェクトを CMC で表示 情報スペースの管理

Right	説明
情報スペースの管理: インデックス化のスケジュール	<p>情報スペースデータのインデックス化をスケジュールできます。</p> <p>このタスクを実行するには、次の権限も必要です。</p> <ul style="list-style-type: none"> Explorer にログオンして、このオブジェクトを CMC で表示 情報スペースの管理
情報スペースの管理: インデックス化の開始	<p>情報スペースデータのインデックス化を実行できます。</p> <p>このタスクを実行するには、次の権限も必要です。</p> <ul style="list-style-type: none"> Explorer にログオンして、このオブジェクトを CMC で表示 情報スペースの管理

27.3.12.11 SAP BusinessObjects Mobile

構文

このセクションの権限は、SAP BusinessObjects Mobile アプリケーションのみに適用されます。

Right	説明
SAP BusinessObjects Mobile アプリケーションへのログオン	Mobile アプリケーションを介して BI プラットフォームにログインし、ドキュメントを表示する権限を許可します。
ドキュメントアラートの購読	<p>ドキュメント/繰り返しアラートを購読する権限を許可します。</p> <div> <p>i 注記</p> <p>以前に「ドキュメントアラートの購読」権限を付与されたユーザは、現在アクセスを拒否されている場合でも、購読中のアラートを引き続き受信することになります。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。</p> </div> <div> <p>i 注記</p> <p>スケジュールに対するドキュメントアラート (または繰り返しインスタンス) を購読するには、ユーザは、セントラル管理コンソール (CMC) の "イベント" の下の "システムイベント" フォルダへの "フルコントロール" セキュリティアクセスが必要です。</p> </div>
デバイスのローカルストアへのドキュメントの保存	<p>ドキュメントを Mobile デバイスに保存する権限を付与します。</p> <div> <p>i 注記</p> <p>「ドキュメントをデバイスのローカルストアに保存」権限が付与されているときにドキュメントをデバイスに保存すると、その後保存権限を失っても、ドキュメントはデバイスに保存されたままになり</p> </div>

Right	説明
	ます。ただし、それらのドキュメントは同期処理中に同期されることはありません。
デバイスからドキュメントを電子メールとして送信	電子メールによってレポートを送信する権限を付与します。

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。

28 サーバのプロパティに関する付録

28.1 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 Business Intelligence プラットフォームサーバに設定可能なプロパティの一覧とその説明を示します。

28.1.1 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。

表 23: 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。	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。	値は自動生成されます。
ノード	サーバが存在するノードの名前。括弧内はノードの実行に使用するホスト名とアカウント名を示します。	インストール中に設定します。
説明	サーバの説明。	サーバの名前。
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。	サーバの種類によって異なります。
リクエストポート	<p>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。</p> <div>i 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。</div>	空白
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。	TRUE

表 24: 自動起動プロパティ

プロパティ	説明	デフォルト値
<i>Server Intelligence Agent</i> 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。	TRUE

表 25: 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。	TRUE
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。	空白
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。	空白

表 26: 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。	FALSE
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。	FALSE
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。	FALSE

表 27: 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

プロパティ	説明	デフォルト値
	<ul style="list-style-type: none"> 指定なし なし 低 中 高 	

関連リンク

[Working with configuration templates](#) [ページ 335]

[トレースログレベル](#) [ページ 495]

28.1.2 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

表 28: 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	<p>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。</p> <div> i 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。 </div>	%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。

表 29: 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	<p>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。</p> <p>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。</p>	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

表 30: 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)	<p>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。</p> <ul style="list-style-type: none"> 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。 <p>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。</p>	1200

Z

表 31: 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

表 32: 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。		

表 33: 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処理スレッド数を指定します。このプロパティの値が“0”に設定されている場合、スレッドプールサイズは、現在のマシンにある CPU コア数に基づく式を使用して決定されます。	0

表 34: 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。		

表 35: 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。		

表 36: 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。		

表 37: 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。		

表 38: バ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

i 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。

表 39: 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
必要な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

表 40: 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)	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

表 41: 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
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
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。

Input File Repository Server のプロパティ

表 42: 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
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
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。 i 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勧めします。	%DefaultInputFRSDir/temp%
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。 i 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/%

Output File Repository Server のプロパティ

表 43: 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
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
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。	%DefaultOutputFRSDir/temp%

プロパティ	説明	デフォルト値
	<p>i 注記</p> <p>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します。</p>	
ファイル格納ディレクトリ	<p>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。</p> <p>i 注記</p> <p>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。</p>	%DefaultOutputFRSDir/%

Web アプリケーションコンテナサーバのプロパティ

表 44: 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)	<p>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。</p> <p>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。</p>	1200

表 45: 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	<p>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。デバッグでのみ使用し</p>	この設定は指定されていません。

プロパティ	説明	デフォルト値
	<p>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。</p> <p>選択可能なメニューは次のとおりです。</p> <ul style="list-style-type: none"> 指定なし なし 低 中 高 	

表 46: ビジネスプロセス BI サービスプロパティ

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。		

表 47: クエリビルダサービスプロパティ

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。		

表 48: RESTful Web サービスシステムの設定プロパティ

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 <code>&pageSize=<m></code> 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	1000

プロパティ	説明	デフォルト値
	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。	
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
デフォルトの HTTP Basic 用認証スキーマ	<p>[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。</p> <p>指定できる値は次のとおりです。</p> <ul style="list-style-type: none"> 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、[secEnterprise] がデフォルト設定となります。

表 49: 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	<p>SAP BusinessObjects Business Intelligence プラットフォーム BI 起動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。</p> <p>指定できる値は次のとおりです。</p> <ul style="list-style-type: none"> AD Kerberos AD Kerberos SSO Enterprise LDAP 	Enterprise

プロパティの種類	説明	デフォルト値
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。たとえば、デフォルトのドメインを “mydomain” に設定し、ユーザがユーザ名 “user” でログインすると、Active Directory ログオン認証機関は “user@mydomain.com” を認証します。	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します。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

表 50: Web サービス SDK および QaaWS サービスのプロパティ

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します。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

表 51: 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	TRUE

プロパティ	説明	デフォルト値
	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、このプロパティを選択解除します。	
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] を選択していない場合にのみ値を指定できます。	localhost
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	リクエストおよび応答の HTTP ヘッダの最大許容サイズ (バイト)。	32768

表 52: プロキシ経由の HTTP の設定プロパティ

プロパティ	説明	デフォルト値
プロキシ経由の HTTP を有効にする	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] を選択していない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 の有効化] を選択している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] を選択している場合にのみ値を指定できます。	空白

プロパティ	説明	デフォルト値
プロキシポート	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のポートを指定します。[プロキシ経由の HTTP の有効化]を選択している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	HTTP ヘッダのリクエストと応答の最大許容サイズ (バイト)。[プロキシ経由の HTTP の有効化]を選択している場合にのみ値を指定できます。	32768

表 53: HTTPS 設定プロパティ

プロパティ	説明	デフォルト値
HTTPS を有効にする	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ーフェース(IP アドレスまたはホスト名)を指定します。[HTTPS の有効化]を選択している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]を選択している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]を選択している場合にのみ値を指定できます。	空白
プロキシポート	フォワードプロキシサーバまたはリバースプロキシサーバのポートを指定します。[HTTPS の有効化]を選択している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]を選択している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、[PKCS12]になります。[HTTPS の有効化]を選択している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。

プロパティ	説明	デフォルト値
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]を選択している場合にのみ値を指定できます。	空白
秘密鍵のアクセスパスワード	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]を選択している場合にのみ値を指定できます。	空白
証明書エイリアス	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]を選択している場合にのみ値を指定できます。	空白
クライアント認証を有効にする	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]を選択している場合にのみ有効にすることができます。	FALSE
証明書信頼リストファイルの場所	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]を選択している場合にのみ値を指定できます。	空白
証明書信頼リストの秘密鍵のアクセスパスワード	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]を選択している場合にのみ値を指定できます。	空白
最大 HTTP ヘッダサイズ	HTTP ヘッダのリクエストと応答の最大許容サイズ (バイト)。[HTTPSの有効化]を選択している場合にのみ値を指定できます。	32768

表 54: 同時接続の設定 (コネクタ別)

プロパティ	説明	デフォルト値
同時接続要求の最大数	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 ~ 9999 です。

表 55: Active Directory の設定

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

28.1.3 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。

表 56: 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。	1200
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。	600

表 57: サービス処理プロパティ

プロパティ	説明	デフォルト値
<p>➡ 注意</p> <p>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。</p>		
接続プール	<p>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。</p> <ul style="list-style-type: none"> 有効 - タイムアウトあり 有効 無効 <p>i 注記</p> <p>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。</p>	有効 - タイムアウトあり
接続プールタイムアウト (分単位)	<p>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。</p> <p>i 注記</p> <p>このプロパティは、<code>cs.cfg</code> ファイルの <code>cs.cfg</code> 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、<code>Max Pool Time</code> 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、<code>Max Pool Time</code> 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。</p>	60
アクティブでない一時的オブジェクトのタイムアウト (分単位)	<p>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。</p>	60
一時的オブジェクトのタイム間隔 (分単位)	<p>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。</p>	5
HTTP チャンキングを有効にする	<p>HTTP チャンキングを有効または無効にします。</p> <p>i 注記</p> <p>HTTP チャンキングは、3 層デプロイメントにのみ有効です。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、<code>[HTTP チャンクのサイズ]</code> を 0 に設定するのと同じ意味を持ちます。</p>	有効

プロパティ	説明	デフォルト値
HTTP チャンクのサイズ (KB)	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

表 58: 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
<p>➔ 注意</p> <p>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。</p>		
ジョブのトレースを有効にする	<p>Connection Server ジョブのトレースを有効にします。</p> <p>i 注記</p> <p>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。</p>	無効
ミドルウェアのトレースを有効にする	<p>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。</p> <p>i 注記</p> <p>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。</p>	無効

表 59: 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
<p>⚠ 警告</p> <p>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。</p>		
データソースを有効にする	<p>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。</p> <p>⚠ 警告</p> <p>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。</p>	未選択

プロパティ	説明	デフォルト値
	<p>➡ 注意</p> <p>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。</p> <p>i 注記</p> <p>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。</p>	
ネットワークレイヤ	<p>接続で使用するネットワークレイヤを指定します。</p> <p>i 注記</p> <p>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。</p>	<ul style="list-style-type: none"> ネイティブ CORBA サーバは ODBC Adaptive CORBA サーバは JDBC
データベース	<p>接続で使用するデータベースを指定します。</p> <p>i 注記</p> <p>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。</p>	データベース名を入力するまでは空白のままです。

表 60: 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。	1200

プロパティ	説明	デフォルト値
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。	600

表 61: ライフサイクルマネジメントサービスプロパティ

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。		

表 62: ライフサイクルマネジメント ClearCase サービスプロパティ

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。		

表 63: Visual Difference サービスプロパティ

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。		

関連リンク

[共通サーバのプロパティ](#) [ページ 777]

28.1.4 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。

- Adaptive Job Server
- Crystal Reports Cache Server
- Crystal Reports Processing Server
- Crystal Reports 2011 Report Application Server
- Crystal Reports 2011 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。

これらのサーバのプロパティを変更する場合、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。

表 64: Adaptive Job Server サービスのプロパティ

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	<p>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。</p> <p>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。</p>	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

表 65: 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
ビューを最新表示すると、常に最新データが表示される	<p>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。</p> <p>i 注記</p> <p>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。</p>	FALSE
クライアント間でレポートデータを共有する	<p>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。</p> <p>i 注記</p> <p>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。</p>	TRUE
アイドル状態の接続のタイムアウト(分単位)	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。	20
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イン認証情報、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。	20
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回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	0

プロパティ	説明	デフォルト値
	<p>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。</p> <p>i 注記</p> <p>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。</p>	
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。	256000
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。	空白
DLL 名		rasprocReport

Crystal Reports Processing Server のプロパティ

Crystal Reports Cache Server と Crystal Reports Processing Server 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。

i 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。

表 66: 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
アイドル状態の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。	20
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。	1000

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	<p>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。</p> <p>i 注記</p> <p>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。</p>	FALSE
クライアント間でレポートデータを共有する	<p>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。</p> <p>i 注記</p> <p>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。</p>	TRUE
アイドル状態の接続のタイムアウト (分単位)	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。	20
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。	0
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。	0

プロパティ	説明	デフォルト値
	<p>i 注記</p> <p>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。</p>	
事前開始された最大子数	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。	1
一時ディレクトリ	<p>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。</p> <p>i 注記</p> <p>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。</p>	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Java のクラスパス	サーバに必要な 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

表 67: 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。	86400

Crystal Reports 2011 Report Application Server のプロパティ

i 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。

表 68: Crystal Reports 2011 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のデータベースへの接続を維持できるようにする	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。	FALSE
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。どちらのキャッシュにもない場合、データベースから取得されます。	100
アイドル状態の接続のタイムアウト (分単位)	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)。	30
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。	100
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。	20000
レポートジョブの最大同時接続数 (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。	75
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。	20

プロパティ	説明	デフォルト値
一時ディレクトリ	<p>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。</p> <p>i 注記</p> <p>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。</p>	%DefaultDataDir%/CrystalReportsRasServer/temp

表 69: 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。	86400

Crystal Reports 2011 Processing Server のプロパティ

i 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。

表 70: Crystal Reports 2011 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
アイドル状態の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。	20
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。	1000
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	<p>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。</p> <p>i 注記</p> <p>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。</p>	FALSE
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。	TRUE

プロパティ	説明	デフォルト値
	<p>i 注記</p> <p>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。</p>	
アイドル状態の接続のタイムアウト (分単位)	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。	20
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。	0
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)	<p>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。</p> <p>i 注記</p> <p>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。</p>	0
事前開始された最大子数	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。	1
一時ディレクトリ	<p>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。</p> <p>i 注記</p> <p>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。</p>	%DefaultDataDir%/CrystalReports2011ProcessingServer/temp

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のデータベースへの接続を維持できるようにする	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。	FALSE
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。	20000

表 71: 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 接続が有効である、有効期限までの時間 (秒単位) を指定します。	86400

28.1.5 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。

表 72: 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。	15 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。	100000

プロパティ	説明	デフォルト値
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。	100000

表 73: 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
<i>Adaptive Job Server</i>	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。	デフォルト値は 5 です。
<i>Adaptive Processing Server</i>	子が再起動前に処理するジョブ数を示します。 Adaptive Processing Server は、プロモーションマネジメントサービスおよびプロモーションマネジメント ClearCase サービスを持ちます。これらのサービスには、CMC で設定できるプロパティはありません。	デフォルト値は 100 です。

表 74: 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。	15
SAP BW マスタシステム	SAP BusinessObjects Business Intelligence プラットフォームで作成した BW システムへの OLAP 接続名。	SAP_BW
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。	空白
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。	空白
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。	空白
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。	3

28.1.6 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。

表 75: 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。	32767
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。	10
接続アイドル時間のタイムアウト (秒)	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。	10800
ステートメントアイドル時間のタイムアウト (秒)	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。	600

28.1.7 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 Job Server
- Adaptive Processing Server
- Web Intelligence Processing Server

Adaptive Job Server のプロパティ

表 76: Web Intelligence スケジュールサービスのプロパティ

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

表 77: 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	<p>BEx クエリから取得するデータのレベルを指定します。</p> <p>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。</p>	<p>-</p> <p><code>Dsap.sl.bics.expandToLevel=n</code></p> <p>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。</p>

表 78: 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
モニタリングの有効化	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 (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。	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

表 79: 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
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低い値を指定することをお勧めします。	600

表 80: 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。		

表 81: ドキュメント回復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。		

表 82: 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。

表 83: 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
値の一覧のキャッシュを有効にする	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)	バッチ単位の値の一覧ごとのエントリ (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(エントリ)	各値の一覧のエントリ(値)の最大数を指定します。	50000

表 84: 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(秒単位)	Web Intelligence Processing Server セッションが交換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交換されて、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(秒数)	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交換などのクリーンアップアクションを実行して、サーバのメモリを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、デフォルト値が 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	TRUE

プロパティ	説明	デフォルト値
	識されます。無効な場合、プロパティは無視されます。	
アイドル状態の接続のタイムアウト(分単位)	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	<p>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、交換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。</p> <div> <p>i 注記</p> <p>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>]を有効にする必要があります。</p> </div>	<p>50</p> <p>有効な範囲は 5 ～ 65535 です。</p>
メモリの分析を有効にする	<p>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。</p> <ul style="list-style-type: none"> • <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> <p>サーバのプロセスメモリが[<メモリの上位しきい値>]の値を上回ると、ドキュメントの保存操作のみ許可されます。プロセスメモリが[<メモリの最大しきい値>]を上回ると、操作は停止し、失敗します。</p>	TRUE
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
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

プロパティ	説明	デフォルト値
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
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示します。	3
APS サービスの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	<p>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。</p> <p>i 注記</p> <p>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。</p>	FALSE

表 85: 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

表 86: 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(分数)	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>に対してチェックされる間隔を分単位で指定します。	120

プロパティ	説明	デフォルト値
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スペース>プロパティの値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)	<p>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。</p> <p>i 注記</p> <p>[最大文字ストリームサイズ]プロパティの値を超えると、Web</p>	<p>5</p> <p>有効な範囲は 1 ～ 65535 です。</p>

プロパティ	説明	デフォルト値
	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。	
バイナリストリーム最大サイズ(MB)	<p>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。</p> <p>i 注記</p> <p>[バイナリストリーム最大サイズ] の値を超えると、Web Intelligence ドキュメントは作成されず、クライアントコンピュータにエラーメッセージが表示されます。</p>	<p>50</p> <p>有効な範囲は 1 ～ 65535 です。</p>
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
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

表 87: 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)	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

関連リンク

[Web Intelligence Server Memory Threshold Settings](#) [ページ 812]

28.1.7.1 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。

メモリの最大しきい値

[<メモリの最大しきい値>]制限に達すると、現在の操作が中断します。

メモリの上位しきい値

この[<メモリの上位しきい値>]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、新しい接続およびその他のメモリを消費するスレッドを開始しないようにします。Web Intelligence ドキュメントの保存オプションのみ許可されます。メモリの割り当てを必要とするアクションをリクエストしたユーザは、「サーバはビジー状態です」というメッセージを受け取り、保留中の変更を保存する必要があることが通知されます。
- 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[<メモリの上位しきい値>]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の削除を試みます。
- 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、表示モードで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、[<メモリの上位しきい値>]: $(20\% * ([<メモリの上位しきい値>]))$ 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。

$$4500\text{MB} - .20 * 4500\text{MB} = 3600\text{MB}$$

- 表示モードでドキュメントを閉じている間に十分な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も含め、開いている残りのドキュメントをすべて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、[<メモリの上位しきい値>]: $(20\% * ([<メモリの上位しきい値>]))$ 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。

$$4500\text{MB} - .20 * 4500\text{MB} = 3600\text{MB}$$

メモリの下位しきい値

[<メモリの下位しきい値>]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のメモリを割り当てます。

28.1.8 Dashboards サービスのプロパティ

Dashboards Cache Server のプロパティ

表 88: Dashboards 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
最大キャッシュサイズ (KB)	クエリ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。	256000

プロパティ	説明	デフォルト値
	サーバが大量のクエリ、または非常に複雑なクエリを処理する場合は、キャッシュサイズを大きくする必要があります。	
アイドル状態の接続のタイムアウト(分単位)	Dashboards 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。	15
クライアント間でデータを共有する	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。	TRUE
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)	<p>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クエリからのリクエストに回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回答することができ、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。重要なデータが頻繁に変更される場合など、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。</p> <div> i 注記 このプロパティはレポートオブジェクト自体に設定でき、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。 </div>	0
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、クエリプロパティ、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。	20

プロパティ	説明	デフォルト値
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。	Xmx858M

Dashboards Processing Server のプロパティ

表 89: Dashboards 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
同時実行ジョブの最大数 (0 は自動)	サーバ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。	0
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。	10000
事前開始された最大子数	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。この値が大きすぎると、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。	1
アイドル状態の接続のタイムアウト (分単位)	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。通常はデフォルト値を変更する必要はありません。	15
アイドル状態のジョブのタイムアウト (分単位)	サーバ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。	15
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。	Xmx858M,Dswfinjection.lang.directory=%CommonJavaLibDir%,Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%

表 90: 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。	86400

29 サーバのメトリクスに関する付録

29.1 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、SAP BusinessObjects Business Intelligence 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。

この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ステータスもモニタリングできます。

サーバステータス	説明
ヘルスステータス	ヘルスステータスは、サーバの全般的な状態を示します。可能な値は以下のとおりです。 <ul style="list-style-type: none">0 = 赤 (危険)1 = 黄色 (注意)2 = 緑 (問題なし)
サーバの有効ステータス	このステータスは、サーバが有効か無効かを示します。可能な値は以下のとおりです。 <ul style="list-style-type: none">0 = 無効1 = 有効
サーバの実行ステータス	このステータスは、サーバの実行ステータスを示します。可能な値は以下のとおりです。 <ul style="list-style-type: none">0 = STOPPED1 = STARTING2 = INITIALIZING3 = RUNNING4 = STOPPING5 = FAILED6 = RUNNING_WITH_ERRORS7 = RUNNING_WITH_WARNINGS

関連リンク

[サーバメトリクスの分析](#) [ページ 332]

29.1.1 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。

表 91: 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。
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。
ローカルの時刻	ローカル時刻。
ディスクサイズ (GB)	SAP BusinessObjects Business Intelligence 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ギガバイト単位のサイズ。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)	SAP BusinessObjects Business Intelligence 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、SAP BusinessObjects Business Intelligence 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ディスク領域が含まれます。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、特定の SAP BusinessObjects サーバについて説明しています。

表 92: 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。

メトリクス	説明
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。
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ります。

表 93: 監査メトリクス

メトリクス	説明
キューにある現在の監査イベント数	<p>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。</p> <div> <p>i 注記</p> <p>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、監査データベースに到達しない監査イベントが発生する場合があります。</p> </div>

表 94: 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。

29.1.2 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。

表 95: 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	Central Manager Server(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

メトリクス	説明
	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。
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。 <ul style="list-style-type: none"> 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。 <p>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。</p>
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	SAP BusinessObjects Business Intelligence 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。

メトリクス	説明
全ユーザー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ーセッション数。この数が大きいほど、システムを使用しているユーザー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。
同時接続ユーザーライセンス	キーコードによって示される同時接続ユーザーライセンスの数。
登録ユーザーライセンス	キーコードによって示される登録ユーザーライセンスの数。
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 システム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ー名	CMS データベースへの接続に使用されるユーザーアカウントの名前。
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。

メトリクス	説明
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。
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。

29.1.3 Connection Server のメトリクス

表 96: 接続サービスメトリクス

メトリクス	説明
データソース	<p>[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。</p> <ul style="list-style-type: none"> [ステータス] (ロード済み) または [エラー]: ドライバの現在のステータス

メトリクス	説明
	<ul style="list-style-type: none"> • 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) <div> i 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。 </div>

29.1.4 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。

表 97: 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。

29.1.5 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。

表 98: 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)。

メトリクス	説明
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)。

29.1.6 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。

表 99: 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。
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。

メトリクス	説明
	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)	<p>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、Java 仮想マシン上で実行中のすべてのアプリケーションコードの実行が停止し、仮想マシンは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を実行します。</p> <p>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。</p>
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。

表 100: DSL ブリッジサービスのメトリクス

メトリクス	説明
<code>DSLServiceMetrics.queryCount</code>	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。
<code>DSLServiceMetrics.activeConnectionCount</code>	クライアントとサービスの間で現在開いている接続数。
<code>DSLServiceMetrics.activeSessionCount</code>	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。

メトリクス	説明
<i>DSLServiceMetrics.activeOLAPConnectionCount</i>	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。

表 101: 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。

表 102: 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。

表 103: 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	MDS 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。

表 104: 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] になります。そうでない場合は、[FALSE] になります。

表 105: 接続サービスメトリクス

メトリクス	説明
データソース	<p>[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。</p> <ul style="list-style-type: none"> ステータス (“ロード済み”または“エラー”): ドライバの現在のステータス 利用可能な接続: 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) <p>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。</p>

表 106: モニタリングサービスのメトリクス

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について、過去 15 サイクルで監視ステータスの計算に要した平均時間。
ユーザが作成したメトリクスの数	すべてのユーザに関する、クラスタのユーザ作成メトリクスの合計。

メトリクス	説明
監視回数	無効な監視と有効な監視の両方を含む、クラスタの監視総数。
<code>serviceBean.monitoringAppPropEnabled</code>	モニタリングアプリケーションが有効である場合は [TRUE] になります。そうでない場合は、[FALSE] になります。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での 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ます。そのため、このメトリクスは CMC の現在の設定とは異なる場合があります。
サービスは利用可能	モニタリングサービスが有効な場合は [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 1 つのモニタリングサービスのみが有効です。
トレンド化されたメトリクスの数	現在モニタリングデータベースに記録されているメトリクスの総数。

表 107: 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で有効なセッションの総数。

29.1.7 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。

i 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。

表 108: 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。継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。

関連リンク

[Adaptive Processing Server のメトリクス](#) [ページ 823]

29.1.8 Adaptive Job Server のメトリクス

表 109: 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。
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トレイ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	サーバで実行中のスケジュール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。
SAP StreamWork 出力先のデフォルト設定が有効	

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。

表 110: スケジュール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。

表 111: 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。
通信エラー	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、 [1] になります。そうでない場合は、 [0] 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、 [1] になります。そうでない場合は、 [0] になります。

29.1.9 Crystal Reports Server のメトリクス

次の表は、Crystal Reports Processing Server および Crystal Reports 2011 Processing Server の **[メトリクス]** ページに表示されるサーバのメトリクスの説明を示します。

表 112: 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。

メトリクス	説明
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 リクエストを処理するのにかかった平均時間 (ミリ秒)。この数字が、常に高く、増加する場合は、他のコンピュータ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、他のコンピュータ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、他のコンピュータに追加サーバを構築することを検討してください。
キュー内にあるリクエスト数	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、他のコンピュータ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。
リクエスト失敗レート (%)	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 [\[メトリクス\]](#) ページに表示されるサーバのメトリクスの説明を示します。

表 113: 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。
オブジェクトの型	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 リクエストを処理するのにかかった平均時間 (ミリ秒)。この数字が、常に高く、増加する場合は、他のコンピュータ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、他のコンピュータに追加サーバを構築することを検討してください。

メトリクス	説明
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、他のコンピュータに追加サーバを構築することを検討してください。
キュー内にあるリクエスト数	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、他のコンピュータ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。
キャッシュサイズ (KB)	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 2011 Report Application Server の [メトリクス] ページに表示されるサーバのメトリクスの説明を示します。

表 114: Crystal Reports 2011 Report Application Server のメトリクス

メトリクス	説明
<i>metric_currentdoccount</i> <div> i 注記 このメトリクスは、CMC の [モニタリング] ページには “document_s_” と表示されます。 </div>	サーバで現在処理中のドキュメントの数。
<i>metric_totaldoccount</i> <div> i 注記 このメトリクスは、CMC の [モニタリング] ページには “document_s_” と表示されます。 </div>	サーバ起動後にサーバで処理されたドキュメントの数。
<i>metric_currentagentthreadcount</i> <div> i 注記 このメトリクスは、CMC の [モニタリング] ページには “agent thread_s_” と表示されます。 </div>	サーバで現在処理中のスレッドの数。
<i>metric_totalagentthreadcount</i>	サーバ起動後にサーバで処理されたスレッドの数。

メトリクス	説明
<p>i 注記</p> <p>このメトリクスは、CMC の [モニタリング] ページには “agent thread_s_” と表示されます。</p>	

29.1.10 Web Intelligence サーバのメトリクス

表 115: 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)。
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。
Cache high mark count	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 usage (%)	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。
Total CPU time (seconds)	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)。
Memory high threshold count	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。
Virtual memory size (Mb)	サーバに割り当てられた総メモリ量 (MB)。
Current number of client calls	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。
Current number of tasks	サーバで現在実行されているタスク数。
Total number of client calls	サーバ起動後にサーバが受信した CORBA 呼び出しの総数。
Total number of tasks	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経過時間 (秒)。
Current number of active sessions	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。
Number of documents	サーバで現在開いているドキュメントの数。
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。
Current number of sessions	サーバで現在作成されているセッション数。
Number of document swap	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。
Number of swapped documents	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。
Number of sessions timeout	サーバ起動後にタイムアウトしたセッション数。

メトリクス	説明
<i>Total number of sessions</i>	サーバ起動後にサーバ上に作成されたセッション数。
<i>Number of users</i>	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)。

29.1.11 Dashboards Server のメトリクス

表 116: Dashboards 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。
平均処理時間 (ミリ秒)	サーバが受け取った直近の 500 リクエストを処理するのにかかった平均時間 (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。
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。
リクエスト失敗レート (%)	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。

表 117: Dashboard 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 Dashboards 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 リクエストを処理するのにかかった平均時間 (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。
キュー内にあるリクエスト数	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。
キャッシュサイズ (KB)	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	現在開いているクライアントへの接続数。
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)。

30 サーバおよびノードのプレースホルダに関する付録

30.1 サーバとノードプレースホルダ

構文

`%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。

プレースホルダ	説明	デフォルト値
<code>%AuditingDatabaseConnection%</code>	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。
<code>%AuditingDatabaseDriver%</code>	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。	使用されるデータベースに依存 - 例: <ul style="list-style-type: none">SQL Server では、<code>sqlserverauditdbss</code> です。MySQL では、<code>mysqlauditdbss</code> です。
<code>%BINDIR%</code>	情報プラットフォームサービス 64 ビットバイナリが格納されるフォルダ。	<ul style="list-style-type: none">Windows では、<code><<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/win64_x64</code> です。Unix では、<code><<INSTALLDIR>>/sap_bobj/enterprise_xi40/<PLATFORM64></code> です。
<code>%BINDIR32%</code>	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。	<ul style="list-style-type: none">Windows では、<code><<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/win32_x86</code> です。Unix では、<code><<INSTALLDIR>>/sap_bobj/enterprise_xi40/<PLATFORM32></code> です。
<code>%CACHESERVER_EXE%</code>	Crystal Reports Cache Server の実行可能ファイル名。	<ul style="list-style-type: none">Windows では、<code>crcache.exe</code> です。Unix では、<code>boe_crcached.bin</code> です。

プレースホルダ	説明	デフォルト値
%CMS_EXE%	Central Management Server の実行可能ファイル名。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> Windows では、ConnectionServer.exe です。 Unix では、ConnectionServer です。
%CR2011_BINDIR%	Crystal Reports 2011 サーババイナリが保存されるディレクトリ。	<ul style="list-style-type: none"> Windows では、<<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/win32_x86 です。 Unix では、<<INSTALLDIR>>/sap_bobj/enterprise_xi40/<PLATFORM32>/ です。
%CR2011_DefaultWorkingDir%	Crystal Reports 2011 サーバのデフォルトの作業ディレクトリ。	<ul style="list-style-type: none"> Windows では、<<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/win32_x86 です。 Unix では、<<INSTALLDIR>>/sap_bobj/enterprise_xi40/<PLATFORM32>/ です。
%CRYSTALRAS_EXE%	Report Application Server の実行可能ファイル名。	<ul style="list-style-type: none"> Windows では、crystalras.exe です。

プレースホルダ	説明	デフォルト値
		<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> Windows では、このプレースホルダは空白です。 Unix では、<<INSTALLDIR>>/sap_bobj/enterprise_xi40/odbc.ini です。
%CommonJavaBundlesDir%	共有 OSGI バンドルが保存されるフォルダ。	<ul style="list-style-type: none"> Windows では、<<INSTALLDIR>>/SAPBusinessObjectsEnterprise 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。	<ul style="list-style-type: none"> Windows では、<<INSTALLDIR>>/SAPBusinessObjectsEnterprise 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です。	<ul style="list-style-type: none"> 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、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。	<ul style="list-style-type: none"> Windows では、<Path> です。 Unix では、<LD_LIBRARY_PATH> です。
%DLLPATH32%	Solaris 32 ビットシステムでは、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、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。	<ul style="list-style-type: none"> Solaris 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白です。
%DLLPATH64%	Solaris 64 ビットシステムでは、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、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。	<ul style="list-style-type: none"> Solaris 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白です。

プレースホルダ	説明	デフォルト値
	インストールされたコンピュータの環境変数の名前。	
<code>%DLLPREFIX%</code>	.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。	<ul style="list-style-type: none"> Windows では、このプレースホルダは空白です。 Unix では、lib です。
<code>%DLLPRELOAD%</code>	プラットフォーム向けの LD_PRELOAD 環境変数名です。	<ul style="list-style-type: none"> Windows では、このプレースホルダは空白です。 AIX では、<code><LDR_PRELOAD64></code> です。 その他の Unix では、<code><LD_PRELOAD></code> です。
<code>%DLLPRELOAD32%</code>	32 ビット AIX システム向けの LD_PRELOAD 環境変数名です。	<ul style="list-style-type: none"> Windows および Linux では、このプレースホルダは空白です。 AIX では、<code><LDR_PRELOAD></code> です。 Solaris では、<code><LD_PRELOAD_32></code> です。
<code>%DLLPRELOAD64%</code>	64 ビット AIX システム向けの LD_PRELOAD 環境変数名です。	<ul style="list-style-type: none"> AIX では、<code><LDR_PRELOAD64></code> です。 Solaris では、<code><LD_PRELOAD_64></code> 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白です。
<code>%DP%</code>	パスの区切り記号。	<ul style="list-style-type: none"> Windows では、セミコロン (;) です。 Unix では、コロン (:) です。
<code>%DefaultAuditingDir%</code>	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。	<ul style="list-style-type: none"> Windows では、<code><<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/Auditing</code> です。 Unix では、<code><<INSTALLDIR>>/sap_bobj/data/Auditing/</code> です。
<code>%DefaultDataDir%</code>	Job Server で使用される一時ディレクトリ。	<ul style="list-style-type: none"> Windows では、<code><<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/Data</code> です。 Unix では、<code><<INSTALLDIR>>/sap_bobj/data/</code> です。

プレースホルダ	説明	デフォルト値
%DefaultInputFRSDir%	Input File Repository Server のルートフォルダ。	<ul style="list-style-type: none"> Windows では、 <<INSTALLEDIR>>/SAP BusinessObjects Enterprise XI 4.0/ FileStore/Input です。 Unix では、<<INSTALLEDIR>>/ sap_bobj/data/frsinput で す。
%DefaultLoggingDir%	ログファイルの保存場所。	<ul style="list-style-type: none"> Windows では、 <<INSTALLEDIR>>/SAP BusinessObjects Enterprise XI 4.0/logging です。 Unix では、<<INSTALLEDIR>>/ sap_bobj/logging です。
%DefaultOutputFRSDir%	Output File Repository Server のルートフォルダ。	<ul style="list-style-type: none"> Windows では、 <<INSTALLEDIR>>/SAP BusinessObjects Enterprise XI 4.0/ FileStore/Output です。 Unix では、<<INSTALLEDIR>>/ sap_bobj/data/frsoutput で す。
%DefaultWorkingDir%	64 ビットサーバの作業ディレクトリ	<ul style="list-style-type: none"> Windows では、 <<INSTALLEDIR>>/SAP BusinessObjects Enterprise XI 4.0/ win64_x64 です。 Unix では、<<INSTALLEDIR>>/ sap_bobj/enterprise_xi40/ <PLATFORM64> です。
%DefaultWorkingDir32%	32 ビットサーバの作業ディレクトリ。	<ul style="list-style-type: none"> Windows では、 <<INSTALLEDIR>>/SAP BusinessObjects Enterprise XI 4.0/ win32_x86 です。 Unix では、<<INSTALLEDIR>>/ sap_bobj/enterprise_xi40/ <PLATFORM32> です。
%EVENTSERVER_EXE%	Event Server の実行可能ファイル名。	<ul style="list-style-type: none"> Windows では、 EventServer.exe です。

プレースホルダ	説明	デフォルト値
		<ul style="list-style-type: none"> • 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です。	<ul style="list-style-type: none"> • Windows では、.exe です。 • Unix では、このプレースホルダは使用できません。
%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、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。	<ul style="list-style-type: none"> • Windows では、<Path> です。 • Unix では、<PATH> です。
%EnterpriseDir%	64 ビットの Business Intelligence プラットフォームがインストールされる場所。	<ul style="list-style-type: none"> • 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 Business Intelligence プラットフォームがインストールされる場所。	<ul style="list-style-type: none"> • 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。	<ul style="list-style-type: none"> • 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。	<ul style="list-style-type: none"> • Windows では、fileserv.exe です。 • Unix では、boe_filesd です。
%HOARD_PATH%	メモリマネージャの場所。	<ul style="list-style-type: none"> • Solaris では、<<INSTALLDIR>>/sap_bobj/enterprise_xi40/solaris_sparcv9/libhoard3.so 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白です。

プレースホルダ	説明	デフォルト値
%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。	<ul style="list-style-type: none"> Solaris では、LD_PRELOAD_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白です。
%INSTALLROOTDIR%	64 ビットの 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。
%INSTALLROOTDIR32%	32 ビットの 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。	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。	\$IntroscopeAgentEnterpriseManagerHost
%IntroscopeAgentEnterpriseManagerPort%	計測データが送信される Introscope Agent Enterprise Manager ポート。	\$IntroscopeAgentEnterpriseManagerPort
%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。 <ul style="list-style-type: none"> 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.HttpsTunnelingSocketFactory
%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

プレースホルダ	説明	デフォルト値
%IntroscopeDir%	Introscope Agent Enterprise Manager がインストールされたフォルダ。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> Windows では、java.exe です。 Unix では、java です。
%JOBSERVERCHILD_EXE%	Adaptive Job Server の子の実行可能ファイル名。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> Windows では、JobServer.exe です。 Unix では、boe_jobcd です。
%JdkBinDir%	JDK バイナリが保存されるフォルダ。	<ul style="list-style-type: none"> Windows では、 <<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/ win64_x64/sapjvm/bin です。 Unix では、<<INSTALLDIR>>/ sap_bobj/enterprise_xi40/ <PLATFORM64>/sapjvm/bin です。
%JreBinDir%	JRE バイナリが保存されるフォルダ。	<ul style="list-style-type: none"> Windows では、 <<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/ win64_x64/sapjvm/jre/bin/ です。 Unix では、<<INSTALLDIR>>/ sap_bobj/enterprise_xi40/ <PLATFORM64>/ sapjvm/jre/bin です。

プレースホルダ	説明	デフォルト値
%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。	<ul style="list-style-type: none"> Windows では、このプレースホルダは空白です。 32 ビットの Unix では、-d32 です。 64 ビットの Unix では、-d64 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。	<ul style="list-style-type: none"> 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_IGNORE_CONSOLE_EVENTS%	Java 仮想マシンによるオペレーティングシステムシグナルの使用を低減するコマンドラインパラメータ	<ul style="list-style-type: none"> Windows では、-Xrs です。 Linux では、このプレースホルダは使用できません。 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白です。
%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。	<ul style="list-style-type: none"> Windows では、"-Xjvms" "-XsapSystem:08" です。 Unix では、このプレースホルダは空白です。
%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。	<ul style="list-style-type: none"> Windows では、<<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/Languages/ です。 Unix では、<<INSTALLDIR>>/sap_bobj/enterprise_xi40/Languages/ です。
%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。	<ul style="list-style-type: none"> 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
%LSTDir%	LST 設定ファイルが保存されるフォルダ。	<ul style="list-style-type: none"> Windows では、 <code><<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/ conf/lst</code> です。 Unix では、<code><<INSTALLDIR>>/ sap_bobj/enterprise_xi40/ conf/lst</code> 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。	<ul style="list-style-type: none"> AIX では、<code>-Xms01M</code> 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白です。
%NCSInstrumentLevelThreshold%	NCS ライブラリのトレースロ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 2011 処理サーバの実行可能ファイル名。	<ul style="list-style-type: none"> Windows では、<code>crproc.exe</code> です。 Unix では、<code>boe_crprocd.bin</code> です。
%PAGESERVERWRAPPED_EXE%		<ul style="list-style-type: none"> Windows では、<code>crproc.exe</code> です。 Unix では、<code>boe_crprocd</code> です。
%PJSContainerDir%	APS コンテナ JAR が保存されるフォルダ。	<ul style="list-style-type: none"> Windows では、 <code><<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/ java/pjs/container</code> です。 Unix では、<code><<INSTALLDIR>>/ sap_bobj/enterprise_xi40/ java/pjs/container</code> です。
%PJSServicesDir%	APS サービス JAR が保存されるフォルダ。	<ul style="list-style-type: none"> Windows では、 <code><<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/ java/pjs/services</code> です。 Unix では、<code><<INSTALLDIR>>/ sap_bobj/enterprise_xi40/ java/pjs/services</code> です。
%Platform%	Business Intelligence 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。	Business Intelligence 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。

プレースホルダ	説明	デフォルト値
%Platform32%	Business Intelligence プラットフォームが稼働しているマシンの 32 ビットオペレーティングシステム。	Business Intelligence 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。
%PS_JVM_OS_STACK_SIZE%	APS 用の JVM スタックサイズ	<ul style="list-style-type: none"> AIX では、-Xms01M 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白です。
%RasBinDir%	Report Application Server のルートフォルダ。	<ul style="list-style-type: none"> Windows では、<<INSTALLDIR>>/SAP BusinessObjects Enterprise XI 4.0/win32_x86 です。 Unix では、<<INSTALLDIR>>/sap_bobj/enterprise_xi40/<PLATFORM32>/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。
%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。	<ul style="list-style-type: none"> 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%		<ul style="list-style-type: none"> 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 環境変数名です。	<ul style="list-style-type: none"> Linux では、\$LD_PRELOAD \$:libmda_api.so:libmda_common.so です。

プレースホルダ	説明	デフォルト値
		<ul style="list-style-type: none"> 他のオペレーティングシステムでは、\$LD_PRELOAD\$ です。
%WEBISERVER_EXE%	Web Intelligence Processing Server の実行可能ファイル名。	<ul style="list-style-type: none"> Windows では、<code>wireportserver.exe</code> です。 Unix では、<code>WIReportServer</code> です。
%WEBI_LD_PRELOAD_ONCE%	プラットフォーム向けの LD_PRELOAD_ONCE 環境変数名です。	<\$LD_PRELOAD_ONCE\$>
%XCCACHE_EXE%	Dashboards Cache Server の実行可能ファイル名。	<ul style="list-style-type: none"> Windows では、<code>xccache.exe</code> です。 Unix では、<code>boe_xccached</code> です。
%XCPROC_EXE%	Dashboards Processing Server の実行可能ファイル名。	<ul style="list-style-type: none"> Windows では、<code>xcproc.exe</code> です。 Unix では、<code>boe_xcprocd</code> です。

i 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%**
- **%WarfilesDir%**

関連リンク

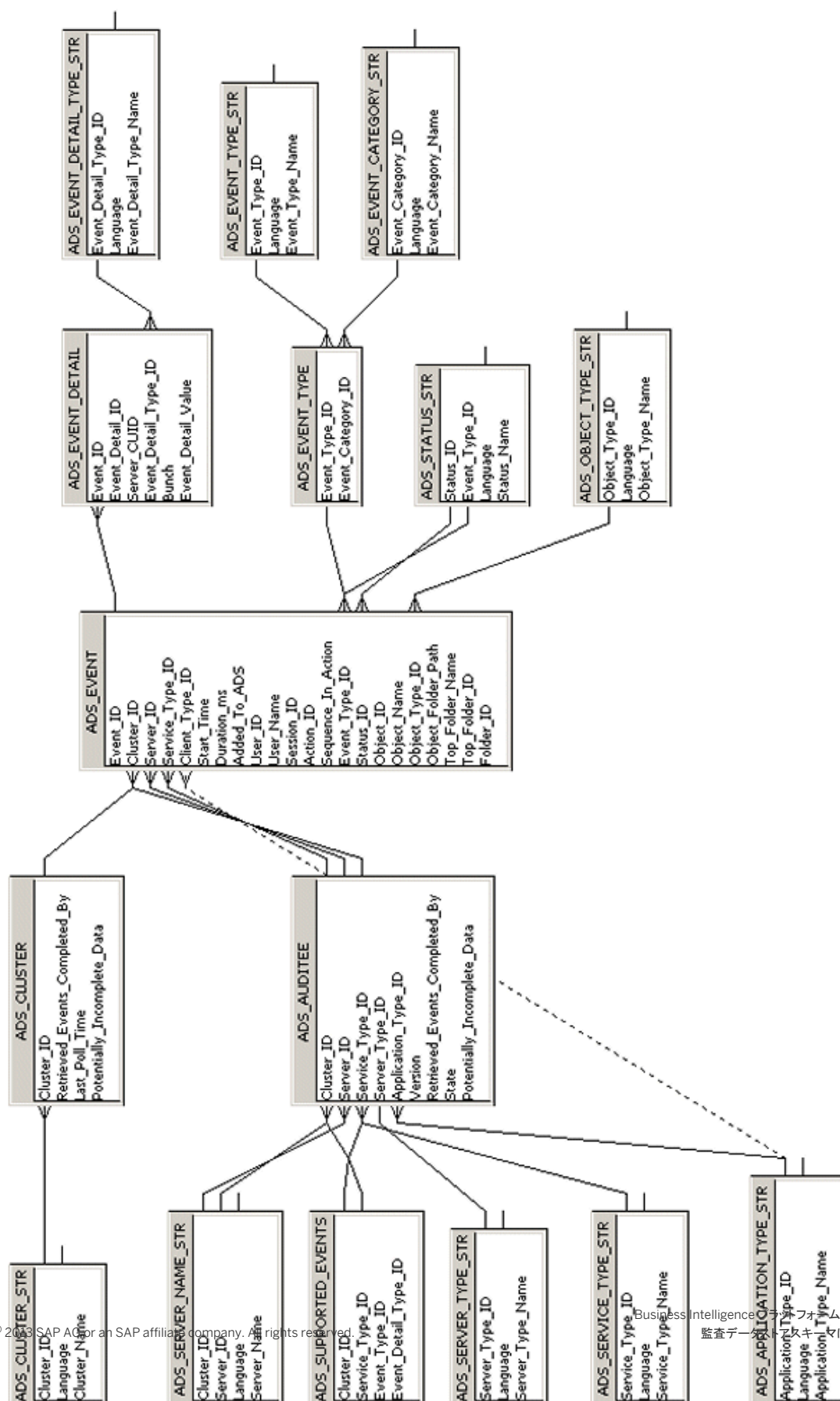
[ノードのプレースホルダを表示および編集する \[ページ 374\]](#)

31 監査データストアスキーマに関する付録

31.1 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。

31.2 スキーマ図



31.3 監査データストアテーブル

ADS_EVENT テーブル

このテーブルは、スキーマ内の他のテーブルとのセントラルリンクポイントとなる各イベントの基本プロパティを記録します。

列名	フィールドタイプ	キー	説明
Event_ID	文字 (64)	1 次キー	イベントに対して生成される一意の ID
Cluster_ID	文字 (64)	ADS_Auditee テーブルの外部キー	監査対象クラスタの GUID。この値が記録されるのは、複数のクラスタが同じ ADS を使用している場合があるためです。
Server_ID	文字 (64)	ADS_Auditee テーブルの外部キー	イベントを呼び出したサーバの CUID
Service_Type_ID	文字 (64)	ADS_Auditee テーブルの外部キー	<ul style="list-style-type: none">イベントを呼び出したサービスタイプの CUID。サーバ上のサービスは自身のサービスタイプ CUID を記録します。BI 起動パッド、Web Intelligence などのクライアントアプリケーションは、そのアプリケーションタイプ CUID を記録します。
Client_Type_ID	文字 (64)	ADS_Application_Type テーブルの外部キー	セッションを確立したクライアントのクライアントタイプ ID を記録します。
Start_Time	DateTime	該当せず	イベントの処理が開始された日付と時刻 (UTC、ミリ秒を含む)
Duration_ms	整数	該当せず	処理時間 (ミリ秒)
Added_to_ADS	DateTime	該当せず	イベントが ADS に記録された日付と時刻 (UTC)
User_ID	文字 (64)	該当せず	アクションを実行したユーザの CUID
User_Name	文字 (255)	該当せず	アクションを実行したユーザの ID に関連付けられている名前。監査 CMS のデフォルト言語で記録されます。
Session_ID	文字 (64)	該当せず	イベントの呼び出し時に実行されていたセッションの GUID。関連セッションがない場合、フィールドは NULL になります。
Action_ID	文字 (64)	該当せず	イベントを呼び出したユーザアクションの ID。1 つのユーザアクションによって発生したイベントのグループ化に使用されます。
Sequence_In_Action	整数	該当せず	マルチサーバ (またはクライアントとマルチサーバ) イベントの場合に、イベントを呼び出したサーバアプリケーション

列名	フィールドタイプ	キー	説明
			ョンまたはクライアントアプリケーションのシーケンス。すべてのスケジュールワークフローで、このシーケンス ID は常に 0 になります。
Event_Type_ID	整数	ADS_Event_type テーブルの外部キー	イベントのタイプ (表示または保存など)
Status_ID	整数	ADS_Status_Str テーブルの外部キー	処理のステータス (例: "0" = 成功、"1" = 失敗)
Object_ID	文字 (64)	該当せず	処理を実行したオブジェクトの CUID
Object_Name	文字 (255)	該当せず	処理を実行したオブジェクトの名前。監査 CMS のデフォルト言語で記録されます。
Object_Type_ID	文字 (64)	ADS_Object_Type_Str テーブルの外部キー	処理を実行したオブジェクトタイプの CUID
Object_Folder_Path	文字 (255)	該当せず	処理を実行したオブジェクトの完全フォルダパス (Country/Region/City など)。監査 CMS のデフォルト言語で記録されます。フォルダパスを特定できない場合、この値は NULL になります。
Folder_ID	文字 (64)	該当せず	処理を実行したオブジェクトのフォルダの CUID
Top_Folder_Name	文字 (255)	該当せず	オブジェクトのトップレベルフォルダの名前。たとえば、オブジェクトが Country/Region/City に配置されている場合は、Country が記録されます。
Top_Folder_ID	文字 (64)	該当せず	オブジェクトが配置されているトップレベルフォルダの CUID。たとえば、オブジェクトが Country/Region/City に配置されている場合は Country フォルダの CUID が記録されます。

ADS_EVENT_DETAIL テーブル

このテーブルはイベント詳細プロパティを記録します。

列名	タイプ	キー	説明
Event_Detail_ID	整数	1 次キー	イベント詳細の GUID
Event_ID	文字 (64)	ADS_Event の外部キー	親イベントの GUID

列名	タイプ	キー	説明
Event_Detail_Type_ID	整数	ADS_Event_Detail_Str の外部キー	イベント詳細のタイプ
Bunch	整数	該当せず	<p>詳細が一連の詳細の一部である場合に、これを使用して詳細をまとめます。</p> <p>たとえば、レポートに州と国のプロンプトがある場合に、国のプロンプトに「米国」、州のプロンプトに「カリフォルニア」および「ネバダ」を入力したとします。これにより、2 つの束 (Bunch) を含むイベント詳細が作成されます。束 1 は以下のように構成されます。</p> <ul style="list-style-type: none"> プロンプト名: 国 プロンプト値: 米国 <p>束 2 は以下のように構成されます。</p> <ul style="list-style-type: none"> プロンプト名: 州 プロンプト値: カリフォルニア プロンプト値: ネバダ
Event_Detail_Value	文字 (ロングテキスト)	該当せず	イベント詳細の値

ADS_AUDITEE テーブル

このテーブルはデプロイメントに含まれるすべての監査対象サーバのプロパティ情報を記録します。

列名	タイプ	キー	説明
Cluster_ID	文字 (64)	1 次キー	監査対象が属しているクラスタの GUID
Server_ID	文字 (64)	<ul style="list-style-type: none"> 1 次キー ADS_Server_Name_STR 	イベントを呼び出したサーバの CUID。イベントがクライアントによって呼び出された場合は、イベントを処理した Adaptive Processing Server の CUID を記録します。
Service_Type_ID	文字 (64)	<ul style="list-style-type: none"> 1 次キー ADS_Service_Type_Str ADS_Supported_Events 	イベントを呼び出したサービスのサービスタイプの CUID。クライアントによって呼び出されたイベントの場合は、アプリケーションタイプの CUID が記録されます。
Server_Type_ID	文字 (64)	ADS_Server_Type_Str	イベントを呼び出したサーバのサーバタイプの CUID

列名	タイプ	キー	説明
Application_Type_ID	文字 (64)	ADS_Application_Type_Str	イベントを呼び出したクライアントのアプリケーションタイプの CUID。サーバイベントの場合は、サービスタイプの ID が記録されます。
Version	文字 (64)	該当せず	イベントを呼び出したサーバまたはクライアントの記録時のバージョン
Retrieved_Events_Completed_By	DateTime	該当せず	前回、監査 CMS が監査対象の一時ファイルをポーリングした日時。これにより、この日時より前に完了した監査対象のすべてのイベントが ADS 内にあることを示します。
State	整数	該当せず	監査対象の状態 (実行中、停止中、削除済みなど)
Potentially_Incomplete_Data	整数	該当せず	監査対象に、ADS に転送されていないイベントが含まれている可能性があるかどうかを示します。

ADS_SERVER_NAME_STR テーブル

このテーブルは、サーバ名の多言語辞書を提供します。サーバの名前が変更されると、値が更新されます。

列名	タイプ	キー	説明
Cluster_ID	文字 (64)	1 次キー	サーバが属しているクラスタの GUID
Server_ID	文字 (64)	1 次キー	サーバの CUID
Language	文字 (10)	1 次キー	サーバ名の言語のコード。〈EN〉、または 〈DE〉 など。
Server_Name	文字 (255)	該当せず	サーバの名前です。

ADS_SERVICE_TYPE_STR テーブル

このテーブルは、サービスタイプ名の多言語辞書を提供します。

列名	タイプ	キー	説明
Service_Type_ID	文字 (64)	1 次キー	サービスのサービスタイプまたはサービスカテゴリの CUID
Language	文字 (10)	1 次キー	サービスタイプ名が記録される言語のコード。〈EN〉、または 〈DE〉 など。
Service_Type_Name	文字 (255)	該当せず	サービスタイプの名前

ADS_APPLICATION_TYPE_STR テーブル

このテーブルは、クライアントアプリケーションタイプ名の多言語辞書を提供します。

列名	タイプ	キー	説明
Application_Type_ID	文字 (64)	1 次キー	アプリケーションのアプリケーションタイプの CUID
Language	文字 (10)	1 次キー	アプリケーションタイプが記録される言語コード。<EN>、または <DE> など。
Application_Type_Name	文字 (255)	該当せず	アプリケーションタイプのテキスト名。「Crystal Reports」、または「Web Intelligence」など。

ADS_SUPPORTED_EVENTS テーブル

このテーブルは、サービスまたはクライアントアプリケーションのタイプごとにサポートされるイベントおよび関連するイベント詳細の一覧を記録します。

列名	タイプ	キー	説明
Cluster_ID	文字 (64)	1 次キー	サービスが属しているクラスタの GUID
Service_Type_ID	文字 (64)	1 次キー	イベントを呼び出したサービスのサービスタイプの CUID。イベントがクライアントアプリケーションによって呼び出された場合は、アプリケーションタイプの CUID が記録されます。
Event_Type_ID	整数	ADS_Event_Type の外部キー	記録されるイベントタイプの ID (「保存」の ID など)
Event_Detail_Type_ID	整数	ADS_EVENT_DETAIL_TYPE_STR	イベントに対して取得されるイベント詳細のタイプを識別する CUID (ファイルパスなど)

ADS_CLUSTER テーブル

このテーブルは、監査対象が含まれているすべてのクラスタに関する情報を記録します。

列名	タイプ	キー	説明
Cluster_ID	文字 (64)	<ul style="list-style-type: none">1 次キーADS_Cluster_Str	クラスタの GUID
Retrieved_Events_Completed_By	DateTime	該当せず	データベース内のクラスタの監査情報の最終取得日時を示します。どの時点においても、実行中のすべての監査対象サ

列名	タイプ	キー	説明
			サーバについて取得された監査タイムスタンプのうち最も古いものを記録します。これにより、この日時より前に完了したすべてのイベントが ADS 内にあることを示します。
Last_Poll_Time	DateTime	該当せず	前回、監査 CMS がこのクラスタ内の監査対象をポーリングした日時
Potentially_Incomplete_Data	整数	該当せず	クラスタ内に不完全な監査情報がある可能性を示します。"0" = すべてのサーバが正常にデータを転送しました。"1" = クラスタ内の少なくとも 1 つのサーバ (実行中または停止中を問わず) に [Potentially Incomplete Data] フラグが設定されています。これは、監査対象の 1 つに ADS に転送されていないイベントがあることを意味します。

ADS_CLUSTER_STR テーブル

このテーブルは、デプロイメント内のさまざまなクラスタの参照レコードを提供します。

列名	タイプ	キー	説明
Cluster_ID	文字 (64)	1 次キー	クラスタの一意の ID
Language	文字 (10)	該当せず	クラスタの言語設定のコード。<EN>、または <DE> など。
Cluster_Name	文字 (255)	該当せず	クラスタの名前。

ADS_EVENT_TYPE テーブル

このテーブルは、さまざまなイベントカテゴリの参照レコードを提供します。

列名	タイプ	キー	説明
Event_Type_ID	整数	複合: <ul style="list-style-type: none"> 1 次キー ADS_Event_Type_Str 	イベントタイプの一意の ID
Event_Catagory_ID	整数	ADS_Event_Category_Str テーブル	イベントのカテゴリ。たとえば、「共通」、「Web Intelligence」、または「ライフサイクルマネジメント」。

ADS_EVENT_TYPE_STR テーブル

このテーブルは、イベントタイプ名の多言語辞書を提供します。

列名	タイプ	キー	説明
Event_Category_ID	整数	1 次キー	イベントのイベントタイプ ID
Language	文字 (10)	1 次キー	イベントカテゴリ名が記録される言語のコード。 <EN>、または <DE> など。
Event_Type_Name	文字 (255)	該当せず	イベントタイプのテキスト名。「表示」または「ログオン」など。

ADS_EVENT_CATEGORY_STR テーブル

このテーブルは、イベントカテゴリ名の多言語辞書を提供します。

列名	タイプ	キー	説明
Event_Type_ID	整数	1 次キー	イベントカテゴリの ID
Language	文字 (10)	1 次キー	イベントカテゴリ名が記録される言語のコード。 <EN>、または <DE> など。
Event_Category_Name	文字 (255)	該当せず	イベントカテゴリの名前

ADS_EVENT_DETAIL_TYPE_STR テーブル

このテーブルは、イベント詳細タイプ名の多言語辞書を提供します。

列名	タイプ	キー	説明
Event_Detail_ID	整数	1 次キー	イベント詳細のイベント詳細タイプ ID
Language	文字 (10)	1 次キー	イベント詳細名が記録される言語のコード。 <EN>、または <DE> など。
Event_Detail_Type_Name	文字 (255)	該当せず	イベント詳細タイプのテキスト名

ADS_OBJECT_TYPE_STR テーブル

このテーブルは、イベントオブジェクト名の多言語辞書を提供します。

列名	タイプ	キー	説明
Object_Type_ID	文字 (64)	1 次キー	オブジェクトのオブジェクトタイプの CUID
Language	文字 (10)	1 次キー	オブジェクトタイプ名が記録される言語のコード。<EN>、または <DE> など。
Object_Type_Name	文字 (255)	該当せず	オブジェクトタイプの名前

ADS_STATUS_STR テーブル

このテーブルは、イベントステータス名の多言語辞書を提供します。

列名	タイプ	キー	説明
Status_ID	整数	1 次キー	処理のステータスを数字で表したもの
Event_Type_ID	整数	1 次キー	イベントのイベントタイプの ID。たとえば、「表示」の場合は 1002。
Language	文字 (10)	1 次キー	イベントステータスが記録される言語のコード。<EN>、または <DE> など。
Status_Name	文字 (255)	該当せず	イベントステータスのテキストによる説明。「成功」または「失敗」など。

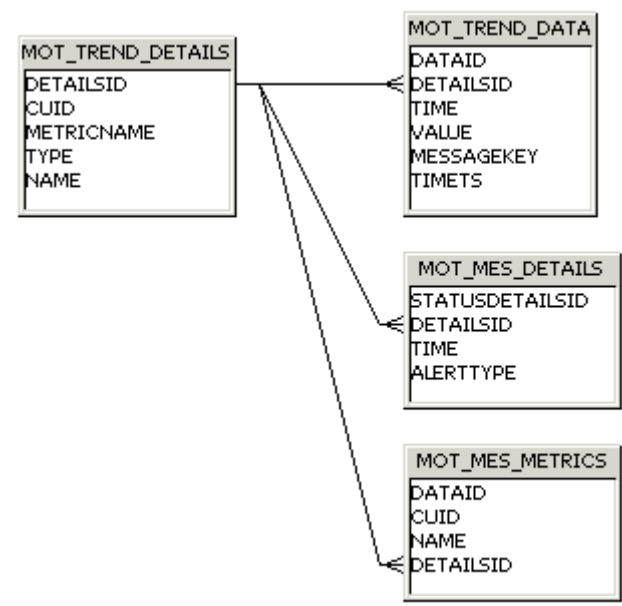
ADS_EVENT_DELETES

この表を使用、またはこの表からレポートを生成しないでください。内部システム使用専用で、今後のリリースで削除される予定です。

32 モニタリングデータベーススキーマに関する付録

32.1 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ダイアグラム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か、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
Type	VARCHAR(32)	該当せず	"Subscription"、"ManagedEntityStatus"、または "Probe" のいずれか
名前	VARCHAR(255)	該当せず	Type が "ManagedEntityStatus" の場合は監視の名前。それ以外の場合は、Type と同じ文字列にデフォルト設定さ

列名	型	キー	説明
			れます。ただし、すべてが大文字になります (例: "PROBE" または "SUBSCRIPTION")。

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ド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 から)	
Time or TimeT	BIGINT、 NUMBER、または FIXED Unix エポック時間	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の Null。監視の場合は "watchEnabled" または "watchDisabled" にすることもできます。これが "キー" であるのは、UI が表示される前にローカライズされたメッセージを取得するため、最終的に使用されることが理由です。
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刻

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	

列名	型	キー	説明
DetailsId	INTEGER	外部キー (MOT_TREND_DETAILS から)	
Time	BIGINT または NUMBER Unix エポック時間	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 から)	
CUID	VARCHAR(64)	該当せず	監視の CUID
Name	VARCHAR(255)	該当せず	監視の名前

33 システムコピーワークシート

33.1 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す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。	
ライフサイクルマネジメント (LCM) のコピーを計画している場合は、LCM データベースフォルダと LCM 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。	



www.sap.com/contactsap

© 2013 SAP AG or an SAP affiliate company. All rights reserved.

本書のいかなる部分も SAP AG の明示的許可なしに、いかなる形式、目的を問わず、複写、または送信することを禁じます。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 AG がライセンス、またはその頒布業者が頒布するソフトウェア製品には、他のソフトウェア会社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 SAP AG およびその関連会社（「SAP グループ」）が情報提供のためにのみ提供するもので、いかなる種類の表明および保証を伴うものではなく、SAP グループは文書に関する錯誤又は脱漏等に対する責任を負うものではありません。SAP グループの製品およびサービスに対する唯一の保証は、当該製品およ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。

SAP、および本書で言及されるその他 SAP の製品およびサービス、ならびにそれらのロゴは、ドイツおよびその他諸国における SAP AG の商標または登録商標です。

商標に関する情報および表示の詳細については、<http://www.sap.com/corporate-en/legal/copyright/index.epx> をご覧ください。