



Web サービス管理者ガイド

■ SAP BusinessObjects Business Intelligence platform 4.0 Support Package 2

2011-05-06

著作権

© 2011 SAP AG. All rights reserved.SAP、R/3、SAP NetWeaver、Duet、PartnerEdge、ByDesign、SAP Business ByDesign、および本書に記載されたその他のSAP製品、サービス、ならびにそれぞれのロゴは、ドイツおよびその他の国々におけるSAP AGの商標または登録商標です。Business ObjectsおよびBusiness Objectsロゴ、BusinessObjects、Crystal Reports、Crystal Decisions、Web Intelligence、Xcelsius、および本書で引用されているその他のBusiness Objects製品、サービス、ならびにそれぞれのロゴは、米国およびその他の国々におけるBusiness Objects S.A.の商標または登録商標です。Business ObjectsはSAPのグループ企業です。本書に記載されたその他すべての製品およびサービス名は、それぞれの企業の商標です。本書に記載されたデータは情報提供のみを目的として提供されています。製品仕様は、国ごとに変わる場合があります。これらの文書の内容は、予告なしに変更されることがあります。また、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誤記・脱落等の過失に対する責任を負うものではありません。SAP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。

2011-05-06

目次

第 1 章	はじめに.....	5
1.1	このドキュメントについて.....	5
1.1.1	このドキュメントの対象者.....	5
1.1.2	Web サービスについて.....	5
1.2	Web サービスの移行.....	7
1.3	レガシーコンシューマアプリケーションのサポート.....	7
第 2 章	デプロイメントの設定.....	9
2.1	デプロイメントの検証.....	9
2.2	個別の Web サービスをアクティブに設定する.....	10
2.3	dsws.properties ファイルの設定.....	10
2.4	クラスタリングによる Web サービスのデプロイ.....	14
2.5	DMZ による Web サービスのデプロイ.....	15
第 3 章	デプロイメントのセキュリティ保護.....	17
3.1	公開鍵暗号化	17
3.2	クライアントおよびサーバー証明書	18
3.3	SSL を使用した安全な接続の確立.....	19
3.4	JDK を使用した証明書とキーストアの生成	20
3.5	Tomcat サーブレットコンテナの SSL の設定	21
3.6	SSL による Web サービスの使用.....	22
第 4 章	拡張性とパフォーマンス	23
付録 A	より詳しい情報.....	25
	索引.....	27

はじめに

1.1 このドキュメントについて

このドキュメントでは、SAP BusinessObjects Business Intelligence (BI) platform Web サービス デプロイメントを設定して管理するための情報と手順を提供します。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。

サポートされている Java Web アプリケーション サーバーに、Web サービスの `dswebobje.war` ファイルなどの BI platform Web アプリケーションをデプロイする方法については、『SAP BusinessObjects Business Intelligence Platform 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 platform のインストールの詳細については、『SAP BusinessObjects Business Intelligence Platform インストール ガイド』を参照してください。

BI platform サーバーの管理の詳細については、『SAP BusinessObjects Business Intelligence Platform 管理者ガイド』を参照してください。

1.1.1 このドキュメントの対象者

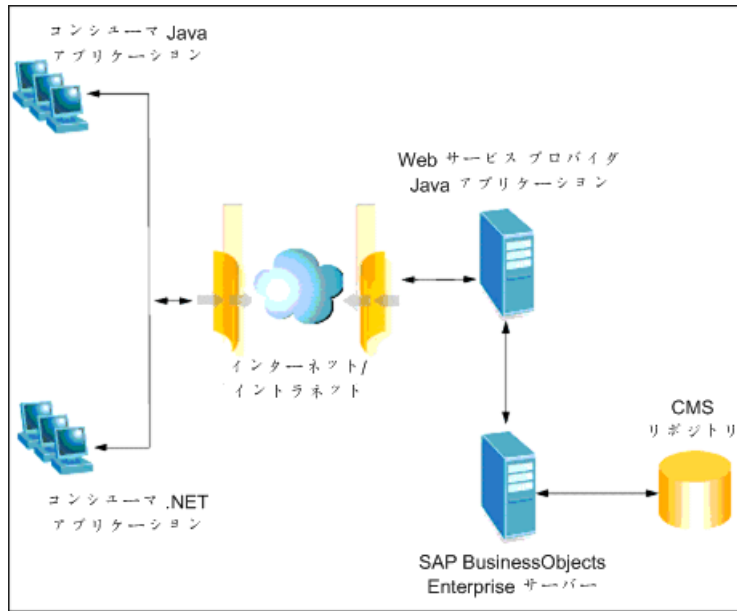
このヘルプでは、設定作業について説明します。次の作業を行うユーザーは、このガイドを参照することをお勧めします。

- ・ 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。

このドキュメントは、BI platform Web サービスの設定、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ー管理やスクリプトテクノロジ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、このドキュメントでは、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。

1.1.2 Web サービスについて

BI platform Web サービスを使用すると、HTTP 経由で BI platform デプロイメント内のオブジェクトをリモート操作できます。これにより、現在のデプロイメントを他の Web ベースのアプリケーションと簡単に統合できます。Web サービスは、プロバイダー Web アプリケーションと一連のコンシューマ API の 2 つの部分によってデプロイされます。



プロバイダーアプリケーション

プロバイダー アプリケーション (dswsbobje.war) は、BI platform システム内にデプロイされるさまざまな Web アプリケーションの 1 つです。プロバイダーアプリケーションは、他のクライアントアプリケーションが Web サービスとやり取りできるようにします。Web サービスプロバイダーアプリケーションは、WS-Interoperability Basic Profile 1.0 に準拠し、Apache Axis2 1.3 を使用して実装されます。

注

Web サービスの実装には Apache Axis2 が使用されるため、生成されるプロバイダーアプリケーションは、Java Web アプリケーションとして Java Web アプリケーションサーバーにデプロイする必要があります。

このドキュメントでは、デプロイされるプロバイダーアプリケーション (dswsbobje.war) を設定する方法について説明します。プロバイダー アプリケーションをデプロイする方法については、『SAP BusinessObjects Business Intelligence Platform 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。

コンシューマ API

プロバイダーによって公開される Web サービスを使用するクライアントアプリケーションがコンシューマアプリケーションです。BI platform は、インストール内にユーザー認証とセキュリティ、ドキュメントとレポートへのアクセス、スケジューリング、パブリケーション、およびサーバー管理を実装するための一連の Java および .NET コンシューマ API を提供します。コンシューマ API は WS-Interoperability Basic Profile 1.0 に準拠しています。BI platform Web サービスを使用してコンシューマ アプリケーションを開発する際は、このコンシューマ API の使用をお勧めします。

コンシューマ API を使用してカスタム アプリケーションを開発する方法については、『SAP BusinessObjects Business Intelligence Platform Web サービス コンシューマ SDK 開発者ガイド』を参照してください。コンシューマ

マ SDK は BI platform に含まれます。BI platform のインストールの詳細については、『SAP BusinessObjects Business Intelligence Platform インストール ガイド』を参照してください。

1.2 Web サービスの移行

ここでは、SAP BusinessObjects Business Intelligence platform Web サービスの以前のバージョンからアップグレードするときに注意する必要がある変更に関する情報を提供します。

廃止のサービス

QueryService、SaveService、および ReportEngine サービスは廃止され、サポートされなくなりました。代わりに、ABIPlatform サービスを使用してください。

小文字のサービス名は廃止

session、biplatform、liveoffice、bicatalog、publish などの Web サービスを参照する小文字の名前は廃止になりました。サービス名は、大文字と小文字が区別されるため、アプリケーション内では、サポートされている次のサービス名を使用してください。

- ・ Session
- ・ BIPlatform
- ・ LiveOffice
- ・ BICatalog (XI 3.0 で使用停止 - 代わりに BIPlatform サービスを使用)
- ・ Publish (XI 3.0 で使用停止 - 代わりに BIPlatform サービスを使用)

例: `http://<servername>:<port>/dswsbobje/services/Session`

1.3 レガシーコンシューマアプリケーションのサポート

SAP BusinessObjects Business Intelligence platform 4.0 プロバイダーは、SAP BusinessObjects Enterprise XI 3.x バージョンのコンシューマ アプリケーションと下位互換性があります。4.0 および XI 3.x プロバイダーは、Apache Axis2 Web サービス フレームワーク上に構築されています。BusinessObjects Enterprise XI Release 2 コンシューマは、Apache Axis 1.1 フレームワーク上に構築されており、XI 4.0 または XI 3.x コンシューマと互換性がありません。

デプロイメントの設定

このセクションでは、Web サービス デプロイメントを確認および設定する方法について説明します。Web サービスプロバイダーアプリケーションの既存のデプロイメントを確認する方法、およびニーズに合わせてデプロイメントをカスタマイズするために利用できる構成プロパティに関する指示が用意されています。

2.1 デプロイメントの検証

プロバイダーアプリケーションが正しくデプロイされていることを確認するには、Web ブラウザーで次の URL を開きます。

```
http://<servername>:<port>/dwsbobje
```

[Axis2 - ホーム] ページに、挨拶と listServices ページへのリンクが表示されます。

注

- ・ <servername> と <port> を Web サービスのデプロイ先のマシン名とポートに置き換えます。
- ・ [Axis2 - ホーム] ページが表示されない場合、またはエラーメッセージが表示される場合、プロバイダーアプリケーションはデプロイされていません。トラブルシューティングと再デプロイについては、『SAP BusinessObjects Business Intelligence Platform 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。

WSDL とサービスの確認

カスタム アプリケーションから Web サービスを使用するために、BI platform のインストールに付属する Java または .NET コンシューマ API を使用できます。ただし、プロバイダーが公開する WSDL からこの API を生成することもできます。WSDL は、WS-Interoperability Basic Profile 1.0 に準拠しています。

注

SAP 提供の Java および .NET コンシューマ API だけがサポートされています。WSDL から生成された API は、公式にはサポートされません。WSDL とコンシューマ API の詳細については、『SAP BusinessObjects Business Intelligence Platform Web サービス コンシューマ SDK 開発者ガイド』を参照してください。

WSDL が正しくデプロイされてアクセスできることを確認するには、Web ブラウザーで次の URL を開きます。

```
http://<servername>:<port>/dwsbobje/services/listServices
```

すべてのアクティブな Web サービスの一覧が表示されます。ここから、次の点を確認できます。

- ・ 名前付き Web サービスのハイパーリンクをそれぞれクリックして、そのサービスの WSDL を表示します。
- ・ WSDL で、アドレスバインディングの記述を確認します。バインディング URL に正しいサーバー名、ポート番号、および Web アプリケーションサーバー名が記載されていることを確認します。

dswsbobje.war の再デプロイ

Web サービス プロバイダー アプリケーション (dswsbobje.war) は、BI platform のデフォルト インストール中に、指定された Java アプリケーション サーバーに自動的にインストールされてデプロイされます。新しいまたは既存の Web アプリケーション サーバーにプロバイダーを再デプロイする方法については、『SAP BusinessObjects Business Intelligence Platform 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。このドキュメントには、dswsbobje.war を含むあらゆる BI platform Web アプリケーションをデプロイする方法が記載されています。以下のセクションで構成されています。

- ・ WDeploy コマンドラインまたは Windows ベースの GUI ツールを使用して、Web アプリケーションをデプロイする方法。
- ・ サポートされている Web アプリケーションサーバーの管理コンソールを使用して、Web アプリケーションを手動でデプロイする方法。
- ・ サポートされているデプロイメントシナリオ。

2.2 個別の Web サービスをアクティブに設定する

サービスの services.xml ファイル内のプロパティ値に基づいて、デプロイメント内の Web サービスを個別に有効または無効にすることができます。Web サービスごとに専用の services.xml ファイルがあります。次の例では、BICatalog サービスを無効にする方法を示します。

- 1 このサービスの services.xml ファイルを見つけて開きます。
たとえば、デフォルトの Windows インストールの場合、BICatalog サービスのファイルは C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\services\bicatalog\META-INF\ にあります。
- 2 activate プロパティを service タグに追加し、その値を false に設定します。
たとえば、BICatalog サービスを無効にする場合は、<service name="BICatalog" activate="false"> のようになります。
- 3 Web アプリケーションサーバーを再起動します。

注

上記の手順を使用してサービスを無効にした場合でも、無効にしたサービスの WSDL ファイルにアクセスできる場合があります。これは、そのサービスがまだ有効であるということではありません。コードでサービスの操作を呼び出そうとしても、エラーメッセージが表示されます。このメッセージは、サービスが無効になっていることを示します。

2.3 dsws.properties ファイルの設定

このセクションでは、Web サービスの実行時の動作を設定する方法を示します。dsws.properties ファイルには、デプロイメント内の変更可能な構成情報が入っています。デフォルトの Windows インストールの場合、このファイルは C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes\ にあります。

dsws.properties ファイルで定義され、設定できるプロパティは次のとおりです。

プロパティ	説明
domain	<p>Central Management Server (CMS) のドメイン名。このプロパティは、CMSname:CMSport 形式で入力する必要があります。セキュリティを向上させるために、CMS ドメインの名前を設定して、Web サービスが適切な CMS にのみアクセスできるようにすることをお勧めします。ドメインを設定しなかった場合は、悪意のあるユーザーがネットワーク上の CMS サーバーにアクセスできる可能性があります。</p> <p>注 クラスタリングデプロイメントを設定して、CMS とは別のサーバーで Web サービスをホストする場合は、このプロパティを設定する必要があります。このプロパティを正しく設定しないと、SAP Crystal Reports for Enterprise 4.0 のようにシステムの Web サービスに依存するアプリケーションは正しく実行されません。</p>
entry.size	辞書エンTRIESに格納できる最大文字数を指定します。entry.size を 0 に設定するか、空白にすると、データベースエンTRIESを任意のサイズにできます。
temp.dir	一時ファイルが保存されるディレクトリ。
image.dir	HTML 形式の Crystal レポートを取得するときに、一時イメージファイルを保存するディレクトリ。
image.cleanup	イメージの内容がフェッチされた後で一時イメージを削除するには、このプロパティを true に設定します。このプロパティを true に設定しない場合は、イメージ削除プログラムがバックグラウンドスレッドで実行され、image.dir プロパティで指定されたディレクトリ内のイメージが定期的に削除されます。
report.server	<p>SAP BusinessObjects Web サービスで使用するレポートサーバー。</p> <p>デフォルト設定は ps です。</p>
bicatalog.defaultObjectProperties=si_in stance,si_name,si_description	BICatalog Web サービスのデフォルトのプロパティ。

プロパティ	説明
clustered	クラスタリングを有効にするには、このプロパティを true に設定します。 デフォルト設定は False です。
fileCachePath	ファイルダウンロード/アップロードのキャッシュデータが保存されるディレクトリ。 デフォルト値は c:\Program Files\Business Objects\Attachment File Cache です。
checksumMethod	チェックサム検証メソッドを指定します。ダウンロードされているファイルチャンクの整合性を確認するために使用されます。 指定できる値: NONE。検証は実行されません。 BYTECOUNT。ファイルチャンクの長さ(バイト数)に基づく検証を行います。 MD5。MD5 (高度な「指紋」アルゴリズム)に基づく検証を行います。 SIMPLE。ファイルチャンク内の各バイトの合計を計算して検証し、この合計を比較に使用します。 デフォルト設定は SIMPLE です。
maximumChunkSize	一度の BIPlatform.uploadFile メソッド呼び出しでアップロードできるチャンクの最大サイズをバイト単位で指定します。 デフォルト値は 262144 です。
maximumUploadFileSize	アップロードできるファイルの最大サイズをバイト単位で指定します。 デフォルト値は 10485760 です。

プロパティ	説明
numChunksPerSDKChunk	<p>一度の BIPlatform.downloadFile メソッド呼び出しでダウンロードされる 64 KB チャンクの数指定します。たとえば、この値が 2 に設定されている場合は、各呼び出しで 128 KB のデータがダウンロードされます。</p> <p>デフォルト値は 4 です。</p>
defaultPageSize	<p>1 ページで返される InfoObject の数を指定します。ページは、パスクエリーを使用して BIPlatform.get メソッドを呼び出すことで返されます。</p> <p>デフォルト値は 100 です。</p>
noPagingQueryLimit	<p>ページングを使用しない場合に、パスクエリーで返される InfoObject の最大数を指定します。クエリー結果をページングするには、OrderBy 句の各 InfoObject プロパティをインデックス付きプロパティにするか、allowedOrderBy プロパティで指定する必要があります。</p> <p>デフォルト値は 1000 です。</p>
defaultSelectList	<p>各パスクエリーによってデフォルトで返されるクエリー言語プロパティのカンマ区切りリストを指定します。アスタリスク文字 (*) を使用すると、すべてのプロパティを指定できます。</p>
searchSelectList	<p>検索によって返されるクエリー言語プロパティのカンマ区切りリストを指定します。アスタリスク文字 (*) を使用すると、すべてのプロパティを指定できます。</p>
allowedOrderBy	<p>並べ替えの基準にするクエリー言語プロパティのカンマ区切りリストを指定します。このプロパティにより、インデックス付けされていないクエリー言語プロパティによるページングおよび並べ替えを実行できます。</p>
validateXML	<p>Web サービスプロバイダーから渡された各 XML メッセージを検証するかどうかを指定します。使用できる値は true と false です。</p> <p>デフォルト値は false です。</p>

例 dsws.properties ファイルの例

以下は dsws.properties ファイルの例です。

```
Trace=0
entry.size=255
temp.dir=
image.dir=
image.cleanup=false
domain=MyCMS:6400
report.server=ps
bicatalog.defaultObjectProperties=si_instance,si_name,si_description
```

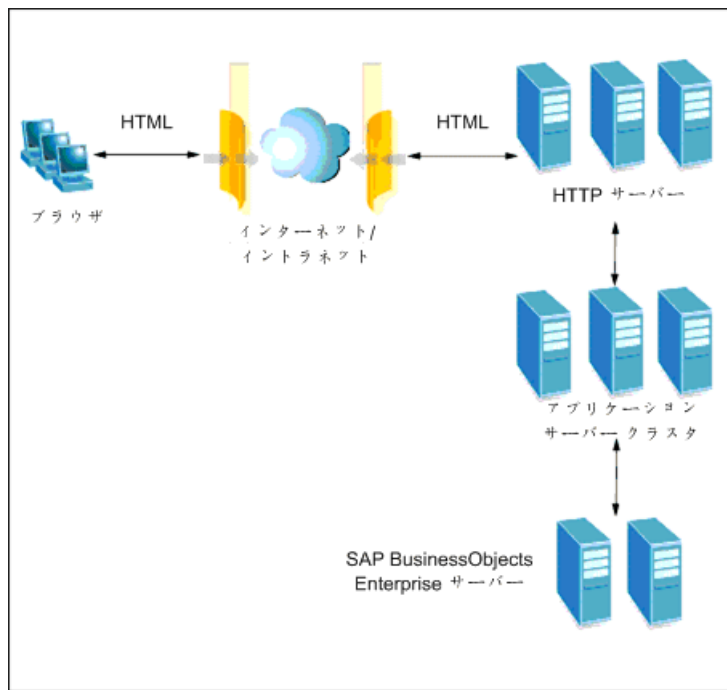
2.4 クラスターリングによる Web サービスのデプロイ

クラスターリングされた構成に Web サービスをデプロイすることができます。クラスターリングを有効にして Web サービスをデプロイすることで、スケーラビリティとフェイルオーバー機能が大幅に強化されます。

注

クラスターリングは、Web ファームとも呼ばれます。

次の図は、一般的なクラスターリングされたデプロイメントを示しています。



Web サービスプロバイダーのデプロイメントでクラスターリングを有効にする

クラスターリングされた環境でプロバイダーアプリケーションを実行するには、各サーバーで dsws.properties ファイルを開き、clustered パラメータの値を true に変更します。

次に、クラスタ内のすべてのアプリケーションサーバーによって共有されるイメージディレクトリを設定します。各サーバーにある dsws.properties ファイルの tmp_images プロパティを更新して、共有イメージディレクトリをポイントするようにします。

次に、web.xml ファイルを編集し、<webapps> タグの間にある <distributable/> タグのコメントを解除します。次に例を示します。

```
<web-app>
<display-name>dsws2</display-name>
<!-- when using tomcat webserver cluster, please make <distributable /> available by recommending follow line -->
<distributable />
```

注

- web.xml ファイルは WAR ファイルに含まれます。web.xml ファイルのデフォルトの場所は、¥Program Files¥SAP Business Objects¥Tomcat¥webapps¥dswsobje¥WEB-INF です。Tomcat を実際の Web アプリケーションサーバー名に置き換えてください。
- クラスタリングを有効にしてアプリケーションサーバーをセットアップする方法については、アプリケーションサーバーのマニュアルを参照してください。

クラスタリングされたプロバイダーに対するコンシューマアプリケーションのデプロイ

クラスタリングを有効にして Web サービスのプロバイダーを使用するには、Web サービスのコンシューマがそれぞれのセッション状態を管理する必要があります。コンシューマ アプリケーションで、SAP BusinessObjects Business Intelligence platform に付属するコンシューマ API を使用すると、この管理は自動的に実行されます。コンシューマアプリケーションが、用意されているコンシューマ API を使用せず、WSDL から生成されたコンシューマを使用する場合は、セッションを手動で管理する必要があります。

ServerInfo クラスは Session サービスの一部として提供されるため、Web サービスコンシューマは、プロバイダーがクラスタリングデプロイメントを使用しているかどうかをチェックできます。コンシューマは、このクラスを使用して、プロバイダーがクラスタリングデプロイメントを使用しているかどうかをチェックする必要があります。使用されている場合、コンシューマはセッション状態を管理する必要があります。

ServerInfo を使用したクラスタリングデプロイメントのチェック

ServerInfo オブジェクトを取得するには、Session.getServerInfo() メソッドを使用します。ServerInfo オブジェクトを取得すると、ServerInfo.getClustered() メソッド (Java) または ServerInfo.Clustered メソッド (.NET) を使用して、プロバイダーがクラスタリングデプロイメントを使用しているかどうかを判別されます。クラスタリングが使用されている場合、これらのメソッドは論理値 true を返し、それ以外の場合は false を返します。クラスタリングが使用されている場合、コンシューマはセッション状態を管理する必要があります。

セッション状態の管理

.NET API を使用して Web サービスのセッション状態を管理する方法については、MSDN オンラインマニュアルを参照してください。Java コンシューマ API を使用する場合は、デフォルトでセッション状態が管理されます。

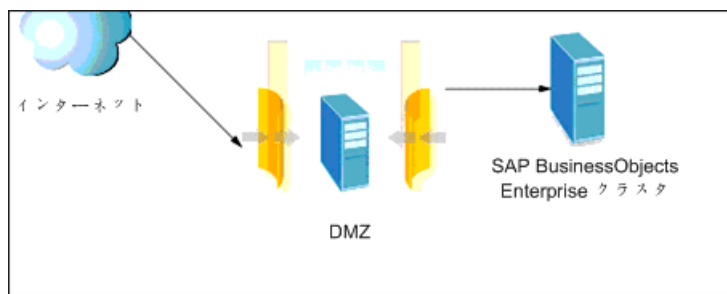
2.5 DMZ による Web サービスのデプロイ

BI platform Web サービスは、エクストラネットレベルのセキュリティを採用しているため、DMZ を使用する Web サービスをデプロイして情報を保護できます。

DMZ (非武装地帯) という用語は、アプリケーションサーバーがファイアウォールの背後にあり、異なるサブネットで実行される Web サーバーとは分離されているネットワークボロジを指します。Web サーバーは、ファイアウォールで外部ネットワークから保護されます。

このように、DMZ は、企業のイントラネットと外部ネットワークまたはインターネットの間の緩衝地帯として保護されます。DMZ は、企業データを保持するサーバーに外部ユーザーがアクセスできないように設計されています。

これを次の図に示します。



DMZ デプロイメントのインストール方法については、『SAP BusinessObjects Business Intelligence Platform 管理者ガイド』を参照してください。

デプロイメントのセキュリティ保護

Web サービスデータ転送のセキュリティを保証するには、SSL (Secure Socket Layers) を使用して、すべての SAP BusinessObjects Web サービス応答を暗号化します。SSL は、Web サービスとコンシューマの間でやり取りされるデータを暗号化します。また、データが送信者から受信者に転送される間に変更されることを防ぐため、トランザクション検証も提供します。データが変更されると認証コードが無効になり、データが変更されたという警告が受信者に示されます。したがって、他の多くの暗号化またはデータ保護スキームに比べて、SSL には主に 2 つの利点があります。

- ・ 公開鍵暗号化により、安全でないデータや盗聴者が通信の暗号を復号化できるようなデータを転送することなくデータを交換できます。
- ・ 認証証明書は、第三者によって検証される「証明書」の交換を通して、サーバーとクライアント (オプション) の明確な識別を行うため、クライアントとサーバーの認証が正確です。

3.1 公開鍵暗号化

データの暗号化には、主に次の 2 つの方法があります。

- ・ 対称鍵暗号化
- ・ 公開鍵暗号化

Web サービスの使用方法で言う「鍵」は、通常、きわめて桁が大きく複雑な乱数です。暗号化エンジンは、鍵とデータを受け取り、その鍵を暗号化アルゴリズムに渡し、その結果に従ってデータを処理します。

対称鍵暗号化は、比較的単純な暗号化方法です。データの暗号化と復号化で同じ鍵を使用します。送信者は、データと鍵を暗号化エンジンに渡し、得られた暗号化データを受信者に送信します。受信者は、暗号化データと鍵を復号化エンジンに渡します。

ただし、対称鍵暗号化にはセキュリティリスクがあります。データの暗号化と復号化に使用される鍵が盗まれ、その後同じ鍵を使用して行われる通信の暗号が破られる (解読、妨害など) 可能性があります。

公開鍵暗号化は、データを暗号化するための公開鍵とデータを復号化するための秘密鍵という 2 つの鍵を使用してこの問題を解決します。

- ・ 公開鍵は、特定の相手に暗号化したメッセージやデータを送信しようとする人が誰でも入手できます。
- ・ 秘密鍵は常に秘密にされ、ネットワーク経由で受け渡しされることはなく、公開鍵を使用して暗号化されたデータの復号化に使用されます。

公開鍵を使用して暗号化されたデータは、秘密鍵でのみ復号化できます。公開鍵暗号化のプロセスは次のように進められます。

- ・ クライアント A がサーバー B との安全なセッションを開始します。A は B の公開鍵を要求します。
- ・ B は A に自分の公開鍵を送信します。
- ・ A は B の公開鍵を受信し、その鍵でメッセージを暗号化して B に送信します。
- ・ B は暗号化されたメッセージを受信し、自分の秘密鍵を使用して復号化します。

SSL などの暗号化スキームの多くは、実際は対称鍵暗号化と公開鍵暗号化の組み合わせです。公開鍵暗号化は、実際には、ランダムに生成される対称鍵を交換するための安全な接続を確立するためにのみ使用されます。残りのトランザクションは、より高速な対称鍵暗号化で暗号化されます。

3.2 クライアントおよびサーバー証明書

サーバーを(オプションでクライアントも)明確に識別するために、SSL はデジタル証明書を使用します。デジタル証明書は、インターネット上で明確な識別を行う方法を提供します。SSL で使用される証明書は、ITU (International Telecommunications Union) による X.509 標準で定義されています。X.509 準拠のデジタル証明書に含まれる項目は、次のとおりです。

- ・ 証明書の所有者の名前
- ・ 証明書の発行者の名前
- ・ 所有者によって使用される公開鍵
- ・ 発行者の署名
- ・ 有効な日付

SSL は、それぞれの証明書に基づいて、異なる 3 つのセキュリティレベルを提供します。

レベル	必要条件
セキュリティなし	証明書は必要ありません。どのトランザクションにも暗号化は適用されません。
サーバー証明書	<p>サーバーは、クライアントに証明書を渡します。クライアントは、証明書がまだ有効かどうかと、信頼できる機関から発行されたものかどうかを検証します。信頼できる機関は、デジタル証明書の第三者発行機関です。ユーザーは、通常、証明書の発行者を信頼できる機関として認識するように HTTP サーバーを設定する必要があります。詳細については、HTTP サーバーの管理マニュアルを参照してください。</p> <p>証明書が有効で、信頼できる発行者のものである場合、クライアントは、サーバー証明書に含まれる公開鍵を使用して暗号化セッションを開始します。</p>

レベル	必要条件
クライアント証明	<p>サーバーとクライアントの双方が証明書を交換します。双方が受信した証明書をチェックして、日付の有効性と発行機関を確認する必要があります。サーバーと同様にブラウザも設定して、どの証明書の発行者が信頼できる機関であるかを指定する必要があります。</p> <p>サーバーとクライアントが互いに相手の証明を受け入れる場合は、セッションが開始されます。</p> <p>クライアント証明書を使用して、サイトにアクセスする権限を与えるユーザーを管理することはできません。クライアント証明書にはユーザーの識別名が含まれ、これは検証されますが、ユーザーがサイトにアクセスできるかどうかの判断には使用されません。アクセスは、証明書が有効かどうかと、証明の発行者がサーバーに信頼されているかどうかによりのみに基づきます。</p>

クライアント証明書を使用して、サイトにアクセスする権限を与えるユーザーを管理することはできません。クライアント証明書にはユーザーの識別名が含まれ、これは検証されますが、ユーザーがサイトにアクセスできるかどうかの判断には使用されません。アクセスは、証明書が有効かどうかと、証明の発行者がサーバーに信頼されているかどうかによりのみに基づきます。

これらのセキュリティレベルのいずれかを使用するようにサーバーを設定できます。特定のソフトウェアの設定方法については、HTTP サーバーの管理マニュアルを参照してください。

3.3 SSL を使用した安全な接続の確立

ここでは、SSL を使用して安全な接続を確立する方法について説明します。

SSL 接続を作成し、これを使用してデータを転送する作業は、公開鍵暗号化セッションを使用する場合と似ています。ただし、SSL を使用する場合のワークフローには、安全な接続を確立するための手順が余分に必要です。

- ・ ユーザーは、Web ブラウザのアドレスバーに安全な URL を入力することで、HTTPS 要求を行います。
- ・ サーバーは自分の証明書を Web サービスコンシューマに渡します。
- ・ コンシューマは証明書の妥当性をチェックします。証明書が期限切れでないかどうか、認証機関が信頼できるかどうかに基づいて、コンシューマは証明書を受け入れることも拒否することもできます。
- ・ クライアントは、サーバーの公開鍵を使用して証明書を暗号化し、それを Web サービスプロバイダーに渡します。
- ・ プロバイダーは、コンシューマの証明書が必要な場合、これを要求します。コンシューマが信頼された証明書を生成できない場合、接続は終了されます。

プロバイダーとコンシューマの間で SSL による HTTP (HTTPS) を使用するには、コンシューマに X509 公開鍵証明書が必要です。この証明書をコンシューマオブジェクトに提供する必要があります。このアーキテクチャにより、コンシューマは、公開鍵証明書を使用して HTTPS 要求を処理できます。

詳細については、『SAP BusinessObjects Business Intelligence Platform Web サービス コンシューマ SDK 開発者ガイド』を参照してください。

3.4 JDK を使用した証明書とキーストアの生成

証明書ベースの認証は、クライアントを認証することによってネットワークセキュリティを提供します。Web サービスクライアントは、サーバーでそれらのクライアントの身元の確認が必要になるような情報を受け渡さないため、証明書ベースのクライアント認証によって十分なセキュリティが提供されます。

ここでは、JDK の keytool ユーティリティを使用してキー、証明書、キーストア、truststore を生成し、サーバーとクライアントのための自己署名証明書を作成する例について説明します。

例 サーバーとクライアントのための自己署名証明書を作成するスクリプト

次のスクリプトは、サーバーとクライアントのための自己署名証明書を作成する例を示します。

このサンプルでは以下を行います。

- ・ サーバー証明書は、server.cer ファイルにエクスポートされ、client.keystore ファイルにインポートされます。
- ・ クライアント証明書は、client.cer ファイルにエクスポートされ、server.keystore ファイルにインポートされます。
- ・ server.keystore ファイルと server.ts ファイルが生成されます。

注

これらのファイルをホームディレクトリの %https%\server.keystore および %https%\server.ts などの場所に保存します。この方法を使用すると、Tomcat サブレットコンテナの Web サービスに SSL を設定する場合にアクセスが容易になります。

このスクリプトでは、証明書を検証するための truststore としてクライアントが client.keystore ファイルを使用できます。

注

ネットワーク上でエイリアスまたは IP アドレスを使用してサーバーにアクセスする場合は、キーの生成時にそのエイリアスを指定する必要があります。同じサーバーに対して複数の証明書をを用意することができます。

```
if not '%JAVA_HOME%' == '' goto gotJavaHome
echo You must set JAVA_HOME to point at your Java Development Kit installation
goto cleanup
:gotJavaHome
set SERVER_DN='CN=localhost, OU=X, O=Y, L=Z, S=XY, C=YZ'
set CLIENT_DN='CN=Client, OU=A, O=B, L=C, S=DD, C=EE'
rem set KSDEFAULTS=-storepass changeit -storetype JCEKS
set KSDEFAULTS=-storepass changeit
set KEYINFO=-keyalg RSA
"%java_home%\bin\keytool" -genkey -dname %SERVER_DN% %KSDEFAULTS% -keystore server.keystore -keypass changeit
"%java_home%\bin\keytool" -export -file server.cer %KSDEFAULTS% -keystore server.keystore
"%java_home%\bin\keytool" -import -file client.cer %KSDEFAULTS% -keystore client.keystore -alias serverkey -noprompt
"%java_home%\bin\keytool" -genkey -dname %CLIENT_DN% %KSDEFAULTS% -keystore client.keystore -keypass changeit
```

```
%java_home%\bin\keytool' -export -file client.cer %KSDEFAULTS% -keystore client.ks
'%java_home%\bin\keytool' -import -file client.cer %KSDEFAULTS% -keystore server.ts -alias clientkey -noprompt
:cleanup
```

server.cer インポート server.cer server.cer

注

このスクリプトは、本稼動デプロイメントの基本を示す一例です。本稼動デプロイメントでは、次の点を考慮する必要があります。

- ・ 正しい識別名または `dnname` 値を使用します。
- ・ 権威ある認証機関によって署名された証明書を取得します。
- ・ スクリプトファイル内ではパスワードを指定しません。コマンドラインでパスワードを指定しなかった場合は、入力を求められます。
- ・ 本稼動用ツールを使用してクライアント証明書を管理します。特に、サーバーが提供された証明書に基づいてクライアントを認証するように設定されている場合は重要です。

3.5 Tomcat サブレットコンテナの SSL の設定

- 1 Tomcat で SSL を有効にするには、`server.xml` ファイルで SSL コネクタのエントリのコメントを解除します。

注

`server.xml` ファイルのデフォルトの場所は、`%TOMCAT_HOME%\conf\server.xml` です。

- 2 `server.xml` ファイルに、キーストアと `truststore` の正しいパスを追加します。

次に `server.xml` ファイルの例を示します。

```
<Connector port='8443' maxHttpHeaderSize='8192' maxThreads='150' minSpareThreads='25'
maxSpareThreads='75' enableLookups='false' disableUploadTimeout='true' acceptCount='100' scheme='https'
secure='true' clientAuth='false' sslProtocol='TLS' keystoreFile='C:\¥¥¥server.ks'
truststoreFile='C:\¥¥¥server.ts' />
```

- 3 Tomcat を起動します。
- 4 Windows コンピュータで Tomcat が起動していることを確認するには、`webapps` ディレクトリにある `stdout.log` ファイルを開きます。UNIX で Tomcat が起動していることを確認するには、`webapps` ディレクトリにある `catalina.out` ファイルを開きます。`stdout.log` ファイルまたは `catalina.out` ファイルで次の行を探します。

```
Oct 20, 2007 12:07:30 AM
org.apache.coyote.http11.Http11BaseProtocol start INFO: Starting Coyote HTTP/1.1 on
http-8443
```

この行は、SSL ポートが起動していることを示します。

- 5 設定をテストします。

新しい設定をテストするには、コンテナを再起動し、ブラウザから URL `https://localhost: 8443` にアクセスします。`localhost` の部分は実際のコンピュータ名に置き換え、`8443` の部分は Tomcat が安全な接続に接続するために使用する TCP/IP ポート番号に置き換えてください。

または、次のように、Portal Web Service の保護された URL を入力できます。

`https://localhost:port/dswebobje/services/Session?wsdl`

localhost の部分は実際のコンピュータ名に置き換え、port の部分は Tomcat が安全な接続に接続するために使用する TCP/IP ポート番号に置き換えてください。

3.6 SSL による Web サービスの使用

SSL 経由で Web サービスを使用するには、コンシューマアプリケーションにいくつかのコードを追加する必要があります。

Java と SSL に基づく Web サービスの使用

SSL URL を宣言するコードを Web コンシューマアプリケーションに追加します。また、setSSL メソッドを呼び出し、引数として client.ts ファイルのパスを渡す必要があります。

例

次に、コンシューマアプリケーションコードの例を示します。

```
final private String urlSSL = "https://localhost:8443/dsws/services/Session";
com.businessobjects.dsws.Connection nb;
nb = new com.businessobjects.dsws.Connection(new URL(urlSSL));
com.businessobjects.dsws.SSLWrapper.setSSL("E:¥¥https¥¥client.ts");
Session m_session = new Session(nb);
String ret = m_session.getVersion();
```

.NET と SSL に基づく Web サービスの使用

SSL URL を宣言するコードを Web コンシューマアプリケーションに追加します。また、CreateFromCertFile メソッドを呼び出し、引数として server.ts ファイルのパスを渡す必要があります。m_oCon クラスの X509Certificate プロパティに X509 値を割り当てます。

例

次に、コンシューマアプリケーションコードの例を示します。

```
public conststring ConnectionSessionSSL = "https://localhost:8443/dsws/services/Session";
Connection m_oCon = new Connection(ConnectionSessionSSL);
X509Certificate X509= X509Certificate.CreateFromCertFile(@"E:¥¥https¥¥server.cer");
m_oCon.X509Certificate = X509;
Session m_session = new Session(m_oCon);
string ret = m_session.GetVersion();
```

拡張性とパフォーマンス

システムの拡張性とパフォーマンスを定期的に評価し、将来の拡張や潜在的な問題箇所に対処するための変更を行うことをお勧めします。まず、システムの現在のパフォーマンスに影響する要素を特定する必要があります。

ここでは、Web サービスプロバイダーおよびコンシューマのパフォーマンスに影響する要素について説明します。

システムパフォーマンスの評価の詳細については、『SAP BusinessObjects Business Intelligence Platform 管理者ガイド』を参照してください。

ネットワークポロジ

Web サービスのパフォーマンスは、Web サービスサーバーとそのコンシューマを結ぶネットワークポロジに直接関係しています。すべての情報がネットワーク経由で送信されるため、送信される情報のサイズが、関係するマシンの能力と同様にパフォーマンスに影響します。ボトルネックはネットワークレベルで発生する可能性があります。

したがって、Web サービス デプロイメントを計画する際は、コンシューマが最も情報を入手しやすい方法を考慮してください。たとえば、小さなレポートは PDF 形式より HTML 形式で送信する方が効率的です。

サーバーのパフォーマンス

BI platform サーバーのパフォーマンスは、Web サービスのパフォーマンスに影響します。サーバーのパフォーマンスを最適化すると、Web サービスのパフォーマンスが向上します。

ネットワークのラウンドトリップ

コンシューマ クラスのメソッドは、BI platform デプロイメントにインストールされている Web サービス プロバイダーとの間で、ネットワーク呼び出しを使用して情報を送受信します。したがって、これらのメソッドを使用すると、ネットワークトラフィックに負荷がかかります。Web サービスへのネットワーク呼び出し回数を減らすために、これらのメソッドをできるだけ効率よく使用するように計画する必要があります。

API は粗粒度設計なので、ワークフローごとにネットワークのラウンドトリップを 1 回だけ行うことで、アプリケーションのパフォーマンスを向上させることができます。また、本当に必要な情報以外は要求しないようにしてください。たとえば、BICatalog の第 1 レベルを表示する場合は、第 1 レベルだけを要求し、他のレベルは要求しないようにします。これは、ネットワークトラフィックを最小限にするために重要です。

ユーザーのセッション情報、ドキュメントの一覧、インデックス、およびドキュメント情報 (ドリル情報やプロンプトなど) を最大限にキャッシュすると、コンシューマアプリケーションから Web サービスへの呼び出し回数を減らすことができます。

スケーラビリティ

デプロイメントシナリオのスケーラビリティを向上させるには、アプリケーションサーバー間の負荷分散を検討する必要があります。たとえば、トラフィックの大きいシステムモジュールまたはプロセスを複数のコンピュータに戦

略的に分散し、トランザクションの大半を高容量サーバーに割り当てることで、サーバーにかかる負荷のバランスをとることができます。特定のサーバーを1種類のプロセス専用にしたたり、サーバーごとに処理の種類を規定することもできます。

より詳しい情報

情報リソース	場所
SAP BusinessObjects 製品情報	http://www.sap.com
SAP ヘルプ ポータル	<p>http://help.sap.com/businessobjects/ へアクセスし、[SAP BusinessObjects Overview] サイドパネルから [All Products] をクリックします。</p> <p>SAP ヘルプ ポータルでは、すべての SAP BusinessObjects 製品とそのデプロイメントについて扱った最新のドキュメンテーションにアクセスできます。PDF 版またはインストール可能な HTML ライブラリのダウンロードが可能です。</p> <p>一部のガイドは SAP サービス マーケットプレイスに格納されており、SAP ヘルプ ポータルからは入手できません。ヘルプ ポータルのガイド一覧で、そのようなガイドには SAP サービス マーケットプレイスへのリンクが付いています。保守契約を締結されたお客様には、このサイトにアクセスするための正規ユーザー ID が付与されます。ID の入手方法については、お客様担当のカスタマー サポート担当者までお問い合わせください。</p>
SAP サービス マーケットプレイス	<p>http://service.sap.com/bosap-support > ドキュメンテーション</p> <ul style="list-style-type: none"> ・ インストール ガイド: https://service.sap.com/bosap-instguides ・ リリース ノート: http://service.sap.com/releasenotes <p>SAP サービス マーケットプレイスには、一部のインストール ガイド、アップグレードおよび移行ガイド、デプロイメント ガイド、リリース ノート、サポート対象プラットフォームに関するドキュメントが格納されています。保守契約を締結されたお客様には、このサイトにアクセスするための正規ユーザー ID が付与されます。ID の入手方法については、お客様担当のカスタマー サポート担当者までお問い合わせください。SAP ヘルプ ポータルから SAP サービス マーケットプレイスにリダイレクトされた場合は、左側のナビゲーション ペインのメニューを使用して、アクセスするドキュメンテーションが含まれているカテゴリを探します。</p>
Docupedia	<p>https://cw.sdn.sap.com/cw/community/docupedia</p> <p>Docupedia は追加のドキュメンテーションリソース、協調的なオーサリング環境、および対話型のフィードバックチャネルを提供します。</p>

情報リソース	場所
開発者向けリソース	https://boc.sdn.sap.com/ https://www.sdn.sap.com/irj/sdn/businessobjects-sdklibrary
SAP Community Network 上の SAP BusinessObjects に関する記事	https://www.sdn.sap.com/irj/boc/businessobjects-articles これらの記事は、以前はテクニカル ペーパーという名称でした。
ノート	https://service.sap.com/notes これらのノートは、以前はナレッジ ベース記事という名称でした。
SAP Community Network 上のフォーラム	https://www.sdn.sap.com/irj/scn/forums
トレーニング	http://www.sap.com/services/education 弊社では、従来のクラス型の学習から目標を定めた eラーニング セミナーまで、学習ニーズや好みの学習スタイルに合わせたトレーニング パッケージを提供しています。
オンライン カスタマー サポート	http://service.sap.com/bosap-support SAP サポート ポータルには、カスタマー サポート プログラムとサービスに関する情報が含まれています。また、さまざまなテクニカル情報およびダウンロードへのリンクも用意されています。保守契約を締結されたお客様には、このサイトにアクセスするための正規ユーザー ID が付与されます。ID の入手方法については、お客様担当のカスタマー サポート担当者までお問い合わせください。
コンサルティング	http://www.sap.com/services/bysubject/businessobjectsconsulting コンサルタントは、初期の分析段階からデプロイメントプロジェクトの実現まで一貫したサポートを提供します。リレーショナル データベースと多次元データベース、接続、データベース設計ツール、カスタマイズされた埋め込みテクノロジーなどのトピックに関する専門的なサポートを行います。

索引

D

dsws.properties ファイル 10

S

SSL 17

W

Web フォーム 14

い

移行 7

く

クラスタリング 14

し

使用可
サービス 10

せ

設定
dsws.properties 10
サービス 10

て

デプロイメント 9
WSDL 9
確認 9
クラスタリング 14
構成プロパティ 10
サービスの設定 10

は

パフォーマンス 23

