Oracleホワイト・ペーパー
2009年6月

Oracle Web Services Manager 11gを使用したWebサービスとサービス指向アーキテクチャの保護

ORACLE

はじめに

世界中の企業が、イントラネット環境とエクストラネット環境の両方で、Webサービスを使用したサービス指向アーキテクチャ（SOA）インフラストラクチャの配置を積極的に進めています。従来の選択肢（分散オブジェクトやカスタム・ソフトウェアなど）と比べてWebサービスには多くの利点があるとは言え、相互接続されたWebサービスのネットワークを配置するには、特にセキュリティや管理の観点で重要な課題が残されています。

標準に準拠したソリューションであるOracle Web Services Manager（Oracle WSM）はOracle SOA SuiteとOracle WebLogic Serverの一部として提供され、Webサービスに基づくSOAのセキュリティと管理の課題に対処します。

Oracle WSMを利用すると、企業は（1）SOAインフラストラクチャを構成する複数のWebサービスに適用される宣言的ポリシーを一元的に定義および保管し、（2）設定可能なエージェントを介してセキュリティと管理のポリシーをローカルで適用し、（3）認証や認可の失敗といった実行時のセキュリティ・イベントを監視できます。

Oracle WSMは、実行中のビジネス・プロセスを中断することなくポリシー変更をリアルタイムで適用することで、セキュリティの脅威やセキュリティ侵害に対する企業の俊敏な対応を可能にします。

Oracle WSMは、Webサービスのセキュリティと管理を行うクラス最高のシステムであり、設計時には開発者によって、また本番環境ではシステム管理者やセキュリティ管理者によって使用されます。

「Oracle Web Services Managerには、ID管理ソフトウェアと統合し、基盤となるサービス・プラットフォームにIDを伝播するための高度な機能が備わっています」

Forrester Research, Inc、**Randy Heffner**

WebサービスとSOAインフラストラクチャ

SOAインフラストラクチャの目的は、プロバイダが公開したサービスをコンシューマから起動できるようにすることです。

B2B環境でのコンシューマの例としては、ABC社の発注処理サービスをリモートから起動するXYZ社のローカル調達アプリケーションがあります。また、イントラネット環境ではコンシューマとプロバイダが同じ企業に含まれているため、異種アプリケーションが統合され、より異種性の低い企業フレームワークが形成されます。

Webサービスはプログラムであり、任意の言語を使用して記述されます。このプログラムが実行できること（実装されている機能）は、Web Services Description Language（WSDL）と呼ばれる標準XMLボキャブラリに記述されます。ある銀行取引Webサービスには、口座のチェック、取引明細書の印刷、入金と引出しの機能が実装されているとします。これらの機能はWSDLファイルに記述されており、あらゆるコンシューマがこれを起動して銀行取引Webサービスにアクセスできます。このため、コンシューマはWebサービスの場所と機能を記述したWSDLファイル以外に、Webサービスについて知る必要はありません。

図1に示すとおり、Webサービス・コンシューマ（デスクトップ・アプリケーションやポートレットを含むJava Platform, Enterprise Edition（Java EE）クライアントなど）は、Webサービス・プロバイダに対して、XMLドキュメントの形でリクエストを送信することで、Webサービスを起動します。Webサービス・プロバイダはリクエストを処理し、その結果をXMLドキュメントとしてWebサービス・コンシューマに返します。

図1に示した例では、Webサービス・コンシューマはSOAPメッセージとしてリクエストを送信しています（SOAPについては業界標準に対するサポートの項で後述します）。Webサービス・プロバイダ（www.xmethods.com）はリクエストを処理し、レスポンス（ここではオラクルの株価）をWebサービス・コンシューマに返します。

WebサービスはXMLドキュメントと（おもに）普及しているHyper Text Transport Protocol（HTTP）を使用してトランザクションを実行します。これはつまり、従来のネットワーク・ファイアウォールだけではWebサービスへのアクセスを十分に保護できないことを意味します。

図1に示した例では、Webサービス・プロバイダによってサービスにアクセスするための資格証明（ユーザー名とパスワードなど）が要求された可能性があります。また、Webサービス・プロバイダによってレスポンス（株価）が暗号化されたということも考えられます。

つまり、Webサービスは疎結合された分散環境であり、企業はこれを利用することで、企業内の異種アプリケーションを統合したり、インターネットを介して顧客やパートナーにビジネス機能を公開したりすることができます。

Webサービスを特徴付けるのは、次の3つの要素です。

- 何をするか（公開するビジネス機能）
- どこにあるか（機能を公開しているWebサイト）
- どのようにしてアクセスできるか（公開された機能を使用するために必要な公開インタフェースのセット）

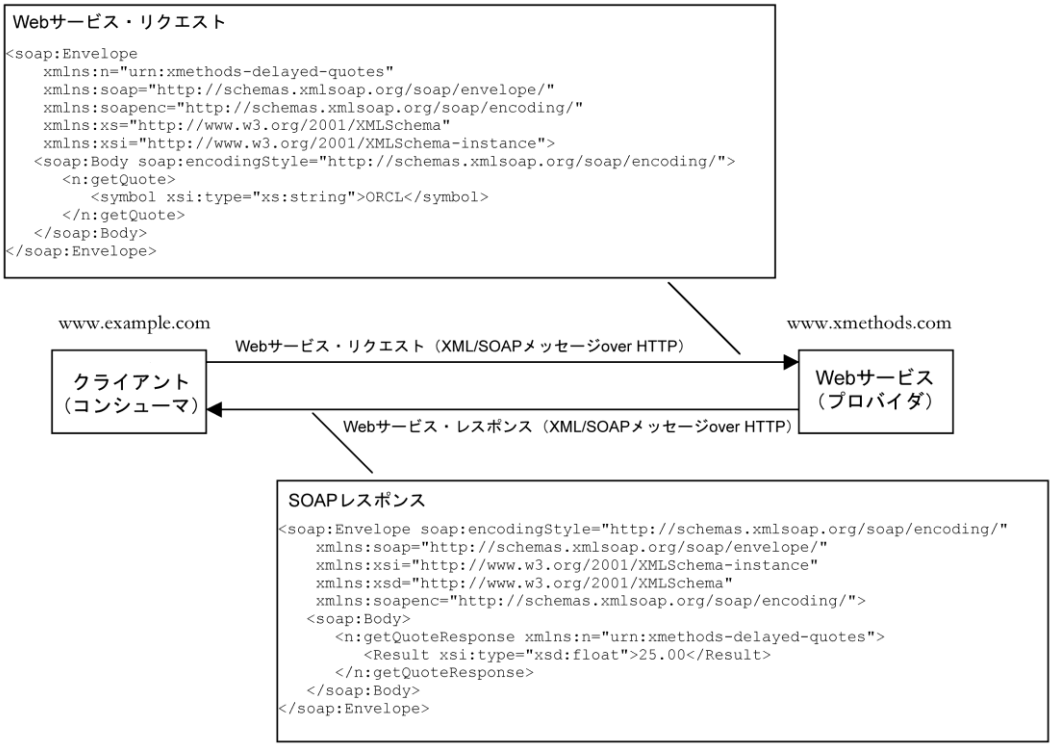

図1：Webサービスのリクエストとレスポンス

WebサービスはXMLに基づく次の業界標準に依存しています。

- Webサービス・コンシューマとWebサービス・プロバイダ間で統一された通信を実現するデータ形式（Extensible Markup Language（XML）仕様）
- ビジネス・トランザクションで使用されるXMLボキャブラリを記述したフレームワーク（XMLスキーマ）
- Webサービス・プロバイダとの間の構造化リクエストの送信と構造化レスポンスの受信に使用されるエンベロープ（SOAP）
- Webサービスの機能を定義する言語（WSDL）
- インターネット上にWebサービスを公開し、検索するためのフレームワーク（Universal Description, Discovery, and Integration（UDDI））

Webサービスのセキュリティ

その性質（疎結合された接続）とオープン・アクセス（おもにHTTP）を使用する点から、Webサービスによって実装されたSOAインフラストラクチャはセキュリティ分野に新しい要件を加えます。

Webサービスのセキュリティには次のようにさまざまな側面があります。

- *認証：*実際のユーザーとユーザーIDが一致することを検証します。ユーザーのIDは、ユーザー名とパスワード、デジタル証明、標準のSecurity Assertion Markup Language（SAML）トークン、Kerberosトークンなどの、ユーザーが提示した資格証明に基づいて検証されます（詳しくは後述）。Webサービスの場合、資格証明はエンドユーザーの代わりにクライアント・アプリケーションによって提示されます。
- *認可（またはアクセス制御）：*認証されたユーザーのエンタイトルメントや特定のロール（企業の発注者など）に基づいて、特定のリソースに対するアクセス権が付与されます。
- *機密保護とプライバシ：*情報の機密性を維持します。Webサービスのリクエスト・メッセージやレスポンス・メッセージには個人情報（PII）や機密のビジネス・データが含まれる場合があります。このようなデータの機密性は、XML Encryption標準を使用してリクエスト・メッセージやレスポンス・メッセージのコンテンツを暗号化することで維持されます。
- *整合性、否認防止：*認証局によるデジタル署名を使用することで、メッセージが転送中に改ざんされていないことを確認します。また、デジタル署名によって送信者が検証されるとともに、タイムスタンプを提供することで、送信者と受信者のいずれも、後からそのトランザクションを否認できないようにします。XMLメッセージはXML Signature標準を使用して署名されます。

また、Webサービスのセキュリティ要件には資格証明の仲介（信頼できる環境でのセキュリティ・トークンの交換）や、サービスの機能と制約（Webサービスがどのような条件下で何をできるかを定義）が含まれます。

多くの場合、Oracle WSMなどのWebサービス・セキュリティ・ソリューションは、公開鍵インフラストラクチャ（PKI）環境に依存しています。PKIは暗号化鍵（データの暗号化または復号化に使用する数学関数）を使用しており、この鍵には公開鍵と秘密鍵の2種類の鍵があります。非対称な暗号化モデルでは、受信者の公開鍵を使用して平文が暗号化され、対応する受信者の秘密鍵を使用して暗号文が復号化されます。また、秘密鍵を使用してデジタル署名が暗号化され、公開鍵を使用してデジタル署名が検証されます。さらに公開鍵の整合性を保証するため、公開鍵証明書（または略して証明書）が使用されます。

Webサービスのセキュリティ要件は、トランスポート・レベル（Secure Sockets Layer）とアプリケーション・レベルの両方で、XMLフレームワークを利用した業界標準によって支えられています。

トランスポート・レベルのセキュリティ

Secure Socket Layer（SSL）またはTransport Layer Security（TLS、Internet Engineering Task Force（IETF）が公式に標準化したSSLのバージョン）として知られるこの規格は、もっとも広く利用されているトランスポート・レベルのデータ通信プロトコルであり、次の機能を提供します。

- 認証（信頼できる2つのパーティ間で通信を確立する）
- 機密保護（交換データを暗号化する）
- メッセージの整合性（データに破損がないことをチェックする）
- クライアントとサーバー間でのセキュアな鍵交換

SSLはセキュアな通信チャネルを提供しますが、"転送中"でないデータは保護されません。このため、マルチステップ・トランザクションにおける攻撃に対して脆弱な環境になります（SSLはエンド・ツー・エンドのセキュリティではなく、Point-to-Pointのセキュリティを提供します）。

アプリケーション・レベルのセキュリティ

アプリケーション・レベルのセキュリティは、トランスポート・レベルのセキュリティを補完する役割を果たします。アプリケーション・レベルのセキュリティを支えているのは、機密性、整合性、認証性、メッセージ構造、トラスト管理、ID伝播を規定するXMLフレームワークです。Oracle WSMでサポートされている仕様について詳しくは、本書後半の業界標準に対するサポートの項を参照してください。

Webサービスのセキュリティ要件

必要とされているのは、（1）トランスポート・セキュリティを使用してWebサービス・コンシューマとWebサービス・プロバイダ間の通信チャネルを保護し、（2）メッセージ・レベルのセキュリティを使用し、仲介サービスを介してエンド・ツー・エンドでトランザクションを保護することです（たとえば、1つのビジネス・トランザクションを完了するために複数のWebサービスが使用されている場合、トランザクションに含まれるすべてのWebサービス間でセキュリティ情報とID情報がシームレスに受け渡される必要があります）。

Oracle WSMは、異種環境におけるWebサービス・セキュリティを規定し、実装するよう設計されています。これには、1つのトランザクションを完了するために使用される複数のWebサービス間での認証、認可、メッセージの暗号化と復号化、署名の生成と検証、ID伝播が含まれます。

Oracle WSMを使用すると、ユーザーはWebサービス・コンシューマの実行時アクティビティを監視できます。たとえば、異常なレベルで失敗している認証があれば、ユーザーは視覚的なグラフを見るだけでこれを発見できます。

Oracle WSM 11g Release 1の機能

Oracle WSMの目的はセキュリティと信頼性に関するポリシーを定義および適用するとともに、実行時イベントの監査機能を提供することにあります。次に、Oracle WSMを使用して実行できるタスクの例を簡単に示します。

- 1つの管理コンソール（Oracle Enterprise Manager）からポリシーを管理します。
- 設計時にはOracle JDeveloperを、実行時にはOracle Enterprise Manager（Oracle EM）を使用して、クライアントとサービス・エンド・ポイントにポリシーを関連付けます。
- WSDLやWS-MetadataExchangeドキュメントを使用してセキュリティ要件を公開します(本書後半にあるセキュリティ標準に対するサポートの項を参照）。
- ポリシーを実際に変更する前に、変更による影響分析を実行します。
- LDAPディレクトリまたはIDインフラストラクチャ（Oracle Access Managerなど）に対して、認証や認可のポリシーを定義します。
- 標準セキュリティ・トークンを生成し、1つのトランザクションで使用されている複数のWebサービスに対してIDを伝播します。
- Webサービス・リクエストのペイロード要素（例：クレジットカード番号）を暗号化します。
- 視覚的なグラフを使用して、アクセス制御イベントを表示します。
- リクエスト・メッセージとレスポンス・メッセージを記録します。

基本的な概念

Oracle WSMを利用すると、Webサービスのセキュリティと管理を、構築したアプリケーションから外部化することができます。セキュリティ・ロジックをアプリケーションにコーディングする代わりに、Oracle WSMの事前定義ポリシーを使用して、宣言型のセキュリティと管理を実装できます。

Oracle WSMのベースとなるのは、定義、適用、監視という3つの主要な処理です。

- *定義*とは、保護対象のWebサービスにセキュリティと管理のポリシーを関連付けることです。ポリシーの例としては、ユーザー名とパスワードを使用したリクエスト・メッセージの認証や、WS-Securityを使用したメッセージの復号化、レスポンス・メッセージの署名などがあります。
- *適用*とは、中央のPolicy Managerから複数のポリシー適用ポイント（PEP）またはエージェントにポリシーを分散する機能であり、Oracle WSMによって提供されています。実行時には、これらのセキュリティと管理に関するポリシーがローカルで実行されます。

- *監視*とは、Oracle WSM適用ポイントで取得されたセキュリティと管理の実行時イベントを（視覚的なグラフを使用して）追跡することです（Oracle WSMエージェントからOracle Enterprise Managerに情報が送信され、アクションを実行できるダッシュボードやグラフにこの情報が表示されます）。

パイプライン・メタファ

Oracle WSMは、パイプライン・メタファを使用します（図2を参照）。リクエスト・メッセージとレスポンス・メッセージに対して、さまざまなカテゴリのポリシーが事前に定義された順序で実行されます。また、この順序は、ポリシーがクライアント側で実行されているか、サーバー側で実行されているかによっても異なります。図2に、サーバー側でのポリシー実行に使用される順序を示します。クライアント側では、逆の順序でポリシーが実行されます。

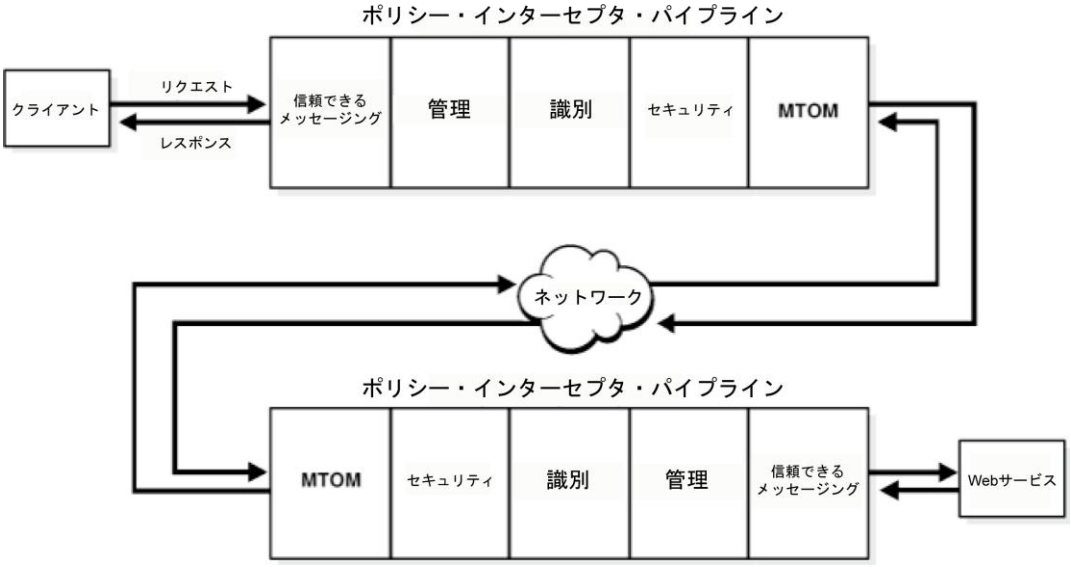

図2：Oracle WSMのポリシー・インターセプタ・パイプライン

通常は、Webサービス・クライアントからWebサービス・プロバイダに対してリクエストが送信されます。Oracle WSMエージェントはリクエストをインターセプトして、リクエスト・パイプライン・ポリシーを実行します。この処理が成功すると、エージェントはリクエストをWebサービスに転送します。Webサービスはリクエストを処理し、Webサービス・クライアントにレスポンスを送信します。エージェントはレスポンスをインターセプトして、レスポンス・パイプライン・ポリシーを実行します。成功すると、エージェントはレスポンスをアプリケーション・サーバーに転送し、そこからさらにWebサービス・クライアントに転送されます。

ポリシー・アサーション

Oracle WSMポリシーは1つまたは複数のポリシー・アサーションで構成されています。たとえば、セキュリティ・ポリシーは（1）ログ・アサーションと（2）WS-Securityアサーションという2つのアサーションで構成されています。

ポリシー・アサーションは、ポリシー内に記述されている順序で実行されます。セキュリティ・ポリシーの場合、ログ・アサーションが最初に実行され（ログ・ファイルへのリクエスト・メッセージのロギング）、次にWS-Securityアサーションが実行されます（送信されたメッセージ内のトークンを使用して要求元を認証し、リクエストが暗号化されている場合はメッセージを復号化）。

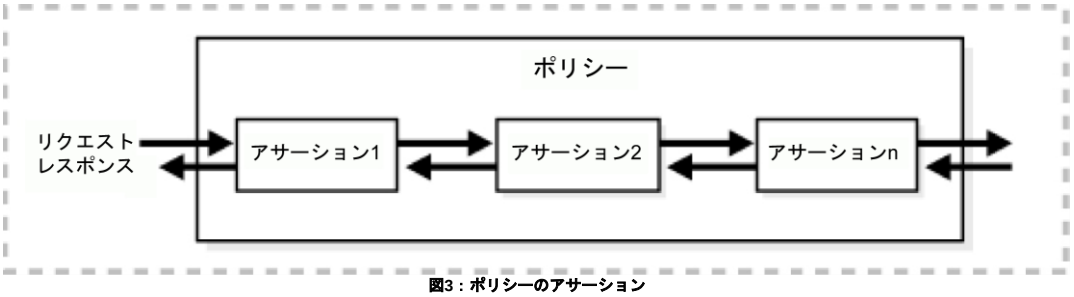

図3：ポリシーのアサーション

ポリシー・アサーション・テンプレート

Oracle WSMのポリシー・アサーションは、ポリシー作成時にポリシーに追加されるポリシー・アサーション・テンプレートのインスタンスです。Oracle WSMには事前定義された一連のポリシー・アサーション・テンプレートが同梱されています。Oracle Enterprise Managerの組込み機能を使用するか、またはカスタム実装を追加すると、組織固有のポリシー要件を満たすために追加のテンプレートを作成できます。

カスタム・ポリシー・アサーション

Oracle WSMでは、カスタム・ポリシー・アサーションを定義し、事前定義されたポリシー・アサーションと一緒にポリシーに含めて実行できます。カスタム・ポリシー・アサーションは、標準外のセキュリティ・トークンのサポートなど、特定の機能が標準で提供されていない場合に使用されます。前述のとおり、ポリシー・アサーションはポリシー・アサーション・テンプレートのインスタンスです。カスタム・ポリシー・アサーションをポリシーに追加するには、Oracle WSMにカスタム・ポリシー・アサーション・テンプレートを追加する必要があります。

カスタム・ポリシー・アサーション・テンプレートは次の2つの部分で構成されています。

- コンパイルされたカスタム・コードと依存ライブラリを含むJavaアーカイブ（JAR）ファイル
- カスタム・ポリシー・アサーション・テンプレートと設定可能なパラメータを表すXMLファイル

Oracle WSMのマニュアル・ドキュメントには、アプリケーション・プログラミング・インタフェース（API）やカスタム・ポリシー・アサーション・テンプレートの開発例が含まれています。

カスタム・ポリシー・アサーション・テンプレートはいったん配置されると、標準のポリシー・アサーション・テンプレートと同じようにOracle WSM環境で使用できるようになります。

リクエストの認証

Oracle WSMのセキュリティ・ポリシーはサービスに適用されているポリシーに基づいて、リクエスト・メッセージからセキュリティ・トークンを抽出します。このセキュリティ・トークンには、ユーザー名/パスワード（問合せ対象のXMLドキュメントをナビゲートするための標準であるXPathを使用して、HTTPヘッダーやWS-Securityヘッダーまたはメッセージ・ボディから抽出）や、リクエストの署名に使用されたX.509証明書、Kerberosチケット、SAMLトークン、Oracle Access ManagerのCookieトークン（専用のSOAPヘッダーから抽出）などがあります。

抽出したセキュリティ・トークンは、Oracle WSMによってOracle Platform Security Services（OPSS）ログイン・モジュールに送信されて検証され、次にトークン内に格納されていた資格証明情報がWebLogic ServerのAuthenticatorに渡されます（OPSSはOracle Fusion Middlewareのセキュリティ・レイヤーであり、Oracle WSMはOPSSのサービスを使用して認証と認可を実行します。OPSSについて詳しくはOracle Platform Security Servicesのテクニカル・ホワイト・ペーパーを参照してください）。

WebLogic ServerのAuthenticatorは、LDAP（Oracle Internet DirectoryやMicrosoft Active Directoryなど）やOracle Access Manager、Oracle Database、CA SiteMinderなどの各種IDストアに対して、資格証明を検証するよう設定できます。処理に成功すると、WebLogic Server AuthenticatorはJavaサブジェクトを作成し、これに対してユーザー名と認証ユーザーに割り当てられたロールを含むプリンシパルを付加します。これにより、サブジェクトは後続のポリシー・アサーションとWebサービス自体から使用できるようになります。

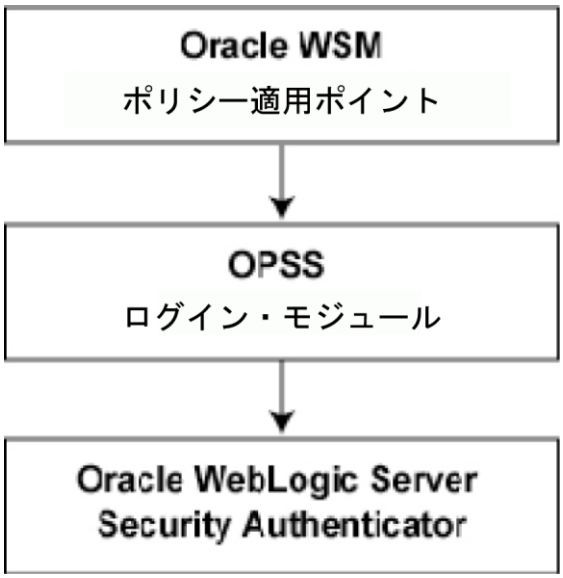

図4：リクエストの認証

リクエストの認可

Oracle WSMでは、ロールベースと権限ベースの2種類の認可ポリシーが提供されています。認可ポリシーを適用するには、先に認証ポリシーを適用して、認可に使用するユーザー・ロールを含むJavaサブジェクトを設定しておく必要があります。

- ロールベースの認可ポリシーは、ユーザーがポリシー内に設定されたロールに属しているかどうかをチェックします。
- 権限ベースの認可ポリシーは、サービスの起動に必要なJava権限が*サブジェクト*に含まれているかどうかを確認します。このポリシーはOracle Platform Security Servicesを利用して、認証された*サブジェクト*に**`oracle.wsm.security.WSFunctionPermission`**権限が付与されているかどうかをチェックします。**`WSFunctionPermission`**は、ユーザーやグループ、またはアプリケーション・ロールに対して付与できます。ユーザーまたはグループに付与されたWSFunctionPermissionは、同じWebLogic Serverドメイン内に配置されたすべてのWebサービスに適用されます。

ポリシー管理

次の項からは、一元化されたOracle WSM Policy Managerを使用してポリシーの関連付け、適用、管理を行い、Oracle Enterprise Managerを使用して監視と監査を実行する方法について説明します。

ポリシーの関連付け

Oracle WSMでは、クライアントとサービスに対してポリシーを関連付けるためのソリューションとして、Oracle JDeveloperとOracle EMを提供しています。

アプリケーション開発者は、設計時にOracle JDeveloper内でOracle WSMポリシーの関連付けを実行できます。この際、ポリシー参照（ポリシー名）のみがWebサービスに関連付けられます。Webサービスがアプリケーション・サーバーに配置されると、Oracle WSMエージェントはポリシー名を検索キーとして提供して、Oracle WSM Policy Managerからポリシー定義の詳細を参照します。

また、管理者はOracle EMを使用して、クライアントやサービスにOracle WSMポリシーを関連付けたり、すでに関連付けられたポリシーを変更したりすることができます。

ポリシーの適用

Oracle WSMエージェントはアプリケーション（クライアントまたはサービス）に対するリクエストやレスポンスをインターセプトし、リクエストやレスポンスに関連付けられたポリシーを適用します。エージェントはOracle WSM Policy Managerからポリシー定義を検索し、ポリシーをキャッシングすることでパフォーマンスを向上し、Policy Managerが使用できなくなるようなシステム停止を回避します。

Oracle WSMでは動的なポリシー更新がサポートされています。より高度なセキュリティ上の脅威に対応するため、管理者がポリシーを変更した場合、Policy Managerによってこの変更がエージェントに伝播されます。エージェントはポリシー・キャッシュを更新し、変更されたポリシーを次に受け取ったリクエストに対して即座に適用します。

ポリシー・ガバナンス

Oracle WSMは一元化されたPolicy Managerアプリケーションを通じてポリシーのガバナンス機能を提供します。このアプリケーションによって、WebLogic Serverドメインに含まれるすべてのOracle WSMエージェントにポリシーおよびポリシーの変更が配信されます。Policy Managerはメタデータ・ストア（MDS）を利用して、ポリシーの影響分析に使用されるポリシー添付データやポリシーを読み取り、保存します。

ポリシー・ガバナンスの観点から見て、Oracle WSMアーキテクチャは次の利点をもたらします。

- *一元化された可視性*: 顧客は1つのコンソール（Oracle EM）から、利用できるすべてのポリシーを閲覧し、ポリシーが関連付けられているサービス数を特定できます。
- *ポリシーの再利用*: 同じポリシーを複数のクライアントやサービスに適用できるようにすることで、ポリシーを再利用できます。

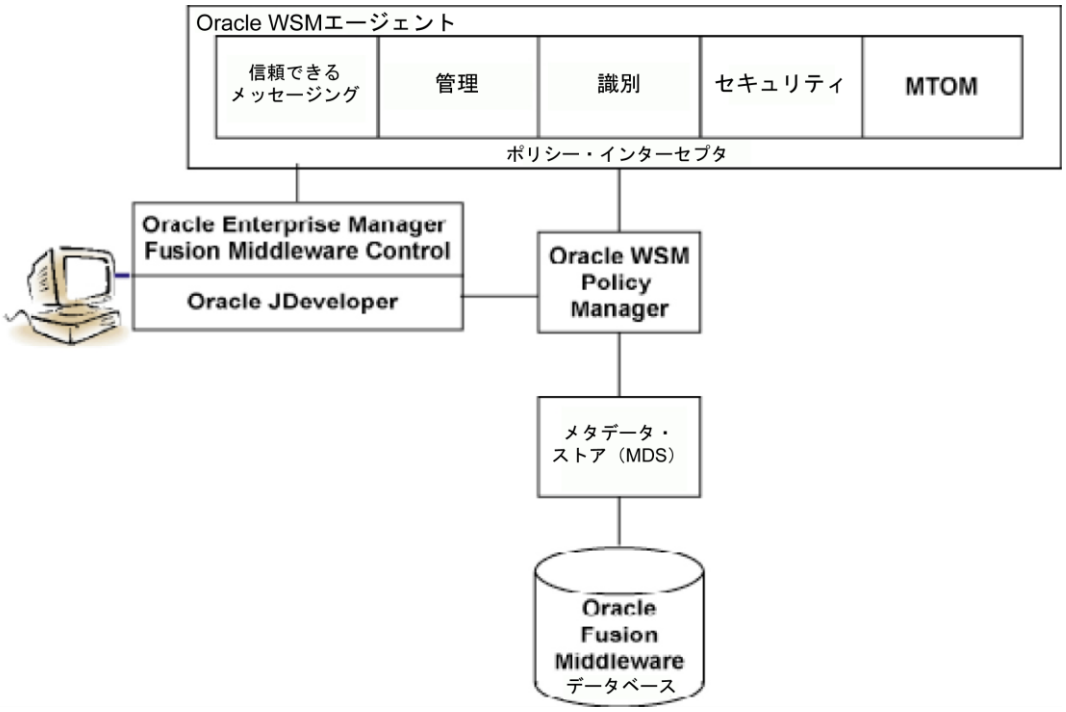

図5：Oracle WSMのアーキテクチャ

- *影響分析*: ポリシーに変更を加える前に、管理者はOracle EMを使用して、このポリシーに関連付けられているすべてのWebサービス・エンド・ポイントを確認し、関連付けられたポリシーの変更による影響を評価できます。
- *ポリシーのバージョニング*: Oracle WSMでは特定のポリシーに対するすべての変更履歴が独立したバージョンとして保持されています。これらはOracle EMから参照できます。この機能は、監査の際に役立ちます（誰が、いつ、ポリシーを変更し、どのような変更が実施されたかが分かります）。さらに、Oracle WSMでは、ポリシーの変更後にポリシー実行が失敗した場合、Oracle EMを使用して以前のポリシー・バージョンにロールバックできます。

ポリシーの監視

Oracle WSMは、成功または失敗した認証の数など、ポリシー実行に関する監視統計情報を収集します。これらの監視統計情報はOracle EMから確認できます。また、Oracle EM SOA Management Pack for Oracle Fusion Middleware 11gのリリース時には、これを利用することで、アラートや品質保証契約（SLA）ルールをこれらの統計情報に適用できます。

監査

ポリシーの適用結果やポリシーの作成、変更、削除を監査するため、Oracle WSMはOracle Fusion Middlewareの共通監査フレームワーク（CAF）と統合されています。

この統合により、管理者はOracle Business Intelligence Publisherを介してOracle WSMの事前定義監査レポートを提供できます。

Oracle WSMの使いやすさ

Oracle WSMは、開発者と管理者にいっそうの使いやすさを提供します。

- *事前定義済みポリシー*: Oracle WSMには、標準やベスト・プラクティスに基づいて事前定義された一連のポリシーが同梱されています。顧客はこれらのポリシーをクライアントやサービス・エンド・ポイントに直接関連付けることで、ポリシーを再利用できます。
- *WSDLを使用したポリシーの公開*: クライアント（Webサービス・リクエスタ）は適切なリクエストを送信するため、起動したWebサービス・エンド・ポイントの保護に使用されるポリシーの種類を認識している必要があります。Oracle WSMはWS-PolicyAttachment標準を使用して、WebサービスのWSDLファイルにWebサービス・エンド・ポイントのセキュリティ要件を公開しています。このため、Webサービス・プロバイダが帯域外でクライアントにセキュリティ要件を伝達する必要はありません（WS-PolicyAttachmentについて詳しくは、業界標準に対するサポートの項を参照してください）。
- *バルク・ポリシーの付加*: サービス・プロバイダとして、いくつかのポリシーをすべてのサービスに適用するという標準化を行った場合、Oracle WSMのバルク・ポリシー付加機能を使用すると、Oracle EMから、一度に複数のサービスに対してポリシーを関連付けることができます。
- *クライアント・ポリシーの生成*: Oracle WSMにより、Webサービス・エンド・ポイントのWSDLが入力として提供され、互換性のあるクライアント・ポリシーを生成できます。Oracle WSMによってWSDLファイル内のWS-Policy情報が解析されて、クライアント・ポリシーが生成されるため、クライアントの開発者と管理者はWS-Policyのセマンティックや関連する標準を理解する必要がなくなります。
- *ポリシーの互換性チェック*: この機能を使用すると、管理者は最初のリクエストを送信する前に、クライアントに関連付けられたポリシーが起動されるWebサービス・エンド・ポイントに対する互換性を持つかどうかをチェックできます。

Oracle WSMとOracle Access Managerの統合

Oracle WSMでは、Oracle Access Managerを使用してWebサービスへのアクセスを認証および認可できます。このような統合がもたらす利点として、顧客はOracle Access Managerを使用してWebアプリケーションとWebサービスの両方に対するアクセス制御を実現するとともに、LDAPルールに基づく動的なグループ機能などの付加価値の高いOracle Access Manager機能を利用できます。

このケースでは、最初にOracle WebLogic Server内にOracle Access Manager Authenticatorを構成する必要があります。これにより、あらゆる種類のトークンに対する認証がOracle Access Managerに対して実行されます。認証に成功すると、Oracle Access Manager Authenticatorによって、認証されたユーザーが属するすべてのグループ（動的グループを含む）がJavaサブジェクト・ロールに付加されます。次に、Oracle WSMのロールベース認可ポリシーを定義し、許可されたロールを追加して保護対象サービスに関連付ける必要があります。認可ポリシーによって、認証されたユーザーのJavaサブジェクトのロール・プリンシパルに許可されたロールが含まれるかどうかがチェックされます。

SOAガバナンスにおけるOracle WSMの役割

Oracle WSMはOracle SOAガバナンス・ソリューションにおけるランタイム・ポリシーのガバナンス・コンポーネントです。ポリシー主導型のセキュリティを介して、配置されたSOAアーチファクトの本番環境が保証されます。また、図6に示したとおり、クローズドループのライフ・サイクル制御のさまざまな段階に関与します。

図6：SOAガバナンスにおけるOracle WSMの役割

- サービス・コントラクト・ワークフローの一部として、サービス・プロバイダは、コンシューマによって合意されたポリシーの目的をサービスに対して定義します。
- サービスが配置されると、ワークフローによってポリシーの目的を含む通知がセキュリティ管理者に送信されます。管理者はポリシーの目的を調べ、配置されたサービスに適したOracle WSMセキュリティ・ポリシーを適用します。
- ポリシーを適用する際、Oracle WSMはポリシー実行に関するメトリックを収集します。これらのメトリックは実行時監視機能による視覚的なグラフを通じて提供されます。

Oracle WSMのユースケース・サマリー

ここからは、典型的なOracle WSMのユースケースについて簡単に説明します。

複数のWebサービス・タイプへのアクセスの保護

Oracle WSMのセキュリティと管理に関するポリシーは、Java Platform, Enterprise Edition（Java EE）のJava API for XML Web Services（JAX-WS）やOracle Application Development Framework Business Components（Oracle ADF BC）、またはOracle SOAコンポジット（Webサービス・インタフェースの公開に使用されるBusiness Process Execution Language（BPEL）プロセスなど）といった各種のWebサービスに適用され、それらを保護します。

Webサービスへのアウトバウンド・コールの保護

アプリケーションからWebサービスを起動して、データを取得または処理できます。このWebサービスがWS-Securityを使用して保護されている場合、Oracle WSMクライアント・ポリシーをサービス・クライアント・アプリケーションに適用することで、アウトバウンド・メッセージを保護できます。ポリシーが適用されると、サービス・プロバイダによって要求されたIDトークンが挿入され、必要に応じてリクエストの署名と暗号化が実施されます。サービス・プロバイダから暗号化レスポンスが返されると、Oracle WSMクライアント・ポリシーは要求元アプリケーションにメッセージを転送する前に、レスポンスを復号化します。Oracle WSM 11g Release 1でサポートされているサービス・クライアントは、Java EE JAX-WS、Oracle ADF BC、Oracle SOAコンポジット、Oracle WebCenterリモート・ポートレットです。

WebアプリケーションからWebサービスへのIDの伝播

WebアプリケーションからWebサービスを起動して、データを取得または処理できます。Webサービスが保護されている場合、WebアプリケーションはWebサービスにリクエストを送信する際に、Webサービスで認証に使用されるセキュリティ・トークンを含める必要があります。Oracle Access ManagerなどのIDおよびアクセス管理ソリューションを使用してWebアプリケーション自体が保護されている場合、Oracle Access ManagerからWebサービスに対して、ログイン・ユーザーのIDを伝播できます。この場合、Oracle WSMクライアント・ポリシーはOracle Access Managerのトークン情報からSAMLトークンを生成し、アウトバウンド・リクエスト・メッセージのWS-Securityヘッダーに挿入します。

Webサービス・チェーンを介したID伝播

Webサービスから別のWebサービスが起動され、そこからさらに次のWebサービスが起動されて1つのトランザクションが完了する場合があります（このようなパターンは"チェーンWebサービス"と呼ばれます）。チェーン内のそれぞれのサービスは、保護される場合があります。Oracle WSMを利用すると、どのサービスがどのサービスを呼び出しているかをチェックするのではなく、Webサービス・チェーンを起動した最初のユーザーを確認できます。また、Oracle WSMポリシーを使用して、最初のユーザーのIDをWebサービス・チェーン全体に伝播できます。チェーン内の最初のWebサービスに対する認証が成功すると、Oracle WSMはトランザクション全体で使用されるJavaサブジェクトとしてユーザーを設定します。別のWebサービスを起動する際、Oracle WSMクライアント・ポリシーによってJavaサブジェクトからユーザーIDが取り出され、サブジェクトの情報に基づいてSAMLトークンが生成され、サービス・プロバイダに送信されるリクエスト・メッセージのWS-Securityヘッダーにこのトークンが挿入されます。これによって、情報を取得するためにチェーン内の1つ前のサービスのIDを使用して最初のWebサービスを呼び出さなくても、チェーンに含まれるすべてのWebサービスでWebサービスのエンド・ポイントを呼び出している実際のユーザーのIDを使用できます。

業界標準に対するサポート

次の表では、Oracle WSM 11g Release 1でサポートされている各種の業界標準について説明します。

標準名	説明と使用法
SOAP 1.1および1.2	SOAPは、Webサービスのリクエストとレスポンスを形式化するために使用されるXMLメッセージング標準です（SOAPはすでに頭字語ではなくなっていますが、仮にそうだとすれば"サービス指向アーキテクチャ・プロトコル"を意味します）。セキュリティ情報は通常SOAPメッセージ・ヘッダーに含まれ、メッセージ・ペイロード（例：発注情報）はSOAPメッセージ・ボディに含まれます。SOAPメッセージの構成例については、本書の図1を参照してください。
SOAP with Attachments（SWA）1.1および1.2	SWAはSOAP機能と標準MIMEメカニズムを使用して、SOAPメッセージの添付ファイルを送信および参照します。MIME（Multipurpose Internet Mail Extensions）はさまざまな要素（テキスト、XMLドキュメント、画像など）をサポートする標準です。
Message Transmission Optimization Mechanism（MTOM）	MTOMを使用すると、Webサービスとの間でバイナリ・データを送受信できます。MTOMは、上記のSWAメカニズムで使用されるMIMEベースの添付ファイルに対する効率的な代替策です。
WS-Security 1.0	WS-SecurityはSOAPのセキュリティ拡張機能を規定するものであり、XML EncryptionによるXML Signatureによるデータ整合性を提供します。またWS-Securityには、認証や認可を目的としてWS-Securityヘッダーに各種のバイナリやXMLセキュリティ・トークンを挿入する方法を指定するプロファイルも含まれています。Oracle WSM 11g Release 1では次のWS-Security 1.0セキュリティ・トークンがサポートされています。Username Token Profile 1.0、X.509 Token Profile 1.0、SAML Token Profile 1.0（SAML 1.1アサーションを使用）、SOAP with Attachments Profile 1.1。
WS-Security 1.1	Oracle WSM 11g Release 1.1では次のWS-Security 1.1セキュリティ・トークンがサポートされています。Username Token Profile 1.1、X.509 Token Profile 1.1、SAML Token Profile 1.1（SAML 1.1アサーションを使用）、Kerberos Token Profile 1.1、SOAP with Attachments Profile 1.1。
WS-Policy 1.2	WS-Policyを使用すると、Webサービスへのアクセスに使用されるポリシー情報を指定できます。ポリシーは1つ以上のポリシー・アサーションとして表されます。ポリシー・アサーションは、機能や要件を表します。たとえば、ポリシー・アサーションを使用して、Webサービスへのリクエストを特定の暗号化アルゴリズムを使用して暗号化するよう規定できます。WS-PolicyはOracle WSM 11g Release 1とOracle Fusion Middlewareの標準セキュリティ・モデルです。

WS-SecurityPolicy 1.1	WS-Security Policyによって、WS-Policyフレームワークのコンテキストで使用される一連のセキュリティ・ポリシーのアサーションが定義されます。WS-Security Policyアサーションは、通信パス上でメッセージを保護する方法を示すものです。
WS-PolicyAttachment 1.1	WS-PolicyAttachmentによって、（WS-Policy）ポリシーがWebサービスに関連付けられる方法が定義されます。ポリシーはWSDLに組み込まれます。
WS-ReliableMessaging（WS-RM）1.0および1.1	WS-RMは、Webサービスのエンド・ポイント間におけるメッセージ配信の信頼性を管理するXMLフレームワークを定義します。WS-RMはSOAPメッセージング構造（SOAPバインド）に準拠しており、WS-Security、WS-Policy、およびWS-Addressingに依存することで、信頼性の高いメッセージングを提供します。
WS-Addressing 1.0	WS-AddressingはXMLフレームワークを提供することで、Webサービスのエンド・ポイントを識別し、メッセージ内のエンド・ポイント識別をエンド・ツー・エンドで保護します。
WS-MetadataExchange（WS-MEX）1.1	WS-MetadataExchangeは、クライアントがWebサービス・エンド・ポイントにアクセスし、通信するために必要なメタデータをリクエストする方法を定義します（メタデータはWSDLまたはWS-Policy情報になります）。WS-MetadataExchangeはWS-Addressingを使用してエンド・ポイントを特定します。
Encryption Algorithms AES-256、AES-192、AES-128、3-DES	WS-Security標準とXML Encryption標準で使用される暗号化アルゴリズムです。
Signature Algorithms RSA、SHA1	WS-Security標準とXML Signature標準で使用されるデジタル署名アルゴリズムです。
Java Key Store（JKS）	JKSはOracle WSM 11g Release 1で使用されるメカニズムであり、キー・エントリと証明書エントリの読取りと保管を実行します。JKSはJavaのコアAPIに含まれています。

結論

Oracle WSMは標準ベースのソリューションであり、これを利用すると、ユーザー（開発者とシステム管理者）はWebサービスのセキュリティを宣言的に実装できます（コーディングは不要であり、セキュリティは保護対象のWebサービスとは分離されます）。

Webサービスのセキュリティ・ポリシーと管理ポリシーはOracle WSM Policy Managerに一元的に定義されており、Oracle WSMエージェントを介してローカル実行されるため、セキュリティ上のサイロが排除されます。

Oracle WSMは標準ベースのID管理インフラストラクチャを利用して、認証処理とアクセス制御処理を実行します。

ORACLE

Oracle Web Services Manager 11gを使用したWebサービスとサービス指向アーキテクチャの保護
2009年6月
著者：Vikas Jain
共著者：Marc Chanliau

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

海外からのお問い合わせ窓口：
電話： +1.650.506.7000
ファクシミリ：+1.650.506.7200
www.oracle.com

Oracle is committed to developing practices and products that help protect the environment

0109