SOA セキュリティ:
ORACLE WEB SERVICES MANAGER

SOA セキュリティ・ソリューション

サポートされる標準

- 暗号化アルゴリズム:
  AES-128、AES-256、3-DES
- メッセージ・ダイジェスト:
  MD5、SHA-1
- メッセージ構造:
  XML/SOAP/WS-Security 1.0
- セキュリティ・トークンのプロファイル: Username、X.509、SAML
- メッセージの整合性:
  XML シグネチャ
- メッセージの機密保護:
  XML 暗号化
- ポリシー・フォーマット:
  WS-Policy
- PKI
  - キー暗号化:
    RSA OAEP-MGF1P、RSA V1.5
  - シグネチャ・アルゴリズム:
    RSA (PKCS #1) (1024 ビット・キー、2048 ビット・キー) 、DSA
  - Credentials store, wallets:
    JKS, PKCS#12

サポートされるプラットフォーム

- オペレーティング・システム:
  Windows、Linux、Solaris、AIX
- アプリケーション・サーバー:
  Oracle Application Server、IBM WebSphere、BEA WebLogic Server、JBoss
- データベース・システム:
  Oracle Database、Microsoft SQL Server

世界各国の企業は、イントラネット環境でもエクストラネット環境でもサービス指向アーキテクチャ（SOA）を積極的に実装しています。SOA は、現行の他の選択肢と比較すると様々なメリットがありますが、Web サービスのネットワークを展開する作業は、特にセキュリティや管理の点で大きな課題を抱えています。オラクル社は、スタンドアロン製品と Oracle SOA Suite のコンポーネントとして提供される標準ベースのソリューション、Oracle Web Services Manager（WSM）により、SOA のセキュリティと管理の実現をめざします。

概要

Oracle WSM は、異種環境における Web サービスのセキュリティの定義と実装を目的として設計された J2EE アプリケーションで、SLA（品質保証契約）に基づいて Web サービスを管理し、ランタイム時のアクティビティをグラフで監視できるツールを備えています。

開発者は、Oracle WSM を使用して開発時に個々の Web サービスのセキュリティを検証できます。システム管理者は、ID 管理インフラストラクチャを活用する社内標準準拠のセキュリティを本番環境で実現できます。

宣言型セキュリティ

Oracle WSM は、プログラミングを必要としない宣言型のセキュリティへの取組みをサポートします。Oracle WSM には、次のコンポーネントが含まれます。

- Policy Manager
- ポリシー施行ポイント
- 運用管理および監視

Policy Manager

Oracle WSM の Policy Manager は、事前定義されたセキュリティ・ポリシーおよび管理ポリシーを Web サービスに付加するためのグラフィック・ツールです。ポリシーは、Policy Manager によってデータベース内に保存され、施行ポイントに伝播されます。

ORACLE IDENTITY MANAGEMENT 製品

Oracle Access Manager は、異機種アプリケーション環境においてアクセス制御、シングル・サインオン、ユーザー・プロファイル管理に不可欠な機能を提供します。

Oracle Identity Manager は、企業 ID のプロビジョニングとコンプライアンス監査のための強力かつ柔軟なソリューションです。ディレクトリ、電子メール、データベース、ERP などの企業システムにおけるユーザーの作成、更新、削除を自動化します。

Oracle Identity Federation は、ドメイン間におけるシングル・サインオンおよびビジネス・パートナ管理に必要な機能を完備したソリューションです。

Oracle Internet Directory は、Oracle 10*g* Database プラットフォームの高可用性機能を活用する堅牢でスケーラブルな LDAP バージョン 3 対応のディレクトリ・サービスです。

Oracle Virtual Directory は、既存の企業 ID 情報をデータの同期化や元の場所から移動することなく、インターネット標準や業界標準の LDAP ビューと XML ビューで表示します。

Oracle Enterprise Single Sign-On は、デスクトップ、クライアント・サーバー、カスタムとメインフレーム・アプリケーションなど、企業のすべてのリソースにわたって統一されたサインオンおよび認証をユーザーに提供します。

ポリシー施行ポイント

ポリシー施行ポイント（PEP）は、Web サービスに対するリクエストをインターセプトし、Web サービスに対して指定されたポリシーを適用します。

PEP は、保護対象となるアプリケーションにデプロイされるエージェント（エンド・ツー・エンド・セキュリティ）、またはプロキシ・サーバーの柔軟性を提供するゲートウェイです。

パイプライン・メタファ

Web サービスのリクエストのポリシー施行手順は、受信パイプラインに順を追って定義します（認証→承認など）。ポリシー施行手順はランタイム時に実行されます。リクエストが正常に実行されると、保護された Web サービスへのアクセス権が与えられます。

Web サービスのレスポンスのポリシー施行手順は、送信パイプラインに順を追って定義します（暗号化→署名メッセージなど）。ポリシー施行手順はランタイム時に実行されます。

運用管理および監視

Oracle WSM のモニタでは、ランタイム時に施行ポイントからデータを収集し、情報を統合してダッシュボードにビューとしてレンダリングします。

ユーザーは、たとえば、確実な待機時間、計画停止時間、最大故障率などの SLA（品質保証契約）を定義できます。SLA はランタイム時に施行され、実行詳細はグラフで表示されます。

Oracle WSM では、認証や承認の失敗回数などのセキュリティ統計情報や、各サービスまたは各操作ごとのメッセージ数やバイト数などのトラフィック解析情報を表示します。

ガバナンス

Oracle WSM は、UDDI 準拠のレジストリと統合し、ランタイム時に実行され監視されるポリシーを介して社内ルールまたは政府規則を実装できます。

Deployment

Oracle WSM は、スケーラビリティ、高可用性、バックアップとリストアを実現するために、基盤となるアプリケーション・サーバーのインフラストラクチャを活用します。Oracle WSM Gateway を使用すると、呼び出された Web サービスが停止した場合、使用可能な Web サービスに Web サービス・リクエストをリダイレクトし、リクエストの内容に基づいて特定の Web サービスにリクエストをリダイレクトすることができます（コンテンツ・ベールのルーティング）。

統合

Oracle WSM は、Oracle SOA Suite のセキュリティの要です。Oracle WSM は、エージェント・タイプとゲートウェイ・タイプのポリシー施行ポイントを使用して、BPEL プロセスと ESB プロセスを保護します。

LDAP ディレクトリに加え、Oracle WSM は、Oracle Access Manager や CA eTrust SiteMinder などの ID 管理インフラストラクチャを活用して認証および承認を実行します。