CHAPTER 1

Cisco ACE XML Gateway の概要

この章では、Cisco ACE XML ゲートウェイ ソリューションの概要を説明します。内容は次のとおりです。

ネットワークでの Extensible Markup Language（XML）

Service-Oriented Architecture（SOA; サービス指向アーキテクチャ）は、コンピューティング リソースをサービスとして提供可能にする Information Technology（IT; 情報技術）システムの設計用構築方法です。基本技術は多様ですが、SOA のサービスの特徴として一般に、モジュラ設計方法、標準、確立された呼び出しインターフェイス、共通のデータ交換形式の使用（通常は Extensible Markup Language（XML）に基づく）などがあります。

SOA 実装の目的は、コンピューティング リソースの俊敏性や再利用率を上げ、結果としてリソースの価値を高めることです。リソースのアベイラビリティ向上によりその価値が高まる反面、リスクや課題も多くなります。業務をネットワークで公開すると、誤使用や攻撃の可能性が生じます。業務リソースの利用を制限すると、管理や監視が困難になる場合もあります。

その他にも課題が存在します。相互運用性を確保するためには、広範な標準や要件に対応し続けることが組織に必要になります。SOA の主要なフレームワークは、Web Service 仕様のファミリー（WS-*）で定義されています。WS-* は、Web サービスを公開するための表記法およびプロトコルを提供します。

多くの場合、SOA システムのエンドポイントは異なる組織で管理されます。また、エンドポイントでは、想定されない形式や形式不良のメッセージに対処が必要なこともあります。

ネットワークでのサービスが増加するにつれ、ネットワーク上のトラフィック量も増えます。こうしたトラフィックによりネットワークやアプリケーション サーバへの作業負荷が大きくなる可能性があります。XML は、その他のメッセージング スタイルに比べて情報量が多いため、ネットワーキングおよび処理リソースの作業負荷を大幅に増やすことが知られています。

SOA、XML メッセージング、WS-* などの技術開発により、ビジネス ポリシーを分散リソースに適用するニーズが増大しています。理想的には、こうしたソリューションは、XML や分散サービスによる IT インフラストラクチャへの負荷を軽減しながら、コンテンツ認識のネットワーク トラフィック セキュリティを提供できます。

Cisco ACE XML ゲートウェイ について

Cisco ACE XML ゲートウェイ は Cisco Application Control Engine（ACE）ファミリー製品を構成し、ネットワークにアプリケーション インテリジェンスをもたらします。ACE XML Gateway は、SOA や豊富なアプリケーションを持つネットワーク環境のセキュリティ保護、管理、監視、最適化に役立ちます。

ACE XML Gateway はサービス仮想化プラットフォームとして働きます。バックエンド アプリケーションとユーザを切り離し、システム全体の安定性、保守性、および柔軟性を高めます。ACE XML Gateway を使用すると、各アプリケーションにビジネス ルールを組み込む必要がなく、メッセージ トラフィックを介してルールを適用できるため、セキュリティ ポリシーやアクセス ポリシーが分散コンピューティング リソースに均一に適用されます。

ACE XML Gateway は高性能 XML 処理エンジンで、計算量の多い XML 処理によるサーバの負担を軽くする結果、セキュリティ、相互運用性、信頼性を損なわずに、アプリケーション トラフィックをすばやく処理できます。

ACE XML Gateway のポリシー作成および管理インターフェイスは ACE XML Manager Web コンソールです。この Web コンソールは ACE XML Gateway ポリシーのブラウザベース開発環境インターフェイスです。ACE XML Gateway のネットワーク導入作業を大幅に緩和するツールおよび機能が含まれています。Web コンソールは、WS-Addressing、XML 暗号化、XML 署名、Security Assertion Markup Language（SAML）、Web Services Security（WSS）UsernameToken などの複雑な新技術を使いやすくします。Universal Description, Discovery and Integration（UDDI）サービス ディスカバリ ウィザードでは、Web コンソールによるすばやいポリシー作成が可能です。

ACE XML Gateway は、アウトオブザボックスのほとんどの統合要件に対応可能であると同時に、機能を追加するために ACE XML Gateway Software Development Kit（SDK; ソフトウェア開発キット）を使用できます。SDK では、カスタム アクセス コントロール モジュール、メッセージ変換、I/O プロセッサなどの各種方法で ACE XML Gateway を拡張できます。ACE XML Gateway SDK の詳細については、『*Cisco ACE XML Gateway Developer Guide*』を参照してください。

Web アプリケーション セキュリティについて

ACE XML Gateway には、Web アプリケーションとそのユーザのセキュリティを確保する、拡張 Web アプリケーション ファイアウォール機能があります。Payment Card Industry（PCI）データ セキュリティ標準による規定など、バックエンド Web アプリケーション セキュリティの広範な要件に対応可能なツールが ACE XML Gateway に用意されています。

ACE XML Gateway ポリシーでは、2 つのポリシー オブジェクト（仮想サービスと仮想 Web アプリケーション）のいずれかを使用して、トラフィック ルーティングを実現します。仮想 Web アプリケーションは、特定のサービス エンドポイントではなく、トラフィック クラスに基づいてトラフィックのルールと処理を定義するためのものです。

Web アプリケーション トラフィックのセキュリティ ポリシーにおける 2 つの主要コンポーネントとして署名とルールがあります。署名は、Cisco ACE XML ゲートウェイ にとって重要なコンテンツを識別するコンテンツ パターンです。ルールによってメッセージ トラフィックに署名を適用します。また、ルールは、その他のアトリビュートとともに署名の一致を検査するメッセージ箇所を示すものです。

Cisco ACE XML ゲートウェイ には、組み込みルールおよび署名のライブラリがあり、Web アプリケーションとそのユーザのセキュリティ保護に使用できます。組み込みルールは、クロスサイト スクリプティング攻撃、SQL インジェクション攻撃、コマンド インジェクション攻撃など、システムに対する多くの一般的な攻撃や脅威を防止するために提供されます。また、独自のメッセージ インスペクションおよびメッセージ リライト ルールを作成することもできます。