# XML と SOAP によるセキュリティ関連情報 Web サービス*

中村 章人† 戸村 哲‡
産業技術総合研究所§

## 1 はじめに

情報セキュリティに対する脅威に対抗するため、平時からの情報収集の重要性、及び緊急時に備えた情報収集体制とそのチャネルを維持することの重要性が改めて再認識されている。しかし、情報量の膨大さと情報システムの多様性を勘案すると、そのコストは大きい。また、情報収集を効率よく行えたとしても、システムの状態を正確に把握し、適切な処置を行うのは難しい。従って、セキュリティ関連情報の収集や分析と、それらを用いた情報システムの管理とを相当程度自動化するシステムの開発・整備が重要である。

我々はこのような要求を満たすために、プログラムで処理可能な XML フォーマットでセキュリティ関連情報を発信し、SOAP を使ってこれらの情報にアクセスする Web サービスを構築している。これによって、情報収集の自動化、検索や統計処理の高度化、アプリケーション間の連携等を可能にし、セキュリティ対策のプロセスを支援する。

本稿では、セキュリティ関連情報を提供する Web サービスの要件と、具体的な脆弱性データベースを用いた Web サービスとその応用例について述べる。

## 2 セキュリティ関連情報サービスの要件

本章では、セキュリティ関連情報を提供するシステムに対して求められる要件を整理し、実現方法を検討する。

### 2.1 データ交換フォーマット

XML は、プログラミング言語やプラットフォームの制約を受けない、オープンな標準フォーマットである。データを XML という標準フォーマットで表現することで、単一のデータを複数の目的に利用でき、アプリケーションの変更にも柔軟に対応できる。また、タグによるマークアップが自己記述的であることと、構造 (文書型) の定義とその検証のフレームワークが用意されているため、プログラム処理に適している。さらに、個別に作られた情報を名前空間を用いて統合することや、メタデータを用いた高度な検索機能を実現できる可能性がある。

これらの観点から、我々は、セキュリティ関連情報の交換フォーマットとして、XML を採用した。

### 2.2 アーキテクチャとプロトコル

Web サービスとは、メッセージとそのフォーマットにより仕様が規定されたネットワーク上で利用できるサービスである。Web サービスでは、サービスの公開、検索、利用のための情報交換を要求/応答メッセージの通信としてモデル化し、そのエンコーディングには XML を用いる。SOAP[3] は、W3C で標準化されている Web サービスのメッセージ交換プロトコルである。

Web サービスの要素技術である SOAP[3] や WSDL[5] はすべて標準化された技術で、XML をベースにしているため、高い相互運用性と、実行環境からの独立性が期待できる。情報提供機能を Web サービスとして実現することで、これをアプリケーションを構成するコンポーネントとして利用できる。

Web サービスのアーキテクチャの特徴は、我々が目指すシステムの開発・実行環境の要件を満たしているので、このアーキテクチャを利用する。つまり、SOAP の RPC モデルに基づいて情報提供サービスを実現する。

### 2.3 セキュリティ

利用者の立場からは、提供された情報を信頼する条件として、メッセージ認証と発信者認証が要求される。すなわち、メッセージの改竄及びメッセージ作成の否認と、情報提供者のなりすましを回避できる必要がある。メッセージ認証は XML または SOAP メッセージの署名 [6, 4] により、発信者認証は SSL により実現する。

情報提供者の立場では、一般に、通信内容の秘密性、すなわちメッセージの暗号化と、受信者認証が求められる。しかし、本システムでは、一般公開を前提とした情報を扱うため、これらの要件は発生しない。また、情報の送信回数は問題にならないので、リプレイ攻撃は脅威と考えない。

## 3 脆弱性情報 Web サービス

前章の検討に基づいて、セキュリティ関連情報の一つとして、ソフトウェア脆弱性情報を提供する Web サービスを構築した。本章では、この Web サービスの概要を述べる。

### 3.1 CVE 互換な脆弱性情報の利用

本 Web サービスは、CVE 互換である。CVE (Common Vulnerabilities and Exposures)[1] は、公知のソフトウェア脆弱性を集積した「脆弱性の辞書」である。それぞれの脆弱性に一意な識別子 (例:CVE-2002-1056) を付与し、脆弱性の包括的なリストを作成し、これを業界標準として用いるという試みである。脆弱性を扱うツール、データベース、サービス等が CVE 名を参照することで、それぞれ独自に名前付けされた情報を相互に関連付けることができる。CVE 名を取り入れた製品やサービスを、「CVE 互換 (CVE-compatible) である」という。

*A Security Information Web-Service using XML and SOAP
†Akihito NAKAMURA (akihito@ni.aist.go.jp)
‡Satoru TOMURA (s.tomura@aist.go.jp)
§National Institute of Advanced Industrial Science and Technology (AIST)

脆弱性情報自体は、米国 NIST (National Institute of Standards and Technology) が提供する CVE 互換の脆弱性データベース ICAT Metabase[2] (以下では ICAT と略す) を利用した。ICAT では、他の情報提供サイトから得られる情報を分析し、各脆弱性情報を 40 個程度の属性で記述する。属性には、深刻度、概要、脆弱なソフトウェアのリスト、脆弱性の種類、攻撃による被害の種類等がある。

### 3.2 SOAP による Web サービスの実装

本システムの構成を図 1 に示す。Web サービスオブジェクトは、Web サービスを実行するオブジェクトである。SOAP プロセッサは、SOAP メッセージの送受信と Web サービスオブジェクトに対するメソッド起動を行う。クライアントが Web サービスにアクセスするためのスタブは、Web サービスへのアクセス方法を記述した WSDL から自動生成できる。Java については、スタブクラスをあらかじめ用意している。リソースアダプタは、実際に用いる個々のデータ記憶システムの相違を吸収する。ここでは RDB を用いているが、ファイルシステムや LDAP を用いることもできる。

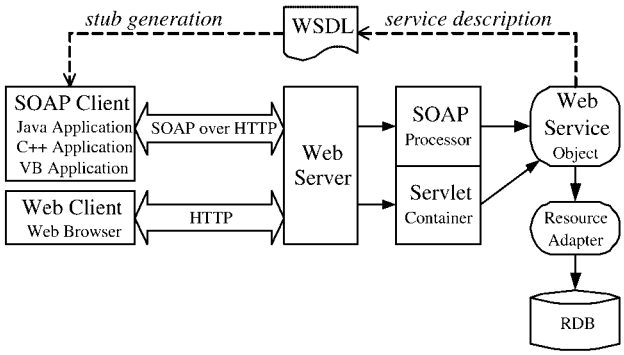


図 1: Web サービスの構成要素

本システムの実装には Apache Web サーバ、Apache SOAP、Tomcat、MySQL を用いた。UNIX/Linux と Windows を対象の実行環境とし、いずれの OS でもシステムを構築できるものを選んだ。プログラミング言語は、実行環境への依存性が少なく、XML 関連のツールやライブラリが数多く提供されている Java を用いた。

SOAP RPC の実行手順や、その上で交換される脆弱性情報のオブジェクトモデルについては、文献 [7] で詳細に論じている。

通常の Web ブラウザによるアクセスを意図した HTTP ベースのサービスも平行して提供している。これは、サーバ側であらかじめ用意した固定の検索・表示サービスを利用するために用いる。

## 4 アプリケーション

本 Web サービスを利用した二つのアプリケーションについて述べる。

### 4.1 複数データベースの横断的検索

ICAT を利用した Web サービスの他に、情報処理振興事業協会 (IPA) が電子政府情報セキュリティ技術開発事業において開発した脆弱性データベースを利用した Web サービスも構築した。このデータベースも CVE 互換であるが、ICAT とは属性の種類が異なっており、データは日本語である。

これら二つのデータベースを横断的に検索するアプリケーションを開発した。本アプリケーションは、Web ブラウザをユーザインタフェースとし、一つの問合せ条件を元に二つのデータベースを SOAP 経由で個別に検索し、結果を統合して表示する。

### 4.2 脆弱ソフトウェアの検出

Red Hat Linux の RPM (Red Hat Package Manager) と脆弱性情報 Web サービスを組み合わせて、システムにインストールされているソフトウェアの中から脆弱なものを検出するツールを開発した。RPM を利用して各ソフトウェアのバージョンを調べ、これと脆弱性情報とを突き合わせることで、脆弱なものを検出する。Web ブラウザを利用して、ネットワーク経由での操作も可能である。

現在は RPM だけに対応しているが、今後、他の Linux ディストリビューションのパッケージングシステムにも対応する。ディストリビューションやパッケージングシステムの違いを透過にし、ネットワーク上の各システムの脆弱性検査を行える管理ツールへと発展させる予定である。

## 5 おわりに

本稿では、XML をデータフォーマットに用いてインターネット上でセキュリティ関連情報を共有・交換するための Web サービスについて述べた。具体的な情報として CVE 互換の脆弱性情報を提供する Web サービスを実現した。

これまでに、(財) 国際情報化協力センターの事業の一環として、本システムの評価を行った。また、IPA の脆弱性データベースとの相互接続を行った。現在、通信総合研究所の不正アクセス事例記憶装置との相互接続実験を開始したところである。今後、侵入検知システムやセキュリティ検査ツールと本システムを統合したときの効果を、実証実験で確認していく計画である。

## 参考文献


[1] Common Vulnerabilities and Exposures. http://cve.mitre.org/

[2] *ICAT Metabase: A CVE Based Vulnerability Database*. http://icat.nist.gov/

[3] W3C Note: *Simple Object Access Protocol (SOAP) 1.1*, 08 May 2000.

[4] W3C Note: *SOAP Security Extensions: Digital Signature*, 06 February 2001.

[5] W3C Note: *Web Services Description Language (WSDL) 1.1*, 15 Marsh 2001.

[6] W3C Recommendation: *XML-Signature Syntax and Processing*, 12 February 2002.

[7] 中村, 戸村: *XML* によるセキュリティ関連情報 *Web* サービス, マルチメディア通信と分散処理ワークショップ論文集, 2002, pp.275-280.