XML/Webサービスのセキュリティ技術の動向と我々の取り組み

Technical Trend and Our Approach to Security of XML/Web Service

沖花　和夫
Kazuo Okihana

概要

インターネットが世界のインフラとして確立され、インターネットを用いたビジネス(e-ビジネス)は強固なセキュリティを必要としている。そして、XML/Webサービスが、情報の共有やプロセスを統合した新しいe-ビジネスを切り開く技術として全世界的に期待され広まりつつある。我々はそういった流れの中で、XMLへの電子署名技術を中心としたXMLのセキュリティ技術を研究するとともに、Webサービス関連の技術を蓄積してきた。これらの技術を統合することで、我々の提供するXML/Webサービスのソリューションをセキュアなものとし、顧客のパートナーとして信頼されることを目指し、継続的なソリューションの拡充と提案に努めている。

1.　はじめに

XML/Webサービスが、次世代のe-ビジネスの姿として注目されるようになってきた。それはXML/Webサービスにより、世界的な情報の共有、プロセスの統合（図1）が実現できると考えられるからである。しかしXML/Webサービスには、セキュリティを始めとする幾つかの課題が残されており、これらのことが実現できるには至っていない。

ここでは、XML/Webサービスの特徴と課題、そして我々がXML/Webサービスにどのように取り組んできたかを述べる。

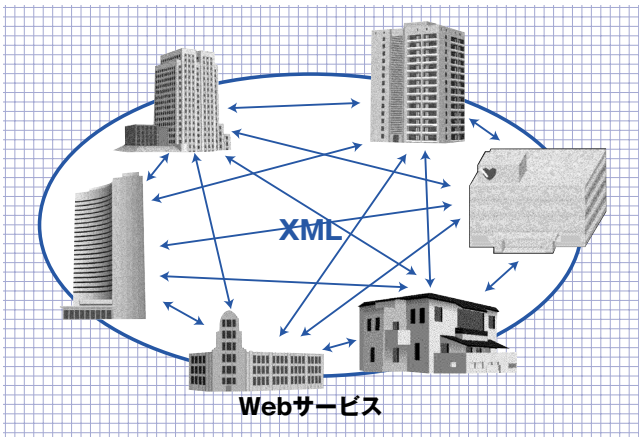


図1　XML/Webサービスによるプロセスの統合

2.　XML/Webサービス

2.1　XML

現在、XMLは全世界で情報の表記法の標準としての立場を確立しつつあり、特にアメリカを中心として急速に広まりつつある。スキーマ標準化の動きの代表とされるのがRosettaNetやebXMLであり、これらの仕様を用いて活発にXMLによるe-ビジネスが展開されようとしている。日本でも海外に比べると遅れはとっているものの、世界に追いつくために徐々にXMLを利用したシステムの開発が広まってきている。そして、SOAPやWSDLといったWebサービス関連のインフラ技術が提案され、仕様が整いつつあり、WebサービスはB2Bにおけ

るXML利用の標準的な技術としての立場が確立されている。

2.2 Webサービス

Webサービスの定義は人によりさまざまであるが、図2のようなXMLを用いた通信の仕様であるSOAPと、XMLによりサービスのインタフェースを記述する仕様であるWSDL、そしてサービスの登録、検索を行うための仕様であるUDDIの3つの仕様を利用したものを指すことが一般的である[参考文献1]。SOAPを利用すれば、通信仕様のデファクトスタンダードであるHTTPにXMLを載せることが可能であるので、Webサービスはインターネットを介してサービスの連携が可能な仕様としても注目されている。また、コンピュータがUDDIに登録されたWSDLを自律的に検索・解析することで、Webサービスのダイナミックな連携が可能になり、企業間のプロセスが連携されることで、ビジネスが大きく変革するといった話がさまざまなところで語られるようになった。このWebサービスにより、XMLをB2Bにおける情報表記の標準として利用する動きが加速された。

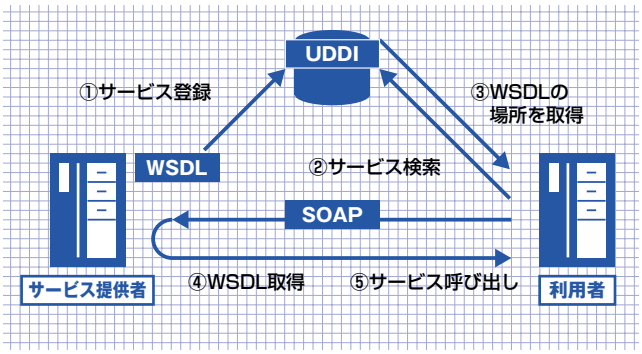


図2 Webサービスを支える3つの技術

3. XML/Webサービスの課題と利用例

XMLを情報の表記法として用いたシステムや、B2Bへの利用は前述のように広まりつつある。また、Webサービス関連の技術であるSOAPなども社内システムを統合するための基盤技術として利用されるようになった。しかし、XML/Webサービスには幾つかの課題が指摘され続けており、世界的な情報の共有及び、プロセスの統合が可能になったとは言い難い。

3.1 XMLのセキュリティ

XML/Webサービスの課題として始めに挙げられるのが、セキュリティの課題である。XML/Webサービスを利用した通信では、XMLはそのままテキストとして送信されるため、簡単に第三者に内容が読み取られ、盗聴の脅威が存在する。また、XMLの仕様はオープンであり、盗聴も容易なことから簡単に内容が把握でき、改竄やなりすましなどの行為が可能である。そして、XMLに限らずe-ビジネスにおける電子データは、誰が送ったものであるか証明できなければならない。これは、後日「送っていない」「そのような内容ではない」と言うような否認のトラブルを未然に防ぐため、データを送信したことと、送られたデータが確かに送信したデータであることを証明できる必要があるということである。

この盗聴、改竄、なりすまし、否認というセキュリティの4つの脅威に対するために、従来から暗号化や電子署名などの技術が研究、開発されてきた。当然、XMLを用いた通信のセキュリティに関しても従来の通信と同様に、暗号化や電子署名などの技術が必要となる。しかし、従来のセキュリティ技術をそのままXMLに適用すると、XMLの特徴を最大限に生かすことができない。このため、XMLに関するセキュリティ技術には、従来のセキュリティ技術には無かった性質が要求されている。

XMLの特徴を最大限生かすには、XMLの要素別に異なったセキュリティポリシーや異なったセキュリティ技術を適用する必要がある。

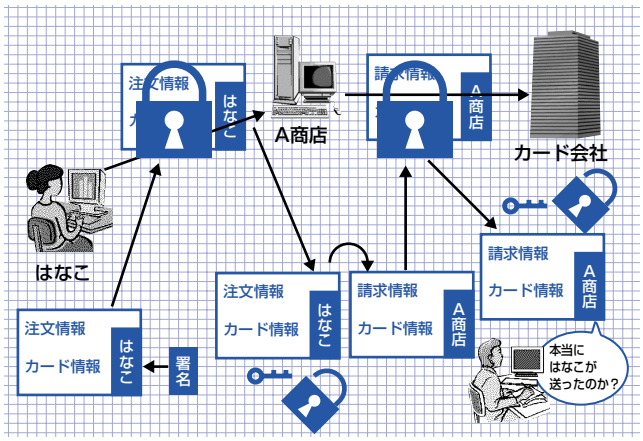


図3 従来のセキュリティ技術の場合

インターネット商店で商品を購入し、カードで決済する場合を考える。図3のような従来のWebアプリケーションなどのセキュリティの場合、商店とユーザの間の通信は暗号化され、商店に注文した商品のデータとカード情報が送られる。注文を受け取った商店はこれらのデータを復元し、商品の発送とともにカード情報にもとづいてカード会社に料金を請求する。この時、カード番号なども商店に知られてしまう。現在の個人情報流出の主な原因の一つに内部の人間が情報を持ち出すことが挙

げられるので、カード番号などの重要な情報はなるべく商店には知られない方がより安全であるといえる。また、商店がカード会社に料金を請求する際、請求が商店から送ったものであることは電子署名でわかるものの、実際にカード所有者がカードを使用したかどうかの確認はとれない。

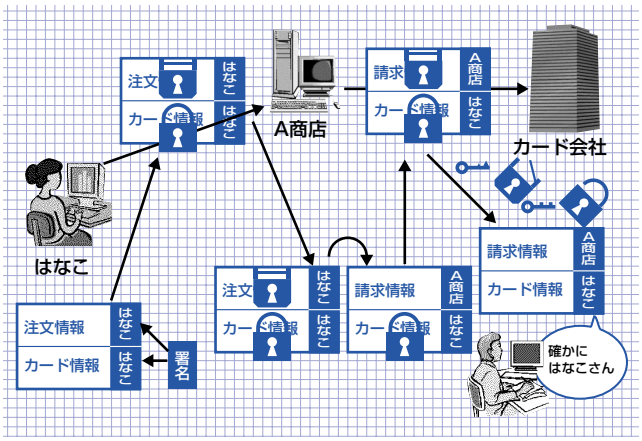


図4　XMLのセキュリティ技術を利用した場合

そこで、XMLを用いた場合のインターネットショッピングの場合、XMLの要素ごとに違ったセキュリティポリシーを適用し暗号化や署名などを行えば、図4のようにカード会社まで安全にカード番号を送信することができ、商店には注文内容のみを知らせるといったことが可能となる。また、個別の要素について電子署名を施すことにより、商店で注文情報の要素を請求情報の要素に変更するなどしても、カード会社へカード情報とユーザの電子署名を送ることができるので、現在問題になっているカード詐欺などを未然に防ぐことが可能である。

このようなXMLのセキュリティに特有な要件を考慮した上で、XMLに対し暗号化処理を行ったり、電子署名を施したりする仕様が、XML-Signature[参考文献2]、XML Encryption、XKMSなどである。これらの簡単な説明は表1にまとめた。

表1　XMLのセキュリティに関連する仕様

仕様の名称	内容
XML-Signature	XMLに電子署名を施す仕様
XML Encryption	XMLの任意の要素に暗号化を施す仕様
XKMS	PKI（公開鍵基盤）利用のための仕様

3.2　Webサービスのセキュリティ

Webサービスは、様々なシステムを連携させることを特徴としたものであり、もし表1のようなXMLのセキュリティ技術を、それぞれのWebサービスに勝手に使用した場合、相互の連携は不可能である。このため、Webサービスのセキュリティに重要なことは、XMLのセキュリティ技術をどのようにWebサービスに適用するかという型（フレームワーク）の標準化である。このフレームワークの標準化は少し時間がかかっていたが、IBM、Microsoft、VeriSignの3社によってOASISに提出されたWS-Securityが、Webサービスのセキュリティ標準となることが有力視されるようになった。またSAML（シングルサインオン）、XACML（アクセス制御）などのXML/Webサービスに関連したセキュリティの仕様も提案され、Webサービスのセキュリティに関する不安が取り除かれようとしている。

3.3　その他のWebサービスの課題

Webサービスにはこの他に、セッション保持の仕様や、トランザクションの扱いなどの仕様が固まっておらず、XML/Webサービスが目指す新しいe-ビジネスの到来には、まだ多少時間がかかると思われる。

3.4　現在のWebサービスの利用例

現時点でのWebサービスは、セキュリティに関する課題が完全に解決されたわけではないので、B2Bの場での利用より、セキュリティをそれほど考慮しなくても良いと思われる部分、つまり社内システムの統合といったイントラネット内での基盤技術（図5）として使用される実例が増えてきた。また、既存アプリケーションのWebサービス化を簡単に行えるソフトウェアが販売されるようになり、既存アプリケーションをWebサービスとして活用できるようになってきた。社内システムの統合にWebサービスを利用する企業の多くは、ただシステムの統合のみを考えているのではなく、将来Webサービスによりビジネスパートナーとシステムを連携させることを想定しているものと思われる。

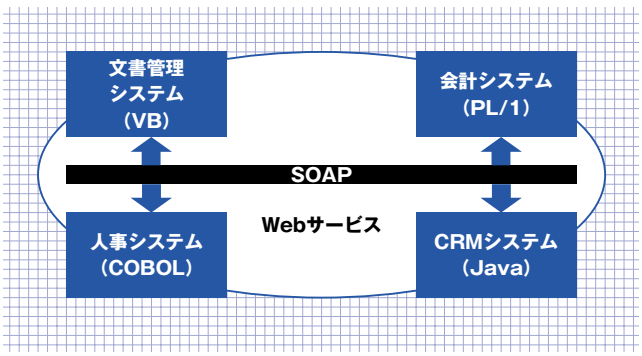


図5　システムの統合基盤としてのWebサービス

4. XML/Webサービスへの取り組み

我々は、XMLやWebサービスに関する情報の提供、コンサルティングなどのほかに、研究で得た技術を利用したソリューションの提供を行い、研究を実用の領域へ転換している。

XMLのセキュリティに関する研究として、電子署名付きXMLの送受信技術についての研究を行った。これは、XML Encryptionの標準化が遅れていたため、暗号化にはSSLを使用することにしたためである。この研究結果を生かした、SOAPを用いたシステムとして実稼動しているものもある。ここでは、XMLによる通信部分にフォーカスを当てて紹介する。

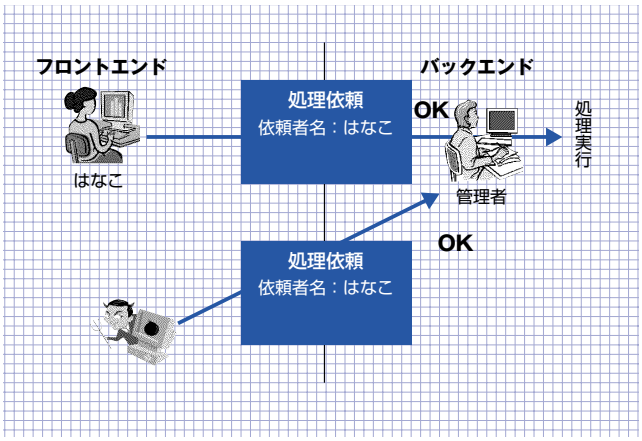


図6　セキュリティを考慮しない場合

図6のアプリケーションの場合、フロントエンドで発行されたXMLの処理依頼書はSSLを使ってバックエンドに送られる。SSLを用いることで、盗聴や改竄などの脅威からシステムを守ることは可能であるが、SSLのクライアント証明書さえ入手できれば、簡単に正規ユーザを騙りバックエンドに処理依頼書を送ることが可能である。これがなりすましであり、バックエンドシステムのオペレーターは正規ユーザと悪意の第三者の区別をつけることができない。

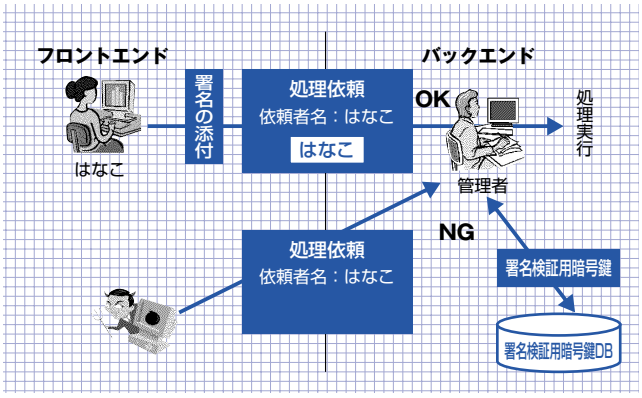


図7　セキュリティを考慮しXML署名を用いた場合

しかし、図7のようにXMLに電子署名を施せば、正規ユーザからの処理依頼書と悪意の第三者からの処理依頼書を簡単に見分けることができ、なりすましを防ぐことができる。

また、この電子署名により、否認のトラブルを未然に防ぐことも可能である。

Webサービスに関しては、SOAPやWSDLを用いたシステムのプロトタイプ（図8）を作成し、それらを用いたシステム開発に備えるとともに、このプロトタイプの中で、前述したWebサービスの課題の一つ、セッションの保持についても挑戦した。このプロトタイプは、ナレッジマネジメントシステムをWebサービスとして作成したものであり、ログイン情報を保持することで、ログインを行わないユーザは他の機能にアクセスしても処理が実行されない仕組みになっている。

また、Webサービスを利用したシステム統合といったニーズが徐々に高まる中、市販のツールではWebサービス化が難しい既存アプリケーションのWebサービス化を実現する方法や、将来Webサービス化を行うことを見据えたアプリケーション開発についても研究を行った。

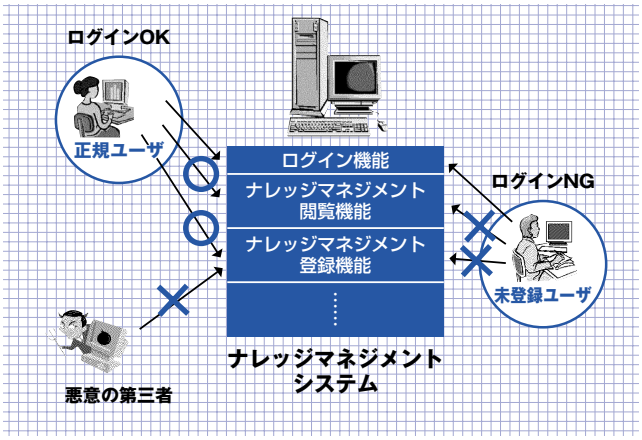


図8　開発したWebサービスのプロトタイプ

5. おわりに

現在のビジネスは変化のスピードが速く、常に変化する情報を迅速に収集し、その情報をビジネスへと生かしていくには変化に柔軟に対応できる特徴を持つXMLとWebサービスが最適であると思われる。また、強固なセキュリティの必要性が増しているなか、XMLによるセキュアな通信、そしてセキュアなWebサービスは必須であるといえる。これまでの研究により、セキュリティを確保したXML/Webサービスを提供できる体制が整った。インテックグループは、常に変化しつづける顧客

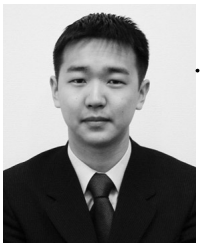
のニーズや市場動向に適合するソリューションの拡充を図っていく考えである。

我々は、2003年中にはWebサービスのセキュリティ標準に関する問題は一通り解決し、2004年、2005年にはその他周辺仕様がほぼ確立され、2006年にはWebサービスを用いたソフトウェア開発がデファクトスタンダードになると考えている。それに従い、前述した取り組みを生かし、今後はそれらを相互に作用させることで、より強固なセキュリティを持ったXML/Webサービスについて研究していきたいと考える。そして、我々はWebサービスを用いてXMLによるビジネスの基盤を支え、セキュアなXMLによるソリューションを提供していけるものと確信している。

参考文献

(1) 嶋本 正, 柿木 彰, 西本 進, 野間 克司, 野上 忍, 亀倉 龍, 松本 健, 福原 信貴,Webサービス完全構築ガイド, 日経BP社, 2001/12/25

(2) Mark Bartel ,John Boyer ,Barb Fox ,Brian LaMacchia,Ed Simon XML-Signature Syntax and Processing, W3C Recommendation, W3C, 2002/2/12



沖花　和夫
Kazuo Okihana

・技術本部付W&G出向
技術部ウェブテクノロジーグループ
・XML、Webサービス関連の調査、研究、開発に従事