XML Consortium

Webサービス・セキュリティの ベスト・プラクティス

2005年12月15日 XMLコンソーシアムDay

XMLコンソーシアム セキュリティ部会
松永 豊 matsu@kabuki.tel.co.jp（東京エレクトロン)

XML Consortium

今日の内容

- Webサービスにおける脅威と 新たなセキュリティ要件
- Webサービス・セキュリティのベストプラクティス
  - セキュリティ対策と導入事例
- Webサービス・セキュリティの基盤
  - アーキテクチャ、処理負荷、認証

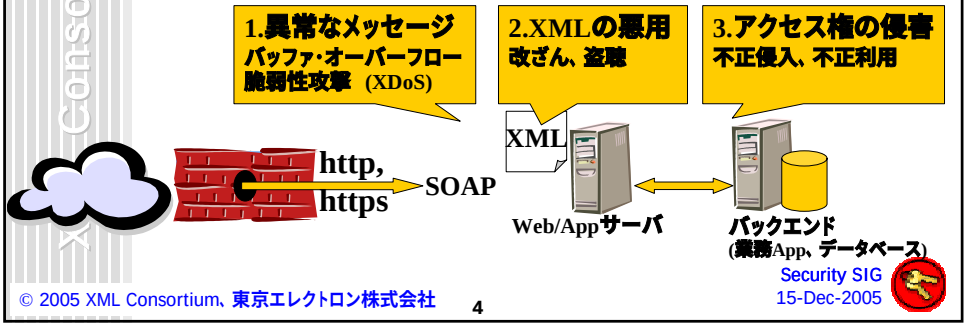
XML Consortium

Webサービスにおける脅威と新たなセキュリティ要件

XML Consortium

Webサービスにおける新たな脅威

- サーバ間の自動処理 (人間のチェックが入りにくい)
- プログラム処理の起動が可能 (SOAP)
- バックエンドのシステムにアクセス可能 (SOAP/http)
- サービスの内容を公開する (WSDL、UDDI)



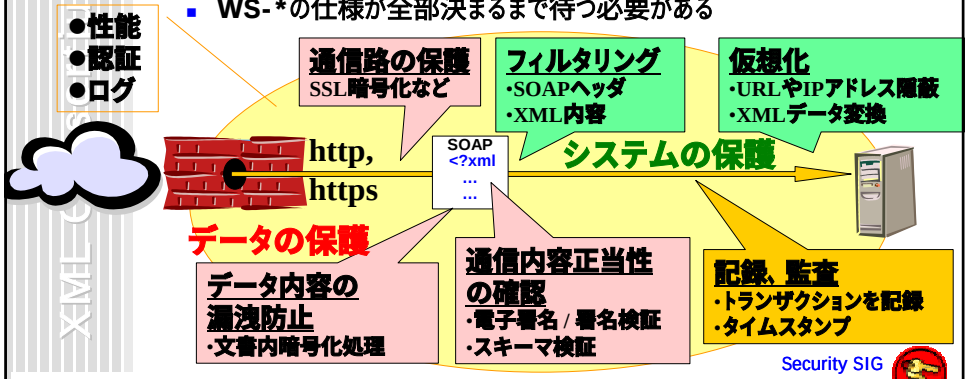
Security SIG
15-Dec-2005

SOAPの危険性

- “Crypto-Gram Newsletter” by Bruce Schneier
  - http://www.schneier.com/crypto-gram-0006.html
  - 「うるさいファイアウォールがアプリケーション間でのコマンドのやり取りを禁止してしまう。
    だからSOAPがコマンドをHTTPの中に隠してファイアウォールに見つからないようにさせてくれる、というわけだ。」
- “Web Services Security” by Bilal Siddiqui
  - http://webservices.xml.com/pub/a/ws/2003/03/04/security.html
  - 「SOAPはWebサービスの機密性を判断できないしユーザ認証、権限認可、アクセス制御を行えない」
  - 「問題の解決には2つの方法がある：
    1. 機密性によって異なるSOAPサーバを立てる（中略）
    2. 2つ目の方法はファイアウォールをXMLとSOAPに
       対応させることだ。（以下略）」

Webサービスに必要なセキュリティ

- 誤解
  - ファイアウォールの内側にはセキュリティは要らない
  - WS-*の仕様が全部決まるまで待つ必要がある



XML Consortium

Webサービス・セキュリティの ベスト・プラクティス

システムの保護 / データの保護
対策技術と事例

ベスト・プラクティス – システムの保護

- XMLのデータ検査をネットワークの入り口で行う

XDoS (XMLサービス拒否攻撃)

Multiple Vendor XML Parser Denial Of Service Vulnerability

bugtraq id	6398
object	
class	Input Validation Error
cve	CVE-MAP-NOMATCH
remote	Yes
local	No
published	Dec 16, 2002
updated	Dec 16, 2002
vulnerable	Apache Software Foundation Axis 1.0 Apache Software Foundation Axis 1.1 beta Apache Software Foundation Xerces C++ 2.1 .0 Apache Software Foundation Xerces Perl 1.7 .0-1

(以下、影響を受けるソフトウェアのリストが続く。Sun One、WebSphere等。以下省略)

- **SecurityFocusに報告されている例**
  - **(説明) XMLパーサーにサービス拒否の脆弱性が存在し、複数のベンダーで利用されているCrimsonまたはXercesで確認されている。**
    攻撃者は、ある方法で作成したメッセージをSOAPインターフェースに送りつけることによりこの脆弱性を利用できる。

XMLパーサーがこれを受け取るとCPU資源を食いつぶし、
システムが他のリクエストに応答できなくなり、
サービス拒否の状況となる。
(以下略)

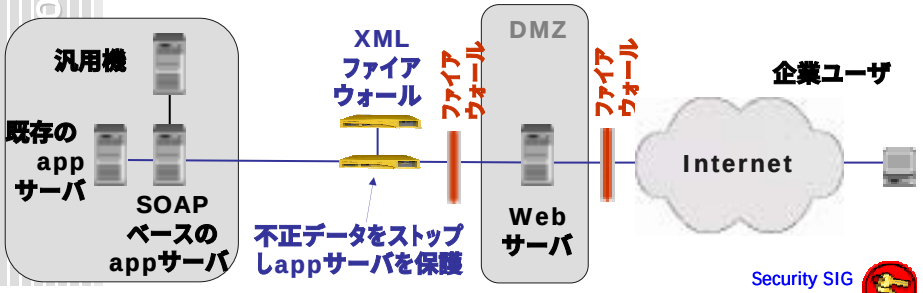
出典: http://www.securityfocus.com/bid/6398/info/

XMLの脆弱性

- [GLSA 200507-15] PHP: Script injection through XML-RPC
  - 2005-07-14 18:00:00 URL: http://www.securityfocus.com/archive/1/405265
- [GLSA 200507-10] Ruby: Arbitrary command execution through XML-RPC
  - 2005-07-10 18:00:00 URL: http://www.securityfocus.com/archive/1/404984
- SUSE Security Announcement: php/pear XML RPC remote code execution
  - 2005-07-07 18:00:00 URL: http://www.securityfocus.com/archive/1/404624
- [GLSA 200507-06] TikiWiki: Arbitrary command execution through XML-RPC
  - 2005-07-05 18:00:00 URL: http://www.securityfocus.com/archive/1/404479
- Adobe Reader 7: XML External Entity (XXE) Attack
  - 2005-06-15 18:00:00 URL: http://www.securityfocus.com/archive/1/402468
- New Python2.2 packages fix unauthorised XML-RPC internals access
  - 2005-02-03 17:00:00 URL: http://www.securityfocus.com/archive/1/389511
- IBM DB2 XML functions overflows (#NISR05012005H)
  - 2005-01-04 17:00:00 URL: http://www.securityfocus.com/archive/1/386096
- IBM DB2 XML functions file creation vulnerabilities (#NISR05012005I)
  - 2005-01-04 17:00:00 URL: http://www.securityfocus.com/archive/1/386097
- Microsoft IIS 5.x/6.0 WebDAV (XML parser) attribute blowup DoS
  - 2004-10-11 18:00:00 URL: http://www.securityfocus.com/archive/1/378179
- Multiple vendor SOAP server (XML parser) denial of service (DTD parameter entities)

事例 - XMLフィルタリング
マサチューセッツ州政府 税金システム

- XML+SOAPを使ったオンライン収受システム
  - 20億ドルの赤字を解消するためにオンライン化
- 既存汎用機をインターネットに接続、Webサービス化
  - ネットワーク管理者がXML/SOAPの内容を検査する要求



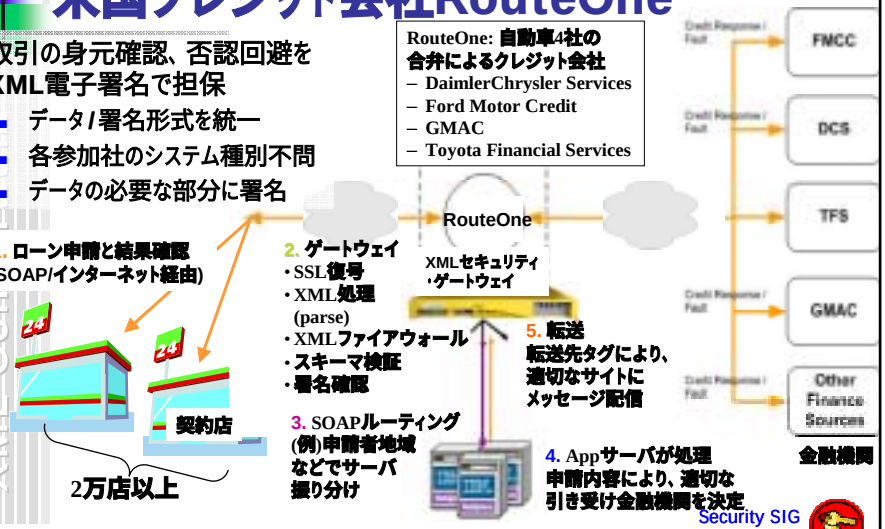
ベスト･プラクティス – データの保護

- 予期しない相手に情報が渡ることを前提に対策
  - ① トランスポート層の保護 (SSL/VPN)
  - ② メッセージ･フィールドの暗号化
  - ③ 全てのメッセージへの署名
  - ④ 全てのメッセージへのタイムスタンプ
  - ⑤ データの仮想化

事例 - XML電子署名
米国クレジット会社RouteOne

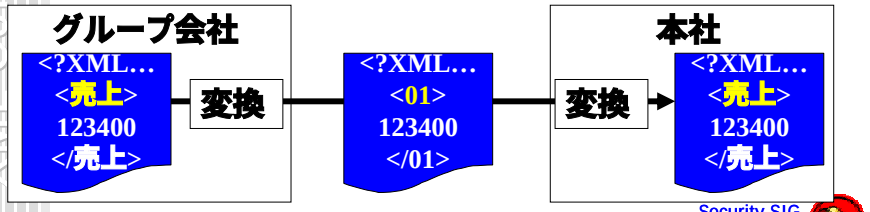
- 取引の身元確認、否認回避を XML電子署名で担保
  - データ/署名形式を統一
  - 各参加社のシステム種別不問
  - データの必要な部分に署名

RouteOne: 自動車4社の合弁によるクレジット会社
- DaimlerChrysler Services
- Ford Motor Credit
- GMAC
- Toyota Financial Services



事例 - データ仮想化
国内化学会社

- XMLはタグを付けてデータを説明するため，漏えいするとデータの中身が分かってしまう。そこで、タグ名を「売上」と明記するのではなく、「01」というように数字の並びに置き換えて明記するようにした。
  - 日経システム構築 2004.9
    「SOAで変化に強いシステムを作る」より



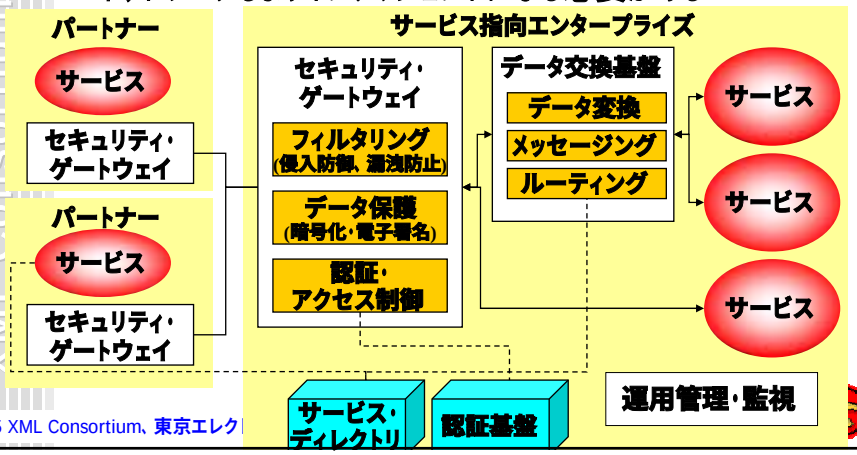
Webサービス･セキュリティの基盤

- アーキテクチャ
- 処理負荷
- 認証

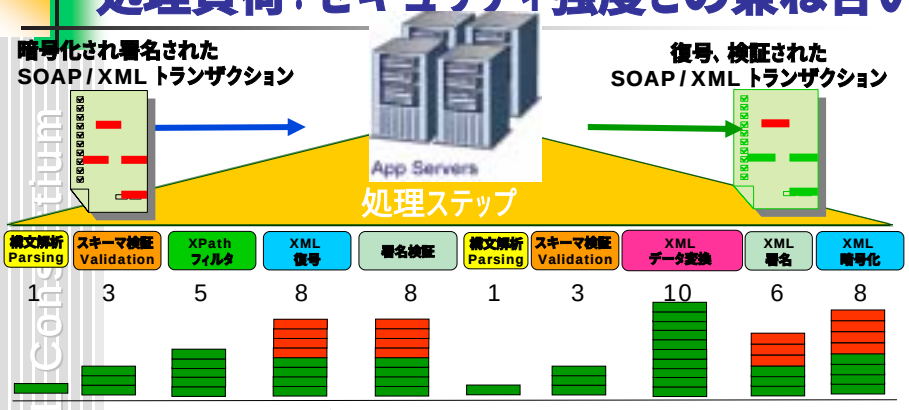
Webサービス･セキュリティの基盤

システム課題
●データ･セキュリティ
●処理負荷
●サービス認証

- SOAを現実のビジネスで活用するには、ネットワークもよりインテリジェントになる必要がある



処理負荷：セキュリティ強度との兼ね合い

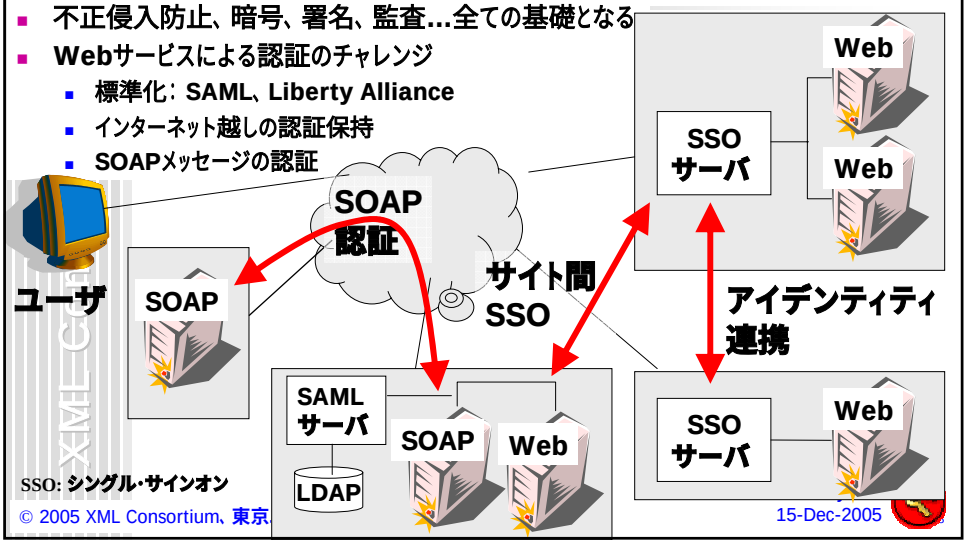


- パフォーマンスがセキュリティのキーとなる
  - 処理能力とセキュリティ機能を天秤にかけられるか?
  - データやユーザ数の拡大に追随できるスケーラビリティ

XML処理負荷
暗号処理負荷

認証: セキュリティの中核

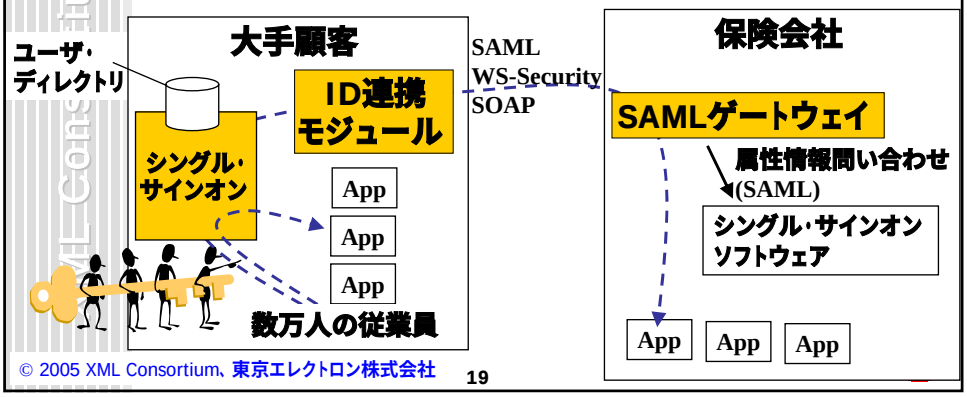
- 不正侵入防止、暗号、署名、監査…全ての基礎となる
- Webサービスによる認証のチャレンジ
  - 標準化：SAML、Liberty Alliance
  - インターネット越しの認証保持
  - SOAPメッセージの認証



SSO: シングル・サインオン

事例 - XML認証(SAML)
米国保険会社での顧客認証

- 顧客サービスのためのエクストラネット
- 顧客のユーザ・ディレクトリは一箇所で管理
- 送信中の情報は暗号化・署名して保護



What's Next?

- 暗号化時のスキーマ検証方法を検討

```
<MemberList>
 <Member>
  <Name>松山</Name>
  <Address>石川県</Address>
 </Member>
</MemberList>

<xsd:element name="Name"
 type="xsd:string" minOccurs="1"
 maxOccurs="1">
```

●対応できる標準規格は
無さそう
●おススメの方法を
まとめられないか?

```
<MemberList>
 <Member>
  <enc:EncryptedData Id="ED01" MimeType="..."
   Type="http..." xmlns:xenc="http...">
   <enc:EncryptionMethod Algorithm="http...">
    <enc:KeySize>192</enc:KeySize>
   </enc:EncryptionMethod>
   <ds:KeyInfo xmlns:ds="http...">
    <ds:KeyName>john</ds:KeyName>
   </ds:KeyInfo>
   <enc:CipherData>
    <enc:CipherValue>Va2tn...
    </enc:CipherValue>
   </enc:CipherData>
  </enc:EncryptedData>
  <Address>石川県</Address>
 </Member>
</MemberList>
```

Security SIG
15-Dec-2005

まとめ

- Webサービスのセキュリティは新たな課題
  - インターネットの時と同様に、新たなセキュリティが必要
  - End-to-endでの設計、検討、検証が必要
    - サーバ、LAN、DMZ、ファイアウォール、インターネット…
  - WS-Securityはデータ・セキュリティをカバー
    → そのほかにシステム保護、認証に留意
- 指針
  - 「便利になると危険が増える」ことを理解し
    必要な対策を把握する
  - 標準規格は動向をウォッチして「重要な規格」を見極める

Webサービス・セキュリティの
ベスト・プラクティス

XMLコンソーシアム セキュリティ部会
松永 豊 matsu@kabuki.tel.co.jp
(東京エレクトロン株式会社)