XML Consortium

～ 第5回 XMLコンソーシアムWeek ～

セキュリティ部会の取り組み
Webサービスを支えるセキュリティ技術

2006年5月22日

XMLコンソーシアム セキュリティ部会
岡村 和英（株式会社ネット・タイム）

アジェンダ

- セキュリティ部会の取り組み
  - 活動の目的、内容、実績
- Webサービスを支えるセキュリティ技術
  - セキュリティ技術マップ
  - OASIS Web Services Security

セキュリティ部会活動要綱

- 活動の目的
  - XMLセキュリティ技術のビジネスシステムへの適用に向けて、規格の調査・翻訳・解説を行ない、また、アプリケーションモデルの検討・試作を通じてシステム構築における様々な問題点の解決方法や具体的な実装ノウハウを蓄積すると共に、それらの成果物を公開することによりセキュリティ技術の普及を促進させるべく活動を行なう。
- 活動の内容
  - セキュリティ規格の調査、解説
  - セキュリティ規格文書の翻訳
  - ビジネス適用事例の調査、収集
  - 開発ツール、ミドルウェア等の調査および比較検討
  - モデルの構築とアプリケーションの検討
  - 試作による技術検証 (他の部会との連係による実証実験)

セキュリティ部会活動要綱 (Cont.)

- 活動の方法
  - メンバー全員による月例ミーティング、WG別ミーティングの開催
  - メーリングリストによる日々の情報交換、ディスカッション
  - 参加メンバー個人によるテーマ別の調査報告の実施
  - 関連製品の紹介セミナーの開催
  - XMLコンソーシアム他部会および他団体との協調による普及推進
  - 翻訳文書、Webページ、雑誌記事、出版など外部向けコンテンツの作成
  - XMLコンソーシアムDay、XMLコンソーシアムWeekでの活動報告

これまでの活動実績 (1)

- ２００１年度
  - **基盤技術部会 共通基盤WG セキュリティSWG**
    - 図解ＸＭＬ（セキュリティ編）
    - ケーススタディを通じた、セキュリティ関連XML規格の調査、解説
    - Ｗｅｂサービス技術解説書への参画
  - **応用技術部会 セキュリティWG**
    - XKMSサーバ、クライアントの開発と、XML-Signatureを用いた電子署名システムの構築
- ２００２～２００３年度
  - **応用技術部会 セキュリティWG**
    - セキュリティ関連XML規格の調査、解説
    - XKMS、XML-Signature、XML Encryptionを用いた旅行発注システムの構築
    - SAMLオーソリティ、SAMLリクエスタの実装と、SSOシステムの構築
    - XML-Signature、XML Encryption、SAMLを用いた電子委任状システムの構築
- ２００４年度～
  - **セキュリティ部会**

これまでの活動実績 (2)

- ２００４年度
  - 標準規格文書の翻訳、公開
    - OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) 日本語訳
      http://www.xmlconsortium.org/wg/sec/wss.html
  - 標準規格及び関連技術の調査、解説
    - Web Services Security
    - SAML 2.0
    - セキュリティ関連XML標準技術規格マップの更新
  - 開発ツール、ミドルウェア等の調査、比較
    - WS-Security 2004の対応状況

2005年度の活動実績

- 標準規格文書の翻訳
  - **OASIS Web Services Security 1.0**
    - **SOAP Message Security 1.0 (WS-Security 2004) Errata 1.0** 日本語訳
    - **Username Token Profile 1.0** 日本語訳
    - **Username Token Profile 1.0 Errata 1.0** 日本語訳
    - **X.509 Certificate Token Profile 1.0** 日本語訳
    - **SAML Token Profile 1.0** 日本語訳
  - 翻訳用語集の拡充
- 標準規格及び関連技術の調査、解説
  - **WSS 1.0概要**
  - **XACML 2.0の概要**
  - **Webサービスのベストプラクティス**
  - **Webサービスポリシーの動向と仕様解説**
  - **WS-Trust概要**
  - **OASIS WS-Security標準について**

2005年度の活動実績 (Cont.)

- XMLコンソーシアムセミナー
  - **オープンなWebアプリケーション環境のためのセキュリティ最新動向 - 認証技術編　　2005年9月13日 (火)**
    - **Webアプリケーション環境のための認証技術：イントロダクション**
      (XMLコンソーシアム セキュリティ部会)
    - **Liberty Alliance Project概要**
      (LibertyAllianceProject Japan-SIG Co-Chair 五味秀仁様)
    - **製品紹介**
      - **Sun Java System アイデンティティ管理製品 (サン・マイクロシステムズ)**
      - **DataPower XS40 XMLセキュリティ・ゲートウェイ (東京エレクトロン)**
      - **ActiveGlobe WebOTX ／ WebSAM SECUREMASTER (日本電気)**
      - **Oracle Fusion Middleware (日本オラクル)**
- 外部団体主催セミナーでの講演
  - **「製造業XMLフォーラム2005」　　2005年6月7日 (火)**
    - **“暗号化対策” その手法と効果について**
  - **「JavaOne Tokyo 2005」　　2005年11月10日 (木)**
    - **Webサービスのベストプラクティス**

2005年度の活動実績 (Cont.)

- sPlat プロジェクト
  - Webサービスにおける暗号化XMLデータの取り扱いに伴なう問題点とその対策についての検討
    http://www.xmlconsortium.org/release/pdf/px060406-security-project-final2.pdf
    - 暗号化XMLデータの妥当性検証とデータバインディング
  - Webサービス実証部会との合同プロジェクト
  - 第1次成果報告

「暗号化XMLデータ利用技術についての課題と対策」
第5回 XMLコンソーシアムWeek 3日目 Web 2.0 Day (2)
5月24日 (水) 14:15～
於 日立製作所 (大森) 大森第二別館 1階講堂

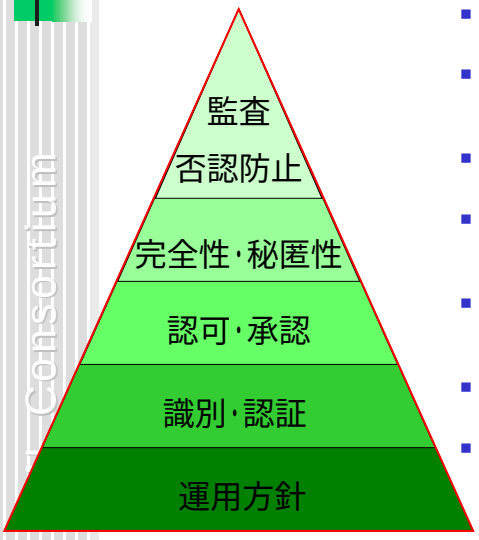
2006年度の活動予定

- 標準規格文書の翻訳
  - WSS 1.1 ?
  - WS-Policy ?
  - SAML 2.0 ?
    - Technical Overview、Executive Overview
  - 翻訳用語集の拡充
- 技術解説書の作成
  - セミナー等での発表スライドをベースに解説文を加え、文書化する。
- 部会内セミナー
  - 部会ミーティングにおける勉強会の実施
- sPlat プロジェクト

Webサービスを支えるセキュリティ技術

- セキュリティ技術マップ
  - Webサービスに求められるセキュリティ要件
  - セキュリティ関連XML規格一覧
  - 標準化の状況
- OASIS Web Services Security

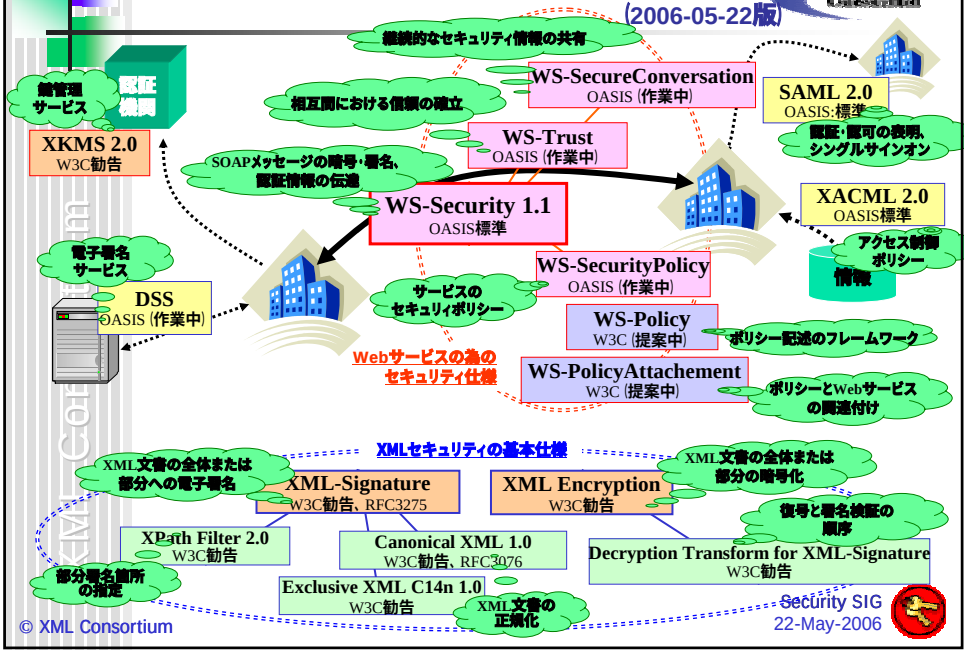
Webサービスに求められるセキュリティ要件



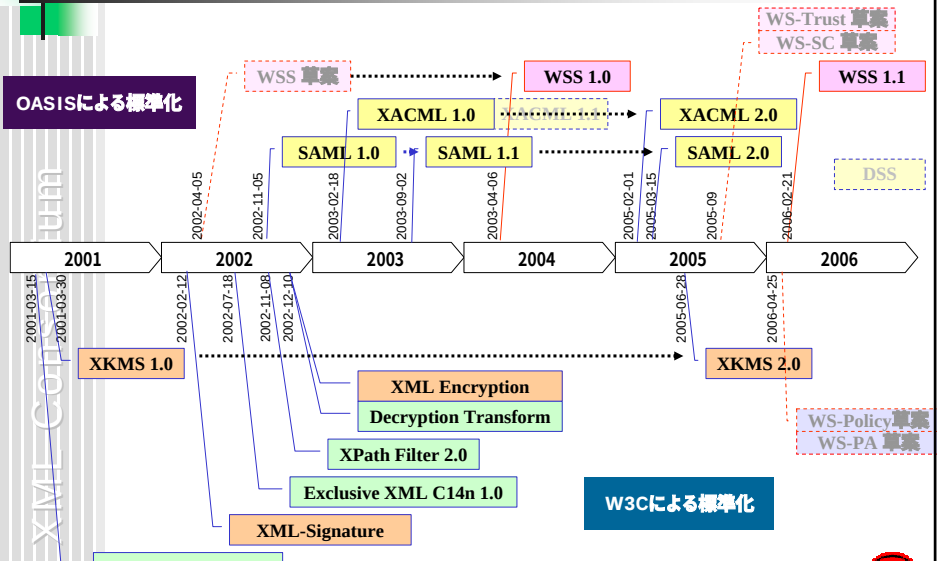
- 識別 (Identification)
  - サービスの相手を識別する。
- 認証 (Authentication)
  - 識別した相手が、その本人であることを証明する。
- 認可 (承認) (Authorization)
  - 操作の権限を判断する。
- 完全性 (Integrity)
  - 送信されたメッセージと受信したメッセージが同一であることを証明する。
- 秘匿性 (Confidentiality)
  - 送信されたメッセージが盗み読みされないことを保証する。
- 監査 (Accounting)
  - サービスの利用状況を事後確認する。
- 否認防止 (Non-repudiation)
  - 受信されたメッセージが、送信されたメッセージであることを証明する。

セキュリティ関連XML規格一覧

(2006-05-22版)



標準化の状況



Webサービスを支えるセキュリティ技術

- セキュリティ技術マップ
- OASIS Web Services Security
  - WS-Security仕様の目的
  - 提供する機能と手段
    - セキュリティトークン
    - 電子署名
    - 暗号

仕様書構成

- Web Services Security:

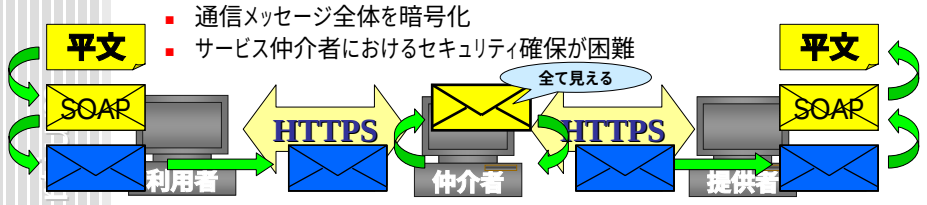
種類	仕様名	V1.0	V1.1
コア	SOAP Message Security (WS-Security 2004)	○	○
トークン・プロファイル	Username Toke Profile	○	○
	X.509 Certificate Token Profile	○	○
	SAML Token Profile	○追加	○
	Rights Expression Language (REL) Token Profile	○追加	○
	Kerberos Token Profile		○
他のプロファイル	SOAP Messages with Attachments (SwA) Profile		○

WS-Security仕様の目的

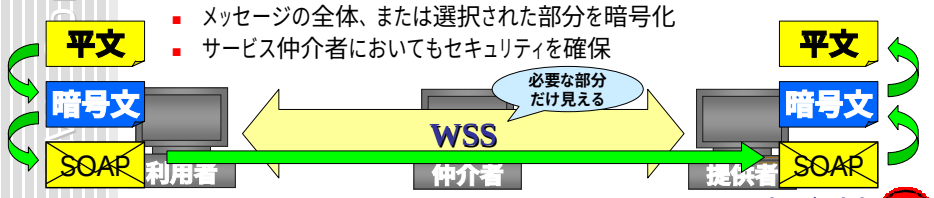
- Webサービスをセキュアにするために、その基本プロトコルであるSOAPを機能拡張する標準を作り、End-to-Endの完全性と秘匿性を実現する。
  - Webサービスのメッセージ通信が、複数のポイントを経由して行われる場合でも、セキュアな通信サービスが確保される。
- 既存のセキュリティ技術を統一的に使う仕組みを提供する。
- 幅広いセキュリティ・モデルのサポート
  - 複数のセキュリティ・トークン形式
  - 複数の信頼ドメイン
  - 複数の署名形式
  - 複数の暗号技術

SSLとの違い

- SSL
  - トランスポート層による、「Point-to-Point」のセキュリティ
  - 通信メッセージ全体を暗号化
  - サービス仲介者におけるセキュリティ確保が困難

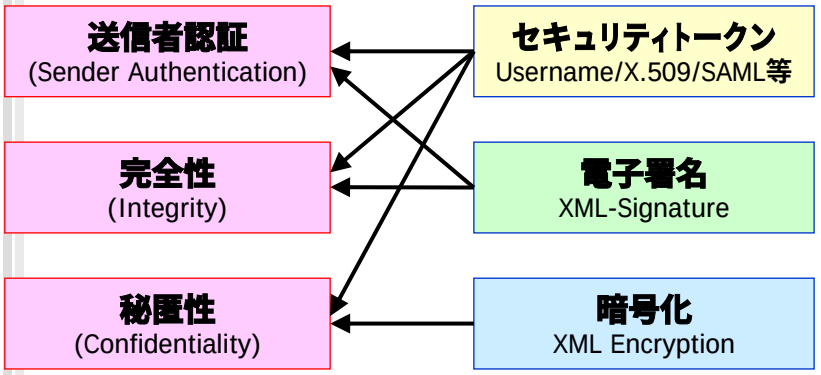


- WSS
  - メッセージコンテントによる、「End-to-End」のセキュリティ
  - メッセージの全体、または選択された部分を暗号化
  - サービス仲介者においてもセキュリティを確保



WSSが提供する機能と手段

- ＳＯＡＰメッセージに対するセキュリティ拡張



Securityヘッダ

- セキュリティ関連情報は**<wsse:Security>**ヘッダ・ブロックに記述

```
<S:Envelope>
  <S:Header>
    <wsse:Security>
      署名関連情報
      暗号化関連情報
      セキュリティトークン
      タイムスタンプ
    </wsse:Security>
  </S:Header>
  <S:Body>
  ...
  </S:Body>
</S:Envelope>
```

セキュリティ・トークン

- 申告の集まり(1つ以上)を表現
- 署名・暗号化の「鍵」を示すためにも利用される

- 利用者名トークン
  - 利用者名の提示
  - **<wsse:UsernameToken>**要素で指定
- バイナリ・セキュリティ・トークン
  - バイナリ符号化された（非XML形式の）セキュリティ・トークンの提示
    - X.509証明書、Kerberosチケットなど
  - **<wsse:BinarySecurityToken>**要素で指定
- XMLトークン
  - XML形式のセキュリティ・トークンの提示
    - SAMLアサーション、RELライセンス など
  - **<wsse:Security>**ヘッダ・ブロックに直接挿入

トークン参照

- どこかに存在するセキュリティ・トークンを参照
- **<wsse:SecurityTokenReference>**要素で指定
  - **<ds:KeyInfo>**の子要素としても利用可

- 直接参照
  - URIを利用してトークンを直接参照
  - **<wsse:Reference>**子要素で指定
  - 同一文書内のトークンはID属性を利用
- 鍵識別子
  - トークンを表現するバイナリ符号化された鍵識別子でトークンを参照
  - **<wsse:KeyIdentifier>**子要素で指定
- 鍵名
  - セキュリティ・トークンの名称で参照
  - **<ds:KeyName>**要素を利用
- 埋め込まれた参照
  - 任意のセキュリティ・トークンを直接埋め込む
  - **<wsse:Embedded>**子要素で指定

電子署名

- XML-Signatureの**<ds:Signature>**を**<wsse:Security>**ヘッダ・ブロックで利用

```
<S:Envelope>
  <S:Header>
    <wsse:Security>
      <wsse:BinarySecurityToken ...>
        ...
      </wsse:BinarySecurityToken>
      <ds:Signature>
          鍵情報(セキュリティ・トークン)への参照
          署名対象への参照
      </ds:Signature>
    </wsse:Security>
  </S:Header>
  <S:Body wsu:Id="body">
  ...
  </S:Body>
</S:Envelope>
```

署名情報

署名対象

暗号化(1)

- XML Encryptionの**<xenc:ReferenceList>**を**<wsse:Security>**ヘッダ・ブロックで利用
- 暗号化されたデータは**<xenc:EncryptedData>**で表される

```
<S:Envelope>
  <S:Header>
    <wsse:Security>
      <xenc:ReferenceList>
        <xenc:DataReference URI=... />
      </xenc:ReferenceList>
    </wsse:Security>
  </S:Header>
  <S:Body>
    <xenc:EncryptedData Id="...">
      ...
    </xenc:EncryptedData>
  </S:Body>
</S:Envelope>
```

暗号化された場所のリスト

暗号化されたデータへの参照

暗号化されたデータ

鍵情報(への参照)も

暗号化(2)

- XML Encryptionの**<xenc:EncryptedKey>**を**<wsse:Security>**で利用
- 暗号化されたデータは**<xenc:EncryptedData>**で表される

```
<S:Envelope>
  <S:Header>
    <wsse:Security>
      <xenc:EncryptedKey>
        ...
        <xenc:ReferenceList>
          ...
        <xenc:ReferenceList>
      </xenc:EncryptedKey>
    </wsse:Security>
  </S:Header>
  <S:Body>
    <xenc:EncryptedData Id="...">
      ...
    </xenc:EncryptedData>
  </S:Body>
</S:Envelope>
```

暗号化に利用した対称鍵

鍵情報(への参照)

暗号化されたデータへの参照

暗号化されたデータ

署名と暗号化の順序

- 処理した要素を順に前に挿入
  - 署名 ⇨ 暗号化

```
<wsse:Security>
    <xenc:EncryptedKey>….</xenc:EncryptedKey>
    <ds:Signature>….</ds:Signature>
</wsse:Security>
```

  - 暗号化 ⇨ 署名

```
<wsse:Security>
    <ds:Signature>….</ds:Signature>
    <xenc:EncryptedKey>….</xenc:EncryptedKey>
</wsse:Security>
```


まとめ

- XML-Signature、XML Encryptionという基本仕様だけではなく、WSSやSAMLの様なWebサービスを想定した応用仕様についてもほぼ標準化が完了し、また、各ベンダー参加による互換性確認も行われており、標準仕様に基づく「安全な」Webサービスの構築・提供が可能なフェーズに到達している。

- 標準仕様を正しく理解し、より柔軟で価値の高いシステム構築を行なうためには、日本語訳文書の存在も重要である。