XML Consortium

ID連携を実現するSAML 2.0 と ID管理の最新動向

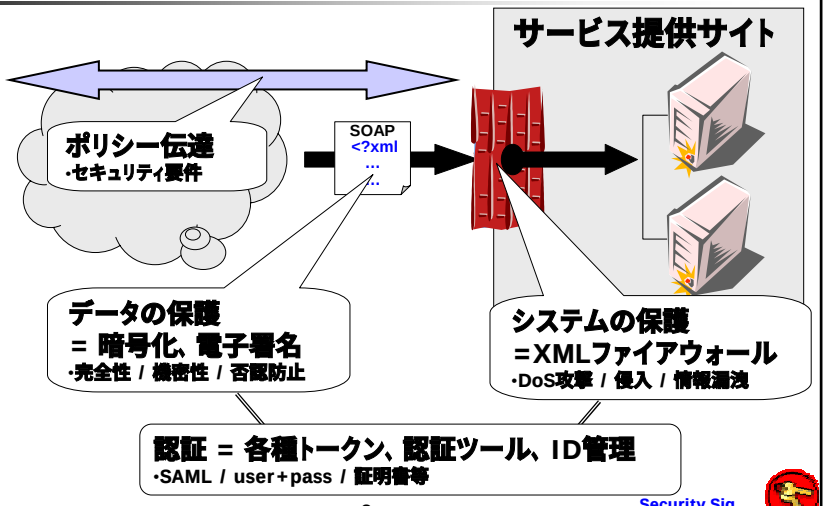
2007年5月21日
XMLコンソーシアムWeek

セキュリティ部会 松永 豊
(東京エレクトロン デバイス)

注: この前回にあたる内容は、2005年6月7日XMLコンソーシアムWeekでの発表「インターネットを変える認証技術 SAML 2.0」

XML Consortium

Webサービスのセキュリティ

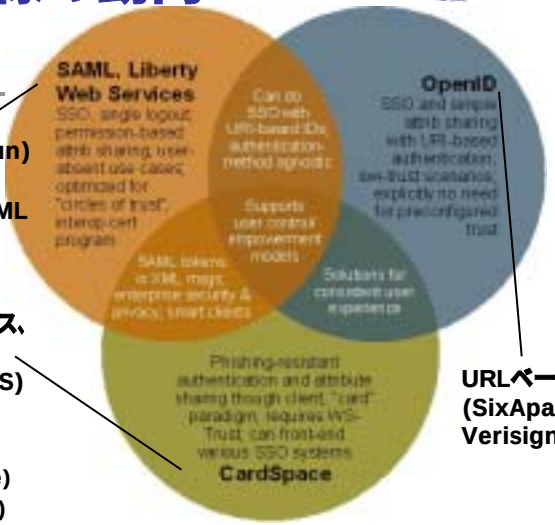


ID管理

- インターネット上でのID管理が急速進化中
- 新たな利用価値 - Web 2.0など
- 深刻化する問題
  - スパム、フィッシング
  - クロスサイト・スクリプティング
  - pump and dump
  - ID盗難 / 不正利用
- ID管理を握れば電子マネーに匹敵する利権

ID管理仕様の動向

XMLベースのトークン
(OASIS, Liberty / Sun)
•OpenLiberty
•Shibboleth OpenSAML
•OpenSSO



「card」ベース、
WS-Trust
(MS, OASIS)

URLベース
(SixApart,
Verisign)

- その他IDメタシステム
  - Higgins (eclipse)
  - Yadis (SixApart)

Sun Microsystems社 Eve Maler氏による図
http://www.xmlgrrl.com/blog/archives/2007/03/28/the-venn-of-identity/

WS-Federation?

SAML：インターネットを変える認証技術

- 2005/6月XMLコンソーシアムWeekで概要紹介
  - Technical Overview Draft04ベース
  - SSOプロファイル中心
- 解説書：Technical Overview
  Committee Draft 01 2007/3/13
  - 概要(1, 2, 3, 4.2, 4.4)
  - 4.5 Privacy in SAML
  - 5.3 Single Logout Profile
  - 5.4 ...Federated Identities
  - 6. ...SAML for Use in Other Frameworks

SAML：概要と利用分野

- SAMLとは
  - SAMLはXMLベースのセキュリティ情報伝達技術
    - 認証、属性、認可
  - アサーションと伝達プロトコルを定義
    … ドメインを超えてセキュリティ情報を共有
- 利用分野
  - シングル・サインオン：特にMDSSO
  - ID連携 (Federated Identity)
  - Webサービス同士の認証

標準化動向

- OASIS Security Services (SAML) TCにて仕様策定
- SAML V1.0: 2002年11月5日 OASIS標準
- SAML V1.1: 2003年9月2日 OASIS標準
- SAML V2.0: 2005年3月15日 OASIS標準
- その後も周辺仕様が続々と策定されている

High-Level SAML Use Cases

- SAMLでの登場人物
  - System entity
    - Asserting Party (Authority, responder)
    - Relying Party (requester)
  - 実際のシステムではSAML role (役割)
    - SSOでは、IdPとSP
- Web SSO Use Case
- Identity Federation Use Case

Web Single Sign-On Use Case

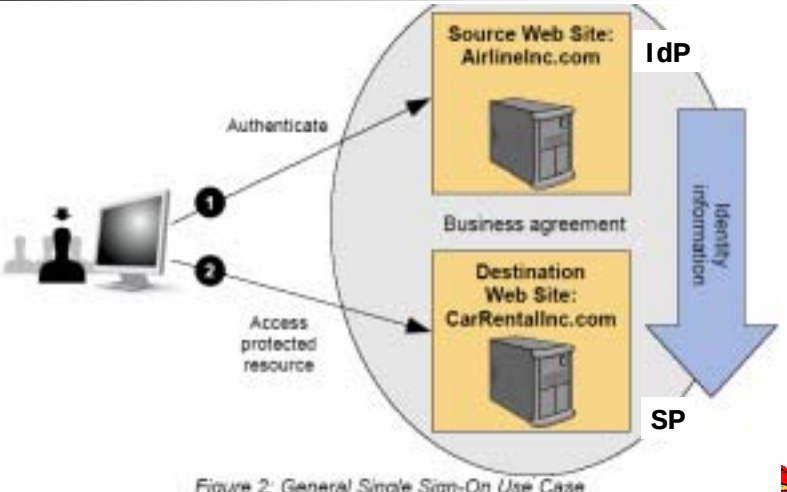


Figure 2: General Single Sign-On Use Case

Identity Federation Use Case

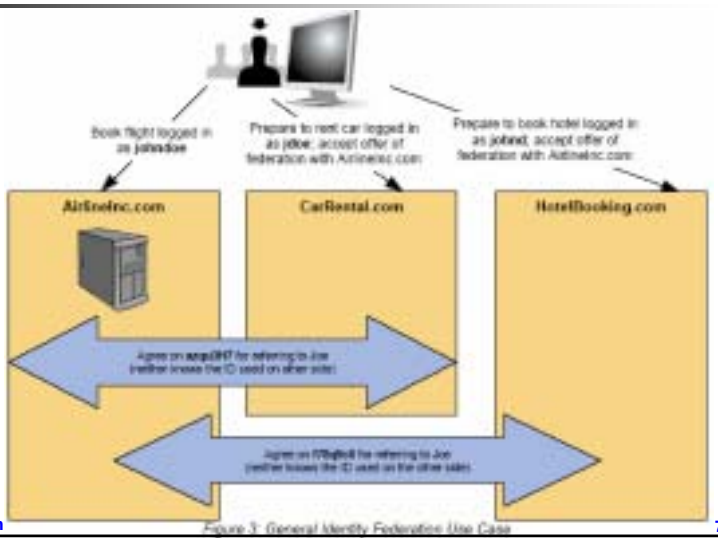


Figure 3: General Identity Federation Use Case

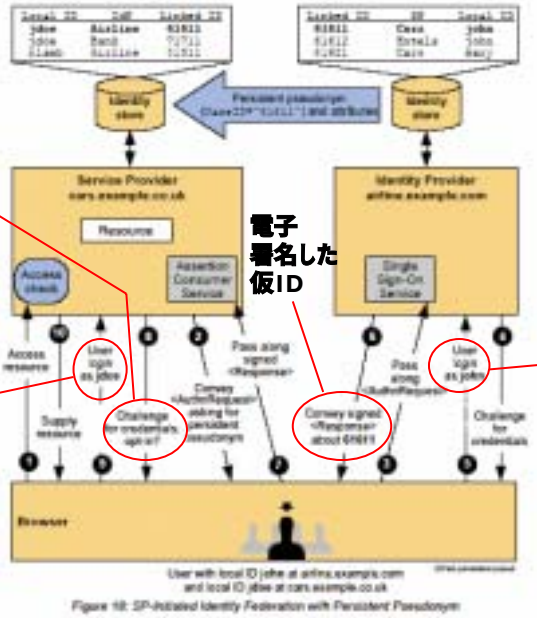
プロファイル

- SAML 2.0のプロファイル
  - Webブラウザsso (SP開始とIdP開始)
  - ECP (Enhanced Client and Proxy)
  - IdP Discovery
  - Single Logout
  - Name Identifier Management
  - Assertion Query/Request
  - Artifact Resolution
  - Name Identifier Mapping
  - SAML Assertion
- Identity Federation (ID連携)

・下線付きはTechnical Overviewでとりあげられている項目

ID連携

永続的なシュードニム (仮ID)
Persistent Pseudonym



連携が無ければログイン処理

こちらではjdoeとして扱われる

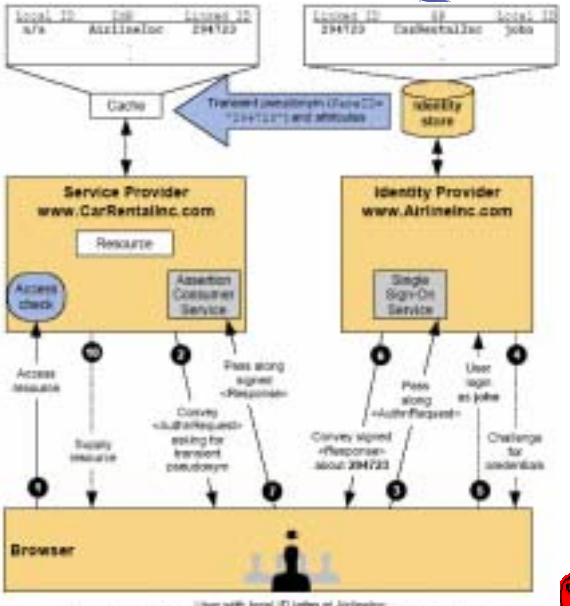
電子署名した仮ID

- 「john」はSPには渡らない

johnとしてログイン

ID連携

一時的なシュードニム (仮ID)
Transient Pseudonym



- SPではID管理を行わないケース

SAMLのプライバシーとセキュリティ

- SAMLはプライバシーを確保する仕組みを提供
  - IDが露出しない仕組み – シュードニム (pseudonym = ペンネーム, 仮名)
  - ワンタイムのID
  - 認証コンテキスト – 必要最低限の情報を伝達
- セキュリティを保つためには、注意が必要
  - SSL
  - 双方向認証
  - 電子署名 (XML Digital Signature)

まとめ

- SAMLは ①Webサービスの一元的な認証と、②インターネット・ワイドのSSO、を実現する、XMLベースのセキュリティ情報伝達技術
- SAML 2.0によって ①ID連携の強化、②プライバシーの考慮
- 技術の成熟に伴い、メーカーの関与が活発化
  - 製品やツールの充実
  - 仕様の統合、発展、競争
- 次は実用サービスのステップ→引き続きウォッチします

補足

ドキュメント・セット

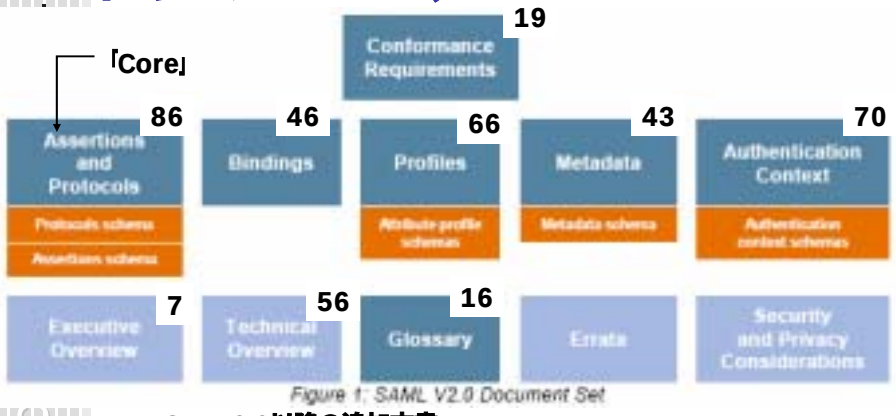


Figure 1: SAML V2.0 Document Set

SAML2.0以降の追加文書

- SAML Metadata Extension for Query Requesters.
- SAML Attribute Sharing Profile for X.509…
- SAML V1.x Metadata
- SAML XPath Attribute Profile
- SAML Protocol Extension for Third-Party Requests

SAML TC最近の文書

- 3/1 SAMLv2.0 HTTP POST “SimpleSign” Binding CD 01
- 3/13 SAML V2.0 Technical Overview CD 01
- 4/1 SAML V2.0 X.500/LDAP Attribute Profile Working Draft 02
- 4/12 SAML V2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems Working Draft
- 4/13 Identity Provider Discovery Service Protocol and Profile CD 01
- 5/7 SAML V2.0 Deployment Profiles for X.509 Subjects CD 01

SAML - 基本的なコンセプト

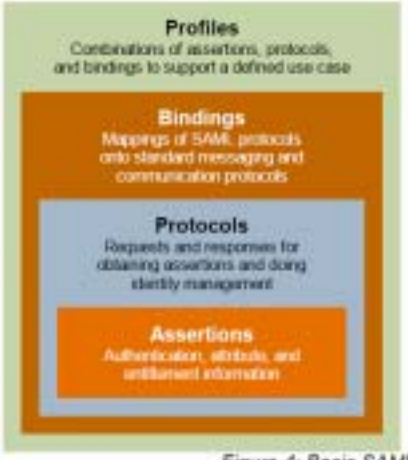


Figure 4: Basic SAML Concepts

ID、バインディング、エンドポイント、証明書、暗号鍵…

Single Logout Profile (SP開始)

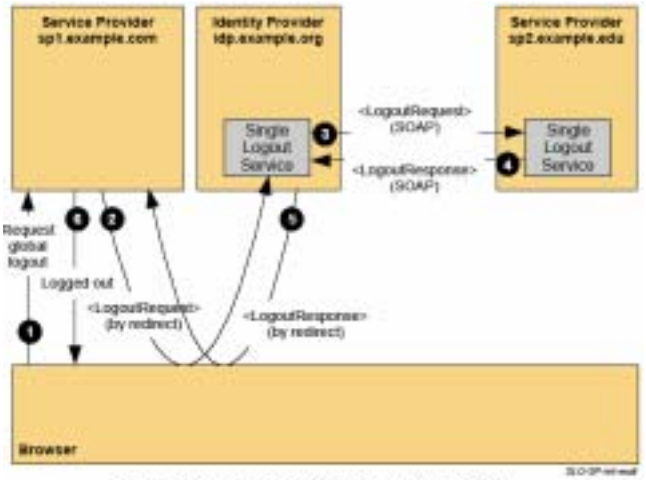


Figure 16: SP-initiated Single Logout with Multiple SPs