XML Consortium

インターネットを変える認証技術
SAML 2.0

2005年6月7日
XMLコンソーシアムWeek

セキュリテ部会 松永 豊
(東京エレクトロン株式会社)

SAML：
インターネットを変える認証技術

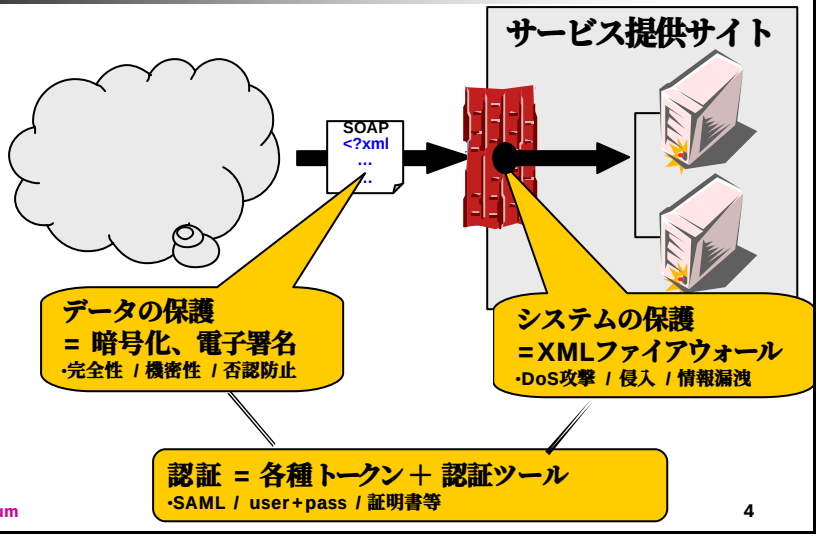
- SAML V2.0がLiberty Allianceの活発な活動に融合
- 認証プロトコルとして数万人規模の実運用システムを含む実績ができてきた

有機的なインターネット・ワイドのサービス構築を実現する為の重要技術

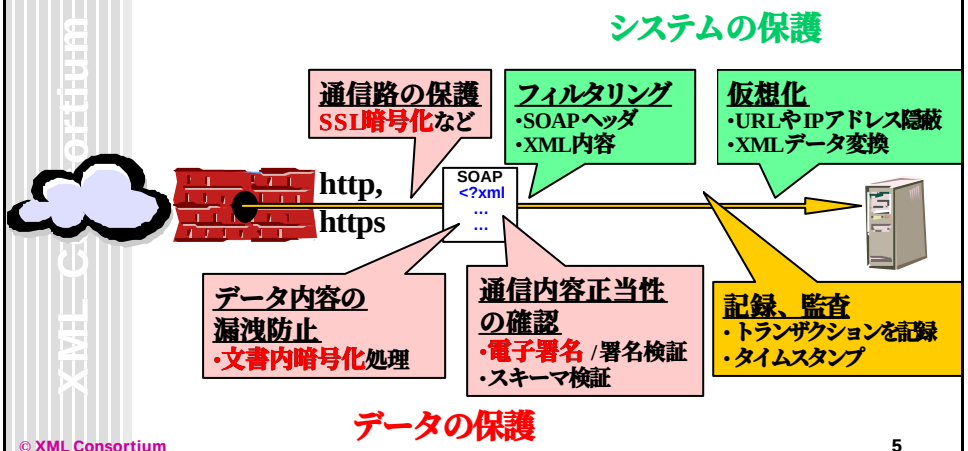
SAML :概要と利用分野

- SAMLとは
  - SAMLはXMLベースの認証情報伝達技術
  - 認証情報(アサーション)の記述と伝達プロトコルを定義
- 利用分野
  - 利用分野1：Webサービスの認証
    SOAPメッセージの認証機能を提供する
  - 利用分野2：Webサイトでの認証をより柔軟に
    サイト間や異種環境などでのSSO(シングルサインオン)、
    アイデンティティ連携 (Federated Identity)

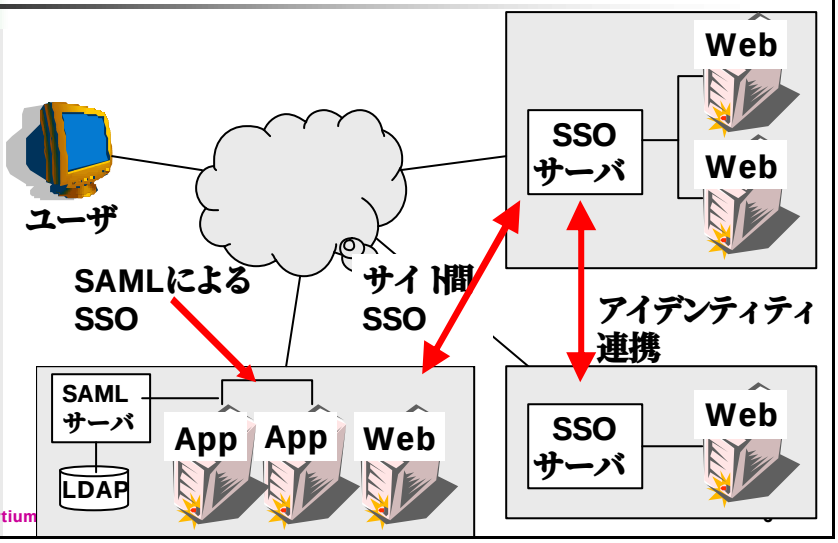
Webサービスのセキュリティ



データ保護とシステムの保護



Webサイトのシングルサインオン



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

SAML V2.0の特徴

- Liberty Alliance仕様との統合
  - ID-FF (Identity Federation Framework) V1.2を取り込んだ
    → アイデンティティ連携
- 他の仕様との連携利用について記述
  - WS-Security
  - XACML
- 暗号処理関連機能の強化：暗号化、電子署名

SAML V2.0の文書

- Assertions and Protocols (コア仕様) 86ページ
  - アサーションの書式と、やり取りのプロトコル
- Authentication Context (認証コンテキスト)70ページ
- Profiles (プロファイル:場合ごとの利用方法) 66ページ
  - SSO関連、アーティファクト解決、アサーション問い合わせ、名前識別子マッピング、SAML属性、等
- Metadata 43ページ
  - ID、バインディング、エンドポイント、証明書、暗号鍵などの情報記述
- Bindings 46ページ
  - プロトコルに対するバインディング: SOAP、PAOS、HTTPリダイレクト、HTTP POST、HTTPアーティファクト、SAML URI
- Conformance Requirements 19ページ
- Glossary (用語集) 16ページ

SAML V2.0での新機能

- シュードニム (Pseudonyms) : 一意で無いほぼランダムなID
- ID情報管理 - 2つの組織間でシュードニムを作成・管理
- メタデータ
  - SAMLシステムの実装を容易にするための情報管理
  - SSOにおけるIDプロバイダ、サービス・プロバイダ
  - 属性のAuthorityとRequester
- 暗号化
- 属性プロファイル: ベーシック X.500/LDAP、UUID、XACML
- セッション管理 – シングル・ログアウト
- モバイル機器、プライバシー
- IDプロバイダの発見

SAML V2.0 相互接続実験

参加社名	役割
eGov/Enspier	eAuthentication Portal
Computer Associates	idP SP
DataPower	SP
Entrust	idP SP
NTT	idP SP
OpenNetwork	idP SP
Oracle	idP
RSA Security	idP SP
Sun	idP SP
Symlabs	idP SP
Trustgenix	idP SP

- RSA Conference (2005年2月)における相互接続実験
- idP: Identity Provider
- SP: Service Provider
- 相互にシングルサインオンとシングルログアウトを実演

SAML V2.0の解説書

- SAML V2.0 Technical Overview
  - 1 Introduction
  - 2 SAML Use Cases
  - 3 SAML Architecture
  - 4 Profiles
  - 5 Documentation roadmap
  - 6 Comparison Between SAML V2.0 and SAML V1.1
  - 7 References
  - 現在、Working Draft 04, 10 April 2005を公開

SAMLの構造

ID情報通信のプロトコルとして機能

WS-Securityの中ではトークンとして利用

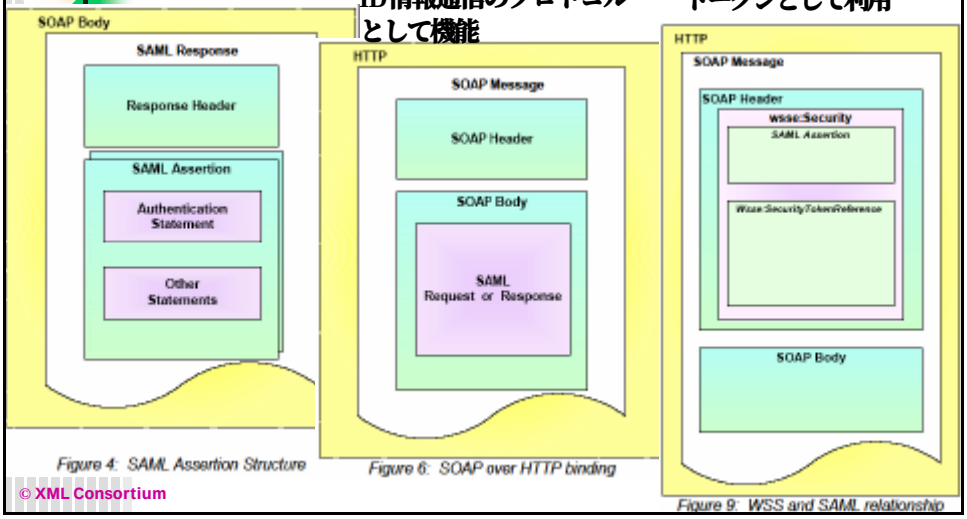


Figure 4: SAML Assertion Structure

Figure 6: SOAP over HTTP binding

Figure 9: WSS and SAML relationship

SAMLの使い方 :SOAP <-> WSS

- SOAP上でのSAMLリクエスト / レスポンスプロトコル
  - SAMLアサーションを取得する為に使用
  - SOAPボディの中のSAMLレスポンスに含まれる
  - SAMLアサーションは信頼される認証局やレポジトリから提供され、要求者とは直接関係無い場合もある
- WSSで規定されたSAMLアサーションの利用
  - SAMLアサーションはそのときのメッセージ自体を保護するために使われ、典型的には電子署名の鍵を含む
  - SOAPヘッダの中の<Security>要素に含まれる
  - SAMLアサーションは繰り返し使われることもあり、送信者のIDに関連している場合が多い

WSSの中でのSAML利用

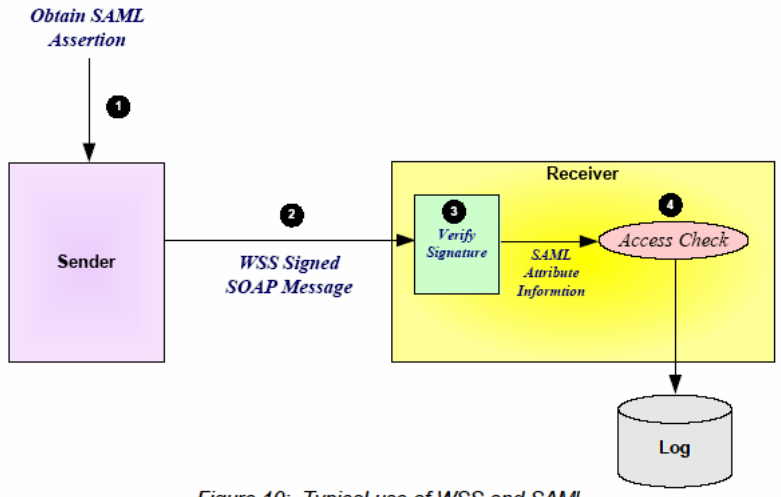


Figure 10: Typical use of WSS and SAML

SAMLとXACML

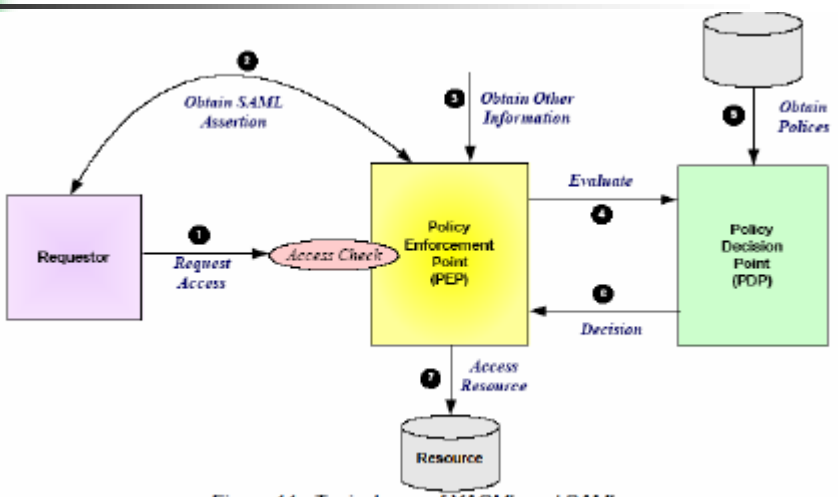


Figure 11: Typical use of XACML and SAML

プロファイル

- WebブラウザSSOプロファイル
  - PULLとPUSH、SP開始とIdP開始
  - SP開始：POST->POST, リダイレクト→POST、アーティファクト→POST、POST→アーティファクト
  - IdP開始: POST、アーティファクト
- ECPプロファイル
- Federation (連携)

WebブラウザSSO：IdP起動とSP起動

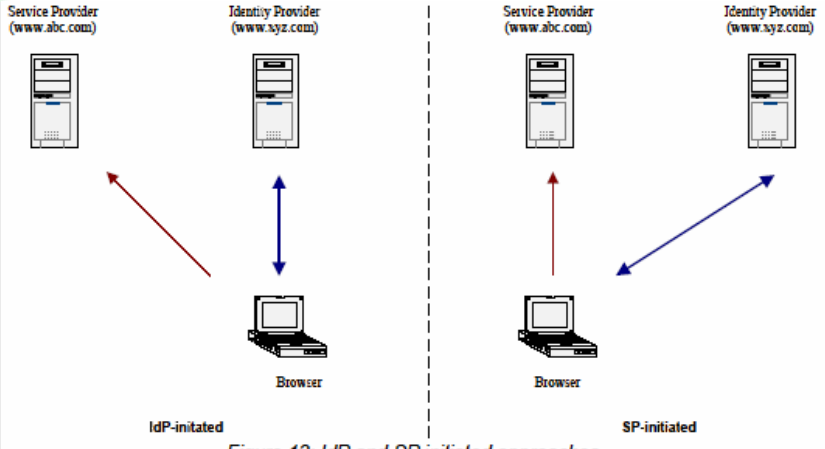


Figure 13: IdP and SP initiated approaches

プロファイル：
WebブラウザSSOプロファイル(例)

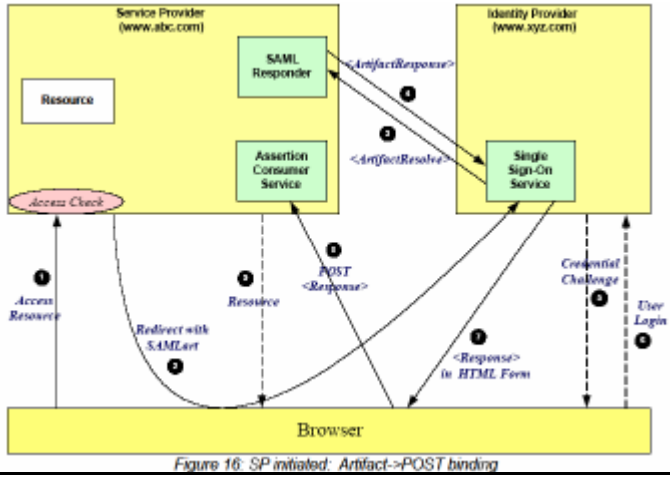


Figure 16: SP initiated: Artifact->POST binding

プロファイル ECPプロファイル

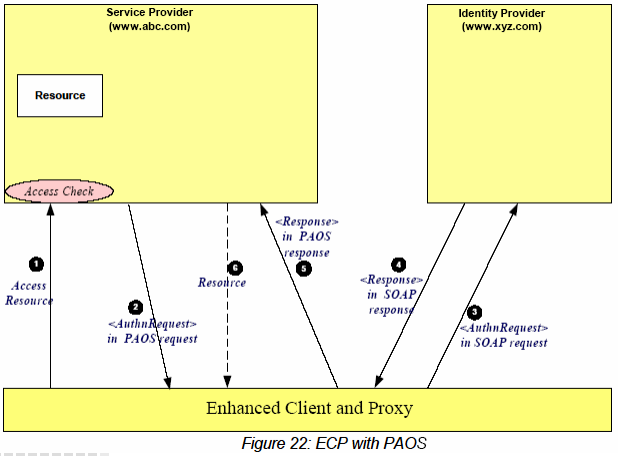


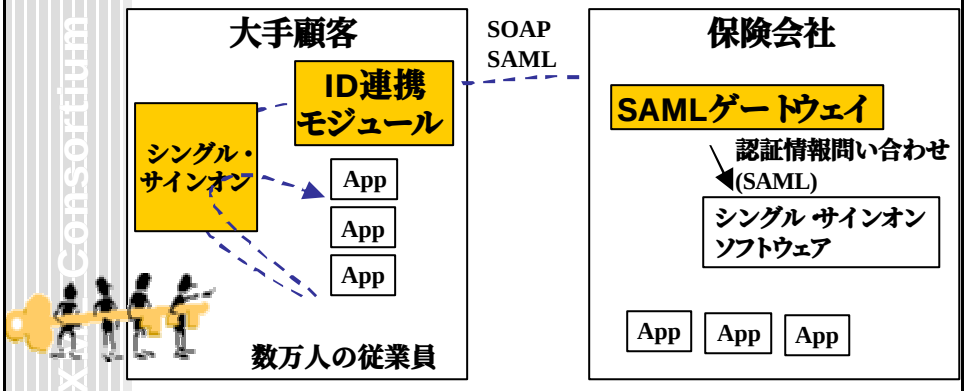
Figure 22: ECP with PAOS

- Enhanced Client and Proxy プロファイル
  - モバイル機器など低機能な端末を利用するシステムでプロクシを立てる場合
  - リダイレクトが使えないクライアント
  - IdPとSPが直接通信できない場合

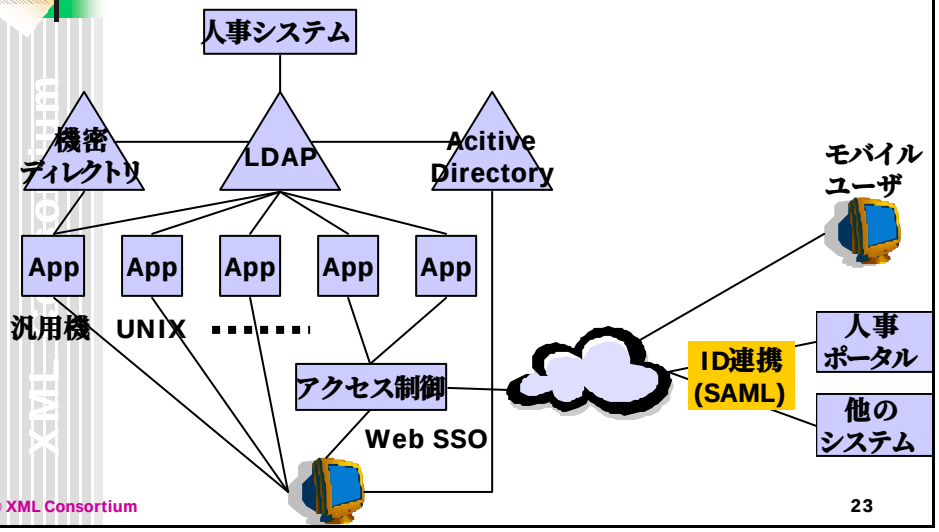
プロファイル：
フェデレーション・プロファイル

- 今の所、内容は空欄
- 予定内容：
  - idPが自分の情報とあるSPにおけるアイデンティティを連携する
  - 連携の終了
  - 既に存在する2つのサービス上のアカウントのマッピング

SAML利用事例
米国保険会社での顧客認証



SAML利用事例：
米国銀行での社内認証システム



まとめ

- SAMLはWebサービスの一元的な認証と
  インターネット・ワイドのシングルサインオンを実現する
  XMLベースの認証情報伝達技術
- SAML V2.0になって、Liberty Allianceと融合し、
  標準仕様としての実用性が確立
- 実システムでの実績も増加中

- インターネット・ビジネスの可能性を
  大きく広げる注目技術です