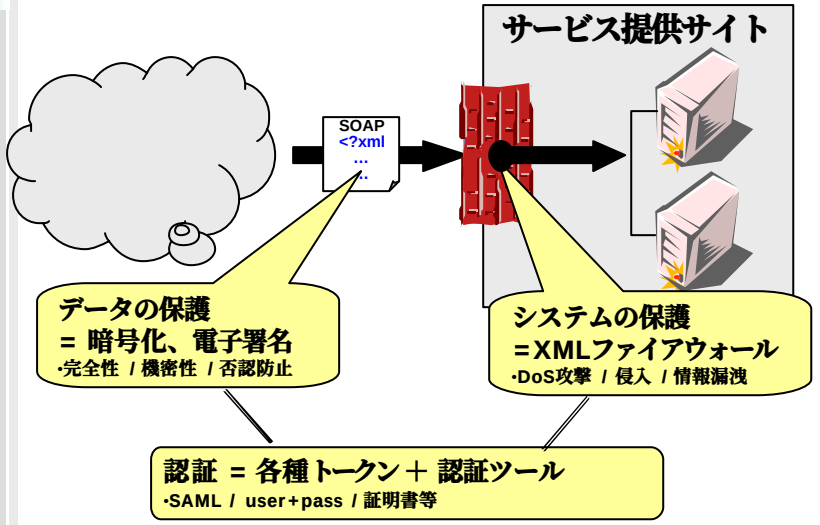
XML Consortium

～ 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

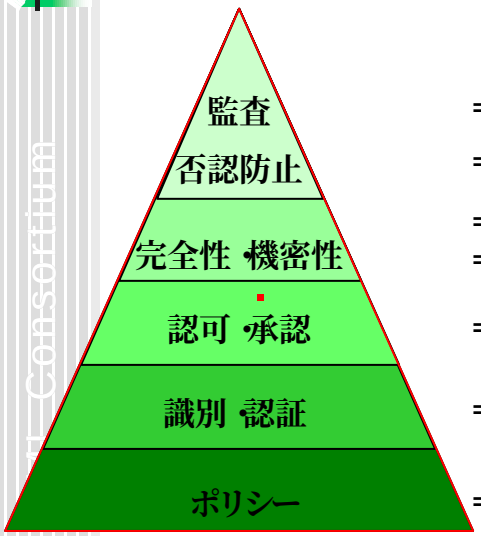
Webアプリケーション環境のための認証技術 :イントロダクション

2005年9月13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)

Webサービスのセキュリティ



セキュリティの階層



＝ 存在の確認（タイムスタンプ）

＝ 捏造の防止（電子署名）

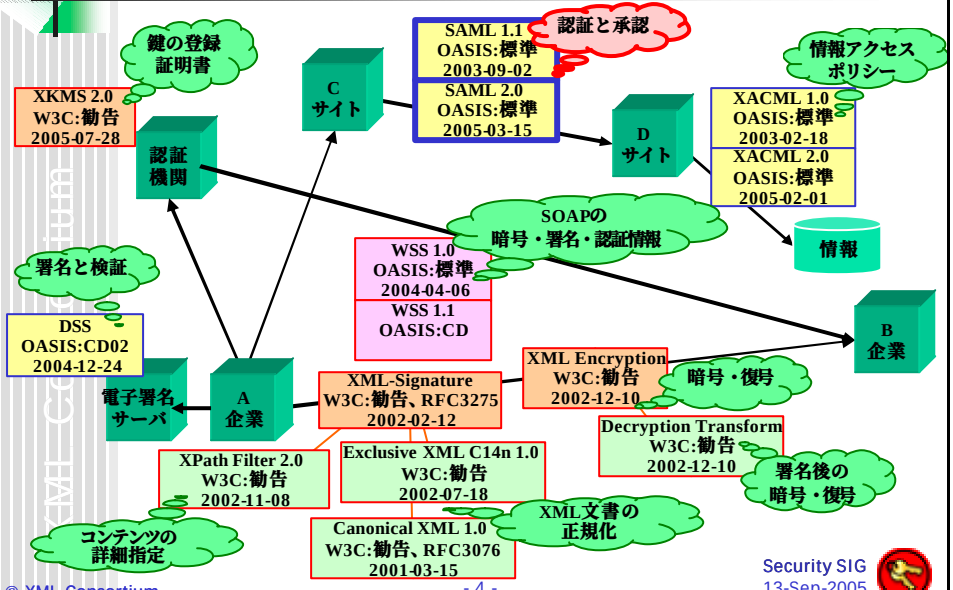
＝ 秘匿（暗号化）
＝ 改竄の防止（電子署名）

＝ 権限の確認（アサーション）

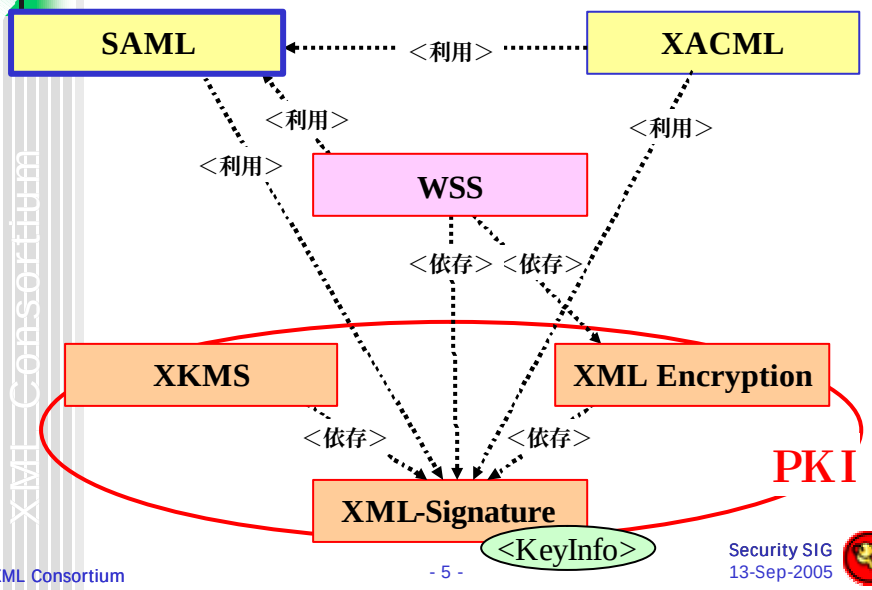
＝ なりすましの防止（電子署名）

＝ 適用・運用方針、ライフサイクル

セキュリティ関連XML規格一覧



規格の関連



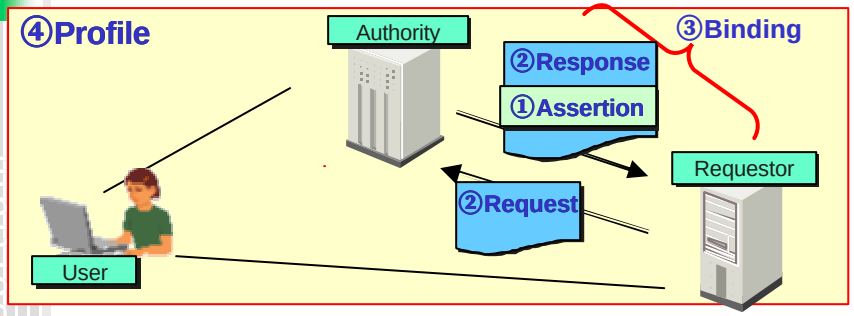
SAMLの概要

- Security Assertion Markup Language
  - 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
- 何を実現するものか?
  - 異なる組織間で認証情報を共有する
    - ユーザの認証状態 ー Authentication Assertion
    - ユーザの属性 ー Attribute Assertion
    - ユーザの持つ権利 ー Authorization Decision Assertion
  - シングルサインオン(SSO)
    - ユーザがあるサイトで認証されたあと、他のサイトにアクセスする際に追加の認証を不要にする。
  - フェデレーション (連携)
    - ビジネスの取り決めや暗号を使った信用情報、ユーザIDや属性等をドメインを超えて確立する。

SAML関連用語

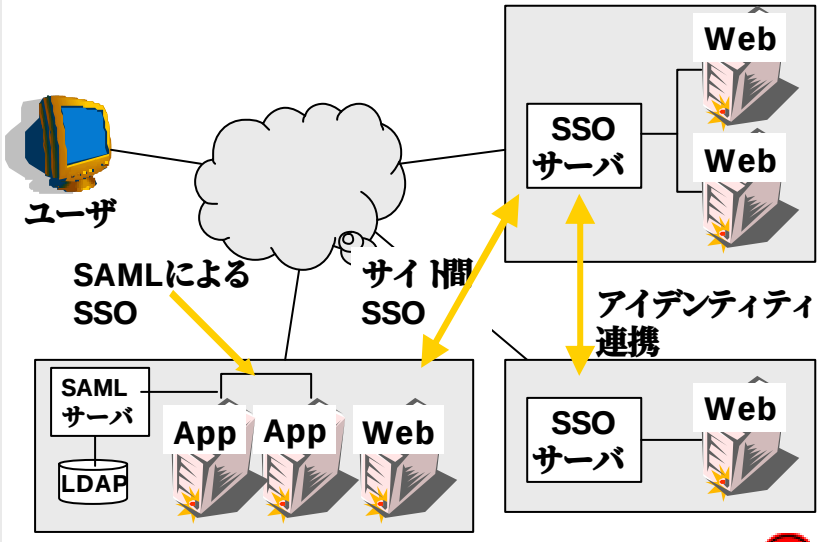
- Subject
  - セキュリティドメインにおける認証/ 承認の対象となる実体
- Assertion
  - SAML Authorityが作るデータ
    - Subjectを認証した行為
    - Subjectに関する属性情報
    - 特定のResource　資源）にSubjectがアクセスすることの認可
- SAML Authority　SAML権限）
  - Assertionを出す抽象的なシステム実体
    - Attribute Authority　属性権限）
    - Authentication Authority　認証権限）
    - PDP　（ポリシーに基づいた権限委譲の判断）

SAMLモデル



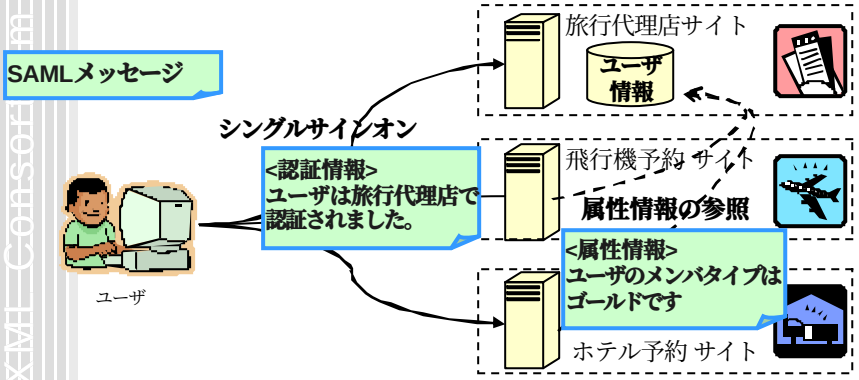
① SAML Assertion　：**認証、属性、許可情報を表現**
② SAML Protocol　：**アサーションを交換するための交換プロトコル**
③ SAML Binding　：**トランスポートプロトコルにどのように乗せるかを規定**
④ SAML Profile　：**実際のサービスを実現するための一連のプロセス規定**

Webサイトのシングルサインオン



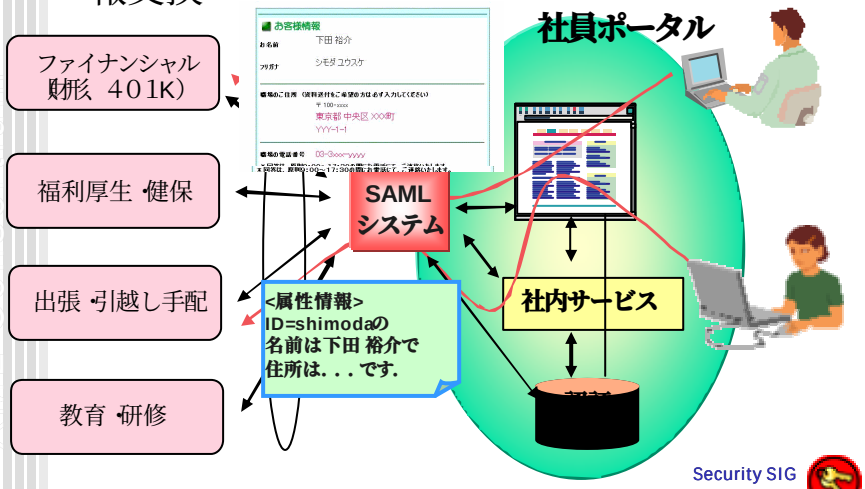
適用例 (1/4) B2C

- ユーザが複数のサイトを用いて、旅行の予約を行う
  - シングルサインオン
  - ユーザ情報の共有



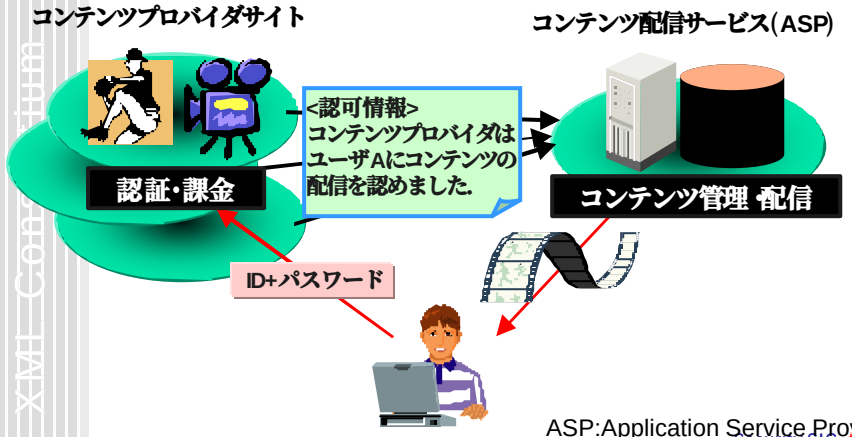
適用例　(2/4) B2Eポータル

- 社外提携サービスへのシングルサインオンや属性情報交換



適用例　(3/4)：ASP連携における認可情報提供

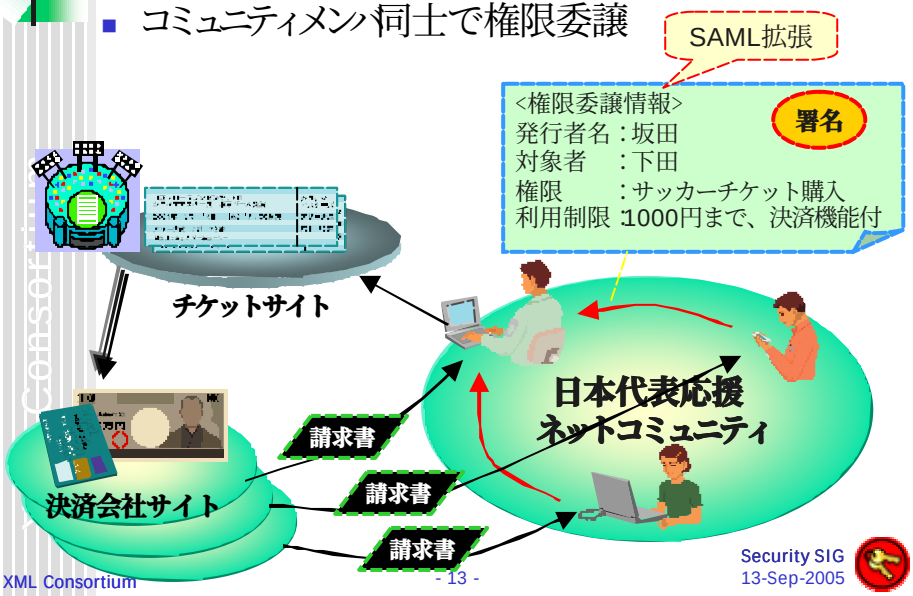
- コンテンツポータルとコンテンツ配信サービスとの連携



ASP:Application Service Provider

適用例　4/4）権限委譲

- コミュニティメンバ同士で権限委譲



まとめ

- セキュリティの基盤となる技術仕様は標準化済み
- これからは使うステージに
- 認証あってこそのセキュリティ
- SAMLでWebサイト間認証を柔軟に
- サイト連携からビジネス連携へ

- インターネットビジネスの可能性が大きく広がる