XML Consortium

WebOS間連携における認証方法の検討状況
SAMLの利用

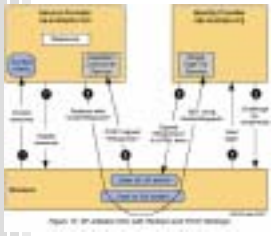
2008年06月06日

a Plat プロジェクト
セキュリティ部会 松永 豊 (TELデバイス)
matsunaga.y@teldevice.co.jp

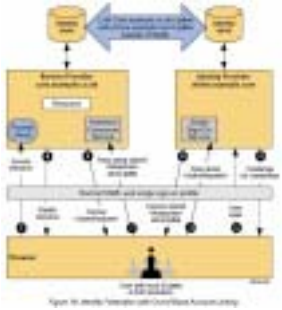
XML Consortium

なぜ、SAML？

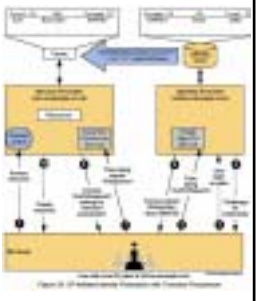
- 包括的 - Web SSO、ID連携、属性、権限...
- XML！



Web SSO



ID連携 (事前にマッピング)



ID連携(一時的仮ID)

図: SAML V2.0 Technical Overview, Committee Draft 02, 25 March 2008
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

aPlatでの検討

- 日本PKIフォーラム
  - http://www.japanpkiforum.jp/
  - 「2000年12月にアジアPKIフォーラム推進協議会として発足以来、経済産業省殿のご指導のもと関係諸機関のご協力を頂きながら、PKIおよび認証一元化（シングルサインオン）関連の普及促進事業」
  - 次世代型電子認証技術基盤を開発
- NEC WebSAM SECUREMASTER
  - http://www.nec.co.jp/middle/WebSAM/products/secmaster/
  - Webシステムなどに対してシングルサインオン（ＳＳＯ）、・アクセス制御を提供する、セキュリティ運用管理ソフトウェア
  - 商用のソフトウェアであり、導入実績もある
- オープンソース？

日本PKIフォーラム

1. 次世代型認証基盤事業
（日本PKIフォーラム、コンソーシアム）

- 認証サービスのプラットホームビジネス化
  - セキュリティ機能の専門化、総合コストの低減
- 認証セキュリティレベル（保証レベル）の相互運用性
  - ネットワークを利用した付加価値の高いビジネス連携の進展
- 認証サービス提供構造の実体化
  - 海外においてもEAP(Electronic Authentication Partnership)などの取り組みがあるが、これらを参考に日本の商慣習に適合したフレームワークを目指す
- オープンな技術仕様による実装
  - オープンな技術仕様を採用することにより、相互運用性を確保し市場原理の導入による競争原理を確保する
- プライバシー保護、個人情報保護への対応
  - 単なる個人情報の保護から、個人情報の活用へ
  - 仮名による認証など
- ID連携から属性の連携へ
  - プライバシー保護強化アーキテクチャの実現へ

コンソーシアム参加企業：NEC、富士通、日立製作所、セコム、三菱電機IS、日本MS、アッカネットワークス、NTTコミュニケーションズ、大阪商工会議所（事業化候補）

日本PKIフォーラム

4. 基盤技術

「次世代型電子認証基盤ソフトウェア版」設計方針

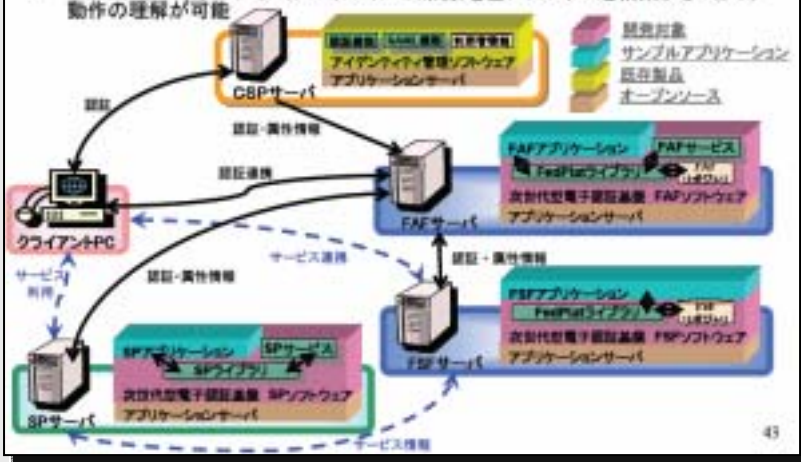
- 既存に存在する製品やオープンソースを利用することを前提
  ⇒開発範囲・開発内容の明確化と効率化
- 一般的に広く使われており、比較的安価に入手可能なハードウェア、オペレーティングシステムを採用
  ⇒PCアーキテクチャ、Windows
- ブラウザを用いたWebのインタフェースと、関連する標準的な仕様をベースに設計
  ⇒SAML、XML署名、SSL/TLS、HTTP 等
- 開発言語は、他のOSへの移植性やメンテナンス性を考慮
  ⇒Java（プラットフォームフリー）
- 公開するソフトウェアを基に次世代型電子認証基盤システムの啓発活動に利用
  ⇒システムテスト環境を提供し、その環境を構築して動作させることで電子認証基盤システムの理解に役立てる

41

日本PKIフォーラム

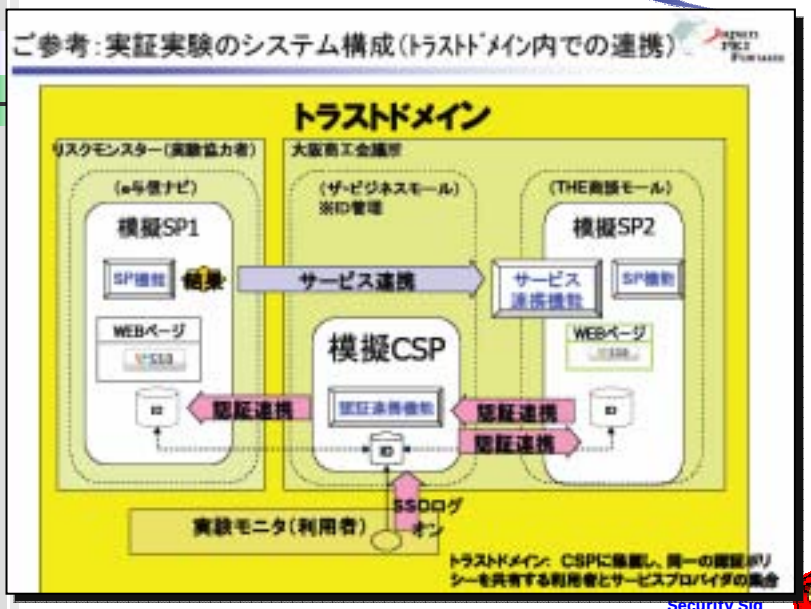
4-2. 開発概要

- 「次世代型電子認証ソフトウェア第2.0版」は、既存のCSP製品や、オープンソースを使用して以下のシステムを構築
- サンプルアプリケーション（システムテスト環境）を基にシステムを構築することで、動作の理解が可能



43

日本PKIフォーラム

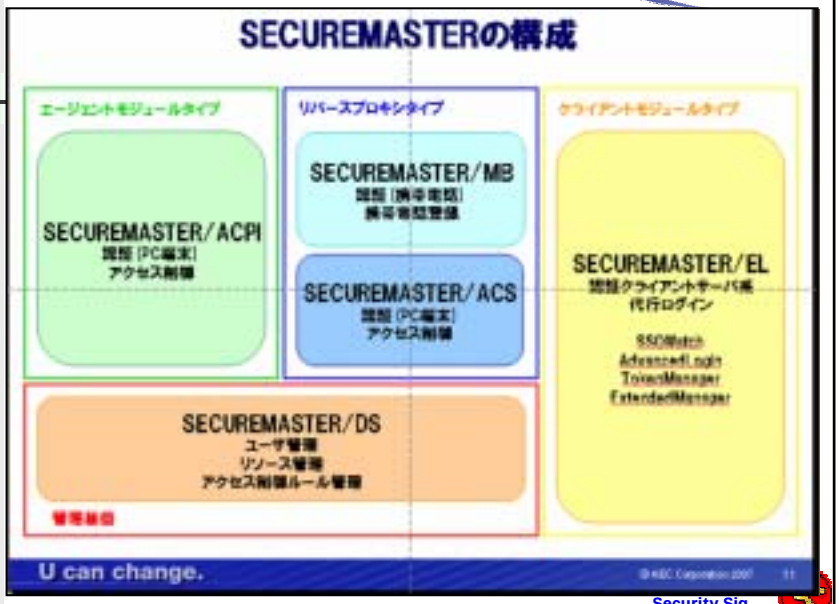


日本PKIフォーラム

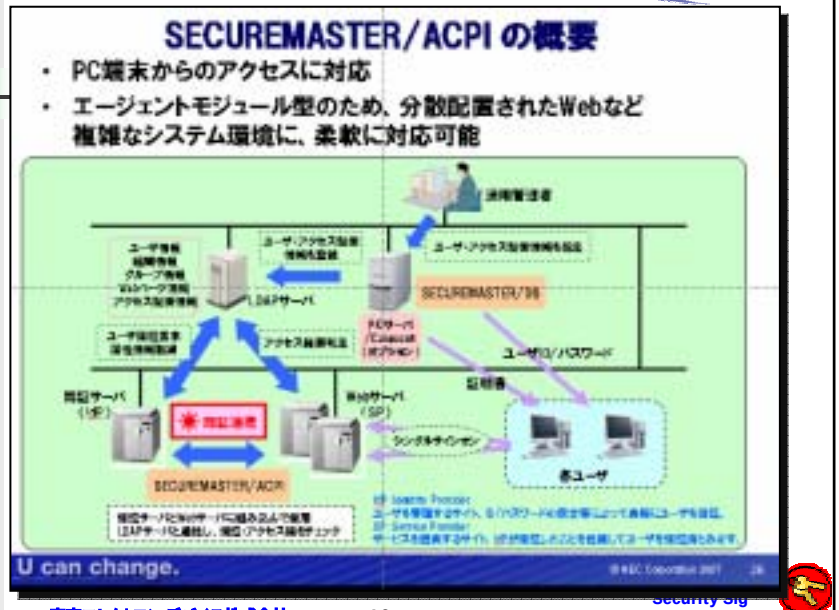
- 次世代型電子認証技術基盤のためのソフトウェア
- 公開されている実装を試用してみた
- 検討結果
  - モデル・機能としては、良さそうだった
  - オープンな仕様を使っているので、制約がない
  - **Apache Tomcat, Sun Java System Access Managerを使って構築できる**
  - 開発の基となった「サンプルアプリケーション」の前提としているプラットフォームが、既に入手できない状態だった

今回は、稼動まで追及することができなかった

SECUREMASTER

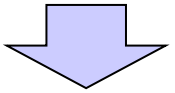


SECUREMASTER



SECUREMASTER

- 説明会の情報を基に、適用を机上検討
- 検討結果
  - 商用ソフトウェアで実績もある
  - 広範な機能が包括的に提供されており、おそらくやろうと思えば何でもできる
  - 異種混在環境に埋め込むためにはカスタマイズが必要
    … 詳細なAPIの仕様は公開されていない



異種混在を含む全体設計に依存 → 保留

今後の展望
SAMLのオープンソース実装

名称	説明	開発元
Enterprise Sign On Engine (ESOE)	SAML V2.0 Java実装 / Includes XACMLv2ベースの機能も	Intient
simpleSAMLphp, SAML V2.0 SP, SAML V2.0 IdP	PHP実装、Shibboleth 1.3と2.0と互換	FEIDE research and development
Lasso - Liberty Alliance Single Sign-On	C実装、JavaやPerl、Python、PHP用のbindingありSAML v2級	Entr'ouvert
OpenSSO	Java実装、SSOCircleで使われている、拡張機能としてRubyのRP、OpenID、PHPクライアント等	Sun Microsystems
OpenSAML	C++とJavaの実装、コア部分、SAML v2.0	Internet2
Shibboleth	IdP (Java)とSP(C++ Apacheモジュール)を含む、OpenSAMLベース	Internet2
SourceID	ID連携、SAML V1.1、ID-FF WS-Fed	Ping Identity
ZXID	C実装、SWIGによりPerl, PHP, Javaサポート、SAML v2 SP	Sampo Kellomaki

参考 http://saml.xml.org/saml-open-source-implementations (2008/05/15)

XML Consortium

検討状況編
OpenID、OAuth
に続きます