



a Plat プロジェクト

WebOS間連携における 認証の一元化

セキュリティ部会 + Webサービス実証部会



紹介内容

- 「WebOS間連携における認証問題」
 - 松永 豊 (TELデバイス)
- 「WebOS間連携における認証方法の検討状況」
 - SAML - 松永 豊 (TELデバイス)
 - OpenID - 松山憲和 (PFUソフトウェア)
 - OAuth - 荒本道隆 (アドソル日進)
- 「今後の展望」
 - 松山憲和 (PFUソフトウェア)





WebOS間連携における 認証問題

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

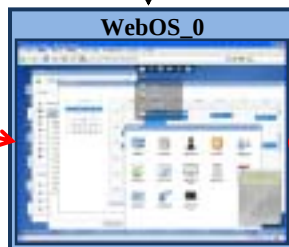


a Plat プロジェクト ゴール



•WebAPI(SOAP/RESTなど)を
使うことでWebOS間で連携

通常使っているWebOS



- WebOS_1で管理されているリソース
 - WebOS_2で動作しているアプリケーション
 - WebOS_3で提供されている機能(検索など)
- をWebOS_0で利用したい



aPlat プロジェクト



Webサービス実証部会

- プロトタイプの実装と検証
- WebOS間連携における課題
- 標準仕様への対応

補完

セキュリティ部会

- セキュリティ関連標準仕様の調査
- ID管理/認証一元化への関心
- 実装時の課題

2007年8月より
合同で活動開始

aPlat プロジェクト

- ◆相互の問題意識を共有
- ◆相互の技術説明会
 - SAML
 - OpenID
 - 日本PKIフォーラム
 - WebOS
- ◆課題解決のための合同検討

- CardSpace
(マイクロソフト様)
- SECUREMASTER
(NEC様)

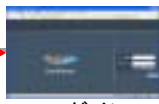
© XML Consortium 2008 All rights reserved.

Security Sig
06-Jun-2008



aPlat プロジェクト

課題 (1)

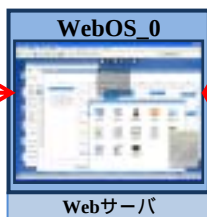


ログイン

認証



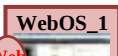
- ▶WebOSの機能を使用するには、認証(ユーザー名/パスワード)が必要
- ▶WebOS毎にユーザー名/パスワードは異なる
- ▶WebAPI経由でWebOSの機能を使用する場合も同様
- ▶認証方法は、WebOSにより異なる
 - ▶WebAPIによるアクセストークン取得など
- ▶認証情報(セッション情報)の保持方法は、WebOSにより異なる



認証

認証

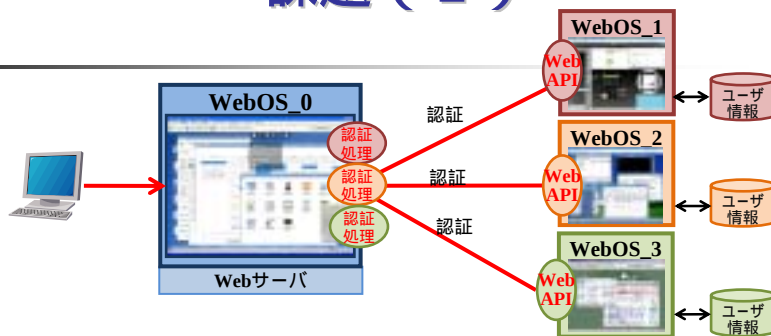
認証



© XML Consortium 2008 All rights reserved.

2008

課題 (2)



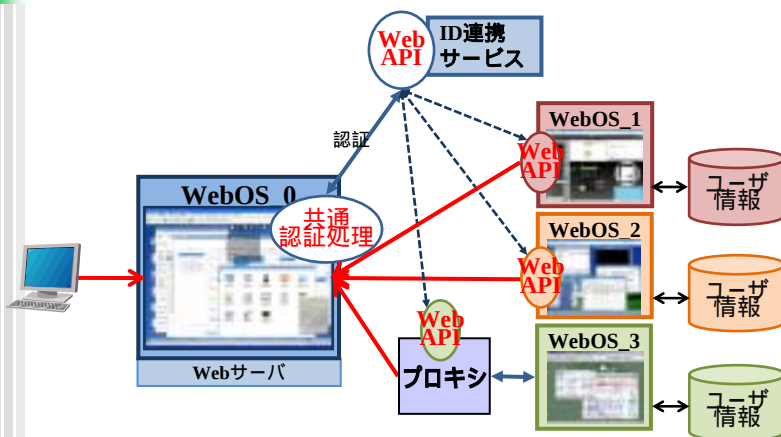
連携するWebOS毎に独自処理(認証方法/ユーザ名/パスワード)を実装すれば実現は可能



単一の共通 (認証) コンポーネントとしたい



WebOSにおけるID連携イメージ (案)



ID管理仕様の動向



XML Consortium

XMLベースのトークン (OASIS, Liberty / Sun)

- OpenLiberty
- Shibboleth OpenSAML
- OpenSSO
- 認可 - XACML

「card」ベース、 WS-Trust (MS, OASIS)

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

SAML, Liberty Web Services

SSO, single logout, permission-based attrb sharing, user-abstract use cases, optimized for "circles of trust", interoperant program

Can do SSO with LRM-based authentication method agnostic

Supports user control, improvement, modularity

SAML tokens in XML, mps, enterprise security & privacy, smart cards

Pushing-resistant authentication and attribute sharing through client "card" paradigm, requires WS-Trust, can front-end various SSO systems

CardSpace

OpenID

SSO and simple attrb sharing with LRM-based authentication, low-trust scenarios, explicitly no need for preconfigured trust

URLベース (SixApart, Verisign)

- 認証機能
- 認可 - OAuth

Sun Microsystems社 Eve Maler氏による図

<http://www.xmlgrrl.com/blog/archives/2007/03/28/the-venn-of-identity/>

Security Sig
06-Jun-2008

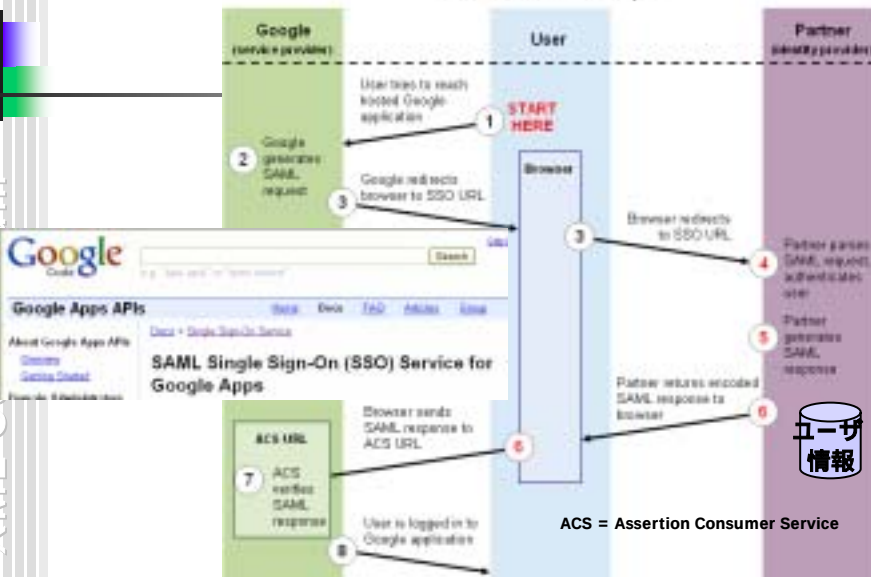


ID連携の例



XML Consortium

SAMLTransaction Steps



http://code.google.com/apis/apps/sso/saml_reference_implementation.html

Security Sig
06-Jun-2008



今までの検討

- 連携の仕組み
 - SAML
 - OpenID
 - OAuth
- アーキテクチャ
 - WebOSに認証連携機能埋め込み
 - WebOSの手前にゲートウェイ
 - プロキシを経由
- ID管理、連携に使えるツールはないか



活動履歴

2007/8/23	aPlat課題確認、方針打合せ
2007/8/23	日本PKIフォーラム次世代型認証基盤説明会
2007/9/26	SAML勉強会 (セキュリティ部会 松永)
2007/10/22	Windows CardSpace紹介 (マイクロソフト様)
2007/10/22	OpenID調査報告 (セキュリティ部会 林)
2007/10/22	WebOS勉強会 (Webサービス実証部会 荒本)
2007/10-11月	次世代認証基盤テスト (Webサービス実証部会 荒本)
2007/12/7	XMLコンソーシアムDay 活動報告
2008/1/30	方針打合せ
2008/2/29	方針打合せ
2008/3/27	SECUREMASTER説明会 (NEC様)
2008/4/25	総括、発表の相談





検討状況編 に続きます

