シングルサインオン認証の実装

牧野 浩之

1　研究背景

インターネットの幅広い普及により，様々なサービスがインターネットを利用して提供されている．本研究室においても，サーバがたくさん存在し，それぞれのサーバ上でそれぞれのサービスが動いている．サービスの多様化に伴って，ユーザがサービスを利用するために必要な ID とパスワード，あるいは鍵や証明書など認証に必要な情報は増大している．このようなことから，ユーザ自身が ID やパスワードを全て管理するのは大きな負担になってきている．また，コンピュータウィルスの感染による情報漏洩などが懸念されるなか，安全に認証が行える環境への意識が高まってきている．さらに，管理者の立場においても，現在のサービスやシステムはそれぞれのサーバやサービスで独自にユーザ情報が管理されており，管理ポリシーなども多様になっている．そのため，異なる管理主体によって情報が管理されている場合において，複数のユーザ認証情報を統合管理する機構が必要となってくる．なりすましや改ざん，不正アクセスなどを防ぎ，本人を確実に，かつ手間をかけずに認証させる必要もある．

このような課題を解決するため，シングルサインオン認証技術が注目されている．本発表では，シングルサインオンを用いることによって一度の認証でサービス間の本人確認，コンテンツへのアクセス権限の付加ができるシステムを提案する．

2　シングルサインオン

シングルサインオンとは，1 回の認証手続きで、複数のサービスやアプリケーションなどにアクセスできること，またはそれを実現するための機能を表す．ユーザの情報はユーザの利用しているパソコンに保存されるのではなく，シングルサインオンを行う認証サーバに保存されており，ユーザが確実に認証サーバへログイン出来た場合，認証サーバがユーザの代理となり他のサービスにログインを行う手法が一般的である．

現在，シングルサインオンは大手各社が様々な規格を提唱している．ここでは代表的なものを挙げて，最近の動向を掴むこととする．

2.1　Sxip(Identity 2.0)

Sxip(Identity 2.0) はアメリカのアイデンティティ管理アプライアンスを販売している Sxip 社がオープンソースで提供しているシングルサインオンソリューションである．Sxip を用いることにより，1 つの ID とパスワードで複数のサイトにログインし，情報を一元管理することができる．そのメカニズムは，Fig. 1 に示すようになっている．

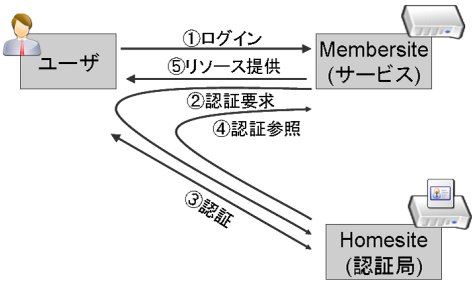

Fig.1　Sxip 認証の構成 (出典：自作)

2.1.1　Sxip 認証の流れ

認証の流れは以下のようになっている．

1. ユーザが Membersite(各サービス) にアクセスする．
2. サービスへのログイン時に，自分の ID を管理している Homesite のアドレスを入力してログインボタンを押す．
3. ユーザが Homesite ですでにログインが完了していれば認証画面を飛ばしてログインできる．ユーザが Homesite で一度もログインしていないときは Homesite の認証画面が出るが一度認証すれば他のサービスも利用できるようになる．

2.1.2　Sxip の長所

Sxip によるシングルサインオンの長所は以下のようなことが挙げられる．

- 実装が容易であること．
- ユーザがサービスに対して公開する情報を選択できること．
- 他の認証プロトコルとも親和性が高いこと．
- Identity Provider(認証局) をユーザが選べること．
- オープンソースであること．

2.1.3　Sxip の短所

逆に，Sxip の短所は以下のようなことが挙げられる．

- サービスに組み込みが必要なこと．
- 通信路が暗号化されていることが前提であること．
- Homesite 間の連携の実装が未開であること．

2.2　SAML

SAML(Security Assertion Markup Language) とは，ID やパスワードなどの認証情報を安全に交換するための XML 仕様であり，標準化団体 OASIS によって策定されている．Fig. 2 に表すように，ユーザは認証局で認証し

たあと，Web サーバへ動的な資源を要求する．Web サーバはアプリケーションにユーザの認可の権限をチェック出来るように認証情報を提供する．別のサイトへ移動した際にも，Web サイトが SAML に対応していれば，移動元のサイトと移動先のサイトが SAML プロトコルで通信し，自動的に認証情報が引き継がれる．前節で述べた Sxip は SAML プロトコルもサポートできるようになっている．

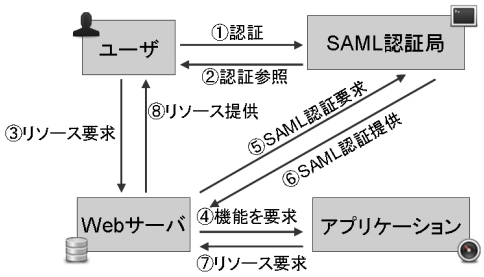

Fig.2　SAML 認証の構成 (出典：自作)

2.3　OpenID

OpenID は，本人を特定する URL とパスワードの組み合わせで ID を生成し，それを元に認証を行う方法である．OpenID に対応したサービスであれば，すべてその ID を用いて認証を行うことが可能になる．同様の仕組みに Six Apart 社の Type Key サービスがある．また，Sxip との親和性も高い．

2.4　Windows CardSpace

CardSpace は，Microsoft が作っており，「Microsoft .NET Framework version 3.0」のコンポーネントの 1 つで，以前は「WinFX」と呼ばれていたものである．インターネット上で個人情報の共有やリソースへのアクセスにおいて，ユーザ名とパスワードに取って代わり，より安全かつ簡単に行うための技術として開発されている．Windows Vista での対応のほか，Internet Explorer 7 や FireFox の拡張機能にも提供される．

2.5　Liberty Alliance

Liberty Alliance は Sun Microsystems が Microsoft に対抗して 2002 年に立ち上げられたシングルサインオンアーキテクチャである．このプロジェクトには，AOL, Intel, IBM, NTT, HP, VeriSign, ORACLE などが参加している．Liberty Alliance アーキテクチャではプロトコルに SAML がベースとなっている．Liberty Alliance が提供するサービスは，ユーザがシングルサインオン用データの登録先を自由に選択でき，データ登録サイトとサインオンサイトが連携して対応している全てのサイトでサインオンが可能となるものである．

2.6　最近の動向

本報告では，Sxip, SAML, OpenID, CardSpace, Liberty Alliance について取り上げたが，それぞれ独自の仕様が提唱されている中で，Sxip は SAML や OpenID とのプロトコルの親和性が高く，シングルサインオン普及にさらなる拍車をかけるのではないかと考えた．そこで今回は Sxip を用いて実装を行うこととした．

3　シングルサインオン Sxip の実装

今回は，2.1 で取り上げた，Sxip(Identity 2.0) を利用して Web シングルサインオンの実装を行った．実装に Sxip を選んだ理由は，Sxip がオープンソースであり，ドキュメント類，各言語の開発キットが揃っており，実装がしやすいことが挙げられる．また，OpenID や CardSpace，SAML とも親和性が高いということも理由の一つである．

3.1　実装手順

認証の手順は 2.1 に示す通りである．実装は異なるドメインの異なるサーバ間で Homesite(認証局) といくつかの Membersite(サービス) を設置する．ユーザは Homesite でユーザ登録を行い，サービス共通のアカウントを作っておく．Membersite ではログイン画面に Homesite を識別するためのタグを埋め込む．認証結果は REST で受け取られる．

3.2　Homesite の設置

Homesite はユーザもしくは他のサーバでアイデンティティ情報をオンラインで交換するためのアプリケーションである．Sxip の公式サイトで配布されている Homesite は Perl でできており，一般的なサーバで動作するように設計されている．Homesite はユーザのアイデンティティ情報を保持，管理する機構であるため Identity Provider とも呼ばれる．

3.3　Membersite の設置

Membersite はサービスを提供を行うためにユーザのブラウザを通じてアイデンティティ情報の要求をするサイトである．Membersite Development Kits(MDKs) は公式サイトで配布されており，Perl, PHP, Ruby, Java の言語の開発キットが用意されている．既存のサービスに合う言語で組み込むことができる．

Membersite では、Homesite にアイデンティティ情報へのリクエストを送る機構 (Fig. 3) と，認証結果を受けとるための REST 機構を実装する．ユーザがログインする際には「Sxip in」ボタンをクリックするだけでログインできるようになるほか，このクリックするプロセスも自動送信で省略することが可能である．

Fig.3　Sxip in 認証画面 (出典：自作)

3.4 Digital Identity eXchange (DIX)

Sxip は Digital Identity eXchange (DIX) というプロトコルを利用してアイデンティティ情報を交換している．DIX は標準化に向けて Internet Engineering Task Force(IETF) で協議されているところである．DIX の目指すところは以下の通りである．

- 自動化…インターネット上でアイデンティティ情報の交換を自動化すること
- 容易…広範囲に適用できるよう導入における障壁をなくすこと
- スケール…インターネット規模でのアイデンティティ交換のスケーラビリティを確保すること
- プライバシー…ユーザのプライバシーを確実に確保すること

アイデンティティ情報は SXIP プロパティと呼ばれており，name 値と value 値を持ったペアのタグで表される．SXIP プロパティは常時，sxip.net というドメインプレフィックスが付く．

DIX を用いて Sxip は Membersite から以下のようなタグをフォームから送信を行い，Membersite の識別とアイデンティティ認証のリクエストを行う．この例は Membersite の識別子とともに，ユーザのファーストネームとメールアドレスのリクエストを送るものである．

```
<input type="hidden" name="dix:/message
 -type" value="dix:/fetch-request"/>
<input type="hidden" name="dix:/message
 -id" value="23AC-34B8-BFD1-455A"/>
<input type="hidden" name="dix:/members
 ite-url" value="http://hoge.hoge/sxip"/>
<input type="hidden" name="dix:/members
 ite-path" value="hoge.hoge/"/>
<input type="hidden" name="first_name" va
 lue="dix://sxip.net/contact/name/first"/>
<input type="hidden" name="email" value="
 dix://sxip.net/contact/internet/email"/>
```

4 まとめと今後の展望

4.1 認証モデル

本発表では，サーバ (サービス) とユーザ間でのシングルサインオンの実装であったが，今後，認証サーバ同士がアイデンティティ情報を交換して認証しあう (Fig. 4) といった代理認証が行えるシステムを目指したい．さらに認証サーバが認証サーバを認証することにより，信頼性の向上にもつながる．ネットワーク上でユーザの信頼性を向上させ識別できることによって，現在の ID があふれている状態を改善し，よりセキュアに，より便利にできるものと考える．また，認証サーバ同士が P2P で通信しあうことにより，ネットワークのスケーラビリティも同時に確保できるものと考えている．

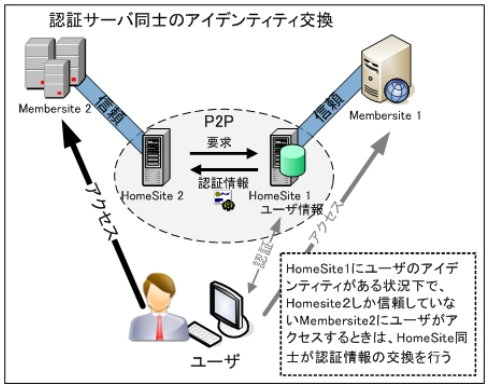

Fig.4 認証局のアイデンティティ交換 (出典：自作)

4.2 コンテンツアクセス制限

ユーザの情報を一カ所で管理できるようになると従来の ID とパスワードに代わって，一丸管理している個人の情報がアイデンティティを持つようになる．そこで，サービス提供者やコンテンツを持っている者がユーザごとに公開範囲を設定し，このアイデンティティを持ってユーザがアクセスするというモデルが今後一般的になっていくと考えられる．Sxip の商用サービスでは，Friend of a Friend（FOAF）プロジェクトによるマシン可読 FOAF プロフィールの標準化に向けた取り組みに適合した形で進められている． FOAF プロフィールとは，vCard と同様にユーザが自分に関する情報を提供する手段であり，名前や電子メール・アドレス，友人関係にある人々などの情報を XML と RDF を使用して記述するものである．これにより，アイデンティティ間の関係を考慮することも可能となる．アイデンティティ間の関係を考慮しながらコンテンツにアクセスする際のセキュリティポリシーを管理することができるようにすることが今後の課題といえる．

4.3 認証の強化

現段階ではパスワード認証であるが，これは認証に必要な情報が漏洩した場合に不正利用される危険性が存在する．そのため，USB セキュリティートークンを利用して，USB キー内に証明書を格納して PKI(Public Key Infrastructure) 認証を行えるようにすることが今後の課題である．

参考文献

1) Sxip Documents
   http://www.sxip.org/Documents
2) A look at emerging Web security architectures from a Semantic Web perspective
   http://www.w3.org/2006/03dc-aus-lga/swauth
3) Digital Identity Exchange
   http://dixs.org/
4) ETech 2006 – Who Is the Dick on My Site?
   http://www.identity20.com/media/ETECH_2006/