OpenID と UPKI

～シングルサインオンで広がるネットワーク～

雨宮 明日香，平岩 健一郎
Asuka AMAMIYA，Kenichiro HIRAIWA

1　はじめに

近年，コンピュータの普及とともに，多くのアプリケーションやサービスが提供される時代となった．多くの人がサービスを利用するようになると，本人確認のための認証というものが重要になる．認証には，パスワード認証や公開鍵基盤 (PKI) などがある．しかし認証は一般的に利用するサービス毎に必要となるため，何度も認証手続きを行うことになり手間がかかる．そして多くのサービスを利用するに従って，ID やパスワードといった認証に関する情報の管理が煩雑化する．また，管理者にとっても複数の認証システムを管理するのは大きな負担になる．

このような状況を打破するために，全ての認証を一元化するシングルサインオン (Single Sign-On : SSO) という考えが提案された．その中でも最近注目されている認証技術として OpenID がある．また，現在最も期待されている技術の 1 つであるグリッドコンピューティングの認証技術においても，SSO が用いられている．

本報告では，OpenID における認証方法及び，グリッドコンピューティングの電子認証基盤である UPKI について述べる．

2　OpenID

OpenID は，自分を特定する URL を ID として認証を行うことによって，SSO を実現する Web ベースの認証システムである．OpenID 対応のサービスとして有名なものには，blog サービスの”LiveJournal”やソーシャルネットワーキングサービスの”Videntity.org”などがある．

2.1　認証方法

Fig. 1 に OpenID の認証時における手続きの流れを示す．Fig. 1 の番号に則して，認証のシステムについて以下で説明する．

1. OpenID 対応の Web サービスでアカウントを作成すると，個人の Web ページが作られるので，この URL を ID として OpenID に対応したサイトにログインできるようになる．このとき，自分が管理する blog 及び HP の URL を個人アカウントとして利用する場合は OpenID Delegate という仕様を用いる．アカウントを作成した Web サービスのサーバが認証サーバになる．
2. ユーザは OpenID に対応する Web サービスを訪れ，ログイン画面で OpenID として取得した URL を入力する．このときにパスワードを入力する必要はない．
3. URL を受け取った OpenID 対応サービスは，それを OpenID とみなし，指定された URL からソースを取得する．
4. 取得した HTML 中に

```
<link rel="openid.server"href="http://
認証サーバ/serverlogin?action=openid"/>
```

という要素を見つけた対応サービスは，実際の認証がその OpenID 認証サーバで行われることを認知する．さらに

```
<link rel="openid.delegate" href=
"http://アカウント名.認証サーバ名/"/>
```

という Delegate 仕様もある場合は，入力された URL ではなくそこに指定された URL が認証サーバ上における本当の ID だということになる．
5. 対応サービスのサーバは認証サーバに対して認証を依頼する．
6. 認証を依頼された認証サーバは，ユーザにパスワード入力を促すページをリダイレクトする．(このとき，すでに認証サーバにログイン済みであれば，パスワード入力の処理を行うことなく，対応サービスにログインできる．)
7. 正しいパスワードを得て認証をする．ここで，ユーザは対応サービスではなく認証サーバにパスワードを渡すことになる．
8. 認証サーバは対応サービスに認証結果を返す．本人確認ができたので，対応サービスはユーザのログインを許可する．このとき，対応サービスはユーザのパスワードを知ることなく，入力された OpenID が正しいものかどうかを確認している．

2.2　OpenID により得られるメリット

一度 OpenID のアカウントを取得すれば，OpenID に対応した Web サービスならどこの認証サーバで作成した ID であっても認証を行うことが可能となる．それに

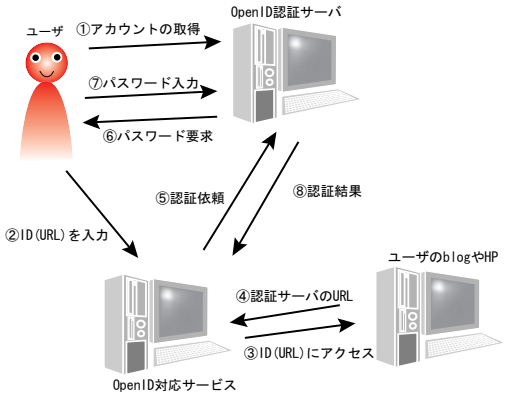

Fig. 1　認証の流れ (出典：自作)

より，各サービスで ID を取り直す必要がなくなるので，ユーザビリティの向上を図ることができる．さらに新しくサービスを提供する場合にも，OpenID に対応させれば認証機能をゼロから開発する必要はなくなる．

2.3　信頼性の不安

認証サーバによってアカウント取得時に必要な本人情報に差がある．そのため，どの認証サーバでアカウントを取得したかによって，ユーザの信頼性が異なる．そして OpenID は，あるユーザが特定の URL に関連付けられていることを保証するが，そのユーザが信頼できるかどうかの保証はない．

3　UPKI

グリッドコンピューティングとは，分散するコンピュータのシステムリソースを統合して有効活用する技術のことである．本章では，グリッドコンピューティング技術を用いた UPKI(University Public Key Infrastructure) について述べる．

3.1　UPKI とは

UPKI は大学間連携のための全国共同電子認証基盤のことである．現在日本で進行中の PKI 事業の一つで，将来の単位互換やシングルサイオンなどに期待されている．UPKI によって，大学のネットワークやコンテンツなどの安全，安心かつ有効な利用を促進することを目指している．この事業は国立情報学研究所と 7 大学全国共同利用情報基盤センターをはじめとする全国の大学が連携して構築を進めている．

大学間連携サービスとして，連携する大学同士の認証局を信頼することで，自大学のアカウントを用いて大学の教師，研究者，学生及び事務職員が，連携している大学のネットワークに自由に入れるようにする．更に共通に利用できる機能を活用することでユーザビリティの向上を図る．

3.2　大学間ネットワークの現状

現在主要大学間は，日本全国の大学及び研究機関等の学術情報基盤として構築・運用されている SINET やスーパー SINET を介して接続されている．しかし，セキュリティレベルの確保は利用者に依存している．そして，商用の証明書発行サービスを利用するには煩雑な事務手続きが発生する．基幹サービスにすら自家証明書の利用が少なくなく，利用者の意識も低い．また，世間では情報漏洩，データ改ざん等のネットワーク上の脅威が拡大しており，平成 17 年 4 月から個人情報保護法が施行され，大学においてもますますセキュリティレベルを向上させる必要性を迫られているのが現状である．

3.3　UPKI に期待される効果

UPKI の構築により，現在 SINET に接続される大学や学術機関の情報交換を安全に行えるようになる．

更に，積極的に国内外の産業や学術機関等との連携も実現させることにより，国内外の知識を集め，研究事業の推進による国際競争力の強化，ひいては経済社会全体の活性化に寄与する．

4　まとめと今後

OpenID は Web ベースの SSO として，今後の認証システムの中核を担っていくと考えられるが，信頼性の部分ではまだまだ不安が残る．ゆえに今後 OpenID が普及していく上でどのように信頼関係を作っていくかが鍵といえる．ユーザが新しく OpenID を取得して，対応サービスを活用するというのではなく，ユーザが既に利用しているサービス側が OpenID に対応するか，すなわち自サービスのユーザを他のサービスにも開放するかどうかが今後注目するところであると考えられる．

UPKI は次世代学術情報ネットワークとして構築され，国際連携，産学連携および地域連携により経済社会に貢献していくだろう．そして平成 21 年以降，7 大学の各基盤センターは学内及び地域の大学等の認証を行っていくと予測されており，同志社大学も今後関わっていくの機会があると考えられる．

参考文献

1) OpenID: Specs
http://www.pp.iij4u.or.jp/ kwi/openid/dsa-specs_ja.html

2) エンジニアのためのキーワードガイダンス [第 29 回]
http://7andy.yahoo.co.jp/esb/docs/column/
books_clm_20060118.html

3) OpenID 認証の仕組み
http://sho.tdiary.net/20051020.html

4) キーワード-ＵＰＫＩ
https://a.yamagata-u.ac.jp/amenity/Keyword/
KeywordWeb.aspx?nKeywordID=5697