L-030

Webブラウジングを基盤としたネットワーク認証システムに関する研究

A Study on Single Sign-On Network Authentication System with OpenID

玉村　尊明[1]　　原　元司[1]
Takaaki Tamamura　　Motoshi Hara

1. はじめに

ネットワーク認証システムは，ネットワーク資源を利用するユーザが正しい人であることを証明するためのシステムである．近年，多くのネットワーク認証システムが提案されているが，シングルサイオン（SSO）の観点，Web サーバへのアクセス制御の双方に対応したものはほとんどない [1]．そこで，本研究では Web ブラウジングを基盤とした認証・認可システム (OpenID)[2] を活用したネットワーク認証システムを提案する．本システムは Web サーバ上のアクセス制御について SSO 機能を実現できるのはもちろん，ゲートウェイ上のパケット通過の制御にも活用が可能である．本稿では，提案システムの概要を報告する．

2. OpenID

2.1 OpenID の概要

OpenID とは，特定のベンダに依存しないユーザ中心の分散型認証システムであり，URL をユーザ ID として利用する [2]．ユーザーは OpenID の認証サーバが提供する ID をコンシューマでのログインに利用することができる．ここで，コンシューマとは OpenID による認証に対応したサービスプロバイダのことで，OpenID をもとに要求があったユーザの管理を行う認証サーバに対して認証を依頼する．ユーザー認証は個人を登録した１つの認証サーバ上で行われるので，ユーザーは ID を１つだけ覚えておけば複数のサービス（コンシューマ）へ，ログインできるようになる．つまり，ユーザーは OpenID によって Web アプリケーションで利用する ID の一元管理と SSO が同時に行えるようになる．以下に OpenID の認証の流れを示す．

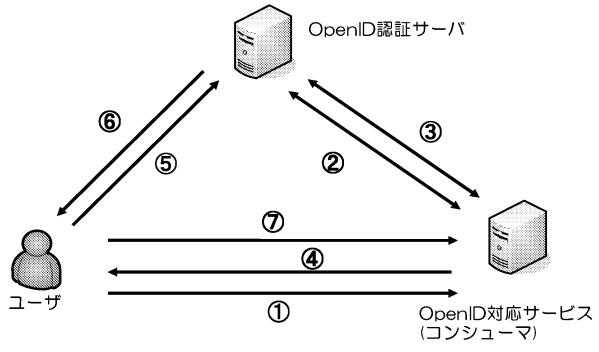

図 1: OpenID の動作

Step1: ユーザは OpenID に対応したサービス（コンシューマ）にアクセスする際に，ID として認証サーバから与えられたユーザページの URL を入力する．
Step2: コンシューマは入力された URL を元に認証サーバにアクセスする．
Step3: コンシューマは認証サーバとの間で暗号化のための鍵を共有する．
Step4: コンシューマはユーザを認証サーバにリダイレクトして認証を要求する．
Step5: ユーザは認証サーバにパスワードなどを送信してログインする．コンシューマからメールアドレスなどを求められている場合はユーザの属性情報も送信する．
Step6: 認証サーバは，認証結果とユーザ属性情報とともにユーザをコンシューマにリダイレクトする．
Step7: 認証が成功した場合，コンシューマはユーザのアクセスログイン等を許可する．

2.2 OpenID の応用

周知の通り，現在さまざまなところで OpenID が使われ始めている．たとえば，Yahoo や mixi といった大手の企業が OpenID を発行し,OpenID を利用可能なサイトが多くみられるようになってきた．これらのサイトでは, ログインする際に OpenID を利用することができる. OpenID を利用することで, 複数のアカウントを持つ必要なく複数のサイトを利用できるメリットがあり，今後も利用が拡大するものと考えられる．

3. 提案システム

3.1 提案システムの動作

本提案では，OpenID により認証を行い，認可を行わせることで，グループ別，個人別にアクセス制御できるネットワーク認証システムを実現する．具体的には，OpenID により SSO を実現し，ある Web ページに対するアクセス制御を加えることでネットワーク認証（ゲートウェイ認証）を実現する．具体的なネットワーク認証手続きは下記の通りとなる（図２参照）．

Step1: OpenID 認証サーバへの ID 登録.
Step2: ユーザは，ネットワーク認証を実現するネットワーク認証サーバの特定ページへのアクセスを Web ブラウザによって試みる.
Step3: 認証サーバは，OpenID の仕組みを利用して認証・認可を行う.
Step4: 認証が成功した場合，認証サーバは CGI を利用してゲートウェイに対してクライアントのパケット通過許可を与え，ネットワーク認証を完了する.

[1]松江工業高等専門学校

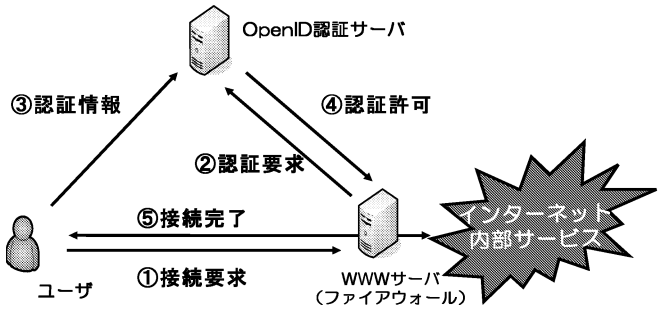

図 2: 提案システムの動作方法

以上の手続きにより，ネットワーク認証が実現できるが，本システムによるとネットワーク認証のみならずローカルネットワークの Web サービスへのアクセス制御にも応用できる．

3.2 システムの応用例

システムの応用例は，次のものが考えられる．

(1) 学内（社内）において，学外（社外）ネットワークへアクセスするためのネットワーク認証システム

(2) 学内（社内）で設置されたイントラネット内のホームページアクセス制御

(3) 学内（社内）で設置されたイントラネット内のファイルサーバ（WebDAV）アクセス制御

(4) 学外（社外）で設置された OpenID 対応サーバへのアクセス制御

(1) は，佐賀大学で開発されたゲートウェイ形ネットワーク認証システムである Opengate と同等な機能を実現するものである．本システムは，従来のネットワーク認証システムに比べて，管理者による ID 管理が不要なことから，管理者の労力を軽減することが可能である．

一方，(2) は学内で設置された各種のホームページへのアクセスを制御する目的での応用である．たとえば，学年や教員，委員会などのグループ単位でのホームページアクセス制御が可能であり，従来の WWW サーバで実現される Basic 認証よりも柔軟な制御を SSO で利用可能となる．さらに，ファイルサーバを WebDAV[3] 方式にすることで，Web ブラウザを用いたファイル共有とそのアクセス制御も実現できる．

(4) は，学内（社内）である程度運用実績が蓄積された段階で，ファイアウォール等の設定によってインターネット上の OpenID 対応サービスと連携する機能である．このことによって，現在広がりつつある OpenID 対応サービスの恩恵を受けることが可能となる．

4. システムの実装方法

4.1 認証の実現方法

OpenID 認証を実現するために，プラットホーム OS を FreeBSD7.2R とし，Web サーバの Apache に「mod_auth_openid」というモジュールを組み込むことで OpenID 認証を実現した．この「mod_auth_openid」は，OpenID Authentication2.0 に準拠しており，OpenID に対応したサービスサーバ（コンシューマ）を構築できる．また,「mod_auth_openid」は規定の OpenID 認証画面を用意しているが，独自に OpenID 認証画面を作成し利用することも可能である．

4.2 認可の実現方法

認可を実現するのあたり，OAuth と MySQL と PHP を併用して使う手法を検討中である．OAuth は，アクセス制御の機能のみを提供する仕組みであり，Web サービスに ID とパスワードを渡すことなく，制御を実現することができる [4]．とくに OpenID との相互運用に有効で，この 2 つを連携させることで柔軟性のあるアクセス制御を実現できる．OAuth では，トークンを利用することで，アクセス制御を行い，ユーザの同意に基づいてアクセス権限を決めることができる．

OAuth の実装には，ライブラリとして提供されている oauth-php を使用する．アクセス制御ポリシやユーザの所属情報などをデータベース (MySQL) に保存しておき，このデータベースの情報を適時利用し，アクセス制御を実現する予定である．

5. まとめ

本研究では，OpenID を用いたネットワーク認証システムを提案した．現在は，必要な機能を順次実装している段階である．続いて行うべき作業として, 認可とアクセス制御ポリシの実装方法の検討があげられる．また，ネットワーク認証システムとしての基本技術であるタイムアウト機能の実現方法についても検討を行う必要がある．今後は，ネットワーク認証システムのプロトタイプを実装した上で, 小規模ネットワーク内で運用実験を行い，より利便性の高いシステムを構築する予定である．

参考文献

[1] 渡辺　義明，他 : 利用と管理が容易で適用範囲の広い利用者認証ゲートウェイシステムの開発，情報処理学会論文誌，vol.42,No.12,pp.2802-2809(2001)

[2] OpenID.ne.jp:
http://www.openid.ne.jp/

[3] WebDAV-Wikipedia:
http://ja.wikipedia.org/wiki/WebDAV

[4] API アクセス権を委譲するプロトコル、OAuth を知る:
http://www.atmarkit.co.jp/fsecurity/special/106oauth/oauth01.html