OpenIDとLDAPの連携による認証統合

柴沼　渓一[†]　　友野　敬大[††]　　上原　稔[†††]　　島田　裕次[†††]

東洋大学工学部情報工学科[†]，東洋大学大学院工学研究科情報システム専攻[††]，

東洋大学総合情報学部総合情報学科[†††]

1. はじめに

近年、Webサービスの多様化に伴って、オンラインストレージへのアクセスや、ポータルサイトでのサービス提供などにおいて認証を行う機会が大きく増えている。

また、企業では、顧客IDをはじめ企業内システムの管理者IDや利用者ID、個人では電子メールの利用者ID、ポータルサイトの利用者IDなど数多くの認証情報を管理しなければならなくなった。

これに伴って、ユーザ側の認証処理にかかる煩雑さや管理者側の情報管理にかかる負荷増加や認証システムのコスト増大の問題が発生しており、認証システムを利用する企業や個人にとって看過することのできない大きな問題となっている。

本研究では、膨大に蓄積されたIDやパスワードなどの情報を統合して認証情報をひとつにまとめる認証統合を実装することで、Web上で展開されるOpenIDや特定ネットワーク内などの異なるネットワークにまたがる認証情報を連携させ、認証情報管理の煩雑さを解消する。その際、オープンソースソフトウェア（OSS）を用いることでコスト問題の解決も実現する。

2. 関連研究

2.1. OpenID

OpenID[1]とは、一つのIDを用いて様々なサービスサイトの認証を行うことができるインターネット上で発展した仕組みを指す。これは、認証に関する仕組みだけを規定しており、アクセス制御に関しては規定していない。OAuthなど他の仕組みと組み合わせることにより、アクセス制御を実現する。

2.2. OpenID実装ライブラリ

OpenIDでは、認証プロバイダ（OpenID Provider；OP）が発行したIDを用いて、複数のサービスサイト（Relying Party；RP）で認証を行う。

RPのライブラリは、Apacheのモジュールライブラリ、PHP、Perl、Ruby、Pythonといったスクリプト言語によるライブラリやJavaのライブラリがある。またOPのライブラリとしてはPHPによるライブラリなどが存在する[2]。

これらのライブラリは、サービス提供サイト（RP）がOpenIDによる認証を認証プロバイダにリダイレクトする仕組みや認証プロバイダ（OP）がOpenIDを発行する仕組みを提供する。

2.3. OpenLDAP

OpenLDAP[3]は、LDAP処理系のOSSである。LDAPはネットワーク上のユーザ名やマシン名などを管理するディレクトリサービスにアクセスするためのプロトコルの一つであり、ユーザ名などのキーとなる値を用いて高度な検索をすることが可能である。また、認証情報を管理する処理系として注目されている。

OpenLDAPでは商用LDAP処理系の互換性の問題を解決すべく、LDAPの仕様に沿ったリファレンス設計がなされている。ユーザインターフェースの面で商用版には劣るが、OSSであるのでコスト削減に役立つ。

3. OpenIDとLDAPの連携による認証統合の提案

本研究では、OpenIDをベースに一回の認証によってWeb、内部ネットワークを問わず、複数のコンテンツへのアクセスを可能にする認証統合システムを構築する。

具体的には、認証のフロントエンドとして、Web側ではOpenIDのRPライブラリ、内部ネットワーク側ではBasic認証を利用する。

Basic認証を利用する理由はLDAPとの連携を実現するモジュールが存在するためだが、現状ではBasic認証をよりセキュアにしたDigest認証との連携が可能なモジュールが存在しない。今後、Digest認証への応用も考慮し、同様な仕組みを利用することとした。

また、OpenIDを特定のメンバーだけが登録できるようにOpenIDのOPライブラリを用いて、OpenID発行プロバイダを構築する。そして、Webと内部ネットワークそれぞれの認証情報の連携のため、OpenIDとBasic認証の認証情報共有にOpenLDAPを用いてOpenIDのMySQL上のデータベースとリンクさせる。具体的には、OpenIDとOpenLDAPのユーザ情報との整合性を保つため、それぞれのIDが共有する識別子を付与する。

4. 認証統合の実装

OpenIDを利用するにあたりOpenID実装ライブラリを用いる。RPのライブラリではApacheに組み込むモジュールとPHPのプログラムを利用し、

Integrate Authentication Cooperating with OpenID and LDAP

Keiichi Shibanuma, Akihiro Tomono, Minoru Uehara, Yuji Shimada

[†]Dept. of Information and Computer Sciences, Toyo Univ.

[††]Dept. of Open Information Systems, Toyo Univ.

[†††]Dept. of Information Sciences and Arts, Toyo Univ.

OP のライブラリは PHP のプログラムを利用する。

また、認証のフロントエンドとしては、Web 側では OpenID の RP ライブラリを利用し、Form 認証を通して OP ライブラリが発行した OpenID で認証できるようにする。内部ネットワーク側では、OpenLDAP と連携可能な Basic 認証を用いることで認証を行う。認証情報の管理には OpenLDAP を用いる。その際、認証情報を管理するデータベースと OpenID の OP ライブラリが管理する認証情報とを連携させる（図 1）。

OpenLDAP では、複数のバックエンドデータベースに対応している。OpenLDAP 側で SQL バックエンドを利用できるようにすることで、OpenID の OP ライブラリが認証情報管理に利用している MySQL データベースとの連携を可能とする。また、OpenID と OpenLDAP のユーザ情報が連携できるように、それぞれの ID 情報として、共通の識別子を付与する。

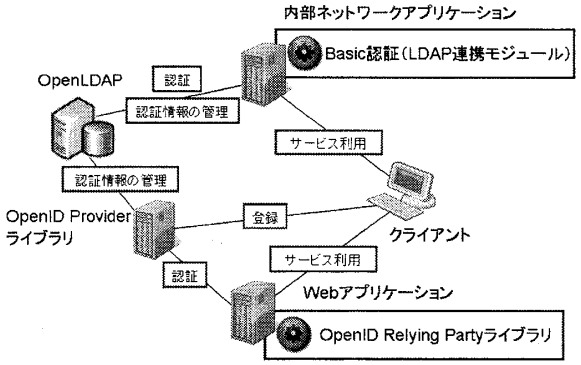

図 1　システム構成図

5. 評価

5.1. Form 認証の統合

OpenID ライブラリを用いることで、Basic 認証では対応できない Web アプリケーションに対してフォーム認証を通してアクセスすることができた。これにより、Web 側のフロントエンドとして安全な認証を提供することが可能であると考えられる。

具体的には、図 2 (1) に示すように、MySQL で認証情報を管理する OP をベースにして、OP から発行された OpenID を用いて複数ある Web アプリケーションに対して RP を通してアクセスすることが可能である。OP には今後、MySQL で認証情報を管理できるように PHP プログラムを改良することで、OpenLDAP との連携を、MySQL を通して実現することができると考える。

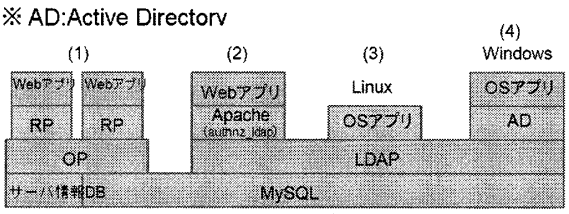

図 2　ネットワーク構成図

5.2. Basic 認証の統合

OpenLDAP に登録したユーザに関して、問題なく Basic 認証を行うことができた。これにより、Basic 認証に関しては OpenLDAP を用いることで認証情報を統合することができた。現状では、認証完了した後、認証セッションを切る仕組みがないので、今後実装を検討したい。認証に関しては LDAP 側のアクセス権限を適切に設定し、ユーザアカウントを作成する際は、適切な属性を付与する必要がある。構成としては図 2 (2) の形となる。

5.3. OS ユーザアカウントの統合

現状では、OpenLDAP は Linux 系のユーザ情報を統合することが可能であり、Windows 系のユーザ情報を統合できる LDAP 処理系の ActiveDirectory との連携も可能となっている。OS のユーザアカウントの連携に関しては OpenLDAP を利用することで現在よく使われる OS については、図 2 (3), (4) のように認証統合を比較的容易に行える。

6. まとめ

従来、認証統合は閉じられたネットワーク、例えばイントラネットといった特定ネットワーク内やポータルサイトの ID に言われるような Web ネットワークそれぞれの中だけで実現されることが多かった。本研究で OpenID をベースとした特定ネットワーク、Web にまたがる認証統合を実現することで、認証情報を管理するデータベースなどを外部に晒すことなく、安全な認証を提供することが可能となる。

OpenID によるフォーム認証と OpenLDAP で認証情報を管理する Basic 認証が実現できたので、今後は OpenLDAP を中心に OpenID と OpenLDAP の連携を目指して、OpenID の PHP プログラムの改良を進めていきたい。また、複数データベース間での同期についても今後、実装について研究する必要がある。

課題について述べると、OpenID と OpenLDAP の連携による認証情報の共有を目指したが、OpenID データベースのデータスキーマでは、OpenLDAP の認証情報として利用するにはユーザ名しか管理しないなど不十分な点が多いため、直接的な連携は困難であることが分かった。これは、PHP プログラム側で新たに MySQL へ認証情報を保持できるように改良することで、データスキーマの問題を解決し、OpenLDAP をも含めた認証統合が実現できると考えられる。

参考文献

[1] OpenID Foundation website
http://openid.net/
[2] Welcome to OpenID Enabled!
http://openidenabled.com/
[3] OpenLDAP, Main Page
http://www.openldap.org/