平成 21 年度 情報処理軽井沢セミナーレポート

京都産業大学　情報センター
尾崎孝治

1. 課題タイトル

所属機関での Shibboleth 導入・活用とその方法について

2. 課題の概要

学内認証基盤として Shibboleth を活用できる。その次にフェデレーションでの活用を考える。これまで出来なかった複数大学間の認証基盤が容易に構築できるため，広くユーザに門戸を開くことで様々な活用事例が出てくるのではないか。

3. セミナーで学んだ技術及び知識

Shibboleth 認証は，自サイトのユーザに，学外の ASP サービスを認証して利用させるケースに適した認証方式の一つである。

学内ではユーザ ID，パスワードの一元化を図っており，ASP の利用も同一ユーザ ID，パスワードで利用したい。しかし ASP プロバイダにユーザ ID やパスワードの情報を渡すことはセキュリティの観点から難しい。Shibboleth ではパスワードなど ID 管理をする ID プロバイダ（以下 IdP）は学内にあれば良く，ユーザは IdP に対して認証を行い，IdP から認証済みを示すデータを貰う。サービスを提供するサービスプロバイダ（以下 SP）はこの IdP から発行された認証済みデータを受け，その情報が偽造されていないことを IdP に確認することでユーザを受け付ける。

Shibboleth 認証を用いたフェデレーションのアーキテクチャは，信頼関係を結ぶ段階では IdP は SP 側に何の情報も知らせる必要がなく，ユーザが SP にアクセスした時点で初めて IdP から SP に情報が提供される。また，渡す情報も個別に制限が出来，最少では（例えば）ハッシュ化した ID だけで良く，個人情報を一切渡さず認証が可能となる。もちろん相手が信用できる場合は学部や氏名など，所有する情報を渡すことができる。

このことは，ユーザの中に個人情報を提供することに非常な抵抗を感じる人が居たとしても，ASP の利用を可能とする。なぜなら，その人がサービスを使わなければそのユーザ情報は一切（ID さえも）SP に渡されることがないからである。ユーザはサービスの利便性と個人情報の提供内容を秤にかけ，納得したユーザだけがサービスを利用すればよい。

4. セミナーの成果

ひととおり IdP サーバ，SP サーバを構築することで，各ソフトウェアの連携がイメージでき，また設定の勘所が分かった。Linux のディストリビューションが変わると様々なパス

が変わるが，セミナー内容を参考に構築が可能と思われる。

5. 事前準備として知っておいた方が良かったと思われること

tomcat のサーバは触ったことがなかったため，設定個所が分からず，また手順書通り編集するものの，何の設定をしているか分からなかった。

Shibboleth は認証時にサーバプログラム間でのリダイレクトが多く発生するので，パケットの流れをイメージするために HTTP のリダイレクト，Apache のリバースプロキシ，tomcat，Shibboleth-idp，OpenLDAP のプログラム関係（443port で受けたパケットがその後どのように流れていくか）を理解しないと，エラーが起きた時にもどの段階でエラーになっているのか，どのログを確認すべきなのかが分からない。これらのサーバソフトウェアについて，一度触っておくことでセミナーの理解が深まる（知らないとほとんど理解できないのではないか)。

また，証明書も Apache に設定するもの，Shibboleth に設定するもの，LDAP サーバに設定するもの，など数種類あり，パスフレーズも数種類ある。混同しない程度の理解が必要である。

6. セミナーの感想

サーバ構築の実習時間がやや不足したものの，充実した研修内容であり，これまで UPKI で培われたノウハウを教えて頂けました。また，時間外にも夜遅くまで講師の方や他の受講生と情報交換ができ，有意義な時間を過ごせたと感じています。少人数であったこともより親密に質問のしやすい環境となり良かったと思います。

また，講師・受講生の方々とつながりが持てたことが何よりの成果です。実際サーバを構築する際には分からないことがたくさん出てくると思いますが，その時質問できる方がいることは非常に心強いです。早く実際のサーバを構築し，理解を深め，逆に質問に答えられるようになりたいと思います。

7. 備考・その他

セミナーを快適に過ごせるように御配慮いただきましたスタッフの方々に御礼申し上げます。ありがとうございました。