平成１９年度情報処理軽井沢セミナーレポート

関西大学 IT センター システム管理課
柿本 昌範

1. 課題タイトル

「IT に強い関西大学を目指した統合認証基盤の構築」

2. 課題の概要

関西大学では、学内の IT 化を推進するため、2006 年度より全学 IT トータルシステムの構築を目的としたプロジェクトが発足した。このプロジェクトの中で今後実現する大学情報システム、教育・研究支援システムを支えるシステム基盤として確固たる統合認証基盤が必要である。そこで統合認証基盤構築のため、以下の施策を実現したい。

(ア) 利用者 ID 体系の刷新
(イ) ID 管理システムの導入
(ウ) シングルサインオンの実現
(エ) 高度認証方式の採用
1. IC カード利用
2. マトリクス認証
3. PKI 認証

今回の課題テーマである PKI の利用については、統合認証基盤の中で、特に厳密な本人認証が必要な場合の仕組みとして PKI 技術を利用した Web システムの認証を実現する。そこで、まずは教職員から証明書の配布を行い、学内に PKI を普及させるための布石とし、今後、S/MIME による暗号化や電子署名によるセキュアメールの利用や文書ワークフロー管理などへの展開を行うこととする。

３．セミナーで学んだ技術及び知識

[講義]

① PKI の基礎

インターネットにある脅威（盗聴、なりすまし、改ざん、事後否認）から身を守るために、暗号化、本人認証、メッセージ認証、電子署名などがあり、それぞれの技術の概要について習得した。また PKI を実現する技術として、公開鍵による証明書と認証局や、PKI 技術を用いたサービスの概要について学習した.

② UPKI 概要

最初に UPKI を構成する PKI 技術についての復習を行った後、UPKI プロジェクトの体制や役割、意義などの紹介があり、UPKI の基本的な概念である 3 層構成の概要について学習した。

最後に以下の UPKI プロジェクトにおける成果の説明があった。

- ✧ サーバ証明書発行・導入の啓発・評価研究プロジェクト
- ✧ UPKI 共通仕様の制定
- ✧ 大学向け認証局スタートパックの開発

③ グリッドでの認証技術の利用

グリッドコンピューティングについての概要とグリッド技術による効用について学習した。また、グリッド環境におけるセキュリティと認証の要件と、実際に NAREGI－CA に適用した認証技術についての知識の習得を行った。

④ shibboleth の最新動向

シングルサインオンの一つとしての shibboleth の概要、及び属性の分散管理が可能な shibboleth の大きな特徴である Federation についての概要について学習した。また Grid との連携や shibboleth の今後の動向､海外での利用動向についての説明があった。

[実習]

① shibboleth の利用（実習）

講師機が利用者 ID を管理する IdP、各受講生機 8 台に実際のサービスを行う SP を VMware 上に構築し、各受講生機は利用クライアントとして shibboleth の環境を構築した。

- ✧ ネットワークの設定を行う（IP アドレス、ホスト名等）
- ✧ VMware 上に SP 用 Linux を配布された DVD より構築する。
- ✧ IdP にて、CA 証明書、サーバ証明書を作成する。
- ✧ metadata.xml に SP サーバ証明書の内容を追加する。
- ✧ 各受講生機 8 台分を追加した metadata.xml を SP に取り込む。
- ✧ 各 SP へのアクセスを確認する。

各 SP に対して、一度ログインすれば再度 ID/パスワードを入力することなく、ページが開けることを確認し、シングルサインオンの機能を確認した。

実習時間の都合上、IdP のリソースポリシーの変更、SP のリソースポリシーの変更については、割愛された。

４．セミナーの成果

課題で報告したとおり、全学 IT トータルシステムにおいて、統合認証基盤を構築してその中で PKI を活用する。教職員と業務システムにおいて PKI を活用した Web 認証を第一の目標として構築する。今後さらに shibboleth をはじめとしてシングルサインオンや Federation について検討を深め、関西大学統合認証基盤の中に取り込むようにする。

また、学内に PKI を展開するにあたっては、学内ユーザに対して、PKI への理解と普及

拡大について活動していくことが必要と感じている。
　将来的には学生が PKI を利用することや UPKI 等、他大学連携を検討したいと考える。

５．セミナーの事前、事後において、参考になった URL とその簡単な内容紹介

・PKI 関連技術解説
　　http://www.ipa.go.jp/security/pki/index.html
・UPKI イニシアティブ
　　https://upki-portal.nii.ac.jp/
・shibboleth Resources
　　http://shibboleth.internet2.edu/

６．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

　PKI の基本的な事項については、概ね理解していたので復習にもなり、さらに理解が深まった。その反面、shibboleth などの SSO や Federation に関する知識が乏しく、もう少し事前に予習すべきであった。

７．セミナーの感想

　今回のセミナーでは、これまで語句を知っている程度の知識でしかなかった事項について深く掘り下げて学習することができ、非常に有意義であったと思う。今後の学内での PKI の展開に際して有効であると思われる。
　あえて要望するとすれば、実習などにおいてグループ討議等、受講生間で連携して取り組めるような課題があれば、よりコミュニケーションが深まると思う。
　セミナー会場では、無線 LAN 等の設備も整っており、事前事後の予習復習に非常に有効であった。会場周辺は避暑地で有名なところであり、真夏でも非常に快適な環境で受講することができた。

８．備考、その他

　PKI の導入に関しては、技術的な面だけでなく運用面での課題が多くあり、学内の調整が困難であることが予想されるが、UPKI 等、他大学の動向を取り入れながら、前進していきたいと思う。
　最後に、カリキュラムの時間外でも講師や受講生、スタッフの方々と有益な情報交換ができたこと、また研修中を通して快適な環境で学習できたことに感謝いたします。