平成１９年度情報処理軽井沢セミナー　レポート

岩手大学 技術部情報技術室
栗田　宏明

１．発表課題のタイトル

「電子事務局化と連携したセキュアなシステム開発の可能性」

２．発表課題の概要

岩手大学の事務局では、ICT を活用することにより、大学における教育・研究支援への利便性の向上と業務の簡素化、効率化、信頼性および透明性の向上を図ることを目的とした「電子事務局化」に取り組んでいる。本セミナーで得た「PKI 認証」の知識と技術を、電子事務局化の一部のシステムに導入することにより、セキュアなシステムの開発と、元来の目的を達成することが可能であると思われる。

３．セミナーで学んだ技術及び知識

（１）　公開鍵暗号方式の基礎

鍵には、１人１人が持つ「秘密鍵」と、世間一般に公開して良い「公開鍵」とがある。２つの鍵の組み合わせにより、暗号化に違いがでる。例えば図１に示すように、Alice から Bob へインターネットを介してデータを送る場合を考える。二人の間には、悪意を持った Carol が潜んでおり、盗聴と Alice のなりすましを企んでいる。下記に鍵の違いによる暗号化の種類と特徴を記す。

(ア) 署名認証　　Alice の秘密鍵で暗号化 ⇒ Bob は、Alice の公開鍵で復号化する。
Carol は盗聴ができるが、Alice のなりすましができない。

(イ) 秘匿　　Alice は Bob の公開鍵で暗号化 ⇒ Bob は自分の秘密鍵で復号化する。
Carol は盗聴ができないが、Alice のなりすましができる。

(ウ) 署名認証秘匿　　Alice の個人鍵で暗号化したものをさらに Bob の公開鍵で暗号化 ⇒
Bob は、自分の秘密鍵で複合化しさらに Alice の公開鍵で復号化する。
Carol は盗聴もなりすましもできない。

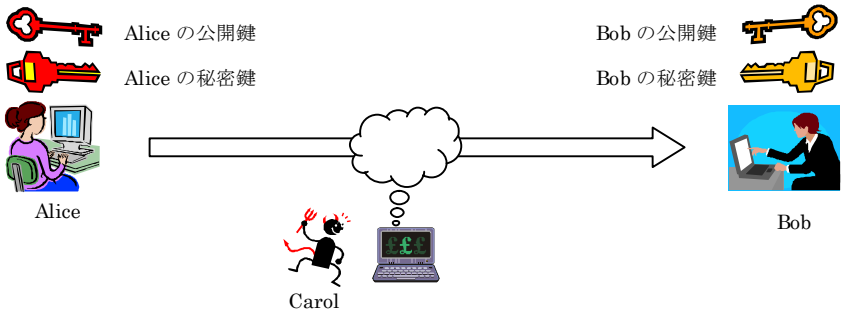

図1　公開鍵暗号方式の基礎

（2） 公開鍵証明書と認証局（PKI について）

PKI の特徴は、公開鍵証明書で公開鍵の授受を行うことである。公開鍵証明書は信頼性がなによりも重要である。信頼性のある証明書を管理・発行する機関を認証局（CA）と呼ぶ。

(ア) 公開証明書

CA が発行する証明書は、ITU-T 勧告 X.509 の規格に準じており、公開鍵の値のほかに、公開鍵のアルゴリズムや鍵の持ち主の名前、発行した認証局の名前、有効期限などの情報が記載されている。

(イ) 信頼性のある認証局を運用するには

専門の知識や技術を持った集団で組織する。CA 独自の CP/CPS を作成して公開し、社会的信頼性を得ることが必要。

CP (Certificate Policy) 証明書の目的、利用用途の規定

CPS (Certification Practices Statement) CA の運用規定。認証実施規定。

(ウ) 認証局の階層構造の実現

インターネットの DNS のように、CA も階層構造にすることができる。階層構造には、最上位にルート CA を置き、トップダウンで認証を行う方式と、下位 CA と認証のやり取りを行うブリッジ CA とがある。

なお、公開証明書の例は、Internet Explorer を起動して、ツール→インターネットオプション→コンテンツ→証明書のボタンをクリックすると、見ることができる。

（3） UPKI 計画

UPKI（University Public Key Infrastructure）は、全国の大学を同じ仕様の認証局で結び、大学が有している学術資源や設備資源をネットワーク上で共有する構想であり、CSI (Cyber Science Infrastructure) 最先端学術情報基盤の中心事業として進められている。身近な例をあげると、離れた大学間で共同研究のプロジェクトを組んだとき、研究者同士での研究成果のやりとりは暗号化したい。もしそれぞれの大学に CA が存在し、階層構造になっていれば、研究者同士での認証と暗号化は容易であり、安全な通信路が確保できる。

UPKI は次の 3 層構造で構成される。

(ア) オープンドメイン PKI　ルート CA に相当するもので、サーバー証明書を発行する。

(イ) キャンパス PKI　各大学独自で持つ認証局。共通仕様の CA を構築するには、NAREGI-CA などがある。

(ウ) グリッド PKI　各大学で所有する計算機資源を安全に共有する。

（4） Shibboleth を利用した Federate 認証

(ア) shibboleth は、1 度の認証で、さまざまなサービスを利用できる SSO（Single Sign-On）を実現する SAML を拡張したもの。利用者や、サービスを提供するサイト（SP : Service Provider など）がどこにあっても、利用できる。

(イ) shibboleth の特徴は、個人個人の属性を扱うことができる。属性とは、例えば、Alice は、コンテンツ A と B と C を参照できるが、Bob はコンテンツ A しか参照できない。というように、ユーザを身分や所属などで特徴付けるもの。

(ウ) 属性を交換する組織の集合体を Federation（同盟）と呼び、個々の組織が属性を分散管理する。

（５） Grid コンピューティングと認証の連携

(ア) Grid とは、ネットワークを介して、計算機資源を共有するものであり、①Computational Grid（計算資源の仮想化）、②Data Grid（DB やファイルなどの仮想化）、③Service Grid（サービスの仮想化）などの種類がある。

(イ) Grid は、ネットワークを介して仮想化されるので、安全な通信路（通信相手が本人であること、他人に盗聴されない、改ざんされない）を構築しなければならない。安全とは、Trust（信頼）の構築であり、技術と組織がしっかりしていて、かつ、第３者から安全である「お墨付き」がなければならない（TTP：Trusted Third Party　信頼すべき第三者機関）。

(ウ) Grid 認証の特徴は、GSI（Grid Security Infrastructure）であり、サイトをまたがって相互認証や、権限委譲ができる。

４．セミナーの成果

- 情報技術室と事務局が合同で研修会を開く。本セミナーで受講した内容をその研修会の中で発表する予定である。
- 認証サーバーNAREGI-CA を Fedora Core 7 でコンパイル・インストールに成功した。現在、PKI 認証システムの動作について検証を行っている。その結果、本大学で CA の運用が可能であるかを探る。なお、Vine Linux 4.1 でもコンパイル・インストールを試みたが、エラーが出た。Red Hat 系だけではなく、Vine や SUSE などにも対応すれば、NAREGI-CA はもっと普及するのではないかと思う。

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

- http://www.atmarkit.co.jp/fsecurity/special/02fivemin/fivemin00.html
  タイトルに「５分で絶対にわかる PKI」とあるとおり、PKI の原理から認証局の重要性までを簡潔にまとめられている。PKI の詳しい説明にもリンクが張られている。
- http://www.blwisdom.com/rtech/13/
  SSO（シングルサインオン）の意味と、shibboleth の概要について簡単に述べられている。

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 と PGP の違いについて
- Shibboleth の概要と、shibboleth 実習で用いた certreq コマンドの詳細
- LDAP の詳細
- Openssl 等による証明書の作り方

７．セミナーの感想

PKI 技術を基礎に、SSO の最新技術である shibboleth や Grid について学ぶことができた。特に shibboleth では、metadata の設定などの実習を行いながら、実際に触れることができ、大変勉強になった。できれば、shibboleth をインストールするところから始めてみたかった。

講師の先生方やスタッフの皆々様には、寝食を共にしながら懇切丁寧にご指導をいただき、心より厚くお礼申し上げます。