1H-4

自律的組織の集合体としての大学における PKI の運用

西村　健†　　佐藤　周行‡
東京大学情報基盤センター　PKI プロジェクト†‡

1. はじめに

近年、インターネットの普及や Web アプリケーションの充実によりコンピュータ上での認証の重要性は増す一方であり、それは大学においても例外ではない。

その一つの解として PKI(Public Key Infrastructure, 公開鍵認証基盤)を利用した電子認証が挙げられる。また PKI の別の側面として電子メールや文書の暗号化および電子署名も重要性が高まりつつある。

大学における PKI において問題となるのは、学部、研究科等の各部局がそれぞれ自律的な組織として機能しているため、統一的な認証局を構築することが難しいことにある。本稿では東京大学において PKI の普及を目指す我々 PKI プロジェクトの活動を紹介し、その一環である認証局の構築および試験運用について、実際に数部局において実証実験を行なった知見から判明した問題点およびその解決策、今後の展望をまとめる。

2. 東京大学情報基盤センター PKI プロジェクトの活動

東京大学は 2004 年に大学の教職員および学生の身分証として IC カードを採用し、認証基盤として PKI を整備する計画があるというプレスリリースを出した。情報基盤センターは PKI を整備し、PKI アプリケーションの利用を促進し、PKI 運用コストの最適化を検討し、東京大学および大学一般における最適な認証のフレームワークを開発するために「PKI プロジェクト」を発足させた。[2]

PKI プロジェクトは大学での運用に合わせたプライベート CA(Certification Authority, 認証局)のプロトタイプを構築し、これを UT-CA と命名した。UT-CA は大学内の数部局の協力を得て共同で実証実験を行なっているところである。一方で PKI アプリケーションの普及のため、既存のサーバ群と安全な認証を行なう上での問題に取り組んでいる。[1]

PKI Management Problem of Inter-Department Cooperation in University
†Takeshi Nishimura, PKI Project,ITC,The University of Tokyo
‡Hiroyuki Sato, PKI Project, ITC, The University of Tokyo

3. UT-CA システム構成

UT-CA のシステム構築にあたって第一に考えなければいけないことは、認証局の一部である登録局(Registration Authority, RA)の分散化と、信頼性への担保となる運用面でのセキュリティである。これらは言わば大学特有の面もあり、以下それぞれについて説明する。

3.1. 登録局の分散化

前に述べた通り、大学においては学部、研究科等の各部局がそれぞれ自立的な組織として機能しているため、それらを統合した一つの登録局を置くことが大変難しくなっている。また物理的に離れた複数のキャンパスがあり、人の移動の面からも登録局を分散させることが望ましい。

UT-CA では、各部局に RA クライアントと呼ばれる登録局の支部となる端末を設置し、登録局は部局内の人員に対する証明書発行等の権限を各 RA クライアントに委譲する。各部局での自律を最大限に尊重するため、RA クライアントの操作要員は各部局が用意した人員を充てることとする。

このようにすることで、各部局固有の情報を元に証明書発行／失効の業務ができるようになるとともに、各登録局支部が担当する対象が字部局内の人員に限られるため、対面での本人確認において確実な認証が行なえるというメリットも併せ持つ。

また、部局毎の設置とした場合小規模な部局において過度な付加となるため、複数の小規模部局が合同で一つの登録局を設置することも想定している。

UT-CA のシステム概略は図 1 のようになっている。発行局(Issuing Authority, IA)内にある IA サーバにより証明書の発行等が行なわれる。登録局内にある RA サーバは、RA クライアントから

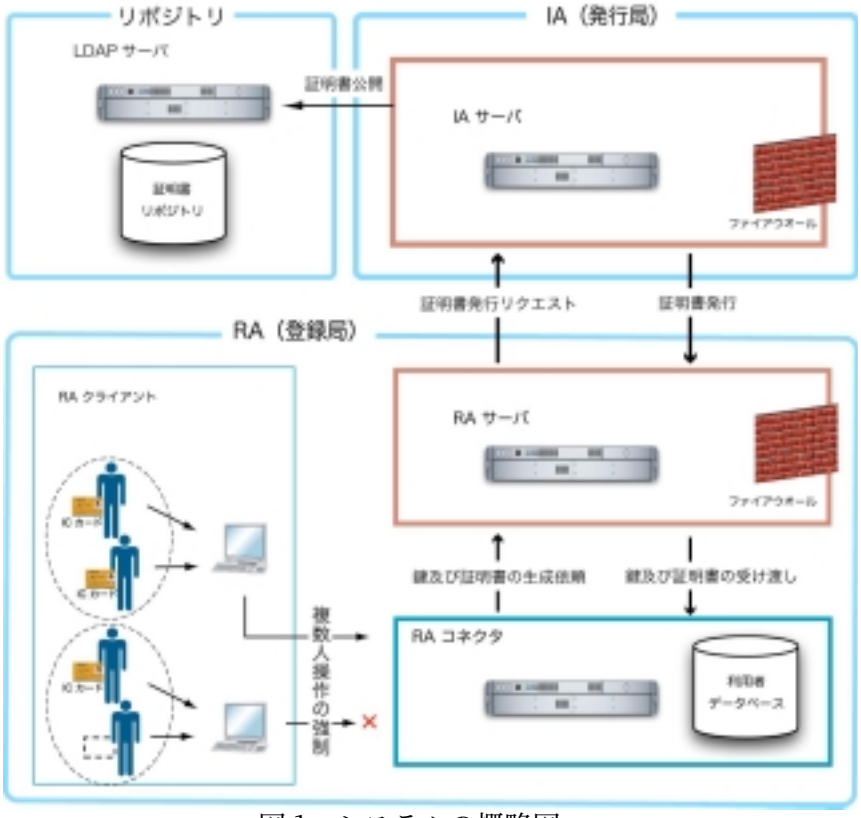

図 1: システムの概略図

の証明書発行依頼にもとづいて IA に対して発行依頼を行なう。RA コネクタは RA サーバと RA クライアントとの仲介を行ない、また利用者に証明書を配付する役割も担う。RA クライアントは各部局に設置され、3.2.で後述する複数人操作の強制の役割も担っている。リポジトリは発行された証明書や失効リストを公開するためのものである。

証明書で利用される識別子については、すでに全学で利用されている共通 ID という、各教職員・学生等大学構成員に割り当てられた部局によらないランダムな数字列を用いている。そのため、RA クライアントからの部局外の人員に対する発行の拒否は単純なアクセス制御では困難である。UT-CA ではマスタデータと呼ばれる、所属部局を併記した共通 ID のリストを別途管理することによりこの問題を回避している。

3.3. 運用面のセキュリティ

認証局でのセキュリティには認証局内の人員による不正の防止も含まれる。UT-CA では認証局の操作に複数人操作の強制を行なっている。例えば RA クライアントにおいては、審査者／承認者と呼ばれる 2 人の操作者を置き、それぞれ専用の IC カードを持つ。2 人が正しい操作をして初めて証明書発行等の操作が完了する。

本運用には設備投資として、可用性を上げるための冗長化、鍵盗難防止のためのハードウェアセキュリティモジュール(HSM)の使用が考えられるが、現在はプロトタイプの実装でありそこまでの実装には至っていない。

4. UT-CA の試験運用

前述の通り UT-CA は試験運用段階に入っている。中でも部局側で負担しなければならないコストは申請書の受け付けから広報・通知に至るまで RA クライアントの操作以外の負担が大きく、オンライン申請を受け付けるなど改善の余地がある。

5. まとめ

本稿では、我々PKI プロジェクトが活動の一環として取り組んでいる、学内認証局 UT-CA の構成について解説した。現在実証実験段階でありそこで得られた知見からより完成された認証局を目指していきたい。

参考文献

[1] T. Nishimura, H. Sato, "Authentication with PKI – a Case Study in Information Technology Center in The University of Tokyo," International Symposium on Advanced ICT, pp. 251-255, Tokyo, Japan, Aug. 2006.

[2] 東京大学情報基盤センターPKI プロジェクト, http://www.pki.itc.u-tokyo.ac.jp/