東京大学認証局(UT-CA)構築に向けて

大島　大輔[†‡]，西村　健[‡]，佐藤　安一郎[†‡]，佐藤　周行[‡]
† アプリケーション支援係　‡ PKI プロジェクト
東京大学情報基盤センター

概要　ここ数年多くの大学，府省庁，民間企業等では情報システムのデータ漏えい事件や不正アクセスなどの被害を受け，安全・安心な認証やセキュリティの重要性が高まってきた。東京大学情報基盤センター（以下，本センター）では大学における安全・安心な認証について，PKI（公開鍵基盤）の調査・研究を開始することになり，プロジェクトを発足した。プロジェクトでは，PKI の技術基盤や認証局構築および運用について調査・研究するほか，それらのコンサルティングを受け，また，利用者に対しては PKI や認証局の理解を得るためにデモンストレーションを行った。本稿では PKI の技術基盤，認証局構築や運用体制構築の調査・研究について，今まで行ったことおよび今後の課題についてご報告する。

1　はじめに

東京大学を始めとする多くの大学では，様々な情報システムが稼動しており，認証についてはセキュリティに不安を抱えながらも ID とパスワードという組み合わせが一般的であろう。そこで本センターでは, 大学における認証の調査･研究を行うプロジェクト (以下, PKI プロジェクトという) [1],[2] を 2005 年 1 月に発足させ，認証に PKI（Public Key Infrastructure:公開鍵基盤)[3]を採用することを前提に検討を開始した。

当初，調査・研究は教員が中心となって行っていた。しかし PKI を使用した認証においては技術面のみならず運用面における検討が重要であることから，事務系職員として本センターアプリケーション支援係が主に運用体制の構築をサポートするべく参画することになった。以下，第 2 章では東京大学の認証の現状，第 3 章では PKI の根幹となる認証局（Certification Authority，以下 CA という）の構築，第 4 章では PKI や CA に対する理解を得るため，利用者に行ったデモンストレーションの模様，第 5 章では今後の展望および課題を説明し第 6 章で本稿の総括をする。

2　東京大学の認証の現状および認証の今後

2.1　東京大学における認証の現状

現在，東京大学の中では，人事・給与システム，財務会計システム，学務システムなどといった情報システムが稼動しており，それらの情報システムなくしては大学の事務や研究は成り立たない。

しかし，それらの情報システムへのアクセスに関するルールはシステム毎にとりきめられ，かつ，それらの多くは ID とパスワードという認証方式で本人性確認を行っている。ID とパスワードという認証は利用者にとって簡単ではあるが，一方セキュリティに関しては，パスワードは高々十数桁の文字，数字，記号の組み合わせであり，総当り攻撃や辞書攻撃など容易であることから，悪意を持った第三者からの情報システムへの不正アクセスは深刻である。このような認証方式は，本学のみならず多くの大学に共通する課題を抱えている。

2.2　認証に PKI を採用した理由

認証については複数の方式があるが，一般的には ID とパスワードの組み合わせが多いだろう。しかし，機密情報を扱うクリティカルなシステムについては，ID とパスワードによる認証では２．１

で述べたように非常に危険である。

PKI プロジェクトでは，認証方式について PKI を採用することとした。なぜならば，PKI は最新の暗号技術を利用してなりすましの脅威を防止することができ，ID とパスワードという認証方式より格段上の安全性を提供するからである。また，正しい運用を行えば現状の認証方式では最強と考えられている。

本学全体においても，取り扱う情報の重要度の違いにより最適な認証は一つに定まるものではないが，少なくとも機密情報を扱うシステムでは認証方式として PKI を採用することになるとの見通しを得た。

2.3 証明書および秘密鍵の格納

PKI プロジェクトにおいてまず検討したのが，証明書および秘密鍵を格納するデバイスの選択であった。候補として挙げられたのはハードディスクと USB トークンおよび IC カードであった。

以下の表 1 で，各デバイスのメリット，デメリットを挙げておく。なお，表中の身分証とは職員（学生）証のことをいう。

表 1　各デバイスのメリット・デメリット

	ハードディスク	USB トークン	IC カード型身分証
メリット	・既設のハードディスクに格納するため費用がかからない ・鍵を使用する PC が限定されていれば，携帯しなくてよい	・「鍵」を持つというイメージにあう。デバイス自体が「鍵」を想像させる ・USB ポートに挿すだけで使える。ただし，ドライバソフトのインストールは必要	・身分証の中に証明書を格納できる ・既に確立した教職員，学生への配付方法がある ・USB トークンと比較して安価
デメリット	・パソコンの盗難や，ネットワーク経由での不正侵入等の可能性があり，セキュリティ面で不安がある	・常時携帯している身分証の他に携帯しなければならない ・デバイス自体が高価	・IC カードを認識するための読み取り機器が必要 ・券面に個人情報が記載されており，盗難の際紐づけて悪用される恐れがある

東京大学では現在，身分証を IC カード化し教職員・学生に配付している。PKI プロジェクトでは，IC カードへの証明書格納を最優先とし，その他のデバイスについても順次検討することとした。

3　UT-CA の構築

PKI の I は Infrastructure（インフラストラクチャ）の頭文字であり，PKI の根幹となる CA が必要である。そこで PKI プロジェクトでは，まず本センター構成員（約 80 名）を対象とした小規模で CA の試験運用を行った。それを足がかりとして CA の全学展開に耐えうる技術基盤の提供を目標とし調査・研究を開始した。その名称を UT-CA とした。なお，UT-CA とは The University of Tokyo Certification Authority （東京大学認証局）の頭文字をとった造語である。UT-CA は第三者からの意見も参考にしつつ 2006 年 3 月末に完成した。

3.1 CA 構築に必要な要素

CA 構築に必要な要素としては，運用体制，CA の構成および CA 構築・運用における費用の 3 つが挙げられる。以下それぞれについて説明する。

3.1.1　運用体制

運用体制の確立は CA 構築にはもっとも必要かつ重要な要素である。東京大学のルート認証局の担当者のほか，CA を運用するために，各部局に対して登録業務の権限を委譲する分散管理体制をとることにした。なお，東京大学において部局とは，学部，研究科，附置研究所，本センターを含む全学センター等である。

PKI の安全性の担保は，サーバの要塞化やサーバ管理室の厳重な管理，そして CP/CPS（Certificate Policy / Certification Practices Statement :証明書ポリシ/認証局運用規定）であるが，最重要なのが的確な運用をすることである。例えば，担当者一人の暴走を防止する体制が挙げられる。そのためには相互牽制を行える運用体制づくりが必要である。

運用体制には様々なモデルがあるが，PKI プロジェクトのモデルは各部局に管理者を 2 名置き，それぞれの役割を「審査者」と「承認者」に分け，2 人がいないと証明書が発行できない運用体制にした。

また，部局によっては PKI の全体像や詳細を知らずに担当者となる場合がある。そのため部局担当者を対象とし，1，2 日程度の教育で担当者としてのスキルを身につけることのできる教育プログラムを作成しなければならない。

3.1.2　UT-CA の構成

図 1 は UT-CA の構成を説明したものである。それぞれの役割を簡単に説明する。IA サーバは証明書の発行を行う。CA 鍵は IA サーバ内の HSM(Hardware Security Module）で安全に管理される。RA サーバは RA クライアントからの鍵および証明書の生成依頼にもとづき IA に発行依頼をし，そのほか，鍵の代理生成も行う。RA コネクタは，RA サーバと RA クライアントとの仲介を行い，利用者に証明書および秘密鍵を配付する役割も担う。RA クライアントは基本的に各部局に存在し，部局の担当者が操作するものであり，利用者の PKI 利用申請にもとづき RA サーバに対して鍵および証明書の生成依頼を行う。なお，RA クライアントはシステムとして複数人による操作を強制する。発行された証明書は，リポジトリ用サーバ（LDAP(Lightweight Directory Access Protocol)サーバ）において公開される。

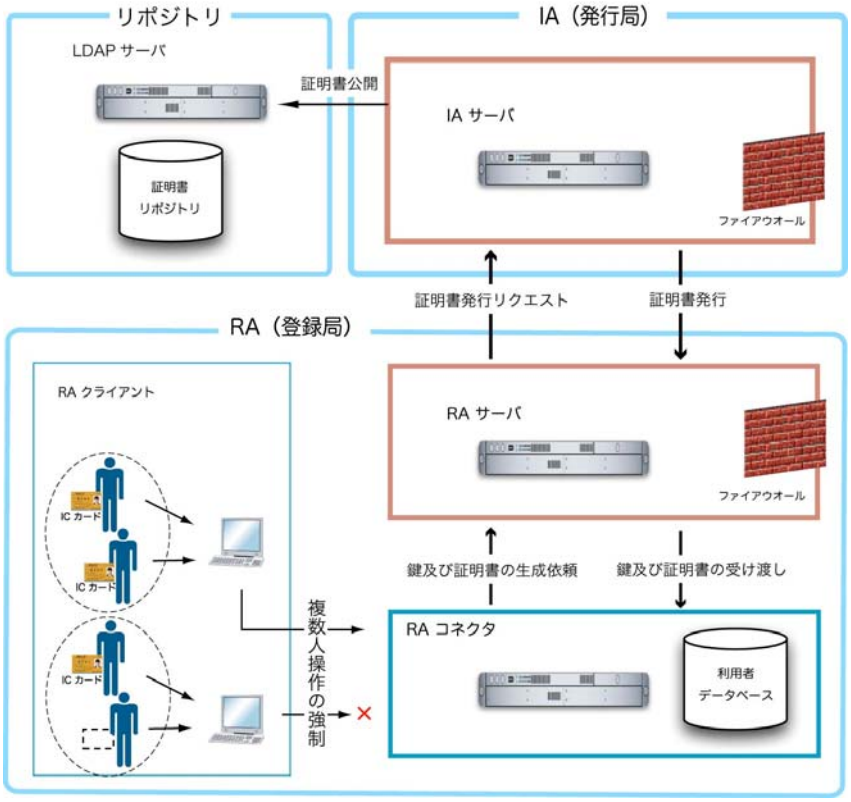

図 1　UT-CA 構成の概念図

また，図２は後述のデモンストレーション時に用いた UT-CA のサーバ群である。
なお，CA 構成の要件ではないが，PKI 用のアプリケーションを５．３で後述する。

図２　UT-CA サーバ群
UT-CA サーバ群には IA サーバ，RA サーバ，RA コネクタ，LDAP サーバ，利用者用 DB がある

3.1.3　CA 構築・運用の費用

CA 構築を実現するためには費用を必要とする。イニシャルコストとランニングコストである。
イニシャルコストでは３．１．２で挙げたハードウェアの調達費とソフトウェアの開発費が必要である。また，全学規模に対応するにはサーバの増設，各部局に配付する RA クライアントの費用も必要である。その他についても東大規模の費用見積りを精力的に行っている。
ランニングコストについても，証明書のライセンス，ハードウェアとソフトウェアの年間保守契約などにかかる費用および認証局担当者と部局担当者などの人件費を評価し，鋭意検討中である。

3.2　小規模 CA の導入

全学に対応した CA を構築するためには，CA 要素の技術的な理解を深めることや運用面での経験を積むことが必要であると考えた。そこで PKI プロジェクトでは，ここまで述べた UT-CA 構築の前段階として本センターの構成員（約 80 名）に証明書を発行する既製品の小規模 CA を導入した。サーバの設置からネットワークの構築，証明書の発行フロー，運用体制など，UT-CA を設計するうえで役にたった。
小規模 CA を運用しているうえで証明書の発行体制について気付いたことは，UT-CA を全学展開した場合，１人で証明書を発行できる体制は大変危険であると認識し，各部局に２人以上の担当者を置いて相互牽制を必要とすることが分かった。

3.3　コンサルティングの活用

PKI プロジェクトでは 2005 年 10 月に，全学展開に対応できる認証局のシステムのプロトタイプを構築することを決めた。同時に CA 構築および運用に関する第三者からの意見の必要性を認識しコンサルティングを受けた。

コンサルティングの必要性を認識した理由は以下の３つに大別される。
・大学という特殊な組織に対応した既製品がない
・認証（特に PKI）についてのノウハウを持つベンダの意見を参考にしたい
・今まで PKI プロジェクトが調査・研究してきた内容，方向性の正しさを確認したい
なお，今回は NTT コミュニケーションズ株式会社に発注した。

コンサルティングの概要は以下のとおりである。
・認証基盤の概要
・証明書ライフサイクル管理
・鍵ライフサイクル管理
・認証基盤の運用環境の管理

コンサルティングは CA の構成や運用体制について，PKI の最前線にいる人たちならではの事例を交えた話も聞くことができ大変参考となった。コンサルティングにはそれを聞く側にも事前準備が必要である。PKI プロジェクトにおいても PKI や CA の構成および運用体制について，小規模 CA を運用することで調査・研究を行ってきた。その結果 UT-CA の設計について非常に活発な議論をすることができた。そして今回のコンサルティングについては，ベンダの持つノウハウと PKI プロジェクトがそれまで調査・研究してきた結果をマッチングさせ，UT-CA の設計に反映させることができた。

４　デモンストレーション

パイロット版完成後 PKI プロジェクトで計画したことは，本学の意思決定に関与する方や一般利用者に対して，PKI および認証局に対する理解を得るため，UT-CA という成果物を見ていただくことであった。そして 7 月 28 日にデモンストレーションを実施（図３）し，評価は概ね好評であった。デモンストレーション参加者に認知してもらえたことは，今後の調査・研究に弾みがつくであろう。

デモンストレーションの内容については，時間配分を飽きのこない構成にした（表２）。また，PKI，認証局といった一般の人には理解しづらいものを，アプリケーションのデモンストレーション（図４）や，認証局の役割について寸劇を行い理解の手助けをした（図５）（図６）。

表２　デモンストレーションタイムテーブル（7 月 28 日）

時　間	内　　容	備　　考
14:00	デモンストレーション開始	PKI の概要を説明後，簡単な質疑応答を行った
14:15	PKI を使ったアプリケーションデモ	使用アプリケーションは SSL-VPN と S/MIME
14:30	認証局運用体制の説明	配役を決め，それぞれの役割について寸劇を行った
14:50	全体についての質疑応答	
15:00	デモンストレーション終了	

図 3　デモンストレーション風景

図 4　S/MIME のデモンストレーション

図 5　役者（役割）の紹介

図 6　部局窓口担当者（左から 2 番目）と一般利用者（左から 3 番目）との PKI 利用申請についてのやり取り

5　今後の展望および課題

5.1　他部局への協力依頼と UT-CA の広報

全学的な認証局を構築するうえで，PKI プロジェクトでできることには限界がある。例えば，本センターには学生が所属していないため，学生に証明書等を配付するノウハウはない。そこで学部学生や大学院生が所属している部局に証明書等の配付を依頼し，配付に対する本務への負荷などを把握する必要がある。

それには認証の重要性を認識し，PKI の需要があるものと予想される部局に交渉し，2，3 の協力部局にテストをお願いする。そして全学展開規模での展開を想定した技術，ノウハウの蓄積を行いたい。

また，今後の予定としては，7 月に行ったデモンストレーションの拡張版として，本郷キャンパスのほか，柏キャンパスや駒場キャンパスなど，可能な限り各部局に出張し PKI および UT-CA の広報を考えている。

5.2　CP/CPS の作成

認証局の憲法というべき CP/CPS（Certificate Policy / Certification Practices Statement :証明書ポリシ/認証局運用規定)については，大学という組織の特殊性を勘案し独自に作成しなければならない。これについては十分なコンサルティングを受け，作成に着手できる段階に近づいている。加えて国立情報学研究所の重点プロジェクトである UPKI(全国共同電子認証基盤)[4]では PKI の大学間連携を計画しており，これと協力して大学間連携可能な CP/CPS 作成を進めていきたい。

将来，PKI プロジェクトの成果の一部として CP/CPS を公開することになろう。

5.3 利用者のご利益

PKI プロジェクトではよく「利用者のご利益」という言葉を使用する。我々は PKI について調査・研究を行い利用者の利便性を考えつつ，セキュリティの重要性についても広報を行っている。しかし，多くの利用者にとっては，セキュリティの重要性がなかなか実感できないのが現実である。それよりも PKI を使うことで利便性が高まれば，その効果を実感しやすいと考えている。

そこで PKI プロジェクトでは「利用者のご利益」となるべく，PKI アプリケーションを模索，開発している[5]。PKI を使うことにより結果的に安全性も担保されれば，PKI プロジェクトにとっても目的が達成されると考えている。

以下で PKI プロジェクトが検討しているアプリケーションを挙げる。

・SSL-VPN(Secure Socket Layer Virtual Private Network)[6]

すでに本センター図書館電子化部門では SSL-VPN の試験運用を開始(http://sslvpn.r.dl.itc.u-tokyo.ac.jp/)[7]しているが，認証方式は従来の ID とパスワードに依存している。

今後の事務電算システムや電子ジャーナル等の利用者サービスは，より Web 化がされることは間違いない。そのときに安全な経路として SSL-VPN がより一層注目され，さらにその情報システムへの入口となる認証には PKI が使われることになるだろう。

・事務ワークフロー（電子決裁，S/MIME，グループウェア）

今後の利用を期待されるのが，電子署名を利用した電子決裁である。今までは認証のことだけを記述してきたが，本来 PKI については認証のほかに電子署名という役割がある。ここでは電子署名についての詳細は述べないが，物理的な押印に対応する機能である。その電子署名を使用し，今まで行っていた紙の上での決裁をオンライン上で行うことができる。また，S/MIME も応用として考えている。

さらに，どこの大学でも使われているだろうグループウェアの認証にも PKI の技術を応用することができる。

・SSO(Single Sign On)

一般利用者にも PKI のメリットが分かり易いアプリケーションである。

主として事務系の一般利用者にとっては，コンピュータは単なる事務処理のツールとして認識されている。その単なるツールにすぎないコンピュータの認証方式（ID+パスワード）は現状システムによって勝手に割り振られるため，ID 管理の煩雑さに戸惑っている。秘密のノートにサーバ毎の ID とパスワードを管理してくれればまだよいが，平気でディスプレイの隅に ID とパスワードを付箋で貼っている人もいるのは事実である。

そこで，SSO と PKI を組み合わせた認証を一般利用者に分かりやすい表現で説明をすると，「安全性と利便性が保たれている」と概ね好評である。

5.4 道なかば…

UT-CA の全学展開に向けて PKI プロジェクトの調査・研究は継続している。

また，PKI は着々と次のステージへ向かっている。総務省が提唱する u-Japan 政策である[8]。u-Japan 政策とは総務省によると「2010 年までにユビキタス（いつでも，どこでも，何でも，誰でも）ネット社会の実現」を目指すものである。そして「いつでも，どこでも，何でも，誰でも」には当然，安全・安心な認証が必要となる。PKI プロジェクトでは大学における認証（PKI）の調査・研究を行い，ノウハウを蓄積し，来るべきユビキタスネット社会にも対応できる PKI を提案したい。

６　まとめ

PKI プロジェクトが今までに行ってきたことは，認証方式および鍵を格納するデバイスの検討，その結果として UT-CA の構築，利用者に PKI や CA について理解を得るためのデモンストレーションである。UT-CA は各部局に対して登録業務の権限を委譲する分散管理体制や証明書の発行時における相互牽制を可能するといった特長を持つ。さらに，UT-CA 構築に向けての協力部局の候補も挙がりつつある。

今後の課題としては，利用者に対して利便性の向上となる PKI 向けのアプリケーション構築，大学という組織の特殊性を勘案した CP/CPS の作成, PKI の全体像や詳細を知らずに担当者となった人向けの教育プログラムの作成が残っている。

また，今後の予定としては，UT-CA の理解や広報のため，可能な限り各部局に行き PKI や UT-CA の説明を行いたい。

【参考文献】

[1]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/

[2]「デジタル世界の身分証明書」，佐藤周行，Digital Life Vol.6 (東京大学情報基盤センター広報誌：http://www.itc.u-tokyo.ac.jp/DigitalLife/Vol6/Digital_Life_Vol.6.pdf)，pp.3-4，ISSN 1345-3017，2005-2006.

[3]「PKI 公開鍵インフラストラクチャの概念，標準，展開」，カーライル・アダムズ，スティーブ・ロイド，ピアソン・エデュケーション，ISBN:4-89471-248-2，2000.

[4]情報・システム研究機構　国立情報学研究所 : http://www.nii.ac.jp/research/project_gaiyo-j.shtml

[5]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, 2006.

[6]「PKI の利用例～情報基盤センター内向け PKI 対応 SSL-VPN の紹介」, 西村健, Digital Life Vol.7 (東京大学情報基盤センター広報誌：http://www.itc.u-tokyo.ac.jp/DigitalLife/Vol7/Digital_Life_Vol.7.pdf)，pp.38-40，ISSN 1345-3017，2006.

[7]「ECCS アカウント認証による附属図書館 FELIX サービスの学内利用」，清田陽司，Digital Life Vol.7 (東京大学情報基盤センター広報誌：http://www.itc.u-tokyo.ac.jp/DigitalLife/Vol7/Digital_Life_Vol.7.pdf)，pp.13-14，ISSN 1345-3017，2006.

[8]総務省：http://www.soumu.go.jp/menu_02/ict/u-japan/index.html