特　集

大学間連携のための全国共同電子認証基盤（UPKI）構想

UPKI：University Public Key Infrastructure

名古屋大学情報連携基盤センター 助教授
Information Technology Center, Nagoya University

国立情報学研究所 客員助教授（連携）
National Institute of Informatics

平野　靖
HIRANO, Yasushi

Abstract

In this paper, the UPKI project is introduced. The UPKI project is promoted by NII (National Institute of Informatics) and several universities and research institutes in Japan. The aims of this project are operation of CA to issue digital certificates for universities, establishment of a model for digital personal authentication for universities, assistance of establishment for grid computing and so on. The UPKI project is a part of the CSI project, and the accomplishment of this project is important to the establishment of the academic information infrastructure in the near future.

１．はじめに

国立情報学研究所では次世代の学術情報インフラストラクチャを構築するために，最先端学術情報基盤（CSI）構築事業を行っている．CSI 事業は物理的なネットワークからバーチャルな研究組織構築までを含む非常に幅広い個別の事業から成り立っている．本稿では，CSI 事業の概要と電子認証基盤について紹介する．

２．最先端学術情報基盤（CSI）構築事業

2.1　CSI 事業の目的

最先端学術情報基盤（Cyber Science Infrastructure, CSI）構築事業がターゲットとする領域は，図１に示すように幅広く，物理的なネットワークなどのハードウェア，認証システムや大規模計算のためのミドルウェア，コンテンツ，およびバーチャルな研究組織の構築など多岐にわたる．これらを一体として構築することによって包括的な最先端の学術情報基盤が出来上がり，今後の学術・産業分野での国際協調に貢献し，さらには国際競争でも有利な立場に立てると考えられる．諸外国でも CSI 事業に含まれる分野が研究され，実用化されている例も少なくない．たとえば欧州の学術ネットワークである GÉANT2 [1)] や，internet2 が開発する認証基盤である shibboleth [2)]，JA-SIG が開発する Single Sign-On システムである CAS [3)]，および米国で機関リポジトリを推進する SPARC [4)] などが挙げられる．しかし，これらは個別の研究機関，研究組織などがそれぞれ行っている場合が多く，必ずしも有機的に結びついているとは言いがたい．

日本の場合には，国立情報学研究所が国内の多

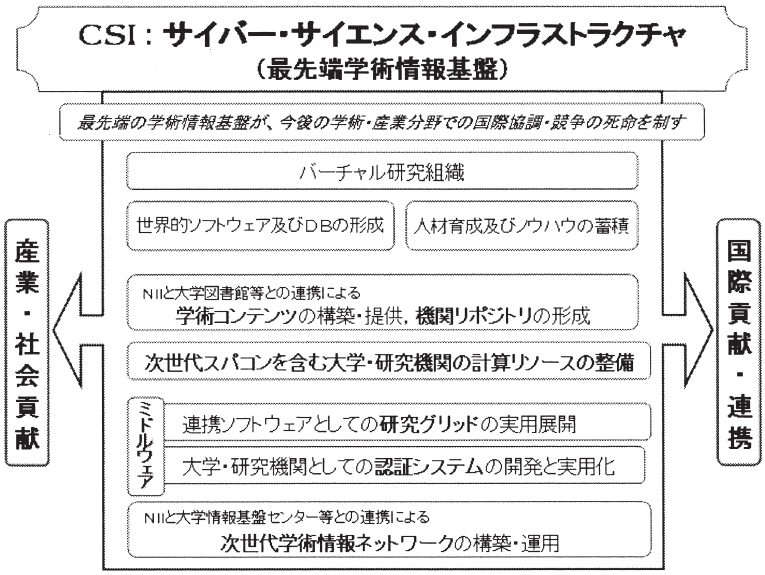

図１　CSI 事業の概要

くの研究機関とともに CSI 事業を推進していくことによってそれぞれの分野間の有機的な繋がりを作るとともに，日本としての標準的なモデルを作ることにより，CSI 事業の成果として構築されたシステムをさまざまな研究機関が導入しやすい状況を作り出し，下記の項目を実現することを目的とする．

- ●知的技術立国化の加速
- ●新たな ICT 産業の創出，および ICT 人材育成
- ●国際・産官学の共同研究
- ●大学の社会基盤化の促進
- ●世界最先端の学術研究基盤の実現
- ●NAREGI，SINET，GeNii との連携
- ●学術資源（コンピュータ，ネットワーク，コンテンツ）の安全・安心な共有・利用・流通基盤の実現

2. 2　国内研究機関との連携

前述のように，CSI 事業が目的とするものは幅広く，かつ専門性を要求されることから，国立情報学研究所だけでなく，全国のさまざまな研究機関と連携をとりながら進められている．具体的には，国立情報学研究所と大学・研究機関が共同で学術情報ネットワーク運営・連携本部と学術コンテンツ運営・連携本部を設置し，前者には７つの旧帝大，東工大，高エネルギー加速器研究機構などの研究機関が，後者には７つの旧帝大，早稲田大，慶応大，国文学研究資料館などが参画している．学術情報ネットワーク運営・連携本部は，情報基盤センター（名古屋大学の場合には，情報連携基盤センター）などの計算資源，ネットワーク資源を管理・運用する部局のセンター長がメンバーとなり，次世代学術情報ネットワーク，電子認証基盤，グリッド環境の整備を目的とする．一方，学術コンテンツ運営・連携本部は附属図書館長や情報関連部局長などがメンバーとなり，学術コンテンツ形成と学術機関統合情報発信システムの構築を目的とする．それぞれの運営・連携本部の下部には，より具体的に事業を推進するために，現在，下記の合計５つの作業部会が設けられている．

学術情報ネットワーク運営・連携本部
- ・ネットワーク作業部会
- ・認証作業部会
- ・セキュリティポリシー策定作業部会
- ・グリッド作業部会

学術コンテンツ運営・連携本部
- ・機関リポジトリ作業部会

本稿で紹介する大学間連携のための全国共同電子認証基盤（UPKI）は認証作業部会が中心となって推進している．また，いずれの作業部会も単独で行動しているわけではなく，互いに連携して事業の推進にあたっている．

CSI 事業の概要はこのぐらいにして，以下では，本稿のテーマである UPKI の紹介を行う．

3．大学間連携のための全国共同電子認証基盤（UPKI）

3. 1　UPKI の概要

UPKI は認証作業部会が中心となって構築が行われている事業であり，学内認証基盤を相互認証しあうことで大学間連携を実現することを目的とする．大学には教育研究用のコンピュータや電子コンテンツ，学内 LAN などの資源が存在する．これらの資源を安全・安心に有効活用することができれば，最先端学術研究の加速の支援や，学術人材の流動への対応が可能になる．たとえば，名古屋大学の教員が他の大学に出張した場合，出張先の大学の認証基盤では，名古屋大学の教員が本当に名古屋大学の教員であるかを認証することができないし，どのような権限を持っている人であるのかを確認することもできない．もし，それぞれの大学の学内認証基盤が相互認証しあい，他の大学の教員や学生であってもその素性を知ることができれば，その人にさまざまな資源を安全・安心に提供することができる．具体的には，無線 / 有線 LAN の提供や電子コンテンツの共有，単位互換などに利用できると考えられる．

ところで，UPKI とは，どういう意味であろうか？　GPKI（政府認証基盤）[5] や LGPKI（地方公共団体における組織認証基盤）[6]，JPKI（公的個人認証）[7] など，さまざまな分野で PKI（公開鍵認証基盤，Public Key Infrastructure）という技術が使われるようになってきている．PKI の技術的な詳細は省くが，この技術を用いることにより，人間ひとりひとりや役職に，あるいはコンピュータ（Web サーバなど）に電子的な証明書を付与することが可能になる．この電子証明書を使用すると，本人の真正性が証明できるだけでなく，電子ファイルや電子メールに電子署名を施してデータの真正性を保証したり，暗号化したりするということが可能になる．UPKI では，主にこの技術を使い，大学（University）の実情に即した汎用的な（Universal），どこでも（Ubiquitous）使える認証基盤を構築することを目的としており，これが UPKI の名称の由来である．ただし，PKI に限定せず，利用目的に応じた認証技術を幅広く扱う．なお，便宜上，本原稿の英文表題には「University Public Key Infrastructure」と表記した．

3. 2　想定する UPKI の効果

UPKI は，PKI を利用した学内認証基盤のためのガイドライン作りと，学内認証基盤の相互認証による大学間認証基盤の構築，という２つの目的を持っている．学内認証基盤が構築されるだけでも学内の情報リソースや電子データ（電子メールや電子ファイルなど）を安全・安心に利用できる環境を構築することが可能になるが，これに大学間認証基盤が加わることにより，下記の効果が期待できる．

- ・大学間の相互認証：研究資源・教育コンテンツの有効活用（e-learning，単位互換）
- ・電子署名・暗号化：情報漏洩・なりすましの防止によるセキュリティ強化．研究成果の真正性の証明．電子決済・電子回覧による効率化
- ・ネットワークローミング：無線LAN．公衆Web端末
- ・グリッドコンピューティング：７大学スパコンリソースをCSI上に統合．京速コンピュータ時代へ向けての利用者管理基盤

さらに，副次的な効果としては，大学間連携の強化が挙げられる．

3. 3　UPKI のアーキテクチャ

UPKI 事業で採用する中心的な認証方法は PKI である．前述のように，PKI は Public Key Infrastructure であるが，PKI にはいわゆる Public なものと Private なものが存在する．前者はベリサインや NTT コミュニケーションズ，セコムトラストシステムズなどが運用する認証局（CA，Certificate Authority）を利用するもので，身元を証明し，料金を支払えば誰でも利用できる．後者は特定の組織内だけで利用できる CA を利用するものである．一般向けに公開するサーバ（Web サーバなど）や，不特定の人とのメールのやり取りにおいては，Public な CA から発行された電子証明書を利用する必要がある．一方，組織内だけに公開するサーバや，組織内で回覧される電子ファイルに対する電子署名や暗号化では必ずしも Public な電子証明書は必要ではなく，Private なもので十分である．なお，一般的に Public な電子証明書を購入するには，発行する枚数に応じた料金が必要になる．Private な証明書の場合には，Private CA

の運用の仕方に依存するが，もし組織内で運用するのであれば運用コストのみが必要となるし，運用をアウトソーシングするのであれば枚数に応じた料金が必要になる場合もある．

UPKI 事業では，Public PKI と Private PKI の両方を併用することを計画している．図２に UPKI のアーキテクチャを示す．UPKI では３層の PKI を考えており，それぞれ一般公開用サーバやメールの署名・暗号化用の Public PKI，学内の学生・職員などを対象とする Private PKI，およびグリッドコンピューティング用の Private PKI である．なお，図２では３つの階層が描かれているが，CA の階層（木構造になっており，上位 CA が下位 CA を認証する）とは一致しない．各層について，もう少し詳しく説明する．Public PKI の層では，国立情報学研究所（NII）が設置する Public CA から発行される電子証明書を，Web サーバやメールクライアント（Thunderbird や Outlook Express などのメーラー）などに組み入れ，暗号化・署名などに使用する．このような Public な用途に使える電子証明書は場合によっては非常に安価で，あるいは無料ででも入手できるが，これらの証明書は，サーバの運営者やメールの受け取り手本人の存在・真正性を確認しないまま発行されることも少なくない．一方で，大手の電子証明書発行企業で発行してもらうためには，非常に手間がかかる上に，費用も高い．そこで，国立情報学研究所では，大学相手であるという制限を設けた上で，大学の実情にあった発行手順で，比較的安価に存在性・真正性の確認を行った電子証明書を発行する．

２番目の階層である「学術系 PKI」とは，各大学に用意される CA の層である．これによって大学内向けのサーバとクライアント間の暗号化通信や，電子ファイルの署名・決済などの大学に閉じた用途向けの電子証明書の発行を行う．ただし，このままではある大学で発行された電子証明書は，その大学内でしか使用できない．そこで，各大学の CA を相互認証させることにより，たとえば名古屋大学の職員が名古屋大学で発行された電子証明書を使って，大阪大学でユーザ認証を受け，大阪大学の情報リソース（無線 LAN やコンピュータなど）を利用できたり，学生の単位互換が可能になったりする．

３層目のグリッドコンピューティング用の「グリッド認証基盤」は，大学に設置されているスーパーコンピュータを仮想的な巨大なコンピュータとして使えるようにするためのもので，ユーザに Private な電子証明書を発行することによって，ユーザはグリッドコンピューティングに参加する任意のスーパーコンピュータで認証され，自動的に負荷が低いコンピュータでプログラムを実行させることが可能になる．

3. 4　国立情報学研究所と各大学の役割

認証作業部会には，国立情報学研究所といくつかの大学・研究機関が参画している．それぞれの

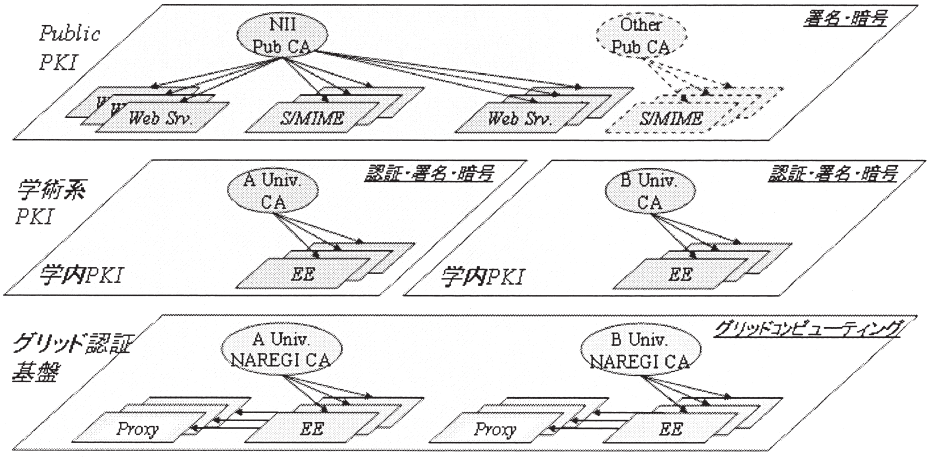

図２　UPKI のアーキテクチャ

役割は，

国立情報学研究所：UPKI の構築

大学：学内認証基盤の構築，および UPKI 上で動作するアプリケーションの開発

となっている．

名古屋大学の学内認証基盤は，CSI 事業が開始される以前に構築がなされており，実際に学生や職員が利用している．現在は，PKI は導入されていないが，全学 ID とパスワードで本人認証を行い，名古屋大学ポータル[8]や情報メディア教育センターの端末利用，メールエイリアス実験サービス[9]などで使われている．その他，http://www2.itc.nagoya-u.ac.jp/center/id.htm に全学 ID で認証を行うサービスの一覧が公開されている．今後，IC カードを搭載した学生証･職員証の導入や，PKI の導入なども計画されており，より安全で，より使いやすい学内認証基盤になるように検討を進めている．

各大学が行うべきもう一つの役割であるアプリケーションの開発について各大学の提案を図３に示す．名古屋大学からは「IC カードによる公衆端末の個人専用機化」を提案している．学内のさまざまな場所にユーザ認証を行わない設定になっている公衆 PC が存在し，誰がいつ使ったのか分からない状態となっている．また，このような公衆 PC で古い OS が稼動している場合には，その公衆 PC に不特定の人間がソフトウェアをインストールできる可能性もある．これは大学として非常に危険な事態を引き起こす可能性がありうる．たとえば，SPAM メールやウィルス・メールを撒き散らすようなソフトウェアをインストールされたり，出版社から購入している電子ジャーナルを大量にダウンロードされたりするかもしれない．このような事案は，行為者のほかに，大学としての責任を問われる可能性がある．

もし，大学が利用資格を与えたものだけが公衆 PC を使用でき，誰がいつ使ったかが分かれば，犯罪的な行為の抑止効果があり，万一，犯罪的な行為が行われたとしても犯人を特定することが可能になる．そこで，我々は文献[10]において，IC カードによる本人確認を行った者だけが利用できる PC 端末を実現するソフトウェアの作成を行った．このソフトウェアは PC 端末にインストールするだけで任意の LDAP サーバ（ユーザ認証用のサーバの一種）に接続し，ユーザ認証を行うことができる．もし LDAP サーバとして情報連携基盤センターが運営している LDAP サーバ（全学的なユーザ認証を行っている）に接続するように設定すれば，PC 端末の管理者はユーザの管理を行う必要がなくなる．なお，このソフトウェアは情報連携基盤センターで開発し，無償で配布する予定であるので，PC 端末の管理者が用意するべきものはカードリーダのみである．

４．UPKI イニシアティブ

国立情報学研究所といくつかの大学・研究機関のみが参加している認証作業部会によって UPKI 事業が推進されているが，本事業の成果として得られる知見やソフトウェアなどは全国の大学・研究機関で使えるものにする必要がある．そこで，

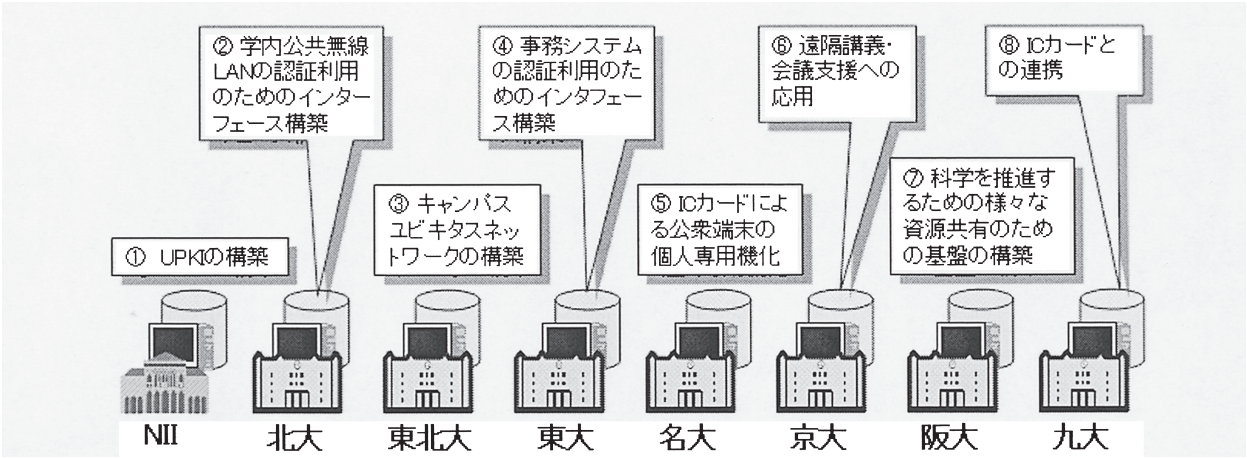

図３　国立情報学研究所と各大学の役割

UPKI 構築推進のための認証技術および利用に関して，仕様の検討・意見交換・情報公開などをおこなうため，UPKI イニシアティブが組織された．会員資格は，「大学・短期大学・高等専門学校または大学共同利用機関等の教職員であること」であるが，これ以外の人でも準会員として参加することが可能である．詳細は下記の URL を参照していただきたい．

https://upki-portal.nii.ac.jp

５．むすび

本文では，CSI 事業，および UPKI 事業の概要を紹介した．これらの事業は，特定の大学・研究機関を対象としたものではなく，日本全国（あるいは海外も）の大学・研究機関を対象とし，日本の次世代学術情報インフラストラクチャのモデルとなるべきものである．国立情報学研究所では，毎年２月末ごろにシンポジウムを開催し，これらの事業の広報に努めている．現在，CSI 事業や UPKI 事業に関与していない機関も，シンポジウムに参加していただき，忌憚のないご意見を聞かせていただきたい．また，UPKI 事業に関しては，４節で述べたように「UPKI イニシアティブ」を組織し，さまざまな機関との意見共有の場を設けているので，ぜひ参加いただき，さまざまな機関での使用に耐えうる成果（知見やプログラム，システム）の創出にご協力いただければ幸いである．

参考文献

１）http://www.geant2.net/
２）http://shibboleth.internet2.edu/
３）http://www.ja-sig.org/products/cas/
４）http://www.arl.org/sparc/index.html
５）http://www.gpki.go.jp/
６）http://www.lgpki.jp/
７）http://www.jpki.go.jp/
８）https://mynu.jp
９）https://mynu.jp/itc/nu_alias.html
10）葛生和人，平野　靖，間瀬健二，渡邉豊英：IC カードによる共有端末認証システムの構築，情報処理学会コンピュータセキュリティ研究会報告，2006-CSEC-35, pp.45-50，2006. 12.