社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－ＱＡＩ－19（３）
2006／5／24

大学間連携のための全国共同電子認証基盤 UPKI における認証連携方式の検討

島岡 政基† 谷本 茂明† 片岡 俊幸† 峯尾 真一† 曽根原 登†
寺西 裕一‡ 飯田 勝吉†† 岡部 寿男‡‡

†国立情報学研究所 〒101-8430 東京都千代田区一ツ橋 2-1-2
‡大阪大学 〒567-0047 大阪府茨木市美穂ヶ丘 5-1
††東京工業大学 〒152-8550 東京都目黒区大岡山 2-12-1
‡‡京都大学 〒565-0456 京都府京都市左京区吉田本町

E-mail: †{shimaoka, tanimoto, kataoka, mineo, sonehara}@nii.ac.jp,
‡teranisi@cmc.osaka-u.ac.jp, ††iida@gsic.titech.ac.jp, ‡‡okabe@i.kyoto-u.ac.jp

あらまし 国立情報学研究所は，７大学(北海道大学，東北大学，東京大学，名古屋大学，京都大学，大阪大学，九州大学)の情報基盤センター等(他には，東京工業大学，高エネルギー研究所など)と連携して，産官学民の共同研究開発，市民大学講座など連携サービスを安全かつ安心に提供するために，全国の大学と連携した電子認証基盤(UPKI)を構築していく．本稿は，UPKI が関連する複数の認証基盤との連携や，ターゲットとするアプリケーション(科学技術計算，学術コンテンツ，高等教育，学術ネットワーク)との連携，相互運用性実現のための構想について述べる．

キーワード 大学間連携，認証基盤，UPKI，認証連携

Designing federation architecture of the UPKI inter-university authentication and authorization platform

Masaki SHIMAOKA† Shigeaki TANIMOTO† Toshiyuki KATAOKA† Shinnichi MINEO†
Noboru SONEHARA† Yuuichi TERANISHI‡ Katsuyoshi IIDA†† and Yasuo OKABE‡‡

†National Institute of Informatics 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430 Japan
‡Osaka University 5-1 Mihogaoka, Ibaraki, Osaka, 567-0047, Japan
††Tokyo Institute of Technology 2-12-1 Ookayama, Meguro-ku, Tokyo, 152-8550, Japan
‡‡Kyoto University Yoshida-Honmachi, Sakyou-ku, Kyoto-shi, Kyoto, 606-8501 Japan

E-mail: †{shimaoka, tanimoto, kataoka, mineo, sonehara}@nii.ac.jp, ‡teranisi@cmc.osaka-u.ac.jp,
†iida@gsic.titech.ac.jp, ‡‡okabe@i.kyoto-u.ac.jp

Abstract National Institute of Informatics and the information infrastructure centers of the seven universities establish the inter-university PKI "UPKI" that collaborates with universities across the country for providing the services (e.g., citizen's college, a joint research and development on academic, business, citizen, and governmental circles) securely. This paper gives three concepts. Firstly gives a concept of the collaboration between UPKI and its related multiple PKI domains. Secondly gives a concept of the collaboration with the target applications (e.g., Grid Computing, e-Learning, academic contents and academic network). And finally gives a concept for achieving the interoperability.

Keyword university federation, authentication platform, PKI, UPKI, University PKI

1. はじめに

ユビキタス社会の創造の原動力は，情報通信技術(ICT: Information and Communication Technology)である．ＩＣＴは，日常生活やビジネスのみならず科学技術，学術研究分野での知的情報活動を便利で効率的なものにする．しかし，ユビキタス社会は光の部分だけを持つわけではない．ウィルスの脅威，個人情報漏洩，不正アクセス，サーバへの攻撃，迷惑メール，匿名掲示板上の誹謗中傷，コンテンツの著作権の侵害，違法な電子商取引やネット利用の悪質商法など安全・安心

な情報活動を脅かす陰の側面をもつ．この情報セキュリティの脅威は，最先端の学術情報流通においても例外ではない．これらの脅威は，情報のデジタル化による真正性の概念の変化，ネットワークの発達に伴う脅威の爆発的な拡大によるトレーサビリティの相対的な低下などが根底にあると考えられる．このようなデジタル社会における真正性の確保，ネットワークの安全な利用を実現するために，電子署名や電子認証を実現する仕組みとしてのPKIが注目されている．

便利で効率的な国際・産官学民連携の実現，学術コミュニティでの共同研究を促進する最先端学術情報基盤(CSI: Cyber Science Infrastructure)の実現においても，安全・安心を提供する電子認証基盤(UPKI: Inter University PKI)が不可欠である[1].

このため現在国立情報学研究所では，７大学全国共同利用情報基盤センターと共同で大学間連携のための全国共同電子認証基盤(UPKI)を構築している[2]．UPKI構築の目的は，大学が有する教育研究用計算機，コンテンツ，e-learning，ネットワークを安全・安心に有効活用することにある．UPKI開発の効率化，全国展開のためには，まず，学術情報ネットワーク運営・連携本部(7 大学とNIIの連携)が先行して開発・実験し，次に，全国の 800 有余の大学・研究機関に展開するという３ヵ年事業計画で進めている．

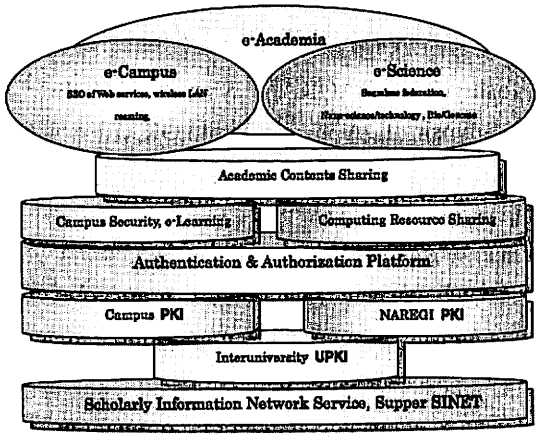


図 1　CSI 構想における UPKI

本稿は，安全・安心のICT基盤を提供する全国大学電子認証基盤(UPKI)について，関連する複数の認証基盤との連携や，ターゲットとするアプリケーション(科学技術計算，学術コンテンツ，高等教育，学術ネットワーク)との連携，相互運用性実現のための構想について述べる．

2. UPKI におけるサービス展開

大学間連携基盤としての UPKI を実効あるものにするためには，例えば，SSL/TLS や S/MIME，学内イントラへの認証で用いられる WebSSO，地理的制約を解消するネットワークローミング，高価な計算機資源を安全に共有する Grid など実用的なサービス提供が不可欠である．一般に，セキュアなサービスを実現するにあたり，セキュリティと利便性はトレードオフの関係にあると言われている．即ち，安全性を確保するにはコストの問題や利便性の問題が想定され，一方で，利便性を追求すれば，安全性は下がる場合がある．

これらの観点から，UPKI 上のサービス構築においても，単にセキュリティ面だけを訴求するのではなく，利用者にとって，より利用しやすく簡単で安心・安全に使えるサービスの実現が望まれる．そのためには，技術面の検討に加え，大学での管理・運営面，法制度・教育制度面等も考慮し，さらには利用者の観点からの検討，例えば，ワークフロー等の実務面を十分に考慮した多面的な検討が必要となる．さらに，今後の展開として，UPKI の社会情報基盤化を想定した場合,大学間の連携に加え，産官学や民との連携等，学以外へのサービス提供も視野に入れる必要がある.以下に,現状，想定しているサービス展開例について概説する．

2.1. 大学間連携サービス

大学間連携サービスでは，3.で示す個々の学内に設置された認証基盤におけるサービスの相互利用を検討している．例えば，学内認証基盤で想定されているサービスとして,学内の各所に設置された共用 IP 電話や共用インターネット環境に認証機能を付加することにより，これらをあたかも個人の端末であるかのように専用化し,キャンパス内のどこにいても IP 電話機での受信や無線 LAN ローミングを可能とするサービスがある．このようなサービスを UPKI により，学間でも相互に利用出来ることを可能とし，サービス提供領域を拡大し，認証による安全性確保に加え，さらなる利便性向上が期待できる．

2.2. 官学連携サービス

官学におけるワークフローの効率的な実現，即ち，BPR(Business Process Reengineering)実現のためのサービス例として，例えば科研費申請サービスを想定している．現状の科研費の申請に関しては，教員・事務・関係省庁に至る調整を必要としているが,これらを UPKI 上で実施することにより，例えば事務処理の効率化が図れるとともに，より研究に専念できる環境を提供しようとするものである．

2.3. 産学連携サービス

UPKI 認証基盤による安全・安心な産学連携の利用促進を目的に，例えば，①バーチャルオーガニゼーシ

ョン(VO)構築による共同研究の促進と効率化，②大学リソースのネット利用促進，③図書館の蔵書，デジタルアーカイブ貸し出しの利用促進，等により，セキュリティを確保・担保することにより，産学連携による共同研究・開発をこれまで以上の活性化が期待できる．

2.4. 国際連携サービス

UPKI 構築により，国際間における産官学連携による学術研究・教育を促進する．具体的には，UPKI の共通要素である，個人・機関認証システム(Web Trust for CA)及びサービス・利用者認証システムにより，国際間でのサの相互利用を安心・安全に利用できるようにし，研究のグローバル化・スピードアップ化，新たな研究領域の拡大への寄与が想定される．

2.5. 民学連携サービス

地域コミュニティの核として大学が機能し，市民生活の高度化を目指して，①一人一人の個性に対応できる社会基盤，②人々の内面に根ざした新しいコミュニティ形成を促進する社会基盤，を実現することにより，例えば，社会人リカレント教育，少子高齢化に対して生涯学習を与える場等の様々な波及効果が見込める．

3. 大学の特異性と UPKI

UPKI は CSI の上に乗せる電子認証認可プラットフォーム(e-Authentication and Authorization Platform)のための基盤である．CSI では，インフラストラクチャとしての UPKI を整備した上で，その上に乗せる大学電子認証認可プラットフォーム(u-AAP)までの実現を目指している．この認証認可の仕組みを実現するため，UPKI で発行したクレデンシャルを使った大学 ID 連携(u-ID Federation)も検討していく．

このような基盤整備においては，各大学が個別に行うより，連携して設計・開発・導入・運用することにより大幅なコスト削減が図れると考えられる．また，2.で述べた国際連携，産学連携，地域社会連携などを実現する上でも産官民とのポリシ共通化や連携フレームワーク，構築・運用ガイドラインを策定する必要がある．こうした目標を実現していくにあたり，大学という行政や企業と異なる特異性を充分に理解しておく必要がある．ここではUPKIに関連する大学特有の課題について述べる．

3.1. 大学間連携の多様性

PKI は技術要素だけで構成されるわけではなく，運用ポリシも含めてアーキテクチャを検討していく必要がある．UPKI においても各大学にポリシが求められることになるが，標準的なポリシにもとづいて運用する大学もあれば，標準的なポリシでは満足できず独自のポリシのもとに高度な PKI を望む大学もあると考えられる．このようなポリシの差異は，観点の違いだけではなく，既存の認証システムとの整合性や各大学・研究機関が所有する研究リソースを安全に管理していく上でも不可欠なものであるため，全国 800 有余の大学・研究機関に対して一元的なポリシやアーキテクチャを実装することは現実的ではない．

このように大規模なセキュリティドメインを設計していく上では，欧米で啓蒙が進みつつある保証レベルの考え方が参考になる．米連邦政府では 4 つの保証レベル[3][4]を定義し，連邦政府と接続する機関は少なくともいずれかの保証レベルに該当するように選択肢を与えている．各機関はそれぞれの保証レベルに応じたサービスを供受できる仕組みである．松本によれば，PKIの適用領域は，この保証レベルを，対象とするアイデンティティ，用途と組み合わせたキューブによって表現することができる[5]．

UPKI においては，PKI を用いた認証にフォーカスして検討を進めていくが，先に述べたように既存の認証システムとの整合性や管理すべき研究リソースに対する運用コストの観点からも全国 800 有余の大学・研究機関が必ずしも一元的に PKI を導入するとは限らない．このため UPKI では，将来的には PKI 以外の認証アーキテクチャとも連携可能な SAML ベースの ID 連携を，また用途やアイデンティティについても対象を順次広げていくことを視野に入れている．

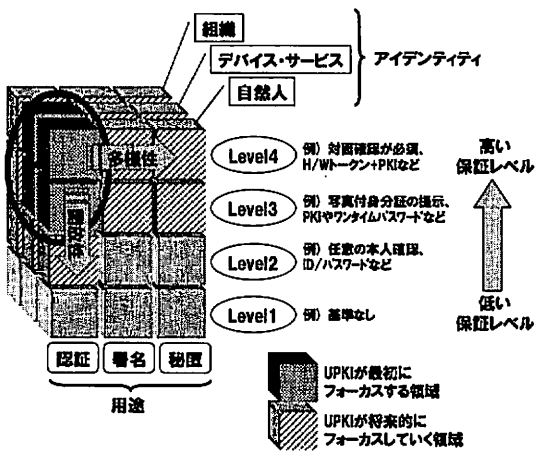


図 2 UPKI のフォーカスする領域

3.2. 認証アプリケーションの多様性

UPKI の目的である科学技術計算，学術コンテンツ，高等教育，学術ネットワークの安全な活用においては，それぞれのアプリケーションとの親和性が重要となる．UPKI では，これらの親和性に応じて 3 種類の認証基盤を活用していくことになるため，各認証基盤同士の連携をどのように実現していくかが大きな課題となる．ここでは 3 種類の認証基盤とそれぞれのアプリケーションとの親和性について述べる．

科学技術計算については，後述のように現在7大学全国共同利用情報基盤センターを中心に，グリッド技術による新しい共同利用サービスの検討が進められている．このサービスでは認証アーキテクチャとして，いわゆるグリッド認証基盤が求められている．

グリッド認証基盤：グリッド認証基盤はPKIの中でも特異な位置づけで，エンドエンティティが権限を委譲するプロキシー証明書[6]を発行し，これを用いて認証を行う仕組みである．このため技術的に既存のPKIを一部活用することは可能だが，運用ポリシの観点からは既存の認証基盤とは独立した認証基盤を運用する必要がある．

学術コンテンツ，高等教育，学術ネットワークについては，学内関係者だけでなく広く一般に公開されるべき内容も多くある．このため大きく学内関係者を対象とした学内認証基盤と，一般を対象としたオープンドメイン認証基盤の活用が求められる．

学内認証基盤：学内認証基盤は自学の学生・教職員など利用者を明確に限定した認証基盤として用いられる．このように利用者を限定した認証基盤を構築することで，学生の成績管理や教職員の電子決裁などをはじめとする安全な学術コンテンツ，高等教育，学術ネットワークを提供するアプリケーションを大学独自に開発・提供することができるようになる．実際に，大阪大学，東京工業大学などではICTアプリケーションのセキュリティおよび利便性向上を目的とした学内認証基盤の構築を，既にUPKIに先駆けて進めている[2][7].

オープンドメイン認証基盤：オープンドメイン認証基盤とは，Webブウラザ[1]*やS/MIME対応クライアントなど主要なPKIアプリケーションに信頼された認証局として登録された認証局によって構築された認証基盤である．学術論文の一般公開や市民大学講座など一般を対象とした安全を提供するには，学内認証基盤とは明らかに異なる認証基盤が必要となってくるため，このようなオープンドメイン認証基盤の効率的な活用が求められる．*

既に主要なPKIアプリケーションに登録され普及が進んでいるオープンドメイン認証基盤に対して，学内認証基盤，グリッド認証基盤はまさにこれから構築が始まろうとしている時期にあり，UPKI としてもこれらの仕様や進展と同期しながら連携方式を検討していくことが求められている．

[1] パブリック認証基盤と呼ばれることもあるが，政府認証基盤や公的個人認証サービスなど第一セクターのPKIと混用を避けるため，オープンドメイン認証基盤と呼ぶことにする．

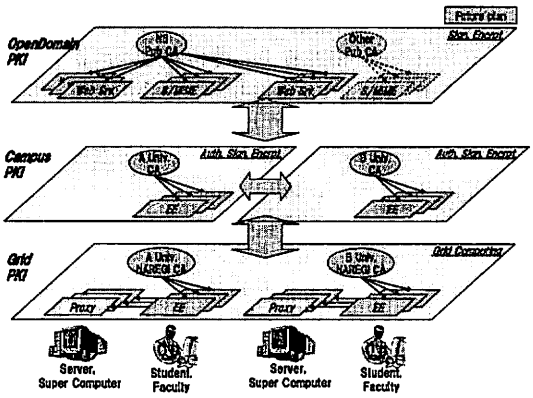


図 3　UPKIの3層構造[2]

4. 認証連携方式の検討

UPKI ではこれら 3 種類の認証基盤を連携させ，最終的に全国 800 有余の大学・研究機関が参加する非常に大規模な基盤を目指す．そのためにはできるだけ多くの大学・研究機関にとって参加しやすい(実装容易性・運用実現性が高い)アーキテクチャを検討する必要がある．

連携を検討するにあたって，それぞれの認証基盤の規模(PKI ドメイン構造)，各 PKI ドメインの信頼点，そして PKI ドメイン間の連携方式といった順に検討していく．

4.1. UPKIドメイン構造の検討

オープンドメイン認証基盤は，文字通り認証基盤の規模を限定しない開放された認証基盤であり，誰でも利用することが可能である．これに対して学内認証基盤，グリッド認証基盤では利用者を限定した運用が望まれる．この時に利用者をどのような単位で限定していくか，という認証基盤の規模について考えてみる．

認証基盤の規模を考えるにあたっては，PKIドメインという概念を理解することが不可欠である．PKIドメインとは，ある共通の証明書ポリシ(以下，ドメインポリシ)の下で運用される認証局の集合(認証基盤)である．ドメインポリシは，当該PKIドメインを他のPKIドメインから信頼してもらうための評価指標として参照される重要な要素となる．UPKIにおいて考え得るPKIドメイン構造を比較した結果を表 1に示す．

表 1　PKIドメイン構造の比較[2]

	特徴	ドメイン規模	期待されるPMA組織	備考
単一ドメイン構造	全ての大学・研究機関でポリシを共有	全国一元の大規模ドメイン	文部科学省，大学共同利用機関法人など	全大学・研究機関に対する一定の支配力が必要．
複数ドメイン構造	いくつかの大学・研究機関でポリシを共有	国・公・私，都道府県単位，地域単位など中規模ドメイン	7大学情報基盤センター，国立大学協会など	共有可能なポリシを策定する協調性が不可欠．
個別ドメイン構造	各大学・研究期間で個別にポリシを確立	個々の大学・研究機関	各大学・研究協議	重複するポリシ策定コストによる負担増．連携時の平準化コスト．

PKI ドメイン構造を検討するにあたっては，ドメインポリシを策定・管理するポリシ管理機関(PMA: Policy Management Authority)をどのような組織が務めるのか，についても留意しなければならない．大学の多様性や米国の学術 PKI の例を考慮すると，独自性の強いいくつかの大学がそれぞれ個別ドメイン構造を，その他の大学はコスト効率を優先して複数ドメイン構造を取る，というハイブリッド構造も考えられる．UPKI では，このようなハイブリッドな PKI ドメイン構造に対応できるアーキテクチャを検討していく．

4.2. UPKI における信頼点の検討

PKIでは，証明書の連鎖(認証パス, Certification Path)によって信頼の伝達が担保される仕組みとなっており，信頼点は認証パスの始点として唯一PKI利用者(Relying Party)から直接信頼される特殊な存在である．従って一般的な考え方として，信頼点は利用者にとって現実世界でも信頼される機関であるべきで，その信頼点が持つ信頼点証明書は安全な方法で利用者へ配布されるべきである[8]．既知の信頼点を活用するオープンドメイン認証基盤や，IGTF(International Grid Trust Federation)において世界的に信頼のフレームワークを策定しようとしているグリッド認証基盤については改めて議論する必要はないが，学内認証基盤においてはこのような信頼点をどのような組織が務めるべきか，またその信頼点の証明書をどのように・誰に配布するか，という課題について次項の学間連携と合わせて検討していく必要がある．

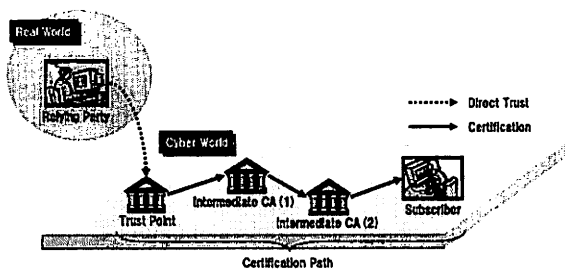


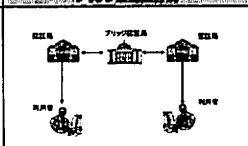
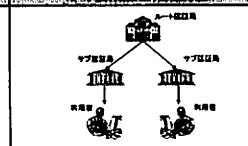
図 4　信頼点と認証パス

4.3. 学間連携のアーキテクチャ

複数ドメイン構造あるいは個別ドメイン構造といったマルチドメインPKI環境において相互のPKIドメインを連携させる方式には，個々のPKIドメインの信頼点をそのまま用いるシングルトラストポイントモデルと，それぞれのPKIドメインの信頼点を共有するマルチトラストポイントモデルがある[9]．

UPKI のように最大 800 有余の大学・研究機関で学内認証基盤を構築するケースでは，マルチトラストポイントモデルは信頼点の管理が煩雑になるため適切ではないため，シングルトラストポインテモデルにおけるブリッジモデルや統合ドメインモデルが検討の対象となってくる．参考に，統合ドメインモデルとは少し異なるが，ブリッジモデルとルートモデルの方式比較した結果を以下に示す．

表 2　(参考)ブリッジ，ルートの検討表[2]

	ブリッジ認証方式	ルート認証方式
イメージ		
事例	F-PKI(米国)/GPKI, JPKI 等	企業内認証局/証明書発行サービス会社 等
メリット	・信頼ドメインの拡張が容易 ・各ドメインの独立性が高い ・機関ごとにCP/CPSが設定可能	・ルート認証局を信頼点にするため簡単でわかりやすい ・証明書検証が簡単
デメリット	・信頼ドメイン横断にポリシーマッピング等の専門知識が必要なため導入しにくい ・ブリッジ認証局を利用した検証パスの構築複雑が必要になり，複雑になる。	・ルートCAの認証ポリシー及び証明書ポリシーに無条件で従う ・ルートCAの証明書ポリシをoverrideするような証明書ポリシは定義できない。 ・ルートの署名鍵が危殆(したらルートCAは下の証明書が無効になり，再発行を余儀なくされる。

また，この他PKI以外の認証方式との連携も考慮するならSAMLを使ったID連携(ID　Federation)モデルなども考えられる．米国の学術界では，Shibboleth[10]を使ったID連携が試験的に運用されており，既存の低い保証レベル(ID/パスワードなど)にも対応していくには，こうしたPKI以外の連携方式についても着目しておく必要がある．

5. おわりに

UPKI のような大規模な連携認証基盤構築にあたっては，このように技術的優劣だけでなく各機関における運用実現性やポリシの整合など様々な要素を考慮していく必要がある．そして様々な PKI ドメイン構造，様々な信頼点のあり方，様々な連携方式に対応していく一方で安全・安心を実現・維持していくためには，複数の保証レベルの考え方が重要になってくると認識している．UPKI では今後，多様な連携方式において保証レベルを共有可能とするために必要となるクライテリア整備や，実装技術の相互運用性(Interoperability)について検討していく．

また，全国800有余の大学・研究機関を広く包含する大規模な連携を成功させるためには，

- 広く全国の大学に支持・合意を得られる仕組みを持つこと
- 広く全国の大学が導入・運用可能なアーキテクチャを持つこと
- 広く全国の大学が導入可能な経済合理性を実現すること
- 広く全国の大学にUPKIの技術や利用事例を啓蒙すること

がポイントになると考えられる．実際に，2006年2月に開催した大学電子認証基盤シンポジウム[2]においても各大学から同様の意見が寄せられている．UPKIではこれらを実現していくために以下のアプローチを検討・実施している．

- 全国のUPKI有志がバーチャルに議論を行い，合意形成できるコミュニティ作り
- デファクトスタンダードを多用したリファレンス仕様の策定
- 全国の大学が効率よく負担できるコスト集中型の運用モデル検討や設計開発
- UPKIのアーキテクチャ，アプリケーション，ケーススタディのKnowledge Base構築

全国の大学・研究機関による最先端学術情報基盤CSIを考える上で，大学・研究機関が安全・安心に連携可能な全国共同利用の電子認証基盤UPKIの必要性・有効性は，漠然とは認識されるようになってきているものの，その具体的な実現方式や利用方法についてコンセンサスが取れているとは言いがたい．UPKI構築に向けては，大学の多様性，複数の認証基盤連携といった難題に取り組んでいく必要がある．さらにUPKIは学術界に閉じたものでなく産官民などとの連携や国際連携など，より広範なサービスへ進化できるように設計されるべきである．残念ながら現状では，一つの大学内においてすら，縦割り事務組織や部局の自治の壁など認証統合への障壁が少なくない．

このような様々な困難を乗り越えて真に実用となる「認証連携」を実現していくには，本論文で扱ったような全体のドメイン構造と個々の認証基盤の連携アーキテクチャについて検討していくだけでなく，運用者と利用者の意見を設計に充分反映できるような仕組みが必要となる．また，組織間の認証連携の実運用には，なにより当該組織間で人と人との信頼関係が構築されていることが大前提である．このような考え方から，UPKIでは，各大学・研究機関で認証基盤に関わる研究者・実務担当者がそれぞれの課題や経験を幅広く情報交換できるコミュニティの形成を，事業の柱の一つに位置づけている．関係各位のご協力を切にお願いしたい．

文　献

[1] 曽根原他，“サイバー・サイエンス・インフラ実現に向けたUPKI構想の提案”，第27回全国共同利用情報基盤センター研究開発連合発表講演会，Aug.2005.

[2] 大学電子認証基盤シンポジウム，http://www.nii.ac.jp/upkisympo/, Feb.2006.

[3] Bolten, J., “E-Authentication Guidance for Federal Agencies”, OMB M-04-04, http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf, Dec.2003.

[4] Burr, W., Dodson, D., Polk, W., "Electronic Authentication Guideline", NIST Special Publication 800-63, Sep.2004.

[5] 松本泰，“認証技術の現状の課題と今後の動向”，JNSAセキュリティセミナー「認証技術の動向」，http://www.jnsa.org/seminar/1209/matsumoto.pdf，Dec.2004年12月．

[6] Tuecke, S., Welch, V., Engert, D., Pearlman, L., Thompson, M., “Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile”, RFC 3820, Internet Engineering Task Force, RFC 3820, Jun.2004.

[7] 岡村，寺西，秋山，馬場，中野，“大阪大学におけるキャンパスPKIの構築”，情報処理学会研究報告，2006-DPS-126, pp.67-72, Mar.2006.

[8] 高木浩光，関口智嗣，大蒔和仁，"GPKIおよびLGPKIにおけるルート証明書配布方式の脆弱性と解決策”，情報処理学会コンピュータセキュリティ研究会，第5回コンピュータセキュリティシンポジウム(CSS2002)，http://securit.gtrc.aist.go.jp/research/paper/css2002-takagi-dist.pdf, Nov.2002.

[9] Shimaoka, M., Hastings, N., and Nielsen, R., “Memorandum for multi-domain Public Key Infrastructure (PKI) Interoperability”, <draft-shimaoka-multidomain-PKI-06.txt>, Internet Engineering Task Force, <draft-shimaoka-multidomain-PKI-06.txt>, Work in Progress, Jan. 2006.

[10] Erdos, M., and Cantor, S., “Shibboleth Architecture v4”, http://shibboleth.internet2.edu/docs/draft-internet2-shibboleth-arch-v04.pdf, Nov.2001.