# 全国大学共同電子認証基盤（UPKI）の構築

## -大学間連携電子認証基盤の実現に向けた「UPKI イニシアティブ」構想の提案-

## Federation architecture of the UPKI inter-university authentication and authorization platform

曽根原 登　岡田　仁志　岡部 寿男

島岡 政基　谷本 茂明　片岡 俊幸　峯尾 真一　渡辺　克也

**Noboru SONEHARA　Hitoshi OKADA　Yasuo OKABE**

**Masaki SHIMAOKA, Shigeaki TANIMOTO, Toshiyuki KATAOKA, Shinichi MINEO, Katsuya WATANABE**

**国立情報学研究所 〒101-8430 東京都千代田区一ツ橋 2-1-2**

**National Institute of Informatics　2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430 Japan**

**概要**　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と連携して，「最先端学術情報基盤（CSI：サイバー・サイエンス・インフラストラクチャ）」の構築を進めている．CSI は，国際・学術コミュニティ間での共同研究や，産学間の共同研究を加速する基盤であるとともに，市民大学講座，リカレント教育など大学と社会の相関を社会実装する．産官学民の連携サービスを安全かつ安心に提供するため，全国の大学と連携した電子認証基盤(UPKI)を構築する．UPKI は，大学の計算機資源，学術ネットワーク資源，学術コンテンツの安全な共有・共同利用を促進し，わが国のＩＴ分野の人材育成や新たなＩＴ産業の創出を目的とする．全国の大学・高等教育機関の連携を強化するため UPKI イニシアティブを結成する．大学運営のワークフローに即した研究開発，実装により，電子認証関連サービスの大学発のグローバルスタンダード化を狙う．

### 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)の構築を目指している[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，全国の大学への普及展開のためには，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，全国の大学・研究機関に展開するという 3 ヵ年事業計画で進める．

本稿は，安全・安心の情報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

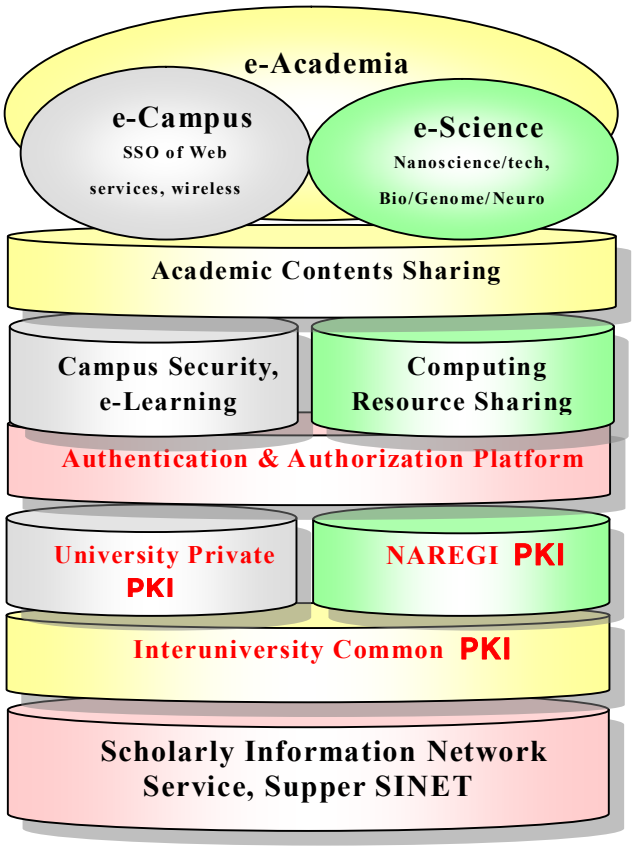



**図 1. CSI 構想における UPKI**

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. CSI と UPKI，その目的と意義

わが国を知的技術立国とするには，科学技術，社会科学に裏打ちされた情報力・文化力の国際競争力強化が不可欠である．そのためには分野，専門を超え，基礎研究，応用研究，サービスサイエンスの学術連携基盤の構築が必要である．産官学民連携の学術基盤を実現し，運営することで，最先端学術研究の推進とそれを支える継続的な人材育成，市民生活の質の向上に資する知識共有が可能となる．

CSI 構想と UPKI の関係を図１に示す[1]．UPKI は，大学電子認証･認可プラットフォーム(u-Authentication and Authorization Platform）のための基盤である．大学電子認証・認可プラットフォームは，大学における計算機資源，ICT を活用した遠隔教育，学術ネットワーク資源，学術コンテンツ資源の安全な共有・共同利用を促進し，最先端学術研究を加速する．また，情報セキュリティ分野の人材育成や新たなセキュリティ・サービス産業の創出も期待できる．

[1]ＰＫＩは，通常「公開鍵認証基盤」の意味で用いられている．Authentication Platform も「認証基盤」と訳される場合がある．一方，日本語では，「認証基盤」は文脈によって，″ＰＫＩ″，″Authentication Platform″，″Authentication and Authorization Platform″を意味することが多い．そこで，大学電子認証基盤を総称して，UKPI と呼ぶ．

## 3. 電子認証関連プラットフォームとサービス

### 3.1. 電子認証関連サービスの現状

大学連携 UPKI プロジェクトの研究開発は，CSI 基盤整備事業の一環として 2005 年から研究開発を開始した．現在，国や産業界では，以下の様な電子認証関連サービスが実用に供されている[2].

(1) 電子認証サービス
- GPKI（府省認証局）/LGPKI
- 公的個人認証サービス
- 法務省商業登記認証局
- 民間認証局，士業認証局
- サーバ証明書発行サービス

(2) タイムスタンプサービス
- 時刻配信サービス
- 時刻認証サービス

(3) 電子公証サービス
- 公証制度に基く電子公証サービス（指定公証人）
- 民間の公証サービス（電子データ交換の証明）
- e-文書法に対応した署名文書保存サービス

これらの電子認証関連サービスの課題として以下がある．

(1) 費用対効果，運用コストの課題

開発・導入したが，運用が回らないという課題が指摘されている．一般に安全・安心に関連するサービス，システムの運用は仮想損益モデル（シャドウコスト）によっている．他の分野と比べると，導入コスト，運用コストに見合う効果を数値的に示しにくいサービス分野である．

情報セキュリティ関連事業では，安全･安心に対する経営層の認識や費用の必要経費化などが必要であし，それを社会インフラとする場合には，法制度などによって強制力を持たせることも必要になるだろう．

(2) 限定された証明書，相互認証/認証局連携の課題

サービスの課題としては，証明書の有効範囲（利用用途）が限定されているという課題がある．また各種証明書とサービスとの密接な連携がないため，連携，相互運用の必然性やそれを実現するためのコスト増大という課題もある．例えば，実社会の印鑑には，実印，銀行印，認印，三文判，などの多様な手段があり，それを取引の重要性や額に応じてセキュリティレベルを選択できる．画一的でなく，“三文判”のように使い勝手の良い証明書を状況に応じて使いこなすといった生

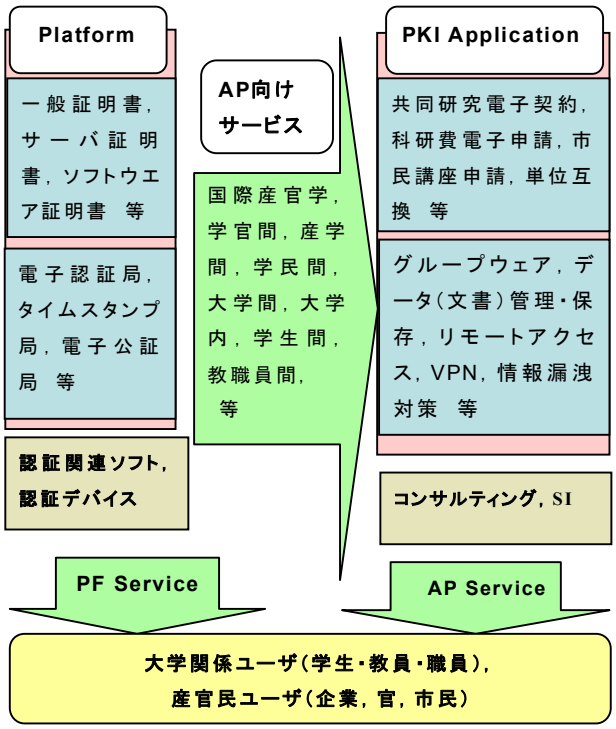



**図 2. UPKI プラットフォームとアプリケーション**

活スタイルや慣習に基づいたモデルを検討していく必要がある．

(3) 電子化処理のワークフロー分析と完結性の課題

電子化手続きは，便利でしかも経済的合理性がないと，適切な運用モデルが構築できない．電子申請による利用者のインセンティブを分析し，紙など物理媒体の介在無しに電子的手続きを完結させる必要がある．

## 3.2. プラットフォームとアプリケーション

UPKI の開発・導入，運用・事業化においても，上記と同様の課題が想定されるので，それらに対処できるよう設計する必要がある．そこで，UPKI を認証プラットフォームとアプリケーションと，それらが提供するサービスと運用モデルについて検討する．電子認証関連サービスのプラットフォームとアプリケーションの構成を図３に示す[2].

(1)　電子認証プラットフォーム

大学電子認証プラットフォーム・サービス・プロバイダ（UAA-PSP）は，電子認証局（ＣＡ），タイムスタンプ局，電子公証局などの運営と各種証明書（一般，サーバ，ソフトウエア）の発行を行う．プラットフォームは，エンドユーザに直接サービス提供する場合と，PKI アプリケーション・サービス・プロバイダにサービス提供する場合がある．

表１　産官学民連携サービス

| | U<br>From U To X, From X To U |
|---|---|
| G<br>（政府） | ・各種電子申請等<br>・科研費など研究公募・申請等 |
| U<br>（大学） | ・グループウェア，データ(文書)管理・保存，リモートアクセス，ＶＰＮ　等<br>・オンラインサービス（文献検索，ＤＢアクセス，計算機，ＶＯ，ＷＥＢ，メール，休講・安否掲示板等)提供<br>・政府統一基準遵守，情報セキュリティポリシ等<br>・情報漏洩対策，プライバシー保護，著作権保護等<br>・シングルサインオン(SSO)等<br>・大学間共同研究・単位互換等 |
| B<br>（企業） | ・電子契約，電子決済，オンライン受注　等<br>・データ共有，IPR 知財管理（著作権・特許）等<br>・計算機資源共有，ネットワーク資源共有等<br>・産学連携共同研究契約，受委託研究契約等 |
| S<br>（学生・教職員） | ・オンライン決済（入試，授業料，奨学金，学割等）<br>・オンラインサービス（文献検索，ＤＢアクセス，ＶＯ，ＷＥＢ，メール，休講・安否掲示板　等)提供<br>・無線ＬＡＮローミング，署名付きメール等<br>・e-ラーニング，通信放送教育，ＷＥＢ市民講座等 |

(2) PKI アプリケーション

大学用PKIアプリケーション・サービス・プロバイダ（UPKI－ＡＳＰ）は，PKIを利用して，大学間・産学官間の共同研究電子契約，科研費などの電子申請・決済，市民講座登録・申請，大学間の単位互換，グループウェア，データ（文書）管理・保存，大学計算機資源の管理・共有，共同研究など仮想組織（ＶＯ）の管理，リモートアクセス，ＶＰＮ，情報漏洩対策などの大学向けの具体的サービスを提供する．

(3) プラットフォームとアプリケーション連携

表１に，プラットフォームとアプリケーションが提供する産官学連携サービスの分類例を示す．連携サービスは，組織体である官（Ｇ），大学（Ｕ），企業（Ｅ）と学生・教職員・市民（Ｓ）などの利用者属性によって分類している．これら連携サービスの開発・導入にあたって，継続的運用が可能なモデルを研究開発する．

大学や大学共同利用機関は，プラットフォーム，アプリケーション，それらが連携したサービスのいずれを提供するかを検討する．これらサービスのトランザ

表2. 開発と運用の検討内容

| | 電子認証<br>Platform | PKI 利用<br>Application |
|---|---|---|
| 開発<br>導入 | 規模の経済モデル，大学共同利用の仕様共通化，共同利用調達 | 大学の地域性・独自性を活かしたサービス開発，規模の経済モデル，大学共同利用の仕様共通化 |
| 運用<br>事業 | ランニング・コストの課題，産官学連携の運用モデル | 各大学での運用モデル開発，産官学連携と連携交渉力 |

クションの発生頻度を分析し，費用対効果の改善が得られるサービスに関して継続的維持運用可能なモデルを検討する．

### 3.3. 開発・導入と運用・事業モデル

大学向け電子認証プラットフォームと PKI 利用アプリケーションの開発，運用の課題・検討内容を表２に示す．これまで述べたように，大学が主として大学向けに提供する電子認証関連サービスは，民間が提供する収益事業サービスとは異なる運用・事業モデルである．そこで，UPKI 構築としての開発・導入，運用・事業モデルを構築する必要がある．

(1) 開発・導入

全国の大学は，独自性・地域性を活かしたサービスを開発する．それら PKI 利用アプリケーションの共通部分と大学共同利用や大学間連携の共通部分についてはサービス，機能仕様の共用化を検討する．

(2) 運用・事業

運用コストについては，行政や民間サービスとの連携を視野に入れ，大学が共同して運用できるようなＷｉｎ－Ｗｉｎのモデルを検討する．

(3) 費用対効果

企業における電子化，電子認証，情報セキュリティの導入・運用と大学のそれが大きく異なる点は，コスト構造にある．大学内サービスの電子化や大学間，産学官の認証連携の効果は，リスク管理コスト，時間コストを削減し，大学・高等教育機関における「研究と教育の質の向上」にあるものとする．また産官学連携の交渉力強化施策についても検討する．

(4) 展開・普及

UPKI イニシアティブが先行して設計・開発・実証実験などを行う．それらの仕様，コスト，機能，性能などの評価結果を順次公開し，全国の大学などからの様々な意見を反映する．その活動のなかでポリシ，フレームワーク，ガイドラインの共通化を実現する．ノウハウが蓄積された後には，全国の大学への電子認証基盤構築の導入を支援する活動を行う．その上で産官学民の連携サービスを展開する．さらに，大学の特異性を反映し，大学発の国際標準化への貢献なども視野にいれた検討する．

## 4. 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．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．

(1) 大学間連携サービス

大学間連携サービスでは，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) 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．受委託・共同など各種研究費の申請・契約に関しては，関係大学，産学官，教官間の調整を必要とし

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．

(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．

(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．

(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．

## 5. 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 (u-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．

### 5.1. 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 1000 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図３のように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．

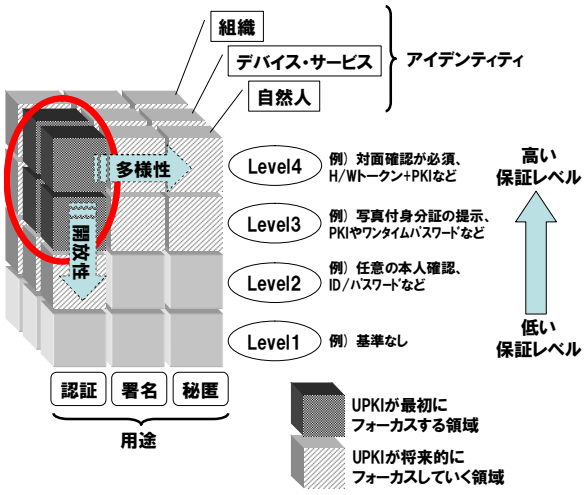



図 3　UPKI のフォーカスする領域

### 5.2. 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．

(1) 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．

(2) 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]．

(3) 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[2]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．

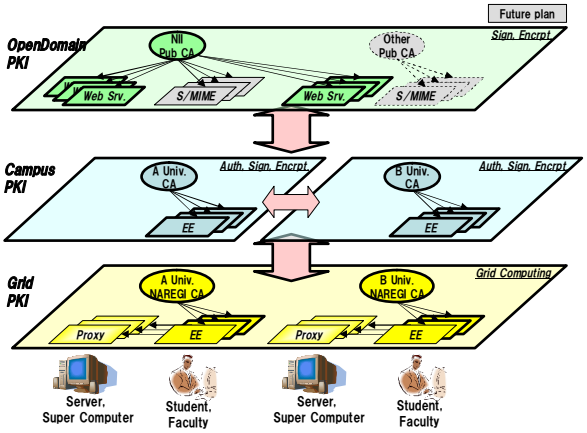



**図 4　UPKI の 3 層構造[2]**

## 6. 認証連携の方法

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する．

### 6.1. 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 3 に示す．

[2] 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．

表 3　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・研究機関毎 | 各大学・研究機関 | 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する．

## 6.2. 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，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する．

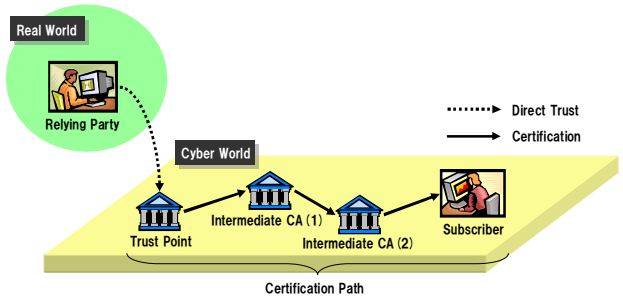


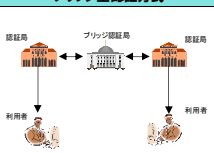
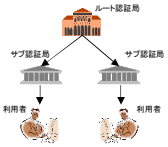

図 5　信頼点と認証パス

## 6.3. 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[10].

UPKI のように最大 1000 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 4　(参考)ブリッジ，ルートの検討表[2]

| | ブリッジ型認証方式 | ルート型(階層型)認証方式 |
|---|---|---|
| イメージ |  |  |
| 代表事例 | 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<br>・各ドメインの独立性が高い<br>・機関ごとにCP/CPSが策定可能 | ・ルート認証局を信頼点にするため簡単でわかりやすい<br>・証明書検証が簡単 |
| デメリット | ・信頼ドメイン構築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<br>・ブリッジ認証局を利用した検証パスの構築機能が必要になり、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<br>・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。<br>・ルートの署名鍵が危殆化したらルートCA以下の証明書が無効になり、再発行を余儀なくされる。 |

## 7. 2006 年度の開発計画

### 7.1.パブリック証明書発行手順確立

UPKI では，学内や大学間用の証明書以外に，全世界で通用するパブリック証明書（サーバ証明書，S/MIME 証明書）の発行について検討する．具体的には，以下を検討する．

(1) 証明書発行フローの詳細設計
証明書発行スキーム/CP ガイドラインをベースに各大学からの申請受付から審査および証明書発行まで，大学の運営実態に即した業務設計を行う．

(2)　Public 証明書発行実施体制の確立
業務設計に基づき業務実施体制の構築を行う．

(3)　Public 認証局の証明書ポリシ検証・規定（CPS)の策定

(4)　証明書ポリシガイドラインをベースに学術機関向けの証明書に関する証明書ポリシを作成する．

(5)　Public 証明書の発行
各大学からの申請を受け Public 認証局より学術機関向けのサーバ証明書等の審査発行業務を検討する．

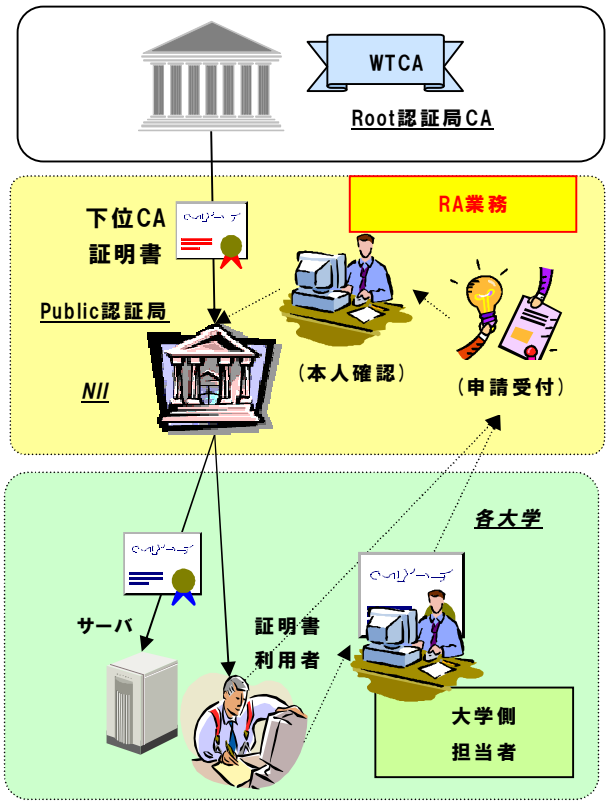



**図 6　大学向けパブリック証明書発行プラットフォームとサービス**

### 7.2. UPKI 相互運用フレームワーク制定

各大学が学内認証システムを導入・構築する際，仕様策定の参考となる，学内認証基盤の共用可能な仕様の雛形を作成する．また各大学の学内認証基盤を構築後の大学間連携に備え，UPKI 相互運用フレームワークを制定する．これに準拠したシステムを導入することで，各大学の学内認証システムは大学間連携が可能となる．

なお，本フレームワークの策定にあたっては，先行して学内認証基盤を導入する東京工業大学及び大阪大学等の導入時の仕様や，運用開始後に判明した問題点をフィードバックする．

### 7.3.連携アプリケーションの開発等

UPKI の普及のためのアプリケーション開発を実施する．

(1) 大学間無線 LAN ローミング方式の検討
(2) 情報基盤センタの各種サービス及びコンテンツサービスの SSO（シングルサインオン）
(3)　認証・認可方式の検討

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[11]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検討する．

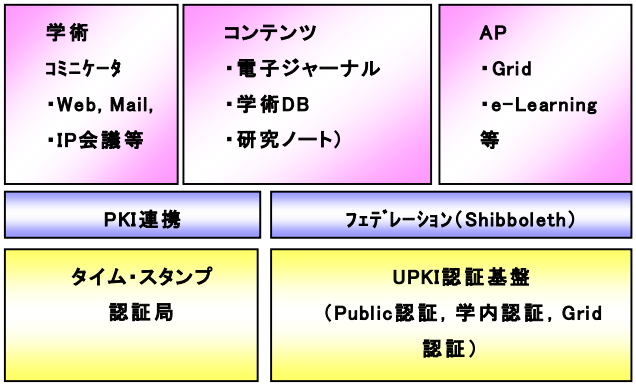



**図 7　大学向け認証・認可プラットフォーム**

### 7.4. CSI 向け認証局の普及と導入支援

NAREGI ソフトウェアのうち，認証に関わるパッケージで　ある NAREGI-CA を，平成 17 年度に改造し，グリッド以外の認証局としても使用可能な CSI 向け認証局ソフトウェアを開発した．このソフトウェアの普及のため，学内認証局として導入する際の導入支援を実施する．17 年度開発版に新たな機能（HSM(Hardware Security Module)不要版[3]）を付加した V2.1.1 を 7 月末に，英語対応版の V2.2 を 10 月末にリリース予定である．これらのリリースにあわせてサポートを開始する．

## 8. UPKI イニシアティブ設立の提案

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．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 1000 有余の大学・研究機関を広く

[3] HSM 不要版：PRAGMA(Pacific Rim Applications and Grid Middleware Assembly)からの要望により，安価なハードウェアでも稼働可能なバージョンをリリース．

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・運用可能な経済合理的サービスを実現すること
- 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 UPKI イニシアティブ（仮称）の設立を検討する．

- 全国の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
- 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
- 全国の大学によ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，規模の経済モデルの適用，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させ，連携の過程を通して大学連携による外部への交渉力強化につなげることとしたい．

真に実用となる「認証連携」を実現していくには，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サービス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とは言うまでもない．

このような理念に基づき，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を UPKI イニシアティブによって形成しようと考えている．関係各位のご協力を切にお願いしたい．

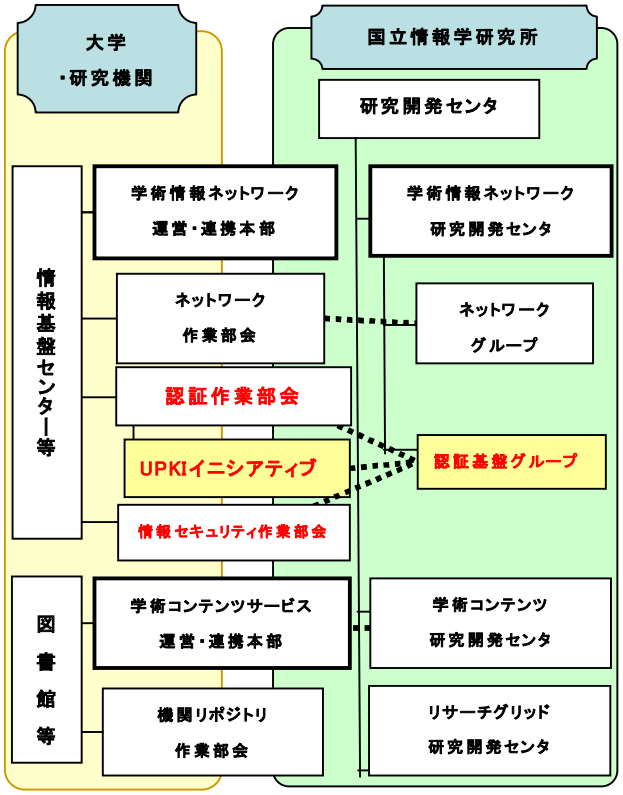



**図 8 UPKI 研究開発体制**
**UPKI イニシアティブ支援体制**

## 参考文献


[1] 曽根原登，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 UPKI シンポジウム，http://www.nii.ac.jp/UPKIsympo/, Feb.2006.
例えば，工藤明彦，「UPKI への期待」

[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),

[9] http://securit.gtrc.aist.go.jp/research/paper/css2002-takagi-dist.pdf, Nov.2002.

[10] 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.

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

[12] 島岡 政基, 他, “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”, 電子情報通信学会技術研究報告, IA2006, pp.13-pp.16, 05-2006.