サイバー・サイエンス・インフラストラクチャ実現に向けた UPKI 構想の提案

Interuniversity Authentication and Authorization Platform for Cyber Science Infrastructure

学術情報ネットワーク運営・連携本部　認証作業部会

曽根原　登（国立情報学研究所）　岡部　寿男（京都大学　学術情報メディアセンター）
高井　昌彰（北海道大学　情報基盤センター）　曽根　秀昭（東北大学　情報シナジーセンター）
佐藤　周行（東京大学　情報基盤センター）　平野　　靖（名古屋大学　情報連携基盤センター）
下條　真司（大阪大学　サイバーメディアセンター）　鈴木　孝彦（九州大学　情報基盤センター）
松岡　　聡（東京工業大学　学術国際情報センター）　川端　節彌（高エネルギー加速器研究機構）
貝田 辰雄 ・ 相原 雪乃 ・ 大山 貢 ・ 樋口 秀樹 ・ 土井 光広（国立情報学研究所 開発・事業部）

国立情報学研究所　〒101-8430東京都千代田区一ツ橋2-1-2

あらまし　ユビキタス社会の創造の原動力は，情報技術（IT: Information Technology）である．ITは，日常生活やビジネスのみならず科学技術，学術分野での知的情報活動を便利で効率的なものにする．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・安心に係わる問題が顕在化してきている．このため，安全・安心の技術基盤が不可欠である．日常生活，ビジネス，行政サービスなどのニーズ指向のアプローチと，最先端科学技術の研究開発，教育・IT人材育成を担う大学・研究機関からのシーズ指向の両側面からのアプローチが不可欠である．本文は，ITの活用によって，便利で快適な科学技術・教育研究活動の活性化を目指したサイバー・サイエンス・インフラストラクチャ（CSI: Cyber Science Infrastructure）構築と，安全・安心の技術基盤を提供する全国大学電子認証基盤（UPKI: University Public Key Infrastructure）の構築に向けた取り組みについて述べる．そして，情報基盤整備にとどまらず，各大学・研究機関の現場での，CSIの付加価値を高めるアプリケーション・サービス研究開発の動向について報告する．

キーワード　ユビキタス，情報インフラ，IT，ICT，情報セキュリティ，認証基盤，グリッド・コンピューティング，Webサービス，シングル・サイン・オン，遠隔教育，メタデータ，学術コンテンツ，学術情報ネットワーク，サイバー・サイエンス・インフラストラクチャ

1.　まえがき

ブロードバンドの普及は，ネットワーク社会の進展を加速し，それはユビキタス社会へと向かう．ユビキタス社会とは，「いつでも，どこでも，何でも，誰でも」ネットワークでつながる社会である．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）あるいは情報技術（IT: Information Technology）である．ITの利活用によって，日常生活やビジネスのみな

らず教育や学術研究といった知的情報活動を便利で効率的なものにする.

ユビキタス社会の情報インフラは, ITが支えるユビキタス・ネットワークである. わが国のユビキタス・ネットワーク整備は, 政府のe-Japan戦略によって急速に進展した. それに伴い, ユビキタス・サービスも現実的になった. 例えば, 電子政府や電子自治体によって, どこでもいつでも(24時間)行政サービスを受けることができる. 遠隔教育やe-ラーニングで, どこの大学の授業でも自宅で聴講でき, 電子カルテや医療ネットワークで, 患者の希望に合った病院や医師を選択できるようになる.

しかし, ユビキタス社会は, 何もかも便利で効率が良く快適な生活だけを提供するのではない. すでに様々な問題が顕在化している. 例えば, ウィルスの脅威, そして個人情報漏洩は年を追って深刻な問題になっている. 事実, 個人のインターネット利用における不安・不満に関するアンケート調査(平成15年度版情報通信白書)によれば,「プライバシー保護」「ウィルスの感染」が上位の1, 2位を占めている. さらに, 不正アクセスやインターネットのサーバへの攻撃, 迷惑メール, 匿名掲示板上の誹謗中傷, 有害コンテンツ, 犯罪の助長, 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と, 数え切れないほどの安全・安心に係わる問題が顕在化してきている. それは大学・研究機関と無縁ではない情報セキュリティ問題となっている.

ユビキタス・ネットワーク社会への期待は, 利便性と効率性を享受することであるが, 安全・安心に関する問題を解決なくしては, 豊かなユビキタス・ネットワーク社会への期待を現実のものとすることはできない.

わが国のブロードバンド・ネットワークは, 世界で最も低料金のインフラである. また, モバイル・インターネットの普及拡大は世界の最先端を走っている. また, 通信と放送の融合の側面から, デジタル放送インフラの整備も着実に進展している.

このような情報インフラの整備とともに, その上で提供される安全・安心なコンテンツ, コミュニケーション, コラボレーションの融合サービスの研究開発を加速しなければ, 世界市場のIT分野で戦うことはできない.

世界に存在感のあるユビキタス社会の創造には, 日常生活, ビジネスや行政サービスからのニーズ指向のアプローチとともに, 最先端の科学技術の研究開発と, 教育とIT人材育成を担う大学, 研究機関からのシーズ指向のアプローチが不可欠である.

本稿は, ITの活用によって便利で快適な科学技術・教育研究活動の活性化を目指したサイバー・サイエンス・インフラストラクチャ(CSI: Cyber Science Infrastructure)の構築と, CSIの安全・安心の技術基盤を提供する全国大学電子認証基盤(UPKI: University Public Key Infrastructure)の構築に向けた取り組みについて述べる. そして, 基盤整備にとどまらず, 各大学現場での付加価値を高めるアプリケーション・サービス研究開発の動向について報告する.

2. CSI 戦略構想

2.1 CSI構築の目的と機能

21世紀に入り, 高等教育・学術研究機関を取り巻く環境は激変した. 学術研究機関と深く係わる社会環境変化には,

- 急速な少子・高齢化の到来
- 低成長時代の到来と持続的発展モデルの模索
- 情報インフラ整備とグローバルネットワーク社会化
- 国際的には, 覇権力・影響力の変化の兆し

などが挙げられる. これら社会環境変化と高等教育・学術研究機関の教育・人材育成・先端技術研究開発の関係は複雑に絡みあっている. このような状況で,「科学技術立国(含む知的ものづくり), 人材立国」という国家ビジョンの明確化と高等教育・学術研究機関の役割を明らかにしていくことは難しい. そこで, これら社会環境変化に即応できる全国の大学・研究機関におけるCSIの戦略構想の目的と役割を考察する.

(1) 魅力ある知的技術立国にむけた寄与

現在, 女性が生涯に出産する出生率は1.29である. これは, 先進諸国の中では最も子供の少ない少子国家である. 直接的には, 学生数の激減を意味する. 全国800の高等教育・学術研究機関は, 市場競争とM&A時代に突入するかもしれない. しかしその時同時に, 65歳以上の人口比率が25%を占める超高齢化社会が到来する. したがって, 市民大学や社会人リカレント教育という新たな教育

事業機会をもたらすという面もある.

さらに，諸外国からの留学生の受け入れも今以上に考慮していく必要があろう. それには，経済産業的，先進技術的，文化的側面が深く関係する. 諸外国からの留学生がたくさん来たくなるような魅力ある国に変えていくことも必要である.

わが国が最先端技術の知的ものづくりを推進し，世界に向けそれを発信できれば，多くの人・技術が集まり，経済活動が活性化する. かつて日本では，欧米の書物，学術誌の日本語翻訳が盛んに行われ，日本語さえ覚えれば世界の情報が入手でき，近隣諸国からの多くの優秀な留学生を受け入れた時代があった. グローバルネットワークが普及した現在は，ICTを活用し，情報・人・技術の分野を超えて国際連携ができるCSIの構築が，多様な大学・研究機関のこれからの生き残りにとって急務である.

(2) 知的ものづくりの持続的運営

1990年に，NTTはVI&P宣言をした(「2005年の情報通信技術」). 1990年に，15年先の2005年のICTサービスのあるべき姿を予測し，それに基づいて技術開発を推進した. このVI&P宣言は，米国のクリントン政権時代のゴア副大統領が，情報スーパーハイウエイ構想あるいは国家情報基盤(NII: National Information Infrastructure)構想として情報基盤整備を進めた. それまでわが国のICT分野は，先行する米国のキャッチアップと考えられていたので，この科学技術開発戦略の輸出は非常に衝撃的であった. また，2003年12月に東京・大阪・名古屋の三大都市圏では地上デジタル放送が始まり，本格的な放送のデジタル時代を迎えた.

VI&P宣言もデジタル放送宣言も，基礎的研究開発，技術開発を経て，実用化に到るまでには十数年の年月が必要とされる. 最先端の知的ものづくり分野で世界に存在感を出すには，基礎研究，応用研究，実用化のプロセスを数十年にわたって継続できる人材供給と研究開発への継続的投資が必要となる. そこで，大学・研究機関での研究・人材育成と企業での実用化・ビジネス化の連携，資金と人と技術が循環できる基盤が必要となる. それが，産学連携を可能とするCSI機能の目的でもある.

(3) 情報発信力・文化力の強化への貢献

国家の覇権力・影響力も長期的には変動している. 産業競争力，経済力，軍事力が大きなウエイトを持っていた時代や，インターネットや衛星などを駆使した情報力，外交力・交渉力が国家の存在感・影響力を持つ時代もある. この変化がさらに進み，文化力が影響力・交渉力となる時代が到来するかもしれない. わが国の独自の精神文化，芸術文化，生活文化を世界に発信し，世界が注目し，尊敬される国家となるには，特に大学での教育・人材育成・研究が果たす役割は大切になる.

世界のICT産業では，コンテンツ関連産業の収益比率が益々増加する傾向にある. また，投資の構造も，設備投資からコンテンツ投資へと流れが変わりつつある. 同時に，ネットワークは，プロのコンテンツからアマのコンテンツ発信へ，そして配信の形態も放送と通信の融合や，P2Pなどへと大きな変動が起きている. 市民，大学や研究開発，製造や運用事業の現場でITを活用し，さらなる知的な付加価値創造を行っていくことで，世界に存在感のある科学技術立国になることを目指す. そのためには，誰でも自由にコンテンツを作って発信し，それをデジタル資産として集積し，それに平等にアクセスできて，安心して付加価値化が行えるような情報循環システムとしてのCSIを実現する必要がある.

また，このようなシステムを持続的に維持運用していくには，科学技術ばかりでなく，法制度の再構築や経済モデルの開発，文化芸術と娯楽産業の活性化，教育と人材育成，コンピュータ科学とコンテンツ工学などが融合できる総合的な研究開発基盤としてのCSIが不可欠である.

(4) 大学・研究機関の社会基盤化

バブル経済の崩壊を機に，日本人の価値観の変化が，学術・研究対象に与える影響も大きい. それ以前の安くても多くのモノを所有するという量の豊かさの基準から，バブル時代では，高くても良いモノを所有するという質の豊かさの基準へと変化した. さらにこの変化は，モノの豊かさより心の豊かさへと，価値観も変化している. 物質的なモノの量という豊かさの基準から，精神的，心という質の満足度が大きなウエイトを占めるに到っている. 心の豊かさを科学技術で支えることが出来るかは難しい. 科学技術はこれまで効率化・利便性・快適性の実現に大きく寄与してきた. 市民生活の質の向上に資する，知識共有，人材育成，能力開発などの情報やサービスを提供するという市民・地域

密着型の大学・研究機関の新たな役割もでてきている．精神的な豊かさを充足する活動を大学・研究機関が支援できれば，地域社会の情報基盤，社会基盤としての新たな役割がでてくる．

2.2 CSIの構成

CSIシステムの構成を図1に示す．CSIは，ネットワーク層，3つの機能プラットフォーム（PF）層，アプリケーション・コンテンツ層から構成されるシステムとして検討している．ネットワーク層は，学術情報ネットワークを基本に，機能性能を拡張した次世代CSIネットワークを想定する．

(1) 配信プラットフォーム

デジタル情報を配信・共有・交換するためのサーバや，キャッシュサーバなどを利用し，配信を効率化するためのCDN（Content Delivery Network）の仕組みなどが含まれる．配信では，サーバ-クライアント型のシステム構成が主であるが，最近では，著作権保護（DRM: Digital Rights Management）機能の利用を前提とし，クライアント間でコンテンツを流通させるP2P型のシステム構成も注目されている．

(2) サービスプラットフォーム

認証や課金，DRM，サイエンス・コモンズ機能など，サービスを遂行するために必要な機能を提供するサービスミドルウェアである．認証基盤については，その必要性や機能について後述する．

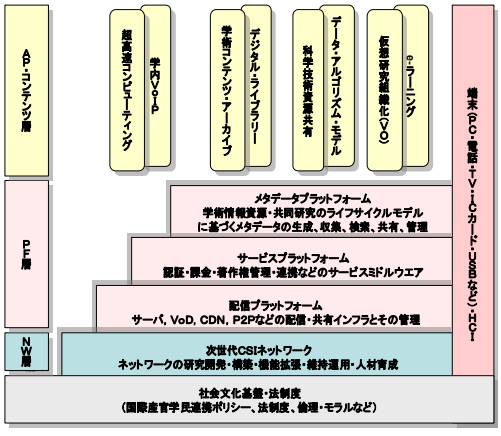

図1. CSIのシステム構成（案）

(a) 課金プラットフォーム

学術コンテンツ配信における著作権料金の代行徴収サービス，グリッド・コンピューティングにおけるASPサービスや計算機資源の利用サービス，大学図書館間の図書の相互貸借，企業や一般市民への貸し出しや文献複写サービスの適用が考えられる．

将来的には，学内IP公衆電話の相互接続料金徴収，大学のTLOやMOTをベースとした特許やノウハウなど知的財産権のライセンス販売や，ネット・コンサルティングなど，有償サービスへの適用を検討する．

(b) デジタル著作権管理（DRM）

e-Learningを用いて，デジタル教材，講義録，論文，レポートなどのコンテンツの著作権管理（配信先，コピー制限，著作者表示，タイムスタンプ管理，価格など）を行う．

コンテンツを教育・研究目的で利用する場合（著作権の権利制限）の目的認証，改変や再利用の利用許諾管理を行う．

(c) サイエンス・コモンズ（Science Commons）

将来的には，表1に示すようなOSS，GPL，OCW，データ，コンテンツ，デジタル教材など，CSIで共有・流通・交換されるデジタル財の統一的管理を行うことを検討する．

表1. Science Commons on CSI

	所有と利用の変化	具体例
ハードウェア・ソフトウェア	コンピュータ，ネットワーク資源，ソフトウェア資源の共同利用・共同開発 例）GGC,GPL,OSS	グリッド・コンピューティング，オープンソース 例）OS,DBなど
コースウェア	教育での権利制限 例）オープン・コースウェアの公的ライセンス	デジタル教育教材の共有，遠隔授業など e-Learningの権利制限
学術コンテンツ	デジタル映像，データ，アルゴリズム 例）Web,Blog,SNA	DRE(Digital Rights Expression),Creative Commons PL, d-mark,cIDf
サイエンス	ネットワーク連携，バーチャル・オーガニゼーションなど	DNA(Bio)，脳神経Neuro，地球環境，気象，天文などデータ共有

(3) メタデータ流通プラットフォーム

CSIシステムの特徴は，コンテンツの共有・流通・交換と，それを媒介とした共同研究やバーチャル・オーガニゼーション（VO），そしてグリッド・コンピューティングによる動的共同実験といったコラボレーション研究の促進を図るために，メタデータ流通プラットフォームを導入する点にある．

メタデータ流通プラットフォームは，CCCO（コンテンツ（C），コラボレーション（C），コミュニケーション（C），オーガニゼーション（O））の生成から管理，評価に至るまでのライフサイクルを考え，各段階で生成されるメタデータを交換する機能を提供することを想定している．

(a) プレゼンス・メタデータ

どこにどんなCCCOが存在するのか，それ発見しアクセスするには，プレゼンス・メタデータが必要である．CCCOにユニークな番号を付与することで，データベース間でのオブジェクトの一元的管理が可能になる．例えば，学術論文を例にすると，どんなデータを基に，どのような論文が出版されているか，論文間の引用関係や親子関係なども極め細かく管理することができる．また，科学技術論文は，投稿や公開の時刻認証，タイムスタンプが重要となろう．

(b) アダプテーション・メタデータ

適合属性は，様々なコンピュータを用い，それに適合したデータやツールがシームレスに組み込まれ実行されるときのデータ変換を制御するのに用いられる．データの記述条件，解析ツールなどの動作条件などを記述するのに用いる．例えば，生理実験データの測定条件を共通的に記述しないと誤った解釈をされる．解析や表示ツールについては，同じく動作条件やプラットフォーム条件を共通に記述しなければならない．

(c) コンテクスト・メタデータ

コンテクスト属性は，コミュニケーションサービスでは会議中・出張・車中など通信状況を示すのに用いられる．科学技術情報の共有においては，どんな研究目的で実験するかという場合に，知識や知見，ノウハウ，コンサルティングとそれに適合するデータや研究者や論文などを検索するのに用いることができる．

(d) 権利・許諾メタデータ

米国での，Publication Modelと呼ばれるガイドラインに見られるように，学術論文が引用され評価されるには，データを保管・共有できる仕組みと提供者に対するcitation/reward/credit/acknowledgmentなどの権利保護が必要である．論文，データ，ツール，計算モデルを公開する研究者のインセンティブを保障するには，それらの利用許諾条件を自ら宣言する必要がある．

このような，改変，再利用可能なコンテンツの許諾条件を与えるものしてCCPL（Creative Commons Public License）がある．科学技術，学術情報流通とその研究者コミュニティにおいては，citation/reward/credit / acknowledgmentなどの利用条件を標準化する必要があろう．言わば，SCPL（Science Commons Public License）のような学術，科学技術の公的ライセンス標準が必要になる．

知見や知識を創出するには，膨大なエネルギーと労力が必要になる．したがって，研究者，科学者自らが，これら知的財産権に対する価格付けを行うようにならないといけない．産業界は，知見やノウハウや技術に対して，独占排他的な使用権利を得ることを要請する．共同研究や特許の共同出願，ライセンスの利用契約など，ITを活用した電子契約（e-Contract）が必要になる．産学連携の場合には，こうした研究者，発明者の権利保護，契約が簡単に締結できる必要がある．

(d) クオリティ・メタデータ

品質属性は，コンテンツなどの内容的な品質保証条件を記述するのに用いる．コンテンツの価格付けは，情報の収集，整理・分析，知見などの付加価値化における品質保証の過程で決まる．引用率による格付けや，表彰などのメタデータを記述することによって，信頼という情報の品質を保障できるような仕組みが必要である．

このように，CSIの構築には，デジタル・オブジェクトを識別するIDを含めたメタデータを相互理解できるメタデータ標準が必要になる．IT活用による学術，科学技術の振興，産官学の連携のためには，研究開発における知的創作，情報及び情報資源の存在，発見，検索，知的財産権の流通，取引，利用を可能とするメタデータ標準が重要な役割を果たすものと考えられる．

標準という意味は，全国の大学・研究機関が相互に理解し合えることが必要となるからである．そう

でなければ，科学技術・学術コミュニティとして，研究者が情報発信し，他の研究者と，そしてビジネス開発者との情報交換，共有，コラボレーションが成立しない．

(e) オントロジー変換

脳神経科学ニューロインフォマティクスなどでは，きわめて多様な世界観に対処しなければならない．脳神経系の研究においては，ゲノムのようなセントラルドグマは存在せず，研究者がそれぞれ独自の世界観に基づいて現象を捉え，多様な様式で知見を表現している．

そのため，情報はありとあらゆる異なったコンテクストとフォーマットで世界中に散在しているのが現状である．数理モデルについても，研究者は自分の研究に適したシミュレーション言語を用いており，また，個別のプログラムで特殊な計算機環境でしか動作しない場合も多い．したがって，こうしたデータベースの内容を表示し，関連づけ，検索するための共有可能な一元的な「サイエンス・オントロジー（用語の定義とそれらの関連の記述）」を定義することが必要とされる．

これがなければ，ITを活用した研究者同志のコミュニケーションや，分野間の融合もできない．研究者コミュニティと産業界との連携も，知識や知恵の流通もできなくなってしまう．オントロジーを，共有可能な客観的部分と個々の研究者の専門的部分に分け，両者の共存を許すシステムが望ましい．

3. 全国大学電子認証基盤 UPKI（University Public Key Infrastructure）構想

3.1 UPKI構築の目的と機能

「連携」というコンセプトのもと，CSIの構築を目指している．そのCSIを安全・安心して利用できるようにするためのUPKIの調査・企画・設計・開発を行っているので報告する．

(1) UPKIの普及展開方針

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，ネットワークなどを安全・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大学等と国立情報学研究所の連携）が先行して開発・実験し，次に，全国の800の大学・研究機関に展開するという4ヵ年事業計画で進めている．図2に示すように，7大学は，各大学内認証基盤と地域の大学との連携を行う．国立情報学研究所（NII）は，総研大の認証基盤と各大学の認証基盤の相互接続を行う方向で検討している．このような，UPKIが構築できれば，

- 大学間の相互認証による教育・研究資源，コンテンツの有効活用が促進
- メール内容の暗号化による情報漏洩の防止
- 電子認証・電子署名を用いた電子決済，電子回覧による効率化
- 各大学の情報セキュリティレベルの向上やセキュリティポリシーと実施手順の見直し
- 各大学が共通して設計・開発・導入・運用することによるコスト削減
- 国際連携，産学連携，地域連携のポリシー共通化
- 大学発・世界初の国際標準への対応，標準化への貢献

などの効果が期待できる．一方，国内外の認証基盤の導入状況としては，

- 中央省庁間（GPKI），地方公共団体（LGPKI）での電子認証
- eIRG（欧州25かカ国＋EU）
- GGF（50かカ国から400機関）

などが先行しており，将来的にはUPKIは，国内での産官学連携や国際連携のための認証基盤との相互運用を視野に入れている．

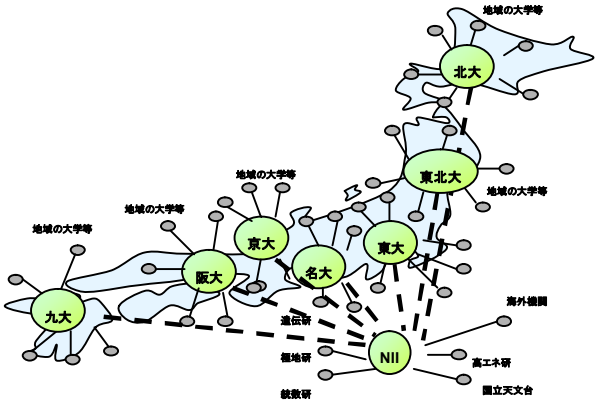

図2. UPKIによる大学・研究機関の社会基盤

(2) 現状の大学内電子認証システムの課題

現状の大学内電子認証システムは，ID/パスワードの組合せを多用しており，パスワードが他人に知られてしまうと，情報リソースに不正アクセスされる可能性がある．また，様々な学内部局が独自のID/パスワード体系を用いており，利用者が混乱するという課題がある．

このため，大学電子認証システムとしては，PKI（Public Key Infrastructure: 公開鍵認証基盤）の導入による不正アクセスの防止，電子証明書による本人証明・暗号化通信，ICカード等に秘密鍵を格納することにより詐称不能など，大学としての一元的な認証システムの構築が求められている．

(3) 大学間連携からの要請

学生は，単位互換制度など他の大学での講義を受けることができる．教員は，所属大学ばかりでなく，非常勤講師，流動教員，企業との連携教員，外部資金による共同研究への参加，などがある．物理的にも，仮想的にも，学生・教員の流動化が進展している．このような流動性に対応できる認証基盤が必要とされている．

(4) 現状の学術情報ネットワークからの要請

現在，主要大学間はSINET/スーパーSINETを介して接続されているが，セキュリティレベルの確保は利用者に依存している．また，商用のサーバ証明書発行サービスを利用するには，煩雑な事務手続きが発生する．

情報漏洩，データ改ざん等のネットワーク上の脅威が拡大しており，平成17年4月から個人情報保護法が施行され，学術情報ネットワークにおいてもますますセキュリティレベルを向上させる必要性が迫られている．

ネットワーク・インフラストラクチャとしての整備及び高度化は世界最高水準に達したところだが，今後は，CSIとして利用者（大学・研究機関）から共同実験や研究における連携をスムーズに実現するため，更なるセキュリティ向上の期待が寄せられている．ネットワークレイヤの脅威については対策を講じているものの，大学間及び外部（国外研究機関・産業界等）と機密性の高いデータを安全に流通させるには，更に高いセキュリティレベルを担保する必要がある．

国公私立大学・研究機関（約800校）の情報流通をセキュアに行うための社会基盤としてのUPKIの構築を行うことにより，ネットワークの利用者が安全にデータをやりとりできるようになる．これにより，CSIとしてのセキュリティ機能を強化し，利用者指向のネットワークへと進化することができる．

さらに，積極的に国内外の産業・学術機関等との連携も実現させることにより，国内外の「知」を集結した研究の推進による国際競争力の強化，ひいては経済社会全体の活性化に寄与することができる．

3.2 UPKIの構成

UPKIの設計・開発に対しては，

- トラスト・モデルの開発
- 開発導入した認証局の継続的維持運用モデルの開発

が重要になる．現状のトラスト・モデルを図3に示す．UPKIの設計に当たって，以下のアナロジーに基づき考察する．

(1) 印鑑モデル

日本での日常生活で用いる印鑑のアナロジーにより，経済的にそれぞれの業務内容に応じたセキュリティ水準を確保する方法で検討する．

- 実印：公的な認証局として大学間共通で利用する（パブリック）．CA局の監査認定コスト，運用時のコストの課題が多く，ホスティングまたはハウジングを想定して設計する．
- 銀行印：各大学にて共通の利用を行う（パブリック or プライベート）．
- 認印：各大学内のみでの運用する（プライベート）．
- その他（三文判）：当面考慮しない．

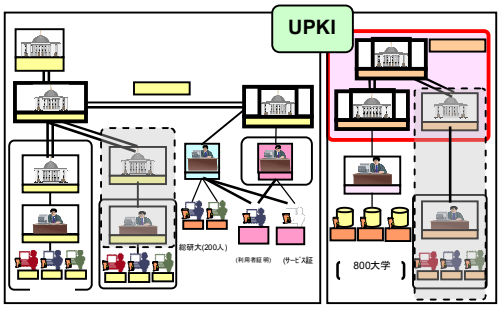

図3. トラスト・モデル（案）

(2) 証明書の定義

(a) 実印モデル

実印モデルとは，大学の公印にあたる．個人のための印鑑証明にあたるものは，公的個人認証で実現されている．ここでは，大学という公的な組織として必要な証明書として定義する．第三者の公的な認証局から発行され大学自身の責任を明確にする必要がある．

組織と職責の認証及び署名を行う．サーバ証明書，学長証明書等がこれにあたる．大学外へ対しての組織証明や公的な書類（各種申請書や証明書）を作成するために用いる．サーバ証明書に対してはWTCA認定済みであることが望ましいが，構築・運用経費の問題から，証明書の登録・配布モデルは，主体者発行（subscriber enroll）かバルク発行（bulk issuing）かをコストの観点から検討する．

(b) 銀行印モデル

大学が認めた対象（学生，教職員等）に対し，大学の責任で発行する証明書（銀行の預金通帳と同じモデル）であり，基本的にはプライベート認証局から発行する．個人の認証，学生証，教職員証がそれにあたる．

S/MIME用証明書を発行する．個人情報保護やお金がからむ業務サービスに利用できるレベルの信頼性を担保する必要性がある．実装としては，ICカード等の耐タンパ性デバイスに入れることが望ましい．用途等の要件定義を明確化する必要があるが，条件によっては商用のパブリック証明書の利用も可能である．

署名を行うとすれば保管期間の問題や，単位互換等のためには認証連携が必要となる可能性もある．

(c) 認印モデル

各大学内でのみ通用するプライベート証明書であり，大学間グリッド連携の際に利用する証明書と同じである．

PCやサーバ内に秘密鍵を保管する場合もありセキュリティレベルは高くない．グリッド用認証局については，IGTF（International Grid Trust Federation）による基準をクリアすれば，システムの国際連携が可能となる．この連携については現在，NAREGI（National Research Grid Initiative: 超高速コンピュータ網形成プロジェクト）で運用中の認証局が先行して実施予定である．

(3) 証明書の発行モデル

(a) 実印モデル

①文部科学省のGPKI認証局（またはNIIに構築したサブ認証局）から発行するが，GPKIからの発行可能性については今後の検討が必要である．サーバ証明書についてはWTCA（Web Trust for CA）ではないので，クライアント側でGPKI認証局の自己署名証明書をダウンロードする必要がある．

②NIIがWTCA認定を受けた商用ルートサイニングサービスを用いてサブ認証局を構築する．最も簡単にWTCA対応の認証局を構築する方法である．NIIが署名やセキュリティシール発行することにより大学間連携の結束を訴求できる．

③NIIが自営で認証局を構築し，WTCA認定を受ける．大学連携・共同利用機関のブランド作りには最適であるが，WTCA認定の構築と運用費用・維持期間についての課題が多い．またWTCAを取得後も実際に各種ブラウザに導入するための期間や費用の検討をする必要がある．

④WTCA認定を受けた商用認証サービスから発行する．機能的・経費的には経済的であるが業者が限られる．証明書の枚数に応じた料金となるので，NIIにおいて全大学一括入札を行うなどが考えられる．

(c) 銀行印モデル

基本的には各大学の責任において認証局を構築する．アーキテクチャ的には，NIIにルート認証局を立ち上げ大学認証局を接続する方法や，NII＋7センターにルート認証局を立ち上げ他の大学を接続する方法が考えられる．

各大学が個別に認証局を立ち上げて，認証の連携を行う場合には，各大学の代表者からなる大学PMA（Policy Management Authority）によるポリシーの管理，及び連携のためのシステム的な仕掛けが必要となる．運用に関しては商用アウトソーシングサービスも利用可能である．商用の認証サービスから証明書を購入することもできるが，その場合には，大学PMAによるポリシー管理ができないので他大学や海外との連携については大学個別

の責任で行うことになる.

NIIは，以下の役割を担うことが現実的である．認証ポリシーの整合を取るためのPMAの事務局及びCP/CPSに基づいた監査を行う．認証連携システム開発及び運用を行う．

大学の認証局コスト削減のためにNAREGI-CAを用いたオープンソースの大学認証パッケージを開発し無償提供する．

認証連携システムは段階的に発展させる方法が考えられる．

当初は，ゆるい連携のためのディレクトリのみを構築し，各大学の認証局証明書を安全・確実に配布する．

次に各大学認証局の失効情報を集中的に提供するOCSPレスポンダを構築する．

さらにNIIにルート認証局を立ち上げて大学認証局の統合を行う．複数のルートが存在する場合の認証連携方法については，相互認証（またはブリッジ接続）を行う．

(d) 認印モデル

基本的には大学独自で自由に認証局を構築し運用が可能である．大学の個別事情に合わせて，多種多様な証明書が発行できる．各大学においてグリッド用証明書を発行し，他の機関と連携する場合については以下の案が考えられる．

①各大学で構築し，IGTFの認定を受ける．
②IGTF認定を受ける予定のNAREGI認証局からグリッド用証明書を一括発行する．
③NIIがルート認証局を構築してIGTF認定を受け，各大学はサブ認証局または登録局を構築してグリッド用証明書を発行する．

4. UPKIを用いたCSIアプリケーションの開発

CSIとその安全，安心な活用にための認証基盤UPKIが構築できても，具体的サービスの訴求力がなければ，基盤は使われないものになってしまう．各大学の個別事情に合わせてCSIアプリケーションの開発を行う．これらアプリケーションは，検証評価，相互運用実験のあと，他の大学にリリースされ，最終的には，全国の大学で利用できるようにする．

以下では，各大学が開発するアプリケーションについて報告する。

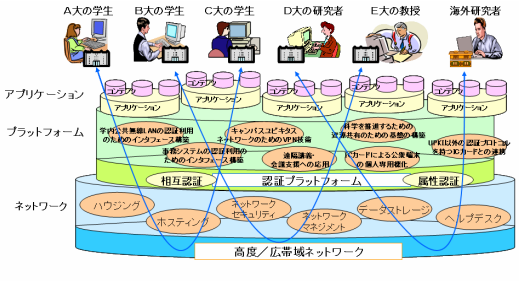

図 4. UPKIを用いたアプリケーション開発

(1) 学内公共無線LANの認証利用のためのインタフェース構築（北海道大学）

学生教職員や他機関からのキャンパスビジターが安全に利用可能な学内公共無線LAN及び大学間無線LANローミングについて，認証情報，属性情報に基づいて適切に認可付与を行うAPIを開発する．

(2) キャンパスユビキタス・ネットワークのためのVPN技術（東北大学）

講義室・会議室等に教職員や学生がノートPCを持ち込んでキャンパスネットワークやインターネットへのアクセスを利用する際に，どこのキャンパスであっても，あるいは訪問先大学であっても，本人のホームネットワークと等しく利用できるユビキタス・ネットワーク環境を安全・安心に提供することが望まれる．そのようなユビキタス・ネットワーク環境を実現するために，認証のための情報を安全に伝送し，PKI認証から得られる属性情報に基づいてコントロールすることにより，ホームネットワークへの仮想的接続と訪問先ネットワークへの制限付き接続を実現する機能をもつスーパーVPN技術を研究開発する．

(3) 事務システムの認証利用のためのインタフェース構築（東京大学）

事務・教務システムに典型的にみられる，アクセス権限に関して込み入った調整を必要とする学内・大学間共同利用サーバについて，認証情報，属性情報を利用して適切に認可付与を行うAPIを開発する．

(4) ICカードによる公衆端末の個人専用機化（名古屋大学）

PKIの秘密鍵を格納したICカードのアプリケーションを開発する．具体的には，キャンパス内の各

所に設置された公衆IP電話や公衆インターネット端末を，ICカードを挿入することにより，個人専用機化するシステムを開発する．これにより，キャンパス内のどこにいてもIP電話機での受信や，利用者を特定した状態での公衆インターネット端末の提供が可能になる．学内だけでなく，互換性を持つ電子認証基盤を有する大学間での利用も可能とする．

(5) 遠隔講義・会議支援への応用（京都大学）

遠隔講義受講時の出欠確認やコミュニケーション支援端末利用時の認証，電子化された講義アーカイブの遠隔からの受講，遠隔会議におけるスケジュール調整や資料の安全な電子的配布，匿名性を考慮した電子投票等，教員・学生双方が物理的にどこにいても講義・会議に自由に参加・発言できるシステム構築のための認証基盤の応用技術を開発する．

(6) 科学を推進するための様々な資源共有のための基盤の構築（大阪大学）

情報基盤センターは，科学を推進するための計算資源，プログラム，観測結果・計算結果データの蓄積等の基盤サービスを提供してきた．これらを認証基盤に対応させることにより，よりきめ細かな資源共有と保護が行える基盤を構築するため，NAREGIで開発中のソフトウェアを含めて導入し，併せてセンターの運用に合わせたAPIを開発する．

(7) UPKI以外の認証プロトコルを持つICカードとの連携（九州大学）

PKIとは異なる独自の認証プロトコルを持つQUPID ICカードが，図書館のID管理及び新キャンパス建物の入退室管理に採用されている．QUPID等の非PKI認証手法と全国共同PKI認証基盤との連携を取るためのブリッジAPIを開発し，セキュリティの評価を行う．独自の学内認証手法を採用した大学がUPKIに参加するための雛形を構築する．

(8) UPKIの構築（国立情報学研究所）

国際産官学連携による学術研究・教育を促進するCSIのセキュリティの確保を目的とした，認証基盤UPKIを構築する．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（Root CA, Bridge CA）を研究開発する．

参考文献

(1) 東倉洋一，他「情報セキュリティと法制度」，丸善サイエンスライブラリー，2004