サイエンティフィック・システム研究会　2005 年 10 月 27 日
平成 17 年度合同分科会資料

大学間連携のための全国共同電子認証基盤（UPKI）構築の構想

京都大学 学術情報メディアセンター
岡部 寿男
okabe@i.kyoto-u.ac.jp

【アブストラクト】 国立大学法人化や個人情報保護法施行などを契機として、全国の多くの大学で、それまで部局やサービスごとにばらばらであった認証系を統合した学内統一認証基盤の構築が進められている。大学間連携のための全国共同電子認証基盤（UPKI）は、公開鍵認証基盤（PKI）をベースに各大学の認証基盤を連携させ、大学間の単位互換や E-learning サービス、ネットワークローミング、グリッドによる研究連携など幅広い利用に供するとともに国際連携の橋渡しともなることを企図するもので、次世代の最先端学術情報基盤「サイバーサイエンスインフラストラクチャ」構想の一環として、国立情報学研究所と 7 大学情報基盤センターの共同事業として検討が進められている。本発表では、本構想の背景、要求要件、解決すべき課題、検討の現状などについて報告する。

【キーワード】 認証・認可基盤（Authentication and Authorization Infrastructure), 公開鍵認証基盤（PKI）, 連携 ID 管理（Federated Identity Management), 大学間連携, グリッド

1　はじめに

インターネット技術の進展とともに、社会のあらゆるサービスが、ネットワークを通じて提供されるようになってきた。大学においてもその例にもれず、研究、教育、図書館サービスから教務・財務・人事・庶務・施設管理・保健管理に至るまで、キャンパスで行われるほとんどすべての活動が、インターネットとキャンパスネットワークを基盤として電子化されつつある。各種サービスを電子的な認証を経て提供するための基盤として、教職員および学生の名簿の全学的な一元管理と各構成員への電子的な共通身分証の配布を進めている大学も少なくない。

これまでわが国では、こうした取り組みは各大学においてそれぞれに行われてきた。これは、目前に迫った大学間の厳しい競争の時代において、IT 戦略の成否が生き残るための鍵であるという認識からは頷けるかもしれない。しかし一方で、このような電子的な認証基盤を各大学に閉じて構築することの限界もある。たとえば、各研究機関が持つスーパーコンピュータなどの資源を組織の壁を越えて相互利用するグリッドの枠組みは、PKI による組織間の認証連携があってこそ成り立つものである。研究者が物理的に他大学を訪れたり、非常勤で他大学の講義を担当するする日常的なアクティビティにおいても、図書館の相互利用、ネットワークローミングサービスの利用などで「紙」ベースの認証を経なくてよいことのメリットは計り知れない。学生に対しても、今後広まると考えられる大学間の単位相互認定や e-learning などへの活用を考える上で、大学間の認証連携は不可欠である。

さらに、グリッドコンピューティングなどの応用においては、大学以外の研究機関との国際的な連携も想定されるべきものである。しかしながら、わが国においては職員・学生の名簿の電子的な一元管理とそれに基づく電子的な認証基盤構築でいくつかの大学が先行しているものの、その対象は大学あるいは法人に閉じたものであり、大学間連携や国際的な共同研究まで視野にいれたものは見当たらない。

全国共同利用情報基盤センター認証研究会では、各大学における情報基盤構築と、全国共同利用サービスにおける認証連携の両方の視点から、全国の大学でこれから導入されるであろう認証基盤がどうあるべきか、どのように構築しどのように連携させていけばよいかの検討を、平成16年度に開始した。その活動の一環として、七大学と国立情報学研究所（NII）が共同で「大学間連携のための全国共同電子認証基盤（UPKI）」の構築を構想し、平成18年度の概算要求として提案している。UPKIは、公開鍵認証基盤（PKI）をベースに各大学の認証基盤を連携させ、大学間でのさまざまな活動の支援に供するとともに国際連携の橋渡しともなることを企図するものであり、かつNIIによる次世代の最先端学術情報基盤「サイバーサイエンスインフラストラクチャー」構想の中核の一つに位置づけられるものである。

以下、2章で全国共同利用情報基盤センターのこれまでの歩みとその間の連携について、3章で大学間連携のための全国共同電子認証基盤の構想について、4章で大学におけるPKIの利用と課題について述べる。

2　全国共同利用情報基盤センターとその連携

国立七大学の情報基盤センター（図1）では、1960年代後半に大型計算機センターとして発足した当初から、全国共同利用の機関として他大学の研究者もユーザとして受け入れてきた。さらに学術情報センター（NACSIS、現・国立情報学研究所）が発足し、七大学間を結ぶ専用のX.25網の運用が始まった1986年からは、共通利用番号制と呼ばれるIDの一元管理とネットワークを通じた第二センター登録の制度を運用してきた実績を持つ。

1988年から始まったJAIN (Japan Academic Inter-University Network) プロジェクトによるIP over X.25での学術系IPネットワークの構築は、WIDEプロジェクトとともにわが国における草創期のインターネットバックボーンの構築に貢献した。1992年には学術情報センターによるSINETのサービスが開始され、七大学は地域の大学の接続拠点として位置づけられている。

また、全国共同利用情報基盤センター長会議の下におかれたグリッドコンピューティング研究会の活動において、SuperSINET上での大学間での認証基盤の実験的な接続も進められ、国立情報学研究所 (NII) のプロジェクトとして2003年に開始されたNAREGI (National Research Grid Initiative)[1] とも連携し、成果をあげている。一方、法人化を契機として、七大学でも、電子事務局構想など共通認証基盤構築の機運が高まりつつあることから、各大学での認証基盤の構築と、共通利用番号制に変わる新たな認証連携のしくみを考える枠組みとしてセンター長会議の下に平成16年度から新たに「認証研究会」が設置され、特に、グリッドコンピューティングの前提となっているPKIのグリッド以外へも応用について検討を進めている。さらに今年からは、七大学とNIIとの連携をさらに強化すべくNIIの中にネットワーク運営・連携本部が設置され、七大学センターのセンター長＋教員がNIIの客員としてSuperSINETの運用等の検討に直接関わるようになった。そし

て、その下に組織された認証作業部会において認証連携が議論され、次節に述べる UPKI 構想の具体化を進めているところである。

全国共同利用情報基盤センター間の連携の歴史について、表 1 に示す。

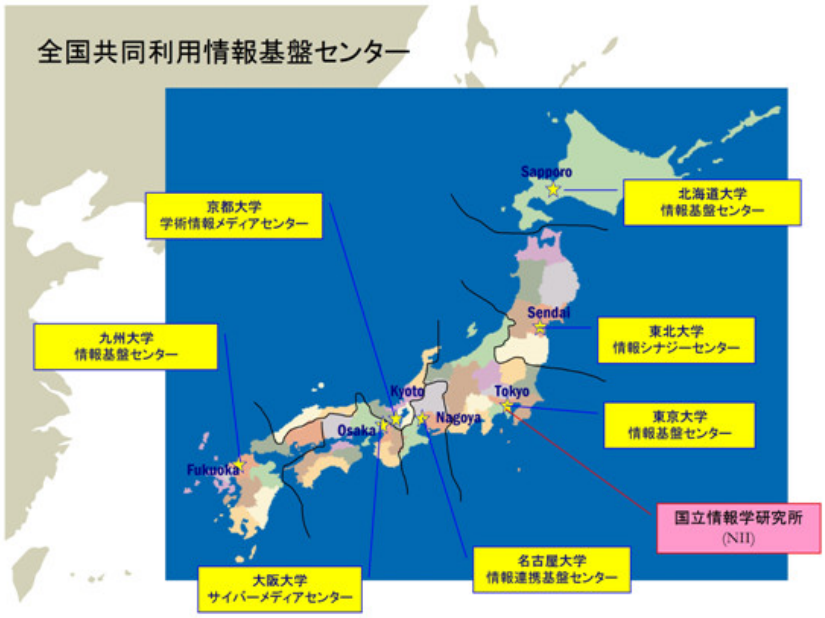

図 1: 全国共同利用情報基盤センター

表 1: 全国共同利用情報基盤センター間の連携の歴史

年代	事項
1965〜70	全国共同利用大型計算機センター、7 大学に設置
1981	X.25（DDX-P 商用パケットサービス）によるセンター間接続
1986	学術情報センター (NACSIS) 設置
	NACSIS による大学間を結ぶ専用 X.25 網サービス開始
	共通利用番号制（〜2004）
1998	JAIN (Japan Academic Inter-university Network) プロジェクト開始
1992	NACSIS による SINET サービス開始
2000	国立情報学研究所 (NII) 設立
2002	SuperSINET 運用開始
2003	NAREGI (National Research Grid Initiative) プロジェクト開始
2005	NII に学術情報ネットワーク運営・連携本部を設置、7 大学センターと NII との連携を強化

3 大学間連携のための全国共同電子認証基盤

大学間連携のための全国共同電子認証基盤 (UPKI) 構築事業の目的は、全国の大学が有するスーパーコンピュータや観測装置などのハードウェア資源、電子コンテンツ、そしてそれらを結ぶネットワークを、安全・安心に有効活用するための電子的な認証基盤を構築

することにある。そして、その構築を、国立七大学と NII が連携して行うことで、大学内の認証基盤と大学間の認証連携の国家的なモデル作りに、各大学はそれぞれの全学認証基盤の構築と地域の大学連携、NII はそれらを相互接続する大学間認証連携の基盤構築の立場で貢献しようとしている。

UPKI の効果は、共同研究や単位互換、e-learning 応用など大学間でのさまざまな活動において、構成員の相互認証を安全・安心かつ簡単に行えることである。具体的には、各種登録、決済、回覧などの業務が Web ベースで電子的に行えること、電子メールのやり取りにおいて暗号化と電子署名が誰とでも確実に使えるになること、他大学を訪問した際に、無線 LAN や公衆インターネット端末などのローミングサービスが受けられるようになること、グリッドコンピューティングにより各大学がもつ特徴的なハードウェア資源を必要なときに連携させネットワーク上で統合できることである。

この事業のコンセプトの背景には、かつて 8 センター間で行われていた共通利用番号制がある。共通利用番号制では、アカウントの文字列の数字の最上位が図 1 に示す地区別を表す[1]ようにして、ID 空間を分割し分散して管理できるようにすることで、今日言うところの Federated Identity Management を素朴な形で実現していた。もう一つ特徴的なことは、主として利用する最寄の大学のセンターを第一センターとして登録する手続きを済ませておけば、他のセンターの利用の手続きはすべてオンライン申請で行えたことである。これは原始的な形の SSO (single sign on) の実現であったと言えると同時に、何事にも捺印を要求する役所の手続きとしては画期的なことであった。特に、他大学の人間がセンターの利用するに際しては大学間で利用負担金のやりとりを行う必要があるが、共通利用番号制では、当該利用者の利用資格だけでなく負担金の支払い能力までも、いわば第一センターが保証していたわけであり、認証・認可連携としてかなり高度なことを実現していたとも言える。

しかるに、現状の大学内の電子認証システムの多くは、ID/パスワードの組み合わせを部局ごとあるいはシステムごとに持つもので、利用者の混乱とモラルの低下を招きやすく、結果的にパスワード漏洩による事故のリスクが高いものである。情報セキュリティ意識の高まりや個人情報保護対応の中で、各大学では急ピッチで学内認証系の統合と SSO（シングルサインオン）の導入による一元的な認証システムの構築を進めているところであり、このようなシステムを各大学でばらばらでなく全国で共通のものにするには、この機をおいてない。

UPKI の構築を「全国共同」で行うことの意義は、大きく三つあると考えている。一つめは、大学間連携に対する直接的な貢献である。電子図書館や e-learning などのコンテンツのネットワークを介した共有だけでなく、今後さらに進むであろう学生・教員の流動化への対応、たとえば学生の単位互換、教員の共同研究や非常勤の講義のサポートも重要な視点である。また、法人化後それぞれの道を歩みつつある国立大学間において一定の絆ともなりうる。二つ目は、仕様の共通化により、各大学におけるセキュリティレベルの一定水準の確保と、システム導入・開発コストの削減を図れる可能性である。三つ目として、日本国内の大学が共通仕様を持つことで、国際的な大学連携、産学連携、あるいは自治体などと地域連携を考える際に一定の発言力を持つことができ、国際標準への対応だけでなく標準化そのものへの貢献もやりやすくなるであろうとの期待がある。

[1]たとえば W**5**5070 というアカウントにおいては数字の 5 が第五地区すなわち京都大学の管轄である京都府、石川県、福井県、鳥取県、島根県を表す。

4　UPKIのアプリケーション

UPKIがターゲットとするアプリケーションは、大学におけるすべての電子化された活動に渡るものと考えている。具体的には、履修登録からe-learning、電子図書館まで各種のWebサービス、ローミングやVPNなどのネットワークサービス、建物入退室管理や講義の出欠確認、そしてグリッドのような研究用資源の共有である。

この中でやはりWebサービスの認証統合は汎用性という点できわめて重要になる。大学ポータルという形でシングルサインオンの枠組みを提供することは、学生や研究者に対して大学が提供するサービスの質とセキュリティレベルの向上に直接的につながるものである。WebサービスのSSOに関してはSAML (Security Assertion Markup Language)[2]やLiberty Alliance[3] などで標準化が進められており、ある意味大学だからといって特段新しい話ではないが、大学のような縦割り志向かつ部局自治の意識の強い組織で、レガシーシステムをいかに全学的なシステムに統合していくかには困難が伴うことが予想される。これについては七大学それぞれが持ち味を生かして異なるアプローチで進めるとともに、横並び意識も活用して他の大学の経験をうまく活用することも考えている。

一方、それ以外のアプリケーションについては、七大学がそれぞれ特徴的なアプリケーションを選択し、それをテーマにリーダーシップをとることにしている。各大学の担当テーマは表2の通りである。テーマの詳細については文献[4]を参考にされたい。

表 2: 各大学の開発テーマ

大学	テーマ
北大	学内公共無線LANの認証利用のためのインターフェース構築
東北大	キャンパスユビキタスネットワークの構築
東大	事務システムの認証利用のためのインターフェース構築
名大	ICカードによる公衆端末の個人専用機化
京大	遠隔講義・会議支援への応用
阪大	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
九大	ICカード連携

5　大学における公開鍵認証基盤の利用と課題

UPKIのもう一つの特徴が、公開鍵認証基盤（Public Key Infrastructure; PKI）の積極的な利用である。これは、電子証明書による本人証明と電子メールなどの暗号化を可能にすること、ICカード等に秘密鍵を格納することでネットワーク経由の不正だけでなく身分証偽造などによる犯罪にも備えること、グリッド技術との親和性によりスーパーコンピュータのサービスへの応用していくこと、の三点を意識している。

わが国でもすでに電子政府関連でGPKI[5]、LGPKI[6]、JPKI[7] などにおいてPKIが実用に使われているが、十分な普及にいたっているとは言いがたく、課題も少なくない。PKIそのものは安定した技術になっているが、その運用技術についてはまだまだ研究すべき余地があると考えている。電子政府では米国においてもe-authentication[8]において省

庁間の独立性を重んじた緩い SSO の仕組みを導入しており、参考にすべき点が多いと考えている。

大学における PKI の展開においては、以下のような課題がある。

(1) 認証局の運用方法

- パブリック CA かプライベート CA か
- プライベート系のアーキテクチャをどうするか

(2) 認証局のソフトウェア

(3) 証明書の登録・配布モデル

(4) 証明の対象

(1) については、たとえば外部に公開する Web サーバの SSL サーバ証明書にはパブリックなものが必須である一方で、学生を含む全構成員のクライアント証明書をパブリックなものにすることについてはその必要性とコストの兼ね合いで検討の余地がある。グリッドのような比較的ゆるいポリシーでの運用が現状想定されている応用にはパブリックなものは使いにくい。そのことから当面はパブリック系とプライベート系の併用が必要であろうと考えている。プライベート系については 7 大学が CA（認証局）を持ち、NII がブリッジ認証局となるアーキテクチャを想定している。

(2) の認証局のソフトウェアについては、NAREGI の成果物である NAREGI-CA の利用を核に考えている。その一方で、本プロジェクトを七大学でやることの意義は多様性の評価にあることも意識しており、可能な限りマルチベンダー環境でのインターオペラビリティの検証につとめる覚悟である。

(3) の証明書の登録・配布モデルについては、主体者発行 (subscriber enroll) とバルク発行 (bulk issuing) のいずれのモデルを採るかが検討課題である。前者は 4 月に新入生数千人に対して短期間に発行が求められる大学の事情を考えると困難が多い。しかし、後者は本人に手渡すまでの間や手渡しの際の本人確認において安全性が損なわれる可能性もある。

(4) の証明書の対象は、クライアント証明書をどこに格納するのか、身分証兼用の IC カード内なのか、USB キーなのか、あるいはパソコンに格納でよいのかに検討の必要がある。身分証の IC カード化についてはクレジットカード会社との提携など技術以外の検討課題もあり、全国の大学で職員証・学生証に同一規格の IC カードを採用するようなことは困難だと考えられる。

我々が PKI にこだわる理由の一つはグリッドとの親和性であり、いわばグリッドの認証連携技術を大学でのさまざまな応用に展開していこうという方向である。ちなみに、米国 Internet2 のプロジェクトである Shibboleth[9] では、Web サービスにおける SSO を主軸に実証的な研究活動を進め、SAML2.0 など標準化への貢献も多いが、最近ではさらに GridShib とよばれる Shibboleth での認証連携の情報をグリッドで用いるようなアプローチが試みられており、Globus Toolkit のプロジェクトの中で開発が進められている。また、欧州の大学間での無線 LAN ローミングプロジェクトである EduRoam[11] でも、Shibboleth の認証連携の活用が検討されている。すなわちこれらは Web サービスの SSO の認証連携技術を Web サービス以外に展開していくアプローチであり、我々と逆であるという点で興味深い。これらがいずれ競合するのか、あるいは相補的に一つの技術へとまとまっていくのか、今後の研究の進展が待たれるところである。

6　おわりに

UPKIの対象とする領域は、各大学の情報基盤センターにおいても、スーパーコンピュータシステム、キャンパスネットワーク、情報処理教育システムなどすべてのサービスにそれぞれ異なる形で関連する。さらに、中央の事務組織や、図書館など全学サービスを行う学内センター等との連携も必要である。大学間の連携以前に、大学の内において情報基盤センター系の教職員と、学内の各部局やセンターの教員、事務部門の担当者などと、人と人との関係という意味でまず連携していくことの必要性を痛感させられている。

かつて、全国の大学のキャンパスネットワーク整備と学術系インターネットバックボーンの構築において、七大学はある種の主導的な役割を果たしたと自負しており、UPKIが、今後の各大学における共通認証基盤の構築とその全国レベルでの相互接続において、同種の役割を担うことができればという期待もある。しかしながら、現状ではむしろ、トップダウン的経営がなされている私学や、国公立でも小回りの利く中規模大学にこそ学ぶべきことが多い。我々としても、七大学の枠組みを主に考えているのは全国共同利用のサービスの連携においてであり、基本的にはすべての大学と対等にあらゆる形で協調していけるようにしていくべきと考えている。このプロジェクトは決して七大学に閉じたものではないことをご理解いただき、各位のご指導とご協力を切にお願いしたい。

謝辞　日頃からご議論くださる国立情報学研究所ネットワーク運営・連携本部認証作業部会の各位に感謝する。

参考文献

[1] 国立情報学研究所グリッド研究開発推進拠点, 超高速コンピュータ網形成プロジェクト, http://www.naregi.org/

[2] OASIS Security Services (SAML) TC, Security Asseration Markup Language V2.0, http://www.oasis-open.org/committees/security/

[3] Liberty Alliance Project, http://www.projectliberty.org/

[4] 曽根原他, 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, 全国共同利用情報基盤センター研究開発論文集, No.27, pp.79–89.

[5] 総務省行政管理局, 政府認証基盤 (GPKI) のホームページ, http://www.gpki.go.jp/

[6] 総合行政ネットワーク運営協議会, 地方公共団体における組織認証基盤 (LGPKI), http://www.lgpki.jp/

[7] 公的個人認証サービス都道府県協議会, 公的個人認証サービスポータルサイト, http://www.jpki.go.jp

[8] Federal Chief Information Officers Council, E-Authentcation http://www.cio.gov/eauthentication/

[9] Internet 2, Shibboleth Project, http://shibboleth.internet2.edu

[10] University of Chicago, GridShib: A Policy Controlled Attribute Framework, http://gridshib.globus.org/

[11] eduroam: Network roaming for higher education and research, http://www.eduroam.org/