

● 事例紹介 ●

九州大学の全学共通ICカード導入プロジェクト

安浦 寛人

(九州大学システムLSI研究センター長・教授)

池田 大輔

(九州大学大学院システム情報科学研究院・准教授)

一 情報化時代の個人認証基盤

情報技術の発展によって、社会の隅々にまで情報技術が利用されるようになり、種々のサービスが自動的に利用者を認証してサービス提供を行うようになってきました。例えば、銀行のATMカードやクレジットカードなどの金融取引、建物や部屋の入退管理、交通機関のプリペイドカードや定期券(Suicaなど)、ポイントカードや電子マネー(Edyなど)、催し物のチケットや利用券、コンピュータシステムの利用やウェブサービスなど、我々の日常生活の中で、情報技術を用いた個人や個人が持つ権利の自動的な認

証は不可欠なものとなっています。このような個人の認証には、磁気カードやICカードなど認証用の証拠の提示、指紋や静脈を用いた生体認証、ID番号とパスワードによる認証などいろいろな方法が使われています。しかし、個々のシステムやサービスごとにその方法が異なり、利用者の負担が大きくなるという問題があります。財布の中のカードが多くて困る、指をケガして指紋認証が使えない、パスワードが多すぎてすぐに忘れてしまうなど、皆さんも思い当たることが多いと思います。

また、社会保険庁の年金問題のように、認証の基盤が杜撰に構築されると、大切な個人の財産や権利に大きな障害

が出てきます。さらに、複数のサービス間で個人の利用情報を統合することでプライバシーが侵害されるというような問題を懸念する声もあります。一方、サービスを提供する側も、個人情報保護法の下で、厳格なデータの管理を要求されており、事故に繋がらないような個人認証の仕組みを最低限のコストで構築・運用する方法が重要になってきます。

このように、個人の認証に関する技術は、情報化社会の中の重要な基盤技術となっており、多くの従業員や利用者を持つ組織(自治体、企業、学校など)の運営においても、最も基本的で重要な技術となっています。本稿では、九州大学で進めている個人認証基盤の開発の現状を紹介し、今後の展開について説明します。

二 PIDモデルとM-IIDシステム

九州大学では、学内サービスの向上、学内業務の効率化、およびこれらの情報化に対応する共通的な個人認証基盤を構築するために、全学共通ICカード導入の準備作業を行っています。将来の社会基盤となり得る新しい認証基盤技術を提案し、それを元に実用的なシステムを構築しようとする

る、研究・開発・利用を統合した学内プロジェクトです。基本的には、

- (一) 一〇年以上有効な安定した枠組み
- (二) 利用者や運用者に分かりやすい仕組み
- (三) 個人情報保護がやりやすい仕組み
- (四) サービスの更新や技術革新への柔軟な対応
- (五) コストがかからない仕組み

を考えています。我々は、独自の認証基盤として、PID(Personal ID)モデルを考案し、それを発展させてM-IID(Media Independent ID)システムを構築しました。具体的には、大学が発行するICカード(将来は携帯電話やUSBデバイスにも搭載)により、学内のいろいろなサービスを受けることができ、しかもサービスの変更や予期せぬ事故による被害に最小限のコストで対応できるシステムとなっています。利用者(学生や職員)は、建物や部屋への入退出のための鍵、図書館などのサービスを受けるための証明書、コンピュータを介したサービスのための個人ID、交通機関や食堂・購買部を利用する際の電子マネーなど幅広い用途にこのカードを使うことができます。

PIDモデルは、IDの発行者、各サービスの提供者、利用者の三者からなるモデルです(図1参照)。

サービス毎に異なる識別子 (SubID) を用いる
サービス間の独立性, 個人情報保護, リスク管理, コスト低減

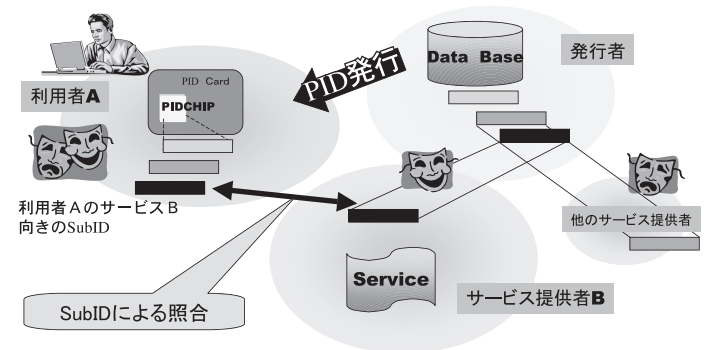


図1 PID(Personal ID)モデルのアイデア

subIDと発行者からもらったsubIDを照合することで正規の利用者であることを認証します。個人名や性別、年齢、住所などの情報は必要最小限のものしかサービス提供者へは与えられません。例えば、入退室管理の場合、入出の権利の有無の情報だけで良く、名前などの個人データは不要なはず。このように、サービス提供者へ与える情報を最小限にすることで、事故の際の個人情報の漏洩を防ぐとともに、サービス提供者の個人情報保護のための対策コストを最小限に抑えます。持っていない情報は漏洩することはありませんから、情報を持たないことが重要なのです。

さらに、利用者側も自分のsubIDをサービス提供者が知っていることを確認することで、正しいサービス提供者であるかを確認できます。このような相互認証の仕組みは、フィッシングなどのなりすまし詐欺から利用者を守る方法として、今後重要になります。

PIDシステムの概念は、ICカードだけではなく、内部に計算機能を持つ携帯機器(携帯電話やUSB端子に接続する機器など)にも適用できます。われわれは、メディアに依存しないIDの仕組みとして、MIID(Media Independent ID)システムを提案しています(図2参照)。情報技術の進歩により、今後ハードウェアの形態はどんな

発行者は、利用者の個人情報などを確認した上で、利用者にICカードを発行します。一般には、大学のような組織がそこに所属する学生や職員にICカードを発行する形をとります。この時、発行者は利用者の利益を守る社会的責任があることを前提とします。このICカードの中には、複数のID (subIDと呼ぶ) が含まれます。ICカードでは、カード内の集積回路 (IC) にコンピュータが搭載されており、種々の計算が行えるので、種となるID (PIDと呼ぶ) から、異なるsubIDを計算するプログラムを搭載することにより、たくさんのsubIDを持たせることができます。複数のサービスの利用にあたっては、サービスごとに異なるsubIDが用いられます。万一あるサービスでsubIDの漏洩があっても、他のサービスには波及しないということになります。

サービスは、一般に発行者とは独立しているサービス提供者が提供します (発行者とサービス提供者が一体となる場合も含む)。サービス提供者は、サービスを提供したい旨を発行者に連絡し、発行者はサービス提供者やサービスが、利用者にとって有害でなく利益をもたらすものであるかを判断して、必要なデータをサービス提供者に渡します。このデータには、各利用者の当該サービスに対するsubIDが含まれます。サービスの提供は、利用者から提示される

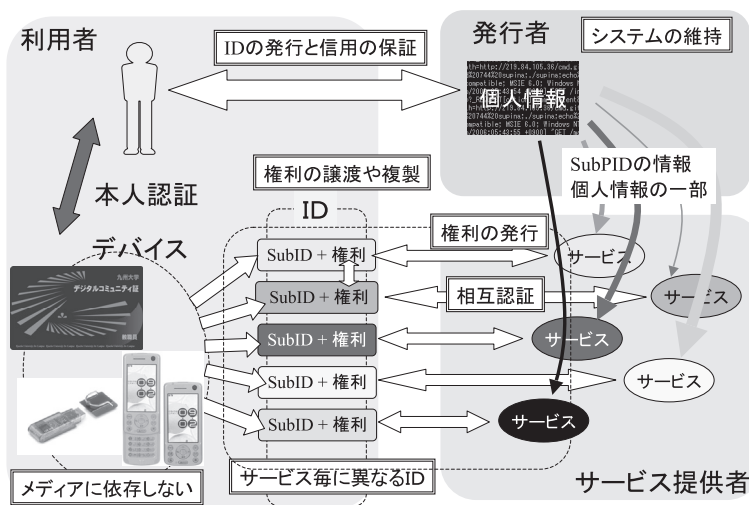


図2 MIIDシステムの概略図



図3 デジタルコミュニティ証（左：教職員用、右：学生用）
デザインは、学内公募で募集

ん変わっていくと考えられます。しかし、その度にIDの仕組みを変えていたのでは、社会が混乱します。IDの仕組みは、搭載するハードウェアや提供されるサービスの種類とは無関係に、長期間安定的に利用される仕組みであることが重要です。

このような新しいMIIIDシステムの採用により、大学のサービスにおいても下記のような点が有利になります。

(一) 利用者から見た利点
* 一枚のカードの発行で複数のサービスを安全に享受できる。

* 発行者（大学）への個人情報の提供のみで複数のサービスが利用できる。

* 一つのサービスで事故が発生しても他のサービスには被害が波及しない。

* サービスを跨いだ個人の追跡が困難であるので、プライバシーが守られる。

* 個人情報とサービスの利用情報を分離することができる。

(二) サービス提供者から見た利点
* サービスごとにIDの発行や個人情報の収集を行わなくて良い。

* それぞれのサービスに見合ったセキュリティ投資で
も他のサービスに迷惑をかけない。
* 利用者の正当性の保証は、発行者に任せることができ
る。

(三) 発行者から見た利点

* サービス提供者を監督できるので、利用者を保護し
やすい。

* 新しいサービスを容易に導入することで、利用者
に便宜を図りやすい。

もちろん、一枚のカードに多くのサービスが集約されることによるカード紛失時のリスクの増大や発行者への情報集中による発行者の責任の増大など欠点もありますが、サービスごとに複数のカードを発行する非経済性や、同じIDで複数のサービスを提供することによる事故の際の被害の波及の増大など現在の多くのシステムが抱える潜在的な弱点は克服することができます。

三 学内での実証実験

平成二一年度からの全学の本格採用に向けて、平成一六

年から、多くの企業と連携しながら技術開発を進めてきました。平成一八年からは、経済産業省の「デジタルコミュニティ実証実験事業」を受託し、学外も巻き込んだ大規模な実証実験を行っています。

現在、伊都キャンパスの学生と職員約五〇〇〇名にデジタルコミュニティ証と呼ぶICカードを配布しました（図3参照）。

現在は、伊都キャンパスの建物の入館管理、講義室などの入室管理、理系図書館への入館管理と本の貸出し管理に利用しています。今後、

キャンパスや駐車場の入構ゲート、学生の証明書発行、各種教務サービス、コンピュータシステムの利用管理などへの展開を考えています。また、事務に関しては、経理システムや成績登録システムなど教員や事務職員の作業の効率化と安全性の向上に利用することを計画しています。また、学内で営業している生協や紀伊国屋書店での支払いも、デジタルコミュニティ証で行えるようにしています。これは利用者の銀行口座と連携したサービスです。

平成一八年度の「デジタルコミュニティ実証実験事業」の中では、学外の六〇社余りの企業と連携し、MIIIDを用いた種々の実験を行いました。交通系では、福岡市営地下鉄、JR九州、昭和バス、昭和タクシーの協力を得て、デジタルコミュニティ証に回数券や定期券の機能を持たせる実験を四〇日に渡って行いました。また、伊都キャンパス周辺の小売業、飲食業、理髪業など種々の店舗でもデジタルコミュニティ証での決済の実験を行いました。

今後は、福岡市内の複数の大学が連携してMIIIDを利用した認証基盤を整備し、交通機関や小売業の利用を地域規模で行えるように計画しています。交通事業者は、定期券などの発行をしなくて済むようになり、大きなコスト削減が実現できる可能性があります。

四 まとめ

個人認証の技術は、今後の情報化社会の中で重要な基盤技術です。九州大学の全学共通ICカード導入プロジェクトは、大学の効率化やサービス向上とともに、今後の社会の方向を考える社会実験の場としても重要な意味を持つと考ええます。

参考資料

池田大輔、安浦寛人、「全学共通ICカードの学内実証実験報告とその基盤技術について」、九州大学情報統括本部ITマガジン、第一巻第一号、一三〇～一二頁、二〇〇七年六月