Vol.2015-CSEC-69 No.29
Vol.2015-IOT-29 No.29
2015/5/22

豊橋技術科学大学における身分証のICカード化

土屋 雅稔[1,a)]　中村 純哉[1,b)]

概要：近年，各種業務をネットワーク上の情報システムで行う場合が急増している．そのような業務には，本人確認が重要な業務も含まれるため，ユーザ名 · パスワード方式に代わる強固な認証が不可欠となっている．そのような強固な認証方式として，個人証明書が格納されたICカードを身分証として利用する方法がある．本稿では，豊橋技術科学大学において身分証をICカード化した事例について述べる．

キーワード：認証，ICカード化

Introduction of integrated circuits on identification cards of Toyohashi University of Technology

Abstract: There are an increasing number of information systems for university management works based on the campus network. Several works claim more secure authentication method than password-based authentication method. A multi factor authentication method using a client validation certificate stored in an integrated circuit on an identification card is a candidate satisfies the above claim. This article explains introduction of integrated circuits on identification cards of Toyohashi University of Technology.

Keywords: Authentication, Integrated Circuit Card

1. はじめに

近年，仮想化技術とネットワーク技術の進展に伴って，各種の業務を，ネットワーク上の情報システムで行う場合が急増している．そのような業務の中には，従来であれば，物理的な本人確認や制約によって安全を担保していたような業務も含まれている．そのため，ユーザ名 · パスワード方式に代わる強固な認証が不可欠となっており，多要素認証方式を導入する例が増えてきている．

多要素認証を実現する方法としては，個人証明書を用いる方法，事前に配布したマトリックスなどに記載された記載された秘密情報を組み合わせる方法，専用のハードウェアトークンを用いる方法，個人所有の携帯電話などにインストールしたソフトウェアトークンを用いる方法などの，幾つかの選択肢が存在する．

豊橋技術科学大学では，学生の長期欠席を早期に検出することなどを目的とする出席管理システムの導入が，教務担当の事務部門により2013年度に計画された．従来，磁気ストライプ方式の学生証および職員証を利用していたが，磁気ストライプ方式のカードリーダは1人あたり15〜30秒程度の処理時間を要するため，大講義室では休憩時間中に出欠登録が完了しない問題が判明した．この問題に対応するため，より短時間に出欠登録が可能な方法として，ICカード方式の身分証に変更することが計画された．

本稿では，豊橋技術科学大学 (以下，本学) において，個人証明書を格納したICカードを身分証として利用して多要素認証を導入した事例について報告する．

2. 多要素認証の必要性

近年，大学の情報システムもネットワーク化が進行しつつあり，従来は紙媒体で実現されていた各種の重要な業務が，ウェブ化されつつある．本学の場合，まず最初に，研究費管理システムと給与明細システムにおいて強固な認証が必要となった．研究費管理システムは，教員が各自の研究費残高を確認できるだけでなく，発注手続きなども行うシステムである．これは，適切な権限を有する教員が行わ

[1] 豊橋技術科学大学情報メディア基盤センター
Information and Media Center, Toyohashi University of Technology
[a)] tsuchiya@imc.tut.ac.jp
[b)] junya@imc.tut.ac.jp

なければならない業務であり，強固な認証が必要である．また，従来の給与明細は，特殊な用紙に印刷して，封筒状に貼り付けることにより，プライバシを確保するという方法が取られていた．しかし，プリンタの老朽化に伴う更新費用の確保の問題，貼り付け作業の人的負担の問題があり，給与明細システムの導入が検討されている．給与明細は，各教職員にとって重要なプライバシ情報であり，これも強固な認証が必要である．

強固な認証を実現する方法として，個人証明書を用いる方法，事前に配布したマトリックスなどに記載された記載された秘密情報を組み合わせる方法，専用のハードウェアトークン [*1] を用いる方法，個人所有の携帯電話などにインストールしたソフトウェアトークン [*2] を用いる方法などの，幾つかの選択肢が存在する．ソフトウェアトークンを用いる方法は，ソフトウェアトークンのインストール先として個人所有の携帯電話を利用すれば，ハードウェアとしては安価に実現できるという利点がある．しかし，全教職員の各種多様な携帯電話に対してソフトウェアを提供することは非常に困難であり，全教職員が業務上必ず利用しなければならないようなシステムの認証手段としては不十分である．ハードウェアトークンを用いる方法は，近年かなりの進歩があり，安価かつ小型の製品が利用できるようになってきている．しかし，ハードウェアトークンは安全に保管しておく必要があるが，全教職員に安全な保管を依頼・徹底することはかなりの教育コストを要する．事前に配布したマトリックスを用いる方法は，東京工業大学 [*3] やオンラインバンキングなどにおいて多数の採用事例がある方式である．大学の場合，身分証の裏面にマトリックスを印字して構成員に配布すれば良い．しかし，マトリックスを複写すれば，容易にアカウントの貸借が可能であるという問題点がある．また，本学で調達のために調査した範囲では，特許などの事情により認証システムがかなり高価で，導入は困難と判断された．上記に対して，個人証明書を格納した IC カードを身分証として用いる方式では，安全に保管しなければならないハードウェアは身分証のみであり，これは従来より安全に保管されているはずである．また，IC カードは偽造や複製が著しく困難であるため，アカウントの貸借のためには，身分証そのものを貸借しなければならず，少なくとも日常的・継続的にアカウントを貸借することは困難であると考えられる．

上記の理由により，本学では，身分証を IC カード化し，IC カードに個人証明書を格納して配布することにより多要素認証を実現することを計画した．

個人証明書を格納する IC チップの形式としては，接触型と非接触型の 2 つが検討対象となる．接触型 IC チップは，ISO/IEC7816–3 によって規格化されている形式である．非接触型 IC チップとしては，ISO/IEC–14443 によって規格化されている Type A 方式や Type B 方式，ISO/IEC–18092 によって規格化されている Felica 方式が一般的である．Type A 方式は，ヨーロッパやアジアで、鉄道など交通機関向けプリペイドカードや身分証明書用として利用されている．Type B 方式は，住民基本台帳カードやクレジットカードとして利用されている．Felica 方式は，日本では交通機関向けプリペイドカードや電子マネー用カードとして，広く利用されている．多要素認証の利用にあたっては，教員各自の端末が利用できること，言い換えれば，OS やブラウザについて強い制限がないことが重要である．この点を重視して調査したところ，非接触型は，接触型に比べて対応ドライバの種類が少なく，制限が強く必要になることが確認された．そのため，本学においては，個人証明書は接触型 IC チップに格納することを計画した．それに対して，出席管理システムなどでは，迅速な出席登録処理のために，非接触型 IC チップが必須である．非接触型 IC チップについては，国内において最も多くの採用例があり，かつ発行枚数も最多である Felica 方式がコスト面において優位であった．

このように選定作業を進めると，職員証については，接触型 IC チップと，Felica 方式の非接触型 IC チップを同梱したハイブリッド方式 IC カードとすることが妥当であると考えられた．しかし，ハイブリッド方式 IC カードは，Felica 方式の非接触型 IC チップのみからなる IC カードに比べて高価であり，学生証を含めて全面的に採用することは，予算的な困難があった．学生証の利用について，慎重に検討したところ，先に述べたような厳重な個人認証が必要となる事例は学生証においては少ないのではないか，という考えのもとに，学生証については Felica 方式の非接触型 IC チップのみからなる IC カードを採用することとした．

なお，職員証・学生証ともに，移行の過渡的措置として，JIS II 規格に準拠した磁気ストライプを有するカードを採用した．

3. 実装

本学の身分証の IC カード化では，非接触型（Felica 方式）と接触型（ISO/IEC7816）の両者を備えたハイブリッド IC カードとして凸版印刷（株）の SMARTICS-PKI Smart Card を採用した．この IC カードはマルチプラットフォーム（Windows, Mac OS X, Linux）に対応している．大学という多種多様な利用環境が想定される組織において，このことは大きな利点である．特に，Windows 用のドライバは WHQL 認証を取得しているため，Windows 環境では IC カードをカードリーダに挿入するだけで自動的に Windows Update からドライバをインストールすることができる．

[*1] 例えば，Yubikey など．
[*2] 例えば，Google Authenticator など．
[*3] http://portal.titech.ac.jp/ezguide/matrix-login.html

接触式 IC カードリーダは USB 接続の HID OMNIKEY 3121 を採用した．IC カードと同様マルチプラットフォームに対応しており PC/SC 規格に準拠しているため，標準的なドライバで利用することができる．本学では全教職員に IC カードリーダを配布している．研究費管理システムや給与明細システムなど，重要な情報を扱う Web サービスを利用する際に，IC カードに格納された個人証明書を用いたユーザ認証のために使用する．

以降では，IC カード化された身分証と関連するシステムについて概要を説明する．

3.1 管理系システム

学内には身分証の新規発行や紛失に対応するために，次の管理系システムが設置されている．

IC カード発行機 新規 IC カードを発行する．発行の際には，認証局によって署名された個人証明書を IC カードの接触型領域に書き込み，IC カードの表面に所有者情報（氏名，所属，顔写真など）を印刷する．発行した IC カードの Felica IDm をユーザ管理システムに送信し，LDAP 属性として他システムから参照できるようにする．新年度前など大量の IC カードを発行する場合は発行作業は業者に委託し，Felica IDm 等の情報は別途 CSV 形式で取り込む．

認証局・登録局 ユーザ管理システムから個人証明書の発行依頼を受けつけ，発行対象のユーザの個人証明書を発行する．ユーザが利用資格を失った場合には，個人証明書の失効処理を行う．

ユーザ管理システム LDAP サーバ上に学生，教職員の Felica IDm や IC カード再発行回数などを持ち，他システムに IC カード情報を提供する．

3.2 サービス系システム

2015 年 4 月現在，学内には IC カード化された身分証によって利用可能なサービス・システムが 4 台稼働している．

プリペイドシステム 食堂・喫茶・売店では，非接触式 IC カードリーダに身分証をかざすことで，キャッシュレスで決済ができる．身分証への現金のチャージは学内に設置されたチャージ機を使う．チャージ金額の情報は Felica の専用領域に格納される．売店では，売価の 10%引きで商品を購入できるサービスを行っている．

出席管理システム 各教室に設置された非接触式 IC カードリーダと，出席状況を確認するための Web サービスから成る．学生が講義出席時に学生証をカードリーダにかざすことで，出席したことがシステムに記録される．このとき学生証に格納された学籍番号を読み取ることで，学生の識別を行う．教員は出席管理システムにアクセスすることで学生の出席状況を確認することができる．各教員が出席状況を確認できる学生の範囲は次のとおり: (1) 担当講義を履修している学生，(2) 自研究室に所属している学生，(3) 担任しているクラスの学生．また出席率の悪い学生や講義を抽出する機能を持つ．

研究費管理システム 各教員が管理する研究費の執行状況を確認や物品購入の申請を行うことができる Web サービスとして提供されており，利用者は接触式 IC カードリーダを手元の PC に接続し，IC カードに格納されている個人証明書によって認証を行うことで利用できる．個人証明書による認証については 3.3 節で述べる．

プリンタ管理システム 情報メディア基盤センター等，学内に設置された教育用端末から送られる印刷ジョブを管理する．ユーザは端末から印刷操作を行った後，プリンタに据付の非接触式 IC カードリーダに身分証をかざすことで認証を行う．印刷ジョブはプリンタ管理システムから認証が行われたプリンタに送られ，実際に印刷が行われる．

3.3 個人証明書を用いた認証

研究費管理システムなど重要な情報を取り扱う Web サービスでは，広く用いられているユーザ名とパスワードによる認証ではなく，IC カードに格納された個人証明書による認証を利用者に要求する．ここでは IC カードに格納された個人証明書によって認証を行う際の流れについて説明し，続く 4 節で Mac OS X 環境で個人証明書による認証を行う際の問題について議論する．

IC カードに格納された個人証明書によるユーザ認証が必要な Web サイトを表示するときは，次の順で操作・通信が行われる．

(1) IC カードリーダを PC に接続し，IC カードを挿入する
(2) Web ブラウザで Web サイトに接続する
(3) Web サイトは，接続を受け入れる認証局の証明書リストを Web ブラウザに送信する
(4) ユーザは Web サイトに送信する個人証明書を選択する
(5) Web ブラウザは Web サイトに選択された個人証明書を Web サイトに送信する
(6) PIN コードの入力ダイアログが表示されるので，PIN コードを入力する
(7) IC カード内の秘密鍵で Web サイトから送信されたデータを暗号化する．Web ブラウザは暗号化されたデータを Web サイトに送信する．
(8) Web サイトは個人証明書に入っている公開鍵を使って，暗号化されたデータを復号する．復号したデータと自分が送信したデータを比較し一致した場合は，正しいクライアントだとみなし，要求されたコンテンツを Web ブラウザに返す．

(6) で Web サイトが送信した認証局リストに含まれない認証局によって署名された個人証明書が送信された場合は，

SSL セッションは確立せず，通信失敗となる．

4. IC カード認証の Mac OS X 対応の問題とその対策

Mac OS X において，IC カードに格納された個人証明書による認証を実現するためには，いくつか問題がある．ここでは，今回の導入にあたって発生した問題について，その原因と行った対策について述べる．

4.1 不透明な OS レベルの IC カード対応方針

Mac OS X で IC カードを扱うためのフレームワーク SmartCard Services は，OS X 10.7 以降 OS から削除された．以降，公式には Mac OS X では IC カードはサポートされていない．SmartCard Services の開発はその後オープンソースプロジェクトとして継続されており，その成果は Mac OS forge にて公開されている [1]．Mac OS X 10.7 以降で IC カード認証を行うためには，Mac OS forge からダウンロードできる最新版の SmartCard Services が必要となる．

一方で Apple は，Mac OS X 10.10 で新しい CryptoTokenKit と呼ばれるフレームワークを導入した [2]．この低レベルフレームワークは IC カードと通信を行うための機能を持っているが，現時点では OS へのログインや Web サイトの認証などで IC カードを使うための機能は提供されてない．今後 Apple が CryptoTokenKit を使用した IC カード認証機能を OS に組み込み，再度公式に OS レベルの IC カード対応を復活させるのかどうかは不明である．

OS 開発元の方針の不透明さは，IC カードドライバのサポート状況にも影響する．今回本学で採用した TOPPAN SMARTICS-PKI Smart Card は，SmartCardServices 向けのドライバが提供されなかった．IC カードを販売する企業としても OS 側の対応方針が不明瞭なので，将来いつまで使えるか不明なドライバを開発するリスクを負いたくないということなのだろうと推測する [*4]．

以上述べてきたように，Mac OS X の IC カード対応は先の見通しが立たない状況である．そのため大学の情報部門として公式に Mac OS X による IC カード認証をサポートすることは，大きな困難を伴うことを認識する必要がある．

4.2 Safari の個人証明書の扱い

Mac OS X では個人証明書は，その格納されている媒体（IC カード，ファイルなど）に依らず，すべてキーチェーンアクセスというアプリケーションによって管理される．Safari には，キーチェーンアクセスに 1 つの個人証明書が登録されている状態で個人証明書による認証が要求される Web サイトにアクセスした場合に，送信する個人証明書をユーザに確認することなくキーチェーンアクセスに登録されている個人証明書を送ってしまうというバグが存在する．

問題は，ユーザが知らないうちにキーチェーンアクセスに個人証明書が登録されてしまうということである．Mac OS X には 10.6.6 から Mac App Store というオンラインのアプリケーションストアの機能が OS に追加された．Mac OS X 10.7 以降は OS アップグレードを Mac App Store 経由で行う形式に変わったため，多くのユーザが Mac App Store を利用している．Mac App Store に初めてログインすると Apple Application Integration Certification Authority[3] が発行した個人証明書がキーチェーンアクセスに自動的に登録されてしまう．

その結果，ユーザが個人証明書による認証が必要な Web サイトにアクセスした際には，ユーザが知らないうちに Apple の認証局による個人証明書がサーバに送信され，Web サーバは接続を許可する認証局でないため SSL セッションを切断する，という問題が発生する．本学のユーザ認証システムは，(1) 最初に個人証明書による認証が可能か試し，(2) 不可能な場合はユーザ名とパスワードによる認証を行う，という設計になっている．しかし (1) の段階で SSL セッションが切断されてしまうため，(2) へのフォールバックが機能しない．このためユーザ認証システム稼働当初，Mac OS X 利用者が認証に失敗するというトラブルが頻繁に発生した．

本問題の原因は，Apple の認証局が発行した個人証明書がユーザの意志によらず勝手に送信されてしまうことである．そこで，本学と Apple どちらの認証局が発行した個人証明書も接続を受けつけるように，ユーザ認証システムの Web サーバの設定を変更した．その上で，Apple の認証局が発行した個人証明書による接続だった場合には，個人証明書による認証を要求しない（最初からユーザ名とパスワードによる認証画面が表示される）URL に利用者をリダイレクトさせる．以上のように設定することで，大学認証局が発行した正規の個人証明書による認証を実現しながら，同時に，Safari のバグによって不正な個人証明書で認証を求めてくる場合の対策を実現することができた．

5. 利用状況

5.1 プリペイドシステム

2014 年度（2014 年 4 月 ～ 2015 年 3 月）のプリペイドシステムの利用状況を図 1 に示す．1 年間で延べ 40 万人がプリペイド決済を行った．本学の構成員は学生教職員を併せて約 2,600 人であることから，プリペイド決済が利用者に定着しており習慣的に利用されていることがわかる．

図 2 に，各サービス（食堂，喫茶，売店）ごとのプリペイド決済の利用割合を示す．食堂と売店では約 80%と高い

[*4] Mac 用として納入業者から提供されたドライバは Firefox 用のものであった．Firefox は IC カードの取り扱い方法が OS に依らず共通であり，Linux 用ドライバとも多くのコードを共有できることからこのような対応になったのであろう．

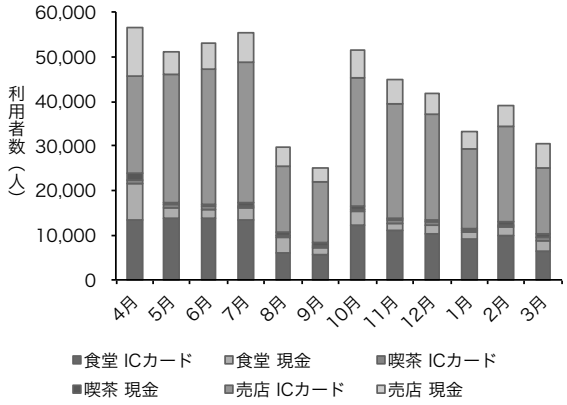

図 1 2014 年度のプリペイドシステム利用者数

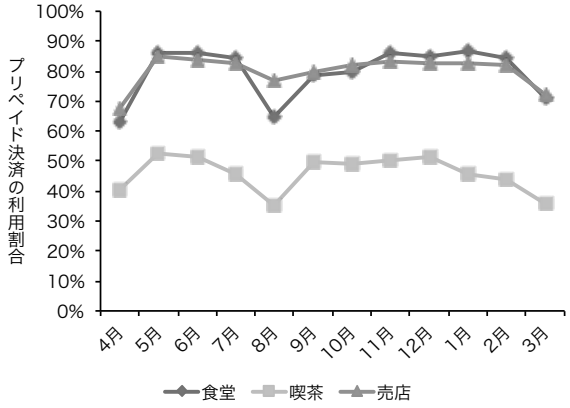

図 2 サービス毎のプリペイド決済の利用割合

利用率を示しており，利用率の観点からもプリペイド決済が大学生活に定着していることが確認できる．喫茶の利用率が他と比べて低いのは，（IC カードを持たない）学外の利用者が多いためと推測される．

プリペイドシステム導入の副次的な効果として，食堂における昼食時間帯の混雑解消がある．これまで食堂では，昼食時間帯に利用者が集中することから，料金支払い時の混雑が問題となっていた．プリペイドシステムの導入により多くの利用者がプリペイド決済を利用するようになったため，一人当たりの決済時間が短縮され混雑が緩和された．

5.2 出席管理システム

2014 年度前期が終わった時点で，出席管理システムの利用状況について教員にアンケートを行った．アンケートの結果，講義において出席管理システムを利用して受講生の出席状況を管理した講義は，全体の 70%であることがわかった．

アンケートで得られたポジティブな感想について次に挙げる．

- 出席を取る必要がないので，利便性・授業効率が向上した
- 欠席の多い問題がありそうな学生の発見が容易になった
- 研究室の指導学生や担任となっている学生の状況が見られるのが良い
- 成績表と一緒に出席状況を保護者に送付すると良いのでは
- 災害発生時の学生の所在把握に使えるのでは
- 出席記録が残る，時間を守るということから，学生に良いストレスを与えている

次にアンケートで得られたネガティブな感想について次に挙げる．

- 退室の記録を取っていない（入室時のみ）ので，講義の最後までちゃんといたのかチェックできない．そのため参考程度の記録にしか使えない
- 2 コマ連続の授業の場合，2 コマ目開始時にもう一度学生証をかざす必要があり不便である
- 出席点を評価の対象としない場合手間が増えるだけである．全授業で使う必要はない
- 学生が学生証を忘れてきた場合に，教員による操作が必要となり不便である

IC カードを用いた出席管理システムの導入によって，教員の出席管理の手間が軽減された一方で，システム導入時に想定されていなかった利用形態があることがわかった．ますますの出席管理の効率化を図るためにも，システムのさらなる改修が必要である．

5.3 問題点

以下，本事例において問題となっている点について述べる．

今回のユーザ認証基盤システムでは，人間を区別する，という立場で設計を行った．技科大においては，学部学生の大部分 (90%以上) が修士学生に進学するという事情があり，情報システムの利用において学部学生と修士学生で，アカウント名やパスワードが変更になることは望ましくない．そのため，ある学生 *A* 君が，学部から修士に進学した場合，学生証においては，

- 学籍番号は変化しない．
- 再発行回数が 1 つ増える．
- 所属情報や身分情報は変わる．

というような変更内容となり，基本的には再発行回数が変化することにより，旧学生証と新学生証を見分けるという実装となっている．しかし，学生証には利用期限があるため，留年などがあると，これも再発行が必要である．最大では，学部入学から博士修了までの期間において，9 回の留年と 9 回の休学があり得るため再発行回数が 18 回に達する可能性がある．しかし，磁気ストライプでは，再発行回数の記録用として数字 1 桁しか利用できないため，オーバーフローの可能性がある．やむを得ず，再発行回数が 10 回に達した場合には，再発行回数を 0 にリセットするようにシステムを設計した．しかし，学籍番号と再発行回数を

組み合わせた全体がカードを区別する番号相当であると考えれば，これは番号の再利用にあたるため，好ましい設計ではない．現在は，第 1 に旧学生証は回収されることが原則であり，第 2 に番号の再利用が発生するには数年以上の期間があること，の 2 点より実際上の問題は発生していない．

先に述べた通り，研究費管理システムを利用する場合には，個人証明書を必要とする設計とし，個人証明書は接触型 IC チップに格納した．しかし，学術振興会特別研究員 (DC) に採用された博士課程の学生は，Felica のみの学生証を持っており，接触型 IC チップを持っていない．そのため，DC は，個人に配分された研究費があるにも関わらず，研究費管理システムを利用できない状態となっており，大きな問題となっている．

6. おわりに

本稿では，豊橋技術科学大学において身分証を IC カード化した事例について報告した．今後は，この IC カード化によって実現された多要素認証基盤を用いて，学内情報システムをより改善していく計画である．

参考文献

[1] Ludovic Rousseau, S. G.: SmartCard Services, http://smartcardservices.macosforge.org. [確認日 2015 年 4 月 15 日].
[2] Apple: What's New in OS X – OS X Yosemite v10.10, https://developer.apple.com/library/prerelease/mac/releasenotes/MacOSX/WhatsNewInOSX/Articles/MacOSX10_10.html. [確認日 2015 年 4 月 15 日].
[3] Apple: Apple PKI, https://www.apple.com/certificateauthority/. [確認日 2015 年 4 月 15 日].