IC カードと電子証明書について 7 年間運用の考察と将来の選択肢

永井靖浩，古村隆明，針木 剛，西垣昌代

京都大学 情報環境機構

Nagai.yasuhiro.6a@kyoto-u.ac.jp

Consideration for 7-years operation of the IC card and electronic certificate, and their future choices

Yasuhiro Nagai, Takaaki Komura, Tsuyoshi Hariki, Masayo Nishigaki

Institute for Information Management and Communication, Kyoto Univ.

概要

京都大学では 2010 年度から統合認証基盤の本格運用を開始した．この際，全学アカウントに加えて,IC カードや電子証明書および必要なプライベート認証局のサービスも開始した．約 7 年経過し，様々な課題も明らかになったので報告する．また，将来の選択肢についても議論する．

1 はじめに

2005 年度末に情報基盤担当理事のもと，個人認証システム検討委員会が設置され，全学の統合認証基盤の検討を開始した.2009 年度に統合 LDAP のサービスを開始し，2010 年 2 月に全学の学生および教職員へ IC カード配付を開始した．この際，教職員の IC カードには電子証明書を埋め込んで提供している．

2010 年度からこれらの統合認証基盤を使った本格的なサービスを提供している．本稿では，約 7 年間運用してきた IC カードや電子証明書を中心に，サービスの経過や課題と対策について述べる．

IC カードや電子証明書の運用は，利便性，業務効率および情報セキュリティの観点から，将来も必要となるが，その選択肢についても議論する．

2　システムと運用の設計と事前準備

2.1 システムと運用の設計

基本設計は，個人認証システム検討委員会の作業部会で行い,部局長会議などへ提案を行う形で進めた．技術面は，2006 年度から情報環境機構内の認証タスクフォースあるいは認証システム運用委員会で議論した.

IC カードについて，交通系で実績があり価格も比較的安くなるとの期待から FeliCa カードをベースとしそのフォーマットは将来の他大学との連携サービスも考慮し FeliCa-Common use Format(FCF)を採用した．また，既存の施設では磁気ストライプが利用されていたため,裏面に磁気ストライプを付けている.カードメニューは,学生カード(学生証)，教職員は常勤(職員証)カードと非常勤(認証 IC カード)カード，鍵代わりに使う施設利用証とした(図 1 参照のこと)．常勤(職員証)カードと非常勤(認証 IC カード)カードは,セキュリティの高い Web サービスを扱うために,接触型チップを埋め込んだハイブリッド IC カードを採用した.

学生(正規生)の場合,4 月期に約 7,000 名が入学するため，職員の稼働軽減の観点から外注とし，紛失などの再発行は内製とした.一方,教職員の場合，毎月転出・転入があることから，すべて内製扱いとし，非常勤職員の雇用期間が短いことにも配意し，状態の良好なカードは ID シートによるリユースを実施し，カード購入コストを抑制した．教職員および学生の再発行コストについては,教育的指導が必要との観点から有償とした.

電子証明書の発行は，市販の電子証明書はパブリックで S/MIME などにも使えるが高価であること，一旦電子証明書サービスを開始すると 10-20 年間の利用が見込まれることから,京都大学プライベート認証局を構築することとした.

常勤(職員証)カードと非常勤(認証 IC カード)カードの電子証明書の有効期限はそれぞれ,2020 年 3 月末および発行より約 5 年後と設定した．なお，認証局の CP/CPS は京都大学電子認証局証明書ポリシーおよび運用規則[1]として公開した.

常勤教職員　　非常勤教職員　　学生(正規生)

券種＼機能	券面(写真付)	磁気ストライプ	電子的ID格納	電子マネー	電子証明書
職員証(常勤)	○	○	○	○	○
学生証(正規生)	○	○	○	○	－
認証ICカード(非常勤)	○	○	○	○	○
施設利用証(その他)	△	○	○	－	－

図 1　IC カードの種類と機能

IC カード認証で教職員の多くが Personal Identity Number (PIN)を忘れることが危惧され，この対策としてリモートでの PIN 再設定方式を採用し，問い合わせ稼働の軽減を図った．また，PKI ドライバのブラウザ対応について，Windows は問題ないが,Mac ブラウザには対応していないため，Firefox にて対応してもらうこととした．

2.2 事前準備

2010 年 2 月より在籍する学生，教職員に対して配付を開始し，以降，2010 年度末までに約 1 万 1 千名の教職員(常勤約6,500名，非常勤約4,500名)の職員証・認証 IC カードおよび約 2 万 3 千名の学生証を配付した．なお，教職員に対しては部局経由でリーダライタおよびドライバインストール用 CD を配っている．

教職員を対象とした電子証明書の運用や IC カード発行には，体制と必要な職員を配置する必要があることから，2009 年度から統合認証センター(2015 年度から新設の情報環境支援センターに巻き取った)を設置し，IC カードや電子証明書などの運用および問い合わせ受付・管理を行った．頻繁な問い合わせに対しては FAQ を充実させている．

教職員の IC カード利用については，電子証明書による本人認証に使うため，その意味や PKI ドライバなどのインストール説明会を 2009 年末に 7 回実施し，約 10%の教職員が受講した．この説明会の意義は，構成員に対して情報セキュリティの重要性を認識してもらうようになったことが大きかったと考えている．

また，教職員および学生の IC カードにはキラーサービスとして生協の電子マネーを搭載し，その技術的な検証やカードの券面やメモリー領域の貸与契約も行った．

教職員による IC カード認証では，PKI ドライバのインストール不具合が予見されたため，IC カードの電子証明書にアクセスできるか否かを自己チェックするサイトも準備した．

3 本格運用でのサービスと経過

統合認証基盤の本格運用に際して，全学アカウント，全学メール，IC カードが教職員および学生向けのサービスである．他にも，Shibboleth 認証連携サービス提供，学生向けのシングルサインオン型ポータルサービスがある．ここでは，IC カードと電子証明書を使ったサービスの経過と問い合わせの推移について述べる．

3.1 提供サービスとその経過

できるだけ多くの構成員が IC カードのサービスを享受することに配意し，下記のようなサービスからスタートした．

- 共通サービス：電子マネー(生協組合員)，物理的セキュリティ(入退管理)，図書サービス(貸し出しなど)，会議や授業の出席などID読み取り，共有PCのログイン制限など
- 学生サービス：証明書自動発行
- 教職員サービス：ICカード認証，セキュアな印刷とコピー

IC カード認証として， 2010 年度から人事給与システムの給与明細閲覧，人事シート，年末調整および財務会計システム(2011 年度開始)のログインに利用された．また，2013 年 1 月から諸手当現況調査にも利用された．

一方，2012 年度より常勤教職員の IC カード(職員証)が廃止され，認証 IC カードに一本化された．これに伴い，在職証明書の発行サービスが新たにリリースされ，IC カード認証が必要になった．

注目すべき動きとして，給与明細閲覧には IC カード認証が必要であったが，IC カード認証が煩雑で，紙の給与明細を大幅に低減させる施策にブレーキをかけているという議論があり，賛否はあったものの給与明細閲覧(年末調整も同様の Web システムであったので同じ扱い)の IC カード認証は 2013 年度から ID&パスワード方式に戻された．

本件は，情報セキュリティより施策に必要な利便性を優先した形となったが，時代に逆行した対応である．認証サービスを提供する立場の反省点は，ID&パスワード方式と PKI 方式の中間に位置する より簡便な多要素認証を準備しておくべきであった．

3.2 ブラウザ，OS などドライバの対応経過

2010 年 2 月の IC カード配付の際，リーダライタ，PKI ドライバおよび中間・ルート証明書が格納された CD を教職員に配付した．Web サーバからのダウンロードも検討したが，教職員のリテラシーレベルにバラツキが大きいことに配意し CD 配付とした．現在は Web からダウンロードしている．

当初，対応 OS として，Windows XP/Vista で IE6-8，Firefox2-3 系，Mac OSX で 10.4.x の Firefox2-3 系でスタートした．その後，Windows7-10 の変遷，Mac OSX Tiger-mac OS Sierra の変遷，IE ブラウザのバージョンアップなど頻繁に起こったため，その都度，職員による動作検証を実施した．特に，32bits 版から 64bits 版マシーンへの変更時は慎重な検証を余儀なくされ，アナウンスを強化した．また，Windows10 で採用された edge ブラウザは対応できていない．リーダライタについては現在，接触型であるために Windows および Mac ともに 標準ドライバが搭載されている．

従来の国産 IC チップが製造中止となり，2014 年度から代替の JAVA チップに変更となったが，PKI アプレットなどの変更は無かったため，構成員には影響がでなかった．

今後，OS やブラウザのバージョンアップが継続的に発生すると考えられ，抜本的な対応が必要である．また，IC チップ変更などの影響を抑制する対策も必要である．

3.3 教職員 IC カードの発行枚数とトラブル

教職員 IC カードの月別発行枚数の年次推移を図 2 に示す．2011 年 11 月の急増(約 560 枚)は財務会計システムを利用する学振特別研究員などへの対応であり，2014 年 1 月の急増(約 650 枚)は，2010 年度に配付した電子証明書の 5 年目の更新時期に伴う対応である．この際，注意喚起なしに証明書が失効したために，非常勤職員へ多大な迷惑をかけた．

上記の異常な急増を赤で示した 2010-2015 年度の発行枚数の年次推移を図 3 に示す．2010 年度から 2012 年度まで増えているが，赤い部分を除くと 2012 年度から約 3500 枚で定常となっている．構成員 11,000 名に対して，30%程度のカード発行が必要であることがわかる．

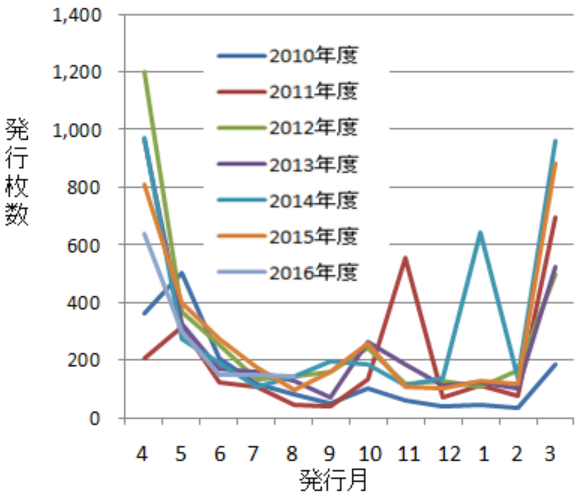

図 2　IC カード毎月発行枚数の年次推移

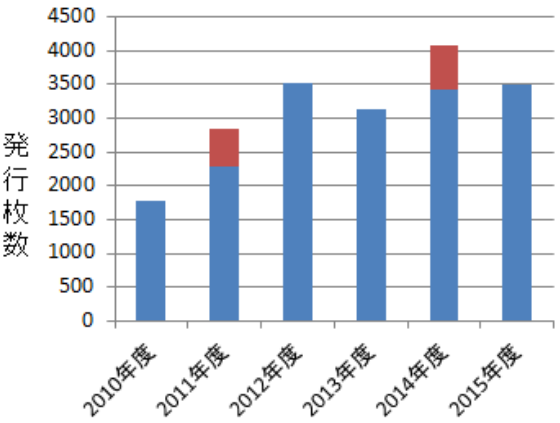

図 3　IC カード発行枚数の年次推移

このような IC カード(電子証明書)の更新時期は分散させることが望ましいが，常勤教職員の更新となる 2020 年 3 月末は同様に発行ピークを迎える．その対策として，常勤教職員に対しても有効期限を非常勤職員と同様に発行より約 5 年間に変更し，これに伴い京都大学電子認証局証明書ポリシー及び運用規則(CP/CPS)を 2015 年 2 月に改訂した．2020 年度末に向けて発行の稼働を平準化するため，有効期限前で更新するなど具体的なアクションが今後必要となる．

3.4 問い合わせの推移

統合認証センタ(現 情報環境支援センタ)では 2010 年度から問い合わせのデータを蓄積している．このデータは Web 問い合わせを集計したものであり，電話での問い合わせを加えるとほぼ 2 倍となる．

2010-2012 年の問い合わせ件数の推移を図 4 に示す．問い合わせ件数の増加は，人事給与閲覧や財務会計のように 最初に IC カード認証を開始した時点，人事シートや年末調整のイベント時点と全く対応しているため，この問い合わせ件数の変化(数値)はイベントや障害などの KPI(Key Performance Indicator)と考えることができる．

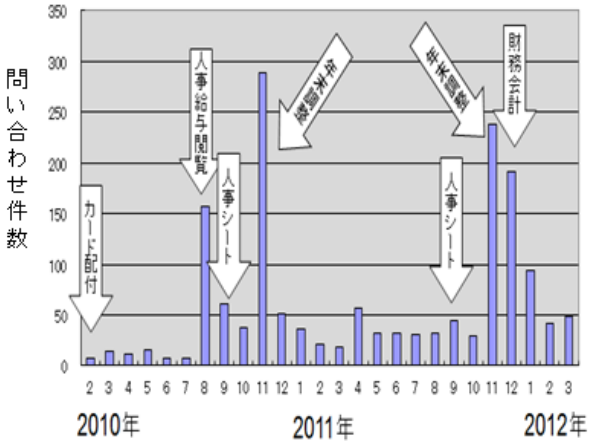

図 4　2010-2011 年の問い合わせ件数の推移

問い合わせ件数とその内容の変化を図 5 に示す．2010-2012 年度に件数が多いのは，給与明細閲覧や年末調整が対象となっていたためであり，その質問の多くは PIN 忘れや再設定であり，年々増えている．一方，2013 年度以降は給与明細閲覧や年末調整が対象外となったため，問い合わせ全体は急減し，PIN や再設定に比べ，PKI ドライバなどのインストールや操作方法の問い合わせが増えている．これは OS やブラウザなどのバージョンアップに呼応しているものと考えている．一方で PIN 忘れはほぼ一定となっていることから，利用が定着していると考えられる．

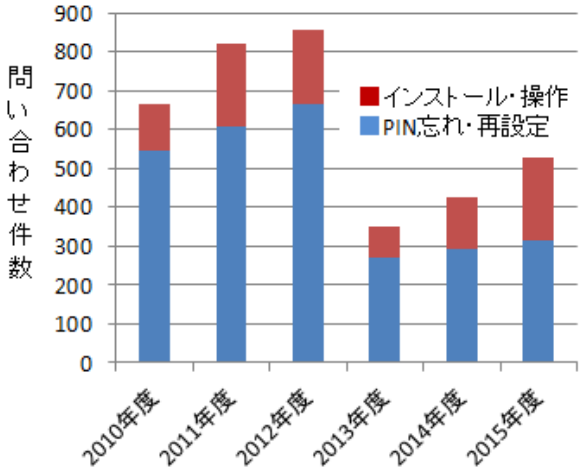

図 5　問い合わせ数の内容の変化

4 課題と対策

ここでは 7 年間の運用で課題となった事項とその対策について考察する．

4.1 OS やブラウザの更新と利用者負担

Windows，Mac も含め OS やブラウザの更新が頻繁に起こる．もちろん動作検証した上でバージョンアップをアナウンスするものの，利用者に負担を強いている．特に，Mac ではブラウザに Firefox を指定しているため，インストール・トラブルが非常に多い．このような観点から，様々な OS やブラウザに対応している PKI ドライバを採用することが望ましい．反面，大学独自のドライバを開発すると非常に高いメンテナンスコストが発生する．一つの方法は，マイナンバーカードで使われている PKI ドライバを採用することである．しかし，後述するように問題が多く残っている．

また別の視点から，クライアント PC に PKI ドライバをインストールするのではなく，PC にアプリをインストールして，OS やブラウザの問題を回避させる方法も最近出てきたが，まだ大規模な実運用としては実績が乏しい．これらについては，将来の選択肢として再度議論する．

4.2 利便性・情報セキュリティと多要素認証

今後，ID&パスワード方式だけの認証では不十分である．IC カード認証は堅牢な多要素認証の一つであるが，今回の運用で，利便性を優先させ ID とパスワード方式に戻すという事例が発生した．情報セキュリティは一般には全てに優先されるため，このような対応は稀であるが，より簡便で利便性に優れた別の多要素認証を準備しておくべきだったと考えている．具体的には，Matrix コード認証やインターネットバンキングで多用されつつあるワンタイムパスワードがその候補である．

4.3 電子証明書の有効期限と稼働平準化

常勤は比較的雇用が長く，非常勤は相対的に短いとの意識から，常勤の電子証明書を 2020 年 3 月末までとし，非常勤の電子証明書を発行から約 5 年としてスタートした．運用してみて，5 年，10 年単位で再発行のピークが来るという問題が顕在化した．対策としては，全ての電子証明書の有効期限を発行から約 5 年とし，稼働を平準化する準備は 2015 年末に完了したが，まだ 2020 年度末のピークを回避する目途は立っていない．

また，本人認証で使う電子証明書については，サーバ証明書と異なり，10-20 年といった長期安定供給の担保が必要であり，本人認証に使う電子証明書には最低 5 年間の有効期限が必要と考える．

5 将来に向けた選択肢について

現在運用している IC カード，電子証明書および電子認証局の運用については，基本的に継続する．一方で，明らかになった課題も意識している．ここでは将来の別の選択肢について，その長所・短所を議論する．

5.1 NII 電子証明書のダウンロードでの利用

著者らは，日本情報経済社会推進協会が開発した JCAN パス(電子証明書)と FCF カードを利用した証明書ダウンロード・アプリケーション[2]を試した．この方式のイメージを図 6 に示す．

電子証明書を IC カードに格納するのではなく，IC カードでアプリケーションを起動させ，電子証明書を一時的にクライアント PC へダウンロードして本人認証などに利用する．

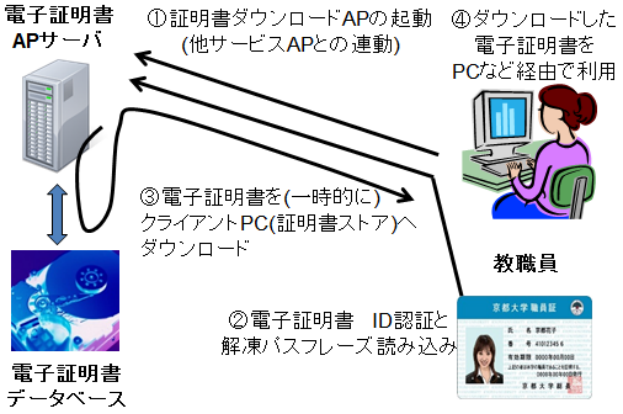

図 6　証明書ダウンロード・アプリケーション
イメージ

基本的な動きは次のとおりである．

(1) 構成員の電子証明書を予め発行・取得しデータベースに格納しておく．

(2) クライアント PC には IC カードからキー情報を読み出すリーダライタとアプリケーションをダウンロードしておく(このアプリケーションは OS やブラウザ依存が無いことが前提)．

(3) IC カードを使ってセキュアにアプリケーションを起動させ，一時的に電子証明書をクライアント PC にダウンロードさせて利用する．

(4) 操作が終了すれば，当該の電子証明書は PC から消去される．

メリットは以下のとおりである．

・IC カードと電子証明書を別に扱うことが可能
・容量の少ないメモリーカードでも利用可能
・電子証明書の個人毎の更新や配付が不要

この方式を国立情報学研究所(NII)がトレースして，よりセキュアな状態で提供しようとしている[3,4]．また，クライアント電子証明書はサーバ証明書と同様のスキームで配付できる．

現在，NII が提供するクライアント電子証明書は 5 年より短いが，IC カードに格納しない前提であれば，有望な選択肢である．

5.2 マイナンバーカードの利用

マイナンバーカード[5]にも署名用電子証明書と個人認証用電子証明書が格納されている．この個人認証用電子証明書は，学内のログインカードとして使える．最も大きなメリットは，PKI ドラ

イバのメンテナンスを総務省にお願いできることである．カードコストも現在無償なので学生・教職員に対しても適用できる．

この方式のデメリットは以下のとおりである．

・券面の自由度がない(シール/ケースでの対応)
・全ての構成員がマイナンバーカードを持つことが前提となる
・現在利用している FeliCa サービスの施設リーダライタ交換，電子マネーなどアプレット改修

以上のように，現状では切り替えに伴うコスト負担や運用切り替えのハードルが高いため採用は困難であるが，今後魅力ある選択肢の一つである．特に，新規に導入する大学にとってはハードルが低い．

6 まとめ

2010 年度から本格運用を始めた統合認証基盤，特に IC カードと電子証明書について，システムや運用の設計や準備段階に実施したこと，約 7 年間の本格運用で発生した事象，蓄積された技術や運用ノウハウについても明らかにした．

これまでの運用で明確になった課題とその対策についても考察した．最後に，大学における IC カードや電子証明書の将来の選択肢についても議論した．

本稿が他大学にとって有益となれば幸いである．

参考文献

[1] 京都大学電子認証局証明書ポリシーおよび運用規則：
http://www.iimc.kyoto-u.ac.jp/services/cert/cp_cps02102015.pdf

[2] 永井，古村，”JIPDEC インタビュー:JCAN パスを実証実験!!”，
http://jcan.jipdec.or.jp/interview/kyoto-u.html

[3] 中村，”UPKI パスについて”，
https://www.nii.ac.jp/csi/openforum2016/track/pdf/20160526PM_G_09_nakamura.pdf

[4] 中村，”JIPDEC インタビュー：大学から広げるクライアント証明書活用の取り組み”，
https://jcan.jipdec.or.jp/interview/nii.html

[5] マイナンバーカード総合サイト：
https://www.kojinbango-card.go.jp/kojinbango/merit.html