IC カード職員証・学生証の導入

内藤久資　久保　仁
平野　靖　葛生和人

はじめに

名古屋大学では2007年12月に，職員証がICカード化されました。また，2008年4月からは学年進行で，学生証もICカード化されることとなっています。この職員証・学生証のICカード化では，情報連携統括本部が技術的なサポートを行いました。

近年「ICカード」という言葉を耳にする機会があった方も少なくないと思われます。JR東日本の「Suica」に代表される交通系ICカード，「Edy」に代表される電子マネーなどだけではなく，クレジットカード，銀行のキャッシュカードなどもICカードを利用していることが少なくありません。また，最近では各大学の学生証がICカード化されたという話も多く耳にします。（名古屋近郊では，名古屋工業大学での事例紹介が［1］に，岐阜大学での事例紹介が［2］に掲載されています。）このように我々の身の回りには，意外に多くのICカードが氾濫し，「ICカードを利用するとよいことがいっぱいある」といった，悪く言ってしまえば訳の分からない喧伝も決して少なくありません。

本稿では，名古屋大学でのICカード職員証・学生証の導入事例の紹介を行ない，ICカード職員証・学生証を使うと，現時点で何ができて，何ができないのかを解説します。また，ICカード職員証・学生証を使った情報基盤の将来像についての解説も行います。

Ⅰ．ICカードとは

「ICカード」とは，一般には，キャッシュカード大のプラスッチックカード内にCPU，メモリ等を搭載し，カード内に種々の情報を蓄積・利用するためのカードを指します[1]。ICカードの主目的は，その内部の情報を蓄積でき，適切な読み取り装置を用いることで，カード内部の情報を読み取り（場合によっては更新を行って）サービスに供することにあります。

例えば，「電子マネー」の例で言えば，ICカード内部には「電子マネーの残額」が記録され，電子マネー支払いの際には，適切な暗号プロトコルの下で残額の書き換えを行っています。また，キャッシュカードなどでは，ICカード内部に「所有者本人であることを保証する電子証明書」が格納され，例えば「生体認証情報」を電子証明書の鍵として用いることで，ICカード内部で鍵演算を行い，電子証明書情報のみをサーバに送信することで本人確認を行うことが行われ

1　広い意味では「RFID」と呼ばれる小さな「ICチップ」を利用したものを含む場合もあります。

ています[2]。

このように，IC カードの一つの目的は，小さなカード内に「本人性を保証する情報」に代表される種々の情報を保存し，情報ネットワークの中での「認証」の方法として利用することが挙げられます。

一方，物理媒体としての IC カードを見たときには，単純には以下の 2 つの分類があります。

★接触型 IC カード

カード読み取り機に挿入して，カード券面上にある「端子」を通じてデータ交換を行う IC カード。

★非接触型 IC カード

カード内部にアンテナを持ち，読み取り機側からの信号に反応して無線通信を利用したデータ交換を行う IC カード。

接触型 IC カードは，現在流通しているカードのほとんどが統一規格[3] となっています。一方，非接触型 IC カードは，その規格の違いにより，3 種類に分類されています。また，1 枚のカードに接触・非接触の 2 つの IC チップを組み込んだ「Hybrid カード」，1 つの IC チップに対して接触でも非接触でもアクセス可能な「Dual カード」などもあります。現在，日本国内で広く流通している各種 IC カードは，上記の方法で分類すると以下のようになります[4, 5]。

★接触型 IC カード　銀行系キャッシュカード・クレジットカードなど。

★非接触型 IC カード

- **▼ Type A**　NTT 公衆電話 IC カード
- **▼ Type B**　住民基本台帳カード
- **▼ Felica**　交通系カード（Suica など），電子マネーカード（Edy など），携帯電話に組み込まれた IC カード

Ⅱ．名古屋大学が導入した IC カード

名古屋大学が職員証・学生証として導入した IC カードは以下の仕様のものです。

★ IC カード種別　接触・非接触 Dual カード，NTT-Communications 社製 eLWISE

★非接触インタフェース仕様　Type B

★内蔵メモリ量　1MB

★暗号化機能　公開鍵暗号：RSA1024 共通鍵暗号：TDES（2Key，3Key）

★カードオペレーティングシステム　Native（独自）OS，Java VM

★初期搭載カードアプリケーション

2　「安全なフレームワーク」の下では，鍵である「生体認証情報」はカード内部で処理され，外部へは送信されていません。

3　接触型カードの標準規格は JIS 6300−X，ISO/IEC 7816 で定義されています。

4　“Felica” は SONY の登録商標です。また，Type A，Type B については ISO/IEC14443 において標準化されています。

5　欧米では，Type A を利用した電子マネー・交通系カードなども広く利用されているようです。

・カード固有 ID（“.com-ID”）
・入退館アプリケーション（OMRON 入退館管理装置に対応）

なお，入退館アプリケーションについては，OMRON 入退館管理装置以外でも利用できる場合があります。

Ⅲ．この IC カードでできること

今回導入した IC カード職員証・学生証を使って何が可能かを紹介します。

★入退館管理

建物・部屋などの入退出ゲートに利用できます。IC カードには OMRON 社製の入退館装置用のカードアプリケーションが搭載されていますので，OMRON 社製及びそれと互換性のある入退館管理装置，及びカード読み取り装置として Type B 対応のものを利用する必要があります[6]。

IC カードに書き込まれた，入退館装置用のカードアプリケーション内には，カード所有者の名古屋大学 ID が書き込まれています。したがって，IC カードを読み取り装置にかざすことにより，読み取り装置からは名古屋大学 ID が返されますので，データベースとして，入館許可者の名古屋大学 ID リストを用意することが必要となります[7]。

★コピー機のコピーカードとして利用する

いくつかのメーカのコピー機には，コピーカード読み取り装置として Type B 対応のものがあります。これを利用すれば IC カード職員証・学生証をコピーカードとして利用可能ですが，詳細はコピー機のメーカにお問い合わせ頂くのがよいと考えています。

★ Windows/Mac スマートカードログイン

Windows 及び Mac に Type B 対応の非接触カード読み取り装置，または接触型のカード読み取り装置を装着し，PC 内またはサーバに格納されたカード固有 ID のデータベース内に一致するカードが挿入されたときに限り，PC の利用を許可することができます。この場合には，Windows 及び Mac いずれの場合にも，スマートカードログイン用のアプリケーションをインストールする必要があります（cf. [11，12]）。

なお，一般に Type B または接触型 IC カードリーダを利用して，カード固有 ID を読み取ることが可能であれば他の用途にも利用可能です。カード固有 ID は，職員証・学生証発行時にカードに電子的に記録され，情報連携統括本部が管理しています。

Ⅳ．IC カード職員証・学生証の発行

IC カード職員証・学生証の発行責任は，職員証については総務部人事労務課，学生証については，学務部学務企画課にあります。情報連携統括本部は，IC カード職員証・学生証発行に係

6　今回導入した IC カードを利用した入退館管理は，名古屋大学赤崎記念館で実際に行なわれています。
7　旧来の職員証・学生証で利用されていたものと同一の磁気ストライプも搭載されています。磁気ストライプ内に記録されている情報は，職員番号・学生番号です。

わる技術支援を行っています。IC カード職員証・学生証の発行に際して，情報連携統括本部がどのように関わったのかを解説し，それらの発行手順を説明します。

1．職員証の発行に際して

今回，IC カード職員証を作成するにあたり，名古屋大学 ID 情報の整備を兼ねて職員証発行対象者の氏名情報の再確認を行いました。職員証発行対象者の基本情報は，総務部人事労務課が管理する「人事データベース」を基礎としています。しかしながら，人事データベースに掲載されている情報は，以下の意味で不備があることが分かりました。

・人事データベース内に格納されている「氏名（漢字表記）」は，CP−932 と呼ばれる，JIS 旧第 2 水準に IBM 拡張文字を含んだ文字セットで記述されている。

・人事データベース内には「氏名のアルファベット表記」は格納されていない。

職員証は「身分証明証」ですから，「可能な限り」正しい氏名（漢字）表記を印字するべきであると考えました[8]。また，職員証の券面に氏名のアルファベット表記を印字すべきとの議論がありました。情報連携統括本部は，これらの要求に答えるため，人事データベースを基礎とした上で，職員証発行対象者本人に，氏名の漢字及びアルファベット表記を確認して頂くこととしました。

また，旧職員証では，写真添付が義務付けられていませんでしたが，新職員証では写真添付が義務付けられたため，本人の写真を収集するために，「写真アップロードアプリケーション[9]」の作成と利用だけでなく，「写真撮影会[10]」の開催を行い，職員証写真の収集を行いました。

なお，職員証の氏名表記確認で収集した氏名表記データに関しては，名古屋大学 ID の氏名フィールドに格納し，そのアルファベット表記は，2008 年 1 月の全学メールサービスのアドレス表記に利用しました（cf. [6]）一方，職員証用写真に関しては，種々の議論がありましたが，職員証に添付することのみを目的に収集した経緯がありましたので，名古屋大学 ID データベースに格納することは行っていません。

なお，新規職員採用時には，写真の提出をお願いし，氏名データの確認の後に，情報推進部情報推進課に設置された IC カード発行機を利用して，名古屋大学内において随時発行を行うこととなります。

2．学生証の発行

IC カード学生証は 2008 年 4 月入学生から，学年進行で発行することとなっています。したがって，全学生に IC カード学生証が行き渡るには，4 年から 6 年が必要となります。従来，学

8　実際に利用可能な「漢字」の文字の範囲は，技術的理由により，Unicode 3.2 で定義されている文字となります。通常の Shift JIS の範囲では収録されておらず，CP−932 に収録されている文字の代表例としては「ハシゴ高」が，また，CP−932 に範囲では収録されておらず，Unicode 3.2 に収録されている文字の代表例としては「つち吉」があります。

9　情報連携統括本部情報戦略室が作成しました。

10　情報企画課主催で行われました。

生証には氏名のアルファベット表記は印字されていませんでしたが，新学生証は，海外でも一定の効力を持たせようという議論から，氏名のアルファベット表記等を印字することとなりました。しかし，人事データベースと同様に，学生データベースにも正しいアルファベット表記は格納されていないため，2008 年 4 月入学生からは，入学時に氏名のアルファベット表記を収集することとなりました[11]。なお，毎年 4 月の新入学生への学生証発行は以下の方法で，学内でのデータ作成の後，業者へ委託して行なわれます。

1. 情報推進部情報推進課に設置された IC カード発行機で IC チップへの搭載データを作成，
2. 情報連携統括本部が作成した職員証・学生証券面データ作成ソフトウェアで，学生証の券面画像を作成，
3. これら 2 種類のデータを業者に送付する。

3．職員証・学生証の券面

職員証・学生証の旧来のものとの券面上の大きな違いは以下の通りです。

★種々の英語表記を記載した

氏名・身分・大学名等の英語（アルファベット）表記が追加されました。

★名古屋大学 ID を記載した

職員証・学生証裏面に名古屋大学 ID を印字しました。また，名古屋大学 ID は CODE−128 によるバーコードとしても印字されています。

★職員番号・生年月日の記載をやめた

職員証に関しては，職員番号及び生年月日を明示的には記載することをやめました。学生証に関しては，一般的な身分証明証として利用する機会が多いため，従来通りとなっています。

なお，職員証・学生証の「磁気ストライプ」には従来通りの情報が記録されています。

図 1　職員証券面

11　従来は，卒業時の氏名確認と同時にアルファベット表記の確認を行っていました。

図２　学生証券面

Ⅴ．IC カードを使った情報システムの将来像

ここでは「IC カードを使うとこんなことができる」的なことを考察してみます。ここでは，大きく分けて２種類の利用法を解説します。一つは，IC カードに搭載された「カード固有情報」や「カード内のアプリケーション」を利用した情報システムの利用法であり，もうひとつは，「電子証明書」を利用した，コンピュータネットワークの利用法です。

１．IC カードそのものを利用したシステムの利用

ここでは，カード所有者とカード ID に類する情報をデータベースに格納し，所有者がカードを提示することにより情報システムの利用を可能にする例を解説します。これは，「カード所有者を信頼した認証」と考えることができます。前節では「入退館管理」，「コピーカードとしての利用」などを例に出しましたが，これらも，「カード所有者を信頼して，カード所有者にサービスを提供する」例になっています。ここでは，特に「スマートカードログイン」と呼ばれる，IC カードの利用者のみが PC を利用できる仕組みを元にした，セキュリティの高い PC の利用法について解説します。

近年の Windows Vista や MacOS X では，PC 利用時に「ユーザ ID ＋パスワード」を入力しない限り，PC の利用ができない仕組みを搭載しています[12]。「スマートカードログイン」は，この「ユーザ ID ＋パスワード」の入力の代わりに，IC カードを挿入することが求められ，IC カード内部の「固有 ID」が PC 内のデータベースに登録されている場合に，カード所有者が正当なユーザであると認め，PC の利用が行なえる仕組みです。一般に，「ユーザ ID ＋パスワード」は「知識認証」の例とされ，知識認証は「パスワード」という「知識」が流出すると認証の意味を持たなくなります。一方，「IC カード認証」はカードという物理媒体が介在するため「物理認証」の一部とされます。物理認証では，認証媒体の紛失により認証の意味を持たなくなりますが，通常は，「カードの挿入」だけでなく，該当するユーザのパスワード入力またはカード呼び出しのためのパスワード（暗証番号）の入力を求められます。そのため，「スマートカードログイン」

12　そうでない場合には，特定のユーザに対する「自動ログイン」が行なわれているだけです。

は「物理認証＋知識認証」となり，より安全な認証であると考えられています。

しかしながら，実際の PC 利用の場面では，「スマートカードログイン」は単なる「ユーザ ID ＋パスワード」の代わりに過ぎませんから，PC 内のハードディスクを他の PC から覗き見られたとき（ハードディスクを取り出して，他の PC につないだりした場合）には，IC カードなしに PC 内のデータを参照することが可能となります。この意味で，「スマートカードログイン」は，認証をより強固にしたに過ぎず，データの安全性を十分には保証できるものではないことに注意してください。

一方，近年の PC 上のオペレーティングシステムは「ディスクの暗号化」などの強力なセキュリティ機能を有しています。例えば，MacOS X であれば Version 10.4 以後で利用できる“File Vault”がその代表例です[13]（cf. [8]）。この暗号化機能と「スマートカードログイン」を組み合せることにより，知識認証と物理認証を組み合せた安全な認証システムのもとに，データの暗号化の解除が可能になり，より安全な PC 利用環境を構築できます。

なお，名古屋大学の IC カード職員証・学生証と［11］，［12］などを利用することにより「スマートカードログイン」を実際に利用することが可能です。名古屋大学で「スマートカードログイン」を検討される方は，情報連携統括本部にご相談ください。

2．PKI の利用

IC カードを用いたセキュリティの文脈の中では，PKI（Public Key Infrastructure）と呼ばれるフレームワークが頻繁にあらわれます。ここでは，PKI の仕組みを簡単に説明し，なぜ IC カードと PKI がセットにして語られるのか，PKI を用いるとどのような「ウレシイこと」があるのかについて，簡単に解説を行ないます。なお，PKI の一般的な議論は［13］などをご覧ください。

2.1　PKI の仕組みと IC カード

PKI とは，「公開鍵暗号」を基本にした「電子証明書」の所有者の正当性を与える仕組みで，コンピュータネットワークでは，すでに広く利用され，多くのユーザが知らないうちに利用しています。それは，SSL（Security Socket Layer）と呼ばれる仕組みで，個人情報などの入力を求められるウェブページなどで広く用いられています[14]。SSL は「サーバ証明書」とよばれる電子証明書を利用し，証明書を提示したウェブサーバが「真正」なサーバ[15]であるか否かを，ブラウ

13　MacOS X の File Vault は，ユーザの「ホームフォルダ」を暗号化する機能です。また，Windows Vista では EFS（Encrypting File System）を利用することにより，任意のフォルダあるいはファイルを暗号化することができます。

14　“https”で始まる URL を持ったページへのアクセスで利用されています。

15　ウェブサーバが「真正」であるとは，少なくとも，アクセスしたサーバが「本当に目的の FQDN を持つホストである」ということです。一見当たり前のように思えるのですが，今日のインターネットではさまざまな「詐称」が実行され，「真正」なサーバにアクセスしているかを確認することは極めて重要であると考えられています。

ザが持っている「ルート証明書」を利用して検証する仕組みです。仮に偽りのサーバ証明書[16]を利用したサーバにアクセスすると，証明書の検証に失敗し，ブラウザは「真正なサーバではない」旨を表示してユーザに警告します。その際の証明書の検証過程で「公開鍵（Public Key）暗号」を用いるため，PKI という名前が付けられています。

なお，サーバ証明書の真正性のチェックには以下の方法が用いられます。PC 内のウェブブラウザには，初期インストールされたいくつかの「ルート証明書」が格納されています。各ウェブサーバでのサーバ証明書は，これらのいずれかのルート証明書による電子証明が行なわれ[17]，サーバ証明書を受取ったブラウザは，ルート証明書からの電子署名により，サーバ証明書の真正性を検証することが可能となります（cf. 図 3）。

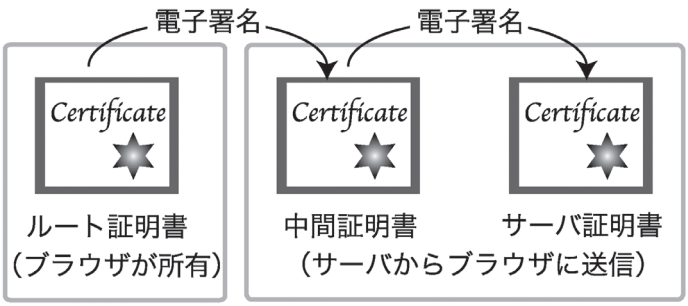

図 3　PKI の証明書チェイン

IC カードを本人性確認の手段として用いる際には，サーバ側ではなくユーザ（クライアント）が電子証明書（クライアント証明書）を提示し，サーバ側が持っているルート証明書を利用して検証を行います。本人の識別名（例えば電子メールアドレス）が記載されたクライアント証明書を，その本人自身のみが利用可能な環境を実現すれば，クライアント証明書を利用した認証は，ユーザ ID とパスワードを利用した認証と同様に，コンピュータネットワーク上の認証として意味を持つことになります。これが PKI の基本的な仕組みです。

では，PKI と IC カードはどのように関わるのでしょうか。PKI では，電子証明書が「間違いなく本人のみが利用できる」ことを前提としています。そのため，「クライアント証明書をどのようにして本人のみに渡すことが可能か？」が問題となります。その際に，身分証明証である IC カードにクライアント証明書を格納することにより，クライアント証明書を正しく本人に渡すことが行われています。

また，一般にクライアント証明書を利用する際には，クライアント証明書発行時に指定した「パスフレーズ」の入力を求められます。これは，暗号化されたクライアント証明書の復号を行うことであり，IC カードを組合せた例では，単なる暗証番号・パスワードの入力だけでなく，

16　偽りでなくても，有効期限の切れた証明書や，ブラウザがルート証明書を持っていない場合も同様です。

17　「中間証明書」が介在する場合もあります。

生体認証が用いられることもあります。特に，IC カード内のクライアント証明書の復号においては，IC カードのチップ内部で計算が行われ，暗証番号や生体認証情報などが IC カード外部に出ないための工夫を行うことも可能です。

2.2 PKI を利用した情報システムのセキュリティ

このように，IC カードを利用することによって PKI による証明書フレームワークの信頼性が向上することが分かりますが，実際に PKI がどのような場面で利用可能かを考えてみましょう。

★ウェブページへのアクセス時の認証

ウェブページへアクセスする際に「ユーザ ID とパスワード」の入力を求められることがあります。「ユーザ ID ＋パスワード」は「知識」をベースにした認証ですから，場合によっては他人がその知識を知りうることが可能です。

この場合に，PKI を利用するとは，ウェブページへのアクセスの際に「クライアント証明書」の提示を求めます。これは，認証の際に「クライアント証明書」（または IC カード）という「物理媒体（電子媒体）」を求めるという意味で，「物理認証」の一種と考えることが可能です。つまり，IC カードがないとウェブページにアクセスできないといういみで，通常のユーザ ID ＋パスワード認証よりも強い認証システムと考えられています[18]。

★電子メールなどの電子署名と暗号化

クライアント証明書は，電子メール，PDF 文書等の電子署名にも利用することが可能です（cf. 図 4）。

電子署名とは，メール，PDF 文書に改竄がないことを保証したり，確かに発信者・作成者本人によって作成されたことを示すものです。

また，電子メールの暗号化にも利用可能です（cf. 図 5）。

このように，PKI を用いると，より高度な認証や署名つき電子メールを利用することが可能になります。これらの仕組みは，今日ではウェブブラウザや電子メールソフトウェアが標準的に対応している場合が多く，適切なクライアント証明書を IC カードと共に配布することにより，情報ネットワークシステムのセキュリティを容易に向上させることが可能です。

このように PKI を用いることにより，情報ネットワークシステムのセキュリティを向上させることが可能です。名古屋大学の例で言えば，学務システムの成績入力ページなど，高度なセキュリティを求められるページへのアクセスにはクライアント証明書を用いた認証を用いることが可能ですし，将来はそうあるべきと考えています[19]

なお，PKI を導入する場合には，パブリック・クライアント証明書を入手するための費用がかかるため，今すぐ導入すべきか否かは議論が必要ですが，大学内の情報システムの安全性を向上

18 通常は，ユーザ ID ＋パスワード認証と組合せて利用します。また，IC カード内の証明書のアクセスに生体認証を組合せたりもします。

19 なお，一般的な「ユーザ ID ＋パスワード」セキュリティでの十分であるページにまで PKI を持ち込むことは望ましくないため，情報連携統括本部では，セキュリティレベルに応じたアクセス制限などの研究も行なっています（cf. [10]）。

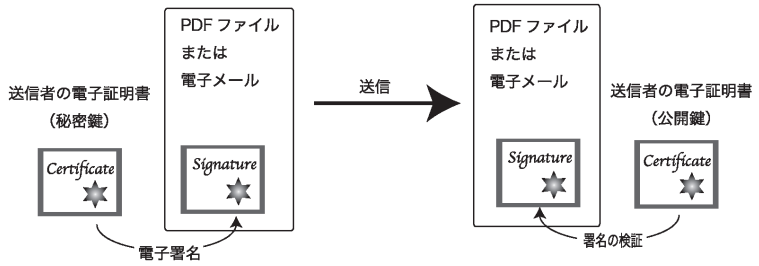

図４　電子署名

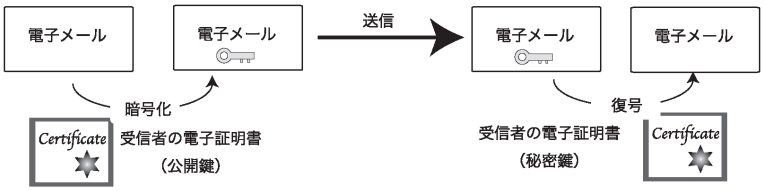

図５　暗号化

したり，大学が発信する文書などの保証を行うためには，将来は必要不可欠なフレームワークとなると考えられます。そのための準備として，情報連携統括本部で今年度には限定的な PKI に関する実験を行なう予定です。

終わりに

本稿では名古屋大学の IC カード職員証・学生証の概要を述べてきました。筆者たちが身分証明証の IC カード化に関わり始めた時点では，世間一般で広く行われている「IC カード化自身が目的」となることは避けるべきと考えてきました。本来は，身分証明証の IC カード化は，それ自身が目的ではなく，IC カード化を通じた ID の統一に始まる Identity Manegement や，セキュリティの向上が目的であるべきと考えます。しかし，種々の制約により，それらを一気に解決することは難しいのが現状です。IC カードが 10 年後には陳腐化していない保証はどこにもないのですが，媒体が替ったとしても，今回の IC カード職員証・学生証が，情報システムのセキュアな利用が広まるきっかけになることを望みます。

また，名古屋大学 IC カード職員証・学生証の利用に関するお問い合わせは，情報連携統括本部にお願い致します。

謝辞

本稿を書くにあたり，NTT Communications 株式会社から eLWISE に関する情報を提供頂きました。また，IC カード職員証・学生証作成に関しては，名古屋大学財務部情報企画課に多大なご協力を頂きました。

参考文献

［1］ 松尾啓志，IC カード導入からスタートする 4 つの統一＝名古屋工業大学での導入事例＝，名古屋大学情報連携基盤センターニュース，**6**，317−319，（2007）

［2］ 篠田成郎，岐阜大学における統合認証と IC カードの導入事例紹介―情報戦略における基盤システムの構築―，システム技術／研究教育環境分科会
http://www.ssken.gr.jp/lib/nl/2006/edu/stg_edu−1/doc6.html

［3］ 間瀬健二，平野靖，梶田将司，名古屋大学 ID の導入について（I）―概要―，名古屋大学情報連携基盤センターニュース，**5**，316−320，（2007）

［4］ 平野靖，間瀬健二，梶田将司，名古屋大学 ID の導入について（II）―全学 ID からの移行―，名古屋大学情報連携基盤センターニュース，**6**，140−145，（2007）

［5］ 梶田将司，平野靖，間瀬健二，名古屋大学 ID の導入について（III）―将来構想―，名古屋大学情報連携基盤センターニュース，**7**，11−17，（2008）

［6］ 内藤久資，山口由紀子，全学メールサービスの概要，名古屋大学情報連携基盤センターニュース，**7**，157−167，（2008）

［7］ 葛生和人，IC カードを用いた共有端末認証―IC カードを利用してユーザごとの作業環境を構築する―名古屋大学情報連携基盤センターニュース，**7**，51−67（2008）

［8］ 内藤久資，Mac OS X ―続 Mac OS X の進化論―，名古屋大学情報連携基盤センターニュース，**4**，211−236（2005）

［9］ 平野靖，内藤久資，UPKI イニシアティブ「サーバ証明書発行・導入における啓発・評価研究プロジェクト」について，名古屋大学情報連携基盤センターニュース，**6**，379−391（2007）

［10］ Hisashi Naito, Shoji Kajita, Yasushi Hirano, Kenji Mase, Multiple-tiered Security Hierarachy for Web Applications Using Central Authentication and Authorization Service. Proceeding of Middleware Workshop on IEEE International Symposium on Applications and the Internet（SAINT 2007）, Hiroshima, JAPAN, 27（2007）

［11］ NTT Communications, Safty Pass SmartOn Solo,
http://www.safety-pass.com/business/service/ser9.html

［12］ NTT Communications, Safty Pass Lock for Mac,
http://www.safety-pass.com/business/service/for_Mac.html

［13］ 小松文子，PKI ハンドブック，ソフトリサーチセンター

（ないとう　ひさし：名古屋大学多元数理科学研究科，名古屋大学情報連携統括本部情報戦略室）
（くぼ　まさし：名古屋大学多元数理科学研究科）
（ひらの　やすし：名古屋大学情報連携基盤センター）
（くずう　かずと：名古屋大学情報連携基盤センター）