情報処理学会論文誌　コンシューマ・デバイス & システム　Vol.3　No.1　34–45 (Mar. 2013)

コンシューマ・システム論文

一般カードを使った一時利用者向け認証システムの設計と実装

清水 さや子[1,2,a)]　岡部 寿男[1]　吉田 次郎[2]

受付日 2012年5月18日, 採録日 2012年12月7日

概要：近年，様々な情報システムの利用のために，認証システムが重要になってきている．IC カードを使った認証システムを導入する組織も増えてきている．しかし，多くの組織では，一時利用者に対してカードコストや管理運用コストが問題になる．そこで，本研究では，一時利用者には IC カードを発行せず，本人が日常的に利用している IC カードを使い，各種認証システムが利用できるようにするための仕組みを提案する．本提案は，セキュリティレベルを 4 段階に設定し，各認証システムはセキュリティレベルに応じて，カード内情報と PIN コード，さらに ID とパスワードを組み合わせることにより認証を行う．PIN コード認証を使うサービスは，認証システム側に PIN コード情報やユーザ情報を持たせない仕組みにより，一時利用者の登録のコストを削減した．

キーワード：一般カード，一時利用者，認証，PIN コード

Design and Implementation of an Authentication System for Temporary Users Utilizing Widely-used Smart Cards

Sayako Shimizu[1,2,a)]　Yasuo Okabe[1]　Jiro Yoshida[2]

Received: May 18, 2012, Accepted: December 7, 2012

Abstract: Recently, authentication systems have become important in use of various information systems. Not a few organizations have introduced authentication systems based on smart cards. However, for temporary users, the cost for issuing and for management of cards is not small. In this paper, we propose an authentication system utilizing several types of widely-used smart cards that are used daily, so as to eliminate the cost. In our proposal, we classify each service into four levels of security. Authentication mechanism for each service is designed according to the security level. Services in medium levels of security are authenticated using the information in the card and PIN code and additionally a combination of password and ID. Authenticated services using PIN code do not have PIN code nor and user information in the system so that we can reduce the cost of the registration of temporary users.

Keywords: widely-used smart cards, temporary users, authentication, PIN code

1. はじめに

近年，統合認証システムや SSO システムの導入により，アカウントとパスワードの一元化が進みつつある [1], [2]．アカウントとパスワードの組み合せは 1 度破られると，後々に重大な被害を被る恐れがある．そのため，さらなる認証の強化のために IC カードが使われることが増えている [3], [4]．大学等の組織においても，情報システムや入退館システムの利用のために認証システムが重要になり，IC カードをそれ単体ではなく身分証と一体化させて導入することが増えている [5], [6]．大学等の組織の特徴として，学生や教職員以外に，様々な身分の人が様々な期間在籍し（以下，一時利用者とする），組織の様々なシステムを利用

[1] 京都大学
Kyoto University, Kyoto 606–8501, Japan
[2] 東京海洋大学
Tokyo University of Marine Science and Technology, Minato, Tokyo 108–8477, Japan
[a)] smz@net.ist.i.kyoto-u.ac.jp

するという傾向がある．このような組織では，一時利用者の管理部署が多部署にわたっていることが多く，全体を把握することが非常に難しい．また，様々なサービスが提供されているが，それらのサービスは学部・学科等のセグメントごとに管理し，身分・所属により利用できるサービスが決まっている．このような組織では，一時利用者が着任するたびにICカードを発行し離任のたびに回収することは難しい．一時利用者には，必要に応じていわゆる白カードの貸出しを行っている組織はあるが [7]，多くの組織では一時利用者にカードの発行等の対応がなく，一時利用者がICカードを用いたシステムが利用不可の状態となっている．

本研究では，ICカードを用いた認証システムにおける一時利用者対応の管理運用の煩雑さやカード発行に関するコストを最低限に抑えるため，一時利用者にはICカードを発行せず，本人が日常利用している交通系ICカードやプリペイド決済用ICカード等，共通規格に基づいて発行されているICカード（以下，一般カードとする）を使い，身分・所属ごとに各システムを利用できるようにするための仕組みを提案する．

一般カードは，組織ごとに専用に作られたカードと異なり，認証用に新たに情報を追記することや，組織固有の暗号化された格納情報を認証に使用することが難しく，利用できる認証情報に制限があるためセキュリティ対策が必要になる．そのため，システムの重要性に応じて要求されるセキュリティレベルの格付けを行い，それに応じて設計を行う．

大学向け一般カードを使った認証は，著者らの先行研究として，認証情報にカード内の読み取り可能情報を組み合わせて使用し，さらにはキー情報を追加して使用し，その情報を一元管理するためのDBを構築するシステムの設計を行った [8]．しかし，最近では，NFC機能搭載の携帯端末の出現により，ICカードをエミュレーションすることが簡単にできるようになり，読み取り可能情報は偽装される恐れがある．さらに，大学という組織の特徴より，一時利用者の情報を中央のDBで一元管理することは非常に困難であった．詳細は2章で述べる．

これらより，本研究では，入退館システム等要求されるセキュリティレベルが比較的低い認証システムは，一般カード内から読み取り可能な情報を認証に使用する．これに対し，中程度以上のセキュリティレベルが要求されるシステムに対しては，カードの紛失や偽装の対策を考慮した認証システムとする．カード内の読み取り可能な情報だけでは不十分であるため，これらに加えて，本人のみ知りうるキー情報（以下，PINコードとする）による認証を併用する．

PINコード認証を行う際，一般カード内には容易に情報を追加できないため，PINコード情報を認証システム側に格納しておく必要がある．しかし，運用上の観点から，一時利用者の認証に関する認証システムの負荷が一般利用者と同等以下であることや，一時利用者の登録・抹消にともなう人的コストが十分小さいことが求められる．また，大学のような組織の特徴として，学部・学科等のセグメントごとに管理している各システムを中央で一元管理することは難しいため，セグメントの管理者が容易に管理できるよう，格納する情報は必要最低限にする必要がある．これらの問題を検討した結果，各認証システムにはPINコード情報は格納せず，PINコード生成式だけを格納することとする．PINコードはカードごとに異なる値にする必要があるが，上記理由より，各認証システムに異なる情報を格納するのではなく，カード内情報のカードごとに異なる値を利用して，生成する手法を提案する．これによって，セグメントごとの管理者はPINコードを管理することなく，一時利用者が保持する一般カードに対して，PINコードを発行すれば，一時利用者はシステムが利用可能になる．また，中央で一元管理しないことにより，地理的にもネットワーク的にも離れた地域内でも，PINコードさえ発行できれば，システムが利用可能となる．

現在，東京海洋大学では，これらの設計をもとに，ICカード認証システムの全学導入に向けて検討を行っているところである．また，近年では，大学間連携のための認証基盤のサービスが整備されつつあるため [9], [10], [11]，全学認証システムの強化を目指して，一般カードを使った大学向け認証システムの実装を行っている．

2章では，大学という組織の特徴と問題点として，一時利用者の管理方法，情報システムの分散管理，その解決策について述べる．3章では，一般カードを使った認証システムの導入事例や先行研究および先行研究における課題を紹介し，4章では，その解決策である一般カードを使った認証方法の提案を述べ，5章では，実装したシステムと実装したPINコードを使った認証方法について述べる．6章では，現在，試験運用中の一般カードを使った認証システムの評価を述べ，最後にまとめを述べる．

2. 大学の特徴とICカードを導入する際の要件

2.1 一時利用者の管理

大学や大学共同利用機関等の組織は，学生や教職員が在籍する以外に，様々な身分の一時利用者が様々な期間在籍し，組織の様々なシステムを利用するという傾向がある．学生と教職員の管理部署は身分ごとに分かれ，一時利用者の管理部署は，身分・所属により多部署にわたっていることが多い．また，一時利用者の情報は集約されていないことが多く，一時利用者を含む組織の全構成員を把握することが非常に難しい．大学等の組織の特徴は，一時利用者の在籍だけではなく，教職員と学生との仕切りが低いことや，元職員にも現職員と同等のサービスを提供しなければなら

ない場合があること，非常勤講師として雇用契約は結んでいるが，年 1 回だけ講義する可能性がある人が，正職員より多い数登録されている場合もあり，このような中では一時利用者を明確に線引きすることも困難である．

これらより，IC カードを導入する場合，一時利用者の扱いが問題となる．一時利用者に，施設利用時等必要に応じて，白カードといわれるカードを貸し出している組織もあるが，通常は，一時利用者が着任するたびに IC カードを発行し離任のたびに回収することは，運用管理の煩雑さやコスト面から非常に難しいため，一時利用者に対してはカード発行等の対応をとらず，一時利用者が IC カードを使ったシステムが利用できない状態となっている組織が多く見られる．大学という組織における一時利用者の人数は，正確には把握できていないが，1 年間における一時利用者数は，東京海洋大学の場合は全構成員の約 1〜2 割と考えられ，現在，多くの一時利用者は IC カードを使った認証システムが利用できない状況となっている．

本研究における一時利用者は，ある程度在籍年数が決まった学生や教職員以外の短期間雇用の非常勤職員，共同研究員，派遣社員等とする．具体的には，組織の情報システムを利用するが，大学に来る期間が短いか期間が長くても来る回数が少ないため IC カードを発行するのが難しい人，あるいは，大学に正式な身分がないため，IC カードを発行できない人とする．一時的に来構する訪問者や受験生は一時利用者には含まない．本研究では，これらの一時利用者が IC カードを使ったシステムを利用できる仕組みを提案する．

2.2　各種システムの分散管理

大学等の組織では，様々な情報サービスを提供している．提供されるサービスは全体のサービスのほかに，学部・学科のセグメントごとに異なるサービスがあり，身分・所属により利用できるサービスが異なる．利用可能なサービスは身分・所属ごとに異なるが，これらの情報サービスのすべてが中央で一元管理されているのではなく，セグメントごとに個別に管理されている場合も多い．これは，組織の特徴として縦割り運営が行われていることと，それに対して学部や学科ごとの特性を出すためでもある．最近では，全学的に統合認証システムを導入し，中央でアカウントの一元管理を行っている組織もあるが，中央では，アクセスしてきた情報の照合をすることはできるが，管理セグメントの異なる各システムからの認証に対して利用者に利用権を与えるいわゆる認可を行うことは難しく，行う場合は管理者に非常に負荷がかかるため行わないことが多い．また，中央で一元管理するシステムに，セグメントごとに管理しているシステムを連携させる際，中央管理のシステムの管理部署とセグメントごとのシステム管理部署との取り決めや，アクセス時の制限等により，連携手続きに時間を要することが多くある．特に，組織内で管理部署が分散され集約するのが難しい一時利用者の情報および，一時利用者の保持する一般カード情報やキー情報等の情報を中央で一元管理する場合は，手続きが困難になる可能性もある．

さらに，セグメントで管理するシステムと中央管理のシステムを連携することができた場合，一元管理することができ，利便性が高くなる反面，つねに，認証システムとの通信が必要であるため，ネットワークが異なる場合や通信が遮断された場合，そのシステムが使用できなくなる．それに比べ，セグメントごとに，独立したシステムにすることにより，中央管理のシステムへアクセスできない環境，たとえば船内 LAN 環境等においても，利用可能なシステムとなる．また，セグメントごとの独自の限定サービスとして提供することができる．これらより，本研究においては，中央管理のシステムとの連携については省略し，セグメントごとに管理するシステムを提案する．

2.3　一般カードによる一時利用者の認証の提案

上記の問題より，本研究では一時利用者に対しては運用管理の煩雑さやカード発行のコストを最低限におさえるため，一時利用者には IC カードを発行せず，本人が日常利用している交通系やプリペイド決済系の IC カードを使う．そして，一時利用者の身分・所属による利用可能な範囲で，組織ごとに専用に発行したカード（以下，専用カードとする）の利用者と同様に認証システムが利用できるよう，各システムの重要性に応じてセキュリティレベルの格付けを行い，各認証システムが利用できるようにするための仕組みを提案する．本研究における一般カードとは，交通系 IC カードやプリペイド決済用のカード等，日常生活で簡単に手に入れて利用することができる共通規格に基づいたカードのこととする．

専用カードは組織ごとに安全性を考慮して作成するカードであるため，セキュリティは比較的高く，カード内情報の書き換えや独自に情報を追加することができ，また，券面表示もできるといった利点がある．このため，本来は専用カードだけで運用するのが望ましい．しかし，大学等の一時利用者が多い組織においては，一時利用者の着任するたびに専用カードを発行し，離職のたびに回収することは，運用管理の煩雑さやコスト面から非常に難しい．一方，一般カードは，カード発行元において重要な取り決めがあるため，新たな情報の追加や，中身の書き換えすることが難しく，自由に新しいサービスを提供することが難しい．また，カード内情報の取扱いにも制限があるため，認証に暗号化された情報を使用することが難しく，読み取り可能な情報を使用することになるため，セキュリティは比較的低くなる．しかし，一般カードの場合，カードを持っていればよく，新たにカードを発行し回収する手間やコストは削減できる．一般カードは，交通機関等で IC カードが発達

している都心では，複数のカードを保持している人が多く，カードが増えることを好まない人もいる．そのような中で，新たに保持するカードを増やすことなく，現在保持しているカードで認証システムが利用できるようになることは，一時利用者の利便性の向上にもつながる．

本研究では，入退館システム等要求されるセキュリティレベルが比較的低い認証システムは，先行研究と同じく一般カード内から読み取り可能な情報を認証に使用する．これに対し，セキュリティレベルが中程度以上を要求されるシステムでは，カードの紛失や偽装の対策を考慮した認証システムとするため，一般カード内の読み取り可能な情報だけを認証に使用するのは不十分であることより，PIN コードによる認証を併用する．本研究では，セキュリティレベルが比較的低いシステムにおいては，製品例とほぼ同等であることより，セキュリティレベルが中程度以上のシステムを重点的に設計し，実装を行う．

なお，本研究で提案するシステムは，セグメントごとに管理するサービスとすることより，各セグメントのシステム管理者の負担は最低限にする必要が求められる．これらより，提案するシステムは，各セグメントの管理者が容易に管理できるよう，個々の利用者情報を認証システムに登録，管理しなくてもよいシステムとする．具体的には，PIN コード発行システムで PIN コードを発行するだけで，システムが利用可能になり，各システムの管理者は，PIN コード管理を不要とするシステムとする．PIN コード情報はカードにもシステムにも格納せず，カード内情報から PIN コードを生成する仕組みとする，新しい PIN コード生成方法を提案する．ただし，入退館システム等，建物ごとに入館者を区別し，入退館履歴等を残す必要があるシステムは，個々の情報を登録しておく必要があるため，この限りではない．

2.4　本研究で想定するシステム

IC カードは，入退館システムや証明書発行システム，PC ログインシステム，各種情報システムの利用等で利用され，それぞれのシステムはシステムの重要性に応じてセキュリティレベルの格付けを行う．本研究では，一時利用者が利用するシステムを**表 1** と仮定し，これらのシステムに対してセキュリティレベルを設定し，それぞれのレベルに応じた認証システムの設計を行う．

（1）は，平日の日中であれば誰でも出入りできるが，平日の夜間や土日祝日にはカードをかざして出入りするシステムとする．重要部屋への出入りシステムではないため，カードの偽装の対応は考えないことと，備え付けの専用カードリーダを使用するためシステム改ざんの可能性は非常に低いと考えることより，セキュリティレベルは比較的低く設定する．（2）は，学内ネットワークに接続すれば誰でも閲覧可能な学内限定サイトを，学外ネットワークから閲覧する際に，カード認証を行うシステムとする．ここでいうカード認証とは，IP アドレスや共通パスワードによる制限のようなものと考え，Web サイトの内容は，重要情報ではなく，簡易な学内スケジュール等を掲載するサイトする．ただし，認証は個人 PC から行うため，システム改ざんやカード偽装等の対応を考慮することより，セキュリティレベル中程度とする．（2）の認証だけではセキュリティレベルが不足する場合は，カード認証の後に，さらなる認証として個々の ID とパスワードによる認証を追加する．これを（3）とする．（3）は，セグメントごとに運用しているポータルサイト等とし，個人認証が必要であり，個々に表示が異なるようなシステムとする．

表 1　本研究で想定するシステム
Table 1　Systems simulating in this report.

	想定するシステム	セキュリティレベル
(1)	建物の入退館システム	低
(2)	学内限定簡易 Web サイト学外から閲覧時の認証	中
(3)	学内限定ポータルサイト学外から閲覧時の認証	中上

なお，本研究における一般カードとは，日本で交通系のカードとして一番利用されている Suica や PASMO 等の交通系 IC カードや nanako や WAON 等プリペイド決済用の IC カード等，日常生活で簡単に手に入れて利用することができる共通規格に基づいた FeliCa タイプのカードに限定して設計および実装を行うが，本提案の基本的な考え方は他のタイプのカードでも広く応用できるものである．また，本研究で構築したシステムの利用者は，一時利用者に限らず，IC カード未導入の組織等の一般利用者でも利用可能である．

3.　先行研究と関連技術

FeliCa タイプの一般カードを使った認証システムとしては，カード内から読み取り可能情報である製造 ID（IDm）等を抜き出し，認証に使用する製品がすでに販売されている．本章ではこれらの製品例を紹介し，さらに著者らが行ってきた先行研究と課題，および一般カードを使った認証方式における課題について述べる．

3.1　一般カードを使用した認証システムの製品事例

大学における導入事例としては，FeliCa タイプのカードや FeliCa 機能搭載の携帯電話を使って，授業の出席管理等を行っている大学がある [12], [13]．日常生活においては，交通系の IC カード（おサイフ携帯も可）を登録すると，提携した店や施設でかざすだけで，ポイントをためることができるシステムや [14]，FeliCa 搭載の携帯電話，運転免許

証（IC カードのタイプは TypeB），taspo（IC カードのタイプは TypeA）カード等，身の回りの各種 IC カードで車キーやドアをロック・アンロックできる製品が販売されている [15], [16]．これらのシステムは，カード内の読み取り可能領域から情報を抜き出して認証に使用しているため，安全性が求められるシステムにとっては，カードの盗難や偽装時に対する対応が少し足りないと考える．セキュリティレベルが中程度以上のシステムにおいては，カードをかざすだけの認証ではなく，悪用可能性の対応として，さらなる認証情報を組み合わせることが求められる．

3.2　一般カードを使用した認証システムの先行研究

著者らは先行研究として，大学の一時利用者向けに FeliCa タイプの一般カードを使って，セキュリティレベルに応じて認証システムの設計を行っていた．セキュリティレベルが比較的低いシステムにおいては，IDm による認証を行い，セキュリティレベルが中程度以上のシステムにおいては，カード内の読み取り可能な情報から情報を組み合わせて認証情報とし（カードシステム ID と呼ぶ），さらに高いセキュリティレベルが求められるシステムは，キー入力による認証を行うシステム設計を行っていた．

ここでは，FeliCa の IDm は簡単に読み取ることができるが [17]，FeliCa タイプのカードはカードの複製が困難であるといわれていたため，IDm 等が読み取られた場合でも，悪用の可能性が低いと考えられていた．また，一時利用者を一元管理するために中央に認証ゲートウェイサーバを構築し，カード内情報もキー情報も中央で管理することとしていた（**図 1**）．

しかし，近年，市場に出回っている携帯電話の多くは FeliCa 機能が搭載されているが，最近は NFC [*1] 機能搭載のものも市場に出てきている [18]．NFC 機能搭載の携帯電話は，リーダ機能も搭載されており，FeliCa カードをエミュレーションすることが簡単にできる．この技術は，IDm だけでなく，非暗号領域も簡単にエミュレーションできる．この技術が悪用された場合，NFC 機能搭載の携帯電話に FeliCa カードをかざすとカード内の読み取り可能情報を取得し，携帯電話がそのカードになりすますことができる．これらより，認証時に IDm だけではなくカードシステム ID を使用した場合でも，なりすましによる悪用の可能性が否定できないため，安全性の問題が出てきた．そこで，カードシステム ID は，認証に IDm のみを読み取って偽装することは比較的簡単であるため，IDm のみを偽装する攻撃に対して，メリットがあることより，カードシステム ID は，IDm の補助的に使うこととし，セキュリティレベル中程度以上の認証方法を再検討することとなった．また，2 章のとおり，大学のような組織の特徴より，中央に認証ゲートウェイサーバを構築し，一時利用者情報や一般カード情報を管理することは難しく，一時利用者の利用システムの可否を中央で管理することは困難であった．

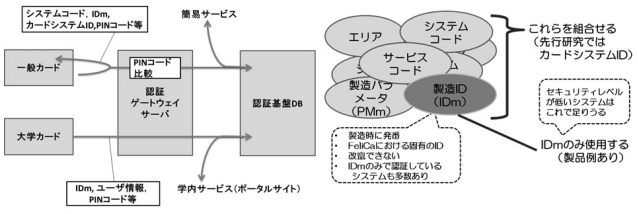

図 1　先行研究の認証図

Fig. 1　Authetication figure of previous research.

[*1] Near Field Communication の略．ソニーとフィリップス（現 NXP セミコンダクターズ）が共同開発し，国際標準規格として承認された近距離無線通信技術．

これらより，本研究においては，セキュリティレベルの重要度に応じた認証方法を再度検討し，さらに，中央で一元管理することなく，セグメントごとに容易に利用できるシステムの提案を行う．

3.3　一般カードを使った認証方法の検討

一般カードは組織ごとに専用に作られたカードではないため，認証用に新しく情報を追記することが困難である．一般カード内の格納情報から認証に使用できる情報について検討，および安全性の検討を行う．

3.3.1　FeliCa 内の情報を使った認証方法の検討

FeliCa 内のメモリは以下の 2 種類のブロックに分かれており，それぞれ**表 2** のような特性がある [19], [20]．

- ユーザブロック：ユーザデータが書き込まれる領域
- システムブロック：FeliCa の構成情報が保存されている領域

本来はユーザブロック内情報を使用する方がよいが，重要な取り決めが必要である．システムブロック内情報はユーザブロック内情報に比べて安全性は高くないが，取扱いは比較的容易である．

3.3.2　一般カードを使った場合の安全性の考慮

一般カードを使った認証方法は，大きくは 3 つの方法に分けることができる（**表 3**）．

ここで，[1] と [2]① の場合は，安全性が確保されるが，カード発行会社と重要な取り決めが必要なため，本研究においては検討を省略する．[2]② は，3.2 節のとおり，先行研究において検討していたが，NFC 機能搭載の携帯電話

表 2　ユーザブロックとシステムブロック
Table 2　User block and system block.

ユーザブロック	システムブロック
• 安全性高い（基本的には暗号化あり） • 相互認証あり • カード種類によって格納されている領域が異なる • 暗号化領域の利用は，発行元と重要な取決必要	• 安全性低い（基本的には暗号化なし，情報の読取可能） • 相互認証なし • FeliCa であれば，格納されているブロックの領域は同じ • 中身の書換は基本的には不可

表 3　一般カードを使った場合の認証方法
Table 3　Authentication methods by using smart card.

	認証方法	備考
[1]	カード内に情報を追記	鍵情報等を格納
[2]	カード内の情報を利用	①　暗号化領域を使用 ②　非暗号化領域を使用
[3]	その他（[1]と[2]以外）の情報の組合せ	①　指紋や静脈認証 ②　キー入力による認証

による偽装問題がある．ただし，セキュリティレベルが比較的低いシステムにおいて使用すればよいと考える．

セキュリティレベルが中程度以上のシステムにおいては，[3]を検討する．ここでは [3]①や [3]②があげられるが，個人情報の取扱い等を考えると，比較的導入に抵抗がない [3]②のキー入力による認証が妥当であると考える．本研究では，この本人しか知りえないキー情報（PIN コード）の新しい生成方法，認証方法，それにともなう管理・運用方法を様々な方面から検討し，設計，構築を行う．

4. 提案する PIN コードを使った IC カード認証システム

4.1 従来方式と新しい PIN コード生成方式の提案

これまでの PIN コードを使った認証システムは，PIN コード情報を一般カード内に格納する方式，もしくは，認証システム内に格納する方式であった．これらの方式は，カードや PIN コードの登録・管理のためのコストが発生する．また，PIN コードを一般カード内に格納する方式は，それぞれのカード発行会社と重要な取り決めが必要となることや，カード紛失時の悪用対策に格納情報暗号化が必要であるため，容易ではない．運用上の観点より，一時利用者が一般カードを使ってシステムを利用する場合，認証に関する認証システムへの負荷は，専用カード利用者の負荷と同等もしくはそれ以下であることが求められる．さらに，2.2 節のとおり，大学のような組織では，セグメントごとにシステムを立ち上げて管理されていることが多いため，セグメントごとの管理者が容易に管理できるシステムが求められる．これらより，本研究においては，各認証システムに格納する情報は必要最低限となるよう，PIN コード情報は，IC カード内や認証システム内に格納せず，IC カード内情報から PIN コードを生成する「PIN コード生成方式」を新しく提案する（**表 4**）．

ここで，セグメントに設置した管理者用 PC 端末から Web 経由で中央の集中サーバにアクセスして PIN コードを渡すことも可能と考えられるが，2.2 節のとおり，本研究では，一般カードの受付を学部・学科に設置したサーバにインストールしたアプリケーションにより PIN コードを生成して渡す設計である．この方式により，セグメントごとに，独自の PIN コード体系を作ることができ，セグメントごとの限定サービスとして提供することができる．

表 4　一般カードの認証方式と特徴
Table 4　Authentication methods and characteristics of the widely-used smart cards.

一般カードの認証方式	特徴
一般カード内に格納する方式（従来方式）	• カードや PIN コード登録・管理のコスト大 • カード発行会社と重要な取決が必要 • カード紛失時の悪用対策に格納情報暗号化が必要
各認証システム内に格納する方式（従来方式）	• カードや PIN コード登録・管理のコスト大 • 認証時にシステムとの通信が常に必要
PIN コード生成方式（提案方式）	• 認証システム側では PIN コードの管理不要 • PIN コード発行すればシステム利用可 • PIN コードは自由に設定不可

生成式：SUBSTR（HASH（n＋SALT），*position*, *length*）
（n：抜出した情報　*position*: 切出す文字の開始位置　*length*：切出す文字長）

図 2　PIN コード生成式
Fig. 2　The formula for PIN code generation.

4.2 PIN コード生成方式

各認証システムに PIN コードの情報は格納しないが，PIN コードの値はカードごとに異なる必要がある．一般カードの読み取り可能領域には，カードごとに異なる値が格納されているため，それらを抜き出し，少し工夫を加えることにより，PIN コードを生成する．具体的な PIN コードの生成方法を以下に記す（**図 2**）．これにより，認証システム上で実装する際には，認証システム上には，PIN コードを生成するための式と，生成した PIN コードと入力した PIN コードを照合するための式だけを格納すればよくなる．認証システム上での実装方法については，5.3 節で記す．

PIN コードの生成方法：

1. 一般カードの読み取り可能な情報から値を抜き出す（カードごとに異なる情報を含んだ値とする）．
2. 抜き出した情報を組み合わせる．
3. SALT を付加する．
4. HASH 化する．
5. 任意の桁数を抜き出す．

SALT を付加する理由は，SALT を付加せずにハッシュ化するだけであれば，ハッシュ関数は公開されているため，生成した PIN コードが漏えいしてしまう可能性がある．そこで PIN コード生成の強化のため SALT を付加する．また，SALT は PIN コードに有効期限をつける際に，SALT を変更することで対応する．

4.3 PIN コード運用手法

PIN コードを運用する際に，悪用される可能性を最小限にするため，運用における工夫が必要となる．以下，PIN コードを使った認証システムに対して，起こりうるリスクを分析し，それに対する対応，コストを比較し，実現可能

性を検討する．

① カードの紛失時・偽装時

基本的にはカードだけでは，PIN コードが分からなければ利用できないため，新しいカードで PIN コードを発行すればよい．悪用の可能性がある場合はカード失効処理を行う．

ただし，カードの取得者・偽装者による PIN コードを何度も試してのブルートフォース攻撃が心配されるため，PIN コード認証には入力制限をつけておく．入力制限にかかると，該当カードよりカード失効処理に必要な情報を抜き出し，管理者に警告をあげるシステムにしておくことで，管理者側でカードの失効処理をする必要があるかの判断を行う．これらは，通常の運用コスト以外に，悪用可能性時のカード失効処理と，警告がある際に，管理者が作業するコストが発生する．

② PIN コードの紛失時・漏えい時

基本的には PIN コードだけでは，カードがなければ利用できないため，単に PIN コードを忘れただけの場合は，再発行を行う．悪用の可能性がある場合は，該当カードに対してカード失効処理を行う．

ただし，離任した人がいつまでも使えたり，知らない間に悪用されていたり等のリスクを最低限に抑えるために，PIN コードの生成の種を定期的に更新し，PIN コードを配布し直す．定期的な期間が短いと多くのコストが発生するため，更新は年に 1 回か 2 回程度とする方がよいと考える．PIN コードの更新時には失効処理情報も一新し，失効処理していたカードも申請し直すことで，新しい PIN コードで利用できる．通常の運用コスト以外に，悪用可能性時のカード失効処理と，定期的に PIN コードを生成し，配布するためのコストが発生する．

③ カードの紛失時・偽装時と PIN コードの紛失時・漏えい時

これは①②に比べて，緊急性が高く，ただちに失効処理を行う．この場合，緊急対応のためのコストが必要となるが，カードと PIN コードの両方 1 度に紛失することはめったに起こらないと考えるため，通常運用においてはめったにコストは発生しないと考える．

これらより，認証システムには，PIN コードの入力制限をつけることと，カード失効処理のために失効リストを作成しておき，失効のたびに追加できるようにしておく必要がある．失効リストに登録する情報は PIN コード生成に必要なカード内情報の一部であり，カードごとに異なる情報を含んだ値とする．

また，PIN コードの更新と失効リストの更新時期は 1 年のうち人の入れ替わりが一番多い年度末にするのが良いと考える．

4.4 カードおよび PIN コードの失効，更新処理

失効処理は頻繁に発生するものではないが，認証システムの利用ユーザ情報はシステムごとに管理するため，失効リストは認証システムごとに格納する．各認証システムにはあらかじめ失効リストを作成しておき，失効処理の際に追加する．失効処理の際に登録する情報はカード内情報とし，カードに対して失効処理を行う．PIN コードはカードと一対であるため，カードが失効していれば，PIN コードも使用できないことより，PIN コードの失効処理はカードの失効処理と同様にカード内情報を登録する．

悪用の可能性を減少させるため，PIN コードには有効期限をつける．有効期限ごとに SALT を変更し更新する．PIN コードの有効期限の更新は，SALT を変更し更新する．PIN コードの更新時には 2 週間〜1 カ月程度の更新手続き期間を設定し，その間に継続利用する一時利用者は新規申請時と同じ手続きを行い，新しい PIN コードを受領する．更新作業の便宜上，更新手続き期間中のみ，今まで使用していた PIN コードと新しい PIN コードを利用可能とする．PIN コードの更新時に合わせて失効リストの更新も行うため，PIN コードの有効期限更新後，新たに PIN コードを発行することにより，失効処理されていたカードも利用可能とする．PIN コードの失効処理が行われたカードに対しては，PIN コードを再設定方法も考えられるが，最近は一般カードを多数保持している人が多いため，失効処理が行われたカードに対しては，いったん使用不可とし，新カードを登録し直してもらい，PIN コードの有効期限更新後，新たな PIN コードで再度利用可能とする．

5. 本研究で実装する認証システム

上記の設計をもとに実装を行う．本システムは，2 章の大学のような組織の特徴より，セグメントごとに管理されるシステムで比較的容易に運用できるよう，セグメントごとのシステム管理者は，重要な情報の管理が不要なシステムであり，PIN コードさえ発行すれば，利用可能となるシステムとする．中央管理のシステムで一元管理を行わず，認証システムごとに，PIN コード生成プログラムと PIN コード認証プログラム，SALT と失効リストを格納することで，組織のネットワークと異なる場所にある部局でも，独立して運用が可能となる．

5.1 本研究におけるセキュリティレベルの設定

セキュリティレベルの制定は組織によって異なるが，本研究では，**表 5** のセキュリティレベルを制定し，これを元に実装を行う．

利用するシステムとそれに対するセキュリティレベルを 4 段階に分け，セキュリティレベルは認証における安全性の重要度に比例して高くなるよう設定する．セキュリティレベル 4 は，専門の常勤職員のみが利用するような重要シ

表 5　一般カード利用によるセキュリティレベル表
Table 5　Table of security level by using smart cards.

セキュリティレベル	認証に必要な情報	利用サービス例	備考
4 (高高)	----------	人事システム 予算システム等	重要システム， 一時利用者利用不可
3 (中上)	読取可能情報(IDm 等) PIN コード， ID, PWD（個人認証用）	情報システム (個人認証付ポータルサイト閲覧)	個人 PC 利用
2 (中)	読取可能情報(IDm 等) PIN コード	情報システム (簡易 Web 閲覧)	個人 PC 利用
1 (低)	読取可能情報(IDm 等)	入退館システム	固定専用リーダ

ステムとするため，一時利用者の利用範囲は 1〜3 とする．セキュリティレベルが比較的低いシステム（セキュリティレベル 1）については，偽装の恐れ等は考慮しないことより IDm 等のカード内の読み取り可能情報を使った認証方法とする．セキュリティレベルが中程度（セキュリティレベル 2）以上のシステムは，偽装等の恐れを考慮することより，カードと本人のみ知る PIN コードを併用する．ただし，PIN コードを使った認証は，2.4 節のとおり，IP アドレスや共通パスワードによる制限のようなものと考える．セキュリティレベルが中上のシステム（セキュリティレベル 3）では，セキュリティレベル 2 の IC カードと PIN コードによる認証だけでは不足すると考え，さらに個人認証が必要とするシステムより，IC カードと PIN コードによる認証後，Web 上での ID とパスワード認証を行うものとする．

なお，セキュリティレベル 1 の認証方法については，すでに商品化されているものがあることより，本章では省略し，ここでは，新しく提案する PIN コード生成方式を使用するセキュリティレベルが中程度以上のシステムについて重点的に記す．

5.2　セキュリティレベル 2 と 3 の認証方法

セキュリティレベル 2 と 3 の認証方法の流れは以下のようになる（**図 3**）．

1)　認証用 Web ページを開く．
2)　カードをリーダにかざす．
3)　システムコードをチェックする．
4)　PIN コードを入力する．
5)　PIN コード生成に必要なカード内情報を取得し，PIN コードの照合する．
6)　失効情報の照合する．
7)　失効情報に情報がなければ認証に成功で，サービス利用可能となる．

さらに，セキュリティレベル 3 では，以下の認証方法を追加する．

8)　ID とパスワード入力し認証を行う．
9)　ID とパスワードが合致すれば，サービス利用可能となる．

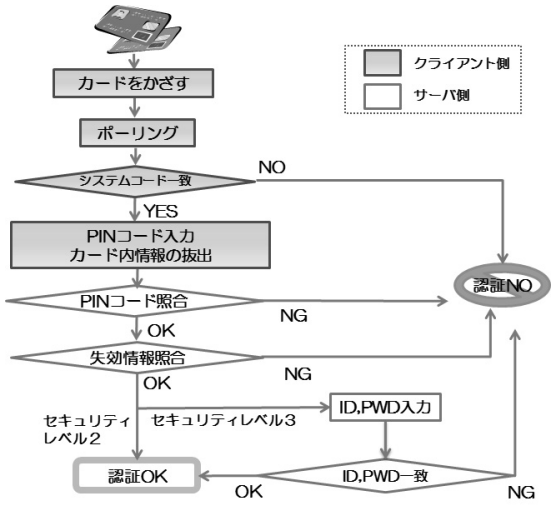

図 3　認証の流れ
Fig. 3　Flow of authentication.

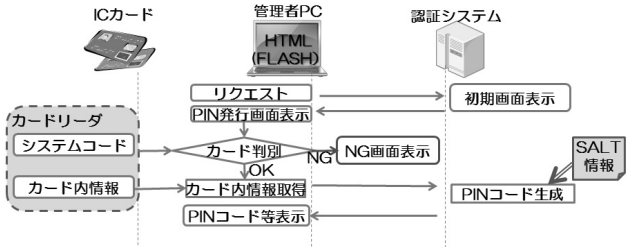

図 4　PIN コード発行のフロー
Fig. 4　Flow of PIN code issuing.

5.3　PIN コード生成方式による PIN コード発行フローと認証フロー

認証システムの中には PIN コード生成用のプログラムと PIN コード認証用のプログラム，および SALT と失効リストを格納し，それぞれ，www 上からアクセスする．開発環境には，SDK for NFC Adobe AIR Flash Basic 1.3.0, Perl 5.16 を用いる．PIN コード発行フロー，PIN コード認証フローを以下に記す．

5.3.1　PIN コード発行システム

管理者用 PC から www 経由で認証システムの PIN コード発行用 URL（管理用）にアクセスし，PIN コード発行画面を表示する．PIN コード発行画面が表示されるとカードリーダに一般カードをかざし，カード判別を行う．カード判別に成功すれば，カード内から PIN コード生成に必要な情報を抜き出し，認証システムに送る．認証システム側では送られてきた情報に SALT を付加して，PIN コードを生成し，PIN コード情報を返す（**図 4**）．

5.3.2　PIN コード認証システム

個人 PC から www 経由で認証システム URL にアクセスし，ログイン画面を表示する．ログイン画面で表示されるメッセージ（「カードリーダに一般カードをかざしてください」）に従い，カードをかざす．カード判別を行い，カー

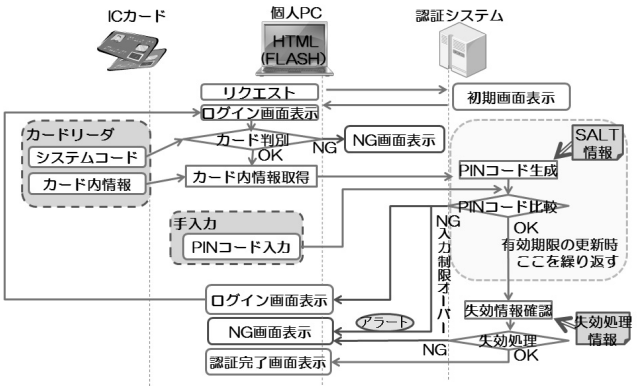

図 5　PIN コード認証のフロー
Fig. 5　Flow of PIN code authentication.

ド判別に成功すれば，PIN コード入力を行う．入力された PIN コードとカード内から PIN コード認証に必要な情報を抜き出し，認証システムに送る．認証システムでは送られてきた情報に SALT を付加して PIN コードを生成し，入力された PIN コードと比較する．PIN コードが合致すれば，失効処理情報の確認を行う．抜き出した情報の一部と失効リスト情報を照合し，失効リスト情報と合致しない場合は，認証成功となる（図 5）．

PIN コード照合が成功しない場合，入力制限回数までは，PIN コードの入力ができるが，入力制限数を超えた際に NG 画面を表示し，カード内から失効処理に必要な情報を抜き出し，管理者にアラートをあげる．また，図 5 の右の点線箇所は有効期限の更新期間に，繰り返し処理をする範囲であり，PIN コード更新期間は SALT を 2 つ持たせ，2 つの PIN コードで認証できることとする．

5.4　実装したシステムの評価

本研究で実装した認証システムでは，ユーザ情報やカード情報は保持せず，PIN コード等の管理は不要である．本研究では，セキュリティレベル 2 は，学外から個人 PC より Web サイト閲覧するための認証システムである．認証システムには，ユーザ情報や PIN コード情報は格納せず，PIN コード生成式のみ格納する．ただし，失効処理を行ったカードについてはカード内の一部の情報を格納する．これらは，2.4 節で記したとおり，組織内ネットワークを IP アドレスや共通パスワード等によりアクセス制限しているものを，組織外ネットワークからは一般カードと PIN コードの所持者であれば全員アクセスを許すような運用である．つまり，一般カードと PIN コードの所持者のうちこの人とこの人だけに見せたい，というような利用制限はしていない．そのため，カード内情報や PIN コード情報を，利用者が追加されるごとに登録して管理する必要はないと考える．1 度発行した PIN コードは，失効処理を行わない限り，有効期限内は利用可能であるが，離職した人でも組織内ネットワークに入れば，利用できるシステムであるため，離職後に PIN コード有効期限は利用できても問題ないと考える．

セキュリティレベル 3 におけるメインの認証は ID とパスワード入力であり，その前段として PIN コード入力による認証を行っているため，セキュリティレベル 2 と同様に，認証システムにはカード内情報や PIN コード情報を格納することなく，利用者が追加されるたびに登録処理を行わなくてもよいと考える．ただし，本システムにおける PIN コードは，カード内情報から少し手を加え発行した値であり，ユーザが指定したものではないため，ユーザが忘れる可能性がある．そのため，運用方法の検討が必要となる．また，実装したシステムでは，失効処理されたカードは，更新期間まで利用できないため，新たなカードに PIN コードを発行して利用する．交通機関等で IC カードが発達している都心では，複数のカードを保持している人が多く，この運用方法でよいと考えるが，カードが発達していない地域では，失効処理後の扱いにおいて再検討が必要となる可能性もある．ただし，カードや PIN コードの悪用，カードと PIN コードの同時紛失は，非常に少ないと考え，本研究では検討は省略した．

6.　東京海洋大学での導入に向けての検討と試験運用

6.1　導入に向けて

現在，東京海洋大学における IC カード発行状態は，学生に対しては，IC カード学生証を発行しているが，教職員に対しては，IC カードは発行しておらず，導入検討中の段階である．本研究における提案は，IC カードが全学導入されており，その中で IC カード発行が困難な一時利用者向けに提案するシステムであるが，要求するセキュリティレベルに応じて一時利用者向けだけではなく，IC カードが導入されていない組織にも応用することができる．東京海洋大学では，将来的には，一時利用者向けに一般カードを使ったシステムとして稼働させる予定であるが，試験運用の時点においては，教職員に対して IC カードが導入されていないため，教職員も一般カードを使用して，本システムにおける試験運用を行う．なお，学生においては，IC カード学生証を利用する．

6.2　セキュリティレベル 1 の試験運用と評価

東京海洋大学の 1 建屋の入退館システムにおいて，セキュリティレベル 1 を実装し，試験運用を約 1 年間行った．システムの登録件数約 200 件であり，そのうち一般カード利用者は約 50 件である．認証は IDm のみを使った認証とし，すでに製品も販売されていることより，認証方法の説明は省略する．入退館システムでは，建物ごとに入館できる人を区別する必要があるため，システムには個別に申請に応じて IDm とユーザ情報を格納している．

約 1 年間，試験運用してきたが，運用でカバーできる問題が 3 件発生したのみで，大きな問題は発生しなかった．一般カードの登録時に，1 件，清掃業者は個人ではなく清掃業者として契約しているため個人カードは利用したくないとの希望があり，白カードを発行して対応した．さらに運用していくうえで，2 件，Suica 等のカードが，自動で新しいカードに変更されていることがあり，ユーザが気付かずカードが使えないことがあった．これは，交通系のカードではカードが変更になることを意識してもらうよう周知する等，運用でカバーする必要がある．今回の試験運用で一般カードを使用した約 50 名の中には，一般カードを保持していない人はおらず，また一般カードを使用することに抵抗を感じる人はいなかった．また，運用においても大きな問題は発生していない．

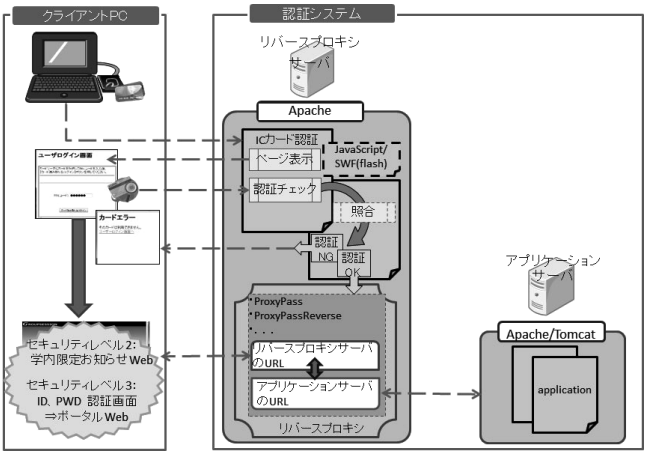

図 6　セキュリティレベル 2 と 3 の構成図
Fig. 6　Overview of security level 2, 3.

6.3　セキュリティレベル 2 と 3 の試験運用と評価

東京海洋大学の 1 セグメントで，セキュリティレベル 2 と 3 のサービスの試験稼働を行った．6.1 節のとおり，IC カードが発行されていない約 15 名程度の教職員向けに試験稼働を行った．セキュリティレベル 2 は，該当セグメント内で利用している学内限定のお知らせが記された Web ページであり，学外からのアクセス時に一般カードと PIN コードによる認証を行う．セキュリティレベル 3 は，該当セグメントで使用している学内限定のポータルサイトであり，学外からのアクセス時に一般カードと PIN コードによる認証を行い，Web ブラウザ上での ID とパスワード認証を併用する．

本試験稼働における環境は，該当セグメントですでに稼働している Web サイトに対して，既存システムに手を加えないよう，認証システムを構築し，個人用 PC から一般カードと PIN コードを使って認証する．具体的には，リバースプロキシサーバを構築し，そのうえで，5 章で実装した PIN コード認証用のプログラムを置く（**図 6**）．利用者は，リバースプロキシサーバ上の指定する URL にアクセスすることで，PIN コード認証画面が表示され，PIN コード認証に成功すると学内限定の Web サイトや学内限定のポータルシステムのログインページが表示される．

なお，試験稼働を行った環境それぞれの環境は，個人 PC の OS は Windows7 と XP，利用ブラウザは IE，Firefox，GoogleChrome，利用リーダは PaSoRi リーダ，型番は RC-330，360，370 であった．これらの環境においては，大きな問題は発生せず，正常に稼働している．ただし，PaSoRi リーダは，初めて PC に接続する際に自動的にドライバをダウンロードする仕組みであるが，ネットワーク環境が不安定な場合，ドライバがダウンロードされず，正常に動作しないことがあるため，運用でカバーする必要があると考える．

6.4　試験運用の全体評価

システムの管理者は，セキュリティレベル 1 の試験運用では，利用者からの申請に応じて IDm とユーザ情報を登録する作業が必要であるが，セキュリティレベル 2 と 3 の試験運用では，利用者には PIN コードの発行処理を行い，PIN コードを通知するだけでよい．システム管理者は PIN コード生成方式を使うことにより，利用者情報の管理が不要となり，管理運用コストの削減につながる．

本研究で提案するシステムは一時利用者向けであるが IC カード未導入の組織や，IC カードが導入されている組織においても，応用できる仕組みである．現在，東京海洋大学では，学生向けに IC カードが導入されているが，教職員向けに IC カードは導入されていない．学内限定 Web サイトの学外からのアクセスの希望があるが，ID とパスワードによる認証だけでは安全性が確保できない可能性があることより，さらなる認証の強化が求められていた．このような組織においては，教職員が普段利用する一般カードを使用し，セキュリティレベルにより本研究で提案するシステムを利用することで，さらなる認証の強化が実現されることが期待される．

7.　まとめ

本研究では，一時利用者に対する管理運用の煩雑さおよびカード発行に関するコストを最低限に抑えるため，一時利用者には IC カードを発行せず，一般カードを使って，身分・所属ごとにそれぞれのシステムを利用できるようにするための仕組みを提案した．

それぞれのシステムに対しては，安全性確保のために，システムの重要性に応じてセキュリティレベルの格付けを行い，セキュリティレベル中程度のシステムを重点的に，設計，実装を行った．セキュリティレベル中程度のシステムで実装した PIN コードを使った認証方法は，PIN コード発行システムで PIN コードを発行するだけで，システム

が利用可能となり，システム管理者はユーザや PIN コード情報の管理が不要であり，容易に運用できる新しい PIN コード認証方法を提案した．セキュリティレベル 1〜3 において試験稼働を行った結果，大きな問題は発生せず，本研究の一般カードを使った認証システムにおいて，5.1 節で分類した 4 段階のセキュリティレベルのうち，一時利用者に求められるセキュリティレベル 3 までの安全性が確保できることが確認できた．

大学の組織の特徴より，一時利用者の全体数の把握は難しい．東京海洋大学において，一時利用者の正確な全体数を把握できていないが，1 年間における一時利用者数は，全構成員の約 1〜2 割であろうといわれている．また，IC カード身分証の 1 枚あたりの単価は 3,000 円前後であり，IC カードを発行すると発行手続きや失効に関する手続き，日々の管理において，運用コストが発生する．一時利用者は 1 年間に数百名から大学の規模により数千名の在籍が予想されることより，本システムの導入コストは発生するが，中長期的に運用することにより，コストが下がり運用の効率化につながる．また，一時利用者も IC カードを使ったシステムが利用可能になるため，利便性が向上する．

本研究における提案システムは，通常のカードリーダ以外には特別なハードウェアを必要としないシステムであり，導入コストは比較的小さい．また今回の提案システムは一時利用者向けに設計を行ったが，専用カードを導入していない組織において全構成員を対象に使用する等の応用も，対象とする認証システムのセキュリティレベルによっては可能であり，広範囲で利用され普及することによりさらなるコストダウンも期待できる．

近年，大学間連携のための認証基盤サービスが整備されつつある中，全学認証システムの強化を目指して，一般カードを使った認証システムの実装を行っていく予定である．また，本研究における実装は，FeliCa で行ったが，今後，他のタイプの IC カードでも利用できるようにすることにより，他社や他大学における IC カード身分証が利用可能となる．今後，大学間連携のための認証基盤サービスにも他大学所属の学生が所属大学の学生証でも利用できるようなシステムとして展開していく予定である．

謝辞　有益なご討論ご助言をいただいた東京農工大学総合情報メディアセンター櫻田武嗣博士，東京海洋大学海洋工学部古谷雅理博士に深謝する．

参考文献

[1] 江原康生：大阪大学における新全学 IT 認証基盤システムの構築と運用，電子情報通信学会論文誌 D，Vol.J95-D, No.5, pp.1172–1182 (2012).
[2] 飯田勝吉，新里卓史，伊東利哉，渡辺　治：キャンパス共通認証認可システムの構築と運用，電子情報通信学会論文誌 B, Vol.J92-B, No.10, pp.1554–1565 (2009).
[3] 清水さや子，横田賢史，戸田勝善，吉田次郎：東京海洋大学における IC カード学生証の運用・評価および今後の展開，学術情報処理研究，No.13, pp.64–73 (2009).
[4] 清水さや子，横田賢史，戸田勝善，吉田次郎：東京海洋大学における全学 IC カード導入と多機能化に向けた取り組み，学術情報処理研究，No.14, pp.149–152 (2010).
[5] 上原哲太郎，清水晶一，永井靖浩，古村隆明，喜多　一：大学における認証 IC カードの導入状況，情報処理学会研究報告—インターネットと運用技術 (IOT)，No.4, pp.253–258 (2009).
[6] 安浦寛人：九州大学全学 IC カード導入プロジェクト，九州大学大学院システム情報科学研究院 21 世紀 COE プログラム第 7 回研究活動説明会資料，pp.5–10 (2004).
[7] 京都大学情報環境機構：IC カード導入の効果，入手先 ⟨http://www.iimc.kyoto-u.ac.jp/ja/services/cert/iccard/merit.html⟩.
[8] 清水さや子，古谷雅理，横田賢史，櫻田武嗣，萩原洋一：大学における複数カードを用いた認証システムの設計，情報処理学会シンポジウムシリーズ，マルチメディア，分散，協調とモバイル（DICOMO2011）シンポジウム論文集，Vol.2011, No.1, pp.344–350, 情報処理学会 (2011).
[9] 島岡政基，片岡俊幸，谷本茂明，西村　健，山地一禎，中村素典，曽根原登，岡部寿男：大学間連携のための全国共同認証基盤 UPKI のアーキテクチャ設計，電子情報通信学会論文誌 B，Vol.J94-B, No.10, pp.1246–1260 (2011).
[10] 中村素典，山地一禎，片岡俊幸，西村　健，庄司勇木，古村隆明，岡部寿男：学術認証フェデレーションを活用するサービスの展開，第 27 回インターネット技術第 163 委員会（ITRC）研究会 CIS 分科会 (2010).
[11] 松平拓也，笠原禎也，高田良宏，東　昭孝，二木　恵，森祥寛：大学における Shibboleth を利用した統合認証基盤の構築，情報処理学会論文誌，Vol.52, No.2, pp.703–713 (2011).
[12] 大見嘉弘：FeliCa を用いた出席管理システムの開発と運用，東京情報大学研究論集，Vol.15, No.2, pp.69–81 (2012).
[13] 新長章典：非接触型 IC カードと携帯電話を用いた出席管理・授業支援システム，京都学園大学経営学部論集，Vol.15, No.3, pp.1–15 (2006).
[14] ならぽん，入手先 ⟨http://www.narapon.jp/⟩.
[15] スキャンロックアールエフ，入手先 ⟨http://www.scanlock.jp/scanlock_rf.html⟩.
[16] 総合型入退室管理システム「秘堰（HISEKI）」，入手先 ⟨http://www.hitachi.co.jp/products/urban/security/business/hiseki/index.html⟩.
[17] ジャストセキュリティ：FeliCa IDm（製造番号）の認証の危険性，入手先 ⟨http://justsecurity.ocnk.net/page/31⟩.
[18] TOPPAN FORMS：NFC ポータル，入手先 ⟨http://www.nfc-world.com/⟩.
[19] SONY: SDK for FeliCa User's Manual ver.1.24 (2004).
[20] SONY: FeliCa, available from ⟨http://www.sony.co.jp/Products/felica⟩.

清水 さや子　（正会員）

2011 年信州大学大学院工学系研究科修士課程修了．2011 年 10 月より京都大学大学院情報学研究科博士課程．現在に至る．修士（工学）．2005 年より東京海洋大学情報処理センター技術職員．2011 年より同技術専門職員．インターネットアーキテクチャ等に興味を持つ．

岡部 寿男　（正会員）

1988 年京都大学大学院工学研究科修士課程修了．同年京都大学工学部助手．同大型計算機センター助教授等を経て，2002 年より同学術情報メディアセンター教授．博士（工学）．インターネットアーキテクチャ，ネットワークセキュリティ等に興味を持つ．電子情報通信学会フェロー．システム制御情報学会，日本ソフトウェア科学会，IEEE，ACM 各会員．

吉田 次郎

1982 年東京大学大学院理学系研究科博士課程修了．理化学研究所研究員を経て，1984 年東京水産大学助手．1995 年同助教授，2003 年東京海洋大学海洋科学部教授．理学博士．大学に職を得て以来，情報処理センター運営に携わり，2008 年から 2012 年 3 月まで情報処理センター長．情報リテラシー，情報処理概論等情報処理教育に永年携わっている．