一般カードを用いた認証システムにおける ハッシュ関数を用いた PIN コード生成方式

清水さや子[†1†2]　岡部寿男[†1]　吉田次郎[†2]　戸田勝善[†2]

近年，様々な情報システムの利用のために， IC カードを使った認証システムを導入する組織が増えている．しかし，IC カードを導入する際に，カード発行や運用管理のコストが大きな課題となっている．そこで，本研究では，専用の IC カードを発行しなくても，本人が日常的に利用している一般の IC カードを使って，セキュリティレベルに応じて IC カードを使った認証システムが利用できる仕組みを検討している．セキュリティレベルが中程度以上の認証システムでは，カード内の読取可能情報と本人のみ知りうるキー情報（PIN コード）を組合せて認証を行う．通常，PIN コードを使って認証を行う際，一般カード内には PIN コード情報の格納が困難なため，認証サーバ内に格納する．それに対し本報告では，カード内にも認証サーバ側にもカード ID や PIN コード情報の登録を行うことなく，カードの登録時に PIN コードを発行するだけで，各種認証システムが利用可能になる「PIN コード生成方式」を新しく提案する．PIN コード生成方式は，IC カード内の読取可能情報から一方向性を持つハッシュ関数により自動で PIN コードを生成するため，カード ID や PIN コード情報の管理は不要になる．この方式を使うことで，一般カードを用いる際のカードの登録管理のコストが軽減できる．

Generating PIN by a hash function at authentication systems utilizing widely-used smartcards

SAYAKO SHIMIZU[†1†2]　YASUO OKABE[†1]
JIRO YOSHIDA[†2]　MASAYOSHI TODA[†2]

Recently, not a few organizations have introduced authentication systems based on smartcards in use of various information systems. However, when introducing a smartcard-based system, administrative works as well as initial cost of it become a serious issue. We have been considering an authentication system utilizing various types of widely-used smartcards that are used in daily life, according to the level of required security. Authentication systems in medium levels of security commonly utilize combination of PIN code and readable information in smartcards. It is difficult to register PIN codes in widely-used smart cards, and hence they are usually stored in the authentication server. In contrast, in our proposed method “PIN code generation”, a user can be authenticated ant can get access to the systems by just getting issued with a PIN code at registration of his smart-card, without storing either the card ID or the PIN code at the authentication server. In the method PIN codes are generated automatically by a one-way hash function from the readable information in the card, and it is not needed to manage information on smart-cards and PIN codes. Deployment of the proposed method will reduce the cost of registration and management of systems utilizing widely-used smartcards.

1. はじめに

近年，統合認証システムや SSO（Single Sign-On）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わせは，フィッシングやブルートフォース攻撃で破られる恐れがあるため, さらなる認証の強化のために IC カードが注目されている 3)4).

大学などの組織においても，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)7). しかし，大学などの組織で IC カードを導入する際，発行・管理する部署を巡って調整に多くの時間を要することや，利用者の身分・属性によって管理部署が異なることより，構成員の全てではなく一部のユーザに対してのみ IC カードが導入されていることがある．

さらに，大学という組織は，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渡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．このような組織では, 全学的に IC カードを導入した場合でも, 一時利用者にはカードを発行せず, 一時利用者は IC カードを用いたシステムが利用できない状態であることが多い．一般企業においても，業態によっては，部署ごとに契約している派遣社員や委託業務従事者, 取引先社員等が在籍し，入れ替わりが激しいため，全体把握が困難となることがある．そのような組織で，IC カードが導入された場合も大学の一時利用者と同じ問題が発生することが考えられる．

そこで，我々は，IC カードを，全体的に導入しているが一時利用者には発行していない組織，IC カードを導入していないが IC カードを使った認証システムを利用したい組織において，IC カードの管理運用の煩雑さやカード発行に

†1 京都大学
Kyoto University
†2 東京海洋大学
Tokyo University of Marine Science and Technology

ⓒ2012 Information Processing Society of Japan

関するコストを最小限に抑えるため，IC カードを発行せず，本人が日常利用する交通系やプリペイド決済用の IC カード等，共通規格に基づいて発行される IC カード（以下，一般カードとする）を使い，身分・所属ごとに認証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ている 8)9).

一般カードには，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読み取ることが難しく，認証に利用できる情報に制限があるためセキュリティ対策が必要になる．最近では，NFC（Near Field Communication）機能搭載の携帯電話の出現により，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ったため，カード内の読取可能な情報だけを認証に使用することは安全性が不十分である．そのため，本研究では，カード内の読取可能な情報に本人のみ知り得るキー情報（以下，PIN（Personal Identification Number）コードとする）による認証を組合せている．一般カードを使って 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，通常，PIN コード情報は認証システム側に格納し，認証システム側で管理すると考える．しかし，運用上の観点から，特に一時利用者向けとした場合は，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，管理に伴う人的コストが十分小さいことが求められること，利用者の管理部署は身分属性によって異なることより，カードの登録は分散して行いたいという要請がある．さらに，大学では，学部・学科等のセグメントごとの特徴を出すため，セグメントごとにシステムを管理していることや，離れた研究所等においてはネットワークが分離されている場合も多くあるため，中央管理の認証サーバで一元管理することは必ずしも容易ではない．そのため，中央管理の認証サーバを前提とせず，それぞれのセグメントや部署ごとに管理するモデルでも利用できるシステムとすることより，それぞれの管理者が比較的容易に管理できるよう，認証システム内に格納する情報は必要最低限にすることが求められる．

本報告では，これらを検討した上で，カードにも各認証システムにもカード固有の情報（カード ID）や PIN コード情報の登録を行うことなく，PIN コード発行システムと PIN コード検証システムに PIN コードを生成する式だけを格納すればよい，**PIN コード生成方式**を提案する．PIN コード生成方式は，カード内の読取可能情報から取り出したカードごとに異なる値にハッシュ関数を適用することにより，PIN コードを生成する手法である．この方式は，システムにユーザ情報や PIN コード情報の登録を行うことなく，一般カードに対して，PIN コードを発行するだけで，認証システムが利用可能になる．また，この方式にすることにより，様々な情報サービスが組織で分散管理されている場合，登録や管理のコストが軽減できる．

現在，IC カードが学生向けだけに導入されている東京海洋大学において，本提案方式を元に，全構成員が IC カードを使った認証が利用できるよう，一部で試験稼働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が整備されつつあることより 10)11)12)，本提案を実現しつつ，全学認証システムの強化を目指している．

2 章では，IC カードを使った認証システム導入の要件について述べ，3 章では，提案するハッシュ関数を用いた PIN コード生成方式について，4 章では，PIN コード生成方式の実装と評価ついて述べ，最後にまとめを述べる．

2. IC カードを使った認証システム導入の要件

2.1 各種情報システムを分散管理する組織

大学という組織では，学生や教職員以外に，研究室で雇用する短期間の非常勤職員，派遣契約者，企業からの研究員等，様々な身分の一時利用者が様々な期間在籍している．学生は学務担当係，教職員は人事担当係，派遣契約者は経理担当係等，身分属性ごとに管理部署が異なる．さらに，一時利用者の管理部署が多部署に渡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，大学において，提供するサービスは，全学向けのサービスの他に，学部・学科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．これらの情報サービスの全てが中央で一元管理しているのではなく，学部・学科等のセグメントごとに個別に管理している場合が多い．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だけでなく，学部や学科ごとに個別に特性を出すためでもある．企業においても組織規模が大きくなると，独立した部署や離れた場所に研究所があり，情報システムも個別に管理している組織もある．このような組織では，IC カードを使った認証システムを導入する際，中央に認証サーバがあれば，そこに認証に必要な情報を集約し，それぞれの部署で個々に管理する情報システムでは，認証時に，中央で管理する認証サーバを参照できることが望まれる．

しかし，このような場合，常に中央管理の認証サーバとの通信が必要になる．大学で提供するサービスは，個別に独立して運用されていることも多く，特に，地理的に離れた山奥や離島，実習船内等，中央管理のシステムと常時通信ができるわけではない場所の場合も多い．これらより，中央で管理する認証サーバとの通信が切断されていても，利用できるシステムであることが求められる．

また，カード情報等の登録は，身分属性ごとの管理者が，中央で管理する認証サーバにアクセスし，登録情報を格納できればよい．しかし，一時利用者の中には，大学と雇用関係を結んでおらず，それぞれの部署で個別に契約している人も含まれているため，彼らの情報を中央で管理する認証サーバに登録するかどうかの取り決めや手続き等に多くの時間を要することが多い．

このような背景より，本報告では，部署ごとに管理する情報システムが中央管理の認証サーバと接続されていなく

ⓒ2012 Information Processing Society of Japan

ても利用できるサービスとするため，それぞれの部署のシステム管理者が比較的容易に管理できる認証システムを目指す．

2.2 IC カードを用いた認証システムの要件

IC カードを発行する際，カード発行のコストだけでなく発行後の運用管理の煩雑さも発生する．本研究ではこれらを最低限におさえるため，専用の IC カードを発行せずに，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 カードを使って，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検討している．

一般カードは，専用カードに比べ，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．要求されるセキュリティレベルが比較的低くカードの製造時に発番される番号を認証に利用するような認証方式は，既に入退館システム等で製品例がある．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 13)14)．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 15)，FeliCa 搭載の携帯電話，運転免許証（ISO/IEC14443 TypeB 準拠），taspo（ISO/IEC14443 IC カードのタイプは TypeA 準拠）カードなど身の回りの各種 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 16)17)．

これらのシステムは，カード内の読取り可能領域からカード毎の固有の情報（カード ID）を抜き出して認証に使用している．従来，SONY より Felica のカード ID である FeliCa IDm の認証の危険性が提言されていたが 18)，FeliCa タイプのカードは複製が困難であると言われていたため，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，様々な製品で使われていた．ところが，近年，NFC 機能搭載の携帯電話が市場に出てきている 19)．NFC 機能搭載の携帯電話は，リーダ機能も搭載されており，IC カードの基本情報をエミュレーションすることが簡単にできる．この技術が悪用された場合，NFC 機能搭載の携帯電話に IC カードをかざすとカード内の読取り可能情報を取得し，携帯電話がそのカードに成りすますことができる．これらより，認証時にカード内情報のみを使用する場合，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来た．

これらより，一般カードを使った認証では，要求されるシステムのセキュリティレベルが中程度以上の場合，一般カード内の読取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，その他の認証情報を組合せることが必要であると考える．

2.3 本研究で想定するサービス

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，Web サイトの閲覧等，各種情報システムの利用で利用されている．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が行われている．セキュリティレベルが中程度以上のシステムに対して設計を行うことより，本研究では表 1 のサービスを想定する．

表 1　本報告で想定するサービス

Table 1　Systems simulating in this report

項	想定するサービス	認証に必要な情報	認証に必要なもの	セキュリティレベル
(1)	学内限定簡易 Web サイトの学外から閲覧（カード認証）	・読取可能情報 (IDm 等) ・PIN コード	・IC カード, ・PIN コード ・PC,カードリーダ, ・インターネット環境	中
(2)	学内限定ポータル Web サイトの学外から閲覧（カード認証）	・読取可能情報 (IDm 等) ・PIN コード, ・ID&PWD	・IC カード, ・PIN コード ・PC,カードリーダ, ・インターネット環境	中上
(3)	利用者限定の比較的重要部屋の出入り	・読取可能情報 (IDm 等) ・PIN コード	・IC カード, ・PIN コード (備付の専用リーダ)	中

本報告で想定するサービスの具体例としては，PC を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 Web サイトを，学外ネットワークから閲覧する際に，カードリーダ付き PC と一般カードを使ってカード認証を行うシステムとする（表 1）．学内限定の制限は，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，機密性の高い情報ではなく，簡易な学内スケジュール等を掲載するサイトする．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し，セキュリティレベル中程度とする．表 1 の項(1)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，個々のアカウントによる認証を追加する．これが表 1 の項(2)である．項(2)は，学内限定という制限だけでは不十分なため，個人認証を必要とするポータルサイトのようなサイトとする．また，本研究で実装するサービスは，(1),(2)とするが，(3)のとおり，利用者が限定されるような比較的重要な部屋の出入りなど，セキュリティレベルが中程度以上の入退館システム等においても応用できるものである．

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 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．

2.4 一般カードを使った認証方法

一般カードを使った認証方法は，大きく 3 つパターンが

ⓒ2012 Information Processing Society of Japan

考えられる（表 2）.

表 2 の[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であり，一般カードでの利用は困難のため，本研究においては検討を省略する．[2] ②は，2.2 節で述べたとおり，NFC 機能搭載の携帯電話による偽装などによる複製や,紛失時の悪用の問題がある．そこで，本研究で対象とす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，カード内の非暗号化領域の情報にその他の情報を組み合わせる方法（[3]）を検討する．指紋など生体情報を利用する方法（[3]①）も考えられるが，個人情報の取り扱い等を考えると，比較的導入に抵抗がない PIN コードのキー入力による認証（[3]①）が妥当であると考える．

表 2　一般カードを使った認証方法

Table 2　Authentication methods by using smart card

項	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

以下，一般カードを使った認証方法において，本人しか知りえないキー情報（PIN コード）の登録方法，配布方法，それに伴う管理・運用方法を様々な方面から検討を行う．

3. ハッシュ関数を用いた PIN コード生成方式の提案

3.1 PIN コードを使った認証方式

3.1.1 従来方式

これまでのカードと PIN コードを使った認証システムは，PIN コード情報をカード内に格納する方式，もしくは，認証サーバ内に格納する方式であった．PIN コードを一般カード内に格納する方式は，2.4 節のとおり安全性が確保されるが，それぞれのカード発行会社と重要な取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．一方，PIN コードを認証サーバ内に格納する方式の場合，2.1 節のとおり，中央管理の認証サーバにカード ID や PIN コード情報を格納しておき，各部署が管理する認証システムから認証時に参照されることが求められる．しかし，その場合は，ネットワークが常に中央管理のシステムと接続されている必要があるが，大学によっては，中央管理のシステムとネットワークが独立している部署がある．また，中央管理のシステムにカード情報や PIN コード情報を登録する際，大学として把握できていない一時利用者の情報を登録することが困難であるという問題がある．

さらに，運用上の観点より，一般カードを使って情報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．これらより，中央管理のシステムとは別に，部署ごとに管理するシステムで，部署ごとのシステム管理者が容易に管理できるシステムが求められる．

3.1.2 PIN コード生成方式の提案

上記より，本報告においては，各認証システム側に，一般カードに関して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，カード ID から一方向関数により 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（図 1）.

PIN コード生成方式は，利用者や管理者が PIN コードを決定し設定する代わりに，システムが自動的に生成したものを利用者に発行する仕組みである．PIN コードを発行するだけで，認証システムが利用可能になる新しい PIN コードの生成方式である．提案する方式は，認証システム側にカード情報や PIN コード情報の登録を行わず，PIN コード生成式を格納するだけよいため，従来方式に比べて利用者ごとの PIN コードの管理や登録作業が不要であり，比較的コストを抑えることができる．ただし，PIN コードの値は自由に設定することができないため，運用でカバーする必要がある（表 3）.

図 1　PIN コード発行の流れ

Figure 1　Outline of PIN code issuing

表 3　一般カードの認証方式と特徴

Table 3　Authentication methods and characteristics of the widely-used smart cards

	認証システム内に格納する方式（従来方式）	PIN コード生成方式（提案方式）
コスト	大	小
登録作業	必要	不要
安全性	高	中程度
PIN コード値	自由に設定可	設定不可
その他	認証システム内に PIN コードの管理が必要	PIN コード発行すればシステム利用可に

本研究で想定するサービスは，2.3 節のとおり，個人 PC にリーダを接続し，学外から学内限定 Web サイトへのアクセスだけでなく，セキュリティレベルが中程度の入退館システム等でも利用可能である．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場合は，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．

ⓒ2012 Information Processing Society of Japan

3.2 PIN コード生成方式

PIN コードを生成する際に，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，異なる値を含めた値を抜出し，少し工夫を加えることにより，PIN コードを生成する．

PIN コードの生成方法を以下に記す（図 2）．

1．一般カードの読取可能な情報から値を抜出す
（カードごとに異なる情報を含んだ値とする）
2．抜出した情報を組み合わせる　（→ n とする）
3．秘密情報として SALT を付加する
4．ハッシュ関数（一方向関数）HASH によりハッシュ化する
5．任意の桁数を抜き出す

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

Figure 2　The formula for PIN code generation

この生成式では，一方向関数に秘密情報を組み合わせていることにより，カード内から抜出した情報だけからでは PIN コードの生成ができない．また，PIN コードが漏えいした場合でも，他の利用者の PIN コードは推測できないため，当該利用者以外への影響を防ぐことができる．後で述べるように PIN コードの有効期限をつける場合には，秘密情報 SALT を変更することにより，新しい PIN コード体系に移行できる．

3.3 運用手法の検討

IC カードと PIN コードを使って認証システムを運用する際，運用時の工夫が必要となる．提案する認証システムに対して，起こりうるインシデントのパターンとリスクを分析し，それに対する対応とコストを比較し，悪用の可能性を最小限にするための方法を，実現可能な範囲で検討する．起こりうるインシデントとして以下の 3 パターンを考える．

- パターン 1：カードの紛失・偽造
- パターン 2：PIN コードの紛失・漏えい
- パターン 3：カードの紛失・偽装と PIN コードの同時紛失・漏えい

3.3.1 パターン 1：カードの紛失時・偽装時

基本的にはカードだけでは，PIN コードが分からないため，利用できないため，新しいカードで PIN コード発行手続きを行えばよいと考える．ただし，カードの悪意の取得者・偽装者による PIN コード悪用の恐れ（何度も試してのブルートフォース攻撃等）がある．その対応として，PIN コード認証時には入力回数の制限をつけて，入力制限を越えると，該当カードよりカード失効処理に必要な情報を抜出し，自動で失効処理を行えるようにすればよい．もしくは，都度，管理者にアラートを上げ，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えばよいと考える．これらは，通常の運用コスト以外に，管理者側が作業するコストが発生する．また，悪用ではなく本人が誤って入力回数の制限を越えて失効処理された場合，失効の解除の作業が必要になる．

3.3.2 パターン 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，再発行を行えばよい．ただし，カードを偽装している等の悪用の恐れがある場合は，該当カードに対してカード失効処理を行えばよいと考える．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 コードを配布し直せばよい．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．通常の運用コスト以外に，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．

3.3.3 パターン 3：カード紛失時・偽装時と PIN コード紛失時・漏洩時

これはパターン 1 や 2 に比べて，悪用の恐れが高いため，緊急性が高く，直ちに失効処理を行う方がよいと考える．ただし，執行処理を行う際，失効処理に必要な情報は当カードより抜出し，緊急対応のためのコストが必要となるが，カードと PIN コードの両方一度に紛失することは滅多に起こらないと考えるため，通常運用においては滅多にコストは発生しないと考える．

3.4 本研究で運用する手法

パターン 1 の対応として，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，失効の度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．パターン 2 の対応として，定期的に PIN コードの更新を行う必要があるが，1 年のうち人の入れ替わりが一番多い年度末に行うのが良いと考える．PIN コードの更新は，SALT を変更することにより新たな PIN コードを発行する．PIN コードの更新時には 2 週間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．PIN コード更新手続き期間による混乱を避けるため，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 コードの両方が利用できるように設定する．また，PIN コード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 PIN コード発行申請をし直すことで，新しい PIN コードが利用できる．不正利用は PIN コードの更新時に失効リストの更新時期もすればよいと考える．

パターン 3 においては，失効処理を行う際，紛失の申請時点に，カード内から失効処理に必要な情報を抜出すが，

ⓒ2012 Information Processing Society of Japan

本提案は，PIN コードの管理は行わなくてよいサービスであることより，該当カードが存在しない場合，該当カードの失効処理が困難になる．これらを厳格に管理したい場合は, PIN コード発行時にユーザ情報やカード情報を登録し，管理すればよい．ただし，情報の運用管理には多額のコストが発生する．カードと PIN コードの両方を一度に紛失・悪用されることは, 滅多に発生しないものと考えることと，本研究における提案では運用管理のコストは最低限にしたいことより，本サービスの利用は，セキュリティレベル中程度の Web サイトの閲覧程度とし, パターン 3 に対する対応は行わないこととする．

4. PIN コード生成方式の実装

本研究で提案する PIN コード生成方式を元に，PIN コード発行システムと PIN コード検証システムを構築した．両システムには PIN コード生成用もしくは検証用のプログラムだけではなく，SALT と失効リストを格納する．PIN コード発行システムは管理者が，PIN コード検証システムは利用者が，Web ブラウザ経由で利用する．

4.1 PIN コード発行システム

PIN コード発行時，管理者用 PC から Web ブラウザ経由で PIN コード発行システム内の PIN コード発行用 URL（管理用）にアクセスし, PIN コード発行用の画面を表示する．初期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，PIN コードを生成し，PIN コード情報，等，認証時に必要な情報を返す（図 3）．

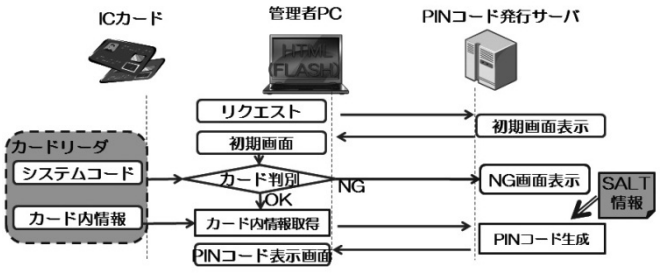

図 3　PIN コード発行フロー

Figure 3　Flow of PIN code issuing

4.2 PIN コード検証システム

PIN コード検証システム利用時，利用者は個人 PC から Web ブラウザ経由で検証システム URL にアクセスし，初期画面を表示する．初期画面で表示されるメッセージには「カードリーダに一般カードをかざしてください」と表示し，メッセージに従い，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，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 コードの検証に必要な情報を抜出し，検証システムに送る．検証システム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の照合を行い，失効リスト情報と合致しない場合は，認証成功となる．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出し，自動で失効リストに追加する（図 4）. 図 4 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．

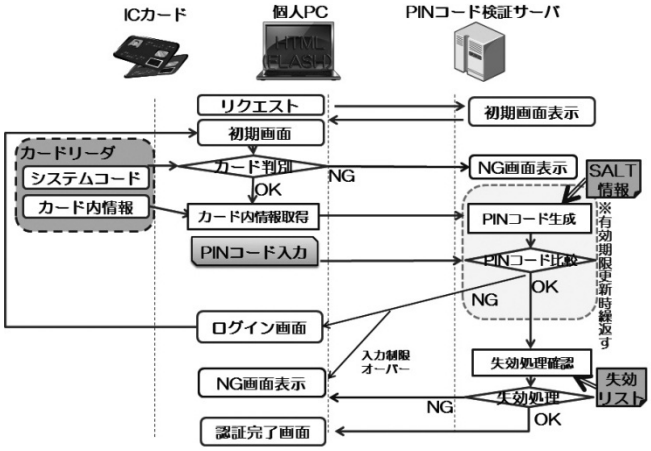

図 4　PIN コード認証フロー

Figure 4　Flow of PIN code authentication

4.3 実装したシステムの評価

本研究で実装した PIN コード発行システムおよび検証システムは，ユーザ情報やカード情報，PIN コード情報等は格納せず，PIN コード生成式による発行プログラムと検証プログラムのみ格納する．ただし，失効処理を行ったカードの失効処理はプログラムを修正しなくても容易に処理できるよう，別のファイルファイルとして格納する．また，SALT 情報も都度変更するものであるため，別ファイルとして格納する．

本システムは，運用管理におけるコスト削減を目指すことより，PIN コードを発行すれば，該当サービスが利用できるシステムである．2.3 節の項(1)のサービスを利用する際, 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となる．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．一度発行した 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．そのため，セキュリティレベルが中程度以上の 2.3 節の項(2)のようなサービス利用時は，PIN コード認証を行ったあとに，メインの認証として ID とパスワード入力を行う．

ⓒ2012 Information Processing Society of Japan

PIN コード認証により，ID とパスワードによる認証画面までは閲覧できるが，ID とパスワードを厳格に管理することにより，セキュリティを確保できる．ただし，2.3 節の項(3)の場合のように，建物ごとに入館者を区別し，入退館履歴等を残さなければならないシステムや，さらに高いセキュリティレベルが求められる場合は，登録時に個々の情報を登録する必要がある．ただし，運用管理において多くのコストが必要になる．本提案方式は，運用管理におけるコスト削減を重視しない場合，PIN コード発行の際にユーザ情報等を登録することで，さらに高いセキュリティレベルのサービスでも利用可能となる．

本提案では一般カード内の情報に基づき，PIN コード生成方式により発行するため，ユーザが自由に設定できない．ユーザが長期間利用しない場合等，忘れる可能性があるため，運用方法の検討が必要となる．また，本提案では，失効処理されたカードは，PIN コードの更新期間まで利用できず，新たなカードに PIN コードを発行して利用する必要がある．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．

4.4 試験環境の構築

本研究の試験稼働として，2.3 節の項(1)(2)のサービスを試験環境の構築を行った．項(1)のセキュリティレベルが中のシステムはカードリーダが接続された個人 PC から一般カードと PIN コードによる認証とする．項(2)のセキュリティレベルが中上のシステムは，同じく個人 PC から一般カードと PIN コードによる認証を行うが，PIN コード認証に成功後，Web ブラウザ上での ID とパスワード認証を併用する．試験環境は，東京海洋大学の一セグメントにて既に稼働している学内限定の Web サイトと学内限定のポータルシステムに対して，既存システムに手を加えず，学外からアクセス時にリーダ付き個人用 PC から IC カードと PIN コードを使った認証システムを構築した．

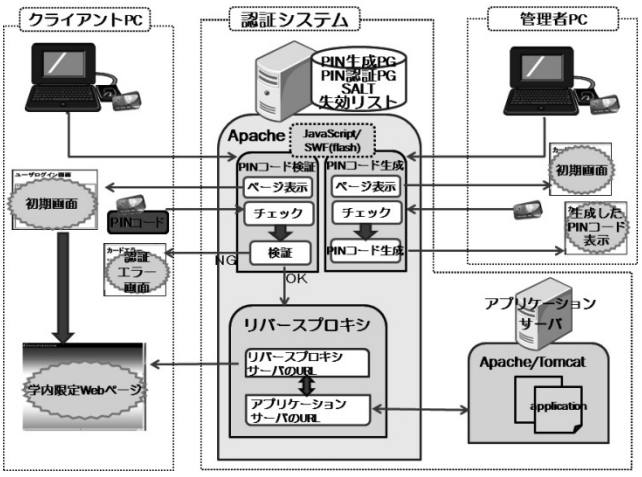

図 5　試験環境の構成

Figure 5　Overview of the prototype

新しく構築したものは，リバースプロキシサーバであるが，リバースプロキシ上で，4.2 節の PIN コード認証用のプログラム，失効リスト，SALT を設置して，PIN コード認証を行う（図 5）．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，PIN コード発行システムは同じくリバースプロキシサーバ上で稼働する．

本システムの開発環境には，SDK for NFC Adobe AIR Flash Basic 1.3.0，Perl 5.16 を用いた．

4.5 試験環境における PIN コードの発行方法

試験稼働における PIN コードの発行方法は，組織内の複数部署で，それぞれの部署が個別に利用者を制限できるよう，システムごとにそれぞれ異なる PIN コードを発行する仕組みとした．サービスごとに異なる SALT を設定することで異なる PIN コードを発行する．本システムは，それぞれの部署で個別に利用者を制限して運用する場合は，今回の方法でよいが，サービスの提供部署が異なっても組織の PIN コードを一つに統一したいような場合は，中央管理のシステムで，PIN コード発行システムを立ち上げ，発行の際にアクセスすればよいと考える．現在は利用者が少ないため，PIN コードの発行は管理者が個別に行えるが，利用者が増えた場合，新たな PIN コード発行方法の検討が必要となる．

4.6 試験運用の稼働と評価

2012 年 11 月より東京海洋大学の 1 セグメントにおいて試験稼働で構築したシステムを開始した．現在 15 名程度が利用しているが，大きな問題は発生していない．試験稼働当初，PIN コードは 6 桁としていたが，覚えられず携帯電話等にメモを残す人が多いため，現在は 4 桁で運用している．PIN コードの有効期限は 1 年とし，PIN コードの入力回数の制限は 15 回としている．ハッシュ関数は SHA-1 を使用している．利用者は，Windows 搭載のノート PC ソニー製非接触 IC カードリーダ(RC-S360/SH)を接続するか，リーダ付きノート PC から使用している．OS は Windows7 もしくは XP を使用しており，ブラウザは IE，Firefox，GoogleChrome のいずれかで使用しているが，大きなトラブルは発生していない．初回利用時のみ，IC カードリーダを初めて PC に接続する場合，自動でドライバーをダウンロードする動きがあるため，ネットワークが不安定な環境においては，ドライバーがダウンロードできず，カードが認識できないことがあるようである．これについては，マニュアルを作成する等して運用でカバーできる範囲である．

4.7 本格導入に向けて

現在，東京海洋大学では，学生向けには 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．しかし，学内限定の Web サイトやポータルシステムの

ⓒ2012 Information Processing Society of Japan

学外からのアクセス希望が多く，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，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，今後，利用サービスの拡大が期待される．

5. まとめ

本研究は，IC カードを導入する際，カード発行コストや運用管理コストを軽減するため，IC カードを発行せず，普段利用する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検討していた．そこで，セキュリティレベルが中程度以上システムに対して，カードの紛失や偽装の対策を考慮し，PIN コード認証を併用することにより，PIN コードを使った認証方式を検討していた．

本報告では，PIN コードの発行について，カードにも認証システムにもカード情報や PIN コード情報の格納することなく，カード内情報から一方向関数を使って PIN コードを生成する PIN コード生成方式を新しく提案した．認証システム側に PIN コード生成式を格納するだけよく，PIN コード生成方式は，PIN コードを発行するだけで各種認証システム利用できる．この提案方式は，従来方式に比べて利用者ごとに PIN コードの管理や登録作業が不要となる．本システムは多少の導入コストが発生するが，新たにカード発行コストやカード回収のコストは削減するため，長期的には運用コストが下がることより，運用の効率化につながる．本報告では，カード発行や登録管理のコスト軽減を踏まえ，セキュリティレベルが中程度のシステムを中心に実装を行ったが，PIN コード発行の際にカードや PIN コード情報等を認証システム側に登録し，管理することで，さらに高いセキュリティレベルのサービスでも利用可能となる．使用する認証システムのセキュリティレベルによって広く応用できるシステムであると考える．

本システムの提案は，IC カードを全体的に導入しているが一時利用者には発行していない組織，IC カードを使った認証を行いたいが導入が困難な組織向けに行った．本提案は，製品例で記したサービスにおいても，セキュリティレベルが合致すれば利用できる等，幅広く利用できるシステムである．

また，本報告における実装は，FeliCa で行ったが，今後，他のタイプの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 カードでもサービスが利用可能となる．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できることを期待する．

謝辞　東京農工大学総合情報メディアセンター櫻田武嗣助教には有益なご討論ご助言を戴いた．また，本研究の試験稼働に向けて東京海洋大学情報処理センターの非常勤職員の諸氏には，多くのご協力を戴いた．ここに感謝の意を表する．

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.5,1172-1182,2012
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, 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, 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），4，253-258
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,5-10,2004
7)　京都大学情報環境機構”都大カード導入の効果” 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 Vol.2011,No.1,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,情報処理学会,344-350
9) 清水さや子，岡部寿男，吉田次郎「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」情報処理学会シンポジウムシリーズ Vol.2012,No.1,マルチメディア,分散,協調とモバイル(DICOMO2012)シンポジウム論文集,情報処理学会,675-683
10)　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.10,1246-1260,2011
11)　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
12)　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 52(2), 703-713, 2011
13)　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 , 69-81（2012） 69
14)　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 第 15 巻, 第 3 号, 1-15，2006
15)　ならぽん：http://www.narapon.jp/
16)　スキャンロックアールエフ：http://www.scanlock.jp/scanlock_rf.html
17)　総合型入退室管理システム「秘堰(HISEKI)」: http://www.hitachi.co.jp/products/urban/security/business/hiseki/index.html
18)　ジャストセキュリティ”FeliCa IDm（製造番号）の認証の危険性”http://justsecurity.ocnk.net/page/31
19)　TOPPAN FORMS ecur ポータル”：http://www.nfc-world.com/

ⓒ2012 Information Processing Society of Japan