大学における複数カードを用いた認証システムの設計

清水さや子[†]　古谷雅理[†]　横田賢史[†]
櫻田武嗣[††]　萩原洋一[††]

大学は学生や教職員，留学生，共同研究員や企業関係者等の様々な身分の人で構成されており，管理部署が統一されていない場合が多い．そのため IC カードを大学全体で導入する場合には学生，教職員以外の構成員に対して，どのように IC カードを発行するかが問題となる．人の入れ替わりが激しいため，IC カード発行の手間やコストも問題となる．そこで本稿では，学生，教職員以外に対して大学としては IC カードを発行せず，利用者本人が既に所持しているであろう交通系の IC カード等を使い，それらを大学の IC カード認証基盤と結びつける方法を提案する．大学発行の IC カードと交通系 IC カードの利点を組み合わせた大学全体としての IC カードによる認証基盤を構築し，運用面における効率化および利用者の利便性の向上を目指す．

Design of authentication system using several types of IC card at university

SAYAKO SHIMIZU[†]　TADASUKE FURUYA[†]　MASASHI YOKOTA[†]　TAKESHI SAKURADA[††]　YOICHI HAGIWARA[††]

In this paper, we designed an authentication system which is used several types of IC card at a university. In the university, there are people of various position such as a student, a teacher, the staff of a school, a foreign student, a coworker. And it is managed in a bureau according to each. In addition, the replacement of the person is intense. Therefore, when you use a IC card system in the whole university, you must publish a IC card frequently, and the expense of the card and costs of the management increase. Our suggestion system is accepted several types of IC card, such as campus IC card published by university, traffic ticket IC card published by railroad. Thus, our suggestion is able to reduce the cost when the authentication system is used at whole of a university.

[†]東京海洋大学　情報処理センター
Information Processing Center, Tokyo University of Marine Science and Technology
[††]東京農工大学　総合情報メディアセンター
Information Media Center, Tokyo University of Agriculture and Technology

1. はじめに

近年情報化が進み，様々なシステムが電子化されている．これまでは，それぞれのサーバやネットワークごとに別々の ID やパスワードを発行して利用されることが多かった．しかしながら，システムが増えてくると，利用者も管理する側も複数の ID やパスワードを管理しなくてはならず，手間が増える．そのため，統合認証システムを積極的に導入するケースが増えつつある．統合認証は効率化の面では多大な効果があるが，ID とパスワードの組み合わせだけの場合は，一度破られてしまうと他のシステムまで被害が及ぶという危険性がある．そこで，物理デバイスとして IC カードが注目されている．IC カードを物理的な鍵として利用することで，セキュリティを高める方法である．他大学においてもセキュリティ向上以外にもその他の利便性を含めて IC カードを運用開始している例も多くみられるようになってきている[１][２].

IC カードの全学導入は簡単にできそうに考えられるが，導入には大きな壁がある．多くの大学では，学生や教員，職員以外にも，留学生，研究生，短期採用の非常勤職員，共同研究者などが多数出入りしている（以下，一時利用者と記す）．これら一時利用者の利用期間は比較的短いことが多く，管理部署は一カ所に統一されていないため，現状を把握することでさえ難しい．そのため，大学において全学的に IC カードを導入する場合，一時利用者の扱いについて問題となることが多い．そのため，人員が管理されている企業と同様に IC カードを発行することは困難であった．

東京海洋大学（以下，本学と記す）では，2006 年より IC カード学生証を導入した[３]．これは TypeB コンビネーションタイプの IC カードのため，システム運用コストが高い点，他の用途への展開が難しい点が問題であった．そこで 2010 年 2 月に FeliCa ハイブリットタイプに一斉更新を行った[４]が，学生証としての利用にとどまっていた．教職員証については未整備のため，IC カード教職員証の導入に向けて検討を始めている[５]．また東京農工大学では教職員のみ FeliCa タイプの IC カードを導入しており，学生への展開を検討している．いずれの大学も一時利用者に対して IC カードをどのように発行するかが問題となっていた．

そこで本稿では，一時利用者には大学の IC カードを発行せず，利用者本人が所持している交通系 IC カード（以下，一般カードと記す）を使い，別途決められている利用権限に応じて，大学カードと同様に認証システムを利用できるシステムの設計について述べる．本稿で述べる仕組みを実現することで，コストを抑え，全学的に IC カード用いたシステムを利用できるようになる．

2. 大学発行カードと一般カードの比較

大学で発行したカードは大学固有に安全性を考慮して発行しているため，セキュリ

ティは比較的高く，大学が独自にアプリケーションを追加できるといった利点がある．このため，大学発行カードだけで運用するのが望ましい．しかしながら前述のように大学は人の入れ替わりが激しく，発行の度に手間やコストがかかるといったデメリットがある．一方，一般カードは FeliCa を持っていれば良く，新規発行は大学で行わない為，発行時のコストは不要となる．しかし，落とした場合の対応が難しく，中身の書き換えもできない為，自由に新サービス提供することが難しい．また，身分証とするためには，券面に表示も必要となるため，一般カードだけで運用することも難しい．そこで，本研究では，大学カードと一般カードの両カードのいいところを組み合わせて，設計することとする．

本稿で述べるシステムは，初回の開発コストは単独のカードを利用する場合に比べて開発コストがかかるが，長期的にみた場合，一時利用者が多い場合，カードコストを下げることができるため，全体的としてはコストが抑えられると考えられる．

上記の点をまとめたものを表 1 に示す．

表 1　各種カード導入場合の比較表

	大学カード	一般カード	大学カード＋一般カード システムコードなど
セキュリティ	○	△	○
発行コスト	大	小	大
利点	セキュリティ高い カードの中身を書換可	Felica を持っていれば良い 新規発行に発行費不要 （大学で新たに発行不要）	大学カード,一般カードの 利点いいとこ取り可
欠点	大学の場合人の入替り激しい(非常勤,アルバイト,短期留学,研究受入れ etc) ↓ 発行の手間大	落とした場合の対応が難しい 中身の書き換えが出来ない ↓ 新サービスが生み出せない	開発コスト大

3.　大学発行カードと一般カード利用時の安全性の検討

本稿では，交通系 IC カードの利用を想定している点，本学では FeliCa ハイブリットタイプの IC カードの導入をはじめている点を踏まえ，FeliCa カードを利用した場合について検討する．

3.1　FeliCa の構造

FeliCa では，エリアとサービスという概念が導入されている．これは，カードに複数の事業者が相乗りすることを前提に設計されているためで，エリアと呼ばれる機能が各事業者間のセキュリティファイアウォールの役割を果たし，サービスがメモリ上にアクセスする際の方法を定義している．

FeliCa 内のメモリ管理は 16 バイト毎に行われており，この 16 バイトの基準単位をブロックと呼ぶ．ユーザがメモリにアクセスする際には，エリアコード・サービスコードと呼ばれる 2 バイトのコードを使用する．また，FeliCa 内のメモリはユーザーデータが書き込まれるユーザブロックと，FeliCa の構成情報が格納されているシステムブロックと呼ばれる領域に分けて管理されている[６][７].

3.2　大学発行カードと一般カード

先述のように FeliCa の格納情報は，ユーザブロックとシステムブロックに分かれている．本学の場合，大学カードのユーザブロックには，大学が発行する氏名，学籍番号や教職員番号，有効期限等，身分証として必要な情報の他，認証時に利用するユーザ ID 等の大学固有の情報を格納している．これらは，FeliCa 共通利用フォーマットである FCF（FeliCa Common-use Format[*a]）に追加する形で IC カードへ格納している．ユーザブロックの一部は暗号化して格納しているため，その部分は PaSoRi リーダではなく専用リーダ・ライタを使用する必要がある．

一般カードのユーザブロックには，例えば Suica 定期券[*b]の場合，氏名，性別，生年月日などの個人情報の他，利用日付，入出駅，残高などの情報が専用アプリケーションとして格納されており，PaSoRi リーダ[８]等と専用アプリケーションを PC にインストールすれば利用履歴については確認することができる[９].

いずれのカードもシステムブロックには，製造時に発行される ID やユーザブロックの情報作成時に発行されるコード情報等が格納されており，PaSoRi リーダ等で読み取り可の情報と不可の情報が存在する．

3.3　FeliCa のシステムブロック内情報

FeliCa を利用したシステムの場合，システムブロック内データが使われることも多い．システムブロック内の情報と暗号化の有無について表２に示す．

[*a] FCF は FeliCa 共通利用フォーマット推進フォーラム組合の登録商標である．学生証・教職員証など教育機関向け仕様 FCF キャンパスカードフォーマットでは，身分や学校を識別できる．

[*b] 鉄道，バス，買い物等で利用できる JR 東日本が発行する FeliCa タイプの IC カード．

表 2　システムブロック内情報における安全性

	暗号化	相互認証	カードリーダ
製造 ID	無	無	PaSoRi リーダ等
システムコード	無	有	PaSoRi リーダ等
エリア	無	有	PaSoRi リーダ等
サービスコード	無	有	PaSoRi リーダ等
発行 ID	有	有	専用リーダ

製造 ID は暗号化されておらず，相互認証もないが，基本的には改竄ができないコードであるため，安全性が高いと言われている．そのため，FeliCa を導入する場合，製造 ID を認証に使用するケースも少なくない．ただし，安全性が確実であるとは言い切れないため，電子マネー等重要な認証においては製造 ID に発行 ID が併用される場合もある．

システムコード，エリア，サービスコードは PaSoRi リーダを使っても相互認証した後で読み込むため，コード自体に信頼性がある．そのため，比較的安全であるといえる．

発行 ID は交通系 IC カードに埋め込まれて発行されるコードである．発行 ID は暗号化されており，専用の読取リーダと専用ツールでなければ読み取ることができない．取扱については，発行元において厳重な規定があることと，現状では，専用モジュールを入れた専用リーダでしか読み取りできないため，PaSoRi リーダ等で接続した PC からは利用不可することができない．

このため，一般カードを PaSoRi リーダ等から利用する場合には，製造 ID とシステムコード，エリア，サービスコードを組み合わせて取得し，認証に利用すれば良いと考えられる．

4.　大学発行カードと一般カードの併用

一般カードの領域に空きがあっても，大学のユーザ ID 情報等を追加することは難しく，現実的ではない．したがって本稿では，一般カードにユーザ情報等を格納することは考えない．大学カード内のユーザ ID の代わりに，一般カード内の読み取り可能な情報より任意の値を抜き出し，それらを組み合わせて認証を行うことで，大学カードと一般カードを組み合わせた認証システムを提案する（図 1）．

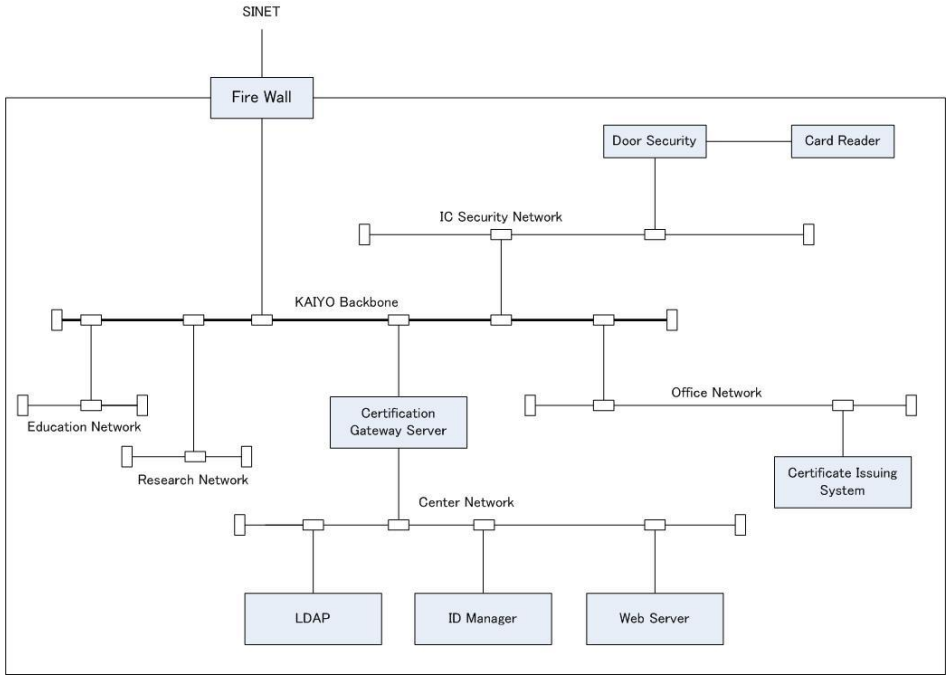

図 1　全体のイメージ図

これまでにも，入退館システムなどで大学発行カードと他機関が発行したカードを併用しているケースがあるが，実際には FeliCa 固有の製造 ID のみ使用しており，認証基盤システムとは連携せず，システムごとに認証していることが多い．そのため，ユーザ ID と結びつけて一元管理することは難しく，IC カードでシステムにログインするなどを行うことが難しかった．

4.1　カード併用時のセキュリティレベル分け

大学で発行した専用のカードだけで運用する場合に比べ，一般カードを用いる場合には危険性がある．そこで，認証の対象ごとにセキュリティレベルを設定し，認証に使用する情報を決める．セキュリティレベルは認証における安全性に比例して高くなるよう設定する．表 3 にセキュリティレベルとその適用システム例を示す．

カード内情報の製造 ID のみを使う場合は，セキュリティレベルを低とする．以後，製造 ID だけでは安全性が低い場合は，製造 ID およびそれ以外の 2 つ以上のコードを

組み合わせた値（以下，カードシステム ID と記す）を認証に使う．そして，さらに安全性を高める場合は，製造 ID およびカードシステム ID の認証に加えて，PIN（Personal Identification Number）コード認証を行う．PIN コード認証を取り入れることで，PIN コードは本人しかわからないため，カード紛失時に悪用される心配が減少する．そのため，製造 ID およびカードシステム ID だけを使用した認証よりセキュリティレベルは高くなる．さらにその上は，大学カードのみの認証とし，一般カードは利用しない．PIN コードの発行方法については，次章で述べる．

これらのセキュリティレベルはあらかじめ各大学において，所属身分，利用システムで分類し，決定しておく．

表 3　セキュリティレベルの例

セキュリティレベル	必要なもの	利用できるサービス例
高	大学カード＋PIN コード	重要文書の閲覧（利用者制限有り） 給与システムの利用（利用者制限有り）
	大学カード	学内限定 Web ページの閲覧 学生向け教務ポータルの利用
	大学カード or 一般カード＋PIN コード	学内ポータルサイトの簡易閲覧 学内掲示板の閲覧
	大学カード or 一般カード	入退室システム
低	カードなし	サービスなし

5. 詳細設計

本システムでの大学発行カードと一般カードを併用した認証方法について，PIN コード等の発行方法およびセキュリティレベルごとの実装方法を示す（図 2）（図 3）．

5.1 PIN コードおよびカードシステム ID

PIN コードは一般カード内のシステムブロックから一部を取り出し，ハッシュ化させた値と本人が決めた値をつなげたものとする．この PIN コードは，一般カードの登録時に本人だけに通知され，本人以外は容易に知ることができない．そのため，カード内情報と組み合わせて認証時に使用すると，安全性が高くなる．PIN コードは認証基盤 DB 上にだけ格納し，安全性を高める．

カードシステム ID とは，システムブロックから PaSoRi リーダ等で読み取り可能なコードの一部を 2 つ以上組み合わせた値である．どのコードを組み合わせているかユーザは知ることができないため，安全性が高い．カードシステム ID も PIN コードと同じく認証基盤 DB に格納する．

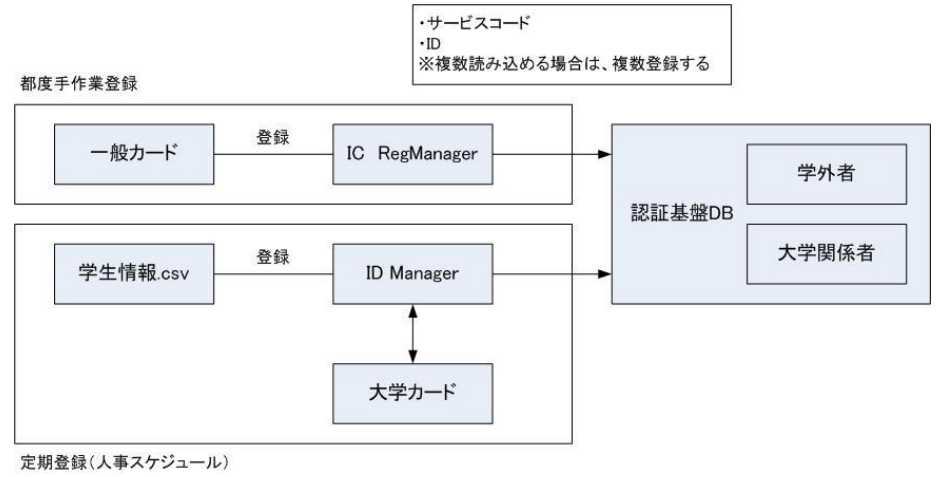

図 2　登録の流れ

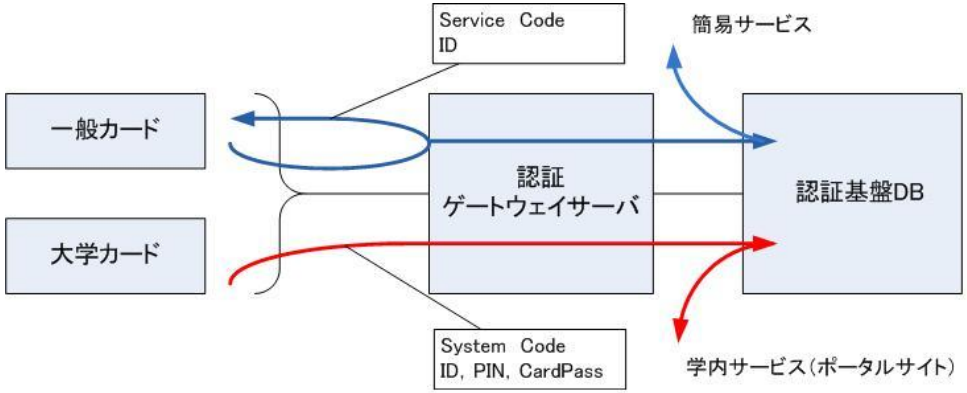

図 3　認証の流れ

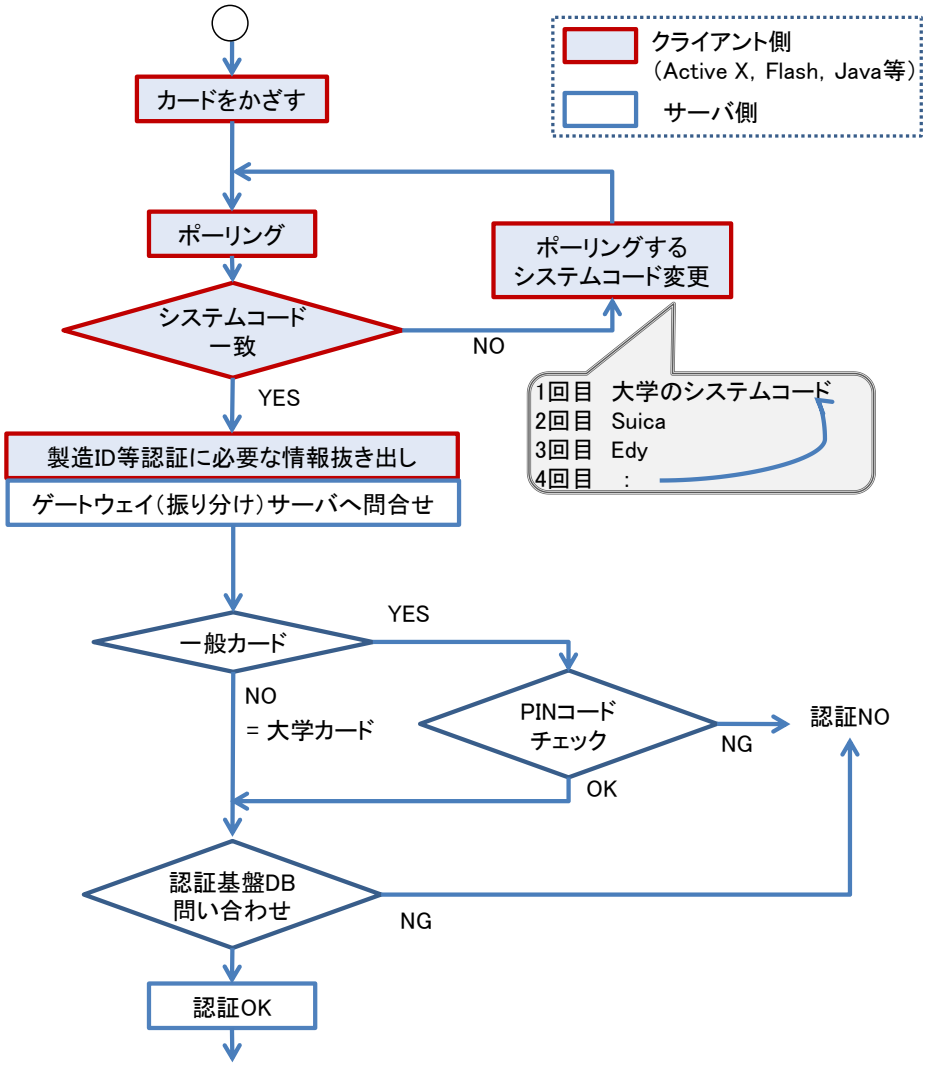

図 4　認証方法

5.2 認証の方法

5.2.1 製造 ID のみを使った認証方法

製造 ID のみを使った認証方法は，大学発行カードおよび一般カードともに，製造 ID のみを使って認証した場合の方法とする．両カードともに製造 ID を使うため，認証の流れは同じになる．認証の流れを以下に記す．

1）　カードをリーダにかざす．
2）　システムコードが一致するまでポーリングする．
　　→登録されているシステムコードかチェックする．
3）　製造 ID を抜き出す．
4）　ゲートウェイ（振り分け）サーバへ問い合わせる．
5）　大学発行カードか一般カードの判別を行う．
　a）　大学発行カードの場合：製造 ID 等の必要情報を認証基盤 DB へ問い合わせる．
　b）　一般カードの場合：製造 ID 等の必要情報を認証基盤 DB へ問い合わせる．
　　→製造 ID と認証基盤 DB の情報が正しいかチェックする．
6）　認証に成功すれば，各種サービスが利用可能となる．

5.2.2 製造 ID およびカードシステム ID を使った認証方法

大学発行カードと一般カードともに，製造 ID およびカードシステム ID を使った認証方法とした場合は，上記 5.2.1 の認証方法にカードシステム ID を追加して読み込む形となる．

ここでは，先に大学発行カードが導入されており，一般カードにおける認証システムを追加する場合の認証方法を記す．大学発行カードの認証情報はユーザブロック内のユーザ情報等とし，一般カードでは製造 ID およびカードシステム ID とした場合の認証方法を以下に記す．

1）　カードをリーダにかざす．
2）　システムコードが一致するまでポーリングする．
　　→登録されているシステムコードかチェックする．
3）　必要情報を抜き出す．
　a)　大学カードの場合：ユーザ ID 等認証に必要なユーザ情報を抜き出す．
　b)　一般カードの場合：製造 ID およびカードシステム ID を抜き出す．
4）　ゲートウェイ（振り分け）サーバへ問い合わせる．
5）　必要情報を認証基盤 DB へ問い合わせる．
　a)　大学カードの場合：ユーザ情報等の必要情報を認証基盤 DB へ問い合わせる．

b） 一般カードの場合：製造 ID，カードシステム ID を認証基盤 DB へ問い合わせる．

6） 認証に成功すれば，各種サービスが利用可能となる．

5.2.3 製造 ID およびカードシステム ID および PIN コードを使った認証方法

上記 5.2.2 の認証方法に一般カードのセキュリティレベルを上げた場合の認証方法を以下に記す（図 4）．

1） カードをリーダにかざす．

2） システムコードが一致するまでポーリングする．
→登録されているシステムコードかチェックする．

3） 必要情報を抜き出す．

a） 大学発行カードの場合：ユーザ ID 等認証に必要なユーザ情報を抜き出す．

b） 一般カードの場合：製造 ID およびカードシステム ID を抜き出す．

4） ゲートウェイ（振り分け）サーバへ問い合わせる．

5） 必要情報を認証基盤 DB へ問い合わせる．

a） 大学カードの場合：ユーザ情報等の必要情報を認証基盤 DB へ問い合わせる．

b） 一般カードの場合：

① PIN コードを入力し，入力した PIN コードの一部とカードシステム ID のハッシュ値が一致した場合に認証基盤 DB へ問い合わせる．

② PIN コードが合致した場合，製造 ID，カードシステム ID を認証基盤 DB へ問い合わせる．

6） 認証に成功すれば，各種サービスが利用可能となる．

5.3 本システムの利点と問題点

本システムでは，重要度の高いシステムは，PIN コード認証も併用する．これによって，カードを紛失した場合でも PIN コードは本人しかわからないため，悪用される可能性は極めて低い．

本システムの構成では，認証基盤 DB へ問い合わせを行うため，DB の負荷が問題となる可能性がある．しかしながら，PIN コードの一部がカードシステム ID のハッシュとなっているため，組み合わせが正しくなければ DB を引くことなくリジェクトできるため，DB の負荷を減らすことができる．

また，本システムの問題点としてカードの種類を検出するため，システムコードを変更しながらポーリングを行う．そのため，システムコードを 1 種類固定にしている場合に比べ，カードと一致したシステムコードが現れるまでに時間を要する．ただしポーリング時間は短いため実用的には問題ない範囲と考えられる．

本研究で設計した仕組みは，大学の専用カードと一般利用されているカードを組み合わせることで導入時の開発コストは専用カードだけに比べ高くなることが予想される．しかしコストの発生は初回導入時のみであり，一時利用者が多く，一般カードを多用する場合には，総コストを抑えることができる．

6. まとめ

本稿では，一時利用者には大学の IC カードを発行せず，利用者本人が所持している交通系 IC カード（以下，一般カードと記す）を使い，別途決められている利用権限に応じて，大学カードと同様に認証システムを利用できるシステムの設計について述べた．本稿で述べる仕組みを実現することで，コストを抑え，全学的に IC カード用いたシステムを利用できるようになる．

大学では企業と異なり，様々な人が出入りするという特異性があり，一時利用者の管理およびカード発行にあたっては，大きな問題となっている．一時利用者における問題解決のため，本研究では一時利用者に対しては一般カードを使うこととした．一時利用者が一般カードを使うことにより，運用におけるコストが削減されるため，運用における効率化につながる．今まで，IC カードの発行に時間を要することや，発行されないことがあるため，各種認証システムが利用できなかった一時利用者にとっても，身分属性に応じてであるが，大学カード保持者とほぼ同等のシステムを利用できるようになり，利便性が向上することが見込まれる．そして，全学的に IC カードを使った認証システムを利用できるようになり，全学的に安全性が高めることができるようになる．

また，本稿で設計したシステムでは，大学カードおよび一般カード情報は認証基盤システムと連携するよう設計している．一般カード内の情報を認証基盤システムと連携させる点は，今後，IC カードを使った認証サービスが増えても，応用していくことができる．

一時利用者の中には，大学側で雇用しておらず，直接，研究室に出入りしている共同研究者や企業研究者等が多く，彼らにおいては，大学側で実態を把握できていないことが多い．しかし，本システムを実現し，一時利用者の一般カードを登録し，必要情報を認証基盤 DB に登録することにより，学内の一時利用者を把握できるようになる．これらは，今後の課題とされている学内で災害が発生した場合の安否確認等にも使える可能性も広がる．

最近では，携帯電話に FeliCa チップを搭載したもの（以下，おサイフケータイと呼ぶ）[１０][１１][１２][１３]が多く出ている．これらは携帯電話をお金のお支払いやポイントカード・会員証の代わりとして使えるサービスであり，お札や小銭，数多く

のポイントカードや会員証が携帯電話で利用できる．実際におサイフケータイを使って，出席管理やスケジュール管理をしている大学や企業が存在している．ただし，これらの認証には製造 ID を使っている．本研究ではおサイフケータイについて検討はしていないが，今後，利用者にとっての利便性の向上を図るため，おサイフケータイとの連携も考えられる．

現在，本システムの設計をもとに今後の実装に向けて，更なる詳細な設計に取り組んでいるところである．今後，この設計を元に全学的に IC カードを導入し，大学発行カードと一般カードを併用した IC カードを使った認証システムを構築することで, 全学的な安全性の向上につながることを期待する．

参考文献

[１] 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

[２] 安浦 寛人：九州大学全学 IC カード導入プロジェクト

[３] 清水 さや子，清水 悦郎，戸田 善勝：IC カード認証・統合認証の連携システムの開発とその現状・評価，大学情報システム環境研究　Vol.11，94-102，2008

[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 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

[５] 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

[６] SONY：SDK for FeliCa User's Manual ver.1.24，2004

[７] SONY：FeliCa，http://www.SONY.co.jp/Products/FeliCa/

[８] SONY：http://www.sony.co.jp/Products/felica/consumer/index.html?j-short=pcrw

[９] 東日本旅客鉄道株式会社：http://www.jreast.co.jp/suica/whats/index.html

[１０] おサイフケータイナビ：http://osaifukeitai-navi.com/

[１１] NTT docomo：http://www.nttdocomo.co.jp/service/convenience/osaifu/

[１２] SoftBank：http://mb.softbank.jp/mb/service/3G/life/s_FeliCa/

[１３] おサイフケータイ（EZ FeliCa）：http://www.au.kddi.com/ez_FeliCa/