解 説

ICカード技術の現状と課題

NTT 情報流通プラットフォーム研究所
吉田　壱　yoshida.hajime@lab.ntt.co.jp
平田 真一　hirata.shinichi@lab.ntt.co.jp



はじめに

近年，電子商取引の普及に伴いICカードは高セキュリティ・高機能なデバイスとして大変注目されており，現在さまざまな分野で本格的に普及しようとしている[1]．クレジットカードやキャッシュカードなどの金融系分野では，偽造防止などセキュリティを高めるために2002～2003年を目処にICカードの導入が予定されている．また，交通分野では，定期券に非接触のICカードが導入されており，今後さらに導入が進むと思われる．一方，通信系の分野では，テレホンカードが1999年にIC化されており，次世代携帯電話の規格（IMT-2000）では，UIMカード（User Identity Module）が規格化されている．

公共系の分野でもさまざまな取組みがされている．総務省では，2002年度に住民基本台帳ネットワークシステムを構築し，本人認証のためにICカードを希望者に配布する[2]．その他にも，健康保険証や運転免許証のICカード化が検討されている．また，経済産業省ではこれらの公共系のカードを1枚のカードに相乗りさせ，利便性の高いシステムを提供することを目指してIT装備都市研究事業[3]を2001年度に行っている．また，欧州では「EuroSmart」[4]や「eEurope Smartcard」[5]等のプロジェクトが進行中でありICカードの相互利用等が検討されている．

ICカードは，従来の金融系，通信系，流通系，入門証・キャンパスカードといった磁気カードの置き換えに加えて，公共系，交通系の分野で大きな伸びが期待されており，2005年には2000年のほぼ10倍のカードが発行されるという予測もされている．

本稿では，ICカード技術について，特に注目されている非接触型ICカードと多目的利用ICカードを中心に解説する．

ICカードの特徴

ICカードとはICチップを内蔵したカードであり，磁気カードに比べ，以下の特徴がある．

(1) 大容量：従来の磁気カードに比べ，約100倍以上の記憶容量を持つ．
(2) 高機能：ICチップにCPUやメモリを搭載し，カード内部で演算することができる．
(3) 高セキュリティ：外部からの不正を難しくする耐タンパデバイスであり，暗号アルゴリズムもサポートできる．

これらの特徴により，ICカードは，暗号化処理が必要な認証サービスや電子決済サービスなどの高セキュリティなサービスに利用されたり，大容量であることを活かし，1枚のカードで複数のサービスを受けられたり，外部からの不正が難しいことから個人情報を安全に持ち運ぶデバイスとして，大きな期待が寄せられている．以下でその構成と機能について述べる．

■ICカードの構成と機能

CPUを搭載したICカードは基本的に，プロセッサに加えて，カード管理OS，データI/O，コマンド処理プログラムを格納したROM（Read Only Memory），通信用バッファ等レジスタの役割を行うRAM（Random Access Memory），利用者情報等を格納するEEPROM（Electrically Erasable Programmable ROM）等の不揮発メモリから構成される．

ハードウェアの進歩によりCPUは従来の8bitから，16，32bitの処理性能を持つものや，暗号コプロセッサを持つものが主流になり公開鍵暗号処理がICカード内で実現できるようになってきた．また，不揮発メ

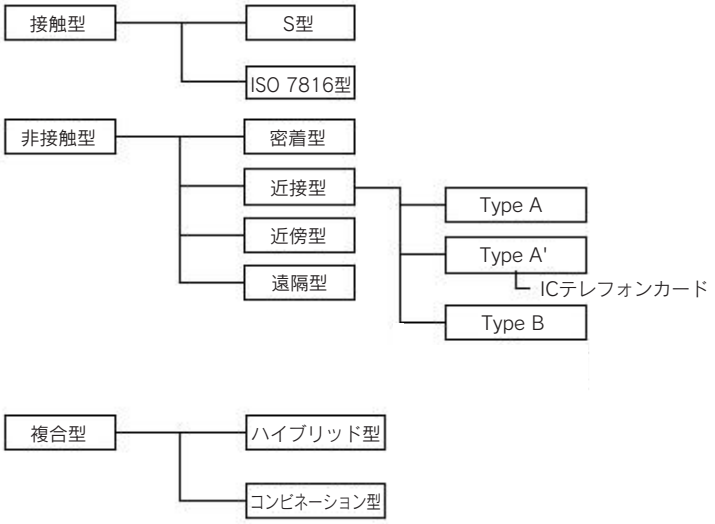


図-1　ハードウェアの観点での分類

モリにおいてはFlashメモリ等の大容量技術により従来主流であった8KBから32KB以上，大きいものでは1MBの容量を持つICカードが出現してきている．また，FeRAM（Ferroelectric RAM）の技術は高速であるという特徴に加え低消費電力といった特徴も併せ持つために，携帯端末やカードのメモリとして有望と考えられている[6]．

ICカードの種類

■ハードウェアによる分類

ICカードは，ハードウェアの側面からみると**図-1**のように分類される．接触型はカードの表面に接触端子があり，この端子を介してリーダライタとカードの間で電力供給と通信を行うタイプのICカードで，種類としては，S型およびISO/IEC 7816型がある．S型カードとは，ISOで仕様が規格化される以前の1980年代に日本国内のメーカ16社で仕様を策定したもので1,600万枚以上の発行実績がある．その後，1995年に国際標準規格のISO 7816が制定され，現在の主流となっている．

非接触型はカードの表面には端子がなく，リーダライタとは無線で電力供給と通信を行うタイプのICカードで，通信可能な距離によって密着型，近接型，近傍型，遠隔型に分類される．中でも近接型はさまざまな用途で利用しやすい通信距離（10cm以下），高速なデータ転送速度，電池が不要などの理由により，多くのサービスにおいて有効であると考えられる．

また，接触および非接触両方のインタフェースを持つ「複合型」と呼ばれるカードも存在し，接触・非接触のインタフェースごとに1つずつのICチップを搭載したハイブリッド型と，両方のインタフェースに対応したICチップを1つ搭載したコンビネーション型がある．

このように，ICカードにはさまざまな種類があり，また，同じ種別でも，メモリ容量やCPU速度などの性能によって価格にも差がある．ICテレホンカードで使われているカードは，単機能で，性能もあまり要求されないため，メモリ容量は128bytesで，8bit CPUを搭載している．それに対して，NTTサイバースペース研究所が開発したELWISEカード[7]はメモリ容量が1Mbytes，16bit CPUを搭載し，暗号処理のためのコプロセッサを搭載している．また，交通系で定期券などに利用する場合は，改札機で高速に処理する必要があるため，非接触カードを使用し，高速なシステムで運用する必要があり，逆に金融系ではデータの漏洩防止，本人認証データの格納が要求されることや，金融系サービスの標準仕様にあわせるため，接触型カードを使用し，バイオメトリクスなどのデータも格納できるような十分なメモリ容量が必要である．このように，システム要件やコストにあわせてカードは使い分けがされると考えられる．

■標準化動向

ICカードに関して大量生産によるコストダウンや相互利用による利便性向上の観点から，標準化が進められている．ここでは，国際標準，国内標準，サービスごとの業界標準の観点でまとめる．

国際標準

ISO/IECでは，JTC 1/SC 17でICカードの国際標準の策定作業を行っている．接触型カードについてはISO/IEC 7816が策定されている．ISO/IEC 7816は現在10のパートからなり，それぞれのパートの内容は**表-1**に示すとおりである．また，非接触型カードでは，先で述べた種類ごとにそれぞれ密着型（ISO/IEC 10536），

パート	概　要
Part1	カードの物理特性（形状・材質など）
Part2	カードの電気的特性
Part3	データ伝送プロトコル
Part4	ファイル構造および共通コマンド
Part5	アプリケーション識別子（AID）
Part6	業務／サービスにかかわらず共通に使用するデータ要素
Part7	SCQL（カード向けクエリー言語）
Part8	セキュリティ関連共通コマンド
Part9	追加共通コマンドおよびセキュリティ属性
Part10	同期式ICカードの電気的特性および伝送プロトコル

表-1　ISO/IEC 7816の概要

項　目	密着型	近接型	近傍型
ISO規格番号	10536	14443	15693
ISO審議組織	【WG8/TF1】	【WG8/TF2】	【WG8/TF3】
周波数（クロック）	4,92MHz	13.56MHz	13.56MHz
通信距離	～2mm	～10cm	～70cm
データ通信速度	9.6Kb/s	9.6Kb/s	～26Kb/s

表-2　非接触カードの国際標準

表　題	内　容
第1部 接触型ICカード	接触型カードの標準仕様であるISO 7816-1～3をもとに，接触型カードの物理特性，電気特性，伝送制御について規定
第2部 非接触型ICカード	非接触近接型カードの標準仕様であるISO 14443-1～4をもとに，非接触型近接型カードの物理特性，電気特性，伝送制御などについて規定
第3部 共通コマンド	ISO 7816-4，8，9をもとに，接触型，非接触型に共通なファイル構造，コマンドインタフェース，セキュリティ機能などを規定
第4部 高速処理用ICカード	日本鉄道サイバネティクス協議会ICカード規格書に基づき，鉄道の改札などに使用できるような高速処理に特化したカード仕様について規定

表-3　JICSAP V2.0の概要

近接型（ISO/IEC 14443），近傍型（ISO/IEC 15693）の標準がある．なお，遠隔型の標準化は未着手である．それぞれの特徴を**表-2**にまとめる．

ISO/IEC 14443では大きく4つのパートからなり，パート1は物理形状，パート2は電力伝送および信号インタフェース，パート3は初期化および衝突防止，パート4は伝送プロトコルを規定している．また，これより上位の共通コマンド等規定は接触型ISO/IEC 7816に準じている．非接触型（近接型）と接触型では，単に電力およびデータ転送を接点を介さずに無線で行うという点だけではなく，近接型のデータ転送速度は接触型の9.6Kbpsに対して約10倍の106Kbpsであること，また，非接触型に適した伝送プロトコル（T=CL）を新たに規定している点（接触型ではT=0，T=1）がある．

ISO/IEC 14443はパート2および3での規定により，タイプAおよびBの2つの方式に分類され，これらの国際標準化は完了している．

国内標準

一方，日本国内では，ICカードシステム利用促進協議会（JICSAP）が中心となって標準化作業を行ってきた．ISO規格のJIS化作業や，実装依存の部分が多いISO規格よりも相互運用性の高い仕様を目指したJICSAP ICカード仕様の策定を行っている．1998年JICSAP ICカード仕様V1.1を策定し，現在，JICSAP ICカード仕様V2.0[8]が公開されている．JICSAP ICカード仕様V2.0の構成および概要を**表-3**にまとめる．V2.0では従来のV1.1に比べて，セキュリティ関連等のコマンドおよび接触・非接触インタフェースなど，大幅に追加・変更されている．

業界標準

また，金融，通信等それぞれのサービスごとにISO規格などをもとに標準化がすすめられている．ここでは例としてEMVと携帯電話用のSIMカードを紹介する．EMVは，金融分野でのICカード仕様の国際デファクトスタンダードである．これはEuropay Int.，MasterCard Int.，VISA Int.の3社により制定された仕様で，その管理はEMVCo[9]により行われている．1998年5月にEMV3.1.1，2000年12月にEMV2000が制定された．また，携帯電話で使用されるSIMカードの仕様は，ETSI（the European Telecommunications Standards Institute）[10]が規定している．これらの規格は基本的にISO/IEC 7816をベースにしており，各々の業界の中での相互運用性を確保するために，サービスを提供するためのファイルの構成や，追加しなければならないコマンドなどを規定している．

非接触型カード

■非接触カードの特徴

非接触ICカードは先で述べたように，リーダライタとICカードが無線で通信し，カード表面に接点がない．そのため以下のような特徴がある．

- ICカードをリーダライタに差し込む必要がなく，近づけるだけでデータのやりとりが行える．
- 物理的な接点を持たないため，寒冷地などの悪条件

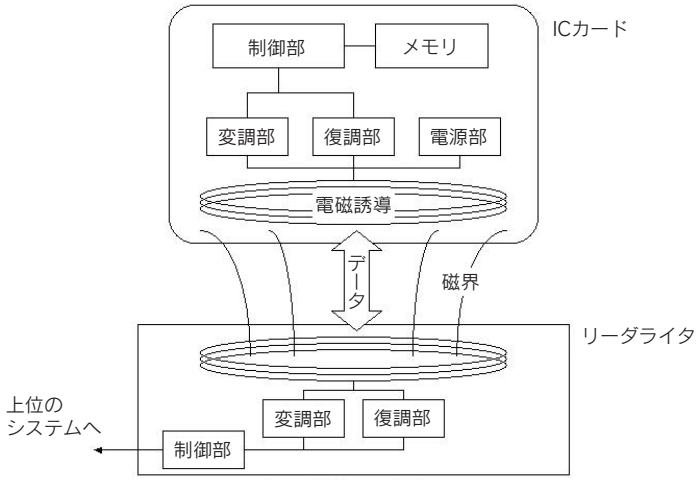


図-2　非接触カードの構成

下での利用も可能.

- 通信速度が高速.
- リーダライタとICカードが接点端子で接続される必要がないため，リーダライタのメンテナンスコストが低くなる.

これらの特徴を持つ非接触ICカードは，高速性および取扱いの容易さにより，通信分野ではICテレホンカード，交通分野ではJR東日本の定期券や香港などの地下鉄の乗車券などに用いられている.

また，接点端子がないため取扱いが容易であることから，日本では公共分野のICカードが非接触カードになっていくと思われる.

■非接触ICカードの動作概要

ここでは，最も有用であると思われる近接型の非接触カードについて述べる．近接型の非接触ICカードシステムの一般的な構成図を**図-2**に示す．ICカードにはコイルが埋め込まれており，リーダライタが発生する搬送波によりコイルで電磁誘導が起こり，電力が供給される．また，データ通信もこの搬送波を用いて行う．リーダライタからカードへの通信は，搬送波の振幅変調で行い，逆にカードからリーダライタへの通信はカードのコイルの負荷を変化させることで磁界を変化させ，リーダライタ内のコイルでそれを読み取ることで行う．近接型非接触カードの場合，1台のリーダライタの通信可能範囲に複数のICカードが存在する場合がある．これらと通信する際に，誤って別のカードと通信を行わないようにする処理が必要である．これを衝突防止処理という.

ISO/IEC 14443のType AとType Bでは，信号の変調方式と符号化方式，および衝突防止処理のアルゴリズムが異なっている．リーダライタからカードへの送信について，タイプAとBでは信号変調度および符号化方式が異なっている．カードからリーダライタへの送信については，いずれも副搬送波を利用しているが，副搬送波の変調方式と符号化方式が異なる．また，衝突防止処理は，タイプAではビットコリージョン／タイムスロットが，タイプBではスロットマーカが用いられる[13].

■非接触ICカードの技術動向

非接触ICカードは，電力やデータが無線にて送られることから，CPUや暗号演算用コプロセッサの動作に対する電力制限等が懸念されていたが，それらを解決する技術が開発されている.

ICテレホンカード（ICテレカ）[14]およびこの方式と互換性を有したCPU搭載の非接触ICカード，コンビネーションカード[15]が開発されている．当初この通信方式は，リーダライタからの信号がASK100%変調であることから，CPU搭載カードに対して不向きであると考えられていたが，消費電力を10数mWまで低下させ，電力伝送効率を向上させる工夫によって，給電能力に制限のあるIC公衆電話機でも通信が可能になった．これらICテレカ互換カードの特徴として，①全国に設置してあるIC公衆電話機を端末として利用できるポテンシャル[11]，②複数枚での利用を前提に設計，③カードやリーダライタに対する互換性規定・評価法の充実等が挙げられる.

また，2001年11月より導入されたJR東日本のICカード定期券（Suicaカード）[12]では，高速処理に特化されたICカードが利用されている．これは1997年に香港で交通系カードとして導入されているものと同じFeliCa[16]というカードで，改札ゲートでのスムーズな通過を優先するため，データ転送速度を初期応答時から212Kbpsとし，カードとリーダライタ間で100ms以下の迅速な処理を実現している．また，独自の信号符

号化方式（カードとリーダライタの双方向で“Manchester”符号を採用）で副搬送波を用いないことから，将来，リーダライタ相互の通信もカードと同様に行うことができる．

ニューメディア開発協会によって開発された新世代ICカード[17]は，電子政府等の公共系多目的サービスを想定したものであり，高性能CPU，公開鍵と共通鍵等を搭載し，①電子署名，②2枚同時処理，③カードプラットフォームとの連携利用によるアプリケーションダウンロード等の機能を実現している．また，タイプB通信方式の互換運用に向けて実装規約が策定されている．

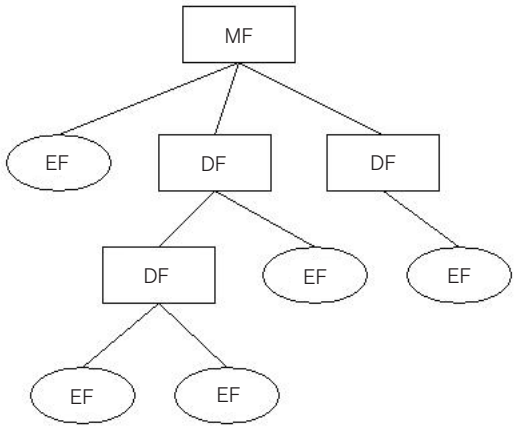


図-3　ISO 7816カードのファイル構造

多目的利用カード

■ICカードの多目的利用

従来，磁気カードやICカードは特定の1つのサービス専用で利用されたり，多目的利用であっても，企業内あるいは特定エリアでの入退室管理，食堂や自動販売機支払いなどに限定した利用のみであった．しかし，ICカードは，磁気カードに比べて大容量であるため，1枚のカードをある程度広範囲にわたって多目的に利用する試みも以前より行われている．たとえば交通系では，1枚のカードでバス，鉄道等で利用でき，かつ売店等の少額決済にも利用できるようにする検討や，自治体等が発行する公共系カードで住民票取得や図書館等の公共施設利用等の複数サービスでの利用の検討がされており，今後，サービス分野や企業を跨ったICカードの広域・多目的利用が普及すれば，利用者の利便性向上，システム構築者／サービス提供者の投資コスト低減といった観点より，徐々に少数のICカードにサービスが集約されていくものと考える．

ICカードを多目的に利用するためには，以下の要件が必要である．

- ICカード内に格納されているサービス用の情報をコンテキストに応じて選択すること．
- 他のサービスの情報が盗聴・改ざんされないこと．

以降にICカードを多目的利用するためのカードOS技術およびプラットフォーム技術について述べる．

■ICカードOS

ICカードはソフトウェアの観点からみると，データキャリー型とプログラム格納型に分類できる．データキャリー型とは，ICカードをファイルシステムを持つセキュアなストレージとして利用するものであり，ファイル構造，セキュリティ機能，およびICカードにアクセスするためのコマンドを規定している．具体例としてはISO 7816などがある．それに対して，プログラム格納型とは，ICカードの中にアプリケーションプログラムの実行環境があり，その上でユーザの作成したアプリケーションプログラムが動作するもので，JavaCard[18]などがある．

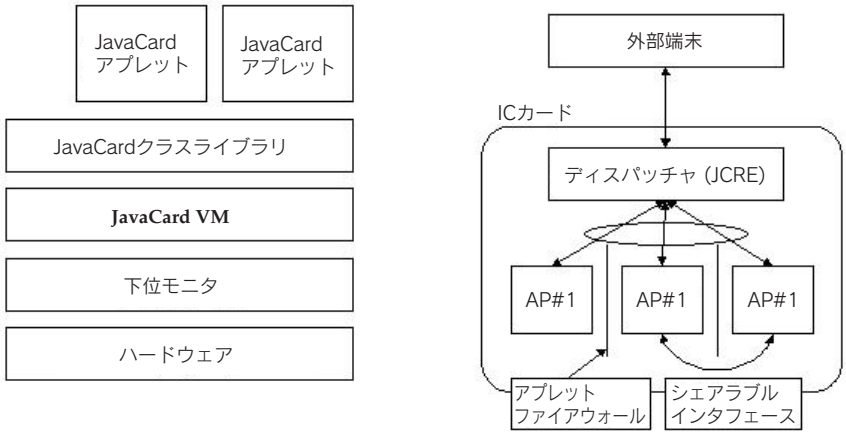
従来は，データキャリー型のICカードが主流であったため，多目的利用の試みもデータキャリー型のカードで行われていたが，ICチップの性能も向上した現在では，プログラム格納型のICカードを利用した多目的利用が実現している．

プログラム格納型カードでは，サービスごとにICカード内で動作するアプリケーションプログラムを作成し，カード内に実行可能な状態で格納する．カードを複数の用途で利用する場合は，複数のプログラムがカードに入れられ，サービス利用時にプログラムを選択する．このとき，あるプログラムで保持している情報が他のサービスからアクセスできないようにすることが必要である．そのため，プログラム格納型カードのOSはアプリケーションファイアウォールと呼ばれる他プログラムからのアクセスを制限する仕組みが必要である．また，現在のところ，後述するJavaCardのようにプログラム選択時にはアクセス制御を行わないものが一般的であるため，ICカードのプログラム設計者はプログラムが選択されてもユーザ認証をしないとその後の処理ができないような設計にするなどの注意が必要である．

ここではデータキャリー型の例としてISO 7816を，プログラム型の例としてJavaCardについて解説する．

ISO 7816

データキャリー型カードの主流カードであるISO 7816型では，ファイルが**図-3**のように階層構造で管理され，カードを複数の用途で使用する場合には，DFごとに1サービスが割り当てられ，サービスの利用時には，まず該当するサービスのDFを選択し，そ



(a) JavaCardの論理構成　　(b) アプレットの共存

図-4

の後，実際にデータが格納されているEFに対して書き込み・読み出しなどの処理を行う．DFごとにアクセス権を設定することにより，他のサービスとの独立性が保たれ，EFごとにアクセス権を設定することにより，同一サービスでもデータごとに複数のアクセス権が設定できる．

JavaCard

JavaCardとは，ICカードなどのようにメモリが小さくCPU性能が低いデバイスでJavaを動作させるための仕様で，Sun Microsystems社が中心となって策定している．**図-4** (a) にJavaCardの典型的な構成図を示す．ICカード上にJavaVMのサブセットを搭載し，Java言語でコーディングされたプログラム（Appletという）がICカード内で動作する．したがって，開発者はICカードのハードウェアの違いを考慮する必要がなく，また，Java言語を使用するため，一般的なJavaプログラムの開発環境を利用することができ，開発効率が向上する．また，JavaCardは，当初から複数のプログラムを格納し実行する環境を提供する目的で仕様が策定されているため，あるAppletの使用しているメモリ領域を他のAppletが使用できないように，Applet Firewallを定義したり，カード内のApplet間でデータの共有をするためのインタフェースを定義したりするなどで，ICカード内のプログラムの独立性および利便性を確保している（**図-4** (b)）．

■ICカードプラットフォーム

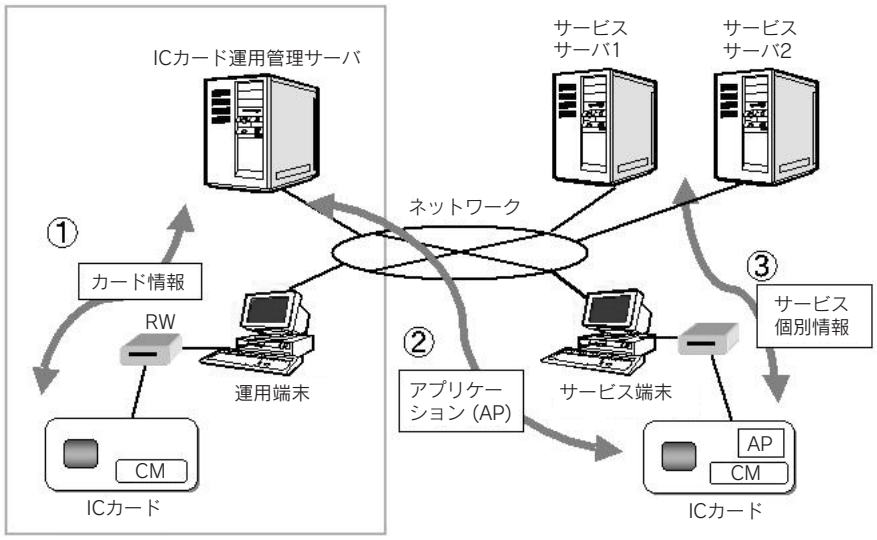
従来のICカードを利用したサービスにおいて，ICカードの運用管理システムはそのサービス専用のシステムとして実現されていた．しかし，多目的ICカードでは，1枚のカードで複数の事業者がサービスを提供することが考えられるため，ICカードを自ら発行せず，サービスを提供するだけの事業者が存在するようなモデルを考慮する必要がある．さらに多目的ICカードは，発行時に固定的に複数のサービスをICカードに搭載する方式と，発行後に動的に複数のサービスの搭載および削除を可能とする方式の2つが考えられ，また，発行後にサービスを搭載・削除する場合，ICカード発行者だけが搭載・削除する方式と，ICカード発行者がICカードサービス提供者に搭載・削除を許可し，サービス提供者が処理を実行できる方式がある．これらの機能を実現し，ICカードの発行・管理と，ICカードへサービスを搭載・削除するための仕組みが提案されている．これらはICカードプラットフォームと呼ばれる．**図-5**にICカードプラットフォームの構成例を示す．現在提案または運用されている代表的なICカードプラットフォームは，MULTOS，GP/VOP（Global Platform/Visa Open Platform），Network-based IC Card Environment（NICE）などがある．

MULTOS

MULTOS[19]は，ISO 7816をベースにマルチアプリケーション対応したICカードOSおよびプラットフォームであり，MasterCard社などが中心となったMAOSCOコンソーシアムで仕様が決定されている．MULTOSの特徴は以下のとおりである．

- ICカードOSであるMULTOS OSでハードウェアを隠蔽し，MELという言語で書かれたアプリケーションはすべてのMULTOSカードで動作する．
- アプリケーションの搭載・削除などのカード内での管理は，MULTOS OSで行う．
- 世界唯一の認証局（MULTOS KMA）が存在し，運用方法も細かく規定されている．

MULTOSでは，カード発行者のみがカードへのアプリケーションの搭載・削除の権限を持つ．また，その際にもMULTOS KMAからALC（アプリケーションロード証明書）やADC（アプリケーションデリート証明書）



① ICカード発行
② アプリケーションダウンロード
③ サービス実行

図-5　ICカード運用管理システムの構成例

を取得する必要がある．

GP/VOP

GP（Global Platform）[20]は，JavaCardおよびWindows Powered Smart Cardsをターゲットにしたマルチアプリケーション運用管理システムの仕様を策定している団体である．GPには，ICチップベンダ，カードベンダ，システムベンダおよび金融などのユーザ企業など，幅広い業種から約40社が参加している．仕様はVisa Internationalが開発したVOPをベースとしている．GPの特徴は以下のとおりである．

- カードOSに非依存な，マルチアプリケーション管理のフレームワークを提供する．プログラムのポータビリティは，JavaCardなどのカードOSに依存する．
- アプリケーションの搭載・削除などのカード内での管理は，カードOS上で動作するカードマネージャが行う．
- アプリケーションの追加・削除などはカード発行者が権限を持つが，セキュリティドメインという仕組みを使用すれば，サービス提供者がカードにアプリケーションを追加できる．

GPには，上記のMAOSCOで中心となっているMasterCardが参加したため，今後，MULTOSの技術も含めたより適用範囲の広い仕様になることが期待できる．

Network-based IC Card Environment（NICE）

NICE[21),22)]は，NTT情報流通プラットフォーム研究所が開発した多目的ICカードシステムで，以下の特徴を持つ．

- 仕様としてはカードOSに非依存．実装としては，NTTが開発した1MBの大容量を持つマルチアプリケーションカードであるELWISEカードを対象としている．
- アプリケーションの搭載・削除などのカード内での管理は，カードOS上で動作するカードマネージャが行う．
- カードへのアプリケーションの追加・削除はカード発行者が権限を持つが，カード発行者がある事業者にICカード内のメモリ領域を貸与したときに，そのメモリ領域にアプリケーションを搭載するときにはカード発行者ではなく，メモリ領域を借り受けた事業者の権限で行うことができる．

このシステムは，先で述べたIT装備都市研究事業で使用されるプラットフォームの1つに採用されている．

ICカードの課題

多目的ICカードでは，以下のような課題がある．

■信頼性の向上

非接触カードは電源供給を無線で行っているため，処理がすべて終わる前にカードがリーダライタから離され，カードへの電源供給がなくなってしまうことがあるため，カード内のデータの状態が不安定になる場合がある．処理中の障害からの復旧や，破損時対応等の異常処理について，ICカードおよびシステム全体でどのようにカード内のデータを保証していくかという課題があり，トランザクション保証等の技術が検討

単語帳

耐タンパデバイス：
内部情報を読み出そうとする外部からの攻撃を困難にするような対策のとられた装置．

ASK100%変調：
タイプA方式におけるR/WからカードへのIC通信方式．キャリア振幅に対する信号振幅の変化の割合が100%であるもの．

MF (Master File) /DF (Dedicated File) /EF (Elementary File)：
ISO/IEC 7816-4におけるICカード内の階層ファイルシステムのファイル規定．EFは実際にデータを格納するファイルを指し，DFはファイルの管理情報が格納されているファイルであり階層構造におけるルートのDFを特にMFという．

されている[23]．

■ICカードの再発行

カードを盗難・紛失したときには，通常カードを再発行してもらう．カードの再発行時には，再発行前のICカードの状態を可能な限り復元することが望ましい．従来のカードサービスでは，1枚のカードのコンテンツは一事業者がすべて管理していたが，上記のようなICカードプラットフォームを利用した場合には，複数の事業者が1枚のカードのコンテンツを管理しているため，再発行前のカードの状態を復元するときに，カード発行者がサービス提供者の管理するコンテンツをカードに搭載して再発行するのか，また，サービスの利用状態などの個人情報をカード発行者がすべて集めてくる場合に，プライバシーの問題はないかなど，さまざまな問題が発生する．

■複数種類のカードの運用管理

前にも述べたように，現状ICカードはさまざまな種類があり，用途によって使い分ける場合もあり統一化は難しい状況である．それぞれのICカードはデータ転送方式やコマンドインタフェースが異なっており，同一のシステムで扱うことは難しい．ICカードが普及し個人認証のインフラになったときに，ICカードプラットフォームでは複数種類のICカードを扱うことが考えられるため，その運用管理方法が課題である．

■利用環境の整備

ICカードの大量導入時代に向けて，従来のサービスだけでなく，インターネット利用のバーチャルな空間も含めて，魅力あるサービスを創出し，またいつでも・どこでもサービスを受けられるようにするために，街頭情報端末ならびに家庭用リーダライタ等インフラ設備の普及促進をするなど，ユーザにとって魅力的な利用環境を整備することが課題として挙げられる．

おわりに

ICカード技術について，特に非接触カードと多目的カードについて紹介した．ICカードはセキュリティを保ちながら持ち運びが容易であるため，ネットワーク社会における個人認証のツールとしての重要度がますます高くなると考えられる．限られた誌面で全体を概観したため，より詳細な情報を得られるように多くの参考文献を紹介した．本稿によって読者の皆様方がICカード技術に興味を持ち，ICカード技術を理解するときの一助になれば幸いである．

参考文献

1) シーメディア: ICカード総覧 (2001).
2) 地域自治情報センタ (LASDEC) : http://www.lasdec.nippon-net.ne.jp/rpo/rss/system_gaiyo/system_gaiyo.htm
3) ICカードの普及等によるIT装備都市研究事業, http://www.itcity.jp/
4) eurosmart, http://www.eurosmart.com
5) eEuropeSmartcard, http://www.cordis.lu/ist/ka2/smartcards.html
6) FeRAMの容量が毎年4倍, ケータイのメモリに変革, NIKKEI ELECTRONICS, pp.33-34 (2001).
7) 竹田ほか: 接触型超多目的ICカードシステムの開発, NTT技術ジャーナル, Vol.49, No.12, pp.733-739 (2000).
8) ICカードシステム利用促進協議会: JICSAP ICカード仕様V2.0 (July 2001).
9) EMVCo, http://www.emvco.com/
10) ETSI, http://www.etsi.org/
11) ICカード公衆電話の新サービス, NTT技術ジャーナル, pp.28-31 (June 2001).
12) Suica: http://www.jreast.co.jp/suica/
13) 織田, 鮎川, 苅部: セキュリティICカードの基礎と応用, シーメディア (2000).
14) 伊達, 竈, 下山, 菅野, 土橋: ICテレホンカードの開発と展開, NTT R&D, Vol.12, pp.626-633 (1999).
15) 竈, 鈴木, 大谷, 永井: コンビネーションICカードシステムの開発, NTT R&D, Vol.12, pp.745-751 (2000).
16) FeliCa: http://www.sony.co.jp/Products/felica/
17) 電子署名や2枚重ね読みなどの機能を搭載した「新世代ICカード」, Card Wave, p.40 (Jan. 2001).
18) JavaCard: http://java.sun.com/products/javacard/
19) MULTOS, http://www.multos.com/
20) GlobalPlatform: http://www.globalplatform.org/
21) 山本, 田路, 平田, 庭野: ICカード情報流通プラットフォーム: NICE, NTT技術ジャーナル, pp.14-18 (Dec. 2001).
22) 山本, 細田: ICカード情報流通プラットフォーム, 電気通信協会 (2001).
23) 吉田, 鈴木, 平田, 山本: ICカードトランザクション処理方式の考察, 信学技報, SS2001-25/KBSE2001-27, pp.19-26 (2001).

(平成14年1月16日受付)