情報処理最前線

ICカードの動向

影井良貴／NTTデータ通信

はじめに

最近，ICカードがいろいろなところで注目されている．日本ではICカードと呼ぶが，欧米ではスマートカードという．最近の主な用途としては，電子マネーの実験において，その電子財布としての利用や，電子商取引などでの本人認証用の情報のIDカードとしての利用など，情報や処理の内容が外部に漏れてはいけないようなものを格納するものとして位置付けられ，利用されている．最近のICカードの技術的な方向性としては，非接触型ICカードの出現によりインタフェースの多様化，ICチップの機能・性能の高度化とそれに基づく高機能な汎用OS型ICカードの出現などが挙げられる．本稿では，このようなICカードの基礎からアプリケーションまでを簡単に解説する．

ICカードとは

最初にICカードとはどのようなものか，ということを簡単に解説する．ICカードの構造は，**図-1**のとおりプラスチックのカードにICチップが埋め込まれているもので，外部との通信は通常接点端子を通じて行われる．ICチップの構造は，CPU，ROM，EEPROM等からなり，メモリからの情報の出し入れは，CPUで管理するため，簡単には読み出せないようになっている．このため情報のセキュアな格納に適しているといわれている．コマンド処理や暗号処理などの機能を提供するためのプログラムはROMに焼き付けられている．そして，随時書き込んだり読み出したりする情報はEEPROMに格納されている．カードとしてよく普及しているものに銀行のキャッシュカードのような磁気ストライプカードがあるが，通常の磁気ストライプが80文字分の容量であるのに比べ，ICカードは平均8000文字分のメモリ容量があり，約100倍になっている．

最近利用されつつある非接触型ICカードの場合の構造は，接点端子の代わりにコイルがカード内に埋め込まれており，原理はトランスと同様である（**図-2**参照）．リーダ／ライタにもコイルがあり，これらのコイル間での電磁的結合により，電力供給とデータ通信が同時に行えるようになっている．したがって，通常，非接触型ICカードは電池を持っていない．

国際標準化動向

ICカードについては，ISO／IEC JTC1／SG17で標準化が行われている．従来からある接触型ICカード（ISOでは端子付きICカードという）の標準化が一番進んでいる．これに続き，順次非接触型ICカード（ISOでは端子なしICカード）の標準化が進められている．ただし，非接触型ICカードについては，密着型，近接型，近傍型等の複数の種類があり，それぞれで利用できるリーダ／ライタとカードとの距離が異なっている（**図-3**参照）．標準化は，この距離が短いものから順に行われており，接触型がISO／IEC7816，密着型がISO／IEC10536，近接型がISO／IEC14443という番号で検討されており，これらより距離が長い近傍型などは，まだ実質的検討に着手されていない．

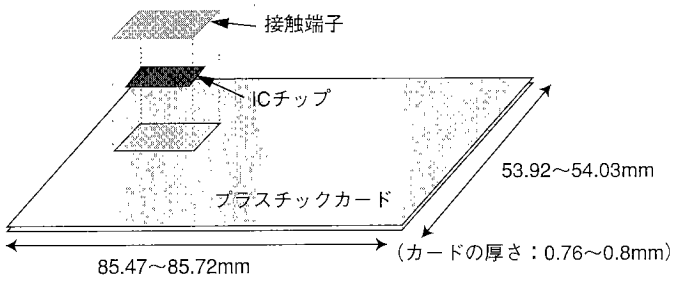


図-1　接触型ICカードの構造

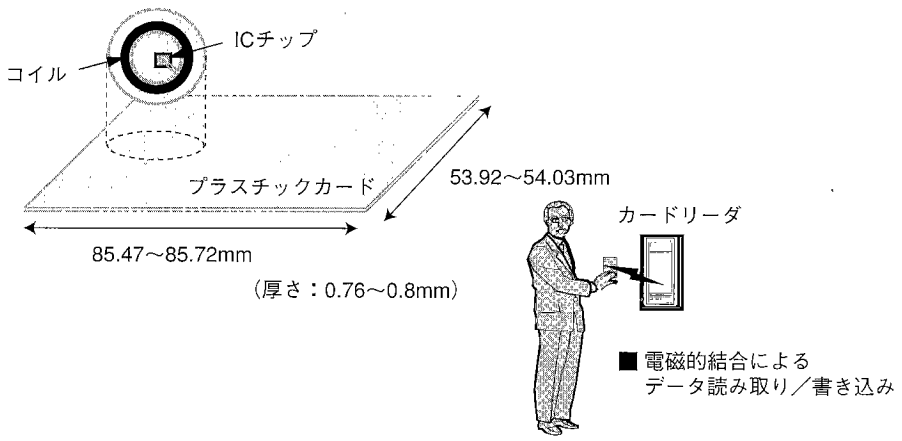


図-2　非接触型ICカードの構造

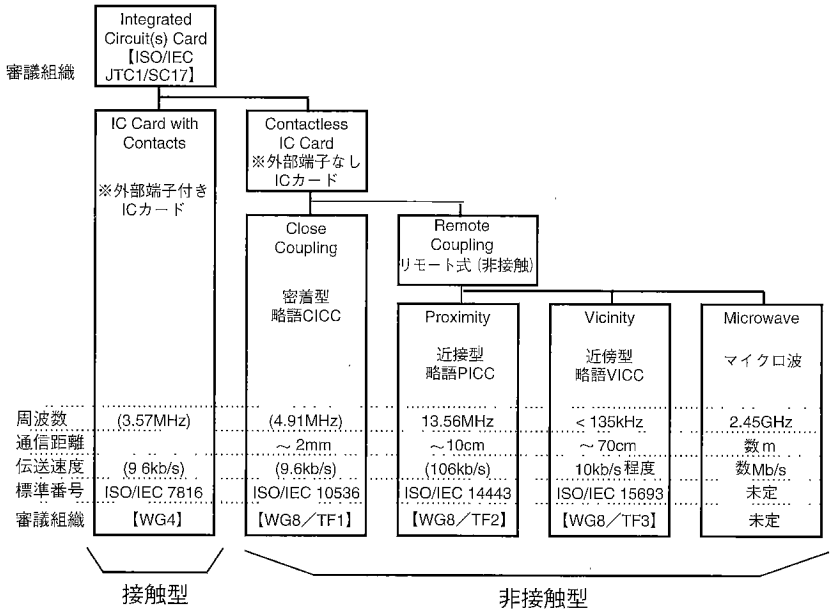


図-3　ICカードの標準化動向

各業界での利用状況

ICカードの利用は，金融分野や公共分野に比べ，産業分野の方が現在のところ盛んである．主なアプリケーションとしては，

- IDカード
  - 入退室管理（ゲートでの本人確認）
  - 社員証，会員証
- ポイントカード，プリペイドカード

といったところである．

もともとのICカードの機能は，

①電子情報のためのセキュアな可搬型ファイル

から始まっているわけであるが，最近では

②処理プロセスを隠蔽可能な小型のコンピュータ

という機能に着目されてきており，実際には，①と②の両方を組み合わせた形で利用されるようになってきている．

具体的に，暗号処理の場面を考えてみる．

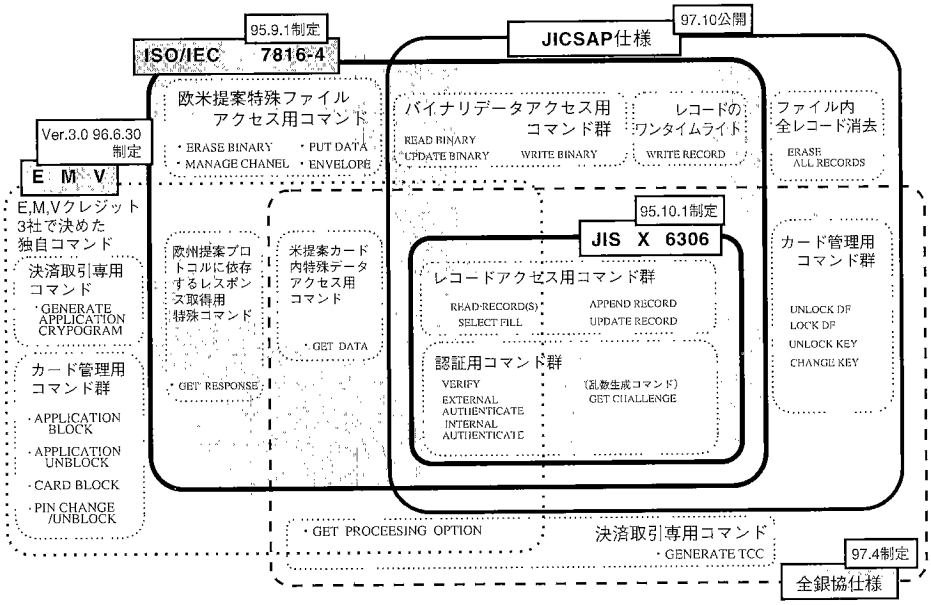
(1) 最初は秘密にすべき固定の暗号鍵をICカードに単純に保管しておき，それを読み出して使用するケース．

(2) 一歩進んで，固定の暗号鍵を保管しておくのではなく暗号鍵を生成するためのプロセスを隠蔽しておくことにより，鍵の保管をより安全にするケース．

(3) さらには鍵と処理プロセスを両方保管しておき暗号化／復号化処理をICカード内で行うようなケース，

というように，よりICカードに重要な役割を持たせつつある．また，暗号化機能だけでなく，公開鍵暗号方式を利用した認証システムをICカードを使用して構築することも行われている．

今後の利用方法の代表例として，近々導入されよう



注：(1) 本包括関係は，コマンド名のみの関係で，各コマンドの機能に関する包括関係は表現していない．したがって，別々のコマンド名でも，機能として同じものもある．また，同じコマンド名でも異なった機能のものもある．

図-4 各標準（コマンドレベル）の相関関係

としているクレジットカードのICカード化がある．この場合には本人確認機能や利用限度額のチェック機能などの，取り引きの正当性，正常性をチェックするロジックをICカード内に持たせておき，不正使用や・事故の発生を極力押さえようとしている．

また，暗号技術を駆使して構築される電子マネーの導入においては，その電子マネーの財布としての役割を担うものとして有望視されているのがICカードである．そのためには，破られない財布として，暗号処理や電子マネーそのものの処理などのプロセスと電子マネーそのものの保管をセキュアに行えるように，1枚のICカードの中にさまざまな機能を凝縮させている．

業界標準

先に述べたように，ICカードについては国際標準が進められているが，すでに各分野において実際の利用が先行している，というのが現状である．国際標準（ISO）や国内標準（JIS）では，物理的な形状や電気的なインタフェースなどを明確に規定しようとしているが，実際にICカードを動作させるための各種コマンド（たとえば，Readコマンド，Writeコマンドなど）については，業界に偏らず共通的に利用できるものに絞って標準化している．したがって，各業界で利用しているICカードは，ISO準拠のカードといっても，通常物理・電気的な部分は準拠しているが，コマンドセットについては，各分野やアプリケーションによって必要なコマンドが異なるため，ISOやJISで規定されているコマンドのうち必要なものと，そのアプリケーション独自に必要な特別コマンドの両方をサポートしている場合がほとんどである．実際の主要なコマンド仕様としては，クレジットカード業界用のEMV仕様，産業・公共分野としてのJICSAP仕様，また，銀行業界用としての全銀仕様などがある．国内で使用されつつあるこれらのコマンドセットレベルの仕様の相互関係は図-4に示すとおりである．

さらに，実際のコマンドや機能の実装について見てみると，たとえば，クレジットカードの場合でも，各カード会社によってもそれぞれ異なることになるようであり，業界標準といっても実際の機能はばらばらになるようである．

非接触型ICカード

現在一番よく使用されているものは，いわゆる接触型ICカードといわれる接触端子を有するものであるが，最近は非接触型ICカードといわれるものが使用されてきている．非接触型ICカードの構造は，前述のとおり，接触端子の代わりにアンテナ（コイル）を有しているもので，リーダ／ライタとの間の通信は，トランスと同じ電磁的結合によって行われている．カードには電池がなく，電力供給も同じコイルで受ける仕組みになっている．

標準化も順次進んでおり，現在仕様がほぼ決まっているのが，密着型といわれるISO／IEC10536であるが，この方式はリーダ／ライタとカードとの通信可能距離が2mmというものであり，接触型とほぼ同様の利用方法に限られるため，実際には，いまだ普及の見通しが立っていない．

仕様項目		1周波方式		2周波方式
		Type A	Type B	Type C
通信距離		10cm	10cm	10cm
電力伝送周波数		13.56MHz	13.56MHz	13.56MHz
データ伝送（PCD→PICC）	周波数	13.56MHz	13.56MHz	（13.56MHz）
	変調方式	ASK100%	ASK10%	（ASK10%）
	サブキャリア	無し	無し	（848KHz）
	サブキャリア変調	−	−	（BPSK）
	ビットコーディング	Modified Miller	NRZ	（NRZ）
データ伝送（PICC→PCD）	周波数	13.56MHz	13.56MHz	（3.39MHz）
	発信方式	Load Switching	Load Switching	（Active）
	サブキャリア	848kHz	848kHz	無し
	サブキャリア変調	ASK	BPSK	（BPSK）
	ビットコーディング	マンチェスター	NRZ	（NRZ）
データ伝送速度	ATR期間中	106kbps	106kbps	106kbps
備考		NTTテレホンカード		

図-5　ISO/IEC14443無線インタフェース仕様

これに対し，通信距離が10cm位までというISO／IEC14443の近接型については，現在すでに入退室ゲートでの本人確認用のカードとして普及が進んできている．しかし，ISOでの標準化はまだ現在進行形である．このような状況の中ではあるが，日本でもNTTのテレホンカードに本方式が利用されることが決まり，定期券のような電子乗車券にも利用することが決まっており，今後の普及が期待されている．ただし，ISO／IEC14443については，現在3つのタイプが提案されている（図-5参照），この中で，ほぼ仕様が固まっているのがTYPE　Aであり，NTTテレホンカードはこの標準に準拠している．電子乗車券については，すでに香港やソウルなどで導入済みであり，日本でも1998年6月から都営地下鉄12号線でフィールドテストの実施が計画されている．このカードの仕様は，ISOのTYPE　Bに似ているが多少異なっており，現在のISOには準拠していない．電子乗車券については，世界中で検討されているが，現段階ですでに実際に稼動している最大のものがISOに準拠していない香港のシステムである．実績からみて，この仕様が今後の標準化に影響を与えていくことも十分考えられる．

残りのTYPE　Cは，TYPE　AとBが1周波型であるのに対し，2周波を利用して全二重通信を可能にしようというものであるが，実質的な審議にはいっていない．

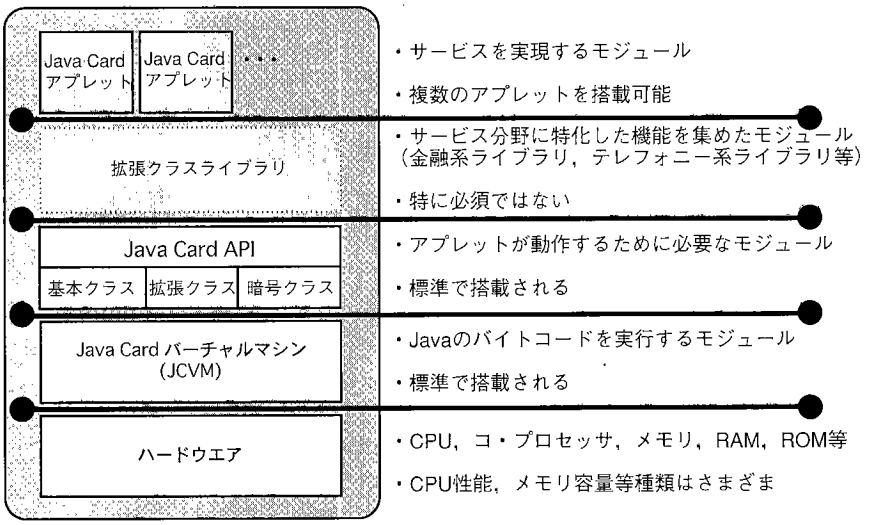
今後は，1枚のカードで非接触型のインタフェースだけでなく，接触型のインタフェースも持っている複合型のカードが作られてきており，移動しながら使う場合は非接触型インタフェースを，移動する必要がない決済などの場合，またすでに接触型のインタフェースのリーダ／ライタが普及しているような場合には接触インタフェースを使用するように，両方のインタフェースを1枚で使用できるようになる．

汎用OS型ICカード

カードの機能は，チップ内のCPUで処理できるようにアセンブラで書かれたプログラムによってすべて実現されている．現在のICカードでは，そのプログラム言語は，それぞれのチップ内のCPUにより異なり，また，そのプログラム自体も必要なカード機能ごとに異なっている．これらのプログラムはチップ内のROMに焼き付けられているのが普通である．したがって，機能の異なるカードはすべて，チップの製造の段階で異なるプログラムを焼き付けることになる．このため，一度カードを作った後で，機能の変更や追加をしたい場合には，カードの製造／配布のやり直しになる．

これに対し，汎用OS型ICカードというのは，プログラムをアセンブラでなく高級言語で作成でき，そのプログラムを後からICカード内にロードして，機能の変更や追加ができるように，パソコンと同様に汎用のOSをカード内に備えているものである．

このようなカードの中で代表的なものとして，現在までのところJavaCardとMULTOSカードの2つがある．JavaCardというのは，その名前のとおり，Java言語で書かれたプログラムがICカード内で実行可能なものであり，JavaCard Forumにおいて，APIの規定が作成されており，オープンな規格として普及を図ろうとしている．これに対して，MULTOSカードは，当初，電子マネーのMondex用のカードとして開発されたものであるが，その後Mondexの開発主体とクレジット業界大手のMaster Cardが中心となってMAOSCOという組織を作り，Mondexに限らず，より汎用的なカードとして普及を図ろうとしているものである．言語は現在のところ，MULTOSカード専用の高級言語であるMEL言語というものを使用してい



※網掛け部はアプリケーションに特化した部分

図-6　汎用OS型ICカードの構造イメージ（Java Cardの例）

るが，将来的にはJava言語もサポートすると発表している．

汎用OS型ICカードの構造イメージは図-6のようになっている．これで分かるように，構造はパソコンと非常に似ており，従来のカードに比べ，より複雑な処理をカード内で行わせることができるようになる．また，これらのカードには，複数のアプリケーション用のプログラムを入れることができるため，多目的利用を目指したカードに適している．しかも後でアプリケーションを追加できるので，必要に応じて機能やサービスを拡大したり，サービス条件をたびたび変更するような利用方法に最適である．

このような機能を，最適に提供できるようにするためには，カードの性能の向上が，実際には不可欠である．カード内に大きなOSを持ち，複数のアプリケーションプログラムを格納するための大きなメモリ容量を持ち，その大きなプログラムを高速で処理するためのより大きなCPUパワーを持ったカードの開発も平行して進められている．メモリ容量は現行の8kバイトから16kまたは32kバイトへと拡大され，CPUも8ビットCPUから16ビットまたは32ビットCPUへとアップグレードされていく計画がある．さらには，Java言語の処理を高速で行えるように専用チップ化する計画も進んでいる．

このような高機能カードについては，前述の2種類のカードのほかにもいくつかの計画があり，注目すべき動向であるといえる．

将来の方向

前述のように，ICカードは，従来のセキュアなポータブルファイルという使い方から，プロセスを隠蔽できるセキュアな小型コンピュータという使い方に変化してきている．使い方も，会社内というような限られた範囲での使用から，汎用IDカード的なものや電子財布のようにより広範囲でオープンな環境での利用の方向に広がってきている．したがって，それに対応してICカードの高機能化，高性能化，高セキュア化が今後も進んでいくと考えられる．

しかし，実際のICカードシステムの導入にあたっては，ICカードを1人1枚配布するとなると，大量のICカードを導入することになり，ICカードのコストが非常に大きなファクタなることが多い．この場合には，高機能，高性能カードではあるが高価であるというICカードより，最適な機能が最適なコストで提供できるカードが必要となり，必ずしもすべてのICカードの高機能化等が望まれているものではない．

また，ICカードの普及は，カードの普及だけではだめであり，それと同時にリーダ／ライタの普及が大前提である．この場合に問題になるのが，ISOに準拠しているといっても，そのISOが接触型だけでなく非接触型もあり，その非接触型にも複数のタイプがあるという状況の中で，社会インフラとしてのリーダ／ライタをどのような仕様でどのように設置していくか，ということである．

さらに，ICカードの普及というのは，ディジタル情報の普及ともいえるわけであり，当然ながらディジタル化に対応した法制度の整備が不可欠である．特に情報保護やカード偽造・情報偽造などに対する法整備を事前に進めておくことが，健全なICカード社会を形成する上で，大切なことである．

（平成10年4月2日受付）