

IC カードシステムの市場・技術動向

IC Card Systems—Market and Technical Trends

北川 修身
O. Kitagawa

谷口 昇二
S. Taniguchi

三浦 謙二
K. Miura

IC カードの普及がいよいよ本格的になってきた。ネットワーク技術の急速な進展に伴う本格的な情報化時代の到来が、IC カードの普及に弾みをつけている。これまで実験および試行が中心であった IC カード利用システムも、電子マネーシステムなどにおいては実用化のレベルへと変わりつつある。今後のデジタル社会のキーマディアとして、IC カードはその地歩を一歩一歩固めつつある。

技術的にはカードの応用範囲の広がりにつれ、カードオペレーティングシステム(COS)のオープン化や暗号処理回路の搭載など新たな課題が登場し、技術開発競争も激しくなっている。

The use of smart cards is rapidly spreading on a wide scale, driven by the progress of information and network technologies. Until now, most application systems using smart cards have been on a trial basis. Some systems have recently reached the phase of practical use, however, especially electronic money systems using smart cards.

Smart cards are thus becoming a key medium for the approaching digitized information society. Technical issues are now being raised such as the implementation of an open platform for card operating systems and the mounting of coprocessors for data encryption, and competition in smart card development is forecast to become increasingly severe.

This paper discusses the trends in the market and technologies for smart cards, and examines the future prospects in this field.

1 まえがき

このところ IC カードが、またスポットライトを浴びている。今から 10 年ほど前にも、IC カードはニューメディアブームの主演として脚光を浴びていた時期がある。そのときは、全国各地で IC カードを利用した各種の実験が行われたが、やがて下火となりブームは終わった。

今回のブームは前回と比較して、情報のデジタル化の進展およびネットワークの普及という点で背景的に異なっており、いよいよ本格的な IC カード時代の到来を予感させるものである。当社は、1984 年 12 月に最初の IC カードシステムを稼働させて以来、端末機能をもカードに取り込んだ多機能カードの開発や種々の IC カード応用システムを開発してきた。

今後のデジタル社会のキーマディアとなる IC カードは、半導体技術の進歩とともに進化し、社会生活の必需品としていろいろな分野での応用が期待される。以下、IC カードシステムの市場の動きと技術動向を述べ将来を展望する。

2 市場の動き

図 1 に世界の IC カード発行枚数の推移および予測、図 2 に IC カードの地域別売上げシェアを示す。

IC カード市場としては欧州が先行しており、日本や北米

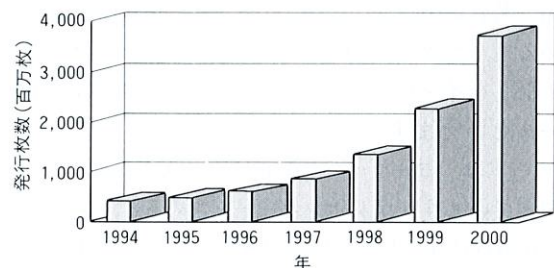


図 1. 世界の IC カード発行枚数の推移および予測 2000 年へ向け、IC カード市場は急速に立ち上がることを予測している(当社調べ)。

Forecast trend in IC card issuance, 1994-2000

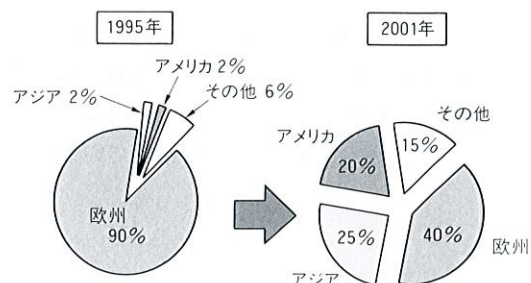


図 2. IC カードの地域別売上げシェア 世界を欧州、アジア、アメリカ、その他に 4 区分し、それぞれの地域ごとのカード売上げシェアを示す(当社調べ)。

Shares of IC card sales in each region

はいまだ市場の黎明(れい)期にある。しかし黎明期にある日本や北米市場も、2,000年へ向けICカード市場の立上りが本格化するものと予想されている。欧州市場が先行してきた最大の要因は、テレホンカードのICカード化の進展である。ヨーロッパではフランスを中心に、10年も前にテレホンカードのICカード化が始まり、96年の総発行枚数は4億枚近くに達している。このテレホンカードに使われるICカードは、CPUのないものであり、今後普及拡大が予想されるCPU付きのハイセキュリティ、高性能のものとは異なる。呼び名も“チップカード”と一般のICカードとは区別されており、安価なことが特長となっている。

日本においては、テレホンカードとして98年から現行の磁気カードに代わり、無線ICカードが採用されることが最近決定された。このテレホンカードの普及が、日本においても欧州同様、ICカード市場の立上りに大きく寄与することが期待されている。テレホンカードの分野は今後もICカード市場の柱の一つであり、その利用は拡大され、2000年には年間21億枚規模の市場となることが予想される。

テレホンカードへの応用がICカードの普及を促進し、市場をつくり出してきたが、最近新しい応用分野が次々と現れており、今後もその応用分野はますます広がるのを見せている。これまではICカードというと、とかく磁気カードの次世代というとらえかたでその応用範囲が考えられがちであったが、情報のデジタル化の進展やネットワークの普及拡大に伴い、ICカードでなければ実現できない応用分野が続々登場している。その代表的な例が電子マネーであり、電子マネーを使う電子商取引(Electronic Commerce)の分野である。電子マネーはICカード型とネットワーク型のものが存在するが、ICカード型については世界各地でいろいろな実験が行われており、その内一部は実用段階に入りつつある。代表的なICカード型電子マネーとしてはVISACash、プロトン、モンデックスがあり、それぞれが独自の展開を図っているが、現時点でとらえるとプロトンがその域で一步リードしている(プロトンとして発行された電子マネーは世界各地で2,000万枚近くに達していると言われている)。

これら国際的な規模で展開する電子マネーのほかに、ドイツではゲルトカルテという電子マネーシステムが稼働し始めた。ドイツ国内限定のローカル仕様とはいうものの、すでに5,000万枚以上のカードが発行され、電子マネーとしては最大規模となっている。日本においても、今年以降電子マネーの実用実験が種々予定されており、電子マネー時代へ向け動きが活発化しつつある。代表的なものとして神戸地区でのVISACash(97年10月開始)、大宮地区での郵貯マネー(98年1月開始)、渋谷地区でのVISACash(98年6月開始)、新宿地区でのNTT型電子マネー(98年10月開始)があり、それぞれの実験とも将来の電子マネー時代

をにらみ、その先兵として利用者の反応を含めたノウハウの蓄積をねらっている。

電子マネー以外の分野では携帯電話用SIM(Subscriber Identity Module)カードとしてのICカードの利用が欧州を中心に広がっており、GSM(Global System for Mobile communications)の普及とともに、世界各国へその利用の拡大が予想されるし、衛星有料放送の普及に伴い、スクランブルの解除とペイパービュー方式(視聴した時間だけに課金する方式)実現のためのICカードの利用についても今後の拡大が予想されている。

一方クレジットカード業界では、その偽造や不正使用による被害金額が無視出来ない水準になっており、それらを減少させる意味で、従来の磁気カードからセキュリティの高いICカードへの移行が具体化している。クレジットカード業界はICカードのISO標準(ISO:国際標準化機構)が制定された後、すぐに業界標準の作成に着手、95年6月EMV^(注1)標準として制定した。

このEMV標準が今後の金融系ICカードの仕様のベースであり、電子マネーの仕様についてもほとんどがEMV仕様を踏まえたものになっている。

これらのほかにも国民カード、健康カード、社員証などの分野へもICカードの利用が広がっており、表1に示すように今後ICカードの発行枚数は急増すると予測される。2000年にはCPU付ICカードの発行枚数が22億枚規模に達し、名実ともにデジタル時代のキーメディアとして社会生活になくてはならない存在になることが予想される。

表1. 分野別のICカード発行枚数の推移および予測
Forecast of IC card issuance in each field

(単位:百万枚)

分野	年	1994	1995	1996	1997	1998	1999	2000
テレホンカード		310	350	400	450	650	900	1,400
移動体通信		9	10	12	15	25	35	50
保健・医療		62	70	75	80	100	150	300
金融		20	30	50	100	200	400	600
IDカード		1	10	30	80	150	300	400
Pay TV		10	15	20	80	90	100	100
交通関係		1	2	10	15	20	100	200
アミューズメント		1	1	1	20	100	250	500
自販機		4	4	4	4	10	20	100
その他		0	0	0	0	10	30	100
合計		418	492	602	844	1,355	2,285	3,750

当社調べ

3 技術動向

ICカードの技術要素を図3に示す。

(注1) EMVは、クレジットカード業界の大手Europay, MasterCard, VISAの頭文字。

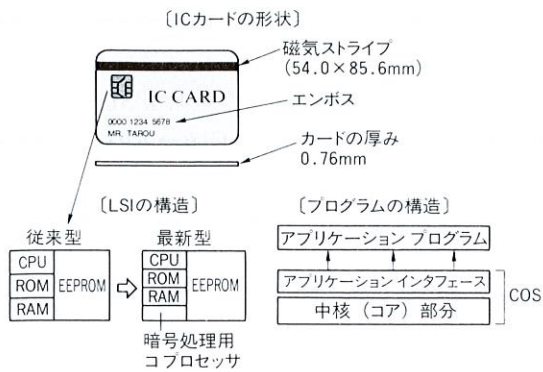


図3. ICカードの技術要素 ICカードがもつ技術要素の主なものであるLSIの構造およびCOSの構成を示す。

Technical factors involved in IC cards

ICカードの機能・性能は、カードに埋め込まれているLSIの機能・性能そのものである。ISOが制定したカード化された後のカードとしての物理的試験をクリアするためには、一般にLSIの大きさは5mm×5mm以下、つまり25mm²以下であることが要求される。この小さなスペースの中に、中央制御装置としてのCPU、カードのオペレーションシステムが書込まれるROM、ワーキングメモリとしてのRAM、データ記憶用メモリとしてのEEPROM (Electrically Erasable and Programmable ROM)、それにプラスして最近では暗号処理専用回路のコプロセッサが配置される。これらのものを5mm×5mmのスペースに入れ込む微細加工技術が基本技術であり、この技術の進歩とあいまってLSIそのものの機能・性能がどんどん進化していくわけである。現在はその制約からCPUは8ビットのものが主流であるが、今後は16ビットさらには32ビットへの進化が予定されている。また、メモリについても現時点の最大容量は8Kバイトが主流であるが、今後は16Kバイト、32Kバイトと拡大することが期待されている。

こういったICカードの進化は、小さなコンピュータがカードの中に入る時代が来ることを意味する。このことは、現在のパソコンの能力が、かつての大型コンピュータ並みになっているコンピュータの進化の速さを見れば、決して夢物語ではない。

微細加工技術のほかに、ICカードに要求される技術として耐タンパ技術がある。ICカードが電子マネーやクレジットカードなどの金融決済系の媒体として利用されるに伴い、物理的に外部から内部をのぞかれたり、変えられたりする可能性を極小化する必要がある。もちろんLSIの内部をのぞくことは、CPUを使いロジックを組むことで論理的にブロックされているが、より安全性を高める意味でこういった物理的な処置も要求される。現在のところこの技術は、製造メーカーの製造技術やノウハウに依存している部分が大き

いが、この技術を体系化する研究も進んでいる。

ICカードの大きな特長の一つに、多機能ということがある。従来の磁気カードではその能力から一つの機能しか実現出来なかったが、ICカードになると記憶容量の大きさや内部コントロール機能から、多種の機能を内在するカードとすることが可能になった。こういった多機能をコントロールし、安全性をも考慮して実現するのがCOSである。このプログラムはLSI内部のROMに書かれるが、この内容についてはそれぞれのカードメーカーが独自なものを作り上げている。小さいROM容量に格納されるプログラム(この場合はCOS)は、メモリをふんだんに使えるようになったコンピュータの世界と異なり、独自の技術ノウハウを必要とする。そのうえ、このプログラムはROMに焼き付けられるため、ひとたびLSIを起こすと変更できなくなる。また、プログラムがROMに焼き付けられるため、カードユーザはこういった機能を盛り込むかをかなり前もって決める必要がある。しかもその開発はメーカーに依存しなくてはならない。ユーザーズが多様化する将来を見据えると、このプログラムはダイナミックに変えることが必要とされるし、ユーザプログラマブルであることが望ましい。こういった要求にこたえようとするのが、COSオープン化の流れである。当社はこの流れに沿うものとして、Java^(注2)言語を使うJavaCard^(注3)の開発に取り組んでいる。

電子商取引の進展に伴い、その決済手段としてのICカードの存在がクローズアップされてきた。インターネットを使った商取引においては、情報の暗号化が避けられない。情報の暗号化に必要な暗号鍵(かぎ)の保管手段としてICカードは適しており、そういった利用が広がっている。ICカード内で暗号化処理をする場合、公開鍵方式においては鍵の長さや処理演算の複雑さから、現行の8ビットCPUでは時間がかかり過ぎるという問題がある。これを解決するために、暗号処理専用の回路であるコプロセッサを配置し、暗号処理時間を短縮する方法が採られている。このコプロセッサ回路の開発・設計技術力もICカードの性能を左右する大きな要因である。公開鍵の鍵の長さがどんどん長くなる傾向の中、より長い鍵を扱え、かつ、より短い時間で処理できる回路の実現へ向け、開発競争が厳しさを増している。

4 あとがき

ICカードは10年以上も前に登場したが、なかなか本格普及しない状況が続いていた。その理由としては、国際標準が決まらなかった(95年ようやく決定)ということが挙げ

(注2) Javaは、米国Sun Microsystems社の商標。

(注3) JavaCardは、米国Sun Microsystems社の商標。

られるが、やはりICカードの特性を生かした利用形態の決め手が出現しなかったことが一番大きな普及阻害要因であった。しかし、ここ数年のネットワーク技術の急速な進歩と、パソコンの飛躍的な普及に伴う情報化社会の進展が、ICカードの活躍の舞台を提供した。

情報化社会の進展とともに情報セキュリティのニーズが急拡大し、その実現手段としてICカードが脚光を浴びているのである。パソコンにICカードのリーダライタが標準装備されることが確実視されており、ICカードは情報化時代のキーメディアとして、その応用範囲をますます広げることが期待される。

当社はグループ会社とも連携し、LSI、カード、関連端末、応用システムとICカードに関するすべての領域での技術開発をしており、今後増大するICカード利用システムニーズ

に対応していく所存である。



北川 修身 Osami Kitagawa

情報・通信システム新規事業企画室 副室長。
情報通信システム市場での新規事業の開発に従事。
Information & Communications Systems New Business Planning Office



谷口 昇二 Shoji Taniguchi

情報・通信システム新規事業企画室 カードシステム事業開発担当部長。カードシステム事業の開発に従事。
Information & Communications Systems New Business Planning Office



三浦 謙二 Kenji Miura

機器事業部 カードシステム営業部部長。
カードシステムおよびカードシステム関連端末機器の営業に従事。
Social Automation Systems Div.