

ICカードシステムの動向

Trends of IC Card System

小林 豊明
Toyoaki Kobayashi

要 旨

ICカードは、暗号処理、認証処理、ICカード内のデータへのアクセス管理といったセキュリティ管理に優れているため、磁気カードに代わる新たなデータキャリアとして注目されている。金融・決済系、交通系、通信系、娯楽系を中心に磁気カードからICカードへの移行・導入が進んでおり、今後、ICカードは磁気カードに代わる新たな社会インフラを形成する。

1. ま え が き

ICカードは、セキュリティ、多目的、携帯性という特徴を持つデータキャリアである。ICカードの移行・導入により、磁気カードでは実現できなかったセキュリティの強化、新たなサービスの提供、サービスの多様化が可能となる。現在、テレホンカード、有料道路自動料金収受システム(ETC; Electronic Toll Collection system)、定期券・乗車券等、さまざまな分野でICカードへの移行・導入が進んでいる。また、磁気カードというインフラを確立しているキャッシュカードおよびクレジットカードも、ICカード化に向けた準備が進められている。ICカード後進国の日本において、ICカードがいよいよ普及フェーズに入り、そして新たなインフラになりつつある。本稿では、ICカードの種別と特徴、ICカードの技術に触れた後、ICカードシステムの動向について述べる。

2. ICカードの種別と特徴

表1に、ICカードの種別と特徴を示す¹⁾。ICカード



小林豊明
システムソリューションカンパニー カスタマコネクティブシステム事業部 ハードシステム開発第三部 ICシステム開発チーム 担当






は、リーダライタとのインタフェースの違いにより、外部端子付きICカード、外部端子なしICカード(コンタクトレスICカード)、さらに両方のインタフェースを持つ兼用ICカードに分類される。コンタクトレスICカードは、リーダライタとの通信距離により密着型、近接型、近傍型に分類される。外部端子付きICカードは、国内外で最も普及しており、電子マネー等の機能を持った決済カードとしての実績が高い。コンタクトレスICカードは、外部端子付きICカードでは困難だった交通分野における定期券や乗車券等への適用が可能であり、今後、交通分野を中心に普及していくものと考えられる。兼用ICカードは、外部端子付きICカードとコンタクトレスICカードのメリットを併せ持ち、たとえば、乗車券の購入は外部端子インタフェースで行ない、改札の入出はコンタクトレスインタフェースで行なうという運用が可能である。

3. ICカード技術

3.1 ICチップ

ICチップのプロセッサの主流は8ビットであるが、アプリケーションの高速化のため16ビット、32ビットプロセッサが開発されている。メモリは、電気的に書き換え可能なEEPROM(Electrically Erasable Programmable ROM)が使用されており、500バイト前後の低容量のものから32Kバイトの大容量のものまで、

表1 ICカード種別と特徴
Table 1 Category and features of IC cards

種別	外部端子付きICカード	外部端子なしICカード(コンタクトレスICカード)				兼用ICカード	
		密着型	近接型		近傍型	ハイブリッド型	デュアル型
			Type-A	Type-B			
インタフェース	 ICモジュール(接触インタフェース)	 ICチップ コンタクトレスインタフェース	 ICチップ コンタクトレスインタフェース		 ICモジュール(接触インタフェース)	 ICモジュール(接触インタフェース)	
規格	ISO/IEC 7816	ISO/IEC 10536	ISO/IEC 14443		ISO/IEC 15693		
通信距離		2mm程度	数cm		~70cm程度		
通信速度	9.6Kbps~	9.6Kbps~	106Kbps~		~26Kbps		
特徴	会員カードから電子マネーまで幅広く使用されている	通信距離が2mm程度と短い。リーダーライターに挿入する、または置くという操作が必要である	CPUを搭載できないため、ワイヤードロジックにてデータのリードライト機能、セキュリティ機能を実現している	CPUを搭載することができるため、外部端子付きICカード(CPU有り)と同等の機能を実現することができる	主としてリードオンリーのため、物流管理等の用途に使用される	外部端子付きICカードのアプリケーションとコンタクトレスICカードのアプリケーションの独立性が高い	外部端子付きICカードのアプリケーションとコンタクトレスICカードのアプリケーションのデータ共有ができる

利用形態により選択することができる。なお、書込速度、書き換え保証回数および消費電力の点から、FRAM^{*1)}(Ferro-electric RAM)が注目されている。

3.2 セキュリティ

DES(Data Encryption Standard)等の共通鍵暗号方式、RSA^{*2)}等の公開鍵暗号方式を使用し、有線・無線伝送路上のデータの暗号化、通信対象との相互認証、デジタル署名等を実現する。共通鍵暗号方式はソフトウェアでの実装が多いが、公開鍵暗号方式の場合、処理に時間がかかるため、専用のコプロセッサを搭載し、処理速度の高速化を図っている。また、公開鍵暗号方式で使用する秘密鍵および公開鍵をICカード内部で生成し、格納することが可能なものもある。これにより秘密鍵を不正に取得する事が不可能となり、より安全なシステムを構築することができる。

3.3 汎用ICカードOS (Operating System)^{2,3,4)}

汎用ICカードOSは、ICカードへのアプリケーションの追加/変更/削除およびその実行可否を管理するセキュリティ管理の機能を提供する(図1)。アプリケーションの追加/変更/削除機能により、サービス提供者および利用者は、ICカードを多目的に利用できる。たとえば、サービス提供者は、カード流通後に現在提供しているサービスを拡張したり、異なるサービス提供者が新たなサービスを追加することができる。また、利用者がそれらのサービスを取捨選択できる。セキュ

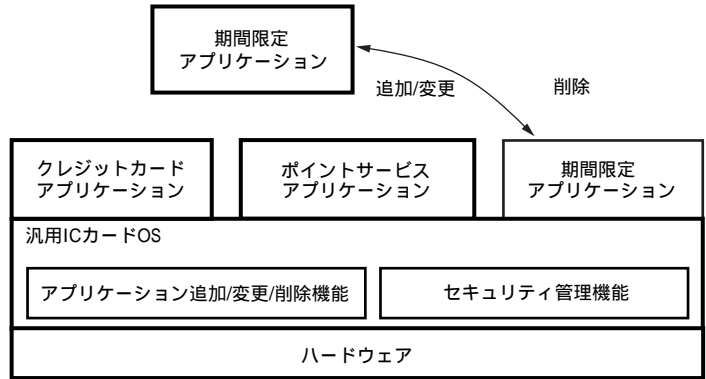


図1 汎用ICカードOSの機能
Fig. 1 Functions of a general-purpose IC card OS

リティ管理機能は、不正者によるアプリケーションの追加/変更/削除の防止、追加/変更するアプリケーションの正当性確認といった管理を行ない、安全なサービス運用を提供する。汎用ICカードOSとして代表的なのは、以下のものである。

- MULTOS^{*3)}(Multiple Application Operating System)
- Java OS^{*4)}
- Windows for Smart Card^{*5)}

4. ICカードシステムの動向

ICカードの普及を牽引する金融・決済系、交通系、通信系、娯楽系の4つの分野について述べる。

4.1 金融・決済系

(1) クレジットカード

*1) FRAMはラムトロン社の米国における登録商標。 *2) RSAの名称は発明者であるRivest, ShamirおよびAdlemanの頭文字による。 *3) MULTOSはMondex International Ltd.の登録商標。 *4) Javaは米国Sun Microsystems, Inc.の米国およびその他の国における商標または登録商標。 *5) Windowsは米国Microsoft Corporationの米国およびその他の国における商標または登録商標。

クレジットカードの不正使用や偽造による被害総額は、97年188億円、98年216億円、99年272億円と急増している⁵⁾。このうち、偽造カードによる被害額は、97年12億円、98年28億円、99年91億円と3年間で7倍以上に増加している⁵⁾。このことから偽造防止の対応策の1つとしてICカードへの移行が急がれている。ICカード化により、クレジット決済だけでなく、電子マネー機能、購入履歴管理機能等のアプリケーションを搭載し、決済の多様化および新たなサービスの提供が可能となる。

(2) キャッシュカード

日本版デビットカードシステム(J-Debit)がサービスを開始した。デビットカードは、キャッシュカードを使用した即時決済方式であり、利用者の口座残高の範囲でショッピングができる。利用者は既存のキャッシュカードをそのまま利用できるため、今後デビットカードの利用が増加すると考えられる。

一方、利用者および利用場所の増加により、クレジットカードと同様にその不正使用が懸念される。今までキャッシュカードは、銀行という安全な環境に設置されたATMで使用されていたが、今後はデパートやスーパーの端末で使用される。つまり、悪意のある者による端末偽造、カード偽造等の出現が予想される。これへの対応策の1つとして、ICカード化が必須になる。クレジットカードと同様、ICカードに電子マネー機能、振込カード機能等のアプリケーションが搭載され、決済の多様化および新たなサービスの提供が可能となる。現在、民間金融機関が中心となり、ICカード規格を共通化するための協議会が設立され、ICカード化に向けた作業が進められている。

(3) 電子マネー

現在、ICカードを使用した電子マネーの実証実験が各地で行なわれている。このICカード型電子マネーは、オンラインショッピングにおける必要不可欠な決済手段になる。たとえば、ネットワークインフラの整備により、家庭で音楽、ゲーム、動画等のデジタルコンテンツをダウンロードできるようになった場合、有料コンテンツのダウンロードサービスは急増する。恐らく、その料金は数百円から2000円程度の小額であり、まさに電子マネーがターゲットとする料金帯である。家庭にリーダーライタがあれば、利用者は家庭でICカードに電子マネーをチャージし、ダウンロードサイトでの支払いに使用することができる。現在、ICカード型電子

マネーは、申し込みが必要、使用可能な店舗およびチャージする端末が少ない等の理由から、利用率は低い。しかし、今後はオンラインショッピングの普及により、バーチャル(インターネット上)での決済としてICカード型電子マネーの利用率が高まるであろう。上述のデビットカードシステムはオンライン決済であり、ある程度のトランザクションコストが生ずる。トランザクションコストの削減のために、デビットカードと決済価格帯が近く、オフライン決済という利点を持つICカード型電子マネーが、リアル(実際の店舗)へ普及するであろう。

4.2 交通系

(1) 定期券・乗車券

香港、韓国では、鉄道、バスなどの乗車券としてコンタクトレスICカードを使用した料金自動徴収システムが本格運用されている。現在、国内でも、鉄道自動改札へのコンタクトレスICカードの本格導入に向け、準備が進められている⁶⁾。磁気式の場合、自動改札機に複雑な搬送機構が必要であり、機器の導入およびメンテナンスのコストが高くなる。コンタクトレスICカードの場合、自動改札機にかざす、または触れるという操作によってデータへのアクセスができるため、コストが削減できる。また、コンタクトレスICカードに電子マネー機能、ポイントサービス機能等のアプリケーションを搭載することにより、駅構内、駅ビル等でのキャッシュレス化および新たなサービスの提供が可能となる。

(2) ETCカード

高度道路交通システムの一分野であるETCにICカードが導入される。ETCとは、車に搭載された車載器と料金所に設置された道路側アンテナとの間で無線通信により料金情報をやり取りし、料金所をノンストップで通過することができるシステムである⁷⁾。ETCカードには外部端子付きICカードが使用され、これに料金支払者の契約情報が記録されている。当初はクレジット支払による口座引き落としで運用されるが、現在のハイウェイカードのような前払いへの対応が検討されている。電子マネー機能、ポイントサービス機能等のアプリケーションを搭載し、パーキングエリア、駐車場、ガソリンスタンド等でのキャッシュレス化および新たなサービスの提供が可能となる。

4.3 通信系

(1) テレホンカード

ICテレホンカードの導入が開始された。ICテレホンカードには、コンタクトレスICカードを採用している。ICカード化により変造は困難となる。また、ICカードの利点を生かし、通話中に電話番号等をICテレホンカードに登録したり、登録した電話番号等を別のICテレホンカードにコピーすることができる⁸⁾。携帯電話の普及が進む中、コンタクトレスICカードおよび公衆電話というインフラを利用した新しいサービスをいかに提供していくかが、今後の課題である。

(2) SIM (Subscriber Identity Module)

欧州で使われるデジタル携帯電話の標準規格であるGSM (Global System for Mobile Communications) では、すでに外部端子付きICカードのSIMを携帯電話に搭載した各種サービスが提供されている。SIMは、本人情報、課金情報、相手先の電話番号、各種サービス情報等を記録している。利用者が携帯電話を新しい機種に変更する場合、古い機種で使用していたSIMを新しい機種にセットすることで、簡単に機種の変更ができる。また、オンラインショッピングにおいて、SIMに電子マネー機能、クレジット機能等のアプリケーションを搭載することにより、携帯電話で決済ができる。今後、国内で使用される携帯電話への搭載も検討されており、携帯電話を使用したモバイル決済としての利用が期待される。

4.4 娯楽系

(1) 電子チケット

コンサート、映画、スポーツ等のチケットをオンラインショッピングで購入し、チケット情報を電子チケットとしてICカードに登録し、会場での入場管理、会場案内等のサービスに使用するという電子チケットシステムがある。電子マネー同様、家庭にリーダーがあれば、利用者は家庭で電子チケットの購入が可能である。また、電子チケットは顧客間での転売・譲渡が容易なため、現在成長中のネットオークションにおいて、ICカードを使用した電子チケット転売サービスの提供が可能となる。

5. あ と が き

ICカードの技術およびICカードシステムの動向を述べた。ICカードは、セキュリティ、多目的、携帯性と

いう特徴を持ったデータキャリアである。さまざまな分野で、ICカードへの移行・導入が進んでいる。一方、ICカード化による事業性が見えないということでICカードへの移行・導入に踏み切れない業種もある。

また、現在のICカードシステムは、ICカードの持つセキュリティ、携帯性という特徴を利用したものであり、多目的という特徴を十分に活かしていない。ICカードには、サービス提供者の異なる複数のアプリケーションを共存できる。そして、ICカードシステムは、サービス提供者ごとのアプリケーションを融合し、マルチアプリケーションという新たなサービスを利用者に提供することができる。つまり、ICカードの多目的という特徴により、ICカードシステムは、サービス提供者間の提携を生み、新たなマーケットが創出され、ICカードへの移行・導入に対する明確な意義が生まれてくると考える。当社は、電子マネーやデビットカードなどの決済システム、決済端末、発券端末、ETC向け車載器等の開発を通して蓄積した経験と実績をもとに、マルチアプリケーションに対応したトータルなソリューションを提供していく。

6. 参 考 文 献

- 1) (株) 中日社：非接触型ICカード，産業情報シリーズ，No64，p.15，1999
- 2) MULTOS (WWW pages)
<http://www.multos.com/>
- 3) Sun Microsystems (WWW pages)
<http://java.sun.com/products/javacard/>
- 4) Microsoft Corporation (WWW pages)
<http://www.microsoft.com/windowsce/smartcard/>
- 5) 通産省に偽造カード刑罰規定の法制化要望(ブルームバーグ)記事2000年3月23日
- 6) JR東日本ホームページ，JR東日本ニュース，平成12年2月25日
<http://www.jreast.co.jp/news/nr/20000206/index.html>
- 7) 建設省道路局ITSホームページ
<http://www.its.go.jp/ITS/j.html/right.html>
- 8) NTT東日本ホームページ，ICカード公衆電話
<http://www.ntt-east.co.jp/ptd/icpublic/index.html>