非接触次世代ICカードとは？

for your information

正会員 大山 永昭†

キーワード：非接触ICカード，マルチアプリケーション，NICSSフレームワーク，住民基本台帳カード，行政連携カード

1. ICカードとはなんですか？

ICカードとは、キャッシュカードやクレジットカードの大きさのカード内に、ICチップ（半導体で作られた集積回路）を埋め込んだものです。その種類は、中央演算装置（CPU：Central Processor Unit）およびインタフェースの接点の有無により4種類に大別されます。CPUの有無は、ICカードの機能に大きく影響するため、CPU付きを単なるメモリーカードと区別するために、スマートカードと呼ぶことがあります。また接点のないICカードには、その動作範囲がリーダ/ライタとの距離により密着型（～約3mmまで）、近接型（～約10cmまで）、近傍型（～1mまで）、遠隔型（数m）の4種類があります。

2. ICカードはどのように利用されるのですか？

ICカードの利用法は、重要な情報をカードに記録しオフラインで利用するデータキャリと、ネットワーク経由でデータベース等にアクセスするための認証デバイスとしての使い方に大別されます。データキャリの使い方では、ネットワークを必要としないという利点がある反面、記録できるデータ量にはカードの記録容量の制限が存在します。これに対し認証デバイスとしての使い方は、この逆の特性を有するため、

両者は相補的な関係になります。したがってICカードを上手く利用するには、これらの利用法の特性とアプリケーションの運用環境等を考慮することが重要ですが、今後はネットワークの普及やより高度なセキュリティを必要とする等の理由により、認証デバイスとしての利用法が増えると予想されます。

近年、ICカードの導入が行われている主たる理由は、カードの偽造や変造を防止することと、マルチアプリケーション等の新たな利用法を実用化することに大別されます。前者は、従来のテレホンカードやクレジットカード等の置き換えとして、後者は、住民基本台帳カードや市民カード等として開発導入されようとしています。

3. なぜICカードなのですか？

ICカードは、1970年代に試作されて以来、欧州においてはプリペイド型のテレホンカードや決済用のカードとして広く普及しています。我が国においても、保健医療情報を記録する保健医療カードや商店街等の各種のポイントカード、さらには近年開始されたICテレホンカード等へ応用されています。これらは、我が国のICテレホンカードを除いて皆、接点付きのICカードです。

CPU付きのICカードが有する重要な機能としては、カード内に作られるファイルへのアクセスコントロールと暗号演算があげられます。具体的には、前者は各ファイルに設定された鍵の照合によりファイル内のデータへのアクセス管理を、後者はカード内に組込ま

れた暗号ソフトウェアとカード内に記録されている暗号鍵を用いて、与えられたデータの暗号化を行う機能です。これらの重要な機能は、CPUにより実現されますが、比較的簡単なアクセスコントロールのみを必要とする応用例では、カードの生産コストを減じるために、ワイアードロジックを用いた廉価版のICカードも用いられています。一方、暗号演算の機能は、電子商取引や電子政府サービス等、電子署名に代表される高度な暗号処理を必要とするアプリケーションの進展にともなって、その有効性が認識されつつあります。

4. なぜ非接触なのですか？

非接触方式のメリットとしては、リーダ・ライタのメンテナンスフリー化と操作性の向上をあげることができま。前者は、接点を持たないことやカードの挿入排出等に使われる機械的な稼動部がないことによります。具体的には例えば、公共の場に置かれる端末等に誰かが過って汚れたままのカードを挿入すると、リーダ/ライタの接点が汚れてしまい、リーダ/ライタの清掃を行わなければならないになりますが、この清掃を含めたメンテナンスにかかる費用を、非接触方式では大幅に減らすことができます。一方後者は、カードの裏表等を意識せずに使うことができることを意味します。特に、近年本格的に導入された鉄道のカードでは、財布に入れたままで自動改札機を通過できる等の利便性を持っています。

さらに、産業政策的には欧州で普及している接触式ICカードを越え、日本

†東京工業大学 フロンティア創造共同研究センター

"Development of Next Generation Smart IC Card System with Contactless Interface" by Nagaaki Oyama (Tokyo Institute of Technology, Frontier Collaborative Research Center, Tokyo)

のカードシステム産業を育成するために、上記のような利点を有する非接触式ICカードの普及を推進しています。

5. 次世代カードとは何ですか？

従来のICカードは、価格を抑えるために、カードの機能やCPUの処理能力さらにメモリー等をカードの利用目的に合わせて作られることが一般的でした。また、1つのアプリケーションで用いるカードの総数も、数万枚から多くても数百万枚でした。そのため、少量多品種生産になり、結果的に大量生産による価格の低下が実現しませんでした。この問題を解決するために開発されたのが次世代ICカードです。機能的には、マルチアプリケーションをサポートするために、カード内のメモリーをアプリケーション毎に割当て、各アプリケーション間の独立性を確保しています。その結果、あたかも従来の複数のICチップが1つになったかのように見えると共に、搭載されるアプリケーションに合わせた機能を同一カード内に複数実現することができます。

このような機能が実現されたことにより、ICカードをインターネット等のネットワークに次ぐ第2のインフラとして位置付けることができます。具体的には電子マネー等の決済系や電子政府等に用いる公的分野系、さらには電子チケット等の交通系等のさまざまな分野に共通して使える次世代ICカードが試験運用されています。さらに次世代ICカードは、今後構築されるIT社会のパスポートとして期待されており、その大規模な普及は、ICカードの大量生産と価格の低下に繋がると予想されています。

図1 次世代ICカードシステムのプレーヤモデル

6. どのような取組みがなされているのですか？

非接触次世代ICカードの開発は、1999年に経済産業省(当時は通産省)の主導により行われ、その後、2000年にこのカードを用いた大規模な実証試験が、54の自治体の協力を得て実施されました。これらの成果から、2003年8月に配布が予定されている住民基本台帳カードや、行政連携カードとして採用される旨が決定しています。また、次世代のICカードでは、図1に示すプレーヤモデルを基礎としているため、カード利用者がカードに載せるサービスを選択できるようになりました。

このような機能は、現時点では国際標準になっていないため、現在、欧米等の諸外国と技術的な意見交換を含めてさまざまな協力を行っています。さ

らにこの機能は、ネットワークに接続される情報家電等を、安全かつ確実にリモートコントロールするための基盤技術として注目されています。これらを実現すれば、次世代ICチップは大量に生産されるため、大幅な価格の低下を実現することが可能になると期待されます。

(2002年4月17日受付)

大山 永昭

1982年、東京工業大学大学院総合理工学研究科物理情報工学専攻博士課程修了。1983年、東京工業大学工学部附属画像情報工学研究施設助手。1986～1987年、アリゾナ大学放射線科研究員(画像再構成についての研究)。1988年、東京工業大学工学部附属画像情報工学研究施設助教授を経て、1993年より、同教授。現在、同大学フロンティア創造共同研究センター教授兼任。専門分野は医用画像工学、光情報処理、工学博士。