

IC カードの実際と課題

吉田 竜、真壁 聡子、平田 真一
日本電信電話株式会社 情報流通プラットフォーム研究所
E-mail;yoshida.hajime@lab.ntt.co.jp

概要 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いる。本稿では、IC カードの技術及び課題について述べる。

Reality and issues of Smart Cards

Hajime Yoshida, Satoko Makabe, Shinichi Hirata
Information Sharing Platform laboratories, NTT
E-mail;yoshida.hajime@lab.ntt.co.jp

Abstract Recently, a smart card is very paid to attention as a high security and high performance device as electronic commerce spreads. In this paper, we described the technology and the problems of the smart cards.

1. 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いる。本稿では、IC カード技術ならびにその課題について述べる。

2 IC カードとは

2.1 特徴

IC カードとは、IC (Integrated Circuit : 集積回路) チップが内蔵されたカードであり以下の特徴を持つ。

- (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。

2.2 種類

IC カードは、通信方式により接触型と非接触型に分類される (図 1)。非接触型 IC カードは更に IC カードとリーダライタ間の通信距離により密着型 (~2mm)、近接型 (~10cm)、近傍型 (~70cm)、遠隔型 (数 m) に分類できる。特に、近接型は交通、通信、決済の分野で注目されており、テレホンカードや乗車券に採用されている。

IC カードの標準化は ISO (International Organization for Standard) により行われており、接触型、密着型の標準化が完了している。[1][2]

2.3 利用動向

IC カードは、金融・通信分野では磁気カードの代替として既に実用化され、2003 年における住民基本台帳カードの交付をはじめとして、公共・医療等でも今後適用されることが決まっている。これにより、IC カードの国内発行枚数は 2003 年までに 2 億枚を超え、様々な分野で利用されると予測される。[3]

このような IC カードの普及を背景に、現在いくつかの大きな取り組みが進んでいる。国内では経済産業省の「IT 整備都市研究事業」[4]による全国 21 都市での多目的 IC カードの実験が 2002 年より開始される。また、欧州では「EuroSmart」[5]や「eEurope smartcard」[6]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。

4 IC カードの技術動向

4.1 チップ性能の向上

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、不揮発メモリにおいては Flash メモリ、FeRAM 等の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 [7] が出現してきている。

4.2 IC カードの多目的化

IC カードの高性能化、大容量化が進むことにより、

1枚の IC カード上に複数サービスの搭載が可能になる。従来の IC カードは偽造対策やイントラネットにおけるアクセス制御等のように単一目的の利用のみだったが、今後は1枚の IC カードの複合的・多目的利用が推進されると考えられる。このような IC カードをマルチアプリケーション IC カードと呼ぶ。

4.3 データキャリア型からプログラム格納型へ

マルチアプリケーション IC カードはデータの管理方法により、データキャリア型とプログラム搭載型に分類できる。従来は、データキャリア型が中心であったが、IC カードの性能向上により IC カード内に汎用 OS を持つカードも出現し、注目されている。以下に、その特徴を示す。

(1) データキャリア型

データキャリア型 IC カードはファイルシステム及びデータの読み書きとアクセス管理機能を持つ。データを格納するための媒体として、IC カードにはサービス毎のデータを格納し、システム側が必要に応じてデータを読み書きし、サービスを実施する。従来主流の ISO 準拠カード、JICSA[8]準拠カード等はデータキャリア型である。

(2) プログラム格納型

プログラムを実行管理する汎用 OS を搭載し、サービスの処理内容に応じたプログラムを格納することが可能な IC カードである。プログラム格納型 IC カードとして、Java カード[9]、MULTOS カード[10]等が挙げられる。このような IC カードではサービスの処理自体を IC カード内で実施するため、改ざんが難しく安全性が高いというメリットを持つ。

4.4 IC カードプラットフォーム

マルチアプリケーション IC カードを運用管理する仕組みについても提案されている。これらは IC カードプラットフォームと呼ばれ、IC カードを発行・管理し、IC カードに複数のアプリケーションを搭載・削除することを目的としている。

現在、提案又は運用されている代表的な IC カードプラットフォームには NICE(Net-based IC Card Environment)[11]、MULTOS[10]、VOP/GP(Visa Open Platform/Global Platform)[12][13]がある。

5. IC カードの課題

5.1 IC カードコストの削減

IC カードは従来の磁気カードよりも単価が高く、カード自体のコストが導入コストの大部分を占めるので、カード発行者の負担が大きいと想定される。そのため、IC カードに複数サービスを相乗りする機能を提供し、複数のカード発行者/サービス提供者間でカードコストを分担するという仕組みが必要となる。

5.2 サービス追加の安全性

マルチアプリケーション IC カードの場合、カード利用者が必要に応じてサービスを追加するという利用が想定される。このような場合、従来カード発行時に安全な環境で実施されてきたサービス追加を店頭端末や利用者の自宅端末等の環境で行うため安全性を保证する仕組みが必要となる。

5.3 複数種類カードの運用管理

本稿でも述べたように、現在 IC カードには複数種類が存在し統一化は難しい状況である。それぞれの IC カードは管理方法が異なっており、同一のシステムで扱うのは難しい。今後、カード発行者等のシステムはこれら複数種類の IC カードを扱うことが想定されるため、その運用管理方法が課題となっている。

5.4 信頼性の向上

IC カードは重要な情報を格納し、さまざまなシーンで使用され、IC カード内のデータの保証が必要となる。そのため、処理中障害からの復旧や破損時対応等の異常処理について IC カード及びシステム全体でどのように保証していくかが課題である。

6. おわりに

本稿では、IC カード技術とその課題を述べた。IC カードがこれからの IT 社会のキーデバイスとして広く普及していくためには本稿で述べたような課題をクリアしていくことが必要である。

7. 参考文献

- [1] Information technology Identification cards Integrated circuit(s) cards with contacts ISO/IEC 7816-4:1995
- [2] JIS X 6304 : 外部端子つき IC カード - 電気信号及び伝送プロトコル
- [3] “IC カード総覧” 株式会社シーメディア 2000
- [4] 「IC カードの普及等による IT 整備都市研究事業」
<http://nmda.or.jp/nmda/iccard/h12hosei/iccardkoubo.html>
- [5] euros smart, <http://www.eurosmart.com>
- [6] eEuropesmartcard,
<http://www.cordis.lu/ist/ka2/smartcards.html>
- [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, PP733-739, 2000
- [8] IC カード利用促進協議会、<http://www.jicsap.com/>
- [9] JavaCard, <http://java.sun.com/products/java card>
- [10] MULTOS, <http://www.multos.com/>
- [11] 山本, 竹内, 細田, “ネットワーク指向 IC カードプラットフォーム”, NTT R&D Vol.49, No.12, 2000
- [12] VISA Open Platform, <http://www-s2.visa.com/>
- [13] GlobalPlatform, <http://www.globalplatform.org/>