非接触ICカードの原理と体系化

井上, 創造
九州大学附属図書館研究開発室 : 准教授

安浦, 寛人
九州大学システムLSI研究センター : センター長 | 九州大学大学院システム情報科学研究院 : 教授

https://doi.org/10.15017/8088

出版情報：九州大学附属図書館研究開発室年報. 2006/2007, pp.30-35, 2007-06-01. 九州大学附属図書館研究開発室
バージョン：
権利関係：

論　文

非接触ICカードの原理と体系化

井上　創造*，安浦　寛人**

〈抄　録〉

非接触型を初めとするICカードは、それ自身が一種の計算機であるといえる。一方でそれ単体では機能せず、リーダと呼ばれる読み取り機を備えたシステムとの協調により種々のサービスを実現する。

本論文では、非接触ICカードおよびそれを用いたシステムの原理と設計の根拠を整理する。

The Mechanism of Contactless Smartcard Systems

INOUE Sozo*, YASUURA Hiroto**

1．はじめに

非接触型を初めとするICカードは、それ自身が一種の計算機であるといえる。一方でそれ単体では機能せず、リーダと呼ばれる読み取り機を備えたシステムとの協調により種々のサービスを実現する。

本稿では、非接触ICカードおよびそれを用いたシステム原理と設計の根拠を整理する。

以下では、ICカードとそのシステムの基本機能を述べ（１章)、動作原理と構成を整理し現実の規格と比較する（２章)。さらに安全性と課題について議論と指摘をする（３章)。

1．1　非接触ICカードは計算機

ICカードとは一般に、「計算・記憶・通信能力を持つ、数センチ大のカード」を意味する。さらに、 非接触ICカードは、「近接型の通信およびリーダからの電力供給能力を持つICカード」を指す。 近接型とは、10cm程度の距離での通信および電力供給ができることを言う。

ただ近年では、上述のようにICカード用のLSIが種々のデバイスに搭載されはじめているため、以下では、**非接触ICカード**を、「計算・記憶・および近接型の通信能力を持つ携帯可能なデバイス」と定義する。接触型カードのようにリーダとの接触点がないため、カードに接触点を露出させる必要がなく、汚れに強いといった耐環境性に優れる。

1．2　識別・権限・価値・秘密の管理

ICカードは本来、非接触型・接触型に限らず、「識別・権限・価値・秘密の管理」に利用する目的で考案された。ICカードから見て他者を常には信用できない場合にカード内の計算機能を用いて、安全な「識別・権限・価値・秘密の管理」が実現できる。

ICカードを発行する組織を**発行者**、ICカードを保有する者を**利用者**、ICカードとのやりとりにより利用者に種々のメリットを提供する者を**サービス**と呼び、図１にその概要を示す。

１（識別）ICカードに記載されたカード固有のIDを用いて、サービスがICカードを識別する。近接型の通信であるため、利用者の意思表示と解釈できることも特徴である。

２（権限）ICカードに記載された秘密情報を用いて、サービスがICカードを認証する。

３（権限）計算能力を用いて、ICカードが利用者やサービス、または発行者を認証する。中でも利用者を認証する場合は、ICカード内に生体情報を保持し、これを用いて利用者を生体認証する。

４（価値）ICカードにポイント情報や電子マネーの情報を載せ、価値を搭載する。あるいは同様の情報をサービスが保持し、１の機能を用いて価値をICカードに与える。

５（秘密の保持）個人情報のような簡単には公

* いのうえ　そうぞう　九州大学附属図書館研究開発室准教授　E-mal:sozo@lib.kyushu-u.ac.jp

** やすうら　ひろと　九州大学システムLSI研究センター センター長、九州大学大学院システム情報科学研究院 教授　E-mal: yasuura@csce.kyushu-u.ac.jp

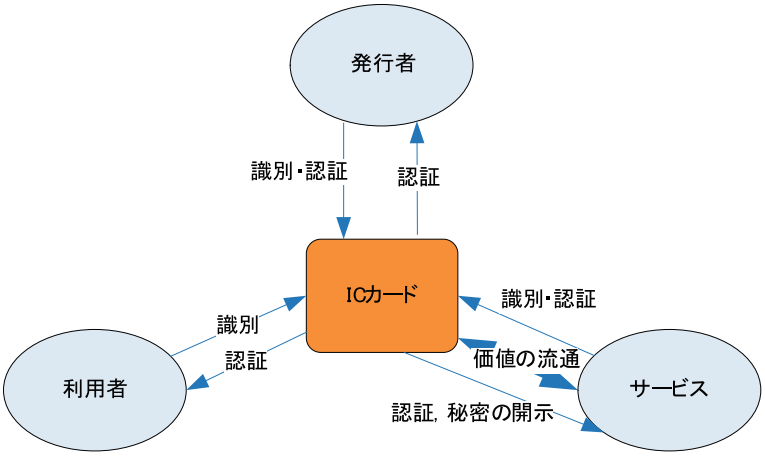

図１　ICカードシステムの役割と機能

開できない情報をICカードに載せ、必要に応じて限られた相手にのみ開示する。

なお、近年では1枚のICカードがマルチサービスに対応することが可能になっており、ICカード内に複数のサービス用領域を持つことが当たり前となってきている。

その他にICカードが持つことができる機能として、通信の暗号化・署名機能・乱数生成機能といったものがある。これらはプログラムを搭載可能なICカードにおいては、用意されたライブラリを、プログラムからAPIを通じて呼び出すことが可能である。

2．動作原理と構成

2.1　原理

ここでは、非接触ICカードがどのようにしてリーダとの間で給電および通信を行うのか、その原理を簡単に紹介する。

1．結合方式

非接触ICカードおよびリーダは、それぞれアンテナを持ち、それらを対向させた時に発生する誘導電磁界を媒体とした結合（これを電磁誘導方式と呼ぶ）が行われる。周波数は通常13.56MHzである。

2．変調方式

通常の無線通信と同様に、搬送波と呼ばれるアナログ信号にデジタル信号を載せる必要があるが、この変換を変調と呼ぶ。非接触ICカードにおいては、信号を2種類の振幅に対応させるASK（Amplitude Shift Keying）方式や位相に対応させるBPSK（Binary Phase Shift Keying）が一般的である。

3．符号化方式

さらに、ノイズへの耐性の強化、クロックの生成、電力取り出しのために、符号化と呼ばれる信号変換が行われる。２.３節の１に述べるType A規格においては各ビットに対応する時間の間に値をLowにするModified Miller, Type B規格においてはNRZ (Non Return to Zero)とビットを値の変化に割り当てるManchesterが用いられる。

4．返信方式

カードからリーダに送る信号は、電磁誘導方式では主に、アンテナが電磁波を反射させる性質を使い、これを制御することで行われる。

5．電力供給とクロック生成

電磁誘導方式では、搬送波である交流電流を、整流回路で直流に変換して電力として使う。クロックは主に、搬送波を分周して利用する。

6．衝突防止

通信範囲に複数のICカードが存在する時には同時に通信する仕組みが必要である。時間で分割する、時分割多重方式が主に採用される。

2.2　構成要素

ICカードを中心に、システムがどのように構成されているかを紹介する。図２はICカードおよびシステムを構成するハードウェアとソフトウェアの要素である。

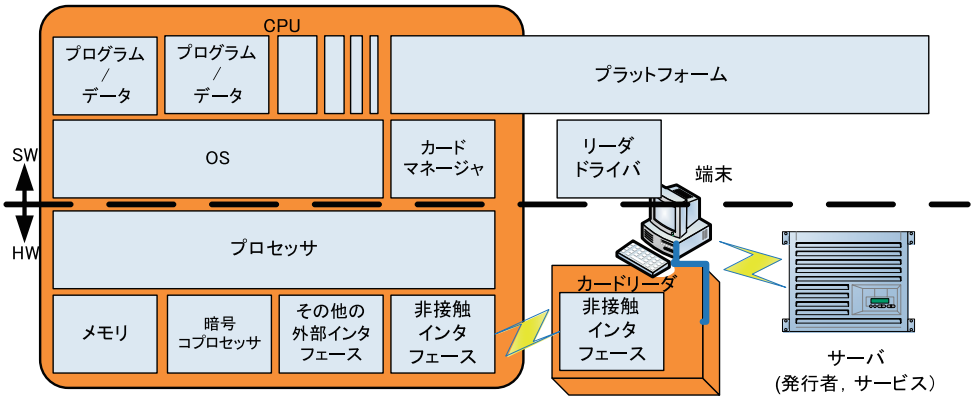

図２　ICカードおよびシステムのハード・ソフトウェア要素

ハードウェア

１．非接触インタフェース

２.１節で述べた給電と通信の原理は、ここで実現される。通常の無線通信と同様にアナログ回路で実現されるため、専用のハードウェアを持つ。リーダにも同様の機能が組み込まれる。

２．その他の外部インタフェース

ICカードによっては、１以外にも外部との通信インタフェースを持つものがある。例えば**コンビカード**と呼ばれるものは、従来の接触型と同様の接触インタフェースも持つ。**携帯電話**に搭載される場合は、携帯電話本体との通信ができる。さらに、USBメモリや不揮発性メモリカードといった**不揮発性メモリデバイス**に搭載される場合には、そのデバイスが本来持つ通信インタフェースを通じて外部と通信することが可能である。

３．CPU (Central Processing Unit)

通常の組み込みシステムと同様のプロセッサコアが用いられることが多い。

４．暗号コプロセッサ

非力なICカード上で暗号処理を効率よく行うためのプロセッサである。

５．メモリ

ROM（Read Only Memory）および、書き込み可能メモリがある。揮発性の書き込み可能メモリはリーダから離した場合などにデータが消えるので注意を要する。

６．リーダ

端末に接続され、ICカードと非接触で通信する。

７．端末、サーバ

端末とサーバは、サービス、発行者（、端末は利用者も）のどれに属する場合も考えられるが、ここでは簡単に同一視している。端末は、リーダを制御しながらサーバとやりとりし、人間との入出力を担当する。その一方、サーバはサービスの業務あるいは発行者の業務を遂行する。

ソフトウェア

８．OS（Operating System）

ICカードに搭載されたプログラムの実行制御を行ったり、外部インタフェースから渡されるコマンドをもとにICカード上のデータにアクセスを制御する。

９．カードマネージャ

プログラム／データのインストールや、確保・解放を行う。

10．プログラム／データ

サービスのためのプログラムやデータを搭載する領域である。

11．プラットフォーム

利用者やサービスに共通する以下の機能をICカードに対して実現するのが、プラットフォームと呼ばれるソフトウェアシステムである。

・初期データ・プログラム書き込み
・券面印刷とそのための利用者データ管理
・カードマネージャを通じたプログラムのインストールやアンインストール
・カードマネージャを通じたデータ領域の確保や開放
・無効化
・サービスとの間で認証を行うためのソフトウェア

表１　構成要素と具体例

	非接触インタフェース	その他の外部インタフェース	CPU	暗号コプロセッサ（暗号処理）	メモリ	リーダ	端末・サーバ	OS	カードマネージャ	プログラム／データ	プラットフォーム
ISO 関連規格	○										
JICSAP 仕様	○			○						○	○
Felica 関連技術	○			○					○	○	○
MULTOS				○				○	○	○	○
Java Card								○		○	
NICE									○		○
MIID									○	○	○
「価値」のための規格										○	○

２.３　具体例と標準

具体的な規格や標準が、２.２節で述べたどの構成要素に関する規定をしているのかを以下および表１に述べる。詳細は、本特集の別記事にゆずることにする。

１．ISO(International Organization for Standardization)関連規格

非接触型ICカードは、ISO/IEC 14443で国際標準化されている。電波出力、変調・符号化方式、衝突防止、および通信の基本プロトコル（ISO/IEC7816-4を参照する）が制定されている。Type A/Bという２方式が規定されている。ICカードの寸法も規定している。この規格は、JIS（日本工業規格）63シリーズに選択し取り込まれている。

２．JICSAP仕様[1]

非接触インタフェースとして、ICカード－リーダ間の通信の基本プロトコルと通信速度が規定される。想定するのはデータであり、ファイル構造と、アクセスのための鍵を設定できる。また複数の暗号方式を搭載し、カード識別子により識別し実行することができる。さらに、発行者が安全かつ確実にICカードを発行管理するための機能と要件を整理している。

３．Felica関連技術[2]（本特集3-1参照）

データをICカードに格納でき、また共通鍵を用いた暗号の使用が可能である。発行や鍵の管理において運用モデルが確立している。またEdyやSuicaといった「価値」の搭載が実現されている。

４．MULTOS[3]

プログラムの追加・削除は発行者が行い、MAOSCOという組織が発行する証明書が必要である。プログラム開発時にはC言語などで記述し、独自言語にコンパイルしてインストールされる。チップのマスク製造、カード初期化といったIC

1 「JICSAP仕様（V1.1）」，ICカードシステム利用促進協議会，http://www.jicsap.com/spec/index.htm.
2 http://www.sony.co.jp/Products/felica/
3 http://www.multos.gr.jp/

カードのライフサイクル管理の手順を厳密に規定している。

5. Java Card [1]

Javaバーチャルマシンの簡略版をOSの一部に持つ。プラットフォーム関連の規定はない。Java言語で開発したプログラムをバイトコードに変換し、ICカード用に最適化してインストールされる。

6. NICE（Network-based IC card Environment)[4]

サービスの持つ端末を通じてでもプログラムのインストールが可能である。Java CardやJIC-SAPに同時に対応できるICカード製品も存在する。

7. MIID: Media Independent ID[5]

九州大学で考案されたICカード規格に依存しないID管理システムである。

8.「価値」のための規格

1.2節で述べた「価値」を扱うための規格は、FelicaにおけるEdyやSuica、MULTOSにおけるMondex[6]、Java CardにおけるGlobal Platform[7]があげられる。

3. 安全性と課題

1章で述べたICカードの機能のうち、権限・価値・秘密の管理については、ICカード内に保持された情報（時にはプログラム）に対するアクセスをICカード自身が制御できるという能力にたよっている。

この能力が侵されれば、以下のような脅威が発生することになる。

1. **不正な読み取り**： ICカードが許可しない者がICカード内の情報を読み取ることができれば、ICカード内の秘密情報が**漏洩**する。またこのことが、同じ機能を持ったデバイスの偽造につながる。
2. **不正な書き込み**： ICカードが許可しない者がICカード内の情報を書き替えることができれば、ポイントの改ざんや、カードの機能停止といった、ICカードの変造につながる。

これらの脅威は、ICカードが接触型か非接触型かにかかわらないが、非接触型では保持者が意識しないうちに攻撃されやすく特に危険性が高いと言える。

3.1 ソフトウェア的な対策

上記の1，2を防ぐことは、偽造や変造を防ぐ必要条件ではあっても十分条件ではない。つまり偽造や変造は、不正な読み取りと書き込みを防ぐだけでは十分に防ぎきれるものではない。ICカードが許可する者であっても、故意にまたは誤ってICカード内の情報を漏洩してしまえば、第3者に偽造あるいは変造の機会を与えてしまう。また、マルチサービスが当たり前となっている現在、あるサービス領域へのアクセスを許可された者が、他のサービス領域にもアクセスできれば、その他のサービスに対しては同様の問題がある。これらをできる限り防ぐため、 データやプログラム、鍵といった、ICカード内の部分毎にアクセスのための認証を行うのが普通である。

3.2 ハードウェア的な対策

上記1，2の脅威に対するハードウェア的な対策は、攻撃者がLSIを解析し、改ざん、偽造するのが難しい性質として**耐タンパ**と呼ばれる。これに関してはLSIの分野で多くの取り組みがあり、文献[2]が詳しいが、理想的な耐タンパはまだ実現できているわけではない。また、設計時や製造時の不正をどのように防止するかと言う問題もある。

3.3 ICカード外部における対策

上記1，2の防止が偽造・変造防止の十分条件ではない以上、発行時やサービス運用時におけるプラットフォーム関連の対策が重要である。その一つにはICカード製造時における秘密管理などの対策があり、文献[3][4]が詳しい。

3.4 表示機能

1.1節の3について、ICカードそのものが表示機能を持たなければ、その結果をICカード利用者に安全に伝える手段がない[5]。例えば

4 http://www.ntt.co.jp/saiyo/rd/review/2002/pf/10.html
5 http://www.slrc.kyushu-u.ac.jp/your-id/
6 http://www.mondex.com/
7 http://www.globalplatform.org/

ATM端末が偽物で、 ICカードが拒否しても利用者にはそれが伝わらずにフィッシングなどの詐欺に遭うことはあり得る。「ICカード利用者がICカードを使って他人を認証すること」はできないのである。このために、ICカードが情報を利用者に安全に伝える方法が今後必要であろう。

3.5 リンク不能性

近年注目されるRFIDタグ（ICタグ）の分野においては、タグに載せられた固定のIDを無意識のうちにリーダから読まれ、その履歴とリーダの位置からタグを持つ人の行動履歴が分かるという問題が指摘され研究されている[6]。実はこの問題は非接触ICカードの「識別」にも共通の問題であり、効率の良い解決法が求められる。

4. おわりに

非接触ICカードを取り巻く技術とその課題を、その原理と体系化に留意しながら紹介した。この分野は実社会の利用の中で改良と発展を続けているため、情況は日々変化している。本稿が、理解と発展の一助になれば幸いである。

謝辞

本稿は、科学研究費補助金 学術創成研究費「社会基盤を構築するためのシステムLSI設計手法の研究」（H.14-18年，課題番号14GS0218）および、21世紀COEプログラム「システム情報科学での社会基盤システム形成」による。議論いただいた、九州大学システムLSI研究センターおよび全学共通ICカード推進チームの諸氏に感謝します。

参考文献

［1］「JavaCard 2.1 Application Programming Interface」，Sun Microsystems, 1999年2月24日.

［2］「LSIを盗聴から守る：暗号回路へのサイドチャネル攻撃とその対策」，日経マイクロデバイス，pp.99-134，2006年2月.

［3］「ICカード型電子マネーシステムセキュリティガイドライン」，電子商取引実証推進協議会，（ECOM），1998年10月.

［4］「ICカード利用ガイドライン」，電子商取引実証推進協議会，（ECOM），1998年3月.

［5］Takahiro Watanabe, Yasunobu Nohara, Kensuke Baba, Sozo Inoue, and Hiroto Yasuura, “On Authentication between Human and Computer”, *Proc. Fourth IEEE International Conference on Pervasive Computing and Communications (PerCom 2006) WORKSHOPS*, pp.636-639, 2006.

［6］井上 創造, 野原 康伸, and 安浦 寛人, “自動認識におけるプライバシーと個人情報保護技術”, 電子情報通信学会誌, Vol.89, No.5, pp.390-394, 2006.