非接触ICカード技術の概観と展望

井上, 創造
九州大学附属図書館研究開発室

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

出版情報：情報処理. 48 (6), pp.551-555, 2007-06. 情報処理学会
バージョン：

1. 非接触 IC カード技術の概観と展望

井上 創造　九州大学 附属図書館 研究開発室
安浦 寛人　九州大学 システム LSI 研究センター／
九州大学 大学院システム情報科学研究院

はじめに

非接触型を始めとする 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．

●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いう．

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．

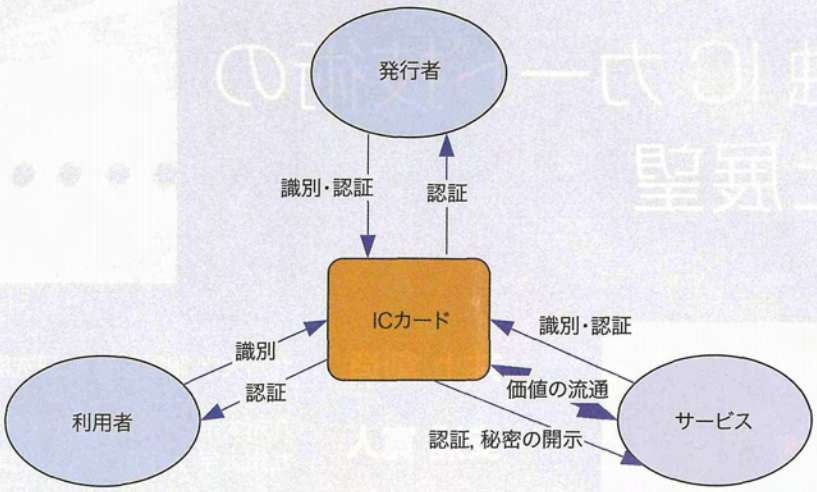
●識別・権限・価値・秘密の管理

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ものをサービスと呼び，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．



●図 -1　IC カードシステムの役割と機能

動作原理と構成

●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ィ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．以降に述べる「具体例と標準」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．

●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．

【ハードウェア】

1. 非接触インタフェース

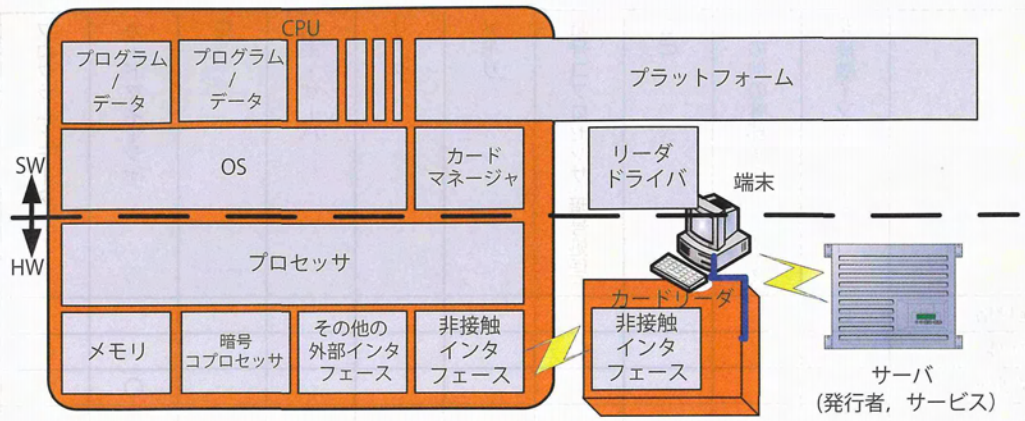
前節で述べた給電と通信の原理は，ここで実現される．通常の無線通信と同様にアナログ回路で実現されるため，専用のハードウェアを持つ．リーダにも同様の機能が組み込まれる．

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．たと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



●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

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解放
- 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

●具体例と標準

具体的な規格や標準が，前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/IEC 7816-4 を参照する）が制定されている．また，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 シリーズに選択され取り込まれている．

2. JICSAP 仕様[☆1]

非接触インタフェースとして，IC カードー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

☆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

	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										○	○

●表 -1　構成要素と具体例

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 2-1 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 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 JICSAP 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

冒頭で述べた「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．

安全性と課題

冒頭で述べた 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頼っている．

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

☆2 http://www.sony.co.jp/Products/felica/
☆3 http://www.multos.gr.jp/
☆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/

攻撃されやすく特に危険性が高いといえる．

●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，第三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 カード内の部分ごとにアクセスのための認証を行うのが普通である．

●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いう問題もある．

● 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 1 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．

●表示機能

冒頭の列挙のうちの 3（権限）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]．たとえば 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．

●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．

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，状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」（平成 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」，および，科学研究費補助金若手研究 A「信頼性を実現する RFID 情報システムの研究」（平成 18 ～ 20 年，課題番号 18680009）」による．

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（Feb. 2006）.
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）（Oct. 1998）.
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）（Mar. 1998）.
5) Watanabe, T., Nohara,Y., Baba, K., Inoue, S. and Yasuura, H. : 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，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（May 2006）.

（平成 19 年 5 月 7 日受付）

井上 創造（正会員）　sozo@lib.kyushu-u.ac.jp

九州大学附属図書館研究開発室准教授．平成 14 年九州大学大学院システム情報科学研究科博士後期課程修了．博士（工学）．データベースおよび RFID 情報システムの研究に従事．IEEE，ACM 各会員，日本データベース学会正会員．

安浦 寛人（正会員）　yasuura@c.csce.kyushu-u.ac.jp

九州大学大学院システム情報科学研究院教授・九州大学システム LSI 研究センター長（併任）．昭和 53 年京都大学工学研究科修士課程修了．工学博士．システム LSI 設計手法の研究に従事．電子情報通信学会，IEEE，ACM 各会員．