ICカード技術と情報セキュリティ
Smart Card Technology and Information Security

吉松　健三　K. Yoshimatsu
川村　信一　S. Kawamura

当社は1981年以来CPU内蔵型ICカードの研究・開発に取り組んできている。すでに世界3大クレジット会社がクレジットカードにCPU内蔵型ICカードの採用を決定しており，今後このようなICカードの需要の急速な立上がりが見込まれる。さらに，インターネットの普及は情報システムのセキュリティ対策の重要性をわれわれに再認識させている。われわれは，ICカードをこうした種々の情報システムにおけるセキュリティ対策のキーコンポーネントの一つと位置づけて，カードそのものに公開鍵(かぎ)暗号方式を含む高いセキュリティ機能を搭載している。

Toshiba has developed a series of smart cards since 1981. Recently, the world's three leading credit card companies jointly announced unified smart card specifications for the next-generation credit cards to ensure transaction security. It is therefore expected that great demand for smart cards will arise in a few years' time. Further, the widespread use of Internet services convincingly demonstrates the importance of security measures.

To overcome threats to both information and financial systems, Toshiba smart cards are equipped with excellent security features including public key cryptography systems. This paper describes these features from the hardware, software, and cryptographic standpoints.

1 まえがき

当社は1981年からICカードの開発に取り組んでいる。ICカードはCPUを搭載しているものとしていないものとに大別されるが，当社は開発当初からCPU内蔵の高いセキュリティのカードに関して研究開発を続けている。フランスを中心に実用化されてきたICカードは，CPUを搭載しないメモリチップであるが，電話用プリペイドカードとして現在ヨーロッパを中心として普及しており，韓国，台湾，香港などアジア諸国でも採用されつつある。また，近年はユーロペイ，マスターカードインターナショナル，VISAインターナショナルの世界の3大クレジット会社がクレジットカードにICカードを採用することを決定し，EMV仕様を作成，公開している。このカードは，電話に比べ大きな金額のお金を電子化して取り扱うため，より高いセキュリティを要求されており，CPU内蔵型のICカードが採用されている。一方，電子化されたお金の情報に限らず，一般の情報のセキュリティ（特にネットワークやパソコンのファイルのセキュリティ）に関してもICカードが利用されている。ICカードのユニーク性，偽変造のしにくさ，利用されるアプリケーションに応じたプログラムを格納できること（特に暗号関数とその利用のプログラム），そしてその携帯性のよさゆえに，便利でかつ安心して利用できるシステムを提供できるからである。

ここでは，このような情報セキュリティのキー技術としてICカード技術を紹介する。

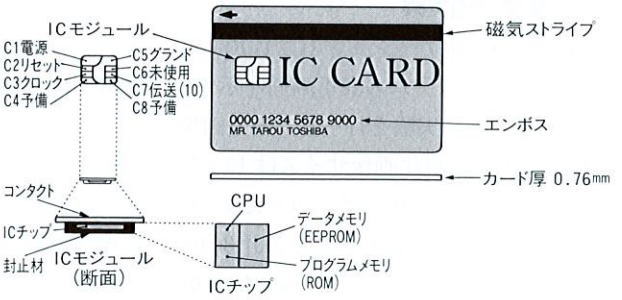

図1．ICカードの構造　ICカードはCPUとメモリを内蔵し外部から供給される電源とクロックにより動作する。
Structure of smart card

2 ハードウェア

まず，ICカードに要求されるハードウェアのセキュリティについて紹介する。図1にICカードの構造を示す。ICカードはクレジットカードやIDカードにICモジュールを埋め込んだものであり，そのセキュリティはモジュールの中のLSIが管理する。このLSIを種々の解析により偽造されたり，変造されたりできないような仕組みを作ることは，ハードウェア（LSI）を供給する製造者の大切な役割である。カードが偽造・変造されてしまうと，システム全体のセキ

ュリティの危機となるからである。

ICカードは，不特定多数の人が持ち，システムのサービスを受けるものである。このことから，偽変造対策に関しては専門家はもとより，専門家以外のアタックにもつねにさらされていることを考慮して対策を施す必要がある。

LSIのセキュリティのために次のことが必要である。

(1) 光を検知した場合には動作しない。
(2) 限定された周波数範囲外では動作しない。
(3) 出荷前に工場内で使用された検査が出荷後は動作しない。

(1)は封止されて，しかもプラスチックに埋め込まれて使われることが正しい使いかたであるのに対し，「光が検知できるということは誰かが解析のために開封した」と判断して，以後の動作をCPU自身で中断してしまうことにより機能の解析を困難なものにしようという試みである。

(2)は，例えば，高い周波数で動作させることで短時間で解析に十分なデータを集めることを防止するための対策である。また，低い周波数で動作させられる場合には，CPUをステップ動作させることにより電流変化などの微妙な情報を時間をかけて収集できることになり，これもまた好ましくない。ICカード用のLSIはある定められた周波数以外では動作しないことがセキュリティ上望ましい。

(3)に関しては，回路のテストルーチンが使えれば，解析が容易になるということから必要性は容易に理解できよう。しかし，実際に製造するLSIにこのような機能を付加した場合，「不良品を解析してその結果をフィードバックし，信頼性を含む品質を強化，改善する」という従来の製造業の常識が通用しなくなり，新しい概念を取り入れた製造ライン，品質チェックの手段を設ける必要が生ずる。

3 COS

ICカードの機能は一般にCOS (Card Operating System)と呼ばれている。カードメーカは各社各様のCOSをもつが，それらに共通するセキュリティの基本機能について具体例を紹介する。

カードはパソコンのファイル構造と同様の構造をもち，ファイルがもつ固有のIDによりアクセスされる。ファイルにはアプリケーションで使用される各種データをライトコマンドで入力し，格納する。また，リードコマンドで出力される。

カードの変造について考えると，カード内のデータを改ざんしにくくすることが重要であり，入力のアクセスレベルは出力のアクセスレベルより通常は高い。したがって，各ファイルには少なくとも2種類以上のセキュリティレベルが登録できるようにしておく必要がある。コマンドはリードライトだけではなく，例えば，不正使用を防止するためにカードを一時的に機能停止にする機能は，いつでも使えるようになっている必要があり，理想的には各コマンドの機能ごとに各ファイルにセキュリティレベルが定義できることが望ましい。

しかしながら，ICカード内のデータメモリの有効利用を考えれば，ファイルの定義データは小さいほどよい。そこで，ICカードがサポートする各種コマンドの機能を洗い出し，グループ分けを行い，各ファイルはそのグループごとにセキュリティレベルを独立に定義できるようにして，さまざまなアプリケーションに対応できるCOSを設計している。このグループ分けをいくつにするかはそれぞれのカードメーカのノウハウである。

4 暗号機能

暗号を適用することにより，対象となる機器に多様なセキュリティ機能をもたせることができるが，ICカードの場合もその例外ではない。また，情報システムにおいて個人を対象としたセキュリティサービス(例えば課金)を実現しようとした場合，各ユーザの暗号鍵を格納し配布するための携帯装置としてICカードは非常に便利である。

ここではICカードにおいて暗号機能がどのように実装されているのかを述べる。

4.1 暗号方式

インターネットの普及に伴い課金情報やパスワードの不正使用の問題が顕在化し，その具体的対策づくりが進められている。そのような対策のうち，クレジットカードによる電子決済におけるセキュリティ対策としては，まえがきで紹介したEMV仕様ICカードと，SET (Secure Electronic Transaction)プロトコルが注目されている。現在急ピッチで実用化が進められているこれら二つの仕様において基本となっているのは暗号技術である。

一般に，暗号技術によって実現される機能は大きく次の二つに分けられる。

(1) 通信電文の内容を漏えいから保護する秘匿機能
(2) 電文や通信相手の正当性を確認する認証機能

また，暗号方式そのものは，大きく秘密鍵方式と公開鍵方式とに分けられ，それぞれに長所・短所があり，目的に応じて使い分けられている。秘密鍵方式は主として電文の秘匿，電文の認証，相手確認に用いられ，公開鍵方式は主として，秘密鍵方式で使われる鍵の配送やディジタル署名作成のために用いられる(**表1**)。

鍵管理の側面から秘密鍵方式と公開鍵方式を見ると，秘密鍵方式は暗号化の鍵と復号の鍵をともに秘密にしておく方式であり，公開鍵方式は一方の鍵を公開し，他の鍵は秘密にする方式である。公開鍵方式は鍵の一つが公開されているために，同じ安全性を実現するには秘密鍵方式よりも

表1．秘密鍵方式と公開鍵方式の比較
Comparison of public and secret key systems

比較項目	秘密鍵方式	公開鍵方式
鍵管理	暗号化の鍵＝復号の鍵 （ともに秘密）	暗号化の鍵≠復号の鍵 （一方を公開）
処理速度	相対的に高速	2けたから3けた遅い
主な用途	秘密通信	ディジタル署名／鍵配送
代表的方式	DES方式	RSA方式
ICカードへの実装	ソフトウェア	専用処理回路 （コプロセッサ）

複雑な処理を行わなければならず，その処理量は秘密鍵方式に比べ約1,000倍にもなる。

従来のICカードにおいても，DES（Data Encryption Standard）方式[1]に代表される秘密鍵暗号方式は電文の暗号化，端末との相互認証，メッセージ認証コード（MAC）の生成に，広く利用されている。これに対して，公開鍵方式をICカードという計算力の小さい装置に実装するには専用の処理回路（以下，コプロセッサと呼称）なしでは実用的な時間での処理は望めない。

4.2 公開鍵暗号コプロセッサ

これまでに多くの公開鍵方式が提案されているが，有力な方式のほとんどは，次の式で示される多倍長のべき乗剰余演算を基本演算としている。

$$C = M^{d} \bmod n$$

変数M，nなどのビットサイズは暗号の安全性と密接な関係にあり，ビット幅が大きいほど安全性は高くなる。マサチューセッツ工科大学で開発された代表的なRSA方式[2]では現在のところ512ビットから1,024ビットの範囲のサイズが広く利用されている。この演算をICカードCPUのファームウェアで実現した場合，数十秒以上の時間を要し実用にたえない。そこで必要となるのが公開鍵暗号コプロセッサである。

公開鍵暗号コプロセッサの開発にあたって検討した課題は次のような4項目である。

(1) 回路規模
(2) 演算の種類
(3) 鍵サイズ
(4) 処理速度

回路規模は他の検討項目と深いかかわりをもつが，必須(す)条件として，コプロセッサはICカード用の1チップLSIにCPUおよびメモリとともに収まる規模であることが要求される。チップサイズは，物理的強度の制約を受けるためあるサイズ以上に大きくすることができないうえに，現状では複数チップ構成はありえない。

演算の種類としては，すでに述べたべき乗剰余演算以外に剰余乗算および多倍長の四則演算をサポートする。後述するようにこれらを組み合わせた上位機能はファームウェアで実現する。なお，これらの演算はビット幅が大きいことを除けば一般的な演算であり，公開鍵暗号以外のICカードアプリケーションから使うこともできる。

鍵サイズは可能な限り大きなものまで扱えることが望ましいが，回路規模と処理速度からの制約を受ける。今回開発した公開鍵暗号コプロセッサは，1,024ビットまでの鍵を扱えるようにした。処理速度は768ビット鍵で中国剰余定理を利用してRSA暗号の署名を作成した場合に，処理が1s以内で完了することを目ざした。

コプロセッサの基本アーキテクチャとしては，ICカードの8ビットCPUおよびメモリとの整合性をとるために，8ビット処理を基本とした。**図2**に示すように，コプロセッサ内部は大きく三つのブロックに分けられる。メモリ部は鍵や電文，処理結果の一時格納に用いる。演算部は主として乗算と結果の累積加算を行うブロックである。制御部は演算手順に従ってコプロセッサの処理内容を制御する部分である。中核となるべき乗剰余演算は剰余乗算（$a \cdot b \bmod n$）に分解して処理されるが，剰余乗算は除算と乗算を同時実行することによって処理時間の短縮を図っている。

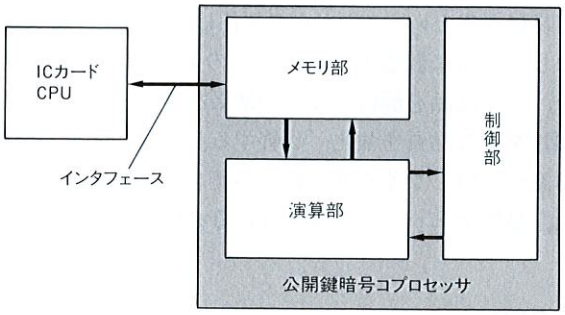

図2．公開鍵コプロセッサの構成　コプロセッサはメモリ部，演算部，制御部という三つの機能ブロックから構成される。
Block diagram of public key co-processor

ここで，処理性能について簡単に述べる。このコプロセッサの基本演算として512ビットのべき乗剰余演算を例にとると，約600msで処理を完了する。RSA暗号の場合には同じ演算を中国剰余定理を用いて高速化することができ，約200 msで処理できる。鍵が768ビットであっても，処理時間は600 ms程度であり，外部との通信オーバヘッドを見込んでも1s以内で処理を終了できる。なお，1,024ビットの場合には中国剰余定理を用いて約1.6sで処理を完了する。

通常のコプロセッサがCPUの処理を補助するよう設計されているように，このコプロセッサもあくまで多倍長演算に関してICカードCPUの処理を補助するものである。し

たがって，各種の暗号方式はCPUのファームウェアとして実装される（図3）。先にも述べたように，代表的な公開鍵暗号方式（RSA，DSA（Digital Signature Algorithm），Fiat-Shamir法，Schnorr署名，変形ElGamal署名[3]など）はいずれも大きい整数を法とする演算で実現されるため，このコプロセッサで容易にサポートすることができる。

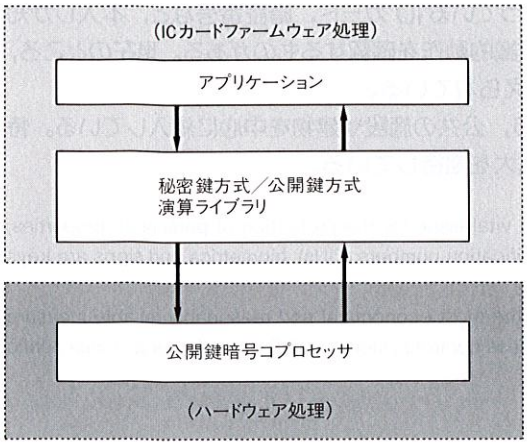

図3．ファームウェアとハードウェアの処理分担　秘密鍵方式はファームウェアで実装され，公開鍵暗号は演算の基本部分をコプロセッサで処理する。

Farmware and hardware configuration

5 あとがき

ICカードが情報システムのセキュリティを実現するためのキーコンポーネントの一つであることは間違いない。セキュリティを実現するには一貫した情報の管理が必要であり，ICカードの場合には発行処理，運用管理，廃棄処理といった一連の流れの中でセキュリティをとらえる必要がある。

ここでは取り上げられなかったが，システム構築をサポートするソフトウェア群の重要性がこれからいっそう高まると考える。さらに，セキュリティ技術と解析技術とは矛と盾の関係にあり，既存の対策はつねに陳腐化する運命にある。例えば，暗号の鍵の長さ一つをとっても計算機の進化とともに長くしていく必要がある。したがって，セキュリティを中心機能とするICカードもつねに新たな対策を取り込むために研究開発を継続していかなければならない。

文　献

(1) Data Encryption Standard, National Bureau of Standard, Federal Information Processing Standards Publications (1977)
(2) R. L. Rivest, et al : A method for obtaining digital signatures and public key cryptosystems, Comm. of ACM, pp.120-126 (1978)
(3) 新保　淳：多重署名可能な変形ElGamal方式，電子情報通信学会春季大会，A-386，pp.1-389 (1995)

吉松　健三　Kenzo Yoshimatsu
柳町工場特殊機器第二部部長附（副参事）。
銀行業務省力機器の開発，ICカードシステムの開発に従事。
Yanagicho Works

川村　信一　Shin-ichi Kawamura, D.Eng
研究開発センター 情報・通信システム研究所研究主務，工博。通信システム技術，情報セキュリティ技術，暗号技術の研究に従事。電子情報通信学会，IEEE，IACR会員。
Communication & Information Systems Research Labs.