モバイル コンピューティング環境でのICカード利用

Smart Card Technologies for Mobile Computing Environment

清水　秀夫　H. Shimizu
酒井　高彦　T. Sakai

近年脚光を浴びているモバイル コンピューティングと，電子商取引のようなICカードを利用したサービスの統合を考え，それによる問題点を取り上げる。

その一つは携帯型情報端末とのインタフェースの共通化であり，当社はICカードメーカとコンピュータメーカ10社によるPC／SC Workgroupに参加し，規格化のための審議を続けている。また，モバイル コンピューティング環境でのセキュリティを確保するために不可欠である公開鍵(かぎ)暗号については，ICカードでの実装に適した方式として楕(だ)円曲線暗号が注目されている。

Smart cards are expected to be used in the mobile computing environment, in order to make advanced network services such as on-line shopping more convenient. To facilitate manufacturing, standardization of the interface between smart cards and mobile terminals is highly important.

This paper describes the activities of the PC／SC Workgroup, which is developing such a common interface and suitable security mechanisms. In addition, elliptic curve cryptography is discussed here as a promising mechanism for smart cards.

1 まえがき

ICカードの話題として，モバイル コンピューティングとのかかわり，パソコン(PC)におけるICカードインタフェース標準化の動きであるPC／SC WorkgroupおよびICカードへの実装に適した公開鍵暗号方式として注目を浴びている楕円曲線暗号方式について述べる。

2 ICカードとモバイル コンピューティング

“いつでも，どこでも，誰とでも”というのが通信の究極の目的であり，例えば携帯電話やPHSは，この目的を達成するために発明された。また，伝送できる情報の種類を増やせるのがモバイル コンピューティングと考えることができ，音声だけでなく文字情報や画像，動画などの情報も扱えるようになる。実際のモバイル コンピューティングでは，利用者はミニノートPCやPDA(Personal Digital Assistant)のような携帯型情報端末を携行し，必要に応じて電話回線などのネットワークに接続して，さまざまなサービスを受けることができる。

モバイル コンピュータ機器の共通規格としては，東芝，IBM，Sun Microsystemsなど全世界11社が合意しているMNCRS(Mobile Network Computer Reference Specification)で詳細仕様の取決めをしている。これはネットワーク コンピュータの共通規格であるNCRP(Network Computer Reference Profile)の機能拡張である。

ICカードを使って受けることのできるさまざまなサービスと，モバイル コンピューティング環境を統合することにより，ICカードによるサービスを，いつでもどこでも受けることが可能となり，利便性が高まる(図1)。

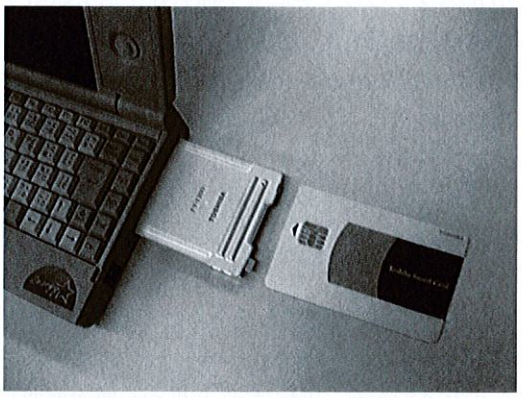

図1．ICカード リーダライタ　ポータブルPCに適したPCカード タイプのICカード リーダライタ(FY1300)。
Smart card reader/writer

しかし，ICカードをモバイル コンピューティングに応用しようとした場合，従来の利用法と異なることから問題となる点がある。特にセキュリティの面で問題となるのは，端末そのものが盗難にあったり粉失したりして，端末の内部に格納してある情報を読み取られてしまうといった，直接的な危険性である。これは，事務所の中に据え付けられている端末には生じない，モバイル コンピューティング特有の問題である。

例として，ISO 7816(ISO：国際標準化機構)で定められ

ているICカードと端末の間の認証機能について考えてみる。ISO 7816では，認証機能としてパスワード照合と秘密鍵暗号を用いるチャレンジ レスポンスの二つが考えられている。後者は端末の発生させた乱数をICカードに送信し，ICカードは内部に保持している秘密鍵を使って，送られてきた乱数を暗号化し端末に送り返す。端末側ではICカード側と同じ計算をし，送り返されてきた計算結果と一致しているかどうかにより，ICカードに正しい秘密鍵が格納されていること，すなわち正しいICカードであるかどうかを判定する。パスワード照合の場合だと，ICカードと端末の間の通信を傍受することによりパスワードそのものが判明してしまうが，チャレンジ レスポンス方式だと秘密情報が通信の中に含まれないため，盗聴に対して安全である。さらに，乱数を使っているので，前回盗聴した結果を端末に送り返すリプレイ攻撃に対しても安全である。しかしながら，これらの方法は端末自身に格納されている秘密情報が安全であるということを前提としており，モバイル コンピューティングのように盗難や紛失といった危険性のある，必ずしも安全であるとは限らない環境に対して有効とは言い難い。

以上は従来用いられてきた手法の限界を示すものであり，新たな方法の開発が必要なことを意味している。従来の秘密鍵暗号を用いる方式では端末に格納された秘密鍵の安全性に問題があり，端末に秘密鍵を格納する必要のない公開鍵方式を用いる必要がある。次節で述べるPC／SC Workgroupが審議している新しい規格では，PCのような安全でない端末での利用を前提とした，公開鍵暗号をベースとする認証方式を含んでいる。

3 ICカードインタフェースの標準化

3.1 PC／SC Workgroup

1996年，Microsoft社を中心とした5社はICカードをPCから利用するためのインタフェースの標準化をするPC／SC Workgroupを結成した（図2）。97年，参加企業は世界の代表的なICカードメーカとコンピュータメーカ10社（表1）に拡大された。その中でも東芝は世界最大のノートPCメーカであり，PC，ICカード，ICカードリーダのすべてを手がける数少ないメーカとして重要な役割を担っている。

PC／SC Workgroupにおける標準化は，“Interoperability Specification for ICCs and Personal Computer Systems”（ICCs：ICカード）という八つのパートからなるドキュメントにまとめられている。各パートの表題は表2のとおりである。現在，ドキュメントのバージョンは0.9であり，バージョン1.0に向けての作業中である。ここで紹介する内容はあくまで審議中の内容であり，変更される可能性がある。ドキュメントのドラフト自体はPC／SCグループのホームページhttp://www.smartcardsys.comから入手することができる。

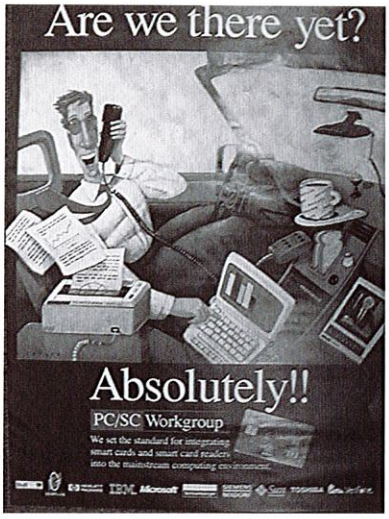

図2．PC／SCのポスタ
各種展示会ではられている PC／SC Workgroupのポスタ。
Poster of PC／SC Workgroup

表1．PC／SC参加企業一覧
Companies participating in PC／SC

企業名	ホームページURL
Bull CP8	http://www.bull.com
Gemplus	http://www.gemplus.com
Hewlett-Packard	http://www.hp.com
IBM	http://www.chipcard.ibm.com
Microsoft	http://www.microsoft.com
Schlumberger	http://www.slb.com
Siemens Nixdorf	http://www.sni.de
Sun Microsystems	http://www.sun.com
Toshiba	http://www.toshiba.com
Verifone	http://www.verifone.com

表2．PC／SC標準ドキュメント一覧
Titles of PC／SC documents

パート1	アーキテクチャ概要
パート2	ICカードと読取り装置のインタフェース
パート3	PC接続インタフェース装置の要求仕様書
パート4	インタフェース装置の設計と参考設計情報
パート5	ICカードリソース管理の定義
パート6	ICカード サービスプロバイダ インタフェースの定義
パート7	開発者向けアプリケーション設計
パート8	ICカードとプライバシー装置のための推奨

表内の内容は当社で原文を翻訳したものであり，正式なものではない。

3.2 PC／SCのアーキテクチャ

PC／SC Workgroupが結成された背景には，ICカードそのものはISOのような国際標準団体により標準化が推進されているが，PC用の読取り装置やインタフェース規格はメーカごとに異なっており，アプリケーション作成者にとって負担が大きいことや，標準的なソフトウェアが出にくか

ったことがあげられる。このため，PC／SC 標準では，次の従来にはなかった多岐にわたる内容を含んでいる。

(1) IC カードそのもの（パート 2）
(2) IC カード読取り装置（パート 3，4）
(3) 複数のメーカの IC カード読取り装置の切換えをスムーズに行うためのメカニズム（パート 5）
(4) アプリケーションから IC カードを利用するためのソフトウェア インタフェース（パート 6，7）

PC／SC 全体の構造は六つの階層からなっている（図 3）。ハードウェアだけでなく，ソフトウェアも含んでいることが特徴である。

IC カード自体は ISO 7816 と互換であり，従来の規格の拡張となっている。

IC カード読取り装置が利用する PC とのインタフェースとしては，既存の RS232C インタフェース，PC カードインタフェース，PS／2 キーボード インタフェース（キーボード内蔵型 IC カードリーダを可能にする技術）を含んでおり，将来的には USB（Universal Serial Bus）インタフェースも含む予定である。

図 3 の IC カードリソース管理は，OSI（Open System Interconnection）のデータリンク層の機能，IC カードリーダのデータベース，要求する機能をもつ IC カードの検索といったリソースの管理を行う。特に，並列動作可能なサブルーチンである複数のスレッドからの利用の調整をするので，マルチスレッド OS（Operating System）の上で動く複数のアプリケーションからの同時アクセスを可能にしている。

図 3 のサービス プロバイダは，IC カードのファイルシステム，セキュリティ機能を提供する。図 4 にサービス プロバイダが提供するサービスを示す。通常のアプリケーションが必要とする機能はすべて含んでいる。

また，PC／SC 規格のパート 7 では IC カードを利用するアプリケーションを作成する際のガイドラインが記述されている。

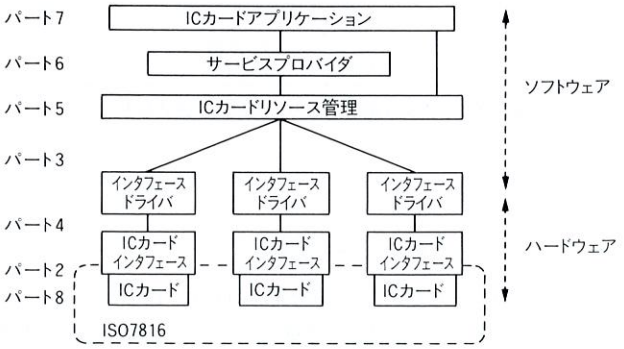

図 3．PC／SC のアーキテクチャ　ハードウェアとソフトウェアを含む，6 層のアーキテクチャが規定されている。
PC／SC architecture

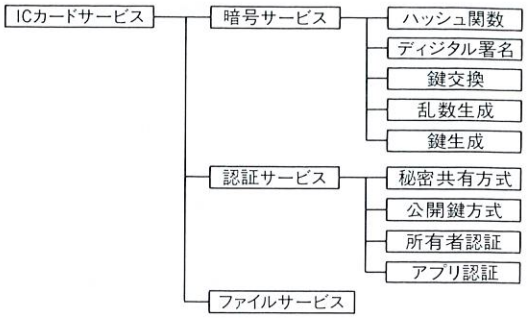

図 4．サービスプロバイダの提供するサービス　ソフトウェアから利用できる IC カードの機能を示す。
Services of PC／SC standard

PC／SC 参加各社は，97～98 年度をめどに製品化を予告しており，Microsoft 社も Windows®(注1)対応製品でサポートする予定となっている。

PC／SC Workgroup による標準化はメーカの垣根を取り払い，PC における IC カード利用を大いに促進することが予想される。

4 IC カード向け暗号技術

モバイル コンピューティングのような必ずしも安全とはいえない環境での IC カードの利用には，秘密鍵暗号方式ではなく，端末側に秘密情報をもたなくてもよい公開鍵暗号方式が不可欠であることはすでに述べた。

現在の公開鍵暗号方式の欠点は，計算量が多いために処理時間がかかる点にある。IC カードは処理能力が低く，CPU だけで公開鍵暗号を計算することが困難であることから，暗号計算専用の公開鍵コプロセッサと呼ばれるハードウェアが開発されている。IC カード上で，実現されている暗号化機能や公開鍵コプロセッサについては文献(1)に詳しく記述されている。また，現状の IC カードの代表的な仕様を表 3 に示す。

楕円曲線暗号は，有限体上で定義された代数曲線上の加

表 3．代表的な IC カードの仕様
Typical smart card specifications

CPU	8 ビット
ROM	10～20 K バイト
RAM	256～512 バイト
EEPROM	8～16 K バイト
チップサイズ	25 mm²以下
通信速度	9.6～11.5 kbps

EEPROM：Electrically Erasable and Programable ROM

(注 1)　Windows は，Microsoft 社の商標。

表4．公開鍵暗号方式の比較
Comparison of public-key cryptography systems

	RSA 暗号	楕円曲線暗号
ブロック長	512～1,024 ビット	216～320 ビット
鍵長	512～1,024 ビット	108～160 ビット
回路規模	大	小
計算時間	署名検証≪署名 暗号化≪復号	署名検証＞署名 暗号化≒復号

群を利用する公開鍵暗号であり，有限体上の素因数分解問題より困難であると予想される楕円曲線上の離散対数問題に，安全性の根拠をおいている。楕円曲線暗号はIEEE P1363で標準化が審議されている。(IEEE：米電気電子学会)

表4に，現在広く用いられている公開鍵暗号方式であるRSA暗号と，楕円曲線暗号について安全性を固定した場合の比較をしている。楕円曲線暗号のほうがRSA暗号よりブロック長が短く，それがICカードの低速の伝送速度と限られた記憶域の両方にとって有効に働く。また，ブロック長が短いことが回路規模に有利に働く。

ICカードに格納された秘密鍵を利用する典型的な処理は署名作成であり，署名時間が署名検証時間より短い楕円曲線暗号は，この点でもICカードに適した暗号であると考えられる。

5 あとがき

モバイル コンピュータとICカードを利用したサービスとの統合における問題点として，インタフェースの標準化，セキュリティの観点から公開鍵暗号の必要性，そして実装面から注目される楕円曲線暗号を取り上げてきた。

ここで取り上げなかった話題としてJavaCard(注2)があげられる。Java appletはインターネットからダウンロードできるプログラムモジュールであるが，これをICカード上でも実行できるようにするのがJavaCardである。外部から持ち込まれる実行モジュールから内部の秘密情報をいかに守るかといったJavaCard特有のセキュリティの問題や現実的な時間でサービスをするための実装の問題など，解決しなければならない問題は多い。しかし，サービス提供者がプログラム開発を行える点や，開発環境の標準化，ICカードの多機能化，ネットワークからのサービス提供モジュールのダウンロードなど魅力的な構想である。当社も今後JavaCardに対応した製品をサポートしていく予定である。

当社では，標準化活動を通し社会に貢献し，より利便性が高く，セキュリティを兼ね備えたサービスをサポートする環境の構築を目ざし，よりいっそうの努力を心がけていく所存である。

(注2) JavaCardは，米国Sun Microsystems社の商標。

文 献

(1) 吉松健三，他：ICカード技術と情報セキュリティ，東芝レビュー，52，2，pp.14-17 (1997)

清水 秀夫 Hideo Shimizu
研究開発センター 情報・通信システム研究所，工博。
暗号・情報セキュリティの研究・開発に従事。電子情報通信学会，セキュリティマネジメント学会会員。
Communication & Information Systems Research Labs.

酒井 高彦 Takahiko Sakai
情報・通信システム新規事業企画室 参事。
ICカードシステム事業推進業務に従事。
Information & Communications Systems New Business Planning Office