特集

スマートカードと発行サービス

Smart Card Issuing Service

あらまし

スマートソリューション全体の中で，最下層のインフラストラクチャを受け持つのがスマートカードである。

スマートカードは，セキュリティの維持という点で最重要なキーデバイスである。そのため，スマートカード内に保存される個人情報を含む各種データを外部の脅威からハードウェア的にもシステム的にも厳重に守らなければならない。したがって，スマートカードはその開発・設計から製造そして発行サービス(活性化・個人情報書き込み)まで，一貫したセキュリティポリシーが貫かれている。

本稿では，スマートソリューション内でのスマートカードの役割や発行サービスにおけるセキュリティについて，その概要を説明する。

Abstract

Smart cards constitute the bottom-layer infrastructure of a smart card system. To ensure system security, the personal data and other data that is stored on a smart card must be protected from unauthorized accesses that are made directly via the hardware of the card or via the software of the card system. Therefore, a high level of security is maintained throughout the development and manufacturing of smart cards and when activation data and personal data are written to smart cards when they are issued. This paper looks at the use of smart cards and the role of security in smart-card issuing services.

植竹光夫（うえたけ　みつお）

スマートソリューション統括部EC ネットワーク機器開発部 所属
現在，スマートカードの技術開発に従事。

三柴昭裕（みしば　あきひろ）

製造統括部生産技術部 所属
現在，スマートカードの製造技術開発に従事。

ま え が き

日本におけるスマートカード(以前は，一般的にICカードという呼称)は，1985年頃の黎明期，1990年頃の第２次発展期を経て，1996年ごろから第３次の本格的立ち上がり時期を迎えている。その背景には，ICチップテクノロジの劇的な進化や低価格化，セキュリティ要求の高まり，インターネットの普及，国際標準化とデファクト標準化の進行といった要因が相乗効果をもたらしたことが挙げられる。さらに，セキュリティの点からみて非力な従来の磁気カードシステムからICチップ内蔵の高セキュリティなスマートカード化への要望が急速に高まってきたことなど，社会環境の変化が追い風となっている。

本稿では，スマートカードとはいかなるものか，またスマートカードの発行サービスとはどういうものかを，セキュリティという側面から述べる。

スマートカードについて

● スマートカードとは

スマートカードとは，媒体内部にICチップを内蔵し，外部からのアクセスに対してインテリジェントな応答機能を持つカード媒体のことである。従来の光メモリカードやPCMCIA型メモリ内蔵カード，磁気カードやエンボスカード，バーコードカードなどはカード型記録媒体であり，スマートカードとは区別する。現状でのスマートカードはクレジットカード型をしており，個人個人で持ち歩き保管管理できるセキュリティデバイスとしては最適なものである。

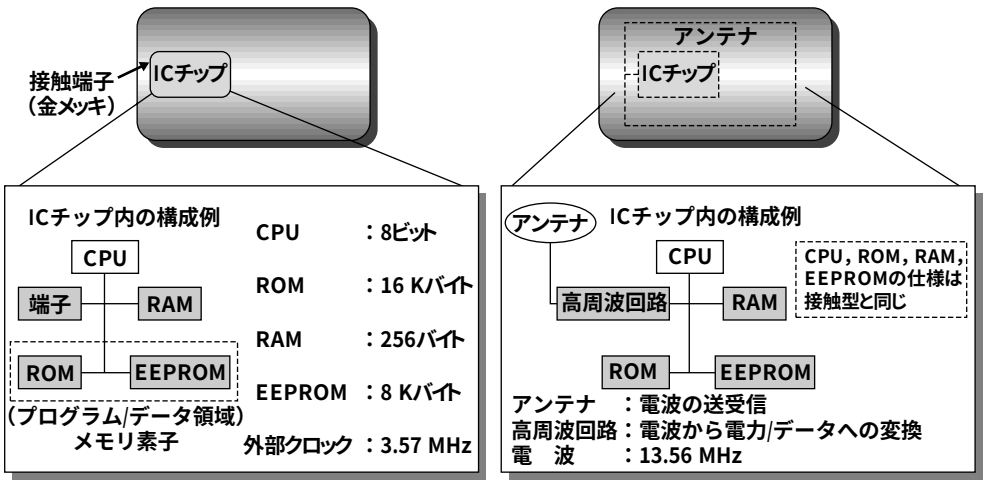
現状でのスマートカードの物理的構成を図-1に示す。ICチップを内蔵し，金属の接触端子が見えているのが接触型スマートカード，接触端子がなく電波を通信方法とするのが非接触型スマートカードである。それぞれ，その内部構造は基本的に同じであり，カード外部との通信方法の部分が相違するのみで，CPU・ROM・RAM・EEPROMなどはどちらにも内蔵されている。

スマートカードは，ROM内に埋め込まれたファームウェア(OSともいう)によりCPUが能動的に動き，外部とのインタフェースにインテリジェント機能が与えられる。また，アクセスコントロール機能(データを見るのにキーデータが必要だったり，見る側の人の資格制限をつけたりなど)を実現することで，システムセキュリティの一翼を担う。

なお，スマートカードの基本的な外部仕様(媒体の大きさ・接触端子の位置・通信プロトコル・電波インタフェースの基本方式など)は，ISOによりほぼ規格化されており，各ベンダともそれに準拠して設計・開発している。

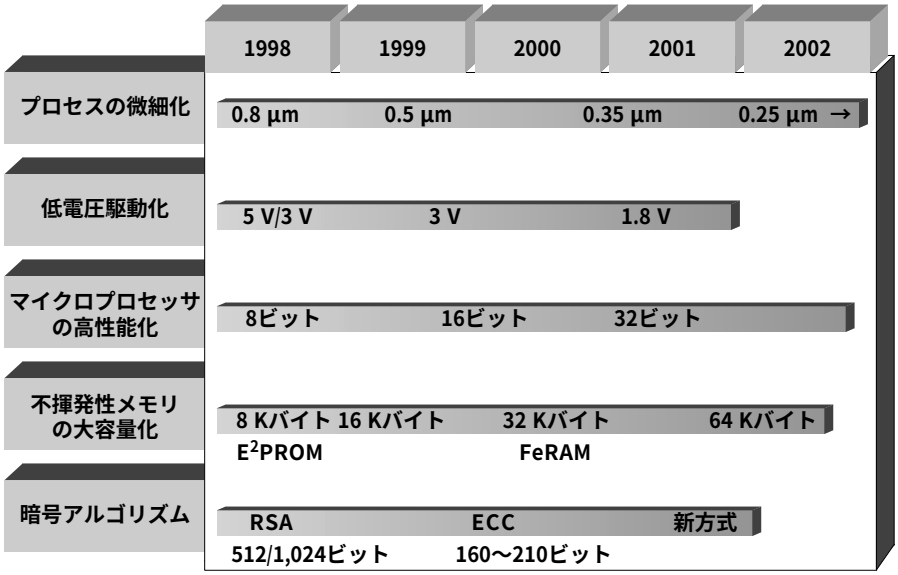
スマートカードの技術的推移やチップテクノロジの推移は，ここ数年劇的に進化しており，今後も加速度的に進むと考えている。

図-２は，過去から将来へかけてのスマートカードに関する技術的推移予想を示したものである。ICチップのプロセス微細加工技術や動作電圧の低駆動化，およびCPUの高性能化やメモリ素子の大容量化が今後も進化し続ける。とくに，セキュリティに重要な暗号技術に関して



(a) 接触型スマートカード　　(b) 非接触型スマートカード

図-1 スマートカードの物理的構成
Fig.1-Physical structure of smart card.



RSA：Rivest Shamir Adelman（素因数分解演算）
ECC：Elliptic Curve Cryptographic（楕円曲線上の離散拡散演算）

図-2　スマートカードに関する技術的推移
Fig.2-Smart card technology in future.

は，従来のDES方式からRSA方式が主流になりつつあり，将来はECC方式など今後も新しい暗号方式が考案され実用化されていくのは必定である。また，耐タンパ性（ICチップ自体の解析難度であり，物理的な面から機能解析ができにくいことをいう）も確実に上がっていくと考えている。

スマートカードは，グローバルな見地からいえば欧州が先進的に導入をしており，米国・アジア地区がそれについで導入を進めてきている状況である。しかし，日本国内では実質これから本格的な導入期を迎えるのが現状で，今後市場として活気を呈する分野といえる。

● スマートカードのファームウェア

スマートカードのセキュリティ機能を高めるのは，第一にカード内蔵のファームウェアの仕様，ついでスマートカードを含む上位のシステム仕様であると考える。現在，接触型ICカード内蔵型のファームウェアには，以下の仕様がある。

(1) ISO仕様：国際標準化に最低限必要な共通仕様をまとめたもの。
(2) EMV仕様：ICクレジットカード系の事実上のデファクト標準。
(3) JICSAP仕様：ICカード利用促進協議会提唱の日本国内における事実上の共通仕様。
(4) MULTOS仕様：マルチアプリケーション対応スマートカードOSとしてMAOSCOが提唱。
(5) JAVAカード仕様：同じくマルチアプリケーション対応スマートカード用OSとしてSUNマイクロシステムなどJAVA陣営が進めているもの。
(6) S. C. W仕様：マイクロソフト社が提唱しているWindows2000に対応するスマートカードの仕様。

これらは，セキュリティ機能の実現にもそれぞれの考え方の相違がでているため，様々なシステム構築や使い勝手に合ったファームウェア仕様を，使う側が選んで使っている。そこで，それぞれ仕様を提唱している陣営は，自仕様のシェア拡大をねらって色々な啓蒙を行っている。

現在のスマートカードのファームウェアは，単機能なシングルアプリケーションを実行するのが主流であるが（ISO/EMV/JICSAP各仕様など），近い将来は１枚のスマートカードで複数のアプリケーションを選択して実行可能な，マルチアプリケーション対応の機能を持つスマートカードが主流となると考える（MULTOS/JAVA各仕様など）。

マルチアプリケーション対応型スマートカードのファームウェア構成を図-3に示す。シリコンハードウェア上に共通プラットフォームとなる基本ファームウェア（OS）を介して，各アプリケーションを安全に選択して実行できるようにセキュリティも考慮された構造となっている。この場合の各アプリケーションは，EEPROM上にローディングして常駐させて実行したり，不要になったアプリケーションは削除して別のアプリケーションに入れ替えたりするなどの機能を持ち，使う側にとって利便

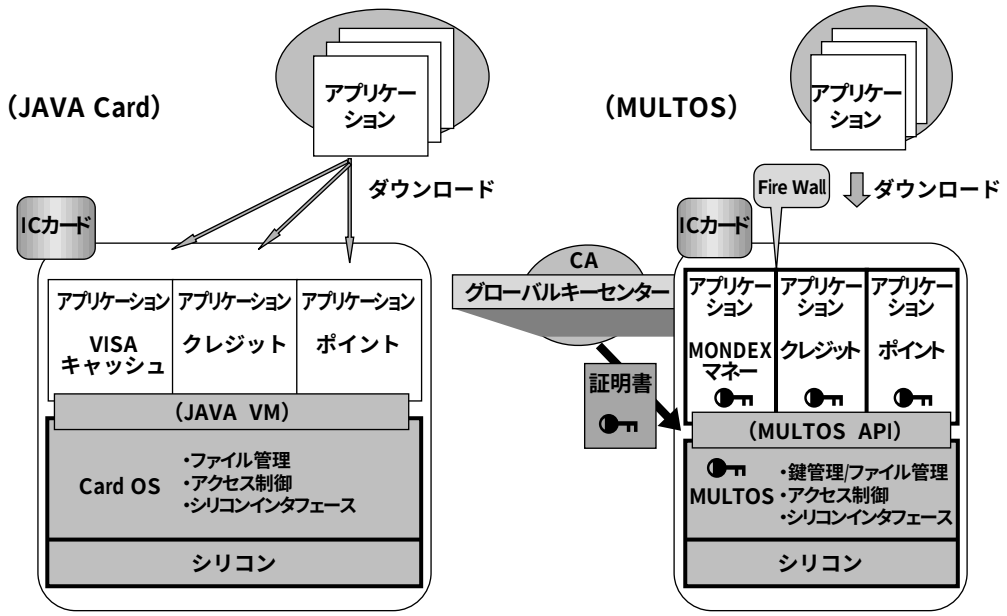


図-3　マルチアプリケーション対応型スマートカードのファームウェア構成
Fig.3-Firmware structure of multi application smart card.

性の高いものになるように考えられている。

● スマートカードの将来像

現在，スマートカードはクレジットカード形状の媒体にICチップを埋め込んで持ち歩けるポータブル性を実現している。しかし，現在のICチップは８～16ビットCPU/16～32 KバイトROM/1 KバイトRAM程度の内容であり，単機能でしかない。一部マルチアプリケーション対応カードがあるが，いまだ実験段階である。

近い将来には，ICチップテクノロジの進化により32ビット以上のCPU，メガバイト級のメモリを搭載した，数年前の卓上型PCに相当するようなスマートカードが出現し，１枚のスマートカードを持ち歩けば色々な場所での様々なアプリケーションの利用が可能となる時代が到来する。これは，数年後に実現すると考えている。しかし，その時，現在のようなカード形状をしているかどうかは需要が決めることであり，不確定な部分が多い。なぜならば，ICチップのテクノロジの劇的な進化とはいえISOで規定するカード形状に埋め込み可能な大きさに，前述のような高機能版ICチップは納まらないと考えるからである（チップ面積で５mm × ５mm程度が限界と考えている）。

ともあれ，現状スマートカードはクレジットカードの形状であり，ここ数年間に日本でも本格的な普及期を迎え，システムセキュリティの核として社会的な認知を得ていくものと考えている。

スマートカードの発行

● スマートカードの発行サービス

発行サービスの処理概要を図-4に示す。

接触型カード発行のプロセスは，カード製造とICのイニシャライズから成る一次発行，およびカードに個人情報などを書き込む二次発行の二つに大別される。

一次発行では次の二つのプロセスがある。まず，カード製造ではクレジットカード形状で表裏面にプレ印刷が施されたプラスチックカードに，ICチップが搭載された電極（ICモジュール）を接着により埋込みを行う。ここでは，ICモジュールの入替えによるカードの偽造を防ぐため，ICモジュールが容易に剥がれない技術の開発が要求される。また，イニシャライズでは，ICチップへカード種別ごとの共通的な，ファイルフォーマッティングやアプリケーションの書き込みを行う。

二次発行では，顧客からあらかじめ入手した個人情報をもとに，カードの個人情報書き込みを行う。その内容としては，ICチップ内への電子情報の書き込みをはじめ，磁気テープ書き込み，エンボス文字，顔写真の印刷やバーコードの印刷などがある。

なお，スマートカード発行ビジネスの顧客に対するサービス向上を目的として，スマートカードサービスセンタを発行工場に併設し，本組織の中で顧客対応，発行作業，品質保証までの業務を総括的に管理・運営するよ

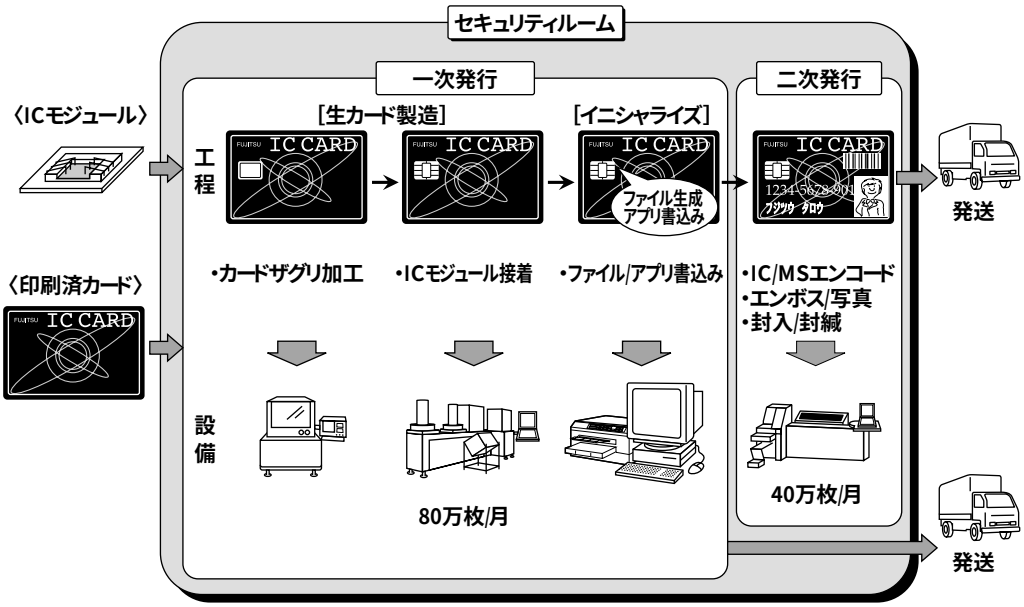


図-4　発行サービスの処理概要
Fig.4-Smart card issuing operation outline.

うにしている。

● スマートカードの発行セキュリティ

発行を進める上で，顧客や富士通の資産(情報/物品)を改ざんや漏洩，盗難などから守る，セキュリティ確保が課題となる。このため，発行業務を委託される顧客に安心していただけるセキュリティ運用体制の構築を進めた。構築に当たっては，富士通社内で協議を重ね，スマートカードに関するセキュリティポリシー(以下，ポリシー)を1998年７月に制定した。

工場でのセキュリティシステム概要を図-5に示す。ポリシーとは，リスクに対して何をどれだけのコストを掛けて守るべきかを明確にする指針であり，その基本方針を「セキュリティ確保の範囲は，限定的で極小化する」こととし，以下を明確にした。

・４段階(S0～S3)のセキュリティ運用レベル
・人/情報/物(物品，施設)に対する脅威の想定と対応方針

また，ポリシーで規定した，人/情報/物に対するセキュリティ確保の対応方針を運用ルール化して，セキュリティ規準を策定した。

規準と運用の要点は以下のとおりである。

(1)　人

・管理責任者を頂点とする運用組織の構築，セキュリティエリア入室権限保有者の認定
・入室権限保有者に対するセキュリティ教育の実施と資格認定
・入室権限保有者のアクセス可能対象(エリア，情報，物品)の限定と承認

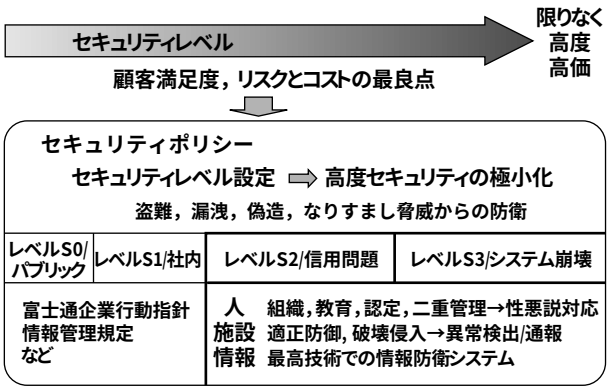


図-5　工場でのセキュリティシステム概要
Fig.5-Security system outline at factory.

(2)　情報/物品

・APL/OSの分割開発
・製造，発行処理における二重管理
・作業/関連行為/工程ごとの記録作成と保管，作業監視/ビデオ記録
・工程ごとの，数の監査記録の整合性確保(audit trail)

(3)　施設

・セキュリティエリア入退室時の個人認証(S3は，生体学的認証併用)
・不法侵入者に対する防護/検知手段敷設

以上により，SET(Secure Electronic Transaction)を提唱するVISA InternationalやMasterCard Internationalの

カード製造施設(部材受入れから出荷までの全体を対象)のセキュリティ要件を最高レベルと考えても，富士通の発行施設は，その要件を十分考慮したものとなっている。

● 発行サービスの今後

スマートソリューションビジネスはスピードが命であり，システム構築とともにスマートカード発行サービスもオーダに対し即カードを配付し，システムが稼働開始できるサービス体制を構築していくことが必要である。これには@niftyなどのネットを有効利用してスマートカードサービスセンタと担当SEやエンドユーザの方々との時間的・物理的距離を縮めて，即応体制を取ることが求められていると考えている。もちろん，将来的にどのようなサービス体制になってもセキュリティの維持が絶対条件であり，これなくして顧客の信頼は得られないことは言うまでもない。

今後の課題

現在はセキュリティ上の問題から専用の発行工場で行っている発行サービスであるが，将来は街角の公衆電話からもアプリケーションの発行ダウンロードができる日が遠からず来るであろうと想像できる。そのためには，今後のビジネススキームの変化に即応できるように先を見越した発行工場運営を考えておくことが肝要であり，現状のサービスと平行して検討していく。

む　す　び

スマートカードとその発行サービスとセキュリティについて，その状況を述べてきた。スマートカードは，スマートソリューションビジネスの最下層のインフラストラクチャを担うキーデバイスであり，今後のビジネス展開とともにますます重要な位置を占めていくものと確信している。

参 考 文 献

(1) ICカード総覧 97～98.(株)シーメディア，推薦ICカードシステム利用促進協議会.
(2) ワイヤレスカードガイドブック99.ワイヤレスカード実用化推進協議会.