H８年－WG０７

ＩＣカードの現状調査報告書

－ 利用ガイドライン策定に向けた現状報告 －

平成９年５月

電子商取引実証推進協議会
ＩＣカードWG

はじめに

ＩＣカードを活用した電子商取引（Electronic Commerce）の実証実験が、国内外に於いて多数実施されている。通産省が推進している実証実験プロジェクトの内、ＩＣカードを活用したプロジェクトも、いよいよ本格的な運用に向けて実験を開始されようとしている。また、国際間の相互運用性を確保するために、国際標準化が積極的に推進されると同時に、これに準拠した業界独自仕様のＩＣカードも広く推進されている。

このような状況の中、本ＩＣカードWG（ＷＧ７）では、ＩＣカードの新規導入、普及拡大、システム応用等への現状調査、課題の抽出、今後の方向性を示す資料として、接触型ＩＣカード、非接触型ＩＣカードの２つの内容を本報告書としてまとめた。

接触型ＩＣカードの検討では、ＩＣカードの実用化と普及の実現を目指して、ＩＣカードを使用した代表的な業務である、①クレジット業務分野、②銀行業務分野、③情報・サービス分野、各分野別に現在の商取引に係わる様々な業務の実態調査と問題点を抽出し、ＩＣカードの具体的な利用方法、ＩＣカード・端末・ネットワークの現状調査と基本要件／課題の抽出を行った。これらの成果を踏まえて、今後のＩＣカード普及の鍵となるＩＣカードの標準化動向、端末の相互運用性、セキュリティー機能、ＩＣカードチップの技術動向等を重点的に調査し、ＩＣカードのあるべき利用モデル策定の為の要件整理と検討作業、及びＩＣカード仕様、端末仕様、業務仕様等に対する各ガイドラインの作成作業に着手した。更に、本報告書では、端末の早期設置を推進するとともに、システムを円滑に運用していくための、端末整備アクションプラン策定についての提言も視野に入れてまとめた。

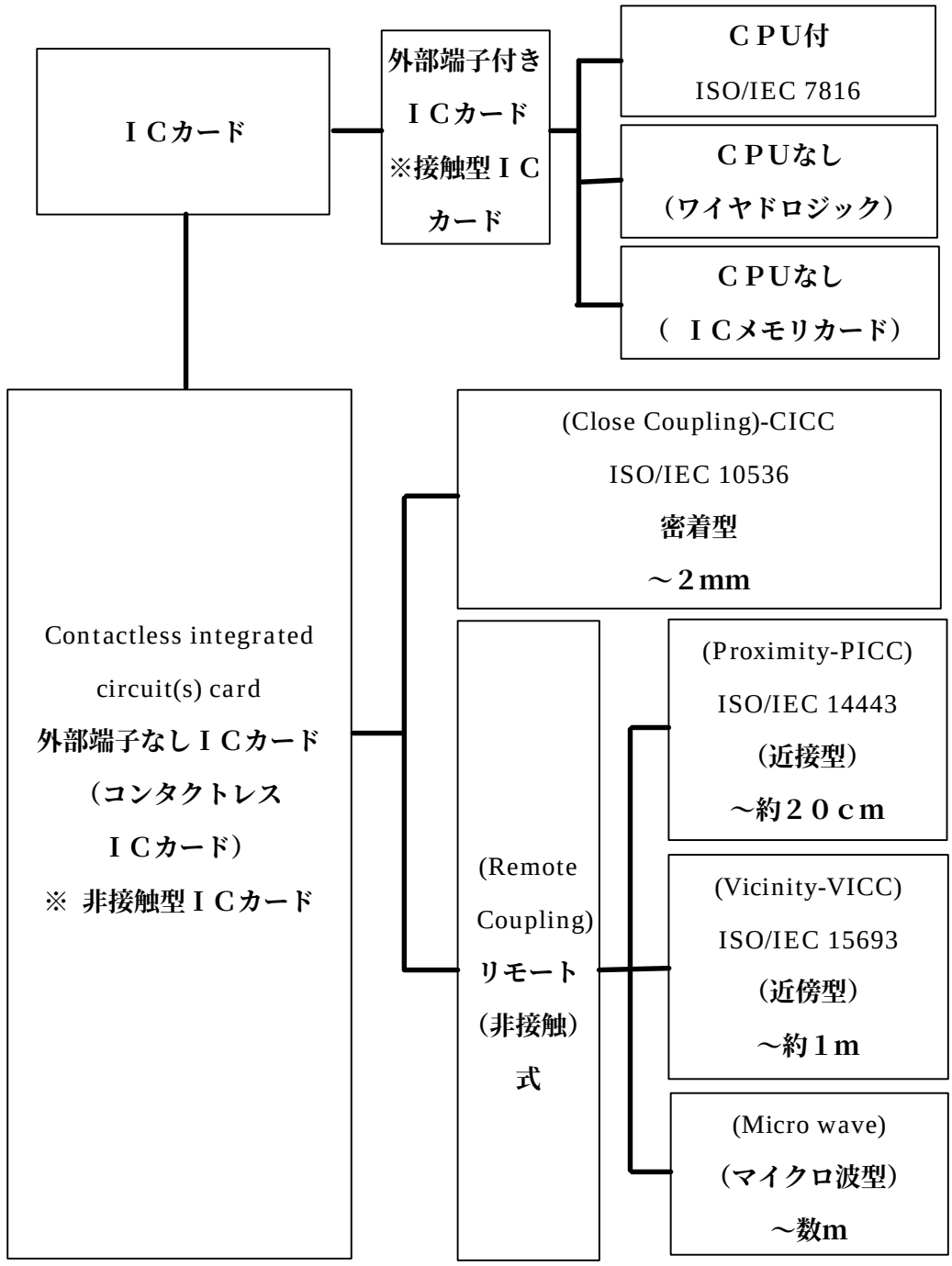
非接触型ＩＣカードの検討では、接触型ＩＣカードと非接触型ＩＣカードとの要件比較、アプリケーション分野、実証実験状況等の調査内容をまとめた。

ＩＣカードを普及・拡大させていくためには、現状の課題を抽出し、検討内容を整理し、運用面･利用面への適用を図る利用ガイドラインの策定が必要であり、本WGの役割と考えている。

本調査報告書は、会員の協力を得て中間成果物としてまとめたものである。

ＩＣカードの分類

本報告書では次のように分類している。



- （　　）内の英語はＩＳＯで審議中、（　　）内の日本語表記は案であり、今後見直しがあり得る。（１９９７年２月、ISO/IEC JTC1/SC17/WG8 ロンドン会議にて開催された会議内容を基に作成） ※は本資料で使用している名称。

用語

ＥＣＯＭ内では、ＥＣに関連する用語の統一化を推進している。

資料に記載しているＩＣカードは、次の内容で使用している。

- 接触型ＩＣカード

  ＥＣＯＭ　ＩＣカードWGでは、ＩＳＯ／ＩＥＣ７８１６準拠のＣＰＵ付ＩＣカードを対象として使用している。

  ＩＳＯでは Integrated circuit cards with contacts、ＪＩＳでは「外部端子付ＩＣカード」と記されている。

  国内の一般的な名称では、ＩＣカード（Integrated Circuit card）、スマートカード（Smartcard）等の名称で使用されている。

- 非接触型ＩＣカード

  ＥＣＯＭ　ＩＣカードWGでは、ＩＳＯ／ＩＥＣ　１０５３６密着型、ＩＳＯ／ＩＥＣ　１４４４３（近接型）、ＩＳＯ／ＩＥＣ　１５６９３（近傍型）の非接触型ＩＣカードを対象としている。（（　）内の名称は、ＩＳＯ国内委員会で審議中）

  ＩＳＯでは Contactless integrated circuit card、ＪＩＳでは「外部端子なしＩＣカード」と記されている。

  国内の一般的な名称は、非接触ＩＣカード（Contactless Smartcard）の名称で使用されている。

  ＥＣＯＭで使用している「非接触型ＩＣカード」の名称は、ＪＩＳでは用いられていないが、「接触型ＩＣカード」との関連上、本報告書で使用している。

ＩＣカードＷＧのホームページ

ＥＣＯＭのWWW上にＩＣカードWGのホームページを開設している。

ＥＣＯＭ　　ＵＲＬ： http://www.ecom.or.jp/

ＩＣカードWG ＵＲＬ： http://www.ecom.or.jp/about_wg/wg07/index.htm

目次

1 ＩＣカードWGの概要

1.1 目的

ＥＣＯＭ設立の目的は、ＥＣ実現のために課題を解決し、ＥＣが実際のビジネスや社会で実現するために必要な、安全性、信頼性、操作性を高めるための共通基盤を構築し、相互運用性を確保する事であり、本内容を踏まえて、ＩＣカードWGでは、「ＩＣカード」を使用した共通基盤技術の構築により「電子商取引の実現とＩＣカードの普及・拡大」を目的とする。

1.1.1 検討項目及び目標

ＩＣカード関連技術と標準化の動向について調査・分析し、実証実験への適用について検討する。さらに必要に応じてパイロットモデル等の開発、標準の作成を行う。

① 接触型ＩＣカードについて開発動向を調査するとともに、実装モデルについても
検討を行う。

② 非接触型ＩＣカードについて、利用環境の検討を行い、開発する仕様を選定。
また、共通技術開発プロジェクトを通じて開発を行う。

③ 実証実験における実験項目の検討と結果をとりまとめるとともに、関連技術の
データベースの構築を行う。

1.1.2 検討対象

電子商取引に絡む「ＩＣカード及びＩＣカードに関連する全体システム」を対象とし、ＥＣＯＭ他WGとの連携を深めて検討する。

1.1.3 検討のポイント

(1) 利用者、加盟店、発行者、各々にとってメリットのあるシステム

使い易さ、安全性、コスト、サービスの拡大

(2) 標準化、互換性、相互運用性

(3) 多目的利用

決済、セキュリティ、情報、ＩＤ、各分野での利用動向

(4) 技術課題

決済方式、本人認証、暗号化技術、プライバシー保護

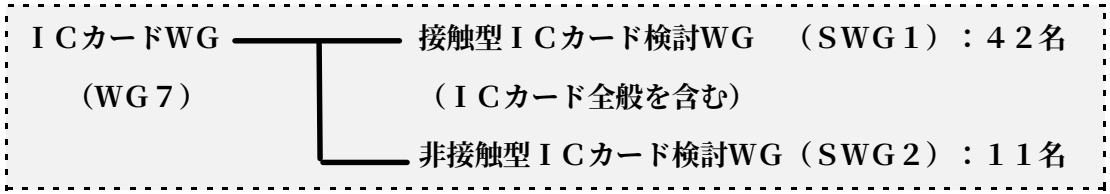
(5) 制度的、法的課題

(6) 国際流通性

1.2 運営体制

ＩＣカードWGへの参加メンバーが多いため、ＩＣカード全般を含めたＩＣカード検討WG（ＳWG１）と、非接触型を対象とした非接触型ＩＣカード検討WG（ＳWG２）とに分かれて推進した。

ＩＣカードWGの参加メンバー合計５３名 ＋ 主査・副主査４名（９７年3月時点）



2 接触型ＩＣカードの現状調査

2.1 ＩＣカード

本章では最初にＩＣカードについて理解を深めるために、ＩＣカードと磁気ストライプカードとの比較、ＩＣカードの標準規格、そしてＩＣカードの内部構造について概説する。

次にＩＣカードチップの技術動向、並びにＩＣカードの標準化動向についての現状調査結果を述べる。ＩＣカードチップについては、ＩＣカードに持つべき高セキュリティー機能を実現するための今後のコア技術と考えられるコ・プロセッサＬＳＩを調査した。また相互運用性のキーとなるＩＣカードの標準仕様については、ＩＣカードで使用されるコマンドについてＩＳＯ／ＪＩＳ並びに全銀協／ＥＭＶ等国内外の主要な団体・企業の標準化動向を調査し、各コマンド仕様を比較した。

最後に、エレクトロニックコマースにおけるＩＣカードの利用形態について述べる。

2.1.1 ＩＣカードと磁気ストライプカードの比較

現在広く使用されている銀行キャッシュカードやクレジットカード等の磁気ストライプカードと接触型ＩＣカードを比較すると表 2-1のようになる。

ＩＣカードでは、キー照合回数制限、暗号による認証とも、各アプリケーション毎に、かつ「読み取り」「追記」「書き換え」の各作業毎に設定することができる。このため、１次、２次、３次、といった発行の段階によって、アクセスできる作業領域を制限することができ、フィールドでの信頼性を高めている。

表 2-1 接触型ＩＣカードと磁気ストライプカードの比較表

		磁気カード	接触型ＩＣカード
機 能 性		単一機能	多機能
データ記憶容量		８０文字	５００～１６,０００文字
演算機能		なし	あり
ＲＯＭ容量		－	６ＫＢ～２０ＫＢ
ＲＡＭ容量		－	１２８～５１２バイト
標準化仕様		ＩＳＯ、ＪＩＳ	ＩＳＯ、ＪＩＳ，EMV
偽　造		容易	困難
セキュリティ	物理的な方法によるデータの読み出し	可	不可 (*1)
	キー照合回数制限	ホストで制限	カードで制限 (*2)
	暗号による認証(*3)	不可	可
カードコスト比		１	２．５～１０
アプリケーション		単一アプリケーション	複数アプリケーション
活用分野		リアル	リアル、バーチャル

*1　物理的方法によるデータの読み出し（Physical Protect）

ＩＣカードは、こじ開けなど、物理的な方法によってメモリ内部に書き込まれている情報を取り出すことができないよう、ＩＣチップに特殊な加工が施されている。

*2　キー照合回数制限

アプリケーションにアクセスする場合に、暗証番号の入力を必要とするように設定し、正しくない暗証番号を設定された回数入力すると、そのアプリケーションへのアクセスができなくなるようにする仕組み。

*3　暗号による認証

端末側とカードとに、共通の暗号化機能を持たせ、アクセスの際に与えられる乱数を端末とカードとで暗号化して照らし合わせ、一致を確認することによってアクセス権を与える仕組み。これによって決められた端末でしかアクセスできないようにする。

2.1.2 ＩＣカードの標準規格

ＩＣカードについての標準規格は、一般のプラスチックカードに関する規格（ＪＩＳ　Ｘ６３０１）及び外部端子付きＩＣカードの物理的特性に関する規格（ＪＩＳ　Ｘ６３０３）によって規定されている。

2.1.2.1 一般カード規格（ＪＩＳ　Ｘ６３０１）

(1) 材質・形状・寸法

① 材質

日本工業規格（ＪＩＳ）の規格（ＪＩＳ　Ｘ６３０１）において、一般のプラスチック・カードのカードの基板は、塩化ビニル重合体、塩化ビニル・酢酸ビニル共重合体またはこれらと同等以上の特性を持つ材料で作られたシートを積層し、一体化したもので、通常のエンボス処理に対して適正なものとされている。

また、この基板が磁気ストライプの特性を損なわないこと、カードの材質及びカードの加工材料がリーダ・ライタを汚さないことなどが規定されている。

② 形状・寸法

カードの寸法に関しては、横８５.６ミリ×縦５４ミリ×厚さ０.７５ミリで、それぞれ誤差の範囲が規定されている。また、カードの４角については決められた半径において丸み仕上げされることになっている。

③ その他

他に、カード縁部の仕上げ、反り、表面の状態などが定められている。

(2) 物理的特性

カードの物理的特性は、下記について、それぞれ数値を示して規定され、試験方法はＪＩＳ　Ｋ６７４５（硬質塩化ビニル板）に規程がある場合それによる、とされている。

・引張強さ
・衝撃強さ
・柔軟温度
・積層性
・耐熱性
・耐燃伸縮性
・耐薬品浸せき性
・粘着性
・耐湿性
・光透過濃度

また、カードは燃えにくく静止した大気中で自己消化性であること、通常の取り扱いにおいて毒性を持たないこと、などが定められているほか、

磁気ストライプの物理的特性、磁気ストライプの電磁変換特性についても規定がある。

2.1.2.2 外部端子付きＩＣカードの物理的特性（ＪＩＳ　Ｘ６３０３）

接触型ＩＣカード（一般カード規格で規定されたカード基板中にＩＣを内蔵し、カード面にＩＣの外部端子をもつカード）については、ＪＩＳ　Ｘ６３０３で規定されている。

(1) 物理的特性

ＩＣカードの、ＩＣ及び端子を除く部分については、ＪＩＳ　Ｘ６３０１で定められた物理的特性が適用されるが、他に下記についてそれぞれ数値を示して規定されている。

- 紫外線、Ｘ線に対する耐性
- 端子の表面とこれに接するカード表面との高さの差
- 機械的強度
- 端子の電気抵抗
- 磁気ストライプ及びＩＣの電磁的相互干渉
- 耐外部磁界
- 耐静電気

(2) 端子の寸法及び数並びに位置

① 寸法

それぞれの端子には、２mm×１.７mm以上の接点面がなければならず、各端子間は電気的に絶縁されてなければならない。

② 端子の数

Ｃ１からＣ８の８個の端子について規定されている。

③ 端子の位置

端子位置は、カードの表面または裏面の左端及び上端を基準として、最大・最小寸法が定められている。

(3) 端子の割付

端子番号（Ｃ１～Ｃ８）のそれぞれの端子について、「端子名」「端子の機能」が規定されている。

(4) その他

ＪＩＳ　Ｘ６３０３では他に、端子配置の測定方法、耐曲げ・耐ねじれ・耐静電気の試験方法が具体的に記されている。

2.1.3 ＩＣカードの内部構造

図 2-1はＩＣカード内部の仕組みを簡単に示したものである。ＩＣチップはＣＰＵ、メモリ、ファイルで構成されておりコンピュータ機能を持っている。ＩＣカードはプラスチックカードに、このＩＣチップを埋め込んだものである。

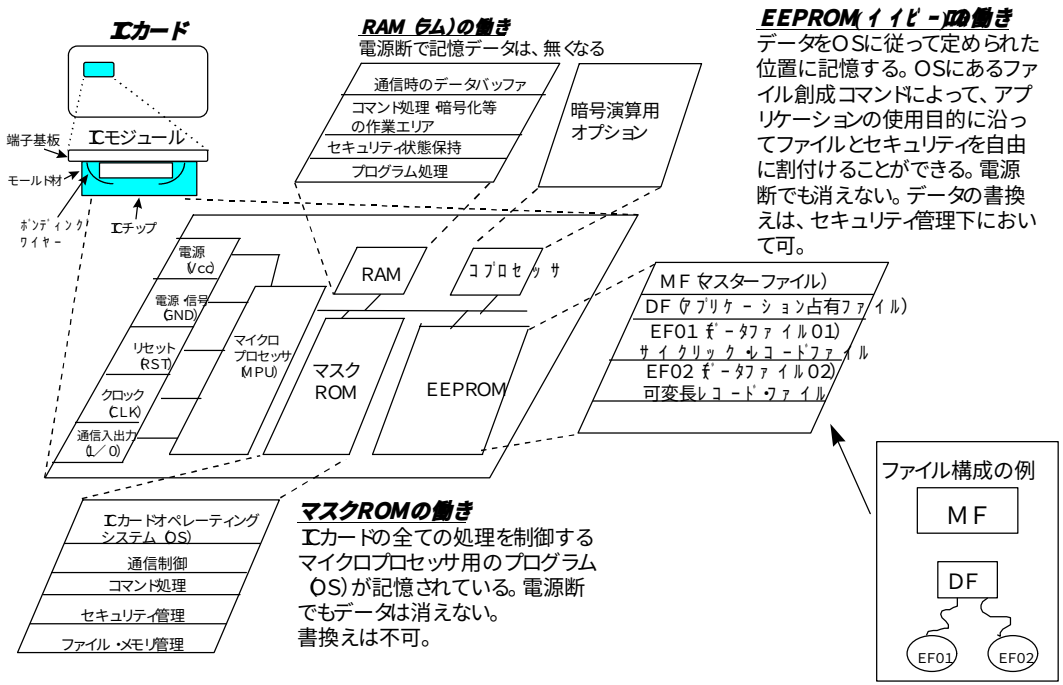


図 2-1 ＩＣカード内部の仕組み

2.1.4 電子商取引に用いられるＩＣカード用ＬＳＩへの要件

電子商取引では、高い安全性が要求されるため、暗号が必要とされる。このため、従来から使用されている共通鍵暗号方式に加え、鍵の配送が容易に行える公開鍵暗号方式の併用が考えられる。

公開鍵暗号方式をサポートしているＩＣカード用ＬＳＩには、公開鍵暗号を処理する専用回路（コ・プロセッサ）を搭載したＬＳＩが出現している。今後、電子商取引に使われるＩＣカードには、コ・プロセッサを搭載したＬＳＩの必要性が高くなる事が考えられる。

2.1.4.1 公開鍵暗号方式の必要性

電子商取引が、インターネットなどのオープンな環境でも安全に実施されるには、暗号技術の取り込みが不可欠である。暗号は、鍵の観点から共通鍵方式と公開鍵方式に二分される。電子商取引では、従来から使用されているＤＥＳに代表される共通鍵暗号方式とＲＳＡに代表される公開鍵暗号方式が併用されていくと考えられる。

共通鍵暗号方式：対称暗号とも呼ばれ、暗号化鍵と復号化鍵が同一の暗号
公開鍵暗号方式：非対称暗号とも呼ばれ、暗号化鍵と復号化鍵が異なる暗号

公開鍵暗号方式の最大の利点は、鍵の配送が容易なことにある。公開鍵で暗号化されたものは、対になる秘密鍵でしか復号化できない。このため秘密鍵の管理のみ厳重に実施すれば、公開鍵はその名の通り公開してオープンなネットワークでの配送もできる。共通鍵暗号方式では、一つの秘密鍵を暗号化・復号化に使うため鍵の配送に当たっては充分な管理が必要となる。

ＤＥＳを代表とする共通鍵暗号方式では、論理演算主体の処理が行われる。これに対し、ＲＳＡを代表とする公開鍵暗号方式では、算術演算主体の処理が行われる。従って、公開鍵暗号方式では、演算量が多大となり、現在ＩＣカード用ＬＳＩに使用されている８ｂｉｔＣＰＵでは能力が不足する場合がある。このため公開鍵暗号方式をサポートするＩＣカード用ＬＳＩでは、専用回路（コ・プロセッサ）を搭載したＬＳＩがある。

ＤＥＳ（共通鍵暗号方式）：ビット列のシフト、ビット単位の転置、排他的論理和
　　等の論理演算
ＲＳＡ（公開鍵暗号方式）：ベキ乗剰余型算術演算

（平文を鍵の一つの値でベキ乗し、その結果を鍵のもう
一つの値で割る。この際の余りを暗号文とする。）

前述のように公開鍵暗号方式は処理に時間を要するため、電子商取引においては、データの重要性に応じて公開鍵暗号と共通鍵暗号が使い分けられていくと考えられる。

2.1.4.2 コ・プロセッサを搭載したＩＣカード用ＬＳＩの特長

以下、各社から出されている資料を基に、コ・プロセッサを搭載したＩＣカード用ＬＳＩの現状・次期・将来（２０００年を目処）を仕様面からまとめる。

表 2-2 ＩＣカード用ＬＳＩ比較表

項目	現状	次期	将来
ＣＰＵ	８ｂｉｔ （68HC05, 80C51, Z80, ｵﾘｼﾞﾅﾙ ）	高速化 （ 16bit 化, 内部ｸﾛｯｸ高化 ）	更なる高速化 （ 一部では RISC の採用も検討 ）
ＲＯＭ	１０～２０ＫＢ	２０～３０ＫＢ	拡張
ＲＡＭ	５１２Ｂ	１ＫＢ	拡張
不揮発性メモリ　技術	ＥＥＰＲＯＭ	ＥＥＰＲＯＭ	ＥＥＰＲＯＭ ＋Ｆｌａｓｈ ＋ＦＲＡＭ
最大容量	８ＫＢ	１６ＫＢ	拡張
ｺ･ﾌﾟﾛｾｯｻ　最大鍵長	１，０２４ｂｉｔ	２，０４８ｂｉｔ	←
性能＊１	１００m秒以下	５０m秒以下	高速化
チップサイズ	２５mm^{2}以下	縮小化 （３×５mm^2）	同サイズでの機能 拡張、高速化
電源	３Ｖ／５Ｖ	←	←
ＬＳＩ技術	０．８μ以下	０．６μ以下	ﾃﾞｨｰﾌﾟｻﾌﾞﾐｸﾛﾝ
検知回路 ＊２	電圧 クロック周波数	←＋α	←＋α

＊１：鍵長５１２ｂｉｔで中国剰余定理を用いた場合のＲＳＡ暗号方式でのデジタル署名の処理性能を表示。

＊２：タンパーレジスタンス機能は、安全性に関わることからそのほとんどが非公開である。但し、その一部である検知回路に関しては公開されているものがあり、現状についてはそれを表示。次期、将来については不明点が多いため何らかの

機能強化は実施されると云う程度とした。

2.1.5 ＩＣカードの標準化動向

2.1.5.1 標準化作業

現在ＩＣカードの標準化については、長年にわたり国際標準化機構（ＩＳＯ）において国際的な標準化作業が進められている。 国内的にもＩＳＯの規格化に準じて、（財）日本規格協会でのＪＩＳ化作業が行われている。

又、これらの標準規格をもとに、各種業界で業界内の標準仕様を作成する動きがある。

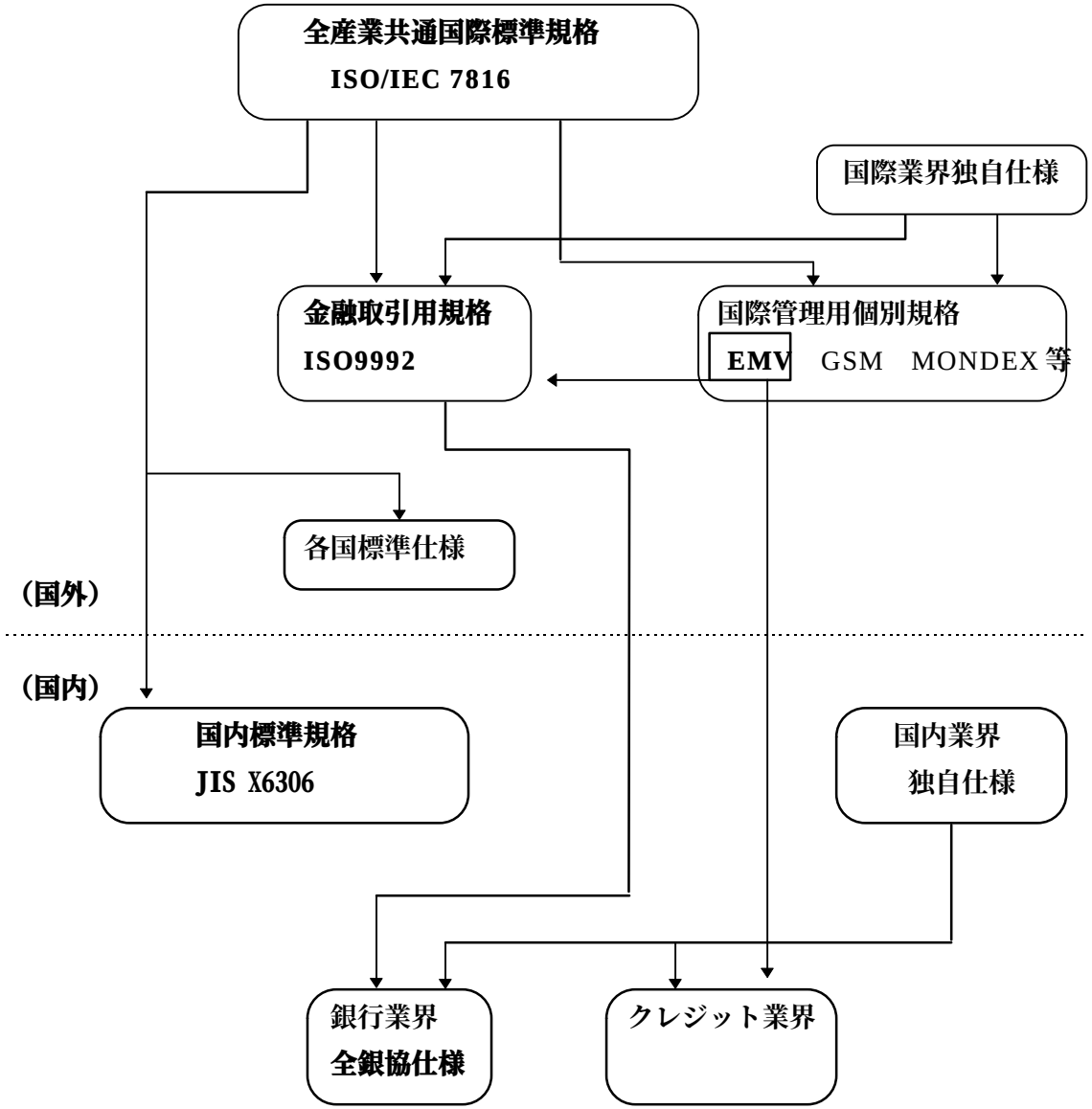

全産業共通国際標準規格
ISO/IEC 7816
国際業界独自仕様
金融取引用規格
ISO9992
国際管理用個別規格
EMV GSM MONDEX 等
各国標準仕様
（国外）
（国内）
国内標準規格
JIS X6306
国内業界
独自仕様
銀行業界
全銀協仕様
クレジット業界

図 2-2 ＩＣカード標準化作業の流れ

標準化の流れを見てみると図 2-2の様になる。

2.1.5.2 各仕様のコマンド比較

表 2-3 コマンド比較表

コマンド		ISO/IEC 7816-4	ISO 9992-2	JIS X6306	全銀協仕様	EMV仕様
基本コマンド						
1	READ BINARY	○	x	―	x	x
2	WRITE BINARY	○	x	―	x	x
3	UPDATE BINARY	○	x	―	x	x
4	ERASE BINARY	○	x	―	x	x
5	READ RECORD(S)	○	○	○	○	○
6	WRITE RECORD	○	x	―	x	x
7	APPEND RECORD	○	○	○	○	x
8	UPDATE RECORD	○	○	○	○	x
9	GET DATA	○	○	―	○	○
10	PUT DATA	○	x	―	x	x
11	SELECT FILE	○	○	○	○	○
12	VERIFY	○	○	○	○	○
13	INTERNAL AUTHENTICATE	○	○	○	○	○
14	EXTERNL AUTHENTICATE	○	○	○	○	○
15	GET CHALLENGE	○	○	○	○	x
16	MANAGE CHANNEL	○	x	―	x	x
伝送用共通コマンド						
17	GET RESPONSE	○	○	―	x	○
18	ENVELOPE	○	x	―	x	x
追加コマンド						
19	DEACTIVATE FILE APPLICATION BLOCK	x	○	x	○	○
20	GENERATE TCC GENERATE AC	x	○	x	○	○
21	GET PROCESSING OPTIONS	x	○	x	○	○
22	REACTIVATE FILE APPRICATION UNBLOCK	x	x	x	○	○
23	UNBLOCK KEY PIN CHANGE/UNBLOCK	x	x	x	○	○
24	CHANGE KEY PIN CHANGE/UNBLOCK	x	x	x	○	○
25	CARD BLOCK	x	x	x	x	○

○…規定　　―…留保　　x…規定せず

ＩＣカードの仕様はＩＳＯ／ＩＥＣ７８１６を中心に前述したような関係にある。これらの仕様を比較するために、ＩＳＯ／ＩＥＣ７８１６、ＪＩＳ Ｘ６３０６、ＩＳＯ９９９２（ＦＤＩＳ）、全銀協ＩＣカード標準仕様（９７年４月改訂版）、EMV仕様（ｖ３．０）の使用されるコマンド一覧を表 2-3に示す。

(1) コマンドの比較表の説明

以下は表 2-3のコマンド比較表を説明する為に記述した一考察である。各標準のコマンド機能は改良や変更があるので、常に最新のドキュメントを参照されたい。

① ISO/IEC 7816-4 と JIS X 6306 のコマンド機能

政府から JIS 規格と ISO 規格を一致させる方針が出されている。従って、この JIS を制定するにあたっては、原則として ISO 規格と一致させている。

しかしながら、従来から日本に存在しているアプリケーションに使用している IC カード(16 社仕様)から ISO 準拠にスムーズな移行が出来る様に、その機能を考慮して制定が行われた。

② 金融分野のコマンド機能

ISO 9992-2 は、ISO/IEC 7816-4 の制定を待って、そ

れをベースに金融取引用 IC カード仕様の制定が始まった。

その制定作業の間に EMV 仕様が出現し、それとの協調が必要となり最小限のコマンドが追加された。また、それが基になって全銀協仕様が作られた。

③ 各アプリケーション分野の規格のうちで制定されていないコマンドについて

A. BINARY 系のコマンド

READ BINARY,WRITE BINARY 等の BINARY 系のコマンド機能は、IC カードの内部のファイル形式に依存している。

これらの BINARY 系は透過ファイルに対するコマンドで、国内の一部を除いて使用されていないので、これらの機能は積極的には取り込まれていない。

透過ファイルは、データを詰め込む事が可能であるが、RECORD 系のファイルはデータのハンドリングがよく、アクセススピードの向上が可能である。従って国内に於てはこの機能に着目して RECORD 系ファイルが選択された。

結果的には金融分野の IC カードコマンド機能仕様である ISO 9992-2 及びそれに基づく全銀協仕様、EMV 仕様等では、おそらく同様な理由によって、これらバイナリー系のコマンドのサポートは必須とされていない。

B. WRITE RECORD コマンド

なぜ JIS を始め、金融分野の IC カード仕様の中に WRITE RECORD コマンドが必須ではないのであろうか。'WRITE'と言う名前が付いているので、誰でもが不思議に感ずる事であるが、このコマンドの機能は、一回だけ書き込む機能と、それと別に、書き込もうとするデータと既に書き込んであるデータの各ビットと AND 論理あるいは OR 論理をとって書き込むという機能を持っている。大変ややこしい機能であるが、半導体メーカがそれぞれの製造プロセスの違いによって生ずるメモリーの初期の状態の違いからこの様な書込み機能が要求されたものである。ロジック付 IC カードでは、この事が問題となるが、CPU 付きの IC カードでは、内部のオペレーションシステム(OS)によってこれらのことは自動的に解決されている。従ってこのコマンドは必須とされない。

C. PUT　DATA コマンド

このコマンドは書込系である。ISO においては GET コマンド(読出し系)とは対をなして提案されたものである。しかし、EMV 仕様に於てこの

コマンドは対としては存在していない。もっと正確に言うと「存在させてはいけない」とう解釈もできる。

それは GET DATA コマンドは内部で作られるデータを読み出すものと定義されているからである。従ってそれらのデータを外部から変更できる機能はあってはならないのである。

JIS が制定されたのは、金融分野の IC カード仕様が制定されるかなり以前のことであったのでこの理由で必須とされなかったのではない。書込には UPDATE RECORD、APPENDRECORD 等のコマンドが存在し、これで十分考えられるアプリケーションに対応できるものと考えたからである。

D. MANAGE CHANEL

通常ロジカルチャネルのチャネル設定は SELECT FILE コマンドの CLA バイトで行う。しかし、SELECT FILE コマンドは、余りにも多くの機能を持ちすぎた為に別々にしたコマンドも必要だという事で規定された。

国内では、SELECT FILE コマンドでチャネルの設定を行うので、このコマンドは必須となっていない。

E. 伝送用コマンド

このコマンドは、キャラクタ伝送通信プロトコル T=0 を用いるときに必要とされるものである。国内では、ブロック伝送通信プロトコル T=1 が用いられるためこれらのコマンドは必須となっていない。しかし、金融分野では、T=1,T=0 の両方を用いてもよいことになっているので、端末側では必要とされる場合が有る。

GET RESPONSE コマンドは、T=0 で必須のコマンドである。

ENVELOPE コマンドはドイツが提案したものであるが使用方法は不明な部分が多い。

F. 追加コマンド

ISO/IEC 7816-4 で現在までに規定されていないコマンド機能であるが、IC カードシステムの管理をして行く上で必要とされるものが追加されている。

現在、ISO ではこれらのコマンドの制定をすすめており、いずれこの部分の ISO が完成すると各分野へも少なからず変更の要請が起こることも考えられる。

当然 ISO に無いものは JIS とはなっていない。同じ行に書かれている上段と下段のコマンド名は、ほぼ同じコマンド機能を示している。

2.1.5.3 コマンド解説

ＩＳＯ／ＩＥＣ７８１６－４

（１）ＲＥＡＤ　ＢＩＮＡＲＹ

ＥＦの内容（の一部）をレスポンスとして与えるために使用する。

セキュリティステータスが、ＥＦに定義づけられた読み出し機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

もし、レコード構造のＥＦを対象に実行された場合には、処理を中断すべきである。

サポート機能

- **読み出し開始オフセットアドレス指定**
- **短縮ＥＦ識別子指定可能。**

（２）ＷＲＩＴＥ　ＢＩＮＡＲＹ

ＥＦ内にバイナリデータの書き込みを行うために使用する。

ファイル属性に依存して、以下の動作の内いずれか１つを行う。

- **コマンドによって得たビットにより、既にカード内に格納されているビットの論理的 OR を取る（ファイルの論理的消去時のビット状態は０である）。**
- **コマンドによって得たビットにより、既にカード内に格納されているビットの論理的 AND を取る（ファイルの論理的消去時のビット状態は１である）。**
- **コマンドによって得たビットにより、カード内に一度きりの書き込みを行う。**

セキュリティステータスが、ＥＦに定義づけられた書き込み機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

もし、透過構造以外のＥＦを対象に実行された場合には、処理を中断しても良い。

サポート機能

- 書き込み開始オフセットアドレス指定
- 短縮ＥＦ識別子指定可能

（3）ＵＰＤＡＴＥ　ＢＩＮＡＲＹ

コマンドによって得られたビットによって、既にＥＦ内に存在するビットの書き換えを行うために使用する。

セキュリティステータスが、ＥＦに定義づけられた書き換え機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

もし透過構造以外のＥＦを対象に実行された場合には、処理を中断しても良い。

サポート機能

- 書き換え開始オフセットアドレス指定
- 短縮ＥＦ識別子指定可能

（4）ＥＲＡＳＥ　ＢＩＮＡＲＹ

ＥＦの内容（の一部）を与えられたオフセットから順番に、論理的消去状態にセットするために使用する。

セキュリティステータスが、ＥＦに定義づけられた消去機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

もし、透過構造以外のＥＦを対象に実行された場合には、処理を中断しても良い。

サポート機能

- 消去開始オフセットアドレス指定
- 短縮ＥＦ識別子指定可能

（5）ＲＥＡＤ　ＲＥＣＯＲＤ（Ｓ）

ＥＦ内の特定のレコード（またはレコードの最初の部分）を読み出すために使用する。

セキュリティステータスが、ＥＦに定義づけられた読み出し機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

もし、レコード構造以外のＥＦを対象に実行された場合には、処理を中断すべきである。

サポート機能

- レコード番号して単一レコード読み出し
- レコード番号指定複数レコード読み出し（指定レコード番号から最終レコード）
- レコード番号指定複数レコード読み出し（最終レコードから指定レコード番号）
- 指定レコード識別子の最初のレコード読み出し
- 指定レコード識別子の最後のレコード読み出し
- 指定レコード識別子の次のレコード読み出し
- 指定レコード識別子の前のレコード読み出し
- 短縮ＥＦ識別子指定可能

（6）ＷＲＩＴＥ　ＲＥＣＯＲＤ

ファイル属性に依存して、以下の動作の内いずれか１つを行うために使用する。

- コマンドによって得たレコードデータにより、既にカード内に格納されているレコードデータの論理的 OR を取る。
- コマンドによって得たレコードデータにより、既にカード内に格納されているレコードデータの論理的 AND を取る。
- レコードの一度きりの書き込みを行う。

セキュリティステータスが、ＥＦに定義づけられた書き込み機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

もし、透過構造のＥＦを対象に実行された場合には、処理を中断すべきである。

サポート機能

- レコード番号指定書き込み
- 最初のレコード書き込み
- 最後のレコード書き込み
- 次のレコード書き込み
- 前のレコード書き込み

- 短縮ＥＦ識別子指定可能

（7）ＡＰＰＥＮＤ　ＲＥＣＯＲＤ

順編成構造のＥＦの最終位置にレコードを追記する、又は循環順編成構造のＥＦにレコード番号１のレコードを書き込むために使用する。

セキュリティステータスが、ＥＦに定義づけられた追記機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

もし、透過構造のＥＦを対象に実行された場合には、処理を中断すべきである。

サポート機能

- １レコード追記書き込み
- 短縮ＥＦ識別子指定可能

（8）ＵＰＤＡＴＥ　ＲＥＣＯＲＤ

コマンドメッセージの所定のビットで指定されたレコードを更新するために使用する。

セキュリティステータスが、ＥＦに定義づけられた書き換え機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

もし、透過構造のＥＦを対象に実行された場合には、処理を中断すべきである。

サポート機能

- レコード番号指定書き換え
- 最初のレコード書き換え
- 最後のレコード書き換え
- 次のレコード書き換え
- 前のレコード書き換え
- 短縮ＥＦ識別子指定可能

（9）ＧＥＴ　ＤＡＴＡ

応用システムの環境に応じて、一つ以上のデータ対象を取り出すために使用する。

セキュリティステータスが、アプリケーションによって定義されたセキュリティ状態を満たしていれば、実行可能である。

サポート機能

- １バイトの BER-TLV タグ指定
- ２バイトの BER-TLV タグ指定
- １バイトの簡易符号化 TLV タグ指定
- データ部で示された BER-TLV タグリスト指定
- 私的利用指定

（１０）ＰＵＴ　ＤＡＴＡ

一つ以上のデータ対象を格納するために使用する。

セキュリティステータスが、アプリケーションによって定義されたセキュリティ状態を満たしていれば、実行可能である。

サポート機能

- １バイトの BER-TLV タグ指定
- ２バイトの BER-TLV タグ指定
- １バイトの簡易符号化 TLV タグ指定
- データ部で示された BER-TLV タグリスト指定
- 私的利用指定

（１１）ＳＥＬＥＣＴ　ＦＩＬＥ

論理チャネルに対して、一時的指定ファイルを設定するために使用する。

サポート機能

- ＤＦ名によるＤＦの選択
- ファイル識別子によるＭＦの選択

- ファイル識別子によるＤＦの選択
- ファイル識別子によるＥＦの選択
- ＤＦ識別子による子ＤＦの選択
- ＥＦ識別子によるカレントＤＦ配下のＥＦの選択
- 親ＤＦの選択
- パスによるＭＦからの選択
- パスによるカレントＤＦからの選択
- ＦＣＩの返信
- ＦＣＰの返信
- ＦＭＤの返信

（１２）ＶＥＲＩＦＹ

接続装置から送られた照合データと、ＩＣカード内に格納されている参照データ（例えばパスワード）とを、ＩＣカード内で比較するために使用する。

セキュリティステータスを比較の結果によって変更しても良い。

比較不一致をＩＣカード内に記録しても良い。（例えば参照データの使用に対する再試行の回数を制限するため）

サポート機能

- 与えられる情報なし
- 共通な参照データ（例えばカードパスワード）
- 固有の参照データ（例えばＤＦ固有のパスワード）
- 参照データ番号指定による比較

（１３）ＩＮＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

外部から種となる情報（例えば乱数）を与えて、ＩＣカード内の機密情報（例えば鍵）から認証コードの計算を開始させるために使用する。

機密情報がＭＦに付随している場合、このコマンドはＩＣカード全体の認証に使用しても良い。

機密情報がＤＦに付随している場合、このコマンドはそのＤＦの認証に使用しても良い。

このコマンドの実行の可否は、先行のコマンド（例えば VERIFY コマンド、SELECT FILE コマンド）又は、機密情報選択の実行結果に依存しても良い。

このコマンドはアルゴリズムが既に選択されていれば、そのアルゴリズムを使用しても良い。

機密情報、又はアルゴリズムの使用回数を制限するために、このコマンドの発行回数をＩＣカード内に格納しても良い。

サポート機能

- 与えられる情報なし
- 共通な参照データ（例えばカードパスワード）
- 固有の参照データ（例えばＤＦ固有のパスワード）
- 参照データ番号指定による比較

（１４）ＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

ＩＣカードに認証結果を計算させ、それに応じてセキュリティステータスを更新させるために使用する。

ＩＣカードは、例えば先行する GET CHALLENG コマンドに対して発行した種、ＩＣカード内に機密情報として格納されている鍵、及びこのコマンドで送られてきた認証関連データを基に認証結果を計算する。

このコマンドを実行するためには、ＩＣカードから送られてきた最新の種が有効でなければならない。

参照データの使用回数を制限するために、認証の不成功をＩＣカード内に記録しても良い。

サポート機能

- 与えられる情報なし
- 共通な参照データ（例えばカードパスワード）

- 固有の参照データ（例えばＤＦ固有のパスワード）
- 参照データ番号指定による比較

（１５）ＧＥＴ　ＣＨＡＬＬＥＮＧＥ

セキュリティ関連処理（例えばEXTERNAL AUTHENTICATEコマンド）で使用する種（例えば乱数）の発行を要求するために使用する。

種は、少なくとも次に送信されるコマンドで有効とする。その他の条件については、この規格では規定しない。

（１６）ＭＡＮＡＧＥ　ＣＨＡＮＮＥＬ

論理チャネルの設定及び解放を行うために使用する。

（１７）ＧＥＴ　ＲＥＳＰＯＮＳＥ

使用する伝送プロトコル上の制約によって、ＩＣカードが接続装置に対してＡＰＤＵ又はＡＰＤＵの一部を伝送することができない場合に使用する。

（１８）ＥＮＶＥＬＯＰＥ

使用する伝送プロトコル上の制約によって、ＡＰＤＵ、ＡＰＤＵの一部又はデータ列を伝送することができない場合に使用する。

ＩＳＯ９９９２－２　（金融取引用ＩＣカード）

（１）規定なし。

（２）規定なし。

（３）規定なし。

（４）規定なし。

（５）ＲＥＡＤ　ＲＥＣＯＲＤ（Ｓ）

順編成構造又は循環順編成構造のＥＦ内の特定のレコード（またはレコードの最初の部分）を読み出すために使用する。

セキュリティステータスが、ＥＦに定義づけられた読み出し機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

もし、レコード構造以外のＥＦを対象に実行された場合には、処理を中断すべきである。

サポート機能

- レコード番号して単一レコード読み出し
- 短縮ＥＦ識別子指定可能

（6）規定なし。

（7）ＡＰＰＥＮＤ　ＲＥＣＯＲＤ

順編成構造のＥＦの最終位置にレコードを追記する、又は循環順編成構造のＥＦにレコード番号１のレコードを書き込むために使用する。

セキュリティステータスが、ＥＦに定義づけられた追記機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

コマンドの実行は順編成構造又は、循環順編成構造のＥＦに限る。

サポート機能

- １レコード追記書き込み
- 短縮ＥＦ識別子指定可能

（8）ＵＰＤＡＴＥ　ＲＥＣＯＲＤ

コマンドメッセージの所定のビットで指定された順編成レコードを更新するために使用する。

セキュリティステータスが、ＥＦに定義づけられた書き換え機能に対するセキュリティ属性を満足しているときに限り、実行可能である。

サポート機能

- レコード番号指定書き換え
- 最初のレコード書き換え
- 最後のレコード書き換え
- 次のレコード書き換え
- 前のレコード書き換え
- 短縮ＥＦ識別子指定可能

（9）ＧＥＴ　ＤＡＴＡ

応用システムの環境に応じて、一つ以上のデータ対象を取り出すために使用する。

例えば、取り出されるデータは、PIN 試行カウンタ、取引カウンタのような、ＩＣカード内で動的に管理されるデータ対象である。

セキュリティステータスが、アプリケーションによって定義されたセキュリティ状態を満たしていれば、実行可能である。

サポート機能

- １バイトの BER-TLV タグ指定
- ２バイトの BER-TLV タグ指定
- １バイトの簡易符号化 TLV タグ指定
- データ部で示された BER-TLV タグリスト指定
- 私的利用指定

（１０）規定なし。

（１１）ＳＥＬＥＣＴ　ＦＩＬＥ

論理チャネルに対して一時的指定ファイルを設定するために使用する。

サポート機能

- ＤＦ名によるＤＦの選択
- ＤＦ識別子による子ＤＦの選択
- 親ＤＦの選択

（１２）ＶＥＲＩＦＹ

接続装置から送られた照合データと、ＩＣカード内に格納されている参照データ（例えばパスワード）とを、ＩＣカード内で比較するために使用する。

セキュリティステータスを比較の結果によって変更すべきである。

比較不一致をＩＣカード内に記録すべきである。

サポート機能

- 与えられる情報なし
- 共通な参照データ（例えばカードパスワード）
- 固有の参照データ（例えばＤＦ固有のパスワード）
- 参照データ番号指定による比較

（１３）ＩＮＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

外部から種となる情報（例えば乱数）を与えて、ＩＣカード内の機密情報（例えば鍵）から認証コードの計算を開始させるために使用する。

機密情報がＭＦに付随している場合、このコマンドはＩＣカード全体の認証に使用しても良い。

機密情報がＤＦに付随している場合、このコマンドはそのＤＦの認証に使用しても良い。

このコマンドの実行の可否は、先行のコマンド（例えば VERIFY コマンド、SELECT FILE コマンド）又は、機密情報選択の実行結果に依存しても良い。

このコマンドはアルゴリズムが既に選択されていれば、そのアルゴリズムを使用しても良い。

機密情報又はアルゴリズムの使用回数を制限するために、このコマンドの発行回数をＩＣカード内に格納しても良い。

アルゴリズム参照子は、コマンドが発行される前に既知となっているか、又はデータフィールド内に指定されているべきである。

サポート機能

- 与えられる情報なし
- 共通な参照データ（例えばカードパスワード）
- 固有の参照データ（例えばＤＦ固有のパスワード）
- 参照データ番号指定による比較

（１４）ＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

ＩＣカードに認証結果を計算させ、それに応じてセキュリティステータスを更新させるために使用する。

ＩＣカードは、例えば先行するGET CHALLENGコマンドに対して発行した種、ＩＣカード内に機密情報として格納されている鍵、及びこのコマンドで送られてきた認証関連データを基に認証結果を計算する。

このコマンドを実行するためには、ＩＣカードから送られてきた最新の種が、有効でなければならない。

参照データの使用回数を制限するために、認証の不成功をＩＣカード内に記録しても良い。

アルゴリズム参照子は、コマンドが発行される前に既知となっているか、又はデータフィールド内に指定されているべきである。

サポート機能

- 与えられる情報なし
- 共通な参照データ（例えばカードパスワード）
- 固有の参照データ（例えばＤＦ固有のパスワード）
- 参照データ番号指定による比較

（１５）ＧＥＴ　ＣＨＡＬＬＥＮＧＥ

セキュリティ関連処理（例えばEXTERNAL AUTHENTICATEコマンド）で使用する種（例えば乱数）の発行を要求するために使用する。

種は、少なくとも次に送信されるコマンドで有効とする。その他の条件については、この規格では規定しない。

（１６）規定なし。

（１７）ＧＥＴ　ＲＥＳＰＯＮＳＥ

使用する伝送プロトコル上の制約によって、ＩＣカードが接続装置に対してＡＰＤＵ又はＡＰＤＵの一部を伝送することができない場合に使用する。

（１８）規定なし

（１９）ＤＥＡＣＴＩＶＡＴＥ　ＦＩＬＥ

ＣＤＦまたはＡＤＦに対するアクセスを、一時的に不可能な状態（閉塞状態）にするために使用される。

事前にEXTERNAL AUTHENTICATEコマンドが成功することを要求しても良い。

（２０）ＧＥＮＥＲＡＴＥ　ＴＣＣ

カード発行者またはサービス提供者が、取引情報の真正性および発信源、ならびに取引が完了したことを確認する目的で、ＩＣカードに取引暗号化コード（ＴＣＣ）を生成させるために使用する。

レスポンスは、ＴＣＣ情報データ、アプリケーション取引カウンタ、ＴＣＣ、および発行者アプリケーションデータ（オプション）を含まなければならない。

ＴＣＣは次のいずれかである

- 取引証明
- 取引否認コード
- オンライン承認コード
- 照会コード

（２１）ＧＥＴ　ＰＲＯＣＥＳＳＩＮＧ　ＯＰＴＩＯＮＳ

アプリケーションに固有のデータのリストの位置を表示する情報を得るために使用する。

ＪＩＳ Ｘ６３０６

（１）原国際規格のために留保されている。

（２）原国際規格のために留保されている。

（３）原国際規格のために留保されている。

（４）原国際規格のために留保されている。

（５）ＲＥＡＤ　ＲＥＣＯＲＤ（Ｓ）

ＥＦ内の特定のレコードの内容を読み出すために使用する。

セキュリティステータスが、ＥＦのセキュリティ属性を満たす場合にだけ実行可能である。

サポート機能

- レコード番号指定、単一レコード読み出し
- 短縮ＥＦ識別子指定可能

（６）原国際規格のために留保されている。

（７）ＡＰＰＥＮＤ　ＲＥＣＯＲＤ

順編成構造のＥＦの最終位置にレコードを追記する、又は循環順編成構造のＥＦにレコード番号１のレコードを書き込むために使用する。

セキュリティステータスが、ＥＦのセキュリティ属性を満たす場合にだけ実行可能である。

サポート機能

- １レコード書き込み
- 短縮ＥＦ識別子指定可能

（８）ＵＰＤＡＴＥ　ＲＥＣＯＲＤ

コマンドメッセージの所定のビットで指定されたレコードを更新するために使用する。

セキュリティステータスが、ＥＦのセキュリティ属性を満たす場合にだけ実行可能である。

サポート機能

- レコード番号指定、１レコード更新
- 短縮ＥＦ識別子指定可能

（９）原国際規格のために留保されている。

（１０）原国際規格のために留保されている。

（１１）ＳＥＬＥＣＴ　ＦＩＬＥ

論理チャネルに対して一時的指定ファイルを設定するために使用する。

サポート機能

- ＤＦ名によるＤＦの選択

（１２）ＶＥＲＩＦＹ

接続装置から送られた照合データと、ＩＣカード内に格納されている参照データ（例えばパスワード）とを、ＩＣカード内で比較するために使用する。

セキュリティステータスを比較の結果によって変更しても良い。

比較不一致をＩＣカード内に記録しても良い。（例えば参照データの使用に対する再試行の回数を制限するため）

サポート機能

- 参照データ番号指定による比較

（参照データ番号とはパスワードの番号又は短縮ＥＦ識別子をいう）

（１３）ＩＮＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

外部から種となる情報（例えば乱数）を与えて、ＩＣカード内の機密情報（例えば鍵）から認証コードの計算を開始させるために使用する。

機密情報がＭＦに付随している場合、このコマンドはＩＣカード全体の認証に使用しても良い。

機密情報がＤＦに付随している場合、このコマンドはそのＤＦの認証に使用しても良い。このコマンドの実行の可否は、先行のコマンド（例えばVERIFYコマンド、SELECT FILEコマンド）又は、機密情報選択の実行結果に依存しても良い。

このコマンドはアルゴリズムが既に選択されていれば、そのアルゴリズムを使用しても良い。

機密情報又はアルゴリズムの使用回数を制限するために、このコマンドの発行回数をＩＣカード内に格納しても良い。

サポート機能

- 機密情報の番号指定による比較

（機密情報の番号とは鍵の番号又は短縮ＥＦ識別子をいう）

（１４）ＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

ＩＣカードに認証結果を計算させ、それに応じてセキュリティステータスを更新させる。ＩＣカードは、例えば先行するGET CHALLENGコマンド

に対して発行した種、ＩＣカード内に機密情報として格納されている鍵、及びこのコマンドで送られてきた認証関連データを基に認証結果を計算するために使用する。

このコマンドを実行するためには、ＩＣカードから送られてきた最新の種が、有効でなければならない。

参照データの使用回数を制限するために、認証の不成功をＩＣカード内に記録しても良い。

サポート機能

- 機密情報の番号指定による比較

（機密情報の番号とは鍵の番号又は短縮ＥＦ識別子をいう）

（１５）ＧＥＴ　ＣＨＡＬＬＥＮＧＥ

セキュリティ関連処理（例えばEXTERNAL AUTHENTICATEコマンド）で使用する種の発行を要求する。

種は、少なくとも次に送信されるコマンドで有効とする。その他の条件については、この規格では規定しない。

（１６）原国際規格のために留保されている。

（１７）原国際規格のために留保されている。

（１８）原国際規格のために留保されている。

全銀協ＩＣカード標準仕様

（１）規定なし。

（２）規定なし。

（３）規定なし。

（４）規定なし。

（５）ＲＥＡＤ　ＲＥＣＯＲＤ（Ｓ）

ＥＦ内の特定レコードの内容を読み出すために使用する。

セキュリティステータスが、アクセス対象ＷＥＦに関するセキュリティ属性を満足する場合にのみ、実行可能。

サポート機能

- レコード番号指定、単一レコード読み出し
- 短縮ＥＦ識別子指定可能

（6）規定なし。

（7）ＡＰＰＥＮＤ　ＲＥＣＯＲＤ

順編成構造のＥＦの最終位置にレコードを追記する、又は循環順編成構造のＥＦにレコード番号１のレコードを書き込むために使用する。

セキュリティステータスが、ＥＦのセキュリティ属性を満たす場合にだけ実行可能である。

サポート機能

- １レコード書き込み
- 短縮ＥＦ識別子指定可能

（8）ＵＰＤＡＴＥ　ＲＥＣＯＲＤ

コマンドメッセージの所定のビットで指定されたレコードを更新するために使用する。

セキュリティステータスが、ＥＦのセキュリティ属性を満たす場合にだけ実行可能である。

サポート機能

- レコード番号指定、１レコード更新
- 短縮ＥＦ識別子指定可能

（9）ＧＥＴ　ＤＡＴＡ

応用システムの環境に応じて、ＩＣカード内で動的に管理されるデータオブジェクトを取り出すために使用する。

セキュリティステータスが、アクセス対象のデータオブジェクトに対して付与されているセキュリティ属性を満足する場合にのみ実行可能。

サポート機能

- １バイトの BER-TLV タグ指定

- ２バイトのBER-TLVタグ指定
- 私的利用指定

（１０）規定なし。

（１１）ＳＥＬＥＣＴ　ＦＩＬＥ

論理チャネルに対して一時的指定ファイルを設定するために使用する。

サポート機能

- ＤＦ名によるＤＦの選択
- ＥＦ識別子によるＥＦの選択

（１２）ＶＥＲＩＦＹ

接続装置から送られた照合データと、ＩＣカード内に格納されている参照データ（例えばPIN）とを、ＩＣカード内で比較するために使用する。

セキュリティステータスを比較の結果によって変更しても良い。

比較不一致をＩＣカード内に記録しなければならなく、照合不一致回数は照合一致時にクリアする。

サポート機能

- カレントＥＦ指定
- 短縮ＥＦ識別子使用可能

（１３）ＩＮＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

外部から種となる情報（例えば乱数）を与えて、ＩＣカード内の機密情報から認証コードの計算し、出力させるために使用する。

サポート機能

- カレントＥＦ指定
- 短縮ＥＦ識別子使用可能

（１４）ＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

先行する GET CHALLENGE コマンドによってカードから出力されたチャレンジ、ＩＣカード内に機密情報として格納されているキーを使用して、外部から送られてくる認証関連データの認証を行い、その結果を出力するために使用する。

結果に応じてセキュリティステータスが更新される。

参照データの使用回数を制限するために、認証の不成功をＩＣカード内に記録しても良い。

サポート機能

- カレントＥＦ指定
- 短縮ＥＦ識別子使用可能

（１５）ＧＥＴ　ＣＨＡＬＬＥＮＧＥ

セキュリティ関連処理（例えば EXTERNAL AUTHENTICATE コマンド）で使用するチャレンジの発行を要求するために使用する。

チャレンジは、少なくとも次に本コマンドが実行されるまで有効である。または、カードが電気的に非活性化されるとクリアされる。

（１６）規定なし。

（１７）規定なし。

（１８）規定なし。

（１９）ＤＥＡＣＴＩＶＡＴＥ　ＦＩＬＥ

ＭＦまたはＤＦに対するアクセスを、一時的に不可能な状態（閉塞状態）にするために使用する。

なお、ＭＦを閉塞した場合、ＭＦ配下のＤＦは、その時点では閉塞状態とはならない。従って、ＤＦを閉塞したい場合には、当該ＤＦをカレント状態とした後に閉塞させる。

セキュリティステータスが、アクセス対象ＭＦ／ＤＦに関するセキュリティ属性を満足する場合にのみ、コマンドを実行することができる。

本コマンド実行後も、セキュリティステータスは保持される。

（２０）ＧＥＮＥＲＡＴＥ　ＴＣＣ

カード発行者またはサービス提供者が、取引情報の真正性および発信源、ならびに取引が完了したことを確認する目的で、ＩＣカードに取引暗

号化コード（ＴＣＣ）を生成させるために使用する。

レスポンスは、ＴＣＣ情報データ、アプリケーション取引カウンタ、ＴＣＣ、および発行者アプリケーションデータ（オプション）を含まなければならない。

ＴＣＣは次のいずれかである

- 取引証明
- 取引否認コード
- オンライン承認コード
- 照会コード

（２１）ＧＥＴ　ＰＲＯＣＥＳＳＩＮＧ　ＯＰＴＩＯＮＳ

アプリケーションに固有のデータのリストの位置を表示する情報を得るために使用する。

（２２）ＲＥＡＣＴＩＶＡＴＥ　ＦＩＬＥ

一時的にアクセス不可能状態（閉塞状態）となっている、ＭＦまたはＤＦに対するアクセスを、可能状態（閉塞解除）にするために使用する。

なお、ＭＦを閉塞解除した場合、ＭＦ配下のＤＦは、その時点では閉塞解除状態とはならない。

セキュリティステータスが、アクセス対象ＭＦ／ＤＦに関するセキュリティ属性を満足する場合にのみ、コマンドを実行することができる。

本コマンド実行後も、セキュリティステータスは保持される。

（２３）ＵＮＢＬＯＣＫ　ＫＥＹ

参照データ（例えばPIN）の閉塞解除に使用する。

セキュリティステータスが、アクセス対象ＩＥＦのセキュリティ属性を満足する場合にのみ、コマンドを実行することができる。

サポート機能

- カレントＥＦ指定
- 短縮ＥＦ識別子使用可能

（２４）ＣＨＡＮＧＥ　ＫＥＹ

参照データ（例えばPIN）の更新に使用する。

セキュリティステータスが、アクセス対象ＩＥＦのセキュリティ属性を満足する場合にのみ、コマンドを実行することができる。

サポート機能

- カレントＥＦ指定
- 短縮ＥＦ識別子使用可能

EMV仕様

（１）規定なし。

（２）規定なし。

（３）規定なし。

（４）規定なし。

（５）ＲＥＡＤ　ＲＥＣＯＲＤ

アプリケーションファイルが選択された後に、順編成構造ファイルからレコード番号を指定してレコードデータを読み出すために使用する。

サポート機能

- レコード番号して単一レコード読み出し。
- 短縮ＥＦ識別子指定可能。

（６）規定なし

（７）規定なし

（８）規定なし

（９）ＧＥＴ　ＤＡＴＡ

現行アプリケーションのレコード内にカプセル化されていない原始データオブジェクトを検索するために使用する。

アプリケーション取引カウンター、最終オンライン ATC レジスタ、PIN 試行カウンタの３種の原始データオブジェクトの検索だけに限定される。

サポート機能

- ２バイトの BER-TLV タグ指定

（１０）規定なし。

（１１）ＳＥＬＥＣＴ

提示されたファイル名又は、AID に対応する ICC PSE（決済システム環境）、DDF（ディレクトリ定義ファイル）、又は ADF（アプリケーション定義ファイル）を選択するために使用する。

コマンドの実行が成功すると、PSE、DDF、または ADF へのパスが設定される。

後続のコマンドは、SFI（短縮ファイル識別子）を使って、選択した PSE、DDF、または ADF に関連する AEF に対して適用される。

サポート機能

- 名前による選択
- ＦＣＩの返信

（１２）ＶＥＲＩＦＹ

コマンドのデータフィールドで送信された取引 PIN データを、そのアプリケーションに関連した参照 PIN データと比較するために使用する。

比較の実行方法は、アプリケーション独自である。

どのように参照 PIN データを見つけるかは、コマンドが発行される前に既知となっているべきである。

（１３）ＩＮＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

外部から送信されたチャレンジデータやＩＣカード内に格納されたデータや、関連秘密鍵を使った、ＩＣカードによる署名済み動的アプリケーションデータの演算を起動するために使用する。

アルゴリズム参照子は、コマンドが発行される前に既知となっているか、又はデータフィールド内に指定されているべきである。

（１４）ＥＸＴＥＲＮＡＬ　ＡＵＴＨＥＮＴＩＣＡＴＥ

ＩＣカード内のアプリケーションに、暗号文を検証するように要求するために使用する。

アルゴリズム参照子は、コマンドが発行される前に既知となっているか、又はデータフィールド内に指定されているべきである。

検証の仕組みは外部から暗号文が送られてくる。その暗号文とＩＣカードの内部で正しい相手と同じ暗号方式、鍵で作った暗号文を比べて同じであれば正当な取引相手、異なれば正当な取引相手ではないことを確認する。

（１５）規定なし。

（１６）規定なし。

（１７）ＧＥＴ　ＲＥＳＰＯＮＳＥ

使用する伝送プロトコル上の制約によって、ＩＣカードが接続装置に対してＡＰＤＵ又はＡＰＤＵの一部を伝送することができない場合に使用する。

（１８）規定なし。

（１９）ＡＰＰＬＩＣＡＴＩＯＮ　ＢＬＯＣＫ

アプリーケーションで選択されているファイルを無効にするために使用する。

コマンドメッセージのデータフィールドは、セキュアメッセージングに従って符号かされたMACデータコンポーネントが含まれる。

（２０）ＧＥＮＥＲＡＴＥ　ＡＰＰＬＩＣＡＴＩＯＮ　ＣＲＹＰＴＯＧＲＡＭ

取引に関するデータをＩＣカードに送信し、ＩＣカードアプリケーション暗号文を生成するために使用される。

この暗号データは、EMV仕様で指定されるアプリケーションクリプトグラムか、独自の暗号データでなければならない。

レスポンスは、暗号情報データ、アプリケーション取引カウンタ、アプリケーション暗号、および発行者アプリケーションデータ（オプション）を含まなければならない。

参照制御パラメータはは次のいずれかである

- 取引証明
- 許可要求暗号

- アプリケーション許可照会
- アプリケーション認証暗号

（２１）ＧＥＴ　ＰＲＯＣＥＳＳＩＮＧ　ＯＰＴＩＯＮＳ

ＩＣカード内で取引を起動するために使用される。

レスポンスとして、アプリケーション交換プロファイル(AIP)、およびアプリケーションファイルロケータ(AFL)が返送される。

（２２）ＡＰＰＬＩＣＡＴＩＯＮ　ＵＮＢＬＯＣＫ

現在選択されたファイルを回復するために使用する。

コマンドメッセージのデータフィールドは、セキュアメッセージングに従って符号かされたMACデータコンポーネントが含まれる。

（２３）ＰＩＮ　ＣＨＡＮＧＥ／ＵＮＢＬＯＣＫ

PINを閉塞解除するか、またはPINの変更と閉塞解除を同時に行うために使用する。

コマンドが成功すると、PIN試行カウンタの値をPIN試行制限の値にリセットされなければならない。

コマンドが成功すると、要求があった場合、参照PINの値を新しいPINの値に変更しなければならない。

コマンドで送信されるPINデータがある場合、機密保護のためにデータを暗号化しなければならない。

（２４）ＰＩＮ　ＣＨＡＮＧＥ／ＵＮＢＬＯＣＫ

PINを閉塞解除するか、またはPINの変更と閉塞解除を同時に行うために使用する。

コマンドが成功すると、PIN試行カウンタの値をPIN試行制限の値にリセットされなければならない。

コマンドが成功すると、要求があった場合、参照PINの値を新しいPINの値に変更しなければならない。

コマンドで送信されるPINデータがある場合、機密保護のためにデータを暗号化しなければならない。

（２５）ＣＡＲＤ　ＢＬＯＣＫ

ＩＣカード内の全てのアプリケーションを永久に無効にするために使用する。

コマンドメッセージのデータフィールドは、セキュアメッセージングに従って符号かされたMACデータコンポーネントが含まれる。

2.1.6 ＥＣにおけるＩＣカードの利用形態

インターネットの急速な発達などにより、様々なビジネスをこの上で展開していこうとする電子商取引（エレクトリック・コマース）実現への動きが活発になっている。このインターネットを利用した電子商取引では、必ずしも従来のような物品の販売に限ったものではなく、画像、音楽、文字、ソフトウェア等のデジタル情報を、注文と同時に回線を通じて直接転送することによって、販売店が何の在庫も持たずに販売したり、インターネットを介したさまざまなサービスに応じて課金を行うなどという、従来の通信販売では考えられなかったことも可能となる。

当然の事ながら、このようなビジネスをスムーズに普及させていくためには、同様にインターネットの上で行える安全な決済手段が必要不可欠である。

従来の取引形態においては、決済の最も身近で、かつ確実な手段は現金であり、その引き渡しによって決済が終了する。他にも、クレジットカード、手形・小切手、銀行口座振替・送金などの手段も存在するが、これらは、当事者間の決済が一応終了した後も、これらの決済手段を顧客に提供した金融機関等には、顧客間の決済により他の金融機関との間に生じた債権債務関係を清算する必要が残り、他の金融機関や中央銀行の口座の振替等によってこの金融機関間決済が行われる。このように、決済には様々なものがある。

しかしながら、これらの決済手段はインターネット上の取引で使うにはあまり便利とはいえない。そこで考えられるのがいわゆる電子決済である。電子決済とは、広義には前述の決済のうち、コンピュータを使用した情報処理等により、実際には紙幣等のモノの移動を伴わずに資金を移動し、決済を行うことと考えることが出来る。もちろん、これ自体は決して新しい概念ではなく、むしろ電子決済が主流となっているものもたくさんある。例えば、銀行間の為替送金を実現する全国銀行データ通信システム（1973 年 4 月開始）や、日銀における銀行間の当座預金振替等に用いられる日本銀行金融ネットワークシステム（1988 年 10 月開始）を使った決済などは電子決済の一種といえる。

しかしながら、それらの多くは銀行対銀行等の大口の決済手段であったり、個人が対象であっても事前に契約を結んでおいた定例的な支払い用途にしか使えなかったり、あるいは銀行にある ATM まで足を運ばないとサービスを受けられないなど、その決済に関わる当事者や用途が限られ、様々な制約を持った閉じた世界における決済方法であった。

これに対して現在求められているものは、利用者が IC カードを持ち歩いて店頭で支払い手段として使用したり、自宅にいながらパソコン経由で送金を行ったりと、従来に比べると自由度が格段に拡がった、日常的な支払い手段としても使える決済方法を指す。

具体的に考えられるものとしては、現金、小切手、クレジットカード等を電子的に代替する（あるいは利便性においてこれを上回る）決済方法のことであり、それぞれ電子現金、電子小切手、電子クレジットカードなどと呼ばれている。それぞれの特徴および利便性は、実現スキームによりかなりの差がみられるが、その概略は以下のとおりである。

2.1.6.1 電子決済の調査分類

(1) 電子クレジットカード

オープンなネットワークであるインターネットにおいて、クレジットカードを安全に使用するために特別な工夫を施したもの。

取引当事者の正当性を保証する仕組みにより、取引の安全性を高めると共に、クレジットカード番号や取引情報を暗号化することなどによって、情報の盗聴、改竄を防止している。決済そのものについては、既存のクレジットカードのスキームをそのまま使っているほか、利用者も手元のパソコンに専用のソフトウェアを導入するだけで利用でき、特別な機器を設置する必要が無いことから、最も実用化が進んでいる。例えば、First Virtual や CyberCash が既に実用化されている他、クレジットカードの二大国際ブランドである VISA と Master Card が制定した SET（Secure Electronic Transaction）プロトコルを取り入れたプロジェクトが多数持ち上がっている。

(2) 電子小切手

インターネット上において、あらかじめ銀行から、銀行のデジタル署名のついたメッセージを交付してもらっておき、商品を購入する際に、そのメッセージあるいはそのメッセージに利用者のデジタル署名を加えたものを、あたかも小切手を切るように小売店に送付することにより支払いを行うもの。

なお、代金は最終的に銀行口座振替により決済される。

(3) 電子現金

受け渡される情報そのものが価値を表章しているとのコンセプトで設計された決済手段。後からこれを使用した当事者の口座の振替等の事後処理が不要で、受け渡しにより支払いが完了するような決済手段と考えることができる。ストアード・バリュー・カードなども、これに分類されると考えられる。これに加えて、匿名性や転々流通性など、現金が持つ特徴の多くを実現するものと説明されることも多い。

(4) オンライン・バンキング

一般の個人を対象とした電子的資金振替サービスのことで、債権債務の決済を、現金や小切手等を利用せず、コンピュータに接続されたパソコン等の操作によって完結するシステム。Quicken 等の PC 用ソフトウェアを使用したシステムでは、単なる資金振替に止まらず、家計簿の代用としてその入出金を事由と共に管理することも可能なことも特徴である。

オンラインバンキングの代表的なものとしては、1995 年 10 月に米国で営業を開始した Security First Network Bank (SFNB)が有名である。この SFNB は実際の店舗としては米国ケンタッキー州に一店を持つのみで、ネットワーク上では 365 日 24 時間体制で営業を行っている。対象業務は ATM による入出金、残高照会、手形・小切手の支払い、給振り等の入出金指図などであり、預金周りの業務については通常の銀行とほぼ同様の処理が行えるほか、特定の手形・小切手の決済状況のチェックや、顧客の手元における残高計算と実際の入出金状況の照合も行えるよう機能強化が図られている。物理的な現金の出し入れを業界の専用ネットワークに接続されている ATM で行う以外、他の全ての指図は、顧客のインターネット端末で行うことが可能である。

2.1.6.2 電子マネーの価値保有形態による分類

電子マネーを保有する価値について形態別に分類すると下記のようになる。

- アクセス型
  - クレジットカード型
  - 小切手型
  - オンラインバンキング
- ストアードバリュー型
  - 電子現金

電子現金の媒体による分類

- IC カード型
- ネットワーク型
- ハイブリッド型（IC カード＋ネットワーク）

電子現金の価値記録方式による分類

- 残高管理型
- 電子紙幣型

電子キャッシュの転々流通性有無による分類

- オープンループ型
- クローズドループ型

2.2 端末

ＩＣカードを早期にかつ広く普及させるためには、相互運用性の高い端末インフラを構築する事が必須である。

現在約５０万台設置されているクレジット端末については、設置済み端末へのＩＣカード機能の拡張、並びに新規端末について共通プラットフォーム／アプリケーション仕様要件について述べる。

またＩＣカード型電子マネーのマイクロ・ペイメント・システムのひとつのアプリケーションとして自販機端末について考え方を述べる。

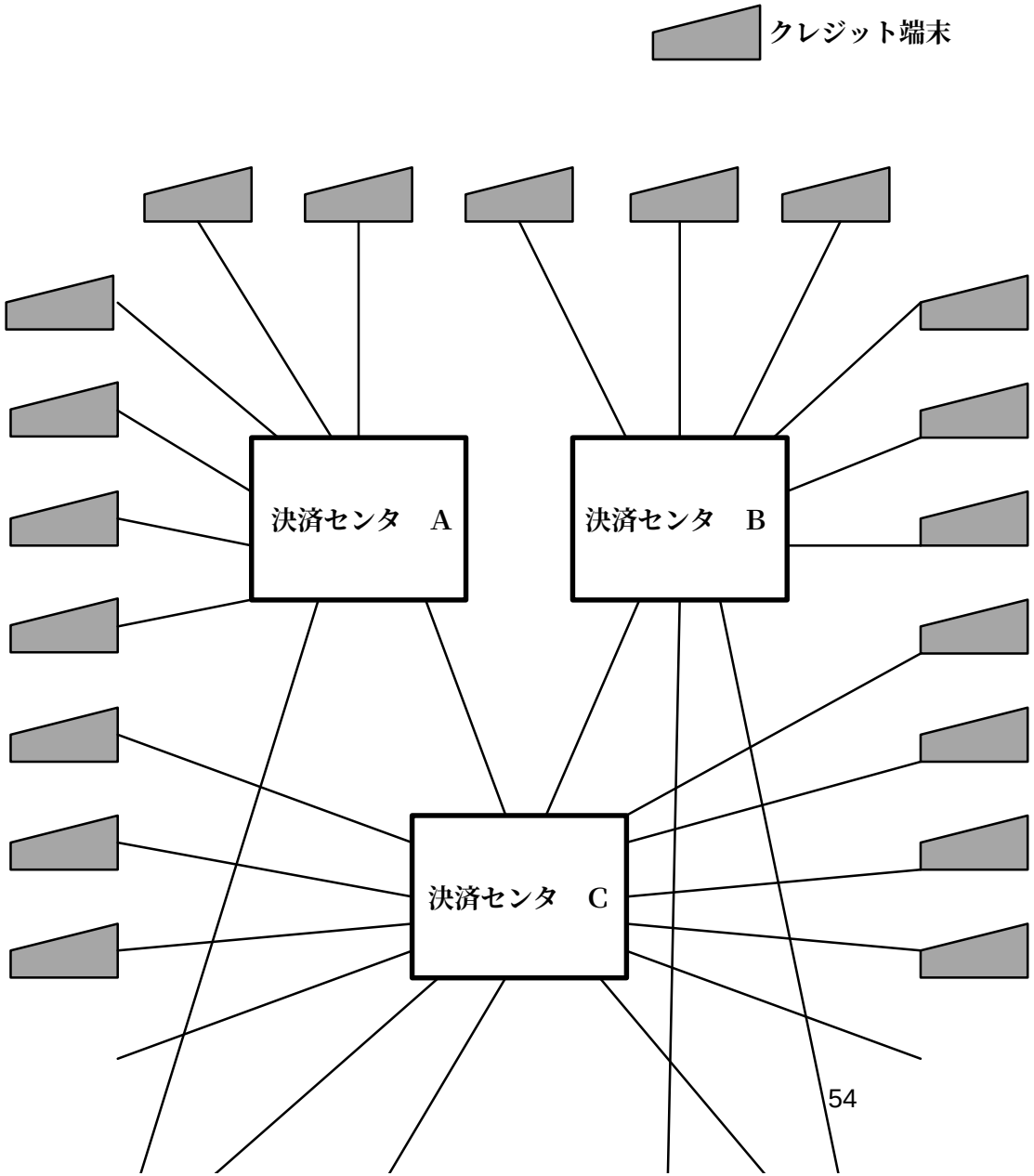
2.2.1　クレジット端末

2.2.1.1 クレジット端末の概要

クレジット端末は、クレジットカード会社と加盟店とを結んでいるクレジットカード決済用オンラインシステムで使用する端末である。クレジットカードの加盟店でのクレジットカードによる支払に際して、不正なカードが使用されたり、そのカードの利用限度額を超えて使用されることを防止するために、自動的にカード会社へオーソリを要求し、カード会社で不正カードの利用や利用限度額をチェックするシステムである。クレジットカードのＩＣカード化を考えた場合、クレジット端末も従来のクレジット端末とは違った機能の必要性が予想される。本章では、このＩＣカード対応クレジット端末の仕様要件について述べている。

クレジットカードのＩＣカードの標準仕様として位置づけされつつあるのがＥＭＶ仕様である。そこで、今回の検討では、クレジット端末が扱うＩＣカードとしては、ＥＭＶ仕様に準拠したＩＣカードを前提としている。

図 2-3に、クレジットカード決済オンラインシステムのシステム構成例を示す。


クレジット端末
決済センタ　A
決済センタ　B
決済センタ　C

カード会社　　カード会社　　・・・　　カード会社　　カード会社

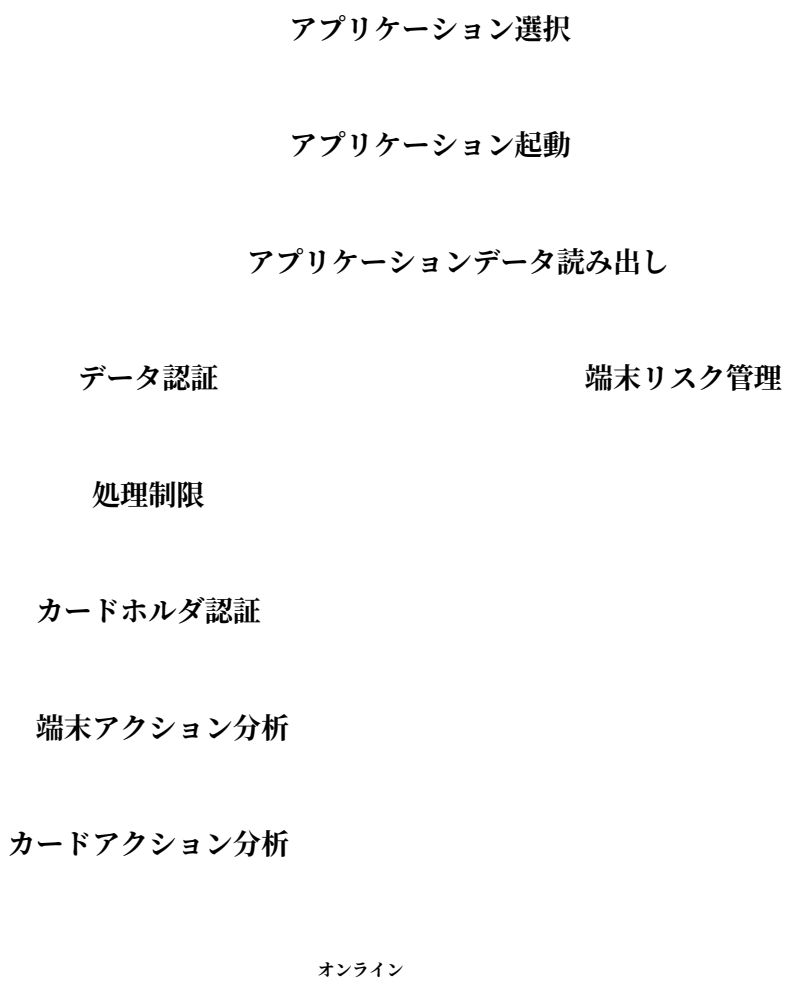
A　　B　　Y　　Z

図 2-3　クレジットカード決済オンラインシステムの構成例

2.2.1.2 ＥＭＶの処理概要

(1) アプリケーションフロー例

クレジット端末の仕様要件に先立ち、検討の前提であるＥＭＶ仕様のアプリケーションの処理概要について、簡単に述べる。図 2-4は、ＥＭＶのアプリケーションフロー例である。



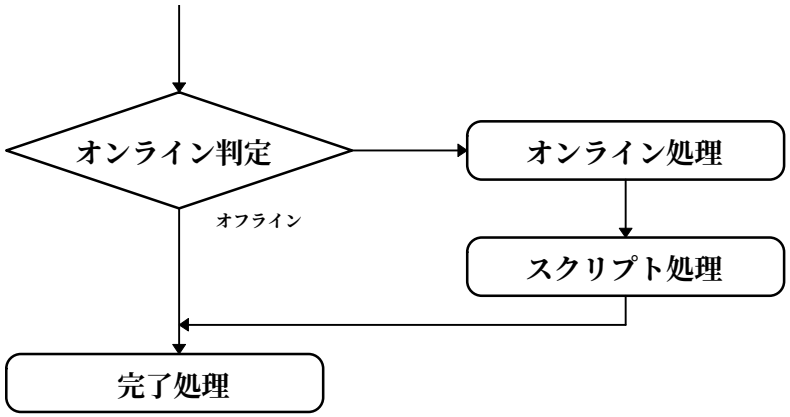


図 2-4 EMVアプリケーションフロー例

(2) データエレメント

表 2-4は、EMV仕様で定義しているデータエレメントで、ＩＣカードとクレジット端末がそれぞれどのような関連情報を保持するかを整理したものである。

表 2-4 ＩＣカードとクレジット端末で保持するデータ

ＩＣカード	クレジット端末
アプリケーション情報	アプリケーション情報
発行者情報	カード会社情報
	加盟店情報
カード管理情報	端末管理情報
ファイル管理情報	
認証データ	認証用パラメータ
磁気ストライプ情報	
取引管理情報	取引管理情報
	取引データ

2.2.1.3 クレジット端末への課題

ここまでは、ＩＣカードに対応するクレジットカード端末に必要な仕様を検討するにあたり、その前提と今回の検討のベースとなるEMV仕様の処理概要について述べてきた。次に本題であるクレジット端末の仕様要件に入る前に、実際にこれらの端末を操作する加盟店の店舗から見たクレジット端末の課題を整理してみる。

(1) 安価な小型端末

本来は、ＩＣカードと磁気カードを利用できる一体型で小型のクレジット端末が安価に提供されることが望ましいが、現在整備されつつある端末インフラを有効活用するためには、当初は既設のクレジット端末に外付けでＩＣカードリーダを付加する形式になるであろう。その場合は、容易に既設端末へ接続でき、端末とＩＣリーダライタが分離されることで場所をとることのないようにする必要がある。また、将来的に一体型の端末に置き換わることも考慮しておく必要がある。

(2) 簡単な操作

近年店舗の売場ではパート・アルバイトの比率が年々高くなっており、ＩＣカード対応のクレジット端末でも操作上現行のクレジット端末との相違があると、売場での対応が難しく、スピード化も望めない。また、カードの種別（提携カード、カード会社等）によって、別々の端末を操作しなければならないことは、売場での対応をさらに難しくし、ＩＣカードの普及促進自体を妨げることにつながる。オペレータがカードの種別を意識せず、従来のクレジット端末と同様に簡単な操作の端末を実現する必要がある。

(3) ＰＯＳレジとの連動

大型店舗、チェーン店、ショッピングセンター等では、ＰＯＳレジによりデータ収集し店舗管理に活用する運用が進んでおり、操作のスピード化および金額の二度打ちによる入力ミスの防止には、ＰＯＳレジとクレジット端末の連動が必要である。また、店舗の形態によっては、ＰＯＳレジから離れた場所でクレジット端末を操作する必要があり、クレジット端末のコードレス化も必要である。

(4) 高速の伝票印字

現行のクレジット端末では、伝票の３枚または４枚の複写印字が必要なため、ドットプリンタを装備している。そのため、伝票の印字時間のクレジット端末の処理時間全体に占める割合は無視できないものである。クレジットカードのＩＣカード化によって決済に要する時間を短縮しようとしたとき、伝票印字の高速化も同時に必要になってくる。

2.2.1.4 クレジット端末の仕様要件

(1) ＩＣカード対応クレジット端末

クレジットカードのＩＣカード化に対応して、店舗でクレジットカードを利用するために必要なクレジット端末には、通常のクレジット端末（磁気カードベースのクレジット端末）とは異なるＩＣカード固有の機能が必要とされる。ここでは、このＩＣカード対応クレジット端末として、固有に必要な機能について述べる。

① 共通アプリケーションの実現

ＩＣカードに持たせるクレジットのアプリケーションは、EMV仕様に則っており、端末側でそのアプリケーションをサポートしていれば、各カード会社ごとに異なるアプリケーションというものも可能である。しかし、端末側から見たとき、各カード会社ごとのアプリケーションをサポートすることは、２０数種のカードが利用可能な店舗の存在の現実から、非常に困難であると言わざるを得ない。少なくとも、ひとつのクレジットシステムでのクレジットアプリケーションを共通にすることが必要である。

また、EMV仕様ではサポートされていない、ボーナス払い、分割払いおよび　　ボーナス併用払いといった国内固有のクレジット決済の方式も実現できなければ　　ならない。このような国内固有の取引についても、それらのサービスを提供して　　いるカード会社固有のアプリケーションとはせず、ひとつのクレジットシステム　　として共通のアプリケーションとすべきである。

② 暗号ロジックの搭載

EMV仕様では、端末とＩＣカード間のデータ認証には、公開鍵方式の暗号ロジックであるＲＳＡが採用されている。ＲＳＡをサポートしようとした場合、まずその処理速度が問題となる。ＲＳＡでの計算は、Ｐｅｎｔｉumプロセッサを使用しても 1〜2 秒要することから、カード端末に使用されるＣＰU能力では、数１０秒要することが予想できる。そのため、専用の暗号化プロセッサ等を別途搭載することが現実的なようである。

また、ＲＳＡのライセンスの問題がある。ＲＳＡのライセンスに要する費用が製品コストを引き上げ、端末の普及を鈍らせることにつながるおそれがある。クレジットシステムのサービスを提供する側で、一括してライセンスを取得し、プログラムまたは専用プロセッサを安価に（または無償で）提供することもひとつの対応策になるであろう。

③ ＰＩＮパッドの接続

ＩＣカードによりクレジット取引では、オフラインにより取引が発生する。その際のカードの持ち主の本人確認には、オフラインＰＩＮが利用

されるため、ＰＩＮ入力のためのＰＩＮパッドを装備する必要がある。ここで、端末のハードウェア構成として、ＰＩＮパッドとＩＣカード関連の処理を行うハードウェアが一体である場合は、入力されたＰＩＮ情報を暗号化する必要はないが、別個のハードウェアで構成する場合は、入力されたＰＩＮ情報を暗号化して転送する必要がある。ＥＭＶ仕様では、この暗号化ロジックとして、ＤＥＳを採用している。

また、ＰＩＮパッドとカード端末本体との接続は、利用場面によってはワイヤレスの場合も十分に考えられる。

④ 磁気カードとの併用運用

クレジットカードをＩＣカード化するといっても、当面は磁気ストライプをカード上に持つことになり、磁気カードのみのクレジットカードが市場からなくなるわけではない。そのため、カード端末はＩＣカードと磁気カードの両カードを扱えなければならない。その際、ＩＣカードと磁気カードをひとつのリーダユニットで読み取るか、別々のユニット読み取るかは、両カードを読み取れるリーダのコスト、取引操作上の使い勝手および利用場面によって、幾つかの端末形態を生んでいくことが考えられる。

⑤ タンパー・レジスタンス機能のサポート

クレジット端末は店頭で利用されるため、端末の盗難、悪意の利用者による操作等の不正から端末内のセキュリティ情報を守る必要がある。現行の多くのクレジット端末でもこのためのタンパー・レジスタンス機能を有しているが、さらにその機能の見直しおよび徹底実施を推し進めていかなければならない。

⑥ 拡張性を考慮したソフトウェア構造の実現

ＩＣカードのアプリケーションとして、通常のクレジット機能だけでなく、カード会社固有のサービスや店舗ごとのサービスが予想され、またそれらが可能であることがＩＣカード普及のための重要な要因でもある。そのために、端末のソフトウェア構造として、将来のアプリケーションの追加や改造に対して、容易に対応できる仕組みが必要である。

また、端末が追加・変更するこれらのアプリケーションを、サービス提供者が短期間で、容易に認定できる端末の仕組みも必要である。

ＥＭＶ仕様では、これらの対応できるソフトウェア構造として、ＡＰＩを利用した例とインタプリタを利用した例を示しているが、端末メーカとしても、保有している技術資産を活用しつつ、新たな端末の仕組みを作り出していく必要がある。

(2) 既設クレジット端末でのＩＣカード対応

現在、約50万台を超えるクレジット端末(ＣＡＴ、Ｇ－ＣＡＴ、ＳＧ－Ｔ等)が各加盟店に設置されており、これらの端末は磁気カードベースの端末である。この端末インフラを有効に、クレジットカードのＩＣカード化に活用するためには、前に述べた仕様要件とは別に、既設端末に対して次の改造が必要になってくる。

① ＩＣカードリーダの追加

ＩＣカードのデータを読み出すためのＩＣカードリーダを付加しなければならない。ＩＣカードリーダを付加するインタフェースは、Ｇ－ＣＡＴ以降の世代の端末では有しているが、ＣＡＴでは有していないため、Ｇ－ＣＡＴ以降の世代の端末がＩＣカード化の対象になるであろう。

② ＰＩＮパッドの追加

クレジットカードのＩＣカード化ではオフライン処理を実現できることが、ひと　つのメリットであり、そのオフライン処理のためにＰＩＮパッドを付加しなけれ　ばならない。ＰＩＮパッドを付加するためのインタフェースの余裕の有無、ＰＩＮ入力操作の方法、入力ＰＩＮの暗号化、および端末が占有する店舗カウンタ上の面積から、選出のＩＣカードリーダとの一体化がまず考えられる。

③ メモリの追加

ＩＣカード関連のアプリケーションプログラム、クレジットセンタとのＩＣカード取引インタフェース、オフライン取引結果のタンキング、およびオフライン取引の送信プロトコルを実現するためには、それらのプログラムやデータを格納するメモリが必要になる。しかし、このためのメモリ上の余裕のある既設端末は少なく、特に最も多く設置されているＧ－ＣＡＴはＲＯＭベースの端末でメモリの余裕のないものがほとんどである。また、予めメモリの追加のためのポートを用意している端末も少なく、既設端末へメモリを追加することは困難である。

そこで、端末の付加するＩＣカードリーダに追加するメモリを搭載し、ＩＣカ　ード関連の処理を分担することが考えられる。

④ 既存クレジットシステムの保持

磁気カードとの併用のためには、既存の磁気カードによるクレジットシステムを実現する機能は、そのまま保持していく必要がある。クレジットセンタとの取引インタフェースについては、磁気カードとＩＣカードのインタフェースを二重に(プログラムとしてではなく、機能として二重に)持つ必要がある。また、端末が印字する取引伝票も同様に、2種類の伝票の印字を実現する必要がある。

ここで述べてきたように、既設端末でＩＣカードを実現するためには、クレジットのＩＣカード関連のアプリケーションまで処理できるＰＩＮ

パッド付きのＩＣカードリーダを既設端末に付加することがひとつの方法であると考えられる。しかし、このようなＩＣカードリーダライタ自体の実現性を考えると、安価に実現できるかどうかは疑問である。

しかし、既設の端末インフラを有効に活用し、クレジットカードのＩＣカード化を促進するためには、端末本体への少ない改造とさらに安価なＩＣカードリーダを実現しなければならない。そこで、クレジットカードのＩＣカード化の利点である偽造への対策とオフライン処理の実現を考慮すると、機能を限定してもこの利点を活かすＩＣカード機能をまず実現し、ＩＣカードの普及を目指すことが重要ではないだろうか。以下に、限定したＩＣカード機能のアプリケーションフローとして、2 つの例を示す。

例１：　データ認証のみを実現した例

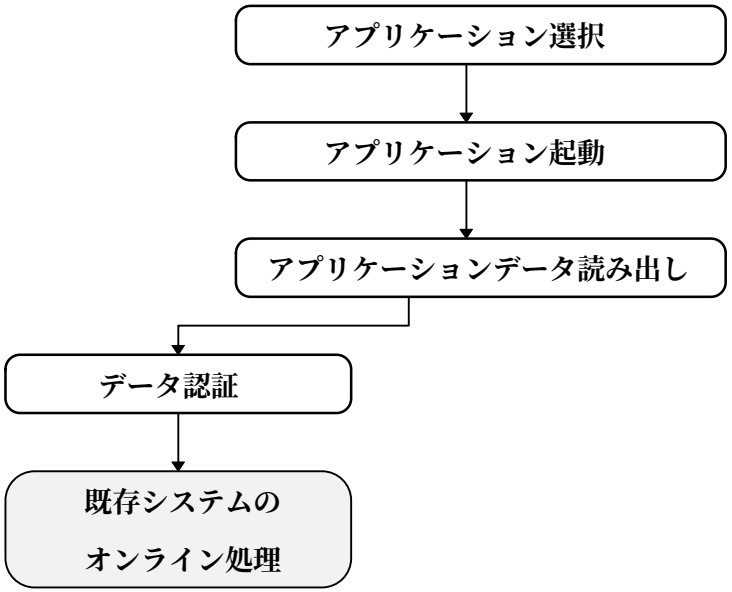


図 2-5　データ認証のみを実現した例

この場合、すべての取引がオンラインになってしまい、ＩＣカード化の重要なセールスポイントであるオフラインによるクレジット取引は実現できない。しかし、もうひとつのセールスポイントである偽造カードの利用に対する対応は可能になる。

例 2： 既存オンラインシステムを利用した例

アプリケーション選択

アプリケーション起動

アプリケーションデータ読み出し

データ認証　　端末リスク管理

処理制限

カードホルダ認証

端末アクション分析

カードアクション分析

オンライン

オンライン判定　　既存システムの

オフライン　　オンライン処理

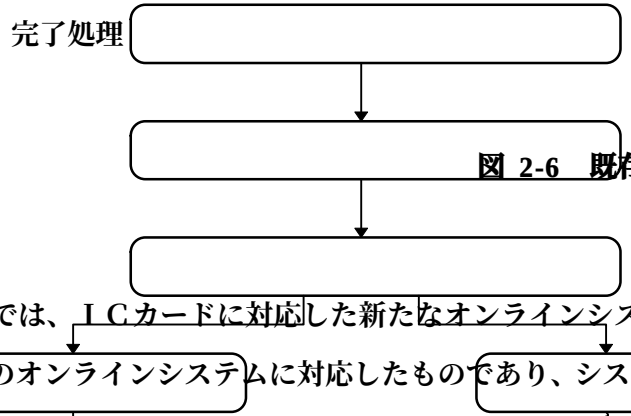


図 2-6　既存オンラインシステムを利用した例

この例では、ＩＣカードに対応した新たなオンラインシステムの整備を待たず、既存のオンラインシステムを利用している。既設の端末はそれぞれ既存のオンラインシステムに対応したものであり、システムとしての品質および運用に関しても実績があり、安定している。端末インフラだけでなく、ネットワークインフラも活用できる運用であると考えられる。

(3)　通信仕様

現行のクレジット端末のうち、幾つかの端末での通信仕様の一覧を表 2-5に示す。

表 2-5　既存クレジット端末の通信仕様

項番	項　　目	ＣＡＴ	Ｇ－ＣＡＴ	ＳＧ－Ｔ	ＪＥＴＳ
1	通信速度（ｂｐｓ）	１２００	１２００	２４００	２４００

2	通信プロトコル	CAT 手順	G-CAT 手順	VISAII 手順	HDLC
3	電文形式	独自形式	独自形式	独自形式	独自形式
4	暗号化の有無	なし	あり	なし	あり

既存のクレジット端末はすべて公衆回線に対応しているが、ＩＳＤＮ、ＰＨＳおよび携帯電話網の普及により、これらに対応した端末開発の動きが出てきている。クレジットカードのＩＣカード化でも、当初は既存の通信システムを利用することが予想されるが、普及をさらに促進していくためには、ＩＳＤＮ等への対応も同時に推進する必要がある。また、クレジット端末の共同利用を実現していくには、汎用プロトコルの採用も検討の対象とすべきである。

(4) クレジット端末の運用および保守

最後に、ＩＣカードに対応したクレジット端末の運用上、および保守上の課題について述べる。システム自体の運用および保守に関する課題は別に議論しており、ここでは端末に関するものに限っている。

① ＩＣカード読み取不能時の運用

入力されたＩＣカードが読み取れない場合、カード上の磁気ストライプを読み取ることによって、クレジット取引を実施することは可能である。端末としては、磁気ストライプ上の情報によって、ＩＣカード付きのカードかどうか判断できるため、幾つかの対応は可能である。ＩＣカード付きのカードであるとして取扱を拒否することもできるし、ＩＣカード付きのカードの磁気ストライプ情報によって取引を行ったという情報をセンタへ渡すこともできる。磁気ストライプ情報のコピーによる不正カードの利用、店舗での利用者の利便性等から、サービス提供者によって決められるものである。

② ＰＩＮの入力

オフラインでのクレジット決済は、低額の利用者に対して、高速の決済を提供するためのものである。現行のクレジット決済でも一部条件付きでサインレスを実施している店舗もあることから、オフラインでのクレジット決済に対してのＰＩＮ入力も運用面から議論されるべき課題である。

③ 伝票の種別と必要性

前述したようにＩＣカードによって高速の決済を実現しようとするわけであるが、現行のクレジット端末での３枚複写（または４枚複写）の伝票では、その印字のために１０秒近くの時間を要してしまう。サーマル伝票等の採用についても、端末コスト、伝票の保存期間等の運用面から議論されるべき課題である。

④ ＰＯＳレジとの連動

大型店舗、チェーン店、ショッピングセンタ等では、ＰＯＳレジが多く導入されており、操作のスピード化および金額の二度打ちによる入力ミスの防止のために、ＰＯＳレジとクレジット端末の連動が必要である。トランザクションの決済センタへの転送をクレジット端末からだけでなく、店舗のストアコントローラから一括転送する運用が考えられる。クレジット端末のコードレス化とともに、ＰＯＳレジへのトランザクション転送機能の実現も検討していく必要がある。

⑤ 取消・返品処理の運用

店舗での購入場面を考えると、クレジットで購入した物品の返品、または取引金額の入力ミスにより取引の取消といった行為が発生する。この場合に、オフラインで売り上げた取引に対する取消方法の方法等は、さらに議論されるべき課題である。

⑥ 端末障害時の売上データの復旧

クレジット端末でのオフラインクレジットデータは、それぞれ決済センタへ送信するまでは端末内に保持することになる。その状態で、端末に障害が発生し決済センタへそれぞれの売上データを送信できなくなった場合に、どのようにそのデータを復旧していくかは、端末の機能として重要な課題である。伝票の運用、データバックアップ機構の装備によるコストアップ等、さらに議論を進める必要がある。

2.2.2 自販機端末

ＩＣカードを導入する端末として自販機を分類すると以下のようになる。

・中身商品からの分類

１）飲料自販機（清涼飲料、乳飲料、酒類）

２）たばこ自販機

３）切符販売機、その他の自動サービス機

４）その他商品の自販機

・電子マネー運用からの分類

１）プリペイドカード（前払い型）仕様

２）クレジットカード（後払い型）仕様

比較的低額の中身商品の販売機はプリペイド型の機能だけを有すると思われる。

また、５４０万台（９５年末）といわれる自販機のうち約４７％は飲料自販機が占めている事から検討の対象として飲料自販機・プリペイド型を例にあげて検討する。

2.2.2.1 自販機システム構成イメージ

ＩＣカード対応自販機システムの構成イメージを（図 2-7、図 2-8）に示す。構成イメージとしては、ＩＣカードリーダライタを内蔵した一体型タイプ（図 2-7）と、ＩＣカードリーダライタを分離した分離型タイプ（図 2-8）が考えられる。

電子マネー機能付きカードの利用者は自販機を小銭の不要な自販機として利用するにとどまらず残高表示機としても利用することができる。

将来的には、自販機は高度な情報を伝達する端末としても利用されるようになり、よりインテリジェント化が進むものと考えられる。また分離型の場合は、外付けユニットが独自に機能拡張され情報端末として進化するであろう。

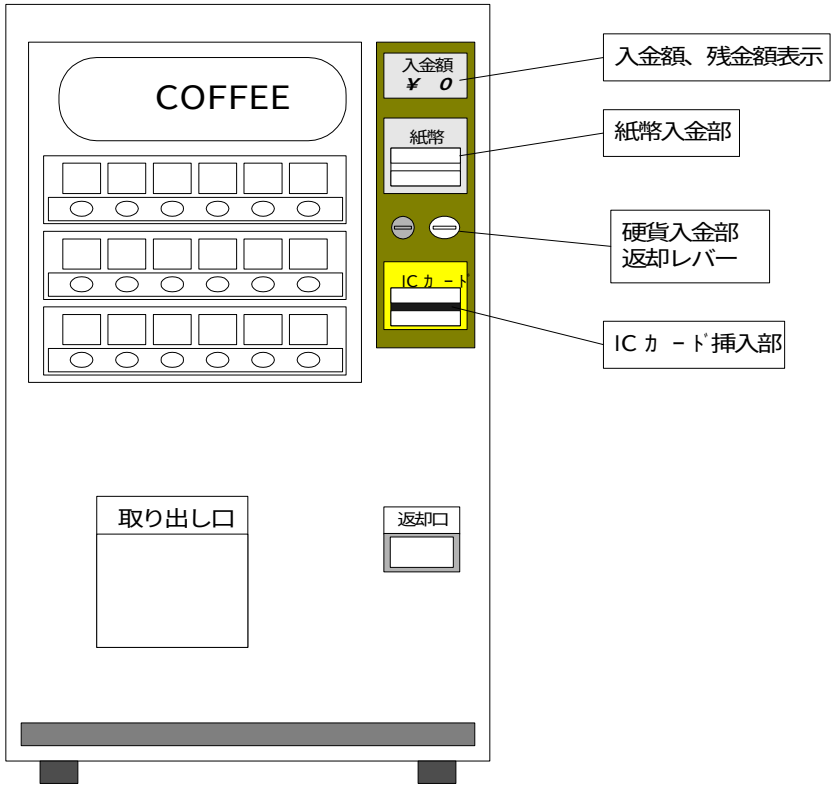


図 2-7 ＩＣカード対応自販機（一体型タイプ）

一体型タイプのＩＣカード対応自販機は設置スペース的に有利である。コスト的には現金との併用方式の場合はＩＣカードユニットを搭載する分だけコストアップするが、将来、ＩＣカードユニットのみとなった場合、装置コストは現在の現金専用機よりも下がると思われる。

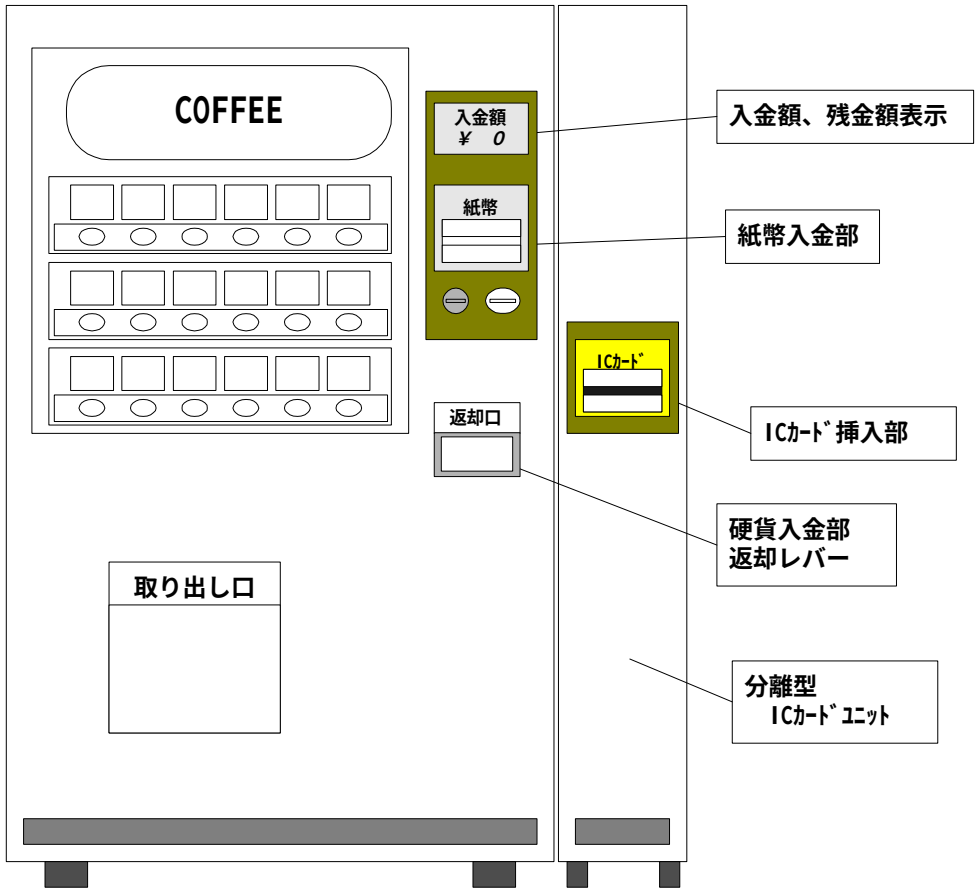


図 2-8　ＩＣカード対応自販機（分離型タイプ）

分離型のＩＣカードユニットを接続した構成では、自販機側にカードユニットが不要なため自販機の機種が限定されない。そのため分離型タイプのＩＣカード対応自販機は、自販機の機種替えを考慮した場合に有利である。また１台のユニットを自販機でサンドイッチして配置するなどして１度に複数台の自販機を制御することで、設置スペースの問題を回避することが可能である。また、一体型では自販機のオペレーターが電子マネーの回収を行う運用が基本になる。分離型タイプでは自販機のオペレート（中身補充、料金回収業務）と電子マネーのオペレート（保守・管理）を分離して運用することが可能であり運用方法も柔軟に構成できる。

2.2.2.2 電子マネー対応自販機の形態別比較

自販機を電子マネー対応する場合の形態別での比較を表 2-6に示す。

表 2-6　電子マネー対応自販機の形態別比較

タイプ	利用方法	利用者	設置者
専用機	電子マネー専用機	釣り銭切れによる購入不可状態がない 小銭を用意する必要がない	釣り銭の準備が不要（現金管理コスト不要） 釣り銭切れによる販売機会の損失がない
兼用機	現金と電子マネーの両方が利用可能	同上 カードを持たない人も利用できる ポイントなどのメリットがあれば積極的に電子マネーを利用する。	カード利用者に対し釣り銭切れによる販売機会の損失がない 準備する釣り銭の量は少なくできる

自販機を電子マネー対応（ＩＣカード）化することで次のような設置者メリットが得られる。

- ＩＣカード内の情報を読み出すことで中身（飲料など）販売業者にとって有効な情報（購買者の年齢や性別など）の収集ができる。
- 設置者にとっては死に金とも思われる釣り銭を自販機内に準備する必要がなくなる。
- 電子マネーの回収を通信回線で行えば即座に集金業務が行え、資金運用を効率化できる。
- 現金が販売機内に無いため現金目的の盗難がなくなる。
- 消費税に対し外税表示など価格設定が柔軟に行える(1円単位)ようになる。
- 特定中身商品（酒・たばこ）の自販機に対し、カード内の情報(年齢)を利用することで未成年者対策を図ることができる。

利用者が便利なのは兼用機である。装置提供者側（カード会社、メーカー、オペレータ）からは、専用機で対応する方法がコスト的に有利である。複

数台の自販機が同時に設置できるのであれば、専用機と従来機を混在して設置することで利用者ニーズにこたえる事が可能である。

自販機が分離型タイプでオペレータが電子マネー管理を行わない場合は、料金の回収方法が異なる。オペレータは自販機内のジャーナルで出力される情報をもとに現金分は従来通りの回収を行う。カードでの売上分については売り上げ代金は電子マネー運営母体に請求することで料金の回収を行う。この場合、電子マネーの回収そのものにオペレータはタッチしない。電子マネーの回収は、電子マネー運営母体（精算センター）が通信ラインなどを通じ回収することになる。

2.2.2.3 自販機のブロック構成

図 2-9に示す様に、ＩＣカード制御ユニット単体でカードの認証等がすべて行えることが望ましい。本体制御部との接続には、ＢＶユニットやコインメックと並んでＪＶＭＡ通信ラインでの接続を行い、課金情報の通信をおこなうことが可能である。

また、課金情報のほかにカードからの情報（購入者の情報：年齢、性別など）が必要なときは、別途専用の制御ラインで接続し本体の制御部内で情報の処理を行う事もできる。カードから得た情報はオペレーターにとって自販機の中身商品の営業戦略に利用する事ができる。これは自販機のＩＣカード化のメリットの１つである。

電子マネーの保存場所としての入金用モジュールは、そのマネーの技術仕様にあわせ本体制御部で処理することも可能であるが、セキュリティ上の技術的裏付けが必要である。

オンライン式の電子マネーを利用するときには通信ユニットが必要になる。現在では PHS 等での接続が有望である。

カードリーダーライタ部分が外付けのタイプではＩＣカード制御ユニットが分離されると考えれば良い。分離型の場合は、ユニット内に通信ユニットを組み込む形態になると考えられる。

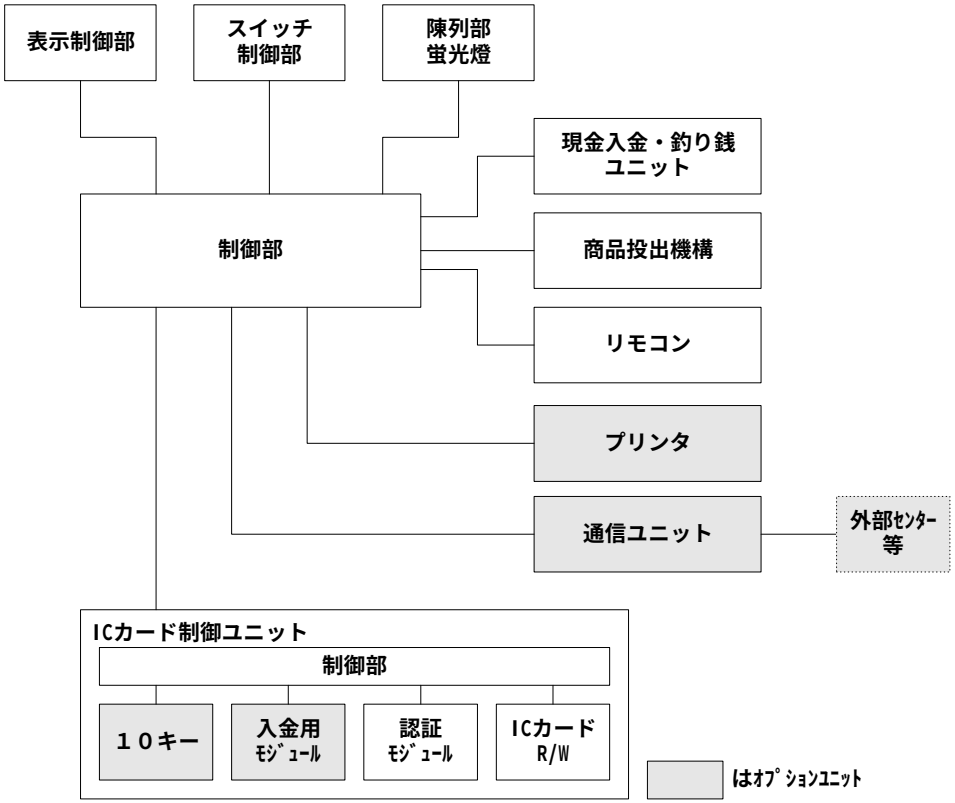


図 2-9　自販機のブロック構成例

2.2.2.4 電子マネー運用におけるメリット

電子マネー運用におけるメリットを各々の立場から纏めると表 2-7、表 2-8の様になる。

表 2-7　電子マネー運用におけるメリット

立場	メリット	備考
カード発行者	・カード発行枚数の増加 ・小口決済での利用総金額の増加 ・カード面上の広告収入 ・退蔵益が得られる	・電子マネーが定着するまでの期間が不明。 ・電子マネーが壊れたとき、バックアップできる体制を作る必要がある。もしくは利用者側でリスクの認知が必要。
装置メーカー	・電子マネー対応装置を提供することで新規需要の開拓 ・特定中身商品（酒・たばこ）の自販機に対し、未成年者対策としてカード情報を利用した装置の開発が可能になる	・開発コストの回収方法。単純に価格転嫁できない。 ・ハード面以外での安全性の技術的裏付けを求められる。本来は電子マネー（ソフト）は電子マネーの開発会社が行うべきもの。
設置者 中身メーカー オペレーター	表 2-8　参照	・装置メーカーからの機器調達コストがアップする ・決済方法が変わっても、必ず設置場所まで行って中身をつめなければならない。 ・売り上げの低い場所ではコストの高い装置の設置はできない。
利用者	・小銭を持ち歩かなくて済む ・ポイントによるキャッシュバックがある。	・精算センターが複数だと沢山カードを持つ必要がある。

表 2-8　電子マネー運用における設置者メリット

- ＩＣカード内の情報を読み出すことで中身（飲料など）販売業者にとって有効な情報（購買者の年齢や性別など）の収集ができる。
- 設置者にとっては死に金とも思われる釣り銭を自販機内に準備する必要がなくなる。
- 電子マネーの回収を通信回線で行えば即座に集金業務が行え、資金運用を効率化できる。
- 現金が販売機内に無いため現金目的の盗難がなくなる。
- 消費税に対し外税表示など価格設定が柔軟に行える(1 円単位)ようになる。
- 特定中身商品（酒・たばこ）の自販機に対し、カード内の情報(年齢)を利用することで未成年者対策を図ることができる。
- 電子マネーをオンライン回収する場合には、その通信回線を利用して中身商品の売れ行きを監視し、オペレート時の商品補充作業を計画化できる。

2.2.2.5 電子マネーと自販機

利用者にとって電子マネーが便利と感じられるのは、毎日のように繰り返し行っている行動の中に現金を必要とする場面があり、そこでわざわざ小銭などを用意する煩わしさが解消されたときであろう。公衆電話がカード化されたときに便利と感じたように、よく利用する自販機で電子マネーが利用できるようになることで、世の中に電子マネーが受け入れられるようになるであろう。

日本における自販機文化というものの中に電子マネーが受け入れられるためには、表 2-7で示した各者が電子マネーのメリットを各々享受できる仕組みを作る事が大切であると考える。

2.3 セキュリティ

セキュリティに関しては、これまでもＩＣカードのＩＣチップ自体のタンパーレジスタンス機能であるとか端末のＰＩＮ入力機能等について述べたが、多目的利用や汎用性を持たせる為に、端末の相互開放による相乗り等をも視野に入れて更に検討すると、チップの設計・製造、ＩＣカードの発行・利用（端末／ネットワーク等の各種機器や社会インフラといった利用環境を含めて）・廃棄という所謂ＩＣカードのライフサイクルとセキュリティという視点が必要となる。

この点に関しては、ＩＳＯ１０２０２－１（金融取引カード－ＩＣカードを使った金融取引システムのセキュリティ・アーキテクチャに関する規定のパート１：カードライフサイクル）の規定を参考に考察し、併せてＩＣカードの場合暗号技術の利用や様々な技術の応用や運用上の取決めによっても高度なセキュリティを保持することが可能である。これらについてはEMV仕様を例として、仕様書に規定されている各種方式について記述することとする。

2.3.1 ライフサイクルとセキュリティについて

前述のとおり、各段階におけるセキュリティ検討の要請から、図 2-10にカードのライフサイクルを示す。

2.3.1.1 セキュリティ管理

ＩＣカードでは、設計・製造、発行及びＩＣカードが配布された後の運用段階において、表 2-9に示すようなセキュリティ管理が必要であると考える。

2.3.1.2 不安要件とセキュリティ対策

(1) 不安要件

ＩＣカードにおける設計・製造、発行、運用・仕様の各段階の不安要件を図 2-11に示す。図 2-11に示したように、単にＩＣカードのみのセキュリティを考えるのではなく、ＩＣカードのライフサイクルやシステムの運用方法を考慮し、システム全体のセキュリティ管理を検討する必要がある。

図 2-11で示した不安要件は、ＩＣカードを利用した場合の一例であり、システムの全容が明らかになった時点で見直す必要があると考える。

(2) セキュリティ対策

表 2-10に、図 2-11で示した不安要件に対するセキュリティ対策を示す。

＊本章における上記各図と表は次頁以降に纏めて示す。

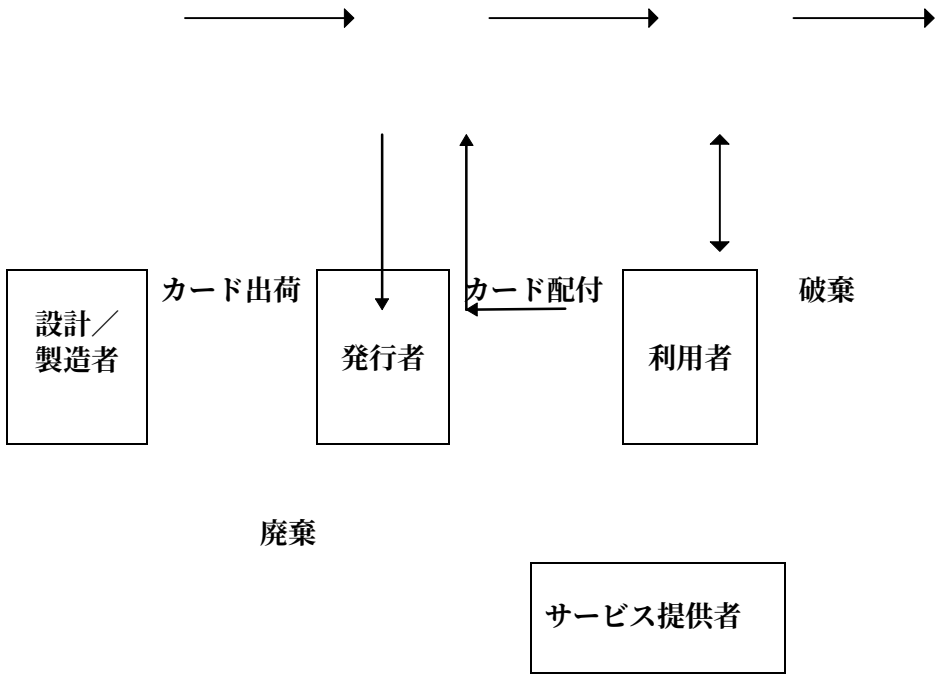


図 2-10ＩＣカードのライフサイクル

表 2-9 各段階におけるアクセス制御と取扱うデータ

段階	処理	アクセス制御	取り扱うデータ	備考
設計	形式認定	――――	・仕様書/被試験カード	
製造	出荷	アクセス制限無	・発行者用仮PINの設定	
			・半導体製造者IDの設定	ISO9992
			・ｶｰﾄﾞ製造者IDの設定	ISO9992
発行	初期化	発行者仮PIN	・発行者用本PINへの書換	
		の認証		
		発行者本PIN	・ファイル構造の生成	
		の認証	・アクセス制御のための各種キー	以後のアクセス
			の設定	制御を決定
	データ登録	ファイルアクセス	・各個人データの登録	
	（発行）	のためのキー認証		
運用	データ取得	カードの認証		ICｶｰﾄﾞの正当性
使用				の確認
		ファイルアクセス	・データの取得	
		のためのキー認証		
	データ登録	ファイルアクセス	・追加サービスのデータの	
		のためのｷｰ認証	登録	
		PIN番号変更	・PIN番号	
廃棄	カード終結	ファイル、暗号	・業務データ消去	
		キーのロック	・個人データ消去	

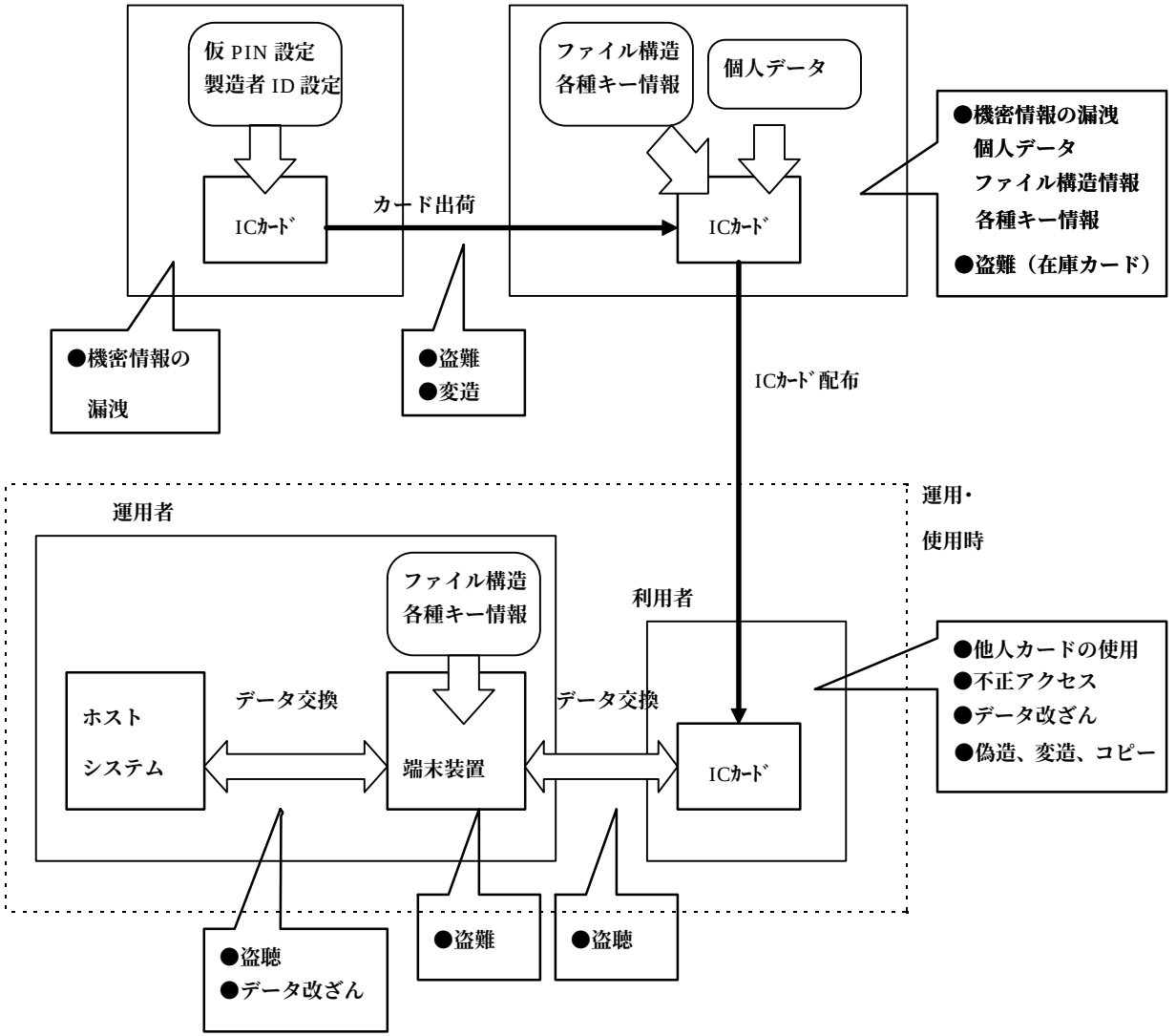


図 2-11 ＩＣカードのライフサイクルにおける不安要件

表 2-10　不安要件とセキュリティ対策

段階	不安要件	セキュリティ対策
設計 製造	●機密情報の漏洩 ●盗難・変造	・形式認定情報の漏洩防止 ・製造者には、機密情報をできる限り持たせない。カード内に設定するファイル構造情報、各種キー情報等については発行者が書き込むべきと考える。 ・仮 PIN（トランスポート PIN）を製造者が設定。仮 PIN を知らない第三者は、カードへのアクセス不能となる。
発行	●機密情報の漏洩 　個人データ 　ファイル構造情報 　各種キー情報 ●盗難（在庫品）	・発行者の責任において外部に漏洩することのないよう管理すべきである。機密情報の取扱者を限定する等の対策が考えられる。 ・発行者の責任において管理すべきである。
運用 使用	【利用者】 ●他人カードの使用 ●不正アクセス ●データ改ざん・コピー ●偽造、変造 【カード・端末間】 ●通信データの盗聴	 ・顔写真による本人確認、PIN による本人確認 ・キー認証によるアクセス制御 正当な権限を持つ運用者および端末装置のみがアクセス可能である。 ・キー認証によるアクセス制御 ・公開鍵暗号による電子署名 ・IC カードと端末間の相互認証 ・IC カードの耐タンパー性 ・ホログラムの利用 ・特にキー認証のときに、通信データの盗聴に対する対策が必要。キー自体は通信データとして交換せずに、乱数と暗号関数を利用した認証方式が考えられる。

	【端末装置】 ●不正アクセス ●盗難 【ホスト・端末間】 ●不正アクセス ●盗聴 ●データ改ざん	 ・有効期限の確認 ・取引条件、前回取引日等の確認 ・端末装置には、IC カードと各種の認証を行うためのキー情報が格納されているため、これらを容易に解析できない仕組みが必要。 ・端末装置の運用方法について検討が必要。 ・有効期限の確認 ・取引条件、前回取引日等の確認 ・ホスト、端末間のデータの暗号化 ・認証コード生成（メッセージ認証）
廃棄	●不正カード再利用	・情報の消去またはファイル、暗号キーのロック ・物理的破壊

2.3.2 ＥＭＶのセキュリティ

本章においては前述のとおり、公開されているＥＭＶ仕様における様々なレベルでのセキュリティ確保の手法を、今後の検討の参考とする為に記述することとした。

2.3.2.1 カードの認証

カードが偽造されたものでないことを証明する為の手法。

(1) 静的認証

ＩＣカードは発行者の秘密鍵で署名されたデータを記憶しており，端末はこのデータを読み出し，発行者の公開鍵を用いてＩＣカードの正当性を確認する。この認証に使用されるデータが固定であるため、静的認証と呼ばれる。認証時に端末は公開鍵暗号の演算を行うが、ＩＣカードは演算

を行わないため、動的認証と比較して処理速度は速い。

尚、発行者の公開鍵はＩＣカードから得られるが、この公開鍵の正当性を確保する為、証明機関の秘密鍵により署名されている。端末は証明機関の公開鍵を有しており、これを用いて発行者の公開鍵の正当性を検証する。

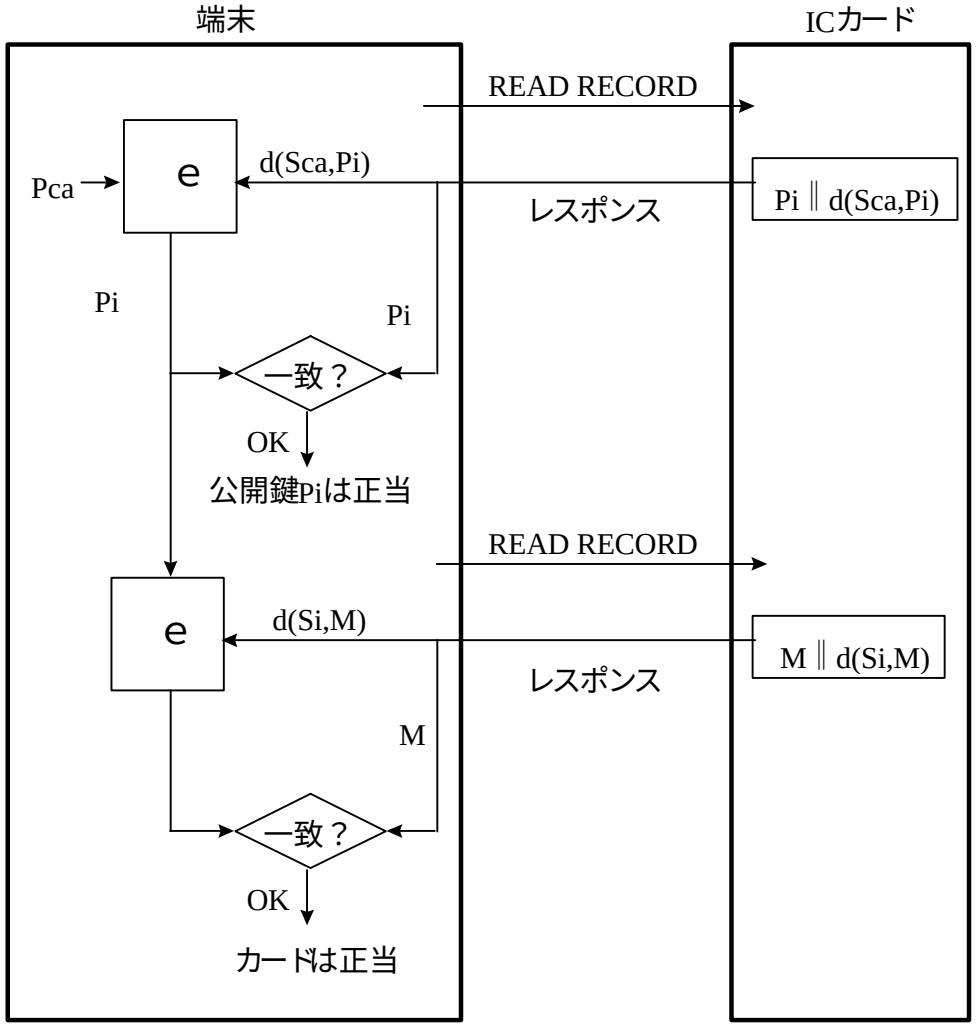
(2) 動的認証

静的認証の問題点は、認証に使用されるデータが固定である為、このデータを盗聴することにより偽造カードを作ることが可能となってしまう点である。 この問題点を解決する為の方法が動的認証であり、ＩＣカードに入力される乱数に対してＩＣカードが自分の秘密鍵で暗号演算を行い、端末がＩＣカードの公開鍵により、その演算結果を検証してＩＣカードの正当性を確認する。ＩＣカードが動的に暗号演算を行う為、セキュリティが向上する反面、処理速度が遅いという欠点がある。

尚、ＩＣカードの公開鍵はＩＣカードから得られるが、この公開鍵の正当性を確保する為、発行者の秘密鍵により署名されている。端末は発行者の公開鍵を用いてＩＣカードの公開鍵の正当性を検証する。

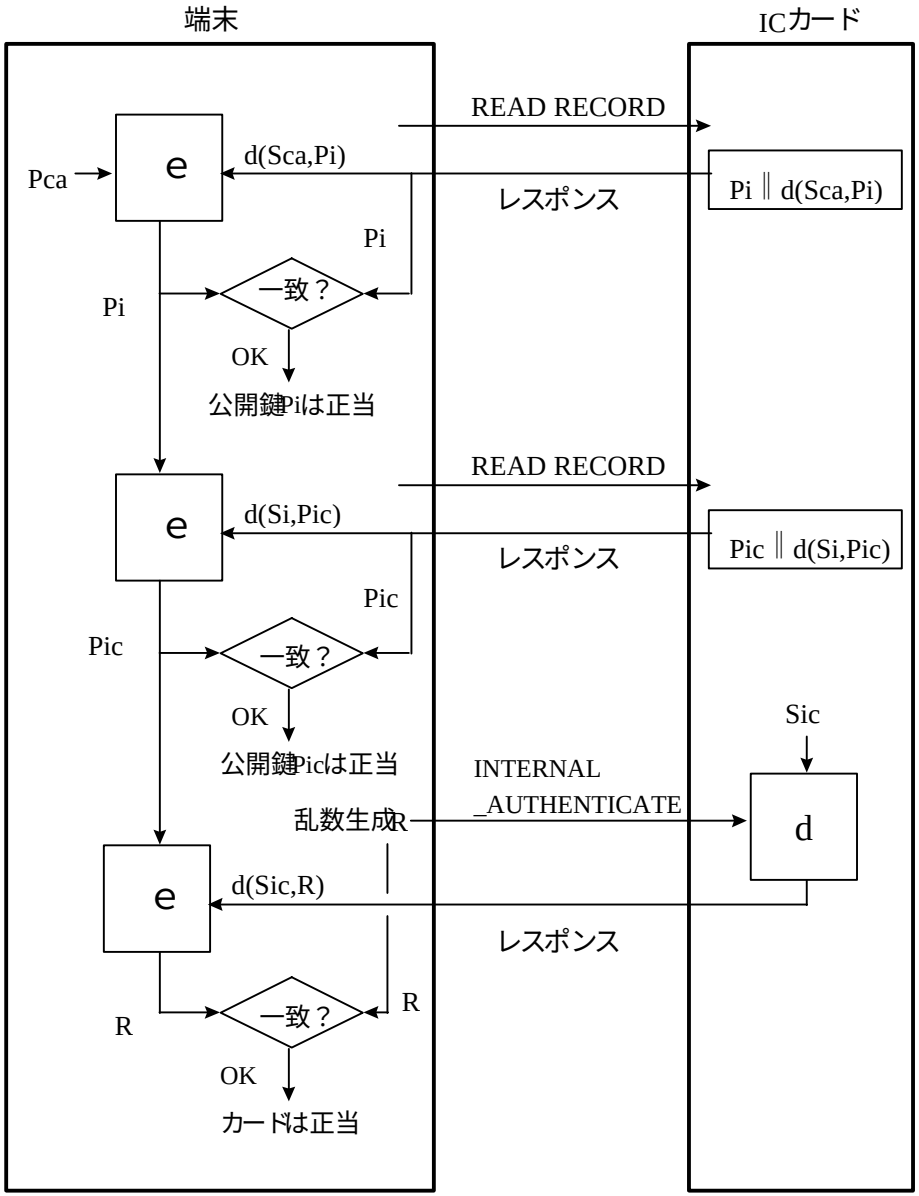
更に発行者の公開鍵もＩＣカードから得られるが、この公開鍵の正当性を確保するため、証明機関の秘密鍵により署名されている。端末は証明機関の公開鍵を有しており、これを用いて発行者の公開鍵の正当性を検証する。

＊各認証の概念図 2-12並びに図 2-13を次頁以降に示す。



Sca ： 証明機関の秘密鍵
Pca ： 証明機関の公開鍵
Si ： 発行者の秘密鍵
Pi ： 発行者の公開鍵
d ： 署名演算
e ： 署名検証演算
M ： 被署名データ

図 2-12 静的認証



Sca ：証明機関の秘密鍵
Pca ：証明機関の公開鍵
Si ：発行者の秘密鍵
Pi ：発行者の公開鍵
Sic ：ICカードの秘密鍵
Pic ：ICカードの公開鍵

d ：署名演算
e ：署名演算の逆演算
R ：乱数

図 2-13 動的認証

2.3.2.2 本人確認

本人確認の為に暗証番号（ＰＩＮ）を入力する。そのチェック方法には次のとおり。

(1) オフラインＰＩＮチェック

ＩＣカードと端末間のみでチェックを行う方式で、カードに入力されたＰＩＮと、カードに記憶しているＰＩＮとをカード内部で照合する。

(2) オンラインＰＩＮチェック

リアルタイムオンライン送信によりカード会社センタホストでチェックを行う。

2.3.2.3 端末リスク管理

カード発行者やシステム等を不正行為から守る為に端末側で行われるリスク管理で、高額取引やオフライン環境では検出できないような各種の脅威から保護する為に、下記方式による一定の条件下でオンラインリアルタイムオーソリゼーションを実施してチェックを行うもの。

(1) フロアリミットチェック

端末に一定金額のフロアリミットを設定し、１回当りの利用金額がこれを超えていないかどうかのチェック。

(2) ベロシティチェック

端末にオフライン上限値と下限値を設定し、オフラインで連続処理できる回数を超えていないかどうかのチェック。

(3) ランダムチェック

フロアリミットより小さい金額で端末にしきい値をセットし、フロアリミット以下の金額で一定確率によりランダムにオンラインチェックをかける。

2.3.2.4 取引証明の生成

端末は端末アクション分析を行い、オフライン承認かオンライン処理要求か取引拒否かの決定を行い、その結果に応じたGENERATE ACコマンドをＩＣカードに送る。

端末からGENERATE ACコマンドを受信したＩＣカードは，カードアクション分析を行い、オフライン承認かオンライン処理要求か照会要求か取引拒否かを最終的に決定し，それに応じたレスポンスを端末に送信する。

オフライン承認の場合，ＩＣカードはトランザクションデータに対して，カード自身の秘密鍵により取引証明を生成し、レスポンスとして端末に送信する。

オンライン処理要求の場合、発行者はＩＣカードの認証を行う。ＩＣカードの認証が正しく行われた場合、発行者の認証を行う為，EXTERNAL AUTHENTICATE コマンドが発行者から返される場合がある。発行者の認証が正しく行われた場合、端末は２番目の GENERATE AC コマンドをＩＣカードに送り、取引証明の生成を要求する。

2.3.2.5 セキュアメッセージング

カード発行者は発行後のカードに対して、以下の処理を行う場合がある。

（1）アプリケーションのロック

（2）アプリケーションのロック解除

（3）カードのロック

（4）カード保持者の暗証番号の更新およびロック解除

上記の処理を行うために発行者が発信するコマンドは，オンラインにより端末を介してカードへ送信されるが、このコマンドが端末によって盗聴あるいは改ざんされないよう，暗号化かつ／またはメッセージ認証コードの付加により保護されて送られる（セキュアメッセージング機能）。従って、端末は暗号化されたコマンドを単にカードに伝送する機能のみを有する。

2.3.2.6 カード発行者に決定が任されている事項

以下に示す内容は，「ＥＭＶ’９６・決済システム用ＩＣカード仕様書」の中で，カード発行者に決定が任されているものである。

(1) カードＯＳのインプリメントに影響を与える可能性があるもの。

① アプリケーションの選択

SELECT コマンドのレスポンスで返送されるＦＣＩ（ファイル制御情報）のオプションデータ

② アプリケーションの起動

Ａ．処理オプションデータオブジェクトリスト（ＰＤＯＬ）の処理方法

Ｂ．GET PROCESSING OPTIONS コマンドのレスポンスフォーマット

③ アプリケーションデータの読出し

特になし

④ データ認証

Ａ．INTERNAL AUTHENTICATE コマンドのレスポンスフォーマット

Ｂ．動的データ認証データオブジェクトリスト（ＤＤＯＬ）の処理方法

⑤ カード保有者の検証

特になし

⑥ カードアクション分析

カード自身によるリスク管理の処理内容

Ａ．カードリスク管理データオブジェクトリスト（ＣＤＯＬ）の処理方法

Ｂ．取引証明データオブジェクトリスト（ＴＤＯＬ）の処理方法

Ｃ．GENERATE APPLICATION CRYPTOGRAM コマンドの演算アルゴリズムと，レスポンスのフォーマット

Ｄ．EXTERNAL AUTHENTICATE コマンドのオプションデータ

⑦ 発行者からカードへのスクリプト処理

Ａ．使用するコマンドの選択

Ｂ．セキュアメッセージングのフォーマット

C．セッションキーの生成方法

(2) カードＯＳのインプリメントには影響を与えないと思われるもの

①規定されているデータエレメントの具体的な値

②規定されているもの以外のデータエレメント

③データオブジェクトからレコードへのマッピング方法

④データファイルのレイアウト

⑤ＤＩＲファイルの各エントリに含まれる任意データの内容

⑥発行者固有のアプリケーション

2.4 業務・制度に関する運用上の要件と課題

これまでのところで、接触型（外部端子付き）ＩＣカードの物理的な条件や電気特性、基本的なコマンド等に関する標準化動向や技術動向については、十分ご理解頂けたことと思う。また、ＩＣカード固有の機能以外のセキュリティ確保の在り方についても概説し、その重要性はご理解頂けたことと思う。

しかしながら、これらＩＳＯ／ＩＥＣ７８１６やＪＩＳ Ｘ ６３０３～６３０６で規定された内容のみでは、到底インプリメントできるものではなく、更にクレジットカード業界において全世界の売上高シェアの大半（売上高の合算で、全世界の８５%超：月刊消費者信用９６年9月号より）を占める、Ｅｕｒｏｐａｙ、ＭａｓｔｅｒＣａｒｄ、ＶＩＳＡの各ブランド保有会社によって作成されたEMV仕様（EMV‘９６ Ver３．０）にしても、各ブランド傘下メンバーがＩＣカード利用のメリットを活かし、自由にアプリケーションをEMV仕様の上に構築でき、且つ、必要な相互運用性の確保ができるよう配慮されているものの、ＩＳＯ／ＩＥＣ７８１６の規定に金融取引き向けに必要なコマンド等を追加しただけの必要最小限の取決めであり、あくまでインプリメントするのは各発行者自身であるという考え方に立っている。このことはブランドホルダーとして当然の配慮であると理解できるが、この場合意図的であるにしても、特定の業界内部で検討・制定されたEMV仕様ですら、そもままでインプリメントできるものではないのが実状である。

従って現在求められているのは、ＩＣカードを具体的にどのようなビジネススキームの中でどのように利用するかという、セキュリティの確保を含めた具体的な業務内容、具体的な利用方法、即ちどのようなアプリケーションをＩＣカードに書込むかということに尽きると言える。

更に、これらアプリケーションを考える時に、EMV仕様の思想ともいうべき考え方の中にも見受けられるが、利用者や発行者の視点からＩＣカード利用のメリットとして挙げられている多目的利用若しくは汎用的な利用という点を視野に入れて検討すると、利用者、加盟店、発行者にとって不可欠である相互運用性の確保、その一環として端末の共用化もまた不可欠と思慮されるが、端末の共用化を考える時に、ただ単にＩＣカードと端末間のセッションのことだけを考えれば良いというものではなく、少なくともこれらにネットワークを加えた三位一体としての検討が最低限必要不可欠であり、これらを取り巻く利用環境整備、運用方法、法制度等々検討すべき課題は多い。これを実現する為には、ＩＳＯ／ＩＥＣ７８１６－５（ＩＤカード－接点付きＩＣカードパート５：アプリケーション識別子の番号体系と登録手順）の理解と国内における付番管理体制の確立も必要となる。

また本章においては、あるべきＩＣカードの利用モデル策定作業上必要な、業務・制度面の検討の中で、特に決済機能を有するＩＣカード利用のメリットとして挙げられている、オフラインでの利用方法に関する要件と実現の為の課題に関する考察と、相互運用性の確保やセキュリティの保持等に運用上必要と思われる点を主体に述べることとする。

2.4.1 アプリケーション識別子（ＡＩＤ）の付番管理について

ＩＣカードの想定されるメリットの一つとして、複数の様々なアプリケーションを実装できることが挙げられているが、これらを正常に作動させる為には、カード内のどのアドレスにどのようなアプリケーションが実装されているかを、正確に認識して読み出しできることが不可欠であり、国内においてもＩＣカードの多目的利用を指向した場合、アプリケーションを識別する為の識別子（Application Identifier＝アプリケーション識別子：以下“ＡＩＤ”という）の付番管理体制の確立が必要と思慮される。以下、ＩＳＯ／ＩＥＣ７８１６－５に規定されている定義や番号体系、登録手順等を確認すると共に、一元付番管理体制確立の必要性を検証したい。

2.4.1.1 ＩＳＯにおける定義及び付番体系

(1) 目的

ＩＳＯ／ＩＥＣ７８１６－５では、ＡＩＤの番号体系とアプリケーション・プロバイダ識別子の登録手順を規定しており、ここで記述されている番号体系は、プロバイダから提供されるアプリケーション及び関連サービスの為の一手段であり、あるカードにそのアプリケーションまたは関連

サービスで必要とされるエレメントが、含まれているかどうかを見分ける為に使用するとされている。またＡＩＤは、カード内のアプリケーションをアドレス指定する為に使用されるとしている。

ＩＳＯ／ＩＥＣ７８１６－５では、ＡＩＤの符号化を規定すると同時に、カード内のアプリケーション部分をアドレス指定する方法及びメカニズムも規定している。

またＩＳＯ／ＩＥＣ７８１６－５では、手順や機関を設定することで登録方法の信頼性を確保し最適化することを目的としている。

(2) 定義

① ＡＩＤ

カード内のアプリケーションを識別するデータ・エレメントで、ＡＩＤは登録済みアプリケーション・プロバイダ識別子（＝Registered Application Provider Identifier：以下“ＲＩＤ”という）を含んでいてもよい。

＊ＲＩＤや発行者識別番号（＝Issuer Identification Number：以下“ＩＩＮ”という）のいずれかが含まれていれば、識別情報として曖昧さがなくなる。

② アプリケーション・プロバイダ

カード上のアプリケーションを実行する為に必要なコンポーネント提供者。

③ 付番体系

ＡＩＤは１６進表記を使って符号化されており、その最大値は１６バイトで登録カテゴリーコード体系は下表 2-11のように規定されている。尚、登録カテゴリーコードは、ＡＩＤの先頭に位置し最初のバイトの最上位４ビットで、登録済み及び固有のアプリケーション識別子を区別する為に使用される。

表 2-11 登録カテゴリーコード一覧

登録カテゴリーコード	内容・用途
‘０’－‘９’	ＩＳＯ７８１２で定義される通り

‘Ａ’	国際登録
‘Ｂ’	ＩＳＯが予約
‘Ｃ’	ＩＳＯが予約
‘Ｄ’	国内登録
‘Ｅ’	ＩＳＯが予約
‘Ｆ’	固有、未登録（登録しない）

＊固有アプリケーション識別子拡張（＝Proprietary Application Identifier Extension：以下“ＰＩＸ”という）を使用することにより、アプリケーション・プロバイダは自分のアプリケーションを識別することができ、また、ＰＩＸの符号化はアプリケーション・プロバイダが自由に決めることができ、国際登録に申請する必要はない。

A．登録カテゴリーが‘０’から‘９’の場合

ＡＩＤの最初の部分はＩＩＮであり（登録カテゴリーはＩＩＮの最初の数字＝磁気カードにおける発行者識別番号）、ＩＳＯ７８１２に規定されている。

B．登録カテゴリーが‘Ａ’（国際登録）の場合

国際登録は、国際的な使用に限定されており、ＩＳＯ指定の登録機関へ登録することと、登録から１年以内に使用することが義務付けられている。尚、ＲＩＤは以下のフィールドより構成される。

a) 登録カテゴリー

１０１０と符号化される４ビット。

b) 登録済みアプリケーション・プロバイダ番号

９個のＢＣＤ数字に符号化される３６ビットで、他の符号化はＩＳＯにて留保。

c) アプリケーション・プロバイダが任意に設定するＰＩＸ

最大１１バイト。

C. 登録カテゴリーが‘Ｄ’（国内登録）の場合

ＲＩＤは以下のフィールドから構成される。

a) 登録カテゴリー

１１０１と符号化される４ビット。

b) 国内登録機関の国コード

ＩＳＯ３１６６に従って３個のＢＣＤ数字の１２ビットに符号化される。（日本の場合は‘３９２’）

c) 国内登録機関が規定するフィールド

ＢＣＤコード化が望ましい。

D. 登録カテゴリーが‘Ｆ’の場合

ＡＩＤの残り部分のコード化は任意であり、ＩＣカードアプリケーション提供者が‘Ｆ’に続くコードを任意に付番することが可能であり、且つ、届出も義務付けられてはいない。

従って、重複する可能性がある。

2.4.1.2 付番管理の必要性

前述の通り、ＡＩＤの一元的な付番管理体制が確立されなかった場合、ＡＩＤが重複する可能性があり、また、ＩＣカードの普及・拡大や相互運用性の確保の点で以下のような問題点が考えられ、混乱は不可避となる思われる。

(1) 重複した場合の問題点

① リジェクト判断遅延による混乱

ＤＦ名が一致する為、本来受け付けてはならない未契約先が発行したＩＣカードに対するリジェクトの判断が瞬時に行われず、カードホルダー、加盟店双方が混乱する可能性があり、無用のトラブルを惹起する原因となりかねない。

② 他社カードのファイル破壊の危険性

ＤＦ内にフリーアクセスファイルを設けた場合、ＤＦ名が一致していると他のアプリケーション用のカードのフリーアクセスファイルにアクセスできる為、異常データを追記したり、場合によっては破壊してしまう危険性もある。

③ 相乗り対応が困難

相乗りの合意に達した会社間で、ＤＦ名が重複してしまっていた場合、相乗りの為の登録ができず、相互運用性が確保できない。

④ 事後対策費等の負担が過大

上記事態は、相当枚数のカード発行・利用された時点で発生する可能性が極めて高く、事後対策に費やされれる時間や費用の負担が過大なものとなると思慮される。また場合によっては、対応策そのものを見出すこと自体が困難となることも十分予想される。

(2) 運用上の問題点

① 海外企業への参入障壁となる危険性

海外企業が、日本国内にて国内企業との相乗りの事業展開を計画し参入しようとした場合、登録受付け機関が存在しないと登録ができず、また、重複していないことの証明が困難な為、その後の事業展開にも調査等に過大な時間・費用が必要となるなど、多大な影響がでる恐れがある。

② 付番の混乱

仮にＩＳＯ７８１６－５に規定に従ったとしても、各社が独自に付番する限りにおいては、解釈の問題等からも付番は混乱し、重複は回避できない。

③ 規格変更時の対応問題

周知徹底が困難である。

④ 問合わせ対応

一元管理機関がない場合、特に海外との整合性を取る必要のある企業が確認する術がないことになる。

以上の点からも、ＡＩＤの付番管理を一元的に行うこと、また、その為の機関の設立は不可欠と思慮される。

2.4.1.3 識別子の登録

(1) ＲＩＤの割り当て要求

名称をもって識別されているアプリケーション・プロバイダは、所定の登録書を国内標準化機構に提出することにより、ＲＩＤの割り当てを要求することができる。

国内標準化機構がなければ、ＩＳＯ／ＩＥＣ７８１６－５を担当しているＩＳＯ技術団体の事務局に対して要求しなければならない。

国内標準化機構（またはＩＳＯ／ＩＥＣ７８１６－５を担当するＩＳＯ技術団体の事務局）は、その要求に対する「補助機関」の役目を担う。

(2) 補助機関

① 割り当て要求

ＲＩＤ割り当て要求は、以下の団体により登録機関に転送される。

A. ＩＳＯの会員団体

B. ＩＳＯ／ＩＥＣ７８１６－５を担当するＩＳＯ技術団体

C. ＲＩＤに関連する目的の為にＩＳＯから認可された組織

② 補助機関の責任

補助機関は、以下のような事柄に責任を負う。

A. 自国または担当地域内からのＲＩＤ登録書の受け付け

B. ＩＳＯ／ＩＥＣ７８１６－５に準拠したＲＩＤ要求書の登録機関への転送

(3) 登録機関

ＩＳＯ／ＩＥＣ７８１６－５の目的及びＩＳＯ指示書にある登録機関の指名・運用方法に従って、ＩＳＯ委員会では以下を登録機関として指名している。

① 名称

ＫＴＡＳ（Copenhagen Telephone Company）

② 所在地

Teglholmsgade 1

ＤＫ－１７９０ Copenhagen Ｖ

(4) 登録機関の責任

ＲＩＤの初期割り当て、ＲＩＤの変更や削除、以降の登録簿への追加に関して、以下の様な責任を負う。

① 割り当て、登録、通知

アプリケーション・プロバイダ番号を割り当て、ＲＩＤを登録し、要求の処置について補助機関へ通知する。

② 登録簿の維持管理

アプリケーション・プロバイダに割り当てられた識別子の登録簿を維持管理する。

③ 登録簿のコピーの提出（その１）

ＩＳＯ／ＩＥＣ７８１６－５を担当するＩＳＯ技術団体に対して、登録簿のコピーを毎年提出する。尚、この書式はＩＳＯ／ＩＥＣ７８１６－５を担当するＩＳＯ技術団体の事務局及び登録機関の合意のあるものでなければならない。

④ 登録簿のコピーの提出（その２）

要求があれば、登録簿のコピーは国内標準化機構にも渡すが、国内標準化機構だけの排他使用とし、第三者には開示しない。

(5) 登録管理グループ（ＲＭＧ）

登録管理グループ（RMG）というグループを設立しなければならない。このグループの責任範囲は、ＩＳＯ／ＩＥＣ７８１６－５を担当するＩＳＯ技術団体で決められた通り。

(6) その他

ＫＴＡＳへの国際登録は、有償である。

2.4.1.4 日本の現状と課題

日本においても必要不可欠と思われるこの仕組に対する取組み等の現況は、ＫＴＡＳへの登録窓口としての事務局のみが、社団法人日本事務機械工業会内に設置されているに過ぎず、日本国内においても今後様々なプロジェクトが計画されている今日においては、早急な付番管理体制の確立が急務と思慮される。

尚、同会において体制の確立に向けて継続検討が行われており、国際的な使用に限らず重複回避の為には一元的な付番管理が不可欠と思慮され、既に国際的なＩＳＯ認定登録機関であるＫＴＡＳとの窓口に同会が指定されている事実を考慮すると、同会が国内の登録受付け機関となることが望ましいと考える。

但し、公的機関や民間のあらゆる業界における様々なアプリケーション全てに関して、事前の割り当て付番は困難と思われるので、例えばクレジットカード業界では、日専連・日商連の各単会をはじめ各地方信販をも含めた国内の主要なカード会社約２００社によって、（財）流通システム開発センターの企業コードの登録制度を利用して参加企業の識別し、管理運用体としてのＣＡＴＳ事務局を主体に加入受付けや端末管理を行う等により、ＣＡＴの共同利用システムを運営している事例もあり、業界単位で行うなど要検討課題である。

また、この一元的な付番管理機関設立の必要性についてはこれまで述べた通りであるが、設立された機関はＩＣカードが存在する限り、存続し続けることが更に重要であり、その為にはＫＴＡＳへの国際登録が有償であるのと同様に、維持費見合いの登録料の負担・有償化も必要と思慮され、この点も検討を要する。

2.4.2 クレジットカード業務（要件と課題）

消費者・企業間の商取引において、既に磁気ストライプのクレジットカードは普及しているが、ＩＣカードへの移行を考えた時、ＩＣカード化によりクレジットカードでも安全なオフライン取引が可能となると考えられる。主としてこのオフライン取引における利用モデルの策定の為の業務上の要件や実現の為の課題となる利用の際の問題点を主体に考察し記述する。尚、設計・製造、発行、廃棄に係わるＩＣカードのライフサイクルとセキュリティについては前述の通りで、これらも視野に入れて考察した。

2.4.2.1 業務フロー

クレジットカード業務の場合、セキュリティの章でも述べたが、信用を供与するという性質上、全てをオフライン取引とするには限界がある。従って現行のクレジットカード業務のフローを活かし、これとの整合性を考慮する為にも、現在のフローを検証し、オフライン取引／オンライン取引双方の要件と課題を考察することとする。尚、図 2-14に現行のフローとオフラインで追加が予想されるフローを示し解説を行う。

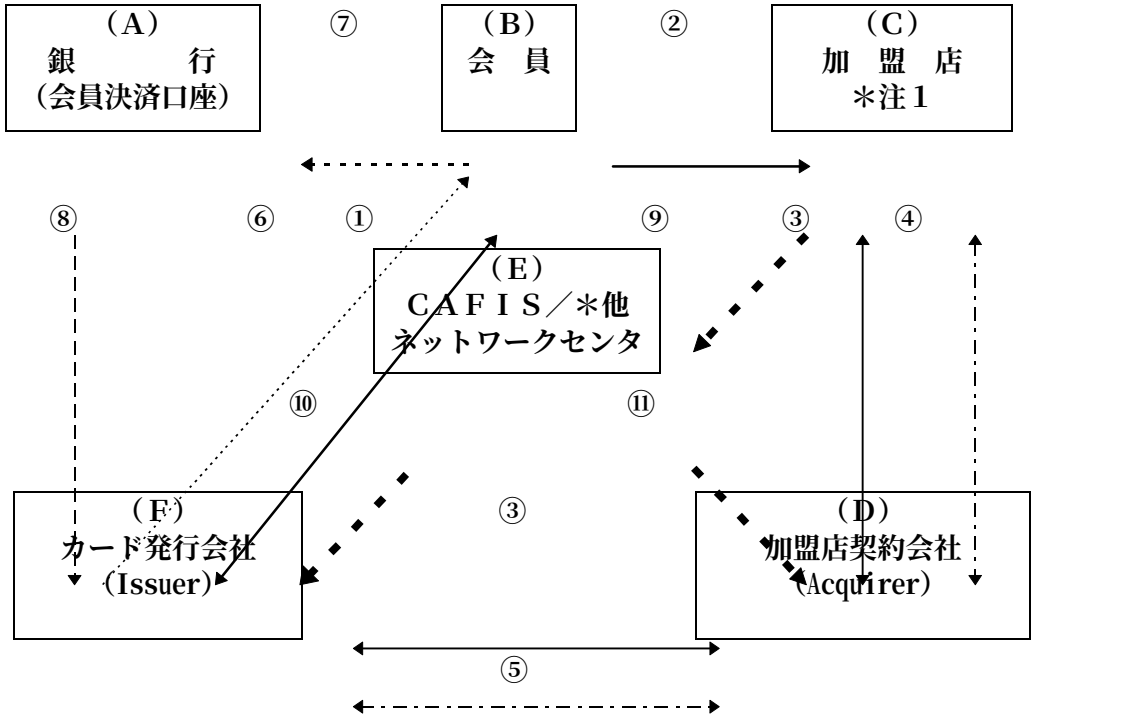


図 2-14 クレジットカード業務フロー

(1) 現行業務フロー解説

① 入会申込／審査／発行

通常カードの所有権は発行会社にあり、会員へは貸与となる。

② 利用

クレジットカードの利用に当っては、日本固有の取引方法として利用の際に会員が以下の支払方法を選択する。

A．一回払い

マンスリークリアーで、例えば銀行系カードの場合一般的には毎月１５日締めの翌月１０日に会員口座から一括自動振替となる。

B．分割払い

割賦販売法上は３回以上に分けての支払いが分割払いとされている。ボーナス一括払いとの併用もあり、金利手数料が付加される。但し、銀行系カードは２回払いのみで金利手数料は不要。

C．ボーナス一括払い

夏冬の分割もあり、その場合金利手数料が付加される。銀行系カードはいずれか一方のみで金利手数料も不要。

D．リボルビング払い

極度額を設定しその枠内で繰り返し利用が可能で、毎月の返済は定額返済。金利手数料を内枠で徴求するウィズイン方式と外枠で徴求するウィズアウト方式がある。

＊現行のクレジットカード端末には、加盟店契約の内容に対応してこれらの支払方法を設定し、会員の求めに応じて指定する機能を有し、支払区分をコード化することにより、判別可能な状態でカード会社センタへ送信する機能がある。

基本的に、ＩＣカード移行後もサポートが不可欠な機能である。

③ オーソリゼーション

現行の販売承認要求電文の流れで、国際ブランド間で見受けられる加盟店契約会社（D）とカード発行会社（F）が異なる例を示している。

④ 売上代金の精算

⑤ 立替金の精算

⑥ 会員請求

⑦ 入金

⑧ 自動振替

以上が現状のフローであり、以下にオフライン取引の場合に必要と思われるフローについて記述する。

注１）加盟店には、様々な業種業態や規模の違いがあり、これらに応じて設置される端末やオーソリゼーション並びに売上処理の仕組みが異なる。

A．大型店（百貨店／ＧＭＳ／ＳＣ等）

基本的にはＰＯＳ端末で、加盟店側のホストとカード会社のホストとを　　ＣＡＦＩＳを介して専用回線（通常加盟店～ＣＡＦＩＳ間はＤＤＸ－Ｐ網を利用し、ＣＡＦＩＳ～カード会社間は主に専用回線）で接続して利用。その接続運用方法には下記の２タイプがある。

a)　Ａタイプ接続

全件リアルタイムオンライン送信によるデータギャザーリング：オーソ　　リゼーションと売上処理を１トランザクションで処理。

b)　Ｂタイプ接続

フロアリミットを設定し、且つ加盟店ホストに無効カード情報としての　　ネガデータファイルを保有する。フロアリミット以下の取引については、　　カード会社センタとの間はオフライン取引で、ＰＯＳで読取った当該クレジットカードの会員番号を、ＬＡＮ接続によりホスト側のネガデータファイルとの　　突合照会のみとし、フロアリミットを超える取引の場合は、リアルタイムオンラインオーソリゼーションを行い、売上データは別途ＭＴやＦＤ、ＣＤＳ（ＮＴＴデータ通信が提供しているＩＳＤＮ回線を利用したデータ伝送サービス）によりカード会社へ送付（送信）される。

B．中・小規模店（各種物販店／料飲食店等）

基本的には公衆電話回線網（１２００／２４００ｂｐｓ）を利用したスタンドアロン型端末を使用しており、その主な種類は下記の通り。

a)　Ｇ－ＣＡＴ（Gathering－Credit Authorization Terminal）

全件リアルタイムオンライン伝送によるデータギャザリング専用端末　　で、オーソリゼーションゼーションと売上計上処理を同時に行う、所謂シ　　ングルメッセージタイプの端末であり、ＦＥＡＬ８を使用して電文の暗号　　化を行い取引データ保護の為のセキュリティを保持している。尚、売上票　　は指定センタにて一括保管。

尚、参考までにＧ－ＣＡＴの設置台数は、約３１５千台である。（平成　　９年３月末現在）

＊Ｇ－ＣＡＴ以前のモデルとしてＣＡＴ／Ｓ－ＣＡＴがあるが、ＲＳ２３　　２Ｃ等の他機器とのインターフェース用のポートもな

く拡張性がないの　　で、検討の対象外とした。

b) ＣＣＴ（Credit Center Terminal）

下記に記述するＣＡＦＩＳ以外のネットワークセンタが独自に開　　発した端末で、一般的にＧ－ＣＡＴ同様全件リアルタイムで伝送するが　　オーソリゼーションと売上処理（ＭＴ若しくはファイル伝送）が区分け　　されて行われる、所謂デュアルメッセージタイプの端末。

＊現行のネットワークセンターには、図 2-14記載のＣＡＦＩＳ（ＮＴＴデータ通信が管理運用、但し、基本的には中継センターの役割のみ）の他、売上処理の代行まで行うＧＰＮ（ＶＩＳＡ系）、ＪＣＮ（ＪＣＢ系）、ＪＮＳ（ＭａｓｔｅｒＣａｒｄ系）等のネットワークセンタも現出しており、これらの構成に関しては、図 2-3を参照。

尚、参考までにＣＣＴの設置台数は、約７０千台である。（平成９年３月末）

＊各種端末の要件については、２.２『端末』に記述しており、そちらを参照願いたい。

(2) オフライン取引の業務フロー

オフライン取引が行われるＩＣカードと端末間並びにその運用廻りと、図 2-14における加盟店（Ｂ）と加盟店契約会社（Ｃ）間の③の流れについて記述する。

① ＩＣカード／端末間

カード発行者が会員へ加盟店に対する信用を供与し、実際の決済は後日会員口座からの自動振替するという後払い方式のクレジットカード業務において、安全なオフライン取引を実現する為には、プリペイド型電子マネーを利用する場合と異なり、ＩＣカードの真正性のチェックのみでは不十分で、より安全な取引とする為下記に示す様々な外部よりの攻撃への対応策として、更に幾つかの認証項目の追加が必要と考えられる。尚、各仕組みについての詳細は2.3.2『ＥＭＶのセキュリティ』を参照願いたい。

A. 偽造対策

ＩＣカードのチップそのものが保持しているタンパーレジスタンス機能のみならず、暗号技術を使用したカード自体の真正性の確認（カード認証）が有効であると考えられる。

尚、真正性のチェックの他現行磁気カードの取扱い同様、カードをリーダライタに通した時点で、カードの発行者を識別し、加盟店契約の締結の有無のチェックや国際ブランド間の取決めに基づいて取扱いが可能かどうかの判断並びにＩＣカードに書込まれたアプリケーションが何かを判別するアプリケーション選択が正しく行われることも必要である。

＊具体的なカード認証方式の事例としては、2.3.2『EMVのセキュリティ』を参照願いたい。

＊アプリケーションの選択や取扱いが可能なカードかどうかを正しく判断する為には、ＩＣカードや端末の仕様を決める以前の問題として2.4.1『アプリケーション識別子（ＡＩＤ）の付番管理について』に示したように、ＡＩＤの番号体系の整理と付番管理体制の確立が必要である。

B．なりすまし対策

下記の方法によりカードを提示した人物が、正当な所有者かどうかの真正性の確認（カード保有者認証）を行う。

a) ＰＩＮの入力

本人確認の為にＰＩＮを入力する。そのチェック方法は次のとおり。

ｉ．オフラインＰＩＮチェック

ＩＣカードと端末間のみでチェックを行う。

ii．オンラインＰＩＮチェック（参考）

クレジットカード業務の場合、リアルタイムオンライン送信によりカード会社センタホストでチェックを行う方法もある。

b) サイン

売上票に記入されたカード保有者のサインと、カード裏面に記載されているサインとの照合によるチェック。

＊現在の磁気カードでは、一部スーパーや百貨店の食料品売場にて、単純にサインを省略するだけのサインレス取引も行われているが、ＩＣカード化によるサインレス取引の堅確な運用の検討も必要である。

c) 上記ａ）、ｂ）の各種組合せ。

② 加盟店／カード会社間

Ａ．オフライン取引された売上データは、当然のことながら取扱った加盟店から加盟店契約を締結しているカード会社へ、原則事後ディレードバッチデータ伝送にて計上されない限り、加盟店側に売上代金の支払いができない。

尚、特にスタンドアロン型端末を使用している場合、既にＣＣＴで行われているのと同様、カード会社センタへの負荷を軽減する目的や処理の合理化・効率化の為に、図 2-14に示す⑨、⑩、⑪のフローのように、いずれかのネットワークセンタへ一括送信し、センタにてＭＴ／ＦＤ等を利用して、各発行者毎に仕分けて送ることも考えられる。

Ｂ、クレジットカード業務の場合、原則的には安全なオフラインの取引によるコストの低減や取引処理時間の短縮を図ることになるが、使い過ぎを防止する為に必要な途上与信管理上の観点や盗難・紛失カードの他人による悪用防止の要請から、ＩＣカード移行後もある一定のフロアリミット（信用販売限度額：１回の取引でカード会社の販売承認が必要な金額）を超えた場合には、現行通りオンラインリアルタイムでのオーソリゼーションは不可欠なものである。このオフライン／オンラインの判定方法としては、ＥＭＶ仕様にも規定されている下記３方式が考えられる。

a) フロアリミットチェック

１取引当りのフロアリミットを設定し、これを超えた場合カード会社ホスト側でオンラインリアルタイムオーソリゼーションを行う。

＊最も一般的な利用方法と考えられるが、加盟店の業種業態及び取扱い商品の内容（換金性の有無）や価格によってフロアリミット額の設定を行う必要がある。

b) ランダムチェック

取引額に関係なく、強制的に任意抽出してオンラインリアルタイムオーソリゼーションを行う。

＊実施するとすれば低価格で、且つ、購入者が自身で消費する他処分方法が見当たらない換金性も低い商品を主に取扱う業種業態の加盟店での運用に適していると考えられる。

c) ベロシティチェック

オフラインで連続処理できる回数を定め、それを超えた場合オンラインリアルタイムオーソリゼーションを行う。

＊ｂ）同様比較的低価格であるが、ｂ）の運用が適している加盟店より、纏まると不正利用の対象となるような危険性を有する商品を扱う業種業態の加盟店での運用に適していると考えられる。

2.4.2.2 オフライン／オンライン取引実現の為の要件と検討課題

クレジットカード業務の場合、信用を供与するという性質上当然オンライン取引も残り、且つオフライン取引をも安全に行う為には、以下のような要件や解決すべき検討課題あると考える。

(1) 導入目的の明確化

実現の為には、明確なビジネススキームの確立が要求され、ビジネスとして成立させる為には以下のような点について考慮・検討が必要である。

① 利用者（カード会員）・加盟店へのメリット供与

如何に利用者並びに加盟店のメリットを供与するか、何がメリットなのか？

A. 処理時間の短縮（狭義の利便性）

現金処理よりも早い取扱い処理の確立。

B. 処理コストの軽減

オフライン化による加盟店通信コストの軽減。

＊これらが達成できると、副次的に経費の削減のみならず加盟店側の人的対応の負担まで軽減できれば、顧客サービスの質的向上にも繋がることも予想され、利用者には更なるメリットが生じることにもなる。また、カード会社にとってもホストコンピュータの負荷も軽減されるなどのメリットあり、全体的にコスト低減の影響が出るものと思われる。

C. 付加価値サービスの創生（広義の利便性）

上記のような流れで、ある意味で対応が均質化されてくると、今まで以上の付加価値サービスでの競争となる。

＊多目的利用やロイヤリティプログラム（ポイントサービス）等

② 流通範囲の明確化（利便性提供に対する基本的な姿勢）

A．リアル／バーチャルのいずれかか、若しくは両方か

B．限られらたエリア（地域／建物等）のみ／国内のみ／全世界のどこまで流通

させる必要があるのか

＊これらの組合せも考えられる。

(2) ＩＣカード

現行の磁気カードからの移行を考えた時の要件と課題について記述すると共に、具体的な利用を考えると、ＩＣカード内にどこまでのどのような情報を書込むかを、各発行者自身で決定する必要あり。保持するデータの概要については、表 2-4に示すとおりであるが、検討の際の制約、考慮条件について考察した内容に関し記述する。

① 磁気ストライプの併用

端末インフラ整備並びに既存の磁気カードの切替えに最低でも３～５年位掛かると思われ、ＩＣチップと磁気ストライプの併用は当面の間必要と考えられる。しかしながら、磁気ストライプが存在する限り、セキュリティ上の要請である偽造防止に関しては抜け道を残す事となり、現行同様決済機能付きカードの相乗りを志向せざるを得ない状況においては、業界内で併用期間の閉塞の是非を含め、検討と合意が必要となる。

② 有効期限／会員番号／氏名のエンボス

基本的には磁気ストライプと同様、その存廃の是非や在り方については実際にクレジットカードを媒介として取引を行う会員・加盟店の立場での検討を加味する必要がある。

③ 鍵の変更とカードの更新について

現行のクレジットカードの場合カードデザイン変更や磁気フォーマットの変更が必要な時には、カードの有効期限が到来し更新カードを発送する際に更新カードを新方式のカードに順次切替える方法をとっている。例えば銀行系のカード会社が発行しているカードの有効期限は最長で３年であり、全切替え迄に３年掛かることになる。しかしながら、鍵についてはセキュリティ上の要請から、一般的に２年間位を目安で変更した方が良いとされているので、効率的な整合性のある仕組み作りの意味合いからも、ＩＳＤＮ回線の利用も含めたオンラインでの変更等に関する対応の検討が必要である。

④ カード及び端末コストの低減

単目的利用（それも業務要件を必要最小限に共通化する等により）のカードとすることも考慮すべきである。当初はこれで実施してみて、多目

的利用は次の段階で実施を検討するという考え方もあると考える。

また、他の発行者と端末を共用（クレジットカード業務の場合、現行複数のカード会社が重複して加盟店契約を締結し、端末やネットワークセンターで取扱いの可否や仕向先の判断を行っており、ＩＣカード移行後も当然継続されるべきである）する場合、調整が必要となる。

(3) 端末

端末の仕様に係わる基本的な要件については、2.2.1『クレジット端末』の章を参照願いたい。

ＩＣカードの普及・促進を考える時、最も重要な点であり、これを如何に可及的速やかに設置するかが最大のポイントとなり、共用化が必要になると考えられるが、その為には、共用する業種間・企業間での調整が必要と思われる。

具体的な設置方法や調整については、後述する2.5『端末インフラ整備アクションプラン』を参照願いたい。

(4) ネットワーク／通信手順

クレジットカード業務の場合、販売時点ではオフライン取引であっても、取引データは必ずオンラインのディレードバッチ伝送か、ＭＴ等によるバッチ処理が必要となる。

従って、ネットワーク網及びこれを統括運用するセンターの役割は重要である。以下関連する要件と課題を述べることとする。

① オフライン取引データの効率的な処理

ＩＣカード化により、オフライン取引が促進された場合、取引データ（売上）について何らかの形でディレードバッチ処理が必要となる。基本的に端末にオンライン機能がある限り、オンライン処理が望ましいが、この場合の考慮点としては以下のものがある。

Ａ．業務フロー図 2-14に示した、ネットワークセンターへ集中させ、各発行者毎にデータを区分けしてＭＴ若しくはファイル転送等で引き渡す。

Ｂ．取扱い加盟店・件数が増大した場合、１加盟店当りのバッチ伝送時間を短縮せざるを得ないので、データの圧縮技術やＩＳＤＮ回線の利用等の検討が必要である。

② 通信手順

端末～ネットワーク間、ネットワーク～カード会社ホスト間の通信手順を考える時のポイントは、以下のとおり。

Ａ．セキュリティの観点からは、カード～端末間で行われると同様タンパーレジスタンス機能を確保したものとすべき。

Ｂ．初期コストの低減の観点からは、カード会社にとってカードと端末のコスト負担の他に、通信手順の変更に伴うカード会社センタの大幅な手直しが必要となった場合、導入に対する大きな障壁になると考えられ、また、磁気からＩＣカードへの一斉切替えが現実の問題として不可能と思われるので、併用期間の対応も考え合わせると現行の通信手順のままとする方がよい。

＊この点に関しても十分な検討が必要である。

(5) セキュリティ

ＩＣカード利用の際のセキュリティに関しては、以下の点の整理が必要と考える。

① カード認証の方式

② 本人認証の方式

特に、サインについては、取扱い処理時間の短縮や売上票の枚数の削減によるコ　ストの低減にも寄与すると思われ、法的な証拠能力の問題と併せて検討を要する。

③ 端末のリスク管理

これらをどのように組み合わせて使うか、また、適用対象とする業種業態や取扱　い商品の性質（換金性の度合い）や価格についても整理する必要がある。

またその為にも、現行クレジットカード業界で使用している商品コードの見直し　も必要と考える。

現状は、ＣＡＴ共同利用システムの中でＰＯＳの商品区分の内大分類を流用した形で商品コードを決めて、オーソリゼーションの際の判断に役立てているが、大雑把であり新しい業種や買い廻り等の不正への対応を考えると、更にきめの細かい区分も必要と考える。

＊参考事例としては、ＶＩＳＡ／ＭａｓｔｅｒＣａｒｄではＩＳＯ８５８３にある加盟店業種コードをベース（大半は同じ）に対応している。

(6) 利用区分

オフライン取引を考える時の課題としては、業務フローの解説にあった分割払いをどうするか（割賦販売法上、取扱い金額の定めはなく、フロアリミットの設定如何では、対象となりうる）かが、大きな課題と考える。

(7) 運用廻り

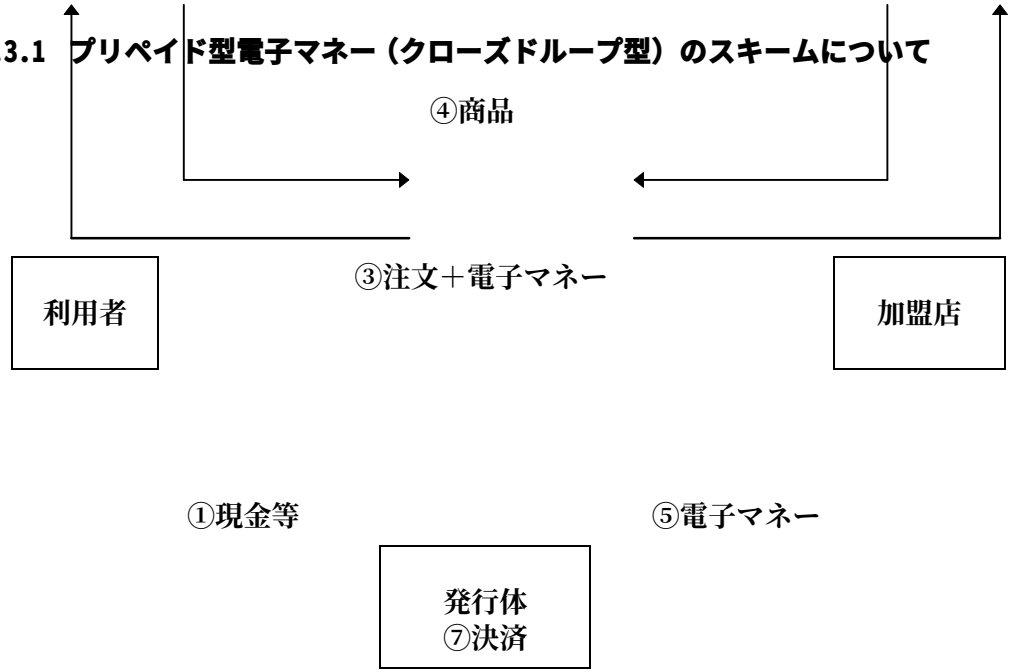
運用に関しても詳細に渡っての検討が必要であるが、検討課題に関しては2.5『端末インフラ整備アクションプラン』を参照願いたい。

2.4.3 プリペイド型電子マネーの取引の在り方についての検討

消費者・企業間の商取引において、ＩＣカードを使用したプリペイド型の電子マネーによる取引について、ＩＣカードのライフサイクルに着目して検討課題を整理する。

尚、MONDEXのようなオープンループ型の電子マネーもあるが、日本の場合所謂プリペイドカード法により発行残高管理と残高に応じて報告と供託が義務付けられているので、当面クローズドループ型の検討とした。また、2.3.1『ライフサイクルとセキュリティについて』の記述と重複する部分は省略した。

2.4.3.1 プリペイド型電子マネー（クローズドループ型）のスキームについて



②電子マネー　　⑥現金等

図 2-15 プリペイド型電子マネー（クローズドループ型）のスキーム

(1) 解説

図 2-15の内容は以下の通り。

①② 利用者は現金等と引換えに電子マネーを取得する。

③④ 利用者は物品やサービス購入の対価として電子マネーを使用する。

⑤⑥ 加盟店は電子マネーを現金化する。

⑦ 発行体において決済処理を行う。

2.4.3.2 検討課題

ＩＣカードの媒体そのもののライフサイクル全般に関わるセキュリティ要件については、2.3.1『ライフサイクルとセキュリティについて』を参照するものとし、ここではセキュリティ要件以外について整理するものとする。

(1) ＩＣ及びＩＣカードの設計・製造

ＩＣカードの媒体そのものに関しては、2.3.1『ライフサイクルとセキュリティについて』を参照。

(2) ＩＣカード（電子マネー）の発行（発行体←→利用者）

① ＩＣカードの媒体そのものに関しては、2.3.1『ライフサイクルとセキュリティについて』を参照。

② 媒体以外

A. 発行体関連

a) 発行済電子マネーの管理方法

発行済電子マネーの管理方法（期日管理、数量管理、残高管理、有効期限等）、発行に関する証拠能力確保等について

b) プール資金の運用方法

プール資金（電子マネーとの交換により受取った見合い資金）の運用方法、運用上限、供託金等の取扱い等について

c) 電子マネー発行システムの構築

電子マネー発行システム構築にかかるコスト、既存システムへのインパクト（投資額、運営コスト、対応期間等）等について

d) 発行体の具体的メリット

サービスの多様化、手数料収入（基本手数料、発行手数料等）、低利の資金調達、現物管理コストの削減、顧客の囲い込み等について

B. 利用者関連

a) 電子マネーと交換できる資金

預金からの振替を前提条件とするのか、現金・小切手等との交換は可能なのか、貸越の利用を認めるのか等、支払い猶予期間等

b) 誰でも

預金との振替の場合は、口座保有者に限定されることになる。

未成年者等の取扱いについて

c) どこでも

発行体に出向かなくても入手できるような方策等について

d) いつでも（電子マネーの取得可能な時間）

２４時間が理想だが、現在の預金引出しを勘案すると発行体の営業時間内に制限する等の割り切りについて

(3) ＩＣカード（電子マネー）の使用・運用

① 電子マネーの使用（利用者←→加盟店）

A. ＩＣカードの媒体そのものに関しては、2.3.1『ライフサイクルとセキュリティについて』を参照。

B. 媒体以外

a) 利用者関連

i．誰でも

電子マネーの保有者（名義人）と利用者の関係について

ii．いつでも（電子マネーの利用可能時間）

発行体とは無関係に使用できることが前提となると考えられる

iii．幅広く

国際間取引への利用について

iv．誤操作時の対応

誤操作をした場合の取り消し、戻し入れの方法について

b) 加盟店関連

i．加盟店の具体的メリット

売上の増加、現物管理コストの削減、代金回収期間の短縮等

② 電子マネーの現金化（加盟店←→発行体）

A．ＩＣカードの媒体そのものに関しては、2.3.1『ライフサイクルとセキュリティについて』を参照。

B．媒体以外

a) 発行体関連

i．電子マネーの受入れ

発行済電子マネーとの突合方法や受入れに関する証拠能力確保等について

ii．加盟店関連

iii．現金化の方法

預金との振替が前提か、現金との交換を認めるのか、分割・統合の取扱い、資金化の時期等について

ⅳ．いつでも（現金化可能時間）

２４時間が理想だが、現在の預金引出しを勘案すると発行体の営業時間内に制限する等の割り切りについて

(4) ＩＣカードの廃棄

ＩＣカードの媒体そのものに関しては、2.3.1『ライフサイクルとセキュリティについて』を参照。

(5) ライフサイクルに関わらない共通課題

① 決済関連

A．決済方法

請求方式による決済等について

B．金融機関間決済

決済インフラ構築にかかるコスト、対応期間等について

既存インフラ（全銀システム、日銀ネット、ＳＷＩＦＴ等）との整合性について海外との決済について（外為法）

C．決済リスク

発行体、金融機関等のデフォルト等について

D．決済手数料

決済手数料について

② 商品性

A．法的性格

電子マネーの法的性格について（出資法、紙幣類似証券取締法、前払式証票規制法等）

B．取得後の電子マネーの取扱い

消失・紛失等の取扱いや使い残しマネーの取扱い（現金化等）、預金保険の取扱い、差押えの取扱い等

C．通用力

通用力を高める方策（資格審査、許認可制度等の導入や届け出事項の洗い出し等）

D. 有効期間

分割・統合使用できることが望ましいが、安全性の観点から有効期間を設定する必要があると考えられるため、その設定方法等について

E. 利用金額の上限

利用金額の上限をいくらにするか

F. 外貨の取扱い

外貨の取扱いや外為法との関係について

G. 相互運用性の確保

各方式間の相互運用性の確保について

H. 利用環境

利用するネットワーク、機器、アクセスのためのインターフェイス、ソフトウェア等について

③ セキュリティ関連

A. ハード、ソフトの安全性

使用機器の安全性について

B. 犯罪防止と検出機能

発行体ホストへの侵入、なりすまし、情報漏洩、改ざん、マネーロンダリング、脱税等の犯罪防止と検出機能の付加について

C. リスク負担のルールの確立

リスク負担のルール作りについて

D. リスクカバー

上記ルールに基づく損害保険等の活用について

E. 認証の必要性

認証の必要性や、認証を行う場合のその範囲（項目、レベル等）、認証機関の設立等について

F．個人データ保護と追跡可能性

個人データ保護と追跡可能性について

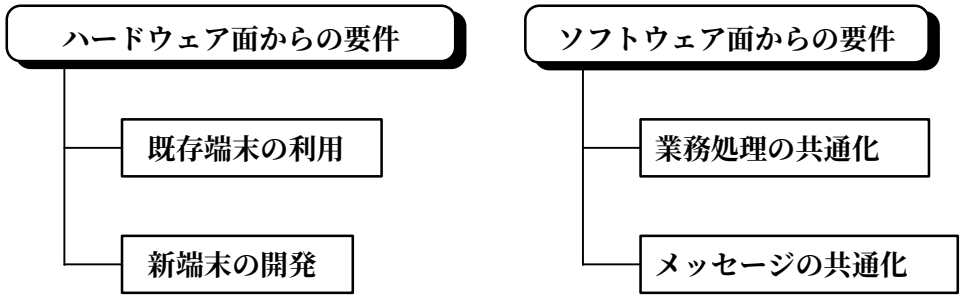
2.5 端末インフラ整備アクションプラン

ＩＣカードの取り扱いが可能なクレジット業務処理端末（以下端末と呼ぶ）の設置については、現状、各種電子マネーの実験において、それぞれの推進母体が限られた地域で専用の端末を置いてパイロットテストを行っているという状況にある。

しかし、今後のＩＣカードの一般化と普及には、端末やネットワークといったインフラを共用できる環境を整えることが、普及促進の上から重要な課題と考える。その為の指針として以下の通りＣＡＴ共同利用システムを参考にアクションプランを提言を試みることとするする。

2.5.1 店舗への導入を促進するための要件

店舗への端末の導入を促進するための要件としては次のような事柄があげられる。



2.5.1.1 ハードウェア面からの要件

導入促進の要件をハードウェア面から考えると、導入コストと新機種への入れ替えによる業務取り扱い方法の変更をいかに無くすかということがポイ

ントになる。

＊詳細は、2.2.1『クレジット端末』の章を参照願いたい。

(1) 既存端末へのＩＣカード・リーダライタの追加

より効率的に既存端末を利用できる方法を、メーカー、カード発行会社が中心となって研究していくことが急務と思われる。

(2) 新端末

売上票はＣＡＴ端末（共同利用を前提として開発された業界の標準仕様端末）用の売上票レイアウトに準拠したものとすることにより、加盟店側での事務取り扱いの変更を避けることができる。

2.5.1.2 ソフトウェア面からの要件

現行のＣＡＴ端末を例にとってみると、業務処理フローや端末メッセージの共通化による加盟店業務への統一的な取り扱い方の導入は、加盟店でのクレジット業務の効率化に大きな効果をもたらしたと言える。それはＩＣカード端末においても同様で、加盟店における運用負担の増加を抑制し、ひいては導入の促進をはかる有効な手段となりえる。

(1) 業務処理の共通化

クレジット処理においては、従来からの基本的な業務処理方法を継続することを原則として、加盟店における取り扱い方の変更を最小限にとどめるための検討が必要である。

ＩＣカードの機能を生かした取り扱いは当然のことながら出てくると思われるが、発行会社やブランドごとにその取り扱い方が極端に違うようでは、加盟店への導入促進にはマイナス要因となってしまうことは明白である。カード業界において、共通業務としてのＩＣカードを前提としたクレジット処理のあり方を早期にまとめ提示していく必要があろう。

(2) メッセージの共通化

端末に表示されるメッセージは、加盟店とカード会社、加盟店とカード利用者の重要な接点となるものである。それを共通化することは、加盟店業務にとって効率化をもたらす大きな事柄であると言える。

2.5.2 端末運用の課題

加盟店におけるＩＣカードの取扱いをスムーズに行っていく為には、次のような課題がある。

2.5.2.1 堅確な運用

(1) オペレーション指導

加盟店へのオペレーション指導は、端末設置カード会社としての基本的な責務である。業務処理やメッセージの共通化は、この面での設置カード会社の負担軽減にも、大いに貢献する事柄である。

(2) 売り上げデータ送信処理

オフラインによる売上処理が導入された場合、オフライン処理されて端末内にタンキングされている売上データを夜間等にカード会社に伝送する必要が出てくる。この処理は、加盟店とカード会社との精算という重要な要素を含んでおり、特に間違いがあってはならない処理である。そうした点からも、処理の自動化と正常終了したことを双方で確認できる手段を備えておくことが必要である。

(3) 売上票の保管

クレジット売上票の保管については、一括保管センターの利用等従来からの仕組みをそのまま利用するのがスムーズな運用を継続できる点から推奨できる。

電子マネー等による売上についての帳票をどう取り扱うかについては今後の検討を待つことになるが、できるだけ既存の仕組みの中で考えていくのが運用に混乱をきたさないのではないかと思われる。

2.5.2.2 イレギュラー対応

端末運用の出発点は、カードが正常に機能するかどうかである。カードが物理的に読めないという場合や、紛失や盗難といったカードの失効、与信枠という運用上の制限等によってそのカードが使用できないという局面が発生する。

(1) ＩＣカードの障害

ＩＣチップを搭載したクレジットカードは、磁気ストライプとの併用カードであっても、ＩＣカードでの取り扱いが優先される（磁気ストライプ内の設定情報により判定される）ようなソフト対応が望まれる。また、それと同時にＩＣチップそのものが物理的に読めないという状況にも配慮しておかなければならない。

その為には、磁気ストライプによる強制的な処理に移すことができる機能やその事実を発行会社に通知する機能を備えている必要がある。

(2) 紛失、盗難カードの取り扱い

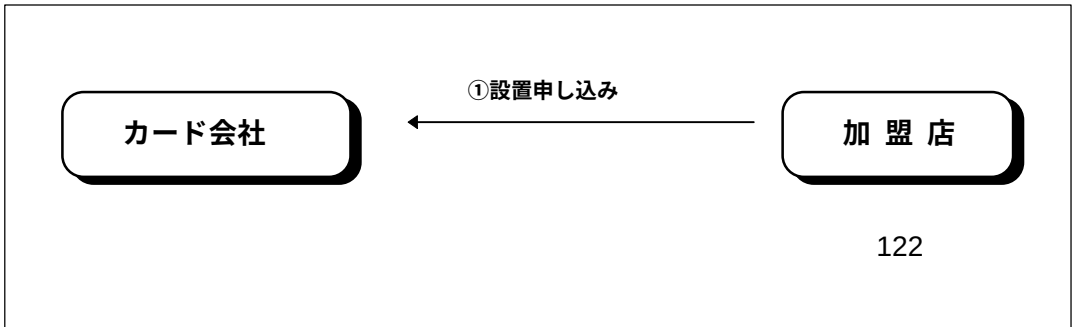
ＩＣカードに期待する機能の中で、セキュリティー面での機能への期待は非常に大きい。単にＩＣチップを搭載したカードが作りにくいということだけでなく、端末にカードを挿入した際、無効カードであればその情報を書き込んで、以降オフラインでもカードの無効チェックによって使えなくすることも可能と思われる。

2.5.3 端末管理

端末を共同利用していく場合は、端末設置会社はその端末を利用するカード会社各社に設置情報を知らせる必要が出てくる。その作業を各々のカード会社が各々のやり方でやりはじめると非常に非効率なものになってしまう。作業をスムーズに間違いなく行っていくには、図 2-16に示す現在ＪＣＣＡが中心になって運営している共同端末管理システムにのせるか、それに準じた運用とするのが必要と考える。

従って、端末識別番号のような基礎的な情報については既存の体系に沿ったものの中で決めていくことが必要である。

また、ＩＣカード特有の考慮点については、具体的な内容が固まった時点で既存システムの変更の必要性を検討し、場合によっては、ＪＣＣＡとの調整も考慮していくことが出てくると思われる。



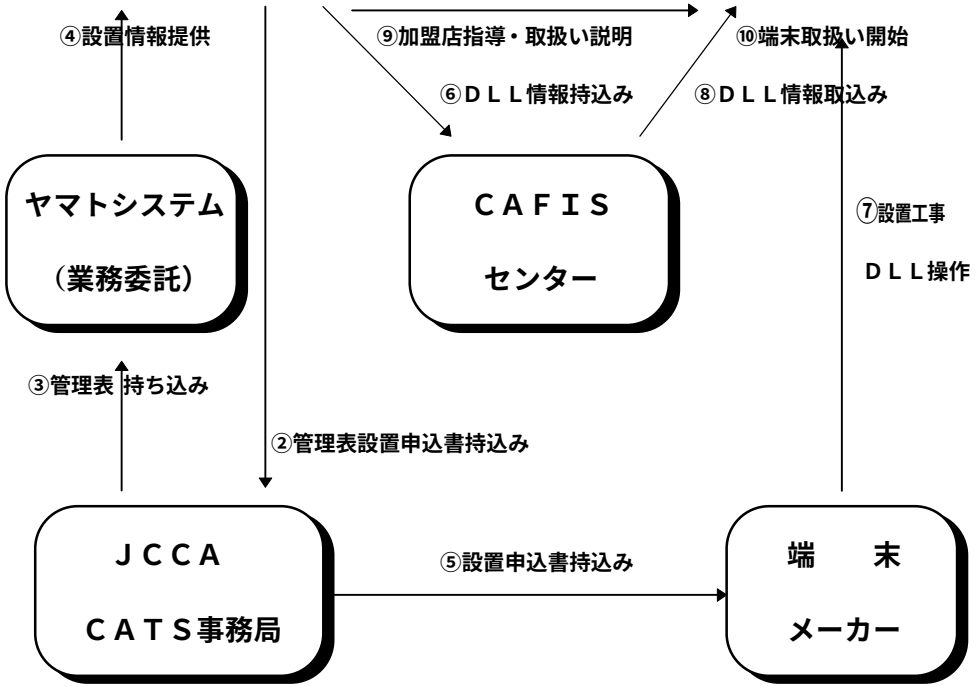


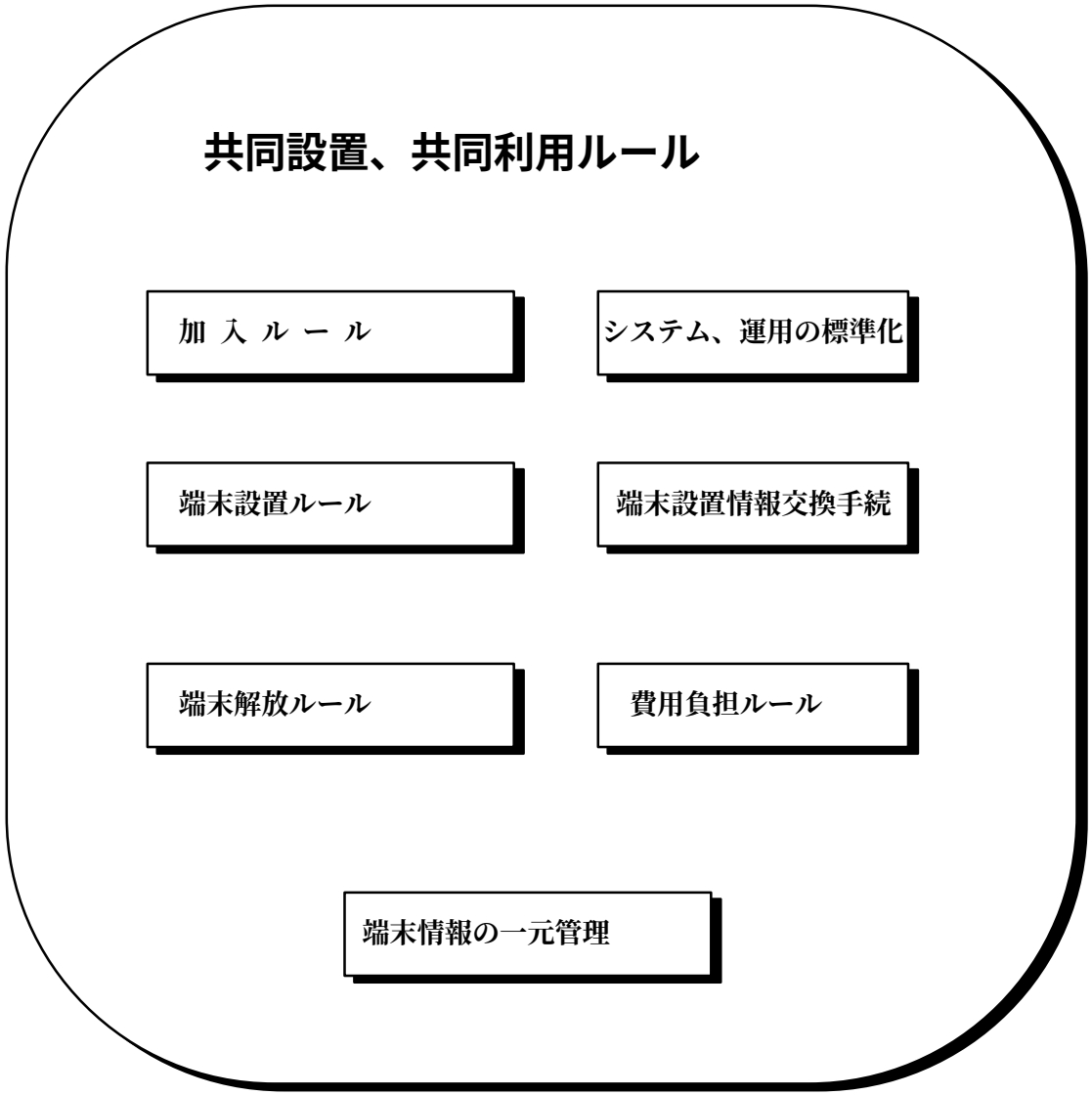
図 2-16　共同端末管理システム

2.5.4 端末の共同設置・共同利用のための機構

これまで端末インフラ整備の必要性や考慮点・手法等に関し述べたが、これらを具現化する為には、端末仕様、端末設置推進策、円滑な運用方法、仕様のメンテナンス等を協議する為の枠組みが必要となってくる。

2.5.4.1 必要な取決め

共同設置・共同利用を推進していく為には、以下のような基本原則や運用の為の取決めが必要であり、その枠組みの中で円滑な運用を図っていくことが重要である。



2.5.4.2 運用組織

前項のような原則に基づいて運用していく為の組織として、以下のようなものが考えられる。

(1) 参加プレイヤー

カード発行企業（クレジットカード会社／銀行／プリペイドカード発行企業）、ＩＣカード／端末メーカー、ネットワーク業者、各種事務処理会社が考えられ、この他にシステムの円滑な運用を管理する管理事務局が主なものと考える。

(2) 組織

① ＜協議会＞

具体的な運営方針や各仕様等に関して議決する機関。

② ＜管理事務局＞

円滑な運営管理の他、並列的に設置する下記各委員会の運営の補助も行い、機構全体の円滑な運営を推進する機関。

構成としては、事務的な処理の専従者（主としてカード発行者側からが望ましい）と仕様のメンテナンスや技術開発担当者（メーカーより）

③ ＜委員会＞

Ａ．制度／運用検討委員会

Ｂ．システム委員会

④ サポーター：ネットワーク業者／事務処理会社等

主に以下の業務を行う。

Ａ．加盟店並びにカード会社固有情報の登録管理／登録業務の代行

Ｂ．端末へのＤＬＬ管理業務

Ｃ．オーソリゼーション等の中継／代行

D．売上処理代行並びにデータの還元

E．設置端末情報の管理：新規／変更／抹消情報の登録受付け並びに配信

F．売上控え等の保管管理（必要に応じて）

3 非接触型ＩＣカードの現状調査

3.1 非接触型ＩＣカードの特長

ＩＣカードの普及には、広範囲で多種多様な利用拠点に、リーダライタ機器を導入しなければならないので、大規模な初期投資が必要である。磁気カードからＩＣカードへ移行する場合は、磁気カードとの併用期間が必要であり、リーダライタの共用化が検討可能な接触型ＩＣカードが選択されるであろう。しかし、導入に際して、移行の制約がない場合、あるいは、非接触型ＩＣカードの特長を生かせる分野では、一気に非接触型ＩＣカードの利用を検討することになる。

3.1.1 非接触型ＩＣカードの利点

(1) 安価なインフラ費用

非接触型ＩＣカードのリーダ・ライタには、駆動装置が不要であり、また精緻さを要するカードの位置合わせ機能が不要等により、設計・製作が容易である。このため、堅牢で安価な端末機器を作成でき、保守費用の削減が期待できる。

(2) 長い使用期間

非接触型ＩＣカードは、科学的な損傷、湿度や摩耗などに強いので、接触型ＩＣカードに比べ、長期に使用可能であり経費節減になる。

(3) 高い機密性

ＣＰＵをカプセル化するため、非接触型ＩＣカードのセキュリティシステムを迂回することができず、機密性が確保される。

(4) ラベルの活用

非接触型ＩＣカードの場合、カード表面をラベル用に活用できる。これは、複数企業あるいは複数アプリケーションの多目的カード作成に有用である。

(5) 多様な適用業務

高速道路の料金所での利用環境では、恒常的に振動、塵や埃などがある。このような悪影響では、精緻な位置合わせが必要な接触型ＩＣカード

では運用が困難である。悪環境での運用に強い非接触型ＩＣカードは、操作が容易なため、どのような環境下でも利用可能である。

3.2 非接触型ＩＣカード利用ガイドライン策定検討項目

非接触型ＩＣカードを採用・導入検討する際に、参考となる非接触型ＩＣカード利用ガイドラインを平成９年度末に策定する予定である。表 3-1は、ガイドライン策定に際して検討すべき項目を掲げた。平成８年度では、検討すべき項目の一部を調査し、成果物（αバージョン）としてまとめたので次葉以下に報告する。

表 3-1 検討に当たっての項目

	検　討　項　目
（1）	非接触型ＩＣカードの位置付け
（2）	接触型と非接触型ＩＣカードの比較
（3）	非接触型ＩＣカードの普及課題（電波法規則等）
（4）	非接触型ＩＣカードのアプリケーション分野とその市場規模
（5）	非接触型ＩＣカードの標準化動向
（6）	非接触型ＩＣカードの相互運用性
（7）	非接触型ＩＣカードのセキュリティ
（8）	非接触型ＩＣカードの実証実験及び利用事例
（9）	非接触型ＩＣカード関連機器メーカー

3.3 非接触型ＩＣカードの種類

非接触型ＩＣカード検討WG（ＳWG２）で対象としている非接触型ＩＣカードの種類を図 3-1に示す。

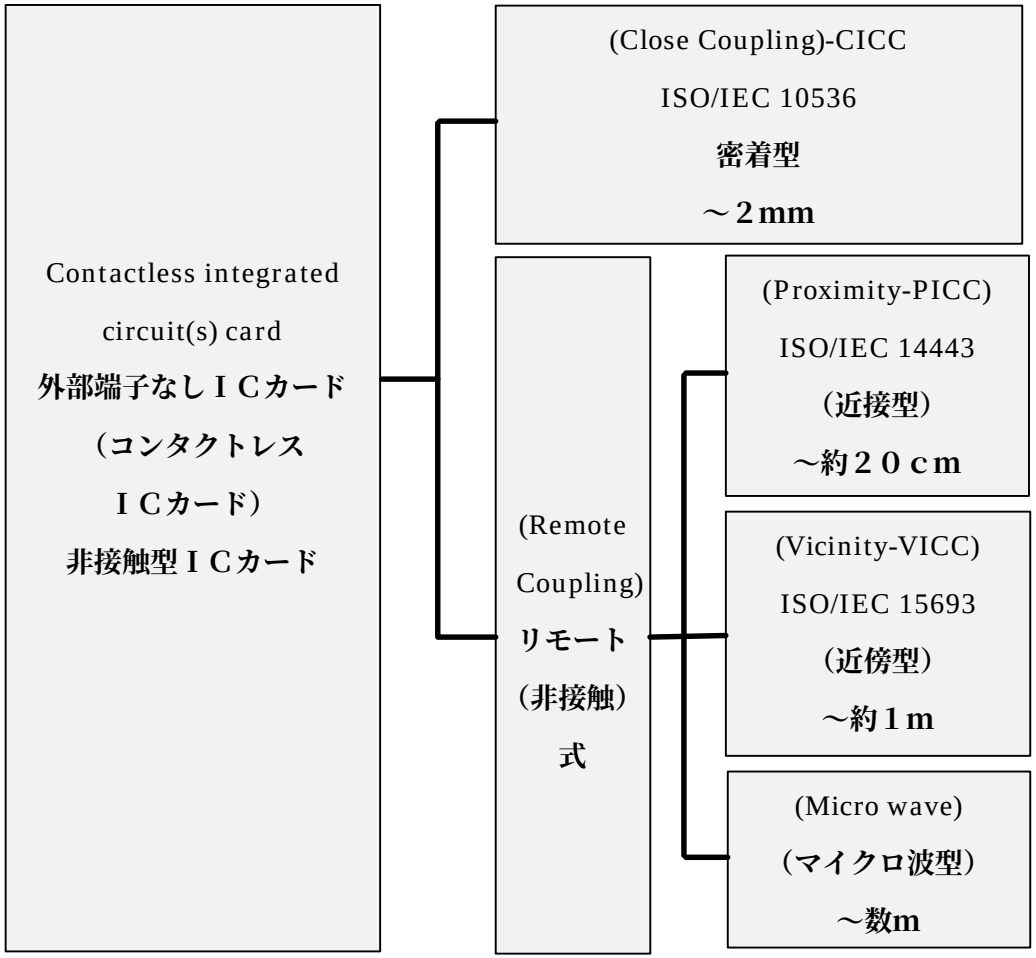


図 3-1 非接触型ＩＣカードの種類

● 図 3-1（　　）内の英語はＩＳＯで審議中、（　　）内の日本語表記は案であり、今後見直しがあり得る。（１９９７年２月、ISO/IEC JTC1/SC17/WG8 ロンドン会議にて開催された会議内容を基に作成した）

3.3.1 非接触型ＩＣカードの分類表

ＩＳＯ国際会議での進捗状況を反映させ、非接触型ＩＣカードに対する定義・分類について統一化した分類表（表 3-2）をＥＣＯＭ　ＷＧで作成し、幅広く世間に広めている

表 3-2　非接触型ＩＣカードの分類表

分　　類	Contactless integrated circuit(s) card 外部端子なしＩＣカード（コンタクトレスＩＣカード）				
種　　類	(Close coupling)－CICC 密着型		(Remote Coupling) リモート（非接触）式		
			(Proximity-PICC) （近接型）	(Vicinity-VICC) （近傍型）	(Micro wave) （マイクロ波型）
国 際 規 格	ISO/IEC 10536		ISO/IEC 14443	ISO/IEC 15693	－
通信結合方式	(Capacitive Coupling) 静電結合方式	(Inductive Coupling) 電磁誘導方式			
伝 送 距 離	1mm	1.5～2mm	1cm～約 20cm	～約 1m	～数 m
電 池 有 無	無	無	無	有・無	有・無
アンテナ方式	1or2ｺｲﾙ	1or2ｺｲﾙ	－	－	－
周 波 数 (電波領域)	4.91MHz	4.91MHz	13.56MHz (短波)	＜135KHz (長波)	2.45GHz (ﾏｲｸﾛ波)
ＣＰＵ有無	有・無	有・無	有・無	有・無	有・無
ﾒﾓﾘ種類・容量					

アクセス方式	読・書	読・書	読・書	読・書	読・書
カードの形状	54mm×85.6mm	54mm×85.6mm	54mm×85.6mm	54mm×85.6mm 可	54mm×85.6mm 可
カードの厚さ	0.76mm±10%	0.76mm±10%	0.76mm±10%	0.76mm±10%	1mm 以上

*（　　）内の英語は ISO 審議中、（　　）内の日本語表記は案であり、今後見直しがあり得る。

* 本資料は、1997 年２月、ISO/IEC JTC1/SC17/WG8 ロンドン会議にて開催された標準化会議内容を基に作成。

ＥＣＯＭ　ＩＣカードＷＧで作成した表 3-2の統一分類表に基づいて、ＩＣカードＷＧに参加されている企業、及びＩＣカード取引システム研究開発事業組合、事務機械工業会国際標準化検討ＷＧ８に参加されている事業者を対象に、非接触型ＩＣカードの販売、及び開発予定製品に関するアンケート調査を実施した。

統一分類表に基づいた資料作成のため、各社製品の仕様状況が、同一判断で確認出来る様になった。

回答を得た企業名と、販売・開発状況一覧を表 3-3に、各社の詳細内容を表 3-4にまとめた。尚、ＩＣカードＷＧでは、現在も情報の提供を受け付けている。

表 3-3　販売・開発状況一覧（９７年１月現在）

松下電池工業（株）	その他	開発中
三菱電機（株）	遠隔型	開発中
	独自仕様	発売中
（株）東芝	その他	発売中
（株）デンソー	近接型	発売中
	遠隔型	開発中
	遠隔型	開発中
昌栄印刷（株）	遠隔型	97 年 4 月発売予定
	遠隔型	発売中
シーメンス（株）	遠隔型	発売中
オムロン（株）	その他	開発中
ソニー（株）	遠隔型	発売中
（財）ﾆｭｰﾒﾃﾞｨｱ開発協会	近接型	開発中(97 年 10 月ｻﾝﾌﾟﾙ)
凸版印刷（株）	その他	発売中
	その他	発売中
レイコムジャパン(株)	遠隔型	発売中
	遠隔型	97 年３月発売予定
（株）ｴｲｱｲﾃｸﾉﾛｼﾞｰ	その他	発売中
	その他	発売中
	その他	開発中
	その他	発売中
	遠隔型	発売中
	その他	開発中
兼松マルチテック（株）	その他	発売中
（株）CSK	近接型	発売中
	近接型	発売中

表 3-4 非接触型ＩＣカードの詳細一覧（1）

会社名	松下電池 1	三菱電機 1	三菱電機 2	東芝	デンソー 1	デンソー 2	デンソー3
回答日	ー	ー	ー	ー	ー	ー	ー
製品型名	未定	MF5201	MF5103B	トスカード	ｺﾝﾀｸﾄﾚｽ	ﾏｲｸﾛ波	ー
発売日	開発中	開発中	発売中	発売中	発売中	開発中	開発中
種類	その他	14443	その他	その他	ー	ﾏｲｸﾛ波	14443
通信結合方式	電磁誘導	電磁誘導	電磁誘導	電磁誘導	静電結合	ﾏｲｸﾛ波	電磁誘導
仕様	その他	その他	その他	その他	10536	その他	14443
					1/2/3/4		
伝送距離	～20cm	～20cm	～1m	～50cm	ー	～1m	～20cm
電池有無	無	無	有	有	無	有	無
アンテナ方式	１コイル	１コイル	１コイル	１コイル	１コイル	その他	１コイル
						ﾏｲｸﾛｽﾄﾘｯﾌﾟ	
周波数	ー	14443準拠	14443準拠	10536準拠	10536準拠	ﾏｲｸﾛ波	14443準拠
		その他	その他	その他	3.57MHz	2.4GHz	13.56MHz
		125KHz	～6KHz	400Hz			
		～4MHz					
伝送速度	≦100kbps	≦100kbps	≦100kbps	≦10kbps	≦10kbps	≦100kbps	>100kbps
	25kbps		25.6Kbps				
ＣＰＵ有無	無	無	有	無	有	無	無
メモリ種類	EEPROM	EEPROM	SRAM	SRAM	EEPROM	SRAM	EEPROM
ﾕｰｻﾞﾒﾓﾘ容量	512Byte	512Byte	320Byte	25Byte	3k,8kByte	40Byte	128～2k
アクセス方式	ﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗｲﾄ
カードの形状	５４ｘ８５．６	５４ｘ８５．６	５４ｘ８５．６	５４ｘ８５．６	５４ｘ８５．６	５４ｘ８５．６	５４ｘ８５．６
カードの厚さ	0.76mm	0.76mm	その他	その他	0.76mm	その他	0.76mm
			2.2mm	1.5mm		1.0mm	
暗号機能	無	無	その他	無	DES	その他	その他

表 3-4 非接触型ＩＣカードの詳細一覧（２）

会社名	昌栄印刷１	昌栄印刷2	シーメンス	オムロン	ソニー	ニュー協	凸版印刷１
回答日	ー	ー	ー	ー	ー	ー	ー
製品型名	HFM16KCC	LFM4KCC	SLE44R35	未定	ＲＣ－Ｓ１０２	ー	MIRO
発売日	開発中	発売中	発売中	開発中	発売中	開発中	発売中
種類	14443	14443	14443	その他	14443	10536	その他
通信結合方式	電磁誘導	電磁誘導	電磁誘導	電磁誘導	電磁誘導	電磁誘導	電磁誘導
仕様	14443	10536	14443	10536	14443	10536	ー
		1/		1/		1/2/3/4	
伝送距離	～20cm	～10cm	～20cm	～20cm	～20cm	～1mm	～20cm
電池有無	無	無	無	無	無	無	無
アンテナ方式	２コイル	１コイル	１コイル	２コイル	１コイル	２コイル	１コイル
周波数	14443準拠	10536準拠	14443準拠	10536準拠	14443準拠	10536準拠	14443準拠
	13.56MHz	その他	13.56MHz	その他	13.56MHz	4.91MHz	その他
	その他	125kHz		530kHz			125Hz
	通信3.39Hz						
伝送速度	>100kbps	その他	>100kbps	≦10kbps	>100kbps	≦10kbps	4kbps
	105.9kbps	7812bps			２５０kbps	19kbps	
ＣＰＵ有無	有	有	無	無	無	有	無
メモリ種類	F-RAM	F-RAM	EEPROM	EEPROM	EEPROM	EEPROM	EPROM
ﾕｰｻﾞﾒﾓﾘ容量	2kByte	496Byte	1kByte	254Byte	1.25kByte	8kByte	5Byte
アクセス方式	ﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ｲﾝﾘｰﾄﾞ・ﾗ	ﾘﾄﾞｵﾝﾘｰ
カードの形状	５４ｘ８５．６	５４ｘ８５．６	５４ｘ８５．６	５４ｘ８５．６	５４ｘ８５．６	５４ｘ８５．６	54X85.6
カードの厚さ	0.76mm	0.76mm	0.76mm	0.76mm	0.76mm	0.76mm	0.76mm
暗号機能	RSA	無	その他	無	その他	DES	無
					独自方式	RSA	

表 3-4 非接触型ＩＣカードの詳細一覧（３）

会社名	凸版印刷２	ﾚｲｺﾑｼﾞｬﾙ1	ｺﾑｼﾞｬﾙ2	ﾔｴｲｱｲﾃ１	ｵﾉｲｱｲﾃﾞ	ｵﾉｲｱｲﾃﾞ	ｵﾉｲｱｲﾃﾞ	ｸﾉ
回答日	ー	961219	961219	970127	970127	970127	970129	
製品型名	ｺﾝﾀｸﾄﾚｽ	LFｼﾘｰｽﾞ	HFｼﾘｰｽﾞ	NDR06	MIROAT45	MIROAT15	TGI-LM	
発売日	発売中	発売中	開発中	発売中	発売中	開発中	発売中	
種類	その他	14443	14443	その他	その他	その他	その他	
通信結合方式	電磁誘導	電磁誘導	電磁誘導	電磁誘導	電磁誘導	電磁誘導	電磁誘導	
仕様	ー	14443	14443	その他	その他	その他	その他	
伝送距離	～5mm	～20cm	～20cm	～1m	～10cm	～3cm	～12cm	
電池有無	無	無	無	有	無	無	無	
アンテナ方式	その他	１コイル	２コイル	２コイル	１コイル	１コイル	１コイル	
	3コイル							
周波数	10536準拠	その他	14443準拠	ー	その他	その他	その他	
	その他	<135kHz	13.56MHz		<135kHz	<135kHz	4MHz	
	4.91MHz							
	2.4576MHz							
伝送速度	38400bps	≦10kbps	>100kbps	≦1kbps	≦10kbps	≦10kbps	≦10kbps	
				≦10kbps	4kbps		<10kbps	
ＣＰＵ有無	有	無	有	無	無	無	無	
メモリ種類	EEPROM	F-RAM	F-RAM	EEPROM	その他	その他	EEPROM	
					ﾏｽｸ	ﾏｽｸ		
ﾕｰｻﾞﾒﾓﾘ容量	0.5KB～	2kByte	2kByte	1D-3Byte	1D-5Byte	1D-5Byte	240Byte	
	32kByte							
アクセス方式	ﾘｰﾄﾞ・ﾗｲ	ﾘｰﾄﾞ・ﾗｲ	ﾘｰﾄﾞ・ﾗｲ	ﾘｰﾄﾞｵﾝﾘｰ	ﾘｰﾄﾞｵﾝﾘｰ	ﾘｰﾄﾞｵﾝﾘｰ	ﾘｰﾄﾞ・ﾗｲﾄ	
カードの形状	54X85.6	54X85.6	54X85.6	54X85.6	54X85.6	54X85.6	54X85.6	
カードの厚さ	その他	0.76mm	0.76mm	その他	0.76mm	0.76mm	0.76mm	
	2.6mm			2.7mm				
暗号機能	DES	無	その他	無	無	無	無	
	その他		CPU対応					

表 3-4 非接触型ＩＣカードの詳細一覧（４）

会社名	ｴ ｲ ｱ ｲﾗﾃ	ｴﾉｲ ｱ ｲﾁﾃ	兼松ﾏﾙﾁ１	CSK-1-1	CSK-1-2
回答日	970127	970131	970128	970218	970218
製品型名	C-SM1	HITAG	1KCARDB	PORTRAC	EYECON
発売日	発売中	開発中	発売中	発売中	発売中
種類	14443	その他	その他	10536	10536
通信結合方式	電磁誘導	電磁誘導	電磁誘導	電磁誘導	電磁誘導
仕様	14443	その他	その他	ー	10536
					1/
伝送距離	～10cm	その他	～50cm	～20cm	～20cm
電池有無	無	無	無	無	無
アンテナ方式	１コイル	１コイル	１コイル	１コイル	１コイル
周波数	14443準拠	その他	その他	10536	10536
	13.56MHz	<135kHz	<135kHz	13.56MHz	13.56MHz
伝送速度	>100kbps	ー	≦10kbps	≦10kbps	≦100kbps
	106kbps				106bps
ＣＰＵ有無	無	無	無	有	有
メモリ種類	EEPROM	EEPROM	EEPROM	EEPROM	EEPROM
ﾕｰｻﾞﾒﾓﾘ容量	720Byte	256Byte	130Byte	128～	1k～
				16kByte	8kByte
アクセス方式	ﾘｰﾄﾞ・ﾗｲ	ﾘｰﾄﾞ・ﾗｲ	ﾘｰﾄﾞ・ﾗｲ	ﾘｰﾄﾞ・ﾗｲ	ﾘｰﾄﾞ・ﾗｲﾄ
カードの形状	54X85.6	54X85.6	その他	その他	54X85.6
			54X86	57X88	
カードの厚さ	0.76mm	その他	その他	その他	0.76mm
		1mm以下	0.8mm	10mm	
暗号機能	その他	その他	その他	DES	DES
	独自	独自		RSA	RSA

3.4 各種カードに期待される特長

カードの種類、市場の要求、相互の関連から、推奨カードが選択出来る『民間市場の各分野に於ける推奨されるカード』一覧表（表 3-5）を策定した。カードの特長と市場の要件から推奨されるカードの選択が簡単に抽出出来るガイドラインとして策定している。

『各カードの特長』一覧表（表 3-6）は、非接触型ＩＣカード、接触型ＩＣカード、磁気カード、各カードが保有している機能的な特長をまとめ、『民間市場の各分野に於ける要件の重要度』一覧表（表 3-7）は、市場がカードに期待する要件をまとめたものである。

掲載資料の全ては、非接触型ＩＣカードWG（ＳWG 2）で作成したガイドライン案であり、今後意見を吸収しながら資料に反映していく。

表 3-5 民間市場の各分野に於ける推奨されるカード

◎：より適している ／ ○：適している ／ △：制限はあるが利用可能 ／ ×：制限あり

推奨カード / 市　場	非接触ＩＣカード			接触ＩＣカード	磁気カード
	ISO/IEC １０５３６	ISO/IEC １４４４３	ISO/IEC １５６９３	ISO/IEC ７８１６	ISO/IEC ７８１１
	密着型	（近接型）	（近傍型）		
交通分野					
乗車券、定期券(電車、ﾊﾞｽ、飛行機、船等)	×	◎	×	×	△
有料道路料金課金カード	◎	○	○	△	△
金融・流通・サービス分野					
キャッシュカード	◎	○	×	◎	○
クレジットカード	◎	○	×	◎	○
電子財布	◎	○	×	◎	×
プリペイドカード	◎	○	×	◎	△
ポイントカード	○	○	×	○	○
自販機カード	○	◎	×	△	△
駐車場カード	△	◎	○	△	△
通信分野					
公衆電話用カード	◎	○	×	○	△
移動体通信用カード	○	○	×	○	×
ネットワークキーカード	○	○	×	○	×
衛星放送用カード	○	○	×	○	×
アミューズメント分野					
入園チケット(テーマパーク等)	×	◎	○	×	△
パチンコカード	○	○	×	△	×
スキー場のリフトカード	×	◎	○	×	×
フィットネスクラブ会員カード	○	○	△	○	△
レース着順判定（ゼッケン）	×	◎	◎	×	×
公営ギャンブルカード	○	○	×	○	△
ＩＤ分野					
社員証	○	◎	△	○	△
学生証	○	◎	△	○	△
物流・ＦＡ分野					
宅配荷物管理カード	○	○	×	△	×
セキュリティ分野					
電子キー	○	○	×	○	△

注) ・推奨カードを決定する場合、上記は目安であり、ＣＰＵの有無及びメモリ容量等を考慮する必要あり。

表 3-6 各カードの特長

◎：より適している ／ ○：適している

カードのタイプ / カードの特長	ISO/IEC １０５３６		ISO/IEC １４４４３	ISO/IEC １５６９３	－	ISO/IEC ７８１６	ISO/IEC ７８１１
	非接触ＩＣカード（密 着 型）		（近 接 型）	（近 傍 型）	（マイクロ波型）	接触ＩＣカード	磁気カード
	静電結合方式	電磁誘導方式	1cm～20cm	1m 程度	数 m		
決済機能対応が可能	◎	◎	○			◎	
カードの価格							◎
高セキュリティ	◎	◎	○			◎	
高速処理（処理速度）			◎	◎	◎		○
耐環境性に優れている	◎	◎	◎	◎	◎		
メンテナンス性が優れている	◎	◎	◎	◎	◎		
耐静電気に優れている	◎	◎	◎	◎	◎		○
耐振動に優れている	○	○	◎	◎	◎		
電池不要	◎	◎	◎	◎		◎	◎
電磁ノイズ	○	○				◎	◎
メモリ容量	◎	◎	◎	○	○	◎	
リードライト機構の単純性	○	○	○	○	○	◎	

・

表 3-7　民間市場の各分野に於ける要件の重要度

［要件の重要度 ： ◎ ＞ ○ ＞ △ ＞ × ］

要　件 市　場	決済機能が必要	ｶｰﾄﾞの低価格化	高ｾｷｭﾘﾃｨ	高速処理(処理速度)	耐環境性に優れている	ﾒﾝﾃﾅﾝｽ性が優れている	耐静電気に優れている	耐振動に優れている	携帯性	電磁ﾉｲｽﾞ
交通分野										
乗車券､定期券(電車､ﾊﾞｽ､飛行機､船等)	◎	◎	◎	◎	◎	◎	○	◎	◎	○
有料道路料金課金カード	◎	△	◎	○	○	◎	○	◎	△	○
金融・流通・サービス分野										
キャッシュカード	◎	◎	◎	○	△	◎	△	×	○	○
クレジットカード	◎	◎	◎	○	△	◎	△	×	○	○
電子財布	◎	◎	◎	○	△	◎	△	×	○	○
プリペイドカード	◎	◎	◎	○	△	◎	△	×	○	○
ポイントカード	×	○	△	△	△	○	△	×	△	○
自販機カード	◎	○	◎	○	◎	◎	○	△	○	○
駐車場カード	◎	○	◎	○	◎	○	○	△	○	○
通信分野										
公衆電話用カード	◎	◎	◎	○	◎	◎	○	△	○	○
移動体通信用カード	○	○	○	○	◎	◎	○	○	△	○
ネットワークキーカード	○	△	◎	○	○	○	○	△	△	○
衛星放送用カード	○	△	○	△	△	◎	○	×	×	○
アミューズメント分野										
入園チケット(テーマパーク等)	◎	○	◎	◎	◎	○	○	△	△	○
パチンコカード	◎	◎	◎	○	○	◎	◎	×	△	○
スキー場のリフトカード	◎	○	◎	◎	◎	○	△	×	△	○
フィットネスクラブ会員カード	×	△	×	△	△	△	△	×	△	△
レース着順判定（ゼッケン）	×	△	×	◎	◎	△	○	○	△	△
公営ギャンブルカード	◎	○	◎	○	○	○	○	×	△	○
ＩＤ分野										
社員証	△	○	○	○	○	○	△	×	○	○
学生証	△	○	○	○	○	○	△	×	○	○
物流･ＦＡ分野										
宅配荷物管理カード	×	○	△	○	◎	○	○	○	△	○
セキュリティ分野										
電子キー	×	△	◎	○	◎	○	△	△	○	○

3.5 非接触型ＩＣカードの標準化

3.5.1 非接触型ＩＣカードの標準化動向

非接触型ＩＣカードの標準化は、接触型ＩＣカードに比べ幾分遅れていたが、近年各国の標準化要望が強くなり標準化が進展している。

3.5.1.1 標準化の進捗状況

(1) Ｃｌｏｓｅ Ｃｏｕｐｌｉｎｇ 密着型 ＩＣカード（ＩＳＯ／ＩＥＣ ＪＴＣ１／ＳＣ１７／ＷＧ８／ＴＦ１）

１０５３６ Ｐａｒｔ １　ＩＳ化　物理的特性

１０５３６ Ｐａｒｔ ２　ＩＳ化　結合領域の寸法と位置

１０５３６ Ｐａｒｔ ３　ＩＳ化　電気信号とリセット手順

１０５３６ Ｐａｒｔ ４　ＣＤ　初期応答と伝送プロトコル

(2) Ｒｅｍｏｔｅ Ｃｏｕｐｌｉｎｇ （近接型）ＩＣカード（Proximity）（ＩＳＯ／ＩＥＣ ＪＴＣ１／ＳＣ１７／ＷＧ８／ＴＦ２）

１４４４３ Ｐａｒｔ １　ＣＤ　物理的特性

１４４４３ Ｐａｒｔ ２　ＷＤ　電波インターフェース

１４４４３ Ｐａｒｔ ３　－　電気信号と伝送プロトコル

(3) Ｒｅｍｏｔｅ Ｃｏｕｐｌｉｎｇ （近傍型）ＩＣカード（Vicinity）（ＩＳＯ／ＩＥＣ ＪＴＣ１／ＳＣ１７／ＷＧ８／ＴＦ３）

１５６９３ Ｐａｒｔ １　－　Physical characteristics

１５６９３ Ｐａｒｔ ２　－　RF power and signal(bit)

１５６９３ Ｐａｒｔ ３　－　Initialization and anti-collision byte coding

１５６９３ Ｐａｒｔ ４　－　Transaction protocols

１５６９３ Ｐａｒｔ ５　－　Registration

(WD:Working Draft　CD:Committee Draft　DIS:Draft International Standerd　IS:International Standerd)

3.5.1.2 国際標準（ＩＳ化）までの目標予定

ＩＳＯ／ＩＥＣ １０５３６：Ｃｌｏｓｅ Ｃｏｕｐｌｉｎｇ 密着型は、ＩＳ化が最も進

んでおり、今年度中にＩＳ化の予定になっている。

ＩＳＯ／ＩＥＣ １４４４３：Ｐｒｏｘｉｍｉｔｙ（近接型）は、通信距離が２０ｃｍ程度までで、今後活用範囲の拡大が期待される標準であるが、着手の遅れから幾分標準化は遅れる。

ＩＳＯ／ＩＥＣ １５６９３：Ｖｉｃｉｎｉｔｙ（近傍型）は、これから標準化作業に着手される予定。

表 3-8に標準化項目の審議日程を示す。

表 3-8 標準化項目の審議日程

	項番	WD	CD	DIS	IS
Close	10536－1	89年9月	90年3月	90年12月	92年9月
	10536－2	92年5月	92年10月	93年10月	95年12月
	10536－3	94年2月	94年5月	94年11月	96年12月
	10536－4	94年12月	95年10月	97年6月	97年12月
Proximity	14443－1	96年10月	96年11月	97年6月	97年12月
	14443－2	96年6月	97年6月	97年12月	98年6月
	14443－3	97年10月	98年3月	98年9月	99年3月

(WD:Working Draft　　CD:Committee Draft
DIS:Draft International Standerd　　IS:International Standard)

3.6 非接触型ＩＣカードの実証実験及び利用事例

非接触型ＩＣカードを活用した実証実験事例、利用事例を調査した。調査資料では、運輸・鉄道関係の事例が多い。

3.6.1 導入・実験プロジェクトの一覧及び記事概要

実証実験事例の一覧表（表 3-9）と記事の概要を紹介する。

表 3-9 導入・実験事例一覧

項目番号	導入・実験事例
3.6.1.1	ロンドンバスＢＥＳＴおよびロンドンバスプロジェクト
3.6.1.2	ロンドン地下鉄
3.6.1.3	ヘルシンキ・メトロポリタン・エリア・カウンシル（ＹＴＶ）
3.6.1.4	パリ交通局（ＲＡＴＰ）
3.6.1.5	マンチェスターＰＣＭＬ
3.6.1.6	豪州の首都圏での鉄道自動改札システム
3.6.1.7	豪州の非接触ＩＣカードによる代金決済カードシステム
3.6.1.8	香港の大都市近距離交通機
3.6.1.9	英国 Merseyside の Merseytravel 社のバスサービス
3.6.1.10	ソウルのバスサービス
3.6.1.11	Ｖａｌａｎｃｅ（仏）でのバスサービス
3.6.1.12	ＪＲ東日本
3.6.1.13	公共旅客輸送部門におけるＩＣカードの活用（汎用電子乗車券技術組合）
3.6.1.14	シンガポールの自動改札実験
3.6.1.15	英国ケント地区およびサリー地区でのパイロット

3.6.1.1 ロンドンバスＢＥＳＴおよびロンドンバスプロジェクト

1994 年 2 月から 1 年間 200 台以上のバスと 1 万人のカードホルダーにより、非接触ＩＣカードを使用し、ロンドン郊外のハロー地区で第二次トライアルが実施された。

カードの名称は、「スマートフォトカード」と言い、顔写真が熱転写された用紙をカード上に貼りつけ、定期券として利用された。利用方法は、乗車時にカードを所定の位置に置く形態を取っている。今後、定期券が不要な現金払いの乗客向けにも、新規に「フェアカード」を発行する。又ロンドン地下鉄との共有カード化も目指している。

参考資料：

(1) 「１９９４年カードシステム欧州調査団報告書」、（社）日本事務機械工業会カード及びカードシステム部会、１９９５年１月

(2) 「鉄道におけるカードシステムの利用可能性に関する調査研究報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９５年７月

(3) 「日本鉄道サイバネティクス協議会海外カードシステム調査報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９４年８月

3.6.1.2 ロンドン地下鉄

クレジットカードサイズ（但し、厚さは 2.5㎜）の非接触ＩＣカード（ＴＡＧと呼ばれる）と、改札機のリーダライタ部（ＴＡＲＧＥＴと呼ばれる）を使用し、50㎜以内の距離で札入れ等に入れたまま利用可能である。

タッチアンドパスの仕組みで、ストアードバリュー方式を採用し、１９９０年４月から７月までに３駅約４００人と、１９９１年３月までに２駅約１００人により試行された。又現在セントジェームズパークにて試行されている。利用者のアンケート結果によると、ほぼ良好な評価となっており、現在新しい仕様が検討されている。

参考資料：

(1) 「鉄道におけるカードシステムの利用可能性に関する調査研究報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９５年７月

(2) 「日本鉄道サイバネティクス協議会海外カードシステム調査報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９４年８月

3.6.1.3 ヘルシンキ・メトロポリタン・エリア・カウンシル（ＹＴＶ）

フィンランドのヘルシンキ首都圏での公共交通を運営する Helsinki Metropolitan AreaCouncil（ＹＴＶ）が、１９９２年６月からバス、同年９月からタクシーで１年間実施された。「ヘルシンキトラベルカードトライアル」の詳細である。接点付ＩＣカードと無端子カード、遠隔結合カードの平行トライアルである点が重要であり、トライアルの結果は、定期券・乗車券を非接触カードに置き換え、１９９７年運用開始の方針となった。

実用化実験の結果および評価評価の報告

利用者の反応

- 接触カードは参加者の半分がよくないとの反応
- 非接触カードは評判が良い

- 参加者の３分の２は、非接触カードが既存の定期券より良いとの反応

結論

- 定期券は Proximity 非接触カードがよい
- １回券はペーパーでも良い

参考資料：

(1) 「１９９４年カードシステム欧州調査団報告書」、（社）日本事務機械工業会カード及びカードシステム部会、１９９５年１月

(2) 「鉄道におけるカードシステムの利用可能性に関する調査研究報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９５年７月

(3) 「日本鉄道サイバネティクス協議会海外カードシステム調査報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９４年８月

3.6.1.4 パリ交通局（ＲＡＴＰ）

フランスのパリ交通局（ＲＡＴＰ）が、非接触カードの導入を計画し、そのトライアル状況の概要である。既存磁気乗車券の不正利用とメンテナンス費用の圧縮を狙い、電磁誘導方式の非接触カードを採用した。バッテリ内蔵で、カードは標準サイズより一回り大きい。ビルのアクセス管理等と平行して、自動改札での部分トライアルが進行している。

バッテリ内蔵のトライアル用カードは、イノバトロン製で、通信周波数７ＭＨｚを採用し、メーカの協力を得て実験を実施中である。９４／８からバージョンアップを予定している。将来的には、スマートカード＋アダプタ方式や、メッセージの表示機能の付加を検討し、９５年度には結論が出される。

参考資料：

(1) 「１９９４年カードシステム欧州調査団報告書」、（社）日本事務機械工業会カード及びカードシステム部会、１９９５年１月

(2) 「鉄道におけるカードシステムの利用可能性に関する調査研究報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９５年７月

(3) 「日本鉄道サイバネティクス協議会海外カードシステム調査報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９４年８月

3.6.1.5 マンチェスターＰＣＭＬ

ＰＣＭＬ（Prepayment Card Manchster Ltd.）は、公共交通機関等が出資して設立したカードシステム運用会社である。非接触式ＩＣカードを採用し、先払い方式のリチャージャブルな電子財布型で進めている。交通機関を中心に、小売り流通でも使用できることが企図された第１期の実験状況が報告されている。

参考資料：

(1) 「鉄道におけるカードシステムの利用可能性に関する調査研究報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９５年７月

(2) 「日本鉄道サイバネティクス協議会海外カードシステム調査報告書」、日本鉄道サイバネティクス協議会調査研究委員会第２分科会、１９９４年８月

3.6.1.6 豪州の首都圏での鉄道自動改札システム

ＣＩＴＹ ＲＡＩＬは、オーストラリアニューサウスウェールズ州の鉄道局が運営しており、シドニーを中心とした首都圏輸送を担当している。２０００年のシドニーオリンピックに向けて、システムを更新し、路線を整備し、新型車両まで投入される。全体で２億Ａ$（１Ａ$＝約９０円）の投資が行なわれる。Automatic Ticketing System（ＡＴＳ）は、顧客操作券売機、自動改札機などの総称である。これらのシステムは、Station Control Computer を経由して、センターコンピュータ（ＤＥＣのＶＡＸ）に接続されている。

現在（調査当時）、コストダウン、信頼性向上を目指して、既存のＡＴＳに替わる非接触ＩＣカードを試行している。

入手資料は路線図・システム構成図、調査時撮影の写真が含まれる。

参考資料：

(1) 「自動出改札システム海外視察　報告書」、日本鉄道サイバネティクス協議会、１９９５年 11 月

3.6.1.7 豪州の非接触ＩＣカードによる代金決済カードシステム

豪州ＴＲＡＮＳＣＡＲＤ社と同社のシステムを試行しているＳｔ．Ｍａｒｙｓ市の視察報告書である。ＴＲＡＮＳＣＡＲＤ社は、１９９１年に公共機関の料金収受システムの開発・普及を目的に設立され、“Ｗｉｚａｒｄ”という非接触カード“ＴＲＡＮＳＣＡＲＤ”

を利用した代金決済システムの開発、運用について、ＣＴＡ社と行った。

Ｗｉｚａｒｄシステムは、バス、鉄道、タクシー運賃・プール入場料・キヨスクでの買い物の代金決済に用いられており、ＴＲＡＮＳＣＡＲＤをプリペイドや電子財布として使用し、バスでの乗車券や店舗での物品等の購入を行う。鉄道では、改札機に近づけることにより読み取られる。読み取り装置は、既存のシステムにＲＳ－２３２Ｃ等の汎用インターフェースで接続でき、簡易にシステム構築が図れる。

カード仕様は、外形が５４×８６×１．５～０．７６mm、メモリは、８ｋビットＥＥＰＲＯＭでバッテリレス、１０万回書き換えが可能。個人化のための写真、テキスト・グラフィックスのプリントも可能である。

通信周波数は、１３．５６MHｚでＩＳＭに準拠し、読み書き共に通信距離は１００mm以下で、通信速度は通常で１００ｍｓ以下である。複数タグを想定したアンチコリージョン機能、Ｄｉｎａｍｉｃ　Ｒ／Ｗ，高速衝突防止機能を備えている。データセキュリティについては、RWD－カード間通信にストリームサイファ方式による暗号化を行い、カードＡＳＩＣ、ＲＣＣＤ－ＡＳＩＣにハードウエア暗号機能を備えている。相互認証はＩＳＯ／ＩＥＣ　９７９８－２に準拠している。

Ｓｔ．Ｍａｒｙｓ市は人口３～４万人の小都市で、平成７年５月１日より同システムの試行を開始した。スタート時から１４，０００件の決済があり、内７，０００件がバス利用である。バス乗客の３０～４０%が同カードを利用している。カード枚数は、２，０００枚で５，０００枚を追加発行される予定である。

同システムのバス運賃の支払いデモでは、やや遅く感じられた。カードコストは、明言されなかったが、３００～４００円程度である（５Ａ$）。将来１０～１５Ａ$でのデポジットを検討中である。

参考資料：

(1)　「自動出改札システム海外視察　報告書」、日本鉄道サイバネティクス協議会、１９９５年 11 月

3.6.1.8　香港の都市近距離交通機関

香港クリエイティブ・スター社による、大都市近距離交通機関の非接触 IC カードシステムの概要である。現行の磁気カードシステムと比べて非接触 IC カードの優れた点、非接触

IC カードシステムの特長、システム構成の技術的な説明が述べられており、カード、リーダー・ライターの仕様等も含まれる。非接触 IC カードシステムの通信概念を図で説明し、相互認証や暗号についても簡単に説明されている。香港システム概観図では、地下鉄、バス、鉄道、フェリー等の適用機器が示されている。

参考資料：

(1) 「海外技術情報：香港への非接触ＩＣカードシステムの開発について」、サイバネティクス、Vol.1、No.1、ｐ２１－２２、１９９６年5月

3.6.1.9 英国 Merseyside の Merseytravel 社のバスサービス

非接触スマートカード（ＩＣカード）が採用された理由

- バスサービスの環境では駆動機構のない装置が良い
- 見込み客の多く、特に老人や児童は、装置にカードを差し込むことが難しい

試行規模

- 非接触スマートカード　　１０、０００
- ドライバー・モジュール　　１５０
- カード発行所　　1

注）１９９６年１月現在で、６千枚以上のカードが使用されている。

将来計画

- プリペイドなどカード機能の拡張
- 鉄道サービスなどアプリケーションの拡張
- Ｍｅｒｓｅｙｓｉｄｅのあらゆるアプリケーションへの適用

参考資料：

(1) 「Contactless Smart Cards in Merseyside」、Card Europe Report into The Future For Contactless Smart Cards、Card Europe、ｐ２６－２９、１９９６年3月

3.6.1.10 ソウルのバスサービス

１９９６年６月までに、８、７２５台のバスにＭｉｆａｒｅの非接触カードの機器が搭載された。このシステムは、ソウル地下鉄と互換性がある。

- カード枚数は、１９９６年末には１５０万枚になる

参考資料：

(1) Report on Smart Cards，１９９６

(2) Smart Card News，Ｖｏｌ５．Ｎｏ８，Ａｕｇ．１９９６

3.6.1.11 Ｖａｌａｎｃｅ（仏）でのバスサービス

ＭＩＦＡＲＥシステムによる非接触スマートカードによるバス・チケットシステムである。

規模

- １０、０００枚のスマートカードを発行
- Ｖａｌａｎｎｃｅの９５台のバスに機器を搭載

参考資料：

(1) Ｓｍａｒｔ　Ｃａｒｄ　Ｎｅｗｓ，Ｆｅｂ．１９９６

3.6.1.12 ＪＲ東日本

１９９４年２月から３月にかけて、東京駅など８駅で、自動改札機にマイクロ波の非接触ＩＣカードを付加した試験が実施された。

１９９５年４月から６ヶ月、首都圏１３駅で短波帯のカードの実験を行った。

参考資料：

(1) 「鉄道分野におけるリモートパスの実証」、CardWave、ｐ４７－４９、１９９６年７月。

(2) 「無線カード定期券システムの現地試験」、第 31 回鉄道におけるサイバネティクス利用　国内シンポジウム論文集、日本鉄道サイバネティクス協議会、ｐ５２－５５、１９９４年 11 月。（要約参照）

3.6.1.13 公共旅客輸送部門におけるＩＣカードの活用（汎用電子乗車券技術組合）

汎用型の非接触タイプのＩＣカードを活用した、非接触自動改札システムや共通乗車カードシステムを研究開発のテーマとする。運輸事業者、電機、機械業界などのメーカー、関係省庁の協力体制を確立して、利用者ニーズを反映したオブジェクト指向の研究開発体

制で実施する。

平成 8 年度から 3 年程度を目途に、以下のステップで実施する。

非接触自動改札システム

- 第一段階　　非接触型的乗車券の実用化
- 第二段階　　前払い式電子乗車券の実用化と非接触型的乗車券とのハイブリッド（併用）化共通乗車カードシステム
- 第三段階　　複数の交通機関を利用できる共通乗車カードの実用化
- 第四段階　　共通乗車カードと金融カード（クレジット、電子マネーなど）のインターフェース技術の開発

参考資料：

(1)　「汎用電子乗車券の実用化の研究開発について」、運輸省、１９９６年７月。

(2)　「汎用電子乗車―組合のご案内―汎用電子乗車技術研究組合」、設立準備会事務局、１９９６年７月。

3.6.1.14　シンガポールの自動改札実験

５００名の学生が、ＬＴＡ（Land　Transport　Authority）の推進する非接触ＩＣカードを活用したバスやＭＲＴの自動改札実験に参加する。

参考資料：

(1)　「Undergrads to test 'contactless' smart card for bur, MRT fares」，The STRAITS Times,June,1996.

(2)　「シンガポールで非接触ＩＣカード使った自動改札実験、ソニーがシステム納入」、日経ニュ―メディア、１９９６．９．２

3.6.1.15　英国ケント地区およびサリー地区でのパイロット

ケント地区（Ｋｅｎｔ　Ｃｏｕｎｔｒｙ）

- １年間の試行期間に、バス通学生およびバス利用老人を対象として、２０００枚のソニー製非接触スマートカードを発行する。
- 機器導入を１９９５年９月より開始し、１１月中旬からカードを発行する。

サリー地区（Ｓｕｒｒｅｙ　Ｃｏｕｎｔｒｙ）

- １９９５年１０月初旬からの第一段階では、バス通学児童にソニー製非接触スマートカードを発行する。
- 第二段階は、居住者を対象に、１９９６年４月から開始しする。
- 将来的には、バス利用者にＳＶＣ（Ｓｔｏｒｅ　Ｖａｌｕｅ　Ｃａｒｄ）を発行する。

参考資料：

(1) Ｓｍａｒｔ　Ｃａｒｄ　Ｎｅｗｓ，Ｊｕｌｙ１９９６

4 ＩＣカード検討メンバー

4.1 接触型ＩＣカード検討WG（ＳWG１）メンバーリスト

名前（敬称略、順不同）	会社名	所属・役職
今林　雅澄	電子商取引実証推進協議会	主席研究員
加藤　正次	電子商取引実証推進協議会	主席研究員
栗山　善吉	アンリツ(株)	情報システム事業部技術部 課長補佐
太田　裕	イオンクレジットサービス(株)	システム本部システム部開発２課
菅野　直行	エヌ・ティ・ティ・データ通信(株)	技術開本MM技術センタ先端通信応用担当　課長
滝沢　俊男	沖電気工業(株)	カードビジネス推進部 課長
井上　剛	(財)金融情報システムセンター	業務調査部 上席調査役
石川　寿男	(株)クレディセゾン	情報システム部 部長
藤田　泰生	グローリー工業(株)	メディアシステム開発部 主事補
西村　一範	国内信販(株)	営業推進部二課
佐藤　泰	(株)コンテック	システム事業部システム部 係長
石田　耕一	(株)さくら銀行	ネットワーク業務部電子決済室　主任調査役
葛西　雅之	(株)ジェーシービー	企画部マルチメディア室 課長代理
百武　昌夫	(株)資生堂	経営企画部
内藤　裕幹	シャープ(株)	情報システム事業本部情報商品開発研究所
亀田　郁雄	(株)ジャックス	企画開発部企画課
宮下　善和	神鋼電機(株)	開発本部研究部
浦部　治福	セコム(株)	開発ｾﾝﾀｰ技術情報管理ｸﾞﾙｰﾁﾌﾟﾌｪﾝｼﾞﾆｱ
赤木　宏至	(株)セントラルファイナンス	開発部
厚見　靖男	(株)ダイエーＯＭＣ	カード営業本部企画管理部
清村　司郎	大日本印刷(株)	ＣＢＳ開発本部ＥＣチーム次長心得
酒井　高彦	(株)東芝	情報・通信ｼｽﾃﾑ新規事業企画室ｶｰﾄﾞｼｽﾃﾑ開発担当主任
小沢　達郎	凸版印刷(株)	金融・証券（事）カードセンターＩＣカード開発部
中山　靖司	日本銀行	金融研究所　研究第２課
與口　真三	(社)日本クレジット産業協会	企画調査部
小野　隆	日本信販(株)	企画本部マルチメディア推進室
越湖　正道	(株)日本ダイナースクラブ	企画部企画課 上席調査役
藤田　茂樹	日本電気(株)	ﾊﾟｰｿﾅﾙﾜｰｸｽﾃｰｼｮﾝ事業部第一商品部
藤井　正哉	(株)野村総合研究所	新社会ｼｽﾃﾑ事業本部ｻｲﾊﾞｰｺﾏｰｽ事業部
今井　仁	ぴあ(株)	情報事業本部ＥＣ推進室
士反　康裕	(株)ピープル	経営企画室
倉部　啓	VISA・インターナショナル	メンバーリレーション

川村　直道	富士通(株)	ソフトウェア事業本部企画部　担当部長
吉川　義幸	ﾏｽﾀｰ ｶｰﾄﾞ・ｲﾝﾀﾅｼｮﾅﾙ･ｴﾝﾊﾞｰﾊﾟｰ ｼｮﾝ・ｲﾝｸ	ﾊﾞﾘｭｰｵﾍﾟﾚｰｼｮﾝｽﾞ
泉　知秀	松下産業機器(株)	技術部ソフトグループ
福島　彰彦	メモレックス・テレックス(株)	ベリフォーン事業本部
佐藤　裕明	ユーシーカード(株)	マーケティング開発部
山崎　勢之助	(株)ライフ	システム企画部
高木　伸哉	松下電器産業（株）	松下電池工業（株）応用機器事業部 SCBｸﾞﾙｰﾌﾟ主任技師
山口　卓	シーメンス(株)	IC Card Office 担当部長
大久保　政雄	(株）ゼクセルインテリジェンス	ICカードｼｽﾃﾑ部
岩崎　宏尚	ヤマトシステム開発（株）	第二営業部ＣＳプロジェクト
田口　廣樹	山陰信販（株）	営業部
辻川　民夫	十六コンピュータサービス（株）	取締役　開発部長

4.2 非接触型ＩＣカード検討WG（ＳWG２）メンバーリスト

名前（敬称略、順不同）	会社名	所属・役職
有賀　淑郎	電子商取引実証推進協議会	主席研究員
大島　雅男	電子商取引実証推進協議会	主席研究員
吉野　真寛	三菱商事(株)	カード事業部
信濃　義朗	昌栄印刷(株)	ニューメディア事業部 課長
陸田　耕吾	(財)ニューメディア開発協会	システム開発部
林　文雄	オムロン(株)	新事業開発ｾﾝﾀｰ・ｶｰﾄﾞ事業推進ｾﾝﾀ
前田　昇	ソニー(株)	カード事業室 室長
高橋　清志	(株)デンソー	電子応用技術部技術6課
岸本　輝昭	(株)日立製作所	ﾋﾞｼﾞﾈｽｼｽﾃﾑ開発ｾﾝﾀｰ　ﾆｭｰﾋﾞｼﾞﾈｽ
高比良　賢一	三菱電機(株)	メモリ応用製品部
清吾　明男	小林記録紙（株）	営業企画本部第二企画部カードグループ係長
植村　泰佳	ICｶｰﾄﾞ取引ｼｽﾃﾑ研究開発事業組合(ICCS)	事務局：（株）ＪＦＰ
千村　茂美	ローム（株）	MODULE LSI商品開発部

平成９年５月発行

発行：電子商取引実証推進協議会

東京都江東区青海２－４５
タイム２４ビル１０階
Tel　03-5531-0061
E-mail　info@ecom.or.jp