

ICカード利用ガイドライン (接触 / 非接触) (1.0版)

平成10年3月



電子商取引実証推進協議会

ICカードWG

はじめに

ＥＣＯＭの基本命題は、『我が国におけるコンシューマＥＣ（企業と消費者間）の実現と普及を目指し、そのために必要な様々な共通基盤の整備』であり、本主旨に基づいて、ＩＣカード検討ＷＧ（ＷＧ７）では『ＩＣカードの実用化・普及』を掲げ、ＩＣカードを導入する事業者・運営者を対象に、消費者・利用者の立場で、役立つ・メリットあるＩＣカードのあり方、検討すべき事項、解決策等を示す『ＩＣカード利用ガイドライン』を策定した。

ＩＣカードを活用した電子商取引（Electronic Commerce）の実証実験は、国内各地で実施され、日常生活に溶け込んでいる。

通産省が推進するＩＣカードを利用した実証実験プロジェクトでは、数万人の参加者を得て実用化に向けた活動が活発に実施され、地域全体で利用できる多目的ＩＣカードの実用化に向けた活動も活発になってきた。

海外では、国民の大多数にＩＣカードを配布し、日常生活（リアル）の中で個人を識別する情報媒体・決済媒体として利用したり、パソコンを活用したインターネット市場（バーチャル）での電子決済用に、個人鍵・電子マネー用の媒体としてＩＣカードが利用されている。

今後、多くの人が１枚以上保有すると思われるＩＣカードを、国内外で共通利用できるようにするためには、国際標準化を推進し、デファクトと連携し、発行者識別コード（ＡＩＤ）を登録し、偽造、改竄、なりすましができないインフラストラクチャを整備し、利用者にとってメリットとなる仕組みを構築することにある。

国内外の実用化に向けたＩＣカード導入の活発な動きに合わせて、本ＩＣカード検討ＷＧでは、ＩＣカードを利用したシステム開発、導入推進する際に必要な情報・検討項目・課題・解決策等、ＩＣカードを普及・拡大するための参考に供するため、『ＩＣカード利用ガイドライン』としてまとめた。

本『ガイドライン』は、ＩＣカードの標準化進捗状況、実用化が予想されているクレジット用ＩＣカード、現金と同様な利用場面が予想される電子現金・電子マネー用ＩＣカード、交通機関・通信分野に利用されるＩＣカード等、広範囲な分野・業務のＩＣカードを対象に検討している。さらに、ＩＣカード端末の要件についてもまとめた。ＩＣカードを導入する際の運用面・利用面で活用されることを希望する。

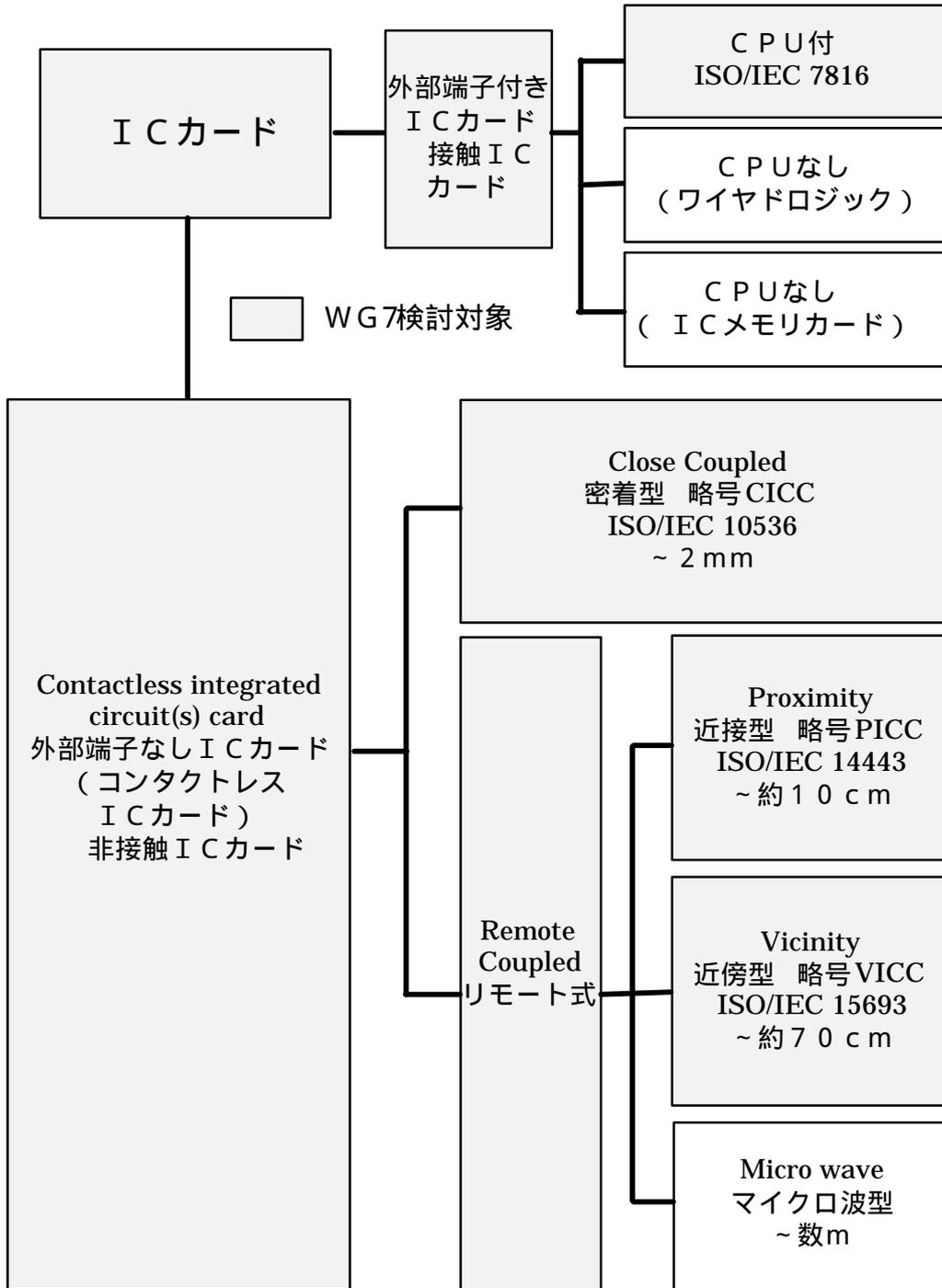
本『ガイドライン』策定に当たっては、ＷＧ７会員各位、関係者各位のご協力をいただき、ＥＣＯＭの成果物としてまとめることが出来た。ここに厚く感謝の意を現わす次第である。

平成１０年３月

電子商取引実証推進協議会
ＩＣカード検討ＷＧ

ICカードの分類

本報告書では、ICカードを次のように分類している。



- 1998年2月までの内容を基に作成。 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ICカード

ECOM ICカードWGでは、ISO/IEC 7816 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ICカードを対象としている。

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ICカード」の名称は、JISでは用いられていないが、「接触ICカード」との関連上、本ガイドラインで使用している。

ICカードWGのホームページ

ECOMのWeb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カードの概要	3
1.1 標準化動向.....	3
1.2 ICカードの利用分野および利用事例.....	5
1.3 今後のICカード潜在市場予測.....	16
1.4 多目的ICカードに求められる要件	17
1.4.1 多目的ICカードの種類	17
1.4.2 多目的にする上での課題(1.4.1 多目的ICカードの種類(3)項を除く).....	17
1.4.3 管理運用上の制約	19
1.5 ライフサイクルとセキュリティについて	19
1.5.1 セキュリティ管理	19
1.5.2 不安要素とセキュリティ対策	20
1.5.3 ICカードのライフサイクルとリカバリー策について.....	22
1.5.4 複数アプリケーションの実装可否について.....	24
1.6 ICカード技術動向	26
1.6.1 ICカードOS	26
1.6.2 ICカードLSIチップ	29
1.6.3 ICカード素材	33
2 接触ICカード利用ガイドライン(決済分野)	35
2.1 検討対象選定の背景	35
2.2 決済分野におけるICカードに求められるもの	37
2.3 明快な役割分担と協調	39
2.4 クレジット.....	40
2.4.1 ICカード利用時のオフライン取引についての考え方.....	40
2.4.2 フロアリミット.....	46
2.4.3 SCJ実証実験に見るICクレジットカードへのEMV仕様の適用について.....	63
2.4.4 オフライン取引データの効率的な事後処理についての考察.....	68
2.4.5 クレジットカード業務関連法について	71
2.5 プリペイド型電子マネー.....	71
2.5.1 電子マネー業務に関する現行法上の各種規制の整理	71
2.6 端末.....	75
2.6.2 クレジット業務用端末.....	76
2.6.3 電子マネー用機器	84
2.7 端末インフラストラクチャー整備アクションプラン.....	88
2.7.1 インフラストラクチャー整備促進の為の要件	88
2.7.2 端末管理機構の構築.....	92
2.7.3 端末共同利用のための諸ルール	93
3 非接触ICカード利用ガイドライン.....	95
3.1 非接触ICカードの位置付け	96

3.1.1 ICカードの分類	96
3.2 非接触ICカードの利点.....	98
3.2.1 推奨される非接触ICカード	98
3.3 非接触ICカードのアプリケーション分野とその市場規模.....	102
3.3.1 ICカードの市場と適性	103
3.4 非接触ICカードの標準化.....	103
3.4.1 国際標準で分類される非接触ICカードの種類.....	103
3.4.2 カードの特徴.....	103
3.4.3 国際標準の進捗状況.....	104
3.4.4 JISの進捗状況	106
3.5 非接触ICカードの相互運用性.....	106
3.5.1 検討の目的と検討項目	106
3.5.2 互換性の確保.....	107
3.5.3 複合機能カード	107
3.5.4 複合機能端末.....	111
3.6 非接触ICカードのセキュリティ	112
3.6.2 システムセキュリティ上からの分類	112
3.6.3 過失の侵害に対するセキュリティ	113
3.6.4 故意の侵害に対するセキュリティ	114
3.7 非接触ICカードの普及課題	117
3.7.1 非接触ICカードの電波法上の扱い.....	117
3.7.2 ICカードのコスト.....	119
3.7.3 導入動向	119
3.7.4 インフラの整備	119
3.7.5 参考文献	120
4 ICカード利用環境整備に関する提言（AIDの付番管理）	121
4.1 ICカード利用環境整備の中核.....	121
5 ICカード検討メンバー	128
5.1 接触ICカード検討WG（SWG1）メンバーリスト	128
5.2 非接触ICカード検討WG（SWG2）メンバーリスト	129

1 ICカードの概要

1.1 標準化動向

ISO並びにJISにおけるICカードの標準化状況に関し下記の通り纏めた。尚、これらの規定の目指すところは、相互運用性を確保するためにも最低限必要な、ハード面におけるICカードの物理的、電気的特性の仕様の統一、またソフト面におけるコマンドの共通化、複数の発行者・複数のアプリケーションの混在を前提とした運用面におけるアプリケーション識別子(Application Identifier:以下「AID」と略す)の番号体系の統一、並びに登録管理機関の設置に関する基準作りであり、各発行者(事業者)が決定すべきICカードに実装する具体的なアプリケーションを規定するものではない。

(1) 接触ICカード(外部端子付きICカード)

接触ICカードにはCPU付きのタイプや、CPUのないワイヤードロジックタイプ/メモリーカードタイプが存在するが、標準化の対象はCPU付きのICカードである。日本国内規格であるJISも、ICカードの仕様策定に当っては、国際的な互換性の確保を図ることを第一義として、国際規格であるISO/IEC 7816と合わせるべく翻訳規格としての制定作業が行われた。そのIS化/JIS化の進捗状況は表1-1の通り。

表 1-1 IS化/JIS化の進捗状況対応表

ISO/IEC	JIS
7816-1: ICカードの形状・物理特性(改訂DIS)	JIS X6303
7816-2: 端子の位置と形状(改訂IS化)	JIS X6303
7816-3: 電気信号及び伝送プロトコル(改訂DIS)	JIS X6304
7816-4: 共通コマンド(AM1 DIS)	JIS X6306
7816-5: アプリケーション識別子及びその登録(IS)	*対応規格無し。
7816-6: 共通データ要素(IS)	JIS X6307 (策定中)
7816-7: SCQL関連コマンド(DIS)	*対応規格無し。
7816-8: セキュリティ関連コマンド(CD)	*対応規格無し。
7816-9: 高機能コマンド(WD)	*対応規格無し。
7816-10: 同期式カードの動作手順及びATR(CD)	*対応規格無し。
7816-11: セキュリティ構造(WD)	*対応規格無し。
*ISO 10373: 識別カード - 試験方法	JIS X6305

注:()内記載の記号は標準化ステップを示す。:WD:Working Draft / CD:Committee Draft / DIS:Draft International Standard / IS:International Standard

尚、ISO/JIS共に基本部分の大半は統一的な規格となっているが、伝送プロトコルに関しては、先行していたフランスのことも配慮し、T=0(バイト伝送)とT=1(キャラクター伝送)の2方式の併記となっている。また、決済業務の関連規格として以下のものがある。

金融取引に関する国際規格

金融業務におけるICカードと同受入装置間のメッセージ。

- A. ISO 9992 - 1 : 概念と構造 (IS)
- B. ISO 9992 - 2 : ファンクション、メッセージ(コマンドとレスポンス)、データ要素と構造 (DIS)

ICカード利用の金融取引システムのセキュリティ

- A. ISO 10202 - 1 : ICカードのライフサイクル (IS)
- B. ISO 10202 - 2 : 取引きのプロセス (IS)
- C. ISO 10202 - 3 : 暗号鍵の諸関係 (DIS)
- D. ISO 10202 - 4 : 提供サービスの安全性のためのモジュール (IS)
- E. ISO 10202 - 5 : ICカードで利用されるアルゴリズム (DIS)
- F. ISO 10202 - 6 : カード保有者の真偽性照合 (IS)
- G. ISO 10202 - 7 : 鍵管理 (DIS)
- H. ISO 10202 - 8 : 一般原則と概観 (DIS)

(2) 非接触ICカード(外部端子なしICカード)

非接触ICカードは接触ICカードと異なり、区分される以下の数種類全てを対象として其々標準化の検討がなされている。

密着型ICカード(Close Coupled = 「CICC」と略す)

ISO/IEC JTC1/SC17/WG8/TF1にて検討。

名称	ISO/IEC	標準化内容	標準化ステップ
Identification cards	10536-1	Physical characteristics 物理的特性	IS
-Close coupled integrated circuit(s) cards	10536-2	Dimensions and location of coupling areas 結合領域の寸法と位置	IS
外部端子なし ICカード	10536-3	Electronic signals and reset procedures 電気信号とリセット手順	IS
密着型 略語CICC	10536-4	Anser to reset and transmission protocols 初期応答と伝送プロトコル	CD

近接型ICカード(Remote Coupled = Proximity : 「PICC」と略す)

ISO/IEC JTC1/SC17/WG8/TF2にて検討

名称	ISO/IEC	標準化内容	標準化ステップ
Identification cards	14443-1	Physical characteristics 物理的特性	CD
-Proximity integrated circuit(s) cards	14443-2	Radio frequency power and signal interface 電波出力と信号インターフェース	WD
外部端子なし ICカード	14443-3	Initialization and anticollision 初期化と衝突防止	-

(近接型)

略語PICC

	14443-4	Transmission protocols 伝送プロトコル	-
--	---------	-----------------------------------	---

近傍型ICカード(Remote Coupled = Vicinity:「VIC C」と略す)

ISO/IEC JTC1/SC17/WG8/TF3にて検討。

名称	ISO/IEC	標準化内容	標準化ステップ
Identification cards	15693-1	Physical characteristics 物理的特性	C D
-Vicinity integrated circuit(s) cards	15693-2	Air interface and initialization 非接触インターフェースと初期化	-
外部端子なし ICカード (近傍型) 略語VICC	15693-3	Protocols プロトコル	-
	15693-4	Registration of application/issuers アプリケーション/発行者登録	-

マイクロ波型ICカード(Micro Wave)
未審議。

1.2 ICカードの利用分野および利用事例

ICカードはその優れた機能により、様々な分野で利用されている。その利用分野は、従来からの磁気カードシステムの延長線にある利用分野ばかりでなく、全く新しい分野でICカードの利用アプリケーションが創出された分野もある。ICカードは当初から磁気カードに比べ、高い偽造防止機能とデータ容量の大きさを生かして、主としてデータキャ

表 1-2 ICカードの利用分野と利用事例

金融分野	銀行キャッシュカード	B
	クレジットカード	B
	電子マネー	C
流通・サービス分野	ポイントカード	A
	メンバーズカード	A
健康・医療分野	自治体医療カード	C
	フィットネスメンバーカード	A
ID分野	企業・学校内IDカード	A
	ビル内IDカード	A
	建設業界IDカード	C
交通・運輸分野	有料道路通行カード	B
	定期券および汎用乗車券カード	B
	車両運行管理カード	A
	宅配便管理カード	A
放送・通信分野	衛星放送加入者管理カード	C
	移動体通信SIMカード	C
行政分野	健康保険証カード	C
	住民基本台帳番号カード	C

その他システム分野	機器外部記憶媒体およびセキュリティカード	A
-----------	----------------------	---

リア機能を中心とした活用がされてきた。さらに最近ではインターネットをはじめとして、ネットワークを通じた様々なサービスが開発・普及するにつれ、ICカードの持つインテリジェント機能と暗号システムの搭載による高セキュリティ機能が着目され、EC分野で不可欠のツールとして一躍脚光を集めることとなった。

本章では、表 1-2の様に分類して、それぞれの利用例、および状況について述べる。

A：従来からICカードが利用されている分野

B：既存のアプリケーションがICカードに置き換わると見られる分野

C：新たにICカードを利用したカードシステムが構築されると思われる分野

また、表 1-3に、各分野において用いられるICカードに求められる機能について、予測を含めて参考としてまとめた。分野毎に、何処に比重が置かれるかという視点でまとめ、特にデータキャリア機能については、ICカードの大きな記憶容量に重点が置かれる分野という意味であり、の付いていない分野に記憶機能が必要ないという意味ではない。また、オフライン機能は、データキャリアとは異なり、カードと、端末間だけで処理が完結するものとしている。これらは、現状で考えられる範囲での必要な機能であるが、サービスの拡大、多目的カードの実現などにより、1枚のカードに複合的な機能が求められるようになる可能性がある。

表 1-3 各分野で用いるICカードに求められるICカードの機能

利用分野 利用業界	利用分野が必要とする 機能	データ キャリア 機能	カード 認証機 能のみ	カード認 証+個人 認証機能	暗号化 機能	オフ ライン機 能
金融	銀行					
	クレジット					
	電子マネー					
流通・サービス	ポイントカード					
	メンバーズカード					
健康・医療	自治体医療カード					
	フィットネスカード					
ID	企業・学校内ID					
	ビル内IDカード					
	建設業界IDカード					
交通・運輸	有料道路通行カード					
	定期・汎用乗車券					
	車両運行管理カード					
	宅配便管理カード					
放送・通信分野	衛星放送加入者管理					
	公衆電話カード					
	移動体通信SIM					
行政分野	健康保険証					
	住民基本台帳					
	運転免許証					
その他システム	機器外部記憶媒体等					

A. 従来からICカードが利用されている分野

ICカードのデータ記憶容量の大きさ、セキュリティの高さ（不正アクセス、改竄防止）を利用し、以下のようなサービスが行われている。現在の所、接触ICカードが多く使われている。ID分野においては、非接触を用いて管理するものや、電子マネー機能を持たせて、接触、非接触の統合型カードを用いるものがある。交通分野では、鉄道が非接触に、高速道路が接触になっている。

a) 流通・サービス分野 <ポイントカード>

商品購入やサービス提供の際に、ICカード内にポイント情報を記録し、顧客サービスに役立てるとともに顧客の固定化を狙っている。石油販売、商店街・ショッピングセンター等での発行事例があり、ある石油販売会社のカードは、国内のICカード導入代表事例でもある。従来の紙やPETカードによるポイントカードとの差別化は、クレジットカードとの一体化が可能なこと、次に取り上げる顧客管理・サービス機能を持つメンバーカードとしても利用できることなどが挙げられる。また電子マネー的な使い方も行われており、ガソリンスタンドでのキャッシュレスが実現している。

今後、従来紙やPETカード、プラスチックカードが利用されてきたポイントカードのICカード化が進むものと思われる。

b) 流通・サービス分野 <メンバーカード>

顧客情報をICカード内に記録し、顧客サービスに利用するとともに、顧客管理データとしても活用している。現在、自動車ディーラーやホテル、ショッピングセンター・商店街などでの利用が行われている。自動車ディーラーの例では、ICカード内に顧客データとともに保有車のメンテナンス情報を管理している。膨大な数の顧客の詳細データを全国の営業拠点で利用してサービスを行うためには、ICカード内にデータを持たせ、顧客とともに来店してもらう方が、すべてをオンラインシステムで構築するよりシステム的には有利な点があると考えられる。これらのデータキャリア的な機能を生かして、さまざまな業種でのメンバーカードとしてのICカード発行が検討されている。

c) 健康・医療分野 <フィットネスメンバーカード>

民間のフィットネスセンタにおいてはICカードによる会員管理を行う企業が多い。ICカード内に会員の体力データやプログラムメニューを記録しておき、これらのデータでプログラム作りのコンサルティングを行ったり、プログラムの進捗管理、体力増進のデータ比較、さらにはフィットネス機器との連動による各会員向けの自動調整サービスなど、サービスの範囲も幅広い。単一フィットネスセンタでの導入も多いが、多店舗展開するフィットネスセンタでは、会員が平日は勤務先近くのセンタ、休日は自宅近くのセンタと移動しても、各会員に対してそれぞれの会員データに基づいたサービスが提供できるとしてICカードを会員カードとして導入する企業が多い。

d) ID分野 <企業・学校内IDカード>

従来の従業員証や学生証をICカード化する企業が増えている。ICカード

化する狙いは、企業内や学校内の情報化に合わせてシステムへのアクセスツールとしてICカードを活用するとともに、多目的な利用を実現しようとするものである。代表的なアプリケーションは、企業では入退室管理、端末アクセス管理、社内食堂等のプリペイドカード、など。学校では入退室管理、出欠管理、学食等のプリペイド、証明書発行管理、などである。決済機能の付与のため銀行やカード会社と提携し、キャッシュカードやクレジットカードと一体化して発行される場合も多い。また、ICカード導入による企業、学校イメージの向上や社員、学生のモラルアップなどの効果もあがっている。

e) ID分野 <ビル内IDカード>

最近、大規模開発で新たに建てられるインテリジェントビルでは、テナント向けにICカードを発行される例が一般的である。これらの最先端のビルでは、ビル内の各種設備、サービスがシステム化されており（ビルオートメーションやビルマネジメントシステムと呼ばれる）、利用者であるテナントが、容易にサービスを受けられるようにICカードを採用している。代表的なサービスは、入退室管理、セキュリティシステムとの連動、空調、照明等のコントロール（予約運転等）、共用施設（会議室、ホール）などの予約管理、ショッピングアークード・自販機等でのプリペイド利用などである。これらのカードでも金融機関、クレジットカード会社との提携により決済機能を付与した一体型のICカードが発行される例が多い。

f) 交通・運輸分野 <車両運行管理カード>

従来タコグラフ等で管理されていたタクシーや建設重機、タンクローリ等の運行データ管理をシステム化するため、ICカード内に運行を記録し、事務所の管理システムへ入力するデータキャリアとして利用するシステムが稼働している。タクシーの場合、従来だと乗務員が帰庫後にタコグラフを解析し、実車/空車距離、売上げ記録を集計し、日報を作成していたが、これらのシステムにより、自動化が図られ日報作成にかかる時間が大幅に短縮された。またプリペイドカードやクレジットカードの受け入れによる売上げデータもこのICカードに記録され、精算システムとの連動がされている。

タンクローリ向けのシステムでも給油所や空港の飛行機への給油業務指示と給油記録がICカード内に記録され、事務所内の情報システムとICカードを通じてデータの受け渡しが行われている。

g) 交通・運輸分野 <宅配便管理カード>

大手宅配便業者のヤマト運輸では、取次店管理にICカードを利用している。取次店とは取扱量によって契約単価が異なっており、荷物集荷の際に、担当者は荷物の伝票バーコードとともに、取次店に保管の取次店情報を記録されたICカードから携帯端末で情報を読み出し、どこの取次店から集荷したもので単価がいくらであるかを記録する。この情報は物流センタで管理システムに投入され、後日精算される。さらに事前に一定額を支払ってもらい、荷物を集荷の際にICカード内からプリペイドカードのように減額していくサービスも導入している。

h) データキャリア分野 <各種機器外部記憶媒体及びセキュリティカード>

ICカードのデータキャリア機能を生かして、各種機器への外部記憶媒体としてこれまで幅広い分野で利用されている。これまでの利用例では、前述の車載機器や携帯端末の他、検眼システム、家庭用ゲーム機器、医療測定機器、カメラ、コンピュータなどである。外部記憶媒体としては、PCMCIAタイプのICメモリーカードが一般的であるが、CPU内蔵でセキュリティ性があったり、小型化、データ入出力端子が少ないことなどから、ICカードを利用する例も多い。

今後さらにインターネットを通じた商取引や情報通信が普及してくると、各種不正行為に対するセキュリティ対策が必要となってくる。この際の実用的なツールとして、高度な認証機能とセキュリティ機能を持つICカードの利用が益々広まってくるものと思われる。すでに海外では今後のコンピュータと通信サービスのインフラとしてICカードを利用するための、コンソーシアムがいくつも結成され、その実用化のための規格化作業を進めている。

B. 既存のアプリケーションがICカードに置き換わると見られる分野

a) 金融分野 <銀行キャッシュカード>

ICカード創生期のICカード利用の代表事例として、ICカードによるオフライン銀行POSシステムの実験導入があげられる。当時、銀行POSシステムの導入が試行されていた時期ではあったが、従来のキャッシュカード(磁気カード)による銀行POSシステムでは、暗証番号、預金残高の確認のためオンラインで銀行のホストコンピュータに接続する必要があり、通信費用、ホストの負荷、ホストの休止する土日・夜間のサービスができないなどの問題があった。これを解決する手段としてICカードの利用が検討され、ICカード内で暗証番号のチェック、一部残高管理を行うことによりオフラインで銀行POSを実現した。都市銀行を中心に多くの実験プロジェクトが相次いだ。しかしながら、従来の磁気カードによるシステムの改良と、銀行POS自体の普及が遅れたことがあり、実験段階のままで本格的な導入はなされていない。

現在銀行で導入されているICカードシステムは、そのほとんどが特定用途向けのICカードに、キャッシュカード機能を付与したカードである。主として 企業、学校内IDカード、インテリジェントビル内のテナントカード、商店街のポイントカード等として発行されるICカードとの一体化である。それぞれの用途でのICカード利用事例は後で紹介するが、それぞれのサービスで決済機能(プリペイド入金、社内経費精算など)に銀行口座を使用するため、キャッシュカードとの一体化を行っている。銀行にとっては、新規顧客の開拓につながると共に、ICカードシステム自体の開発、販売、および決済処理による手数料収入などの新たなビジネスチャンスを期待している。今後もこのような用途での導入が続くものと考えられる。

全国銀行協会連合会では、キャッシュカードのICカード化を見通して、全銀協「ICカード標準作業仕様」を策定している(昭和63年2月発行、平成9年4月改定)。

全銀協仕様の中で、銀行が発行するICカードは多目的利用が可能で、標準業務、任意業務とともに、領域貸与業務としてこれら提携先向けアプリケーションを規定している。

さらに、今後の銀行汎用ICカードとして本命視される「電子マネー」とキャッシュカードの一体化されたICカードの発行が計画されている。国内でもVISAによるビザキャッシュと銀行キャッシュカード、NTT電子マネーと銀行キャッシュカードの一体化発行が1998年より開始される見込みである。

b) 金融分野 <クレジットカード>

これまで国内のクレジットカードとしてのICカード発行は、前述の銀行キャッシュカードと同様に、特定顧客（企業、ビル、商店街、ショッピングセンター等）との提携カードとして発行され、ICカードの機能は提携顧客のサービス業務に利用されているものであった。

本格的クレジットカード業務でのICカード利用については、世界的なクレジットカード会社がICカード化戦略を発表し、これを受けて、国内でもICカード化の実験導入が始められている。またその国際的実現のための共通規格として、VISA、マスターカードなどは、EMV仕様と呼ばれるクレジットカードの統一仕様を発表している。

クレジットカード会社におけるICカード化のシナリオは、まず第一に、従来のクレジットカード機能のICカード化である。これはインテリジェンスを持つICカードの採用により、深刻な問題となっている偽造・改竄等の不正使用による被害を解消するとともに、従来オンライン管理によって行われていた与信管理業務等の一部をICカード内に取り込むことにより、セキュリティレベルを保ちながらオフライン処理等を実現して、既存システムの負荷及び経費を削減し、さらにはロイヤリティプログラムや提携先業務のICカード内取り込みによるサービス機能の向上を目指している。また、第二に、従来のクレジットカードが対象としてきた商取引より、小額の決済にも新たな決済手段を提供するべく、ストアードバリューカードと呼ばれる小額決済システムの導入があげられる。VISAはビザキャッシュを開発し、マスターカードはMONDEXとの提携を行うなど、新たな小額決済システムの提供によりクレジットカード会社のビジネス領域拡大を期待している。さらに、第三に、インターネットを通じたショッピングの際に、クレジットカードを安全に利用するための手段としてVISA、マスターカード等が提唱するSETでは、更に安全な取引引き実現のため、ICカード内で証明書や鍵情報を管理するために、クレジットカード用ICカードを利用することが考えられている。

いずれにしてもクレジットカードのICカード化は世界的に大きな流れとなっており、21世紀はじめにはICカードによるクレジットカード発行が本格化するものと思われる。

c) 交通・運輸分野 <有料道路通行カード（料金自動収受システム）>

既に海外では実用化が進んでいる料金自動収受システムであるが、国内でも実用化に向けて小田原厚木道路で実験が進んでいる。現在、有料道路での渋滞

の一部は、料金所の通行ゲートでの車両停止が原因とも言われ、渋滞の解消とともに、利用者の通行券、現金のハンドリング煩雑さの解消、料金收受の自動化による低コスト化等が料金自動收受システムの導入によって期待できる。利用されるICカードについては接触ICカードと車載機利用が検討されている。

将来的に、現在発行されているハイウェイカードのICカード化が実現すれば、より一層の効果が期待できる。

d) 交通・運輸分野 <定期券及び汎用乗車券>

鉄道の磁気定期券、磁気切符を利用した自動改札導入・普及に続いて、さらに利用者にとっての利便性向上を図るため、非接触ICカード利用による定期券と汎用乗車券の開発が進められている。いちいち改札に定期券や乗車券等を挿入する煩雑さがなく、出札のスピードアップ化も図られ、利用者にとっては導入による恩恵は大きいものと思われる。既に香港では地下鉄、バス、フェリーで共通カードとして稼働しているが、国内でもJR東日本が数度に亘る非接触ICカードによる定期券の実験を行っているとともに、関連企業・団体が集まり、汎用電子乗車券技術研究組合を結成し、ストアードバリュー方式の汎用乗車券の開発を進めており、1998年には地下鉄都営12号線で実験導入されることが決定している。

C. 新たにICカードを利用したカードシステムが構築されると思われる分野

a) 金融分野 <電子マネー>

現在、従来の貨幣に代わり、デジタル情報としての貨幣による決済を実現する試みが数多く行われている。その一つの形態として、カード内にこれらの情報(電子マネー)を内蔵して電子財布としてICカードを利用する方式(ICカード型電子マネー ネットワーク型電子マネー)が有力視されている。実際には、ICカードによる電子マネーも従来のプリペイドカードとしてのデータをICカード内に記録してあるものから、高度な暗号システムにより、デジタル情報として作られたデジタルコインを利用するものまで、システムも技術レベルも多種多様である(オープンループ/クローズドループ型、電子コイン/残高管理型、など分類も様々)。欧米を中心に最先端の電子マネーシステムの開発、導入が進められているが、国内でも新たな決済手法として大きな注目を集めている。従来のプリペイドカード的なものまで電子マネーとしてマスコミ等に取り上げられているが、本格的な電子マネーとして、独自システムの開発・実験導入がすでに行われ、前述のVISAによるビザキャッシュの実験も開始されている。さらに98年にはビザキャッシュの拡大実験とともに、NTT電子マネーおよび郵貯電子マネーと大型国産電子マネーの大型実験開始が予定されている。

貨幣の形態は時代を追って様々に変化している、今後貨幣情報のデジタル化が進み、ICカードによる電子マネーシステムの普及も確実と思われる。

b) 健康・医療分野 <自治体医療カード>

地域住民への医療サービス向上を目指して、ICカード利用の医療カードシステムが、1988年兵庫県五色町を導入されたのをはじめとして、全国の自

自治体でモデル実験として導入されている。I Cカード内に基本情報・検診情報のほか、一部では診療情報、投薬情報まで記録し、診療の際に役立てるとともに、緊急時には救急車等でも必要情報が読み出せるようになっている。自治体住民にとっては、的確、迅速な医療サービスが期待できるとともに、医療機関にとっては、診療の支援情報を入手することができる。これらのプロジェクトは、厚生省や（財）医療情報システムセンタ等により標準システムの構築が図られている。

さらに、これらの医療情報のほかに行政基本情報等もI Cカード内に記録し、行政窓口サービス等で活用しようとする「地域カード」のモデル導入も進んでいる。このカードで各種証明書の自動交付や、申請書の自動交付をはじめさまざまな行政サービスを手軽に受け取ることができる。カード発行対象者は老人検診対象の65歳以上や、乳幼児から学童、40歳以上の成人病検診対象者など、自治体によって異なる。「地域カード」は、地方公共団体の情報化を目指す「コミュニティネットワーク構想」の一環として自治省、（財）自治情報センタより、全国17自治体がモデル自治体として指定されている。1997年よりこのシステムは公開され、希望する自治体は標準システムを低予算で導入することができるようになり、導入自治体の数が増加されることが予想される。

c) I D分野 < 建設業界I Dカード >

建設業界では建設業従事者の管理と、建設現場の情報化のために、建設従事者、および車両へのI Cカード発行準備が進んでいる。建設業では、さまざまな職種の従事者と車両が入場するため、各種トラブルが発生するとともに現場事務が煩雑を極めている。I Cカードの導入により、建設従事者の入場情報管理を自動化するとともに、健康管理、資格管理、勤務管理等を、システム的に行うとともに、車両のカードと合わせて作業履歴、日報、届け出書類等もシステム化し現場事務の情報化を図る。さらには、本社事務所とのオンライン化等も可能になり、大幅な効率化が図られる。

同時に従事者にとっても、健康管理や導入教育が的確に行われるとともに、作業条件の適正化や労災時の的確な対応が迅速に行える。建設従事者は現場間の移動が激しいため、企業レベルのみでなく業界あげての導入が必要となる。建設省、および（財）建設機械化協会により標準システム構築がなされ、本年より業界内に建設施工情報化協議会が設立され、I Cカードの発行が進められている。

d) 放送・通信分野 < 衛星放送加入者管理カード >

地上波放送の電波が届かない地域の多いアメリカで発展したD S S（Digital Satellite Systems / デジタル衛星多チャンネル放送）は、我が国でも相次いで開局される。

我が国では民間放送局が全国ネットで展開されているため「テレビは無料である」という概念が一般的で、このためC A T V（有線テレビ放送）、衛星放送などの普及が今一つ進展していないとも言われているが、D S Sは高機能化・多機能化された新しいメディアチャネルの一つとして、今後の発展が注目

されている。

I Cカード内で放送のスクランブル解除を行うとともに、加入者情報及び視聴情報の管理を行っている(図 1-1)。I Cカード内でスクランブル解除を行うため、デコーダー内で行う処理より物理的安全性が高い、万一の場合もカードの交換によりセキュリティシステムの切り替えが行なえる。また加入者情報、および視聴情報がI Cカード内に記録されているため、視聴した内容によって料金徴収を行なうペーパービュー方式の導入も可能になった。

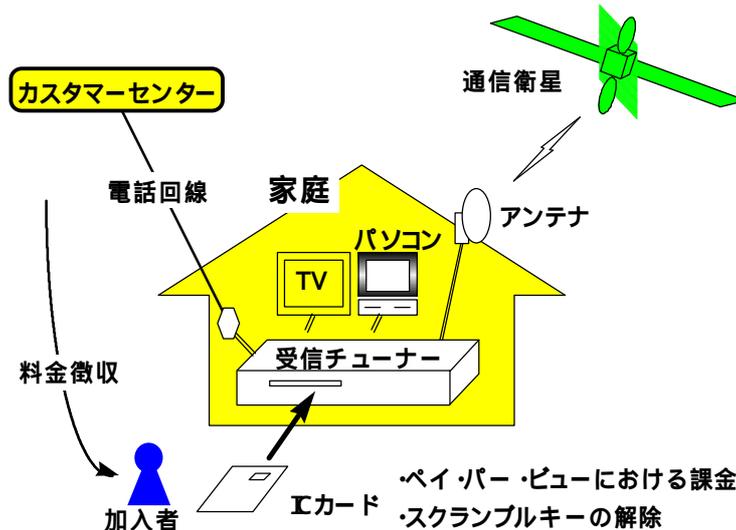


図 1-1 デジタル衛星放送のI Cカードシステム

図 1-1のように、D S SにおけるI Cカードの利用方法は以下の二点である。

i. ペーパー・ビューにおける課金

「どのチャンネルを、いつ、何時間観たか」という情報をI Cカードに蓄積し、一定期間に一度I Cカード内のデータを電話回線を通じて吸い上げて課金する。

ii. スクランブルキーの解除

カードの所有者があらかじめ登録(契約)しているチャンネルを、所有者のI Cカードを挿入することによって視聴できる。

e) 放送・通信分野 <移動体通信S I Mカード>

欧州を中心に普及するデジタル式移動体通信システムG S Mでは、加入者管理、および通信のスクランブル解除をI Cカードを利用して行なっている。S I Mカードと呼ばれるこのカードは、携帯電話に利用される場合はプラグインS I Mと呼ばれる小型のカードである。国内では別方式のデジタル電話方式が採用されているが、N T Tドコモが自動車電話で同様なI Cカード利用を決定している。利用者にとっては電話の買い替え時や故障時、容易に別端末の利用ができるとともに、レンタカー等の自動車電話での利用なども想定できる。

【S I M】

移動通信体すなわち携帯電話は、1990年代に入ってから急速に普及し、ヨーロッパ域内での標準化が急がれていた。そこで登場したのがヨーロッパ共

通仕様であるG S M (Global System for Mobile communication)である。ブリティッシュテレコム、ノキア他の通信事業者、通信機器メーカーが共同して開発したデジタル方式の移動通信システムで、ヨーロッパ40ヶ国、その他中国、東南アジアなど世界110ヶ国で採用され、事実上世界規格とされている。そして92年G S Mに、I Cカードが導入されるようになり、本格的に稼働し始めた。I Cカードには本人I D以外にも多様なデータが保存できこの機能をS I M (Subscriber Identity Module 加入者識別素子)と呼んでいる。

【S I Mの機能】

S I Mには二つの機能があり、一つは加入権と携帯端末の分離、もう一つは多様なサービスのデータ蓄積機能である。

G S Mの利用者にはS I Mカードが発行されるが、このカードにはI Cカードが使用されている。カード内に本人情報、コード解読の秘密鍵に当たるアルゴリズムが記録されており、このI Cカードを携帯電話に差し込んで利用する。利用者が携帯電話を利用する際、ネットワーク管理者と、S I Mの双方向で乱数が送信され、認証されると利用が可能になる。認証の段階は、2段階であり、まずカードを電話機に差し込んだ際に4～8桁のPINにより電話機とカード間で認証が行われ、続いてネットワーク管理側との認証は、G S Mネットワーク側から発信される乱数(要求 RAND)をS I Mカードがアルゴリズム(秘密鍵)によってコード化し返送(S R E S)、S R E Sをネットワーク側は同じアルゴリズムで復号化し送信した乱数と一致すれば認証されるというステップを踏む。この様な認証手続きにより不正使用の防止ができ、複数の携帯電話を、1枚のカードでかけられる。もう一つのS I Mカードの役割としてデータ蓄積機能があるが、これは、G S Mのダイヤル短縮機能、ポケベル、留守番電話、銀行口座の金銭出し入れ、スポットニュースサービス、交通情報、天気予報、スポーツニュースなどの情報提供サービスをS I Mにバイナリ形式で送り、それをテキスト表示させることによって、情報を提供できるようにするものである。将来的には電子マネーシステムに活用することも可能で、実用化が大いに期待される。

【海外の状況】

アメリカは、現在有力な3種の移動通信システムがある。G S M (P C S 1900)、C D M A、T D M Aである。P C Sはワシントン地区、ニューヨーク地区でサービスが行われており、またI Cカードを用いないC D M Aが競合しており、地域によって採用されているシステムが異なっている。しかし、これらのシステムは、相互に補完しあい、互換性があるため、どこからでも電話が掛けるようになっている。

東欧諸国に於いてもG S Mの普及が進んでいる。まだまだ加入者数は少ないものの、94年にハンガリーが、96年にはチェコ、ポーランドが、97年にはスロバキアでG S Mの導入が実現している。また、ノキア、エリクソンなどにより中国でのG S M普及が図られ、加入者数をのばし、またモトローラ、アルカテル、フィリップスなどにより、インド、アフリカ、中東、東南アジア、

ラテンアメリカ、オセアニアに販売が行われ、世界規模での普及が進んでいる。実際、ヨーロッパでの加入者数の年間成長率44%に対し、アジアでは72%にも及び、今後のマーケットとしてアジアが大いに期待されている。

【日本の状況】

日本は独自仕様として、PDC(Personal Digital Cellular Telecommunications System)が採用されており、国際的な販売マーケットには大きく出遅れているが、96年、郵政省とNTTが共通企画の策定で合意し、SIMカードの開発が進んでいる。98年春よりNTT移動通信網がSIMを自動車電話に導入し、DDI系の移動通信会社も98年夏前には導入する。導入されるのは、個人のICカードを携帯移動端末機に挿入することで通話が可能になるシステムである。これにより新たな加入契約をしなくても済むため、携帯電話のレンタルや、複数の携帯電話を、1枚のICカードで利用できるようになる。当面は通話のみに利用するが、将来的には、電話帳機能を持たせるなど、アプリケーションの拡大により、様々なサービスが展開できるようになる。また将来的には、国内、欧州、アジア各地でどの携帯でも利用できるようになる。既に郵政省はGSMとの共通企画とすることを決めており、国際的に利用できる携帯電話の普及が期待される。

f) 行政分野 <健康保険証カード>

社会保険庁では健康保険証のICカード化を検討し、1995年より熊本県八代市で実験を開始している。保険業務のシステム化と、前述の医療カード機能による医療サービスの向上を目指している。

g) 行政分野 <住民基本台帳番号カード>

自治省では住民基本台帳番号の全国統一化により、行政サービスシステムの全国的なシステム化を検討している。この際に、番号カードとしてICカードの採用を検討している。このカードでは前述の医療カード、地域カード等のサービスを加えて、カード所持者への様々なサービスが提供できるカードを目指している。

D. ICカードの将来像

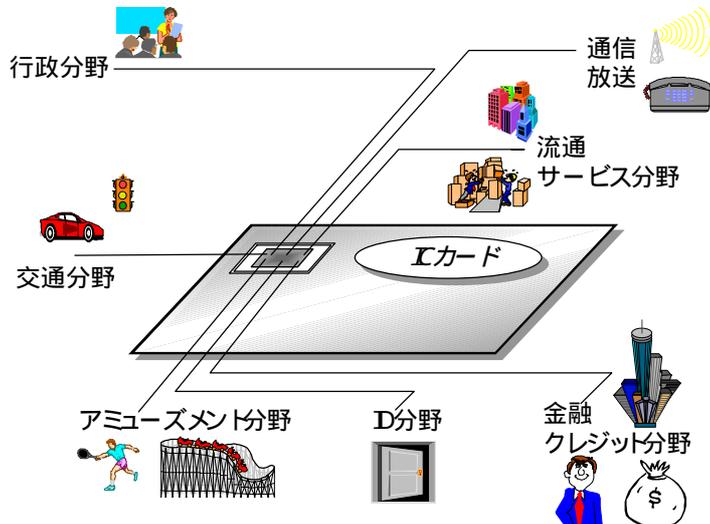


図 1-2 I Cカード展開事例

今後のI Cカードの展開を表すと、図 1-2の様になると考えられる。全ての分野のアプリケーションが相乗りするとは考えにくい、例えば行政カードは別個に普及し、金融、クレジットを中心に各分野の相乗りが考えられる。また、I D分野、交通分野などは、非接触の導入が進み、単体での普及と、接触との統合カードの普及が考えられる。いずれにしても、共通プラットフォームを搭載した多目的I Cカードの普及が考えられる。

1.3 今後のI Cカード潜在市場予測

現在予測される今後のI Cカード潜在市場について、下記の通りまとめた。

A：従来からI Cカードが利用されている分野

B：既存のアプリケーションがI Cカードに置き換わると見られる分野の市場規模を表 1-4に、

C：新たにI Cカードを利用したカードシステムが構築されると思われる分野の市場を表 1-5にまとめた。

表 1-4については(株)シーメディア発行の「I Cカード総覧」における市場規模予測を参考に、既存のアプリケーションにおいて発行されている従来媒体の発行枚数を潜在市場規模の根拠とし、表 1-5については、それぞれのアプリケーションごとに、市場規模を推定する根拠材料を設定し、その現在の統計数値を市場規模の最大値と仮定した。

表 1-4 潜在市場予測 (単位：万枚)

市場	アプリケーション	既存の媒体	既存発行枚数
交通	高速道路	ハイウェイカード	6,000
	鉄道・地下鉄	プリペイド式PETカード	10,000
	バス	バス共通カード	5,000
金融	銀行・郵貯	キャッシュカード	28,000
	クレジットカード	クレジットカード	22,000
流通・サービス	量販店・専門店	プリペイドカード・ポイントカード	3,000
	商店街・ショッピングセンター	ポイントカード	4,200
	ガソリンスタンド	会員証ポイントカード	4,000
	自動車メーカー	メンテナンスサービスカード	6,000
通信	公衆電話カード	テレホンカード	40,000
アミューズメント	スポーツ・レジャー	会員カード	1,500
	会員カード	倶楽部、ビデオ店等会員カード	1,000
	ゲーム・アミューズメント	入場券、会員証、ポイントカード	10,000
	パチンコ	プリペイドカード	300,000
I Dカード	企業団体内	社員証、入館証	6,000
	教育	出欠等管理カード	2,300
	建設	現場管理カード	600
合 計			449,600

表 1-5 潜在市場予測 (単位：万枚)

市場	アプリケーション	潜在市場推定材料	潜在市場規模
金融	電子マネー	全人口が1枚持った場合	10,000
通信	携帯電話	平成9年9月末の携帯電話加入数	3,300
行政	運転免許証	運転免許保持者数	6,600
	健康保険証	健康保険、国民健康保険加入者数	7,800
	行政カード	平成9年10月1日の人口	12,400
医療	医療カード	平成8年10月の全国推計患者数	1,000
航空	航空会社カード	平成9年9月の国内海外線利用者数	500
放送	有料放送カード	衛星放送の97年までの加入者	1000
合計			42,600

1.4 多目的ICカードに求められる要件

ICカード使用者の利便性を高めるためには、一枚のカード上に有効な複数アプリケーションを搭載し、一枚のカードでいつでも多様な利用目的に、しかも安全に使用できるようにする必要がある。また、カード発行者にとっても、多目的ICカードは、アプリケーションあたりのカードコストを下げる事ができ、価値あるものである。このようにICカードの多目的利用の実現は、ICカードを普及させるための鍵であり実用化が期待されている。しかし、多目的利用を実現していくためには、セキュリティ、カードフェイス表示、運用等、多くの課題がある。課題の整理と対応策について述べる。

1.4.1 多目的ICカードの種類

(1) 同一業者の機能付加による多目的利用

事業者が複数のアプリケーションを、同一のICカードに使用して多目的利用。

(例)

カード業者：クレジット+電子マネー

(2) ファイルの領域貸しによる多目的利用

カード発行した事業者が、他の事業者に業務別データファイルを貸し出す。

(例)

銀行と大学：銀行カード+IDカード(学生証)

(3) その他多目的利用<今回は検討しない>

運転免許証と健康保険証など

1.4.2 多目的にする上での課題(1.4.1多目的ICカードの種類(3)項を除く)

課題項目を15項目に整理し、表1-6の多目的ICカードの種類別課題整理一覧表に示す。また表中の種類の項目は<課題と多目的カード種類の関係>に示す通りである。

<課題と多目的カード種類の関係>

- 同一業者の機能付加並びに領域貸しによる多目的利用に共通するものは：<共通>

- 領域貸しによる多目的利用に固有のものは：＜ファイル＞

表 1-6 多目的ICカードの種類別課題整理一覧表

課題項目	種類	内容
セキュリティ	共通	<ul style="list-style-type: none"> ・ ICカードの偽造あるいは端末ソフトウェアの改竄等により不正が起こらないよう管理、運用面での対策が必要である。 ・ データを不正に操作できないようセキュリティの高いOSを使用する必要がある。
発行管理	ファイル	<ul style="list-style-type: none"> ・ 領域を貸し出す側が、共通データを入力し発行管理する。
データ参照	ファイル	<ul style="list-style-type: none"> ・ 共通データ及び提携先毎のデータを参照できることを基本とする。 ・ ポイントなど提携をまたがる場合は、そのデータを共通データに組み込む。
カード費用負担	ファイル	<ul style="list-style-type: none"> ・ 提携先との協議により決定する。
カード紛失	共通	<ul style="list-style-type: none"> ・ 発行機関へ届け出る。
カード破損	共通	<ul style="list-style-type: none"> ・ 発行するまでの破損は、カードメーカ責任とする。 ・ 発行後は、所持者の責任、もしくは、発行主と提携先にて責任範囲を決定する。 ・ 破損状態を診断できるアプリケーションソフトが必要である。
共通データ	ファイル	<ul style="list-style-type: none"> ・ 協議機関を設けその内容を決定する。
カード有効期限	ファイル	<ul style="list-style-type: none"> ・ 提携先は、カード発行主の有効期限に合わせる。
データ移行処置	共通	<ul style="list-style-type: none"> ・ カード紛失・破損時の再発行 1) 各アプリケーション毎のデータを発行機関に集めコピーする。 2) 新規発行と同様に共通情報をコピーし再発行する、後に各提携先毎でバックアップデータよりコピーもしくは更新する。
データバックアップ	共通	<ul style="list-style-type: none"> ・ カード紛失、破損等の再発行を行う上で、各アプリケーションデータのバックアップ管理が必要である。
データの追加・削除	共通	<ul style="list-style-type: none"> ・ アプリケーションデータファイル及びデータの追加・削除における権限規定を策定し運用、管理する必要がある。
認証	ファイル	<ul style="list-style-type: none"> ・ 領域貸しの場合、各々のサービス機関にて認証する必要がある。
処理時間	共通	<ul style="list-style-type: none"> ・ サービス利用を行う上で、その動作に支障が無いまたは、感じない程度の時間に処理スピードを上げる必要がある。 1) 定期券などのキー通過速度に合わせる場合など：1秒以内 2) その他：3秒以内
カードフェイス表示 (カードの有効期限表示)	共通	<ul style="list-style-type: none"> 1) ICそのものの有効(寿命)期限の表示 2) 発行カードそのものの有効期限の表示 <p>いずれもIC内に各サービス毎の有効期限を設け、内容の書き換えが行える事が必要である。</p>
カードフェイス表示(問合わせ)	共通	<ul style="list-style-type: none"> ・ 各々のサービス機関毎のフリーダイヤル、機関名称、住所を記載する必要がある。

1.4.3 管理運用上の制約

- (1) カードフェイスに記載されている有効期限と付加サービスの有効期限との連動が取れない場合。
- (2) 各々でID管理、認証ができない場合。
- (3) 物理的にデータ容量を超える場合。
- (4) サービスにより匿名性が必要で個人の特定制と矛盾が生じる場合。

1.5 ライフサイクルとセキュリティについて

前回の中間成果物では、カードのライフサイクルとセキュリティについて、各段階における一般的なセキュリティ確保の要件に関し、ISO 9992の規定に基づいた検討結果を報告した。その間、JAVACardや、MULTOSのようなICカードの多目的利用に関する検討が進み、従来から繰り返されてきたチップが高価格であることへの批判を躲すための一方便としか思えないような、容量の大きさだけからのみ語られるICカード多目的利用の話から、多目的利用を具体的に可能とする技術の方向性が示されるようになった現況から、当然の事として、ICカードを多目的利用するため、複数のアプリケーションを実装する場合のセキュリティ面での問題点を検討する必要がでてきた。また、これまであくまで破られてはならない前提で、ライフサイクルとセキュリティの検討を行ってきたが、永久・絶対に安全という保障はどこにもなく、実運用上においては、破られた場合に、如何に可及的速やかに解決を図るか、どのようにリカバリー策を講じておくか、ということも非常に重要と考えた。この点に関しては、現段階では不明な点も多く、主として問題提起を行なうこととする。参考に、図 1-3にライフサイクルの概念図を示す。

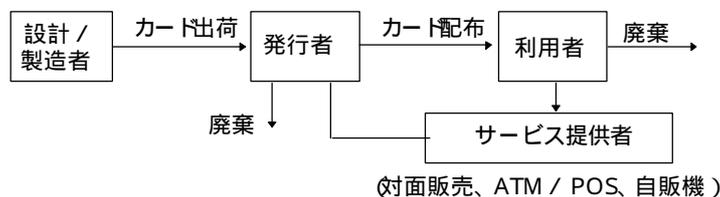


図 1-3 ICカードのライフサイクル

1.5.1 セキュリティ管理

表 1-7 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
			・カード製造者IDの設定	ISO9992
発行	初期化	発行者用仮PIN の認証	・発行者用本PINへの書換	
		発行者用本PIN の認証	・ファイル構造の生成	
	データ登録 (発行)	ファイルアクセス のためのキー認証	・アクセス制御のための各種キー の設定	以後のアクセス 制御を決定
			・各個人データの登録	
運用 使用	データ取得	カードの認証		ICカードの正当性 の確認
		ファイルアクセス のためのキー認証	・データの取得	
	データ登録	ファイルアクセス のためのキー認証	・追加サービスのデータの 登録	
廃棄	カード終結	ファイル、暗号 キーのロック	・PIN番号変更	
			・業務データ消去 ・個人データ消去	

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 1-7に示すようなセキュリティ管理が必要であると考えます。

1.5.2 不安要素とセキュリティ対策

1.5.2.1 不安要素

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素を図 1-4に示す。図 1-4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 1-4で示した不安要素は、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ます。

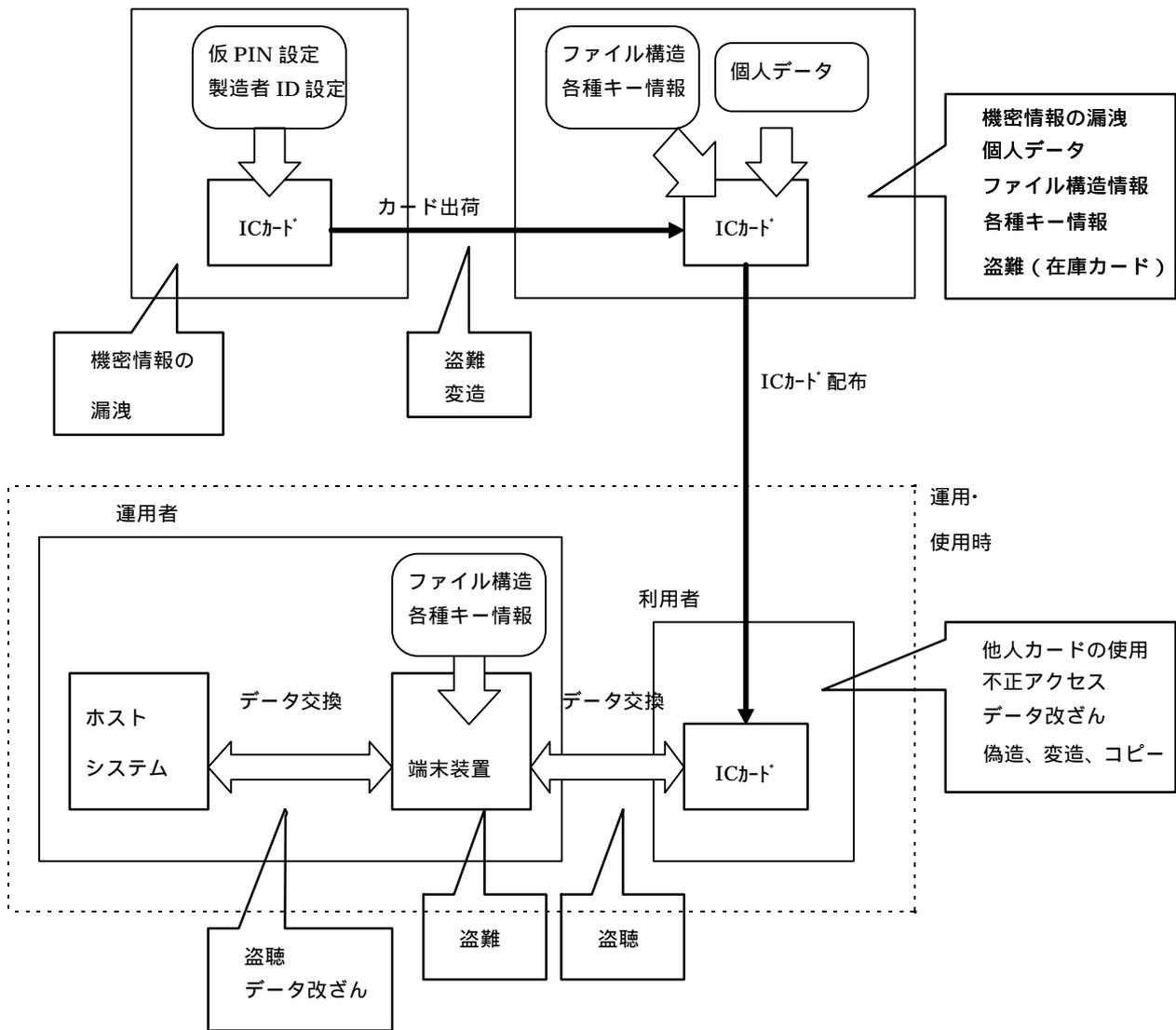


図 1-4 ICカードのライフサイクルにおける不安要素

1.5.2.2 セキュリティ対策

表 1-8に、図 1-4で示した不安要素に対するセキュリティ対策を示す。

表 1-8 不安要素とセキュリティ対策

段階	不安要素	セキュリティ対策
設計 製造	機密情報の漏洩 盗難・変造	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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

	ファイル構造情報 各種キー情報 盗難（在庫品）	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 【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	・ 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。 ・ 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

ここで示したセキュリティ対策についても、部内関係者による仮PIN、本PINの漏洩等、部内関係者によりセキュリティが破られる可能性はあるが、ここでは一般的な対策を示す。システム関係者を含めた内部犯罪を想定した脅威と対策は、1.5.3項に示すが、影響が大きいだけに防ぐためには、製造・設計、発行の各段階において情報を一人に集中せず分散化させる等、システムとして情報管理を強化する方向での対処が望まれる。また、ICカードのように大量に配布され、回収・データ変更が困難なものに関しては、MONDEXの暗号方式の切り替え、JavaCard等のダイナミックローディング機能のように、時間とともに弱体化する暗号アルゴリズムを変更する仕組みを盛り込むことを検討すべきと考える。

1.5.3 ICカードのライフサイクルとリカバリ策について

ICカードのライフサイクルにおける不安要素と、セキュリティ対策については先に述べた通りであるが、其々が破られた場合（あってはならないことなので、余り想定されてい

ない)の不安要素と対応策について示す。

1.5.3.1 発行者用仮P I Nの漏洩

(1) 想定被害

発行者用仮P I Nの情報とカードが入手できれば、運用時のデータ送受信情報をタッピングすることにより、発行コマンドを知っていればどんなシステムのカードであっても発行できてしまう。(完全なデッドコピーではないかもしれないが、チェックには引っかからない程度に)

(2) 対応策

発行者用仮P I Nの漏洩を避けるために、P I Nを分割して情報が一人に集中しない等、仕組み作りが必要と思われる。(これは他の不安要素についても同様)

対応策として、タッピングされても送受信データが解釈できないように暗号化する案が考えられ、より安全な対策としてセキュアメッセージング機能を利用することも考慮すべきである。

1.5.3.2 発行者用本P I Nの漏洩

(1) 想定被害

発行者用本P I Nの情報とカードが入手できれば、他のシステム用のファイルを空きエリアに追加することができる可能性がある(他システムの発行情報は先のタッピングによる)。

また、発行者用本P I Nはスーパーバイザ的なキーに使われることが多いと思われるため、たとえばファイルのアクセス権をすり抜けたら、ロック解除が可能となった等、データの改竄につながる。

(2) 対応策

流布しているカードの本P I Nを変更することが考えられる。しかし、一斉には変更できないため、ある程度の被害は覚悟しなければならない。

1.5.3.3 アクセス情報(アクセス権情報、アクセスキー)の漏洩

(1) 想定被害

ファイルアクセスが可能となるため、ファイル情報を盗聴されたり、改竄されたりする。

(2) 対応策

流布しているカードのファイルアクセス情報を、オンラインで変更することが考えられる。しかし、一斉には変更できないため、ある程度の被害は覚悟しなければならない。

1.5.3.4 カードの紛失・盗難

(1) 想定被害

拾った盗難カードが、P I N入力なしで利用できるものであれば、不正使用されてしまう。プリペイドカード、クレジットカードが該当する。

(2) 対応策

システム一意の識別子をカードに書込んでおくことにより、紛失・盗難時にはブラックリストチェックを行い、カードをロックして使用不可能とする。

1.5.3.5 暗号アルゴリズム・鍵の変更

暗号強度は時間とともに弱体化するものであるから、MONDEXで実現されている暗号方式を変更する仕組みを盛り込むことが考えられる。また、JavaCardのように暗号アルゴリズムをダイナミックに変更していく方式も検討すべきである。

1.5.4 複数アプリケーションの実装可否について

従来、一つのシステムで複数アプリケーションを一枚のカードに実装することは行われてきたが（機能的には実現できるけれども、1アプリケーションしか実装していないケースがほとんど思われる）、これからはJavaCard、MULTOSの概念に見られるように、異なる業種・業態の複数アプリケーションを一枚のカードに実装することが求められてくると考えられる。異なる業種・業態の複数アプリケーションを実装する場合のライフサイクル上の問題について検討する。

1.5.4.1 権利主体とユーザ用件対象者による分類

カード発行、サービス業務、カード所有者の各権利主体を、誰が担うかで整理して以下の3種類に分類する（ニューメディア開発協会の検討を参考にしている）。

(1) 従来

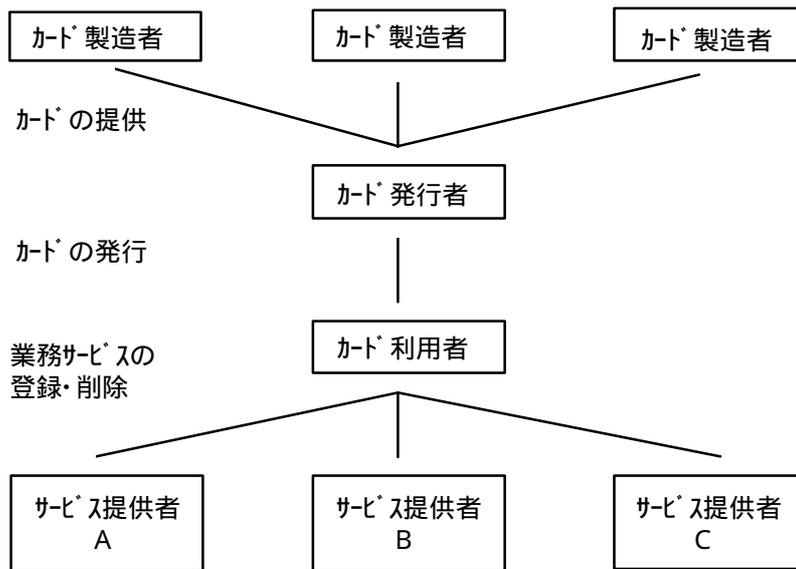
権利主体	ユーザ用件対象者
カード発行処理主体	カード発行者
アプリケーションサービス発行処理主体 削除処理主体	カード発行者
カード所有者	カード発行者

現在、一般的に行われているケースで、カード発行者が全権限をもち、追加発行もカード発行者のもとへ回収してサービス追加を行うものである。

(2) 検討案

権利主体	ユーザ用件対象者
カード発行処理主体	カード発行者
アプリケーションサービス発行処理主体 削除処理主体	アプリケーションサービス提供者
カード所有者	カード発行者

複数アプリケーションを実装する形態として検討されている方法である。構成例を以下に示す。



(3) 将来

権利主体	ユーザ 用件対象者
カード発行処理主体	カード利用者
アプリケーションサービス発行処理主体 削除処理主体	アプリケーションサービス提供者
カード所有者	カード利用者

この方法は、カード発行者がサービスを規定するのではなく、利用者がサービスを選択し、カードに関わる一切の責任を負わなければならないため、現状では実用化困難な発行処理形態と想定されている。

1.5.4.2 検討

ここでは、1.5.4.1(2)のケースを想定して検討する。

(1) 複数アプリケーション提供者が同一と異なる場合

提供者が同一の場合、使用するサービスファイル・データ等に対するセキュリティは、提供者の責任において処理される（場合によってはサービス間でファイルアクセス権を異にする必要はないかもしれない）が、提供者が異なる場合には、サービス間でファイル・データ等についてセキュリティが確保される仕組みが必要となる。

(2) 追加アプリケーションを書き込む場合の方法論のパターン化(端末による発行を想定している)

セキュリティの確保された場所でSAM(Security Access Module)を内蔵したサービス業務発行端末により追加アプリケーションの書き込みが行われる。

サービス提供者の認証

カード発行システムとサービス業務システム(端末)との相互認証により、サービス提供者(SAM)がカード発行者との間に正しい契約を結んでいるかを認証す

る。

カードの認証

カード発行システムとカードとの相互認証により、正しいカード発行システムで発行されたカードであるかを、カード内の認証キーを用いて認証する。

サービス業務発行

サービス提供者、カードの認証がされた後、カード利用者のPINをキーとしてサービス業務発行が行われる。カード内には、サービス提供者の識別情報、その他必要情報が登録される。

(3) ICカードの空き領域の表示方法や運用について

サービス業務発行システムでは、ICカードのメモリ空き容量がサービス業務の登録に十分であることを確認する必要があり、その機能を実現する。

(4) サービス提供者が異なるアプリケーションを追加した場合のカード表面デザイン及び運用方法

現状、シールを貼る程度の解決策しかなさそうである。将来的にはサービス提供者発行処理システムで、業務追加するときシールの代わりに印刷するような形態が想定される。

(5) ダイナミック要求の仕向先のパターン化ならびにデータの管理要件や運用

サービス業務追加は、ダイナミックローディング機能でしか実現できないわけではないが（従来機能であってもサービスに制約条件を付与することで可能）、サービスで使用する特有機能までローディングできるという意味で、ダイナミックローディング機能があれば自由度は高いと言える。

1.6 ICカード技術動向

1.6.1 ICカードOS

利便性の高い多目的ICカードを実現するためには、高度なセキュリティを持った多機能ICカード用オペレーティングシステム（ICカードOS）が必要である。

近年のICカード用LSIチップの技術進歩には、CPU性能、ROM、並びにファイル容量の大容量化等目覚ましいものがある。このようなLSIチップの技術革新は、パーソナルコンピュータ（PC）のオペレーティングシステム（OS）のようなOSとしての基本的機能を持った多機能ICカードOSを実現させた。

ICカードOSは下記のような基本的機能を持つ必要がある。

- 高度なセキュリティ機能
- 多様なアプリケーションソフトに対する共通プラットフォーム
- 利便性の高い運用機能
- LSIチップに対する独立性

今日、このような機能を持った代表的なICカードOSとして、JavaCard、並びにMULTOSがある。これらのOSについて紹介する。

1.6.1.1 JavaCard

(1) 要件

アーキテクチャニュートラル
ネットワークローダブル・オブジェクト
セキュリティ

(2) アーキテクチャニュートラル

プラットフォームに依存しない開発・動作環境
共通のJava実行環境を準備すれば、対応アプリケーションが使用できる。

メリット

- 利用者は多くのアプリケーション、カードから自由に選択

開発環境と動作環境の分離

特別な開発環境が不要、対応アプリケーションには多くのカードが、カードには多くのアプリケーションが提供される。

メリット

- 開発投資の低減
- 多くの実行環境（カードとアプリケーション）が予め準備される相乗効果

汎用言語で開発

ICカードも一般的なコンピュータアプリケーションへ。

メリット

- UNICODEで言語の壁（日本語・英語）を解決
- 多くの開発者が参入可能

(3) ネットワークローダブル・オブジェクト

既存のネットワークを利用して実現

A. アプリケーションの配布・追加・変更

発行済みのICカードに、アプリケーションを追加、変更できる。

- カード発行者以外もアプリケーション提供者

B. アプリケーションの生成（起動）・停止

アプリケーションの動作制御（アプリケーションサービスの制限）

C. アプリケーションの消滅

配布済みアプリケーションの消去可能（アプリケーションサービスの消去）

(4) セキュリティ

個人データの保護

個人データを不正なアプリケーションから保護

異なるアプリケーション間のデータ保護

アプリケーション間のデータ破壊、不正使用を防止

- 不特定多数のアプリケーション共存が発生

アプリケーション配布時の改竄、盗聴などの不正行為の防止

アプリケーションプログラム配布時の暗号化、電子署名機能の実現

1.6.1.2 MULTOS

MULTOSは、JavaCardと同様、「プラットフォームを問わないアプリケーシ

ョンの実現」を基本コンセプトとして開発されたICカード用のOSである。従来のパソコンにおける基本OSと同じようにOSとアプリケーションとを独立させ、多様なアプリケーションに対し共通のプラットフォームを提供する。

従来は、互換性のないOS、アプリケーションをICチップごとに開発しなければならなかったが、MULTOSはカードOSがハードウェアの違いを吸収し、「MEL言語」で書かれたアプリケーションであれば異なるハードウェア上でも実行が可能であり、1枚のカードに複数のソフトを搭載することができる。

発行済みカードへアプリケーションの追加、更新、削除も可能である。またアプリケーションごとにファイアウォールを設けることによって、セキュリティを高めている。

(1) アプリケーションの開発

MAOSCO.Ltd (MONDEXインターナショナル社の子会社)

ライセンス供与

アプリケーション開発のための仕様書を入手

(2) アプリケーションの追加・更新・削除

方法

発行されたMULTOSカードは、カード固有の認証キー、およびカード発行者のデータを持っていて、アプリケーションの追加・更新・削除をする場合には、カード発行者の同意が必要(カードへのインストールの際に、アプリケーションにカード固有のキーと、カード発行者の同意書を添付する必要がある)。

MULTOSのアプリケーションの暗号化

電話回線、ATM等通信回線を通じて送受信

アプリケーションの復号化(MULTOSカード内部)

メリット

アプリケーション追加、更新、削除に当たって、カードの回収、再発行等が不要

(3) MAOSCO.Ltdの役割

MULTOSのライセンス供与

認証キーの発行・管理

ライセンスフィー、及び認証等のカード1枚/1アプリケーション当りの手数料管理

(4) MULTOSコンソーシアム

参加企業

MasterCardインターナショナル、MONDEXインターナショナル、大日本印刷、日立、モトローラ、ジェムプラス、シーメンス、キーコープ、G&Dの9社が加盟(将来的に通信系が加わり、12社になる)。

主旨

MULTOSの普及、業界標準化、継続的開発(バージョンアップ)

(5) MULTOS採用の動向

ヨーロッパでは、通信会社と銀行などが提携して、携帯電話用ICカードの機能(GSM)と、クレジット機能(EMV)、及び電子財布(MONDEX)の機能を併せ持った多機能ICカードが98年中にも発行される可能性があり、北米ではマスター

カードがMONDEXを搭載したクレジットカードの発行を検討している。

わが国でもマイカルカードがMULTOSをOSとする多機能カードを発行するとの新聞発表を行っている。

1.6.2 ICカードLSIチップ

ICカードにはリーダライタと端子を接触させてデータのやり取りをする接触ICカードと、非接触でデータを読み書きする非接触ICカードがある。さらに、接触・非接触の両方の利点を生かすために生まれたメモリ共有型複合カードがある。これは、接触・非接触モジュールをワンチップ化したものである。

非接触ICカードの仕様は各社各様であるため、現在LSIは主にカスタム用として開発されている。従って、ここでは、仕様が明確になっている接触ICカードのLSIチップを中心に述べる。

ICカード市場としては、電子商取引等の金融分野での普及が今後とも重要視されていくものと思われる。それら電子商取引では高い安全性が要求されるため、暗号処理が必須の要件であり、ICカード用LSIチップの仕様において重要な検討項目の一つと考えられる。

そこで、その暗号処理に視点をおいてみると、共通鍵方式暗号で現在提案されているものについては、現行ICカード用LSIの主流である8ビットCPUの処理能力で十分な処理性能が得られる。しかし、公開鍵方式暗号で現在提案されているものは、ベキ乗剰余型の演算方式を使うものが主流であり、共通鍵方式暗号に比べて演算量が飛躍的に増大する。このため公開鍵暗号方式を扱うICカード用LSIでは、8ビットCPUとは別にコ・プロセッサと呼ばれる暗号処理専用回路を備えている（共通鍵方式暗号の専用プロセッサを持っているICカード用LSIも存在する）。

今後さらに市場が開けていくと思われる電子商取引等に利用されるICカード用LSIは、公開鍵方式暗号を処理するコ・プロセッサを備えたものを前提としている。以下、コ・プロセッサを搭載したICカード用LSIの現状と次期、さらに将来の展望について述べる。

1.6.2.1 現行品の特長

現行品のコ・プロセッサを搭載したICカード用LSIを比較すると共通した仕様の傾向が見えてくる。この共通する仕様が、特に電子商取引に利用されるICカード用LSIに要求される現時点でのチップについての要件と考えられる。以下、CPU、ROM、RAM、不揮発性メモリ、コ・プロセッサ、チップサイズ、電源、LSIプロセス技術、耐タンパ技術についてその仕様の特長について述べる。

(1) CPU

現時点では全て8ビットCPUを採用している。68HC05（モトローラ）、80C51（インテル）、Z80（ザイログ）といったマイコンメーカーのCPUをそのまま流用しているものが大半である。それ以外の場合は、各メーカー独自のCPUを搭載している。

(2) ROM

ほとんどのLSIが10～20KバイトのROMをカードOS用に備えている。8ビットCPUを制御し、現行要求される機能を満足するには、この程度の容量が必要となると考えられる。

(3) RAM

作業領域として512バイトのRAMをほとんどのLSIが搭載している。現行取り扱いが要求されるデータ量と処理性能を考えると、最低この程度の容量が必要になると考えられる。

尚、ほとんどのLSIが、暗号処理の作業領域用に専用のRAMを別に搭載している。

(4) 不揮発性メモリ

不揮発性メモリ技術は、一部強誘電体メモリ(Ferroelectric RAM)を使っているメーカーもあるが、EEPROMが主流である。容量は、最大で8Kバイトである。但し、多目的用途のカードの要求に伴い、取り扱うデータ量が増大しているため、容量の不足が指摘され始めている。

EEPROMに要求される性能として、エンデュランスとリテンション性能がある。エンデュランスはEEPROMに何回データを書き込み・読み出しをしても問題ないかを示す性能であり、現在EEPROMでは 10^5 回が世界の標準である。また、リテンションは書き込んだデータが+85℃で何年消去されないで保持されるかを示す能力であり、現在の世界の標準は10年である。これらの値は、今後ますます大きく、また長くなっていくものと考えられる。

(5) コ・プロセッサ

公開鍵方式の暗号処理専用の回路をコ・プロセッサと称している。公開鍵暗号方式としては、デファクト・スタンダードと言えるRSAを全てのメーカーがサポートしている。これに加えてDSAなど複数の公開鍵暗号方式をサポートしているメーカーもある。

取り扱える鍵長は、最大1024ビットまでのものが大半である。電子商取引の決済プロトコルのデファクト・スタンダードになると思われる「SET」においては、ルートCAを除いては1024ビットの鍵長が推奨されている。従って、ここまでの対応が要求されるものと考えられる。

性能は、鍵長512ビットと1024ビットでのRSA暗号方式のデジタル署名の処理時間で示すのが一般的である。鍵長512ビットの場合には100m秒以下、鍵長1024ビットの場合には500m秒以下の処理性能が一つの目安と考えられる。尚、この値は、暗号処理の方法として中国剰余定理を使用した場合のものである。

(6) チップサイズ

ICカードには、その取り扱い方から曲げに対する耐力が要求される。ICカードが曲げられるとチップにもその力が加わり信頼性が損なわれる。これを回避するためには、チップサイズを小さくする必要があるが、過去の実績からチップサイズの最大限度は、25mm²程度とされ、現行のチップの大半がこれ以下のチップサイズとしている。最近の傾向としては、より高い信頼性要求に基づき、3mm×5mmといったチップサイズを一部のメーカーで実現している。

さらにチップに要求される項目としては、チップの厚みがある。カードにLSIを内蔵するためには、カードの使用者から見れば薄いチップの方が好まれる。しかし、チップが薄くなればなるほど割れやすくなるので、現在は250 μ mで対応している。非接触カードの場合には、チップが完全にカードに入ってしまうために、チップ厚をより薄くする必要がある。

(7) 電源

ほとんどの製品が、従来の5V単一電源に加えて3V対応も可能としている。3V対応は、低消費電力化、ポータブル機器でのICカード利用を目的としている。尚、3V未満の対応については、現在、ISO/IEC7816にて審議中である。

(8) LSIプロセス技術

不揮発性メモリとしては前述の通りEEPROM、その他のメモリとしてROM・RAMを加え、残りのロジック部はCMOS技術が使用されている。CMOS、プロセスルールとしては、0.8 μ m程度のサブミクロン技術をほとんどのメーカーが採用している。

最近は、プロセスルール0.6 μ mで量産対応しているベンダもでてきている。

(9) 耐タンパ技術

現在、開発中のLSIは、磁気カードで発生したような偽造問題が発生しないように耐タンパ回路を内蔵している。耐タンパとはアタッカが、LSIを解析し、その動作を解析して、中のデータを改竄、偽造することを防止する回路/仕組みのことで、銀行、クレジットカード用LSIはこのタンパ回路を内蔵していないと採用されない。耐タンパ回路については、さまざまな論文が発表されているが、ここまで実施すればタンパ回路はパーフェクトであるということではなく、アタッカの技術の進歩に合わせて、一步先を進んでいる必要がある。

タンパ回路の例としては、周波数検知回路、電源検知回路、温度検知回路などがある。

大半のベンダは、周波数検知回路、電源検知回路を最低限装備している。以下主な回路の概要を述べる。

周波数検知回路

アタッカが、CPUへのクロックを1命令ごと入れながら解析する手法をとることが考えられ、この解析を防ぐために低周波数回路を内蔵している。

電源検知回路

規格電圧以外の電圧を印加して動作が不安定になることを防止するために、電源電圧のモニタ回路を内蔵させている。これにより、正常以外の電圧ではLSIは動作しないようにしてある。

温度検知回路

LSIはどんな温度でも動作するというわけではなく、必ず最適な動作温度というものがある。この動作温度外になったとき動作が保証できなくなるため、温度検知回路を設け、規格温度外ではLSIの動作を停止させる。

1.6.2.2 次期ICカード用LSI

次期I Cカード用L S Iの案内が幾つかのメーカから出されている。これらの仕様、および現状の問題点を整理すると次期I Cカード用L S Iに求められる仕様が見えてくる。以下、メモリ、コ・プロセッサ、L S Iプロセス技術について要求される仕様を記述する。

(1) メモリ

不揮発性メモリに関しては、次期製品ではE E P R O Mに代わる不揮発性技術は、まだ出てこない。現行問題が顕在化している容量不足の解消を図ることが先決と思われる。次期製品の容量は、各社とも16 Kバイトを案内している。

また、I Cカードを使ったサービスが拡大し、要求される機能が多岐に亘ってきている。このためカードO Sでサポートする機能が増えるため、カードO Sを格納するR O M容量も20 ~ 30 Kバイトと増大している。これに加えて作業領域であるR A Mも、倍程度容量の増加が図られている。

(2) コ・プロセッサ

コ・プロセッサの強化としては、最大鍵長の拡大と処理性能の向上が図られる。鍵長は、最大2048ビットまでのサポートが案内され始めている。処理性能については、現行の2倍程度を目標にしている。中国剰余定理を用いたR S A暗号方式でのデジタル署名において、鍵長512ビットの場合には50 m秒以下、鍵長1024ビットの場合には250 m秒以下の値が案内されている。

(3) L S Iプロセス技術

各種機能強化を図るに当たっては、チップサイズの維持、あるいは更なる縮小が前提条件となる。従って、C M O Sサブミクロン技術の微細化がより一層図られ、0.6 μmを下回る設計ルールが採用されてくる。

また、チップ厚においては、特に非接触I Cカードの場合、50 μm以下にする必要がでてくるであろう。

1.6.2.3 将来

ここでは、2000年に向けてのI Cカード用L S Iの機能強化について記述する。一部のメーカは開発の概要を明らかにしている。また、現状の問題点、市場動向などからあるべき姿が模索できる。ここでは、将来採用されると考えられる技術について、その一端を紹介する。

(1) 不揮発性メモリ

不揮発性メモリの技術としては、現行のE E P R O Mに加えてF R A M、F l a s h - E E P R O Mが採用される。F R A Mは、E E P R O Mに比べてセルサイズが小さいため、チップサイズ縮小あるいは容量拡大が図れる。加えて書き込み処理時間の短縮、低消費電力といった特長がある。F l a s h - E E P R O Mは、大容量化を図れる特長がある。

(2) 高速化

I Cカードが扱うデータ量の増大、サービスの多様化から、処理性能の向上が要求されてくる。特にC P U周りの性能向上が図られると考えられる。現行の8ビットC P Uのビット数の拡張、内部クロックの高速化といった手法が取られるものと思われる。C P Uについては、R I S Cアーキテクチャの採用の検討も進められている。

システム動向としても、現在、各社ごとに異なるLSIを使用するときに、開発環境をそのたびに変更する必要がでてくるが、このような不都合をなくすために、開発言語としてJava（米国Sun Microsystems社の商標）を使用するようになると考えられる。Javaのアプレットと言われるプログラムをICカードに乗せて動作させるが、これは中間言語であり、カードはそのアプレットを解釈しながら動作する必要があるため、そのために必要な処理能力はより高いものが要求される。これに対してやはり8ビットCPUでは困難であり、16ビット、32ビットCPUを使用したシステムに移行すると考えられる。

(3) 非接触との一体化

交通分野では料金収受の利便性から非接触が要望されているが、金融決済分野では、安全性、決済意志の確認を考慮して接触が引き続き要望されている。両者に対応できる多目的カードとして接触と非接触の一体化が進むと考えられる。既に幾つかの製品が発表されているが、非接触部分、特に通信方式の標準化が遅れている。この標準化の進行あるいは業界標準の確立が本分野の課題である。

LSIは従来の機能にRF部（無線I/F）を加えたものが1チップで実現される。従ってこの一体化カードは、1チップLSI+アンテナで構成される。

1.6.3 ICカード素材

表 1-9 ICカード素材一覧表

	カードタイプ	特徴	用途
接触ICカード			
塩ビ系	一般グレード	自己消火性 素材が低価格	キャッシュカード クレジットカード
	耐熱グレード	自己消火性 耐熱性に優れる	SSカード カーライフカード
非塩ビ系	超耐熱グレード	自己消火性なし 最も耐熱性が高い	ETC用ICカード SIMカード
	インジェクションタイプ	成形が容易で低コスト	電話カード
非接触ICカード			
塩ビ系	一般グレード	自己消火性	磁気ストライプとの コンビネーション
非塩ビ系	一般グレードPET	自己消火性なし 薄型加工可能	鉄道改札用 薄型化用

現在ICカードに用いられているカード素材には、通常の使用に耐えられる仕様、また用途によって薄型素材、耐熱性、対環境性が求められている。通常は塩ビ系素材が用いられることが多く、用途としては幅広く用いられている。この塩ビ系はカード素材として従来から最も多く用いられている素材で、加工が容易であり、自己消火性（着火しても燃えずに自然消火する）を持っている。但し、加熱された場合に变形しやすいため、耐熱性を持たせた塩ビが開発された。しかし、塩ビ系カード基材は、消却する際にダイオキシンを発生させるため、環境問題が問題視される中、対環境性に優れたカード素材が求められるようになり、現在、非塩ビ系素材が開発され、耐熱性、対環境性に優れたものとして紹介

されている。しかし、この素材には自己消火性が無いため、今後の開発が期待されている。

ICカードに用いられるカード素材を表 1-9のようにまとめるが、各メーカー毎に開発を進めている現状である。

2 接触I Cカード利用ガイドライン(決済分野)

1章では、第一段階として、一般的なI Cカードの現状調査・分析という形で、I Cカードの標準化動向、技術動向、想定される利用分野の特性や多目的利用の課題等に関し、WG内での検討・議論だけではなく国内外の利用事例や導入の為の実証実験の事例についても資料収集や現地の訪問調査を行い、これらに関し整理した内容を記述した。

本章では、第二段階として、より具体的なI Cカード利用の在り方を模索するため、先ず、接触I Cカードの利用方法の検討として、クレジットカード/プリペイド型電子マネーを主体とする具体的なアプリケーションの想定に基づいて、実用化・普及の具体的な実現策をも視野に入れ、運用面の課題・要件の抽出整理、および可能な限り課題に対する解決策をも含めた検討を中心とする活動結果について述べる。

2.1 検討対象選定の背景

主たる検討対象として、クレジット、プリペイド型電子マネーを選択した事由は以下の通りである。

(1) ECOMの基本命題との整合

ECOMの基本命題は、『我が国におけるコンシューマEC(企業と消費者間=‘B to C’)の実現と普及を目指し、その為に必要な様々な共通基盤の整備』であるが、国内の状況を客観的に分析すると、現状では当分の間リアルモールにおけるECが圧倒的に主流であると言わざるを得ないこと。また、決済分野がコンシューマECにおいて最も重要な分野であること。

(2) 道具としてのI Cカードの適正

リアルモールにおけるコンシューマEC、特に、その中の決済分野を担う最適な道具は何かを考えると、携帯性に優れ、従来の磁気カードに比べ、カードの偽造・変造が非常に難しく、且つ、オフラインでのカード真正性のチェックが可能であることから、偽造・変造の抑止効果も期待できるI Cカードが最適であること。

(3) WG7の基本命題との整合

WG7が活動期初に掲げた基本命題は、『I Cカードの実用化・普及』であり、これを実現する為の要件は次の通りである。

インフラストラクチャーの整備

I Cカードの実用化・普及において特に不可欠なものは、端末(R/W)インフラストラクチャーの整備である。特に、民間企業が決済機能付き汎用I Cカードを発行する場合は、カード発行時点で日常の利用に不足のない現実の利用場所の提供として端末設置を行なっておく必要があり、そのカード発行・端末設置の前提となるのは次の事柄で、これなくしては何事も始まらない。

A. カード利用に関する契約の締結(発行者・消費者間)

B. カード取扱いに関する契約の締結(発行者・加盟店間の加盟店契約)

整備に要する投資コスト負担並びに対応時間の削減

前述の通り、可及的速やかな端末インフラストラクチャーの整備が重要であるが、一朝一夕に行なえるものではなく、整備には多大なコストと時間を要する。特に複

数の発行者の混在を想定した場合の解決策としては、以下の事が考えられる。

A. コストの削減策

- a) 端末仕様の共通化による低価格端末の開発
- b) 共用端末の共同設置

B. 対応時間の削減策

現実的な対応の基本は、導入し易いところから、必要なところから対応することである。

a) 既存スキームへの切替えによる対応

純粋に新規ビジネスとして一からの構築は極めて大変であり、現在ビジネススキームとして成立しているものの切替えが現実的である。その意味において、クレジットカードやプリペイドカードは、ICカード化による基本機能の継承・向上は非常に現実的、且つ有効な対応策の一つである。

b) 既存インフラストラクチャーの活用

上記のクレジットカードやプリペイドカードの加盟店網自体が立派なインフラストラクチャーであり、特にクレジットカードの場合、ICカード化しても利用金額に応じてオーソリゼーションが必要であり、既存ネットワーク網の活用を含めて、カード利用も多い現行磁気カード端末設置店のICカード対応端末への置換えが、現実問題として普及のために極めて重要である。

c) 共用端末の共同設置

一般的に共用端末の共同設置はコスト削減策でもあり、整備対応時間削減策でもある。特に、クレジットカード業界には、既に磁気カードベースのCAT端末共同利用システムが存在し、50万台強の端末共同利用が管理・運用されており、これに習い、これをベースとすることも普及実現のための有効な対応策である。

(4) 国内外の標準化動向・適用動向との整合

接触ICカードのIS化・JIS化

国際的な標準化動向としては、接触ICカードの形状・物理特性、端子の位置と形状、電気信号及び伝送プロトコル、共通コマンド、アプリケーション識別子、およびその登録、共通データ要素の基本事項は、ISO/IEC 7816-1~6にて既にIS化されており、JISについてもISOと合わせる為に、7816の翻訳規定としてAIDに関するものを除いて制定されている。更に、金融取引に関連規定として、金融業務におけるICカードと端末間のメッセージについては、ISO 9992-1~2にて、また、ICカード利用金融取引システムのセキュリティについては、ISO 10202-1~8にてほぼ制定されている。

国内外における電子マネー／電子財布システムの展開

ISO 7816等の制定に並行或いは連動する形で、従来クレジットカード／デビットカードが入り込めなかった小口決済市場の取込みを目指して、ISO 7816に準拠した接触ICカードを使った様々な形の電子マネー／電子財布システムの導入や、導入に向けた実証実験が多数展開されている。また、我が国においても、現行法制度の下でもICカード型プリペイドカードとして導入が可能であり、

且つ、非金融系企業の参入も可能である。

EMV仕様の出現

国際間の相互運用性の確保が基本命題となるクレジットカード業界において、全世界のクレジットカード取扱高の実に85%強を占めるVISA/Masterの2大国際ブランドと、Europayの3社共同により、接触ICカード型クレジットカードの仕様であるEMV仕様が制定され、日本でも通産省が公募した19のEC関連プロジェクトの一つで、昨年秋から、神戸でクレジットカード機能に電子マネー機能を加えた形で実証実験がスタートしたSCJ(3万人を対象予定)、現在会員公募中で、間もなく開始される郵政省の大宮プロジェクト(7万人対象)、今年6月スタート予定の都市銀行・クレジットカード会社共同の渋谷プロジェクト(10万人対象)等、EMV準拠のICカード利用プロジェクトも目白押しである。また、WG7のメンバー構成自体を見ても、クレジットカード発行企業の主要な企業が多数参加している。

以上のような事柄を勘案し、クレジットカードとプリペイド型電子マネーの在り方について検討を行なった。クレジットカードについては、既述通り、業界の事実上のデファクト・スタンダードと思われるEMV仕様の内容検証・解説を含め、これらをベースとして実際にICカード型クレジットカードの発行を目指す企業にとって参考となるよう、特に、カードと端末によるリスクコントロールに関する、よりインプリメント仕様に近いものへのアプローチ的な検討を行なった。また、ICカードを現実の市場で実用に供する当って最重要事項となる、インフラ整備アクションプランをも含めた、具体的な実用化・普及促進のために必要なICカード利用環境整備に関する提言をも視野に入れて、極力具体的なものとなるよう検討した。(別章にて記述)

尚、プリペイド型電子マネーについては法制度に絡んだ課題の整理、並びに法改正の動き等を主体とした検討内容を記述する。

2.2 決済分野におけるICカードに求められるもの

2.1節でも触れたが、ICカードはあくまで道具の一つであり、決済分野に適用されるICカードは支払のための道具に過ぎず、商取引全般から見た場合、あくまでその補助のための道具でしかない。従って、決済分野に適用される道具としてのICカードの在り方を考える時の基本要件(考慮点)を整理すると以下のようになる。

(1) 道具の一般的な考慮点

まず、一般的な道具に求められる基本的な考慮点は次の通り。

誰が使うのか?

高度な知識を有する技術者等の専門家が対象の場合と、一般消費者を対象とする場合では、習得している知識・技術レベルの違いや、そのレベルの違いに起因する理解力・対応力も大きく異なるので、その差異をも十分考慮して、利用環境の整備や運用廻りへの細心の注意・配慮を要する。

どこで使うのか?

使用する場所の特性に十分な配慮が必要。

何に使うのか？（何の為に／何を得的為に）

上記の場所の特性の他、使う目的の違いにより要求される処理時間や、安全性／コスト等を的確に把握し、相応しい対処が必要である。

(2) 決済分野に適用されるICカードの要件

上記の道具に対する一般的な考慮点を踏まえて、更に、決済分野に適用される道具としてのICカードを考える時、求められる要件は以下のようなものが考えられる。

ユーザーの視点

決済分野に適用される汎用ICカードは、一般消費者を対象として発行される。従って、通常一般消費者の関心の的は、どのようなサービスを受けられるか（或いはメリットを享受できるか）、その内容が具体的・明確に伝わるものであることや、現金や従来の磁気ストライプ方式のカードより、例えば、早くて簡単などの使い易いもの（極論すると、使うということを全く意識する必要も無いくらい簡単に目的が達せられるものと言うことも考えられるのでは）かどうかが第一のポイントである。

例えば、暗号方式を使っているから安全だ、というような純粋に専門的・技術的な事柄よりも、発行者が企業体力等から見て何か問題が発生し、不利益を被った場合でも、あくまで生じた不利益は一時的なもので、最終的にはその損害に対する弁済の保証を受けられる限り、少なくともそのように期待できると信頼できる場所である限りにおいては、一般的には技術面についてはあまり気に留められないものと考えられる。

従って、具体的な商品設計においては、ユーザーの視点に立つて行うことが第一である。

加盟店の視点

国や地方自治体が、国民の福祉等の請求に応えるために、法律や条例を定めて導入する場合を除き、特に、決済分野に適用されるICカードの場合、発行されたICカードの取扱いは、受入れ取扱いのための加盟店契約を、何らかの形で締結した加盟店側に委託することになる。従って、加盟店にとっても取扱いのメリットがあり、少なくとも従来の現金や磁気ストライプ方式のカード以上に処理時間の短縮や、障害時の対応等を含めた取り扱い易さが明確に示せなければ、特に、初期においては忽ち取り扱い拒否に繋がり、加盟店にそのような対応をされた一般消費者の継続利用を望むことは困難になる。

ICカード以外に必要な道具

A. 端末／ネットワーク

それ単体では、有する本来の機能を果たすことが一切できないICカードにとって、不可欠であるR/W端末のインフラストラクチャー整備の必要性については既述の通りであるが、決済分野においてICカードを利用する場合には、更に、取引き時点はICカードと端末間だけのオフライン処理であっても、オフライン取引した売上データは、発行者へ取り扱った加盟店の加盟店端末より発行者へ還元される必要がある。また、将来的には付加された電子マネーへの加盟店端末等を使ったりロード手段の拡大実現のためにも、通信ネットワークが不可欠であ

る。よって、ICカード/端末/ネットワークは三位一体のものである。

B. 利用環境の整備

ICカード/端末/ネットワークは三位一体と述べたが、これらはシステム構築というハード面の話であるが、これらの運用や取り巻く法律を含めた制度等ソフト面とも言うべき利用環境の整備も必要である。

特に、今後多方面でICカードが導入され、先例として法解釈の問題等に起因する規制により、汎用性が保持できなかったことも災いしてその大半が失敗し、撤退を余儀なくされたプリペイドカード専門業者の教訓を活かし、複数の事業者が、相互開放により汎用性を確保しようとするのが予想される現状において喫緊の課題は、AIDの付番コード体系の整理と、一元管理体制の確立である。(別途詳述)

2.3 明快な役割分担と協調

以上のような点を考慮して、ICカードの導入を具体的に行おうとする場合、その推進者には其々次のような役割分担が考えられ、其々の推進者が其々の責務を互いに有機的に結び合い、連携することにより全うすることが何より肝要と考える。

(1) 発行者の責務

発行者の責務としては、消費者の視点、加盟店の視点での商品設計、即ちマーケティングに根ざした商品設計、しかも、利益を生み出す構造と継続性のある商品設計を行う責務は発行者にある。

商品設計に当たって考慮すべき点は、先の道具の要件に関する記述の通りであり、将来的には十分予想される使用方法、或いは目指すべき方向であっても、幾つかの限定条件(例えば技術の向上や市場の変化といった可変要素の存在)が付くような場合には、現時点では簡単にその条件がクリアできない時は、一気にその予想される理想形を実現しようとするのではなく、段階を追うべきであると考え。例えば、単機能/単目的の道具として成立たないものを幾つも組み合わせると多目的に使えると言っても、受入れられるものではない。

(2) 技術提供者に求められること

ICチップ/カード、端末、セキュリティ(特に暗号や鍵管理等)、ネットワーク制御等々、技術を必要とすることだらけであるが、発行者が決定した商品設計には、必ずしも最新技術が全てにおいて相応しいとは限らないことも往々にしてあり、発行者と一緒にユーザーの視点で考え、発行者に対して適切な技術面での助言を行なうことも必要である。

とは言え、技術自体を何等否定するものではなく、様々な技術の適用都度、適用事例が示すノウハウを吸収し、更なる技術開発の継続は言わずもがなではあるが、重要な使命である。

(3) 加盟店

既述の通り、多くの発行されたICカードを受け入れる為に必要な端末の設置にしても、先ず加盟店契約ありきである。従って、既存の加盟店網自体も重要であり、更に、契約に基づき設置したこれら端末操作を含めた取扱いの習熟度を深め、一定レベ

ル以上に保つことは、利用者のICカード利用時における様々な心理的な阻害要因を払拭し、且つ、継続的な利用を促す為にも重要である。また、このレベル維持の実現の為には、日常的な加盟店指導を含めた発行者と加盟店の協調関係の維持が重要である。

2.4 クレジット

前述のような事由から、検討対象としたクレジットカード業務において、ICカードを適用する為の課題は、如何に安全なオフライン取引を確立できるかであり、以下EMV仕様をベースに、クレジットカード業務の特性も踏まえて、この分野でのICカードのメリットを最大限活かす利用の在り方について記述する。

2.4.1 ICカード利用時のオフライン取引についての考え方

クレジットカードのICカード化最大のメリットは、一般的にはカードの偽造による不正利用の防止という点で、現行の磁気カードに対比して格段に優れている事である。更に、CPU付きのICカードで暗号技術を利用することで、磁気カードが現在の技術レベルにおいて、その脆弱となった安全性故に、脆弱性を内包したまま高負荷、高コスト、非効率な取扱い手法である全件オンライン・リアルタイム・オーソリゼーションへと傾斜せざるを得ない状況を打破し、安全なオフライン取引をも可能とし、処理時間の短縮や通信コストの削減並びにカード会社センターの負荷軽減へも寄与する点が挙げられる。

しかしながら、発行者が個々のカードホルダーに対し、信用供与（利用分をどこまで保証するか）する後払い方式というクレジットカードの特性故に事は単純ではなく、真正なカードホルダーによる真正なカードの利用であっても、カードホルダー個々の支払能力を超えた過剰利用を適正な範囲に収めるための途上与信管理の観点や、カード自体は真正であっても、第三者が盗難・紛失カードで換金性商品の買い廻りを行う不正利用や、自己消費型の不正利用も含めた不正利用防止の観点から、全てをオフライン取引できる訳ではない。従って、これらを考慮したクレジット業務における、可能な限り安全なオフライン取引の在り方に関する考察について記述する。

尚、仮に現行の磁気クレジットカードをICカードに切替えるとした場合、通常有効期限の到来に伴う更新カードへの切替えの形で順次行うことになり、一般的に2～3年、一部のクレジットカード会社では5年程度掛かるものと予想され、この期間内は、日本国内で発行されるカードのみを対象として考えても、磁気カードも併存することとなるので、当然この点にも留意し、現状での運用との整合性も視野に入れて、以下の通り、特に重要な、カード認証/本人認証、加盟店の業種業態別のフロアリミットの設定の在り方、端末リスク管理の在り方について考察すると共に、これらに関する参考事例として、神戸で行われているSCJの実証実験でのEMV仕様の適用事例（考え方の整理）を紹介する。更に、オフライン取引データの事後処理の在り方についての考察も記述する。

2.4.1.1 カード認証/本人認証

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確立する為の第一のポイントは、カードの真偽を如何にチェックするかである。また、カード自体は真正なカードで

あっても、例えば盗難・紛失カードの場合、届出に基づき事故カードとして登録・手配されるまでは、受入れる加盟店側では通常に受入れざるを得ないのが実状である。このため、カードの提示者が発行者のカード使用許諾を得た本人かどうかを確認するための本人認証も必要となる。以下にその仕組み・方法について記述する。これらの方法によりCPU付きのICカードと暗号技術の組み合わせが、クレジットカードのICカード化に最大の利益をもたらすこととなる。

(1) カード認証

静的認証

ICカード認証の最も基本的な方法として、端末とICカードが共に同じ秘密データを持ち、そのデータを端末がICカードから読み出して自分の持つ秘密データと照合する方法が考えられる。しかし、この方法では、端末側の秘密データを如何に安全に保持するかが問題となる。

この問題点を解決するため、EMV仕様ではICカードの認証に公開鍵暗号を用いている。公開鍵暗号を用いてICカード認証を行う場合、端末はその公開鍵を知る必要がある。EMV仕様では、各ICカードにその公開鍵を持たせ、端末がそれを読み出して使用する方式を採用している。

この方式では、ICカードから読み出した公開鍵が正しいものであるということを証明する必要があるため、公開鍵には信頼できる認証局(CA: Certification Authority)の署名(以下、認証書と記す)が付加されている。端末は認証局の公開鍵を有しており、これを用いて認証書を検証する。

ICカードの静的認証を行う為に、ICカードおよび端末が所持すべき主なデータと暗号アルゴリズムを以下に示す(図 2-1参照)。

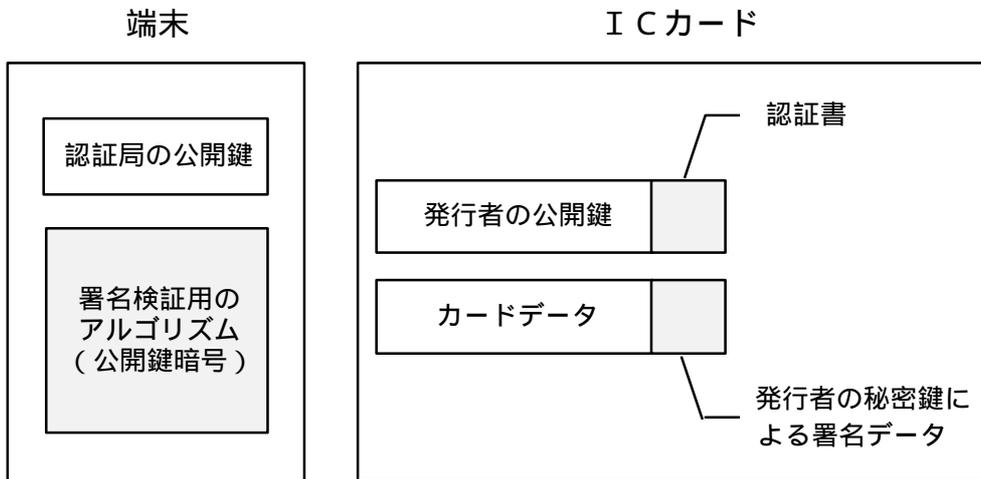


図 2-1 EMVの静的認証模式図

- A. ICカード
 - a) データ
 - i. 発行者の公開鍵と、その認証書(認証局の秘密鍵による署名データ)
 - ii. カードデータと、発行者の秘密鍵による署名データ
 - b) 暗号アルゴリズム

なし

B. 端末

a) データ

認証局の公開鍵

b) 暗号アルゴリズム

署名検証用の公開鍵暗号アルゴリズム

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ため、静的認証時にICカードと端末間で伝送される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ための方法が動的認証である。

動的認証では、ICカード自身も公開鍵暗号アルゴリズムによる暗号演算を実行する。また静的認証が2対の秘密鍵/公開鍵を用いたのに対して、動的認証では3対の秘密鍵/公開鍵を用いる。

ICカードの動的認証を行うために、ICカードおよび端末が所持すべき主なデータと暗号アルゴリズムを以下に示す。(図 2-2参照)

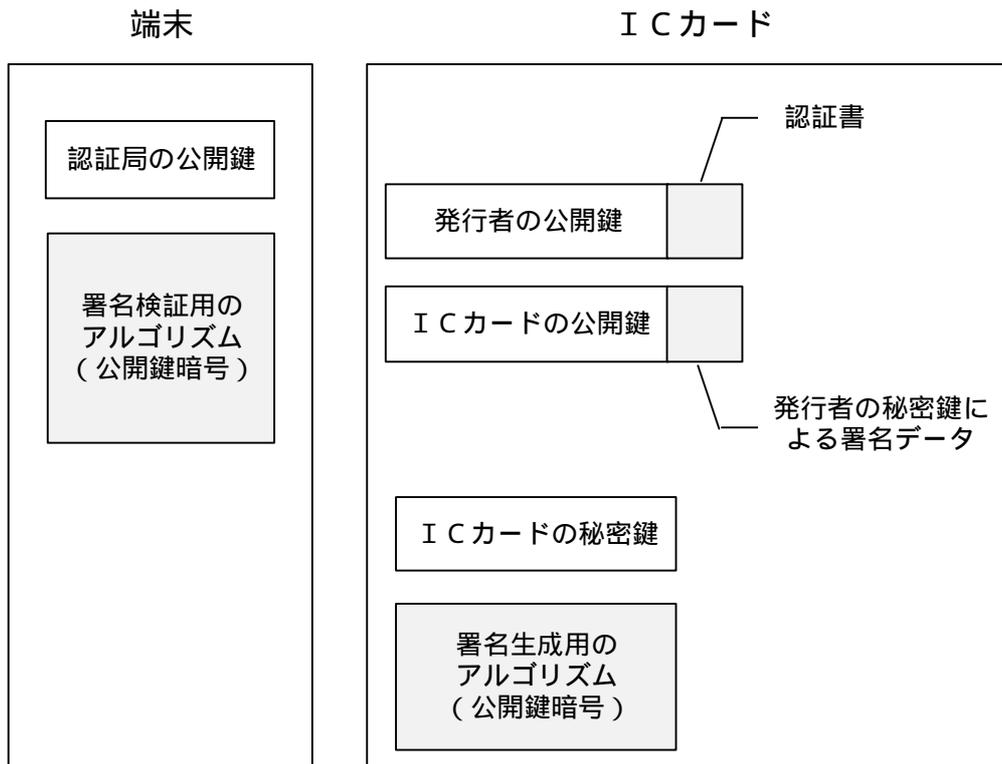


図 2-2 EMVの動的認証模式図

A. ICカード

a) データ

i. 発行者の公開鍵と、その認証書 (認証局の秘密鍵による署名データ)

ii. ICカードの公開鍵と、発行者の秘密鍵による署名データ

iii. ICカードの秘密鍵

b) 暗号アルゴリズム

署名生成用の公開鍵暗号アルゴリズム

B. 端末

a) データ

認証局の公開鍵

b) 暗号アルゴリズム

署名検証用の公開鍵暗号アルゴリズム

動的認証では、ICカードが動的に暗号演算を行うため、セキュリティが向上する反面、処理速度が遅いという問題点がある。処理速度はICカードおよび端末で実行される暗号演算の回数が目安となる。特に、CPUの処理能力、および鍵長の点から、ICカードによる暗号演算、とりわけ署名生成の回数が大きく左右する(表2-1参照)。

表 2-1 各認証における暗号処理の回数

		署名生成	署名検証
静的認証	ICカード	なし	なし
	端末	なし	2回
動的認証	ICカード	1回	なし
	端末	なし	3回

(2) 本人認証

前述の通り、カード認証によりカードの真正性が確認されても、カードの提示者が正当なカードホルダーかどうか、本人を確認する手法としては、従来通りのサインの照合と現在でもCD/ATM等でキャッシュサービスを受ける際に利用されているPIN(Personal Identification Number:暗証番号)入力/チェックによる本人認証の手法もあるが、前者は現実には全ての加盟店の店員が筆跡鑑定能力を有している訳ではなく、不正利用の防止という観点からは極めて曖昧模糊とした対応方法と言わざるを得ない。

従って本章では、CPU付きのICカードに適用した場合、更にその堅確性が高まる後者について、如何に下記の導入目的を達成するかという観点から考察した内容について記述する。

導入目的

- A. 本人確認の強化による不正利用の防止
- B. オペレーションの簡略化とスピードUP
- C. オフラインによる通信コストの削減

PIN入力・サインレスを用いたクレジットカード利用フロー
表 2-2に一般的なフローを示す。

表 2-2 P I N + サインレスの処理フロー

操 作 手 順	オペレータ	備 考
1. 初期画面の状態です上キーを押下	店員	
2. 端末にICカードを挿入・読取り	店員	原則店員が操作する。 * 但し、店員による不正防止策について、顧客操作も含めた検討を要す。
3. 決済アプリケーションの選択	店員（顧客の要望に応じる形）	クレジット / 電子マネーの選択。
商品コード入力	店員	任意入力。 * 現行でも実運用上は難しく、未実施の場合が大半。
4. 売上金額入力	店員	任意入力。
税・その他金額の入力	店員	カード会社との契約により異なる。（一回払い / ボーナス一括払い / 分割払い / リボ払い等）
5. 支払方法の選択	店員	発行者が試行チェック回数のパラメーターを設定。
6. P I N（暗証番号）入力	顧客	* 暗証番号忘れへの対応。 キャンセルキーの設定 / 最終トライの表示 / 試行回数の表示。 オフライン / オンラインの判定。
7. 売上処理		
8. 伝票発行署名	顧客	原則サインレスの運用とし不要。 * 伝票に「署名不要」の表示。

* ICチップの不良、読取り端末の不良、データ異常時など、イレギュラ時の対応については検討を要す。

P I Nの仕様

A. P I Nの桁数について

桁数の変更は、現行システムへの影響が大きすぎると考えられるため、P I Nは「4桁」とする。

* CCPS (Chip Card Payment Service: VISAが開発したICカードの仕様の一つ) では物理的に「12桁」までサポート。

B. 入力ミス回数の設定について

現行の磁気カードでは「3回」が主流となっているが、各カード発行会社毎に異なる事も有り得、統一すべきかどうかについても検討する。また、最終トライ前に端末上に表示を出し、注意を促すことも検討を要するものと考えられる。尚、回数情報はICチップ上に持つ。

C. 入力端末の機能について

a) P I N入力の操作性を高めるために、端末のKEY配置や大きさにも配慮。

また、周囲から盗見できないようにガード（目隠し）を設ける等の配慮が必要と考える。

* 状況によっては、盗見の可能性が無いところでオペレーションを行うような環境を設定することも必要と考える。

b) 端末上に売上情報（金額、日付、等）を表示し、顧客が納得した後PIN入力をする。

c) 売上情報をPIN入力端末に判りやすく表示する。（店員による確認案内も必要）

入力ミス・トラブルへの対応

A. PIN入力間違いによるカード利用STOP（ガード）の解除について

a) カード会社で本人確認の上解除とする。再発行の対応が考えられるが、電子マネー併用型ICカードの場合、この運用は複雑・困難と見る。

b) 入力ミスの履歴は成功時にクリアする。現行の仕様と同じ。

B. PIN（暗証番号）の二重化について

当面、PINはキャッシング等に使用する暗証番号と同じとする。店員や周囲の顧客に操作状況を盗み見される危険性が発覚した場合は、キャッシングと別の暗証番号の採用（暗証番号の二重化）を検討する。

* 神戸のSCJの実証実験では同一暗証コードを使用。

C. PINコードの変更について

行わない方向で検討中。万一、トラブルが多発した場合は、パスワードと同様の考え方で頻繁に変更が出来るものも検討する必要がある。その際、旧番号の入力を必須とし、銀行/カード会社の専用端末で行うなど、セキュリティへの配慮が必要。

D. カード、端末の不良によりPIN入力が不可となった場合の対応について

従来通り、磁気ストライプ+エンボス・インプリンター+サインで対処する。加盟店がPIN入力が可能な状態で、従来通りの運用を行わないよう、運用条件の設定が必要。また、当面の間、ICカード上には磁気ストライプ、エンボス、サインを残す必要がある。

サインレスの対応について

A. 効果

サインレスは処理が早く、特にレジ待ちの多い加盟店では利用促進に効果がある。

B. 現行の磁気カードでの利用状況

食料品売場、通販、レジャー施設（入場券売場）、公共施設（高速料金所）等、加盟店により詳細は異なるが、一般的には1回あたり3万円程度以内、1回払い、換金性のあるもの（酒、金券など）は除外。カード会社により基準が異なっている。

C. 問題点

現行法の下では、カードホルダと債務の存在を争うような事態に立ち至った時、クレジット伝票にサインが無い事が、裁判上の証拠能力に影響する可能性がある。

即ち、顧客利用の真正性の保証の意味合いにおいて証拠としての立証能力は弱い。よって、司法上の制限が掛かることとなり、利用代金の回収に困難を来す事が考えられる。

この点を解決するためには、PIN入力による伝票の証拠能力が司法上認められるという、制度上の整備が必要と考える。

PIN入力とサインレス運用の併用について

サインレスとPIN入力の併用の必要性、行う場合の条件や対応方法について検討する。

A. 課題と対策

フロアリミットによるサインレス若しくはPIN入力判断を行う場合、オペレータ判断またはシステムの制御が必要となるが、こうした運用方法への対応を検討した。

a) 現行クレジットカードの取扱いが多い大半の加盟店では全件オンラインオーソリを実施しており、オンライン端末未設置店では、フロアリミット以下は「無効カードリストチェック」のみを行い、フロアリミットを超える場合は「電話による販売承認の取得」を行っている。(フロアリミットは現行では5万円が一般的。来年より3万、1万へと下がる傾向)

b) 高速道路ではオフライン&サインレスである上、フロアリミットの導入をしていない。

c) 商品コード(換金性商品など)や商品金額による制御、フロアリミット変更とPIN入力制御などを、ターミナルのアプリケーション変更で実現するのは現行では困難。

d) 全件PIN入力を必須とした場合、以下の問題点が想定される。

i. 全件入力する事による煩雑性が発生する。サービスレベルの後退となり得ないか?

ii. 顧客の納得性の問題。PIN入力の有無が発生する事により、顧客感情面でのトラブルが発生しないか?セキュリティの確保の為に全件PINのほうが判りやすいのではなからうか。サインレスの廃止を望む顧客の声もあり。

B. 今後の対応

サインレスは現状、レジ等で行われている小額決済(マイクロペイメント)の中で行われており、定着している。ここにPIN入力を無条件に導入する事で、現場での混乱が危惧される。反面ICカードの普及度合に依っては、他の売場・店舗での利用方法との不整合も危惧される。本件に関しては、ICカードの普及度合がその鍵を握ることになるものと思われ、その意味においては、当面従来よりサインレスで運用されている売場では、特に問題が発生しない限りサインレスの運用は継続させて良いのではと考える。(今後検討を要する課題である)

2.4.2 フロアリミット

ICカードを利用した場合、途上与信管理・多重債務防止・第三者による不正利用防止の手法として、後述するカードと端末の組み合わせたりリスク管理の手法も幾つかあるが、

クレジットカード業務における基本は、一取引において一定金額を超える都度行なうオンライン・リアルタイム・オーソリゼーションによる販売承認の判定である。この販売承認が必要かどうかの最低限の基準として設定されるのがフロアリミット(販売承認限度額)である。

現在のクレジットカードの加盟店は、業種業態により様々な商品・販売形態がある。加盟店毎に適用されるフロアリミットに関する基本的な考え方について記述する。

2.4.2.1 現行のフロアリミット

先ず、既述の通り磁気カードとの併存が不可避なため、現行磁気カード運用との整合性をはかることも必要であると考えられる。現状では、表 2-3に示すような基準に基づいて運用されている模様で、一般的な傾向として将来的には引き下げの方向にある。

表 2-3 フロアリミット(参考)(平成9年12月末現在)

加盟店	96年1月～	98年1月～	99年1月～
オンラインオーソリ可能加盟店	3万円	3万円	1万円
オフライン加盟店	5万円	3万円	未定

但し、カード発行会社個社の判断により、ハイリスク店・悪用発生店等の場合は上記表2-3に示したフロアリミットとは異なる場合があり、独自に加盟店業種毎にフロアリミットを設定している場合もある。ICカードでのクレジット利用時においても、フロアリミットは現行の運用通り業界基準とは別に、各カード発行会社において検討する必要がある。

2.4.2.2 加盟店業種について

前述の通り、基本的にフロアリミットは加盟店業種毎に設定が異なる。フロアリミットの設定のみでも、オフライン取引が比較的適用し易い業種として以下の形態が考えられる。

(1) オフライン対象業種

原則として、小口取引・換金性のない商品を取り扱う業種が望まれる。

物品販売店

食料品を中心としたスーパーマーケット・コンビニエンスストア・キオスク・食品専門店・観光地土産物屋・本屋・日用品雑貨店・文房具店・レコードショップ・花屋・ドラッグストア・リッカーストア・たばこ販売店・健康食品店

サービス

クリーニング・駐車場・喫茶店・ファーストフード・ファミリーレストラン・理容店・宅配(ピザ)・写真現像店・レンタル店(ビデオ・衣装等)

施設

(ゴルフ場)・ゴルフ練習場・テーマパーク・スキー場・スポーツ観戦施設・映画館・美術館・博物館・ボーリング場・会員制スポーツクラブ・病院・健康センタ

(2) 商品コード

上記以外にも様々な加盟店業種があり、これらを統一的に判断するコードとして、現行では表 2-4に示すCAT、POS端末等で利用されている商品コードが、途上与信管理上

の販売承認の判定の一助として加盟店業種を識別するために利用されている。

表 2-4 CAT / POS使用商品コード一覧表

商品コード	商品名・サービス名	商品コード	商品名・サービス名
0XX	海外利用	6XX	物品(2)
000	一般利用	610	工具・園芸用品
010	キャッシング	650	電気製品
020	通販(電話)	652	音響製品(ステレオ・ラジオ・アンプ・テレビ)
030	通販(郵便)	653	ビデオ
040	医療費	655	エアコン
050	学費	660	照明器具
060	宿泊代	680	OA機器(パソコン等)
070	レンタカー	7XX	物品(3)
080	交通費	710	自動車・自動二輪
090	飲食	720	自転車
1XX	ローン・C/S	760	タイヤ・カーエアコン・自動車用品
100	C/S	790	メガネ・コンタクト
110	ローン	8XX	物品(4)
120	通販	810	薬・化粧品
2XX	旅行・運輸	820	家庭用品
200	鉄道・バス運賃	830	衣服・呉服
201	鉄道回数券	831	毛皮・生地
210	国内航空券	840	バック・カバン
211	航空回数券	850	靴
212	国際航空券	860	寝具・カーペット
220	乗船券	870	周辺雑貨品
230	国内パッケージ旅行	880	家具
231	海外パッケージ旅行	9XX	物品(5)
240	レンタカー・バイク・タクシー	910	スポーツ用品・玩具・人形
250	引越代金	911	ゴルフボール
3XX	サービス(1)	912	クラブセット
300	宿泊	920	書籍・レコード
310	食事・宴会	950	楽器
320	飲食	970	美術・骨董品・古銭切手
330	施設利用料・ゴルフ場・結婚式場	980	進物・歳暮・中元
340	入浴(サウナ)	981	流通券(ビール・ラム・ショウ・図書旅行券)
4XX	サービス(2)	990	区分できないもの
400	修理・営繕(含む車検)		
410	理容・美容		
420	医療		
5XX	物品(1)		
500	宝石・貴金属		
540	時計等		
541	ライター		

560	カメラ(含レズ・8ミリ)		
570	事務用品		

(3) ISO8583加盟店業種コードについて

クレジットカードをICカード化した場合、上記CAT・POS商品コード別のフロアリミット設定も考えられるが、大まかな分類であり、きめ細かな途上与信管理のためには、本来利用の都度購入商品自体が判別できるよう加盟店側からの情報発信が望ましい。

しかしながら、店舗によっても異なる流通小売の商品コードの現状や加盟店側での対応の付加を考えると、ある程度の割り切りは必要となるものとする。今後発生頻度が高くなると思われるネットワーク等上での取引、クレジット決済対象商品の多様化や、後述する端末リスク管理とカードのリスク管理におけるよりきめ細やかな対応を想定すると、現状の商品コードでは、個々の詳細な取扱い商品・販売形態の判定が困難であり、細かい加盟店毎の取扱商品・販売形態の業種毎の識別のためのコード化検討も将来的に必要とする。以下に示すものは、既に磁気カードにおいてもVISAやMasterで利用されている「ISO8583(1993年度版)カード引受者(加盟店)業種コード」を元に、加盟店業種を見直したものである。

尚、見直しに当たっては、MasterCard Internationalの「Quick Reference Booklet, Oct 97」の「Merchant Category Codes」をも参照・対比し、以下の点を補足した。

- ・()で表示したもの：ISOにあるがQuick Referenceにないもの。
- ・太字で表示したもの：Quick ReferenceにあるがISOにないもの。

また、一応大雑把な取捨選択を行い、その結果不要と判断したものについては一線で抹消したが、最終的にはクレジットカード業界で、必要に応じた十分な検討・議論が待たれるところである。更にVISAについても「Visa International Operating Regulation」の「Merchant Category Code」を参照し、VISA独自のコードを末尾に追加記入した(それ以外は基本的にはMasterCardのコードと同じ)。尚、参考にMasterCardの「Wholesale Distributors And Manufactures」のコードも追記した。

農業

- ~~0742~~ 獣医サービス
- ~~0763~~ 農業協同組合
- ~~0780~~ 造園、園芸サービス

請負業

- ~~1520~~ 全般的な請負業者—その他建築物
- ~~1711~~ 暖房、配管、エアコン業者
- ~~1731~~ 電気業者
- ~~1740~~ レンガ、石材加工、タイル、左官、絶縁材業者
- ~~1750~~ 大工
- ~~1761~~ 屋根、壁、板金業
- ~~1771~~ コンクリート業
- ~~1799~~ その他の請負業者

運輸業

- 4 0 1 1 鉄道
- 4 1 1 1 地方、郊外通勤者の交通手段（連絡船含む）
- 4 1 1 2 旅客鉄道**
- ~~4 1 1 9 救急サービス~~
- 4 1 2 1 タクシー、リムジン
- 4 1 3 1 路線バス、貸切バス、ツアーバス
- 4 2 1 4 陸上普通運送、市内、長距離トラック運送、輸送、倉庫業、配達
- 4 2 1 5 宅急便サービス
- 4 2 2 5 公共倉庫 - 農産品、冷蔵品、家庭用品の保管
- 4 4 1 1 貨物船、巡航船、クルーズライン
- 4 4 5 7 ボートレンタル、リース
- 4 4 6 8 マリーナ、マリンサービス
- (4 5 1 1 航空会社、航空貨物)
- 4 5 8 2 空港、飛行場、空港ターミナル
- 4 7 2 2 旅行会社
- (4 7 6 1 旅行関連サービスのテレマーケティング)
- 4 7 8 4 通行料（道路、橋）
- 4 7 8 9 その他運輸業

公共サービス

- 4 8 1 2 電話機を含む通信機器
- 4 8 1 4 市内、長距離の通信サービス、クレジットカード通話、磁気ストライプ読取機能付き電話による通話、FAXサービス
- 4 8 1 6 コンピューターネットワーク、インフォメーションサービス**
- 4 8 2 1 電報サービス
- 4 8 2 9 電信為替
- 4 8 9 9 ケーブルテレビ、有線放送
- 4 9 0 0 公共サービス - 電気、ガス、水道、清掃業

小売業

- 5 2 0 0 家庭用品の卸し売り**
- 5 2 1 1 材木、建築材料店
- 5 2 3 1 ガラス、ペンキ、壁紙店
- 5 2 5 1 金物店
- 5 2 6 1 苗木、芝生、庭用品店
- ~~5 2 7 1 モービルホームディーラー~~
- 5 3 0 0 ホールセールクラブ(会員制問屋クラブ)**
- 5 3 0 9 免税店**
- 5 3 1 0 ディスカウントストア
- 5 3 1 1 デパート
- 5 3 3 1 バラエティストア

5 3 9 9	雑貨店
5 4 1 1	食料品、スーパーマーケット
5 4 2 2	食肉業者
5 4 4 1	キャンディ、ナッツ、菓子店
5 4 5 1	日用品店
5 4 6 2	ベーカリー
5 4 9 9	食料雑貨、専門店、コンビニエンスストア
5 5 1 1	自動車、トラックディーラー（新車、中古車）、サービス、部品
5 5 2 1	自動車、トラックディーラー（中古車）販売
5 5 3 1	自動車販売、家庭用品販売
5 5 3 2	自動車タイヤ店
5 5 3 3	自動車パーツ、アクセサリー店
5 5 4 1	ガソリンスタンド（有人）
5 5 4 2	ガソリンスタンド（セルフ式）
5 5 5 1	ボートディーラー
5 5 6 1	トレーラー、キャンピングカーディーラー
5 5 7 1	オートバイディーラー
5 5 9 2	モーターホームディーラー
5 5 9 8	スノーモービルディーラー
5 5 9 9	その他カーディーラー
5 6 1 1	紳士、男児衣類、小物店
5 6 2 1	婦人既成服店
5 6 3 1	婦人小物、専門店
5 6 4 1	子供、幼児服店
5 6 5 1	家族衣料店
5 6 5 5	スポーツウェア、乗馬服店
5 6 6 1	靴店
5 6 8 1	毛皮店
5 6 9 1	紳士、婦人衣料店
5 6 9 7	テーラー、仕立て、修理、寸法直し
5 6 9 8	かつら店
5 6 9 9	その他アパレル、アクセサリー店
5 7 1 2	家具、家庭用品、道具店（電気製品を除く）
5 7 1 3	カーペット店
5 7 1 4	カーテン、室内装飾
5 7 1 8	暖炉、暖炉小物店
5 7 1 9	その他家庭用品専門店
5 7 2 2	家庭電気製品店
5 7 3 2	ラジオ、テレビ、ステレオ店
5 7 3 4	コンピューターソフトウェア店

5 7 3 5	レコード店
5 8 1 1	仕出し店
5 8 1 2	食堂、レストラン
5 8 1 3	飲酒店 - バー、居酒屋、ナイトクラブ、カクテルラウンジ、ディスコ
5 8 1 4	ファーストフードレストラン
5 9 1 2	薬局、薬店
5 9 2 1	酒屋
5 9 3 1	中古品店
5 9 3 2	アンティークショップ
5 9 3 3	質屋
5 9 3 5	解体業、廃品回収業
5 9 3 7	アンティークリサイクル店
5 9 4 0	自転車店 - 販売、サービス
5 9 4 1	スポーツ用品店
5 9 4 2	本屋
5 9 4 3	文房具、オフィス用品、学校用品店
5 9 4 4	宝石、時計、銀製品店
5 9 4 5	ホビー、おもちゃ、ゲーム店
5 9 4 6	カメラ、写真用品店
5 9 4 7	ギフト、カード、記念品店
5 9 4 8	カバン、革製品店
5 9 4 9	縫い物、編み物、織物、反物店
5 9 5 0	ガラス製品、クリスタル製品店
5 9 6 0	ダイレクトマーケティング - 保険サービス
5 9 6 1	カタログ販売を含む通信販売業、本、レコードクラブ
5 9 6 2	ダイレクトマーケティング - 旅行関連手配サービス
5 9 6 3	直販業者、訪問販売
5 9 6 4	ダイレクトマーケティング - カatalog通販
5 9 6 5	ダイレクトマーケティング - カatalog兼小売り業者
5 9 6 6	ダイレクトマーケティング - 海外テレマーケティング
5 9 6 7	ダイレクトマーケティング - 国内テレマーケティング
5 9 6 8	ダイレクトマーケティング - 通販による継続取引
5 9 6 9	その他のダイレクトマーケティング
5 9 7 0	美術用品、工作用品店
5 9 7 1	美術商、画廊
5 9 7 2	収集目的の切手、コイン店
5 9 7 3	宗教用品店
(5 9 7 4	ゴム印店)
5 9 7 5	補聴器販売、サービス店
5 9 7 6	整形用品、義手・義足店

5 9 7 7	化粧品店
5 9 7 8	タイプライター販売、サービス、レンタル
5 9 8 3	燃料店 - 石油、薪、石炭、液化石油
5 9 9 2	花屋
5 9 9 3	たばこ屋
5 9 9 4	新聞販売店
5 9 9 5	ペットショップ、ペットフード
5 9 9 6	スイミングプール - 販売、用品
5 9 9 7	電気剃刀店 - 販売、サービス
5 9 9 8	テント、天幕販売店
5 9 9 9	その他専門小売店
サービス業	
6 0 1 0	金融機関 - 手動現金支払(預金、トラベラーズチェック、両替、為替、貴金属、貯蓄国債)
6 0 1 1	金融機関 - 自動現金支払
6 0 1 2	金融機関 - 金融商品、金融サービス
6 0 5 1	非金融機関 - 外国通貨、為替(電信以外)、トラベラーズチェック、郵便切手
6 2 1 1	証券業 - ブローカー、ディーラー
6 3 0 0	保険業 - 販売、引受
(6 3 8 1	保険配当金)
(6 3 9 9	その他保険業)
(6 6 1 1	過払い金返還要求)
7 0 1 1	ロッジ、モーター、リゾートホテル
7 0 1 2	タイムシェア(期間限定リゾート会員権)
7 0 3 2	スポーツキャンプ、リクリエーションキャンプ、子供キャンプ
7 0 3 3	トレーラーパーク、キャンプ場
個人サービス業	
7 2 1 0	洗濯、クリーニングサービス
7 2 1 1	洗濯サービス - 家庭、商用
7 2 1 6	ドライクリーニング
7 2 1 7	カーペット、室内クリーニング
7 2 2 1	写真スタジオ
7 2 3 0	美容院、理髪店
7 2 5 1	靴修理店、靴みがき、帽子クリーニング
7 2 6 1	葬儀屋、葬儀用品
7 2 7 3	デート、エスコートクラブ
7 2 7 6	税金準備サービス
7 2 7 7	カウンセリングサービス - 結婚、個人
7 2 7 8	買い物・ショッピングサービスクラブ

- ~~(7 2 7 9 負債カウンセリング)~~
- ~~(7 2 8 0 患者の個人資金の引き出し明細)~~
- (7 2 9 0 ベビーシッター)
- 7 2 9 6 貸衣装 - 衣装、ユニフォーム
- 7 2 9 7 マッサージ
- 7 2 9 8 健康美容温泉
- 7 2 9 9 その他個人サービス業

業務用サービス

- 7 3 1 1 広告サービス
- ~~7 3 2 1 消費者信用レポート代理店~~
- ~~(7 3 2 2 借金集金代理業)~~
- (7 3 3 2 青写真、写真複写サービス)
- 7 3 3 3 商業用写真、アート、グラフィックス
- 7 3 3 8 クイックコピー、複写サービス
- 7 3 3 9 速記サービス
- (7 3 4 1 窓クリーニングサービス)
- 7 3 4 2 駆除、消毒サービス
- 7 3 4 9 掃除、メンテナンス、管理サービス
- 7 3 6 1 職業紹介、人材派遣
- 7 3 7 2 コンピューター、情報処理サービス
- (7 3 8 9 旅行関連サービス以外のテレマーケティング)
- 7 3 9 2 マネージメント、コンサルティング、個人関連サービス
- 7 3 9 3 探偵社、警備、装甲車、番犬サービス
- 7 3 9 4 設備レンタル、リース、道具、家具レンタル
- 7 3 9 5 写真現像所
- 7 3 9 9 その他業務用サービス
- ~~7 5 1 1 トラック駐車場~~
- (7 5 1 2 自動車レンタル、リース)
- 7 5 1 3 トラック、トレーラレンタル
- 7 5 1 9 モーターホーム、RVレンタル
- 7 5 2 3 駐車場、車庫

修理業

- 7 5 3 1 自動車車体修理店
- 7 5 3 4 タイヤ修理店
- 7 5 3 5 自動車塗装店
- 7 5 3 8 自動車修理店 (非ディーラー)
- 7 5 4 2 洗車場
- 7 5 4 9 牽引サービス
- 7 6 2 2 ラジオ、テレビ、ステレオ修理店
- 7 6 2 3 エアコン、冷却装置修理店

7 6 2 9	電気、小器具修理店
7 6 3 1	時計、宝石修理店
7 6 4 1	室内装飾、家具修理、家具再生
7 6 9 2	溶接業
7 6 9 9	その他修理業
娯楽サービス	
7 8 3 2	映画館
(7 8 3 3	映画館 (即時支払いサービス))
7 8 4 1	レンタルビデオストア
7 9 1 1	ダンスホール、ダンススタジオ、ダンススクール
7 9 2 2	(映画を除く) 演劇興行、チケット代理店
7 9 2 9	バンド、オーケストラ、エンターテナーズ
7 9 3 2	ビリヤード場
7 9 3 3	ボウリング場
7 9 4 1	商業スポーツ、プロスポーツクラブ、競技場、スポーツ主催者
7 9 9 1	旅行者向けアトラクション、展示
7 9 9 2	ゴルフコース、パブリック
7 9 9 3	ビデオゲーム販売店
7 9 9 4	ビデオゲームセンター
7 9 9 5	賭け金 (宝くじ、カジノチップ、場外馬券、場内馬券等)
7 9 9 6	遊園地、サーカス、祭り、占い
7 9 9 7	会員制クラブ (スポーツ、リクリエーション、アスレチック) カントリークラブ、プライベートゴルフコース
7 9 9 8	水族館
7 9 9 9	リクリエーションサービス (スイミングプール、ミニゴルフ、運転場、スキー場、スポーツ、ゲーム教室、ボートレンタル、飛行機レンタル)
専門・資格職、団体	
8 0 1 1	医者
8 0 2 1	歯医者、歯列矯正医
8 0 3 1	整骨医
8 0 4 1	指圧師
8 0 4 2	検眼、眼科医
8 0 4 3	光学器械
(8 0 4 4	光学商品、眼鏡)
8 0 4 9	足治療医
8 0 5 0	看護、パーソナルケア
8 0 6 2	病院
8 0 7 1	医学、歯学研究所
8 0 9 9	その他医療サービス
8 1 1 1	弁護士

- ~~8 2 1 1~~ 小中学校
- ~~8 2 2 0~~ 大学、専門学校、短期大学
- ~~8 2 4 1~~ 通信教育学校
- ~~8 2 4 4~~ ビジネス、秘書学校
- ~~8 2 4 9~~ 職業、貿易学校
- ~~8 2 9 9~~ その他教育サービス
- ~~8 3 5 1~~ 育児サービス
- ~~8 3 9 8~~ 慈善、社会奉仕組織
- ~~8 6 4 1~~ 市民友愛組織
- ~~8 6 5 1~~ 政治団体
- ~~8 6 6 1~~ 宗教団体
- ~~8 6 7 5~~ 自動車組織
- ~~8 6 9 9~~ その他組織団体
- ~~8 9 1 1~~ 建築、工学、測量サービス
- ~~8 9 3 1~~ 経理、会計、簿記サービス
- ~~8 9 9 9~~ その他専門サービス

行政サービス

- ~~9 2 1 1~~ 訴訟費用、別居手当、養育費含む
- ~~9 2 2 2~~ 罰金
- ~~9 2 2 3~~ 保釈金
- ~~9 3 1 1~~ 税金
- ~~9 3 9 9~~ その他行政サービス
- ~~(9 4 0 1~~ 食料割引券)
- ~~9 4 0 2~~ 郵便サービス (政府のみ)
- ~~(9 4 1 1~~ 行政ローン支払い)

Wholesale Distributors And Manufacturers

- 2 7 4 1 その他出版業、印刷業
- 2 7 9 1 植字関連サービス
- 2 8 4 2 特殊クリーニング、ポリッシング
- 5 0 1 3 車関連用品、パーツ
- 5 0 2 1 業務用家具
- 5 0 3 9 その他建築用材料
- 5 0 4 4 オフィス、写真、写真複写、マイクロフィルム器具
- 5 0 4 5 コンピュータ、コンピュータ周辺機器、ソフトウェア
- 5 0 4 6 その他業務用備品
- 5 0 4 7 歯科、実験、医療、眼科、病院器具・備品
- 5 0 5 1 メタルサービス
- 5 0 6 5 電気部品
- 5 0 7 2 ハードウェア器具・備品
- 5 0 7 4 配管、暖房器具

5 0 8 5	その他工業用備品
5 0 9 4	宝石、貴金属、時計、装飾品
5 0 9 9	その他の耐久消費財
5 1 1 1	事務用品、オフィスサプライ、用紙
5 1 2 2	薬品、特許売薬、薬品雑貨
5 1 3 1	反物、小間物、呉服
5 1 3 7	男性・女性・子供向け業務用制服
5 1 3 9	業務用靴
5 1 6 9	その他の化学類似商品
5 1 7 2	石油、石油製品
5 1 9 2	定期刊行物、新聞
5 1 9 3	花関連商品、苗木、花
5 1 9 8	ペンキ、ニス関連商品
5 1 9 9	その他生活必需品
7 3 7 5	情報検索サービス
7 3 7 9	その他コンピューターメンテナンス、修理サービス
7 8 2 9	動画・ビデオ制作、配信
8 7 3 4	テストングラボラトリー（薬品以外）

Visa 独自のコード

4 5 1 1	（リスト以外の）航空会社
4 7 2 3	パッケージツアーオペレーター（ドイツ専用）
7 0 1 1	（リスト以外の）ホテル・ロジ
7 5 1 2	（リスト以外の）レンタカー会社
9 7 0 0	International Automated Referral Service (for Visa use only)
9 7 0 1	Visa Credential Server (for Visa use only)
9 7 0 2	GCAS Emergency Services (for Visa use only)
9 9 5 0	Intra-Company Purchases

2.4.2.3 フロアリミットの設定

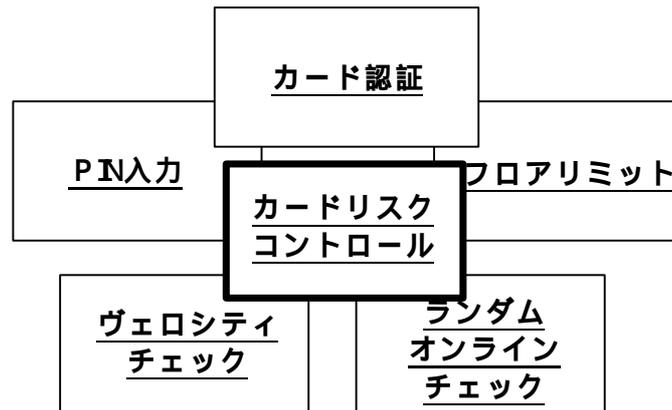
フロアリミットについては、各商品コード別で過去の平均単価・換金性商品の有無等を加味し、本来のICカードの特性を生かして利便性を損なわない様、業界でのある程度の基準として、フロアリミットの設定をする必要がある。また、ハイリスク店・悪用発生店については、個社毎の判断をもとに、適切なフロアリミットを検討する必要もある。

加盟店業種の識別について何処まで行なうかと言う問題と、識別された加盟店業種毎のオフライン適性の判断については、最終的には業界内での十分な検討と、その結果に基づくコンセンサスが必要である。

2.4.2.4 フロアリミットとリスクコントロール

クレジット業務において、ICカードを使ってより安全なオフラインを含めた取引を行なうには、上記フロアリミットのみカードリスクコントロールでは不十分な場合も有

り得る。ICカードの特性を生かして、別のリスクコントロール手段、例えば、ランダムオンラインチェック・ヴェロシティチェック、カード会員のPIN入力、カード認証等と合わせて、リスクを低減することが可能であれば、発行者のみならず加盟店側に対しても、ICカードを使ったオフライン取引のメリット（通信コストの削減、ホストコンピュータ負担軽減、処理時間の短縮）を最大限に活かし、且つフロアリミットの設定金額をある程度高めることも将来的には可能であると考えられ、ICカード普及のために加盟店側へアピールするものと思われ、クレジットカード業務へのICカードの適用並びに普及の実現に向けて有効なものとなる。以下に手法と効果を示す。



ICカードリスクコントロールの手法と効果

1. カード認証：カード偽造・変造の防止
2. PIN入力：第三者によるカード不正利用を防止
3. 端末リスク管理
 - フロアリミット
 - ランダムオンラインチェック
 - ヴェロシティチェック
 - 途上与信管理・多重債務防止・買い回り、本人カード乱用の防止。

2.4.2.5 端末リスク管理手法

ICカード利用に伴うICカードと端末間の基本的なトランザクションフローは、図2-3の通りであるが、実際に実行される順序はカード発行会社や、加盟店、端末により異なる場合もあり確定したものではない。

本章で言う端末のリスク管理は、ネガチェックとフロアリミットチェックを基本とし、これを補完する形でヴェロシティチェック・ランダムチェックの二つを効果的に組み合わせることにより、オンライン処理に劣らないリスク管理を実現するものであり、図2-3の塗り部分を対象とするものである。

即ち、ネガチェックとフロアリミットチェックによる現行のオフライン機能に対し、ICカードの特性を活かした、チェック機能（ヴェロシティチェック、ランダムチェック）を付加することにより、オフライン環境では検知することのできない、種々の不正・リスクを防止するものである。

尚、各々のチェック内容・機能は後述の通りであるが、これらの機能を活用する為には

各種パラメータの設定が不可欠である。

パラメータの設定は、原則加盟店とカード会社の契約に基づくものであるが、加盟店店頭における運用上の混乱を回避するために、業界で統一することの検討も必要である。

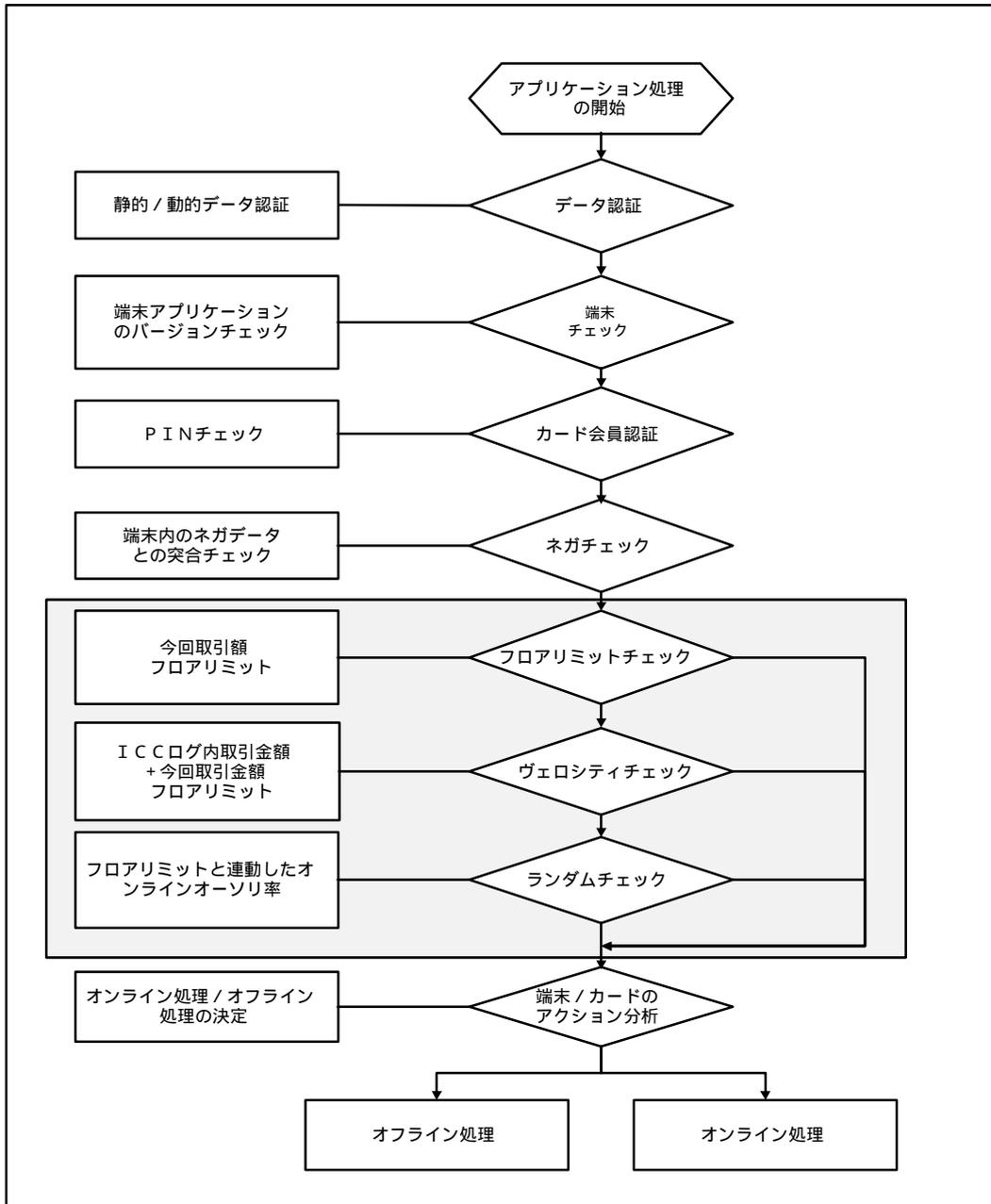


図 2-3 端末リスク管理のトランザクションフロー

(1) フロアリミットチェック

フロアリミットは、加盟店及び端末単位にあらかじめ取り決めされた金額で、これを超えた取引は、カード会社へのオンラインオーソリが必要となる。

フロアリミットチェックは、今回の取引金額がこのフロアリミットを超えているか否かをチェックするものであり、現状の磁気カードと同様の考えである。

しかし、ICカードでは、フロアリミット未満の小額取引に分割した不正取引の発

生を防止するために、ICカード内の取引ログを利用したチェック機能も有しており機能強化されている。

(2) ヴェロシティチェック

ヴェロシティチェックは、オフライン取引件数/金額を管理することにより、フロアリミット以下の取引であっても、オンライン処理を行うか否かのチェック方法を決定するものである。

連続したオフライン処理の件数/金額が予め設定されたものを超えると、その取引金額に係らずオンライン処理されることになるが、件数/金額の何れか一つを超える場合も、オンライン処理の対象となる。

オフライン処理の件数/金額のパラメータは、レギュラーカード・ゴールドカード等のカード種別毎の設定が可能であると同時に、不正使用や事故発生状況に応じてカード会社の判断により変更が可能である。

(3) ランダムチェック

ランダムチェックは、端末内に設定された表 2-5のパラメータにより、オンライン/オフライン処理の決定を行うものである。

即ち、ランダム選択のしきい値以下ならば一定の確率(目標パーセンテージ)でオンライン処理を選択し、ランダム選択のしきい値以上フロアリミット未満であれば、金額に比例して確率(最大目標パーセンテージまで)を上げていき、オンライン処理を行うものである。

尚、フロアリミットを超えた場合は、フロアリミットチェック機能によりオンライン処理となる。

表 2-5 パラメータ項目別設定例

パラメータ項目	設定例
フロアリミット	1 0 0
端末乱数	2 5
しきい値	4 0
目標パーセンテージ	2 0 %
最大目標パーセンテージ	5 0 %

各パラメータ(表 2-5)の相関を図 2-4に示す。

<例 1: 利用金額が 20 の場合>

利用金額(20)は、しきい値(40)以下なので、端末乱数(25)と目標パーセンテージ(20%)を比較し、端末乱数の方が大きいのでオフライン処理となる。

<例 2: 利用金額が 60 の場合>

利用金額(60)は、しきい値(40)を超えているが、フロアリミット(100)以下である。

利用金額(60)は、しきい値(40)より20(60 - 40)大きく、フロアリミット(100)としきい値(40)の差(60 = 100 - 40)の1/3(20/60)となる。

次に、最大目標パーセンテージ(50%)と目標パーセンテージ(20%)の差(50% - 20% = 30%)の1/3(30% × 1/3 = 10%)は、10%となる。

これにより、しきい値を超える金額は、利用金額20毎に10%ずつ目標パーセンテージが上昇することになる。

この例では、端末の乱数(25)が目標パーセンテージ(30%)以下なのでオンライン処理となる。

<例3：利用金額が150の場合>

利用金額(150)は、フロアリミット(100)を超えているのでオンライン処理となる。

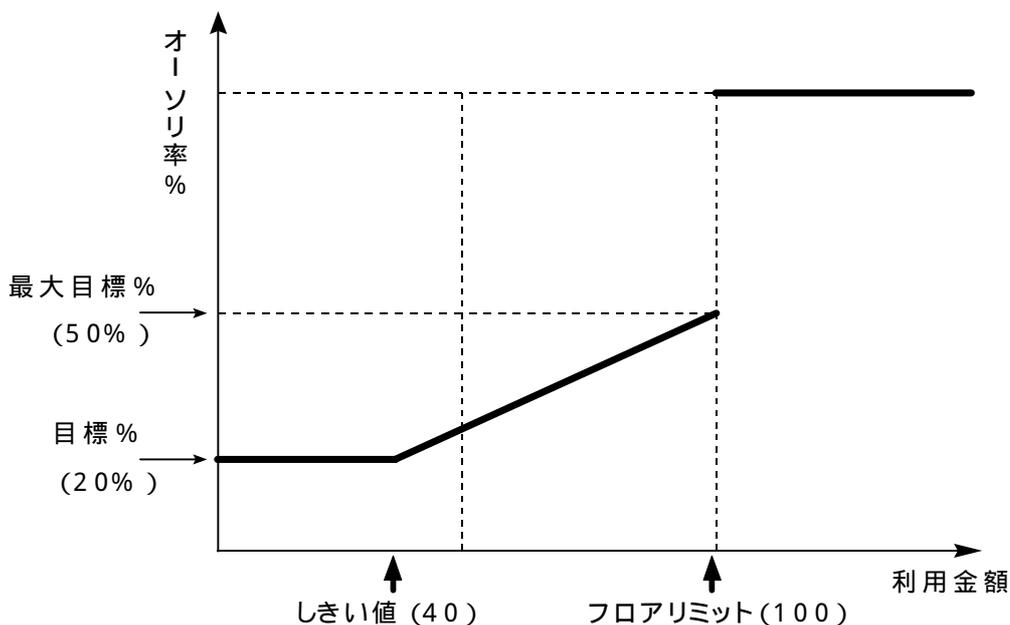


図 2-4 ランダムチェックにおける各パラメータ関連概念図

端末リスク管理の各機能は以上の通りであるが、これらの機能を活用するためのパラメータの設定に際しては、下記事項を十二分に検討することが不可欠である。

パラメータの登録及び変更方法

端末の設置手続き並びに各カード会社への設置情報の回付する為の機関(現行C A T事務局の様なもの)と、各種パラメータの登録・変更等に係る処理について、加盟店、カード会社に負荷の掛からない方法を検討しなければならない。

パラメータの設定基準

パラメータの設定に際しても、個別カード会社の判断による設定も可能であるも、実際の利用先である加盟店において、カード会社毎に設定基準が異なると混乱を招く事が懸念される。

いくら先進的な技術であっても、市場に受け入れられなければ意味がなく、原則業界統一の方向で検討すべきである。(個別加盟店の状況に応じた個社対応は必要であるが)

2.4.2.6 業種別の具体的な利用方法の提案

現状CATを利用する場合、ハイリスク商品の信用販売では商品コードを入力するようになっているが、EMV仕様の規定上では端末にあらかじめ業種コードを設定するようになっている。

ISO 8583で列挙されているコードには日本の実状にそぐわない職種もあるため、全部をサポートする必要はないと考える。(前章のコード表参照)

前項の3種のパラメータの組み合わせを変えることによってさまざまなリスク管理が可能になるが、一方でカード会社側の運用が複雑になるため、一定数のパラメータの組み合わせパターンにまとめるのが当面の妥当な方法と考える。

ここでは前項の解説を踏まえて、その具体例を提案したい。

(1) 業種の分類

業種の分類については次の2つのカテゴリーの組み合わせにて検討する。

一般店、ハイリスク店

現在カード会社では加盟店のカテゴリーを、一般店と、換金性の高い商品を取り扱う店、あるいは不正使用の頻度が比較的高いと考えられる業種(ここでは「ハイリスク店」と称する)との2種に大別しているため、これにしたがって分類する。

利用単価の大小

オフライン取引の導入にあたっては、平均利用単価を何段階かに分類することが望ましいと考える。ここでは3段階とする。

強制オンライン実施店

悪用発生率が極端に高い店などは加盟店の共謀の可能性もあるため、一時的にでもフロアリミットをゼロにして全件オンラインオーソリに変更できるなど、厳格に対応できることが望ましい。

この3要素を組み合わせ、表2-6の6通りのパターンを検討することとする。

表 2-6 パターン区分例示一覧

	平均単価	対応業種	パターン
一般店	5,000 円未満	レストラン、スーパー、書籍・レコードなど	
	30,000 円未満	テーマパーク、レンタカーなど	
	30,000 円以上	百貨店、衣料品店、ホテル、ゴルフ場など	
ハイリスク店	5,000 円未満	タクシーなど	
	30,000 円未満	カメラ店など	
	30,000 円以上	宝石店、電化製品など	
強制オンライン実施店			

(2) 具体案

1999年1月より一般的な店舗における業界統一のフロアリミットは1万円に引き下げられる予定となっている。ICカードがクレジット取引分野で本格導入されても、当面は磁気ストライプによる取引が多数を占めるため、フロアリミット低減化の傾向はリスク管理上の理由からも否定できない。しかしながら、処理時間を短縮す

ることによって利用者の使用感の向上に努めることがICカード導入の主目的の一つである。ここで提案する内容は、ICカードのインフラが十分に普及した段階のものであり、実際にはこれらが段階的に達成されるべきもので、磁気ストライプによる取引はこの限りにあらずということが前提である。

フロアリミットとランダム・チェック

フロアリミットとランダム・チェックは端末内のパラメータだけで実行する。(表 2-7)

表 2-7 フロアリミットとランダム・チェック

パターン	フロアリミット	ランダム・チェック		
		閾値	オンラインオフライン率	
			閾値以下	閾値～フロアリミット間
	10,000 円	2,000 円	10%	2,000 円毎に 10%上昇
	20,000 円	5,000 円	20%	3,000 円毎に 10%上昇
	30,000 円	10,000 円	30%	5,000 円毎に 10%上昇
	10,000 円	2,000 円	30%	2,000 円毎に 10%上昇
	20,000 円	5,000 円	40%	3,000 円毎に 10%上昇
	30,000 円	10,000 円	50%	5,000 円毎に 10%上昇
	0	0	100%	-

ヴェロシティ・チェック

ヴェロシティ・チェックはICカード内に記憶される連続オフライン取引回数、もしくは金額をチェックし、どちらか一方でもそのパラメータを超えた時点でオンライン・オーソリゼーションを行なうように仕向ける。(表 2-8)

表 2-8 ヴェロシティ・チェック

	取引回数	取引金額
ワールドカード	10	30 万円
一般カード	5	10 万円

最後に、本来これらのパラメータはイシュー、アクワイアラが個別に設定できるよ
うすべきであるが、全てのカード会社がこれに対応するとは限らず、また企業体力や
企業ポリシーの違いからリスク設定には自ずと差異が生じるはずである。業界で一本
化すべきかどうかをまず十分議論すべきである。

2.4.3 SCJ実証実験に見るICクレジットカードへのEMV仕様の適用について

ここでは、SCJ実証実験におけるICカードの発行状況を参考とし、一般論としての
ICカード型クレジットカードの業界標準とされるEMV仕様の適用状況を確認し、各カ
ード会社では、どのような仕様を検討すれば良いかを日本国内のクレジットカード業務の
現状も踏まえて、EMV仕様の範囲外も含めガイドラインとして記述する。

SCJ実証実験では、上記EMV仕様を基にVISAが開発したICカード仕様 VISA
Integrated Circuit Card Specification (VIS) と、ICカードのセキュリティ仕様であ

る Chip Card Payment Service (CCPS) を採用している。データに関しては、将来要求されるいわゆるフルスペックではなく、比較的現行に近いアーリーオプション (Early Option) が採用されている。

2.4.3.1 カード仕様

CPU搭載のICカードの基本仕様については各社とも発券実績がないため、それぞれ自社内関係部署のほかビザ・インターナショナル(日本支社)とも協議の上策定されている。

(1) クレジットカード基本仕様

原則として現行のクレジットカードの機能に同じ。従って、磁気ストライプ上にエンコードされた会員番号等の情報により通常のクレジットカードとして利用することが可能である。

(2) ICカードパラメータ

カードに搭載するICチップは、一定の判定条件によりオンライン承認とオフライン承認が発生する。EMV仕様では、その要素が提示されており、これに各社・ブランド毎にいくつかのパラメータを組合せることになる。

主な判定条件・アクション指示は以下の通り。

基本設定

A. 地理的制限チェック

EMV仕様が国内トランザクションのみで適用されるものかどうかを判定、文字コードレベルでのデータ互換性を確認する。国際汎用カードの場合、原則として制限は設けていない。

B. データ認証(静的/動的)

アプリケーション選択によりクレジットカードを選択した場合、後払い故の与信の供与という性格上、基本的にはカードの真正性のチェックが必要且つ重要であり、『Easy Entry』アプリケーションを採択する場合を除いて、静的若しくは動的データ認証を行なうようにパラメータの設定が必要で、EMV仕様にその方法が記載されている。尚、仮に動的認証を行う場合でも、静的認証の方法は変わらないと考えられる。

C. 各種アプリケーションチェック

通信手順制御に必要。バージョンチェックや、ショッピング、キャッシング事業の分類、期間判定ならびに有効期限チェック等が考えられる。

D. カード保持者認証

EMV仕様では、PINのほか指紋等のバイOMETRICS照合も規定されている。国内では4桁のPINが一般的だが、ISOでは12桁まで設定可能であり、また、既に一部の地域では指紋の認識装置が廉価で入手できることもあり、世界的にはセキュリティの向上が目覚ましい。

認証方法は、リトライ可能回数を含めて、IC・端末間の個別アプリケーションが制御・判定する為、カードブランド毎(正確にはカード毎)の設定が可能である。

E. 端末リスク管理

ICカードの特長であるオフライン承認を認める場合を、主に頻度の観点から制限するためのテーブル。

具体的には、以下のものが想定される。

a) 端末フロアリミット

カード発行会社（イシュア）ではなく、加盟店契約会社（アクワイヤラ）が端末ごとに設定する。各業種・個店による細分化された設定を行うことにより、より効果的なオン・オフリスク管理が実現される。その際、消費者保護の観点から、現在のフロアリミットのガイドラインに準じ、高くても30,000円以下であることが望ましいと考えられる。

b) ランダムトランザクション選択（ヴェロシティチェック）

カードのオフライン承認利用機会が増加するため、ランダムにオンライン化することにより悪用を防止する。

当該判定は、他の全てのオフライン承認処理判定が下された後に、一定確率でオンライン判定を出し、オンライン処理プロセスへ移行するため、他のオンライン承認処理時間と比較しても著しく長い。EMV仕様に準拠したICカード型クレジットカードを発行しているSCJ実証実験においても同様の事象が発生している。

従って、小口買上が高頻度で発生した場合でのオフライン承認の阻害要因となることを避けるため、オンライン承認の頻度をオフライン承認金額累計額に比例させると効果的であると思われる。

c) 連続オフライン金額チェック

オフライン処理した累計金額がチェック金額を超過した際にオンライン処理を指示する。オンライン処理が実施されると0クリアされる。

d) 連続オフライン回数チェック

連続オフライン決済処理の回数を制限すること。ただし、オフライン承認判定が発生した際、端末がオンライン承認不能である場合が考えられるが、これらに該当（もしくは超過）した場合のフローについては、上述の金額と連携した承認・不承認判定を行うことや、判定を別テーブルを保有し管理するのが一般的。

F. カード真正性確認

オンライン処理を行う場合、予めカード会社やブランドが定めた暗号方式により作成されたデータを添付して送信する。

カード会社ホストでは当該データを解析し、当該カードの真正性を確認する。

現在、磁気カードでも類似した認証方法が採用されている。

a) キャッシュディスペンサ

キャッシュディスペンサ（CD）などでPINを送信する際、（カードではなく）CDとカード会社のホストコンピュータの間での暗号通信を行い、盗聴の防止と、通信相手の（同一の鍵を保有しているという事実からの）認証を行っている。

b) カード内に暗号コード

カード内に一定の暗号コード（チェックコード）を登録しておく事により、当該カード番号や磁気ストライプ上にエンコードされた情報を改竄した番号偽造カードに対しては非常に効果がある。また、磁気カードデータに書き込むことで利用できる為、VISAやMasterCardでもCard Verification Numberとして制度化されている。

G. イシュー認証

オンライン処理が行われた場合、カード会社からのレスポンスデータを受け取る際、予めカード会社やブランドが定めた暗号方式により作成されたデータが添付されている。F.のカード真正性確認の同様の暗号通信で構成され、カード内のチップは当該データを解析し、（カード自身からは自らのイシューである）カード会社のホストコンピュータの真正性を確認する。

H. 発行会社固有プログラム

EMV仕様では、カード会社の必要に応じプログラムを無効化したりPINを変更することが可能となっている。ただし、カード会社では以下の課題解決が前提となる。

a) カード会員データベースを基点

カード会社ホストにおける最も負荷のあるカードオーソリゼーションシステムに対し、カード会員データベースを基点としたレスポンス時の新規データの生成・配信への対応負荷が要求される。

b) ネットワーク環境

CATやG-CAT、またはPOSの接続で最も一般的に利用されているCAFISや、ビザ・インターナショナルのVISA-NET、MasterCardインターナショナルのBANK-NETなどの錯綜したネットワーク環境では、確実なコマンドデータ配送が非常に難しいと考えられる。

イシューアクションアイテム（端末に提示される承認・不承認要素）

上記各種リスク管理項目に対する対応方法をパラメータとして検討する。

基本的には、「0：オフラインで承認」、「1：オンライン判定」、「2：オンライン、できなければ承認」、「3：オンライン、できなければ不承認」、「4：オフラインで不承認」が考えられる。

ここで言う「0：オフラインで承認」、「1：オンライン判定」、「4：オフラインで不承認」の3つの判定に関しては、現行の磁気カード型クレジットカードの概念にもある為比較的理解し易いが、他の2つについては簡単に補足する。「2：オンライン、できなければ承認」は、オンライン承認の範疇と見做された処理をされることで問題がない状況ではあるが、敢えてオンライン・オーソリゼーションをするような時、つまりカード利用に関する確認（途上与信管理上の確認）よりもカードの真偽そのものに重点を置いた確認時に用いる。これとは逆に「3：オンライン、できなければ不承認」は、磁気カード型クレジットカードにおけるネットワークセンターによる代行オーソリゼーション（キャッシング利用時）の際に多く採用されている方法で、カードの利用頻度・内容自体が途上与信管理の上で問題とされ

る場合である。

EMV仕様から想定される主な判定条件・アクション指示に関する考え方は以下の通り。

A. 静的認証が正常に完了しなかった

静的認証はICカードのデータ改竄の有無を検証するために行われるものであるため、正常に完了していない場合、偽造確認とオンライン処理によるカード真正性確認を行うことが望ましい。

B. 静的認証が失敗した

A. と類似した状況であるが、ICカードデータの改竄もしくは破損の可能性が非常に高いため、ICカード発行に関する本来の意義からすると不承認にすべきであるが、ICクレジットカードとしての耐性評価がなされていない現状ではオンライン承認の余地を残すことが望ましいと思われる。

C. PIN試行制限超過

本人確認手段としてPIN入力を定義しているため、原則的には誤操作を許容した制限回数を超過した会員はオンライン確認を経ることなく不承認として問題はないと思われる。但し、磁気カードからICカードへの切替え初期においては、現行キャッシング利用時以外ではほとんど一般的ではないPIN入力が、通常の見引き形態として定着するまでの暫定的な運用については、現状でも特にPIN入りに抵抗感を抱いているものと想定される高齢者への配慮を含めて十分な検討を要するものと思われる。

D. PINパッドなし

正確に評価すると、これにより承認可否の判定を行うことは適当ではない。ただし、端末操作者が意図的にPINパッドがない状態にした場合を考慮し、ネガティブな方向の判定のほうが望ましい。

E. PIN入力なし

上記PINパッドがあるにもかかわらず、PIN入力がなされない場合は、PIN試行回数制限超過同様オンライン確認を経ることなく不承認として問題はないと思われる。

F. フロアリミット超過

個社のポリシーによる影響が大きい部分であり、連続オフライン金額や加盟店業種により相対的に決定されるべきである。

カードアクション分析（その他承認・不承認選択要素）

上記各種リスク管理項目のほかの対応方法をパラメータとして以下のものを設定する。

基本的には、イシューアクションの場合と同様と考えられるが、想定される主な判定条件・アクション指示に関する考え方は以下の通り。

A. 当該カード初利用

特に必要があるわけではないが、以下の理由からオンラインが望ましい。

- a) カード発券から送達時のカード損傷が発生していないことを確認するため
- b) カード実効時期を特定させるため

B. 前回未完了

会員・加盟店のいずれの責によるかが分からない状態であることから、オンライン承認を指向し、本件により承認可否の判定を行うことは適当とはいえない。

SCJ実証実験においては、参加カード会社は「2：オンライン、できなければ承認」を選択しているが、ICカードが普及した時点では「3：オンライン、できなければ不承認」が適当だと考えられる。

C. 前回イシュア認証失敗

イシュアからの暗号通信が正常に完了していない場合はカードのステータスが異常である可能性がある為、オンライン処理を行い再検証することが望ましく、

「3：オンライン、できなければ不承認」が適当だと考えられる。

D. 連続オフライン上限超過

ICカードの特長としてオフライン決済を指向する特性上、スタンドアロン・オンライン端末の導入が将来的に発生すると思われる。この場合を考慮し、承認を取得時に必ずしもオンラインを強制することができない場合が考えられる。

(個々の判定条件は独立しており、仮に限度額を超えたらというような仮定は別判定要素として扱う)その為に、連続オフラインの回数を複数設定すると効果的である。その際のオフライン限度回数を上限とするので、「3：オンライン、できなければ不承認」が適当だと考えられる。

E. 連続オフライン下限超過

オフライン限度回数を連続オフライン上限とした場合、当該回数よりも低いところに一次限度回数を設定することになる。一般的には、この一次限度回数は連続オフライン上限と対照し、連続オフライン下限と呼ばれているようである。従って、「2：オンライン、できなければ承認」が適当だと考えられる。

F. 連続オフライン合計金額超過

1回当りのオン・オフ判定は、端末フロアリミットで制限されており、これはアクワイヤラ要件である。従って、買い廻り等を考慮したオフライン買上金額は連続オフライン金額にて管理することになるため、「3：オンライン、できなければ不承認」が適当だと考えられるが、SCJ実験においては、取り敢えず承認ということで実施中である。

(3) その他

EMV仕様では、起動アプリケーションが指定された後は、当該アプリケーションがEMV仕様に準じた機能を果たすが、EMV仕様に規定しない項目でも、アプリケーションが独自に特定の機能を満たすことができる。従って、上記に記載のない判定要因を独自に設定することも可能である。

2.4.4 オフライン取引データの効率的な事後処理についての考察

クレジットカード業務においてはその後払いという特性故に、ICカードの普及により増加する売上精算データとしてのオフライン取引データを、適宜発行者へ計上する必要がある。特に現行の磁気カードが完全に切替わった場合を想定した時に、売上精算データの事後処理を迅速且つ効率的に行うことが重要になる。以下この点に関して考察した内容

を記す。

2.4.4.1 効率的な事後処理に求められる要件

前節の通り、ICカード化により偽造カードによる不正利用が防止され、カードと端末のリスクコントロール機能を上手く組み合わせ、オフライン取引であっても、買い廻りが防止されるとすると、安全に完了したオフライン取引の売上精算データについては、現行の磁気カードシステムにおけるネガチェックのみで取扱われた売上精算データ程には、途上与信管理の観点からもデータ授受の頻度（緊急度）は問われないものと考えられる。（勿論事務処理の平準化の要請は残るので、特定日への集中回避を考慮する必要はある）

そこで考えられるのは、各カード会社センタについては、オンラインオーソリゼーションによる販売承認の判定が必要な取引のレスポンスを向上させるために、余分な負荷をかけないことであり、特に電子データ化されたものであれば、各加盟店から必ずしも個々に直接カード会社へ売上精算データを送信する必要は認められないし、大半のカード会社センタはCAFIS手順対応のみのセンタ構築であり、直接受信する為に一気に全てのカード会社センタの改修を行うことは、コスト面を含めて現実には不可能である。つまり、何ヶ所か各加盟店が保有するオフライン取引の売上精算データを集約し、カード会社毎に振分ける業務を行なう業者があればよいことになる。このことより、各種端末の管理業務等も行なうであろう情報処理センタ（ネットワークセンタ）が重要な役割を担うことになるものと考えられる。

2.4.4.2 売上精算データ授受の手法について

上記の通り、情報処理センタ（ネットワークセンタ）が加盟店とカード会社間に介在するとすると、売上精算データの授受の手法については、先ずデータ授受が行なわれる場としては、加盟店（端末）～情報処理センタ（ネットワークセンタ）間、情報処理センタ（ネットワークセンタ）～カード会社センタ間の二つの場があり、それぞれの手法や課題は以下の通り。

(1) 加盟店（端末）～情報処理センタ（ネットワークセンタ）間

基本的には、毎日営業時間終了後に端末貯まったオフライン取引による売上精算データを、情報処理センタ（ネットワークセンタ）ヘディレードバッチ伝送により、送信処理を行なう。

この場合、現行のG-CATのバッチ伝送と同様、端末側で深夜等繁忙期を避けた時間帯の中で、端末毎に起動タイマを設定して自動的にデータ伝送をおこなうことになる。

しかしながら、この手法の場合端末インフラの整備が不十分な時点においては、現行のアナログ公衆回線接続でも、十分センタ側でコントロール可能なものと思慮されるが、将来端末台数が数十万台から百万台を超えるような状況を想定した時、タイマ設定のみでは混乱の回避は不可能であろうと思われる。

この場合必要なことは、各端末からのデータ伝送を如何に短時間で終了させるかということであり、実現策としてはISDNの利用とデータの圧縮が考えられる。この点は今後の重要な検討課題である。

* 現在考え得るものを表 2-9に示す。

表 2-9 データ伝送の要件一覧

伝送データレコード フォーマット	主として各CCTのフォーマットに準拠 *クレジットカードをベースにしているのでICカード に必要な項目は盛り込み、不要なものはカットする
通信プロトコル	主として各CCTのプロトコルに準拠
通信回線の電氣的・ 物理的条件	INSネットサービスのインターフェースを適用
伝送速度	9600bps、64Kbps

(2) 情報処理センタ（ネットワークセンタ）～各カード会社間

次に、情報処理センタ（ネットワークセンタ）～各カード会社間の売上精算データの授受の方法に関しては、カード会社毎のデータの容量の差異等から、凡そ次の2つの方法によるものとする。

データ伝送

カード会社毎に振り分けた売上精算データの容量が多い場合は、専用線若しくはDDX-P網を使った情報処理センタ（ネットワークセンタ）～カード会社間のデータ伝送が最も効率的と考える。この場合双方大型のコンピュータを備えているので、起動は双方向とも可能で、繁忙期を避けての授受の設定も容易であるものとする。

尚、通信プロトコルの問題であるが、現行のCAFIS手順は全くICカードの対応（特にEMV）は想定もされておらず、大幅な見直しが必要と思われる。ISO 8583に準拠して策定されたCC手順への対応等重要課題である。

MT・FD交換

比較的売上精算データの容量が少ないカード会社との授受については、受取るカード会社側のセンタ構築の問題も勘案すると、MT若しくはFDで十分と考える。

売上交換日は、1回～6回/月の中で選択できるものとし、フォーマットについては、各カード共現行の統一標準フォーマットに準拠したものが望ましい。新しく策定する場合でも、統一フォーマットは必要である。

2.4.4.3 情報処理センターでの一括処理を行う場合の役割・要件

上記のような運用を実現する為に、ICカードの利用システムの中核をなすものと考えられる情報処理センタ（ネットワークセンタ）の果たす役割は非常に重要であり、特に以下のようなことが求められるものと思われる。

先ず単純に、売上精算データの集配信等に関する業務処理においては、売上精算データ処理は、加盟店とカード会社との精算という重要な業務の仲介であり、特に間違いがなくてはならない処理である。そうした点からも、処理の自動化や正常終了したことを双方で確認できる手段、並びに、万が一案件数/金額の不一致が発生した場合、データの精査・照合システムを備えておくことや、売上控え伝票が存在する場合には一括保管の仕組みも必

要である。

また、端末情報の管理、その他あくまで契約を伴ってではあるが、鍵の管理までをも行なうことも必要となるものと考ええる。

従って、情報処理センタ（ネットワークセンタ）には、基本的な業務処理の為のみでなく、様々な情報に関するセキュリティ確保の面から、認証局に求められるものと同等の事務取扱いを含めたセキュリティ機能の保持を伴うセンタ、並びにシステム構築が要求され、義務付けられるものと考ええる。この点に関しては、先述のWG 8の認証局の運用に関する様々なガイドライン、センタの建物を含めた安全基準については、通産省で定め通産大臣名で認定を行っているものに『情報処理サービス業電子計算機システム安全対策実施事業所認定制度』があり、また、（財）金融システム情報センタ（FISC）が策定した『金融機関等のコンピュータシステムの安全対策基準』と『同解説書』（1998年6月を以て7年ぶりに大幅改定作業中）も現在FISCで検討されており、これらを参考にその具体的な要件を詰める必要がある。

2.4.5 クレジットカード業務関連法について

クレジットカード業務については、関連法律として主要なものとしてショッピング分野について規定する「割賦販売法」と、貸金分野について規定する「貸金業規制法」があるが、クレジットカードがICカード化されても適用の上では、現行の磁気カードへの適用と基本的には変わらないものと考えられ、内容に関する詳細説明は省略する。

2.5 プリペイド型電子マネー

電子マネーの定義・分類に関しては様々な見解があるが、冒頭でも述べたように本章では現行法制度下においても、また、一般的に様々な企業が参入し易く、その意味において実用化・普及が実現可能と思われるプリペイド型電子マネーを主体に、発行体の形態・適正要件や運用上の一番の課題である法的課題やその改正の動きに関し記述する。ただ、前述の通り電子マネーの定義そのものが確定していない現状も踏まえて、広義の電子マネーに関連する法律についても併せて記述する。

2.5.1 電子マネー業務に関する現行法上の各種規制の整理

電子マネーについては、様々な発行形態があり形態によっては関連する現行の法制度も異なってくるものと思われるが、ここでは先ず、ICカードを用いたプリペイド型電子マネーに関連深い「前払証票等の規制に関する法律」と、広義の電子マネーに関連する「銀行法」「出資法」について見てみることにする。

無論これらの法律以外にも、発行されたICカードが有する汎用性の度合いによっては「紙幣類似証券取締法」、海外でも利用できるというのであれば、「外為法」というように様々な法律が関係してくるものと考えられる。

2.5.1.1 発行にあたって

(1) 前払証票等の規制に関する法律

プリペイド型電子マネーに、現行の法制度の中で最も関連がある（適用される）と

思われる「前払証票等の規制に関する法律」について見てみる。

前払式証票の定義（法第2条第1項第1号抜粋）

同法では「証票その他の物に記載され又は電磁的方法により記録されている金額に応ずる対価を得て発行される証票等であつて、当該証票等の発行者又は当該発行者が指定するものから物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの対価の弁済のために提示、交付その他の方法により使用することができるもの」と定義している。

この定義においてポイントとなるのは、対価を得て、証票等が発行されるということと、その証票を提示等することにより使用することができるということである。

ICカードを用いた電子マネーの場合には、あらかじめ現金、クレジットカード、預金等の移動により、価値データがICカードにロードされることにより対価が支払われており、ICカードという証票も現に発行されている。そして、その証票を交付することにより物品の購入やサービスの提供ができる。即ち使用することができる訳であり、本法の対象となると考えられる。

同法では3条で適用除外を規定している。

- a) 国又は地方公共団体が発行するもの
- b) 法律に基づき設立された法人等が発行するもの
- c) 発行者の従業員に発行されるもの
- d) 割賦販売法等の法律によって前受金の保全措置があるもの
- e) その他使用者の商行為取引で使用するもの

発行形態

法は証票の利用範囲の違いにより、「自家発行型」と「第三者発行型」の二つの形態に分けられてる。

証票の発行者からのみ物品の購入やサービスの提供を受けることができるものが、自家発行型であり、それ以外のものが第三者発行型と区別される。

参入にあたって

A. 発行者の人格

a) 自家発行型

規制なし。

b) 第三者発行型

法人格を有する者で資本の額は1億円以上。但し、地域限定型は1千万円。

B. 発行時の規制

a) 自家発行型

発行に当たっての規制はないが、基準日未使用残高が700万円を超えるときは、所轄の財務局に届け出が必要。

b) 第三者発行型

事前に所轄の財務局に登録が必要。

C. 発行保証（自家発行型、第三者発行型共通）

a) 発行保証金基準

基準日の未使用残高が、1000万円を超える場合、基準日未使用残高の二

分の一の額。

b) 発行保証金

供託、保証、保険。

* その他、帳簿書類、報告・検査等、証票表示事項などに関する規制が存在する。

(2) 銀行法

電子マネーの発行が、銀行等の付随業務に該当するかどうか問題となる。

銀行法では、その第10条第1項において、銀行の固有業務を規定し、合わせて第2項で銀行業に付随する業務を規定している。

付随業務としては10項目を列挙している他、「その他の銀行業に付随する業務を営むことができる」という表現により、付随業務に弾力性を持たせている。

最終的にこの付随業務に該当するかどうかは行政当局の判断に委ねられることになるが、現在の大蔵省の見解としては、電子マネーが現在の銀行の決済機能を高度化するものであることと、諸外国でも電子マネーは銀行が中心となって取り組んでいることを理由に、電子マネーの発行・流通業務は銀行の付随業務であるとの判断を示している。

(3) 出資の受入れ、預り金及び金利等の取締りに関する法律

電子マネーに一般換金性を持たせた場合、出資法上の「預り金」に該当するかどうか問題となる。

出資法はその第1条第1項で、業としての「預り金」を禁止しており、同法第2条第2項で「預り金」を定義している。

大蔵省銀行局内プリペイドカード研究会がまとめている「プリペイドカード法の手引き」によれば、「預り金」とは預金と同様の経済的性質を有するものとして、名称の如何を問わず通常、以下の要件を満たすものとしている。

不特定かつ多数の者が相手であること

金銭の受入れであること

元本の返済が約されていること

主として預け主の便宜のためになされたものであること

そして、「預り金」に該当するかどうかは預金と同様の経済的性質があるかないかにかかっており、仮にプリペイドカードが換金性を有したとしても、そのみをもって直ちに出资法違反となるとは断定できないとする。

但し、プリペイドカードについて、一般的換金を行なうような、即ち一般的に元本の返還が約されていると解されるような場合には、出資法違反の疑いが生じようとしている。

電子マネーについても、一般換金性を持たせれば出資法に抵触する可能性が高いと考えられる。

* 銀行等については、もともと「預り金」が認められており、銀行等が発行する電子マネーについては、これらの問題は生じない。

2.5.1.2 大蔵省の「電子マネー及び電子決済の環境整備に向けた懇談会」における中間的な

論点整理」について

同懇談会では、電子マネー・電子決済の健全な発展・普及のための環境整備を目的として、現在検討を行なっているが、この環境整備の中には、新たな立法措置を含む法制度の整備も含まれている。

この法整備に対する考え方が示されていることから参考までに概略を示すこととする。同懇談会では、今後検討を進めて行くべき具体的な論点として、次のことを掲げている。

- (1) 電子マネー・電子決済に係る公正な取引ルールと利用者保護の在り方
当事者間の権利義務関係の明確化（強制執行等の第三者との関係等を含む）
利用者に対するサービス提供者の行為規範（説明義務、情報開示、責任分担等）
- (2) 電子マネー発行体の適格性要件
参入要件、業務の適正性確保、財務の健全性確保等。
- (3) 電子マネー発行体の破綻時の対応
発行体破綻時の早期対応、権利実行手続の整備、権利の実体的な保護。
- (4) その他
不正使用・不正行為の防止（電子マネーを用いたマネーロンダリングといった犯罪の防止等）
技術面での適正性確保
等となっている。

2.5.1.3 運用上の課題と対応について

特に電子マネー業務の場合、運用上の課題は法的な規制に係わるものが多い。課題とその対応について記す。

(1) カード紛失・破損時の保障

電子マネーの運用上の問題の一つは、カード紛失・破損時の保障をどうするかということであるが、前者に関して、MONDEXはオプションで暗証番号を入力しないと利用できないというロック機能を付加しているものの、これとて他人に利用されないというだけで、基本的には現金と同様紛失したら何等保障されないというのが一般的である。

後者に関しては、プリペイド型電子マネーの運用に適用される「前払式証票に関する法律」について電子マネーを意識した約款の改定が行われたので、以下その内容を記す。

《平成9年5月に行われた前払式証票標準約款の改訂点》

磁気カード式第三者発行型に関し下記項目を改訂。

取引標準約款

- A. 発行者・加盟店間の決済以前に利用者が抗弁権の接続を主張できる場合の規定
- B. カードの物理的破損が著しく、残高の推計不能な場合にカードの再交付をしないとの発行者の免責規定

更に、加盟店の不正から利用者保護の為、次のものも盛り込まれている。

加盟店規約

- A. カード所持者からの要求に対する、約款の交付義務

B. カード利用時にカードリーダーの残高表示等を利用者が確認できる措置を講ずる義務

C. カード利用代金決済の例外として、カードが不正利用され、加盟店が悪意、重過失の場合には発行者が支払義務を負わない旨の規定、また、その調査のため決済を留保することができる旨の規定

(2) 個人間譲渡

現状認められていないが、駒ヶ根市の「つれてってカード」では、親子等の家族間でもできないと使い勝手が悪いとの住民の要望により、個人間譲渡も開始したと聞き及んでいる。また、サイバービジネス協議会が1998年9月から開始予定の電子マネー実験では、インターネット上で電子マネーの有効期限を設け、制限付きで転々流通を認める計画である。

(3) 端末の操作ミス等による過剰減算に対する措置について

以下のような対応が考えられる。

現金で過剰減算分を返却

換金性の問題がある。

端末でICカードに過剰減算分を戻し入れする

この場合、過剰減算分以上の戻し入れのないことの確認が必要であり、また、端末ソフト対応の問題並びに発行体以外でのICカードへの加算が認められるのかという問題がある。

発行体へ持ち込んでICカードに過剰減算分を戻し入れする

発行体としては、過剰減算分を超える戻し入れのないことの確認が必要となり、どうやって過剰減算分を発行体を確認するのが問題となる。クレジットの赤伝と同じく、商店等が戻し入れ依頼書を発行し、それに基づいて実施するという考えもあるが、僅少の金額の戻し入れの為にどこまでやるかといった問題もあるものと思われ、具体的な手法については検討を要す。

(4) 発行体自体の破綻

電子マネーの発行体自体が破綻した場合については、2.5.1.2項で記述の通り、大蔵省主催の『マネ懇』における中間論点整理の中でも、その対応が課題として掲げられている。

本件の焦点としては先ず電子マネーを経理上、預金として扱うかどうかであるが、この点に関しては預金とは定義せず預金保険機構の対象としない案が有力視されており、別途利用者保護の観点から、発行体自体が破綻した場合、利用者に見合い資金が還元されるようなルールの整備が待たれるところである。(大蔵省では本年3月から検討する模様)

尚、このことは預金の受入れを認められていない銀行以外の企業にも電子マネーの発行を認める為の新たな法制度の制定の動きとも整合するものと考えられる。

2.6 端末

ICカードを利用した電子商取引システムは、世界各地でクレジット、電子マネー等の実験が多く進められており、リージョナルなシステムでは既に実用化もされている。その

利用現場も、店舗等でのリアル取引だけでなく、フランスで実験中のCSETや、近々公開予定のSETバージョン2.0のように、バーチャルでの利用に向けた仕様制定も進められている。ただ、ICカードを利用した電子商取引の普及という点から考えると、リアル取引現場での利用を促進することが最も重要である。そこで、店舗内、銀行内、自動機等のリアル取引現場において、ICカードを利用した決済取引を行う場合に使用する端末の要件およびその課題について、検討することにした。また、検討する取引の種別としては、予想される実用化時期および実施されている実験内容から、クレジットとクレジットシステムを利用した電子マネーを対象にした。

利用するICカードとしては、接触ICカード、非接触ICカード、および両機能を搭載した複合ICカードがあるが、今回はクレジットおよび電子マネーを利用する端末を中心に検討のため、既存端末インフラの活用も考慮し、接触ICカード用端末を対象にした。

対象とする端末は大別して次の3種類で、それぞれの要件および普及に向けての課題を検討した。

(1) クレジット業務用端末

店舗での支払に利用するクレジット端末および電子マネー端末

(2) 電子マネー用機器

電子マネーのバリューを充填する機器をはじめとした電子マネーの運用に利用する機器

(3) 専用機

自販機、券売機、コインロッカ、パーキングメータ等の利用者が操作するマイクロペイメント用端末

2.6.2 クレジット業務用端末

店舗での商品の購入や供給されるサービスに対する支払にクレジットカード等のカードを利用する場合、カード決済用のカード端末を利用する。磁気カードを使用するためのカード端末のインフラは既に整備されていると言えるが、これらのカードのICカード化の動きに対して、新たにICカード用のカード端末を普及させる必要がある。そこで、ICカード用カード端末の仕様、および今後解決していくべき課題について検討した。この検討に際しては、クレジット端末を中心に店舗でのカード支払に利用する端末を対象にしており、クレジットではないが店舗で利用する電子マネー端末もその対象としている。また、これらの端末をPOSと連携して利用する場合についても、今回の検討対象に含めた。

2.6.2.1 クレジット端末

磁気カードによるクレジット決済に使用するカード端末としては、G-CAT、CAT、SG-T等があり、既に50万台を超えるカード端末が店舗で利用されている。今回の検討では、クレジットカードのICカード化に対応するクレジット端末として、新規端末の仕様だけではなく、既に設置され利用されているクレジット端末も考慮におき、検討した。

今回のクレジット端末の仕様検討では、クレジットカードとして利用するICカードのカード仕様として、EMV仕様が既にデファクト・スタンダードとして認識されつつある

ため、EMV仕様で定義している端末アプリケーションのサポートレベルによって端末をタイプ分類して、検討することにした。尚、検討の対象としたEMV仕様のバージョンは、バージョン3.0(“EMV‘96”)である。

(1) EMV仕様をフルサポートしたクレジット端末

図 2-5は、EMV仕様で定義している端末のアプリケーションを全て実施する場合の端末のアプリケーションフローである。

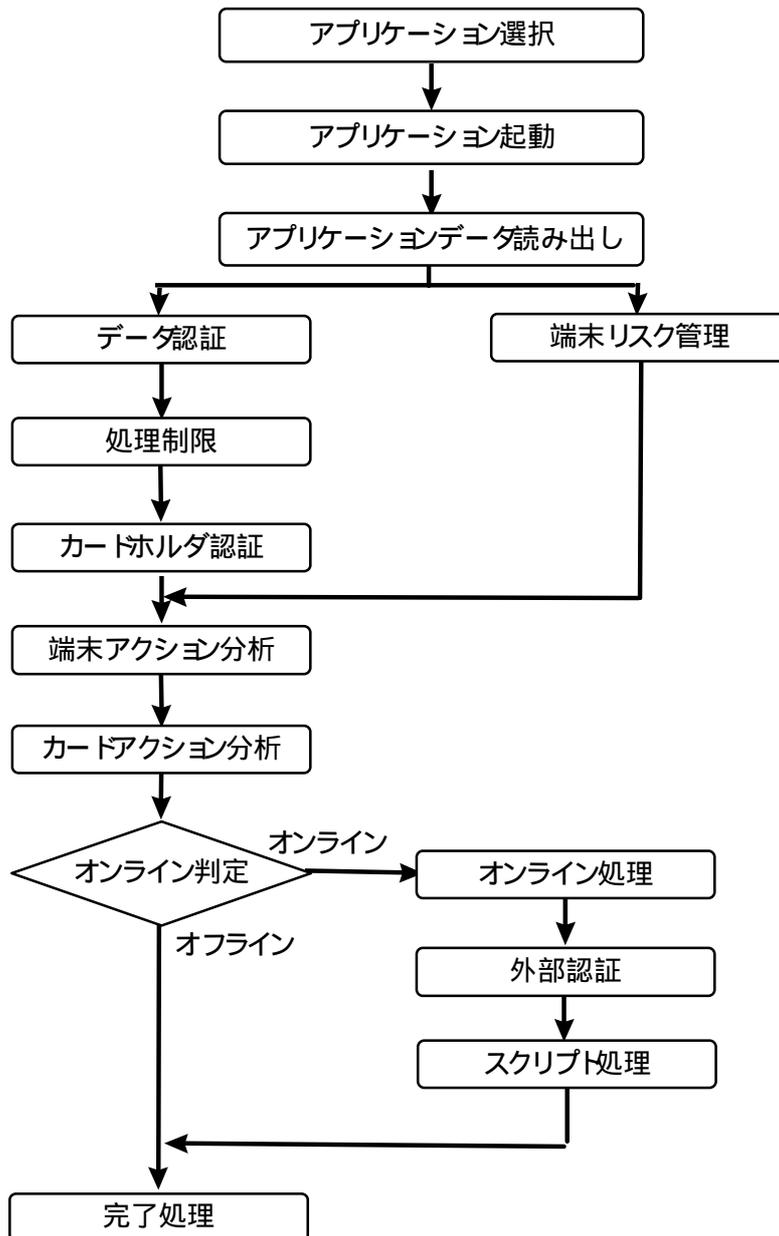


図 2-5 アプリケーションフロー

このクレジット端末について、「操作性」、「安全性」、「既設端末への影響」、「センターシステムへの影響」、「端末コスト」および「用途」の6項目における評価を行った。表 2-10はこの評価内容である。

表 2-10 評価内容

	項目	内容
1	操作性	<p>現行の端末で使用されているCPUの能力では、データ認証(静的認証または動的認証)をファームウェアで実現すると、処理速度に大きく影響する。</p> <p>個人認証にPIN入力を設定していると、顧客のPIN入力操作が増える。</p> <p>端末リスク管理の設定パラメータによるが、オフライン取引によって処理の高速化が図れる。</p>
2	安全性	<p>磁気カードのICカード化という意味で、カードの偽造、改竄等に対して、ICカード自体の持つ強度が期待できる。</p> <p>データ認証によって、カード自体の真正性を端末でチェックできる。</p> <p>不正カードをセンター側が検知した場合に、センター側からの制御でカードのロック等が可能である。</p> <p>ICカードがセンターを認証できる。</p>
3	既設端末への影響	<p>データ認証をファームウェアで実現するには、その為のメモリ増設と暗号ソフトを、またデータ認証をコ・プロセッサで実現するには、その為の暗号用コ・プロセッサを、本体またはICカードR/Wに増設することになる。</p>
4	センターシステムへの影響	<p>外部認証データの生成及びスクリプト処理の追加が必要である。</p> <p>オフライン取引を扱う一括センターが必要である。</p> <p>ICカード処理用パラメータの管理及び端末への配信処理の為の機能追加が必要である。</p>
5	端末コスト	<p>操作上許される処理速度を考慮すると、データ認証をコ・プロセッサで実現することになるが、現在の暗号用コ・プロセッサの価格では、端末価格に及ぼす影響は多大である。</p>
6	用途	<p>実用面からは最も一般的な端末タイプであると考えられるが、各カード会社センター側のサポートレベルの差異を許容できる端末の機能が必要である。</p>

(2) 他のタイプのクレジット端末

EMV仕様で定義するアプリケーションの各処理のサポートレベルを考えれば、数種類のタイプのクレジット端末が考えられる。ここでは、この内の2つのタイプの端末に対する評価をまとめる。

データ認証を実施しないクレジット端末

データ認証を実施しないでICカードによるクレジット取引を行う端末である。データ認証を実施しないため、暗号用コ・プロセッサ等が不要であり、比較的安価な端末にできる。また、既設端末も同様に比較安価に活用できる。ただし、データ認証等を実施しないことによる安全性への課題が残ってしまう。

オフライン専用クレジット端末

端末アクション分析およびカードアクション分析で「オフライン」と判定された取引のみを実施するクレジット端末である。低額商品のみを扱い、高速処理を必要とする店舗用の端末タイプといえるが、フロアリミットを超える取引等に対する運用対応およびネガリスト用のメモリ増設に伴う端末コストが課題である。

(3) 課題と方向性

ICカード対応クレジット端末について、機能別にタイプ分けをして検討してきたが、この検討のまとめとして、端末の普及という面から現在考えられる課題と今後の方向性を以下に整理する。

端末の操作性

現在行われている店舗での支払現場では、クレジットカードの場合であっても、現金の場合であっても、顧客が端末を操作することはなく、クレジットカードの場合の伝票へのサイン程度である。しかし、ICカード化によって、顧客のPIN入力が必要となり、カード自体も顧客が端末に挿入する運用も起きてくることで、顧客側の混乱が予想できる。また、当然磁気カードとの併用も相当期間必要であり、カード自体をオペレータが挿入するケースとの混在が発生し、オペレータの混乱も予想される。

操作の違いに対する顧客やオペレータへの指導の徹底が必要になってくるとともに、個人認証技術の開発や運用の見直しによって、現在と変わらない支払現場でのオペレーションの実現を目指すことが、普及にとっては必要である。

高速処理の実現

現在利用されているクレジット端末では、通信回線への接続時間を短縮するため、支払の確定を待たず、接続するカード会社が識別できた時点で、ダイアリングを開始する「先行ダイアル」機能を有している。しかし、ICカード化によってオフライン取引も可能となり、オンラインかオフラインかの判定結果がICカードから返答されるまで、ダイアリングを開始できない。そのため、オンラインとなった場合に、現在よりも時間がかかることになってしまう。そこで、端末でのオンライン/オフラインの判定を早い時期に実施し、その結果をもとにダイアリングを開始するといったように、処理速度を念頭に置いた端末機能の見直しが必要である。

また、現在は回線品質を考慮して、1200bpsまたは2400bpsの通信速度の端末がほとんどであるが、店舗の回線状況によって通信速度を選択できたり、ISDN回線を選択できるといったように、端末機能の充実や豊富な端末種別の準備も必要である。

端末のコスト

機能タイプ別での端末の検討でもあるように、端末コストを決定する大きなファクタにデータ認証をどのように実現するかという課題がある。ファームウェアで実現するにしても、暗号用コ・プロセッサを使用するにしても、端末コストへの影響は非常に大きいといえる。暗号用コ・プロセッサを使用する場合は、コ・プロセッサ自体のコストダウンを期待することも考えられるが、データ認証に使用する暗号ロジックの変更も検討されるべきである。小さなサイズのファームウェアで高速に実行でき、十分な強度を持った暗号ロジックを開発していくことも、端末を普及していくには非常に重要な課題である。

磁気カードとの併用

クレジットカードをICカード化するといっても、すべてのクレジットカードを一斉にICカード化することはできず、すぐに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。また、ICカード対応ができていないカード端末を利用する場合、入力されたICカードが読み取れない場合等のために、ICカード上にも磁気ストライプを持たせる必要がある。

磁気ストライプ上の情報によってクレジット取引が実施された場合に、磁気ストライプのみのカードを使用したのか、ICカードが読取れずに磁気ストライプを使用したのか、あるいはICカードでありながら磁気ストライプ情報を直接利用したのかを判別する必要がある。磁気ストライプのみのカードかICカードかの判別についてはカード内の情報で比較的容易である。しかし、ICカードをどのように使用したかの判別は、現状では使用上の制限をつけるか、カードの不正使用を一部許容してしまうかといった運用上の課題が残っている。その対応として、ICカードと磁気ストライプをひとつのリーダユニットで読み取るカード端末が必要であるが、カード端末のコストおよび既存端末の活用上の制限といった課題を解決していかなければならない。

2.6.2.2 電子マネー端末

電子マネーは、クレジットでは困難な少額の支払に利用でき、現金のハンドリングコストや現金の持つリスクを軽減できるシステムとして注目されている。世界各地で多くの実験が進められ、一部実用化にまで至っているものもある。電子マネーが現金に換わる支払手段として認知されていくには、電子マネーのスキーム自体の課題もあるが、リアルでの利用を考えると店舗で電子マネーを利用するための電子マネー端末の普及も重要な課題である。そこで、電子マネー端末の運用上の課題、および端末上でのクレジットや他電子マネーとの共存について検討した。

(1) 電子マネー端末の運用上の課題

電子マネーは顧客や店舗のオペレータにとっても全く新しい支払手段であり、その普及を目指すならば、店舗での現金やクレジット等による支払の運用の中に、混乱なく組み入れられていくことが重要である。電子マネーをどのように現在の店舗の運用に組み込んでいくかといった電子マネー端末の運用上の課題について、次に述べる。

操作上の課題

ICカード対応のクレジット端末でも述べたが、現在行われている店舗での支払現場では、クレジットカードの場合であっても、現金の場合であっても、顧客が端末を操作することはなく、クレジットカードの場合の伝票へのサイン程度である。

しかし、電子マネー端末では、支払金額を確認した上で支払実行の操作を顧客がするものが多く、カード自体も顧客が端末に挿入する運用が主である。そのため、顧客としては今までしたことのない端末の操作を要求されることになり、支払時の混乱が予想できる。また、現在の運用にはないオペレータの顧客への操作指導も必要になる。

操作の違いに対する顧客やオペレータへの指導の徹底が必要になってくるとともに、現在と変わらない支払現場でのオペレーションが実現できるように、電子マネーシステムの改良が普及にとっては必要である。

電子マネー支払結果データの収集

少額の支払に適した電子マネーの特長を生かし、普及を推進していくには、大型店舗、自動販売機等での利用を可能にすることは不可欠である。多くの電子マネーはその支払結果データを電子マネー端末からバッチ処理で決済センターへ送信するシステムである。しかし、通常、大型店舗ではPOS等を使った情報管理を目的とする店舗システムに決済システム自体も含まれており、また、自動販売機も公衆回線を利用できる場所にすべて設置されているとはいえず、逆に多くは公衆回線を利用できない場所に設置されているのが実状である。自動販売機では、PHS等の通信手段を有する機種を利用することも考えられるが、それでも設置場所は制約を受けざるをえない。

支払結果データを決済サーバから送信したり、オフラインで収集できるように、店舗システムや使用する機器の運用に合わせて、支払結果データを収集できるシステム運用を検討していく必要がある。

(2) 複合支払機能への対応

通常、店舗では現金、クレジット、ギフトカード等の複数の支払方法が可能である。そのことから、広く利用される端末としては、電子マネーのみを扱う端末ではなく、複数のカードによる支払が可能な端末が必要になってくる。また、現在実験等が進められている電子マネーも多く存在する。そこで、複数の支払機能を有する端末について検討した。ここでは、クレジットと電子マネー、および複数の電子マネーを扱う端末を中心に、実用に向けての課題を述べることにする。

操作上の課題

現在の電子マネーの運用で複合支払の端末を考えた場合、単独の電子マネー端末でも述べた操作上の課題に対して、クレジットで支払うか電子マネーで支払うか、またはどの電子マネーで支払うかといった選択のための端末操作が、さらに顧客に負わされることになる。また、利用する支払によって、その後の操作も異なることも考えられ、それぞれの操作の理解を顧客に要求することになる。これは、電子マネーは現金に優る利便性を特長としているにも拘わらず、現在の支払現場にない幾つもの端末操作を顧客に求めることになる。

電子マネーの普及のためには、顧客や店舗のオペレータといった利用者の習熟に期待するのではなく、各地で実施されている実験を通して、利用者の立場からの操作性の検討も重要な課題のひとつである。

セキュリティチップの搭載

現在実験等が進められている電子マネーでは、それぞれ固有のセキュリティチップによって、そのセキュリティを実現している。端末上での複数の電子マネーまたはクレジットとの共存のためには、複数のセキュリティチップを搭載する必要があり、4～5個のセキュリティチップの搭載が搭載可能な端末も現実に開発されている。しかし、端末コストの見地から考えると、搭載のためのハードコスト、およびセキュリティチップ自体のコストは無視できない。サービス提供者がセキュリティチップを提供する場合でも、サービス提供者等でのコスト負担は発生する。端末コストを下げていくには、例えば共通の暗号ロジックを使用し、それぞれのサービス

提供者が電子マネーのセキュリティアプリケーションを提供していくようなシステムの検討が必要である。そのためには、共通アプリケーションの実行環境を提供できる端末のソフトウェア構成、不正な攻撃に対する端末の強度等の課題を端末で解決していかなければならない。

通信プロトコル

前述のセキュリティチップの課題と同様に、各電子マネーやクレジットのシステムでは、それぞれ異なる通信プロトコルを使用している。そのため、端末での複数の電子マネー及びクレジットの共存には、それぞれの通信プロトコルをサポートしていく必要がある。端末コストだけでなく、決済センターの構成等も考えると、汎用プロトコルでの通信プロトコルの共通化が必要である。

2.6.2.3 POSシステムとの連携

店舗でのI Cカードによるクレジット及び電子マネーの利用を普及させるためには、大型店での利用を押し進めなければいけない。そのためには、店舗の情報管理の基幹機器であるPOSでこれらの支払をどのように実現していくかが重要な課題である。ここでは、POS自体でこれらの支払をすべて実現する場合ではなく、前述のクレジット端末や電子マネー端末をPOSに接続し、連携して支払を実現する場合の課題と、業態別のシステム構成例について述べる。

(1) POS連携での課題

今まで述べてきたカード端末をPOSと連携して、クレジットや電子マネーの支払を実現していくには、まず、現行のPOSシステムでのクレジット処理、および現在運用されているG - C A T等のクレジット端末との連携から、予想される課題を洗い出していく必要がある。次に、POSとの連携によって導入を推進していく上での課題について述べる。

POSシステムとの整合性

業態、店舗規模等によって、運用されているPOSシステムは異なっている。ストアサーバ - POS間、POS - POS間等の接続方式や、本部サーバとの通信方式だけでも多種多様である。カード端末についても、これらのPOSシステムとの整合を取れるように、単に公衆網だけでなく、I S D N網、P H S網、L A N、無線L A N等への接続が可能な端末の整備が必要である。

また、POSとの接続も、R S - 2 3 2 Cでのシリアル接続だけでなく、I r d A接続等も含めた、各種の接続形態への端末の対応も検討していく必要がある。

POSと端末での操作

クレジット端末および電子マネー端末の課題でも述べているように、現在実験等が進められているI Cカードによるクレジットや電子マネーでの支払時には、P I N入力や支払の確定操作のために、顧客操作が必要である。例えば、百貨店のよう接客販売が主で、POSの設置場所と接客場所が離れている場合に、どのような方法で、どのタイミングで顧客に操作してもらうかといった顧客操作に関する課題は、各業態ごとに種々考えられる。各業態毎に異なる支払業務の流れに対して、POSと端末でどのような操作や機能の分担が最適であるか、実験等を通して積極的

に検討していく必要がある。

POS 接続仕様

現在運用されているクレジット端末とPOSとの接続仕様は、端末メーカー毎の個別仕様であり、またPOSメーカー毎にも相違があることもある。このように、カード端末毎、POSごとの接続仕様であると、各店舗の導入コストを引き上げるばかりである。POSと連携して利用するカード端末を普及させていくためには、共通POS接続仕様の整備が必要である。尚、磁気クレジットカードに対応したものであるが、現在、「OLE POS技術協議会」において、POS - クレジット端末間の接続仕様の検討が進められている。

(2) 業態による連携方式例

同じ業態であっても、店舗のPOSシステムの形態や店舗規模等によってその連携方式は異なるが、ひとつの参考例として、ここでは業態別にPOSとカード端末の連携方式の幾つかの例について述べる。

百貨店

図 2-6は、百貨店や一部の専門店のよう、接客場所とPOSの設置場所が離れている場合の連携例である。

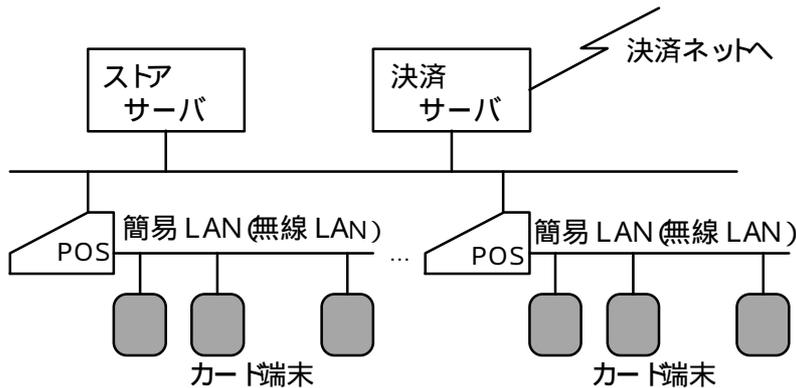


図 2-6 連携方式例(1)

大型スーパー

図 2-7は、大型スーパー、スーパー、量販店等のようにカウンタにPOSが設置されている場合の連携方式例である。

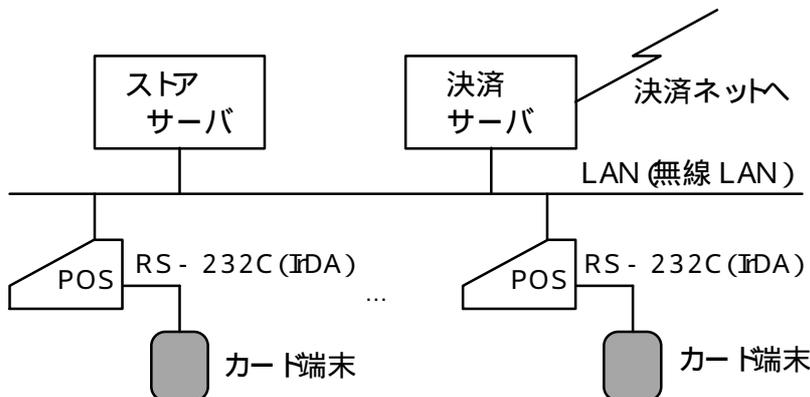


図 2-7 連携方式例(2)

例に示した連携方式だけでなく、ショッピングセンターのようにテナントが自社のPOSを持込んでいるため、POSではなく入力端末がデベロッパーの店舗システムに接続している場合や、専門店のように店舗にPOSが独立して置かれISDN等で本部サーバと接続をしている場合等といった店舗システムの運用形態によって、多くの連携方式が考えられる。

2.6.3 電子マネー用機器

電子マネーを取り扱うシステムに使用する機器の内、特に電子マネーをICカードにローディングする機器が必要となる。以下にはこれらの電子マネーをローディングする場合の端末の要件の検討内容を記す。

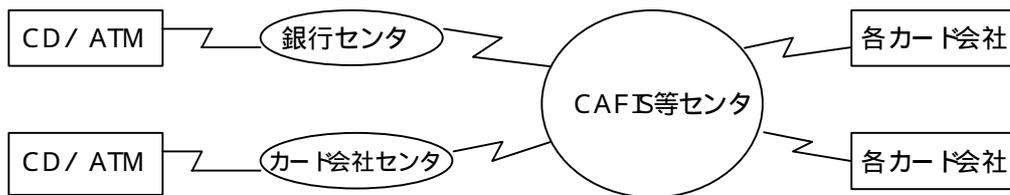
2.6.3.1 CD / ATM

CD / ATMは現金をハンドリングする顧客操作型端末として、広く一般的に使用されているが、電子マネーが使用されるようになった場合に、どのような要件が必要となるかについて検討した。

(1) システム構成概要

CD / ATMを使用する場合の一般的なシステム構成図を図 2-8に示す。現在日本のATM / CDネットワークはCAFIS等センタを介して、全国的なネットワークができています。

電子マネー等の決済に関しても、現在のこのインフラストラクチャーを使いつつ新規の電子マネーシステムを構築していくことになると考えられる。下記CAFIS等センタには、GPN(Visa系)、JCN(JCB系)、JNS(MasterCard系)等を含む。



CD : キャッシュディスペンサ

ATM : オートテラマシ

図 2-8 CD / ATMシステム構成図概要

(2) 端末要件

a) 機能要件

現在のATMは、銀行店舗の合理化のため、かつて窓口で行っていた業務をできるだけATMで行えるよう多くの機能を備えている。現金の預け入れ / 引き出しはもちろんのこと、口座振り替え / 振り込み、通帳記入も可能である。口座振り込みには、振り込みカードが使われる場合も有る。

ECの時代になっても、当面は現金(紙幣+硬貨)はなくなることはないし、それ

に付随する通帳等も使われると想像されるので、CD / ATMの機能としては、現状の機能に加えて、電子マネーの新しい機能が追加されることになると考えられる。

また、現金の扱いはやめて、電子マネーのみのロードを専用に行うようにした端末も考えられている。神戸のSCJの実証実験ではこのような専用ローディング端末が実際に使用されている。

ただし本稿においては、現状のCD / ATMに上位ホストからICカードに電子マネーをローディングする機能について考察する。

電子マネーの名称を仮に EcomCash として、図 2-9にクレジットカードを使用してローディングする場合の概要を示す。

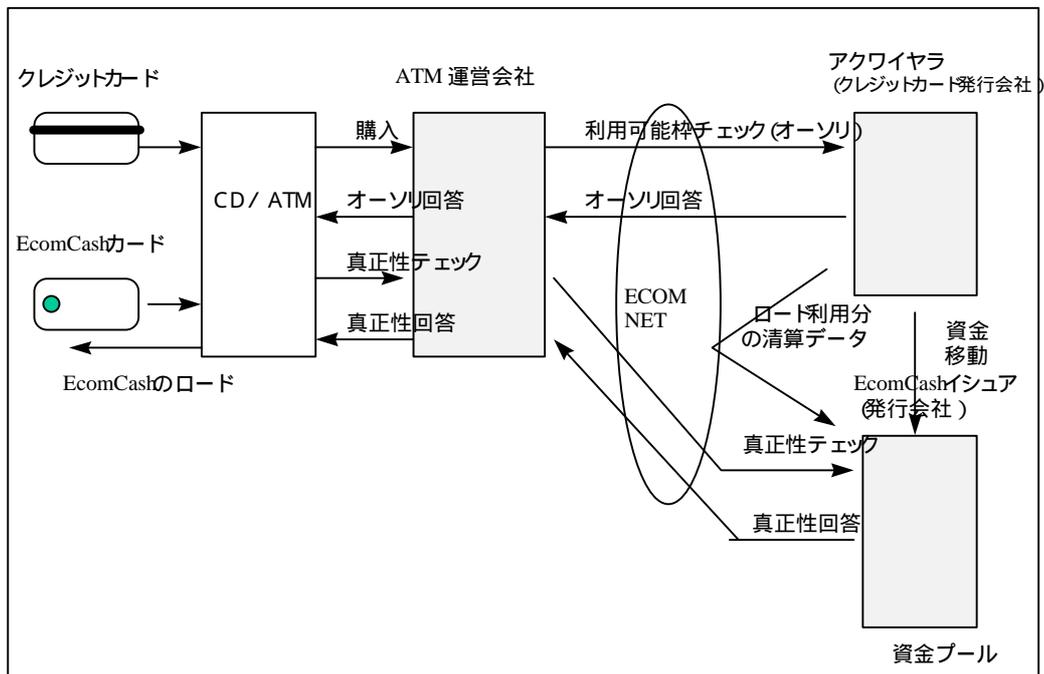


図 2-9 クレジットカードによる電子マネーリロード機能の概要

CD / ATMに挿入されたクレジットカードにより、アクワイヤラに利用可能枠のオーソリをかける。

アクワイヤラは利用可能枠のチェックを行いその結果をATM運営会社を経由してCD / ATMへ返す。これがOKならば次へ移る

次にリロードを行うためのEcomCashカードの真正性をEcomCashイシューアに対してチェックする。

EcomCashイシューアはEcomCashカードの真正性をチェックの後、アクワイヤラを経由してCD / ATMにチェック結果の回答を返す。チェック結果がOKであれば、同時にEcomCashの入金指示がCD / ATMへ通知され、EcomCashカードへロード金額が入金される。

一方、ファンドイシューアからEcomCashイシューアに対しては、ロード利用分の清算データが送信されるとともに、資金の移動が行われる。EcomCashイシューアは、カードへローディングされたEcomCashの店舗等での使用に備えて、

資金をプールしておく。

以上はクレジットカードにより、EcomCashの入金の例を示したが、次に銀行カードを使って、自分の預金口座から預金を引き落として、リロードする場合について参考事例を図 2-10に説明する。

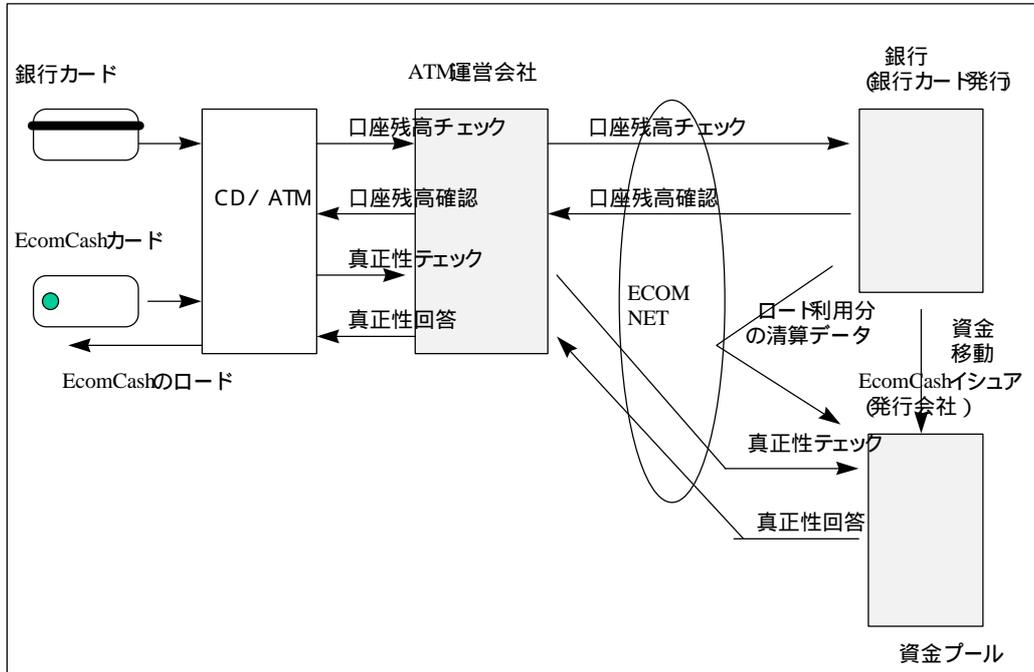


図 2-10 銀行カードによる電子マネーリロード機能の概要

CD / ATMに挿入された銀行カードにより、対象銀行にたいして、自分の預金口座の預金からリロードするための確認チェック要求を行う。この場合はカードホルダの暗証番号の確認も同時に行う。また暗証番号は暗号化されて授受される。

銀行は銀行口座の預金額のチェックを行いその結果をATM運営会社を経由してCD / ATMへ返す。これがOKならば次へ移る

次にリロードを行うためのEcomCashカードの真正性をEcomCashイシューに対してチェックする。

EcomCashイシューはEcomCashカードの真正性をチェックの後、アクワイヤを経由してCD / ATMにチェック結果の回答を返す。チェック結果がOKであれば、同時にEcomCashの入金指示がCD / ATMへ通知され、EcomCashカードへロード金額が入金される。

一方、銀行からEcomCashイシューに対しては、ロード利用分の清算データが送信されるとともに、資金の移動が行われる。EcomCashイシューは、カードへローディングされたEcomCashの店舗等での使用に備えて、資金をプールしておく。以上のような形で電子マネーのリロードが行われる。

また、電子マネーを扱うICカードの種類については、現在、以下の種類が考えられているが、どの種類を使うことになるのかは、サービス提供者が決めることになる。

- ・全銀仕様カード
- ・MasterCard系(Mondex)カード
- ・Visa系Cashカード
- ・スーパーキャッシュ(NTT・日本銀行方式)
- ・郵貯ICカード等

決済型ICカードの仕様に関して、現在業界標準と呼ばれているのはEMV仕様である。

当面のCD/ATMに使われるカードの仕様については、現在の磁気カードはまだ残ると考えられるので、磁気カードをベースにしたシステムに対応した機能をオンラインネットワークとして確立することと、加えて現在のインフラに、EMV仕様ICカードの扱いを追加する形のシステムになると考えられる。

b) 端末構成

i. CD/ATMブロック図概要

CD/ATMの構成についてブロック図概要を図2-11に示す。

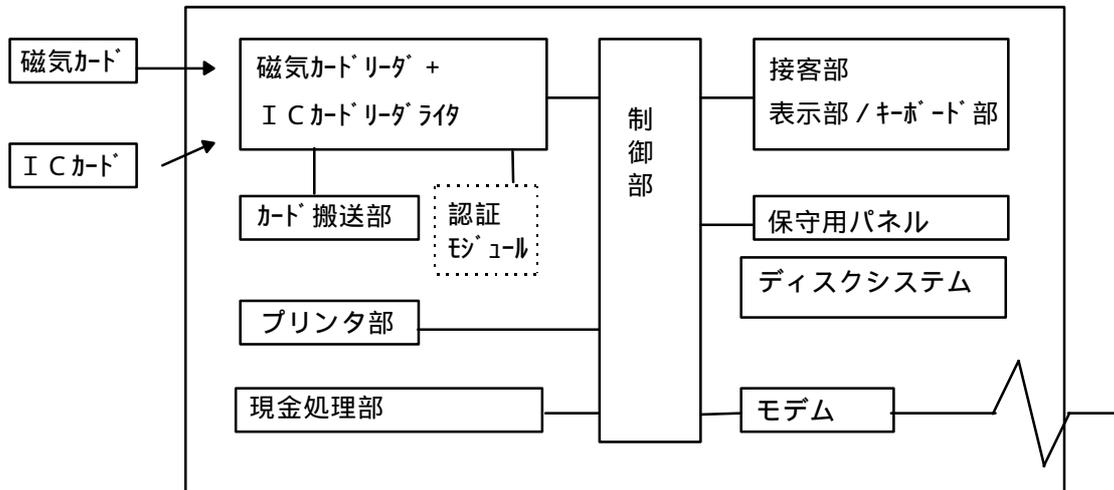


図 2-11 CD/ATMブロック図概要

挿入されたカードが、磁気カードか、ICカードかを判定し、それぞれに対応した処理を行う。

上位ホストと認証を行う場合(オンライン認証)には、認証モジュールは不要となる。

EMV仕様の場合は、セキュリティ仕様についてはオプションになっており、サービス提供者(ICカードイシューア等)が実際にインプリメントする具体仕様を決めることになるので、サービス提供者が決めた実行仕様に従って製品の開発設計を行う必要がある。

カードの挿入口について、磁気カードの挿入口とICカードの挿入口と両方持つ必要性があるかないかについては、どちらでも機能的には問題無く処理が行われるので、CD/ATMの設計仕様に任される。1挿入口の場合は、磁気カードを最初に入れて、一旦取り出し、次にICカードを入れることで行える。また2挿入口の場合は、しかるべき挿入口に磁気カードとICカードを同時に

挿入して行えばよい。ただし、挿入口を間違えないようにする等の配慮が必要である。

2.6.3.2 ロード専用端末

電子マネーの専用ロード端末は、前述のCD/A T Mに対して現金処理部分を除いた形態になると考えられる。

ロード専用端末についても用途、機能によって各種の形態が考えられている。また今後の市場動向により、各種の端末が開発されていく事が想像される。ロード端末の設置場所により、以下の場合の用途に分類されると考えられる。

(1) 無人コーナ型

銀行のCD/A T Mコーナのようなところに設置する自立型で、カード会員が誰でも利用できるように設置し利用する形態。この場合のセキュリティについて、一般の人々が自由に入退出することを考慮して設定する必要がある。また不正使用に関する防御や故障時の対処等について考慮しておく必要がある。

システム構成は、前記CD/A T Mにて示した形態が基本構成となる。

(2) オフィス設置型

個人事業者のオフィス等に設置するタイプで、卓上型の形態が想定される。利用は一般カード会員ではなく、そのオフィス等のカード会員のみが使用できるように設置する形態が考えられる。この場合は、オフィスが一つのセキュリティ空間として設定されるので、無人コーナの自立型タイプに比較して物理的なセキュリティは軽減されると考えられる。本形態では、磁気ストライプのカード(クレジット/銀行カード)での取り扱いは、しない形態になるかもしれない。(ICチップ付きカードのみ)

(3) 家庭設置型

利用形態としては一般家庭に設置しカード会員が自宅で電話回線を介して自分のカードに電子マネーをロードすることができるようにした端末で、扱うカードはICチップ付きカードのみ扱う単機能の端末になると考えられる。

この場合は、単に電子マネーをロードする機能があれば良いが、上位ホストとカードの真正確認や本人確認等基本的なセキュリティを具備することが必須条件となる。

また、電子マネーの普及にとっての一つの課題である、電子マネーを利用したい場合に、利用する前にロードするだけの為にどこかへ(ロード端末の設置場所へ)行かなくてはならないというのは、利用者側から見た場合あまり歓迎されるものではないと考える。自宅にて好きな時間(従って発行者センター若しくは銀行は、24時間の対応が必要となる)にロードできる本端末の開発普及が必要と考える。

2.7 端末インフラストラクチャー整備アクションプラン

記述の通り端末インフラストラクチャーの構築は、ICカードの実用化・普及に向けて不可欠である。本章ではその具体的な実現策に関する提言を行なう。

2.7.1 インフラストラクチャー整備促進の為に要件

端末インフラストラクチャー整備の具体的な解決策の一つは、複数の発行者が共同で共

用端末を設置し、相互開放することである。

この前提のもとに現状を見渡すと、各種電子マネーの実験においては、大半が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。

他方決済分野におけるICカード適用において、その実現可能なプレイヤーの内の一つとして考えられるクレジットカード業界を例にとると、現在既に磁気カードベースでオーソライズーション端末の共同利用システムを1983年に構築し、現在では銀行系/信販系/流通系及び日専連/日商連傘下等のクレジットカード企業約200社が参画し、設置台数50万台超の端末を共同設置・共同利用するという参照すべきモデルが実存し、ICカードへの切替え期間中における磁気カードとの併用期間での両者の整合の考慮の必要性も勘案して、今後のICカードの一般化と普及には、これら既存インフラの活用も視野に入れた、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こそが、普及促進の上から重要な課題と考え、このCAT共同利用システムをベースとした、具体的な普及促進案策定の指針として以下の通りアクションプランの提言を試みるものである。ICカード受け入れの為の端末インフラストラクチャーの整備促進には、端末は加盟店に容易に受け入れてもらえるものであることが大前提である。そのためには端末のハードウェアおよびソフトウェア面からの共通要件の整備と、それらをベースにして運用面を支えていく統一的な推進母体並びに運用に関する様々な取決めが必要である。本章では先ず、推進母体を中核とする組織・体制において検討すべき端末の要件について記述する。(2.6節と併せて検討を要す)

2.7.1.1 端末の要件

(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、導入コストと新しい端末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。

既存端末へのICカード・リーダライタの追加

クレジットカードがICカード化されれば、まず現在端末が設置されている場所でのICカードの取り扱いがまず考えられる。設置コストをより少なく、且つ、早期導入を図ろうとするならば、既存のインフラ(端末やシステム、ネットワーク)をできるだけ利用できることが望まれる。勿論既存の端末を使うのが効率的か、新たに入れ替えた方が良いのかは、それぞれの端末やシステムの現有機能が大きく影響するところであろう。より効率的に既存端末を利用できる方法を、メーカー、カード発行会社を中心となって研究していくことが急務と思われる。

新端末

ICカード取り扱い用端末として新たに開発される端末には、端末の仕様要件の項で述べたように磁気ストライプのみのカードの取り扱いも考慮して磁気ストライプリーダを備えたものとする必要がある。また、通常のクレジット処理では売上票のプリントアウト機能も必要となる。

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) 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。

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毎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る。

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。

クレジット処理における端末メッセージはCATの標準仕様としてほぼ共通化されており、それを踏襲していく形になると考える。

電子マネー等についても、商品スキームは様々であろうが用語の統一や端末メッセージの共通化を図って行くべきである。

2.7.1.2 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ためには、次のような課題がある。

(1) 堅確な運用

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。

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。

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と思われる。

(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。

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。

そのためには、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。

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。

2.7.1.3 端末管理

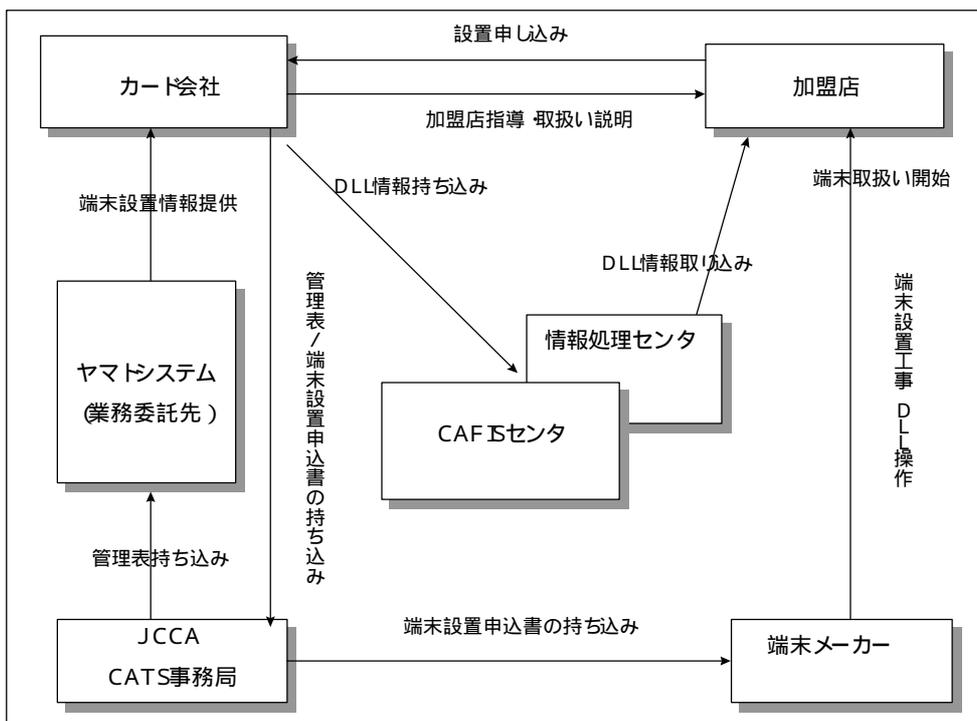


図 2-12 C A T 共同利用システムにおける端末共同管理機構図

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始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、現在 J C C A が中心になって運営している共同端末管理システム(図 2-12)にのせるか、それに準じた運用するのが効率的と考える。

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、I C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、J C C A との調整も考慮していくことが出てくると思われる。

2.7.2 端末管理機構の構築

I Cカード用端末の設置促進を図り、早期にI Cカード受け入れのための社会インフラを整備するためには、その推進母体となる機構が必要とされる。ここでもC A T共同利用システムを参照して、組織・体制の役割について述べる。

2.7.2.1 機構の目的

I Cカード利用促進を目的に、I Cカードがより広範囲に利用できるための端末設置を効率的に促進することを主たる目的とする。(インフラ整備促進)

効率的な設置のためには、端末の相互解放を前提とすることが不可欠であり、そのために必要な端末仕様や運用規則の策定が必要になる。(共通仕様、運用規則の策定)

また、端末設置情報を加盟カード会社に効率的に知らせ、遅滞なく各社のカードを利用できるようにするには、端末情報を集中管理し設置情報を集配するシステムが必要になる。(端末設置情報の集中管理)

こうした事業を展開していく中では様々な利害や軋轢が生じる得る。それら設置に関わる諸問題を集約し、共通する問題について共同で解決策を検討し、利害の調整を図っていくこともこの機構が果たすべき重要な責務であろう。(利害の調整)

2.7.2.2 機構の組成

I Cカード用端末の適用業務は、クレジット業務はもとより電子マネーやポイント管理等従来のC A T端末よりも幅広いことから参加メンバの範囲も広がる。組織としては、それら参加メンバが各々の役割に応じて運営に参加できる組織であることが必要であり、そのためにはそれら参加メンバの業界の代表による上部機関の組成が望まれる。

2.7.2.3 参加メンバ

I Cカードによるクレジット機能、電子マネー機能を提供するカード発行会社が参加することを原則とする。

また、システム全体が円滑に機能するよう、端末メーカー、情報処理センタ等もオブザー

バとして参加することが望ましい。

2.7.2.4 運用

CATの例をみても、こうした事業を継続的に進めていくにはそれなりのノウハウとカードシステムと端末に関する専門的な知識が必要であり、且つ、それらを有効に機能させる組織力が求められる。その為には実務を担当する事務方と運営を司る組織が必要であり、特に事務方については前述したようなノウハウと専門知識が要求されることから専任体制が望まれる。

2.7.3 端末共同利用のための諸ルール

2.7.3.1 相互解放ルール

端末の相互解放のための共通要件については標準仕様として定め、共同端末の必須要件とするが、それ以外の部分についてはオプションまたは自由とする。

クレジット機能のようにすでに標準仕様が定められている機能については、それをベースにした仕様であることが必要である。

標準仕様を定める以上、それに合致しているかの審査と認定が必要になってくる。

認定は技術的な側面が強いことから、情報処理センター等の専門機関が代行する形が現実的であろう。

2.7.3.2 設置ルール

G-CATをはじめとするクレジット業務処理端末（以下CAT）が、すでにかかなりの範囲に設置されている現状では、ICカード処理機能のついた端末を設置しようとした場合、加盟店にはすでにCATが設置されているケースが多いと思われる。

原則として、置換えの場合は処理レベル等の向上（最低でも既存の機能を損なうことがないということ）が前提であるが、そうした加盟店への置換え設置の場合、既設置端末の設置会社の資産の問題にも関係してくる問題であるため、そのルールの策定には十分な議論と合意が必要である。

単に機能の優劣で押し通せない事柄であるという認識を持って対処すべき問題であろう。しかし、同時にそれは技術の進歩に伴う新製品の進出を拒むものであってはならないということも重要である。より高機能で使いやすい端末を普及させることは、加盟店サービス、会員サービスの上からカード会社にとって大きな責務である。

2.7.3.3 費用負担ルール

加盟店においてカードが使われたとき（端末を使って）、当該カードの発行会社は端末設置会社に対して相応の端末利用料を支払うこととする。これにより端末設置会社の費用負担が多少なりとも軽減でき、かつ、端末設置のインセンティブにもなる。

利用料をいくらにし、いつまで負担するかは非常にデリケートな課題であり、既存のルールへの影響を考慮しながら十分な議論とコンセンサスが必要な事項である。

端末利用会社および設置会社間での利用料の精算のためのシステムが必要となるが、既

存のC A Tにおける利用料精算システムをベースに準拠することで対応可能である。

3 非接触ICカード利用ガイドライン

現在は磁気カードが普及しているが、磁気カード単体でのセキュリティは弱いので、システム全体でセキュリティ面を確保しない限り、磁気カードはICカードに置き換えられるであろう。また、磁気カードが普及していない分野においては、高いセキュリティが要求される利用分野において、ICカードが検討されるであろう。

ICカードの普及には、広範囲で多種多様な利用拠点に、リーダー・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となり、検討が進んでいる接触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ICカードの特長が生かせる分野では、非接触ICカードの利用を検討することになる。

磁気カードから接触ICカードを経由して、非接触ICカードに移行していくという考え方よりも、接点がないため摩耗による信頼性の低下がなく、駆動部がないためリーダー・ライタの保守が大幅に軽減でき、財布から取り出さなくても、かざすだけで処理出来る操作性のよさ、利便性が高いことを考慮すれば、利用分野によっては磁気カードから一気に非接触ICカードへ移行する可能性がある。

本資料作成の狙い

WG7（ICカードWG）SWG2（非接触ICカード検討グループ）では、ICカードを活用した様々なシステム、特に『非接触ICカード』を利用したシステム開発・導入検討の参考に供するため、ガイドラインとして本資料をまとめる。

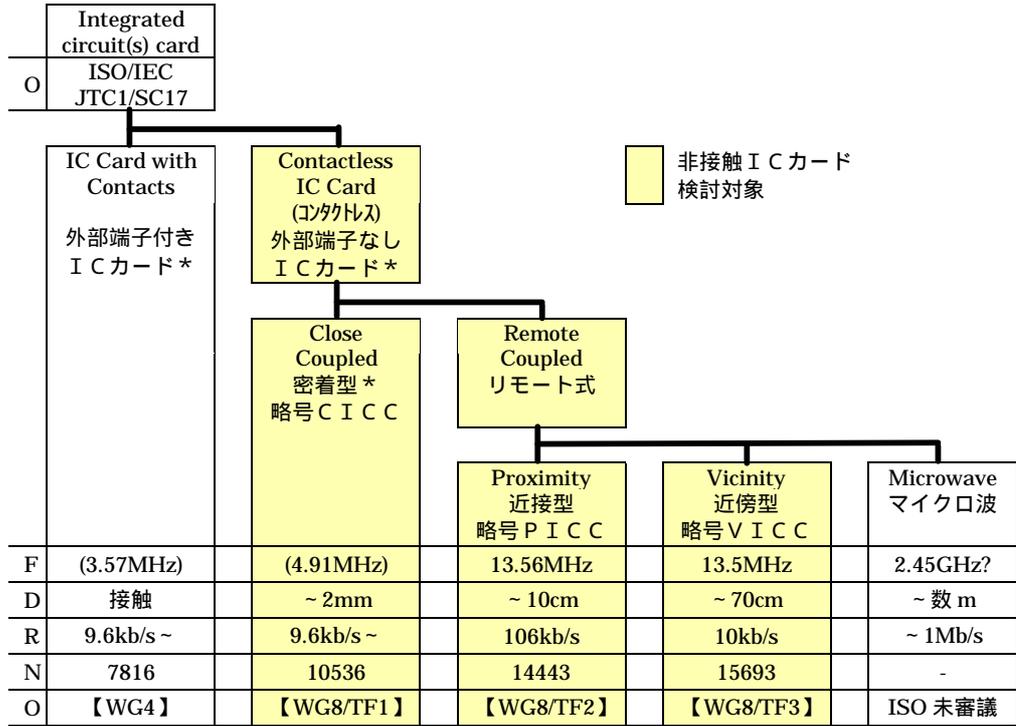
資料の内容

利用者にとって利便性が高く、導入者にとっても運営・保守が簡単な「次世代のICカード」と言われる『非接触ICカード』を対象とし、非接触ICカードの有効性、技術開発の現状、標準化の動向、普及の見通し、普及課題と解決策、利用可能なアプリケーション分野、適性等々、『非接触ICカード』の一般的な知識を紹介する。

3.1 非接触ICカードの位置付け

3.1.1 ICカードの分類

認識 (ID) カード及び関連機器に関する国際標準化委員会 (ISO/IEC JTC 1 / SC 17 Identification Cards and Related Devices) で位置づけられているICカードの分類を整理した。



O : 【ISO 審議組織】 F : 周波数 (クロック) D : 通信距離 R : データ速度 N : ISO / IEC 標準化番号
JTC:Joint Technical Committee SC:Sub Committee WG:Working Group TF:Task Force

* :JIS で使用。他の用語は今後見直しがあり得る。(9 8 年 2 月までの内容を反映)

図 3-1 ISO規格上でのICカードの分類

表 3-1 非接触 I Cカードの分類表

分 類	Contactless integrated circuit(s) card 非接触 I Cカード (コンタクトレス I Cカード)				
種 類	(Close coupled) - CICC 密着型		(Remote Coupled) 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	I S O未審議
通信結合方式	(Capacitive Coupling) 静電結合方式	(Inductive Coupling) 電磁誘導方式			(radio frequency) 電波方式
伝 送 距 離	~ 1mm	~ 2mm	~ 約 10cm	~ 約 70cm	~ 数 m (電池有)
電 池 有 無	無	無	無	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)	13.56MHz (短波)	2.45GHz (マイクロ波)
通 信 速 度	9.6kb/s ~	9.6kb/s ~	106kb/s ~	~ 10kb/s	~ 1Mb/s
C P U 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	54mm × 85.6mm
カードの厚さ	0.76mm ± 10%	0.76mm ± 10%	0.76mm ± 10%	0.76mm ± 10%	0.76mm 以上可

本分類表は、各社製品仕様を統一的に分類作成するため、I S O基準に基づいてE C O M (S W G 2) で作成した。

今後の各社製品紹介は、本資料の区分を基に作成することを希望する。

3.2 非接触ICカードの利点

接触ICカードに比べ、非接触ICカードが有する利点は表 3-2に示す通りである。

表 3-2 非接触ICカードの利点

利 点	内 容
安価な インフラ費用	非接触ICカードのリーダ・ライタには、カード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が製作可能で、保守費用の削減が期待できる。
長い使用期間	非接触ICカードは、化学的な損傷、湿度や摩耗などに強いので、接触ICカードに比べ、長期に使用可能であり経費節減になる。
不正侵入が 困難	接点端子を露出させていないため、不正侵入によるセキュリティ保護がしやすい。
カード全面の 活用	非接触ICカードの場合、表面に接続端子がないため、カード全面をデザインに活用できる。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。
耐環境性	恒常的に振動、塵や埃などのような悪環境下では、精緻な位置合わせが必要な接触ICカードでの運用は困難である。この様な悪環境下での運用にも強い非接触ICカードは、操作が容易なため、多様な環境下でも使用可能であり、適用業務の選択幅が広がる。

3.2.1 推奨される非接触ICカード

カードの種類、市場の要件、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 3-4)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できるガイドラインとして策定している。

『各種カードの特長』一覧表(表 3-3)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 3-5)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ICカード検討WG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する必要がある。

表 3-3 各カードの特長

: より適している / : 適している

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	~ 10cm	~ 70cm 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 3-4 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 / x:制限あり

市場	推奨カード	非接触ICカード			接触ICカード	磁気カード
		ISO/IEC 10536 密着型	ISO/IEC 14443 (近接型)	ISO/IEC 15693 (近傍型)	ISO/IEC 7816	ISO/IEC 7811
交通分野						
	乗車券、定期券(電車、バス、飛行機、船等)	x		x	x	
	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			x		
	クレジットカード			x		
	電子財布			x		x
	プリペイドカード			x		
	ポイントカード			x		
	自販機カード			x		
	駐車場カード					
通信分野						
	公衆電話用カード			x		
	移動体通信用カード			x		x
	ネットワークキーカード			x		x
	衛星放送用カード			x		x
アミューズメント分野						
	入園チケット(テーマパーク等)	x			x	
	パチンコカード			x		x
	スキー場のリフトカード	x			x	x
	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)	x			x	x
	公営ギャンブルカード			x		
ID分野						
	社員証					
	学生証					
物流・FA分野						
	宅配荷物管理カード					x
セキュリティ分野						
	電子キー			x		

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 3-5 民間市場の各分野に於ける要件の重要度

[要件の重要度 : > > > ×]

市場	要件	決済機能 が必要	カードの 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	電磁ノイズ
交通分野											
	乗車券、定期券(電車、バス、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	×									

3.3 非接触ICカードのアプリケーション分野とその市場規模

インフラのデジタル化が急速に進むなか、ICカードがより身近な存在となってきた。従来の金融の他に交通や通信分野、あるいはこれらを複合しようとするサービスも具体化しつつある。こうしたなかで、非接触ICカードが注目されている。

非接触ICカードの特長は、カード自体に機械的接点をもたないため、静電気によるIC破壊がおこりにくい。またICチップへの直接的な接続が不可能なため、内容解析が困難で偽造し難い。さらに油膜ゴミ等による接点劣化がない等、高度な信頼性および耐久性がある。優れた利便性も特長のひとつである。

これらの特性を生かせる市場として交通分野、通信分野、IDカード分野、物流・FA分野が予測できる(表 3-6)。特に電子乗車券や定期券による自動改札システムはインフ

表 3-6 民間市場におけるICカードの市場規模推移予測

市場	対象	1997年数量(万枚)			2000年数量(万枚)			2003年数量(万枚)		
		合計	接触	非接触	合計	接触	非接触	合計	接触	非接触
交通	高速道路	0	0	0	100	100	0	400	400	0
	鉄道・地下鉄	10	0	10	800	0	800	4,000	0	4,000
	バス	0	0	0	300	0	300	600	0	600
	小計	10	0	10	1,200	100	1,100	5,000	400	4,600
金融・流通	キャッシュカード	0	0	0	500	500	0	1,200	1,200	0
	クレジットカード	0	0	0	350	350	0	1,800	1,800	0
サービス	量販店・専門店	10	8	2	300	150	150	500	250	250
	商店街・ショッピングセンター	5	3	2	200	100	100	300	150	150
	自動販売機	0	0	0	100	50	50	400	120	280
	SS	200	200	0	500	250	250	1,000	300	700
	自動車メーカー	20	20	0	500	250	250	500	150	350
	小計	235	231	4	2,450	1,650	800	5,700	3,970	1,730
通信	テレホンカード	200	200	0	4,700	500	4,200	11,500	1,000	10,500
	携帯・自動車電話	50	50	0	1,000	1,000	0	3,000	3,000	0
	PHS	0	0	0	500	500	0	1,500	1,500	0
	衛星放送	0	0	0	500	250	250	500	250	250
	PCネットワーク	0	0	0	200	100	100	500	250	250
	小計	250	250	0	6,900	2,350	4,550	17,000	6,000	11,000
アミューズメント	スポーツレジャー	20	6	14	100	20	80	400	40	360
	会員カード	20	14	6	500	150	350	500	50	450
	ゲーム・アミューズメント	3	2	1	500	250	250	1,000	300	700
	パチンコ	0	0	0	0	0	0	2,000	0	2,000
	小計	43	22	21	1,100	420	680	3,900	390	3,510
ID	企業・団体内	30	15	15	100	40	60	300	60	240
	教育	5	3	2	100	50	50	500	250	250
	建設	3	2	1	100	50	50	50	25	25
	小計	38	20	18	300	140	160	850	335	515
物流・FA		0	0	0	400	0	400	700	0	700
	小計	0	0	0	400	0	400	700	0	700
セキュリティ	ビル内セキュリティエリア	3	1	2	10	5	5	20	4	16
	小計	3	1	2	10	5	5	20	4	16
合計		579	524	55	12,360	4,665	7,695	33,170	11,099	22,071

注：上記予測は、非接触ICカード検討WG内にて議論して作成した数字である。

ラに関わるため、非接触ICカードは社会的に大きな影響力を及ぼす。一方でNTTのテレホンカードが実用化に向けて動き始めていることもあり、非接触ICカードの利用数と用途はますます増大していくと予想できる。テナントサービス(IDカードによる身分証、入退出等)と食堂・売店、自販機のキャッシュレス化や電子決済という電子マネーサービスが特定の地域で具現化され、金融分野での活用も試行される可能性がある。

接触ICカードのインフラを考慮して、複合型と言われる統合カードや、コンビネーション・カードも現段階で検討されているが、長期的に見ればこれらのカードは非接触マーケットが大きくなるにつれて、相対的に利用機会が減っていくのではないかと予測もある。

3.3.1 ICカードの市場と適性

図3-2は、接触・非接触の2種類のICカードをプラットフォームとして見た場合、各々の市場に対して、現時点でいずれがより適性を持つかをイメージで表わした図である。注1に示したように、市場によっては両機能を1枚のカードに合わせ持つ複合カードも選択肢となりうる。但し、サービスの多様化により将来的には、適性が変化することも考えられる。

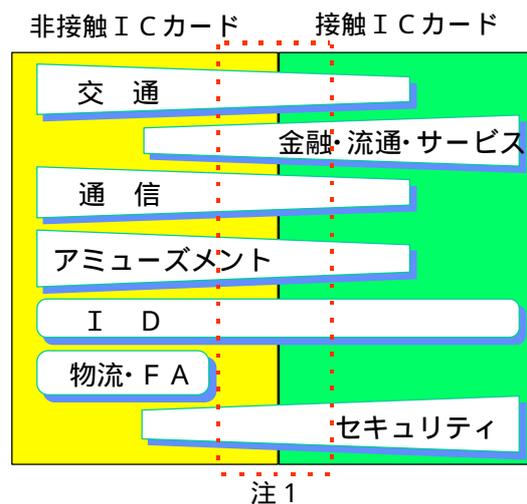


図3-2 ICカードの種類と適性

注1：接触・非接触の両機能を有する複合カードの採用もありうる。

3.4 非接触ICカードの標準化

3.4.1 国際標準で分類される非接触ICカードの種類

ISO/IEC JTC1/SC17/WG8 では現在3種類の非接触ICカードを標準化している。

- (1)密着型 (Close Coupled) 略語 C I C C ISO/IEC 10536
- (2)近接型 (Proximity) 略語 P I C C ISO/IEC 14443
- (3)近傍型 (Vicinity) 略語 V I C C ISO/IEC 15693

3.4.2 カードの特徴

(1) 密着型

1989年より審議開始。密着で動作。挿入式あるいは表面読み取り式カード。コンタクト付きと類似の用途。

(2) 近接型

1994年より審議開始。10cm程の距離で動作。高速、複数カードの衝突防止機能、高セキュリティ機能を持つ。認証あるいは精算用。

(3) 近傍型

1997年より審議開始。70cm程の距離で動作。低コストを特徴。簡易な認識用。IATAのバゲッジタグ等のRFIDタグの用途とカード形状を除けば類似している。IATAにリアゾンとして参加の予定。

3.4.3 国際標準の進捗状況

3.4.3.1 ISO/IEC 10536 密着型 (Close coupled) IC カード関連

(1) ISO/IEC 10536-1 物理的特性(Physical characteristics)

SC17事務局より改訂を指示され、98年2月より改訂を実施していく予定。

(2) ISO/IEC 10536-2 結合領域の寸法と位置(Dimensions and location of coupling areas)

1995年12月に出版された。

(3) ISO/IEC 10536-3 電気信号とリセット手順(Electronic signals and reset procedures)

1996年12月に出版された。

(4) ISO/IEC CD 10536-4 初期応答と伝送プロトコル(Answer to reset and transmission protocols)

1996年、次の 時点までは、DIS化あるいは再CD化を待つこととなった。

内容が関連する ISO/IEC 7816-3 の改訂の目処が立つ時点

T=2 (全二重通信) のフランクフルト大学での実証実験結果が出る時点

は解決されたが、はまだ結果を待たねばならない。次段階への移行は具体化されていない。

(注) CD 10373-4 の試験方法

WG8として、投票コメントに対するDispositionを1997年末までにおこなう。遅れの原因は、静電試験の箇所、現状の案がコンタクトレス・コンタクトに関係無く、実用的では無いとの意見があり、10373-3との共同の検討の必要性があるためである。CD投票のコメントへのdispositionを行い、1998年2月にはFCD投票に進める予定。また、近接型及び近傍型の試験方法については、単独の10373のパートを作成することとなった。

3.4.3.2 ISO/IEC 14443 近接型 (Proximity) IC カード関連

この標準の最初のタイトルは次とする。

“ Identification cards - Contactless integrated circuit(s) cards

- Proximity cards - Part x: xxxxxxxx “

(1) ISO/IEC CD 14443-1 物理的特性 (Physical characteristics)

CD投票が1997年3月15日まで実施され、コメントへのdispositionを完了した。
98年4月にはFCD投票開始の見込み。

(2) ISO/IEC WD 14443-2 電波出力と信号インターフェース (RF power and signal interface)

次回1998年5月までにCD投票開始の見込み。

(3) 後続のパート

パート3 初期化と衝突防止 (Initialization and anticollision)

パート4 伝送プロトコル (Transmission protocols)

の予定である。

(4) ISO/IEC 14443 の標準化の予定

ISO/IEC 14443	WD	CD	FCD	FDIS	IS
-1 Physical characteristics	96-10	96-12	98-04	98-12	99-06
-2 RF power and signal interface	97-10	98-04	98-10	99-04	99-12
-3 Initialization and anticollision	98-10	99-02	99-09	00-04	00-12
-4 Transmission protocols	99-10	00-02	00-09	01-04	01-12

標準化のステップ : WD : Working Draft / CD : Committee Draft / FCD : Final Committee Draft / DIS : Draft International Standard / FDIS : Final Draft International Standard / IS : International Standard

3.4.3.3 ISO/IEC 15693 近傍型 (Vicinity) IC カード関連

この標準の最初のタイトルは次とする。

“ Identification cards - Contactless integrated circuit(s) cards

- Vicinity cards - Part x: xxxxxxxx “

97年度は、一旦決めた“Hands-free card”が却下されたが、今回の“Vicinity card”は承認された。

(1) ISO/IEC CD 15693-1 物理的特性 (Physical characteristics)

CD投票が1998年2月末まで実施され、コメントへのdispositionを完了した。
98年3月には、FCD投票開始の見込み。

(2) 後続のパート

パート2 非接触インターフェースと初期化 (Air interface and initialisation)

パート3 プロトコル (Protocols)

パート4 アプリケーション / 発行者登録 (Registration of application/issuers)

の予定である。

(3) ISO/IEC 15693 標準化の予定

ISO/IEC 15693	WD	CD	FCD	FDIS	IS
-1 Physical characteristics	97-10	97-10	98-03	98-10	99-04
-2 Air interface and initialization	98-09	98-10	99-03	99-10	00-04
-3 Protocols	99-03	99-04	00-09	00-04	00-10
-4 Registration of application/issuers	99-09	99-10	00-03	00-10	01-04

3.4.4 JISの進捗状況

98年には、ISO/IEC 10536, Information technology-Identification cards-Contactless integrated circuit(s) cards を基に、国際規格の技術的内容及び規格票の様式を変更することなく、日本工業規格(JIS)「外部端子なしICカード-密着型-」としてまとまる予定である。

JISの構成では、次の4部で構成される。(名称等の変更はあり得る)

第1部：物理的特性

1. 適用範囲、2. 引用規格、3. 用語の定義、4. 物理特性

第2部：結合領域の寸法及び位置

1. 適用範囲、2. 引用規格、3. 定義、略語及び符号、4. 結合領域の寸法、5. 結合領域の数と位置

第3部：電気信号及びリセット手順

1. 適用範囲、2. 引用規格、3. 用語の定義、略語、及び記号、4. 外部端子なしICカードの操作手順、5. 電力伝達、6. 通信、7. CICCのリセットの条件、8. リセット後の条件

第4部：初期応答と伝送プロトコル

3.5 非接触ICカードの相互運用性

3.5.1 検討の目的と検討項目

非接触ICカードの相互運用性について検討する場合にはいくつかの切り口が考えられ、検討に先立って、何を目的として相互運用性を確保しようとしているかを明確にしておく事が大切である。

相互運用性に関する具体的検討項目は非接触ICカードシステムの導入形態によって決まる要素が多い。予想される主な導入形態と既存システムとの関係、相互運用性の検討項目について表3-7に示す。

表 3-7 非接触ICカードシステムの導入形態と他のアプリケーションとの関係

No	導入形態	既存システムとの関係	相互運用性検討項目
1	単独の新規業務への導入	なし	<ul style="list-style-type: none"> ・カード、R/Wのマルチベンダー間の互換性の確保 ・異なるタイプの非接触複合機能ICカード、複合機能端末の実現
2	既存システムからの移行を伴う新規業務への導入	カードを介した疎結合システム	・既存システムで使用するカードとの複合機能カードの実現
3		端末等を共用する密結合システム	・既存システムで使用する端末との複合機能端末の実現

非接触ICカードシステムを導入する場合、既存の磁気カードシステムや、接触ICカードシステムを単純に置き換えることは考えにくく、何らかの非接触ICカードを必要と

する新規業務があると想定される。

この新規業務システムと既存システムとの関係は、既存システムとはまったく無関係に新規システムを導入する場合と、既存システムからの移行を伴う新規システムの導入の2つに大別される。

前者の場合は、異なった複数のタイプのICカードの機能を1枚のカードに搭載した複合機能ICカード（接触型と近接型の複合型等）の実現という検討項目と、カードやリーダー・ライターを複数のサプライヤーから調達する場合の互換性の確保という検討項目が想定される。

後者の場合には既存システムと新規システムがカードのみを介して緩やかに接続される疎結合方式と、端末などのシステムのある部分を共有する密結合方式が考えられ、既存のカードの機能と非接触ICカード機能の複合した複合機能カードや複合機能端末の実現が検討項目となる。

3.5.2 互換性の確保

カード、リーダーに関する複数のサプライヤー間の互換性は、国際的な標準規格の制定と、これに準ずる製品の採用により確保できると期待したいが、3.4節に述べたように非接触ICカードの標準規格制定作業は接触ICカードに比べ遅れている。

従って、国際規格制定作業完了までの間、互換性を確保するためには、密着型（ISO/IEC 10536）および近接型（ISO/IEC 14443）の範囲の製品を使用するべきであろう。（3.4.3項参照）

また、3.4節に示すように、密着型や近接型においても標準化項目は伝送プロトコル迄（3.4.3項参照）であり、カード内部の論理構造やカードの動作を外部から指示するコマンド等の一部に、標準化されない部分が有るので注意が必要である。

複数のサプライヤから製品を調達する場合の留意点を以下に示す。

互換性を要求するレベルの明確化

通常の読み書きができればよいのか、カード発行システムの互換性が必要か等。

準拠する国際標準規格の確認

標準化項目以外の部分の仕様確認

3.5.3 複合機能カード

3.5.3.1 磁気ストライプとの併用

国内の市場では既存のカードシステムとしては磁気カードを使用するものが圧倒的に多いため、既存システムからの移行性を目的とする複合機能カードは主として磁気ストライプとの併用型とが必要となる。

この場合の検討課題は、非接触ICカードとしての動作によって磁気ストライプに記録されている情報が破壊されないことの保証である。

磁気情報の破壊は非接触ICカード用のリーダーライターによって引き起こされる可能性がある。リーダーライターからICカードに電力を供給し、データの送受信を行うために、リーダーライター側の結合コイル/アンテナに流す電流によって磁界が発生する。この磁界の中

にカードが置かれる時、磁界の強さが磁気ストライプの抗磁力より強くなると磁気情報が破壊される。

磁気ストライプの抗磁力に関しては、日本国内で発行されているJIS規格の磁気カードでは券面の表裏に1本ずつ磁気ストライプが有り、それぞれ抗磁力が異なっているので注意が必要である。

また、非接触ICカードのタイプ別の状況について言えば、結合コイルのサイズが小さく、リーダライタとカードとの距離も短い密着型の場合が最も強い磁界を発生し、他の種類では相対的に弱い磁界となる。

以下に磁気ストライプ併用時の留意事項を列挙する。

- 磁気ストライプの抗磁力の確認
- JIS 1、JIS 2等
- 磁気情報の使用形態
- 読み取り専用 / 読み書き
- リーダライタ側の仕様の確認
- 磁気ストライプ情報破壊の可能性

3.5.3.2 エンボスの可否

現在使用されている磁気カードにはエンボスが施されているものがあるが、これは単にカードの見栄えを良くするだけでなく、インプリントを取ることにより使用されたカードを特定する根拠として利用するためのものである。

従って、エンボスを有するカードシステムからの移行性を考慮すると、複合機能カードにエンボスを施すことが必須となる場合が予想される。

非接触ICカードへのエンボスの可能性については、一般的には機能部品（ICチップや結合コイル/アンテナ等）の配置されていない部分へのエンボスは可能と思われる。この点では、エンボス領域を避けて結合領域を定義している密着型（ISO/IEC10536）はエンボス可能であろう。他のタイプの非接触ICカードではアンテナのサイズや位置は規定されないと思われるので個々に仕様確認が必須であり、エンボス可能領域の制限等があると予想される（図 3-3参照）。

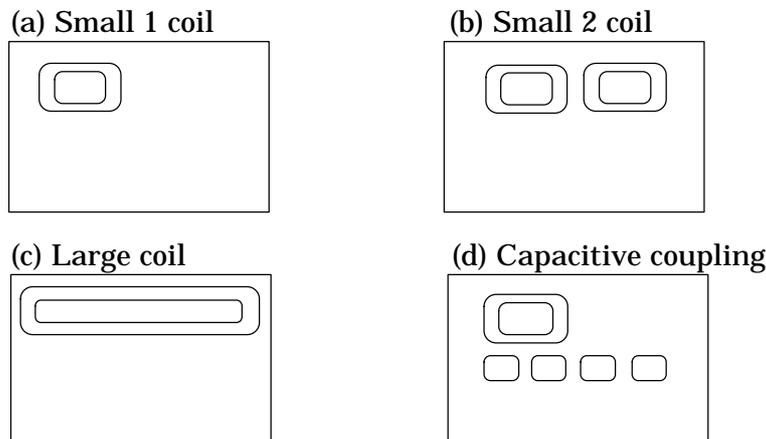


図 3-3 密着型ICカードの結合領域

また、現在使用されているカードの素材はPVCが主流であり、エンボスはPVCのカードに施すのが前提となっている。しかし、PVCは塩化物であるため焼却時に有毒ガスの発生が避けられず、PETや木質系等の代替素材の検討が進んでいる。

これらの代替素材ではエンボスが不可能であったり、既存のエンボス機では対応できず専用機が必要になったりするので注意が必要である。

更に、クレジットカードを複合機能カード化する場合は、機能モジュールとしてICチップ、結合コイル/アンテナの他に磁気ストライプ、サインパネル、ホログラムシートが必要になると思われるが、エンボスを行う際にはこれらの位置関係を配慮することが重要である。

以下にエンボスに関する留意事項を列挙する。

- 既存カードシステムでのエンボス領域の確認
- 複合機能カードの機能モジュールの確認
- 複合機能カードのエンボス可能領域の確認
- 複合機能カードの材質の確認
- 使用可能なエンボス機の確認

3.5.3.3 異なるタイプのICカード間の複合化

ICカードはどのようなタイプでも半導体の回路で構成されているため、原理的には結合領域（接点、結合コイル、アンテナ等）の干渉がない範囲で、全ての組み合わせが可能である。

しかし、表 3-4に示すICカードの適用分野を考慮すると、自ずから必要な組み合わせは決まってくる。

接触、密着型、近接型の3つは、カード使用者がカードを使う意志を示す何らかの動作（カードを差し込む、カードを決められた位置に置く、カードをかざす）を行うことによって初めてカードの読み書きが行われる分野で使用されている。

一方、近傍型やマイクロ波型はカード保持者やカードが貼付されている物を自動的に認識し、情報を読み取る分野で使用されている。

前者は一般的なカードの分野であるが、後者はいわゆる電子タグの分野であり、両者でシステムの性格や使用目的がまったく異なり、カードに記録される情報自体も異なっている。

この二つの群の間での複合化、一体化は技術的に可能であっても運用には疑問が残るため、ここでは、今後、主として必要となると予想される接触、密着型、近接型の3タイプ間での組み合わせの実現見通しと留意点について記す。

複合機能ICカードの構成は、図 3-4の(a)に示すように機能毎にICチップが別れていて同一カード上に搭載され、各々独立して動作するものと、(b)に示すように1つのICチップの中に複数の種類の外部接続回路を持っていてデータは共用されるものが考えられる。

(1) 接触と密着型の複合タイプ

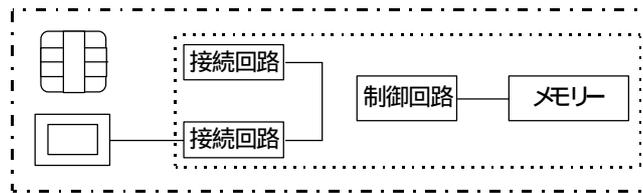
密着型は使い勝手からみると接触型とほぼ同等であり、接触型の接点を無くすことにより耐環境性を向上させたものである。適用分野も接触型に近いことから、接

触と密着型の複合タイプのカードは主として接触から密着型への移行用として使用される。

(a) メモリ独立型複合カード



(b) メモリ共用型複合カード



┌──┐ : ICカード ┌──┐ : ICチップ

図 3-4 複合機能 IC カードの構成

この点では、接触のインフラの普及度が低い日本国内では、このタイプの必要性はあまり高くなり、むしろ、接触のインフラが既に出来上がっているヨーロッパ市場での必要性が高まってくるものと予想される。

カードの構成は、移行用として使用することを考慮すれば、今後市場に供給されるものは (b) のメモリ共用型複合カードが主流となるものと思われる。

具体的なブロック図を図 3-5 に示す。

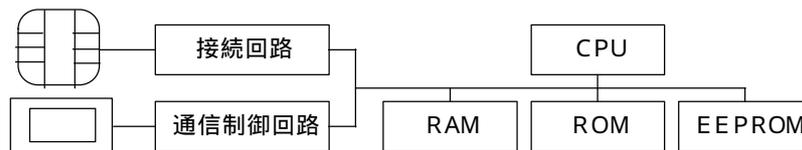


図 3-5 接触・密着型のメモリ共用型複合カード

(2) 接触と近接型の複合タイプ

近接型はその使い勝手の良さから主として鉄道、バス等の交通分野の乗車券・定期券としての用途に広く利用されるものと期待されている。

従って、このタイプの機能カードは、接触中心で考えられているクレジットカードやデビットカード、電子マネー用カードなどの決済系カードで交通機関を利用可能にする場合や、ストアードフェア型乗車券への金額充填の便を図るためにデビットカード機能を持たせる場合に利用される。

この点では、日本国内では決済系カードの IC カード化が見えてきた後に、需要が立ち上がるものと予想される。

このタイプのカードの構成は、当面、図 3-4 (a) のメモリ独立型複合カードが供給されるが、先行きは (b) のメモリ共用型複合カードが中心となるものと予想され

る。具体的なブロック図を図 3-6に示す。

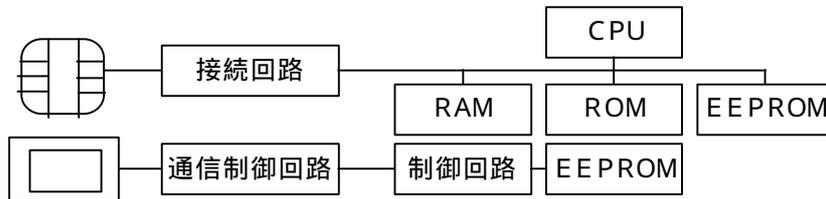
このタイプの複合化を検討する上で特に注意しなければならない点は、利用者側からの視点で考える必要があるという点である。

現在、一般的にはクレジットカード等の決済用カードは財布や専用カード入れで保管し、定期乗車券は別のケースに入れている人が多いが、これは取り出す頻度の差であると同時に管理レベルの違いを示しているものと思われる。紛失時のリスクの大きさにも直結している。

この様に考えると、必ずしもこのタイプの複合機能カードがユーザの利便性の向上に貢献できるとは言い切れない。

カード事業者の便宜のみを考えた複合機能カードの採用はユーザ側に受け入れられないため、十分にユーザ側の意識調査を行うことが必要である。

(a) メモリ独立型複合カード



(b) メモリ共用型複合カード

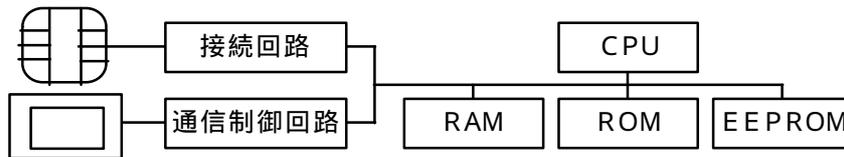


図 3-6 接触・近接型の複合タイプ

(3) 密着型・近接型の複合タイプ

密着型はすでに述べたように接触型の後継として徐々に切り替えられてゆくので、(2) 項と同様の状況と考えればよいが、具体的に製品化される場合は図 3-4 (b) のメモリ共用型複合カードとなると思われる。図 3-7に具体的ブロック図を示す。

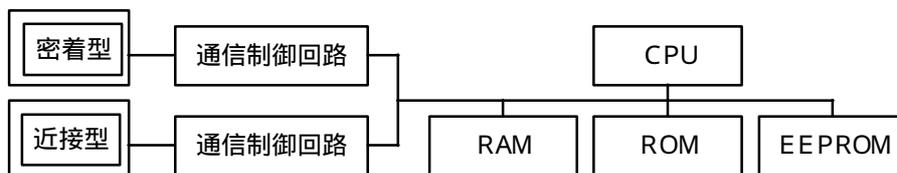


図 3-7 密着型・近接型のメモリ共用型複合カード

(4) 接触型・密着型・近接型の複合タイプ

このタイプは理論的にはあり得るが、必要性には疑問が残る。また、(1) ~ (3) 項の検討結果を組み合わせれば、状況は理解いただけるので記述は省略する。

3.5.4 複合機能端末

複合機能端末の開発は技術的には充分可能であるが、利用者にとっては、利用する機能(磁気ストライプ、接触ICチップの別等)によって挿入場所が異なる等カードの操作

が変わってしまっは非常に使いにくい。

一方、同一操作で利用できるようにすると端末のサイズやコストに影響がでる。

最終的にはシステムの導入コストやメンテナンスコスト等も含めたシステム全体の評価により決定すべきものであるが、端末だけに着目した場合、顧客操作型端末（ATM、情報提供端末等）であるか、従業員操作型（CAT、POS等）であるか区別し、顧客操作型は操作性重視の仕様とし、従業員操作型はサイズやコストを重視した仕様とすべきであろう。

端末の種別は多岐にわたるため、端末メーカーとの十分な打ち合わせ、仕様確認が必要である。

3.6 非接触I Cカードのセキュリティ

非接触I Cカードのセキュリティとしては、

(1) 非接触I Cカード自体に関するセキュリティ

(2) 非接触I Cカードとリーダーライタとのやり取りに関するセキュリティ

を取り扱い、その他のリーダーライタ自身、リーダーライタと上位システムのやり取りに関するセキュリティや、上位システムのみに関連するセキュリティに関しては、ここでは扱わない。

I Cカードのセキュリティが論じられる場合、その要求されるレベルは、そのカードが利用されるアプリケーションの種類及び対象、その中でI Cカードが果たす機能、役割、例えば、カードが決済を扱うか否か、また、決済を扱う場合にも、カードの内部に金額、もしくはそれに類する価値データ、また決済を成立させる鍵情報等を格納しているか否かといったことにより異なる。

高度なセキュリティを搭載する方法として、カードにCPUを搭載し、暗号アルゴリズムをカード内部で計算するための専用のプロセッサを搭載したりする技術上の対応策があるが、それによりカードのコストアップや、処理時間が長くなるといった問題も発生する。

それ故、アプリケーション側から要請されてカードに必要とされるセキュリティのレベルと、カードに搭載される機能の間にバランスが必要となる。

さらに、セキュリティ問題として、I Cカード共通に発生するものと、非接触I Cカード固有に発生する問題がある。非接触I Cカードでは、オープンエアでデータがやり取りされるので、カードホルダに気づかせずにその通信圏に別のリーダを入り込ませて、やり取りのデータを盗むことができなくはない。また、携帯の可能なリーダを持ち、カードホルダに接近することでその許可無しにデータを読み取ることも不可能ではない。そのため、カードとリーダーライタの間に通信されるデータは、容易に解析可能なデータであってはならないことが意識される必要がある。ここでは主に、非接触I Cカードを対象とする。

一方、消費者保護の観点から、カードホルダにとっての安全対策として、カードに記録されたプライバシー情報の保護に関しても配慮する必要があるが、ここでは触れない。

3.6.2 システムセキュリティ上からの分類

システム構築の観点から、カードシステムへの侵害を分類すると表 3-8のようになる。

表 3-8 カードシステムへの侵害

項目	内容	詳細
(1)災害	自然現象による事故	カードおよびリーダライタでの対応は困難 システム全体での対策必要 リーダライタの破損等に対応し、代替設置の体制整備
(2)障害	災害以外のシステム の事故	アプリにより稼働中の保守も要請される システム障害がカード側に影響しない設計必要 ICカードの採用がシステムに対する障害対策の一つ システム障害時にカード側のログの活用も可能
(3)過失	人が起因となる事故	後述
(4)故意	システムへの攻撃	後述
(5)漏洩	プライバシーの侵害	カード情報漏洩は、過失、故意に分けてそれぞれに含める

3.6.3 過失の侵害に対するセキュリティ

非接触ICカードシステムを取り扱う場合に、過失でカードの機能を阻害する例は下記の2点であると思われる。

3.6.3.1 処理の中断

3.6.3.2 カードの物理的損傷

基本的に非接触ICカードに関する操作不慣れが原因と考えられるが、そういった過失により、システム全体に影響することなく、是正が可能なように、ICカード及びシステムのそれぞれにおいて配慮されている必要がある。

3.6.3.1 処理の中断

非接触ICカードでも、密着タイプと、近接型、近傍型等のそれ以外のタイプで条件は異なる。密着型は、アンテナとカードが基本的に正対してセットされることがリードライトを可能とするための要件となるので、一般的にカードをスロットへ挿入するなり、所定の位置へカードをセットすることが必要となる。その場合、カードとリーダライタの間の処理も安定して実施できる可能性が高い。それに対して、近接型等の通信エリアにカードをかざすことで通信を行う場合は、リードライトの処理の途中で、カードが通信エリアを外れてしまう場合や、カードとリーダライタの間に通信を遮断するものが入り込むこともあり得る。

この場合、処理が途中で中断されたカード、及びリーダライタの双方が、それを原因として機能に障害を受けず、再度、通信可能となった時点で、処理を実施できるような仕組みが必要となる。

例えば、データのバックアップ領域を設けることにより、常に以前のデータを保持しておき、いざというときに、以前のデータに復旧させるといったシステムが考えられる。

アプリケーションによっては、その処理をどの段階で終了させ、次回にどの段階から実施させるかは様々となるが、決済が伴うカード処理の場合、特にカードとの決済処理が全体のフローの中のどこで実施されるかによって、その取引を成立したものと見なすのか、未成立として取り消してしまうのかの判断が分かれるので、システム設計上留意すべきで

ある。

いずれにせよ、カードが故意に寄らず通信エリアを外れたことにより、上位システムが何らかのダメージを受けたり、カードが使用不能となったり、カードを再度使用する時に煩雑な手続きが必要となったりすることは避けるべきである。

3.6.3.2 カードの物理的損傷

非接触 I C カードには、0.8 mm の厚みの中に I C チップモジュールが搭載されているので、過失でカード内部の I C を破損してしまふことはあり得る。

接触 I C カードの場合は、カード表面に接点端子が露出しており、I C チップは通常その接点端子の裏側に格納されている。あえてその上に無理な力を加えたりしないとなれば、通常使用でカードのチップ自身が破損する蓋然性は低い。接点端子部分を含めたモジュール全体がカードから剥落することはあり得るが、その場合でもチップは破損しない場合が多く、チップのデータを確認する手段は残る。

非接触 I C カードの場合は、カードの表面からはどこにチップが格納されているかはわからない。そのため、部分的にカードにかかる力が偶然チップの上であり、破損を引き起こすことが想像できる。さらに、カードの中から壊れたチップモジュールのみを取り出すことは、極めて困難なので、実質的にカードの内部データを解析し再現するのは不可能となる。

そこで、そのようなチップ破損の場合、破損カードが保有していたデータの継承をどのような方法で実施するか、継承できないデータをどうやって再現するかを、カード再発行システムとして保証する必要がある。継承できずに破損によって失われてしまうデータに関しては、カードホルダに十分説明が必要である。

3.6.4 故意の侵害に対するセキュリティ

I C カードの処理の安全性を保証するためには、

- 端末と I C カード双方の正当性を確認するための相互認証機能
- なりすまし、改竄、否認等の防止のために通信相手の真正性を常に確認する機能
- メッセージの秘匿機能

等が重要となる。

これらの脅威に対する最も有効な技術が暗号技術であり、一般に、共通鍵暗号方式と公開鍵暗号方式が採用されている。ただ、これらの暗号方式を採用したセキュリティ技術は、I C カードの内部に C P U が搭載されていることが前提となる。さらに、公開鍵暗号方式のひとつとして R S A があるが、カード内部でこの方式のアルゴリズムを処理させるためには、メインの C P U 以外に、それを高速で実行するための専用のプロセッサを搭載する必要があると認識されている。尚、公開鍵暗号方式には、専用プロセッサを必要としない方式の提案もある。

C P U を搭載せずに I C カードに一定のセキュリティを搭載しようとする場合、ワイヤードロジックでセキュリティ処理を実現することもできる。この場合、決められた P I N を照合したり、カード内部データの一定のエリアを書替え不能とするようなことは実現可能である。

以上は、接触、非接触にかかわらずICカードに共通するセキュリティの問題である。そこで、下記の項目に関して、非接触ICカード特有の問題を検討する。

- 3.6.4.1 相互認証
- 3.6.4.2 電子署名
- 3.6.4.3 暗号化
- 3.6.4.4 チップの不正解析
- 3.6.4.5 チップの物理的破損

3.6.4.1 相互認証

(1) 故意の中断

密着型は相互認証を安定して実施できる可能性が高いが、その手順の途中でカードが強制的に引き抜かれた場合、それが故意であるか否か容易に判断が付くようなカード保持構造であることが望ましい。

近接型の場合、相互認証の途中で、カードが故意にその通信エリアを外されても、過失であるとの主張を退ける根拠を持たない。少なくとも相互認証が途中で故意に中断されても、その後のカードの機能に影響を及ぼさないよう工夫されている必要がある。

また、相互認証が中断した場合、初期に相互認証において予定された確認処理が、次回カードがアクセスされた場合に、確実に全て実施されるようにしなければならない。しかも、電力供給自体が処理途中で遮断されることを想定して、それでもそのような条件を満たす工夫が必要となる。

(2) 不正解析

カードの相互認証を論理的に突破しようとする、カード内部に格納されている鍵情報や暗号化アルゴリズムを盗み出す必要が生じる。本来ICカードは、そういった情報は、いかなるアクセスによってもカード外部へ読み出されることがないように設計されているのが通例である。さらに、相互認証が正当に行なわれていれば、正規のリーダーライタでしかカードへのアクセスが許可されず、不正なリーダーライタでのアクセスが重なれば初期に設定した回数によりカードを閉鎖（ロック）してしまう機能を持つ。

しかしながら、正規のリーダーライタ自体を、盗難や横流しといった何らかの方法で入手され、それをを用いて繰り返し多数のカードへアクセスされ、相互認証の約束事を解析されることも予想せねばならない。まず、正規のリーダーライタが、不正チャンネルへ流れないように運用を徹底し、さらに、端末が屋外の無人環境に設置されるアプリケーションも想定されるため、機器をタンパーフリー構造とするなど、別途、何らかの対策が講じられるべきである。

また、アプリケーションによっては、最初からユーザの手元へリーダーライタが渡ってしまうようなものもあるので、例えば、定期的上位ネットワークから、随時セキュリティ鍵や暗号方式が更新されるような工夫があることが望ましい。

さらに、正規なリーダーライタとカードが相互認証のやり取りをしているのを、通信エリア近傍で傍受されたデータが、それだけでは解析されないよう暗号化されたり、

スクランブルをかけられたり、また一定の条件で更新したりすることが必要であろう。

3.6.4.2 電子署名

データの真正性を確保し通信相手を確認するための手法として、暗号化技術を用いた電子署名が用いられる。非接触ICカードの場合、相互認証のところで述べたように、カードとリーダライタ間を傍受されることで、多くの通信データからの解析により、それらの暗号化手法や電子署名の技法を解読されることがないように十分な強度の電子署名が検討されるべきである。また、それらの方法が、随時、更新されるなどの工夫が必要となろう。

しかし同時に、密着型以外に顕著であるが、非接触ICカードの取り扱い上、通信時間は短ければ短いほど望ましい。電子署名が通信文に付加されることで、いたずらに通信時間が延びて、運用に支障を来す場合も想定される。

現在、提案されている公開鍵暗号方式には、処理速度、消費電流といった特性において問題点が残っている。

この点でも、バランスが重要であるが、高額決済に用いられる場合と、決済以外及び低額決済に用いられる場合の処理を分けて、運用もそれに応じた設計をする必要がある。例えば、近接型カードであっても、高額決済の利用時には、カードを所定のスロットに挿入する運用を要求することなどが考えられる。

3.6.4.3 暗号化

データの内容を秘匿し、システム外部に漏洩させないために、カードとリーダライタのやり取りは、基本的に平文ではなく暗号文でやり取りされることが望ましい。特に、非接触ICカードの場合、傍受されたデータからの漏洩は十分起こりうると思え、対策を施すことが必要である。また、カード内部に格納される重要なデータに関しても、万が一、読み出されることを考え、暗号文で格納されていることが望ましい。

尚、ICカードが複数の発行主体の間で多機能カードとして使用される場合、発行主体間において、それぞれが管理するデータに対して、相互に関与できないことを確保する必要が発生する。そういったデータの管理は、CPUが搭載されているカードにおいては、ファイル構造を多階層構造とし、それぞれのファイルにアクセス権限を管理する鍵を付与することにより達成できる。

3.6.4.4 チップの不正解析

カードのICモジュールをカードから取り出し、それを物理的に解析することで、データを調べる方法がある。この方法は極めて専門的で電子顕微鏡などの高価な設備を必要とするが、対策を講じる場合には、ROMエリアの格納場所について工夫したり、ダミー回路を設計するなどの方法がある。

3.6.4.5 チップの物理的破壊

故意にチップを破壊された場合、カードの券面記載事項との関係が問題となる。例えば、初期一定額で発行したプリペイドカードを全て使ってしまったから、チップを破壊して、未使用だと申告された場合、カードのIDナンバ等から、ホストで管理する使用履歴を即

座にチェックしたり、利用残額自体をカードに保有させずにホストで一括管理して、申告を拒否することができるようなシステムを構築するとすれば、規模の大きなシステムの場合、相当なコストが必要となる。

カードの券面に可変の残額表示ができないが、非接触の運用特性を損なわないような、内部データを常時表示できるような表示機構の開発が必要となる。

カードシステムを会員制としてカードホルダを特定できるようにしたり、カードに有効期限を付与したり、破損したカードの残金の払い戻しを現金で実施せず、プリペイドカードの同額のもので対応するなどの対応が考えられるが、あらゆる脅威に対して、事前に対応することは困難である。

3.6.4.6 その他

その他、ICカードに関連し、セキュリティ確保上、注意を必要とする点と対策を列挙する。

- (1) ICチップ、チップモジュール、発行前カードの流出
対策：厳密な数量管理、保管場所の施錠、製造番号管理
- (2) チップへの、熱、ストレスなどを通じての誤動作による不正アクセス
対策：事故診断機能の保有
- (3) 流通経路における発行前ICカードの盗難
対策：発行コマンドの秘匿、発行パスワードの別管理
- (4) 廃棄されたカードの不正利用
対策：廃棄時のチップ破壊
- (5) ICカードの不正発行
対策：発行履歴の管理資料作成、発行監査体制強化

3.7 非接触ICカードの普及課題

市場で非接触ICカードを普及させていくためには、カード仕様の標準化という問題は重要なポイントとなる。詳細については第3.4節を参照していただきたい。

3.7.1 非接触ICカードの電波法上の扱い

非接触ICカードは、電波を利用するため電波法による規制を受けることになるが、非接触ICカードは、社会に広く普及し、個人や一般にも利用されることが期待されるものであるため、電波法に基づく規制もこれに応えるものである必要がある。

その一つの考え方として、非接触ICカードシステムについて一定の技術基準を満足するものは、無線局の免許を不要にする等の手続きを適用することが望まれるので、具体的な基準および技術的条件について検討される必要がある。

3.7.1.1 割り当て周波数の国内外比較

国際的に産業用、科学用、医療用として周波数（ISMバンド）が割り当てられているが、地域や国により内容に差違がある。今後標準化されていくことが望まれる部分である。現状の割り当て周波数の国内外比較を表 3-9に示す。

表 3-9 割り当て周波数の国内外比較(*1)

周波数(MHz)	許容偏差	注番号(*2)		告示(*3)
		国内	国際	
6.780	± 15kHz	J30	524	-----
13.560	± 6.78kHz	J40	534	該当
27.120	± 162.72kHz	J40	546	該当
40.68	± 20.34kHz	J40	548	該当
(433.92)	± 0.87MHz	-----	661	
(915)	± 13MHz	-----	707	
2450	± 50MHz	J40	752	該当
5800	± 75MHz	J40	806	該当
24125	± 125MHz	J40	881	該当

(*1) ISMの国内電波法での取り扱い・・周波数の公開(電波法 26)

「...割り当てることが可能である周波数及び割当てた周波数の現状を示す表を作成し、公衆の閲覧に供しなければならない。」 『周波数の割当原則』に明記

(*2) 周波数の割当原則・・無線通信規則の周波数分配表(国際)と日本の周波数分配表の注番号の中で規定。

J 40 の記載

『...産業科学医療用(ISM)の使用に指定する。これらの周波数帯で運用する無線通信業務は、ISM 装置の運用によって生じる有害な混信を容認しなければならない。また、ISM 装置は、本装置からの輻射をできる限り抑制するとともに、これらの周波数帯の外側においても、無線通信業務に有害な混信を生じさせないレベルにその輻射を抑制しなければならない』

(*3) 通信設備以外の高周波利用設備の電界強度の最大許容の特例(公示第 257 号)

『該当の周波数帯内においては、通信設備以外の高周波利用設備から発射される基本波又はスプリアス発射による電界強度の最大許容値を定めない』

3.7.1.2 リモート式カードに関する現状の電波法

現状のリモート式カードに関する電波法について図 3-8に示す。

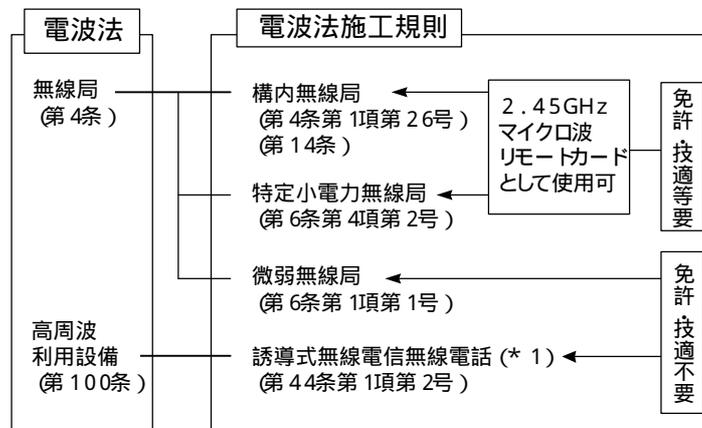


図 3-8 リモート式カードに関する現状の電波法

注*1【誘導式無線電信無線電話】は次の3つの要件を満たすものをいう。

- 電線路を有すること。
- 10 KHz 以上の高周波電流を通ずること。ただし、 $1/2$ の距離において電界強度が $15 \mu\text{v/m}$ を超える設備にあっては、10 ~ 250 KHz の範囲内の周波数であること。
- 通信設備であること。

現状、マイクロ波型(2.45GHz)を除いた非接触ICカードは、微弱無線局の範囲で利用しなければならない。今後広く普及させていく上では、距離を伸ばしたい近接型、近傍型では、新たな電波割り当てが必要である。

現在、電気通信技術審議会にて【非接触式定期券システム】用の技術的要件が、近接型の審議を参考として検討されている。また、【入退室システム】用を検討開始の予定であり、これは、近傍型の審議を参考にされると思われる。

3.7.2 ICカードのコスト

ICカードに限らず、カード普及の条件としてコストはかなり重要な位置を占める。

カード普及を考える上でのコストとは、カード自体のコストと、周辺機器関係のコスト、さらに全体システムのコンピュータシステムコスト、システムのアプリケーションソフトの開発コスト、およびランニングコストである。

汎用化を目指すアプリケーションであれば、市場から要求される価格は自ずと投資対効果費用で決定されてくる。ここで言う投資対効果費用とは、ICカードの持つ機能、セキュリティ性、利便性等が考慮されるべきであり、単に磁気ストライプカードとの比較で論じられるべきものではない。また、カードの価格は当然需要と供給のバランスの上になり立っており、非接触ICカードの仕様がどのように選択されるかによっても変化する。いずれにしても、メンテナンス性に優れた非接触ICカードは市場での認知度も上がり、システム価格は低下してくるものと予測される。

3.7.3 導入動向

非接触ICカードは、ここにきて大きなアプリケーションへの実用化が顕在化してきた。主な物として、

- NTTテレホンカード
- 汎用電子乗車券

などである。

今後の普及に向けては、これらアプリケーションとのリンクを考慮しながら検討を進めていくことが重要と考える。

3.7.4 インフラの整備

接触式・非接触式に関わらずICカードシステムでは、チップを搭載したカードを使用することから得てしてこのチップにのみ着目し、過大な期待を寄せ、すべてをチップが担いとうと考えがちである。信頼されかつ安全対策も十分なシステム構築は、システム全体で取り組むことが重要である。

現状ICカードシステムのインフラ整備はまだまだこれからの状態である。しかしながら、先ほど紹介した非接触ICカードのアプリケーションは大きな社会的インフラとなっていくと考えられる。これらのシステムインフラの内容を吟味して、それとのリンクを検討していくことは、今後の非接触ICカード普及において重要となってくると考えられる。

また、非接触式あるいは接触式のICカードの共通利用アプリケーション、共通利用端末の開発等利用者サイドで利便性の高いインフラ整備を行っていくことが求められる。

3.7.5 参考文献

- 「共通セキュリティ関連技術WG中間報告書」(ECOM:WG05)
- ICカード総覧((株)シーメディア)
- ISO/IEC JTC1/SC17/WG8 報告書各種(社団法人 日本事務機械工業会)

4 I Cカード利用環境整備に関する提言(A I Dの付番管理)

2.1節においては、I Cカードの実用化・普及のために必要な道具としてI Cカードの具体的な在り方を例示し、更にI Cカード普及の鍵であり不可欠なインフラストラクチャーの整備に関しても、クレジットカードを例にとってより具体的な提言をも行なった。

本章ではこれを受け、同章でも触れたが、先の平成8年度WG7活動成果報告書『I C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』の中でも、I S Oの規定、並びにその考え方に関する解説をはじめその必要性に関し記述した、日本におけるA I Dのコード体系の整備及びその付番方法案並びに、国内登録機関の設置による一元管理体制の構築の必要性に関し、現在再開されたJ I S化検討の叩き台とも言うべき原案の紹介も含めて、改めてより具体的に記述することとする。

4.1 I Cカード利用環境整備の中核

あるべき道具としてのI Cカードの利用方法の検討や、そのI Cカードを正しく受け取り扱い処理する為の端末(R/W)とネットワーク網の構築も然る事ながら、これらが円滑に運用される為に必要な、これらを取りまく利用環境整備において、A I Dのコード体系及び付番方法の制定と一元登録管理機関の設置による、国内A I D付番登録管理体制の構築は、下記事項を基本前提とする場合において、I Cカード利用環境整備の最重要事項であり中核と考える。

(1) 基本前提

I C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る。

我が国においては、公的機関・民間を問わず、各種I Cカードの自由な発行権は当然の事乍ら認められであろうし、且つ、これら複数の発行者が混在し、利用者の視点に立ち、運用面において発行者間の相互運用性を図ることによって汎用性を保持すると共に、I Cカードの多目的利用をも実現する方向にあり、このことを将来に渡って可能足らしめるものは、各発行者並びにアプリケーションの識別並びにユニーク性の確保・保証することが基本前提である。

(2) アプリケーション識別子(A I D)の付番管理の現状

既述の通り、既に国際的には定義や番号体系、登録手順等に関して、I S O / I E C 7 8 1 6 - 5で規定されており、E M V仕様もこの考え方に従って、I Cカードと端末間のリセット応答(A T R : Answer To Reset)の方法、アプリケーション選択の方法、各種コマンドを規定している。

翻って日本の現状はと言うと、I S O指定の国際登録機関であるK T A S (Copenhagen Telephone Company)への登録を行うに際しての受け窓口としての事務局が(社)日本事務機械工業会(以下「J B M A」と略す)内に設置されているだけで、日本国内においても国内専用の各種アプリケーションによるI C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“ A I D ” という) の付番管理体制の確立が必要不可欠と考えざるを得ない状況となりつつある。

付番管理の必要性

A I D の一元的な付番管理体制が確立されなかった場合、A I D 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と思われる。

特にICカードの場合、今後公的機関或いは民間企業により、汎用 / 非汎用のICカードが多数発行されることが予想され、一度発行者の手を離れて利用者の手に渡った段階から、R / W端末が不可欠故にICカードの受入機関や加盟店側の人的対応（目視）による取扱いの可否判定はほとんど行われず、単純に端末での機械的な判断に委ねられることとなる。従ってA I D の付番体制並びに一元管理体制が確立され、各発行者によって遵守されない限り、汎用型ICカードの相互運用性の確保も、逆に非汎用型ICカードの相互不可侵も、厳正且つ適正な運用は保証されないこととなる。

以下万一重複した場合の問題点や運用上の問題点を可能な限り列挙する。

A. 重複した場合の問題点

a) リジェクト判断遅延による混乱

D F 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。

b) 他社カードのファイル破壊の危険性

D F 内にフリーアクセスファイルを設定した場合、D F 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。

c) 相乗り対応が困難

相乗りの合意に達した会社間で、D F 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。

d) 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。

B. 運用上の問題点

a) 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、登録受け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。

b) 付番の混乱

仮にISO 7816 - 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。

c) 規格変更時の対応問題

周知徹底が困難である。

d) 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。

尚、本章の冒頭に記した通り、JIS化に向けての検討が再開されたが、その検討の叩き台となるのは、以下に示すJBMAのカード部会において検討された国内付番体系案である。本案は既にISOにおいても日本国内利用と言うことで基本的には認められている。ECOMWG7(ICカードWG)としてこれを支持し、ISO 7816-5で規定されている‘F’の使い方、特に‘D’との使い分け等の運用面等も含めた最終的な検討作業や国内登録機関の設立の為の検討原案策定作業に参画することとしている。

(3) 日本国内におけるAIDコード体系・付番案(JBMAカード部会案)

以下にJBMAカード部会作成の原案を示す。

*原案をそのまま掲載する。

3版97年6月4日

ICカードアプリケーション識別子の登録様式(案)

Registration procedure for IC card application identifiers

JBMS -

(1997年)

序文 この規格は、1995年に第1版として発行されたISO/IEC 7816-5: Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers を元に、対応する部分(登録番号の取り方)について技術内容を変更することなく作成した国内規則に国内における登録管理様式を追加している。

1. 適用範囲

この規格は、国内で使用するICカードアプリケーション識別子の登録様式について規定する。

2. 引用規格

次に掲げる規格は、この規格に引用されることによって、規格の一部をなす。

JIS X 0401 都道府県コード

JIS X 0402 市町村コード

JIS X 0403 産業分類コード

JIS X 6303 外部端子付きICカードの物理的特性

JIS X 6306 外部端子付きICカード - 共通コマンド

ISO 3166 Code for the representation of names of countries

ISO/IEC 7812 Identification cards - Numbering system and registration procedure for issuer identifiers

ISO/IEC 7816-4 Identification cards - Integrated circuit(s) cards

with contacts - Part 4: Interindustry command for interchange

ISO / IEC 7816 - 5 Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers

3. 定義

この規格の目的のために、次の定義を適用する。

(1) DF (専用ファイル)

ICカード内のファイルの一つで、ファイル制御情報及び任意選択の割付可能メモリを含むファイル。

(2) 16進数

4ビットで0から15までの数をあらわす数値表記方法。0から9までは10進数表現と同じだが、10から15までの数値にはそれぞれアルファベットの“ A ”、“ B ”、“ C ”、“ D ”、“ E ”、“ F ”と表記する。

(3) 桁

1バイト(8ビット)を上位4ビット及び下位4ビットの2つに分割した分割単位。

(4) 産業用分類コード

登録者が民間企業及び民間団体であることを示す符号。

(5) 行政用分類コード

登録者が日本国の行政機関であることを示す符号。

(6) 広域地域サービス用分類コード

登録者が日本国の行政機関または行政機関から委託された団体であり、カードを利用するサービスが複数の都道府県又は市町村に及ぶことを示す符号。

(7) 特定地域サービス用分類コード

登録者が民間団体であり、カードを利用するサービスが都道府県又は市町村に地域限定されることを示す符号。

4. アプリケーション識別子

アプリケーション識別子は(以下AIDという)、ICカード内のDF(専用ファイル)を識別する6バイトから最大16バイト長の領域を持ち、登録カテゴリ、国コード、国内独自の種別コード、分類コードおよび任意コードで構成される。AIDは、4ビット単位の16進数を用いてコード化される。AIDの機能についてはISO / IEC 7816 - 5、JIS X 6306を参照のこと。

A I Dの構成は図1のとおりである。

図1 A I Dの構成

1バイト	2バイト	3バイト	4~6バイト	7~16バイト
D	3 9 2			最大10バイト
	国コード		分類コード	任意コード

登録カテゴリ - 国内独自の種別コード

a) 登録カテゴリ

1バイト目の上位4ビットは、ISO/IEC 7816-5に基づく国内専用アプリケーションのカテゴリコードを示し、16進数“D”とする。登録カテゴリコードは表1のとおりである。

表1 登録カテゴリコード

登録カテゴリコード	内容,用途
“0-9”	ISO 7812で定義される
“A”	国際登録
“B”	ISOにより保留
“C”	ISOにより保留
“D”	国内登録
“E”	ISOにより保留
“F”	登録しない

- 参考 1)登録カテゴリコード“ A ”は国際登録A I Dを示す。
 2)登録カテゴリコード“ F ”は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、また、その登録も義務付けられていない。異なるICカードアプリケーション提供者が同一の番号を付番する可能性があることに注意すること。

b) 国コード

1バイト目の下位4ビット及び2バイト目は、A I D登録管理における国別コードを示し、日本国コードはISO 3166に基づき16進数“392”とする。

但し、国コードは、登録カテゴリコード“ D ”以外には意味を持たない。

c) 国内独自の種別コード

3バイト目は、次に示す16進数2桁の国内独自の種別コードである。

- “00”：産業用分類コードは、JIS X 0403の数字部分に準拠する。
 “01”：行政用分類コードは、JIS X 0401及びJIS X 0402に準拠する。

” 0 2 ” : 広域地域サービス用分類コードは、J I S X 0 4 0 3の数字部分に準拠する。

” 0 3 ” : 特定地域サービス用分類コードは、J I S X 0 4 0 1及びJ I S X 0 4 0 2に準拠する。

” 0 4 ” ~ ” F F ” : 将来の利用のために保留する。

d) 分類コード

4 バイト目から 6 バイト目は、次に示す分類コードである。

1) 産業用分類コード

1 6 進数 6 桁の数字 (3 バイト) とし、J I S X 0 4 0 3の大分類から細分類を使用する。大分類、及び中分類、小分類で終わる場合は 6 桁となるよう 1 6 進数 ” F ” を付加する。

2) 行政用分類コード

1 6 進数 2 桁の都道府県コード (J I S X 0 4 0 1) 及び 1 6 進数 3 桁の市町村コード (J I S X 0 4 0 2) を使用することとし、コード長統一のため 6 桁目に 1 6 進数 ” F ” を付加する。また、都道府県コードのみで市町村コードを使用しない場合は、都道府県コードの後に 4 桁の 1 6 進数 ” F F F F ” を付加する。

3) 広域地域サービス用分類コード

1 6 進数 6 桁の数字 (3 バイト) とし、J I S X 0 4 0 3の大分類から細分類を使用する。大分類、及び中分類、小分類で終わる場合は 6 桁となるよう 1 6 進数 ” F ” を付加する。

4) 特定地域サービス用分類コード

1 6 進数 2 桁の都道府県コード (J I S X 0 4 0 1) 及び 1 6 進数 3 桁の市町村コード (J I S X 0 4 0 2) を使用することとし、コード長統一のため 6 桁目に 1 6 進数 ” F ” を付加する。また、都道府県コードのみで市町村コードを使用しない場合は、都道府県コードの後に 4 桁の 1 6 進数 ” F F F F ” を付加する。

e) 任意コード

任意コードは、7 バイト目から 1 6 バイト目までの最大 1 0 バイトの領域を持ち、業種及び団体で任意に決定する識別のための任意コードである。任意コードは、空き領域にキャラクタを挿入する必要はない。

1) 利用業界は、発行企業コード、アプリケーション種別、その他相互運用のためのコード、ネーム等を含む任意コードを統一して作成する。

2) 自治体・団体等で利用する場合は、共通運用に必要な情報識別子を含む任意コードを統一して作成する。

5. アプリケーション識別子の登録管理と申請

A I D 管理は、A I D 登録、一定期間毎の A I D 再登録及び A I D 廃番について管理を行うことである。A I D 登録申請はつぎの申請書様式により行なう。

a) A I D 登録申請

A I D 登録申請は、様式 1 の用紙に必要な事項を記入して申請する。

b) A I D 再登録申請

A I D再登録申請は、様式2の用紙に必要事項を記入して申請する。

c) A I D廃番申請

A I D廃番申請は、様式3の用紙に必要事項を記入して申請する。

*以下の付属文書あり。

付属文書1「A I D登録申請書」(様式1)

付属文書2「A I D再登録申請書」(様式2)

付属文書3「A I D廃番申請書」(様式3)

(4) A I D国内登録管理体制について

A I Dのユニーク性の保持・保証の為に、保険的な意味合いも含めて、一元管理が望ましいが、前記「BMA案を具体的なイメージで示すと下図4-1のようになる。

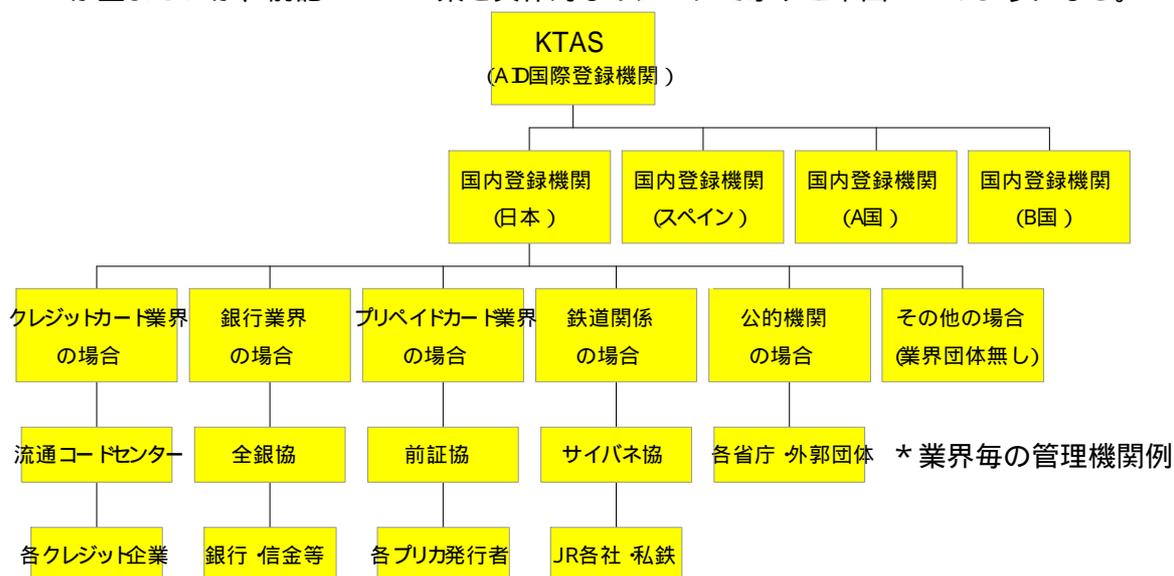


図 4-1 A I D登録体制イメージ図

5 ICカード検討メンバー

5.1 接触ICカード検討WG(SWG1)メンバーリスト

お名前 (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
岩切 美和	(財)金融情報システムセン ター	業務調査部 業務調査第二課 調査役
藤田 潔	(株)クレディセゾン	営業企画部 EC推進担当
曾谷 直人	グローリー工業(株)	メディアシステム開発部 技師
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
中谷 明広	(株)ジェーシービー	情報ネットワーク事業部マルチメディア開 発課 係長
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
大石 幸範	(株)ジャックス	カード部カード企画課 推進役
宮下 善和	神鋼電機(株)	新規事業開発室
浦部 治福	セコム(株)	開発センター技術情報管理グループ チーフエンジニア
新谷 敦	(株)セントラルファイナン ス	カード事業部 主任
厚見 靖男	(株)ダイエー((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)	BF事業部営業開発本部東京市場開発部市場 開発室 室長
酒井 正美	(株)東芝	情報・通信システム新規事業企画室 ICカード・ 無線タグ事業推進担当
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	業務部マルチメディア推進室
藤田 茂樹	日本電気(株)	ワークステーション・サーバ 事業部 第二技術部
藤井 正哉	(株)野村総合研究所	新社会システム事業本部 サイバー・コマース事業部
今井 仁	ぴあ(株)	データベース本部 EC推進室 室長
土反 康裕	(株)ピープル	総合企画部 マルチメディア課

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	マスターカード・インターナショナル・ジャパン イク	メンバーリレーションズ
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)	ペ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
大屋 隆	(株)ライフ	カード事業部カード企画課 課長
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グル ープ主任技師
山口 卓	シーメンス(株)	IC Card Office 担当部長
松田 康男	(株)ゼクセルインテリジェ ンス	ICカードシステム部 担当部長
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
京極 朗	(株)オリエントコーポレー ション	カード企画部 課長代理
飯田 佳也	ユニタバコサービス(株)	研究員
松井 泰彦	光村印刷(株)	総合企画室 課長
一柳 宏司	(株)三和銀行	ネットワーク開発部(東京) 部長代理

5.2 非接触ICカード検討WG(SWG2)メンバーリスト

お名前 (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)	カード事業部課長 カード企画開発ユニット
信濃 義朗	昌栄印刷(株)	ICカード販売グループ 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・カード事業推進センタ
小川 幸男	オムロン(株)	新事業開発センター・カード事業推進センタ
前田 昇	ソニー(株)	カードシステム事業室 室長
盛 雅博	ソニー(株)	B & I 営業本部プロフェッショナルシステ ム
水野 一男	(株)デンソー	電子応用技術部第3技術室
岸本 輝昭	(株)日立製作所	システム開発本部
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
富永 彰	小林記録紙(株)	営業企画本部第二企画部カードグループ
植村 泰佳	ICカード取引システム研究開発 事業組合(ICCS)	事務局長
千村 茂美	ローム(株)	MODULE LSI商品開発部M3G

田口 治生 ローム（株）

MODULE LSI商品開発部M 3 G

禁無断転載

平成10年3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2-4-5
タイム24ビル10階
Tel 03-5531-0061
E-mail info@ecom.or.jp

「8
WG07

ICカード利用ガイドライン(接触/非接触)
(1・0版)

平成10年3月

電子商取引実証推進協議会

WG
7