決済機器におけるセキュリティ技術

池田　文幸（いけだ　ふみゆき）　清沢　久（きよさわ　ひさし）　井澤　晴信（いざわ　はるのぶ）

1　まえがき

IT（Information Technology）化社会の到来を受け，コンピュータ技術・ネットワーク技術の進展と，経済活動のグローバル化やライフスタイルの変化などの社会・産業構造の変革により，高度情報化社会に適した決済手段として「電子決済」が進展してきた。その中で富士電機は少額の買物を対象とした「IC カードを中心としたリアル型電子マネー」についていろいろな推進事業者と共同で実験や実運用に参画し開発を進めてきた。

特にここ１年は，非接触 IC カード媒体による東日本旅客鉄道(株)の「Suica」カードの発行や，銀行，コンビニエンスストア，通信キャリア会社までをも巻き込んだ電子マネー運用会社による数百万枚単位のカードの発行による広域の電子マネーシステムができつつある。また，1999 年に改正された「住民基本台帳法」や「情報整備都市計画」などで各地域にも IC カードを利用した進展を図っていこうとする動きがある。

本稿では，リアル型電子マネーシステムを中心とした決済機器におけるセキュリティについて，富士電機の対応の現状と，今後の取組みについて紹介する。

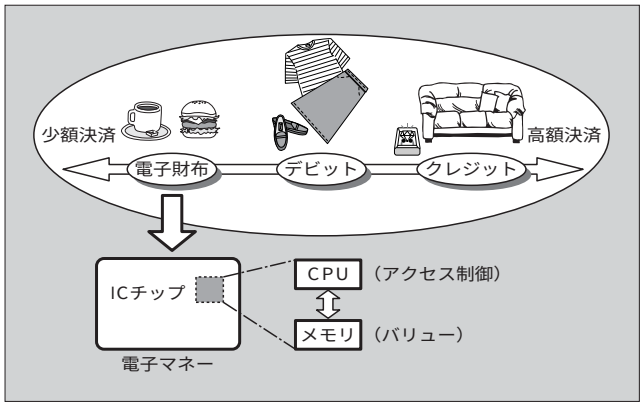
2　電子マネーの概要

2.1　電子マネーの現状

電子マネーとは，現実に流通している貨幣価値に裏付けられた電子的な価値情報で，支払いの手段として利用できるものをいう。現在，現金通貨に代わるものとしては，手形，小切手，クレジットカードなどの決済手段があるが，これらはそれ自身が貨幣価値を持っているのではなく，補助的な貨幣（決済手段）としての役割・機能を果たしているにすぎない。

それに対して電子マネーは電子財布とも呼ばれ，それ自身が貨幣価値を持っていて，直接的に決済を完了させる機能・役割を持っているところが最大の特徴である。**図１**に電子マネーの位置づけを示す。

図１　電子マネーの位置づけ



電子マネーの媒体として使用される非接触 IC カードは，バリューなどを記録するメモリのほかに，決済機器などのカードリードライトデバイスとのアクセス制御を行うマイクロプロセッサの搭載により，暗号技術などを駆使して，外部からの脅威に対してきわめて高いセキュリティ機能を備えることが可能となっている。IC カードに格納された電子マネーはまさにきわめて安全な「電子のお金」ということができる。

今から５年ほど前までの電子マネーは，利用環境も作りやすい点から，クローズドな環境の中で，例えば大学の学生証との一体型電子マネー，あるいはオフィスビル内の社員証，入館証との一体型電子マネー，アミューズメントパークの入場券と一体になったものであった。しかしながら近年は，鉄道，バスなどの交通分野に代表される新たな利用分野，マーケットチャネルへと展開がなされており，普及に向けてすそ野の広がりが大きく期待されている。

電子マネーで買物をする場合の決済および精算の方法は，いずれのシステムでもほぼ同じ仕組みとなっている。電子決済機器の場合には，装置内に IC カード内バリューの読取りおよび書込み装置（通称：IC カードリーダライタ）を備え，電子マネーデータを通信ネットワークを介して，電子マネー発行母体のクリアリングセンタへ転送し，月末に銀行振込みなどで精算される仕組みが一般的となってい

池田　文幸

各種エレクトロニクス機器およびセキュリティの研究開発に従事。現在，事業開発室ネットワークソリューション部担当課長。

清沢　久

通貨関連機器および IC カード関連機器の開発に従事。現在，信州富士電機(株)技術部シニアエンジニア。

井澤　晴信

通貨関連機器および IC カード関連機器の開発設計に従事。現在，信州富士電機(株)技術部。

図２　電子マネーシステムの仕組みの一例

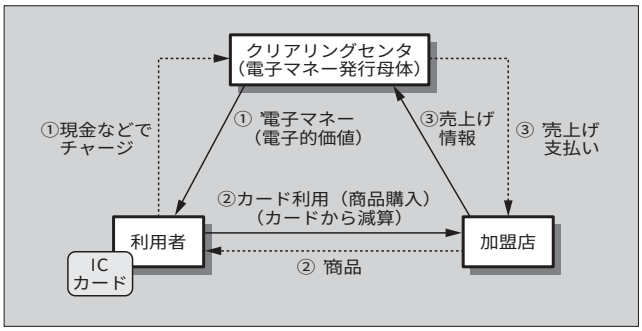
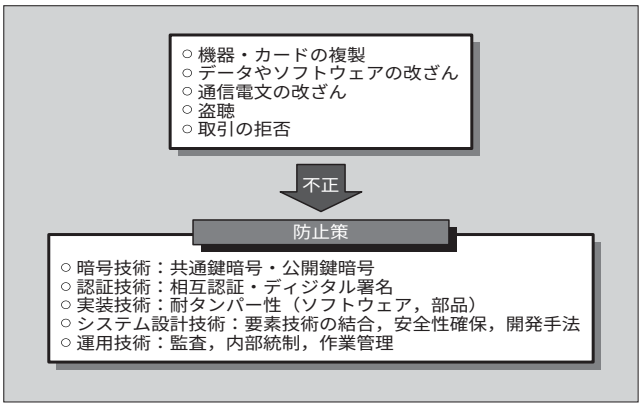


図３　各種セキュリティ技術



る。**図２**には電子マネーシステムの仕組みの一例を示す。

2.2　電子マネーの利点と課題

電子マネーの第一の利点は，現金の保管・移動がない点であり，集計業務が合理化できる点である。すべてコンピュータ処理が最初の段階から行われるため，金銭の手渡しミスや売上金集計ミスなど人的なミスが発生しにくく，集金後の集計業務も発生しないため，大幅な業務改善が期待できる。第二の利点は，現金のハンドリングがなく短時間で支払い（決済）ができることである。

一方で電子マネーの課題としては，不正防止の観点からICカードの複製や改ざんおよび成りすましの問題，消費者保護の観点から匿名性の問題，返品・払戻しの問題，電子マネー紛失などのリスク負担の問題などが一般的にあげられる。これらは，セキュリティ技術に代表される技術面での対応策に加えて，運用の仕組みや制度面から解決を図っていくことが必要で，今後，社会的なルールが確立されていくと考えられる。また，防御だけでなく不正が発覚した場合の迅速な対応が求められる。

そのほかの課題としては，一般消費者，特に高齢者や障害者にとって使いやすい簡単な機器や，共通化された使用環境の提供があげられる。また，電子マネーは一般的にネットワークを介してクリアリングセンタで管理されるため，通信コストの低廉化も重要である。特に，コンシューマーEC（Electronic Commerce）と呼ばれる企業ー消費者間の取引では数百円単位の少額決済が考えられるが，通信コストが相対的に高ければ企業にとってもユーザーにとってもメリットがなく多くの利用は見込めない。電子マネーの普及には，技術的問題，法制度課題をクリアしていくと同時に，こうした消費者の利用観点に立った決済機器のあり方を提案していくことが必要である。

3　決済機器へのセキュリティ対応

3.1　セキュリティ基本技術

電子マネーシステムでは，電子マネーを電子データの形で扱うことから，各種不正に対するセキュリティ技術は最も重要な基本必須要件である。セキュリティにおける課題には「データ盗聴」「複製などによる成りすまし」「データ改ざん」があり，それらへの技術的対策や仕組みが必要である。

その解決に必要な技術として**図３**に示す暗号技術，認証技術，実装技術，システム設計技術，運用技術がある。特に決済機器で重要なのは，前述の暗号技術・認証技術だけでは電子決済機器としてのセキュリティは確保できないため，それを確保するために，耐タンパー（変造されない）技術が求められている。これは電子マネーシステムの運用にもかかわることであるが，決済機器が盗難，またはリサイクル・廃棄されるときに電子決済処理を施すボードが流出し，内部の処理方式または鍵を解析するリバースエンジニアリングにより同様の複製品ができた場合は，電子決済システムは多大な金額損害を被るだけでなく信用失墜によりシステムそのものが崩壊してしまう。したがって，これを防止するための実装技術（耐タンパー性）が必須になる。

富士電機では，自動販売機や小売店舗での電子マネー対応決済機器，レジャー施設などのクローズド環境での電子マネーシステムを中心としたビジネスを展開しており，無人販売，設置場所が点在しているなどの特性を持っている。そのため，決済機器にはリバースエンジニアリング対策も含めた高セキュリティ，高信頼性を確保する必要があった。

以上のことから，下記(1)〜(3)の開発コンセプトを立て，セキュリティ部の共通プラットフォームの開発を推進してきた。

(1)　電子マネー決済機器用の汎用制御方式の開発
(2)　高セキュリティを確保するSAM（Secure Application Module）の実現
(3)　電子決済データの信頼性向上

3.2　電子決済機器の汎用制御方式の開発

電子決済機器に求められる機能としては，ICカードをハンドリングしカードデータを読み書きする機能（リーダライタ）と，暗号処理を施し電子マネーを安全に記憶する機能（SAM）と，そのデータをクリアリングセンタへ送信する通信機能とがあり，これらの機能を持つ装置のことを，一般的にCAD（Card Accepting Device）と呼んでいる。**図４**にCADの適用例を示す。

決済機器における制御方式の汎用化のため，組み込まれる装置側とのインタフェースの共通化と，SAM（次節で

図４　決済機器における CAD の適用例

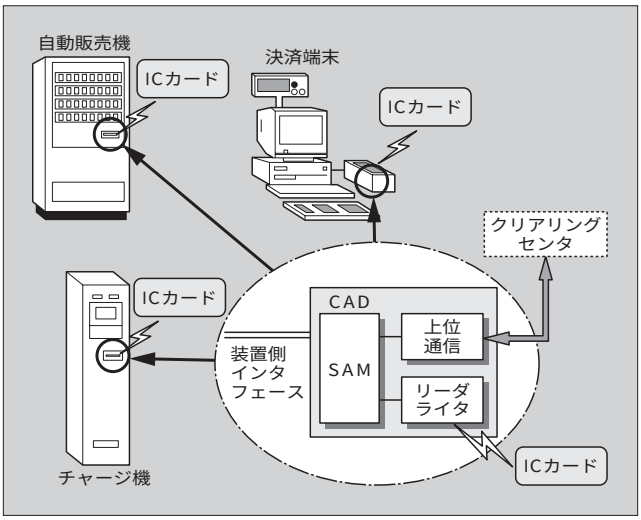
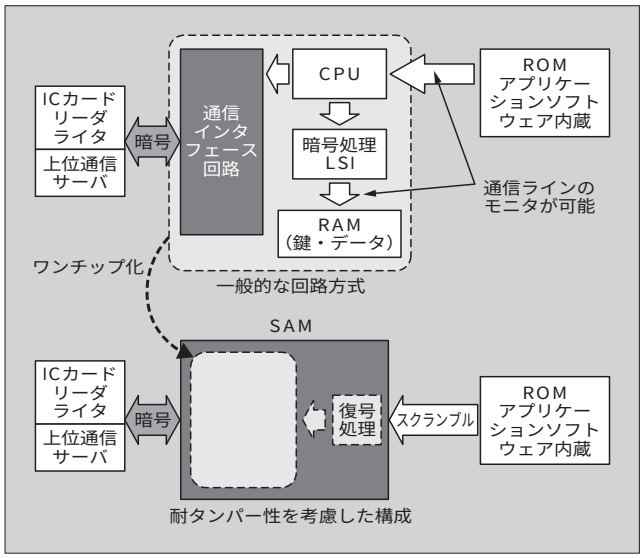


図５　SAM の構成



解説）の開発，カードリーダライタの制御手順の標準化を行った。これにより，自動販売機，店舗端末などに共通して適用ができ，しかも，各装置は一貫したセキュリティの確保も可能となった。

3.3　電子マネー決済機器用 SAM の開発

SAM は，電子マネー対応機器に搭載される CAD の中でセキュリティの中枢を担う部分であり，実際に決済処理を行うために，鍵情報を内蔵し，暗号化されたカードデータの処理や，上位装置との通信制御を行うものである。

決済機器の耐タンパー性を実現するためには，暗号データ，秘密鍵，認証データを保持し，外部からリバースエンジニアリングにより読み出せないようにすることが必須である。

対応策として，CPU，暗号・認証機能，通信インタフェース機能，暗号鍵，認証データを格納するメモリをワンチップの LSI に内蔵する方式を採用した。**図５**に示すように，一般的な回路方式では，装置内の回路（信号ライン）を流れるデータを何らかの方法でモニタすれば，前述の機密データを知り得てしまう。これに対し，ワンチップ化することで信号ラインのモニタは不可能となり，SAM の耐タンパー性は守られる。また，プログラムを格納する ROM（Read Only Memory）はアプリケーションごとに対応するため，SAM の外側に設置しているが，ROM 内のプログラムコードにスクランブルをかけて，SAM 内部で復号化してソフトウェアの実行をすることで，リバースエンジニアリングを防止している。SAM の概略仕様を**表１**に示す。

3.4　電子決済データの信頼性向上

電子マネー決済機器は，一般の電子機器同様，絶対故障しないとはいえない。現金であれば，決済機器内に保存され残っているが，電子決済データであれば機器内に記憶されているだけで，精算処理を行うためのクリアリングセンタとの通信で精算処理が完了するまでは売上金として計上できない。その間に，機器の停電や機器の故障により制御ユニット交換によって電子決済データが消失することのないような高い信頼性が必要である。そのため，決済データは機器の故障時に決済データの抜取りができるメモリカードと，内部制御ユニットは停電にもデータが消失しないフラッシュメモリの二重バックアップの冗長性を持たせている。

表１　SAM の概略仕様

項　目	仕　様
暗　号　方　式	共通鍵方式
相 互 認 証 方 式	2パス方式
メッセージ認証方式	共通鍵 MAC 方式
暗　号　鍵　長	56，112 ビット
鍵　管　理	階層型
処　理　時　間	1μs/64 ビット

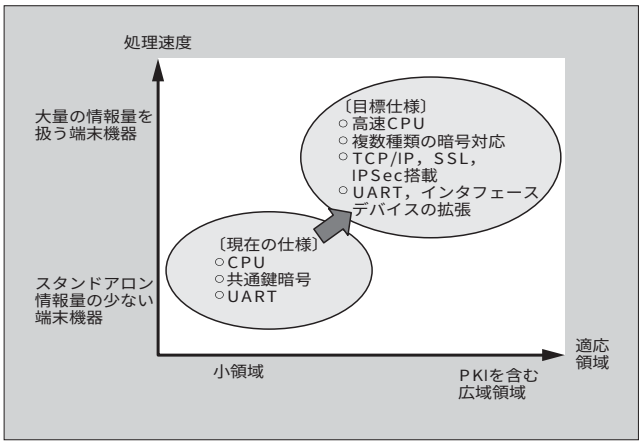
4　今後の電子決済機器対応

今後ますます，電子マネーの普及は促進していくと予測され，携帯電話を含んだモバイル決済への対応，インターネットに代表されるオープンネットワーク接続による即時決済への対応が求められてくる。

その場合，インターネット対応のセキュリティ技術である SSL（Secure Socket Layer），IPSec（Internet Protocol Security）への対応化，PKI（Public Key Infrastructure）認証技術が要求される。そのためにも，決済機器はオープンネットに特有なアクセス制御機能（ファイアウォールなど）と，暗号処理の高度化，対面決済での待ち時間短縮のための暗号処理高速化を図っていく必要があり，**図６**にその方向性を示す。

セキュリティ製品の信頼性を図る尺度として，2000 年７月にセキュリティ評価基準 ISO15408（JIS X 5070）が

図６　今後の決済機器用 SAM の方向性



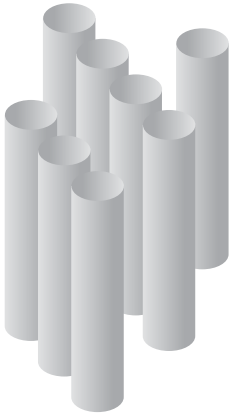
制定された。これを踏まえて，決済機器のみならず，企業活動（開発ー製造ー廃棄までの製品ライフサイクル）においても，今後一貫したセキュリティポリシーを考えて開発を進めていく必要がある。

5　あとがき

電子マネーはようやく離陸したばかりであり，今後いろいろな媒体を介した決済手段の提案が各事業者間で生まれていくと予想される。また，決済機器もこの電子マネー対応を契機に，より社会全体に貢献できるよう，新しい役割・機能を持った提案をしていく所存である。

参考文献

(1)　日経デジタルマネー・システム編．デジタルマネーのすべて．日経 BP 社．1997.



e-Front runners

＊本誌に記載されている会社名および製品名は，それぞれの会社が所有する
商標または登録商標である場合があります。