電子マネーと確証 : 現状と課題

藤田, 昌也
九州大学経済学部 : 教授

時永, 祥三
九州大学経済学部 : 教授

https://doi.org/10.15017/4494284

出版情報：經濟學研究. 64 (3/4), pp.1-19, 1998-01-31. 九州大学経済学会
バージョン：
権利関係：

電子マネーと認証—現状と課題

藤田昌也
時永祥三

1．はじめに

インターネットの急速な普及は，情報産業のみならず多くの産業分野における製品開発，流通形態，あるいは企業内における意思決定のあり方などに大きな影響を与えている。インターネットの持つオープン性は，世界的規模でのデータアクセスを可能にし，従来の情報検索や情報ナビゲーションの方法論までも揺るがし始めている。しかし，一方では，不特定ユーザ間での情報交換を前提としており，情報のセキュリティの問題，個人のプライバシ保護の問題，ネット上での倫理的規制などの課題が生じている。特に，電子商取引に代表されるネット上での商品の購買，決済には直接的な経済的利害が関連しており，本格的な解決策が模索されている。

本論文では，このようなネット上での取引を中心として，現状と課題について議論を展開している。具体的には，決済の有力な手段とされている電子マネーについて，その実現技術，社会的制度を中心に，現状と解決されるべき課題について述べている。電子マネーは，その形態や利用範囲，実施主体などさまざまであり，社会的インフラとして確立するには時間が必要であろうが，産業や社会のネットワーク化，グルーバル化の傾向はますます強まっており，個人や企業を問わず関わりを持つことになるであろう。この場合，ICカード製造や高度なセキュリティの確立など技術的な課題は大きな要素を占めるが，国の金融制度に係わる大きな問題を含んでおり，金融機関や国のサイドからの本格的な政策提示が必要な時期となっている。

以下，第2章では，電子マネーの流通の主たる舞台となる電子商取引に現状について述べる。第3章では，電子マネーの実現方法とその特徴について整理し，制度的な問題を考察する。第4章では，認証の必要性とその論理について述べ，社会的に保証されるべきポイントについて展開する。第5章では，電子マネーと認証技術に関して，現在解決されるべき課題とされている点を整理し，電子マネーが社会的インフラとして受け入れられるべき条件を考察している。

2．電子商取引の現状

電子マネーに関しては欧米での試行が先行し，日本はその技術面での貢献だけが注目されてきたが，日本でも通産省による電子商取引プロジェクトが動きだすなど，新たな局面を迎えている。例えば，電子マネーによる商品の購買実験が東京のファッションタウンで進められており，モンデックス型のICカードによりシステムが実現されている。このほか，さまざまな分野に

おける商品の売買が，いわゆるサイバーモールとよばれるインターネット上での商店街においてなされている。現在，試行段階であり，評価について本格的な公表はなされていないが，急速に拡大するまでにはいたらず，参加企業も積極的な利益追求よりは宣伝や企業イメージの向上を重視している。

形態としては，銀行のデポジットを背景として，不特定の商店で購買と決裁が可能であることを売り物としているが，すでにクレジットカードによる購買が普及しており，一部にはデパートや商店街の共通カードがあり，また，消費者が頻繁に利用する社員食堂や売店でのカードによる購買があるなかでは，ICカードにより決済手段を実現する意味や特徴をいかに出すかが問われている。

このような中で，電子マネーの利用については，相対的にインターネット上での電子商取引（サイバーモール）および企業間の調達・決済に移行してきていると考えられる。従って，以下では，この電子商取引と企業間の調達・決済に関連して電子マネーの現状について整理し，問題点を明らかにしていく。

2.1 電子商取引

電子商取引について，最近の日本と米国のデータを表1に整理している。日本では，通産省などが中心となり，1997年度ころから実験を始めており，現在，その基礎データが収集される段階となっている。表1には，現在では良く知られるようになったプロジェクトもあり，日本でも，形式的には電子商取引のシステムが整備される段階となっている。

表1に示されている米国のデータは，主としてインターネットのホームページで公開されている情報を基礎としている。詳細は省略するが，米国では，いわゆるCALS(Continuous Aquisition and Logistics System，あるいはCommerce at Light Speedと表現される）に関する国家的なプロジェクトがあり，全米の各地にその推進センターがある。このCALS推進の組織が，現在では本来の電子的な大規模調達のシステム構築から電子商取引の実現へとプロジェクトの目的をシフトさせてきており，この推進組

表1（a） 米国の電子商取引(EC)の規模

年度	1996年		1998年
市場規模	518 millon dollar(実績)		2.3 billion dollar (予測)
内訳	コンピュータ製品	140 million dollar	323 million dollar
	旅行	126	276
	娯楽	85	194
	アパレル	46	89
	贈り物	45	103
	食品・飲料	39	78
	その他	37	75

資料：Forrester Research調べ，など

表1（b） 米国の電子取引(EC)の事例

テレビショッピングの子会社　Internat Shopping Network
（メーカ600社の製品35000種類の製品を販売）
会員制オンラインサービスの子会社　Shoppers Advatage
（1700社250000種類の製品を販売）
CD，ビデオ販売　CDNow
（165000種類のCD，8500種類の音楽ビデオ）
書籍販売Amazon
（100万種類の書籍）
競売システム　ONSALE
（再生品や生産打ち切り品などの限定商品）
コンピュータ管理サービス　TuneUP
（コンピュータ管理ツールのオンライン提供）
株式売買　E*TRADE
（インターネット上の株式売買）
中古車販売　BargainFinder
（最も安くするディーラの情報提供）

資料：ジェトロ・サンフランシスコ事務所調べ，など参考

織による情報提供が重要な位置を占めている。日本と米国における電子商取引の評価については，初期段階であるため，さまざまであり，結論的なものは未だ出ていない。しかし，次のようなことは一般的な評価としてあげられており，これが自然と日本と米国における商習慣の違いとなっている。

（1）開設と閉鎖の同時進行

インターネット上のホームページを開設する企業が増加する傾向にあるが，一方では企業にメリットがないとして閉鎖するケースも存在している。米国の統計によると1994年に開設したホームページのうち1996年末に閉鎖したものが約40%あるとされている。これらは電子商取引を目的としたホームページであり，一般の企業広報活動を目的としたホームページについては，更に悲観的な傾向にあると考えられる。インターネット上の広告業についても，拡大よりは縮小傾向にある。

インターネット上の商店の閉鎖の理由は，取引が極めて少ないことが原因であるが，その販売金額が小口であることが特徴となっている。米国の統計では，10ドル以上の買い物は2割程度であり，日本の場合も，1万円を越えない買い物が半数となっている。個人が高額の買い物をしない最大の理由が，クレジットカード情報などがインターネットを通じて漏れる危険性についての懸念であり1万円というのがその限度額となっているのであろう。

また，日米では一般的な通信販売の市場規模が大きく異なっていることも，今後の展開では重要である。米国では小売市場の13%が通信販売によるものであり，その中で約1割がオンラインショッピングである。一方，日本では通信販売の総額は小売市場の2%程度であり，極めて小さい。通信販売がサイバーモールの基礎を成していると考えると，日本では市場開拓が先行される必要があろう。

（2）分野の特定化

インターネットによる電子商取引（サイバーモール）に限定して，取引される商品を分類すると，書籍，音楽関連，旅行，ワイン，保険，中古車などに大きな成長が見られる。販売の方法にはいくつかのバリエーションがあるが，通信販売などで定着している購入申込，宅配業者(UPSなど)による配送，更にクレジットカード番号による決済が主要なルートとなっている。これらの分野の特徴としては，個人の好みに依存する面があり情報検索が前提となること，最新の情報を収集したいこと，ダイジェスト的な情報を求めていること，可能な選択肢を同時に検索できること，などがあげられるであろう。

しかし，ホームページを開設する企業には株式投資，投資信託など個人投資に関するものが増加する一方で，貴金属，衣料などでは撤退が顕著となっており，インターネット上のサイバーモールも，やや分野が特定化される傾向にあることは否めない。従って，個人が選択しやすい旅行，書籍，嗜好商品などでホームページを開設する方向へと進と思われる。

（3）採算ライン

詳細な情報は公開されていないが，米国では電子商取引により利益を計上できる企業がそろそれ現れてきている段階であると言われている。しかし，サイバーモールとして大々的に展開しているシステムでは，撤退する企業も出てきており，特に，最近ではIBMが主催しているワールドアベニュー（コンピュータ販売，百貨店，スポーツイベントチケット販売など）の撤退(1997年6月店舗を閉鎖）が知られている。また，

日本では全般に不振であり，いわゆる「バスに乗り遅れない式」の参加が目立っている。従って，もともとすでに存在しているデパートやスーパーの機能を代替するものではなく，かなり限定的な分野での販売に威力を発揮すると考えられる。米国では，特に企業におけるリストラの進行で，勤務時間の有効活用や実質的な時間延長（ハリス調査では1973年の週40時間に対して現在は週51時間）などにより，時間を節約するシステムが歓迎される傾向にある。また，日本ではサイフを実質的に管理している主婦がデパートなどの主要な顧客になっているのに対して，米国では反対の傾向にあることも大きな差異であろう。

このように，日米の習慣の違いなどにより差異は存在するとしても，大きな枠組みでは，特定分野での電子商取引優位の構造が確立されていくものと思われる。

（4）クレジットカードか電子マネーか

米国におけるインターネット上の電子商取引の決済手段として，現在，ほとんどのケースがクレジットカードによりなされている。もともと，チェックやクレジットカードなどの，現金ではない手段で支払いをする習慣が極めて広く取り入れられている米国では，クレジットカードを使用して支払いをすることへの抵抗感が少ない。もっとも，アンケートの結果では，日常生活で現金を使用した支払が全体の8割程度を占めており，小額であるスタンドでの支払い，タクシー料金など，現金での支払が件数としては多くなっている。表2に米国における個人ベースの決済方法のデータを示している。支払いのケース数の比較であり，現金が多いことが目立つが，小額は現金で，中程度は小切手で，更に額が大きい場合にはクレジットカードによる支払いと区別してされれている現状を示している。

電子商取引の決済手段として，今後，電子マネーがクレジットカードなどに置き変わる可能性，あるいは時期について明確ではないが，すでに存在するクレジットカードの制度，いわゆる社会的なインフラに相当するものが整備されないと，電子マネーが本来の「スマートマネー」として流通することにならないであろう。これは，電子マネーのメリットそのものも評価の対象であるが，カードの紛失や虚偽のデータによる個人の損害をカバーする保険機構の存在が大きいであろう。従って，現在，マスターカードによりモンデックスが買収されたように，電子マネーは機構としては興味ある存在ではあるが，これをインフラとして整備するには，既存のシステムによる運用実績に大きく依存する。

現在，日本でもNTTと都銀により電子マネーの新システムが開発されようとしており，電子マネーの信頼性を担保する実験として注目される。このシステムでは，銀行とは別のカード登録機関を設けて個人のプライバシー保護やセ

表2（a） 米国における決算区分ごとの規模

従来手法	5150 B(billion dollar)
電子マネー計	245 B
(主要内訳)	E-Money via TV 45 B, E-Money via business to business 140 B
	E-Money vua Onlien commerce 60 B

資料：Killen&Associates

表2（b） 米国における個人決済の区分(件数ベース)

Cash	Credit card	Check	Store credit Card	Debit cards	other
54%	39%	23%	7%	1%	1%

資料：Killen&Associates調べ

キュリティ対策を講じている。ATMからのICカードへの預金の移転を基本としており，2000年の実現をめざして，1000店舗での協力を進めている。

2.2 企業間の決済と電子マネー

米国におけるインターネットを通じた消費者の商取引の総額を金額ベースで比較した場合，その額はGE 1社が調達する金額に相当しているとされており，企業の行う調達や取引の大きさが分かる。従って，企業間での取引や決済が本格化することになると，電子的決済についても大幅なコストダウンがはかられ，電子マネーの普及にも大きな影響を与えると考えられる。銀行の本業を融資と考えると銀行にとっては，銀行から企業へのサービスメニューの変更程度になるかもしれないが，いわゆる決済システムを独自に企業が構築する段階になると，金融業を浸食する影響を与えることになるであろう。しかし，現在のところ，企業と銀行との共同作業として進んでおり，米国のBankAmericaインターネットビジネスとして，表3のようなメニューが提供されている。

企業間の決済が電子的に行われることになるには，いくつかの条件が整備される必要がある。現在，この分野ではEDI (Electronic Data Interchange)プロトコルを実現したシステムが業界ごと，あるいは業界をまたがって作成されているが，今後，これが拡大することになるには，次のような問題が解決される必要がある。

(1) 電子商取引による調達の進展

米国のGEでは，年間，10億ドルの部品を電子商取引により調達していると言われている。GEはCALS推進でも主動的な企業であり，特に，その決済情報の交換に不可欠であるEDIの分野では，自社開発のシステムを社外の企業にも提供する試みを行っている。このように，一般の消費者向けの商品がインターネットで取引されている以外にも，工業製品や中間製品の宣伝，販売のメディアとしても利用されている。

表3 BankAmericaの勧めるFinancial EDI over Internat

開始次期	1995年9月より6カ月の実験
内容	BankAmerica, Lawrence Livermore国立研究所との間で決済情報(settlement and payment)をインターネット経由で処理する(Financial EDI)
試験内容	電子メールでの伝票伝送，ディジタル署名，DES公開鍵，RSA
送信データ	purchase order, invoices, shipping notes, payment
送信プロトコル	ANSIのACH(Automated Clearing House)手順
セキュリティ	PEM/MIMEの使用により保護 PEM(Privacy Enhanced Mail)ディジタル署名付きメール MIME(Multipurpose Internat Mail extension)バイナリ暗号化メール

資料：ホームページwww. bankamerica. comなどより

すでにパソコン製造，自動車生産など組み立て産業の分野では，広域的な部品調達によるコストダウンが戦略として組み込まれており，そのためには自社の関連企業だけではなく，広く社外企業からの部品の調達が必要となっている。このため，従来は，個別的に企業間の関係をもつことが行われてきたが，インターネット上での産業情報の公開，交換は，このような機会を増大させていると言えるであろう。現在，従来の企業間の関係を代替するほどではないが，オープン指向を強める企業にとっては，インターネット上での電子商取引は避けては通れない課題となっている。

更にGEのシステムで注目されるのは，インターネットを通じた調達を決済を実行するシス

テムを提供していることである。この概要について表4に整理している。これは，すでに述べたオープン指向をシステムの上でも実現したことになり，調達に応じる企業（供給側）からのシステムへのアクセス，決済システムとしての完結性が追求されている。

このような試みは，米国では，サンフランシスコのLawrence Livermore国立研究所が中心となってなって進められており，その概要についても表4に整理している。このプロジェクトは米国のCALSの大きな柱となっている。

EDIは複雑な企業間連携をVAN上で推進する方法として1980年代に導入され，1980年後半になりようやく，米国標準，欧州標準，更には世界標準がさだめられるにいたっている。このように，EDIはVANをベースに長い時間をかけて導入されている背景には，企業におけるセキュリティの確保とこれを実現する閉じたネットワークへの強い要求がある。

表4　GEのTradeWeb

開始次期	1996年1月よりサービス開始
内容	GEの集積したEDIソフトウェアやシステムを中小企業に提供 EDIをインターネット経由で処理する GEはすでの過去25年間にわたり40000社とEDIで取引している
提供内容	ANSI X12標準のもとでのEDIメールボックス，GE Trade Web Directry
送信データ	purchase order, purchase order acknowledgement, invoices functional acknowledgement
送信プロトコル	ANSI X11手順
セキュリティ	SSL（NerScape社の提案した規格で公開暗号鍵とX. 509証明書からなる）により保護

資料：ホームページwww. getradeweb. comなどより

（2）決済システムの安定性

個人のインターネット上での取引で個人情報の保護やクレジットカードの情報の漏洩が基本的な問題となっているように，企業間での取引情報，決済情報の交換に関しても，セキュリティが重要な柱となる。現在のところ，EDIによるデータ交換は，米国においては業界や，あるいは部分的には業界をまたがった標準ができあがっており，電子的なデータ交換が定着化しつつある。しかし，このようなEDIを実際に導入する場合にも，インターネットのようなオープンなシステムではなく，VANによる閉じたシステムとなっている。

米国ではVANの普及が1970年代であり，現在，米国ではVANとインターネットの中間をいくような運用形態がとられており，米国政府の調達（総額は20兆円といわれる）を実行するネットワークであるFACNETにおいては，政府の認定した25社のVAN業者の専用回線を通じて民間企業が調達に参入する方式となっている。

従って，今後，企業の境界をなくして，インターネットを通じて決済までも含めたデータ交換が実現するには，個人の商取引以上のセキュリティが必要となるため，場合によってはインターネットが保証している手軽さなどのメリットが失われる危険性がある。

決済システムの安定性を別の面からみた場合には，企業間の信用情報の伝播形態に大きな変化をもたらすことがある。電子マネーの導入にも，部分的にこの要素が含まれている。企業間

の取引を，例えば，現金や預金などの銀行での信用情報をもとにしないで，企業間での決済情報(例えば納品と支払いを相殺する情報の交換)により完結する場合には，１つの企業の倒産や経営不振が，中間となる銀行などのバッファを経由しないで，直接的に業界全体，あるいは極端な場合には，国の経済全般に波及してしまう危険性がある。

このような意味で，金融における信用の創造，あるいは身近には企業間の信用の形成，あるいはその担保がどのように確保されるかといった基本的な問題を含んでいる。

この問題に関しては，当面は銀行の信用情報(例えば預金総額)を基本として進行するが，インターネット銀行や一部の電子マネーで構想されている，通貨に相当する情報を自由に生成できるシステムのもとでは，架空に近い通貨が多量に発行されることになる。同様なことが，企業の信用取引を基礎として発生する可能性もあり，法的な規制はもちろん，金融システムなどを含めた根本的な指針作りが必要となる。

3．電子マネーの種類

既に別の箇所において，電子決済の概要を紹介した[1]。ここでは消費者がかかわる小口の取引を対象とする電子マネーについて特にセキュリティを中心に問題点を指摘したい。

都市銀行10行と地方銀行約60行は，2000年の電子マネーの実用化を目指して，共同実験を始めるという[2]。新聞報道でみるこの日本版電子マネーは，ICカードを使用したモンデックス型の方式を採用するようである。プリペイドカード，キャッシュカード，テレフォンカード以外にもさらにインターネット上のヴァーチアルショップへの支払いを可能にするものであるという。ビザ・インターナショナルがJAVAカードと呼ばれる多機能カードの開発に着手し，他方モンデックス・インターナショナルを中心として，日立製作所，米モトローラ，独シーメンスなど日米欧の７者と企業連合を結成し，98年はじめには世界各国で，多機能ICカードを商業化する[3]という計画がある。また最近では米サイバーキャッシュ社が電子決済サービスを始めるという報道もある[4]。

電子マネーとは何かであるが，大蔵省の「電子マネー及び電子決済に関する懇談会」の報告集は，次のような特徴をあげている[5]。すなわち同じく電子化といっても「決済手段の電子化」と「決済方法の電子化」に区別する。前者は，「貨幣価値の電子化」と説明され，利用者の保持する電子機器に記録されたデジタル・データがそれ自体「価値」を有し，これを交換又は増減することにより決済を行うものである。後者は，利用者が決済のための「価値」の移転を第三者に対して指図する場合にその指図を電子機器や通信機器を通じた電子的な方法により行うものであり，インターネットを通じた銀行振替やクレジット決済等がふくまれると説明している。電子マネーとは，前者の「決済手段の電子化」を意味するものとしている。ここではこの定義

1) 藤田昌也「マルチメデイアと電子マネー」『マルチメデイア環境と経済学』児玉・岩本編，1996年３月，時永祥三，「マルチメディア環境とプライバシイ」，『経済学研究』は，共同研究の成果である。そのため一部資料について，共用している部分があるが，それぞれの署名の論文について，それぞれが責任と著作権があることで合意している。

2) 『日本経済新聞』197年６月20日朝刊
3) 『日本経済新聞』197年５月16日朝刊
4) 『日本経済新聞』197年８月５日朝刊
5) 大蔵省「電子マネーおよび電子決算に関する懇談会」報告集，1997年５月

に従っている。

電子マネーの出発点は，インターネット上の安全な決済である。直接銀行口座から口座へと決済する危険を避けている。たとえばカードやファイルに「貨幣価値」を封じ込めて現金と同様な機能を持たせるというのも，いわばどの電子マネーもとっているように直接銀行口座にアクセスせずに，間接的電子的バリュウの間でのみ決済するというのも工夫の結果の一つである。それがあるタイプの電子マネーでは，ファイルの間で決済という形をとるし，また他タイプの電子マネーでは，ICカード間の情報の移転ということになる。しかし同時にこのことは決済の前払いを前提としなければならない。クレジットカードでは，決済は取引の後になり，取引と決済の間の期間は，カード会社が与信し，債務保証することになるが，電子マネーでは，何らかの電子的ヴァリュの発行を銀行の口座残高の減少と見返りに行ったとき，すでにユーザは前払いをしていることになる。クレジットカードを後払いによる決済というならば，電子マネーは前払いであり，いわば汎用性のあるプリペイドカードと同じことと理解することができる。電子マネーによる決済は，債権の譲渡である。

電子マネーは，媒体からみてネットワーク型とICカード型がある。前者はコンピュータのファイル上に前払いをして得た「価値」を持たせたもので，インターネット上においてのみ，バーチアルショップと利用者である消費者との取引の決済を行うものである。ICカード型は，ICカードに同様に「貨幣価値」を封じ込め，取引の決済は，一方のICカードーから，他方に価値を移転させることによっておこなわれるが，同時にインターネット上の取引の決済も，カードとコンピュータとの接続によって可能となる。

また決済の方法からオープン型とクロズード型の分類がある。オープン型は，取引において電子マネーを受け取った側は必ずしも発行主体に戻して現金化はせず，次々と電子マネーが移転してゆく。クローズド型は決済の度に電子マネーは，発行主体に戻り，現金化・預金化される方式である[6]。

	オープン型	クロズード型
ICカード	モンデックス	Javaカード
ネットワーク型	E-キャッシュ	サイバーキャッシュ

なお，（1）ネットワーク型，（2）ICカード型，（3）電子マネー型と分類することもある。（1）にはビザ・インターナショナルとマスターカード・インターナショナルによるクレジットカードをベースにした決済手段が，（2）には，IC－ドに個人情報も書き込むことができるビザ・キャッシュが，（3）には，モンデックスやデジキャッシュが分類されている[7]。

とくに話題になっているE-キャッシュとモンデックスを簡単に説明する。

E-キャッシュは，アメリカ・ミズリー州のマークトウイン銀行において，1995年10月より試行されている電子マネーである。技術はオランダのデジキャッシ DegiCash から提供を受けている。①買い手と売り手がマークトウイン銀行に口座を持つ。②口座開設と同時にE-キャッシュ専用の疑似口座 MINT を持つ。③MINT に預金残高の範囲内で，必要額の電子的バリュウを振り替える。④買い手は，必要に応じてMINT から電子的バリュウをハードデイスクに引き出す。⑤決済は，この電子的バリュウが，買い手から売り手へと，ハードデイスクからハ

6) 日立製作所・新金融システム推進本部編『電子マネー』1996年　日刊工業新聞社，p. 33)
7) 『日経流通新聞』97年5月15日

ードデイスクへと振り替えられことによって行われる。⑥通貨単位は，cyberdollar で米ドルとリンクしている[8]。

以上のようなE-キャシュは，パソコンからパソコンへ，email またはインターネットを通じて決済を行うために考えだされたものである。

決済は，基本的に，マークトウエン銀行の債務の振り替えによって決済が行われることになる。ただそれが直接銀行の口座から口座にふりかけが行われるのではなくて，いったん銀行の口座とは区別された疑似口座の間で振り替えられることによって，銀行口座は決済あるいはデータの改竄などの不正から保護されている。また後でも述べるように，デジタル署名の技術も利用されることになる。

この方式について問題点も指摘されている。この方式がユーザーにとって比較的なじみがないため，馴染むのに相当の時間を要するのではないかということ，及び，セキュリテイの問題である[9]。

モンデックスカードは，カード自身に貨幣価値を封じ込めることによって，持ち運びができるとともに，店頭での決済に使用でき，またコンピュータにつなぐことによって，インターネット上の取引の決済に使用できるように工夫されたものである。National Westminstar 銀行と Midsland 銀行および British Telecom が，一緒になって，Swindon において，1995年より試行されている。

そのモンデックス（MONDEX）の仕組みは，以下のようになっている。各国あるいはひとつの地域に通貨の中央銀行がひとつあるように，オリジネータがひとつあり，そのオリジネータのみがモンデックスマネーを生成，消滅することができる。メンバー銀行は，必要に応じて預金・現金を提供することによって，オリジネータより等価のモンデックスマネーを得る。交換したモンデックスマネーがあまれば，その都度返却して，預金を返済してもらうことが可能という[10]。消費者は，銀行口座から ATM，公衆電話などをとおしてモンデックスバリュを，IC カードにチャージし，商品の購入などに使用する。小売店は受け取ったバリューを，「ワレット」という機器を使って，他の支払いに使用することもできるし，また後日銀行で決済することもできる。当然さらにまたコンピュータとつなぐことによって，インターネット上の取引の決済が可能となる。

他のシステムでは，カード上のデータは単なるプリペイドマネーの取引データであり，電子マネーというよりカードをもちいた電子的決済であるが，モンデックスシステムは，電子的バリューを保有する現金と同じ「電子的財布」であり，通信機能を兼ね備えることによって現金の欠点も補うものであるという[11]。消費者と商店のみならず，個人の間においても携帯用の「ワレット」を通して授受が可能という。

4．認証の技術と保証

電子マネーが普及するには，上述のようにコスト負担が重要であるが，さらに他方で安全性

8) 日立製作所・新金融システム推進本部編，前掲書，pp. 97-99，インターネットアドレスhttp://www.digicash. com/

9) 田中辰雄，「現金型がいずれ主導権をにぎる」『エコノミスト』，'96. 8. 6

10) 日立製作所・新金融システム推進本部，前掲書，108頁

11) 日立製作所・新金融システム推進本部，前掲書 109頁

などセキュリテイの問題がある。

電子マネーが，「マネー」として機能するには，少なくとも2つの要件がみたされなければならない。ひとつは交換手段として「価値」を持つということである。2つには，「偽物」ではないという保証である。第1の問題は先に述べたように電子マネーがすでに前払いされている一種のプリペイドカードであるということ，換言すれば債権証票であるということによって保証されている。もう一つの要件は，磁気式媒体はコピー・改竄が容易であるため，予防するための方策がとられていなければならないということである。

電子マネーは，磁気媒体を使用するため，データーの改竄やコピーは容易である。これを防ぐには，発行時に電子マネーに「貨幣番号」をしかも，発行体のデジタル署名を付し，ユーザーに譲渡するとともに，発行体に登録し，取引後に毎回発行体にもどし，電子マネーの動きを追跡することである。そのためにはデジタル署名解読の暗号の工夫とともに，電子マネーの追跡によって改竄とコピーの予防することができる。

しかしこのチェック方法にも問題はある。一つはこの方法を成功させるためには，電子マネーを追跡しなければならないが，そのためには取引の内容を発行体が知るところとなり，プライヴァシーが守られないからである。

プライヴァシーの確保は，デジキャッシュの場合は次のようになされている。電子マネーは，受け取られると発行体たる銀行に戻され，貨幣番号がチェックされる。したがって当然受取人の情報も銀行が知ることになるというのは上述のごとくであるが，もし銀行が貨幣番号を追跡していたら，同時に支払人の情報も知るところなる。そこでプライヴァシーを守るため，デジキャッシュを発行する場合，貨幣番号をユーザが作成し，一定の関数で変換して，内容がわからないまま銀行がデジタル署名する（ブラインド署名）[12]。そして貨幣番号が前もって登録されず，受取人から銀行に戻されると登録し，重複チェックをすることによって，電子マネーのコピーなどの不正の防止をすることができる。電子マネーの受取人を銀行は知ることになるが，支払人の情報はわからない。

しかしこの方法にはコピーされた電子マネーを受け取る可能性をゼロとはしない。そのときコピーされた電子マネーを受け取った人に対する保証はどのようにするのかである。重複した貨幣番号を無効とするこのような予防策は，コピーの意欲を削ぐものではあるが，通常の取引によってコピーされた電子マネーを受け取ることを皆無とするものではない。

他方で取引ごとに貨幣番号を追跡してゆく方法は，かかる問題を避けることはできる。したがってプライヴァシーを守るか，コピーを予防するのかの選択はされなければならないことになろう。

さらにICカードに「貨幣価値」を閉じこめる方法も，取引ごとに発行体に電子マネーが戻り如上の管理が可能であれば問題は生じないが，電子マネーが次々と譲渡されてゆくオープン方式では，データ改竄の危険性は十分ある。

ICカードをつかうモンデックスは，つぎのような予防をしている。それはICカードそのものに暗号化された電子署名が前もって書き込まれることによって，カード相互が譲渡時に確認しあうとともに，相互のデータ交換そのものも

12) インターネットアドレスhttp://www. digicash. com/publish/digibro. html 1997/06/02

デジタル署名されており，その解読の鍵もすでにICに組み込まれることによって，「価値」が移動するに際してチェックが働くのである。さらにそれでもなお暗号解読にたいする対策として，暗号の構造を解読に相当の時間を要するようするように工夫するだけではなく，定期的に暗号自体を変更してゆくという方法によって対処している[13]。

電子マネーの「価値」や改竄などの問題はこのように，技術的には，解決の方策が考えられている。

以上のような電子マネーに種々の工夫されたからといて，それによってヴァーチアルリアィティの取引の安全性が確保されるというものではない。さらに電子マネーを使用するインターネットという不可視の市場で，取引そのものを成り立たせる条件を作り上げなければならない。電子マネーはその結果の決済手段であり，自ずと問題が異なる。

それはセキュリテイの確保である。その内容は，①情報の送り手と受け手の存在の認証(Authentication) ②情報に改竄のないこと(Integrity) ③プライヴァシイの確保(Privacy) ③支払いの保証（Non-repudiation）である[14]。

とりわけ通常の取引おいては，無関心であった情報の送り手と受け手のアイデンテイテイの確認の手続きは多くの示唆を与えてくれる。この確認を認証という。認証の持つ意味を分析する前に，ヴァーチアルリアリテイ市場における認証の方法を紹介する。

認証は暗号技術を利用してなされる。認証に使用される暗号技術の種類は，一般的には（1）共通カギ方式と（2）公開カギ方式の二種類に大別される。

共通カギ方式は，発信者と受信者が同じ暗号カギ（共通カギ）を共有して暗号化（をかける）と複号化（元に戻す）する方式で，代表的なものとしてDES（共通カギ方式の代表で米国の標準方式）や，FEAL（NTTが開発した共通カギ方式の暗号技術）がある。

共通カギ方式は，70年代半ばまでは暗号技術の中心であったが，共通カギを秘密にして管理しなければならないことや，不特定多数との通信を行うには，多数の共通カギを持つ必要があるなど，不都合があった。

一方，公開カギ方式は，暗号化カギと複号化カギが異なり，Aあてに送るのに公開されたAの公開カギで暗号化して送信し，AはAだけが持つ秘密カギで復号化する方式で，復号化カギを多数の人に配ることなく，不特定多数との通信に利用できるものである。

同一組織内に限定して秘密に使用されていた暗号が，情報ネットワーク社会の信頼関係を築くために公開的共通基盤技術になったのである。また秘匿を主な機能としていた暗号が，それとあわせてヒト・モノや情報の真正性を保障し，情報に信用を付与し，情報財流通を促進するため認証機能，すなわち署名・改竄防止の機能をもつこととなった。

そのメカニズムはつぎのようになっている[15]。認証機関CAは自分の公開カギ暗号系を設定する。すなわち認証機関CA用の秘密カギと公開カギを定め，公開カギを全ユーザーに公開する。各ユーザは自分のID（たとえば氏名，社会保険番号）と公開カギ番号をひと組みにしCAに登

13) 日立製作所・新金融システム推進本部編，前掲書，162-165頁
14) About GTE Cyber Trust, http://www. cybertrust. com/about/AboutCT. html, 07/18/97 00: 44: 14
15) 辻井重男『暗号』講談社，1996年4，121-122頁

録する。その際CAは，もとより身分証明書やパスポートなどの提示を求め偽名登録を防止する。

認証機関CAは，登録されたユーザーの「ID公開カギ」を，CAの秘密カギで署名する。CAのお墨付きである。だれでもあるユーザーにたいするCAによる署名（お墨付き）を公開カギで検証することができる。

認証は次のようになされる。送りたいデータや文章に署名を付けたい場合，それらに秘密カギを作用させて署名文を作成する。その署名分を受け取ったヒトは，署名したヒトが公開している公開カギをその署名文に作用させて署名が本物であることを確認する。あるいはデータそのものを暗号化して送る場合も同じである。

署名人が公開している公開カギで，そのような意味のある文章に戻せるのはその公開カギに対応する秘密カギで署名したからであり，その秘密カギは署名者のみの秘密であるから，本人確認ができたことになるということである。

送る側をインターネット上のヴァーチアルショップ，受け取る側を消費者とおきかえると，以上のことはより理解できる。消費者は公開カギを利用して，ショップを確認することができる。反対に消費者は自らのIDを，公開カギを利用して暗号化する。ショップは，秘密カギをつかって本人確認することができるということになる。注文の中身の確認やクレジットカード番号あるいは上述の電子マネーもかかる暗号技術を利用して決済することができる。

問題は，どこから消費者はこの公開カギを得るかである。ショップはまえもって認証機関CA（Certificate Authority）に登録するとのべたが，消費者は，この認証機関に照会して，デジタル署名をした公開カギを得ることになる。あるいはインターネット市場そのものが，認証機関によって組織され，出店しているショップは，一定の手続きを経て参加することで認証をうけることになるので，そのインターネットアドレスにアクセスすることによって公開カギを得るということもある。

この認証はつぎのような比喩で表せる[16]。公開暗号方式において秘密カギによる署名を手書き署名とすると，公開カギによる署名の確認は，受取人による署名（本人しか書けない＝秘密）をパスポートにおける署名（公開されている）によって確認することと同じである。判子を押すことによってできた印影を，印鑑証明で確かめることは，本人しかもたない判子（秘密）を，印鑑証明という公開カギで突き合わせることと同じである。

公開カギの使用は，当然暗号破りがあることを前提しなければならない。これに対処するため，コンピュータにより暗号化(秘匿)，複合あるいは署名，検証を高速に行なうとともに，不正な解読，改竄にたいしてはいかにコンピュータを駆使しても計算が爆発に膨大になるように暗号装置を設計されている。[17]

この方式の代表的なものが，開発者の三人の頭文字をとったRSA（77年にRivesti Rivest, Shamir, Adlemanの三人により開発された公開カギ方式の暗号技術）である。現在，インターネットでの取引に関するセキュリティー確保の大半は，この方式を利用している。また，方式の原理を利用して，取引した事実を否認できないようにするデジタル署名の技術も開発されている[18]。

16) 辻井重男，前掲書　108頁
17) 辻井重男，前掲書　97頁
18) 日経金融新聞　96/7/26

人工現実世界（ヴァーチャルリアリテイ）の一種の不可視性から不正を防ぎ，情報の価値を保障する技術，それが暗号を中心とする情報セキュリテイ技術である[19]。

認証は単に情報の論理整合性ということにとどまるものではない。秘密カギと公開カギとの照応が，一方の方向で秘匿に，他方で認証として役立つことは述べたとおりである。しかし公開カギを使用する者その者が，存在するのかどうか，一致するのかどうかはわからない。公開カギで暗号化されたものが，秘密カギで復号化されるからといって，公開カギを知っているということであって，架空の人間であり得る。インターネットで注文して，商品を受け取ったが，支払いがないということはあり得る。反対に秘密カギで署名してどの相手にも公開カギで検証させるからといって，信用があるというわけではない。前金をうけとってそのまま商品を送らないとか，クレジットカードの番号を悪用する場合もある。したがってこの認証をも認証機関CA（Certificate Authority）が与えなければならない。

コンピュータあるいはICカードの本来の所有者かどうかの確認は，技術の開発の結果たとえば指紋の照合する事によっても可能になりつつある。すなわちインターネット上の仮想商店街ならば，認証機関が個人の暗証番号を発行する。ICカードにはこうした個人情報や指紋データを入れておく。読み取り機にカードを差し込んで，同じ指を読み取り台に乗せれば本人かどうか判定したり，例えば銀行と企業のパソコンを回線でつなぎ，送金する場合，まず送金先と金額を決め，ICカードと指紋で本人確認を済ませれば，オフィスにいながらにして作業が始まるというわけである。印鑑は紛失しやすいが，指紋なら紛失することはない。印鑑を偽造して振り込ませるといった犯罪も防げるというわけである[20]。あるいは筆跡による確認さえ考えられている。パソコンに接続した小型電子入力板（タブレット）にサインすると，筆跡だけでなく，筆圧や書くスピードを登録済みの署名と照合し，本人かどうか確認する。暗証番号だと盗まれたり忘れてしまう恐れがあるが，これならその心配がないというわけである[21]。

以上のように認証という手続きすなわちIDの確認という手続きは，電子取引においてはきわめて重要なものである。通常の場合においても認証手続が必要な場合もあるが，可視的な世界では可視ゆえに当然のものとして前提にしていたものが，不可視の世界で改めて確認されなければならなくなったということであるが，その手続きにきわめて興味深い論理を見出すことができる。つまりヴァーチアルショップの加盟企業は，認証機関に自らの名前や社会保険番号など，他と区別されるユニークなものをもって認証機関に登録し，その登録されたものを開示することによって認証されるということである。認証の過程をたとえて，公開暗号方式において秘密カギによる署名を手書き署名とすると，公開カギによる署名の確認は，受取人による署名（本人しか書けない＝秘密）をパスポートにおける署名（公開されている）によって確認することと同じであるという比喩は妙を得ている。すなわち個別性がチェックと登録（Register）と開示（Oeffentlichkeit）を経てはじめて個別性として認知されるのである。機関による登録と開示

19) 辻井重男，前掲書，80頁

20) 日経産業新聞 96/7/18

21) 日経産業新聞 96/7/18

を経なければ個別性が個別性として成立しない。これが認証の論理である。

そして重要なことはここでの認証は当然取引主体としての認証である。したがって支払不能に陥ったりあるいは詐欺・不正が生じることがあれば当然認証機関が保証すべきものであるということである。電子マネーの展開のための環境整備はもちろんであるが，認証に伴う補償問題も整備しなければならないのではなかろうか。たとえばヴァーチアルショップへの出店に際しては，デポジットをとるとかあるいは損害保険のような仕組みにするなどの工夫が要せられるのではないかと思われる。

以上のようにインターネットの取引においては，かかる認証サーヴィスがきわめて重要となるが，この認証の手続きが，重要になるにつれ，認証サービスの市場も拡大する。この市場をめぐって日米間で，この電子商取引の中核となる電子認証サービスの主導権争いが激しさを増している。たとえばインターネット上での電子商取引で，本人や相手先を確認する認証サービスのベリサイン（カリフォルニア州）は1996年2月，日本電信電話（NTT）の子会社三社と共同出資で，日本ベリサイン（東京・港）を設立した。またGTEは，ソフト開発会社BUG(札幌)と組んで，1996年夏頃より，日本法人を設立し，認証サービスに参入するという動きがあった。日立製作所，富士通，NECの三社が国内初の認証会社を1997年10月にも設立することで合意した[22)]。

インターネット上の電子決済方式の世界ではいま，二つの手法が大きく対立している。米ビザ・インターナショナルなどが最終案を発表する予定の米国生まれの「SET（Secure Electronic Transaction)」と，日立など三社が国内の電子商取引実験で推進する「SECE」だ。

しかし他方で認証コストを回避するため，認証そのものを回避するシステムの開発する努力もある。

三菱総合研究所が実験開始を予定しているEC実証実験「スマートカラークラブ」では“ツケ払い”の感覚で少額決済に対応できる収納代行方式の決済システム構築を目指しているのがその例である。特徴は認証局を省いた構成だ。インターネット上に仮想銀行を構築。東京三菱銀行や第一勧業銀行の銀行口座を持つ消費者が仮想銀行の口座に買い物代金を“ツケ”でプールしておき，一カ月に一回程度の頻度で精算する。「その都度，消費者の身元を認証局で確かめなくても，現実の口座情報を持っているため取りはぐれの心配は少ない」。認証局を置けば，それだけプロセスが増え，コスト増になることは目に見えているということである。電子空間上での認証サービス自体を否定する考え方だ。

以上のようなこれら様々な企業の参入，認証機関の競争は，その数だけまた電子マネーの数があるということになる。現金ならば1種類の十分であるのに，便利なはずの電子マネーは，複数種類を管理しなければならなくなる。何らかの方法で統一化しない限り，利用に煩雑さをもたらすことになるのではなかろうか。

5．電子マネーとその課題

5.1　電子マネーと実施主体

すでに述べたように携行型のシステムとしてはモンデックスシステムが先行している。しかし，この方式についても問題点がある。一つに

22)『日経産業新聞』96/7/18

は専用の端末が必要なことである。そのためのコストがかかるということである。この方式の特長としている個人から個人へとマネーが譲渡される場合も，その端末が必要とされよう。そしてそのコストをかけてまで，普及のインセンティヴがあるのかである[23]。単に店頭で現金の代用として利用することに限定するならば，なにもこのようなことを工夫する必要はない。

たとえばイギリスにおけるデビドカードあるいはスウィッチカードのようにそれぞれのショップの帳場に，銀行とオンラインでつながったカード読取器をおき，売り上げとともに，顧客のスウィッチカードを読みとらせ，顧客の銀行口座から，自分の口座へと，売上金額を振り替えれば決済はこれで十分である。これはむしろICカードに貨幣価値を封じ込めて持ち運びするより確実な決済の方法である。つまりはクレジットカードの決済期間の短縮化であり，銀行預金が保証の裏づけとなっている。もしこのようなことだけが期待されているならばスウィッチカードで十分である。あるいは現金の方が便利というということさえある。とりたてて電子マネーといったものは，不必要であろう。事実モンデックスカードは，現金の代用としては，それほど活用されているという風でもない[24]。

そしていずれを採用しようとも，電子マネーの普及にとってきわめて大事なことは，どの方式を採用するかで，コストが異なるとはいえ，どの段階で直接誰が負担するかである。電子マネーは，一般の消費者をユーザーとして前提している。そのユーザーが，コストを負担してまで電子マネーを使用するであろうかである。電子マネーは，一種のプリペイドカードであると述べたが，プリペイドカードは，通常割引されてあるいはある種の優遇が付加されて売却されている。たとえば1000円券ならば，1050円相当分のものが購入できるとかである。反対にクレジットカードは，後払いであるので，実質的には利子が手数料の名目で支払われる。このような経済上の慣例を前提にするとき，プリペイドカードたる電子マネーにたいして，ユーザーがコストを負担してまでも利用するかである。そういう意味では，ここでいう電子マネー以前のクレジットカードを利用した方式の方が，手数料の負担ということに関していえばユーザーとしては納得のいくものがあるのではなかろうか。

そうすると電子マネーの直接のコスト負担は，ヴァーチアルショップに出店の企業である。しかしその企業にとってはコスト負担は二重になる可能性がある。ひとつは出店認証の手数料の支払いであり，もう一つは電子マネーのコスト負担である。前者については従来のクレジットカード利用の場合と同じであるから馴染みやすい。しかし後者についてはなかなか理解しがたいものがあるのではないかと想像できる。さらに反対に認証機関がインターネットのヴァーチアルショップを組織し，出店企業を募集し認証手数料やランニングコストを徴収することに経営のインセンテイヴがあることは十分理解できるが，しかしそれとは別に電子マネーを発行するというインセンティヴがあるのかどうかという点についてみれば理解が困難である。電子マネーの発行体として，銀行が一番適当と思われるが，コストをかけて参加する電子マネーの発行そのものが，銀行にとって積極的に取り組む

23) 田中辰雄，前掲書
24) 日立製作所・金融システム推進本部，前掲書，121-122頁
25) 野口亘,「実用化で先行するビザ・マスターカード」『エコノミスト』，'96. 8. 6

メリットがあるのかどうかである[25]。

5.2 暗号技術と攻撃法

電子マネーの導入に不可欠なものとして暗号化の技術がある。暗号化技術は，軍事利用という暗い側面もあり，現在までさしたる注目もあつめていなかったが，電子的な取引の拡大やデータ転送に拡大にともない，現在では必須な技術となっている。

暗号化が果たす役割と認証システムにおける位置については，すでに3章で述べているが，ここでは，暗号化技術そのものの開発とその普及に関して課題とされている点を明らかにしていきたい。

現在，インターネットにおける交信の確保は主としてパスワードによりなされており，極めて多くのトラブルが発生することとなっている。その多くがパスワードの不正入手であり，悪用されるケースとしてはインターネットへの接続料金を他人の口座へ振り替えるなどの金銭に関連したものから，誹謗中傷にいたるものまである。この原因としてユーザは安易なパスワードの設定をすることが指摘されているが，常に初心者がいる状況では基本的な解決方法は得られていない。

暗号化の技術は，このような問題を基本的に解決すると同時に，より信頼できる交信手法を提供するものである。しかし，暗号化には，基本的に2つの大きな問題点が含まれており，この解決や社会的な合意がシステム導入の決め手となっている。

（1）攻撃法

暗号を解読する方法を開発することを，一般に攻撃法とよんでいる。攻撃法の基本は，繰り返し通信されるメッセージから暗号を割り出す技術であり，分かりやすく言えば，同じパターンで暗号を送信すれば，そのデータから暗号を作成する仕組みが分かることを指している。暗号化技術は，ほとんどの場合，送信すべきデータに代数的な操作を加えて送信し，これを受信してサイドで，この計算を逆に行うことにより，もとのデータを回復することができる。この代数演算の規則は，交信をする両サイドだけが知りえる秘密であるが，これをメッセージから見つけ出すのが攻撃法である。

攻撃法に関しては，日本の三菱電機のグループの研究が国際的にも評価されている。これによると，米国の標準となっている暗号化技術であるDES（Data Encryption Standard）についても，効率的な攻撃法（つまり有限の採算がとれる範囲でコンピュータで解読できる）が存在しており，暗号化がいかに難しい課題であるかを象徴している。

攻撃法に対抗する方法には，代数演算をする方法を複雑にする，送信したい情報に加える暗号部分を長大にする（現在では40ないし256ビット）などの方法が可能とされている。しかし，現実には，有限のコンピュータ資源を用いて経済活動に有用なデータ交信を保証する必要があるので，ある程度のリスクを含むものとなる。

従って，現状では，この経済性と複雑さのかねあいにより選択されることになる。現在，主流となっている56ビットの暗号化によるオーバーヘッドはその意味では，適切な基準となっている。現在ではDESを多重化するなどの範囲での対策が考えられている。

（2）輸出禁止措置

暗号化技術で世界をリードしている米国では，その主たるユーザが国防省であることから，暗号化技術を実現するソフトウェアを海外に販売

することを禁止する，いわゆる禁輸措置がとられてきた。暗号化技術が米国以外の国にもれることにより，米国の国防上の秘密や文書を解読される危険性が増大するというのがその理由である。しかし，1997年になって，この禁輸措置を一部解除する方針が示され，その意味で，暗号によるセキュリティ技術の普及に１つの弾みがつくことになった。

しかし，暗号部分の長い暗号技術については禁輸措置が解除されておらず，日本のNTTによる暗号の開発など，独自技術に依存せざるを得ない面をもっている。

（3）clipチップ

米国の暗号化技術のもう１つの側面として，ここにあげるclipチップの導入問題がある。米国政府の計画として，すべての情報機器にこのclipチップを装着させ，情報の入出力のたびにこのLSIによるハードウェア的な暗号化と復号化を行わせることが提案されてる。ソフトウェアによる暗号化よりは演算速度が向上することや，clipチップにより簡素化できることがあげられている。しかし，このclipチップには，暗号化そのものより重大な問題が含まれており，これが導入への障害となっている。政府の計画では，clipチップに含まれる暗号化の方法（アルゴリズム）は政府だけは特別に入手できる権利が保証されている。これは，マネーロンダリングなどの不正行為を防止する目的で，捜査権限の範囲で政府が担保できるとする理由による。

しかし，現実には，民間利用だけではなく，国を越えて技術が導入された場合には，国家間の情報解読に対する不均衡が生じることになる。

(4) ICカードの耐タンパ性

これまで述べたきた事項が，いわばシステムのソフトウェア面の問題であったのに対して，ICカードの機能そのものからデータの不正使用をはかる問題が存在している。簡単にまとめれば，ICカードを製造しているプロセスを逆にたどることにより，チップに格納されている暗号や符号化の部分を解読し，これを不正に使用することである。このようなICカードをいわば解剖していくことをタンパリングとよび，これに対応できる能力を持たせることを耐タンパリング，耐タンパ性と言う。もともと，ICカードは一世代前のLSI技術を使用していると言われ，それだけ構造を解明する可能性は高いと言われている。

このICカードを製造しているプロセスを逆にたどる技術は，化学反応により皮膜を剝がすなどの初歩的なものから，電子ビーム照射による信号のトレース，あるいは故障診断時の信号を送信することにより内部構造の解明などの及んでおり，費用と時間とをかければ，それだけ性能の高い解読が可能となる。

問題は，このような逆技術をどこまで防ぐか，あるいは直接的にはそのような機能をもつICカードのコストの増加をどこまで許容するかの問題となる。現在でもICカードの信頼性は必ずしも高いとは言えないとされており，今後，より耐タンパ性のある製品を開発する必要がでてきた場合には，多量に流通されるべきICカードのコストは，市場性をはるかに越えるものになるであろう。

現在，すでにいくつかの機関や個人により解読がなされたとのデータもあるし，経済事件の場合には，最近では国も関与するような大がかりな犯罪に発展する可能性もあるので，安易に見過ごすことはできない。問題は，どの程度の精密さや堅固さでICカードを製造すべきかといったことであるが，データが少ないうえに，

いったん事件が発生した場合には極めて大きな社会的影響をもつことから，見積もりが難しいのが現状である。

従って，現状ではテレフォンカードなどの小額のICカードにより実績を作った上で，徐々に適用範囲を拡大していき，これにともない，ICカードの流通方法（例えば，頻繁に製造工程を変更する，カードを確実に回収するなど）が確立されていくと考えられる。

5.3 認証機関の構成

電子鍵を使ったデータ交信を保証する機関として，いわゆる認証機関を設けることが提案されている。現在，通産省の実験システムや福岡市における実験プロジェクトでの小規模な認証システムが計画されている。この認証機関を誰が，どのように運用するかが1つの課題となっている。部分的，あるいは実験的なシステムでは，小規模な機構ですむが，全国規模の取引となる場合には，公的なシステムであるか民間によるかは別として，社会的インフラともよべるようなシステムが必要となるであろう。しかし，このような社会的な合意形成がなされるには，あまりにも施行から浅い年月しか経過しておらず，現実的には個別的に認証機関を構成することになる。

従って，いくつかの実験システムでは，電子商取引を行う主体であるデパートとか販売業者がみずから認証機関となっている例が多い。ここで，認証機関がどのように定義され，運用されるかについて，現在までの消費者のプライバシー保護のありかたとの関連で，整備されるべき課題があげられる。

現在，日本において消費者金融の膨大な個人データが不正に引き出される事件が相次ぎ，6年間で85万件に達しているとされている。消費者金融の機関で構成されている全国信用情報センター連合会には，すべての顧客の借入額や債務残高，勤務先などの個人情報が格納されている。これを利用できるのは，本来，構成メンバーである消費者金融の機関に限定されているが，銀行などが入手できない仕組みとなっている。しかし，現実には，銀行を経由して銀行の顧客など広い範囲に個人情報が漏洩している事実がある。

漏洩のルート，方法の詳細は省略するが，電子マネーの場合には，負債でないにもかかわらず，個人の購買記録がすべて残る仕組みとなるため，個人に関する膨大なデータが蓄積されることになる。この中には，債務などの，いわゆるブラックデータだけではなく，個人の日常生活に関連する情報が多く含まれるため，その処理方法には本格的な法体系をもってのぞむ必要がある。

認証機関はこのような個人情報のすべてを記録する必要もないが，認証機関と実施主体が同じである場合には，必然的に個人情報の集積がなされ，同様な問題が発生する可能性がある。

このような個人のプライバシー保護の課題については，やや範囲を外れるので省略するが，例え法律は制定されても，利用拡大が新たな法規制を生むといった関係にあり，かなり長期間にわたる問題となる。

5.4 ハードウェア構成

電子マネーの導入にあたって，ほとんどのケースでICカード方式による読み取り，あるいはATMからの金額情報の移動の方式を採用している。インターネット上で通用する通貨を使用する場合もあるが，これもICカードによ

る消費市場での延長上で考えられている。このように，ICカードおよびその読み取り装置を前提とした運用形態では，多数の簡易型の端末を前提とせざるをえない。このことが，システムのセキュリティに一定の限界を与えることも予想できる。

具体的には，企業内LANやWANの構成で用いられるワークステーションの階層的な配置を前提としたファイアーウオールなどの厳密なセキュリティシステムではなく，ICカードレベルの機密保護あるいは認識システムを前提とせざるをえないことになる。セキュリティ面での防護対策と，これを破ろうとするサイドの技術の攻防については，よく言及されるところであるが，ICカードにおいても，完全な防護が可能なわけではない。いずれ，不正使用の技術が開発されることになるであろう。

CAのサイドで行われるシステム上の防護措置としては，メインシステムに格納された暗号鍵などのユーザ情報を外部からの侵入に対して防護することが主たる任務となるであろう。これ以外の，例えば，商店でのカードの不正使用を監視するなどの機能を実現するには膨大な費用と人力を要するであろう。

このような意味でも，すでに述べたような障害や不正使用に対する保険機構を設けることが必要となるであろう。

6．まとめ

本論文ではネット上での取引の有力な手段とされている電子マネーについて，その実現技術，社会的制度を中心に，現状と解決されるべき課題について述べた。具体的には電子商取引に現状，電子マネーの実現方法とその特徴について整理し，認証の必要性とその論理について述べ，社会的な保証されるべきポイントについて展開した。また，これらを総合して，電子マネーと認証技術に関して，現在解決されるべき課題とされている点を整理した。電子マネーが社会的インフラとして確立するには時間が必要であろうが，ICカード製造や高度なセキュリティの確立など技術的な課題とならんで本格的な金融政策の提示が必要であることを指摘した。

現状では，電子マネーは実験段階であるとの認識がもっぱらであるが，最近，大手のクレジット会社であるVISAとMASTERカードがインターネット上での決済プロトコルを共通化するなどの進展が見られ，また，日米の政府により持続的に電子的取引全般への強い関心とプロジェクトの実施がなされるなど，具体的な運用を視野に入れる必要があることを示している。今後とも実態を踏まえ分析を続けていきたい。