日本大学大学院総合社会情報研究科紀要　No.6, 335-346 (2005)

電子マネーの決済適用領域

大嶋　一慶
日本大学大学院総合社会情報研究科

Application of Electronic Money to Payments

OSHIMA Kazuchika
Nihon University, Graduate School of Social and Cultural Studies

Advances in information technology in the late 20th century brought about rapid and widespread use of the Internet. Facilitating communication through the sharing of information beyond boundaries of time and space, and with its widespread business application, the Internet accelerated the progress of the IT Revolution.

The expansion of the e-commerce market led to the development of electronic money as a safe and efficient means for making payments and settlements across the Internet. Electronic money is expected to be used for small-sum payments as the entire process can be completed off-line.

By contrast, the payment and settlement system using credit cards, which are already accepted as 'access' products, is also expected to advance into the small-sum payment area, just as electronic money, as it gradually shifts to 'IC credits'. This means the application of these two different payment systems will overlap in the small-sum payment area.

This paper shows that the same level of security is enforced for both electronic money and IC credits, and therefore, these services do not differ in terms of security. And yet, the paper further shows that electronic money is superior to IC cards in making small-sum payments and settlements.

Ⅰ. はじめに

20 世紀後半からの情報技術（Information Technology 以下、「IT」）の発展は、インターネットの急速な普及をもたらすと共に、それが持つ時間、空間を超越するコミュニケーション能力とビジネスとの融合を果たすことで、IT 革命が進展した。これによる電子商取引市場（Electronic Commerce 以下「EC」）の拡大は、ネット上でも安全且つ効率的な決済手段として電子マネーを出現させた。電子マネーにおける決済処理は、従来のアクセス型決済手段に比べホストコンピューター間通信、与信処理等が不要になり、全てオフライン処理にて完了するため低額決済領域への適用についても期待さる決済手段である。

一方、アクセス型決済手段として一般へ定着化を見せるクレジットカード決済においても磁気ストライプカードから IC カード化へと移行が進むことで、電子マネー同様にオフライン処理が可能な IC クレジット決済が姿を見せている。これにより、両決済手段では、低額決済領域において適用領域が交わることが想定される。

本稿では、まず電子マネーを構成する様々なセキ

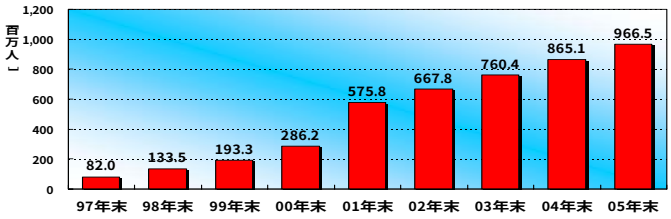
ュリティの内、主要なセキュリティ要素である暗号技術、IC カード技術における適用方法について解説を行う。また、IC クレジットにおいて決済手順、セキュリティ状況を明確にする。これにより両決済手段において同様のセキュリティ要素が適用され、安全面で同等レベルを確保可能であることを示す。その上で、電子マネーが IC クレジットに比べ低額決済領域に優位性のある決済手段であることを明確にする。

Ⅱ. インターネットの発展と電子商取引の拡大

20 世紀後半からの情報技術（Information Technology 以下、「IT」）の発展は、産業革命以来の工業化社会から情報化社会へと社会構造に劇的変化を与え、いわゆる IT 革命を巻き起こした。IT 革命を巻き起こした主要因は、情報端末（デスクトップ PC、モバイル通信端末等）の高性能化、大容量化の技術革新、及び通信インフラの高速化、大容量化はもとより、これらそれぞれの技術を融合させ世界規模のネットワーク化を可能としたインターネット技術の出現とその急速な普及に大きく起因する。

インターネットは第二次世界大戦後、通信手段確保のための米国軍事目的で開発された「分散型通信ネットワーク」概念に基づく通信ネットワークであるが、1969 年 11 月 21 日に米国 4 大学（UCLA、UCSB、スタンフォード、ユタ）の大型コンピューター接続による公開実験がその始まりとなる。[1]

インターネットの最大の特徴は、異種コンピューター間通信を可能とする TCP/IP プロトコル（Transmission Control / Internet Protocol）を採用することで 1 つのネットワーク、即ちインターネットに接続された全世界のコンピューター間通信を可能にする世界規模のネットワークの構築を実現化したことにある。この世界規模の一大ネットワークの実現により、インターネットはこれまで成し得なかった時間、空間を超越する世界規模の情報共有とコミュニケーション能力を具現化した。世界のインターネット利用推移と予測を以下の図 1 に示す。



［出所］
財団法人インターネット協会『インターネット白書 2004』**インプレス**, 2004 **年** 7 **月** 11 **日**, p.370.

図 1　世界のインターネット利用数推移と予測

世界のインターネット利用者数は、2003 年末において 7 億 6,040 万人に達しており、2005 年末には、9 億 6,650 万人に到達すると予測される。2000 年末から 2001 年末にかけて極端な伸びを見せたが、その後は年 1 億人前後の増加分で順調に推移していることが分かる。

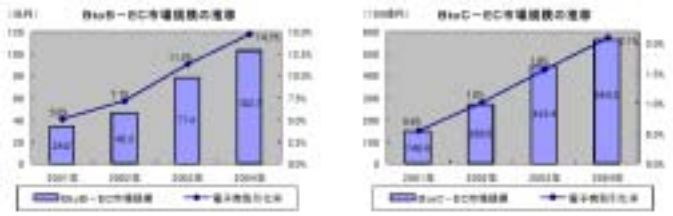
しかしながら、インターネットの一般への普及だけでは、情報共有、コミュニケーション手段の充足に過ぎず IT 革命が経済、社会構造を変革するものには成り得ない。インターネットの急速な普及と一般への浸透が推進力なり、ビジネスと融合することではじめて情報化社会への変革、つまり IT 革命が成し得るのである。

インターネットと融合したビジネスは一般に「e ビジネス」と呼ばれ、それらは主に電子商取引（Electronic Commerce 以下「EC」）によりビジネスを展開することで、情報交換や流通コストを劇的に低下させ少量生産、商品、情報のパーソナル化、需要に応じた生産、消費者優位を実現化する。

EC 市場の成長は、我が国においても着実な伸びを確認することができる。以下に経済産業省、次世代電子商取引推進協議会、NTT データ経営研究所が共同で実施した『平成 16 年度電子商取引に関する実体・市場規模調査』から B to B-EC（企業間取引）、B to C-EC（企業-消費者間取引）市場規模の推移と、調査結果概要をそれぞれ図 2-1、図 2-2 に抜粋掲載する。[2]

[1] ：上村賢治「情報処理論Ⅰ」日本大学大学院総合社会情報研究科, 1999 年．その他文献による。

[2] ：本資料は、経済産業省ホームページから入手可能。
<http://www.meti.go.jp/press/20050628001/20050628001.html>



注）調査対象は、VAN・専用線等の従来型EDIを含む広義のBtoB-EC（企業間電子商取引）、インターネット技術ベースの狭義のBtoB-EC（消費者向け電子商取引）、モバイルBtoC-EC、さらにCtoC-EC（ネットオークション）も対象に含める。

【出所】

経済産業省,"平成 16 年度電子商取引に関する実態・市場規模調査", 28 Jun. 2005, <http://www.meti.go.jp/press/20050628001/20050628001.html>(22 Sept. 2005)

図 2-1　日本の EC 市場規模の推移

① 狭義の B to B-EC の市場規模は 102 兆 6,990 億円と前年比 33%増となっており、100 兆円の大台を突破した。これまで先行していた「自動車」、「電子・情報関連製品」の占める割合が減少し、幅広い品目・業界で EC 取組みが拡大している。

② 幅広い品目・業界における拡大動向として、「従来型 VAN・専用線から IP が主流に」「中小企業の利用環境の向上と利用拡大」「間接業務の IT 化と B to B の連動」の大きく 3 つの動向が見られる。

③ VAN・専用線などの従来型EDIを含む広義のB to B-EC の市場規模は、約 191 兆円となっている。このうち、金額規模で半分以上をインターネット技術ベースの狭義の EC が占めている。

④ B to C-EC の市場規模（モバイル含む）は、消費者に具体的なメリットを提供したネットショップが、消費者からの支持を得ており、その傾向は顕著になりつつある。たとえば、ブログ等を活用したきめ細かな情報提供や、24 時間以内発送、送料無料等、付加的なサービスの提供を通じて、消費者からの支援を得ているショップが増加する傾向にある。

⑤ また、消費者にとって「密着性の高い」携帯電話と連動した、高付加価値サービスに対する支持が拡大している。たとえば、大手航空会社や一部のバス会社による、携帯電話を利用したチケットレス搭乗サービスなど、単に「取引を電子化」するのみならず、携帯電話と連動した「サービスの電子化」に対する支持が拡大しつつある。その結果、B to C-EC 市場規模は、5 兆 6,430 億円と前年比 28%増加した。

⑥ モバイル EC においても、着うたサービスへの支持や、若年女性による衣料・アクセサリー等の物販の拡大等により、モバイル EC 市場規模は、9,710 億円と前年比 25%増加した。

⑦ C to C-EC の市場規模は 7,840 億円に達していることが分かった。これは B to C-EC に比べ 14%の規模であり、物販系 B to C-EC のどの特定品目よりも大きい規模となっている。

【出所】

経済産業省,"平成 16 年度電子商取引に関する実態・市場規模調査", 28 Jun. 2005, <http://www.meti.go.jp/press/20050628001/20050628001.html>(22 Sept. 2005)

図 2-2　日本の EC 市場規模の調査結果概要

上記調査結果概要①③からは、インターネット技術ベースである狭義の B to B-EC 市場規模が前年比 33%増（102 兆 6,990 億円）の高い伸びを示し、その市場規模が広義の B to B-EC 市場規模（約 191 兆円）の半分を超えたことからインターネット利用拡大、浸透による市場規模拡大を窺うことができる。また、①②からは、その浸透が特定業種から幅広い品目、業界へと利用範囲を拡大していることも窺うことができる。

一方、B to C-EC 市場規模においても⑤より前年比 28%増（5 兆 6,430 億円）の高い伸びが確認できると共に、⑤⑥からは生活に溶け込んだ携帯電話との連動等、高付加価値サービスに関する消費者支持の高揚。⑦からは消費者間取引である C to C-EC 市場規模が全体の 14%（7,840 億円）の規模に達している等、インターネットの一般への浸透が EC 市場規模の拡大をもたらしていることを窺うことができる。

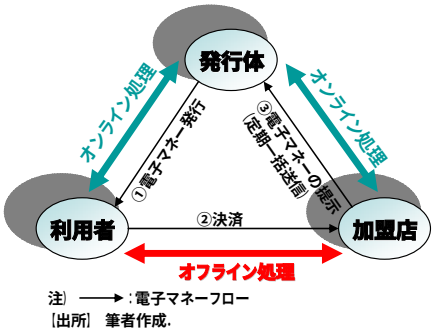
上記の通り、インターネットの普及と一般への浸透は、EC 市場規模の拡大をもたらしていると共に、今もなお成長させている。この EC 市場の成長を今後も支え、促進させるためにはネット上でも安全かつ効率的な決済手段が必要不可欠であり、それを担うものとして現在最も注目を集める電子決済手段の 1 つが、次世代通貨「電子マネー」である。

Ⅲ. 電子マネーのセキュリティ

(1) 電子マネーの決済フロー

電子決済手段には、ネットワークを介すことで遠隔地から預金口座に対し支払指示を行う従来型の決済手段であるアクセス型と電子的価値(金銭的価値)を保有者自身で保有・管理し取引の際、直接電子的価値を取引先に引き渡す自己完結型の電子決済であるストアドバリュー型に大別することができる。電子マネーにおいては、後者のストアドバリュー型として認識されるのが一般的である[3]。電子マネーにおいては、ストアドバリュー型電子決済手段の特徴に見られるように取引の際、当事者間で電子マネーの引渡し、いわゆるオフライン処理(ネットワークを介在しない処理)の実現によって決済が自己完結される。

従来型の電子決済手段であるアクセス型においては、決済の都度ホストコンピューターとのオンライン接続(ネットワーク接続)を行うことで本人確認や与信等、必要な処理が実施される。それに対しストアドバリュー型電子決済手段である電子マネーにおいては、暗号技術や IC カード技術を採用し、セキュリティを十分に確保することで、オンライン処理を不要とした決済処理即ち、当事者間で完結するオフライン処理を実現している。オフライン処理の実現は、これまでオンライン処理に費やされた通信コスト、ホストコンピューター処理コストの削減を可能とするものである。電子マネーの決済フローを以下の図 3 に示す。



注) ⟶ :電子マネーフロー
【出所】 筆者作成.

図 3　電子マネーの決済フロー

電子マネーの決済フローにおいては、①電子マネー発行(格納媒体への電子マネー充填:チャージ)、②決済、③電子マネーの提示が一般的なフローとなる。オンライン処理は、①②で必要となるが、①においては決済時の電子マネー不足、③においては定期一括送信となるため、②の決済処理に比べれば頻発する処理ではない。頻発する②の決済処理では発行体への通信処理は行われず利用者、加盟店の当事者間で処理が完結する。このため、従来型電子決済手段であるアクセス型に比べ通信コスト、ホストコンピューター処理コストの削減が期待できる。

(2) 公開鍵暗号

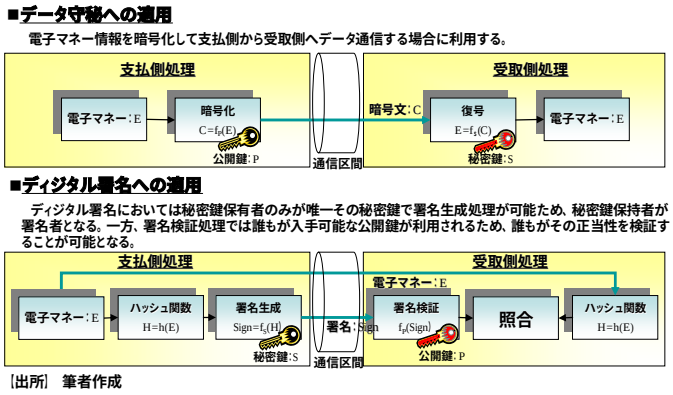
公開鍵暗号は、20 世紀後半に登場した暗号技術であり、従来の共通鍵暗号と異なり暗号化鍵(公開鍵)と復号鍵(秘密鍵)を異にし、暗号化鍵を公開、復号鍵を秘密にする暗号方式である。従来の共通鍵暗号と違い通信相手に予め秘密裏に鍵を配送する必要がなく、また、秘密鍵は受信者のみが保有するためネットワーク上の流通もなく、ハッキングの心配もない。この特性から電子マネーのような不特定多数との暗号通信を必要とするものに極めて有効となる。

本暗号方式に関する最初の報告は 1976 年、スタンフォード大学の Diffie と Hellman により、その原理と機能について報告が成されている。それ以降、安全性が依拠する数学の問題から素因数分解問題に基づく方式、ナップザック問題に基づく方式、離散対数問題に基づく方式、楕円曲線上の離散対数問題に基づく方式の 4 つの分類。機能面によるデータ守秘方式、ディジタル署名方式に分かれた様々な方式が発明されている。現状、最も一般的な方式には 1978

[3] :日本銀行金融研究所(編)『電子マネー・電子商取引と金融政策』東京大学出版会,2002 年 7 月 17 日,pp.6-11.にも同様の見解が見られる。本書は、日本銀行設置フォーラム「電子決済技術と金融政策運営との関連を考えるフォーラム」(1997-1999 年　計 8 回)報告書(金融研究所機関誌『金融研究』第 18 巻 3 号<1999 年 8 月>)、「技術革新と銀行業・金融政策—電子決済技術と金融政策運営との関連を考えるフォーラム」(計 11 回)(金融研究機関誌『金融研究』第 20 巻 1 号<2001 年 1 月>)の重要箇所の整理、データのアップデイトを加えた著書である。

年に報告された RSA 暗号/署名がある。本方式は、素因数分解問題に基づく方式であり、データ守秘方式及びディジタル署名方式の両方に利用可能な方式である。RSA 暗号/署名は報告以来、素因数分解よりも効率的な解読法は発見されておらず、安全面で高い信頼と評価を受け幅広い分野で実用化される。[4]

公開鍵暗号におけるデータ守秘及びディジタル署名の電子マネーへの適用方法を以下の図 4 に示す。



〔出所〕 筆者作成

図 4　公開鍵暗号の電子マネーへの適用例

データ守秘への適用においては、電子マネー情報を暗号化して支払側から受信側へデータ通信する場合を例として掲載している。支払側処理において電子マネーE を公開鍵 P による暗号変換 $f_P(E)$を行うことで暗号文 C を作成し受信処理側へ送信する。受取側処理では、通信区間から得た暗号文 C を秘密鍵 S による復号変換 $f_S(C)$を行うことで電子マネーE を取得する。

次にディジタル署名への適用についてであるが、まず、支払側処理では電子マネーE をハッシュ関数変換 h(E)し H を作成する。H を秘密鍵 P による署名生成 $f_S(H)$を行い署名 Sign を生成する。その後、電子マネーE と署名 Sign を受信処理側へ送信する。受信処理側では、受信した署名 Sing と電子マネーE をそれぞれ公開鍵 P による署名検証 $f_S(Sign)$、ハッシュ関数変換 h(E)を行い、両者を照合し一致することで間違いなく電子マネーE に対して署名されたものであることを確認する。ディジタル署名においては秘密鍵保有者のみが唯一その秘密鍵による署名生成処理が可能である。そのため署名生成者が秘密鍵保持者であるとすることができる。一方、署名検証処理では誰もが入手可能な公開鍵が利用されるため、誰もがその正当性を検証することが可能となる。

(3) IC カード技術

電子マネーを管理保存する格納媒体には、PC 汎用端末等のハードディスクを格納媒体とするネットワーク型とクレジットカード等と同様なプラスチックカードに大量データ保存、高速演算処理を可能とした IC チップを埋め込んだカードタイプがある。ネットワーク型は、インターネット上の仮想店舗（以下、「バーチャルショップ」）に仕組みの上で利用が限定される。これに比べ IC カードは、バーチャルショップの他に実加盟店（以下、「リアルショップ」）との併用利用が可能であること、携帯性に優れるという利便性はもとより内部情報、即ち電子マネーの盗難、改竄等を困難とするセキュアなデバイスとして現状では、電子マネーの格納媒体を IC カードとするのが一般的である。

IC カードが電子マネー格納媒体として利用される理由は、従来の磁気ストライプカードには情報保存のための僅かなメモリ機能しか装備されていない。このため、いくら複雑な暗号処理を施したデータを保存しても毎回同じデータが読み出されることになり、その規則性の解析は比較的容易となる。また、メモリ情報読取機も安価に入手可能であることも問題となる。

これに比べ IC カードは、CPU（Central Processing Unit：中央演算処理装置）、大容量メモリ（ROM、RAM、EEPROM）、暗号処理用演算処理装置の構成による高速演算処理機能の実現により、公開鍵暗号等の複雑な暗号処理を IC チップ内部で高速処理可能とし、暗号アルゴリズムの解析を従来の磁気ストライプカードに比べ非常に困難としている。この他、IC カードには耐タンパ性を実現するために重要となるセキュリティ回路やメモリアクセス制御回路が実装される。

中山靖司氏/太田和夫氏/松本勉氏らの論文によれば、耐タンパ技術とは「外部からの不正な手続きにより、秘密の情報を観測・改変することや、本来の

[4] ：相澤英孝（編著）『電子マネーと特許法』弘文堂，1999 年 7 月 15 日，pp.51-79．その他文献による。

設計意図とは異なる動作を行わせること等を困難にするための物理的･論理的技術」(抜粋掲載)であり、物理レベル、論理レベル、構造レベル、運用レベル各層に分け、これらの各技術を組み合わせることでより高い耐タンパ性の実現が可能であるとしている[5]。これら 4 つの各層について整理したものを以下の表 1 に示す。

表 1　IC カードの 4 つの耐タンパレベル層

レベル	該当事象	主な対策
物理	IC チップの取り出し/露出、回路/メモリの物理的解読。EEPROM データの物理的破壊対策	■ チップ表面のアルミ等カバー ■ 構成要素のチップ上分散 ■ 配線の複数層分散、ダミー配線の混入 ■ ROM 上にダミーの全面電極配置 ■ 酸化しやすい材質によるチップ構成と表面への不活性ガスの封入。 ■ ホイートストンブリッジ回線の組込 ■ 特殊素材保護層による紫外線、X 線、電磁波による改竄防止 ■ EEPROM 情報のハッシュ値保存
論理	不適切な電気信号や電源電圧印加による IC 動作制御、単身による電子信号読取対策	■ 低周波検知回路 ■ 温度センサー ■ 電圧電流のモニタ回線 ■ 紫外線検出回路 ■ メモリパリティチェック機能 ■ 再計算による計算結果チェック ■ 計算処理時の乱数による錯乱処理
構造	プロセッサ、コプロセッサ、メモリアクセス制御回路等の機能及び、その構成の解読対策	■ OS や開発ツールの独自化 ■ チップ/CPU 等の専用化
運用	カード詳細情報の守秘管理やカード発行管理。カードの有効期限設定、旧カード回収/無効化等の IC カードライフサイクル管理や運用面からの対策。	■ IC カードの短期更新 ■ リトライ回数制限 ■ 上限金額設定、取引相手や用途等の利用制限 ■ 取引追跡監視、取引履歴を使用した斜塔バランスチェック

【出所】
中山靖司･太田和夫･松本勉「電子マネーを構成する情報セキュリティ技術と安全性評価」『金融研究』第 18 巻第 2 号, 1999 年 4 月, pp.62-67. を基に整理作成。

IC カードの耐タンパ性への攻撃は、多額のコストを費やして半導体製造、検査を行う最新の装置類を用いれば可能との見解は多く、中山氏らの報告においてもセキュリティ技術は絶対的安全性を持つものではなく、一定の条件のもとでの安全性を保証するに過ぎないと指摘する。しかし、少なくともここでは上記の耐タンパ性対策の導入及び前述の暗号技術を組み合わせることで、従来の磁気ストライプカードとは比較にならないセキュリティを確保することができると言える。

Ⅳ. 電子マネーと IC クレジットのセキュリティ

IC クレジットカードとは、接触型の IC（Integrated Circuit = 集積回路）が搭載された IC カードであり、偽造カード対策等のセキュリティ面の強化、オンライン通信コストの削減、電子マネー等多機能、高機能カードの展開等の実現を目的として、従来の磁気ストライプクレジットカードに替わり開発されたクレジットカードである。本仕様は、金融取引用 IC カードの実質的国際標準である EMV 仕様[6]に準拠しており、2003 年 7 月から我が国でも本格導入が開始されている。日本クレジットカード協会では、IC クレジット化動向予測として 2007 年に IC クレジットカード発行比率約 70%、IC クレジット端末 40 万台を見越している[7]。

(1) IC クレジットカードの取引手順

IC クレジットカードによる取引手順として従来の磁気ストライプクレジットカードと大きく異なる点は、与信処理のオフライン化及び、本人確認方法の 2 つである。

従来の磁気ストライプクレジットカード取引における与信処理は、磁気カード端末にカードを通すことで取引内容の大小に関わらず常に磁気ストライプ

[5] ：中山靖司・太田和夫・松本勉「電子マネーを構成する情報セキュリティ技術と安全情報評価」『金融研究』第 18 巻第 2 号, 1999 年 4 月，pp.60-67．本論文は、日本銀行金融研究所ホームページから入手可能（ホームページアドレスは次項脚注に続く）。<http://www.imes.boj.or.jp/japanese/kinyu/fkinyu99.html>

[6] ：大手カード会社ユーロペイ（Europay）マスターカード・インターナショナル（Mastercard International）ビザ・インターナショナル（Visa International）の 3 社間で合意した IC カードと端末の使用及び双方の取引実行手順を定めた統一規格。3 社の頭文字をとって「EMV」と呼ぶ。アメリカン・エクスプレス等の他のカード会社もこの仕様を支持しており、金融取引用 IC カードの実質劇国際標準。EMV 仕様書は、EMVCo.ホームページから入手可能<http://www.emvco.com>

[7] ：IC クレジット化動向の予測詳細は、日本クレジットカード協会ホームページから入手可能。日本クレジットカード協会,"IC クレジットカード導入について",
<http://www.jcca-office.gr.jp/index.html>(24 Sept. 2005).

に記憶されるカード情報（カード番号、有効期限等）をカード発行会社のホストコンピューターにオンライン送信する。この情報を基にカード発行会社は、当該カードの利用状況の審査（与信）を行い、取引承認結果をオンライン返信する。審査に問題がなければ磁気カード端末から売上伝票がプリントアウトされ、本人確認（本人認証）のため顧客から所定箇所に直筆サインをもらい取引を完了する。

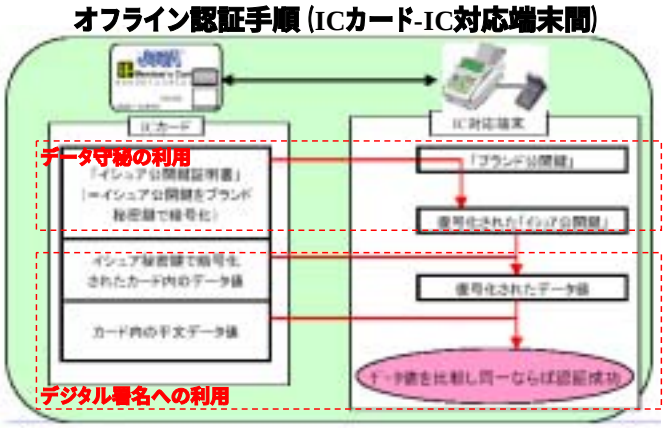
一方、IC クレジットカード取引の場合、IC 対応端末に附属する PIN パッドに IC クレジットカードを挿入する。この際、利用顧客は IC チップ内に暗号化保存される暗証番号（カード PIN）を PIN パッドから入力する。これにより IC チップと IC 対応端末間のオフライン処理にて IC カードの正当性を確認する IC カード認証（オフライン認証）、及び暗証番号照合による本人確認が行われる。その後、IC カード対応端末からプリントアウトされる売上伝票を受け取り取引は完了する。尚、売上伝票受け取りの際、先の暗証番号照合により本人確認は完了しているため利用顧客による直筆サインは不要となる。

IC クレジットカードの取引の場合、リスクパラメータ[8]と呼ばれる取引内容規定範囲が存在し、その範囲内であれば基本的に磁気ストライプクレジットカード取引のようなカード発行会社とのオンラインによる与信処理は不要となり、全て IC チップと IC 対応端末間のオフライン処理にて取引が完了する。但し、リスクパラメータ範囲を超える取引については、IC チップとカード発行会社間のオンライン処理による IC カード認証（オンライン認証）、及び与信処理が行われる。

この他、取引タイミングとは別に加盟店処理として IC 対応端末の中に蓄積された取引内容を一定周期でカード発行会社へオンライン送信される処理が必要となる。

(2) IC クレジットカードのセキュリティ

IC クレジットカードが従来の磁気ストライプクレジットカードに比べ、強固なセキュリティを具備しているとされる理由は、認証機能を有しているからである。IC クレジットにおける認証は、先に示した通り IC カードと IC カード対応端末間で行われるオフライン認証と IC カードとカード発行会社ホストコンピューター間で行われるオンライン認証の 2 つがある。オフライン認証手順を以下の図 5 に示す。



［出所］
日本クレジットカード協会,"IC **クレジットカード導入について**",
<http://www.jcca-office.gr.jp/index.html>(24 Sept. 2005).
上記資料及び本稿掲載図 4 公開鍵暗号の利用例の比較により作成。

図 5　IC クレジットの認証手順

上記認証手順においては、まず第 1 段階として IC カードから IC 対応端末へのイシュア公開鍵証明書（=イシュア公開鍵をブランド秘密鍵で暗号化）の送信、それに対する IC 対応端末でのブランド公開鍵によるイシュア公開鍵の取り出し（復号化）が成される。この時点では、イシュア公開鍵の正当性は確認できない。次に第 2 段階として IC カードは、カード内データ値をイシュア秘密鍵で暗号化すると共に、暗号化したデータの平文（暗号化前のデータ）を送信する。これに対し IC 対応端末では、先に取得したイシュア公開鍵による暗号化データの復号化を行う。復号化データは同時に受信した平文データと照合する。照合が一致することで第 1 段階で復号化されたイシュア公開鍵の正当性確認、即ち正しいイシュア公開鍵証明書の保有が確認されると共に、イシュア秘密鍵の正当性も確認が可能となる。

ここで上記処理を公開鍵暗号利用例との比較を試みる。第 1 段階処理では、イシュア公開鍵、ブラン

[8] ：リスクパラメータについても上記ホームページ（脚注 7）から入手可能。

ド秘密鍵、ブランド公開鍵をそれぞれ電子マネーE、公開鍵 P、秘密鍵 S に置き換えることでデータ守秘への利用と全く同じ処理であると言うことが分かる。第 2 段階の処理でもカード内データ値、イシュア秘密鍵、IC 対応端末内で復号化されたデータ（イシュア公開鍵）をそれぞれ電子マネーE、秘密鍵 S、公開鍵 P に置き換えることで、ハッシュ処理の有無を除いてディジタル署名への利用と全く同じ処理であることが分かる。これらのことから電子マネーに適用される暗号技術と IC クレジットに利用される暗号技術は同様であり、セキュリティレベルに違いはないと言うことができる。

一方のオンライン認証においては、公開鍵暗号の利用は見られず共通鍵による暗号データのやり取りが行われるため、IC カード内に保存される共通鍵の観測をいかに困難としているかがセキュリティとして最も重要となる。(鍵強度については、しかるべき鍵長を採用していると考えられる。）この場合、IC クレジットが電子マネーと同様の IC チップを採用することでセキュリティレベルは同様なものとなる。

以上から、暗号技術、IC カード技術における電子マネーと IC クレジットに関するセキュリティレベルは、ほぼ同レベルでの実現が可能であると言うことができるだろう。但し、電子マネーにおけるオープンループ型流通形態においては、個人間取引が行われるため、同じオフライン処理においても個人と加盟店の信用度について電子マネーの方が低下すると考えることもできる。

Ⅴ．電子マネーの適用範囲

ここでは、Super Cash 実証実験による利用金額の公表結果､及び電子マネーと IC クレジットの利用制限を比較することで電子マネーの適用範囲についての考察を進める。

(1) 電子マネーの低額決済対応

電子マネーは､先に示した公開鍵暗号や IC カードを用いてセキュリティを十分確保することで利用者､加盟店間で電子マネーを直接の媒介手段とする決済であり、磁気カードによるクレジットカード決済とは異なり、その場で決済が完結する自己完結型電子決済手段であることは､これまでの説明通りである。

従来の磁気カードによるクレジットカード決済においては、取引の大小に関わらず常に加盟店に設置される磁気カード端末に磁気カードを通し、磁気ストライプに記憶されるカード情報をカード発行会社のホストコンピューターにオンライン送信することで利用状況の審査（与信）を行う必要がある。このため、加盟店によっては利用最低額を設定する場合もあった。

一方、電子マネーにおいては、IC カードを加盟店に設置される IC 対応端末に差し込むことでホストコンピューターに接続することなく､IC チップと IC 対応端末間のオフライン処理で電子マネーの受渡しが完了するため、通信コスト及び与信処理コストが削減される。出現当初の電子マネーにおいては、この特性が重視され、適用領域としては比較的安価な商品の購入の際に用いる小額決済として利用し、比較的高価な決済については、後払いとなる従来型の磁気カードによるクレジットカード決済を適用領域とする提供側の志向が前提となっていた。実際に展開された実証実験における結果として Super Cash 実証実験の利用状況を以下の表 2 に紹介する。

表 2　Super Cash【2000.05.31 利用実績】

		件数	金額 (平均金額)
チャージ	全体	20,600	2 億 8,349 万円 (13,718 円)
	[内訳]		
	銀行設置チャージ機 (39 台)	11,712	1 億 9,676 万円 (16,800 円)
	公衆電話 (49 台)	3,726	5,564 万円 (14,933 円)
	バーチャル (パソコンから)	5,228	3,109 万円 (5,947 円)
支払い	全体	54,179	2 億 4,233 万円 (4,473 円)
	[内訳]		
	リアル (実際の店舗)	53,194	2 億 3,845 万円 (4,483 円)
	バーチャル (パソコンから)	985	388 万円 (3,936 円)
加盟店数	リアル		914 店舗
	バーチャル		8 モール (8 店舗)
カード発行枚数		22,058	

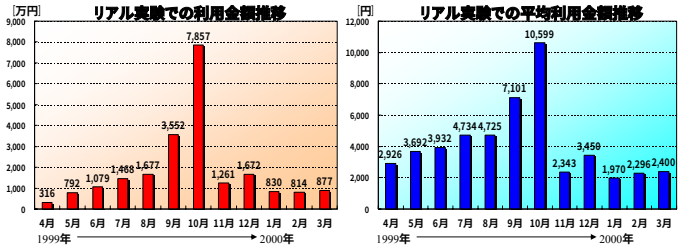
[出所]

スーパーキャッシュ協議会ならびに NTT コミュニケーションズ株式会社,"利用実績",「スーパーキャッシュ共同実験」フェーズ 1 実験結果について,発行日不明,
<http://www.s-cash.gr.jp/whats_new/1016/r4_zisseki.html>(31 May. 2001).

Super Cash の利用金額は、2000 年 5 月末時点で 2 億 4,233 万円となっている。このうちリアルショップにて利用された金額は 2 億 3,845 万円であり、利用金額に占めるリアルショップでの利用金額の割合は、98.4%とその殆どがリアルショップにて利用されたことになる。利用件数においても 98.2%（総利用件数 5 万 4,179 件、内リアルショップ利用件数 5 万 3,194 件）と同様な結果となっている。

この結果からは、我が国においてインターネットショッピングが広く定着していないという考えも導き出せるが、リアルショップ 914 店舗に対しバーチャルショップ 81 店舗と店舗数の規模からも明らかなようにリアルショップ中心の実験展開であり、バーチャルショップ利用において魅力的サービス展開ができなかったことが大きいとする考え方が適切であろう。事実、「スーパーキャッシュ利用促進キャンペーン（スーパーキャッシュポイントキャンペーン）」において、リアルショップ利用のみが対象であり、バーチャルショップにおいては対象外であった。利用者サイドからは、「買いたい商品がない」、「メリットを感じない」と言うのが本音であったと推察する。

リアルショップ利用状況に着目するとスーパーキャッシュ利用促進キャンペーン期間中の 10 月に月額利用金額 7,857 万円と極端なピークを迎えるが、翌月には極端な落ち込みを見せ、その後は横ばい状態となる。このことから、我が国において電子マネー利用は一般的ではなく、利用メリットが十分に見込めなければ利用しないという傾向にあると言うことができるだろう。また、キャンペーン終了後の 2000 年 11 月～2001 年 3 月の期間において平均利用額は 1,970 円～3,450 円、平均 2,482 円であり、利用メリットが十分に見込めない場合、つまり単なる決済手段としての決済金額は、比較的小額決済に利用される傾向があると言うこともできるだろう。Super Cash リアル実験における利用金額推移を以下の図 6 に示す。

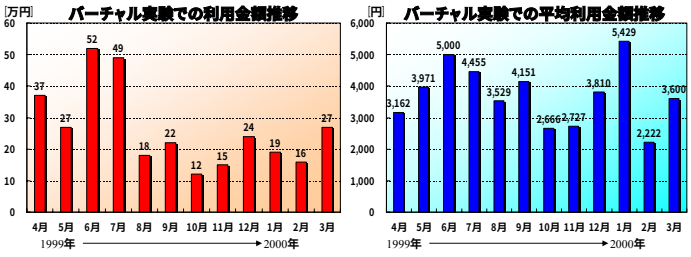


[出所]

(左図) スーパーキャッシュ協議会ならびに NTT **コミュニケーションズ株式会社,"リアル実験での利用状況",「スーパーキャッシュ共同実験」フェーズ** 1 **実験結果について**,
<http://www.s-cash.gr.jp/whats_new/1016/r1_3.html >(31 May. 2001).
より掲載.
(右図) 上記及び、同ページ掲載の利用件数を基に作成.

図 6　Super Cash リアル実験利用状況推移

一方、バーチャルショップ利用状況においては先に示した通り店舗数が少なかったこともあり、利用金額もそれ程大きなものではなく 1999 年 6 月に 52 万円、7 月に 49 万円の最大期を迎えるが、その後は 12 万～27 万の間で推移を見ることができる。（図 7 左参照）また、平均利用金額は、実験期間中（1999 年 4 月～2000 年 3 月）において 2,222 円～5,429 円の推移を見せ平均 3727 円となっており、リアルショップに比べ 1,000 円程度高額となる結果が得られている。（図 7 右図）しかし、この結果を結論付けるためにはリアル/バーチャルの両ショップにおける品数、価格帯等を十分に考慮する必要があるだろう。尚、バーチャルショップでは、リアルショップのような利用者メリットを増幅するキャンペーン等は実施されることはなかった。Super Cash バーチャル実験における利用金額推移を以下の図 7 に示す。



[出所]

(左図) スーパーキャッシュ協議会ならびに NTT **コミュニケーションズ株式会社,"バーチャル実験での利用状況",「スーパーキャッシュ共同実験」フェーズ** 1 **実験結果について**,
<http://www.s-cash.gr.jp/whats_new/1016/r2_3.html >(31 May. 2001) .
(右図) 上記及び、同ページ掲載の利用件数を基に作成.

図 7　Super Cash バーチャル実験利用状況推移

以上のことより、電子マネーの利用金額についてリアル/バーチャル両実験において 1000 円程度の若干の差異は認められたものの、何れも低額決済としての利用実態を確認することができる。現段階における決済手段としての電子マネーの適用領域は低額決済としての位置づけに留まると言うことができる。このことは、現在進展中の鉄道乗車券をその主な購入目的とした交通系電子マネーSuica や Edy によるコンビニエンスストア等の低額決済への積極的な導入動向からも Super Cash 実証実験に限定するものではないと言うことができるだろう。

ここで、電子マネーはオフライン処理特性を活かし通信コスト、与信処理コスト削減を可能とした点において従来型磁気クレジットカード決済と適用領域を異にする低額決済領域への適用が認められる。しかし、オフライン決済を可能とした従来型磁気クレジットカード決済に替わる IC クレジットの出現によって、低額決済領域への優位性に懸念が残る。

(2) 電子マネーと IC クレジットの利用条件比較

IC クレジット決済は、従来型磁気クレジットカード決済に替わりオフライン処理を可能として近年登場した電子決済手段である。また、そのセキュリティにおいても電子マネー同様の暗号技術、IC カード技術を採用することで、電子マネーと同等のセキュリティレベルを確保している。また、電子マネーにおいては、電子マネーを媒介手段として取引相手と直接電子マネー受渡しをオフライン処理にて行うことで通信コスト、与信コストを削減し低額決済領域への適用を可能としている。しかし、IC クレジットにおいてもオフライン処理は可能となり、電子マネー同様に通信コスト、与信コスト軽減が可能となったことで、従来型磁気クレジットカード決済の適用が困難であった低額決済領域への適用が期待される。

IC クレジットは、従来型磁気クレジットカード決済の更改版であるため、磁気クレジットカードが順次 IC 化され、日本クレジットカード協会によれば 2007 年度には IC カード化率約 70%に達すると予想される。一般へ十分な浸透を見せるクレジットカード決済、一方で発展段階にある電子マネーの両者において決済領域が交われば、電子マネー決済量が侵食されることは必然的であり、電子マネーの今後の発展に大きく影響を与えることは容易に想定できる。ここで電子マネーと IC クレジットの違いを以下の表 3 に整理する。

表 3　電子マネーと IC クレジットの比較

	電子マネー	IC クレジット
利用資格	■ クレジット決済型[*1]：年齢制限 ※カード会社の審査有り ■ 現金決済型[*2]：特になし 銀行決済型[*3]：銀行口座保有	■ 年齢制限 ※カード会社の審査有り
利用額制限	■ 数万円（一律固定） ※但し、カード種類により利用上限額が異なる場合がある。	■ 利用者毎に設定
オフライン性	■ チャージ処理：オンライン ■ 決済処理：オフライン	■ 決済処理：オフライン ※但し、リスクパラメータ[*5]設定値より随時オンライン処理が行われる。
手数料	■ 利用者 ・クレジット決済型[*1]：クレジットカード会員費 ※カード種類によって費用が異なる。無料もある。 ・現金決済型[*2]：無料 ・銀行決済型[*3]：無料 ■ 加盟店：加盟店毎に設定。 ※現金決済型、銀行決済型の場合、電子マネー価値根拠となる現金または、預金通貨の確保が、事前に行われる。	■ 利用者：クレジットカード会員費 ※従来のクレジットカードと同様。 ※カード種類によって費用が異なる。無料もある。 ■ 加盟店：加盟店毎に設定。

＜補足＞
*1：クレジットカード決済スキームを利用した電子マネー。
*2：現金通貨と引き換えに電子マネーを発行する電子マネー。
*3：銀行口座との直接連動により電子マネー価値根拠を預金通貨にて管理する電子マネー。預金口座引落タイミングにより、プリペイドカード方式と預金ホールド方式がある。

【出所】
日本クレジットカード協会,"IC クレジットカード導入について",
<http://www.jcca-office.gr.jp/index.html>(24 Sept. 2005).
を基に作成。

利用資格において、IC クレジットは従来型クレジットカード決済であるため年齢規制がある。電子マネーにおいても、クレジットスキームを利用するクレジット決済型においてはクレジット決済同様に年齢制限がある。しかし、銀行決済型については当該銀行口座を保有するだけの至って軽微な制限であり、現金決済型においては特に制限は設けられていない。

利用額制限においては、IC クレジットでは利用者の経済能力に応じた利用額が設定されるのが一般的である。これに対し、電子マネーは決済方法に関係なく各電子マネー単位で一律数万円の固定額となる。電子マネーの種類によっては、カード種別により（例

えば子供用、老人用等）一般カードと利用限度額が異なる場合もある。

オフライン性においては、IC クレジットではリスクパラメータ設定範囲内でオフライン処理による取引が完結する。しかし、リスクパラメータの設定範囲を超えるものについては、従来通りカード発行会社ホストコンピューターとのオンライン処理による与信が行われる。一方、電子マネーにおいては決済処理は全てオフライン処理となるが、電子マネー充填、電子マネーの提示（加盟店からの定期一括送信）においてオンライン処理が必要となる。しかし、このオンライン処理は、決済処理に比較すれば頻発する処理ではないと言うこともできる。ここで、IC クレジットにおけるリスクパラメータの主な内容を以下の表 4 に示す。

表 4　主なリスクパラメータ

【IC カード内の主なリスクパラメータ】

名称	内容
1.暗証番号試行上限回数	暗証番号の試行上限回数
2.連続オフライン上限金額	連続でオフライン取引できる上限合計金額
3.連続オフライン上限回数	連続でオフライン取引できる上限合計回数

【IC 対応端末の主なリスクパラメータ】

名称	内容
1.フロアリミットチェック	予め端末に設定されたオフライン取引の上限取引金額とカードのオフライン取引上限金額との比較を行う。
2.ベロシティチェック	IC カードがオフライン取引の連続回数制限に達したかどうかのチェックを行う。
3.ランダムトランザクションセレクション	予め端末に設定された値に基き、全ての IC カードを対象に、ランダムにオンラインに遷移させる機能

【出所】
日本クレジットカード協会,"IC クレジットカード導入について",
<http://www.jcca-office.gr.jp/index.html>(24 Sept. 2005).
より抜粋掲載。

リスクパラメータの設定値により実際にオンライン処理が発生するのは、オフライン決済の連続積算額、及び連続積算回数が設定範囲を超過した場合の他、無作為に行われるランダムアクセスの場合となる。連続積算額は、電子マネーにおける利用額制限に該当するものであり、この値の設定を電子マネー利用額制限より大きくすることで電子マネーよりも高いオフライン性の実現が可能となる。連続積算回数においては、低額決済を前提とした電子マネーでは持ち合わせない概念であるため、IC クレジットが電子マネーと同等のオフライン性を実現しようとした場合、この値を無限大に設定することで電子マネーと同等のオフライン性が達成可能となるだろう。また、ランダムアクセスによるオンライン処理においては実施頻度にもよるが、連続積算額設定を電子マネー利用額制限よりも若干上乗せすることや電子マネーのチャージ頻度を考慮することで IC クレジットは電子マネーと同等のオフライン性を確保可能と考えることができる。

最後に手数料についてであるが、IC クレジット利用者手数料は、カード種類によって様々であるが、一般的には従来のクレジットカードと同様の会員費が必要となる。IC クレジットにおける加盟店手数料は公開されていないが、オフライン処理による与信コストの軽減により従来のクレジットカード加盟店手数料よりも若干の安価な価格設定が可能であることが推測できる。一方、電子マネーにおける利用者手数料は現在のところ無料となっている。また、加盟店手数料においては IC クレジット同様に非公開であるが、現金決済型、及び銀行決済型の電子マネーにおいては電子的価値根拠､即ち現金通貨または、預金通貨は常に確保されており、発行体にかかるリスクはその分軽減される。そのため、IC クレジットの加盟店手数料より安価な価格設定が可能であることが推測できる。但し、クレジット型決済においては、クレジットカード決済スキームを利用しているため、クレジットカード決済と同等のリスク負担が発行体に要求される。しかし、クレジット決済型と他 2 決済型との複合型を採用することでリスクを他 2 決済に分散可能であり、IC クレジットよりも安価な価格設定が可能であると考えることができる。

VI. まとめ

電子マネーの低額決済領域への適用は、利用者、加盟店間（取引相手）で直接電子的価値（電子マネー）をやり取りすることで、従来のアクセス型決済手段に必要となるホストコンピューター通信や与信処理を不要としたオフライン処理の実現によるものである。オフライン処理の実現においては、IT 技術の発展、特に暗号技術、IC カード技術による耐タンパ機能の組み合わせによるセキュリティの確保が大きく貢献を果たしている。一方、アクセス型決済手

段として一般へ定着化するクレジットカード決済においても、磁気ストライプカードからICカードへの移行によるICクレジット決済において、セキュリティの充実を図りオフライン処理を実現可能としている。ここで両決済手段におけるセキュリティ技術は、同様のものを採用していることから、オフライン処理における安全性は同等のレベルで確保可能であると言うことができる。また、ICクレジットにはリスクパラメータ設定によりオンライン処理が発生するが、連続積算額、連続積算回数の設定値如何、及びランダムアクセス頻度と電子マネーチャージ頻度、電子マネー提示処理を考慮すればオフライン性に大差は生じないと想定できる。

電子マネーのICクレジットへの優位性は、利用資格が比較的低く、万人に提供可能な決済手段（クレジット決済型は除く）であること。現金決済型、銀行決済型、クレジット決済型の3つの決済方法を併用したサービス提供を行うことで加盟店手数料をIC クレジットより安価に抑えることが可能であり、IC クレジットよりも更に低額な決済領域に適用が可能となることである。換言するなら、電子マネーは低額決済領域において現金感覚により近い適用領域を見出すことができる決済手段であると言うことができる。電子マネーの今後の発展においては、これを基軸とする展開、拡張が必要である。

参考文献

1. 財団法人インターネット協会（監修）『インターネット白書2004』インプレス，2004年7月11日，p.370.
2. 経済産業省,”平成16年度電子商取引に関する実態・市場規模調査”,28 Jun. 2005, <http://www.meti.go.jp/press/20050628001/20050628001.html>(22 Sept. 2005).
3. 日本銀行金融研究所（編）『電子マネー・電子商取引と金融政策』東京大学出版会，2002年7月17日，pp.6-11.
4. 相澤英孝（編著）『電子マネーと特許法』弘文堂，1999年7月15日，pp.51-79.
5. 中山靖司・太田和夫・松本勉「電子マネーを構成する情報セキュリティ技術と安全性評価」『金融研究』第18巻第2号, 1999年4月, pp.60-67.
6. 日本クレジットカード協会,”IC クレジットカード導入について”, <http://www.jcca-office.gr.jp/index.html>(24 Sept. 2005).
7. スーパーキャッシュ協議会ならびに NTT コミュニケーションズ株式会社,”リアル実験での利用状況”,「スーパーキャッシュ共同実験」フェーズ1実験結果について, <http://www.s-cash.gr.jp/whats_new/1016/r1_3.html>(31 May. 2001).
8. スーパーキャッシュ協議会ならびに NTT コミュニケーションズ株式会社,”バーチャル実験での利用状況”,「スーパーキャッシュ共同実験」フェーズ1実験結果について, <http://www.s-cash.gr.jp/whats_new/1016/r2_3.html>(31 May. 2001).
9. EMVCo, “Book1 Application independent ICC to Terminal Interface Requirements”, (EMVCo,2000/12).
10. EMVCo, “Book2 Security and Key Management”, (EMVCo,2000/12).
11. EMVCo, “Book3 Application Specification”, (EMVCo,2000/12).
12. EMVCo,“Book4 Cardholder,Attendant,and Acquirer Interface Requirements”, (EMVCo,2000/12).
13. EMVCo, “Version4.0 Analysis of EMV2000 Changes for Backward Compatibility”, (EMVCo,2000/12).

（Received: January 10, 2006）
（Issued in internet Edition: January 31, 2006）