電子マネーの最近の動向と諸問題

村松 晃

1．はじめに

電子マネーがひろく話題にのぼるようになってから，1年以上が経過した．日本の国内でもいくつかの実験が行われ，また，大規模なトライアルも計画されている．世界的に見ると，動きはさらに激しい．すでに技術実験の段階を脱して実用化フェーズに入りはじめた電子マネーも存在する．また，それにともなって電子マネー間の競争も激化している．技術面では，ICカードが電子マネーを含むいくつかのアプリケーションを動的にロードして実行する超小型コンピュータへと変貌するきざしが見えるほか，電子マネーが簡便な支払手段を提供することにより，インターネットが商取引の一大インフラに発展していくというシナリオが現実のものとなりつつある．本稿ではこのような最近の電子マネーの動向を報告するとともに，解決を迫られている問題点についても述べる．

2．電子マネーの背景

電子マネーに関心が集まっている背景の1つとして，世界は急速にネットワークで結ばれた1つの結合体になろうとしている事実があげられる．すなわち，真のグローバル化が進行しつつある．かつて多国籍企業（multinational corporations）と呼ばれた会社群は，いまや完全に無国籍化し，international corporationsになっている．ひとびとはマクドナルドでハンバーガーを食べるとき，これがアメリカの会社であるとは意識しない．日本でもロシアや中国でも，若い人はナイキのシューズをはいている．世界は，機能的にすぐれリーズナブルな価格であれば，どこの国の会社の製品であろうとよろこんで受け入れようとする．

むらまつ あきら
㈱日立製作所 新金融システム推進本部
〒140 品川区南大井6-26-2 大森ベルポートB館

世界のグローバル化は，交通機関の発達と政治体制の自由化により，多くの人が自由に他国を訪れることができるようになったことによっても加速されている．そして，インターネットの発達が決定的かつ最終的な一押しとなった．どこの国の政府も規制できないグローバルなコミュニケーション手段が，人類の前に置かれたのである．インターネットは当初，情報の交換媒体として利用されていたが，最近ではその上で商取り引きを行うことができるように成長しつつある．いうまでもなく，人類のもっとも基本的な活動は経済活動である．その経済活動が，インターネットというグローバルな基盤の上で行えるようになってきたのである．

もう1つ，まったく異なる話題として，偽造の問題を指摘したい．印刷・複写技術の進歩により，紙幣の偽造がより精巧に，より容易に行えるようになってきた．あまりに大量のドル札偽造に耐えかねて，米国はついに100ドル紙幣のデザイン変更を余儀なくされた．これには先ほど述べた，人々のmobilityの高まりも関係している．すなわち，国際的な偽造団の存在である．偽造は紙幣だけでなく，磁気ストライプ型のプリペイド・カードやクレジット・カードにも及んでいる．日本では最近，パチンコという日本独特のゲームのためのプリペイド・カードの偽造が発覚したが，その被害額は600億円を超えていると報道された．日本最大の通信会社NTTでは，電話用プリペイド・カードの偽造による経営圧迫を理由の1つとして，近々ICカードに交換する計画を立てている．

以上述べた世界の急速なグローバル化と急増する紙幣やカードの偽造，この2つが電子マネーへと向かう流れの背後に存在するのである．

3．通貨の歴史と電子マネーの分類学

電子マネーは，通貨の歴史における第3の波である．まず，古代の貨幣から金属貨幣までが「第1の波」を形成する．これは素材そのものに価値の根源がある．

すなわち，第1の波の通貨の本質は「物」である．人類は貨幣の登場によって本格的な分業体制に移行し，生産力を大幅に向上することができた．

「第2の波」は現在われわれが使用している紙幣である．紙幣は紙に数字を印刷した物であるから，はじめから情報そのものであった．金銀などの金属貨幣は，その産出量以上に増加させることはできないが，紙幣は印刷すればいくらでも増やすことができる．さらに，紙幣には信用創造の作用がある．発行された紙幣が同時にすべて金と交換されることは事実上ありえない．したがって，一定の金準備があれば，その何倍もの紙幣を印刷することができる．さらに，ニクソン・ショック以後，米ドル紙幣は不換紙幣となった．米国という国の中央銀行の信用で紙幣が印刷できるようになったのである．人類は信用創造のおかげで，経済活動を何倍にもふくらますことができ，高度経済成長を享受することができるようになった．

このような歴史を経験して，「第3の波」電子マネーが登場した．電子マネーも情報であるが，紙幣との違いは通信できる価値であるという点である．ネットワーク上を光の速度で送れるお金，それが電子マネーである．電子マネーというとセキュリティが話題になることが多いため，セキュリティに問題があると思う方もいるかもしれないが，事実は逆で，電子マネーは非常に高いセキュリティを実現している．この高いセキュリティとネットワーク上で可能な高度な決済能力により，電子マネーはこれからのグローバル化した社会に対応した新しいお金として定着していくであろう．

この電子マネーの分類によく用いられる概念の1つは，マネーの入れ物である．ICカードに入れるタイプをICカード型，コンピュータのハードディスクに入れてネットワーク上でだけ使うタイプをネットワーク型という．しかし，お金を両方に入れることのできるタイプも現れたため，完全な分類とはいえない．

もう1つの分類は，利用のされ方である．発行された電子マネーが一度使われるとすぐに銀行に還流するタイプをクローズド型，人から人に転々流通するタイプをオープン型という．クローズド型はお金が移動するとかならず銀行を経由するため，ハンドリングコストがかかり，匿名性が損なわれる．しかし，お金の動きはトレースしやすい．オープン型は現金にもっとも近い性質をもち，匿名性があり，かつ，ネットワークのない環境でも利用できるため，インフラコストを低く抑えることができる．一方，お金の動きの追跡能力（トレーサビリティ）は低い．

代表的な電子マネーを以上の分類で示すと，モンデックスはICカード型でオープン型，ビザキャッシュやGeldKarteはICカード型でクローズド型，e-cashはネットワーク型でクローズド型となる．

最近では「残高管理型」と「電子紙幣型」という分類（国際決済銀行や日銀 岩村 充氏など）や「カード内残高管理型」と「センター管理型」という分類（NTT大田和夫氏）も使われるようになってきた．残高管理型とは，お金そのものが預金口座からICカードなどに移され，カードに移された金額の合計残高として管理されるタイプで，モンデックスが代表的である．センターで電子マネーの流通をリアルタイムで管理する必要が必ずしもなく，相対的に低コストでインフラを構築することができる．このタイプは匿名性，転々流通性が実現しやすいが，現金と同じで落とせばなくなるし，転々流通を許す場合にはトレーサビリティも乏しくなる．これに対し，電子紙幣型あるいはセンター管理型というのは，現行紙幣のように電子マネーに発行番号がつけられ，還流してきた電子マネーをセンターで突き合わせ処理し，正当性を確認したり清算処理を行ったりするタイプである．これにはICカードを使用するもの（ドイツのGeldKarte）と，e-cashのようにソフトウェアだけで実現するものとがある．ICカードを紛失しても本体が消えずに残っているから安全，また，お金の移動の記録が残るため，盗難やマネーロンダリングの防止に有効という利点がある．反面，記録が残ることが，現金の特徴である匿名性を損なう恐れがある他，センターでの突き合わせ処理にコストがかかるという難点がある．e-cashでは暗号技術を駆使して匿名性を確保している．以上は，どちらが優れているという問題ではなく，目的に応じて使い分けられていくものと思われるし，NTTの電子現金のように両者の特徴を併せ持つ方式も提案されている．

4．ビジネス面での新しい動きとトライアルの現状

ビジネス面における顕著な動きとして，銀行に代わってクレジットカード会社が前面に登場してきたことがあげられる．モンデックスは世界展開を図るためにモンデックス・インターナショナル社を設立したが，これはすぐにマスターカードの傘下に入った．近年事業拡大に積極的なビザキャッシュは，当初からクレジ

ットカード会社の電子マネーである．このような動きの背景には，前述した世界のグローバル化という潮流にある．いま，世界中どこでも共通に使える「お金」は，クレジットカード会社が発行する１枚のプラスチックカードだけである．全世界に展開する加盟店と，それら加盟店を結合するグローバルなネットワークがこれを可能としている．電子マネーを早期に普及させるためには，クレジットカード会社がこれをリードするのがもっとも効果的である．さらに，現在クレジットカード会社は，不正防止のために磁気ストライプ型のカードをＩＣカードに切り替えようとしている．そのための設備投資を正当化するために，付加価値としての電子マネーが期待されている．

電子マネーは世界的な規模で実験が行われ始めている．「世界的」という言葉の意味は，単に世界各地で実験されているということではなく，同じ規格の技術とビジネススキームが，文化や制度，慣習の異なる世界各地でテストされているという事実を指す．実験と呼ばれていても，そのまま継続していけば，それらの実験地は世界制覇のための進出拠点あるいは橋頭堡となりうる．したがって，単なる技術的実験ではなく，ビジネス展開の一環である．ビザキャッシュ，モンデックス，プロトンなどが覇を競っている．図１はこの３種類の電子マネーの代表的な実験地である．ローカルな電子マネーも多数存在するが，早晩，グローバルな標準に吸収されていくであろう．

5．電子マネーのセキュリティ

電子マネーにおけるセキュリティは，以下に述べるように広い概念である．

1．偽造が困難であること（狭義の安全性），
2．簡単には盗まれないこと，
3．マネーロンダリングやプライバシーの問題が起きにくいこと，
4．電子マネー発行元は容易には倒産せず，倒産した場合でも発行された電子マネーは保護されること，
5．紛失・破損したときに補償されること，
6．お金の移動に関する法的証拠が存在すること，

等の幅広い課題が含まれる．これらに十分答えることができて初めて，電子マネーは安心して使うことのできる「電子のお金」になることができる．

偽造が困難という意味での狭義の安全性をとりあげても，多くの技術的工夫が開発されている．なかでも，暗号とICカードが，偽造されにくい電子マネーを実現する中心的要素である．ICカードのICは，通常のICと異なり，内容を解明されにくくするための工夫が施されている．たとえば，メモリ（EEPROM）に保護レイヤーがあり，これをはがすとメモリ内容が消去される仕掛けがしてあったり，回路が２層構造になっていたり，あるいはメモリやデータが分割レイアウトされていて，暗号鍵がこの上に分散配置されていた

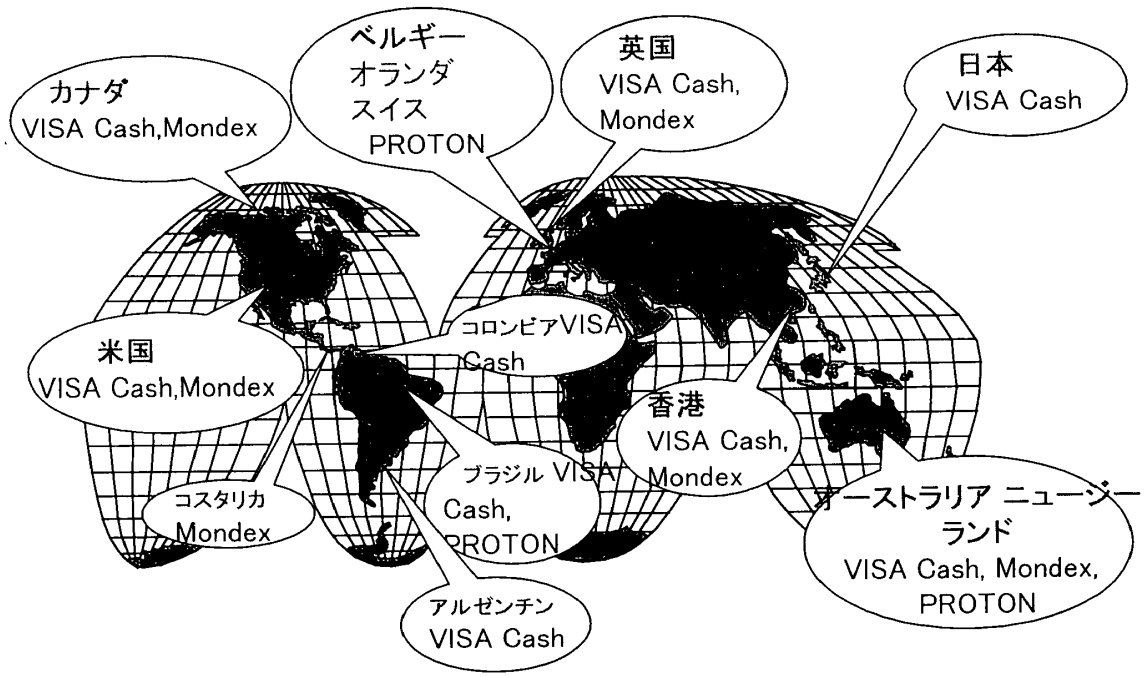

図１　世界規模での電子マネー実験

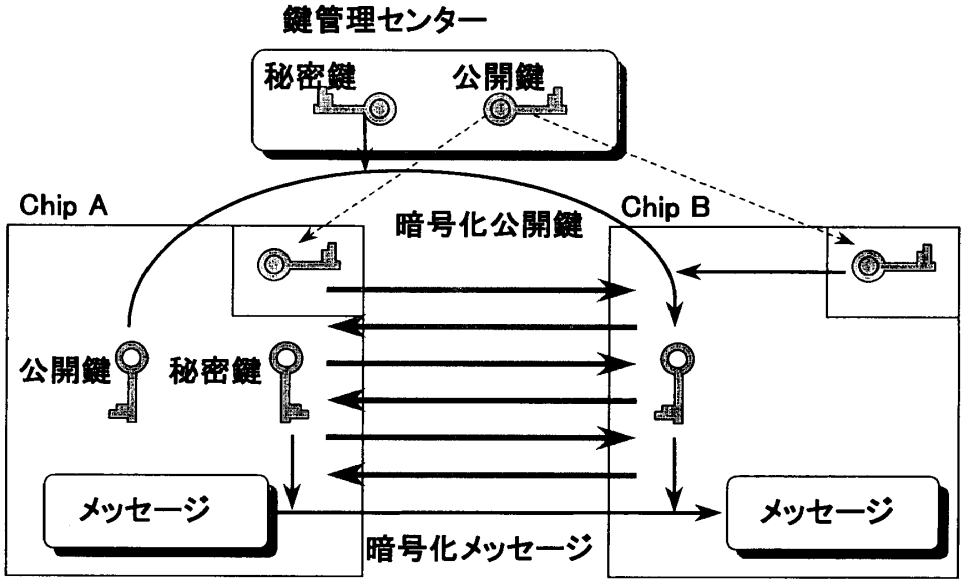

図2　モンデックスの暗号方式

りする．こうした偽造防止のための性質を耐タンパー性（Tamper Resistance）という．

暗号については，先進的な電子マネーでは公開鍵暗号が用いられる．モンデックスは特定の暗号方式に依存しないが，特許においては公開鍵暗号を用いたケースについて，くわしく開示している（図2）．

モンデックスでは，お金を移動させる場合にはチップ間で会話を行い，会話が成功裏に終了すると，各チップが自分の残高を書き換える．お金が外部に出て行かないので安全性が高い．上述の特許では，この会話メッセージは，各チップ毎に生成された一対の公開鍵と秘密鍵のうち，秘密鍵を用いて暗号化される．このメッセージを受け取ったチップでは，暗号をデコードするためにもう1つの公開鍵が必要であるが，これは暗号化されたメッセージと一緒に送られてくる．ただし，それには当然ながら鍵がかけられている．この鍵は全チップに共通の秘密鍵で，それを開けるための公開鍵は製造時にチップに焼き込まれている．すなわち，合計4個の鍵が使われている．これらの鍵は1カ所で集中管理されているのではなく，全チップに共通の鍵だけを管理するキーセンター，半導体製造会社，ICカード発行側により分散管理されていて，どこか1カ所から機密がもれても破られない仕組みが可能である．**表1**に，このような分散型の鍵管理システムを示す．もちろん，モンデックスマネーを発行するオリジネーターが残高ゼロのカードに金額を書き込む場合には，これとは別の暗号システムが用いられる．モンデックスでは，このように暗号システムだけでなく，鍵管理にも最高の技術が用いられている．

表1　分散型鍵管理方式

	共通の鍵システム		個別の鍵システム	
	公開鍵	秘密鍵	公開鍵	秘密鍵
鍵管理センター	●	●	●	
カードプロバイダー			●	●
チップ製造業者	●			

モンデックスではさらに，カードには消費者用，商店用，銀行用などさまざまなタイプがあり，それぞれ収納できる金額に上限がある．そして消費者用カードから商店用カードへお金を転送することはできるが，その逆はできない等のマネーフロー制御が可能である．これにより強盗（消費者用カードを持っている）が店の売上金を強奪しようとしてもできないなどの，犯罪防止機能が埋め込まれている．

また，カードには2種類の暗号鍵のセット（A，B）があらかじめ内蔵されていて，最初はAがアクティブな状態で出荷されるが，途中でBをアクティブにしたカードを市場に投入すると，接触するカードは全部Bに変わってしまうという，コンピュータウィルスのような仕掛けも組み込まれている．そして2年たつとカードは総入れ替えされ，このとき暗号鍵だけでなく暗号方式も入れ替えることができる．これらも偽造防止が目的である．

6．ビジネスモデルとその問題点

電子マネーを実際に適用しようとすると，多くの課題がある．ひとつはコスト負担の問題である．

便利な電子マネーも，導入しようとするとフランチャイズ権獲得やインフラ構築に多額のコストがかかる．このコストを誰がどの程度負担するかが，必ずしも明確ではない．一応，電子マネー事業の収入として，以下の4種類が想定される．

1）発行会社（モンデックスではオリジネーターと呼ぶ）が電子マネーを発行することによって得る発行益．日銀のように無から発行できれば，発行金額それ自体が発行益である．現金と同額で引き換えるなら発行益はゼロである．しかし発行手数料を徴収すればそれが発行益となる．

2）電子マネー発行と引き換えに得た現金の運用益．モンデックスでは，現金との随時交換可能性を保証するためにこの運用は厳しく規制されている．

3）利用者が負担する会費や引き出し手数料．

4）商店における売り上げから回収する手数料．

これらを関与者が得る利便性に応じて負担するのが原則であるが，それは簡単な話ではない．たとえば電子マネーを現金の電子化と考えると，利用者が新たに会費やATM利用料などを払ったり，商店が「現金払い」の売り上げから手数料を払うことに抵抗があるかもしれない．金融機関は現金のハンドリングコストが低下するから，ある程度の負担には応じるであろうが，利用者からも回収したがるであろう．そしてこれら収入総額が事業収入として適切な額に達する見通しがなければ，電子マネーは事業としてなかなか立ち上がらないことになる．さらに，各クレジット会社が電子マネーを発行する場合，売り上げから回収する手数料は会社ごとに異なるかもしれない．そうすると，各社発行の電子マネーは色付けする必要があり，合算することはできなくなる．電子紙幣型ではもともと電子紙幣ごとに個別に管理されるため問題は少ないが，大半のICカードタイプである残高管理型ではこれは大きな困難をもたらす．このように，電子マネーのビジネススキームを確立することは，なかなか難しい仕事である．

7．技術展望1：多目的カード

最近の技術的話題としては，複数のアプリケーションを1枚のカードで実行するためのカード用OSがある．これにより，クレジットカードと電子マネーを1枚のICカードで利用できるだけでなく，各種ロイヤルティプログラムやアクセス管理用身分証明などの応用プログラムをICカード上にローディングしてきて，

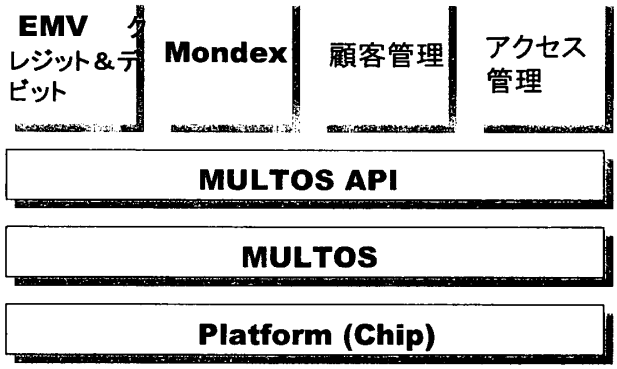

図3　MULTOS

これを一種の安全（タンパーフリー）なコンピュータとして活用することができるようになる．このようなOSの例としては，JavaCardとMULTOS（図3）がある．前者はサン・マイクロシステムズ社が，後者はモンデックス・インターナショナル社が開発したものである．両者の設計思想はよく似ている．いずれもインタープリターによりJava Byte CodeあるいはMELという中間言語を実行する．したがって，ハードウェア，つまりマイクロプロセッサに依存しないほか，アプリケーションが直接ハードウェアリソースをアクセスしないため，安全性が高い．アプリケーション自体は電話回線やインターネットなどのネットワークを通してリモート・ローディングが可能である．たとえばMULTOSでは，このローディングと削除を安全に行うために，認証キーを用いて正当なアプリケーションであるかどうかを確認する．また，各アプリケーションは別々のメモリ空間にマッピングされ，他のアプリケーションに影響を与えることができない仕掛けとなっている．さらにOS全体がヨーロッパのセキュリティ規格であるITSECの最高度の基準をパスするように作られることが要請されている．このように，金融応用を念頭に置いた高いセキュリティがMULTOSの売り物である．JavaCardはすでにシュランベルジュ社がサイバーフレックスというICカードで製品化している他，ジェンプラス社も製品を発表している．MULTOSも来年初めには製品が登場するものと予想される．また，これに合わせて世界中の各クレジットカード会社や銀行，一部の政府機関などで，多目的カードの導入が具体的に検討され始めている．

8．技術展望2：インターネット応用

もう1つの技術的話題は，インターネット上での電子マネー支払いプロトコルである．これに関しては，モンデックス・インターナショナル社が発表したOTP

(Open Trading Protocols) が最大の注目を集めている．OTPはモンデックスだけでなく，ビザキャッシュやサイバーコインなどの一般の電子マネーをも対象にしている．さらに，支払段階でプロトコルをＳＥＴ (Secure Electronic Transaction) にスイッチすることにより，クレジットやデビットにも対応できる．言い換えれば，クレジットにおけるSETプロトコルが支払いプロセスのみを規定しているのに対し，OTPは商品購入プロセスや支払後の請求書発行，注文キャンセル，払い戻し，銀行口座からの預金引き出しまたは預け入れ，両替，さらには商品配送のトレースまでの広い範囲をカバーするビジネスプロトコルである点に特徴がある（図4）．しかし，当初はこれら全範囲をすべて扱うのではなく，購買などの基本的なプロトコルを規定し実験していく予定である．今後，SETはOTPの中に包含されていく可能性もある．現在，コンピュータ関連会社，クレジットカード会社，銀行，通信会社など多数の企業が集まってOTPの仕様定義作業を行っており，引き続いてOTPの製品化も計画されている．近い将来，インターネットに接続したパソコンにICカードを挿入して，OTPサーバーから新聞記事などのデジタルコンテンツを電子マネーで購入することができるようになるであろう．

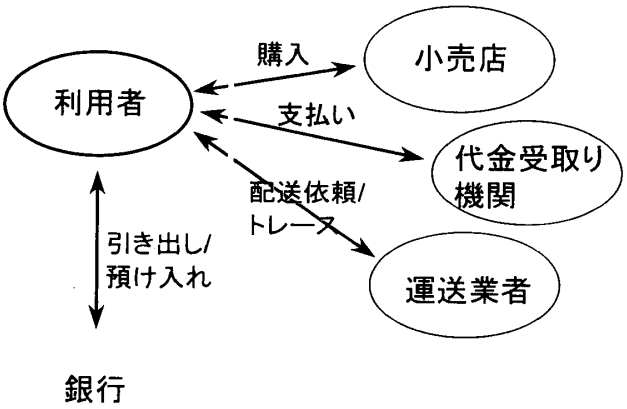

図4　OTPの対象範囲

9．おわりに

世界のグローバル化に対応して登場しつつある電子マネーの，主として技術的側面における最近の動向と課題について紹介した．要約すると，

代表的な電子マネーの技術とビジネススキームが世界各地でテストされ，真にグローバルな電子マネーの追求が加速されている．

そこでは，偽造防止といった狭義の安全性だけでなく，広義の安全性も評価対象となっている．

狭義の安全性については，耐タンパー性を備えたICカードと公開鍵暗号の実用化が，基本要素として認識されるようになってきている．

セキュリティ技術の進展にひきかえ，電子マネーを事業として確立するための適切な事業収支モデルが未開発である．

複数のアプリケーションを1枚のICカードで実行するためのOSが登場し，ネットワークと結びついた新しいcomputing platformを形成しようとしている．

インターネット上で商品購入から支払い，各種証明書の発行，キャンセル，払い戻し，預け入れ／引き出し，商品配送依頼など，物流以外のすべての商取引を行うためのビジネスプロトコルが登場し，グローバル化の進展を加速しつつある．

参考文献

1）日立製作所新金融システム推進本部編：図解よく分かる電子マネー（日刊工業新聞社）1996
2）国際決済銀行編：電子マネーのセキュリティ（ときわ総合サービス株式会社）1997
3）MAOSCO Limited : MULTOS freedom to deliver (1997)
4）Ted Goldstein : JavaCard 2 (JavaSoft) 1997
5）Mondex International : Major New Players Join Effort to Finalize Open Standards for Internet Commerce (1997)