インターネット時代の情報セキュリティと電子マネー

鈴木　幹夫

1．はじめに

情報通信技術の進展により，私たちはマルチメディア通信の世界がますます地域的広がりを持つようになり具体化してくるのを実感する．インターネットを利用することにより，世界の情報を自由に検索でき，世界の人たちと情報の交換がより手軽にできるようになってきた．さらにコンピュータの技術は，パーソナルコンピュータやハンディコンピュータあるいはモーバイルコンピュータのようにいつでもどこでも誰にでも使えるコンピュータというように進展してきている．

このような中で，情報化社会のセキュリティをどのように保つかという課題は，情報通信技術の発達とともに，身近で重要な課題となっており古くて新しい問題ということができる．情報化社会が地域的広がりを持ってくれば，これに伴って情報化社会の混乱も同様に広がるものである．今や，通信は日常的にも国境を越えて行われていると言っても過言ではない．情報セキュリティの課題は，単に暗号技術者だけでは解決しがたい問題である．たとえば，国が異なれば社会習慣やモラルも異なるといった，国境を越えた解決し難い問題も存在する．すなわち，セキュリティの社会的導入にあたっては単に暗号技術の観点からの議論ばかりに限ることなく，情報社会が私たちに与えている新しい社会秩序をどのように保つべきかという観点からも広く議論されるべき問題である．情報通信処理のシステムを研究する立場では，システムの運用，体制，規約や教育などの観点も含め総合的に検討を進めていく必要がある．

特に，インターネットの中ではセキュリティはどうなるか衆多の注目する話題だけに慎重に議論しなければならないと考える．インターネットはネットワークを次々に経由して通信が行われる．したがって，その中継ではさまざまなコンピュータがかかわっており，途中で通信内容を見られる可能性が充分にある．したがって，インターネットが出現して以来，インターネットでの通信にはセキュリティが重要な課題であるという意識が強く存在している．そのような一種の無防備（オープンネットワークもいいことだけではない）な通信環境の状況にもかかわらず，これだけインターネットが浸透しているのはその利便性が優れているからである．インターネット電話なども，実に良い例である．電話信号をパケットレベルでインターネットで伝搬すれば，その音声の一部は漏れる可能性が十分にある．盗聴されるという危機感より，話している相手側に情報が到着するという価値の方が優越している．しかも利用者にとって一見安価？である．本当に安いかどうかは，アクセス料金との比較であるという問題を残しているが．

さて，インターネット時代の暗号技術は，上に述べたように通信環境がオープンであることを前提とし，このうえで情報のやり取りを安心しておこなうための技術として必須なものとなってきている．従来，暗号といえば，情報隠蔽のための戦略的手段であり，したがって暗いイメージをもっていた．しかし，インターネットでは新しいサービスもどんどん考えられており，この中での重要な技術として位置づけられつつあり，いまや情報処理の花形と言える技術であろう．現に，暗号技術は各国の専門家たちが競って研究を続けている．楕円曲線暗号は，正にその最も良い例といえよう．インターネット文化は新しい世界の共通文化ということができると思える．この情報のコミュニティをどう構築していくかが暗号技術者に限定されるのではなくコンピュータ関連の技術者，利用する人たちの責務となっているのではないだろうか．

従来，暗号技術はコンピュータ犯罪などに対抗して研究・開発されてきた．コンピュータ犯罪からいかに

すずき　みきお　日本電信電話㈱ 情報通信研究所
〒238-03　横須賀市武1-2356

情報を守るかという観点からの技術開発と言える．しかし，現代の暗号技術は守るという観点から脱却して，むしろ攻めるという新しい観点からサービスが生まれようとしている興味深い現象が現われつつある．暗号技術と通信プロトコルとを組み合わせた安全な通信の価値形態すなわちビジネスチャンスが生まれてきているといって良い．このように，インターネット時代のセキュリティ技術は種々の形態で使われ，展開されてくると信じている．

本論文では，この問題について電子マネーのセキュリティ技術を例として検討してみる．なぜ，電子マネーを取り上げたかといえば，現金に関わるこの技術は正に，現金としての安全性が最も重要な要求条件として問われるわけで，議論を進める上でちょうどよい事例となるからである．

2．通信環境と情報セキュリティ

2.1 情報セキュリティとは

本節では，いよいよインターネットが到来している現代に必要とされる情報セキュリティとは何か，を説明する．一言で言えば，ここで言う情報セキュリティとは，通信する情報そのものに注目して，その内容あるいは価値が正しく伝達するという通信の本来の機能を達成するための技術を扱っている．いわゆる広く計算機のセキュリティとして言われる計算機の信頼性などの問題は対象としていない．このセキュリティと区別する意味もあって情報セキュリティと呼んでいる．

いわゆる暗号技術は情報セキュリティの中核をなす技術で暗号なしに情報セキュリティを語ることはできない．情報セキュリティは従来から情報の内容を犯罪者から守るという観点から技術開発がなされてきたと言える．第二次世界対戦中のドイツが開発したEnigma暗号，日本の紫暗号などがその良い例である．この辺の興味深い話は諸兄・諸本に譲る．

しかし，ここであえて議論を深めるために情報犯罪とこれに対抗する人間の運用を含めた犯罪と対抗する防御技術とはバランスが必要であるという考え方が工学的な観点から必要であることを述べよう．

確かに，暗号技術を駆使することにより成りすまし防止や関連する犯罪防止を防ぐことができるが，セキュリティに対する投資コストと犯罪コストという観点からのバランスは必要である．いくら，犯罪防止であるからといって，むやみやたらにセキュリティを厳重にしたシステムを作り上げると，セキュリティによるシステムへの負荷が大きくなり効率の悪いシステムになったり，あるいはユーザインタフェースの悪い，したがって使い勝手の悪いシステムができあがってこないとも限らない．

いわゆる通信インフラストラクチャに対する情報セキュリティというのもまた，まったく新たに見直すべきであるといえないだろうか．通信インフラストラクチャに限らずいわゆる社会的インフラストラクチャがシステム的に不安定であればその影響は社会的な問題になる．たとえば，思いつきではあるが，道路交通信号の制御などに盗聴がありかつ信号の擾乱などが発生するようなことがあれば交通渋滞などが想定され混乱が生じかねないのではないだろうか．地震などの災害時にこのような事態が発生しかねないように感じているのは私個人だけだろうか．その道の専門家たちは十分この辺の設計を考えていると信じたいが．

従来はシステムの信頼性の観点からの設計は十分配慮されてきたように思う．一方で，システムはコンピュータ制御がどんどん進んできているので，システムの制御信号が擾乱を受けるようなことになれば誤動作の原因となるわけである．システム設計者への1つの提言としたい．この点で言えば，情報を守るための研究は重要である．しかも，ソフトウェア的な制御で議論できる暗号技術の研究は情報化社会の安全を保つためという意味でその重要性は言を待たないといえる．

あるいは，犯罪防止という観点からの重要性も付言する．現在あるいは今後は，成りすましなどの犯罪が多く見られるようになるであろう．最近での，クレジットカードの犯罪の増加などがその例であり，このために暗号技術が早急に導入されるべきであり，新しい情報通信の形態が生まれようとしている．特に，通信環境がオープンになってくるとセキュリティの新しい課題も増えてくると考えられる．

2.2 オープンネットワークのセキュリティ（個から社会へ）

そこで，そもそも通信環境がオープンになったことによってセキュリティの状況がどのように変化するかを分析する．ここでは，通信の中で必要となるセキュリティについて，個人と社会の関係から論じる．セキュリティはそもそも技術的要素も含まれるが，むしろ社会的な要素も重要でその観点からの検証が必須である．

人間は社会的動物である．言語を利用して他人と通

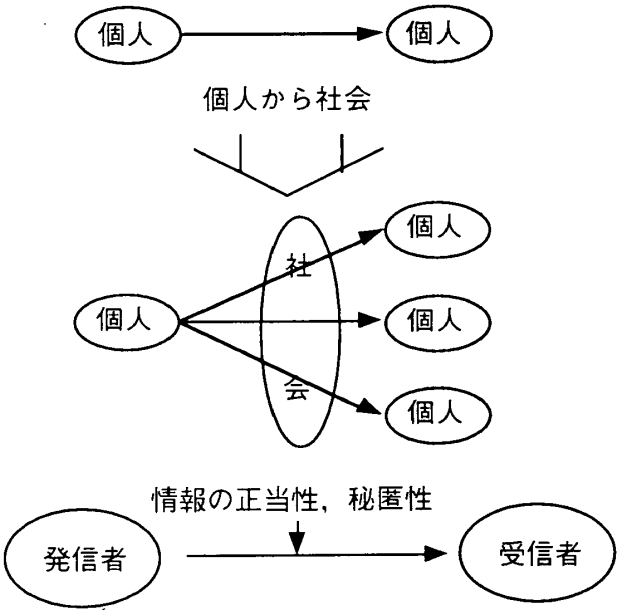

図1　オープンネットワークでの通信のセキュリティ
（個から社会へ，通信のセキュリティ）

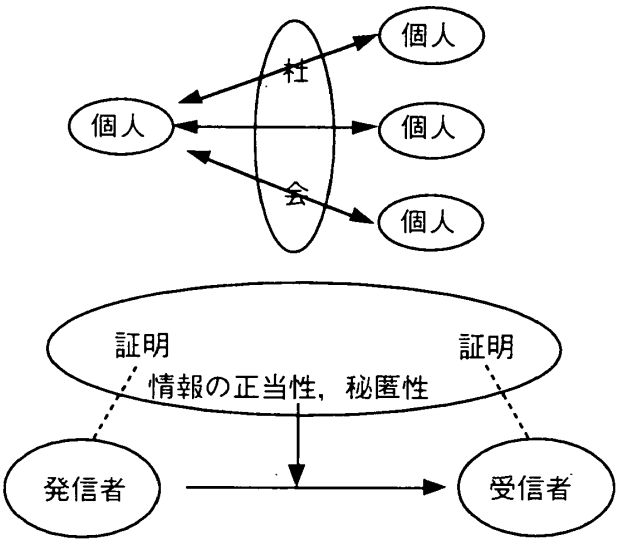

図2　オープンネットワークの通信が必要とする
セキュリティ課題
（社会から個へのアクセスが発生）

信しあう．ここで要求されることは安全に通信できることである．ある個人と社会との通信を考えるとき，個人と社会との関わりという観点から図1に示すような状況で通信が拡大しているということが言えるであろう．そして，一番オープンな状態すなわち，社会という環境と個人が安全に通信できるためのセキュリティの機能は次のように列挙することができる．

・発信者の証明：自分が情報の発信者であることの証明，
・受取人の証明：受け取る側も同様に正しく自分自身が正当な受信者であることの証明，
・情報の正当性：やり取りされるデータが正当であること，英語ではIntegrity（無傷なとか，統一性がとれているという意味），
・情報の秘匿性：他人に盗聴されて情報が漏洩しないこと．

2.3　オープンネットワークのセキュリティ（社会から個へ）

今度は，自己を中心にして社会から情報が流れてくる状態を考えてみる．インターネットの環境では勝手に他人からのメールが飛び込んでくるわけで，図2の通信状況では，次のようなセキュリティ上の課題が挙げられる．

すなわち認証機構などで議論されているように情報と対応する人との所有関係を明確にできるようにするため，次の2点が付加されている．

・発信者の情報の所有性：発信した情報が正しく発信者の情報であることの証明，
・受信者の情報の獲得性：受信する情報の正当性を検証できて，受信したことを証明できること．

たとえば，見ず知らずの人からメールなどが来た時のことを想定しよう．そのときあなたはどうするであろう．だれだろう，こんな人知らないが何だろう．たぶん，興味津々とメールを読み始めるであろう．たとえば，メールアドレスから，どこの国からのメールだろうとか，発信時間などあれこれと詮索をめぐらすのではないだろうか．しかし，それはクレジットの請求内容であったりしたらどう対処すべきであろうか．これらが，現実のオープンネットワークで起こりうる課題である．

すなわち，社会から個人へのアクセスが生じることによって個人が守らなければならない状況が生じるわけである．このようなことは，厳密に言えば電話のような通信環境でも起きていた．しかし，インターネットのように種々のサービスが可能になってくる通信環境では，守るべきセキュリティの課題は複雑多岐にわたってくる．

上に述べたことを通信の世界で考えるとき，通信内容をいかに安全に保つかということに関して通信システムの一部として第三者が必要になってくるといえる．この第三者がいわゆる保証という観点からの機能を果たすように考えるのである．ここでは，通信と言っているのがデータを運搬するという機能のみにとどまらずデータの内容にまで言及していることが重要である．オープンな通信環境では通信内容の保証が課題になっ

てくると言える．すなわち，社会的な通信環境から個人へのアクセスがある場合，社会が個人に対して内容保証やプライバシーの保護などの機能が必要になってきているといえる．

さらに言えば，ここで問題とする社会的機能は，国際的視野に立った議論でなければならず，インターネット時代のセキュリティ機能として特徴的なことである．このことは，文化やモラルの異なった国々の人たちと積極的に通信するときの問題で，いわゆる国際化ということで世界に乗り出すときに出くわす種々の課題の一部であるという見方もできる．すなわち個人が国際という場に進出する時に生じる社会との関わりの問題の一部である．ここではこれらの問題を技術的な観点から議論していきたい．

3．電子マネーのメリットと基本メカニズム

ここで，本論で主たるセキュリティの検討課題にしている電子マネーとは何かについて触れておこう．

3.1 電子マネーとそのメリット

電子マネーとは，その名前のごとく，現金を電子的なデータに置き換えたものと言える．電子的な形態になっているので，次のような便利な点が生じる．

(1) 空間的制約からの脱却

通常の現金では，手渡しという行為が不可欠である．したがって，現金を支払うためには，その場にいなければならない．言い換えれば，通常のお金ではたとえ大金を持っていても地球の裏側では買い物ができない．しかし，電子マネーならネットワークでつながってさえいれば，どこへでも支払いが可能である．

(2) 時間的制約からの脱却

私たちは，現在，銀行システムに慣れ親しんでいる．現金が不足すると，私たちはATMで現金をおろす．真夜中になって，手元に現金がなくて困った経験がある．銀行の口座には大金があっても，自由に使えない状態は不便なものである．しかし，電子マネーでは家庭にあるパソコンやICカードに入力することが可能となるので，いつでも現金をおろせる可能性が出てくる．

もっと重要なことは，海外などへの資金の送付などの問題である．現在の資金送付は銀行員が扱っているので，その日の内に現金が届くということはあり得ない．しかし電子マネーではこれが可能になってくるのである．しかも，個人宛に送金というのも可能になる．

(3) 現金を持ち歩くということがなくなる

現金を送金するとき，大金を持ち歩かなければならないという必要がなくなってくる．それだけ，安全ということである．たとえ，現金のように落としたとしても本人の所有している現金であるということを確認できるので，他人が拾っても使用できないようにすることが可能である．

(4) “おつり”が不要になる？

日常，物を買うとき必ず必要なおつりであるが，電子マネーでは値段に等しい現金を支払うことができるので，おつりという概念がなくなるのである．すなわち，現金で一番トラブルが生じやすいおつりを間違えることや，おつりを渡すための人件費が不要になる．

(5) 即時支払いが可能

上に述べたことは，電子マネーがインターネットのWWWで買い物をするときに有効であることを物語っている．インターネットでは，情報が商品になり得る．情報化された商品は時間と空間を乗り越えてその場で手に入れることができる．したがって，それに対応する対価は即金であるのがふさわしい．クレジットや，プリペイド方式では支払いという行為と物を獲得する（納入）という行為に時間差があるため，この間に何らかの危険が生じる可能性があり，そのための保険が必要になっているのが現状である．

(6) キャッシュレジスタの消滅？

さらに，現実的な例での効果を考えると限りなく多くの効果を考えることができる．デパートなどでの買い物をするとき，会計での長蛇の列に我慢しなければならない経験を多くの方が持っている．店員の方々も現金を取り扱うことに神経をとがらせているわけである．また，日毎の売り上げでも大金を扱うため，これに伴う警備の経費も馬鹿にならない．パチンコ店などでの現金強奪などの犯罪の大きな原因は，大量の現金が扱われているからともいえる．

以上，現在の現金が電子化されることのメリットを述べたが，いいことばかりではない．現実化するまでには多くの解決すべき課題が存在する．金融政策，金融制度にからむ問題や，電子マネーを支えるハードウェア環境や人間要因を含んだ運用などの問題である．一方で，電子マネーの研究者らは，研究・開発する立場から技術的な問題の解決に傾注し，特に，情報セキュリティ上安全な電子マネー方式を提唱しようとしている．

3.2 電子マネーの基本メカニズム：3役モデル

電子マネーシステムではデジタル署名の技術を頻繁に使用している．この基本メカニズムを3役モデルで説明する（図3）．二者間での何らかの取引においてこれを第3者が保証する必要があり，したがって，ネットワーク上での取引が行われる場合には，3役モデルが通信の基本モデルとなると考えられる．

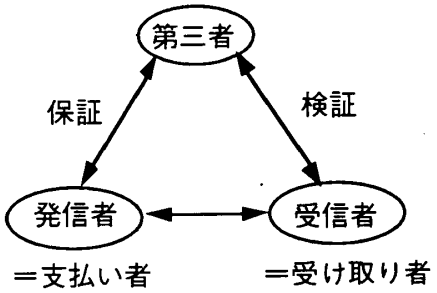

図3　三役モデル

デジタル署名はこれを支える暗号技術ということができる．デジタル署名はあるデータに署名を附加するがその署名を作成した人の唯一性（厳密に言えば，署名を作成するために必要とする秘密鍵を所有している人の唯一性）が保証でき，かつ，誰もがその唯一性を確認することができるという効果を持っている．これによって，署名は印鑑などのもつ効果と同様に，データの内容について何らかの保証を設定できるようになる．

たとえば，日本銀行券に押印されている印鑑によって，日本銀行券という単なる物理的な紙に印刷されている物質が貨幣という価値保証をしているということが言える．ここで，署名になぞらえてその重要性を強調すれば，日本銀行券に押印されている印鑑は唯一日本銀行が所有している印鑑であり，誰もがその印鑑が日本銀行のものであるということも認め得ることができるからである．さらに，ここで重要なのは，印鑑はどこにでも押印できるから，実は暗黙のプロトコルとして紙幣という紙には貨幣価値という主張があり，印鑑はこの主張を保証するという約束になっている．

同様なことが，デジタル署名についても言えることができる．すなわち，現金としての価値保証を与えるためには，発行機関がデジタル署名を附加し，これによって受け取る側が価値の確認をすることができるわけであるが，この価値を受け取った人が価値を享受するためには，デジタル署名を附加したひとが直接的にあるいは間接的に価値に対応する保証を義務づけられるわけである．

4．電子マネーの3層レイヤ論

上に述べた，3役モデルは発展して考えれば従来の金融システムにも現に存在している機構といえるものである．貨幣価値を保証する日本銀行のような機構などがわかりやすい例である．電子マネーのセキュリティシステムとしての構造を検討すると，図4に示す3つのレイヤで成り立つことがいえる．構造は現実の金融システム自身がとっている構造に自然と対応するものである．特に，ここで強調したいのはAdministrativeな階層の必要性である．セキュリティを必要とするシステムには，必然的にセキュリティを監督できる仕掛けが必須である．これがあることによって，いざというときにシステム全体をコントロールできるようになる．電子マネーの場合には特に，犯罪防止の仕組みが課題となりうるわけで，このAdministration Layerによって，ユーザや国家機関あるいは金融にたずさわる方々から安心して使用できる電子マネーとなりうるわけである．さらに，延長していえば，国を越えて電子マネーでの決済などを考えるような場合には，お互いの立場で安全性が確認できる仕組みが必要と言える．

Administration Layer (Governmental organization)	Keeping the value of the money, Money Supply, Law Enforcement, Against the Crime (Counterfeiting, Fraudulent use, Copy, Tax evasion, etc.)
Bank Operation Layer (Bankers)	Management of the user's account (Deposit, Withdraw, Transfer to another Bank.)
User's Layer (Consumer Merchant Provider)	Shopping over the Internet /Real Shop /Abroad /Telephone use Wireless withdraw / deposit World Wide stores

図4　電子マネーセキュリティシステムの基本構造

5．おわりに

以上，インターネットに代表されるオープンな通信環境におけるセキュリティの新たな課題と，オープン通信環境で重要なサービスであるエレクトロニック・コマースに必要となってくる決済手段としての電子マネーの技術について関連するセキュリティ課題を述べた．

電子マネー技術については，現在ではまだまだ実用

的には研究あるいは実験段階であるが注目されつつある．特に，情報化社会の安全という観点から電子マネーのセキュリティが論じられるべきであることは本論に示したとおりである．

また，最近では国際の場での議論が進もうとしており，中でもインターネット環境で電子マネーをどう扱うべきかは金融の自由化・グローバル化とあいまって加熱する課題となりつつある．