2. e-Societyを推進する暗号技術

3. 電子ビジネスと暗号技術

岩下 直行
日本銀行 金融研究所
iwashita@imes.boj.or.jp

暗号技術の普及は，ビジネスの世界にも大きな影響を与えている．電子商取引の急速な拡大，電子決済，電子マネーの普及から，電子株主総会の開催まで，従来，紙と印鑑で進められていたビジネスの現場が大きく変わりつつある．現在，どのような電子ビジネスが可能となっているのか，今後さらに電子ビジネスを拡大していくためには，どのような技術的問題を解決していく必要があるのか，暗号技術との関連を踏まえて考えてみたい．

10年目を迎えた電子商取引

2004年は，電子商取引が始まってから10年目にあたる年だといわれている．最近の新聞報道によれば，世界で最初の電子商取引は，1994年8月に，米国ニューハンプシャー州で行われたのだそうだ．インターネット上の暗号技術を利用してクレジットカード番号を送信し，音楽CDが購入されたのだという．それ以降，現在までの10年間は，電子商取引が急速に拡大した期間であると同時に，インターネットを通じて暗号技術が一般の人々に普及した期間でもあった．

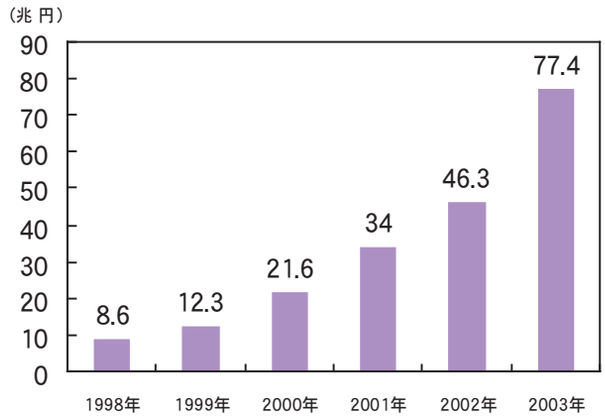


図 -1　BtoB 電子商取引の市場規模の推移

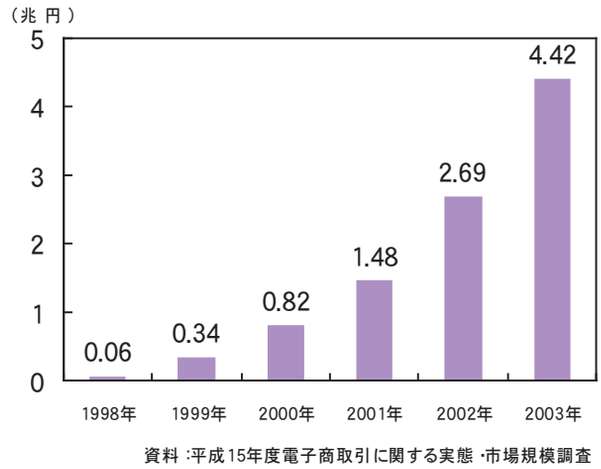
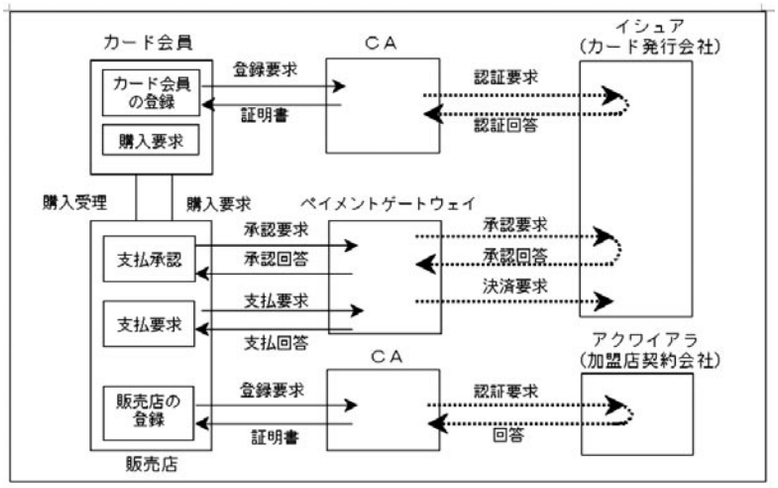


図 -2　BtoC 電子商取引の市場規模の推移

経済産業省の調査によれば，我が国における2003年の電子商取引は，企業間（BtoB）で約77兆円，消費者向け（BtoC）で約4.4兆円に達し，いずれも前年比7割近いスピードで急拡大している（**図-1，2**）．

10年前の音楽CDを出発点として，その後，さまざまな商品が電子商取引の対象とされるようになった．最近では，インターネットを用いて大規模マンション販売のプロモーションを行ったり，新型乗用車の見積り依頼が行われることも珍しくない．さすがにそうした高額商品の場合は，電子商取引とはいっても，インターネットが利用されるのは購入申し込み段階だけで，決済は後日，銀行振り込み等で行われることが多いが，書籍，パソコン，家電製品等のオンライン・ショッピングでは，発注から決済までのすべてをインターネット上で完結させる取引が一般的となりつつある．

こうした電子商取引の決済において，現在最も広く利



資料：電子商取引推進協議会 Web ページ

図 -3　SET の概要

用されているのは，10 年前と同様，暗号技術を利用してクレジットカード番号を安全に送信するという方法なのである．

電子商取引の要請が暗号政策を変えた

暗号技術は，つい 10 年ほど前までは，学術研究の対象とされる以外には，軍事・外交などの特殊な通信に用いられるものと考えられており，民生用として利用されるのは，一部の金融ネットワークなど，特別に高いセキュリティが必要とされる業務のみであった．当時，標準的に利用されていた暗号アルゴリズムは，鍵長 56 ビットの DES であり，DES が組み込まれた電子機器は，「兵器」として輸出規制の対象となっていた．

今では意外に思われるかも知れないが，ほんの数年前までは，日本からであれ米国からであれ，暗号を利用した電子機器やソフトウェアを海外に輸出しようとする場合，鍵長を短くして暗号強度を下げるなどの機能制限を行った上で，個別に認可を受けることが必要だった．たとえば，当時，米国製のソフトウェアである Internet Explorer には，米国国内向けと米国国外向けの 2 種類のバージョンが存在し，実装されている共通鍵暗号の鍵長が異なっていた．国内向けは 128 ビットであるのに対し，国外向けは 40 ビットに制限されていたのである．米国外に居住する利用者が Internet Explorer を利用すると，相対的に安全性の劣る暗号技術しか利用できず，それが電子商取引を推進する上での障害となっていた．しかし，インターネット上での電子商取引を拡大したいという社会的要請が高まったことから，各国の暗号技術の輸出規制が徐々に緩和され，現在では，かつて各国で輸出規制の対象となっていた強度の暗号が，世界中で利用可能となっている．このような経緯を経て，現在，事実上の標準として利用されている暗号通信プロトコルである SSL (Secure Socket Layer) において，共通鍵暗号として鍵長 128 ビットの RC4，公開鍵暗号として鍵長 1,024 ビットの RSA が利用できるようになり，それらがインターネット・バンキングやクレジットカード番号の送信に利用されているのである．

より安全な電子決済を実現しようとする試み

実は，電子商取引において，SSL を用いてクレジットカード情報を暗号化しただけでは，真の意味で安全に電子決済ができるわけではない．購入者の側から見ると，たとえ通信経路上は暗号で保護されていたとしても，見ず知らずの販売店にクレジットカード番号を開示してしまうため，情報漏洩のリスクを感じることになる．販売店の側からみると，購入者の風体を確認することも，伝票に署名して貰うこともできないから，情報を送信してきたのが正当なカード保有者であるか不安だし，後で「そんな買い物はしていない」と否認されるおそれもある．

こうした問題に対処するため，1996 年に VISA と MasterCard が SET (Secure Electronic Transaction) と呼ばれる標準仕様を提案した．この方式を用いれば，販売店は，取引の都度，真正なカード保有者が情報を送信したことを確認でき，ディジタル署名を用いて取引の証拠を残すことができ，購入者は，クレジットカード番号を販売店に開示しなくとも，カードが利用可能であることの認証を受けることができる作りであった (**図-3**)．

ところが，SET は，いくつかの実証実験プロジェクト

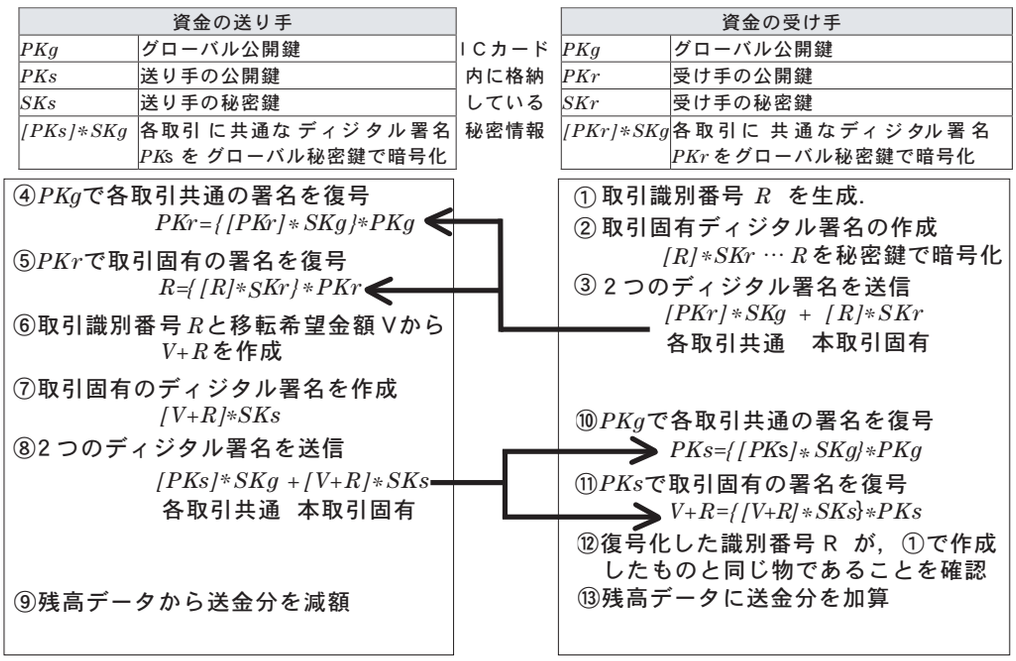


図4　IC カード型の電子マネーの価値移転プロトコルの例

に実装されて市場テストが行われたものの，複雑な仕組みと，利用者が操作するのに手間がかかることを主因に，あまり普及しなかった．このため，VISAは，SETと類似の機能を持ち，利用者の負担を軽減した3D Secureと呼ばれる技術を提案しているが，こちらもあまり普及していない．引き続き，SSLを利用したクレジットカード番号の送信が圧倒的に多いようである．

インターネット・バンキングの課題

インターネット・バンキングにおいても，利用者負担と安全性のトレードオフを巡って，技術選択の変遷が見られた．

1997年頃に我が国の銀行がインターネット・バンキングを導入し始めた当時は，銀行の安全性に対する意識が強く，高いセキュリティを追求していた．このため，インターネット・バンキングにも，SETの技術に基づく，厳格に利用者認証を行う通信プロトコルを採用していた．ところが，この方式は，利用者が専用ソフトウェアをインストールし，公開鍵証明書を取得する必要があるなど，利用者側にコストと運用の手間がかかるものであったため，あまり普及しなかった．

これに対し，2000年頃から，SSLにパスワードを組み合わせただけの簡易な認証方式によるインターネット・バンキングが提供され始めると，急速に普及率が向上した．この方式では，SSLはパスワードの盗聴を防ぐための守秘機能のみを担っており，金融機関側のシステムにおける利用者認証は，パスワードや乱数表といった，素朴な手段のみによって行われる．この方式は，利用者の負担こそ軽いものの，運用環境次第では安全性が脅かされるリスクがあると指摘されている．

電子マネーと暗号技術

最近，国内でも，ICカード型の電子マネーが普及し始めている．電子マネーとは，ICカードの中に「価値」を表す数値を格納し，これを売り手と買い手の双方で増減させることによって電子的に決済を行う仕組みのことである．

ICカード型の電子マネーにも，さまざまなバリエーションがあるが，暗号技術との関連で特に注目されるのは，オープン・ループ型と呼ばれる，カード同士で価値を移転する方式である．この方式は，利便性が高い反面，万一，各ICカード間での価値の移転において不正が発生すると，それを検知することが難しく，システム全体の崩壊につながりかねない．このため，価値の移転には，公開鍵暗号を利用した高度なセキュリティ・プロトコルが必要になる．実際の電子マネー・プロジェクトにおける具体的なプロトコルは公開されていないが，論文などで発表されている例を**図-4**に示す．

この方式では，各ICカードが公開鍵と秘密鍵を持ち，各カードの公開鍵をグローバルな秘密鍵（電子マネーの

発行主体が持つ秘密鍵）でディジタル署名することによって，一種の「お墨付き」として機能させ，相互に相手を真正なカードと認証しながら，取引の前後で価値が不正に増加してしまうことを避けつつ，価値を移転することを可能としている．

ICカード型の電子マネーの場合，ICカードの内部情報を不正に読み出すことの困難性（耐タンパー性）がどの程度信頼できるかが，重要な論点となる．

電子株主総会における議決権の行使

こうした決済を巡る技術革新以外にも，暗号技術の普及がビジネスに影響を与えている事例は多い．たとえば，遠隔地からの参加を可能とする電子株主総会の実現は，その典型的な例といえるだろう．

2001年の商法改正によって，インターネットを利用した株主総会における招集通知の発送や議決権の行使が法制化された．2003年度には，140社が株主にインターネット経由の議決権行使を認めた．株主は，招集通知書に記載された議決権行使番号とパスワードを使って専用のWebサイトにアクセスし，議決権を行使できる仕組みが用いられている．

こうした法制度の変更は，インターネット上で安全にパスワードを送受信するためのSSLなどの技術を，特別な知識を持たない一般の利用者（株主）でも使いこなせることを前提としている．このような新たな電子ビジネスの展開は，暗号技術の裾野の広がりを背景として，初めて可能となったものである．

これからの課題

以上見てきたように，暗号技術を利用した電子ビジネスは，量的には急速な拡大を続けているとはいえ，質的な面では，なお発展途上にあるといわざるを得ない．SSLのように，差し当たって容易に適用できる領域については暗号技術を利用しているものの，暗号技術が潜在的に持つ機能を活かしきっていないように思われるからである．これはなぜなのだろう．

1つには，さまざまなビジネスの現場で必要とされる業務要件が多様であるため，それを個々の現場で電子的に実現しようとすると，その都度アプリケーションを作り変えざるを得ず，カスタマイズに大きなコストがかかってしまう，という理由が挙げられる．標準化されているSSL以外の暗号技術を必要とするアプリケーションを開発，普及させていくのは大変である．ただし，こうしたコストの問題は，外部環境が変われば容易に変わり得る．つまり，業務要件としてセキュリティへの要請が強まれば，暗号技術を何とかして利用しようとすると考えられる．

むしろ，より本質的な問題は，現時点の暗号技術だけでは解決できない業務要件が存在し，そのために，ビジネスの電子化が進められないということであろう．たとえば，ビジネスで利用する各種の契約書を電子的な文書に置き換えたいというニーズは多いが，契約書が果たしている長期的な証拠性を電子的に実現しようとすると，ディジタル・タイムスタンプや長期的な有効性を保証し得るようなディジタル署名など，さまざまな道具立てが必要になる．このため，実務での利用に耐えられるような電子文書保管のソリューションを構築することは難しい．他に先駆けてビジネス書類の電子化を進めている企業は，自らのリスクで適切と思われる対応を採っていくしかない．安全性と効率性を併せ持った電子決済手段についても，なお技術的な改良を図る余地があるといえるだろう．

しかし，そのような技術的な未解決問題が存在するということは，電子ビジネスの領域に，豊かな鉱脈が隠されていることを示しているのではないだろうか．電子ビジネスにおける暗号技術の利用は，まだ始まったばかりなのだから．

参考文献
1）岩村　充，神田秀樹：電子株主総会の研究，弘文堂（2004）．
2）五味俊夫：インターネット取引は安全か，文春新書（2000）．
3）経済産業省，平成15年度電子商取引に関する実態・市場規模調査（2004）．
4）松本　勉，岩下直行：インターネットを利用した金融サービスの安全性について，金融研究，21巻別冊1号（2002）．
5）松本　勉，岩下直行：デジタル署名の長期的な利用とその安全性について，金融研究，22巻別冊1号（2003）．

（平成16年9月30日受付）