IMES DISCUSSION PAPER SERIES

金融分野における情報セキュリティ技術の現状と課題

松本勉・岩下直行

Discussion Paper No. 98-J-25

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES
BANK OF JAPAN

日本銀行金融研究所
〒100-8630 東京中央郵便局私書箱 203 号

IMES Discussion Paper Series 98-J-25
1998年11月

金融分野における情報セキュリティ技術の現状と課題

松本 勉[*1]・岩下 直行[*2]

要　旨

従来、わが国の金融業界では、コンピュータ・システムを外部から物理的に隔離することによってセキュリティを守るというポリシーを採用してきたため、暗号技術等の情報セキュリティ技術の重要性が十分に認識されているとは言い難かった。しかし、社会全体のネットワーク化の進展に伴い、金融業界においても、オープンなネットワークを活用して新しい金融サービスを提供しようとする動きが活発化している。このため、オープンなネットワークにおけるセキュリティを確保する手段として、暗号技術の重要性が高まってきている。今後、わが国の金融機関が金融サービスを安全に提供し続けていくためには、情報セキュリティ技術に対する正確な理解と経験が必要とされていると言えよう。

情報セキュリティ技術は様々な要素技術を複雑に組み合わせた「総合技術」であり、その実効性を評価するためには、採用されているセキュリティ・ポリシーから暗号アルゴリズムの安全性に至るまで、ひとつひとつの要素技術について詳細な評価を積み重ねることが必要である。また、各要素技術には、各々「耐用年数」とでも言うべき安全性の期限があり、技術進歩や新しい攻撃法の出現により、従来安全と考えられていた技術が急に安全でなくなってしまう可能性もある。従って、金融機関が情報セキュリティ技術を活用して安全に金融サービスを提供していくためには、常に新しい技術革新に対応し、最新の安全対策を講じていかなければならない。そのような対策を講じる場合には、各金融機関が自らの情報セキュリティ対策の枠組み等を適切に開示し、オープンな議論の俎上に乗せていくことも有効な手段と考えられる。

また、今後、わが国の金融業界が新しい情報セキュリティ技術の採用を検討する場合には、最近の欧米主要国の金融機関における新しい暗号技術の採用状況等を踏まえて、国際的な整合性、説得性のある技術を採用していくことも重要であろう。

キーワード：情報セキュリティ技術、暗号、認証、金融取引の安全対策、情報開示、国際標準化
JEL classification: L86、L96、Z00

*1 横浜国立大学大学院工学研究科人工環境システム学専攻（E-mail: tsutomu@mlab.dnj.ynu.ac.jp）
*2 日本銀行金融研究所研究第2課（E-mail: iwashita@imes.boj.or.jp）

本論文は、1998年11月4日に日本銀行で開催された「金融分野における情報セキュリティ技術に関するシンポジウム」への提出論文に加筆・修正を加えたものである。

目　　次

頁

１．はじめに

インターネットの爆発的な拡大に伴い、オープンなネットワークを利用した様々なビジネスが拡大してきている。こうした環境変化を受けて、従来はさほど一般には関心を持たれていなかった「情報セキュリティ技術」が、このところ急速に注目を集めるようになってきている。パソコンに標準装備されたWWW ブラウザや電子メールなどのインターネット用ソフトウェアには、暗号機能が予め組み込まれるようになり、インターネットの利用者の間では、認証や通信機密の保護のための暗号通信が当然のように利用されている。新聞や雑誌で暗号技術や電子マネーに関する一般向けの技術解説を目にすることも珍しくなくなった。この数年の間に、情報セキュリティ技術は、我々の日常生活の中にかなり深く入り込んできた。

こうした情報セキュリティ技術は、金融業務の分野にも大きな影響を及ぼしている。現在、首都圏を中心に、数万人規模の参加者を募った電子マネーの実証実験プロジェクトがいくつも進められている。インターネット・バンキングを提供する銀行も増えてきた。IC カードを利用した電子的支払手段を店頭での小口決済に利用するという構想は 10 年以上前から実験されてきたが、最近の電子マネー、電子決済のプロジェクトが従来のものと異なるのは、店頭での支払いもさることながら、インターネット上で「電子商取引」を行うための手段として提案されているところにあるように思われる。世界中に張り巡らされ、数千万人が利用しているインターネットの上で、安全かつ効率的な資金決済が可能になれば、その波及効果は極めて大きいものがある。

インターネットは、それ自体はセキュリティを確保する機能を持たないネットワークであるため、現在提案されている電子マネー、電子決済などのプロジェクトは、いずれも独自の暗号技術を用いて、金融取引にふさわしいセキュリティ水準を確保しようとしている。ただ、こうした暗号技術は急激な技術革新にさらされており、常に「完全な」セキュリティを保証できるものではない。このため、そのコストをも考えながら、常に適切なセキュリティ対策を講じていく必要がある。その意味で、わが国の金融機関が、これからの新しい金融業務の担い手として金融サービスを安全に提供し続けていくためには、暗号技術などの情報セキュリティ技術を正しく評価し、有効に活用していく能力が必要とされていると言えよう。

２．金融業務と情報セキュリティ技術

金融業務と情報セキュリティ技術、暗号技術とは、かなり縁遠いもののように思われるかもしれない。しかし、金融業界における暗号技術の利用には、実はかなり長い実績がある。暗号は、かつては軍事情報や外交機密の秘匿のために利用されるものであった。しかし、1977 年に、DES（Data Encryption Standard）が米国政府標準暗号（FIPS: Federal Information Processing Standard）に認定され、ビジネス分野で利用されるようになってから、暗号の商用利用が急速に広がった。DES の開発・普及の背景には、コンピュータ・ネットワークを利用して資金決済情報や顧客の秘密情報を送受信する際に、情報の改竄や不正侵入を防止したいという米国金融業界の強いニーズがあったと言われている。金融業務を電子化された手段を用いてネットワーク上で実施する場合は、特に高いセキュリティ水準が求められるため、米国を中心に、銀行の決済ネットワークには DES を利用したセキュリティ装置が次々に導入され、金融業界は暗号技術の最大のユーザーとなった。こうした経験の延長と考えれば、金融業界が暗号技術を活用した電子マネー、電子決済の実験に積極的に取り組んでいることは、ある意味で当然のことと言えるだろう。

暗号は、データを第三者には判読不能な形態に変換し（暗号化）、「鍵」と呼ばれる特殊な情報を持っている人にだけ、元のデータに戻すこと（復号）を可能にする技術である。この技術は機密情報の保護に使用されることが多いが、それだけではなく、「認証」にも利用することができる。送られてきた暗号文が「鍵」によって意味のある文章として判読できたとすると、受信者側は、その暗号文を作成したのは「鍵」を知っている人だと推定できる。例えば取引データを送信者と受信者しか知らない「鍵」で暗号化すれば、安全性の高い権限確認の手段として機能する。このように、ビジネス分野で利用される暗号は、通信の秘密を守る機能（守秘）だけでなく、情報が正当な利用者によって作成されたもので、改竄を受けていないことを確認する機能（認証）が重要になる。この認証機能は、従来は小切手などに署名･捺印することによって実現されてきたもので、これを通信ネットワーク上で実現するために暗号が利用されている。そう考えると、金融と暗号との関係も理解し易い。

通信ネットワークを利用した形態以外でも、例えば IC カードを利用してオフラインで安全性の高い認証を行うとか、指紋、虹彩、音声、筆跡といった人間の身体的特徴を利用して本人確認を行うバイオメトリクスと呼ばれる技術など、取引の安全性に対する要請の強い金融業務に利用可能な様々な情報セキュリ

ティ技術が開発されている。これらの技術を組み合わせることで、銀行券や小切手といった既存の紙ベースの決済システムのセキュリティを強化するために利用することも可能と考えられる。

３．わが国金融業界におけるこれまでのセキュリティ対策への取り組み

わが国の金融業界においても、従来から、コンピュータ・システムのセキュリティ対策への取り組みは進められていた。特に、リアルタイムのオンライン・システムを事故から守るための様々なバックアップ手段の充実や、機密性、真正性確保の要求の高いデータに関する物理的なアクセス制御については、かなり進んだ対策が講じられてきた。しかし、情報セキュリティ技術、暗号技術の観点からの対策については、あまり関心が払われてこなかった。これは、これまでわが国の金融業界が構築してきた決済ネットワークが、企業内、業界内に閉じたものであったためである。わが国の金融機関は、巨大なコンピュータ・センターにメインフレームを並べ、支店との間を専用回線でつなぐことにより、システムを外部から物理的に隔離してきた。このようなシステムにおいては、ネットワーク提供者が利用者のアクセスを厳格に管理すれば、システム全体のセキュリティを高めることが可能と考えられてきた。

例えば、銀行の現金自動支払機で預金を引き出す取引をみてみると、キャッシュカードと四桁の暗証番号を入力すれば良く、高度な暗号技術など利用されていない。これは、現金自動支払機が銀行の店舗内に設置されており、銀行のコンピュータ・センターとも専用回線で接続された「閉じたシステム」だったからである。このような環境の下でシステム全体のセキュリティが確保されているのであれば、盗聴や改竄のリスクも低いので、暗証番号程度でも権限確認の手段として十分機能すると考えられてきた。このため、わが国の銀行のオンライン・システムにおいては、情報セキュリティ技術や暗号技術は補完的なセキュリティ対策と位置付けられてきた。

４．金融ネットワークのオープン化と情報セキュリティ技術の必要性

金融ネットワークのセキュリティを外部からの隔離によって守ることができていたのは、金融業界が他の業界に先駆けて独自の決済用コンピュータ・ネットワークを構築していたからに他ならない。しかし、インターネットの拡大等、最近の社会全体における情報ネットワークの広がりは、そうした前提を崩しつつある。

金融機関間取引の分野では、情報通信技術の急速な進歩と取引のグローバル化を受けて、複数のシステムがリンクする取引が増えてきている。売買、約定、決済等、複数のシステムに跨る取引を、できるだけ人手を介さずに、効率的に処理するためには、システムを相互接続し、入力されたデータを自動的に処理・転送する仕組みを作ることが必要である（このようなコンセプトを STP ― Straight-Through Processing という）。しかし、これまでわが国の金融機関が採ってきたような「システムの隔離によってセキュリティを確保する」という方針だと、相互接続によってセキュリティの枠組みが崩れてしまう。このため、従来とは異なるセキュリティ対策を講じる必要が生じてくる。

対顧客取引の分野でも、EDI（電子データ交換）の普及、インターネットの発達に伴い、一般の企業や個人が何らかのコンピュータ・ネットワークに接続している状況になってきているため、顧客は、金融サービスを自らが接続しているネットワークに対して提供して欲しいというニーズを持つようになっている。例えば、金融 EDI を実現するためには、企業間取引のデータと金融データを組み合わせて処理する必要があるため、何らかの形で顧客側の EDI システムと、銀行の金融ネットワークに接点を作る必要がある。どのような方法を採るにしても、銀行システムのセキュリティ対策を考え直す必要が出てくると考えられる。

金融ネットワークのオープン化が進み、ネットワークの提供者がシステム全体のセキュリティを確保するという考え方が機能しなくなると、個々の取引単位のセキュリティを確保する手段として、暗号技術が非常に重要となってくる。例えば、オープンなネットワークの中で送信する資金支払指図データの安全性を確保するために、ディジタル署名による認証を行うとか、特定の相手以外には開示できない情報をオープンなネットワークで送信する場合に、暗号による秘匿を行うことが必要となってきている。

こうした現状を踏まえて、欧米の金融機関と比較した場合、わが国の金融業界が情報セキュリティ技術の重要性を十分に認識しているとは言い難く、具体的な取り組みも進んでいないように思われる。これはひとり金融業界の責任という訳ではなく、そもそもわが国では、金融ネットワークを標的とした犯罪がさほど多くなく、セキュリティ対策に対する顧客の関心も低いため、金融機関としてそれを強化するインセンティブを持たない、という外部環境が大きな原因となってきたと考えられる。有効な情報セキュリティ対策を講じるためには、相応のコストが必要となる以上、金融機関とその顧客の側に強いニーズがない

のであれば、そもそも情報セキュリティ対策に費用を投じることは、ビジネスの世界では現実的とは言えなかったのであろう。

しかし、インターネットに代表される情報通信ネットワークの国際的な広がりは、金融業務に新たな利便性、効率性をもたらす一方、従来存在しなかった新たなネットワーク社会の脅威をも作り出した。複雑に絡み合ったネットワークのどこかに、システムへの不正侵入を図る犯罪者が潜んでいるかもしれない。従来は専用回線のセキュリティに対する信頼が根強かったが、通信の自由化が進むと、利用者間の回線のセキュリティについて通信事業者が責任を持って保証することも困難となる。このため、オープンな情報ネットワーク上でビジネスを行う企業にとっては、適切な情報セキュリティ対策を講じることが必要不可欠となってきている。特に金融機関の場合、取り扱う情報の性格から、要求される安全対策の水準は極めて高い。仮に、そうした新しい脅威を恐れて、金融業務にこうした新しいオープンな情報ネットワークを利用することをためらうと、新たなビジネスチャンスを失うこととなる。

従って、わが国の金融機関がインターネット・バンキングや電子マネーといった先端分野についても、良いサービスを安全に提供し続けていくためには、情報セキュリティ技術に対する正確な理解と経験が必要となっているといえよう。

５．どのような情報セキュリティ技術が利用されるか

それでは、金融業務に利用される情報セキュリティ技術には、どのようなものがあるのだろうか。主な要素技術を整理すれば、以下のとおりである。

(1) 暗号アルゴリズム

① アルゴリズムと鍵

既に述べたように、暗号とは、データを一定の手順に基づいて変換することによって、守秘と認証を実現するための方式である。そのための具体的手順となる算式を「暗号アルゴリズム」といい、複雑なコンピュータ・プログラムやハードウェアの形態を取る。一般に、暗号アルゴリズムの構造は広く知られているが、「鍵」と呼ばれる数十～数百桁の数値列からなるパラメータを合わせて用いることにより、暗号化と復号を、それぞれに対応する鍵を知っている人のみに実施させることができる。異なる鍵を用いれば、多くの人が同じ暗号アルゴリズムを利用して、別々に暗号通信を行うことができる。

暗号アルゴリズムは公開しても、鍵さえ秘密にしておけば安全だ、という

のが現代の暗号の考え方である。50 年ほど前までは、暗号を作る技術と暗号を破る技術とが拮抗していたため、暗号のアルゴリズムも秘匿しておくという使い方が一般的であったが、暗号理論の進歩によって、暗号を作る側のアドバンテージが高まり、アルゴリズムを公開しても安全であると期待できるようになった。現在では、むしろ暗号アルゴリズムを公開することにより信頼性を高めるという考え方が一般的である。暗号アルゴリズムは高度な数学理論に基づいて考案され、高度なコンピュータ技術に基づいて実装される。基礎となる理論に見落としはないか、プログラムやハードウェアに欠陥はないか、チェックすべき多くの項目がある。技術を公開して、大勢の研究者の目にさらされることによって、問題点が洗い出されることが期待できるのである。

② 暗号アルゴリズムの分類

暗号アルゴリズムは、その利用目的からは守秘と認証とに分けられ、利用者への鍵の配置の仕方から共通鍵方式と公開鍵方式に分けられる。これを整理すれば、下表の通りである。

暗号アルゴリズムの分類と代表的な例

		利用者への鍵の配置の仕方	
		共通鍵方式	公開鍵方式
利用目的	守秘	共通鍵暗号方式 DES、Triple DES、IDEA、MULTI、MISTY、CAST、RC2、RC4、RC5、AES など	公開鍵暗号方式 RSA、ElGamal、楕円曲線 ElGamal など
	認証	共通鍵認証方式 同上（共通鍵暗号アルゴリズムを利用して MAC 等を生成）	公開鍵署名方式 RSA 署名、ElGamal 署名、DSA、楕円曲線 ElGamal 署名、楕円曲線 DSA など

暗号による守秘機構とは、メッセージ（平文）を暗号化鍵で暗号化し暗号文に換え、これを伝送し、受信側で暗号文を復号鍵で復号して平文に戻す仕組みのことである。特定の受信者にしか平文の意味を知らせないためには、復号鍵を受信者だけが秘密に保持していなければならない。暗号化鍵も秘密にしておく方式が「共通鍵暗号」で、暗号化鍵は復号鍵と同一となるのが普通である。代表的なアルゴリズムとしては、DES、Triple DES、IDEA、MULTI、MISTY、CAST、RC2、RC4、RC5 などがある。米国は DES の後継暗号として AES の公募を始めた。

暗号による守秘機構において、暗号化鍵から復号鍵を導くために莫大な計算量を要すと期待できる場合には、暗号化鍵を公開しても差し支えない。これが「公開鍵暗号」である。代表的なアルゴリズムに、RSA、ElGamal、楕円曲線 ElGamal などがある。

暗号による認証機構とは、平文を生成鍵により変換して認証文を生成し、これを伝送し、受信側で検査・復号鍵を用いて認証文を検査・復号する仕組みである。特定の送信者しか検査に合格する認証文を生成できないようにするためには、生成鍵は、送信者だけが秘密に保持していなければならない。検査・復号鍵も秘密にしておく方式が「共通鍵認証方式」で、検査・復号鍵は生成鍵と同一となることが普通である。共通鍵暗号の暗号文が認証文そのものであるといった形式と、認証文が平文に認証子（MAC: Message Authentication Code）と呼ばれる短いデータを付加した形式であるものとがある。

暗号による認証機構において、検査・復号鍵から生成鍵を求めるための計算量が莫大であると期待できる場合には、検査・復号鍵を公開しても構わない。これが「公開鍵署名方式」で、アルゴリズムとしては、RSA 署名、ElGamal 署名、DSA、楕円曲線 ElGamal 署名、楕円曲線 DSA などがある。公開鍵署名方式の認証文の形式は共通鍵認証方式の認証文の形と同様に２通りあるが、一方向性ハッシュ関数を併用する形式がよく使われる。通常、このようにして生成される認証子はディジタル署名と呼ばれる。

③ 暗号アルゴリズムの強度と鍵長

共通鍵暗号において利用される鍵の長さ（鍵長）はアルゴリズムにより様々であり、最も普及している DES 暗号の場合、鍵長は 56 ビットである。この鍵長が短いと、可能性のある全ての鍵を試してみるという「全数探索」による攻撃が可能となる。このため、暗号解析技術の進歩に対抗して暗号の強度を維持するために、今後は 80 ビット以上、おそらくは 128 ビット以上の鍵を利用する暗号アルゴリズムが使われるようになると思われる。

ある暗号アルゴリズムを解読すること、つまり暗号文と平文を結び付ける鍵を導出することは、最も単純な鍵の全数探索以外にも、暗号アルゴリズムの欠陥を突くことによってより巧妙に行える可能性がある。しかし、少なくとも鍵の全数探索には耐えられるものでなければその暗号は安全とはいえないので、全数探索への耐性は最低限確認しておくべきポイントである。以

前から、DES の 56 ビットの鍵を虱潰しに調べることは、数億円で製造可能なハードウェアにより数日で実行できると予想されていたが、1998 年 7 月に行われた DES 鍵全数探索装置を用いた実験によって、その予想が実証された。これと同程度の計算能力を持ったハードウェアで、タイム・メモリ・トレードオフ解読法という方法を実行すれば、数日の事前計算を実施した上で、想定される平文に対応する未知の鍵による DES 暗号文が入手された後、１時間程度でその未知の鍵を求められることも分かっている。さらにインターネット等を用いて数万台、数十万台の規模のパソコンを繋いで超並列計算を行う試みも多数実施され、鍵の虱潰し探索が可能な鍵長は延びている。しかし、実用化されている共通鍵暗号において、128 ビットの鍵全数探索が現実的脅威となることは、ここ数十年程度はないであろうと予想されている。ただし、このことは、128 ビットの共通鍵暗号において、全数探索以外の巧妙な方法で鍵を導出することが事実上できないことを保証するものではないことに注意が必要である。利用目的に応じた十分長い鍵長を持つことは、安全な暗号の必要条件ではあっても、十分条件とはならないということである。

公開鍵暗号／署名方式についても、同じことが言える。代表的な公開鍵暗号である RSA 暗号／署名方式の場合、従来、鍵長（メッセージブロック長）が 512 ビット程度のものがよく使われていたが、暗号解析技術の進歩に伴い、適用分野によっては 1024 ビットや 2048 ビットといった長さの鍵が要求されるようになってきた。そのため、比較的短い鍵長である程度の強度を確保でき、暗号化／復号に要する計算量も少なくて済む楕円曲線暗号／署名方式が盛んに開発されている。

(2) 暗号鍵管理

暗号アルゴリズム自体が十分強いものであったとしても、それだけでは暗号をうまく利用できない。鍵の生成、保管、アクセス制御、配送、共有、認証、更新、廃棄、再生などの鍵管理が必要となる。潜在的な暗号通信相手が極めて多数存在しうるシステムにおいて鍵管理は特に問題となる。

共通鍵暗号／認証方式においては、通信相手と鍵を共有することが重要事項であり、①鍵配送センタと個々の通信者との間で共通鍵暗号により通信者間の鍵を配布する方式、②公開鍵暗号により通信当事者相手に鍵を配送する方式ないし鍵共有専用の公開鍵方式である公開鍵配送方式、および、③鍵事

前配布方式（KPS: Key Pre-distribution System）等がある。

公開鍵暗号／署名方式においては、公開鍵の入手と持ち主の確認が重要事項であり、④鍵認証センタ（認証機関）の発行する公開鍵証明証に基づき公開鍵を入手して確認する方式や、⑤個人的に信用できる通信者による保証の連鎖により公開鍵を入手して確認する方式等がある。

メッセージに直接作用する鍵は頻繁に更新し、それをより寿命の長い鍵により共有・配送する階層的な鍵管理がしばしば用いられる。法律執行や鍵紛失対策の支援のために、通信当事者以外の者にも復号機能を与えることを可能にする機構が組込まれることもある。

(3) 暗号プロトコル

暗号アルゴリズムは複雑に組み合され、電子マネー等のシステムの根幹をなす暗号プロトコルとして働くことがある。ここで、プロトコルとは、２者間以上の参加者の間でメッセージを授受しながら計算を進めていくための分散されたアルゴリズムのことをいう。個々の暗号アルゴリズムが十分安全であったとしても、プロトコル全体として安全になるとは限らないところが難しいところである。形式論理等を用いて、プロトコルの安全性を保証しようという息の長い研究が行われているが、実用規模の複雑な暗号プロトコルに対して意味のある結論を導くのは極めて難しい模様である。従って、失敗と成功の経験を積んだ専門家の直観的評価に、最後は頼らざるを得ないのが実状である。

(4) 耐タンパー技術

電子マネー等で用いられる暗号の鍵や取引データなどが暴露されないよう、また、残高データなどが改竄されないよう、これらを物理・論理的に厳重に管理することが必要となる。このため、耐タンパー性（Tamper Resistance）を有するハードウェアやソフトウェアのモジュール、すなわち、秘密データを外部から不当に観測・改変することや秘密データの利用制御部を不当に改変することが極めて困難であるよう意図して作られたハードウェアまたはソフトウェアのモジュールの重要性が高まっている。電子マネーを扱う IC カードはもちろんのこと、IC カードを受け入れる装置、電子マネーを発行・管理する装置、あるいは、認証機関の証明証発行装置などに耐タンパー性が必要である。暗号装置（複数の部品からなるハードウェア）

の耐タンパー性に関する要求条件については、国際標準化機構・金融専門委員会（ISO／TC68）や米国政府が策定する国際標準・国内標準として整備されつつあり、これらに基づく技術評価も進められている。

しかし、半導体チップ等の部品そのものやソフトウェアについては、耐タンパー性の明確な基準は整備されておらず、当該チップ／ソフトウェアのメーカー以外の者が耐タンパー性の評価を十分に行う方法も確立されていない。IC カードの耐タンパー技術については、２チップから１チップへ、高集積化、ライフサイクル管理、回路パターンの難読化技術等々の技術が開発されているが、その詳細な情報がメーカーからユーザーに公開されることはあまりない。それでは、現在普通に用いられている一枚 100 円程度の IC カードの耐タンパー性はどの程度信頼できるものなのだろうか。半導体製造技術・検査技術の進歩と解析技術の進歩のバランス次第ということになるが、おそらく、一世代前の IC カードチップの回路パターンや内部に記録されているデータを取り出すのは困難でないと思われる。しかし、暗号技術が客観的に評価可能な技術として認められ広く役立ちつつあるように、評価可能で方式を公開しても誰もが安心して利用できる耐タンパー・モジュールを構成する体系的な方法が強く望まれている。

６．総合技術としての情報セキュリティ

ここでは、個々の要素技術についてではなく、それらの「総合技術」として、情報セキュリティ技術を位置付けることの重要性を説明したい。

金融分野に利用される情報セキュリティ技術としては、①公開鍵暗号、共通鍵暗号、暗号鍵管理、暗号プロトコル等を創り出すための「暗号基礎技術」、② IC カードや各種情報機器を組み合わせてセキュリティ対策を実現するための「実装技術」、③ビジネスとして大きなシステムの構築を安全に進めるための「システム設計技術」、④構築したシステムを安全に運用したり、その安全性を鑑査・評価していくための「運用管理技術」等が挙げられる。

金融分野に利用される情報セキュリティ技術は、こうした様々なセキュリティ技術を統合した「総合技術」として評価すべきものである。というのは、金融業務のセキュリティを守ろうとする場合、パーツとしての暗号技術や IC カード等の耐タンパー性、システム設計、運用管理といった技術の全体の「チームワーク」が大切であり、それらのどこに穴があってもセキュリティを侵害されてしまうリスクが高まってしまう。その意味では、例えば「この電子マネー

は、何ビットの暗号を利用しているのでとても安全です」といった説明はミスリーディングであることが分かる。

また、これらの技術には、各々「耐用年数」とでも言うべき安全性の期限があるということも重要な論点である。例えば、共通鍵暗号の場合、原理的には、全ての考えられる鍵の候補を試してみることによって破ることができてしまう。同様に、IC カードの耐タンパー性にしろ、暗号プロトコルの安全性にしろ、一定の条件の下での限定された安全性しか保証されていない。技術進歩や新しい攻撃法の出現により、従来安全と考えられていた技術が急に安全でなくなってしまうということを、これまで何度も経験してきた。

このように、金融分野に利用される情報セキュリティ技術には、「絶対的な安全」ということは有り得ず、その安全性を評価するためには、一定の前提条件と留保が必要となる。従って、金融機関が情報セキュリティ技術を活用して安全に金融サービスを提供し続けるためには、常に新しい技術革新に対応し、最新の安全対策を講じていく必要がある。

７．セキュリティ対策のコストと政策的配慮

一般に、情報セキュリティ技術を金融業務に適用しようとすると、様々な技術についての踏み込んだ検討が必要であり、新たなシステム対応など、追加的なコストがかかる。時には、サービスの処理速度など、利用者の利便性を犠牲にしなければならないこともある。ところが、利用する金融サービスのセキュリティに関する切実なニーズが、利用者の側にあるとは限らない。そうした部分にコストをかけるよりも、安価にサービスを提供すべきという要望もあると考えられる。

ここで、安全だが高価な決済サービスを提供する金融機関と、やや安全性に問題はあるが安価な決済サービスを提供する金融機関が競合した場合、「悪貨が良貨を駆逐する」事態に陥る可能性もありえよう。一般の商品であれば、そのような競争によって消費者が真に望むものが効率的に実現されるということが言えるのであろうが、電子マネーや電子決済のような特殊なサービスの場合、そう割り切ってしまって良いのか、やや議論のあるところである。この点を考える上で、次のようなエピソードを紹介したい。

よく知られた事例であるが、1995 年 9 月、代表的な WWW ブラウザである Netscape Navigator Ver.1.2 の暗号プログラムに問題点があることが指摘された。暗号通信のための鍵を生成するプログラム（すなわち鍵管理）に問題があ

り、暗号が容易に破られてしまうことが分かった。その報道を受けて、当時インターネットを利用したオンライン・バンキングのサービスを提供していた米国の銀行は、相次いでサービスの停止に踏み切った。この事例は、善意の解析者が問題点を指摘したという点で、個々の利用者の被害を未然に防ぐ効果があり、暫くして問題点を修正したプログラムが Ver.2.0 として配布されたことによって解決されたが、暗号技術の問題が決済システムに深刻な影響を与え得ることを示していると思われる。

電子マネー・電子決済が実験的適用の段階でも、攻撃を狙う者は当該システムについての解析を欠かさないと考えるのが自然であろう。悪意の解析者は実験段階で弱点を指摘したりはせず、広く使われるようになった時に攻撃するために備えていると見るべきである。従って、実験段階で問題点が指摘されなかったとしても、当該システムに重大な欠点が潜んでいないとはいえない。

仮に上記と同様の事件が、広く電子マネー・電子決済が普及した社会で発生した場合、決済サービスが提供できないという事態に陥る可能性がある。その意味では、将来、広く普及した局面を想定した場合、電子マネー・電子決済の技術的安全性を高めるような、政策的な配慮が必要になるものと思われる。

８．安全な情報セキュリティ対策を講じるために

既に述べたように、情報セキュリティ技術は総合技術であって、特定の技術のみ切り出してその強弱を論じても、システム全体の強度を評価したことにはならない。何とも迂遠なようだが、システムのセキュリティを評価するためには、そのシステムが採用しているセキュリティ・ポリシーから利用している個々の要素技術まで、ひとつひとつの詳細な評価を積み重ねることが必要になる。その作業は、システムの提供者が自らの安全のために真摯に進めるしかないが、なかなか実現することは大変である。

このような評価を行う場合、非常に大切と思われるのは、情報セキュリティ技術に関する過度の秘密主義を廃することだと考えられる。このような提案に対しては、「暗号とか情報セキュリティ技術というのは、そもそも外部者から情報を秘匿するための対策ではないか」との反論を受けるかもしれない。もとより、外部にセキュリティに関する情報を不必要に漏らすことは適当ではないし、共通鍵暗号であれ、公開鍵暗号であれ、秘密の「鍵」を安全に秘匿することがセキュリティの基礎であることは言うまでもない。しかし、暗号技術を利用したシステムの仕組みやそれに対する評価については、それをある程度開示

し、オープンな議論の俎上に乗せていくことが、良いセキュリティ対策を講じる上では不可欠と考えられる。

金融機関における情報セキュリティ対策においては、適切に開示して評価すべき部分と、厳格に機密として管理する部分とを区分することが大切である。しかし、現状を見ると、セキュリティに関連する情報は一律に機密として管理されるため、多くの情報は本来必要とされる以上に秘匿されてる傾向があるように思われる。セキュリティに対する過度な秘密主義は、経営層がセキュリティの問題に関与することを難しくするし、時にはそのシステムを維持管理している部門自身がその技術の詳細を把握できず、技術動向の変化をセキュリティ対策に正確に反映させることが難しいという深刻な事態に陥るケースもある。万一、金融機関のコンピュータ・システムのセキュリティに深刻な問題があった場合、巨額の損失に繋がるリスクがあり、実際、過去においてそのような事故が発生した事例も存在する。従って、情報セキュリティ対策は金融機関経営の問題として認識されることが必要である。

そのような情報セキュリティ対策に関連する情報を外部に対して秘密にすることによって、いかほどセキュリティが高まることになるのだろうか。勿論、機密通信やディジタル署名に利用される暗号の「鍵」については、極めて厳格にその機密を管理する必要がある。しかし、それ以外の情報については、仮に有効に外部と情報を隔離したとしても、そのシステムに関わった技術者は内部情報を知っている訳で、仮にシステムの仕様や構成が明らかにされるとシステムが脆弱になってしまうのであれば、そもそも最初から内部者に対しては脆弱であったと評価せざるを得ない。ネットワークを経由したコンピュータ犯罪が増えてきている現在でも、ハイテク犯罪の過半は内部者犯罪との統計がある。そのような前提に立てば、そもそも情報を外部から「隠す」ことは、さほど有効な対策でないことが分かる。

むしろ、金融機関は、自らの顧客に対して、達成しているセキュリティの水準について積極的に情報を開示し、その理解と信頼を得ようと努力していくことが望まれている。また、情報セキュリティ技術は専門技術であるため、外部の専門家にシステムの仕様や構成を開示し、その診断を受けることも有効であろう。こうした観点からも、金融機関が採用している情報セキュリティ技術について、適切な情報開示を行うことが重要と考えられる。

９．国際的整合性への配慮

わが国の金融業界における情報セキュリティ技術の適用のあり方を検討する場合、コンピュータ・システムの安全対策に対する国際的な関心の高まりの影響を考慮する必要がある。欧米主要国の金融業界においては、1998 年 7 月の DES 暗号解読実験の成功によって DES の強度低下が決定的なものとなったことを受け、従来利用していた DES に基づくセキュリティ対策を見直し、Triple DES に移行する動きが見られている。こうした動きが活発化すると、国際的に相互接続されたネットワークの一部を構成するわが国の金融ネットワーク・システムでどのような安全対策が講じられているかについて、海外の金融業界の関心が高まってくるものと考えるべきだろう。わが国の金融業界としても、国際的な整合性、説得性のあるセキュリティ対策を講じていくことが必要となってくるものと考えられる。

最近の DES を巡る問題は、仮に十分に安全性が検討され、信頼されて利用されてきたセキュリティ対策であっても、技術の進歩に伴ってその安全性、信頼性を急速に失うということが有り得ることを如実に示した例と言えるだろう。金融分野において有効な情報セキュリティ対策を講じ続けていくためには、最新の技術動向を常に注視していなければならない。仮に、構築したシステムのセキュリティ対策をブラックボックスのままとしてしまうと、こうした適切な情報セキュリティ技術のアップデイトが行われない惧れがある。こうした観点からも、情報セキュリティ技術が従来のタブーの頚木を解かれ、オープンな討議が可能となることが、金融業界がより安全な情報セキュリティ対策を講じていくためにも重要なことと考えられる。

以　上

【参考文献】

（審議会、研究会等報告書）

大蔵省銀行局･国際金融局、『電子マネー及び電子決済に関する懇談会報告書』、1997 年 5 月

大蔵省銀行局、『電子マネー及び電子決済の環境整備に向けた懇談会報告書』、1998 年 6 月

金融情報システムセンター、『電子決済研究会報告書』、1996 年 3 月

金融情報システムセンター、『電子決済研究会（第２部）報告書』、1997 年 3 月

金融情報システムセンター、『安全対策に関する情報開示研究会報告書』、1998 年 4 月

社会安全研究財団 情報セキュリテイ調査研究委員会、『情報セキュリティ調査研究報告書』、1997 年 4 月

社会安全研究財団 情報セキュリテイビジョン策定委員会、『情報セキュリティビジョン策定委員会報告書～安全なネットワーク社会の実現を目指して～』、1998 年 3 月

通商産業省機械情報産業局、『セキュリティ・プライバシー問題検討委員会報告書』、1995 年 7 月

通商産業省機械情報産業局、『電子商取引環境整備研究会－中間論点整理』、1997 年 11 月

法務省民事局、『電子取引法制に関する研究会報告書』、1998 年 3 月

郵政省電気通信局、『暗号政策と電子現金』、「電子決済、電子現金とその利用環境整備に関する調査研究会」報告書、1996 年 4 月

（技術標準、安全対策基準）

金融情報システムセンター、『金融機関等コンピュータシステムの安全対策基準』、1998 年 7 月

通商産業省、『コンピュータウイルス対策基準』、通商産業省告示第 429 号、1995 年 7 月

通商産業省、『コンピュータ不正アクセス対策基準』、通商産業省告示第 362 号、1996 年 8 月

Common Criteria Implementation Board, "Common Criteria for Information Technology Security Evaluation, Version 2.0," May 1998.（http://www.radium.ncsc.mil/tpep/library/ccitse/）

ISO/TC68/SC2, ISO/TR 13569 "Banking and related financial services – Information security guidelines," October 1997.

ISO/TC68/SC6, ISO 13491-1 "Banking – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods," May 1996.

ISO/TC68/WG3, ISO 7982-1 "Bank telecommunication – Funds transfer messages – Part 1: Vocabulary and universal set of data segments and data elements for electronic funds transfer messages," April 1998.

National Institute of Standards and Technology, "Data Encryption Standard（DES）," Federal Information Processing Standards Publication（FIPS PUB）46-2, December 13, 1993.

National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules," Federal Information Processing Standards Publication (FIPS PUB) 140-1, January 11,1994.（http://csrc.nist.gov/fips/fips1401.html）

（その他）

飯田全広・高橋勝己・宮田裕行・松本勉、「タイムメモリトレードオフ解読法による暗号強度評価装置の実現性検討」、『1998 年暗号と情報セキュリティシンポジウム講演論文集』、SCIS '98-6.2.C、電子情報通信学会、1998 年 1 月

岩下直行、「金融業務に利用される暗号技術と国際標準化」、『金融財政』、時事通信社、1998 年 6 月

岩下直行・谷田部充子、「金融分野における情報セキュリティ技術の国際標準化動向」、日本銀行金融研究所 情報セキュリティ・シンポジウム提出論文、1998 年 11 月

宇根正志・太田和夫、「共通鍵暗号を取り巻く現状と課題― DES から AES へ」、日本銀行金融研究所 情報セキュリティ・シンポジウム提出論文、1998 年 11 月

宇根正志・岡本龍明、「公開鍵暗号の理論研究における最近の動向」、日本銀行金融研究所 情報セキュリティ・シンポジウム提出論文、1998 年 11 月

金融情報システムセンター、『平成 10 年版 金融情報システム白書』、財経詳報社、1997 年 2 月

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評価」、日本銀行金融研究所 情報セキュリティ・シンポジウム提出論文、1998 年 11 月

藤井友位・NTT データ通信、『金融ネットワークマニュアル』、企画センター、1988 年 8 月

D.W. Davies and W.L. Price, “Security for Computer Networks － An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer,” Second Edition, John Wiley & Sons, 1989.

Electronic Frontier Foundation, “Cracking DES － Secrets of Encryption Research, Wiretap Politics & Chip Design,” O’Reilly & Associates, May 1998.

OECD, “Cryptography Policy: The Guidelines and the Issues － The OECD Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy," March, 1997.（http://www.oecd.org//dsti/sti/it/secur/prod/）