情報セキュリティ技術の信頼性を確保するために

松本 勉（まつもと つとむ）／岩下直行（いわしたなおゆき）

要 旨

暗号、電子認証、ICカード等の情報セキュリティ技術が、わが国の金融業界においても実務に利用されるようになってきた。欧米では、従来から、こうした情報セキュリティ技術が金融実務に利用されてきたが、わが国でも、その必要性が徐々に認識される状況にある。

オープンなネットワークで金融業務を提供する場合、金融機関がどのような情報セキュリティ技術を採用するかによって、業務の安全性が規定されることになる。もしもセキュリティ技術の選択を誤り、業務の安全性を十分に確保できなかった場合、当該金融機関は、セキュリティ侵害による業務の停滞や金銭的被害のリスクにさらされるだけでなく、レピュテーションを損ない、経営面にもダメージを受ける惧れがある。また、技術進歩や新しい攻撃法の登場等の環境変化に適切に対応できないと、従来想定していなかったリスクにさらされてしまう危険性もある。

こうした問題に対処するためには、暗号アルゴリズムなどの基礎技術については、政府機関や学界が進めている安全性評価と標準化の結果を参照していくことが考えられる。また、実装や運用管理などの応用技術については、第三者機関が評価・認定するという枠組みが実用化されつつあり、これを活用することが考えられる。さらに、万一システムに何らかのセキュリティ技術上の欠陥が発生した場合に、それが適切に報告される制度的な枠組みを整備していくことについても、今後検討が必要であろう。

わが国の金融機関は、こうしたさまざまな手段を活用しつつ、情報セキュリティ技術の選択について正確な判断を下し、金融業務の安全性を確保していくことが要請されているといえよう。

キーワード：情報セキュリティ技術、安全性評価、標準化、暗号、電子認証、ICカード

本稿は、2000年11月22日に日本銀行で開催された「第3回情報セキュリティ・シンポジウム」への提出論文に修正を施したものである。本稿に示された意見はすべて筆者達個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

松本 勉　横浜国立大学大学院環境情報研究院（E-mail: tsutomu@mlab.jks.ynu.ac.jp）
岩下直行　日本銀行金融研究所研究第2課（E-mail: iwashita@imes.boj.or.jp）

1．わが国の金融業界における情報セキュリティ技術の利用拡大

暗号、電子認証、ICカード等の情報セキュリティ技術が、わが国の金融業界においても実務に利用されるようになってきた。インターネットを利用した銀行取引や証券取引では、SSL[1]と呼ばれる暗号通信プロトコルによって暗証番号や取引内容の機密を保護することが一般的となっている。銀行が発行するキャッシュカード／デビットカードも、従来の磁気ストライプカードから、耐偽造性を高めたICカードへと移行するための検討が進められている[2]。これまで専用回線を使用したクローズド・システムであることを安全性のよりどころとしてきた銀行の勘定系システムにおいても、通信内容の機密保持や端末機器の認証のために、暗号や電子認証を利用しようとする動きが拡大している。欧米では、従来から、こうした情報セキュリティ技術が金融実務に利用されてきたが、わが国でも、その必要性が徐々に認識される状況になってきたといえよう。

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先が多かったため、情報セキュリティ技術はあまり利用されてこなかった。わが国の金融業界におけるコンピュータ・システムのセキュリティ対策といえば、オンライン・システムの障害による業務の停止を防ぐためのさまざまなバックアップ手段や、重要なデータに関する物理的なアクセス制御に重点が置かれ、そうした目的に関しては、世界的にみても最先端のシステムが利用されてきた。しかし、ここ数年のインターネットの普及に伴い、わが国の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することが大きな潮流となりつつあり、そうした環境のもとでのセキュリティ確保手段として、暗号、電子認証、ICカードなどの情報セキュリティ技術の重要性が高まってきている。

2．欧州諸国における情報セキュリティ・リスク顕現化の事例

そうした状況になると、金融機関がどのような情報セキュリティ技術を採用するかによって業務の安全性が左右され、金融機関の情報セキュリティ・リスクが規定されることになる。もしも金融機関が選択した情報セキュリティ技術によって業務の安全性を十分に確保できなかった場合、セキュリティ侵害による業務の

1 SSL（Secure Socket Layer）：ネットスケープ（Netscape）社が提唱する暗号通信、認証等のセキュリティ機能が付加された暗号通信プロトコル。

2 平成12年4月18日、全国銀行協会は、キャッシュカードのICカード化を進めるための環境整備として、同協会内に「ICカード標準仕様検討部会」を設置し、ICカードの新しい標準仕様を策定することとしたと発表した。

停滞や金銭的被害のリスクにさらされるだけでなく、金融機関としての信認を損なうレピュテーション・リスクや、訴訟を提起されるリーガル・リスクをも招来し、経営面にもダメージを受ける惧れがある。

こうした問題が顕現化した例として、最近、欧州の金融業界で注目を集めた2つの事件を紹介したい。欧州では、従来から、銀行取引のセキュリティを高めるために、暗号やICカードといった情報セキュリティ技術が広く利用されていたが、最近、こうしたシステムの信頼性を揺るがす事件がいくつか発生した。以下に紹介する2つの事件は、いずれも、金融機関やその顧客に金銭的被害が生じたわけではないが、セキュリティの脆弱性が金融機関のレピュテーション低下につながった事例である。

フランスでは、1999年から2000年にかけて、フランス銀行カード協会（Groupment des Cartes Bancaires、以下、CBと表記する。）のICカードに関するセキュリティの欠陥を巡る事件がマスコミで大きく報道され、注目を集めた。CBは、フランスの金融業界が1985年に共同で設立した非営利団体で、ICカードに関する技術研究や規格策定を行っており、各銀行は、その規格に準拠してICカードを発行している。フランスでは、CBがインフラとしてICカードやカードリーダーの標準規格の整備を進めた結果、ICカードの普及率が高まり、カードの不正使用も大幅に減少したと評価されてきた。ところが、そのCBのICカードが偽造され、不正使用される事件が起きた。この事件は、CBのICカードのうち、古い規格に準拠して製造されたものに搭載されているRSA公開鍵暗号の鍵長が、200ビット程度と短かったことに起因している。この程度の鍵長のRSAは比較的容易に解読できることが知られているが、CBは、その技術仕様を外部には公開していなかった。

新聞報道等によれば、ある技術者が、CBの発行するICカードとカードリーダーを解析してその技術仕様を入手し、偽造カードを製作した。当該技術者は、地下鉄の切符を購入して偽造カードの機能を確認し、CBにその偽造カードの「買取り」を要求したとされている。CBはその要求を断り、当該技術者は偽造カードを製作・使用した疑いにより逮捕された。この事件はフランス国内でセンセーショナルに報道され、また2000年3月には、何者かが当該ICカードに格納された暗号鍵の情報をインターネット上で公開したため、ICカードの脆弱性は周知のこととなり、業界全体としての信認が大きく損なわれた。

こうした事態に対し、フランス銀行は、2000年3月にプレスリリースを発表し、CBと加盟金融機関に対し、ICカードの安全性強化を要請していることを明らかにした。CBは、信頼性を回復させるために、RSAの鍵長を768ビットに伸ばした新しい規格に基づく、より安全性の高いICカードとカードリーダーを普及させることを表明したが、その移行にはカードリーダーの更新を含め、かなりのコストが必要といわれている。

ドイツでも、銀行の発行するICカードの安全性を巡る事件があった。ドイツの銀行業界では、デジタル署名用ICカードの規格を策定し、各銀行がそれに基づくIC

カードを発行している。当該規格の中では、ISO9796[3]に基づくメッセージ復元型のRSAデジタル署名を使用することが定められていた。ISO9796は、署名変換対象データに冗長性を持たせることによってRSAデジタル署名方式の安全性を高めた国際標準であり、十分な安全性を持つ技術と考えられていた。しかし、1999年に、ISO9796に対する新しい署名偽造攻撃法[4]の存在が明らかとなった。この攻撃法自体は理論的なものであり、ドイツのデジタル署名用ICカードに直接適用されたものではない。しかし、この潜在的な脅威によって、当該ICカードにより生成されたデジタル署名の信認が揺らぐこととなった。この事件は、一般にはさほど大きな反響があったわけではなかったが、情報セキュリティ技術者の間で注目を集め、RSAデジタル署名の実装方法の選択には細心の注意が必要であることを関係者に再認識させることとなった。

これらの事件を契機として、欧州の金融機関の間では、単に「暗号を利用している」、「ICカードを利用している」というだけでは十分ではなく、利用する情報セキュリティ技術が、最新の評価基準によりきちんと評価された、信頼できるものであることが必要であるという認識が強まっている。

3．信頼できる情報セキュリティ技術を選択することの重要性

これらの事例からわかるように、金融機関が情報セキュリティ対策を講じる場合、技術の選択が適当でなかったり、技術進歩等による環境変化に適切に対応できないと、従来想定していなかったリスクにさらされてしまう危険性がある。フランスの事件もドイツの事件も、当初システムを導入する際には、安全性について一定の検討を行ったうえで技術を選択したものであったが、その後の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安全でなくなってしまったものといえる。これらの事例は、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ことを物語っているといえよう。

そもそも情報セキュリティ技術は、悪意を持ったシステムへの侵入者・攻撃者に対抗するための手段であり、侵入者・攻撃者は、システムの最も脆弱な部分を狙って攻撃を行ってくると考える必要がある。システムの一部にわずかでも脆弱な部分があれば、それ以外の部分をどんなに適切に防御していようとも、その欠陥を衝か

3 ISO9796：1991年に策定された、メッセージ復元型デジタル署名方式の国際標準。

4 1999年4月、コロン（Coron）、ナカッシェ（Naccache）、スターン（Stern）が、ISO9796に対する署名偽造攻撃法を発表し（Coron *et al.*［1999］）、さらに1999年8月、カッパースミス（Coppersmith）、ハルビ（Halevi）、ジュトラ（Jutla）は、コロンらの攻撃法を改良した新たな攻撃法を発表した（Coppersmith *et al.*［1999］）。この間の経緯について解説した資料として、宇根・岡本［2000］がある。

れることにより、システム全体の安全性が低下してしまうということを意味する。これを金融機関のシステムの安全対策に当てはめると、金融機関は、暗号やICカードといった個々の技術の安全性だけではなく、運用面まで含めたシステム全体の安全性を評価したうえで、適切な技術を選択することが必要となっている。

それでは、わが国の金融機関が情報セキュリティ技術で自らの業務の安全性を確保しようとする場合に、信頼できる情報セキュリティ技術を見極め、適切に選択していくためには、どうすればよいのだろう。理想的な姿を思い描くならば、おのおのの金融機関が、候補となるさまざまな技術の信頼性について十分に検討したうえで、自らの業務におけるリスクを勘案して利害得失を判断し、利用すべき技術を選択していくことが望ましい。しかし、わが国の金融機関にとって、情報セキュリティ技術は耳新しいトピックであるうえ、技術自体が日進月歩で変化しているため、過去の経験や実績に基づいて技術を選択していくことは難しい。また、暗号や電子認証の仕組み、ICカードの内部構造等は複雑である上、それらの技術を実装し、1つのシステムとして組み立てていくためには、極めて幅広い分野の知識が必要とされるため、利用者自身がそうしたシステムの内容を正確に理解したうえで安全性を評価することも容易なことではない。

こうした問題に対処するための1つのアプローチとして、現在、各国で、政府機関や学界など、技術面での専門知識に優れ中立的な立場にある主体が、一定の基準に基づき、情報セキュリティ技術の安全性を評価し、その結果を公表するという試みが進められている。これらは、例えば暗号アルゴリズムやデジタル署名方式など、情報セキュリティの基礎となる技術を対象とするものであり、安全性が高いと評価された技術は、国際標準や政府調達標準として選定されることも多い。利用者は、評価機関の評価結果や国際標準を参考に、自らが採用する技術を選択することで、信頼性を確保することができる。

一方、より実装や運用に近い応用技術の領域については、技術自体が多様であるため、基礎技術に適用されるような精緻な評価を行うというアプローチが難しかった。しかし、最近、安全性評価に関する市場ニーズの高まりを反映して、第三者機関が、ビジネス・ベースで、おのおのの製品や各企業の運用管理を外部から評価・認定するという枠組みが提案され、実用化されつつある。以下では、この2つのアプローチについてみていくこととしたい。

4．暗号アルゴリズム等の安全性評価と標準化

情報セキュリティ技術のうち、暗号アルゴリズムやデジタル署名方式などの基礎技術については、その信頼性を高めるために、中立的な機関による安全性評価と、その評価結果に基づく標準化が行われてきた。暗号アルゴリズムは、情報セキュリティ技術の心臓部とでもいうべき重要な要素技術であり、万一、欠陥がみつかれば、その暗号アルゴリズムを利用している通信プロトコルや業務アプリケーションな

ど、極めて広範囲に問題が波及する。一方、暗号アルゴリズムの原理やそれに対する攻撃法は、極めて高度な分析が必要とされる研究領域であり、一般の利用者には特に評価が難しい部分である。このため、信頼性の高い中立的機関が安全性を十分に吟味し、標準化を行うことによって、利用者がその技術を安心して利用できるようにしてきた。

従来、こうした暗号アルゴリズムの安全性評価と標準化は、米国を中心に進められてきた。DES（Data Encryption Standard）は、米国連邦政府の政府調達標準（FIPS: Federal Information Processing Standard）として選定されたものであり、また、DESの後継暗号として金融業界で広く普及しつつあるトリプルDESは、米国の金融業界の標準化団体であるANSI X9（事務局は米国銀行協会）によって米国国内標準（X9.52）として制定されている。

さらに、最近、米国政府は、次世代の政府調達標準暗号AES（Advanced Encryption Standard）を選定するために、米国内外から広く候補を募ってコンテストを実施した。DESはブロック長64ビット、鍵長56ビットのブロック暗号であったが、AESでは、ブロック長として128ビット、鍵長として128、192、256ビットが利用可能とすべきだとされ、全数探索法や暗号文一致攻撃に対して十分な安全性を確保できるスペックが求められていた。そのうえで、提案された暗号アルゴリズムの安全性、効率性等を評価して最も優れたアルゴリズムを選定することにより、今後20～30年程度の長期間にわたって安全に利用可能な標準暗号を選定することが企図されていた。

具体的には、米国商務省の下部機関であるNISTが事務局となって、1997年1月にAESのプロジェクトをスタートさせ、候補アルゴリズムを全世界に公募した。1998年8月に行われた第1次選考において候補は15に絞られ、1999年4月の第2次選考においてさらに5つに絞られた。そして、最終選考（2000年10月）において、ベルギーのバンクシス（Banksys）社のデェーメン（Daemen）とルーベン・カトリック大学のライメン（Rijmen）によって開発されたラインドール（Rijndael）がAESとして選定された。NISTは、ラインドールを選定した理由について、「安全性、処理速度、効率性、実装性、柔軟性等が最もバランス良く設計されていたため」としている。

これまで暗号アルゴリズムの安全性評価と標準化が米国を中心に進められてきたのは、米国において、政府と金融業界が暗号技術の大口ユーザーとしてのニーズを有してきたという要因が大きいと考えられる。新しい暗号アルゴリズムの開発は、わが国を含め世界各国で盛んに行われてきたが、ビジネスに利用される技術として普及する際には、信頼性の高い中立的な機関による安全性評価が必要であり、さらに、標準化が普及に弾みをつける力となる。こうした安全性評価や標準化はコストの掛かるものであるため、政府と金融業界という巨大なマーケットを持ち、関係者がコストを分担できる米国が有利であった。一方、わが国では、従来、情報セキュリティ技術の利用ニーズがあまり高まってきていなかったこともあり、そうした技術の普及の大前提となる安全性評価や標準化について、体制整備が十分でなかったようにうかがわれる。

しかし、近年、インターネットの普及によって暗号技術の応用範囲が飛躍的に拡大した結果、米国以外でも、暗号アルゴリズムの安全性評価や標準化にイニシアチブを発揮しようとする動きが出始めている。すなわち、①ISO/IEC JTC1/SC27[5]における暗号アルゴリズムの国際標準化（ISO18033）、②欧州のNESSIEプロジェクト[6]、③わが国の暗号技術評価委員会（CRYPTREC）[7]、などである。

5．情報セキュリティ機器や運用管理に関する評価・認定

一方、情報セキュリティ機器やシステムの運用管理のような、個別具体的な情報セキュリティ技術の適用場面については、第三者機関による評価・認定スキームとして、ISO15408[8]やBS7799[9]といった標準が提案され、実用化されつつある。情報セキュリティ技術の評価・認定スキームに対するニーズが強まってきた背景としては、次のような点が挙げられよう。

① 情報セキュリティ技術を実装した製品やサービスが増加し、さまざまな業者がその提供者となった結果、ある製品やサービスがある標準への準拠を謳っていたとしても、利用者からみて、それが信頼できないというケースが増えてきたこと。

② 従来であれば、システムを構築するSI業者（システム・インテグレーター）が、セキュリティ関連機器を含めて、その技術内容を十分に把握し、その信頼性を保証していたが、分散システム化、マルチベンダー化などの結果、SI業者にとっても、ブラックボックスとなる機器を使用する割合が増えてきていること。

5 SC27（ISO/IEC JTC1/SC27）：汎業界的なセキュリティ技術に関する国際標準を策定するISOの専門委員会。

6 NESSIE（New European Schemes for Signature, Integrity and Encryption）プロジェクト：欧州域内で利用される暗号アルゴリズムを標準化するために、ベルギーのルーバン・カトリック大学のプリニール（Preneel）教授らが中心となって、2000年1月に開始された。現在、安全性評価等の作業が進められており、2002年12月を目途に、評価結果が公表される予定である。NESSIEプロジェクトの標準化の対象は、共通鍵ブロック暗号に加え、ストリーム暗号、デジタル署名、公開鍵暗号アルゴリズム等を含んでいる。

7 暗号技術評価委員会（CRYPTREC）：2003年度を目途として構築が予定されている「電子政府」において利用可能な暗号アルゴリズムをリストアップすることを目的として、各種暗号アルゴリズムの性能等を客観的に評価するために、通産省によって組成された、わが国の有力な暗号学者、暗号研究者をメンバーとする委員会。

8 ISO15408：欧米主要国におけるセキュリティ関連機器の調達基準を統合して開発されたセキュリティ評価基準の国際標準。第三者機関がセキュリティ関連機器の安全性を評価・認定する仕組みを規定している。ISO15408およびBS7799については、宇根・中原［2000］を参照。

9 BS7799：利用者サイドにおける情報セキュリティ技術の運用管理方法を規定した英国の国内標準。BS7799-1とBS7799-2の2つのパートから構成されており、BS7799-1は、情報セキュリティ対策を実施する際の留意点をガイドラインとして規定し、BS7799-2は情報セキュリティ管理に関する評価・認定スキームを規定している。英国の国内標準ではあるが、欧州各国では、金融分野をはじめとして幅広く利用されている。このうち、BS7799-1については、2000年7月に、英国がSC27において国際標準化を提案し、世界各国による投票により支持されたため、2000年12月に、国際標準ISO17799として発行された。

③　インターネットの普及などの結果、一般の利用者もシステムのセキュリティ対策について関心を持つようになり[10]、その結果、例えば金融機関のようなサービスの提供者にとっても、第三者による評価・認定を受けていることが、顧客への説明手段として有効という考え方が出始めてきたこと。

この結果、情報セキュリティ技術の分野でも、何らかの標準に準拠していることを第三者機関が評価、認定するという方向に、大きな変化が生じている。こうした動きは、情報セキュリティ技術の実務への適用が比較的早かった欧米の金融業界において、その典型例をみることができる。

ひとつの注目すべき動きは、米国の金融業界の標準化機関であるANSI X9が米国政府（NIST）と協力して構築している「技術標準適合性評価制度（ANSI / NIST Standards Validation Program）」というアプローチである。近年、米国金融業界で利用される国内標準は、技術的に非常に高度なものとなっているため、ユーザーである金融機関がこれらの標準を実際の業務に適用する際に、その適合性を評価することが難しくなっている。この問題に対処するために、ANSI X9では、米国政府による適合性評価制度を準用する形で金融機関向けの制度を導入することとした。この制度では、セキュリティ機器の製造業者や新たなシステムを構築した金融機関は、その機器やシステムがANSI X9の国内標準に適合していることを確認してもらうために、政府が認定した研究機関に評価を依頼する仕組みとなっている。これにより、金融機関は、専門の研究機関により標準適合性評価を受けた製品を調達することが可能になる。この仕組みは、暗号モジュール機器に関する米国政府標準FIPS 140-1、140-2[11]等において実施されている適合性評価制度を、金融用途に利用される一般的なセキュリティ機器に拡大するものといえる。従来、金融分野では、標準への適合性を外部機関が評価する枠組みがなかったが、情報セキュリティ技術に対する信頼性を確保するための枠組みとして、こうした制度が米国で導入されようとしていることは、注目に値するといえよう。

6．情報セキュリティ技術の脆弱性の報告を受けるための仕組み

このように、情報セキュリティ技術の信頼性を確保するためのさまざまな仕組みが実用化されつつあるが、これらをいかに有効に活用しても、システムに何らかの

10 例えば、2000年5月に、デビットカード・システムのセキュリティに関するテレビの報道が相次いだことなどは、こうした一般の関心の高まりを示す証左といえよう。

11 FIPS140-1, 2：情報システムで重要な情報を保護するための暗号モジュールが満たすべき要件について規定した米国の政府調達標準。情報の重要度を4つに分類し、これに応じて暗号モジュールが満たすべきセキュリティ・レベルも4つに分類されている。1994年に発表されたFIPS140-1では、セキュリティ要件は、暗号モジュールの設計と実装にかかわる11分野を網羅している。1999年11月に公開されたFIPS140-2では、セキュリティ要件に改訂が加えられ、新しい攻撃法に対する対処法に関する規定が追加された。

セキュリティ技術上の欠陥が存在する可能性はゼロにはならない[12]。そのような欠陥は、存在しないことが最も望ましいが、仮に存在した場合、できるだけ早い段階でみつけ出せた方がよい。以下では、万一、金融システムで情報セキュリティ技術の利用に関する欠陥が指摘される事態となった場合、どのような体制が整備されていることが望ましいかについて整理する。

情報セキュリティ技術を利用している金融機関の立場からみると、システムの欠陥を指摘されることは快いものではなく、また、特に公表された場合、レピュテーションの低下につながることもあり、できるだけ発見されないことが望ましいと思うのが普通であろう。しかし、事実として欠陥があるならば、これを早期に発見し対応策を講じていくことが重要である。したがって、仮に外部の研究者などから欠陥を指摘してもらえるとすれば、むしろ、それを幸運と捉えるべきであろう。

従来、情報セキュリティ技術の研究においては、学会等で発表された方式について欠陥を発見したら、これを学会等で発表するという伝統が培われてきた。これは、欠陥を知らずにその技術が実際に使われたり、その技術をベースとした技術が提案されたりすることを通じた被害の拡大を防止するためでもあると同時に、学術的には、なぜそうした欠陥が生じるのかを解明する道を開き、新たな評価基準の作成や新たな技術開発への貢献を図るためでもある[13]。

金融機関が業務に使用するソフトウェアやハードウェアがどのようなセキュリティ技術を採用しているかは、必ずしも公表されないことが多い。また、採用されている技術自体が論文や特許等で公表されていないものである場合もありうる。しかし、仮に、一般の利用者が直接利用するシステムにおいて、使用されているソフトウェアやハードウェアに欠陥が存在したとすれば、その欠陥はいつかは発見されるであろう。セキュリティ技術の利用が拡大すればするほど、セキュリティ製品やシステムの欠陥をみつけ出すことができる人の数も増加していく。動機はさまざまであっても、開発者とは異なった発想でセキュリティ製品やシステムの解析を試みる人々が多数存在しうるのである。

実際に運用されている金融関連のシステムについて、セキュリティ技術に欠陥があることを発見した人は、どのように振る舞うであろうか。彼がセキュリティ技術の発展に寄与することを願う人であれば、何らかの形で当該システムの提供者に知らせたいと思うであろう。また、例えば、金融取引カードが簡単に偽造できてしまうなど、その欠陥が深刻であり、別のだれかが既に気づいて不正を行っているかもしれない場合には、被害を抑えるために、早期かつ明確にその欠陥を公表して、欠

12 2章で紹介したドイツのデジタル署名用ICカードの事件は、ISOによって安全性が評価され、標準化されたデジタル署名方式（ISO9796）について、セキュリティ技術上の欠陥が発見されたものである。

13 例えば、本稿の共同執筆者である松本を含む研究チームは、最近学会で発表した論文において、情報セキュリティ機器として市販されている指紋照合装置が、安価に作成された人工的な指の模型を受け入れてしまうことを実験によって確認し、指紋照合装置の安全性向上の必要性を指摘した（山田・松本・松本［2000a、2000b］）

陥の存在する技術の拡散に対する警鐘を鳴らすべきとの考え方もありえよう。しかし、公表という手段をとった場合、有効な対策が講じられない間にその欠陥が悪用されて、かえって被害を拡大してしまうこともありうるし、レピュテーションの低下という形で当該システム提供者の経営にダメージを与えてしまう可能性もある。

また、欠陥を発見する人は、必ずしもセキュリティ技術の発展に寄与することを願う人ばかりとは限らない。単に、ハッカー仲間の世界で実力を示して有名になりたいといった動機で、アンダーグラウンドのネットワークに欠陥の情報を流す人もいるかもしれない。あるいは、その欠陥に対する防御方法を開発してビジネスにつなげたいといった動機を持つ人は、欠陥に関する情報の公開が求められるような状況においても、自らの開発が完了するまで、これを秘匿しようとするかもしれない。

このようにみてくると、セキュリティ技術の欠陥を発見した人の処遇や発見された情報の取扱いについて、何らかの制度的な対応が必要であるように思われる。例えば、セキュリティ技術の欠陥を発見した場合、そこに届け出ると、その人の発見者としての名誉が保証され、場合によっては経済的な報酬も得られるような届出機関を作り、届けられた欠陥はそこで吟味されてから、適切な方法で公表される、というような仕組みも考えられる。ちなみに、こうした仕組みは、例えばネットワーク・セキュリティに関するセキュリティ・ホールを指摘する自主的な制度としては、既に広く普及している。

7．おわりに

本稿では、金融機関が信頼できる情報セキュリティ技術を選択するうえでの基本的な考え方や、参考となる技術研究動向について説明した。

かつて、暗号アルゴリズムといえばDESしかなく、情報セキュリティ機器も少数のベンダーの提供する製品に限られていた時代には、金融機関が情報セキュリティ技術の選択にさほど深刻に悩む必要はなかった。そもそも選択肢が少なく、一定のセキュリティ評価の行われた製品が提供されることが多かったからである。また、従来のクローズド・ネットワーク環境下では、金融機関のセキュリティ対策に関する情報が外部に公開されること自体がほとんどなく、万一、何か問題のある技術を使っていたとしても、それが金融機関のレピュテーションの低下につながることはまれであった。

しかし、情報通信技術の発達とオープン・ネットワークの普及は、情報セキュリティ技術の裾野を広げるとともに、金融機関のセキュリティ対策にも、極めて豊富な選択肢を与えることとなった。金融機関がオープン・ネットワークを用いた新しい金融サービスに挑戦したり、既存の金融サービスにおけるセキュリティ対策を強化するためには、最新の情報セキュリティ技術を活用することが必要となっている。このような環境変化は、金融機関にとって、新しい時代に対応したビジネスを効率的に行う道が拓けたと評価できる反面、金融機関が新たに深刻な検討課題を抱え込

んだ状況ともいえる。特に、情報セキュリティ技術は、伝統的に、システムを守る側と攻撃する側のせめぎ合いの中から技術進歩が生み出されてきた技術分野であり、現時点でどんなに優れた技術と評価されていようとも、いつ、時代遅れの技術と評価されてしまうかわからないという性格を持つ。

このため、わが国の金融機関が情報セキュリティ技術を利用していくに当たっては、さまざまな手段を活用しつつ、情報セキュリティ技術の選択について正確な判断を下すとともに、万一問題が生じた場合、直ちに適切な対応をとることにより、金融業務の安全性を確保していくことが要請されているといえよう。本稿が、わが国の金融機関におけるこうした新しい課題への対応の一助となれば幸いである。

参考文献

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」、『金融研究』第18巻第2号、日本銀行金融研究所、1999年4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―」、『金融研究』第18巻第2号、日本銀行金融研究所、1999年4月

――――・岡本龍明、「最近のデジタル署名における理論研究動向について」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年4月

――――・中原慎一、「最近の金融業務における情報セキュリティ評価・認定を巡る動向について」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年4月

情報処理振興事業協会、「平成11年度　スマートカードの安全性に関する調査　調査報告書」、2000年2月

日本銀行、「金融機関における情報セキュリティの重要性と対応策 ――インターネットを利用した金融サービスを中心に ――」、2000年4月

松本 勉・岩下直行、「金融分野における情報セキュリティ技術の現状と課題」、『金融研究』第18巻第2号、日本銀行金融研究所、1999年4月

――――・――――、「金融業務と認証技術：インターネット金融取引の安全性に関する一考察」、『金融研究』第19巻別冊第1号、日本銀行金融研究所、2000年4月

山田浩二・松本弘之・松本 勉、「指紋照合装置は人工指を受け入れるか」、『電子情報通信学会技術研究報告』Vol. 100 No.213、ISEC2000-45、電子情報通信学会、2000年7月a

――――・――――・――――、「指紋照合装置は人工指を受け入れるか（その2）」、『コンピュータセキュリティシンポジウム2000論文集』、情報処理学会シンポジウムシリーズVol. 2000 No.12、情報処理学会、2000年10月b

American National Standards Institute, “X9.52 - 1998, Triple Data Encryption Algorithm Modes of Operation,” 1998.

Coppersmith, D., S. Halevi, and C. Jutla, “ISO 9796-1 and the new forgery strategy,” submission to IEEE P1363a, August 23, 1999.(http://grouper.ieee.org/groups/1363 /contrib.html)

Coron, J.S., D. Naccache, and J. P. Stern, “On the Security of RSA Padding,” *Proceedings of CRYPTO '99*, LNCS 1666, pp.1-18, Springer-Verlag, 1999.

Daeman, J. and V.Rijmen, “AES Proposal: Rijndael”, June 11, 1998.
(http://www.esat.kuleuven.ac.be/rijmen/rijndael/Rijndaeldoc.pdf/)

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