# 第3回情報セキュリティ・シンポジウムの模様
## ― 情報セキュリティ技術の評価と信頼性 ―

### 1. はじめに

日本銀行金融研究所では、2000年11月22日、「情報セキュリティ技術の評価と信頼性」をテーマとして、第3回情報セキュリティ・シンポジウムを開催した。

いわゆるIT革命が進展し、金融分野においてもインターネットや携帯電話を活用した新しいサービスが拡大する中で、情報セキュリティ技術の重要性が高まっている。オープンなネットワークを利用して銀行取引や証券取引を行う場合、利用者の真正性を確認したり、送受信される個人情報や機密情報を保護したりするためには、暗号、電子認証といった情報セキュリティ技術の活用が必要である。わが国の金融業界においても、このところ、勘定系システムへの暗号の導入や、キャッシュカードのICカード化など、情報セキュリティ技術を積極的に活用する動きが始まりつつある。こうした状況において、金融機関は、「信頼できる情報セキュリティ技術を適切に選択する」ことが必要となる。現在、情報セキュリティ技術を提供する側からは、安全性を評価し、信頼性を保証するためのさまざまな仕組みが提案されているが、情報セキュリティ技術を利用する側としても、こうした仕組みを的確に把握し、技術の選択に有効に活用していくことが求められている。

日本銀行金融研究所では、1998年と1999年に、第1回と第2回の情報セキュリティ・シンポジウムを開催し、金融機関による新しい金融サービスの提供等に関連する情報セキュリティ技術について、最新の技術動向を紹介してきたが、今回のシンポジウムでは、情報セキュリティ技術が金融機関の実務に積極的に活用されつつあることを踏まえて、情報セキュリティ技術の安全性評価や信頼性確保の問題を取り上げることとした。シンポジウムの構成は、キーノート・スピーチ、2つのパネルディスカッション、1つの研究発表から成る。プログラムの詳細は次のとおりである。

＜プログラム＞

▼キーノート・スピーチ：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（横浜国立大学助教授）

▼パネルディスカッション1：暗号アルゴリズムの安全性評価と国際標準化

・導入報告①：今井秀樹（東京大学教授）

・導入報告②：櫻井幸一（九州大学助教授）

・パネリスト：松本 勉（横浜国立大学助教授）
東井芳隆（通商産業省機械情報産業局情報セキュリティ政策室長）
岡本龍明（NTT情報流通プラットフォーム研究所主席研究員フェロー）

・モデレータ：岩下直行（日本銀行金融研究所研究第2課調査役）

▼発表：電子文書の送受信証明を行うためのプロトコルの研究動向と安全性評価

・発表　　：宇根正志（日本銀行金融研究所研究第2課）

・コメント：櫻井幸一（九州大学助教授）

▼パネルディスカッション2：ICカードの安全性評価を巡って

・導入報告①：植村泰佳（電子商取引安全技術研究組合常務理事）

・導入報告②：廣川勝久（ジー・ピー・ネット技術顧問）

・導入報告③：古原和邦（東京大学助手）

・モデレータ：岩下直行（日本銀行金融研究所研究第2課調査役）

▼総括コメント

・今井秀樹（東京大学教授）

今回のシンポジウムのフロアには、暗号学者、金融業務と情報セキュリティ技術に関係の深い官庁関係者、金融機関や電機メーカーの研究開発部門・標準化部門の実務家や技術者等、約80名の参加を得たほか、日本銀行職員約20名が参加した。以下では、プログラムに沿って、シンポジウムにおける発表や議論の概要を紹介する（文責：日本銀行金融研究所、なお、肩書きはシンポジウム開催時点のものであり、また本文中では敬称を省略している）。

## 2. キーノート・スピーチ：情報セキュリティ技術の信頼性を確保するために

**松本**は、本シンポジウムのキーノート・スピーチとして、**岩下**との共同執筆による提出論文[1]に基づき、金融機関が「信頼できる情報セキュリティ技術」を選択することの重要性を強調し、そのために考えられる対策を紹介する発表を行った。

まず、金融機関が、自ら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確保できなかった場合、業務の停滞や金銭の損失といった直接的な被害だけではなく、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とを指摘し、その具体的な事例として、フランスとドイツで発生したICカードのセキュリティ侵害を巡る事件を紹介した。そして、こうした事例を踏まえ、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く必要があることを指摘した。

次に、こうした問題への対応策について、理想的には、おのおのの金融機関が、候補となる技術の信頼性を十分検討し、自らの業務におけるリスクを勘案して最適な安全対策を選択することが望ましいものの、それは容易ではないと指摘したうえで、現実的な対応策として、次の3つの手段を紹介した。

第1に、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については、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、一定の基準に基づいて安全性を評価したり、国際標準や政府調達標準を選定するといった作業が進められており、こうした評価結果や国際標準等を参考とすることによって、信頼性を確保することが考えられると指摘した。

第2に、情報セキュリティ機器やシステムの運用管理など、個別具体的な情報セキュリティ技術の適用事例については、第三者機関による評価・認定の仕組みとして、ISO15408 やBS7799といった標準が提案され、実用化されつつあることを紹介した。

最後に、事前にどのような対策を講じても、システムに何らかの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ため、万一何らかの問題が発生した場合、できるだけ早い段階に適切な報告が行われるように制度的な枠組みを整備すべきであることを指摘した。そして、具体的な仕組みの一例として、セキュリティ技術の欠陥を発見した人からの届出に基づき、これを吟味のうえで適切な公表を行う届出機関の構想を提示した。

1 松本勉・岩下直行、「情報セキュリティ技術の信頼性を確保するために」（本号所収）を参照。

## 3. パネルディスカッション1：暗号アルゴリズムの安全性評価と国際標準化

パネルディスカッション1では、暗号アルゴリズムの安全性評価と国際標準化をテーマに、**今井**、**松本**、**櫻井**、**岡本**、**東井**をパネリストに迎えて議論を行った。まず、**今井**と**櫻井**が導入報告を行い、続いて自由討議が行われた。

### (1) 導入報告①：暗号技術評価委員会における活動状況

まず最初に、**今井**が、暗号技術評価委員会（CRYPTREC）の活動状況について以下のとおり説明した。

CRYPTRECは、2003年度を目途として構築が予定されている「電子政府」における暗号アルゴリズムの利用に向けて、各種暗号アルゴリズムの性能を、技術的・専門的見地から客観的に評価するために設立された委員会であり、通商産業省（現在の経済産業省）の委託により、情報処理振興事業協会（IPA）が事務局を務め、暗号学者、暗号研究者11名が参加している（委員名簿：表1）。

表１　CRYPTRECの委員名簿

| | | |
|---|---|---|
| 委員長 | 今井秀樹 | 東京大学生産技術研究所教授 |
| 委員 | 岩下直行 | 日本銀行金融研究所調査役 |
| 委員 | 岡本栄司 | 東邦大学理学部教授 |
| 委員 | 岡本龍明 | NTT情報流通プラットフォーム研究所主席研究員フェロー |
| 委員 | 金子敏信 | 東京理科大学理工学部教授 |
| 委員 | 櫻井幸一 | 九州大学大学院システム情報科学研究院助教授 |
| 委員 | 佐々木良一 | 株式会社日立製作所システム開発研究所主管研究長 |
| 顧問 | 辻井重男 | 中央大学理工学部教授 |
| 特別委員 | 苗村憲司 | 慶應義塾大学環境情報学部教授 |
| 委員 | 松井 充 | 三菱電機株式会社情報技術総合研究所チームリーダー |
| 委員 | 松本 勉 | 横浜国立大学大学院工学研究科助教授 |

電子政府を実現するためには、セキュリティの共通基盤の確保が重要な課題とされており、なかでも暗号技術は、電子化された情報の守秘性および非改ざん性の確保や、電子認証の実現のための重要な基盤技術と位置付けられている。電子政府で利用される暗号アルゴリズムについては、十分に安全性が評価されたものである必要がある。このため、CRYPTRECでは、2000年6～7月に、「わが国の電子政府システムに適用可能な暗号技術」について、詳細な技術要件を定めて一般公募を行った。これに応募された暗号アルゴリズムを、書類審査であるスクリーニング評価、実装評価である詳細評価の2段階で評価し、安全性、実装性等の特徴を分析・整理したリストを作成する予定となっている（作業スケジュール：表2）。

表2　CRYPTRECの作業スケジュール

| | 2000 | | | | | | | 2001 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 1 | 2 | 3 | 4 |
| 公募 | ← | → | | | | | | | | | |
| スクリーニング評価 | | | ← | → | | | | | | | |
| 詳細評価 | | | | | ← | | | | | → | |
| 結果報告 | | | | | | | | | | | ☆ |

CRYPTRECの評価対象は、公開鍵暗号、共通鍵暗号、ハッシュ関数[2]、疑似乱数生成アルゴリズム[3]である。公開鍵暗号については、暗号プリミティブ[4]ではなく、暗号スキーム[5]を募集対象とし、守秘、署名、認証、鍵共有の4つの用途に分けて評価を進めている。共通鍵暗号については、ストリーム暗号[6]、64ビット・ブロック暗号[7]と128ビット・ブロック暗号に分けて評価を進めている。

CRYPTRECでは、2000年8～9月にスクリーニング評価を実施し、その結果、公開鍵暗号15件、共通鍵暗号12件、疑似乱数生成アルゴリズム1件を詳細評価の対象とした。また、CRYPTRECでは、既に広く普及しており、安全性や処理速度に関する研究成果も充実していて信頼性が高いと認められるデファクト標準の暗号アルゴリズムを、「その他評価が必要と判断される暗号技術」として評価対象に追加することとしている。これらも含めると、現在、評価の対象となっている暗号技術は、公開鍵暗号19件、共通鍵暗号14件、ハッシュ関数3件、疑似乱数生成アルゴリズム2件である（表3）。

CRYPTRECでは、現在、詳細評価の作業を進めており、最終的な評価結果は2001年4月に公開される予定である。

CRYPTRECは、電子政府において信頼性の高い暗号技術が適切に利用される環境を整備するという、大変重要な役割を担っている。このプロジェクトを成功させるためには、ISOにおける国際標準化や、米国、欧州における安全性評価プロジェ

2 ハッシュ関数：任意長の入力データを固定長の「ハッシュ値」に圧縮する関数のこと。ハッシュ値から原文を再現することはできず、また同じハッシュ値を持つ異なるデータを作成することは極めて困難であるような性格を持つものが利用される。

3 疑似乱数生成アルゴリズム：適当な長さの入力ビット・パターンから、みかけ上ランダムなビット･パターン（疑似乱数）を生成するアルゴリズム。疑似乱数は、ストリーム暗号における鍵ストリームの生成や、公開鍵暗号における秘密鍵、暗号文、電子署名の生成等に用いられる。

4 暗号プリミティブ：RSA暗号やElGamal 暗号のような基本的な公開鍵暗号方式の原理等、暗号通信や電子認証のコアとなる要素技術のこと。

5 暗号スキーム：暗号プリミティブと補助関数（ハッシュ関数、疑似乱数等）とを用いて暗号通信や電子認証といった機能を実現させるための具体的な方式のこと。RSA暗号とハッシュ関数を用いて構成されるRSA-OAEP（注10参照）等を指す。

6 ストリーム暗号：暗号化する平文と同じ長さの鍵ストリームを疑似乱数生成アルゴリズム等によって生成し、平文と鍵ストリームの排他的論理和を計算することによって暗号文を生成する方式の共通鍵暗号。

7 ブロック暗号：暗号化する平文を一定の長さ（ブロック）ごとに分割し、ブロックごとに同一の鍵で暗号化を行う方式の共通鍵暗号。ブロック長の長さには、64ビット、128ビット等がある。

表３　CRYPTRECで現在評価の対象となっている暗号技術

| | | | アルゴリズム名 | 応募者 |
|---|---|---|---|---|
| 公開鍵暗号（19） | 守秘（6） | | RSA-OAEP | RSAセキュリティ（デファクト標準） |
| | | | HIME-2 | 日立製作所 |
| | | | EPOC暗号 | NTT |
| | | | PSEC暗号 | NTT |
| | | | ECAES | 富士通／Certicom |
| | | | ACE Encryption | 日本IBM |
| | 認証（1） | | ESIGN認証 | NTT |
| | 署名（7） | | RSA-PSS | RSAセキュリティ（デファクト標準） |
| | | | DSA署名 | （デファクト標準） |
| | | | MY ELLTY ECMR-192-h | 松下電器産業 |
| | | | MY ELLTY ECMR-OEF-h | 松下電器産業 |
| | | | MY ELLTY ECMR-160-h | 松下電器産業 |
| | | | ESIGN署名 | NTT |
| | | | ACE Sign | 日本IBM |
| | 鍵共有（5） | | DH鍵共有 | （デファクト標準） |
| | | | HIME-1 | 日立製作所 |
| | | | ECDHS | 富士通／Certicom |
| | | | ECMQVS | 富士通／Certicom |
| | | | HDEF-ECDH | 北陸先端科学技術大学院大学／松下電器産業 |
| 共通鍵暗号（14） | ストリーム暗号（2） | | MULTI-S01 | 日立製作所 |
| | | | TOYOCRYPT-HS1 | 東洋通信機 |
| | ブロック暗号（12） | 64bit | Triple DES | （デファクト標準） |
| | | | CIPHERUNICORN-E | NEC |
| | | | MISTY1 | 三菱電機 |
| | | | FEAL-NX | NTT |
| | | | Hierocrypt-L1 | 東芝 |
| | | 128bit | Rijndael | （デファクト標準） |
| | | | CIPHERUNICORN-A | NEC |
| | | | Camellia | NTT |
| | | | RC6 | RSAセキュリティ |
| | | | SC2000 | 富士通 |
| | | | MARS | 日本IBM |
| | | | Hierocrypt-3 | 東芝 |
| ハッシュ関数（3） | | | SHA-1 | （デファクト標準） |
| | | | MD5 | （デファクト標準） |
| | | | RIPEMD-160 | （デファクト標準） |
| 疑似乱数生成アルゴリズム（2） | | | SHA-1を使った疑似乱数生成器 | （デファクト標準） |
| | | | TOYOCRYPT-HR1 | 東洋通信機 |

クトと適切に協調していくことが必要である。また、こうした安全性評価の作業は、定期的に見直しを行うことが不可欠である。そうした役割を担うためにも、恒久的な暗号技術評価機関を設立することが望ましいと考えられる。

### (2) 導入報告②：ISO/IEC JTC1/SC27における暗号標準化

続いて、**櫻井**は、SC27[8]における暗号標準化について、以下のとおり説明した。

暗号アルゴリズムを普及させるためには、その安全性を正しく評価し、標準化を行うことが大切である。その代表的な成功例は、米国の連邦政府標準（FIPS）に選定されることで広く普及したDESである。しかし、ISOにおける国際標準化活動では、データ守秘を目的とする暗号アルゴリズムは対象とされてこなかった。これは、暗号の利用に関する政策が国ごとに異なっていたことに加え、暗号アルゴリズムの安全性を評価するためには大変なコストと技術力が必要であり、民間企業の自主的な集まりであるISOでは、その責務を担い切れないと考えられていたためであった。

その代わりに、SC27では、1991年に暗号アルゴリズムの登録制度であるISO 9979を発足させた。この制度は、登録に当たってアルゴリズムの開示や安全性評価を要求せず、必要な書類を整えればどのような暗号アルゴリズムでも登録できるものであるため、この制度に登録されている暗号は、必ずしも信頼性が高いものばかりとはいえなかった。1990年代後半には、DESの強度低下の問題が広く認識され、新しい暗号アルゴリズムに対するニーズが高まったが、ISO 9979による登録制度を利用することは適切な解決にはならなかった。こうした中で、米国や欧州は、独自に暗号アルゴリズムの安全性評価プロジェクトを開始させた。

米国では、1997年1月から、米国商務省の下部組織であるNISTを中心として、DESに続く次世代暗号技術の連邦政府標準を選定するために、AES（Advanced Encryption Standard）プロジェクトが開始された。暗号アルゴリズムを公募し、提案された暗号アルゴリズムの安全性、効率性、実装性等について2年半にわたって詳細な評価を行ったうえで、2000年10月、ベルギーのデェーメン（Daemen）とライメン（Rijmen）が開発したラインドール（Rijndael）をAESに選定した。

一方、欧州では、ベルギーのルーベン・カトリック大学のプリニール（Preneel）教授らを中心として、欧州域内で利用される暗号アルゴリズムの安全性評価と標準化を目指すプロジェクト、NESSIE（New European Schemes for Signature, Integrity and Encryption）が開始された。NESSIEにおいても、暗号アルゴリズムの公募を行い、その技術評価を行ったうえで、2002年12月を目途に評価結果を公表する予定としている。

8 SC27（ISO/IEC JTC1/SC27）：ISO（国際標準化機構）とIEC（国際電気標準会議）の共同専門委員会（JTC1）の分科会のひとつ。汎業界的な情報セキュリティ技術に関する国際標準の策定を担当している。

こうした中で、SC27においても、守秘目的の暗号アルゴリズムについて、国際標準化を進めることが決定され、1999年10月から、公開鍵暗号（守秘用）、共通鍵ブロック暗号、共通鍵ストリーム暗号を国際標準化するプロジェクト（ISO18033）が開始された。現在、各国から表4のような暗号アルゴリズムが提案されている。特に、多くの提案があった共通鍵ブロック暗号については、2000年10月に開催されたSC27の国際会議において、AES（ラインドール）とトリプルDES[9]が、ISO 18033に採択されることがほぼ確実となった。それ以外の暗号アルゴリズムについては、今後、NESSIEやCRYPTRECにおける安全性評価結果に基づいて絞り込みが行われていくものと考えられる。

表4　ISO18033に提案されたアルゴリズム

| | | | アルゴリズム名 | 提案国（提案企業） |
|---|---|---|---|---|
| 公開鍵暗号（6） | | | ACE Encryption | ドイツ |
| | | | RSA-OAEP | 米国・スウェーデン |
| | | | ECIES | 米国 |
| | | | HIME-2 | 日本（日立製作所） |
| | | | EPOC暗号 | 日本（NTT） |
| | | | PSEC暗号 | 日本（NTT） |
| 共通鍵暗号（14） | ストリーム暗号（1） | | MULTI-S01 | 日本（日立製作所） |
| | ブロック暗号（13） | 64 bit | IDEA | スイス |
| | | | CAST-128 | カナダ |
| | | | MISTY1 | 日本（三菱電機） |
| | | | Hierocrypt-L1 | 日本（東芝） |
| | | 128 bit | AES（Rijndael） | 米国 |
| | | | RC6 | スウェーデン |
| | | | SEED | 韓国 |
| | | | Zodiac | 韓国 |
| | | | Xenon | 韓国 |
| | | | Camellia | 日本（NTT） |
| | | | CIPHERUNICORN-A | 日本（NEC） |
| | | | Hierocrypt-3 | 日本（東芝） |
| | | | MARS | 日本（日本IBM） |

9 トリプルDESはどの国からも提案されてはいないが、広く利用されている共通鍵ブロック暗号アルゴリズムであることから、採択が確実視されている。

## (3) 自由討議

上記2件の導入報告を受けて、パネリストによる自由討議が行われた。

まず、**岡本**は、本シンポジウムの数日前に、安全性証明が付与された公開鍵暗号スキームRSA-OAEP[10]の証明に問題があるとの指摘[11]が公表されたことを紹介したうえで、万一標準化の対象となった暗号アルゴリズムの安全性に問題が生じた場合、標準化機関自身の信頼性や権威が揺らぐ惧れがあるため、暗号アルゴリズムの標準化を行う際には、対象となる技術の安全性を十分に評価することが必要不可欠であると述べた。

また、**東井**は、通商産業省において電子商取引や電子政府の実現を推進している立場から、CRYPTRECのプロジェクトを開始した背景について説明した。暗号技術によってサイバー空間の安全性、信頼性を確保することは、電子商取引等が円滑に発展していくための基盤となることを強調し、その整備を図るために、優れた暗号技術を自由に利用できる環境を確保していくことが大切であると指摘した。こうした観点から、欧米における政府利用暗号の選定や国際標準化が進む中で、国際的に高いレベルにあるわが国の暗号技術を適切に評価することによって、電子政府や民間における利用を促進することが、CRYPTRECの狙いのひとつであると述べた。なお、CRYPTRECは、2000年度には「我が国電子政府システムに適用可能な暗号技術のリスト」を作成することを目的とするが、2001年度も続行し、総務省と経済産業省の局長に直結する委員会としたうえで、特に優れた暗号アルゴリズムを選定する「絞り込み作業」を実施することが検討されていることを明らかにした。

続いて、モデレータである**岩下**が、米国でAESとしてラインドールが選定された一方、欧米の金融機関では、強度の低下したDESからトリプルDESへの移行が進んでいることを指摘し、トリプルDESとの対比で、今後、ラインドールがどのように普及するとみられるかについて、パネリストに意見を求めた。

これに対し、**松本**は、ラインドールの評価について、①AESプロジェクトで「安全性、処理速度、効率性、実装性、柔軟性が最もバランス良く設計されている」とされ、米国の連邦政府標準に選定されたこと、②2年半という時間をかけて評価が

10 RSA-OAEP（Optimal Asymmetric Encryption Padding）：ベラーレ（Bellare）とロガウェイ（Rogaway）によって1994年に提案されたパディング方法（OAEP）を用いて、RSA暗号の安全性を強化したデータ守秘用の公開鍵暗号スキーム。理想的なランダム関数が利用可能であり、RSA暗号関数が一方向性を有しているという仮定のもとで、能動的攻撃（攻撃者が暗号文に対応する平文を入手できる場合の攻撃）に対して強秘匿であることが証明されていると考えられていた。

11 RSA-OAEPは、「能動的攻撃に対する安全性が証明されている」ことを最大の特徴としている。しかし、2000年11月、IBMチューリッヒ研究所のシュープ（Shoup）は、ベラーレとロガウェイの原論文における安全性証明が、それまで信じられていた結論とは異なるものであることを指摘した。この指摘は直ちにRSA-OAEPの脅威となるものではなかったが、「安全性が証明されている」という主張について、十分な検証が必要であることが改めて認識されたほか、証明可能な安全性を持つ公開鍵暗号の代表といえるRSA-OAEPの信頼が揺らいだことは、研究者の間で注目を集めた。

行われたが、脅威となる攻撃法が発見されておらず、安全性に対する信頼性が極めて高いこと、の2点から、これから新しい暗号アルゴリズムの導入を検討する際に、ラインドールが最も有力な候補のひとつになることは確実との見解を示した。その一方、従来DESを利用していたユーザーが、移行が容易で実績の豊富なトリプルDESを選択することには合理的な理由があり、ラインドールを選ぶかトリプルDESを選ぶかは、各利用者の判断の問題であると述べた。また、この2つのアルゴリズムに限らず、AESをはじめとする各種の安全性評価プロジェクトにおいて、暗号アルゴリズムの詳細な評価結果が公開され始めているため、安全であることを確認して利用できる暗号アルゴリズムの候補が増えてきていることを指摘し、今後は各利用者が用途に合わせて安全な暗号アルゴリズムを選択して利用することが可能となってくるとの見解を示した。

これに関連して、**岩下**は、暗号アルゴリズムの利用者側では、通信の相互接続性向上やコスト低減化などの観点から、世界中で使用される暗号アルゴリズムがひとつに統一されることが望ましいという声も多いことを紹介し、唯一の国際標準暗号アルゴリズムを定めることの是非について、パネリストに意見を求めた。

これに対し、まず、**岡本**は、国際標準暗号アルゴリズムを一本化した場合、そのアルゴリズムに万一有効な攻撃法が発見されれば、世界中が危険に陥ることになると指摘し、リスク・ヘッジの観点からは、複数の暗号アルゴリズムを使い分けた方が安全であるとの見解を示した。また、**今井**は、複数の暗号アルゴリズムを搭載することによるシステムのコスト上昇率は数パーセントに過ぎなかったという実例を紹介したうえで、使用している暗号アルゴリズムの安全性の信頼が揺らいだ場合に迅速な対応が可能になるよう、複数のアルゴリズムを予め搭載しておくことが望ましいシステムもあることを指摘した。なお、**東井**は、暗号技術の進展を考慮するならば、情報システムに組み込まれる暗号化モジュールは、暗号アルゴリズムの安全性に問題が発見された場合等に備えて、容易に交換できる仕組みにしておくことが求められるようになるのではないかとの見解を示した。

次の論点として、**岩下**は、AES、NESSIE、CRYPTREC、SC27等、複数の暗号標準化プロジェクトが存在することについて、リスクヘッジのために複数の暗号アルゴリズムを標準化する必要があるとしても、その評価プロジェクトが複数存在することが必要か、各プロジェクトの存在意義を見出すことが可能か、例えば、各プロジェクトで評価結果が異なってしまった場合にどれを信じるべきか、といった問題に関するパネリストの意見を求めた。

これに対し、まず、**岡本**は、現在進められているプロジェクトのうち、CRYPTRECは電子政府用の暗号アルゴリズムを選定する場であり、SC27は汎業界的な暗号アルゴリズムの国際標準化を行う場である等、おのおののプロジェクトには異なる目的や位置付けがあることを指摘し、各プロジェクトにおける評価結果が異なることは当然あり得るが、その場合、各利用者が、プロジェクトの目的を理解したうえで、自らのニーズに適した評価結果を採用すべきであると述べた。一方、**東井**は、暗号アルゴリズムの安全性評価や標準化のプロジェクトが国際的に複数存

在することは一見無駄にみえるが、プロジェクト同士が互いに競争しつつ評価技術を高め合うことができるため、暗号アルゴリズムの研究・開発を促進させる効果があるとの見方もできるのではないかとの見解を示した。

これに関連して、**松本**は、現在、新たな暗号アルゴリズムを開発することに比べ、それらの安全性を評価することはあまり重要な仕事とは思われていない面があるが、信頼できる暗号アルゴリズムを選択することが極めて重要になってきている状況のもと、暗号を評価する人材を育成することの重要性が増してきていることを指摘した。

## 4. 発表：電子文書の送受信証明を行うためのプロトコルの研究動向と安全性評価

次のセッションでは、電子文書の送受信証明に関して**宇根**が発表を行い、これを受けて、**櫻井**によるコメント、および同コメントに対する**宇根**のリジョインダーが行われた。

### (1) 発表の概要

最初に、**宇根**が、提出論文[12]に基づき、インターネット等のオープンなネットワーク上において電子文書の送受信の事実を証明するためのプロトコルの枠組み、研究開発動向、送受信証明プロトコルのひとつであるタイムスタンプ・プロトコルの安全性評価等について、以下のとおり発表を行った。

#### ①電子文書の送受信証明を実現する技術の必要性

インターネットを利用した電子商取引においては、暗号技術を利用することによって、通信相手の確認や通信データの守秘・一貫性を確保することが多いが、安全な電子商取引を実現するためには、それだけでは必ずしも十分ではない。例えば、ある送信者が電子文書を特定の受信者に送信し、その受信者が正しく電子文書を受け取ったとする。その後、送信者が電子文書を送信した事実を主張する一方、受信者がその電子文書の受信を否定した場合、どちらの主張が正しいかを第三者が判断することは困難である。このような問題に対応するためには、「だれが、いつ、どのような電子文書を、だれに対して送信（あるいは、だれから受信）した」という事実の証明（電子文書の送受信証明）を可能にする技術が必要となる。

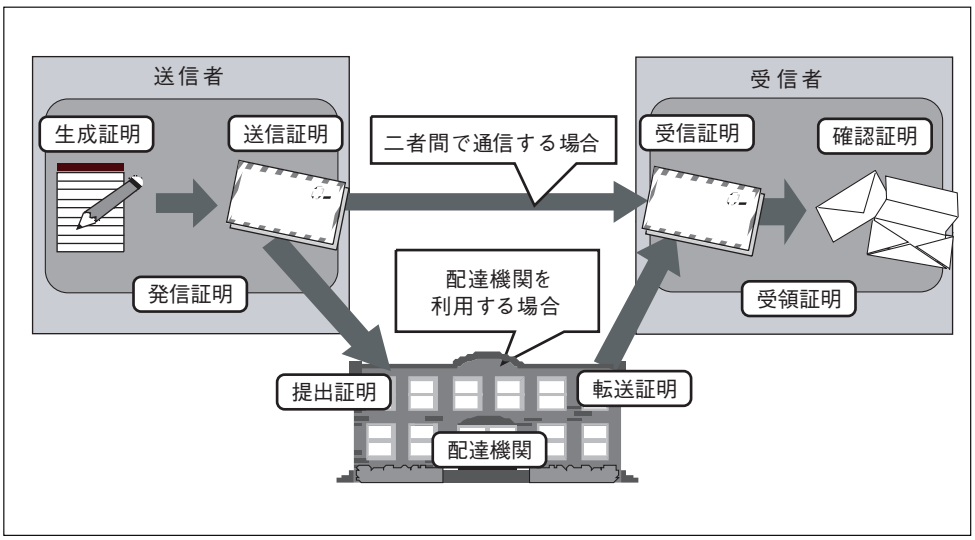
12 宇根正志、「電子文書の送受信証明を行うためのプロトコルの研究動向と安全性評価」（『金融研究』第20巻別冊第1号、日本銀行金融研究所、2001年4月）を参照。

②電子文書の送受信証明プロトコルの基本的な枠組み ― ISO13888

電子文書の送受信証明を実現するプロトコルの基本的な枠組みは、国際標準ISO13888に規定されている。ISO13888では、送受信証明の種類として、生成証明、送信証明、提出証明、転送証明、受信証明、確認証明、の6つを規定しており、さらに、生成証明と送信証明の双方を含むものとして発信証明が、また受信証明と確認証明の双方を含むものとして受領証明が規定されている（図1参照）。これらの各種証明は、データ送受信の各プロセスに対応しており、データ送受信の形態としては、送信者と受信者の二者間で通信を行う場合と、配達機関が送受信者間の通信を中継する場合の2つのケースが規定されている。ここで、配達機関は、業務運営に関して送信者や受信者から高い信頼を得た主体（TTP：trusted third party）であることが前提とされている。

また、ISO13888では、配達機関以外にも、電子文書の送受信証明に関与する各種のTTPの機能が規定されており、例えば、ある事象・行為が発生した時刻を証明するタイムスタンプの生成を行うタイムスタンプ発行機関などがこれに該当する。

図１　ISO13888で規定される送受信証明




③送受信証明プロトコルの研究開発動向と今後の課題

電子文書の送受信証明プロトコルに関する最近の理論研究においては、「公平」な情報交換を実現するプロトコルが重要なテーマとして研究されている。ここでの「公平」とは、送受信者のいずれか一方がデータを相手に持ち逃げされるという問題が生じないことを意味する。また、タイムスタンプの生成・利用に関するタイムスタンプ・プロトコルの研究も盛んに行われており、ISO 13888に規定されている簡素なプロトコル（simple protocol）に加え、連鎖型プロトコル

（linking protocol）や分散型プロトコル（distributed protocol）等さまざまなプロトコルが提案されている。これらの研究を基に、各種実装研究が世界各国で進められており、一部では商用サービスも開始されている。

ただし、安全性の観点から信頼性の高い送受信証明プロトコルを実現するためには、いくつかの課題が残されている。主な課題として、TTPの業務要件の確立と適正な管理・運営体制の維持、各種プロトコルの安全性確保、利用者にとって利便性・透明性の高いサービスの確立、の3つが挙げられる。

**④タイムスタンプ・プロトコルの安全性評価 ― 宇根・松本の研究の紹介**

送受信証明プロトコルの安全性を確保するためには、プロトコルを構成する各主体の不正行為や暗号技術の安全性低下も考慮した評価手法を確立することが今後の重要な課題である。このような観点からの研究の一例として、タイムスタンプ・プロトコルを対象とした宇根と松本の研究[13]が挙げられる。宇根と松本は、タイムスタンプに含まれる情報、タイムスタンプの生成方法、タイムスタンプの検証に必要な情報（検証情報）の取得可能性、の観点からプロトコルを分類し、その中の一方式である「連鎖・取得型の時刻付・証拠無タイムスタンプ方式」における検証情報のさまざまな保管形態について、タイムスタンプの改ざんを目的とする攻撃法が成功するための必要十分条件を導出した。そのうえで、これらの攻撃法に対する安全性の観点から、検証情報のさまざまな保管形態のうち、いずれが最も望ましいかを明らかにした。

## (2) 櫻井のコメント

**櫻井**は、宇根の発表のうち、主として宇根と松本によるタイムスタンプ・プロトコルの安全性評価を巡る研究についてコメントし、既成概念にとらわれずに、タイムスタンプに含まれる情報の種類によってプロトコルを分類している点などが独創的な研究であることを認めつつも、実際に運用されているタイムスタンプ・サービスと対比した場合に、仮定や結論が妥当なものとなっているかについて疑問を呈した。例えば、宇根と松本の研究において安全性評価の際の前提に利用されている「検証情報を保管するエンティティと攻撃者が結託する」という条件があまり現実的ではないと考えられることや、同研究の結論で「安全性評価上最も望ましい」とされた方式が現実のサービスとしては存在しないことを指摘した。

また、一定の数学的な仮定のもとで、暗号アルゴリズムやプロトコルが安全であることを証明する「証明可能安全性」の研究を巡る現状について説明したうえで、証明可能安全性を持つタイムスタンプ・プロトコルを設計することができるか、

13 宇根正志・松本勉、「連鎖型タイムスタンプの検証に用いられる情報の管理」（『コンピュータセキュリティシンポジウム2000予稿集』、情報処理学会、2000年、25～30頁）。

また、宇根と松本の研究によって最も望ましいとされたプロトコルは安全性が証明されていると解釈できるかと質問した。

### (3) 宇根のリジョインダー

このコメントに対し、**宇根**は、確かに、現時点では本研究で「安全性評価上最も望ましい」とされた形態のタイムスタンプ・プロトコルは、現実のサービスとして提供されていないが、この分野は技術開発が始まったばかりであることや、現実の開発では、本研究では捨象した管理コストなどの要因を考慮する必要があることから、「安全性評価上最も望ましい」形態が実際に提供されるとは限らないことを説明した。また、前提の妥当性については、いかなる組織であれ、内部者による不正の可能性を完全に排除することは困難であるため、内部者による不正行為が発生してもプロトコルの信頼性が大きく損なわれることのないように予め対策を講じておくことが大切であり、最悪の事態として、「検証情報の保管エンティティと攻撃者が結託する」という局面を想定することは、妥当な前提と考える、と反論した。

また、証明可能安全性との関係については、タイムスタンプ・プロトコルの設計上、一定の条件のもとで安全性を証明することは可能であろうとの見解を示した。ただし、本研究の枠組みは、特定の攻撃法を対象に、タイムスタンプ・プロトコルへの攻撃が可能となるための必要十分条件を導出するというものであるため、公開鍵暗号等で研究されているような、攻撃法を特定しない証明可能安全性とは性格が異なるものと解釈すべきであるとの見解を示した。

## 5. パネルディスカッション2：ICカードの安全性評価を巡って

パネルディスカッション2では、ICカードの安全性評価をテーマに、**植村**、**廣川**、**古原**をパネリストに迎えて議論を行った。まず、各パネリストが導入報告を行い、続いて自由討議が行われた。

### (1) 導入報告①：ISO15408によるITセキュリティ評価とICカード

**植村**は、わが国でICカードのセキュリティ評価に携わっている立場から、セキュリティ評価基準の国際標準ISO15408[14]の概要を説明するとともに、それを用いたICカードの安全性評価について説明した。

14 ISO15408： 個々の情報セキュリティ関連製品・システムが備えるセキュリティ機能および品質を、統一化された評価尺度に基づいて第三者機関が客観的に評価・認定する際に用いられるセキュリティ評価基準の国際標準。欧米の統一的なセキュリティ評価基準「コモン・クライテリア」をベースに、1999年に策定された。2000年には、わが国でも、日本工業標準JIS X 5070として国内標準化されている。

まず、ISO15408の枠組みについて、①利用者が作成する要求仕様書（プロテクション・プロファイル、PP）、②開発者がPPに基づいて作成する設計仕様書（セキュリティ・ターゲット、ST）、③セキュリティ保証要件の満足度に応じて決定されるセキュリティ保証レベル（EAL）などの基本的な概念を説明したうえで、セキュリティ要件の基本となるPPを作成するのは利用者自身やその業界団体であり、開発者は作成されたPPを読んで、その要求仕様の実現方法を検討し、製品を開発してSTを作成する、という作業分担となるため、ISO15408による安全性評価の実効性を高めるには、利用者がセキュリティ要件の検討に主体的に関与することが重要であることを強調した。そして、現在、わが国でPPやSTを作成できる技術者が十分に育っていないことがISO15408を利用していくうえでの障害となっていると指摘し、人材育成の必要性を訴えた。

続いて、ISO15408のICカードへの適用について説明し、もともとICカードの利用者にはセキュリティを高めたいという強いニーズがあること、ICカードは外部とのインターフェースが限定的な構造であるため、ISO15408によるセキュリティ評価の対象としやすいことから、これまでに世界中で作られたPPの約半分はICカードに関するものであり、現在、日米欧でICカードのPPに関する共通理解を進める枠組み作りが進められていることを紹介した。その一方で、ICカードを構成するICチップやソフトウエア等の部品の安全性評価をどう行うべきか、利用者がソフトウエアの書き換えを行う場合、安全性がどこまで評価できるか、といった実務的な問題を抱えていることを示し、こうした問題について、国内の企業や海外の評価機関、利用者団体等と連携を取りつつ、解決策を模索していると説明した。

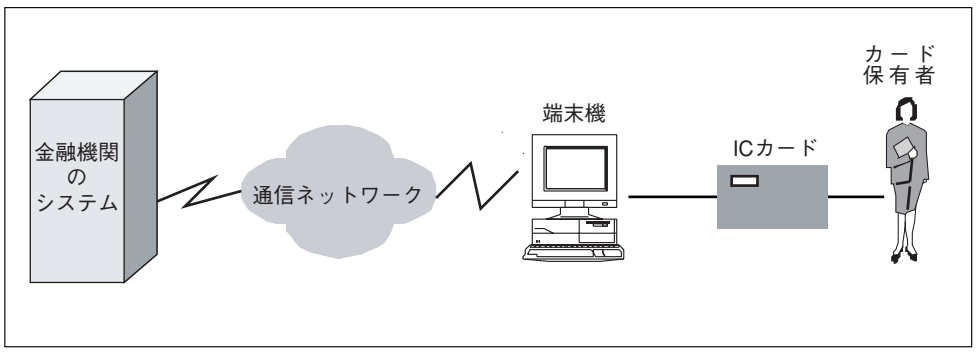
### (2) 導入報告②：ICカードを利用したリテイル金融取引のセキュリティの確保における留意点

続いて、**廣川**は、ICカードの技術開発に長く携わり、またICカードの国際標準規格の検討に参加してきた立場から、ICカードを利用したリテイル金融取引に関し、システム全体の安全性を守る際の留意点について説明した。

最初に、わが国における金融業務向けICカードのシステム開発の歴史を概観し、1980年代にICカードを金融業務に利用し始めた時点では、ICカードを導入する目的が、欧米とわが国とでは大きく異なっていたことを紹介した。当時、欧米諸国では、ICカードを、カード偽造に対するセキュリティ対策と位置付けて導入していた一方、わが国では、セキュリティ対策としてはあまり意識されず、金融機関が提供するサービスの利便性を高める「マルチ・アプリケーション化」の手段と位置付けられていたことを説明した。しかし、1990年代後半以降、欧米諸国でもマルチ・アプリケーション化のニーズが強まる一方、わが国でもICカードの機能をセキュリティ対策として評価するようになるなど、国内外における認識の違いは少なくなっていることを指摘し、金融業務へのICカードの導入においては、利便性とセキュリティ対策のバランスを取っていくことが大切であるとの見解を示した。

次に、金融取引カードを磁気ストライプ・カードからICカードに移行させる際の留意点について、抽象化したシステム・イメージ（図2参照）を示して説明した。ICカード導入の効果をセキュリティの観点から考えた場合、リテイル金融取引には、カードの偽造以外にも、端末機の変造や通信ネットワークへの侵入といったさまざまな脅威が存在するため、単にカードと端末機との間におけるカード保有者の本人確認を強化するだけではなく、リテイル金融取引のシステム全体のセキュリティ向上を図ることが必要であり、そのためにはICカードを用いて生成する認証のための情報を、通信ネットワークを通じて金融機関側に送信する仕組みとしたうえで、これを各段階でのセキュリティ確保に利用することが有効であると指摘した。また、リテイル金融取引においては、1回の取引を完結させるために、カード保有者、販売店、ネットワーク事業者、金融機関など、さまざまな利害関係者が関与することを指摘し、ICカードから金融機関までの間で適切な情報の伝達と処理が行われることによって、万一、セキュリティ侵害が発生した場合でも、おのおのの利害関係者の権限と責任の範囲を正しく切り分けることができるようなセキュリティ対策を講じていくべきであると主張した。

図2　抽象化したリテイル金融取引システムのイメージ




### (3) 導入報告③：ICカードの耐タンパー性に対する攻撃とその対処方法

続いて、**古原**は、ICカードの耐タンパー性に関する研究を行っている立場から、情報処理振興事業協会の委託を受けてメーカーの研究者と共同で執筆した調査レポート[15]の概要を発表する形で、ICカードの耐タンパー性に対する攻撃とその対処方法について発表した。

まず、問題の所在として、金融分野でICカードを利用する場合、その耐タンパー性[16]を利用して暗証番号などの秘密情報や電子マネーの残高情報等を格納すること

15 情報処理振興事業協会　平成11年度プロジェクト「スマートカードの安全性に関する調査」報告書（http://www.ipa.go.jp/security/enc/SmartCard/sc-survey.pdf）。

16 耐タンパー性：ICカードなどのデバイスに求められる属性のひとつで、デバイス内に格納された情報が、解析されて勝手に読み出されたり、書き替えられたりすることが困難であること。

が多いが、すべてのICカードがいかなる攻撃に対しても耐タンパー性を持っているとはいえず、近年、ICカードの内部情報を不正に読み出したり、書き替えたりする事例が報告されるようになってきていることを説明した。そのうえで、これまで学会等で発表されてきたICカードの耐タンパー性に対する代表的な攻撃法とその対策方法について、以下の4つのパターンに分けて概要を説明した。

①プローブ攻撃

代表的な破壊型解析法であり、ICの内部回路に直接プローブ（探知針）を当ててデータを観測することで秘密情報を得る、極めて強力な攻撃法である。ただし攻撃の実行には攻撃対象に関する詳細な知識と高度な技術習熟度が要求されるため、攻撃の実現可能性は高いとはいえない。プローブ解析に対する対策としては、ICチップに対してシリコン・コーティングを施して解析をやりにくくしたり、周波数、電圧、温度などのセンサーを装備して、解析を検知した場合に内部状態をゼロ化する方法などが提案されている。

②故障利用解析

放射線などで一過性の故障を生じさせ、攻撃者が意図した異常な処理による出力と正常出力とを比較することで秘密情報を推測する解析法であり、その対策としてはプローブ解析への対策と同様なアプローチが有効である。

③タイミング解析

ICカード内で暗号処理を行う際に、格納された秘密情報に依存して処理時間が異なる場合に、統計的解析を用いて秘密情報を推測する解析法であり、その対策としては処理時間を一定化する実装アルゴリズムを採用する方法や、ランダムな遅延を発生させて処理時間をカムフラージュする方法などがある。

④電力解析

ICカード内で暗号処理を行う際に、格納された秘密情報に依存して消費電力が異なる場合に、秘密情報を推測する解析法であり、特に統計的手法を用いる電力差分解析では効率的な解析が可能となっている。その対策としては、消費電力に関するある程度の情報漏洩は不可避なものと仮定したうえで、実装するアルゴリズムのレベルで、消費電力から秘密情報を推定されにくい技術を選択する方法が効果的と考えられている。

古原は、こうした説明を行ったうえで、ICカードにおいて「完璧な耐タンパー性」を安価に実現する方法は現在のところ知られていないが、現在知られている多くの攻撃法は、わずかな工夫を施すことにより防ぐことが可能であると指摘した。そして、実務においてICカードを利用する場合、守るべき情報の重要度と破られた場合の影響を考慮して、コストに見合った技術を採用していくことが重要であり、例え

ば、公開鍵暗号方式を用いて、おのおのの利用者ごとに異なる秘密鍵の情報のみをICカードに格納し、耐タンパー性への依存度を小さくすることなども考えられるとの見解を示した。

### (4) 自由討議

3件の導入報告に引き続き、パネリストによる自由討議が行われた。

まず、モデレータである**岩下**が、**古原**の報告で指摘されたICカードの耐タンパー性に対する攻撃法の存在とその対策は、**植村**の報告にあったISO15408によるICカードの安全性評価にどのように織り込まれるかについて、パネリストの見解を尋ねた。

**植村**は、ICカードの要求仕様書（PP）を作成してきた経験から、PPの作成作業の過程で「脅威分析」を実施する際に、耐タンパー性に対する攻撃法を含め、考えられる脅威をできる限り取り込み、それをPPに織り込むという作業を行っていると説明した。また、開発者側でも、そうした利用者の要求を意識して、適切な対策を講じたうえで、それを設計仕様書（ST）に反映させていると説明した。

これに対し、**古原**は、ISO15408の基本的な仕組みは、PPに示された要件と製品の機能とを照合するものであるから、ICカードのセキュリティを守るためには、「良いPPを作ること」がポイントとなると述べた。また、耐タンパー性に対する最新の攻撃法に対処していくためには、PPの作成者が最新の技術動向をウォッチしていくことが大切であると指摘した。

続いて、**岩下**が、**廣川**の報告で指摘された「リテイル金融取引システム全体のセキュリティを守る」という観点から考えた場合、ICカードの安全性をISO15408によって評価することは、どのような意義を持つかについて、パネリストの意見を求めた。

これに対して、**廣川**は、現在、リテイル金融取引カードの不正使用が深刻な問題となっていることを指摘し、「現在存在する一番安全なメディア」として、ICカードへの移行が進められているとの認識を示したうえで、ICカードといえども完璧なものではなく、金融機関と利用者、加盟店の間で、ICカードがどこまで安全かについての共通認識を構築していくことが必要であり、そのためにISO15408の枠組みを活用することが考えられると指摘した。

これに関連して、**古原**は、ICカードは「完全な安全性」を求めようとすると、コストが跳ね上がってしまう性格を持つことを指摘し、高いコストで高度なセキュリティ対策を実施することが必ずしも望ましいわけではなく、現実的なコストの範囲で必要とされる耐タンパー性を実現するための、最適なレベルを模索していくことが必要ではないかと述べた。また、**植村**は、金融機関やその利用者の間に、「ICカードを使えば（それだけで）安全」という認識が広まってしまうことに懸念を表明し、システム全体のセキュリティを確保するためには、ICカードの耐タンパー

性からシステムの運用管理まで、さまざまなセキュリティ対策を組み合わせていくことが必要であると指摘した。

## 6. 総括コメント

最後に、**今井**は、議論の総括として、本シンポジウムのパネルディスカッションや発表の内容を簡単に整理したうえで、共通テーマである「情報セキュリティ技術の評価と信頼性」について、その重要性を改めて強調する以下のようなコメントを述べた。

インターネットが急速に普及する中で、さまざまなセキュリティ侵害事件が発生したこともあり、電子商取引の推進や電子政府の実現に当たっては情報セキュリティの確保が必要不可欠であるとの認識が強まってきている。わが国の金融業界や政府においても、情報の真正性確保や取引相手の認証のためにさまざまな情報セキュリティ技術を導入する動きが出てきており、こうした動きは積極的に評価できる。その一方で、情報セキュリティ技術に慣れていない利用者の間では、「暗号を利用すればもうそれだけで安全である」とか、「ICカードを利用していれば安全である」といった誤った認識が今なお多いのも事実であろう。システムの安全性は、さまざまなセキュリティ対策を組み合わせて総合的に保護されるべきものであり、暗号などの個別要素技術も、その信頼性を確認したうえで利用する必要がある。「暗号を利用すれば、それだけでよい」といった考え方は、システム全体のセキュリティ対策を進めていくうえでは、むしろ有害である。

情報セキュリティ技術を実務に適用していくうえで、「信頼できる技術」を適切に選択し利用するためには、技術を提供する側が、安全性評価や第三者認証などの枠組みを整備することに加え、技術を利用する側も、そうした仕組みを十分に理解し「信頼できる技術」を見分ける目を持つことが大切である。そうした観点からみて、本シンポジウムのような機会を通じ、金融業界や政府などの情報セキュリティ技術の利用者に、安全性評価に関する最新の技術動向が紹介されることは、わが国の金融システムの安全性を確保していくための重要な一歩といえよう。

また、今後、金融業界が情報セキュリティ技術を適切に利用していくためには、それを担う人材の育成が大切である。金融業界は、金融業務と情報セキュリティ技術の両方に精通した人材の育成に努めていく必要があろう。