『金融研究』（第18巻第2号）所収論文の紹介

日本銀行金融研究所では、その研究成果を広く外部に公表することを狙いとして、『金融研究』(注)を発行している。以下は、第18巻第2号（平成11年4月発行）所収論文の概要を紹介したものである。

情報セキュリティ・シンポジウム会議の概要

インターネットの爆発的な拡大に伴い、オープンなコンピュータ・ネットワークを利用してビジネスを行う「電子商取引」に対する期待が高まっている。「情報セキュリティ技術」は、電子商取引におけるプライバシーや個別取引の安全性を確保する上で不可欠な技術である。わが国の金融機関が、今後、オープンなネットワークを利用して新しい金融サービスを本格的に展開していく際には、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必要があり、その基礎理論として暗号技術等の理解を深めておく必要がある。

日本銀行金融研究所では、このような問題意識に基づき、昨年11月4日、「金融分野における情報セキュリティ技術の現状と課題」をテーマにシンポジウムを開催した。日本銀行金融研究所は、従来から、国際標準化機構の金融専門委員会（ＩＳＯ／ＴＣ68）の国内審議団体の事務局を務めていることもあって、国際的な動向を視野に入れながら、金融業務に利用される情報セキュリティ技術に関する技術研究を行ってきている。今回のシンポジウムは、上記のような問題意識を国内の金融機関の実務家や標準化担当者、関連業界の技術者と共有し、わが国の対応の一助となることを目的として開催したものである。

『金融研究』本号は、本ワークショップに関する特集号である。シンポジウムにおける各発表の概要をとりまとめた「会議の概要」のほか、５本の提出論文を掲載している。

各提出論文の要旨は以下のとおりである。

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

わが国の金融業界においては、従来、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が採用されてきたため、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い面があった。しかし、オープンなネットワークを利用した新しい金融サービスに対するニーズが高まるに連れて、金融機関が安全かつ効率的に金融サービスを提供してい

(注)『金融研究』所収論文の内容や意見は執筆者個人に属し、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。なお、『金融研究』第18巻第2号（定価1,050円）は、ときわ総合サービス（株）（本『日銀調査月報』刊行物一覧を参照）より販売。

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になってきている。

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、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対して詳細な評価を積み重ね、総合的に管理していくことが必要である。また、各要素技術には、各々耐用年数とでもいうべき安全性の期限があり、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するためには、常に新しい技術革新に対応し、最新の対策を講じていかなければならない。同時に、金融機関は、自らの情報セキュリティ対策の枠組み等を適切に外部に開示することにより、安全性に対する信任を勝ち得ていくことも必要とされている。

また、最近、欧米主要国の金融業界においては、新しい暗号技術を採用する動きが盛んになっている。わが国の金融業界においても、海外の状況等を踏まえて、国際的な整合性、説得性のある情報セキュリティ技術を採用していくことが重要となろう。

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

岩下直行・谷田部充子

金融業界では、従来から、様々な金融業務に関する「標準化」が行われてきた。標準化は、金融取引における不要な多様性を排除し、事務の合理化、安全性の向上に資するものである。また、標準化は、情報セキュリティ技術の観点からも大きな意味を持っている。暗号技術等の情報セキュリティ技術は、複雑な情報技術や高度な数学理論に基づくものが多く、一般の利用者がその安全性・信頼性を評価することは難しい。信頼できる中立的な機関が安全性を十分に吟味した上で標準化を行うことは、利用者がその技術を安心して利用する上では有用であり、一般の利用者は、専門家が標準化した技術を利用することによって、高いセキュリティ水準を達成することが期待されている。

国際標準化機構の金融専門委員会（ＩＳＯ／ＴＣ68）では、金融業務に利用される国際標準を策定しているが、その多くは金融分野で利用される情報セキュリティ技術に関するものである。また、ＩＳＯ／ＴＣ68では、ＤＥＳの安全性低下への対応、公開鍵暗号を実用化するための認証機関の機能、金融機関の情報セキュリティ対策に関するガイドラインと評価基準等、金融業務に利用される情報セキュリティ技術の安全性や標準化のあり方全般に関する検討も行ってきた。

今後、わが国の金融業界が新しい情報セキュリティ技術を採用していく際には、こうした国際標準化動向を意識しておくことが重要と考えられる。本稿では、ＩＳＯ／ＴＣ68の組織と活動状況、主な国際標準の概要等について紹介する。

電子マネーを構成する情報セキュリティ技術と安全性評価

中山靖司・太田和夫・松本　勉

電子マネーのセキュリティ対策については、既に様々な理論的・実証的研究が行われているが、電子マネーの安全性を確保するためには、発生し得る不正のリスクを十分考慮の上、これに見合った効果的なセキュリティ対策を施していく必要がある。そのためには、こうしたリスクの種類、程度を十分把握した上で、使用して

いるＩＣカードが実際に必要なセキュリティレベルに達しているか、使用している暗号アルゴリズムやその鍵長の設定が適当か、鍵管理が適切に行われているか、などを総合的に評価していくことが必要となる。

本稿では、まず、電子マネーを構成する様々な情報セキュリティ技術のうち、特に代表的な要素技術として暗号技術と耐タンパー技術を取り上げ、こうした要素技術は一定の条件のもとでの安全性を保証するものに過ぎず、絶対的な安全性を持つものではないことを指摘する。次に、これらの情報セキュリティ技術のうち、ＩＣカード等の耐タンパー性に頼ることなく電子マネーを構成した場合に、その論理的な構成方法（電子マネー実現方式）の違いによって、電子マネーの安全性にどのような差が出てくるのかを、発生し得る不正のリスクの種類、程度、範囲を分析することにより評価する。このような評価結果は、各電子マネーの持つ技術的特徴が安全性にどのように影響するかを示すとともに、それぞれの電子マネー実現方式が「総合的な安全性」を確保するためには、さらにどのような要素技術（耐タンパー装置等）を追加するなどの工夫を施すことが必要となるかといった検討の指針を与えるものである。

共通鍵暗号を取り巻く現状と課題
― ＤＥＳからＡＥＳへ ―

宇根正志・太田和夫

共通鍵暗号は、暗号化と復号に同一の鍵を用いる暗号であり、金融分野をはじめとして幅広い分野で利用されている。共通鍵暗号の中でもブロック暗号と呼ばれる方式が主要な商用暗号として利用されており、1977年に米国政府標準暗号に認定されたＤＥＳ（Data Encryption Standard）が事実上の標準として利用されてきた。

しかし、ＤＥＳは、鍵長が56bitであることから、近年のコンピュータのコストパフォーマンス向上等によって安全性が徐々に低下している。このため、現在金融分野を中心に、ＤＥＳの代替暗号としてTriple ＤＥＳを利用する動きが広がっている。Triple ＤＥＳは、ＤＥＳのアルゴリズムを３回繰り返す方式であり、①ＤＥＳからの移行が比較的容易である、②全数探索法に対する安全性が向上する等の利点を有している。

一方、米国政府は、次世代の標準暗号としてＡＥＳ（Advanced Encryption Standard）の標準化を進めている。ＡＥＳは、標準化完了後、一般に利用可能となるまでにはさらに数年はかかるとみられており、Triple ＤＥＳの次の主要な暗号方式として位置付けられている。

ＤＥＳからTriple ＤＥＳ、さらにはＡＥＳへの移行に象徴されるように、共通鍵暗号を取り巻く環境は急速に変化している。本稿では、共通鍵暗号の機能、構造、主要な解読法のほか、主要な共通鍵ブロック暗号に関するこれまでの安全性評価結果について整理するとともに、ＤＥＳからTriple ＤＥＳ、そしてＡＥＳへの移行の経緯と現状について説明する。

公開鍵暗号の理論研究における最近の動向

宇根正志・岡本龍明

公開鍵暗号は、暗号化と復号に異なる鍵を用いる暗号であり、復号に用いる鍵を秘密にする一方、暗号化に用いる鍵を公開する。公開鍵暗号は、公開する鍵の真正性を確保する仕組みが必要となるものの、①事前に通信相手に鍵を配送する必要がない、②通信相手確認や受信デー

タの真正性確認等を可能にするディジタル署名を実現できるなどの利点を有することから、インターネット等オープンなネットワークにおける情報セキュリティ技術として幅広く利用されている。

公開鍵暗号の理論研究は、1976年にDiffieとHellmanによって公開鍵暗号のアイデアが提案されて以来、多くの暗号学者によって進められてきた。これまでにＲＳＡ暗号やElGamal暗号をはじめとする様々な暗号方式が提案されている。

最近の公開鍵暗号の理論研究において特に注目されているのは、証明可能な安全性と実用性を兼ね備えた暗号方式に関する研究である。現在実用化されている暗号方式の中には、これまでに効率的な解読法が見つかっていないものの、安全性が証明されていないものが多い。したがって、それらの暗号方式について、効率的な解読法が存在する可能性を否定することはできない。これに対し、最近では、ＯＡＥＰやＥＰＯＣ等、既存の方式に改良を加えることによって証明可能な安全性と実用性を両立させる暗号方式が提案されている。ＯＡＥＰ等これらの方式の一部は、既に実用化されている暗号プロトコルの安全性を高める目的から、ＰＫＣＳ＃１等いくつかの業界標準で採用されている。

公開鍵暗号の安全性証明に関する研究は、公開鍵暗号を利用した様々なシステムにおける信頼性を高める上で、今後一層重要になると考えられる。本稿では、こうした最近の安全性証明に関する研究の動向を中心に、これまでの主要な公開鍵暗号に関する研究成果について説明する。