情報セキュリティ・シンポジウム

会議の概要

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。金融業界においても、従来から、セキュリティ対策の重要性は認識されていた。しかし、わが国の金融機関は、堅固なコンピュータ・センターと専用通信回線の使用等により、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基本としてきたため、この分野で先進的な欧米諸国と比較すると、インターネット等を使用するオープンなシステムで不可欠とされる暗号技術等の情報セキュリティ技術の重要性が十分理解されているとは言い難い状況にあるように思われる。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た。シンポジウムには、次の５つの論文が提出され、各執筆者による発表が行われた。

・提出論文 1 「金融分野における情報セキュリティ技術の現状と課題」

執筆者	横浜国立大学 助教授	松本 勉
	日本銀行 金融研究所	岩下直行

・提出論文 2 「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」

執筆者	日本銀行 金融研究所	岩下直行
	日本銀行 金融研究所	谷田部充子

・提出論文 3 「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」

執筆者	日本銀行 金融研究所	中山靖司
	横浜国立大学 助教授	松本 勉
	日本電信電話（株）特別研究員	太田和夫

・提出論文 4 「共通鍵暗号を取り巻く現状と課題 ―DESからAESへ―」

執筆者	日本銀行 金融研究所	宇根正志
	日本電信電話（株）特別研究員	太田和夫

・提出論文 5 「公開鍵暗号の理論研究における最近の動向」

執筆者	日本銀行 金融研究所	宇根正志
	日本電信電話（株）特別研究員	岡本龍明

なお、フロアには、金融業界のみならず、暗号学者、金融分野における情報セキュリティ技術を担当する官庁、電機メーカー、通信会社等の研究開発部門、標準化部門の実務家、技術者等約80名、日本銀行職員約20名が参加した。以下では、シンポジウムにおける各発表の概要について紹介する（文責 日本銀行金融研究所）。

発表の概要

1．松本・岩下論文「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（敬称略、以下同様）は、**岩下**との共同論文に基づき、金融分野で必要とされる情報セキュリティ技術に関する基礎的な解説を行った上で、わが国の金融業界における本分野への取り組みや、金融機関のセキュリティ対策に関する情報開示のあり方などについて提言し、問題提起を行った。発表の概要は以下の通りである。

（1） 金融業務と情報セキュリティ技術

金融機関がコンピュータ・ネットワークを利用して資金決済情報や顧客情報を送受信する場合、情報の漏洩や改竄を有効に防止する対策を講じることが必要である。このため、欧米では、金融ネットワークにDES等の暗号技術を利用したセキュリティ対策が導入されており、金融業界が暗号技術の最大のユーザーとなっている。

一方、わが国についてみると、金融業界では、これまで、情報セキュリティ技術、暗号技術をセキュリティ対策として利用することにはあまり関心が払われてこな

かった。これは、わが国の金融業界が構築してきた金融ネットワークが、企業内、業界内に閉じたシステムであり、システムを外部から物理的に隔離し、利用者のアクセスを厳格に管理することにより、システム全体のセキュリティを確保するというポリシーを採用してきたためであった。

しかし、インターネットの利用拡大等、企業や業界を跨ぐ情報ネットワークの発達に伴い、「金融サービスを金融業界独自の閉じたネットワークで提供する」という従来の前提が崩れつつある。たとえば、金融機関間取引の分野では、STP（Straight-Through Processing）と呼ばれるコンセプトに基づき、売買、約定、決済等、複数の金融ネットワークを相互接続し、入力されたデータを自動的に処理する取引が増えてきている。相互に接続された複数のネットワークを経由する取引の場合、金融機関は物理的なアクセス制御だけでは自らのセキュリティを確保することができない。対顧客取引の分野でも、インターネットの発達や、企業間のEDI（Electronic Data Interchange〈電子データ交換〉）の普及に伴い、オープンなネットワーク上で金融サービスを提供することへの要請が高まっている。そうした要請に応えるためには、銀行の金融ネットワークに外部との接点を設けなければならず、従来の「物理的な隔離」という対策に代わる新たなセキュリティ対策が必要となる。

金融ネットワークのオープン化が進む中で、金融業務のセキュリティを確保していくためには、欧米主要国の金融機関のように、機密情報を送信する場合に暗号による秘匿を行うとか、資金支払指図データの安全性確保のために電子署名による認証を行うといった形で、暗号技術等の情報セキュリティ技術を利用していくことが有効と考えられる。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、利便性の高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きている。

（2） 暗号技術とその安全性

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。暗号技術は機密情報の保護（守秘）に使用されるが、情報が正当な利用者によって作成され、改竄を受けていないことを確認する機能（認証）にも利用される。

共通鍵暗号に利用される鍵の長さ（鍵長）はアルゴリズムによって区々であり、現在最も普及しているDESの鍵長は56 bitである。鍵長が短いと、全数探索法[1]による攻撃が容易となるため、安全性を維持するために、今後は128 bit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ものと思われる。

公開鍵暗号についても同様であり、代表的な公開鍵暗号であるRSAの場合、鍵長が512 bit程度のものが使用されてきたが、暗号解析技術の進歩に伴い、1024 bitや

1 全数探索法：候補となる鍵をしらみつぶしに試して真の鍵を探索する暗号解読法。

2048 bitといった長さの鍵が要求されてきている。このため、比較的短い鍵長で強度を確保でき、暗号化や復号に要する計算量も少ない楕円曲線暗号が盛んに研究されている。

（3）有効な情報セキュリティ対策を講じるために

情報セキュリティ技術とは、①暗号基礎技術のみならず、②実装技術、③システム設計技術、④運用管理技術、等の要素技術を複雑に組み合わせた「総合技術」である。金融業務のセキュリティを守る場合、各要素技術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侵害のリスクが高まってしまう。このため、セキュリティ対策の実効性を評価するためには、採用するセキュリティ・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と同時に、システム全体として総合的に検討していく必要がある。

また、各要素技術には、耐用年数とでもい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の安全性が急に確保されなくなってしまう可能性も否定できない。したがって、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。さらに、セキュリティ対策を講じる場合には、技術を秘匿するのではなく、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外部に開示し、オープンな議論の俎上に載せていくことが有効と考えられてきている。

情報セキュリティ技術は日進月歩の技術であり、先進ユーザーである欧米主要国の金融機関においては、DESに基づくセキュリティ対策からTriple DESへの移行という、新しい動きもみられている。わが国の金融業界が情報セキュリティ技術の適用を検討する場合にも、こうした国際的な動向を十分考慮する必要がある。金融市場のグローバル化が急速に進展する中で、わが国金融業界においても、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の必要性が強まっている。

2．岩下・谷田部論文「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」

岩下は、**谷田部**との共同論文に基づき、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に関する発表を行った。**岩下**は、日本銀行が国内審議団体を務めるISO／TC68での国際標準化活動の経験を踏まえ、欧米の金融機関において金融業務に利用されている様々な情報セキュリティ技術が、ISO／TC68の国際標準となっていることを紹介した。その上で、最近の暗号技術の進展により海外の金融機関がセキュリティ対策を改善させつつあることをも踏まえて、わが国の金融業界においても、ISO等の国際標準を踏まえながら、適切な情報セキュリティ技術を採用していくことが必要ではないかと指摘した。発表の概要は以下の通りである。

（1）金融業務と標準化

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。伝統的な紙ベースの金融業務では、手形、小切手や各種帳票類の様式の統一という標準化が行われていた。最近の電子的な金融業務では、金融機関間のデータ通信フォーマット、金融機関コード、銀行取引カードのフォーマット等が標準化されている。こうした標準化は、金融機関間および金融機関－顧客間の金融取引において、不要な多様性を排除し、業務を円滑に行うために必要不可欠なものであり、金融機関の事務の合理化、安全性の向上や顧客サービスの向上にも資するものである。

ただ、従来のわが国で進められてきた金融業務の標準化は、主に国内・業界内を念頭においた標準化であり、国際標準との整合性に十分な注意が払われてきたとは言い難かった。金融の国際化、電子化の進展に伴い、わが国の金融業界においても、様々な分野で「国際標準」の重要性が高まっている。特に、コンピュータ・ネットワークを利用した金融機関間のデータ送受信や、磁気カード・ICカード等を用いたリテール金融取引等の分野については、今後、国際的な相互乗り入れがさらに進むものと考えられるため、わが国の金融業界における標準化に当っては、海外との調和、整合性を考慮する必要性が高まってこよう。

（2）情報セキュリティと標準化

今日、金融業務の「標準化」については、情報セキュリティ技術の標準化が大きな意味を持ってきている。代表的な共通鍵暗号であるDES（Data Encryption Standard）や、その後継として選定作業が進んでいるAES（Advanced Encryption Standard）が「Standard」と名付けられていることからも明らかなように、暗号アルゴリズムなどの情報セキュリティ技術の普及においては、公的機関による標準化が大きな影響力を持っている[2]。暗号アルゴリズムや情報セキュリティ技術は、高度な数学理論に基づくものが多いので、一般の利用者がその安全性や強度を容易には測定できない。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を策定することは、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、専門家が策定した標準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。

（3）ISO／TC68における国際標準化の枠組み

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暗号アルゴリズムやそれを利用したプロトコル、鍵管理方式、ICカード、認証機関の業務の進め方等、情報セキュリティ技術に関するものである。

2 「標準」には、公的な標準化機関が制定する「デジュール標準」と、市場における競争を通じて事実上決定される「デファクト標準」がある。技術革新のスピードの速い情報通信技術の分野ではデファクト標準が広く利用されているが、情報セキュリティ技術においては、標準化のプロセスが透明かつ公平であるため、デジュール標準が重視されている。このため、本稿では、主にデジュール標準を分析の対象としている。

ISOは、工業製品やサービスに関する国際標準化活動を行うために1947年に設立された非政府間機構であり、各分野毎に専門委員会（TC：Technical Committee）が設置され、標準化作業を進めている。現在、TC1（ねじ）からTC218（製材）まで184の専門委員会が活動しており、TC68は、こうした専門委員会の１つである。TC68の下には、３つの分科委員会（SC）が設置され、各分科委員会の下にも作業グループが設けられており、日本、米国、英国、フランスなど20か国が投票権を持つメンバーとして参加している。

（４）ISO／TC68に対応するわが国の国際標準化活動

ISOには、各国の最も代表的な標準化機関が、会員団体（member body）として１機関だけ加入できることになっており、わが国からは日本工業標準調査会（JISC）が1952年に加入している。JISCは、ISOの各専門委員会（TC）毎に研究団体、業界団体等に国内意見の取りまとめ等を行う国内審議団体を委嘱している。金融業務に関するTC68については、日本銀行が国内審議団体の委嘱を受けている（事務局は日本銀行金融研究所）。日本銀行は、国内の銀行、証券会社、金融界の諸団体・機関、メーカー、通信事業者、学者、官公庁等をメンバーとするISO／TC68国内委員会（委員長：南部鶴彦学習院大学教授）を定期的に主催しているほか、関連する国際会議への出席や、国内意見の取りまとめ等を行っており、こうした活動がわが国金融業界の情報セキュリティ技術の向上に資することを期待している。

（５）ISO／TC68で策定されている国際標準

ISO／TC68では、主に欧米の金融機関が業務に利用している様々な情報セキュリティ技術が国際標準化されている。たとえば、金融業務において遵守すべき情報セキュリティ・ガイドライン（ISO/TR 13569）、耐タンパー性を持つ暗号装置の要件（ISO 13491）、認証機関による公開鍵証明書の管理（ISO/CD 15782）などにおいては、金融業務に利用される最新の情報セキュリティ技術が標準化されている。また、ホールセール分野で利用されるMAC（メッセージ認証子、ISO 8730）、暗号鍵管理方式（ISO 8732）、PIN（暗証番号）の暗号化（ISO 9564）等の国際標準では、暗号アルゴリズムとしてDESを使用することが前提とされている。

また、ISO／TC68では、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に関する検討も行っている。本検討作業の一環として、ISO／TC68では、1994年頃からDESの安全性に対する懸念を認識し、技術的な研究を進めると同時に、DESの後継暗号の必要性を訴えるポリシー・ステートメントを作成・発表してきた。この作業の一環として、日本銀行金融研究所は、1996年に、DESの強度評価に関する技術レポートを提出し、遅くとも2000年までには、現実的な費用で、専用解読装置を用いた全数探索法によって短時間のうちにDESを解読することが可能となることを指摘した。

こうした金融業界からの働きかけの効果もあって、米国ではDESの後継としてTriple DESの国内標準が策定され、米国政府もAESの標準化を開始した。ISO／

TC68で策定している標準も、今後、より安全な暗号技術を利用するものに改定されていく予定である。

（6）わが国の金融業界としての対応

これまで、わが国の金融業界では、磁気カードの仕様、銀行間通信プロトコル等の標準化はある程度進められてきており、また金融機関が利用する情報機器の安全対策については、通産省や金融情報システムセンターが基準を策定してきた。しかし、わが国の金融機関が採用する安全対策基準においては、コンピュータ・システムの外部からの隔離が基本的なポリシーとなっており、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。また、国内での標準規格の策定において、ISO／TC68で策定している国際標準を意識したものは少ない。

しかし、わが国の金融業界においても、ネットワーク上で金融業務の安全を確保する手段として、従来とは異なる観点から情報セキュリティを確保することの重要性が高まってきている。また、今後、インターネットの利用等も含め、国境を越えた国際的な金融取引が増加してくるという認識も必要であろう。そうした中では、わが国の金融業界においても、ISO／TC68が策定する情報セキュリティ技術関連の国際標準を意識し、最新の技術動向を理解しておくことが有用であろう。

３．中山・松本・太田論文「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」

中山は、情報セキュリティ技術の具体的な応用事例として電子マネーを取り上げ、**松本**、**太田**との共同論文に基づき、その安全性評価に関する発表を行った。**中山**は、暗号技術やICカードといった電子マネーを構成する個々の情報セキュリティ技術は、耐用年数等、一定の条件の下での安全性を保証するものに過ぎないことを指摘した。その上で、電子マネーの安全性を総合的に確保していくためには、様々な電子マネー実現方式を発生し得るリスクの観点から分析し、それに対応して情報セキュリティ技術の組み合わせ方を検討することが必要として、その分析結果を紹介した。発表の概要は以下の通りである。

（1）本研究を実施した経緯

日本銀行金融研究所では、日本電信電話(株)情報通信研究所と電子マネーの実現方式に関する共同研究を行い[3]、1996年には、日本電信電話(株)が、その研究成果を取り入れた実験システムを開発・発表している。この共同研究では、将来、電子マネーが決済手段として広く普及した場合を想定し、現金同様の匿名性の実現など、

3 中山靖司・森畠秀実・阿部正幸・藤崎英一郎、「電子マネーの一実現方式について ―― 安全性、利便性に配慮した新しい電子マネー実現方式の提案 ――」、『金融研究』第16巻第２号、日本銀行金融研究所、1997年6月を参照。

電子マネーがどのような条件を満たしている必要があるかを検討して設計している。電子マネーが利用者に信頼されて広く利用されるためには、その安全性が確保されていることが重要である。このため、共同研究では、偽造、変造、二重使用を有効に防止できる、安全性の高い電子マネーの実現方式を提案した。今後は、こうした研究成果を含め、様々な電子マネー実現方式が考案され、それらの競争によってイノベーションが促進されていくことが望まれる。その過程では、電子マネーの安全性評価が重要であることはいうまでもない。

電子マネーは、様々な情報セキュリティ技術を組み合わせることによって構成されているが、それらの個々の情報セキュリティ技術は、必ずしも絶対的な安全性を保証するものではない。したがって、安全な電子マネーを実現するためには、個別の要素技術に過度に頼ることなく、「総合技術」としての安全性を確保する工夫が必要である。本研究は、現在提案されている電子マネー実現方式を主な技術的特徴に基づいてモデル化し、これに具体的な暗号技術を適用して安全性を評価するというアプローチにより、電子マネーの実現方式全般について悉皆的に分析することが可能な評価方法の提案を試みたものである。

（2）電子マネーを構成する情報セキュリティ技術

電子マネーの安全性を議論するためには、まず、電子マネーがどのような技術で成り立っているのかを念頭におく必要がある。電子マネーは情報セキュリティ技術の組み合わせによって構成される総合技術であり、暗号技術、耐タンパー技術といった要素技術のほか、これらを複雑に組み合わせて設計を行う電子マネー実現方式、電子マネーを実際に構築し稼働させるための実装技術、運用技術等によって構成されている。電子マネーの安全性を評価するためには、組み合わせられた技術ひとつひとつの安全性を評価すると同時に、「全体としての」電子マネーのシステムに欠陥がないことを確認する必要がある。

本研究では、電子マネーを構成するために必要とされる代表的な要素技術として、①暗号技術と②耐タンパー技術を取り上げる。暗号技術は、電子マネーが真正な発行機関によって発行され、取引において正当な手続を経て流通し、偽造・変造等の不正が行われていないことを保証したり、取引の内容を外部から秘匿するために使用される。暗号技術は、そのアルゴリズムや実装方法が開示され、多くの研究者が客観的な評価を可能とする技術研究を行っているため、どの程度のリスクがあるかを認識した上で適切な運用を行えば、比較的安心して使用することができる。

一方、耐タンパー技術とは、「外部からの不正な手続等により、秘密の情報を観測・改変することや、本来の設計意図とは異なる不正な動作を行わせること等を困難にするための物理的・論理的技術」のことである。耐タンパー技術を実現した製品として、CPUを内蔵したICカードがある。ICカードは、その中に格納された秘密情報に不正にアクセスしようとする攻撃への対策が講じられているが、メーカーによって具体的に想定している攻撃やその対策方法に関する技術開示が行われていないため、実際に使用するICカードがどの程度のリスクを持つものかを客観的に評価

することが困難なのが現状である。

電子マネーを設計するに当っては、「個々の要素技術の安全性が期待通りでなかったとしても、全体としては安全性を保てる」という「総合的な安全性」を実現することが重要である。そこで、本研究では、技術が十分開示されていないという意味でも客観的に安全性が評価されているとは言い難い「耐タンパー技術」を度外視し、耐タンパー技術に頼らずに電子マネーを実現した場合の安全性を、様々なケースについて評価した。こうして得た評価結果を基に、各電子マネー実現方式に耐タンパー技術あるいはその他の運用技術を導入して補完することにより、総合的な安全性を高める方法についての検討も可能となる。

（3）電子マネーの安全性評価

以下では、本研究で行った電子マネー実現方式の安全性評価について概説する。評価に当っては、電子マネーを主な技術的特徴に基づいてモデル化し、これに具体的な暗号技術を適用させた場合の電子マネー実現方式について、「価値を不正に入手する行為」に対するリスクを分析し、このリスクが小さいほど安全であると評価している。具体的には、各評価対象の電子マネー実現方式について、①利用者が不正に電子マネーの支払いを行うリスク、②商店が売り上げた電子マネーを不正にセンターに還流させるリスク、③センターの秘密情報を入手した利用者が不正に電子マネーの支払いを行うリスクを、「偽造・変造・複製等のどんな種類・程度の不正行為を許す可能性があるか（未然の防止対策有無）」、「不正が行われたときにこれを検知することはできるか（検知可否）」、「さらに不正が検知されたときに被害が広がることを押さえる二次的な対応策があるか（抑制）」、の3つの観点から評価している。

まず、電子マネーをモデル化するには、①電子マネーを価値の形態（残高管理型、電子証書型）、②転々流通性の有無（オープンループ型、クローズドループ型）、③価値情報の管理場所（センター管理、ローカル管理、センター・ローカル併用）、④取引時のセンター接続の有無（オンライン、オフライン）、の４つの技術的特徴について、考えられるすべての選択肢の組み合わせを候補として挙げ、その中で現実的にあり得るものを評価の対象モデルとした（実際に存在し得るモデルは全部で９種類）。

次に、それぞれの電子マネーモデルに対し、共通鍵暗号を使った方式、公開鍵暗号を使った方式、その中間的な方式の３種類の代表的な暗号技術およびそれを使ったプロトコルを適用した電子マネー実現方式を想定し、発生し得るリスクについての分析を行った。その結果、各電子マネーの技術的特徴が安全性に与える影響や、耐タンパー性等を組み合わせることにより総合的な安全性を高めることが必要なのはどのような場合か、等の考察が得られた。たとえば、センター接続を伴う特定の電子マネー以外は、基本的には耐タンパー性を持ったICカード等による付加的な安全対策を講じることが必要となるが、その必要性の程度には、利用する技術によって格差が存在すると評価できる。すなわち、ローカルに価値を管理する残高管理型の場合、仮に耐タンパー性が破られると不正の未然防止も検知もできなくなってしまうという意味で、耐タンパー性への依存度が高い。一方、電子証書型の場合には、

ローカルに価値を管理するケースにおいても、仮に耐タンパー性が破られても、偽造や二重使用を行った者が事後的に摘発可能であり、それが不正行為の抑止力として期待し得るため、耐タンパー性への依存度は低いと評価できる、等の考察が得られた。

４．宇根・太田論文「共通鍵暗号を取り巻く現状と課題 ― DESからAESへ―」

太田は、**宇根**との共同論文に基づき、最近の共通鍵暗号を巡る動向に関する発表を行った。**太田**は、金融分野で従来広く利用されてきた共通鍵暗号であるDES（Data Encryption Standard）が、コンピュータ技術の発展に伴って安全性が低下してきていることを紹介した上で、より安全な暗号としてTriple DESが米国国内標準となったこと、さらに米国政府によってAES（Advanced Encryption Standard）の選定作業が進められていることを紹介し、金融機関等の暗号技術の利用者も、こうした共通鍵暗号の研究動向に注目していく必要があることを強調した。発表の概要は以下の通りである。

（１）共通鍵暗号とDESの概要

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、情報の秘匿・改竄防止技術として、金融分野を中心に従来から幅広く利用されている。共通鍵暗号は、通信相手に鍵を安全に配送する必要があるものの、鍵の配送が不要な公開鍵暗号よりも高速で暗号化・復号を行うことができる。このため、データの暗号化手段として共通鍵暗号が利用され、共通鍵暗号の鍵を配送する手段として公開鍵暗号が利用される場合が多い。

これまで世界で最も幅広く利用されてきた共通鍵暗号方式は、1977年に米国政府標準暗号に認定されたDESである。DESは、鍵長が56 bit、ブロック長が64 bitであり、F関数と呼ばれる非線形変換を16回繰り返すことによって暗号化・復号を行う構造となっている。

（２）DESの安全性を巡る様々な議論

DESの安全性については、DESの標準化が行われた1970年代から、様々な論争が繰り広げられてきた。標準化を担当した米国商務省標準局は、「1秒間に約2500万個の鍵を検証可能な解読装置を構築できたとしても、全数探索法によって真の鍵を見つけるためには約91年かかる」との試算結果を発表し、DESが高い安全性を有していることを強調した。これに対し、暗号学者であるDiffieとHellmanは、「1秒間に約1兆個の鍵を検証可能な解読装置を利用すれば、１日足らずで解読できる。こうした解読装置を製作するためには現時点（1977年当時）で約2000万ドルが必要であるが、今後の技術進歩により、近い将来現実的な費用で同程度の性能を有する解読装置を製作できるようになる」と主張した。その後、コンピュータのコスト・パ

フォーマンス向上に伴って、DiffieとHellmanが指摘した解読装置の製造コスト低下は現実のものとなり、全数探索法に対するDESの安全性低下が多くの暗号研究者によって指摘されるようになった。

DESの安全性低下が指摘される中、RSA社は、DESの安全性を実証するために、1997年から1999年にかけて４回の懸賞金付きDES解読コンテストを実施した。この結果、1998年7月に開催された第３回のコンテストにおいて、約25万ドルで製作された解読装置によって56時間でDESが解読された。現実的な費用で製作された専用装置を用いてDESを短時間で解読できることが実証されたことで、DESの安全性に対する信頼は大きく低下し、DESに代わるより鍵長の長い暗号方式が必要との認識が一層強まっている（なお、本シンポジウムの後に開かれた1999年1月の第４回のコンテストでは、上記専用装置と約10万台のパソコンによって、約22時間でDESが解読されている）。

（３）Triple DESの提案

DESのアルゴリズムを利用しながら、全数探索法に対する安全性を高める方法として、DESの組み合わせ暗号であるTriple DESが提案されている。Triple DESは、異なる２つもしくは３つの異なる鍵を利用して、DESのアルゴリズムを３回繰り返す方式である。異なる３つの鍵を利用する場合（3-key Triple DES）には鍵長が168 bitに拡張され、異なる２つの鍵を利用する場合（2-key Triple DES）には鍵長が112 bitに拡張されるため、DESに比べ全数探索法に対する安全性が格段に向上する。さらに、Triple DESは、DESを利用したシステムを移行させることが比較的容易であるという利点も有している。このため、金融分野を中心にTriple DESを採用する動きが出てきており、米国における金融分野の標準化機関であるANSI X9[4]では、金融分野で利用される暗号アルゴリズム（ANSI X9.52）として、Triple DESの標準化を既に完了している。また、米国政府も、Triple DESをDESの次の米国政府標準暗号に認定するとみられている（なお、1999年1月、米国政府は、Triple DESを米国政府標準暗号〈FIPS 46-3〉として認定する方針を発表し、DESを利用している米国政府機関に対し、リスクに見合ったセキュリティ水準を確保できるようにTriple DESへの移行計画を慎重に策定することを要請している）。

ただし、Triple DESはDESに比べて処理速度が低下するほか、安全性に関する問題点がいくつか指摘されている。現時点では、これらの安全性に関する問題点は現実的な脅威とはならないとみられているものの、今後20～30年といった長期にわたって利用することを前提にすると、鍵長・ブロック長ともにより長い、単体の暗号方式が望ましいとされている。

4 ANSI（American National Standards Institute）：米国内の技術標準を策定する民間標準化団体。金融分野における情報セキュリティ技術の標準策定は、その専門委員会の１つであるX9（事務局：米国銀行協会）が担当している。

（4）AES標準化の動き

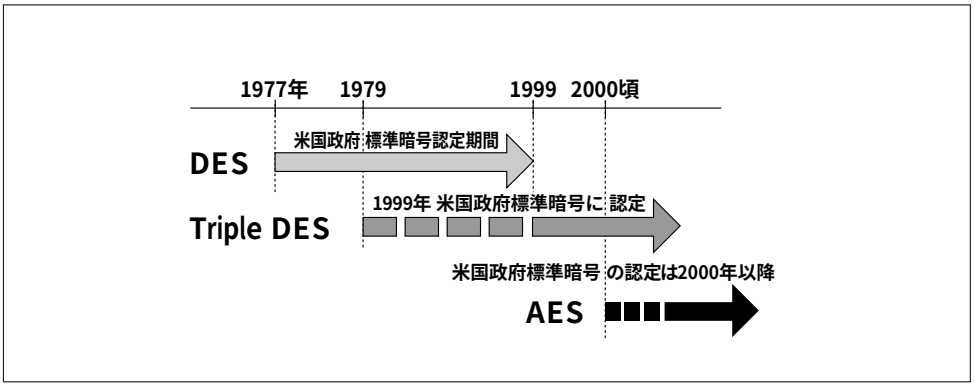
米国政府は、DESの安全性低下が深刻化していることを受け、1997年1月に次世代の米国政府標準暗号AESを公募によって選定する方針を発表し、同年9月にはその要件や評価基準等を公表している。

AESの要件としては、①共通鍵ブロック暗号であること、②鍵長として128、192、256 bitが利用可能であること、③ブロック長として128 bitが利用可能であること、④ロイヤリティ・フリーであること、の４つが挙げられている。また、AESの評価基準には、①安全性（解読困難性）、②コスト（処理速度等）、③実装環境からの中立性、等が挙げられている。

（5）より安全な暗号を求めて

現在発表されているAESの標準化スケジュールによれば、早ければ2000年内にも、現在候補となっている15のアルゴリズムのうち１つがAESとして認定される予定となっている。もっとも、標準化完了後、AESのアルゴリズムがその安全性について高い信頼を得て、AESを採用した暗号製品が普及するまでには、さらに数年程度はかかるものとみられている。このため、AESが一般に利用可能になるまでの間は、Triple DESがDESの後継暗号として利用されることになるとの見方が一般的となっている（図参照）。

現在米国政府は、AESの候補アルゴリズムの安全性・処理速度等に関する分析・評価を進めているほか、多くの暗号学者・研究者も候補アルゴリズムの安全性に関する分析を積極的に進めている。今後、こうしたAES標準化の進展とともに、共通鍵暗号に関する研究がより一層活発になるとみられる。金融業界は、実際もしくは潜在的には、共通鍵暗号の主要ユーザーのひとつであり、今後の研究動向についても、引き続き注視していく必要があると思われる。



５．宇根・岡本論文「公開鍵暗号の理論研究における最近の動向」

岡本は、**宇根**との共同論文に基づき、オープンなネットワークのセキュリティを守るために不可欠とされる公開鍵暗号を巡る理論研究の動向に関する発表を行った。**岡本**は、RSA暗号を利用した暗号通信プロトコルであるSSL（Secure Sockets Layer）に対する新しい攻撃方法が考案されたことを踏まえ、公開鍵暗号を利用する際に、RSA暗号の改良方式であるOAEP等、安全性が数学的に証明された方式を採用する動きがみられていることなどの最近の動向を紹介した。その上で、公開鍵暗号の実装技術とその安全性については、活発に研究が進められている分野であるため、理論研究と実用化研究とを密接に関連させて検討していくことが重要であることを指摘した。発表の概要は以下の通りである。

（１）公開鍵暗号の概要と種類

公開鍵暗号は、暗号化鍵と復号鍵が異なり、復号鍵（秘密鍵）を秘密にし、暗号化鍵（公開鍵）を公開する暗号方式である。公開鍵暗号には、認証機関が発行する公開鍵証明書等によって公開鍵の真正性を確保するためのインフラ（公開鍵インフラ）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各利用者は自分の公開鍵と秘密鍵のみを管理すればよい、③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、等の利点がある。このため、公開鍵暗号は、インターネット等不特定多数の利用者が参加するオープンなネットワークにおいて、情報セキュリティを確保するための必要不可欠な技術として位置付けられている。

現在実用化されている公開鍵暗号は、依拠している数学の問題によって、①素因数分解問題に基づく方式、②離散対数問題に基づく方式、③楕円曲線上の離散対数問題に基づく方式の３つに分類することができる。また、機能面から、①データ守秘方式と②ディジタル署名方式の２つに分類できる。

（２）安全性が証明されていない公開鍵暗号の問題点

これらの公開鍵暗号のうち、現在、事実上の標準となっているのがRSA暗号である。RSA暗号は素因数分解問題の困難性に依拠した方式であり、アルゴリズム発表後20年以上経過した現在まで、素因数分解よりも効率的な解読法が発表されていない。このため、RSA暗号は、安全性について信頼性の高い方式として、幅広い分野において利用されている。もっとも、RSA暗号の安全性は、素因数分解問題の困難性と等価であることが数学的に証明されていないため、素因数分解よりも効率的な解読法が存在する可能性は否定できない。

RSA暗号を利用する主要な暗号通信プロトコルとして、SSLが挙げられる。SSLは、Netscape Communications社が提唱する暗号通信、認証等のセキュリティ機能を有するプロトコルであり、代表的なブラウザーであるNetscape NavigatorやInternet Explorerに標準装備され、インターネット上で幅広く利用されている。SSLはセッ

ション鍵の配送等に公開鍵暗号方式を利用しており、その暗号化方法として、RSA暗号を利用した暗号通信データ形式に関する規格PKCS#1を採用している。

このSSLの潜在的な脆弱性が、1998年6月に、米国ベル研究所のBleichenbacherによって指摘された。Bleichenbacherは、ある特定の条件を満足する実装環境においてPKCS#1を利用した場合、能動的攻撃[5]によって暗号文を効率的に解読できることを示し、同様の条件を満足する実装環境下で利用されるSSLに対しても本攻撃が適用可能であるとの研究成果を発表した。これまでのところ、実際にSSLの暗号文を解読したという事例は報告されていないが、本攻撃はインターネットのセキュリティに対する潜在的な脅威として認識されており、インターネット技術者の間で注目を集めている。

（3）RSA暗号からOAEPへ

Bleichenbacherの研究成果は、RSA暗号が能動的攻撃に対して安全ではないことを示すとともに、実装環境次第では、SSLに対して能動的攻撃が適用できる可能性を示すものである。このため、RSA社は、PKCS#1を改良し、OAEP（Optimal Asymmetric Encryption Padding）を利用した平文の事前処理やパディングを実行するPKCS#1 Version 2を発表している。OAEPはRSA暗号の改良方式であり、RSA暗号と同程度の実用性を有していることに加え、一定の仮定の下で能動的攻撃に対する安全性が証明されている。

（4）証明可能安全性と実用性を両立させる公開鍵暗号の提案

公開鍵暗号の安全性の証明については、従来から多くの暗号学者によって研究が進められ、様々な「安全性証明付きの公開鍵暗号」が提案されてきた。しかし、それらの大半は、暗号化・復号のための計算量が莫大になる等の問題があったため、実用化は難しかった。しかし、最近、既に実用化されているいくつかの方式に改良を加えることによって、実用性を損なうことなく証明可能な安全性を有する方式を構成することができるとの研究成果が相次いで発表されている。

証明可能安全性と実用性を両立させる主なデータ守秘方式としては、OAEPが挙げられる。OAEPの暗号化・復号に必要な計算量は、RSA暗号の暗号化・復号の計算量に２回のハッシュ関数演算を加えたものに等しくなっており、RSA暗号と同程度の実用性を有している。

また、証明可能安全性と実用性を両立させる主なディジタル署名方式としては、PSS署名が挙げられる。PSS署名におけるディジタル署名の生成・検証に必要な計算量については、RSA署名の署名生成・検証の計算量に１回のハッシュ関数演算と２回のデータ拡張演算を加えたものに等しくなり、RSA署名と同程度の実用性を有している。

---

5 能動的攻撃：攻撃者が自分にとって都合のよい暗号文やディジタル署名に対応する平文を利用可能な環境下で行われる攻撃。

（5）インプリケーション

従来、公開鍵暗号の安全性の証明は、純粋に理論的な研究と考えられてきた。しかし、BleichenbacherによるSSLへの攻撃法の発表を受けて、こうした理論研究がセキュリティ技術の実用化に有用であることが理解されるようになってきている。公開鍵暗号は、インターネット等のオープンなネットワークで電子商取引を実現する上で必要不可欠な技術であるが、公開鍵暗号の実装を進める際には、従来、理論的にしか考えられてこなかった攻撃方法をも考慮に入れていくことが必要になる。情報セキュリティ技術においては、理論研究と実用化のための技術研究とを密接に関連させて検討していくことが必要である。

また、このSSLへの攻撃法は、RSA暗号を直接攻撃するものではなく、SSLの実装環境で実現される攻撃者と攻撃対象者の交信データから、対応する平文の情報を入手するというものであった。このことからわかるように、公開鍵暗号の安全性を検討する際には、利用される暗号アルゴリズムの選択やその鍵長について素朴な判断を下すだけではなく、実装環境や実用化方法をも考慮して安全性を評価していくことが必要となっていると言えよう。