第2回情報セキュリティ・シンポジウム

― 金融業務と認証技術 ―

会議の概要

Ⅰ．はじめに

インターネットを利用した金融サービスが拡大している。自宅や勤務先のパソコンから、オープンなネットワークを通じて、自由な時間に利用できるような金融サービスを提供して欲しいという顧客ニーズに応えるべく、銀行や証券会社は、こぞってオンライン・バンキングやオンライン証券取引等のサービスを開始している。この結果、金融機関の利用する情報通信ネットワークは、従来の企業内および業界内に閉じたネットワークから、オープンなネットワークに変化しつつある。金融機関にとっては、取引相手や取引内容の真正性を電子的に確認するために、情報セキュリティ技術を利用することが重要となっている。今後は、デジタル署名、デジタルタイムスタンプ、バイオメトリックスといった新しい認証技術を有効に活用していくことが必要になるものと思われる。

日本銀行金融研究所では、こうした問題意識に基づき、1999年11月1日に「金融業務と認証技術」をテーマとして、第２回情報セキュリティ・シンポジウムを開催した。金融研究所では、1998年11月に、「金融分野における情報セキュリティ技術の現状と課題」をテーマとした、第１回情報セキュリティ・シンポジウム[1]を開催しているが、今回のシンポジウムは、前回を引き継ぐ形で、金融機関が認証技術を利用して新しい金融サービスを提供していくために必要となる最新技術動向を紹介することを目的に開催された。シンポジウムには以下の６本の論文が提出され、各論文の内容に基づいて各執筆者による発表の後、総括および質疑応答が行われた。

1 第１回情報セキュリティ・シンポジウムの模様については、金融研究第18巻第２号（1999年4月）を参照。

・提出論文１「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」

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「金融業界におけるPKI･電子認証について ― 技術面、標準化に関する最近の動向を中心に」

執筆者　日本銀行金融研究所（現システム情報局）谷口文一

・提出論文３「最近のデジタル署名における理論研究動向について」

執筆者　日本銀行金融研究所　宇根正志

日本電信電話株式会社フェロー　岡本龍明

・提出論文４「デジタルタイムスタンプ技術の現状と課題」

執筆者　日本銀行金融研究所　宇根正志

東京大学講師　松浦幹太

日本電信電話株式会社主任研究員　田倉昭

・提出論文５「バイオメトリックスによる個人認証技術の現状と課題 ― 金融サービスへの適用の可能性 ―」

執筆者　東京大学助教授　中山靖司

早稲田大学教授　小松尚久

・提出論文６「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」

執筆者　日本銀行金融研究所　宇根正志

日本電信電話株式会社主任研究員　中原慎一

なお、フロアには、金融業界に加え、暗号学者、金融業務と認証技術に関連の深い官庁、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90名、日本銀行役職員約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。

Ⅱ．各発表の概要

１．松本・岩下論文「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[2]」

岩下（敬称略、以下同様）は、**松本**との共同論文に基づき、金融機関が従来提供してきた金融サービスにおいても、印鑑や暗証番号といった広義の認証技術が重要な役割を果たしてきたことを指摘したうえで、インターネット金融取引においてセキュリティを確保するために利用される新しい認証技術への取組み方について問題提起を行った。発表の概要は以下の通りである。

（１）インターネットを利用した金融サービスの拡大

わが国の金融機関の間でも、インターネットを利用した新しい金融サービスへの取組みが本格化しつつある。銀行業界では、インターネットを利用したオンライン取引サービスを拡充したり、インターネット・バンキングの専業銀行を設立しようという動きがある。証券業界でも、インターネットを利用したオンライン証券取引を拡大する証券会社が増えているほか、インターネットを主たる対顧客チャネルと位置付けた証券会社の新規参入が相次いでいる。

インターネットを利用した新しい金融サービスを金融機関が安全に提供していくためには、情報セキュリティ技術、とりわけ認証技術を有効に活用していくことが不可欠である。オープンなネットワーク上での金融取引が拡大する中で、金融業界にとって、認証技術の重要性が急速に高まってきている。

（２）従来の金融業務と認証技術

認証技術という言葉は、金融業務とはあまり関係のない専門用語のように受け取られてしまう傾向がある。しかし、金融機関にとって、「取引相手や取引内容の真正性を確認する」という意味での「認証」は、金融業務を構成するきわめて重要で本質的な手続のひとつであった。例えば、紙の世界における銀行との預金取引においては、通帳と印鑑が、真正な取引相手であることを認証する方式として利用されてきた。また、銀行のCD/ATMを利用する預金取引においては、磁気カード（キャッシュカード）と暗証番号の組合せによる認証が利用されている。これらの認証方式は、現状、人手をかけた監視を組み合せていることにより、実用レベルとしてはほぼ問題のないセキュリティを実現できている。しかし、①将来にわたって、現在と同じ金融サービスに現在と同じ認証方式を継続して危険はないか、②今後、新たな環境（例えば、オープンなネットワーク環境）で新たな金融サービスを提供する場合、現在の認証方式の延長で考えてよいか、については慎重な検討が必要である。

2 提出論文については、金融研究 第19巻別冊第１号（2000年4月）を参照。

（4）インターネット上でのセキュリティ確保の方策 ── SSLの安全性

オープンなネットワーク上における認証を実現するための技術として、SSL[3]やSET[4]、SECE[5]などといった標準規格を利用した電子認証技術が実用化されつつある。とくにSSLは、無償で配布されるブラウザーに標準で搭載されたソフトウェアであり、インターネットを利用したオンライン銀行取引、証券取引において現在最も標準的に利用されている。SSLを利用する場合、そのセキュリティ機能を正確に理解する必要がある。

SSLに対応したシステムを構築する場合、設計者は、多くのオプショナルな機能から、必要なセキュリティ・レベルに合わせてパラメータを設定できる。機能の選択方法によっては、比較的安全性の高い暗号通信と認証を行うこともできるし、強度の弱い暗号通信しかできない場合もある。そうした機能を正確に理解せずに、「SSLなら安全」、「共通鍵暗号の鍵長が128ビットなら安全」といった評価を与えることは適当ではない。とくに、①利用者に公開鍵証明書を取得させ、これを用いてクライアント認証を行っているか、②鍵交換やデジタル署名に利用されるRSA公開鍵暗号[6]の鍵長が十分安全か、といった観点を含め、正確な理解と評価が必要である。もちろん、SSLを部品として組み込んだシステムであっても、システム全体への配慮如何では、ある程度のセキュリティ上のニーズに応えられる優れたシステムになり得る。そのような観点から、システム全体のセキュリティをどう守るかを検討することが大切である。

（4）おわりに

認証技術についての検討が必要なのはインターネットを利用する場合に限らない。伝統的な金融取引において、比較的脆弱なセキュリティ対策が通用していたのは、利用環境が不正を排除する仕組みをもっていたためであった。金融機関を取り巻く環境は大きく変化しているため、新しい金融サービスにチャレンジする場合はもちろんのこと、既存の金融サービスにおけるセキュリティ対策のあり方を考えるうえでも、考えられるさまざまなリスクを検討したうえで、有効な対策を講じていく必要がある。

金融機関は、新しい情報技術や通信インフラを活用してその業務を展開していくことが要請されており、それを実現するうえで、認証技術を活用したセキュリティ対策は不可欠なものである。そうした対策について着実な検討を積み重ねていくこ

3 SSL（Secure Sockets Layer）: Netscape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。

4 SET（Secure Electronic Transactions）: VISAとMaster Cardによって提案された、インターネット上でのクレジットカード決済を安全に実現するための技術仕様。

5 SECE（Secure Electronic Commerce Environment）: SETに準拠して日本で作成された、インターネット上で銀行取引、クレジットカード取引を安全に行うための技術仕様。

6 1978年にRivest、Shamir、Adlemanによって提案された、素因数分解問題の困難性に依拠した公開鍵暗号方式であり、現在金融分野をはじめとする幅広い分野において実用化されている。

とにより、わが国の決済システム全体の利便性、効率性、安全性を高めていくことは、わが国全体の利益に繋がることと考えられる。

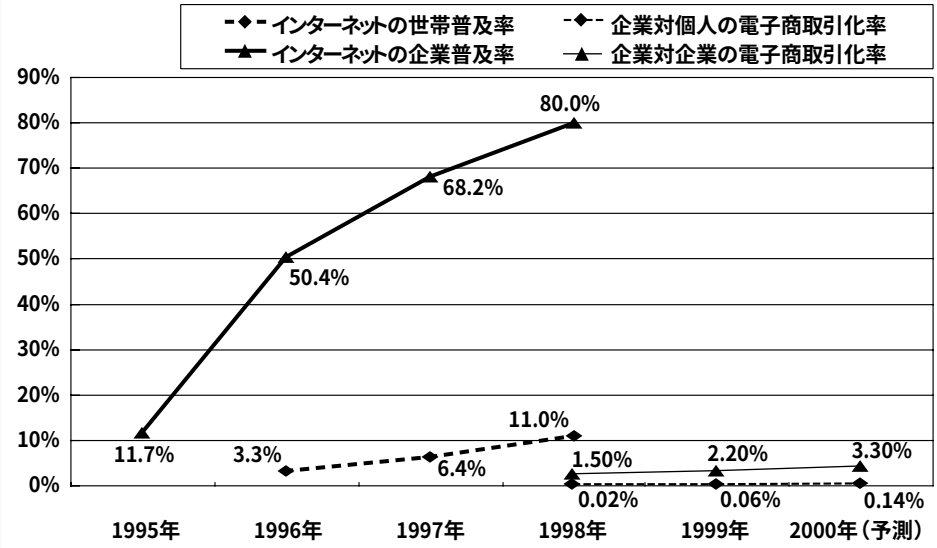
２．谷口論文「金融業界におけるPKI・電子認証について ― 技術面、標準化に関する最近の動向を中心に[7]」

谷口は、標題論文に基づき、金融分野においてPKI（Public Key Infrastructure）・電子認証を活用していくうえでの技術面からみた問題点とその対応策等について発表を行った。発表の概要は以下の通りである。

（1）インターネット上でのセキュリティ確保

近年、一般家庭においても企業においても、インターネットが急速に普及してきているが、電子商取引の規模はあまり拡大していない（図参照）。その理由の一つとして、セキュリティ面での不安が挙げられる。インターネット上でのセキュリティを確保するためには、取引相手・データ内容の真正性を確認することが重要であり、このために電子認証が必要と言われている。

インターネットの拡大と電子商取引



（出典）平成11年度通信白書（郵政省編）、日米電子商取引の市場規模調査（通産省）

7 提出論文については、金融研究 第19巻別冊第１号（2000年4月）を参照。

（2）PKI・電子認証とは

電子認証とは、電子的な取引において送信されたデータが、①本人が作成したものであること、②途中で改ざんされていないこと、を電子的に作成された署名であるデジタル署名により確認することである。電子認証には公開鍵暗号を用いるが、通信相手の正当な公開鍵をいかに配布するかということが電子認証の実現にとって決定的に重要である。そのために利用されるのがCA（Certification Authority）である。CAは、公開鍵の真正性を証明するために、取引の当事者双方に信頼される第三者機関として、公開鍵証明書の発行・維持管理を行っている。このようなCAや公開鍵証明書といった、公開鍵暗号に基づいた技術を用いて安全な通信を行う全体的な仕組みをPKIと呼ぶ。

電子認証が普及してくると、異なるCAを利用する相手とも取引を行いたいというニーズが高まってくるが、その解決策としてCA間で信頼を確立する方法がいくつか存在する。

（3）金融とPKI・電子認証

もともと、金融では業務の大部分が情報の交換のみで完結するため、電子的な取引と親和性が高い。金融では高額の取引を扱うことが多いため、これまで金融機関の情報化は第三者からの専用線を用いて、自ら十分管理できるコンピュータセンターやATMを利用するのが中心的であった。しかし、電子認証を用いることにより安全性を確保しながら、インターネット上で情報化を進めることができれば、元来金融が有している電子的な取引との親和性の高さを活かし、より広い顧客ベースに対して、より低コストで、より高い利便性をもってサービスを提供することが可能になる。

（4）PKI・電子認証の標準化

金融分野でPKI・電子認証を実現するうえでは、相互運用性や一定の信頼性の確立のために、標準規格に準拠する必要がある。その際に利用可能な標準規格として、ISO15782等の国際標準、FIPS140-1等の米国国内標準、PKCS等の業界標準等が存在する。一つの標準がPKI・電子認証のすべての部分をカバーしているわけではないため、電子認証システムを構築するためには多くの標準を組み合わせることが必要になる。

(5) 技術的側面からみたCAの重要な役割

CAが果たすべきさまざまな技術的役割のうち、とくに重要であると考えられるのは、CAの秘密鍵の保護、公開鍵証明書の有効性確認、認証実施規定（CPS[8]）の作成・周知である。CAの秘密鍵保護のためには、FIPS 140-1で定められている安全

8 認証実施規定（CPS: Certification Practice Statement）: CAが、（そのシステム構成や組織運営手順の中で）公開鍵証明書を発行する際に用いる運用の規程。

な暗号モジュールを用いる方法や秘密鍵を分割する方法が有効であろう。公開鍵証明書の有効性確認のためには、廃棄された公開鍵証明書のリストであるCRLを作成・配布する方法と、必要な都度サーバーにアクセスして公開鍵証明書の最新の情報を確認するOCSP（Online Certificate Status Protocol）を利用する方法が一般的である。CPSの作成・周知は、CAが提供する認証サービスの安全性を利用者に理解してもらうという意味で重要である。一方、CA間での相互運用性を確保する目的では、CPSをより簡単にした認証ポリシーを用いることが一般的である。

（６）PKI・電子認証に関する最近の技術的動向

PKI・電子認証に関する最近の技術的動向としては、秘密鍵と本人を結び付ける目的で、身体的特徴により暗証番号を代替、補完するバイオメトリックスの採用や、秘密鍵の分割の一方法であるProactive Signature、社内の役職等属性による認証等が挙げられる。

（７）総合的なセキュリティ対策の必要性

今後は、CA側での十分なセキュリティ対策を前提として、クライアント側での対策を含め、電子認証システム全体で総合的にセキュリティ対策を行っていくことが重要であろう。

３．宇根・岡本論文「最近のデジタル署名における理論研究動向について[9]」

岡本は、**宇根**との共同論文に基づき、最近のデジタル署名方式に関する動向として、RSA署名をベースとしたデジタル署名方式の国際標準や、安全性が証明されているデジタル署名方式を巡る動向について発表を行った。発表の概要は以下の通りである。

（１）デジタル署名の機能と原理

デジタル署名は、署名者固有の情報（署名生成鍵）を用いてデータを変換することによって生成されるデータであり、①データの作成者を特定する機能、②データの改ざんを検出する機能、③いったん生成された署名に関して、その署名を生成した事実の否認を防止する機能を有している。デジタル署名は公開鍵暗号方式に基づいて実現される。すなわち、公開鍵暗号における秘密鍵を署名生成鍵とし、公開鍵を署名検証鍵とすることにより、「署名の生成は特定の個人にしかできないが、署名の検証は誰にでもできる」という紙ベースにおける署名や印章の機能をデジタルデータにおいて実現することができる。

これまでの研究によってさまざまなデジタル署名方式が提案されてきたが、その中で最も代表的な方式がRSA署名である。これまでにRSA署名の安全性に関する研究成果が数多く発表されており、RSA署名をベースとした署名方式が金融分野をは

9 提出論文については、金融研究 第19巻別冊第１号（2000年4月）を参照。

じめとする幅広い分野において利用されてきた。

（2）RSA署名をベースにした署名方式の国際標準に対する攻撃法とその影響

しかし、最近、RSA署名をベースにした署名方式に対して有効な攻撃法が提案され、従来の安全性評価の方法では不十分であるとの認識が広がっている。

攻撃法が提案されたのは、RSA署名をベースとしたデジタル署名方式の国際標準ISO/IEC 9796であり、ISOの場でその安全性が十分に検討されたと思われていた。しかし、米国の暗号研究者Coppersmithらは、1999年8月に本署名方式に対して有効な攻撃法を発表し、本署名方式が実装環境によっては十分な安全性を確保できないことを示した。これを受けて、情報セキュリティ技術の標準化を担当するISO/IEC JTC1/SC27が1999年10月にISO/IEC 9796を廃止することを決定し、ISOの国際標準となっている暗号アルゴリズムの安全性に対する信頼が大きく低下することとなった。

（3）安全性が証明されているデジタル署名方式

ISOによるデジタル署名方式の国際標準に有効な攻撃法が提案されたことによって、「安全性が証明されている署名方式」が必要であるとの見方が広がっている。「安全性が証明されている署名方式」は従来からいくつか提案されてきたが、署名生成・検証に必要な計算量が莫大であり、いずれも実用性の面で課題が残されていた。しかし、近年では、既に実用化されている署名方式に改良を加えることによって、実用性を維持しつつ、安全性証明を付与することのできるデジタル署名方式が相次いで発表されている。例えば、RSA署名をベースとした方式としては、FDH-RSA署名、PSS署名、PSS-R署名が提案されており、これらの署名方式を利用することによって、既存のRSA署名における実用性を大きく損なうことなく、「安全性が証明されている署名方式」を実現することができる。

（4）インプリケーション

インターネットの急速な拡大に伴ってデジタル署名の利用環境の多様化が進んでおり、従来想定されていなかった攻撃法が現実のものとなってきている。このため、デジタル署名方式の安全性を検討する際には、既存の攻撃法を前提とした評価結果を参考にするだけでは不十分である。

「安全性が証明されているデジタル署名方式」には、証明の前提となる仮定の現実的な妥当性が必ずしも自明でないといった問題もある。しかし、安全性証明の研究は、従来の評価方法よりも理論的に精緻な評価を可能とする。金融分野においてデジタル署名方式を用いた情報システムを構築しようとする際には、安全性証明に代表される理論的な評価を考慮していくことが必要であろう。

４．宇根・松浦・田倉論文「デジタルタイムスタンプ技術の現状と課題[10]」

松浦は、**宇根**、**田倉**との共同論文に基づき、デジタルタイムスタンプ技術の特徴や安全性に関する分析結果のほか、最近の主要な研究プロジェクトや商用サービスについて発表を行った。発表の概要は以下の通りである。

（１）デジタルタイムスタンプ技術の重要性の高まり

近年、インターネットの急速な拡大に伴い、オープンなネットワーク上での電子商取引が活発化しているほか、紙ベースの文書を電子媒体に置き換えて管理する電子文書管理を採用する動きが広がっている。このため、「誰が、いつ、どんなデータを生成し、交信したか」を第三者が証明する「電子公証」の必要性が高まっている。電子公証は、データの送受信者の特定、時刻情報の付与、改ざんの検知等の機能を備えるものといわれている。

デジタルタイムスタンプ技術は、電子公証を構成する技術の一つであり、①データが特定時刻に存在していたことを証明する機能（存在証明）や、②特定時刻以降にデータが変更されていないことを証明する機能（完全性証明）を実現する技術である。

（２）デジタルタイムスタンプの分類と安全性に関する分析

デジタルタイムスタンプは、一般に、その生成機関（Time Stamp Authority〈TSA〉）の性質とその生成方法によって分類される。まず、TSAの性質によって、「TSAが予め規定された業務規律に従って業務を遂行する」ことを信頼できる場合と信頼できない場合に分類されるほか、タイムスタンプの生成方法によって、Simple Protocol、Linking Protocol、Distributed Protocolに分類される（各プロトコルの概要については下の表参照）。

プロトコル	概要	主な特徴
Simple Protocol	1つのTSAが、タイムスタンプの対象データのハッシュ値に時刻情報を付与し、デジタル署名をタイムスタンプとして生成。	・TSAが信頼できることが必要。 ・システム構成が比較的単純。
Linking Protocol	TSAが複数のハッシュ値を相互に関連づけるリンク情報を生成し、そのリンク情報を利用してタイムスタンプを生成。	・リンク情報の一部を新聞等に公表することで、TSAを信頼できなくてもシステム全体の安全性を確保可能。 ・システム構成が比較的複雑。
Distributed Protocol	複数のTSAが生成するデジタル署名を用いてタイムスタンプを生成。	・複数のTSAを利用することで、各TSAを信頼できなくてもシステム全体の安全性を確保可能。 ・システム構成が比較的複雑。

10 提出論文については、金融研究第19巻別冊第１号（2000年4月）を参照。

Simple Protocolでは、タイムスタンプの安全性がTSAの管理・運営体制に全面的に依存することから、攻撃者がTSAと結託可能な場合、タイムスタンプの改ざんを防止することが困難となる。ただし、Simple Protocolは、他のプロトコルに比べてシステム構成が単純なため、安全性よりもコスト面を重視するアプリケーションに向いている。一方、Linking Protocolは、システム構成が複雑になるものの、リンク情報の一部を新聞等に掲載することによって、リンク情報の改ざんを困難にする。この結果、たとえ攻撃者とTSAが結託し、そのTSAが管理するタイムスタンプやリンク情報の一部が改ざんされた場合でも、改ざんの事実を検出することが可能となる。このように、Linking Protocolでは、TSAが信頼できない場合でも、安全性を維持することができる。Distributed Protocolにおいても、タイムスタンプの生成に必要となるTSAの数が増えると、攻撃者とTSAとの結託がより困難になるため、個々のTSAが信頼できない場合でも、安全性を維持することが可能となる。

（3）研究・実装動向

現在、デジタルタイムスタンプの研究プロジェクトが世界各国で進められている。わが国では、法務省が電子公証制度の検討を行っているほか、海外では、ベルギー、スペイン等において政府が関与したプロジェクトが進められている。

また、主要な商用サービスとしては、米Surety社のDigital Notary Serviceが挙げられる。本サービスは1992年から開始されており、Linking Protocolをベースとしたシステムが実用化されている。本サービスでは、ハッシュ関数[11]を階層的に用いて生成したリンク情報の一部が毎週日曜日にニューヨーク・タイムズ紙に掲載され、リンク情報を衆目にさらすことによってリンク情報の改ざんを困難にしている点が特徴である。

（4）インプリケーション

デジタルタイムスタンプ技術は、電子公証を構成する技術の一つとして電子商取引や電子文書管理の実現に不可欠な技術であり、今後金融機関の情報システムにおいても利用される可能性があることから、今後の研究動向や標準化動向に注目していくことが有用であろう。

５．中山・小松論文「バイオメトリックスによる個人認証技術の現状と課題 ― 金融サービスへの適用の可能性 ―[12]」

小松は、**中山**との共同論文に基づき、バイオメトリックスによる個人認証技術と、その金融サービスへの適用の可能性について発表を行った。発表の概要は以下の通りである。

11 ハッシュ関数とは、任意長の入力データXから固定長のデータH（X）を出力する関数。情報セキュリティの目的で利用される場合は、①出力データから入力データを求めることが難しいこと（一方向性）、②出力データが同一となるような、異なる複数の入力データを見つけることが難しいこと（衝突困難性）、といった性質を満たす必要がある。

12 提出論文については、金融研究 第19巻別冊第１号（2000年4月）を参照。

（1）ネットワークを介した金融取引と個人認証技術の重要性

情報通信技術の進展によって、金融サービスのほとんどはコンピュータ・ネットワークを介して提供されるようになってきている。銀行のCD/ATMにおける現金の受払や振込、クレジットカードやデビットカードを利用した決済等は、いずれもコンピュータ・ネットワークによって金融機関に接続された端末から提供される金融サービスである。また、最近では、利用者がインターネット等のオープンなネットワークを通じて自宅のパソコンや携帯電話から金融取引を行うことも可能になってきている。

ネットワークを介して金融取引を実施する場合には、取引相手の真正性を確認することが必要となる。キャッシュカードやデビットカードでは、取引を行おうとしている相手がカードを保持し、かつあらかじめ登録してある４桁の暗証番号を知っているということを確認することによって本人であると判断している。また、クレジットカードでは、カードを保持していることと、目の前でカードにあらかじめ記入されているのと同じ署名を行うことができることを商店が確認することによって本人確認を行う仕組みとなっている。しかしながら、こうした本人確認方法は必ずしも確実な手段とはいえない。さらに、これらの決済サービスがインターネットを介して提供される場合には、カードや署名の物理的な提示ができないため、口座番号と暗証番号等を送信するだけの確認となり、不正使用が容易になるという問題がある。このように、既存の本人確認手段は、とくにオープンなネットワークでの利用においては、安全性の面からみると、多くの課題を抱えている。

（2）バイオメトリック認証への関心の高まり

そこで、安全で確実に本人を確認する手段として、バイオメトリック認証が注目されている。バイオメトリック認証とは、対象者の身体的特徴（指紋、網膜等）や身体的特性（筆跡、音声等）などの対象者個人に固有の情報をあらかじめ計測してシステムに登録しておき、取引の都度測定する本人の特徴・特性が登録データと合致するかどうかによって相手の真正性を確認する方法である。バイオメトリック認証は、さまざまな要素技術の研究が進められているほか、金融分野を含め、実用化された事例もある。

バイオメトリック認証を用いて本人を特定する場合、誤りの有無や程度をどう捉えるかが非常に重要になる。通常、登録された個人の特徴に関する情報と入力された情報が全く同じということはあり得ないため、両者がどの程度似ているかという観点から本人を特定せざるを得ず、統計的な取扱いが必要となる。他人を受理してしまう誤りと本人が否認されてしまう誤りのどちらを重視するか、暗証番号等の他の手段の併用を行うか、等についても慎重な検討が必要である。

（3）バイオメトリック認証の実用化を進めるために

バイオメトリック認証に関する研究は一部では実用段階へ入りつつある。しかし、この技術が実際に個人認証の手段として使われるようになるためには、安全性の問

題に加えて、さまざまな側面について配慮が必要である。例えば、社会的な容認を得るためのコンセンサスづくりの必要性、操作の容易性、端末の小型化・低廉化等である。

とくに、バイオメトリック認証においては、個人の身体的特徴等のプライバシーに関わる情報を扱うため、利用者に受け入れられるような社会的な配慮を行うことによって、バイオメトリック認証の導入に関するコンセンサスを得ておくことが必要不可欠である。どういう機関がバイオメトリック情報を登録して管理するのかという、運用面の課題も解決されていなければならない。

バイオメトリック認証は、本人であることを証明するために何かを携帯したり、暗証番号を記憶する必要がなくなる可能性もあり、利用者にとって利便性が高いほか、既存の個人認証方式よりも高度なセキュリティを実現することが期待できる。現在、多くの産業分野で実用化が進みつつあるが、金融取引の安全性を高める手段としても検討に値する認証技術と考えられる。

６．宇根・中原論文「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[13]」

宇根は、**中原**との共同論文に基づき、金融機関が情報セキュリティ対策を検討する際に参考となる標準規格や評価・認定スキームについて発表を行った。発表の概要は以下の通りである。

（１）金融ネットワークのオープン化と情報セキュリティ対策

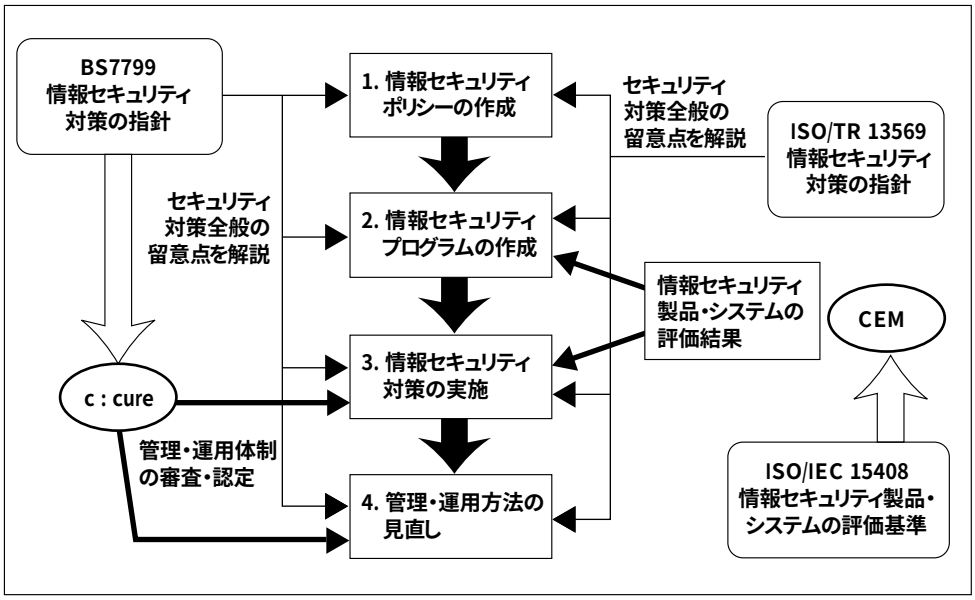
従来の金融ネットワークは、銀行の本支店間のオンラインシステムや全銀システムに代表されるように、企業内、業界内に閉じたネットワークが中心であった。このため、金融ネットワークにおける情報セキュリティ技術は、入退室管理等物理的なアクセス管理が中心であったほか、国内や業界内のみ利用可能な独自方式が採用されていた。

しかし、近年のインターネットの急速な拡大に伴い、インターネット・バンキング等オープンなネットワークを利用した金融サービスを開始する金融機関が増えており、金融ネットワークのオープン化が進んでいる。この結果、外部から金融機関の内部システムへの不正アクセスの可能性が高まっており、電子認証技術を利用した論理的な情報セキュリティ対策が必要となっているほか、国際的なセキュリティ水準との整合性も考慮することが必要となっている。

こうした観点から情報セキュリティ対策を検討する場合、情報セキュリティ技術の中でも国際的に高い評価を得ている技術を規定し、従来から欧米の金融機関を中心に幅広く利用されている標準規格や指針が参考になる。これらの中でも、ISO/TR 13569、BS 7799、ISO/IEC 15408が有用である（図参照）。

13　提出論文については、金融研究 第19巻別冊第１号（2000年4月）を参照。

情報セキュリティ対策の実施手順と関連する標準規格



（2）情報セキュリティ対策の指針と評価・認定スキーム

金融業務における情報セキュリティ対策全体の指針としては、ISO/TR 13569とBS 7799が挙げられる。ISO/TR 13569は、金融分野を対象とした情報セキュリティ対策の指針であり、金融サービス関連の技術の標準化を担当するISO/TC68において策定されたものである。ISO/TR 13569はISO/TC68が策定した情報セキュリティ手段に関する国際標準をベースに作成されていることから、ISO/TR 13569を利用することによって、ISOの国際標準に準拠した対策を講じることが可能になる。

一方、BS 7799は、汎業界向けの情報セキュリティ対策の指針であり、英国の国内標準である。BS 7799には、①国際標準ではないものの、欧州の金融機関において情報セキュリティ対策を講じる際に利用されているほか、②第三者機関が情報セキュリティの管理・運用体制を評価・認定するスキームc:cureが運用されているという特徴がある。c:cureの制度的な枠組みには、品質管理に関する評価・認定スキームであるISO 9000シリーズの英国における枠組みが利用されている。

（3）情報セキュリティ製品・システムの評価基準と評価・認定スキーム

情報セキュリティ製品・システムを選択する際の指針としては、ISO/IEC 15408が挙げられる。ISO/IEC 15408は、情報セキュリティ製品・システムの評価基準の国際標準であり、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」をベースに策定されたものである。また、ISO/IEC 15408に基づいて第三者機関が情報セキュリティ製品・システムの評価・認定を行うスキームとしてCEM（Common Evaluation Methodology）が提案されており、現在欧米６カ国がその利用を検討している。

（4）インプリケーション

金融機関が情報セキュリティ対策を講じる際には、ISOの国際標準や各種指針等を利用するほか、第三者機関によるセキュリティ評価・認定スキームを活用することが考えられる。ただし、第三者機関による評価・認定は、情報セキュリティ対策の一面について最低限のセキュリティ水準を保証するものであり、情報システム全体のセキュリティを保証するものではないことを十分認識しておく必要がある。

Ⅲ. 総括

松本は、金融業務と認証技術を取り巻く環境の変化について整理した後、６つの発表の内容について以下のように総括を行った。

従来の金融業務では、紙やクローズドな金融ネットワークを前提として、「通帳と印鑑」や「磁気カードと暗証番号」といった認証技術が利用されてきた。しかし、最近では金融ネットワークのオープン化が進展しており、従来の金融ネットワークにおける前提が崩れてきていることから、電子認証やPKIをはじめとする新しい認証技術の活用が必要となっている。こうした金融業務と認証技術を取り巻く環境の変化、新しい認証技術の必要性やそれを利用する際の留意点が、**提出論文１「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」**によって説明された。

この問題提起を受けて、提出論文２～５に基づく発表では、具体的な認証技術について説明が行われた。**提出論文２「金融業界における**PKI**・電子認証について」**では、PKIや電子認証の動向について説明があった。PKIは、ネットワークを介して、直接対面することができない相手を確認するメカニズムといえよう。

提出論文３「最近のデジタル署名における理論研究動向について」では、安全性が証明されているデジタル署名方式が最近注目されている背景やその現状について説明が行われた。デジタル署名方式単体では安全性の証明が可能になってきているが、今後は、情報システム全体の安全性が理論的に保証されるようなシステムの構成方法に関する研究の進展も期待される。

提出論文４「デジタルタイムスタンプ技術の現状と課題」では、電子商取引や電子文書管理の実現の鍵となるデジタルタイムスタンプ技術について説明が行われた。後々の係争や情報公開等に備えるための電子公証において時刻付与と改ざん検知を実現する技術として、今後はとりわけ評価手法も含めた研究が期待される。

提出論文５「バイオメトリックスによる個人認証技術の現状と課題」では、バイオメトリック認証技術の現状と課題について説明があった。バイオメトリック認証技術を実際に活用するためには、プライバシー情報をいかに管理するか等、運用上の課題が残されており、こうした課題をどのように解決していくかについて議論を深める必要がある。

提出論文6「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」では、金融機関が認証技術を検討する際に参考になる標準規格や第三者機関による評価・認定スキームが説明された。だたし、いくら優れた認証技術を利用して情報システムを構築したとしても、利用者の行動次第で情報セキュリティは損なわれる可能性がある。適切な管理・運用体制に沿った情報システムの利用をいかに確保するかについても考慮することが必要である。

Ⅳ. 質疑応答

総括の後、フロアから、「インターネット・バンキング等のオープンなネットワークにおけるリテール金融取引の分野では、日本の金融業界の取組みは米国の金融業界に比べて遅れている」と聞くことが多いが、日本は米国にキャッチアップすることができるか、との質問が寄せられた。

これに対し、**岩下**は、これまで本分野における日本の金融業界の取組みが米国に比べて遅れたことは否定できないものの、今後キャッチアップできないほどの致命的な遅れではなく、オープンなネットワークを利用した金融サービスの市場は日本の金融業界にとって非常に有望な分野であると思う、と回答した。さらに、**岩下**は、日本の金融業界が、これまでクローズドな金融ネットワークを前提としたセキュリティ対策に注力してきたため、金融ネットワークのオープン化という環境変化の中で適切な情報セキュリティ対策への対応が遅れ、ビジネスチャンスを活かすことができなくなってしまうといった事態を防ぐことが必要であると指摘した。

また、フロアから、バイオメトリック技術を活用するうえで、プライバシーを確保するための技術的な検討だけでなく、社会的なインフラ整備をどのように進めていくかについても検討する必要はないか、との質問があった。

小松は、バイオメトリック技術を実際に利用していくためには、ヒューマン・インターフェイスやパターン・マッチング等の「バイオメトリック認証を実現するための技術」に加えて、個人のプライバシー保護をはじめとする倫理的問題にも目を向ける必要があると回答した。**小松**は、学際的な場を利用して社会的、制度的な面からも検討を加え、「社会に受け入れられやすいバイオメトリック技術をどのように実現するか」という観点から研究・開発を進めることが大切であると指摘した。