『金融研究』（第19巻別冊第1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1)を発行している。以下は、第19巻別冊第1号（平成12年4月発行）所収論文(注2)の要約を紹介したものである。

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

松本　勉／岩下直行

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。こう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。

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極めて重要で本質的な手続きのひとつである。本稿では、既存の金融業務において利用されてきた認証方式の変遷を辿るとともに、その視点から、インターネットを利用した金融業務においてセキュリティを確保するためには、認証技術をどのように利用していくべきかについて整理する。

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―

谷口文一

近年、金融業界において、電子認証および電子認証関連サービスのインフラであるＰＫＩ（Public Key Infrastructure）が注目を集めている。ＰＫＩ・電子認証は、インターネット上で行う電子商取引を安全・確実なものにするためには欠かせない要素技術である。インターネットは、従来のクローズドなネットワークに比べて通信コストが圧倒的に低い、全国・全世界のユーザーと通信可能であるというメリットがある反面、通信相手ややり取りするデータが本当に正しいのかどうか確認することができなかった。ＰＫＩ・電子認証はこのインターネット上でクローズドなネットワークの場合と同等の安全性を可能とするものである。とくに安全で確実な処理が求められる金融機関にとって、インターネットを

（注1）『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19巻別冊第1号（定価1,050円）は、ときわ総合サービス（株）（本『日本銀行調査月報』刊行物一覧を参照）より販売。

（注2）所収論文は、日本銀行金融研究所ホームページ（http://www.imes.boj.or.jp/）「発表論文等」コーナーにも掲載されています。

通じたサービスの提供を可能にするＰＫＩ・電子認証は、顧客との関係を大きく変える契機となる可能性がある。

そこで本稿では、金融業界におけるＰＫＩ・電子認証に関する最近の動向について技術面・標準化面を中心とした検討を行うこととする。とくに、ＰＫＩ・電子認証では公開鍵証明書の発行等管理を行う認証機関（ＣＡ）が非常に大きな役割を果たすため、金融業務に利用されるＣＡが認証サービスを提供する場合に関連する標準の内容や果たすべき技術的役割について検討することとする。なお、ＰＫＩ・電子認証の実装技術の細部については未だ主流となる技術が確立していない部分も多い。このため、本稿では、今後注目していく必要があると思われる最新の技術動向についても紹介する。

最近のデジタル署名における理論研究動向について

宇根正志／岡本龍明

本稿は、これまでに提案されている主要なデジタル署名方式のアルゴリズムや標準化動向を紹介したうえで、最近明らかになったＲＳＡ署名に対する攻撃法や、安全性が証明されているデジタル署名方式の理論研究の動向について説明するものである。

従来、デジタル署名方式の安全性評価は、既存の攻撃法を前提とした評価が中心であった。しかし、デジタル署名方式の実装環境が多様化する中、これまで検討されていなかった攻撃法が有効になる可能性が高まっている。こうした中、1999年８月、ＲＳＡ署名を利用したデジタル署名方式の国際標準ISO/IEC 9796に対して有効な攻撃法が提案され、本国際標準の標準化を担当するISO/IEC JTC1/SC27は、同年10月にISO/IEC 9796を取り下げることを決定した。この結果、既存の攻撃法を前提とした安全性評価では不十分であり、一定の数学的な仮定のもとで効率的な攻撃法が存在しないことを証明する「安全性証明」のような理論的な安全性評価が必要との認識が強まっている。

最近では、安全性が証明されているとともに、処理速度の面で実用性の高いデジタル署名方式が相次いで提案されており、ＩＳＯやＩＥＥＥ等では、安全性が証明されている署名方式の国際標準への採用が検討されている。今後、デジタル署名を利用する際には、実装技術に関する研究成果に加えて、安全性証明に関する研究等、最新の理論的な研究成果を十分考慮することが必要であろう。

デジタルタイムスタンプ技術の現状と課題

宇根正志／松浦幹太／田倉　昭

デジタルタイムスタンプ技術は、デジタルデータがある特定時刻に存在していたことを証明するとともに、その時刻以降データが変更されていないことを証明する技術である。近年、インターネット上での電子商取引の活発化や、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の利用拡大に伴い、「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」の仕組みが必要とされている。電子公証は、送信受信者の特定、到達確認、時刻情報の付与、改ざんの検知、電子文書保管等の機能を具備するものといわれており、デジタルタイムスタンプ技術は、このうち、時刻情報付与や改ざん検知の機能を実現する技術である。

従来からデジタルタイムスタンプ技術に関す

る理論研究が行われてきたが、最近では、実装を視野に入れた研究が世界各国で開始されている。日本では、法務省が、電子確定日付サービスを含む電子公証制度の実現に向けて検討を行っているほか、海外では、ベルギーやスペイン等において研究プロジェクトが進められている。また、米国や英国では、既に民間企業がサービスを開始している。

一方、デジタルタイムスタンプ技術の標準化も進められている。インターネット上での公開鍵インフラに関する標準化を行うIETF PKIXは、タイムスタンプ・プロトコルの標準規格の策定を行っているほか、情報セキュリティ技術の国際標準化を担当するISO/IEC JTC1/SC27においても、デジタルタイムスタンプのサービスに関する標準化作業が進められている。

デジタルタイムスタンプ技術は、今後、金融分野をはじめとする幅広い分野において利用されるようになるものとみられる。本稿では、デジタルタイムスタンプ技術の特徴や機能について整理したうえで、最近の研究・実装動向、標準化動向や、デジタルタイムスタンプ技術に関連する主要な特許を紹介する。

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 —

中山靖司／小松尚久

本稿は、バイオメトリックスによる個人認証（バイオメトリック認証）について、金融サービスへの適用を想定しつつ、その概要、研究開発動向、標準化動向、安全性評価、実用化事例等を紹介したものである。

近年、情報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・システムによって提供されるようになってきており、利用者がインターネット等を通じて自宅のパソコンからサービスを受けることも可能になってきている。ネットワークを介してサービスを提供する場合には、サービスを受けようとしている相手の真正性を確認することが重要である。しかしながら、キャッシュカードと暗証番号の組合せなど、既存の金融サービスで用いられている一般的な本人確認方法は、安全性の面から必ずしも確実な手段とはいえず、多くの課題を抱えている。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、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。

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

宇根正志／中原慎一

インターネットを利用したオンラインバンキングやオンライン証券取引等、オープンなネッ

トワークを活用した新しい金融サービスを提供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展している。このため、金融分野では、暗号技術等を利用した情報セキュリティ対策の実施が喫緊の課題として位置付けられている。

金融機関が情報セキュリティ対策を検討する場合、ＩＳＯやＩＥＣ等の国際標準化団体によって策定された標準規格や技術文書が参考になる。例えば、欧米では、金融業務における情報セキュリティ対策の指針ISO/TR 13569が、金融機関による情報セキュリティ対策に関する有用な資料として利用されている。

最近では、第三者機関による情報セキュリティ製品・システムやその管理・運用体制に対する評価・認定の枠組みが整備されつつある。情報セキュリティ製品やシステムの評価基準ISO/IEC 15408が1999年６月に国際標準化されており、現在、本標準に基づく評価スキームとしてＣＥＭの検討が進められている。

また、情報セキュリティ管理に第三者機関による評価制度を導入した、英国国内の情報セキュリティ対策の指針であるBS 7799は、従来から欧州の金融機関をはじめとして幅広く利用されていたが、1998年には、BS 7799に基づく評価・認定スキームとしてc:cureが発足している。

このように、情報セキュリティに関する指針に加えて、情報セキュリティ製品・システムやその管理・運用体制に対する評価・認定の枠組みが整備されつつある。情報セキュリティ評価・認定のスキームは、企業が情報システムのセキュリティ対策を検討する際の有効な手段であり、今後幅広い分野において利用されるようになると考えられる。金融分野においても、有効なセキュリティ対策の実現に向けて、情報セキュリティ評価・認定のスキームを活用していくことも考えられる。

日本の銀行業における全要素生産性と仲介・決済サービス

大森　徹／中島隆信

本稿では、銀行業の決済機能を単なる為替取引のみではなく、銀行業が預金の受入と貸出を併せて行っていることによって、決済手段としての預金通貨を創造しうるという点が銀行業の決済機能の供給にとって本質的に重要な点であると考え、短期の貸出を決済サービスの一部として取り扱うと定義したうえで、銀行業の固有業務を大きく決済サービスと金融仲介サービスに区分した。次に、95年度の資金量平残ベース（長信行、信託行を除く）で１～10位の銀行から６行、同11～30位から７行、同31～60位から７行を任意に抽出し、この対象行20行の有価証券報告書を利用して、ユーザーコスト・アプローチにより、対象行20行の金融資産・負債の各項目を投入・産出に振り分け、1987～1995年度の両サービス等の生産性とＴＦＰの推移についての特徴点を整理した。そのうえで、金融資産・負債の投入・産出への振分結果をもとに、本稿で定義した決済サービスと金融仲介サービスとの間に何らかの「範囲の経済性」が存在するか、それによって銀行業がどのような便益を得ているのかという点を検討した。その結果は両サービスを併せて供給することによる範囲の経済性は費用節約効果という形で確認されたが、この費用節約効果は銀行業の規模によって変化しており、総資産規模の大きい銀行ほど費用節約率が大きいというものであった。なお、本稿の分析結果を踏まえ、情報技術革新と銀行業との関係やナローバンク論へのインプリケーショ

ンも併せて整理している。

金融と保険の融合について

森本祐司

本稿は、「金融と保険の融合」をキーワードとして、次の３つのトピックについてまとめたサーベイ研究である。

１．ＡＲＴ：実務面における融合の象徴的分野として、保険リスクの証券化などが挙げられる。こうした手法は一般にＡＲＴ（*alternative risk transfer*、代替的リスク移転）と呼ばれており、現在保険・金融双方で関心が高まっている。本稿では、ＡＲＴの定義、分類、商品概要、価格設定の考え方などをまとめる。

２．保険数理と金融工学の融合：理論面、とくに価格理論において融合の萌芽が見え始めている。保険数理と金融工学がこれまでどのような発展経緯を辿り、昨今どのように関連を強めているかについて説明する。

３．ＥＶＴ：リスク管理の高度化、金融リスクと保険リスクの統合管理に向けて、重要な役割を果たす可能性を期待されているＥＶＴ（*extreme value theory*、極値理論）について、基礎的な内容を解説した後、数値例等を示す。

本稿は、上記の各項目ごとに、それぞれ一章ずつを割当てている。これらの内容は、広い意味で密接に関連し合っているものの、本稿ではそれぞれ独立した解説として扱っており、読者の興味・関心に応じて、必要な章に焦点をあてて読むことが可能である。