第4回情報セキュリティ・シンポジウムの模様
―インターネットを利用した金融サービスの情報セキュリティ対策―

1. はじめに

日本銀行金融研究所では、2002年2月28日、「インターネットを利用した金融サービスの情報セキュリティ対策」をテーマとして、第4回情報セキュリティ・シンポジウムを開催した。

今回のシンポジウムは、インターネットを利用した金融サービスが急速に拡大してきていることを踏まえ、こうした形態での金融サービスの提供における情報セキュリティ対策の現状と今後の課題について考えることを企図したものである。

今回のシンポジウムの問題意識は、次のようなものである。すなわち、インターネットを利用した金融サービスは、利用者の利便性を大きく向上させるものであるが、同時に、インターネットという、誰からでも、どこからでも利用可能なオープンなネットワークを利用することに伴い、さまざまな情報セキュリティ上の脅威にさらされている。したがって、こうした形態で提供される金融サービスの円滑な発展を図っていくためには、関連する制度基盤の整備状況や技術面での研究・開発動向を踏まえながら、適切な情報セキュリティ対策を講じていくことが重要であると考えられる。

今回のシンポジウムは、第1部・パネル・ディスカッション、第2部・研究発表の2部構成で進められた後、東京大学・今井秀樹教授による総括コメントで締め括られた（プログラムは、次表のとおり。なお、参加者の肩書きはシンポジウム開催時点のものである）。また、フロアには、暗号学者、行政庁関係者、金融機関や電機メーカーにおける研究開発部門・標準化関連部門の実務家・技術者等、多数の参加を得た。

＜プログラム＞

第1部　パネル・ディスカッション 「インターネット・バンキングにおける情報セキュリティ対策のあり方を巡って」	
	・キーノート・スピーチ：松本勉（横浜国立大学教授）
	・導入報告①：高木浩光（独立行政法人産業技術総合研究所主任研究員）
	・導入報告②：佐々木良一（東京電機大学教授）
	・導入報告③：小松尚久（早稲田大学教授）
	・自由討議 パネリスト：松本勉、高木浩光、佐々木良一、小松尚久 モデレーター：岩下直行（日本銀行金融研究所研究第2課調査役）
第2部　研究発表	
	・発表①「金融分野におけるPKI：技術的課題と研究・標準化動向」 ：宇根正志（日本銀行金融研究所研究第2課）
	・発表②「RSA署名方式の安全性を巡る研究動向について」 ：齊藤真弓（日本銀行金融研究所研究第2課）
総括コメント：今井秀樹（東京大学教授）	

以下では、プログラムに沿って、パネル・ディスカッション、研究発表および総括コメントの概要を紹介する（文責、日本銀行金融研究所。文中敬称略）。

2. パネル・ディスカッション「インターネット・バンキングにおける情報セキュリティ対策のあり方を巡って」

(1) キーノート・スピーチ（松本）「インターネットを利用した金融サービスの安全性」

松本は、岩下との共同論文[1]に基づき、現在のインターネット・バンキングで用いられている利用者認証の方式の安全性について､以下のような問題提起を行った。

ここ1、2年の間に、インターネット・バンキングの利用者が急速に拡大してきているが、その背景の1つとして、利用者を認証する方式が簡便なものに変更されてきたことがあげられる。従来のインターネット・バンキングでは、SET[2]やSECE[3]といったプロトコルによる比較的厳格な認証方式を用いる金融機関が多かった。こうした方式では、利用者において、専用のソフトウエアをパソコンにインストールしたり、公開鍵証明書を取得してパソコンに組み込んだりするための作業負担が大きく、それがインターネット・バンキングの普及を阻害していた面もあった。しかし、最近では、パソコンにあらかじめ組み込まれている暗号プロトコル（SSL[4]）とパスワードを組み合わせて認証を行う「SSL＋パスワード認証」が主流となっている。SSLは、守秘や認証のためのさまざまな機能を有しているが、「SSL＋パスワード認証」では、SSLはパスワードの盗聴を防ぐための守秘機能のみを担っている。「SSL＋パスワード認証」は、利用者が特別なソフトウエア等の導入作業を行う必要がなく、金融機関にとってもシステム構築や利用者に対するサポート等の負担が軽いというメリットがある。その反面、金融機関側のシステムにおける利用者認証はパスワードのみによって行われるため、インターネット・バンキングのセキュリティ対策として十分なものかどうかという問題がある。インターネット・バンキングを提供する金融機関が最も重視しなければならないセキュリティ対策は、無権限者による成りすましなどの攻撃によって正規の利用者や金融機関自身に損害が生じる事態を回避することにあるが、「SSL＋パスワード認証」だけでは、必ずしも十分な対策とはいえないのではないか。

1 松本 勉・岩下 直行、「インターネットを利用した金融サービスの安全性について」（『金融研究』第21巻別冊第1号、日本銀行金融研究所、2002年6月）を参照。

2 SET（Secure Electronic Transactions）：ビザとマスターカードによって提案された、インターネット上で安全にクレジットカード決済を実施するための通信プロトコル。

3 SECE（Secure Electronic Commerce Environment）：インターネット上で安全に金融機関口座を利用した決済を実施するための通信プロトコル。SETをベースに、富士通、日立製作所、日本電気によって共同開発された。

4 SSL（Secure Socket Layer）：ネットスケープ社が提唱した暗号通信、認証等のセキュリティ機能を持つ通信プロトコル。

暗証番号やパスワードによる認証に対しては、考えられるすべての番号を試してみるとか、パスワードによく使われる単語を辞書から選び次々に試してみるといった、基本的な攻撃法が存在する。従来、金融機関の店舗内で金融サービスを提供する場合においては、金融機関職員や防犯カメラによる監視等が可能であるため、そうした攻撃は脅威と認識されることがなかった。しかし、インターネットを利用して金融サービスを提供する場合は、①世界中どの端末からでもアクセスが可能なため不正行為の監視が難しい、②コンピュータに指示して大量の試行を繰り返させることができるなどの理由から、そうした攻撃が現実的な脅威となる。金融機関側のシステムで、パスワード相違の認証エラーが一定回数を超えたら入力を制限するといった防御機構が採用されている場合でも、さまざまなIDとパスワードをランダムに組み合わせて大量の試行を行えば、そうした防御機構を回避してIDとパスワードの組み合わせを推定できてしまう可能性がある。

こうした問題に対処するため、最近のインターネット・バンキングでは、認証手段を二重化し、ログイン用のパスワードに加えて、特に重要な取引に関する操作については「乱数表[5]によるチャレンジ・レスポンス方式」による認証を導入している先が多い。この認証方式は、各金融機関があらかじめ利用者ごとに配付しておいた乱数表の中の位置をランダムに質問し、その位置に記された数値を応答させる手法である。この方式では、ある取引の認証における質問と利用者の入力情報が何らかの理由で漏洩してしまい、認証データが攻撃者に察知されたとしても、他の取引の認証における質問が漏洩した質問とたまたま一致する確率は低いため、攻撃者による成りすましが困難となる、という効果が期待されている。しかし、もしも金融機関側のシステムにおいて、攻撃者が取引入力のキャンセルを繰り返すことによって、自分にとって都合のよい質問が出るまで「質問の出させ直し」を行うことが可能な仕組みとなっていた場合、ある取引における認証データが漏洩しただけで攻撃が可能となり、乱数表導入のメリットが活かされない。また、攻撃対象者を次々に変更しながら当てずっぽうの入力を繰り返す攻撃により、認証エラーが一定回数を超えたら入力を制限するという防御機構を回避して、乱数表の一部のデータを推定できてしまう可能性もある。このため、少なくとも、固定パスワードに加えて乱数表によるチャレンジ･レスポンス方式を導入するだけでは、利用者認証の安全性が著しく高まると評価することはできないと思われる。

このように、現在のインターネット・バンキングにおける認証方式には、セキュリティ侵害のリスクが存在するため、金融機関は、システムを運用していく際に十分留意していく必要がある。こうしたリスクは、現時点ではさほど深刻な問題とはいえないものの、将来、インターネット・バンキングがより広範に利用されるようになると、実際の被害につながりかねないものと思われる。わが国の金融機関が、

5 ここでの「乱数表」とは、利用者ごとに異なるランダムな数値の表が記載された名刺大のカードのことであり、インターネット・バンキングの取引開始前に、金融機関から利用者宛に郵送される。金融機関では、これを「IDカード」、「お客様カード」、「ご契約カード」、「確認番号表」等と呼称している。

今後、インターネットによる金融サービスを拡大していくためには、成りすまし等を有効に防止するためのセキュリティ対策について、適切に対処していくことが必要であろう。

(2) 導入報告①（高木）「インターネット・バンキングに迫り来る現実的脅威」

高木は、既往発表論文[6]の概要を紹介する形で、金融機関のインターネット・バンキングに関連したセキュリティ・ホール（セキュリティ上の脆弱性）について、以下のような指摘を行った。

インターネット・バンキングのシステムは、金融機関のウエブ・サーバー上に構築されている。こうしたウエブ・サーバーを動かしているプログラムの中には、さまざまな既知のセキュリティ・ホールが存在しており、これを放置すると、個人情報が漏洩してしまったり、成りすましを許してしまったりするおそれがある。

こうしたセキュリティ・ホールの1つであり、実際に多くの金融機関のウエブ・サーバーで存在が確認されているものとして、クロスサイト・スクリプティングと呼ばれる攻撃法に対する弱点（クロスサイト・スクリプティング脆弱性）があげられる。クロスサイト・スクリプティングとは、攻撃者が攻撃対象のクライアントのブラウザーにジャバ・スクリプトなどのスクリプト言語で書かれたプログラムを実行させ、当該クライアントがアクセスする他のサイトのウエブ・サーバーから当該クライアントに関する情報を、クライアントのブラウザーを経由して攻撃者へ転送させる攻撃法のことであり、2000年2月に判明したものである。この攻撃が行われた場合、①クッキー[7]の情報を奪取され、セッションをハイジャックされる、②金融機関のウエブ・ページに偽の入力欄が設置され、利用者が入力した個人情報等を別のウエブ・サイトに送信される、という2つの脅威が発生しうる。昨年7月時点の調査では、わが国の金融機関のウエブ・サイト22のうち、8割近い17のサイトが、クロスサイト・スクリプティング脆弱性を有しているとの結果を得た。インターネット・バンキングにおいてクッキーをクライアントの識別のために利用している場合、クロスサイト・スクリプティング攻撃によってクッキーの情報を奪取され、セッションがハイジャックされてしまうと、攻撃者が利用者本人に成りすまして、預金残高、入出金明細等の個人情報を盗み見たり、ログイン用パスワードを勝手に書き換えたりすることができてしまう可能性がある。すべてのサイトがクッキーを用いてセッションを管理しているわけではなく、また、この攻撃を成功させるためには、利用者を罠にかけ、利用者のブラウザーに不正なプログラムを実行させる必

6 2001年10月に情報処理学会コンピュータセキュリティシンポジウムで発表された「クロスサイト・スクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策」、および2001 年9月に情報処理学会全国大会で発表された「IT コマースの脆弱な現実と危機回避に向けた展望」。

7 クッキー（cookie）：ウエブ・サーバーがクライアントを識別し、過去のアクセス履歴等を把握するためにブラウザーに送るデータ。

要があるとはいえ、実際に金融サービスを提供しているウエブ・サーバーにおいてこうした問題が存在することは、あまり望ましい状態ではない。

このようなセキュリティ・ホールは、ウエブ・サーバー用プログラムのバージョンが古いとか、エラー表示用の画面が適切に設計されていないといったことが原因で発生する。そこで、金融機関がインターネット・バンキングに使用しているウエブ・サーバー用プログラムのバージョンを調査してみると、昨年7月の時点では、調査対象の金融機関の過半が、このセキュリティ・ホールのある古いバージョンのプログラムを利用していた。その後、2001年10月に、情報処理振興事業協会・セキュリティセンターが国内の電子商取引用サイトの運営者等に対して警告を発する文書を公開したこともあり、本年2月までに、いくつかの金融機関のウエブ・サーバーでは、セキュリティ・ホールのない新しいバージョンのプログラムに変更されたが、2月時点でも古いバージョンのままの金融機関がかなり残っている状態であった。金融機関がインターネット・バンキングに利用するウエブ・サーバー用プログラムは、常に最新のバージョンに更新しておくべきである。

こうしたシステム面の問題以外にも、現在のインターネット・バンキングには、セキュリティを損ないかねない、いくつかの問題が存在する。例えば、一部の金融機関が提供するインターネット・バンキングでは、ログイン時に、強制的にブラウザーの表示設定が「アドレス・バーを表示しない」に変更され、現在接続しているサイトのアドレスが隠されてしまう。ブラウザーを用いてウエブ・サイトに接続する場合、利用者は、自分が確かに意図したサイトに接続しているかどうかをアドレス・バーで確認することができるが、これらの金融機関のサイトに接続した場合、その確認ができないため、「偽ウィンドウによる攻撃」に対して脆弱になってしまう。この攻撃は、攻撃者が利用者を罠にかけて、利用者のパソコンの画面上に当該金融機関のウエブ・ページに似せた偽ウィンドウを開かせ、そこから入力させたパスワード等を攻撃者のサイトに転送させて情報を奪取するものである。普段からアドレス・バーが表示される設定となっていれば、利用者は表示されたアドレスを確認することでウィンドウが本物か偽者かを判断することができる。しかし、これらの金融機関は、常にアドレス・バーを隠すことによって、利用者がアドレスを確認しないように習慣付けてしまっていることになる。さらに、一部の金融機関のインターネット・バンキングにおいては、利用者がアドレス・バー以外の方法（マウス・ボタンを右クリックし、ページの属性情報を表示させる等）によりアドレスを確認しようとしても、そのための操作がシステム的に禁止されてしまっている。

このように、現在のインターネット・バンキングのシステムを、ウエブ・アプリケーションの安全性という観点から評価すると、十分な対策が講じられているとは言い難い面がある。こうした問題を回避するためには、現場でシステム開発に携わる技術者が、ウエブ・アプリケーションのセキュリティに関する正しい知識を持ち、システム、運用の両面について、安全性を高めるための対策を進めていくことが必要であろう。

（3）導入報告②（佐々木）「社会基盤としてのデジタル署名の安全性」

佐々木は、インターネット等を利用した電子的な金融取引の安全性を高めるうえで、デジタル署名の導入が有力な手段であること、その場合、デジタル署名の長期的な有効性の維持が問題となることについて、以下のとおり説明した。

インターネット等を利用した電子的な金融取引においては、成りすましの防止に加えて、事後的な取引否認を防止することが大切であり、デジタル署名は、そのための有力な手段である。電子的な金融取引の証跡となる電子文書にデジタル署名を付与すれば、事後的な改ざんを検知することができる。しかし、ある程度長期間にわたってその機能を利用しようとすると、公開鍵暗号技術に基づくデジタル署名に固有の問題が発生する。紙の文書に押印した場合は、時間が経ったからといって押印の有効性が低下することはないが、デジタル署名が付与された電子文書の場合、利用された公開鍵暗号技術が破られてしまうと、通常のデジタル署名では、改ざんを有効に検知することができなくなってしまうのである。

例えば、RSAデジタル署名方式の場合、公開鍵を素因数分解することができれば、秘密鍵を推定し、デジタル署名を偽造することができる。素因数分解が可能な公開鍵のサイズは、コンピュータのコスト・パフォーマンスと素因数分解アルゴリズムの進歩に応じて変化するため、デジタル署名が付与された電子文書は、時間が経つにつれて徐々に改ざんに対して脆弱化する。また、仮に、量子コンピュータのような新しい計算機の実用化や数学上の新発見の結果、デジタル署名方式を支える理論が破綻してしまった場合、その方式に基づくデジタル署名がすべて有効でなくなってしまうといった事態も発生しうる。

デジタル署名を長期にわたって使い続けていくためには、万一、破局的な事態が生じたとしても、デジタル署名が一定の証拠能力を維持できるよう、あらかじめ対策を講じておくべきである。こうした発想から、「ヒステリシス署名」と呼ばれる技術が提案されている。この技術は、デジタル署名を生成する際に、直前に生成された自分や他人の署名を署名対象データに追加して署名生成履歴の連鎖を作り、その情報を安全に保管しておくことによって、デジタル署名の有効性をできる限り持続させようとする構想である。すなわち、この方式をとった場合、仮にある時点でデジタル署名の基礎をなす公開鍵暗号技術が破られたとしても、その時点以前の署名生成履歴の連鎖まで偽造することは困難であるので、その時点以前の署名の証拠能力は失われないこととなる。

今後、デジタル署名を社会基盤として有効に活用していくためには、こうした破局的な事態への対応について、周到な準備をしておく必要があろう。また、デジタル署名が付与された電子文書の有効期間の考え方などについて、利用者の間で共通の認識が形成されることも必要と考えられる。これらの対策については、技術者のみならず、法律家、実務家が相互に協力して総合的に検討していく必要があるのではないか。

（4）導入報告③（小松）「バイオメトリクス個人認証技術とその課題」

小松は、インターネット等を利用した電子的な金融取引において活用することが期待される技術の一例として、バイオメトリクス個人認証技術について、以下のとおり説明した。

インターネット等を利用した電子的な金融取引において、端末で利用者の本人認証を行う際に利用しうるデータは、①本人の所有物、②本人の知識、③本人固有の特徴の3つに分類することができる。「本人の所有物」とは、IDカードのように、正当な本人しか持ち得ないはずの物を提示させることにより認証する方法である。「本人の知識」とは、暗証番号やパスワード等、正当な本人しか知らないはずの情報を提示させることにより認証する方法である。そして、「本人固有の特徴」とは、指紋、虹彩、音声、筆跡等を計測し、正当な本人固有の特徴と合致するかどうかを確認することによって認証する方法である。この最後の方法を、「バイオメトリクス個人認証」といい、既にこれを利用したさまざまな製品が開発、実用化されている。

これまで、インターネット・バンキングへのログイン等の利用者認証においてデータとして用いられてきたのは、主に「本人の知識」である暗証番号やパスワードであった。暗証番号等を利用者が自由に設定できる場合、安全性よりも覚えやすさを優先してしまい、容易に推定される値を選んでしまうというリスクが指摘されている。例えば、キャッシュ・カードの暗証番号について、6割以上の利用者が、誕生日もしくは電話番号をそのまま当てはめているといった調査結果もある。パスワードや暗証番号による認証は、こうした個人情報から容易に推定されてしまったり、うっかり他人に漏らしてしまったりするリスクが高いという意味でも、オープンなネットワーク上で金融取引を行うための認証手段としては、十分に安全とはいえない。このため、利用者本人に固有の身体的特徴（指紋、虹彩等）や身体的特性（音声、筆跡等）を利用して本人認証を行うバイオメトリクス個人認証が注目を集めている。

現在のところ、バイオメトリクス個人認証は、コンピュータ・ルームの入退室管理など、特に高度なセキュリティが要請される環境において、物理的な鍵の代りに利用されることが多い。しかし、今後は、インターネットを利用した金融取引における利用者認証や、ICカードを利用する局面での本人確認などに活用されるようになるものと考えられる。ただし、バイオメトリクス個人認証も、完全無欠な認証手段であるわけではない。情報セキュリティ対策は、総合的な取り組みが必要であり、例えば、バイオメトリクス個人認証をパスワードや暗証番号と組み合わせて用いることが考えられる。そうすれば、利用者に過度の負担をかけることなく、少なくとも既存の認証方式よりも高い安心感を利用者に与えることができるものと思う。

（5）自由討議、質疑応答

上記のキーノート・スピーチおよび導入報告を受けて、パネリストによる自由討議、およびフロアとの間での質疑応答が行われた。

松本は、自らのキーノート・スピーチや高木の導入報告を踏まえると、金融機関が提供するインターネット・バンキングの情報セキュリティ対策の現状には改善を要する部分があり、早急な対応が必要ではないか、と述べた。同時に、インターネット・バンキングにどのような脅威が存在するかについて、利用者が正確に把握できるよう、適切に情報を公開していくことが必要であると主張した。**高木**は、システムの安全性というと、要素技術である暗号技術等に焦点が当てられることが多いが、もっと単純な部分に多くのセキュリティ・ホールが存在することに留意する必要があると指摘した。そして、インターネット・バンキング等の安全性を高めるためには、システム開発段階で欠陥を作り込まないようにすることが必要であり、システム開発者がセキュリティ・ホールに関する情報を共有することが有効ではないかと述べた。

これに関連して、**松本**は、本席で紹介された攻撃法の中には、インターネットのアンダーグラウンド向け掲示板などではよく知られているものも多いとしたうえで、こうした情報を、より一般的なルートで技術者たちが共有できる枠組みを整備していくことが必要だと主張した。**高木**もこれに同調し、セキュリティ・ホールに関する情報を隠すと、一般の開発者はセキュリティ・ホールの存在を知らずにシステムを構築してしまう一方、アンダーグラウンドでは情報が共有されてしまうので、むしろ攻撃に対して脆弱になってしまうことを指摘した。

こうした議論を受けて、**フロア参加者**からは、セキュリティ・ホールに関する情報の共有を具体的にどのように行うべきか、学会等での研究発表だけでは情報共有者の範囲が限定されてしまうため、より強い影響力を持ちうる情報開示の枠組みが必要ではないかといった点について、質問が寄せられた。

これに対し、**佐々木**は、米国においては、国の機関がセキュリティ・ホールに関する情報共有に積極的に貢献しているとともに、例えば金融機関同士によるコミュニティでも情報セキュリティに関する情報交換が行われていること等を紹介し、わが国でも、類似の仕組みを作っていく必要があるのではないかと述べた。**松本**は、前回の本シンポジウムで、情報セキュリティの脆弱性が発見されたときに適切な報告が行われるようにするための仕組みとして「届出機関」の構想を提言したことに触れ、インターネットの利用拡大に伴い、ますますそうした体制整備の必要性が高まってきていると述べた。

また、**高木**は、インターネット・バンキング等のセキュリティについて、仮にウエブ・サーバー側に問題がなくても、クライアント側のブラウザーにセキュリティ・ホールが存在すれば、情報漏洩等が発生する可能性があることを指摘し、セキュリティ・ホールが発見された場合、一般利用者の側でも、バージョン・アップや修正プログラムの適用等の適切な対応をとることが必要であると指摘した。

これに対し、**フロア参加者**から、ブラウザーのバージョン・アップや修正プログラムの適用が利用者の責任とされるとなると、技術的な弱者ほどトラブルに巻き込まれやすいということになってしまうが、これに関する救済策を考える必要があるのではないかという質問が寄せられた。**高木**は、ブラウザーを提供しているメーカーや、パソコンを販売しているメーカーは、ブラウザーにセキュリティ・ホールがあったとしても、上位バージョンや修正プログラムを提供することまでを自分たちの責任領域としており、残念ながら、個々のユーザーに積極的に連絡をするといったことはしない立場をとっているのが現状であると思うと述べたうえで、例えば、インターネット・バンキングなどの高い安全性を必要とするサービスを提供している企業が、利用者に対してセキュリティ・ホール等に関する注意喚起を行い、利用者側のセキュリティの向上を働きかけることが考えられると指摘した。

3．研究発表

(1) 発表①（宇根）「金融分野におけるPKI：技術的課題と研究・標準化動向」

宇根は、標題の研究論文[8]に基づき、金融分野におけるPKIの情報セキュリティ対策の現状と今後の課題について、以下のように発表を行った。

イ．PKIとCP／CPS

インターネット・バンキング等の金融サービスでは、交信データの暗号化や利用者の本人確認を行う手段として公開鍵暗号方式が利用されている。公開鍵暗号方式は、暗号化鍵と復号鍵が異なり、復号鍵（秘密鍵）を秘密に管理し、暗号化鍵（公開鍵）を公開する暗号方式である。公開鍵暗号方式を利用する際には、公開鍵の正当な持ち主を特定し、それに対応する秘密鍵が適切に管理されていることを確認する必要がある。PKIは、公開鍵暗号方式を安心して利用可能にするための仕組みであり、具体的には、認証機関（CA：certification authority）と呼ばれる第三者機関が公開鍵の正当な持ち主等を示す公開鍵証明書を発行するとともに、既存の公開鍵証明書の失効情報を提供する、という形態となっている。

PKIにおける情報セキュリティ対策は、公開鍵暗号方式の用途や対象となる取引の性格および利用環境等に依存する。こうした認証業務の基本方針は証明書ポリシー（CP：certificate policy）として規定され、CPに基づいて決定される認証業務の具体的な施策は認証実施規程（CPS：certification practice statement）として規定されるケース

8 宇根正志、「金融分野におけるPKI：技術的課題と研究・標準化動向」（『金融研究』第21巻別冊第1号、日本銀行金融研究所、2002年6月）を参照。

が一般的である。認証機関はCP／CPSを活用することによって、情報セキュリティ対策の体系的な検討が容易となるほか、CP／CPSが公表される場合には、PKIの利用者が認証機関やPKI全体の情報セキュリティ対策を評価することも可能となる。

ロ．金融分野が参画するPKIにおける情報セキュリティ対策

金融機関によるPKIの利用形態をみると、従来は、インターネット・バンキング等における利用者認証を目的として、電子認証サービスを提供する企業が発行した公開鍵証明書を活用するという形態がほとんどであった。これに対し、最近では、ICカード認証や企業間EDIにおける認証等、PKIの用途が多様化しているほか、金融機関自身が認証機関として参画する事例が増えている。こうしたPKIの代表例として、全国銀行協会、アイデントラス、スイフト、TEDI[9]の各PKIが挙げられる。

しかし、これらのPKIにおける情報セキュリティ対策に関する情報は、現時点では必ずしも十分に公表されていないように思われる。CP／CPSについては、アイデントラスのPKIにおいて一部のCPが公表されているだけであるほか、認証業務の中でも特に重要とみられる①認証機関の秘密鍵の管理、②証明書失効情報の管理、③セキュリティ監査・ログ管理についても、公表情報は非常に少ない。例えば、認証機関の秘密鍵の管理に関しては、多くのPKIで耐タンパー性を有するハードウエアを用いる旨は公表されているものの、秘密鍵の使用・廃棄方法や、秘密鍵が漏洩した場合の対処方法等については公表されていないようである。

ハ．PKI構築に向けての今後の課題と対応策

こうした現状を踏まえると、今後、金融機関が認証機関としてPKIの運営に参画するに際しては、認証業務に必要な情報セキュリティ対策を適切に講じたうえで、これを利用者に効果的に示していくことが最も重要な課題であると考えられる。本課題への具体的な対応策として、次の2つが有用と考えられる。

第1に、PKIのシステム構築時に情報セキュリティ技術を適切に選択し、その内容を反映したCP／CPSを作成したうえで、情報セキュリティを損なわない範囲でCP／CPSの内容を開示することである。情報セキュリティ対策の選択にあたっては、ISOの国際標準等を参考としながら、専門家による十分な評価を得た技術を採用することが望ましい。CP／CPSの作成にあたっては、2001年に標準化が完了した米国国内標準ANS X9.79-1が参考になる。また、これらの対応に関連して、第三者機関による評価・認定を受けた情報セキュリティ製品・システムを採用し、その旨を開示していくことも考えられる。例えば、こうした製品・システムの評価基準であるISO 15408に基づく評価・認定の活用が考えられる。

9 TEDI（Trade EDI）：貿易取引に関連する各種手続に用いられる書類を電子化し、ネットワーク経由で安全かつ迅速に授受できるようにすることを目的として、通商産業省（現経済産業省）の支援のもとで1998年に開始されたプロジェクト。

第2に、PKIのサービス開始後に認証業務が適切に運用・管理されていることを第三者によるセキュリティ監査によって確認し、その結果を開示することである。セキュリティ監査の結果の開示は、認証業務の運用・管理の適正さに対する利用者の信頼を向上させるほか、認証機関の職員や関係者に対して適切な行動を促すことにもつながると考えられる。また、これらの対応に関連して、「電子署名及び認証業務に関する法律」に基づく特定認証業務の認定制度を利用して、認証業務の運用・管理体制が一定基準を満たしていることに関する認定を受けることも考えられる。

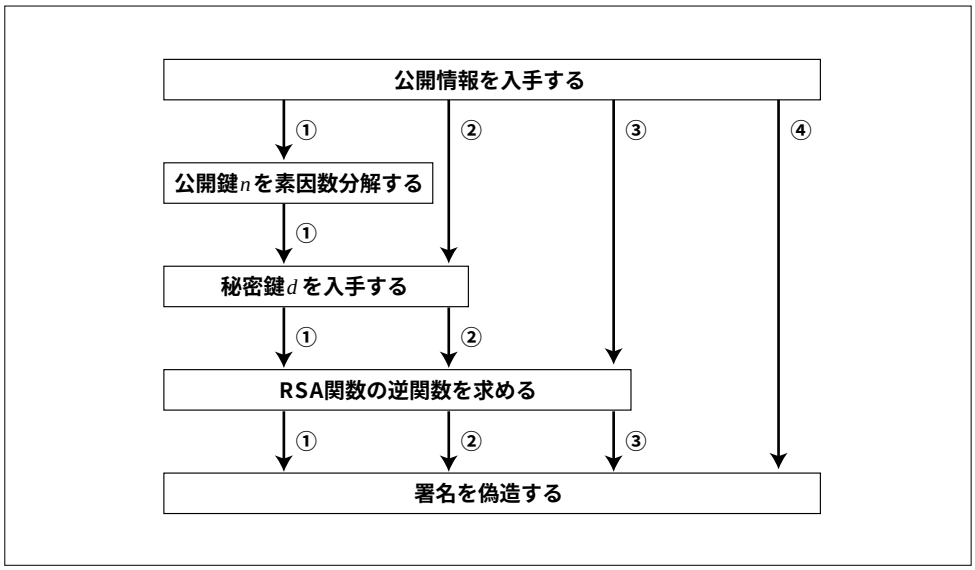
(2) 発表②（齊藤）「RSA署名方式の安全性を巡る研究動向について」

齊藤は、標題論文[10]に基づき、RSA署名方式の安全性を巡る研究動向について、以下のように発表を行った。

イ．RSA署名方式の安全性を評価する枠組み

RSA署名方式の安全性について説明する場合、「RSA署名方式の安全性は、素因数分解問題の困難性に依拠している」といった表現が用いられることが多い。しかし、この表現は必ずしも正確ではない。RSA署名方式の安全性を正確に理解するために、どのようなルートで署名の偽造が行われるか、整理してみよう。

図　署名を偽造する4つのルート



10　齊藤真弓、「RSA署名方式の安全性を巡る研究動向について」（『金融研究』第21巻別冊第1号、日本銀行金融研究所、2002年6月）を参照。

通常想定されるルートとして、公開鍵nを素因数分解して秘密鍵dを求め、RSA関数の逆関数を導出し、署名を偽造する、ということが考えられる（図の①）。しかし、偽造が目的であるならば、nの素因数分解を行うことなく秘密鍵dを推定し、それを用いてRSA関数の逆関数を導出し、最終的に署名の偽造を行うルート（図の②）、秘密鍵dを求めることなく、RSA関数の逆関数を導出し、それを用いて署名の偽造を行うルート（図の③）、およびRSA関数の逆関数を導出することなく、署名の偽造を行うルート（図の④）も想定することが可能である。このうち、②や③のルートについては、RSA暗号／署名方式が考案されて以来、さまざまな研究が行われてきたが、これまでのところ、このような攻撃が成功したという事例は報告されておらず、現在では、これらのルートによる有効な攻撃法は存在しないと想定することが多い。しかし、④のルートを用いた署名の偽造は実際に存在することが知られている。その意味で、素因数分解の困難性を仮定しただけでは、RSA署名方式が無条件で安全ということにはならない。

ロ．公開鍵nを素因数分解するルート

最もオーソドックスな「公開鍵nを素因数分解するルート」では、素因数分解の困難性が問題となる。一般に、合成数nを素因数分解することは原理的には可能であるが、nの桁数が非常に大きい場合、実際に素因数pとqを導出することは計算量的に困難となる。したがって、どの程度の桁数のnであれば素因数分解が計算量的に困難となるのかがポイントであり、より高速な素因数分解アルゴリズムの研究や、十分な安全性を確保するために必要な鍵長に関する研究が進められてきた。この結果、現時点での最高速の素因数分解アルゴリズムである数体ふるい法を前提として、商用でRSA署名方式を用いる場合には、公開鍵のサイズを1,024 bit以上に設定することが推奨されるケースが多い。

ハ．RSA関数の逆関数を導出することなく署名偽造を行うルート

これに対し、「RSA関数の逆関数を導出することなく署名偽造を行うルート」については、RSA署名方式の乗法性を利用した攻撃が存在するため、メッセージをそのまま署名変換データとして利用するのではなく、パディング[11]やハッシュ関数[12]を利用してメッセージを変換することにより署名変換データを作成する方式が提案されてきた。しかし、パディングだけでメッセージを変換する方式に対しては、いくつかの有効な攻撃法が存在しており、安全性は保てないことが知られている。また、ハッシュ関数のみを利用する方式についても、有効な攻撃法が発見されている。

11 パディング（padding）：通信メッセージを一定の長さのデータ（ここでは、署名変換データ）に拡張する方法の1つであり、その通信メッセージの前や後に別のデータ（例えば「0」）を付加することをいう。

12 ハッシュ関数（hash function）：与えられた任意のデータから固定長の疑似乱数を生成する関数であり、生成された疑似乱数から入力データを求めることが困難であるという性質をもつ。

このため、現在では、パディングとハッシュ関数の両方を用いた方法が主流となっている。しかし、ISO 9796-2に規定された署名方式のように、パディングとハッシュ関数の両方を用いたとしても有効な攻撃法が存在する場合があるので、注意が必要である。現在最も広く普及しているのは、PKCS#1 Ver.1.5署名方式であり、この方式には、今のところ有効な攻撃法は発見されていない。ただし、同方式については、数学的に安全性の証明が可能であることが示されているわけではない。このため、最近では、一定の仮定のもとで数学的に安全性の証明が可能であることが示されている、RSA-PSS署名方式が注目されている。

ニ．RSA-PSS署名方式

RSA-PSS署名方式は、1996年にベラーレとロガウェイによって提案されたものであり、パディングとハッシュ関数を組み合わせることによって安全性を向上させている。RSA-PSS署名方式の特徴は、「一定の仮定のもとで、数学的に安全性を証明することが可能である」という証明可能安全性と、通常のRSA署名方式と同程度の実用性を兼ね備えている点である。今後、幅広い分野においてRSA-PSS署名方式が利用されるようになることも考えられる。

4．総括コメント

今井は、総括コメントとして、前記のパネル・ディスカッションや研究発表の内容を簡単に整理し、それらの意義を高く評価したうえで、次のような指摘を行い、今回のシンポジウムを締め括った。

今回のシンポジウムは、前回までに比べると、実際の金融機関の業務に直結したトピックスが多かった。これは、インターネットが金融機関による金融サービス提供の有力なチャネルとして活用されるようになり、情報セキュリティ技術が金融業務の最前線で活用されるようになってきたことを反映したものであろう。本日の議論でも明らかになったように、インターネットを利用した金融サービスはまだ黎明期にあり、どのような情報セキュリティ技術を選択するかについても、試行錯誤が繰り返されているようである。導入のしやすさやコストといったビジネス上の要請があることは理解できるが、安全性、信頼性に関する議論がまだ十分には行われていない面があるように思われた。

従来、わが国の金融業界では、情報ネットワークを外部から遮断することによって情報セキュリティを確保しようとすることが多かったものと理解している。そうした場合、利用する技術に関する情報はあまり公開されず、また、それで特に問題はなかった。しかし、インターネットというオープンなネットワークを利用して金融サービスを提供する場合には、セキュリティを確保するための枠組みも大きく変わらざるを得ない。こうした形態での金融サービスの提供における情報セキュリティ対策を考えていくに当っては、極力オープンな場で、システムの提供者、利

用者、そして研究者が情報を共有し合いながら、情報セキュリティ技術の安全性について、さまざまな角度から評価を行い、その結果について議論していくことが重要であろう。

今回のシンポジウムにおいて行われたパネル・ディスカッションや研究発表も、そうした問題意識に基づいたものであると理解している。今回のシンポジウムが、金融分野のシステム構築等にかかわる方々にとって、情報セキュリティ対策を巡るさまざまな問題への認識を深める契機となり、今後、その対応策について活発な議論がなされていくことを期待したい。