第8回情報セキュリティ・シンポジウム「金融機関の情報セキュリティ対策のあり方」の模様

１．はじめに

金融研究所は、平成18年3月28日、「金融機関の情報セキュリティ対策のあり方」をテーマとして、第8回情報セキュリティ・シンポジウムを開催した。

情報セキュリティの問題は、各金融機関の経営の根幹にかかわる問題であり、社会的責任やレピュテーション・リスクを考慮して適切に判断、対応していかなければならない。しかし、金融業務に関連する情報システムの高度化・複雑化、情報セキュリティ対策の技術的な難解さ等を背景に、どのレベルまで対策を実施すべきかを正確に見極めることが難しいのが実情である。

こうしたことから、今回のシンポジウムは、金融分野における情報セキュリティの問題について、いくつかの具体的なテーマに即して、情報技術的な観点からどのような対応が望ましいと考えられるかについての判断材料を提供することを目的として開催した。まず、キーノート・スピーチにおいて偽造カード問題とインターネット・バンキングにおける脆弱性を例に、金融機関の情報セキュリティ対策のあり方について問題提起を行った。そのうえで、金融分野における利用者認証、暗号技術の2010年問題、ICカードを利用したシステムの安全性に関する発表をそれぞれ行った。次に、パネル・ディスカッションにおいて情報セキュリティ対策を研究レベルから実践レベルへ移行していく必要性について議論した後、総括コメントを行った（プログラムは次頁のとおり）。

フロアには、金融業務における情報セキュリティ対策を担当している金融機関関係者のほか、暗号学者、情報セキュリティ技術に関係の深い官庁関係者、電機メーカーの研究開発部門・標準化部門の実務家や技術者約100名の参加を得た。

●**キーノート・スピーチ**「金融機関の情報セキュリティ対策のあり方について」
― 岩下直行（日本銀行金融研究所情報技術研究センター長）
●**発表1**「利用者認証技術のセキュリティにつき改めて考える」
― 松本 勉（横浜国立大学教授）
●**発表2**「暗号アルゴリズムの2010年問題について」
― 宇根正志（日本銀行金融研究所情報技術研究センター）
●**発表3**「金融分野におけるICカード・システムのセキュリティについて」
― 田村裕子（日本銀行金融研究所情報技術研究センター）
●**パネル・ディスカッション**「金融機関の情報セキュリティ対策のあり方：研究から実践へ」
・**パネル発表1**「最近の情報セキュリティの現状」
― 三角育生（情報処理推進機構セキュリティセンター長）
・**パネル発表2**「CSIRTとJPCERT/CC」
― 歌代和正（JPCERTコーディネーションセンター代表理事）
・**自由討議**「金融機関の情報セキュリティ対策のあり方」
― モデレータ：岩下直行
― パネリスト：松本 勉、三角育生、歌代和正
●**総括コメント** ― 今井秀樹（東京大学教授・産業技術総合研究所情報セキュリティ研究センター長）

（備考：所属についてはシンポジウム当日現在のもの）

以下では、プログラムに沿って、本シンポジウムの概要を紹介する（以下、敬称略。文責：日本銀行金融研究所）。

2．キーノート・スピーチ「金融機関の情報セキュリティ対策のあり方について」

岩下は、標記論文[1]に基づき、金融機関の情報セキュリティ対策のあり方について、次のとおり問題提起を行った。

1 岩下直行、「金融機関の情報セキュリティ対策のあり方について」、本号所収。

（1）金融機関は情報セキュリティ対策をどこまで充実させるべきか

金融業界では、偽造カードによる不正預金引出、スパイウエアによる個人情報の漏洩、インターネット・バンキングでの不正送金等、金融機関の情報システムに対する信任を脅かす事件が次々に発生し、利用者は不安をつのらせている。金融機関には、利用者の信頼をつなぎとめていくために、こうした脅威に対処するための情報セキュリティ対策を一段と充実させることが求められている。

（2）偽造カード問題の経緯とそのセキュリティ対策の現状

2006年2月に施行された「偽造・盗難カード預貯金者保護法」により、金融機関には、被害の補償に加え、偽造カード犯罪の事前予防策として、利用者認証の安全性強化を行うこと等が義務付けられることとなった。現在、一部の金融機関は、キャッシュカードのICカード化、ATMにおける生体認証の導入等を進めている。しかし、実際にこうした対策を採用した金融機関は限られているほか、ICカード化を行った金融機関の中には、利用者の利便性を維持するために、ICカードに磁気ストライプを併用する先が多い。その場合、磁気ストライプ部分のみであれば偽造することが容易であるため、偽造カード犯罪の事前予防策としての有効性はあまり期待できない。

この間、金融機関は、ATMでの預金引出限度額の引下げと、異常取引の検知を行うことにより、偽造カードによる被害の拡大に対処しようとしてきた。こうした対策が適切に講じられていれば、偽造カードが使用された場合でも被害額を限定できるという意味で、実戦的な意味は大きいと思われる。しかし、これらの緊急対応が、偽造カード問題への対策における最終的な到達点とは考えにくい。その次のステップとして、磁気ストライプを併用しないICカードの導入や生体認証の導入等により、セキュリティ・レベルを抜本的に向上させることが必要となろう。ただし、その場合には、新たに採用する本人認証方式の安全性を厳密に評価する必要がある。

（3）インターネット・バンキングのセキュリティを巡って

現在のインターネット・バンキングは、パソコンにあらかじめ組み込まれている暗号通信プロトコル（SSL）と、利用者が記憶しているパスワードを組み合わせて認証を行う方式を採用している。さらに、ログイン用のパスワードに加えて、乱数表によるチャレンジ・レスポンス方式による認証を導入したものも多い。しかし、SSLとパスワードによる認証や乱数表によるチャレンジ・レスポンス方式においても、なりすましを可能とする攻撃の存在が指摘されていることから、一部の金融機

関においては、ワンタイム・パスワード生成機[2]を利用者に配付し、認証に用いる動きも出始めている。

インターネット・バンキング用のシステムは、①ウェブサイトのプログラムの中身が公開されており、システムの仕組みを外部から解析可能であること、②金融機関が利用者のパソコン管理を徹底できないこと、③不特定多数の相手から攻撃を受けるリスクがあることから、伝統的な金融機関の情報システムとは大きく異なる性格を持っており、金融機関は、従来のシステム開発の発想を切り替える必要がある。具体的には、外部の専門家によって指摘された具体的な問題点を解決していくとともに、積極的に情報を開示し、対策を進めていることをアピールしていくことが重要である。また、利用者のITリテラシーの向上を企図した啓発活動に取り組むことも必要である。

(4) 金融機関のセキュリティに対する信頼をつなぎとめるために

現時点において顕現化しているリテール金融取引を対象とした攻撃は、その被害金額の規模からみると、各金融機関の経営を揺るがすような問題にはなっていないが、将来ホールセール分野にまで波及するリスクを考えた場合、被害金額が増大する可能性がある。そのため、現時点の被害金額の範囲内で対策費用を賄うというアプローチでは、過少な投資で良いと誤って判断してしまう可能性がある。こうした点にも留意したうえで、金融機関は、情報セキュリティ上の要請と自らのビジネスとに折り合いをつけながら、その時点で採用すべき適切なセキュリティ対策を選択していく必要がある。

偽造カードやインターネット・バンキングの脆弱性のような、広く一般の注目を集めた問題以外にも、取り組むべき問題は少なくない。例えば、①ATM・センター間のPINの暗号化が必須となっていないこと、②現在金融業務において広く使われている暗号アルゴリズムはあと5年足らずで安全性の保証が切れる見込みであること、③生体認証で利用される装置の技術仕様が公開されていないため、安全性の評価が難しいこと等が挙げられる。

こうした問題に適切に対処するためには、各金融機関は、まず、各種対策の有効性について情報を収集し、知見を深めていくことが必要である。また、業界全体として取り組んでいかなければ実効性の得られない対策も多いことを考えると、業界団体や規制当局が、業界内での情報共有を進めるための枠組みを提供していくことも重要な課題である。

2 1回しか使えない「使い捨てパスワード」を生成するセキュリティ・トークン。現在の時刻や取引1件ごとに増加するカウンタ値等を基に、共通鍵暗号アルゴリズムの演算を行うことによって、取引の都度、1度限りしか使えないパスワードが生成され、かつ、送受信される情報から共通鍵暗号の鍵を推定することが計算量的に困難となるような設計がなされている。

３．発表1「利用者認証技術のセキュリティにつき改めて考える」

松本は、利用者認証方式の特徴やその安全性評価方法について、以下のとおり発表を行った。

（1）利用者認証技術の特徴

金融分野においては、金融取引や入退室管理等さまざまな場面で利用者認証が行われている。利用者認証とは、利用者が「本人」（主張した身元に対応する人物）であることを確認することであり、①利用者が記憶している情報、②利用者が所持しているもの、③利用者の身体的特徴や行動的特徴を利用して行われるほか、これらの組合せによって行われることも多い。

まず、記憶している情報を利用した認証方式については、PINやパスワード等を利用するものが例として挙げられる。こうした方式は、特別な読取装置を必要とせず、比較的実装が容易であることから、現在広く普及している。

しかし、①利用者が情報を忘れてしまった場合には、利用者認証として有効に機能しないこととなるほか、②第三者による情報の覗き見、③認証者へのなりすましによる情報の盗取（フィッシング）、④脅迫による情報の盗取、⑤利用者自身による情報の横流し等の攻撃に注意が必要である。

続いて、所持物を利用した認証方式の具体例としては、身分証明書、パスポート、磁気ストライプ・カード、ICカード等を用いるものが挙げられる。認証時には所持物を提示するのみでよく、利用者に求められる操作が容易であることから、こちらも現在広く利用されている。利用者に配付する所持物については、偽造が困難であるよう適切に作製することでなりすましを防止することができる。また、所持物にプロセッサを搭載することで、暗号技術に基づく高度な認証処理を利用可能であるという特徴がある。

ただし、①所持物の紛失・盗難が発生した場合には、利用者認証として有効に機能しない、②各所持物用の読取装置（カード・リーダ等）が必要である、③所持物や読取装置に耐タンパー性が求められる、④暗号技術を利用する場合にはその強度等を確認することが求められる、⑤利用者自身による所持物の横流しが可能であるといった点に注意が必要である。

次に、利用者の身体的・行動的特徴を利用した認証方式（生体認証）は、万人不同かつ生涯不変であるといわれる特徴を利用して行われる認証であり、指紋、虹彩、血管パターンをはじめとするさまざまな特徴を利用する方式が存在する。生体認証は、利用者による記憶や媒体の所持を必要としないというメリットがあるほか、適切に生体認証システムを構築できれば、身体的特徴等の偽造や横流しを困難にすることができると考えられる。

ただし、①身体的特徴等の情報（生体情報）の読取装置が必要であるほか、②生体情報の読取装置に耐タンパー性が求められる、③偽の読取装置の設置によって生

体情報が盗取（フィッシング）されるおそれがあるといった点について注意が必要である。また、④環境等の影響によって常に同じ生体情報を採取することが難しく、本人拒否や登録失敗が発生してしまう、⑤生体情報の無効化が困難である、⑥生体情報は機微な個人情報であることから、情報の管理を厳格に行う必要があるといった点にも十分な注意が求められる。このほか、⑦生体情報の採取が利用者に対して心理的抵抗感を与えることもあるといった点にも配慮する必要がある。

（2）利用者認証システムを導入するうえでのポイント

利用者認証を利用するうえでは、認証システムにおいて想定されるあらゆる攻撃を考慮し、対策を講じておく必要がある。こうした対策については、設計や実装方法が適切でなければ、期待されたレベルの効果を発揮しないこととなる。例えば、所持認証等に利用される媒体の偽造に対する耐性を考えたとき、ICカードであっても、実装される認証プロトコルが脆弱な場合等においては、磁気ストライプ・カードと同程度の安全性しか確保できない。そのため、ICカードの持つ技術的可能性を適切に活用できるような設計・実装が求められる。

また、暗号技術を利用する場合には、暗号アルゴリズムそのものの安全性に加えて、暗号モジュールに対する攻撃についても考慮する必要がある。近年注目される攻撃の1つに、暗号モジュールの動作時の漏洩情報を測定し、それらを用いて秘密情報を推定するサイドチャネル攻撃があるが、こうした最新の攻撃についても留意が必要である。そのほか、利用者認証に採用すべき認証技術を決定する際には、認証技術の有する性質を総合的に判断することが求められる。

（3）生体認証システムの安全性について

生体認証の安全性については、生体部分でない対象物の受入可能性に関する考察が重要である。生体認証の装置においては、提示される対象物が生体であるか否かを検知する機能（生体検知機能）が組み込まれるケースもある。しかし、本人拒否や登録失敗ができるだけ少なくなるようパラメータを設定することにより、生体検知が適切に機能しないことも考えられるため、生体検知機能が有効に機能しているか否かを見極めることが重要である。

このような観点から生体認証システムの安全性を評価する手順としては、まず、生体部分でない対象物を提示し、①登録できるか否か、②登録できた場合、再提示して照合できるか否かを調べ、次に、③生体部分でない対象物を登録し、生体部分で照合できるか否か、④生体部分を登録し、生体部分でない対象物で照合できるか否かについて調べることが考えられる。「生体でない対象物」としてさまざまな物体を作製したうえで、上記の4種類の実験を順次行い、生体部分でない対象物の受入率と対象物の製作コストから、当該製品における安全性の評価を行うことができる。実際に、われわれの研究チームでは、指紋、虹彩、静脈パターンを生体情報と

して利用するいくつかの生体認証システムにおいて、こうした評価のための実験を行っている。

生体部分でない対象物による攻撃からの防御を考えた場合、まず、そうした対象物の使用を防止するためには、生体検知機能が有効に機能することが重要であるほか、システム運用時の監視によって対応することも考えられる。また、生体部分でない対象物の作製を防止するためには、生体部分に関する情報の盗取を防止すること、例えば、偽のATM等による生体情報のフィッシングを阻止すること等も重要である。

生体認証をはじめとする利用者認証技術については、利用者にとってわかりやすく、確かに信頼できると実感できるものであることが求められる。そのため、金融機関には、利用者認証技術がどのようなものであるか、それを育て、いかに適用していくか等につき、更なる検討をお願いしたい。

4．発表2「暗号アルゴリズムの2010年問題について」

宇根は、神田との共同論文[3]に基づき、暗号アルゴリズムにおける2010年問題とその背景や同問題への対応のあり方について、以下のとおり説明を行った。

(1) 暗号アルゴリズムにおける2010年問題とは

暗号アルゴリズムの2010年問題（以下、単に2010年問題と呼ぶ）は、現在金融分野で主流となっている暗号アルゴリズムが、米国立標準技術研究所（NIST）による安全性に関する「お墨付き」を2010年頃に喪失する見通しとなっており、2011年以降もそれらのアルゴリズムを使用し続けた場合、当該情報システムの安全性に関するレピュテーションが損なわれてしまうという問題である。

(2) 金融分野で主流となっている暗号アルゴリズムとその安全性評価

ISOの国際標準やEMVをはじめとする業界仕様等を参照すると、金融分野では、共通鍵暗号には2-keyトリプルDESとRC4、公開鍵暗号やデジタル署名方式には鍵長1,024ビットのRSA（以下、1,024ビットRSAと呼ぶ）、ハッシュ関数にはSHA-1が広く採用されているようである。これらの安全性評価結果をみると、現時点で直ちに問題となるほどの安全性の低下が指摘されているわけではない。しかし、今後、中・長期（10～15年）での利用を想定する場合、十分な安全性を確保し続けることは困難との見方が暗号学者の間で大勢となっている。

1,024ビットRSAの安全性評価結果をやや詳しく説明すると、現時点ではアルゴリズム構成については特段問題は指摘されていない。しかし、鍵長（1,024ビット）に

3 宇根正志・神田雅透、「暗号アルゴリズムにおける2010年問題について」、本号所収。

関しては、今後の計算機のコスト・パフォーマンスの向上等を考慮すれば、中・長期的に十分な安全性を確保できなくなるおそれがあるとの研究結果が複数発表されている。このように、中長期的にみれば、1,024ビットという鍵長が問題となるといえる。

（3）安全性に関する「お墨付き」の意味とその影響

情報システムにおいて暗号アルゴリズムを採用する場合、アルゴリズムの種類とその実装形態（鍵長等）について検討する必要がある。ただし、実際に暗号アルゴリズムの安全性を利用者が適切に評価することは容易でない。高い専門性と豊富な経験を備えた第三者的な機関による評価結果を参照できるとすれば、それらの機関が「十分な安全性を有している」と評価した結果を「お墨付き」として位置付け、暗号アルゴリズムの選択の有力な材料とすることが合理的かつ妥当である。実際にこうした機関は存在し、その代表がNISTである。

NISTは、米国連邦政府の情報システムで使用する暗号アルゴリズムの認定や推奨を行っている。NISTによる評価結果への信頼は厚く、例えば、暗号技術検討会（CRYPTREC）によるわが国の電子政府推奨暗号リスト、欧州の暗号アルゴリズム評価プロジェクトNESSIEの評価結果、汎業界における守秘目的の暗号アルゴリズムの国際標準ISO/IEC 18033には、NISTの評価結果が引用され、それに沿った判断が下されている。金融分野に関する国際標準化を担当するISO/TC68も、これまでDESやトリプルDESを国際標準に規定するに当たって、NISTの評価結果を有力な材料として考慮したといわれている。

NISTが現時点で認定・推奨している暗号アルゴリズムをみると、2-keyトリプルDES、1,024ビットRSA、SHA-1の使用はいずれも2010年までとなっており、2010年で「お墨付き」が喪失するといえる。RC4は現時点でも推奨されていない。2010年以降、こうした「お墨付き」を失った暗号アルゴリズムを使用し続けた場合、当該システムの安全性に関するレピュテーションの低下は避けられないと考えられる。また、暗号アルゴリズムの安全性上の欠陥から何らかの金銭的な損害が発生した場合、「お墨付き」を喪失した暗号アルゴリズムを使用し続けていたという点で批判を受ける可能性も考えられる。

（4）2010年問題への対応について

2010年末まで5年足らずであり、システム変更等にかかる時間も考慮すると、2010年問題への対応に関する検討に早急に着手する必要があるといえる。

まず、どの暗号アルゴリズムへ移行するかであるが、NISTが2011年以降に米国連邦政府の情報システムでの使用を推奨しているものに加え、CRYPTRECやNESSIEで評価されているものや、ISO/IEC 18033に規定されているものも候補となる。このように、候補となる暗号アルゴリズムは複数存在しており、検討対象となる情報システムの形態や要件を考慮したうえで選択することとなる。また、その際

には、当該システムと接続している他の情報システムとの相互運用性等に配慮することも必要である。

こうした対応に加え、個々の金融機関および金融業界全体として、将来の暗号アルゴリズムの危殆化に迅速かつ適切に対応するための体制の整備についても中長期的に検討することが重要である。

5．発表3「金融分野におけるICカード・システムのセキュリティについて」

田村は、宇根との共同論文[4]に基づき、金融分野におけるICカードを利用した本人認証システムのセキュリティ要件について、以下のとおり説明を行った。

(1) ICカードを用いた安全な本人認証システムを構築するために

わが国では、偽造カードを用いたなりすましによる不正な預金引出が深刻な問題となっており、金融機関は、こうした問題への対応として従来の磁気ストライプによるキャッシュカードのICカード化を進めている。ICカードを利用した本人認証システムを構築する際には、システム全体に存在する脆弱性を明確にしたうえでセキュリティ要件を導出し、当該システムがそうした要件を満足しているか否かを適宜評価していくことが重要である。その際、まず、想定する脅威に対して、脅威を具体化する攻撃手法を洗い出し、それらへの対策手法からセキュリティ要件を導出することが必要となる。

(2) ICカードによる所持認証のセキュリティ要件

ICカードによる所持認証とは、金融機関が配付した真正なICカードを携帯するユーザを本人（被認証者によって主張された身元）であると判断することである。ICカード認証は、提示されたICカードが金融機関によって配付されたものであることが確認可能であること、および、カード所持者のユーザIDを特定可能であることの2つを満足させるための手段であり、ICカードの動作の違いによって動的認証と静的認証に分類できる。さらに、認証者が端末であるかホストであるかによってオフライン認証とオンライン認証に分類できるほか、認証プロトコルに利用する暗号技術の違いによって分類できる。

ICカード認証においてなりすましを行うシナリオとしては、①真正な端末やホストに対してなりすましが成功する偽造カードを作製すること、あるいは、②攻撃者が作製した偽造カードと整合性を持つように端末を不正操作することが考えられる。こうした具体的な攻撃を列挙し、対策手法からセキュリティ要件を導出すると、

4 田村裕子・宇根正志、「金融取引におけるICカードを利用した本人認証について」、本号所収。

表1　ICカード認証におけるセキュリティ要件

ICカード認証の形態		セキュリティ要件					
		端末の真正性確認	ICカードの耐タンパー性	端末の耐タンパー性	ICカード・端末間のデータ漏洩防止	端末・ホスト間のデータ漏洩防止	認証プロトコルの安全性
動的認証	オフライン		○	○			○
	オンライン		○				○
静的認証	オフライン	○		○	○		○
	オンライン	○			○	○	○

認証形態の違いによってセキュリティ要件に差異が生じる（表1参照）。動的認証では、ICカードの耐タンパー性がセキュリティ要件となるのに対し、静的認証では、端末の真正性確認が必要となるほか、ICカードと認証者（端末、ホスト）間のデータ漏洩を防止する機構が必要となる。そのほか、オフライン認証には端末の耐タンパー性が求められる。

（3）PINによる知識認証のセキュリティ要件

PINによる知識認証とは、金融機関に登録されるPINを提示するユーザを本人であると判断することである。PIN認証は、提示されたPINが金融機関に登録されたデータ（参照PINデータ）に対応するものであることを確認するための手段であり、PINの照合を実行するエンティティと参照PINデータを格納するエンティティによって分類することができる。

PIN認証においてなりすましを行うシナリオとしては、①カード所持者のPINを盗取する、あるいは、②攻撃者が適当に設定したPINと整合性を持つように、システム側に保管されている参照PINデータを改ざん・偽造することが考えられる。PINの管理に関する国際標準であるISO 9564-1に規定されている5つの認証形態に対して、こうした攻撃に対するセキュリティ要件を導出すると、PINの照合先や参照PINデータの格納先の違いによって、セキュリティ要件に差異が生じる（表2参照）。ICカード内に格納されるデータを利用する形態ではICカードの耐タンパー性が要件として求められるほか、参照PINデータが送受信される形態では、受信した参照PINデータが金融機関によって設定されたものであるか否かの確認をMACやデジタル署名を利用して行うことが要件となる。

（4）セキュリティ要件の活用

ICカード認証およびPIN認証のなりすましに対するセキュリティ要件をみると、安全な本人認証システムの構築には、ICカードの耐タンパー性のみならず、システム全体に存在する脆弱性を考慮する必要があることがわかる。本人認証システムの

表2　PIN認証におけるセキュリティ要件

PIN認証の形態		セキュリティ要件					
PINの照合先	参照PINデータの格納先	PIN入力時の覗き見防止	端末の真正性確認	データの安全な暗号化	ICカードの耐タンパー性	端末の耐タンパー性	MAC/デジタル署名の安全性
ICカード	ICカード	○	○	○	○	○	
	ホスト	○	○	○	○	○	○
端末	ICカード	○	○	○	○	○	○
	ホスト	○	○	○		○	○
ホスト	ホスト	○	○	○		○	

ツールであるICカードを期待通りの安全性を提供するものとして利用する場合には、採用する認証方式に留意し、そのセキュリティ要件を参照したうえで実際にそれらが達成されているか否かを検証することが重要である。

6．パネル・ディスカッション「金融機関の情報セキュリティ対策のあり方：研究から実践へ」

(1) パネル発表1「最近の情報セキュリティの現状」

三角は、最近の情報セキュリティに関する情報処理推進機構（IPA）への届出状況、および、昨年特に注目されたインターネット上のセキュリティ問題について、以下のように発表した。

イ．近年の情報セキュリティに係る脅威の傾向

IPAは、コンピュータ・ウイルス、不正アクセス、脆弱性情報に関する届出を受け付けているが、近年、その届出件数が増大している。ウイルスに関するIPAへの届出件数は増加傾向にあり、2005年には約5万件に達している。

不正アクセスについては、攻撃者の目的が愉快犯的行為から経済的利得へと移行しており、犯罪者の組織化や分業化がみられるようになっている。2005年の届出状況としては、特定のサイトからスパイウエアがインストールされ、不正請求書が表示され続けるといった、いわゆる「ワンクリック不正請求」に関するものが最も多かったほか、SSH（Secure SHell）[5]で使用するポートからの侵入被害等も増加している。また、こうした不正アクセスの被害の原因は、利用者によるパスワード管理の不備であることが多い。

5 ネットワークを介して別のコンピュータにログインしたり、遠隔地のコンピュータでコマンドを実行したり、他のコンピュータへファイルを移動したりするために使うプロトコルのこと。

2005年の脆弱性関連情報の届出状況については、オープン・ソース・ソフトウエアに関する届出の増加が目立っているほか、ウェブ・アプリケーションに関する脆弱性としてはクロスサイト・スクリプティングに関する届出が全体の半数近くを占めている。

ロ．2005年の10大脅威

IPAでは、届出情報をもとに、セキュリティ上の10大脅威を選び、利用者・管理者・開発者のそれぞれからみた脅威を分析し、今後の課題等を検討したものを「情報セキュリティ白書2006年版」として公表している。

2005年に発生した注目すべき脅威のうち、金融業界に関連が深いものとして、まずフィッシング詐欺とスパイウエアが挙げられる。最近は、フィッシング詐欺の手口も悪質化しており、攻撃対象を絞り込んだうえで、知人の名前等を使って電子メールを送付するといった「スピア型フィッシング詐欺」と呼ばれる攻撃手口が出現している。そのため、IPAでは、利用者に対して、メールで個人情報や信用情報を送信しないことや、メールが本物であるか迷う場合には直接金融機関に確認するといったこと等を呼びかけている。スパイウエアについても、修正プログラムを適用すること、スパイウエア対策ソフトの利用および定期的な定義ファイルの更新・検査を行うこと、怪しいサイトや不審メールに注意すること等を利用者に対して呼びかけている。既に一部の金融機関では、ホームページ上で利用者に対してわかりやすい言葉で具体的なセキュリティ対策の手法について説明している例もあるが、金融分野にとって利用者のセキュリティ意識を向上させるという活動は今後より重要になってくると思われる。

インターネット上での攻撃方法は日々変化しており、管理者には継続的なセキュリティ対策および運用が求められている。また、総合的なセキュリティ・レベルを保つためにも、セキュリティ・ポリシーや情報セキュリティ管理の指針を定め、それを実践するとともに、導入しているソフトウエアに対する脆弱性対策やトラブルが発生した場合の対処法等を適切に定めておくことが必要である。

（2）パネル発表2「CSIRTとJPCERT/CC」

歌代は、JPCERTコーディネーションセンター（JPCERT/CC）の活動内容について、以下のように説明した。

イ．CSIRT（Computer Security Incident Response Team）について

インターネットの原型は、1970年頃に始まったアーパネット（ARPANET）という研究目的で構築されたネットワークである。その後、1980年代初めに、現在のTCP/IPによる通信が開始され、インターネットが本格的に始動した。当時のインターネットは研究者の集まりで構成されており、インターネットに対する攻撃は想定されていなかった。しかし、1988年にロバート・モーリスが作成したワームにより、

インターネットが大きなダメージを受けるという事件（モーリス・ワーム事件）が発生した。事件の発生後、利用者がインターネットの接続を遮断してしまっていたために、モーリス・ワームへの対処法が明らかとなった後もその解決策を普及させることができなかった。こうした経験から、インターネット上での攻撃に対して緊急に対応する組織（CSIRT）が必要であるとの認識が高まり、米国でCERT/CC（コンピュータ緊急対応センター）が設立された。また、1990年には世界中のCSIRT同士の連携を目的とした組織であるFIRST（Forum of Incident Response and Security Teams）も発足している。わが国においては、1992年にJEPG/IPという研究者のグループを中心としたボランティア・ベースの活動が開始し、その後、任意団体としてJPCERT/CCが発足している。

コンピュータ緊急対応センターは、さまざまな組織によって設立されており、そのタイプも多様である。こうした組織は世界中に多く存在しており、現在は180余りがFIRSTに加盟している。金融業界からも10組織前後が加盟しているようであるが、他の業界と比較すると、インターネット上の攻撃に緊急対応するための体制整備が遅れているように感じられる。わが国の金融業界としても、自らの組織内にCSIRTを設立し、国際フォーラムに加盟することで、情報共有やインシデント対応の国際協力を行うことが考えられる。

ロ．JPCERT/CCの業務内容

近年のJPCERT/CCの活動の軸足は、インターネットを介して発生する不正侵入やサービス妨害等のコンピュータ・セキュリティ・インシデントに対する事後対応から事前対応に移行し始めている。事前対応に関する活動の1つに脆弱性情報ハンドリングがある。これは、ソフトウエア等における脆弱性関連情報をベンダに周知することにより、ベンダの速やかな対策を促すものである。こうした情報は、攻撃者に悪用されることのないよう、適切に情報をコントロールしたうえで流通させていくことが重要となる。このほか、インシデントの早期把握のための観測および情報提供を目的としてインターネットの定点観測システムの運用も行っている。

JPCERT/CCは、2005年に「早期警戒グループ」を発足させ、金融等の重要インフラの事業者に対して、一般とは別の仕組みを利用して早期警戒情報を提供する取組みを始めた。こうした分野に早い段階で情報を提供することで迅速な対応を促し、インシデントの発生を未然に防いでいくことが目的である。そのほか、想定される脅威、および、インシデントが発生した場合に取るべき対応に関するセキュリティ演習の機会も提供していきたいと考えている。

（3）自由討議

上記のキーノート・スピーチ、研究発表およびパネル発表の内容を受けて、以下のとおり、パネリストによる自由討議が行われた。

イ．偽造カード問題について

まず、**岩下**は、偽造カード問題を巡る金融機関側の対策の現状をどう評価するかについて、パネリストの見解を尋ねた。**松本**は、ATMでの引出限度額の引下げ等、犯罪被害額を限定するための対策が進んでいるのに比べて、偽造カード犯罪を発生させにくくするためのキャッシュカードのICカード化への取り組みが不十分であることを指摘し、金融業界全体として検討が必要であることを訴えた。また、生体認証については、金融機関が業務システムに適切に実装したうえで、その効果を利用者に説明し、安全であると納得してもらう必要があると述べた。一方、**三角**は、利用者に提供するシステムが安全であることをアピールする手段として、第三者機関がIT製品やシステムの評価を行う「ITセキュリティ評価・認証制度」が利用可能となっており、ICカードについて認証を取得している事例もあることを紹介した。これに関連して、**松本**は、ICカード単体はもとより、ICカードを利用するシステム全体の安全性に留意する必要があることを強調し、過去に実際に発生したATMでの隠しカメラによるPIN盗撮事件等を例示して、「対策の検討に当たって、どのような脅威を想定するか」について十分に検討されることが必要であると述べた。これに対し、**岩下**は、これまで、金融情報システムセンター（FISC）の安全対策基準において、ATMのセキュリティ要件が検討・整理されてきたことを紹介したうえで、新しく発生した脅威については、金融機関が迅速に情報を共有して対処することで、被害の拡散を防止していくことが今後の課題であろうと述べた。

ロ．インターネット・バンキングのセキュリティについて

続いて、**岩下**は、インターネット・バンキングの安全対策の現状について、パネリストの見解を尋ねた。**歌代**は、インターネットにおける攻撃について、これまでは愉快犯的攻撃が主流であったが、近年は金銭的利益を目的とした攻撃へと変容してきているため、従来の対策技術やセキュリティ・サービスの適用が難しいことを説明した。特に、インターネット・バンキングについては、金銭的利益を目的とした攻撃の標的となりやすいため、これまでとは異なる視点から、関係者が協力して対策を考えていかなければならないと指摘した。また、**三角**は、利用者側がインターネット・バンキングを利用する際のリスクについて十分認識しておくことが重要であり、リテラシー向上のための利用者教育が必要となると述べたうえで、IPAとしても、怪しいサイトや不審メールに注意することといったような、インターネットを安全に利用するために必要な知識の取得を促進する情報の発信を行っていると説明した。また、**歌代**は、セキュリティ対策に必要なコストと顧客の利便性とがトレード・オフの関係にあることを考えると、金融機関は、単にセキュリティ対策を追加していくだけではなく、顧客に提供するサービスの内容や条件を見直すことにより、顧客自身が高度なセキュリティ対策を選択するような誘引を与えてもよいのではないかと指摘した。

ハ．個人情報保護について

次に、**岩下**は、金融機関における個人情報保護を巡る最近の動きに関して、パネリストのコメントを求めた。**三角**は、ウィニー[6]を通じたウイルス感染による情報漏洩について、本来管理されている情報が持ち出された、あるいは、持ち出さざるを得ない状況が発生し、それに加えて、情報を格納したパソコンにウイルス対策が施されていなかったということが問題であったと説明した。そのうえで、情報を取り扱うパソコンを適切に管理するとともに、自宅に仕事を持ち帰らざるを得ない状況を作らないといった対応が重要であると述べた。また、**歌代**は、利用者のモラルや情報管理に関する体制整備等のほか、システムのサポート強化も重要であり、そうしたソフトウエアの技術開発が今後必要であると述べた。**松本**は、ボットネット[7]等が銀行のサーバにサービス妨害攻撃を仕掛けることも十分に考えられることから、銀行のネットワークに対して想定されるインシデントへの対応について検討することが必要であると述べた。**歌代**も、ボットネットの脅威について強調し、金融業界全体としての対応策の検討の必要性を指摘した。これに関連して、**岩下**は、インターネット・バンキングにおける利用者認証において、ボットネットを利用して、ユーザIDに対するパスワードを検索するという攻撃にも警戒が必要であると述べた。

ニ．まとめ

最後に、パネル・ディスカッションのまとめとして、各パネリストが金融機関の情報セキュリティ対策のあり方に関する留意点を述べた。**松本**は、金融機関が実効性のあるセキュリティ対策を講じていくためには、預金者、金融機関、装置や技術を提供するベンダの三者間でコンセンサスを得る形でセキュリティ対策を行っていく必要があると指摘した。**三角**は、金融機関は自ら利用者に対してセキュリティ対策に関する情報を発信し、利用者のリテラシー向上に努めてほしいと述べた。**歌代**は、今後インターネット・バンキングの利用者が増加することに伴い、個人情報の漏洩による不正送金等、海外で既に深刻化しているセキュリティ上の問題がわが国においても発生し、深刻な状況に陥る危険性が高いと考えられることから、そうしたリスクを念頭において、どのような金融サービスを提供していくか検討していくことが重要であると述べた。

6 インターネットを利用して不特定多数のユーザ間でファイルを交換できるソフトウエア。
7 外部からの悪意ある命令を実行するソフトウエアである「ボット」に感染したコンピュータが束になって構成するネットワーク。攻撃者による命令によって、ボットネット上のパソコンが一斉に活動するため、大規模なサービス妨害攻撃等が可能である。

7．総括コメント

今井は、総括コメントとして、キーノート・スピーチ、研究発表およびパネル・ディスカッションの内容を振り返ったうえで、次のようにコメントを行い、シンポジウムを締め括った。

本日のシンポジウム全体を通して、金融業界における情報セキュリティ対策について、改めてその重要性を痛感するとともに、困難な課題が多数残されていることを認識した。金融業界は、本日指摘されたさまざまな課題について、その解決のための適切な対応を進めていくことが必要である。そのためには、各金融機関において、セキュリティ対策の有効性、技術上の課題等を十分に見極められる能力をつけるべく、本シンポジウムのような場を利用して、情報を収集し、知見を深める努力を続けていくことが求められている。

日本銀行金融研究所の情報技術研究センターは、金融業界に求められる情報技術に関して、最新の情報を収集・把握したうえで、それをわかりやすく金融業界に示していくことが重要な役割であり、昨年4月に設立されてから1年間で大きな成果を残したと評価している。一方、私がセンター長を務める産業技術総合研究所の情報セキュリティ研究センターも、情報セキュリティに関する最先端の研究開発と人材育成を目的に、昨年4月に設立された。今後、より一層、両センターの活動を充実したものにするうえで、互いの知識を共有することが重要であり、さらに連携を進めていきたいと考えている。