第10回
情報セキュリティ・シンポジウム
の模様

1. はじめに

金融研究所は、平成20年2月5日、「金融業務と情報セキュリティ技術：この10年の経験と今後の展望」をテーマとして、第10回情報セキュリティ・シンポジウムを開催した。

本シンポジウムは、平成10年に第1回を開催してから毎年度開催し、今回で10回目となる。これまでのシンポジウムでは、わが国の金融業界が直面する情報セキュリティ上の課題を取り上げ、その現状や今後の対応のあり方について議論を行い、そうした情報を金融業界の実務家と共有することを目的としてきた。今回のシンポジウムでは、過去のシンポジウムの内容を振り返り、今後の金融業界の情報セキュリティ対策のあり方について議論した。

まず、キーノート・スピーチにおいては、この10年間の金融業界における情報セキュリティ上の問題とその対応状況について整理された。2件の研究発表では、電子マネー・システムのセキュリティ、および、情報セキュリティ製品・システムにおける第三者評価・認証制度に関する研究成果の報告がそれぞれ行われた。パネル・ディスカッションにおいては、金融分野において幅広く利用されている5つの情報セキュリティ技術分野が取り上げられ、各技術分野における最新動向について議論が行われた（プログラムは次頁のとおり）。

フロアには、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、ベンダーの研究開発部門・標準化部門の実務家や技術者等、約140名が参加した。

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）。

本稿に示された意見はすべて発言者ら個人に属し、その所属する組織の公式見解を示すものではない。

【第 10 回情報セキュリティ・シンポジウムのプログラム】

- キーノート・スピーチ「金融業務と情報セキュリティ技術：この 10 年の経験と今後の展望」
  —岩下直行（金融研究所情報技術研究センター）
- 発表 1「電子マネー・システムにおけるセキュリティ対策：リスク管理に焦点を当てて」
  —廣川勝久（金融研究所情報技術研究センター）
- 発表 2「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において活用していくために」
  —田村裕子（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「オープンなネットワークにおけるオンライン金融取引の情報セキュリティ技術：その進化と今後の展望」
  - パネル発表 1：ハッシュ関数の脆弱性について
    —太田和夫（電気通信大学教授）
  - パネル発表 2：パスワードを用いた認証方式について
    —古原和邦（産業技術総合研究所情報セキュリティ研究センター主幹研究員）
  - パネル発表 3：生体認証について
    —小松尚久（早稲田大学教授）
  - パネル発表 4：暗号モジュールの耐タンパー性について
    —松本　勉（横浜国立大学教授）
  - パネル発表 5：ウェブ・アプリケーションのセキュリティについて
    —高木浩光（産業技術総合研究所情報セキュリティ研究センター主任研究員）
  - 自由討議
    - モデレータ：岩下直行
    - パネリスト：太田和夫、古原和邦、小松尚久、松本 勉、高木浩光
- 総括コメント—今井秀樹（中央大学教授）

2. キーノート・スピーチ「金融業務と情報セキュリティ技術：この 10 年の経験と今後の展望」

岩下は、標記論文[1]に基づき、これまでの情報セキュリティ・シンポジウムの内容（図表 1）を参照しながら、わが国の金融業界が直面してきた情報セキュリティ上の問題とその対応状況や、今後の情報セキュリティ対策のあり方について、次のとおり発表を行った。

図表 1　これまでの情報セキュリティ・シンポジウムのテーマ

開催回	テーマ	現状分析と指摘された課題
第 1 回（平成 10 年）	金融分野における情報セキュリティ技術の現状と課題	金融情報システムにおけるネットワークのオープン化 → 情報セキュリティ技術を導入していくことが有効
第 2 回（平成 11 年）	金融業務と認証技術	既存の認証方式（MS カード＋PIN 等）のセキュリティ・レベル低下、インターネットを利用した金融サービスの本格化 → 適切な認証方式（IC カード、生体認証、SSL）の検討が必要
第 3 回（平成 12 年）	情報セキュリティ技術の評価と信頼性	ネットワークのオープン化による情報セキュリティ技術の必要性に関する認識の高まり → 情報セキュリティ技術の安全性評価を適切に活用すべき
第 4 回（平成 13 年）	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	インターネット・バンキングの定着、既存の認証方式（SSL ＋ パスワード ＋ 乱数表）の安全性に関する指摘 → セキュリティ上の脅威に対する適切な対策の検討
第 5 回（平成 14 年）	デジタル署名の長期的な利用とその安全性	電子署名法の成立や電子政府に向けた取組みの結果、紙文書からデジタル文書への置換えが加速 → デジタル署名付き文書の長期保管に関する検討
第 6 回（平成 15 年）	金融分野における人工物メトリクス	画像処理技術の発達等による人工物の偽造・複製事件が増加 → 人工物の安全性・信頼性を維持するための技術的な枠組みの整備
第 7 回（平成 16 年）	金融業界における情報システムの脆弱性検知と情報共有	偽造キャッシュカードによる不正預金引出、フィッシング詐欺等、金融ハイテク犯罪の脅威の顕現化 → 金融業界における脆弱性検知・情報共有のための体制整備
第 8 回（平成 17 年）	金融機関の情報セキュリティ対策のあり方	偽造キャッシュカード問題、スパイウエアによる個人情報漏洩、インターネット・バンキングでの不正送金 → 金融業界内で情報共有を進めるための枠組みの必要性
第 9 回（平成 18 年）	リテール・バンキングのセキュリティ	IC キャッシュカードや生体認証はあまり普及していない → やや長い目でリテール・バンキングのセキュリティを向上させるためのグランド・デザインの検討が必要

1 岩下直行、「金融業務の情報セキュリティ技術：この 10 年の経験と今後の展望」、本号所収。

(1) 情報セキュリティ・シンポジウムの 10 年間

わが国の金融機関は、この 10 年間、金融情報システムにおける情報セキュリティを確保するために対策の高度化を進めてきた。第 1 回の情報セキュリティ・シンポジウムが開催された平成 10 年当時、金融機関の情報システムにおいては、比較的素朴なセキュリティ対策が主流であった。専用回線を利用したクローズドなネットワーク・システムを採用し、データの暗号化やデジタル署名技術をほとんど利用していなかった。当時は、最先端の情報セキュリティ技術を導入しなくても、一定の安全性が期待できる環境下にあり、利用者が金融ハイテク犯罪の被害者となることはほとんどなかった。

しかし、インターネットの普及や電子マネーへの関心が高まり、金融機関はオープンなネットワークを利用したさまざまなサービスの提供を始めた。そのため、従来のクローズドなシステムでは想定されなかった新たな脅威に対処することが求められ、最新の情報セキュリティ技術の導入を含めた情報セキュリティ対策に関するグランド・デザインを再考する必要に迫られることとなった。

第 1〜4 回のシンポジウムにおいては、こうしたネットワークのオープン化に伴う課題について検討を行った。例えば、第 2 回のシンポジウムでは、インターネット・バンキング等、オープンなネットワーク環境のもとで提供される金融サービスにおいては、従来と同じ素朴なセキュリティ対策のままでは安全性を確保することが困難であり、暗号技術を活用した高度な対策の導入が必要ではないかとの問題提起を行った。

(2) 偽造キャッシュカード問題の衝撃

ネットワークのオープン化の動きに加えて、金融機関による情報セキュリティ技術の利用に拍車をかけるきっかけとなったのが、平成 16 年から 17 年にかけて社会問題化した「偽造キャッシュカード問題」であった。その結果、金融機関の情報セキュリティ対策に関する世間の関心が高まり、被害者への補償や、キャッシュカードの IC カード化や生体認証等の新しい情報セキュリティ対策の導入が進められた。その後、ATM における引出限度額の引下げ等の効果もあって、その被害は減少し、金融機関に対する批判も沈静化してきた。しかし、カード偽造犯罪の予防策として IC カードや生体認証を導入した金融機関はまだ限られており、利用者の間でも普及しているとは言い難い。また、IC キャッシュカードであっても、現在発行されているものの多くは磁気ストライプが併用されており、磁気ストライプ部分のみを偽造することが容易であることから、カードの偽造への対策として有効であるとは言い難い。

偽造キャッシュカード問題とその対策については、第 7～9 回のシンポジウムで取り上げて議論を行った。例えば、第 8 回のシンポジウムでは、偽造キャッシュカード問題への対策として、磁気ストライプとの併用でない IC キャッシュカードの利用や生体認証の導入を挙げており、そうした対策によってキャッシュカードと ATM における情報セキュリティを抜本的に向上させることが重要ではないかとの問題提起を行った。

(3) 脆弱性情報の公開と共有を巡って

本シンポジウムにおいて継続的に取り扱われてきた重要なテーマの 1 つに、「金融情報システムにおける脆弱性情報をどう取り扱うべきか」という問題が挙げられる。金融機関では、セキュリティ上の問題を「機密事項」として取り扱う傾向が強く、自らの採用する技術が学術的な研究の対象とされることや、技術的な論評をされることを忌避する先が多い。その傾向が行き過ぎると、セキュリティ・システムに問題があったとしても、実際にセキュリティが破られて事件とならないと発覚しないということになってしまう。実際、これまでにも、脆弱なリテール・バンキング・システムが改善されずに利用され続けてしまった実例は少なくない。

第 3 回のシンポジウムでは、仮に、金融情報システムにおいて情報セキュリティ技術の利用に関する欠陥が指摘される事態となった場合、どのような体制が整備されていることが望ましいかについて議論を行った。その後、ソフトウエア製品とウェブ・アプリケーションの脆弱性については、「情報セキュリティ早期警戒パートナーシップ」が実現したものの、金融情報システムを対象とした脆弱性情報の取扱いに関しては今後の課題として残されている。

(4) シンポジウムで指摘された脆弱性の顕現化事例

金融情報システムにおける脆弱性については、顧客に被害が及ぶ可能性がある事件が発生する前に、その潜在的な問題点について検討しておくことが重要である。本シンポジウムにおいても、金融ハイテク犯罪や情報セキュリティの要素技術の脆弱化の事例について、極力具体的に取り上げ、分析結果を発表して議論を行ってきた。

これまでに取り上げてきた脆弱性の顕現化事例をみると、学術的な研究動向をフォローしておくことで、起こりうるセキュリティ侵害への事前の警鐘として機能すると期待できるケースとそうでないケースがあることがわかる。例えば、暗号技術やネットワーク・セキュリティに関する研究分野では、セキュリティの研究と実務との距離が近く、研究成果を実務に直接参照することができる。また、仕様がオープンとなっている技術や製品については、セキュリティ分析のために外部の専門家の知恵を借りられるという特徴がある。これに対して、従来から金融分野で利用されてきたインフラについては、現在では特定の分野以外ではあまり使われない特殊な

技術を利用しているケースが多く、セキュリティ評価を依頼できる専門家が非常に少なくなってきている。さらに、システムの仕様も公開されていないため、セキュリティ侵害が発生する前に警鐘を鳴らすことが難しいのが実情である。

しかしながら、情報セキュリティ技術上の欠陥が存在する可能性がゼロにはならないことを考慮すると、現行システムに配慮しつつ、何らかのかたちで脆弱性に関する情報が金融機関に伝達されるルートを作っておくことは有用であろう。脆弱性に関する情報伝達のあり方については、金融業界の問題として検討していく必要があり、そのための情報を提供していくことも本シンポジウムの重要な役割である。

(5) 今後の展望

従来は、高価なレガシー系システムを使い続けることにより、「金融機関であれば、どこのシステムも安全で信頼できる」という業界全体としてのブランドが確立していた。しかし、システムのオープン化が進むと、安全性、信頼性の観点から、業界全体のブランドが維持できなくなるおそれがある。実際、インターネット・バンキングのセキュリティ向上やICカード、生体認証等の導入を行っているのは、個別企業として安全性や信頼性のブランド向上を企図する金融機関であり、そうした対応を選択しない金融機関も存在しているのが実情である。金融機関のシステムは相互に連携して機能していることを考慮すると、個別の金融機関のシステムだけが優れていても、業界全体として利用者の安全性を確保することができなくなる可能性が残る点に留意が必要である。

こうした観点からは、すべての金融機関がシステムのオープン化に伴うセキュリティの高度化に対応していく必要があり、そのためには、人材の育成と業界内での適切な情報共有を進めていくことが求められる。本シンポジウムを今後も継続していくことにより、広く学界、金融業界の方々の理解とサポートをいただきながら、引き続き、その一翼を担っていきたいと考えている。

3. 発表1「電子マネー・システムにおけるセキュリティ対策：リスク管理に焦点を当てて」

廣川は、鈴木・宇根との標記論文[2]に基づき、電子マネー・システムにおけるセキュリティ対策とリスク管理について、次のとおり発表を行った。

2 鈴木雅貴・廣川勝久・宇根正志、「電子マネー・システムにおけるセキュリティ対策：リスク管理に焦点を当てて」、本号所収。

(1) 金融取引システムの一形態としての電子マネー・システム

電子マネーは、実証実験の段階を経て、広く一般に普及し始めている。そうしたなか、一部のサービスにおいては電子マネーを不正に使用する事件等が発生しており、電子マネー・システムにおける脅威を分析し、適切な対策を講じることによって、システム全体としてのセキュリティを確保することが一層重要になってきている。

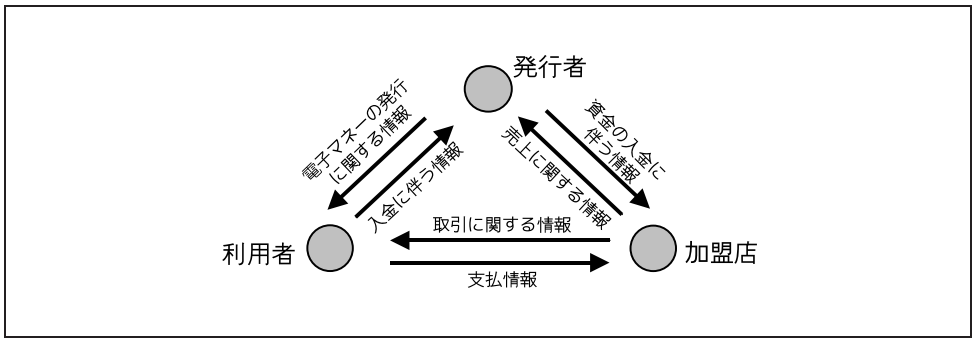
そうした検討を行う際には、電子マネー・システムを既存の金融取引システムの一形態として位置付けて検討することが有用である。例えば、キャッシュカード・システムでは、当該銀行が取引時にオンラインで取引の承認（以下、オンライン取引承認と呼ぶ）を行うほか、クレジットカード・システムでは、オンライン取引承認のほかに、小額取引等取引のリスクが相対的に小さいケースでは、店頭において取引の実行を認め、カード発行主体が事後的に取引の承認（以下、オフライン取引承認と呼ぶ）を行うこともある。近年注目を集めているプリペイド型電子マネーにおいては、オフライン取引承認が主流となっている。このように、各金融取引システムの取引承認の形態は、利便性や取引金額等さまざまな条件の組合せを反映して異なっている。セキュリティ対策についても、承認形態の差異に対応して異なるものの、IC カードや端末等のデバイスや暗号アルゴリズムを共通して活用している場合が多い。そのため、金融取引システムによって事件・事故等の内容が異なっていても、その原因・背景が共通している場合があるという意味で、他のシステムでの経験が参考になる。

(2) 電子マネー・システムのモデル化とセキュリティ評価の概要

今回、プリペイド型電子マネーに焦点を当てて、電子マネー・システムのセキュリティ評価に関する検討を行った。特に、①電子マネーを発行し、使用された電子マネーに対応する資金を支払う「発行者」、②電子マネーを発行してもらい、電子マネーを使用して商品やサービスを購入する「利用者」、③利用者に商品やサービスを販売し、取引で得られた情報を基に資金を発行者から得る「加盟店」によって構成される単純化されたモデルを前提とした（図表 2 参照）。そのうえで、電子マネーを利用して商品やサービスを購入する際に、利用者から加盟店に送られる支払いに関する情報（以下、支払情報と呼ぶ）を偽造することで不正取引が成立するか否かを分析した。こうした分析については、第 1 回の情報セキュリティ・シンポジウムで研究成果（中山・太田・松本論文[3]）が報告され、そのなかで体系的なセキュリティ評価が既に行われている。今回は、中山・太田・松本論文をベースとして、想定環境の変化等を考慮し、分析内容を拡張するかたちで検討を行った。

3 中山靖司・太田和夫・松本 勉、「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」、『金融研究』第 18 巻第 2 号、日本銀行金融研究所、1999 年、57～114 頁

図表２　想定する電子マネー・システムのモデル



想定環境については、中山・太田・松本論文では、「デバイスは危殆化し、暗号アルゴリズムは安全である」という状況が想定されていたが、今回は、デバイスと暗号アルゴリズムの両者について、安全な状況と危殆化した状況の両方を想定した。これは、近年デバイスのセキュリティ評価・認証の制度が整備されてきている、また、運用上の制約等から危殆化が懸念されている暗号アルゴリズムが使用され続けているケースがあるといった現状を踏まえたものである。

また、今回検討対象とする電子マネー・システムは、現行のプリペイド型電子マネー・システムで主流とみられる「残高管理型かつクローズド・ループ型」とする。すなわち、チャージや支払いの際に電子マネーの残高金額に関する情報（以下、残高情報と呼ぶ）を増減するとともに、利用者間における残高情報の譲渡を認めないという特徴を有するシステムである。このような電子マネー・システムはいくつかのタイプに細分化されるが、中山・太田・松本論文と同様に、取引承認の形態と残高情報の管理場所の観点から５つのタイプに分類した。残高情報の管理場所の観点からは、利用者が所持するデバイス内での管理（以下、ローカル管理と呼ぶ）、利用者のデバイスと発行者のサーバの両者での管理（以下、併用管理と呼ぶ）、発行者のサーバでの管理（以下、センター管理と呼ぶ）の３つが想定される。このような分類と２つの取引承認の形態を組み合わせると、オフライン取引承認かつローカル管理を行うタイプ、オフライン取引承認かつ併用管理を行うタイプ、オンライン取引承認かつローカル管理を行うタイプ、オンライン取引承認かつ併用管理を行うタイプ、オンライン取引承認かつセンター管理を行うタイプの５通りとなる。

攻撃のシナリオについては、攻撃者本人が自分の支払情報を偽造する攻撃、他の実在する利用者の支払情報を偽造する攻撃、架空の利用者の支払情報を偽造する攻撃の３つを想定した。

(3) セキュリティ評価の結果

こうした整理に基づき、各タイプについて 3 種類の攻撃が成功するか否かを検討した。その結果の一端を紹介すると、他の実在する利用者の支払情報を偽造する攻撃に関しては、デバイスと暗号アルゴリズムの少なくともどちらか一方が危殆化してしまうと、オフライン取引承認やローカル管理を行うタイプでは、加盟店のレベルでは、当該利用者の残高情報を確認することができず、攻撃が成功してしまうことがわかった。また、オンライン取引承認かつ併用管理を行うタイプとオンライン取引承認かつセンター管理を行うタイプでは、当該利用者の残高が十分に存在する場合にはチェックができず攻撃が成功してしまうことがわかった。

このような検討結果をみると、デバイスや暗号アルゴリズムが危殆化すると、偽造を検知できず、不正取引が成立する可能性があることがわかる。

(4) 電子マネー・システムにおけるリスク管理

デバイスや暗号アルゴリズムの危殆化により、支払情報の偽造等による不正取引が仮に成功したとすれば、関係者（利用者、加盟店、発行者等）に金銭的被害をもたらすだけでなく、サービス自体のレピュテーションの低下を引き起こす可能性がある。こうしたリスクを軽減する方法として、1 回当たりの取引金額やチャージ金額、残高情報の上限を低く抑え、1 回の不正で被る損失を少なくするという対策が考えられる。

また、被害の発生頻度を抑える対策もリスクの軽減につながる。具体的には、デバイスや暗号アルゴリズムを危殆化させないよう、定期的なセキュリティ評価の実施や、新しいデバイス等への速やかな移行を実現するためのシステム設計の採用等が考えられる。また、デバイスや暗号アルゴリズムが危殆化したとしてもリスクを許容レベル以下に抑える対策も考えられる。具体的には、電子マネー使用時等における本人確認の実施、電子マネーによる商品やサービスの購入パターンの事後検査、残高情報の不足や突合検査、不正な利用者の識別情報を記録したブラックリストでの検査等が挙げられる（図表 3 参照）。これらの対策のうちどれが適用可能であるかについては電子マネー・システムのタイプによって区々であり、その際の対策の効果（不正取引の阻止、攻撃の検知、被害拡大の防止）も異なっている。ただし、これらの対策を導入する際には、本人確認の実施の方法、購入パターン検査の方法、残高情報の検査の方法、ブラックリストの更新頻度等に関する検討を行うことが必要となり、必ずしも容易に実施可能であるというわけではない。

こうしたリスク管理のあり方を考えるうえで参考になる海外の電子マネーの事例として、IC 乗車券、ポストペイ型電子マネー、クレジットカードの 3 つの機能が一体となっている英国バークレイカード（Barclaycard）社の「スリー・イン・ワン・カード（3-in-1 card）」が挙げられる。本カードにおいては、非接触 IC カードのイン

図表３　他の実在する利用者の支払情報を偽造する攻撃への対策と効果

		電子マネー・システムのタイプ				
		オフライン取引承認		オンライン取引承認		
		ローカル管理	併用管理	ローカル管理	併用管理	センター管理
対策の効果	不正取引の阻止	・本人確認		・本人確認 ・購入パターンの即時検査		
	攻撃の検知	・購入パターンの事後検査	・購入パターンの事後検査 ・残高情報の不足や突合による検査	（不正取引の阻止が困難な場合、攻撃検知も困難）	・残高情報の突合検査	・利用者による残高情報の照会
	被害拡大の防止	・加盟店におけるブラックリストでの検査		・発行者におけるブラックリストでの検査		

ターフェースによってIC乗車券とポストペイ型電子マネーの機能が提供されているが、IC乗車券はロンドン地下鉄等の交通用途に限定して使用できるようになっているほか、ポストペイ型電子マネーは1回の取引金額の上限が10ポンドに制限されている。一方、10ポンド以上の支払いを行う場合には、クレジットカードとして端子付ICカードのインターフェースによって取引が行われる仕組みとなっており、取引時に本人確認を行うことが必須となっている。このように、取引の形態に応じて承認の形態を変化させている。

(5) まとめ

電子マネー・システムを円滑に発展させていくためには、利用環境や業務目的等に応じた情報セキュリティ技術を選択し、選択した技術を含めた適切な運用を行うことが必要である。そのうえで、利用環境や業務目的、情報セキュリティ上の環境等の変化に適切に対応していくために、運用も含めたシステム全体としてのリスク管理を行い、目標とするセキュリティを維持していくことが求められる。

4. 発表２「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において活用していくために」

田村は、宇根との標記論文[4]に基づき、わが国において整備されてきた情報セキュリティ製品・システムの第三者評価・認証制度を利用するメリットや利用する際の留意点について、次のとおり発表を行った。

4 田村裕子・宇根正志、「情報セキュリティ製品・システムの第三者評価・認証制度について：金融分野において活用していくために」、本号所収。

(1) わが国の金融業界におけるセキュリティ対策

近年、わが国では、インターネット等のオープンなネットワークを利用したさまざまな金融サービスが提供されるようになってきており、金融情報システムにおいては、従来のクローズド・システムでは想定していなかった新たな脅威に対抗することが求められている。こうしたなか、各金融機関は、金融情報システムへのセキュリティ対策に関する計画（plan）・実施（do）・確認（check）・処置（act）からなるサイクル（PDCA サイクル）を繰り返し実行することによって、セキュリティを一定以上に維持するためのマネジメントを行っている。

ただし、金融業務の多様化や情報システムへの脅威となる攻撃手法の高度化に伴い、金融情報システムが一層複雑なものとなってきており、PDCA サイクルによってセキュリティ対策を実施した当該システムが一定のセキュリティ要件を満足しているか否かの確認が容易でなくなってきているのが実情であろう。実際に、日本銀行考査等においては、各金融機関による情報セキュリティ対策の不備が指摘されているほか、海外で運用されている暗号アルゴリズムを実装したソフトウエアやハードウエア（以下、暗号モジュールと呼ぶ）の試験・認証制度においては、試験対象となった暗号モジュールの約半数にセキュリティ上の問題点が存在したとの報告がある。

(2) 第三者評価・認証の有用性

こうしたなか、特定の環境において情報セキュリティ製品・システムが想定される脅威に対して十分な耐性を有していることを中立的な立場の評価機関が評価し、その結果を別の機関（認証機関）が認証するという制度的な枠組みが近年整備されてきている。第三者によるセキュリティ評価・認証制度は、金融機関が情報セキュリティ対策を検討する際に活用することができる手段の 1 つであると考えられる。具体的には、管理運用面からのセキュリティ評価を目的とした「ISMS 適合性評価制度」や、技術面からの汎用的な情報セキュリティ製品・システムに適用可能な制度である「IT セキュリティ評価及び認証制度（JISEC: Japan Information Technology Security Evaluation and Certification Scheme）」と「暗号モジュール試験及び認証制度（JCMVP: Japan Cryptographic Module Validation Program）」が挙げられる。情報セキュリティの管理運用面については ISMS 適合性評価制度がわが国の金融機関によって既に活用されている一方、技術面については JISEC および JCMVP の金融分野における活用事例は少ないようである。このため、本発表では、JISEC と JCMVP に焦点を当てる。

これらの制度を金融機関が利用することによって、金融機関が独自に評価者を選定し、評価を依頼する場合に比べ、評価者を審査・選定するための手間を削減可能であるほか、認証機関による評価結果への「お墨付き」によって、評価対象の製品・システムのセキュリティに関する信頼を海外の顧客も含めて広くアピールしやすい

といったメリットを享受することができると考えられる。ただし、こうした制度を適切に活用していくためには、その目的や仕組みを正しく理解し、制度の限界や問題点を把握しておくことが必要である。

(3) JISEC と JCMVP

JISEC は、情報セキュリティ製品・システムのセキュリティ機能が、設計時の想定通りに適切に実装されているか否かを評価・認証する制度であり、平成 13 年 4 月から運営されている。評価対象の製品・システム（TOE: target of evaluation）のセキュリティ機能は、TOE の開発者によって作成されるセキュリティ・ターゲット（ST: security target）において記述される。ST は、セキュリティ評価基準の国際標準であるコモンクライテリアに基づいて作成されるものであり、ユーザとなる業界団体等によって作成されるセキュリティ要求仕様書であるプロテクション・プロファイルが公開されている場合には、それを参考に ST を作成することができる。また、ST が主張するセキュリティ機能の実装の確からしさを検査する範囲や検査の程度は、評価保証レベル（EAL: evaluation assurance level）で表される。

わが国の金融機関がこれまでに JISEC による認証を取得した TOE を利用していることを示唆する公開情報は非常に少ない。ただし、「全銀協 IC キャッシュカード標準仕様」や財団法人金融情報システムセンターによる「金融機関等におけるセキュリティ・ポリシー策定のための手引書」においては、セキュリティ対策を実施するうえでコモンクライテリアを参考にすることが推奨されており、JISEC の活用への関心も窺われる。

JCMVP は、暗号モジュールに「承認暗号アルゴリズム」が適切に実装されているか否か、および、暗号モジュールが一定のセキュリティ機能（セキュリティ要求事項と呼ばれる）を満足しているか否かを試験・認証する制度であり、平成 19 年 4 月から運営されている。JCMVP における承認暗号アルゴリズムは、わが国の電子政府推奨暗号リストを中心として選定されており、承認暗号アルゴリズムが実装される暗号モジュールが試験対象となる。暗号モジュールのセキュリティ要求事項は、当該暗号モジュールの開発者によって作成されるセキュリティ・ポリシーに記述され、当該セキュリティ・ポリシーを達成できているか否かの試験・認証が行われる。セキュリティ・ポリシーは、米国連邦政府標準規格である FIPS 140-2 をベースに国内規格化された JIS X 19790: 2007 に準拠して作成される。

わが国の金融分野における活用状況をみると、JCMVP 自体が運営開始後間もないこともあり、これまでに具体的な活用事例は公開情報によって調べる限り存在しないようである。ただし、IC キャッシュカードのアプリケーション向けに各銀行に対して公開鍵証明書を発行している全銀協認証局では、その署名生成鍵を格納する装置のセキュリティ要件として FIPS 140-2 の前身となる FIPS 140-1 を参照しており、わが国の金融分野においても従来から暗号モジュールの試験・認証制度に関心が向

けられていたようである。

(4) JISEC と JCMVP を利用するうえでの留意点

金融機関が JISEC を活用する方法としては、(A) 金融向け製品・システムに関するプロテクション・プロファイルの作成に参画する、(B) 認証を取得した製品・システムを調達する、(C) ST および TOE の開発に直接参画し、認証を取得するといった方法が考えられる。JCMVP を活用する方法としては、認証を取得した暗号モジュールを調達する、または、暗号モジュールのセキュリティ・ポリシーの作成や開発に直接参画し、認証を取得するといった方法が考えられる。こうした選択肢を踏まえつつ、わが国の金融機関が今後 JISEC や JCMVP の活用を検討していくうえで、次の 5 つの事項が留意すべき点として挙げられる。

① JISEC に関して、ST に記述される EAL が当該製品・システムのセキュリティ・レベルの指標として誤って認識されるケースが少なくないが、EAL はセキュリティ機能自体と直結するものではない。認証を取得した製品・システムを調達する際には、EAL のみを指標として判断するのではなく、アプリケーションの想定環境やセキュリティ要件と整合的な内容となっている ST および TOE を選択する必要がある。また、JCMVP を利用するうえでも、アプリケーションの想定環境やセキュリティ要件と整合的な内容となっているセキュリティ・ポリシーを有する暗号モジュールを選択することが求められる。

② JISEC に関して、TOE を構成する可能性のある要素技術のなかに、もともと評価の対象となっていない、あるいは、評価が技術的に困難なものが存在しており、そうした要素技術について別途評価が必要となる。例えば、仮に当該要素技術の効果が損なわれたとしても、製品・システムとして、あるいは、アプリケーション全体として一定レベルの情報セキュリティが確保されることを別途確認するといった対応が重要となろう。

③ JISEC や JCMVP における認証には有効期限が設定されていない。したがって、認証を取得した製品・システムであっても、そのセキュリティ機能が陳腐化していないことを別途確認する必要がある。

④ JCMVP では、現在金融分野で広く利用されている 2-key トリプル DES 等の暗号モジュールは、試験・評価の対象外となっている。したがって、JCMVP を活用する際には、そうした暗号アルゴリズムに代わって、今後、中長期的に利用していく暗号アルゴリズムの選定も同時に検討する必要がある。

⑤ JCMVP では、暗号モジュールの消費電力量から内部の暗号鍵を効率よく推定するといった高度な攻撃に対して、具体的なセキュリティ要求事項が JIS X 19790: 2007 において規定されていないほか、セキュリティ評価の手法も十分確立していないことから、そうした攻撃に対する耐性の評価を別途行う必要がある。例えば、適切な対策が別途講じられているか否かをセキュリティ・ポリシーで

確認するなどの対応が必要となろう。

(5) まとめ

金融サービスで利用する情報システムのセキュリティに関する信頼を確保していくうえで、当該システムのセキュリティ評価結果を何らかのかたちで顧客に示していくことが重要であり、システムの高度化や複雑化が進むなか、そうした活動の必要性は一層高まっている。こうした観点から、JISEC や JCMVP をどのように活用することができるかは、わが国の金融業界における重要な課題であると考えられる。実際の評価事例等も参照しつつ、今後検討を深めていくことが求められる。

5. パネル・ディスカッション「オープンなネットワークにおけるオンライン金融取引の情報セキュリティ技術：その進化と今後の展望」

(1) パネル発表１：ハッシュ関数の脆弱性について

太田は、ハッシュ関数の１つである MD5 の脆弱性が実運用されているシステムに与える影響とその対応状況について、次のとおり発表を行った。

ハッシュ関数は任意長の入力を固定長の出力に変換する関数であり、暗号学的に安全であると評価されるハッシュ関数には、「出力が一致する異なる入力ペア（以下、衝突ペアと呼ぶ）を現実的な時間で推定することが困難である」という性質が求められる。MD5 については、衝突ペアが現実的な時間で推定可能であることが既に示されていたが、こうした脆弱性が MD5 を利用したシステムの安全性に与える影響についてはこれまで明確になっていなかったこともあり、現在でもさまざまなアプリケーションに利用されているのが実情である。そこで、MD5 の脆弱性がシステムに及ぼす影響について検討を深めるために、MD5 を利用している代表的なプロトコルの１つである APOP（Authenticated Post Office Protocol）に着目し分析を行うこととした。

APOP は、クライアントがメール・サーバからメールを受信する際に行われるユーザ認証プロトコルであり、サーバから送信された乱数（以下、チャレンジと呼ぶ）やユーザのパスワードからなるデータに対する MD5 の出力をクライアントが生成し、サーバがその出力を確認することによってユーザの認証を行う。APOP に対して MD5 の脆弱性を適用して解析を試みたところ、パスワードをある値として仮定したうえで異なるチャレンジに対する衝突ペアを一定の手順で求め、それらのチャレンジに対してクライアントが生成するデータを利用すると、パスワードを効率的に推定できることがわかった。さらに、本攻撃を用いて実際にパスワードを推定で

きるか否かを確認するために、研究室内でネットワーク環境を構築し本攻撃を汎用の PC によって実行したところ、約千回の APOP の認証に利用されるデータを入手できれば、12 文字のパスワードを推定できることを実証した。APOP の認証を 1 時間に 1 回行う場合には、約 40 日で 12 文字のパスワードを特定することができることとなる。また、追加的な分析によって、単語を含むパスワードや英数字のみのパスワードは、記号が含まれているパスワードに比べて本攻撃に対する耐性が低いこともわかった。

本攻撃への当面の対策としては、SSL による暗号通信や異常なチャレンジの検出による攻撃の検知、パスワードの定期的な更新が挙げられ、長期的な視点からの対策としては、SHA-2 等のより安全なハッシュ関数への移行や APOP のプロトコルの仕様見直しが挙げられる。

こうした APOP におけるパスワード漏洩の脆弱性については、情報処理推進機構（IPA）に届け出た後、平成 19 年 4 月 19 日付の新聞に掲載され広く知られることになった。しかし、実運用されているシステムやソフトウエア製品における本脆弱性への対応は十分とは言い難いようである。例えば、本攻撃への注意をユーザに喚起しているインターネットのプロバイダは数社にとどまっているとの調査報告があるほか、ソフトウエア製品の対応状況について独自に調査したところ、11 の製品のうち、対策が講じられているのは 2 つの製品のみであることが判明した。このように、脆弱性が公表されたからといっても、実運用されているシステムに必ずしも速やかに対応がなされるわけではなく、タイムラグが存在する点に留意が必要である。

APOP の事例を踏まえると、金融分野において採用する情報セキュリティ製品・システムについても、少なくとも既知の脆弱性への対策が十分に施されているか否かを確認することが必要であるといえる。そのためには、金融分野において実際に利用されている暗号技術の研究動向を自らフォローしていくことが求められる。

(2) パネル発表 2：パスワードを用いた認証方式について

古原は、パスワードの盗取・漏洩に対する既存の対策の限界とパスワードの漏洩を前提とした対策の必要性について、次のとおり発表を行った。

インターネット・バンキング等のサービスを安全に利用するためには、サーバとユーザが相互に認証を行う技術や、両者が暗号通信を行うための秘密鍵を共有する技術が必要であり、社会基盤の 1 つとなってきている。特に、一般になじみの深いパスワードを用いて相互認証や鍵共有が行われる場合が多い。ただし、そうした場合には、フィッシング詐欺のように不正なサイトにパスワードを入力してしまう、あるいは、同じパスワードを複数のサーバで使用しているケースにおいて、それらのうち脆弱なサーバからパスワードが漏洩してしまうといったセキュリティ上の問題が存在する。また、利便性の観点からは、サーバごとに異なるパスワードを登録するためには、複数のパスワードを記憶しておく必要があるといった問題がある。

こうした問題を解決するためには、ユーザの教育・啓発〈対策1〉、ユーザの注意を喚起するインターフェースの導入〈対策2〉、新たな認証と鍵共有を行う方式（以下、認証鍵共有方式と呼ぶ）の検討・導入〈対策3〉という3つの対策が考えられる。対策1は、URLの確認やパスワードの管理の重要性を利用者に説明するアプローチであり、即座に対応を開始できる反面、すべてのユーザに周知徹底することが難しいという問題がある。対策2は、暗号通信中であることを示す南京錠アイコンをブラウザに表示する、サーバの認証結果をブラウザのアドレス・バーに反映する、ユーザ自身が選択した画像をログイン画面に表示するといったアプローチであり、対策1より周知徹底しやすい反面、即座に対応することが難しいという問題がある。対策3は、対策2より周知徹底が容易な反面、検討・導入までより長い期間が必要になると考えられる。

また、フィッシング詐欺によるパスワードの漏洩に関する最近の研究では、フィッシング・サイトの見分け方や対応方法について一定の教育を受けていたとしても、巧妙に作成されたフィッシング・サイトへの誤入力を防止することがほとんど期待できないことを示す結果が発表されている。さらに、フィッシング・サイトを見分けるチェックポイントばかりに注意が集まり、逆に、そうしたチェックポイントを巧みに偽装したサイトにパスワードを誤入力してしまう頻度が高まったとの研究報告もある。こうした研究成果を踏まえると、対策3を選択し、仮にパスワードが漏洩したとしても攻撃者が他の利用者になりすますことが困難な新しい認証鍵共有方式を検討していくことが望ましいと考えられる。

われわれは、こうした方式として、デバイス等に記録した秘密情報とパスワードの2要素を用いた認証鍵共有方式を提案している。本方式では、2つの要素を用いて認証を行うため、攻撃者がパスワードだけを入手してもなりすましが困難であるほか、安全に共有した秘密鍵を使用して暗号通信を行うため、ユーザとサーバ間に攻撃者が割り込んで不正を行う攻撃に対しても耐性を有している。また、秘密情報については、正規のユーザが認証に成功するたびに更新されるため、秘密情報が仮に漏洩したとしてもその情報を無効化することができるという特徴を有している。

当面は、対策1や対策2を適切に講じることでパスワードの漏洩に対して一定の効果を期待できると考えられるものの、人間は間違えやすい生き物であり、うっかりミスによるフィッシング詐欺の被害をゼロにすることは困難である。そのため、パスワード等のユーザが直接入力する情報だけに安全性を頼る方式には限界がある。こうした問題を根本的に解決していくためには、長期的な視点に立ち、新しい方式を検討していく必要があると考えられる。各金融機関は、こうした方式に関する研究動向をフォローするとともに、その活用方法について検討することが必要であろう。

(3) パネル発表 3：生体認証について

小松は、生体認証の特徴とその活用、および生体認証における研究動向について、次のとおり発表を行った。

本人認証の手段は、パスワード等を用いた知識認証、トークンを用いた所持認証、個人の身体的・行動的特徴を用いた生体認証に分類されることが多い。これらの手段を比較すると、まず、本人の識別能力の観点では、知識認証や所持認証においては、パスワードのサイズを伸張する、あるいは、トークンに格納する秘密情報のサイズを伸張するといった対応によって、パスワードや秘密情報が適切に選択・管理されているという前提のもとで、他人を誤って本人と判定してしまう確率を低く抑えることができる。これに対し、生体認証においては、他人であっても類似した生体情報を有する個人が存在するという特徴があるほか、本人を誤って他人として拒否してしまうケースもあり、本人拒否の頻度を低く抑えようとすれば他人受入の頻度が高くなるというトレードオフの関係が存在するという特徴がある。そのため、他人受入の頻度を判定しきい値によって調節することができるものの、本人拒否の頻度を一定レベル以下に抑えることを考慮すると、他人受入の頻度は他の手段に比べて高まる傾向にあるとみられている。

運用上発生するヒューマン・エラーの観点で比較すると、知識認証では、パスワードを失念してしまう可能性があるほか、ユーザが比較的推定しやすいパスワードを選択してしまうという問題がある。また、所持認証では、トークンの紛失・盗難等の問題がある。一方、生体認証については、個人の身体的・行動的な特徴を利用するため、ユーザが何か特別な管理を実施する必要性が非常に低く、ユーザの状態が本人認証の実行可能性に及ぼす影響の度合いも低い。

このほか、システムとしてのセキュリティの強度という観点では、知識認証や所持認証では認証に利用するパスワードやトークンの情報を更新できるのに対し、生体認証では指紋等の身体的特徴を変更できない。そのため、システムに登録された生体情報（以下、テンプレートと呼ぶ）が漏洩した場合には、なりすましが発生する可能性があるという問題もある。

このように、各認証方式にはそれぞれ特徴があり、一長一短であることがわかる。そのため、各認証方式の特徴を適切に整理・理解したうえで、各認証方式の強みをどのように活用していくことができるかを検討することが重要である。生体認証については、今後適用分野が一層拡大していくとの見通しを示す調査結果もあり、とりわけ利便性が重視されるアプリケーションにおいて広く活用されていくのではないかとの分析結果がある。こうした見通しと、ヒューマン・エラーによる影響を受けにくいという特長を組み合わせて考えると、高齢者向けの認証方式として重要になっていくのではないかと考えられる。日本の総人口に占める 65 歳以上の人口割合は、40 年後には約 4 割に達するとの推計もあり、潜在的なニーズも大きいと思われる。

こうした点を踏まえると、金融機関が生体認証を今後も活用していくうえで、ま

ずは生体認証がパスワードやトークンを利用する方式に比べて、どのような点で優れているのかを理解しておくことが重要である。どのような生体認証の手法が望ましいかについては、各アプリケーションに応じた検討が必要であるが、例えば、判定しきい値の設定に必要となる各種の運用要件については、既に関連するガイドラインも整備されており、そうした文献を参照することができる。また、高齢者向けの金融サービスを検討する際には、生体認証の特長をどのように活用できるかについても検討しておくことが有用であろう。

生体認証におけるテンプレート漏洩の問題については、近年対策に関する研究が活発化している。例えば、指紋そのものではなく、秘密のパラメータで変換した値をテンプレートとすることでテンプレートの更新を可能とする方式や、提示された指紋等の情報を基に生成される秘密鍵を認証に利用する方式等が提案されている。金融分野では、現在 IC カードにテンプレートを格納して ATM における本人認証に利用しているが、そうした IC カード内のテンプレートを保護する技術の候補の 1 つとして、こうした技術の研究動向についてもフォローしていくことが重要であろう。

(4) パネル発表 4：暗号モジュールの耐タンパー性について

松本は、暗号モジュールの耐タンパー性の重要性、および、耐タンパー性に関する試験・認証制度と今後の課題について、次のとおり発表を行った。

暗号アルゴリズムを実装したソフトウエアやハードウエアは暗号モジュールと呼ばれており、IC カードや携帯電話等のデバイスに組み込まれて利用されている。当該モジュールには、暗号処理のための秘密鍵が格納されており、仮に攻撃者によってモジュール内部から秘密鍵が抽出・推定された場合には、暗号モジュールが偽造され、なりすまし等の不正行為につながりうる。そのため、暗号モジュールの機能を改変する攻撃や内部の秘密情報を抽出する攻撃に対する耐性である「耐タンパー性」の確保が重要になっている。

こうした暗号モジュールの耐タンパー性については、本シンポジウムの発表 2 において説明があったように、高度な知識・技術を有する第三者機関が試験し、その結果を認証する制度が整備されてきている。わが国においては、昨年 4 月から「暗号モジュール試験及び認証制度（JCMVP）」の運用が本格的に開始されている。JCMVP は、米国・カナダにおける暗号モジュールの試験・認証制度である CMVP（Cryptographic Module Validation Program）がベースとなっている。JCMVP では、暗号モジュールにおける 4 つのセキュリティ・レベルが設定されており、各レベルに応じたセキュリティ要求事項が JIS X 19790: 2007 に規定されている。そのため、暗号モジュールで保護すべきデータの重要度や使用環境に応じてセキュリティ・レベルを選択し、試験を受けることが可能となっている。平成 19 年 6 月に了承された「政府機関の情報セキュリティ対策のための統一基準」においては、暗号化や電子署名を実装する情報システムを調達する際に、JCMVP による認証を取得している暗号モジュールを

選択することが強化遵守事項として定められている。

ただし、JCMVP による試験・認証にはいくつかの課題が残されている。例えば、サイドチャネル解析に代表されるように、暗号モジュールに対する新たな解析手法の研究が進展しており、そうした攻撃への耐性評価が JCMVP において十分にカバーされているわけではない。サイドチャネル解析は、暗号モジュールにおける正規の入出力以外のチャネルから漏洩する情報が暗号処理の内容を決定する秘密鍵の値に依存するという現象に着目し、そうした情報を捕捉して秘密鍵を効率よく推定する手法である。CMVP においては、現在、サイドチャネル解析等の新しい解析手法に対応する方向で検討が進められており、JCMVP においても今後検討していく必要がある。

このように、まだ十分とはいえないが、10 年前に比べて暗号モジュールが一定の情報セキュリティを確保していることを確認可能となってきている。暗号モジュールを適切に利用していくためには、その潜在的な脆弱性を理解したうえで、暗号モジュールの情報セキュリティを客観的に把握するよう努めるべきである。金融分野においても、関連技術の研究動向をフォローするとともに、セキュリティ評価手法や対策等の研究成果を活用していくための方法を検討することが重要である。

(5) パネル発表 5：ウェブ・アプリケーションのセキュリティについて

高木は、ネットワークを利用した金融サービスを実現するシステムが抱える問題とその対応のこれまでの経緯や今後のあり方について、次のとおり発表を行った。

これまでのネットワークを利用した金融サービスを振り返ると、約 10 年前に、SET（Secure Electronic Transaction）や SECE（Secure Electronic Commerce Environment）等の専用ソフトウエアを利用した金融サービスが登場し、その後、専用の電話番号にダイヤルアップ接続してウェブ・ブラウザを利用する「ブラウザ・バンキング」が登場した。しかし、これらは、専用のソフトウエアのインストールや専用の設定を必要としたため、使い勝手の悪さから十分な普及には至らなかった。その後、現在主流となっているウェブ・アプリケーションによる SSL を利用したインターネット・バンキングが登場した。ウェブ・アプリケーションには、セキュリティに配慮した構築方法に関する標準規格が存在せず、各システム開発者独自の知識や技術の範囲内でセキュリティ対策が実施されており、その結果、脆弱なウェブ・アプリケーションが散在しているのが実情である。

インターネット・バンキングのシステムは、一般に、製品化されたソフトウエアと当該システムの開発者が独自に設計したソフトウエアを組み合わせることで実現されている。ソフトウエア製品に関する脆弱性については、脆弱性に関する情報の届出と流通の枠組みが整備され、平成 16 年 7 月から IPA に届出することが可能となった。一方、独自に設計されたソフトウエアに関する脆弱性については、当該サイトに固有のものであり、個々のサイト管理者やシステム開発者が各自のサイトの

脆弱性を把握したうえで対処していくことが求められる。しかし、各サイト管理者やシステム開発者のスキルが低いため、適切な対応が図られないケースが多いのが実情である。

こうした問題に対して、金融業界の過去の取組みにみられるように、ウェブ・ブラウザを使用せずに、インターネット・バンキング専用のソフトウエアを開発し、脆弱性が発見された場合には関係者で情報を共有して修正を加えていくというアプローチがある。本アプローチは、専用ソフトウエアをインストールするといった負担がユーザ側に発生するものの、口座開設時に通帳とともに当該ソフトウエアを顧客に渡すなどの方法によって適切に専用ソフトウエアを配付することができればフィッシング詐欺を防止できるという大きな利点があることから、今一度、専用ソフトウエアを用いる方式というのも一考の価値がある。

もう1つのアプローチは、安全なウェブ・アプリケーションの構築方法に関する標準規格を作成し、それに従うというものである。現在、ウェブ・アプリケーションの設計・実装のガイドラインの策定が経済産業省において進められており、本ガイドラインをベースとして標準規格の検討を行うことが考えられる。本ガイドラインでは、設計や実装の段階で生じる脆弱性を排除するための方法が具体的に記述される予定となっている。そのため、脆弱性への対策の有無を検査する際のチェックリストとして活用可能であり、検査にかかる負担が削減可能になることに加え、システム開発の発注者と受注者との間でセキュリティ上の問題発生に関する責任の所在をより明確にすることも可能になる。

現在策定中のガイドラインでは、フィッシング詐欺対策上重要な要件として、「システムが使用するURLのすべてにおいて、ドメイン名は1つとすること」、「サイト運営者とドメイン名保有者を一致させること」といった要件が記載される予定である。ただし、こうした要件が満たされていないインターネット・バンキングのシステムは少なくないのが実情である。そうしたシステムのユーザがフィッシング詐欺の被害を受ける可能性が考えられるだけでなく、フィッシング・サイトなのか本物のサイトなのかを見分ける方法を一般のユーザに周知していくうえで悪影響を及ぼすおそれもあると考えられる。

一方、フィッシング詐欺への技術的な対策として、われわれは、相互認証技術を利用した新しいプロトコルを開発し、このプロトコルの各ブラウザへの標準搭載を目標に現在活動を行っている。

ところで、ユーザの端末がスパイウエア等の悪意のあるソフトウエアに感染している場合には、そもそもどのような認証方式を採用していたとしても対策の実施は困難である。したがって、スパイウエア等に感染しないようにすることが必要であり、そうした対策の1つとしては、TPM（Trusted Platform Module）を利用する方法が挙げられる。TPMは、耐タンパー性を有するICチップであり、PC等に内蔵され、当該PCがスパイウエア等の不正なソフトウエアに感染しているか否かを自動的に検査するといった機能を実現するものとして検討が進められている。TPMを利用することで、例えば、ユーザのPCにスパイウエアが存在しないことの確認を行っ

たうえで、インターネット・バンキングのサイトへログインを認めるといった対応が可能になると考えられる。金融機関は、こうした技術的な対応の可能性についても検討していくことが有用であろう。

(6) 自由討議

上記のパネル発表の内容を受けて、次のとおりパネリストによる自由討議が行われた。

イ. 金融機関の情報セキュリティ対策の現状について

まず、岩下は、金融機関における情報セキュリティ対策について、最近、最も気になっていることは何かとパネリストに尋ねた。太田は、現在普及し始めている電子マネー・サービスのセキュリティについて懸念を示し、仮に何らかの問題が発生した場合においても適切に対応できる体制を整備することが一層重要になってきていると述べた。古原は、個々の金融機関が直面している情報セキュリティ上の問題や研究動向を金融業界内で共有することが必要となってきており、そうした情報共有体制の充実を今後どのように図っていくかが重要であると述べた。小松は、金融取引においては各種の個人認証方式が利用されているものの、採用に当たって各方式の評価が必ずしも十分とはいえないのではないかとの見方を示したうえで、PIN 認証と生体認証を横並びで比較・評価するなど、各方式の特徴を整理し、アプリケーションに応じた適切な方式を採用していくことが重要であると述べた。松本は、現行の IC キャッシュカードでは磁気ストライプのデータによる取引の実施も可能となっており、現時点では、相対的に偽造が容易な磁気ストライプ部分が攻撃対象となっているのではないかとの認識を示した。そのうえで、今後 IC チップによる取引が大勢を占めるようになれば、IC チップが次の攻撃対象となると予想されることから、そうした状況に備えてセキュリティ対策を講じておく必要があると述べた。高木は、ウェブ・アプリケーションにおける情報セキュリティ対策の取組みをみると、金融機関によって対応が区々となっているとの印象をもっているとの見方を示したうえで、安価に十分な対策を実施するための方法について検討することが求められると述べた。

ロ. 電子マネーのセキュリティの現状について

太田の発言を受けて、岩下は、電子マネーのセキュリティの現状について他のパネリストの見解を尋ねた。松本は、現行の電子マネー・システムについては、具体的な仕様が公開されていないため、システムが安全であるか否かを判断することが困難になっていると指摘した。そのうえで、センターを介さずに利用者間で電子マネーを譲渡するオープン・ループ型の電子マネー・システム等の次世代の電子マネー・システムにおいては、技術面での情報セキュリティ対策が一層重要になってくると考

えられるため、客観的な評価を受けた情報セキュリティ技術を採用していく必要性が高いと思われると述べた。また、太田は、通信コストの低下によってセンターでの不正取引の検知をより低いコストで実施できるようになってきていることに加えて、評価・認証制度の整備によってICカード等が一定のセキュリティを確保していることを確認可能となっており、そうした製品を利用することによって、安全性の高い電子マネー・システムをより安価に構築可能になってきていると説明した。そのうえで、こうした技術環境の変化を活用し、情報セキュリティ対策の高度化をどのように進めていくかが今後の課題であると指摘した。

ハ．脆弱性情報の取扱いについて

次に、岩下は、現状の脆弱性情報の取扱いに関する問題についてパネリストの見解を尋ねた。古原は、情報セキュリティ技術の専門家と金融業務の実務家が脆弱性やその対策に関する情報を共有するための場が必要であると述べた。小松は、脆弱性を内包し適切な対策が講じられていない情報セキュリティ技術が普及し、後に当該脆弱性が発見されて大きな被害が生じてしまうと、ユーザから当該技術が実用に耐えないものであると判断され、将来有望な技術であったとしても以後利用されなくなるおそれがあると説明した。こうした事態を避けるためには、脆弱性を発見した専門家が対策についても検討し、システム開発者が運用も含めて対策を講じる努力を行うことが重要であり、こうした取組みのなかでユーザに対して最低限もつべき知識を平易かつ正確に説明していくことが求められると述べた。

これに対し、太田は、発見された脆弱性が特定のソフトウエア製品に関するものか、あるいは、暗号プロトコルや汎用的な技術仕様に関するものかによって発見後の対応が異なり、製品の脆弱性の場合にはその情報を公表することによる社会的な影響も考慮する必要があると説明した。また、今回発表したAPOPの脆弱性の情報については、IPAに届出を行った後、関連するベンダー等が対策を講じるために必要な時間を考慮して、約10ヵ月が経過したところで詳細な攻撃方法を公表することとしたと説明した。これに関連し、高木は、IPAの脆弱性情報届出制度について、個々の製品等の脆弱性に関する情報の悪用を防ぐ目的で、修正パッチが公表されるまで原則非公開とする方針を採用しており、汎用的な技術仕様の脆弱性を対象としているわけではないと説明した。そのうえで、汎用的な技術仕様の脆弱性についても修正されるまで非公開にすべきであるとの意見もあるが、その場合には、当該脆弱性に関する情報の共有が遅れてしまうだけでなく、発見者が学会で発表する機会を逸してしまうという問題にもつながると指摘し、発見者の責任で公表することが必要ではないかとの見方を示した。

次に、岩下は、脆弱性の顕現化による影響が大きい製品・システムが対象となるケースについてパネリストの見解を尋ねた。松本は、脆弱性情報を公表する場合、修正パッチが存在せず対策を講じることができないまま被害が継続して発生する可能性があり、逆に脆弱性情報を公表しない場合には、当該脆弱性を発見した攻撃者に

よって脆弱性が悪用され続ける可能性があると説明したうえで、基本的にはケース・バイ・ケースで対応を判断すべきであるが、どちらかといえば脆弱性情報を公表していく方向での検討が望ましいのではないかとの見方を示した。これに関連し、小松は、脆弱性情報の公表が社会に与える影響を考慮したうえで、開示する対象者やその情報の範囲を慎重に検討していくことが必要であると述べた。高木は、脆弱性情報を他社に先駆けて入手したにもかかわらず外部に開示しなかった場合、当該脆弱性に関連する情報セキュリティ上の問題がその後発生し多大な損害を他の組織が被るというケースも今後想定されると説明した。そのうえで、そうしたケースでは、即時に情報を公表しなかったという点について責任を問われる可能性がある点を考慮すると、脆弱性情報をなるべく公表する方が望ましいのではないかと述べた。また、太田は、従来自動車業界では、自動車の欠陥等を隠蔽してしまうという体質が存在していたが、その後紆余曲折を経て、欠陥等が発見されればその情報を公表してリコールを行うという望ましい状況に変わってきていることを指摘し、情報セキュリティ分野における脆弱性情報の取扱いのあり方を検討する際にはこうした自動車業界の事例も参考になるのではないかと述べた。

ニ．まとめ

最後に、岩下は、本シンポジウムへの意見や要望、金融機関の情報セキュリティ対策全般等についてパネリストに意見を求めた。まず、本シンポジウムについて、太田と小松は、情報セキュリティの専門家と金融業務の実務家が認識を共有できる場として、今後もシンポジウムを継続して開催していってほしいと述べた。また、金融機関の情報セキュリティ対策に関して、古原は、フィッシング詐欺等への対策としてヒューマン・エラーを考慮したシステムの設計に関する検討が重要であると述べた。また、高木は、金融情報システムの設計・開発における発注者と受注者の責任範囲の明確化が一層重要になるとの見方を示したうえで、発注者となる金融機関も自社のシステムにおけるセキュリティ要件を示すだけでなく、脆弱性をできる限り組み込まないようなシステム仕様を提示するところまで踏み込んだ検討を行うことが望まれると述べた。情報セキュリティ技術の今後の研究課題について、松本は、情報セキュリティに関する攻撃と対策の「いたちごっこ」に対して今後技術的にどうアプローチするか、また、いたちごっこを止めることは可能なのかといった本源的な疑問についても研究を行うことが重要であり、今後検討してみたいと述べた。

(7) フロアからの主な質問

フロア参加者から、高齢者向けの本人確認の手段として生体認証が有用ではないかとの小松の説明に関連して、そうしたアプリケーションのなかには生体認証だけでは必ずしも十分な効果を発揮できないものも存在するのではないかとの質問があった。これに対し、小松は、パスワードを記憶したり、IC カードを所持したりする手

間が相対的に少ないという生体認証の特長を活用することができるアプリケーションの候補の1つとして高齢者向けのアプリケーションを紹介したと説明したうえで、個々のアプリケーションにおいてどのように生体認証を活用できるかについては別途検討が必要であると説明した。

6. 総括コメント

今井は、シンポジウム全体の内容を振り返ったうえで、次のとおりコメントし、シンポジウムを締め括った。

今回のシンポジウムでは、過去9回のシンポジウムのテーマやキーワードを基に、この10年でわが国の金融業界が直面してきた情報セキュリティに関連する環境の変化とそれに伴って発生した問題、金融機関の対応状況が整理され、今後の展望が示された。

情報セキュリティ上の問題は、実運用されているシステムにおいて問題となる前に学会で学術研究の成果として議論されるケースが多く、学会での研究動向をフォローしておくことはそうしたシステムの情報セキュリティ対策を検討するうえで重要である。日本銀行金融研究所の情報技術研究センターは、こうした問題意識のもと情報セキュリティに関する最新の研究動向をフォローし、シンポジウムでの議論を通じて、それらの実務へのインプリケーションを金融業界に還元する役目を果たしてきたといえよう。わが国の金融機関は、これまでの経験を踏まえ、情報セキュリティ技術に明るい人材の育成や業界内での適切な情報共有のあり方について検討を深めていくことが望まれる。情報技術研究センターにおいては、引き続き学界と金融業界のパイプとしての役割を担うとともに、本シンポジウムを継続して開催し、わが国の金融業界における情報セキュリティ対策に関する検討や活動をサポートしていくことを期待したい。