IMES DISCUSSION PAPER SERIES

金融分野における情報セキュリティ技術の
最新動向と今後の方向性
―第13回情報セキュリティ・シンポジウムの模様―

Discussion Paper No. 2012-J-2

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2012-J-2
2012 年 2 月

金融分野における情報セキュリティ技術の最新動向と今後の方向性

―第13回情報セキュリティ・シンポジウムの模様―

要　　旨

日本銀行金融研究所は、2011 年 10 月 28 日、「金融分野における情報セキュリティ技術の最新動向と今後の方向性」をテーマとして、第 13 回情報セキュリティ・シンポジウムを開催した。

金融機関は、情報システム全体や個々の取引の安全性・信頼性を確保するために、暗号技術、認証技術、ネットワーク技術等の情報セキュリティ技術を利用している。情報セキュリティ技術やそれを取り巻く環境は絶えず変化しており、情報システムの構築・運用にあたっては、こうした技術の動向や環境の変化を把握したうえでリスクを適切に評価・管理することが求められている。

今回のシンポジウムでは具体的なテーマとして、①最近急速に普及が進み、金融分野でも活用され始めている高機能携帯電話（スマートフォン）に関するセキュリティ、②インターネットの住所に相当する「IP アドレス」の枯渇に伴い導入が避けられなくなりつつあるインターネットの次世代仕様「IPv6：Internet Protocol version 6」の概要とその導入による影響、③通信の暗号化や認証等に利用される暗号アルゴリズムにおける世代交代の状況、④IC カード等を利用するペイメントシステムに関するセキュリティを取り上げ、これらの現状や今後の方向性等について講演や研究発表が行われた。

本稿では、本シンポジウムを構成するキーノート・スピーチ、3 件の講演、研究発表、総括コメントの概要を紹介する。

キーワード：情報セキュリティ技術、スマートフォン、IPv6、暗号アルゴリズム、サーバ証明書、IC カード、EMV 仕様

JEL classification: L86、L96、Z00

目　次

1. はじめに

日本銀行金融研究所は、2011 年 10 月 28 日、「金融分野における情報セキュリティ技術の最新動向と今後の方向性」をテーマとして、第 13 回情報セキュリティ・シンポジウムを開催した（プログラムは次頁のとおり）。

金融機関は、情報システム全体や個々の取引の安全性・信頼性を確保するために、暗号技術、認証技術、ネットワーク技術等の情報セキュリティ技術を利用している。情報セキュリティ技術やそれを取り巻く環境は絶えず変化しており、情報システムの構築・運用にあたっては、こうした技術の動向や環境の変化を把握したうえでリスクを適切に評価・管理することが求められている。

今回のシンポジウムでは具体的なテーマとして、①最近急速に普及が進み、金融分野でも活用され始めている高機能携帯電話（スマートフォン）に関するセキュリティ、②インターネットの住所に相当する「IP アドレス」の枯渇に伴い導入が避けられなくなりつつあるインターネットの次世代仕様「IPv6 : Internet Protocol version 6」の概要とその導入による影響、③通信の暗号化や認証等に利用される暗号アルゴリズムにおける世代交代の状況、④IC カード等を利用するペイメントシステムに関するセキュリティを取り上げた。上記①②③については専門家から各テーマの現状や今後の方向性に関する講演が行われたほか、上記④については当研究所スタッフの研究成果が発表された。

本シンポジウムのフロアには、情報セキュリティ技術にかかわる金融機関の実務家や官庁関係者、暗号学者、システムの開発・運用に携わる実務家や技術者等、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）。

【第 13 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「金融分野における情報セキュリティ課題」
松本 勉（横浜国立大学大学院教授）

●講演 1「スマートフォンのセキュリティ」
竹森敬祐（株式会社 KDDI 研究所研究主査）

●講演 2「IPv6 の導入におけるセキュリティ上の影響と対策」
衛藤将史（独立行政法人情報通信研究機構主任研究員）

●講演 3「暗号の世代交代や利用をめぐる話題から」
神田雅透（独立行政法人情報処理推進機構研究員）

●研究発表「IC カード等利用システムにおける情報セキュリティ」
発表 1「システムとしての新旧課題と対策」
廣川勝久（日本銀行金融研究所テクニカル・アドバイザー）

発表 2「新たに顕現化した攻撃（中間者攻撃）とその対策」
鈴木雅貴（日本銀行金融研究所）

●総括コメント
今井秀樹（中央大学教授）

（備考）プログラム中における各参加者の所属ならびに肩書きはシンポジウム開催時点のものである。

2. キーノート・スピーチ「金融分野における情報セキュリティ課題」

松本は、金融分野における情報セキュリティ上の課題と対応について次のとおり発表した。

(1) 金融機関の情報システムやその環境の変化

金融機関が管理・運用する情報システムは、これまで絶えず変化してきた。例えば、汎用技術を用いた分散系システムの利用、システムのオープン化・統合・共同利用、クラウドに代表されるアウトソーシングの進展といった変化のほかに、IC カードや生体認証等の新たな情報セキュリティ技術の導入が挙げられる。

こうした変化をまず技術的な観点からみると、安全性評価手法が十分に確立されていない先端技術が利用されているほか、パソコンの小型化や性能向上等によりこれまで現実的でなかった攻撃が顕現化する可能性が生じている。また、インターネットや外部システムと接続するケースが増加しており、自社システムと依存関係にある別のシステムの障害やセキュリティ侵害を通じて被害を受けるリスクが増大している。

次に管理・運用的な観点からみると、従来は情報システムにアクセスする端末が限られていたのに対し、情報システムのオープン化によりアクセスするユーザが多様化しており、攻撃を意図したアクセスに直面するリスクが高まっている。また、インターネット・バンキング等においては、パソコンやスマートフォン等の端末の管理はユーザに委ねられているため、適切に管理されていない端末との接続が問題となる。このほか、海外データセンターの利用や海外システムへの接続等を行うケースが増えており、当該国の規制・法令に対する配慮も不可欠になってきている。

(2) 金融機関に求められる対応

上記の課題を踏まえると、金融機関には次の 3 つの対応が求められる。1 つ目は、環境変化が金融機関の情報システムのリスクにどのような影響を与えるかを評価し、留意すべき環境変化を明確にすることである。その際、専門家にリスク評価を依頼することも考えられる。また、環境変化に伴って生じるリスクへの技術的対策が存在するもののコスト等の問題から実施が困難な場合には、これに代わる管理・運用面での対策を別途考える必要があるほか、より抜本的な対策への移行計画を検討することも求められる。このほか、クラウドの利用を含め、金融機関の情報システムが他の情報システムと依存関係にある場合には、そうした外部情報システムの障害等に起因する影響を排除・制御する仕組みや、障害発生時の対応・責任分担等を考えるために、情報システム間の相互依存性や影響度の評価方法を確立していくことも求められる。

2 つ目は、想定するリスクへの対応の必要性に関する意識を関係者間で共有しておくことである。金融機関の情報システムがオープン化した結果、関係者が多様化してきており、セキュリティ対策の実施や事業継続管理を行ううえでより多くの関係者を巻き込んでいく必要性が高まっている。特に、インターネット・バンキング等において、一般顧客の管理下にあるパソコンやスマートフォン等を端末として使用する場合には、端末の適切な管理の必要性に関する啓蒙活動が一層重要になる。

3 つ目は、情報技術に対する新たな脅威や脆弱性の顕現化に備え、想定される事象への対応方針を事前に検討しておくことである。こうした検討を行う際に、

金融業界が既に経験した事例や現在進行中の事例を参考することが有益である。例えば、1990 年代に行った暗号アルゴリズムの移行や、偽造キャッシュカード問題を契機に進められているキャッシュカードの IC カード化の事例等が挙げられる。また、学界における研究成果を参考にすることも考えられる。例えば、①1990 年代半ばに設計された特定の IC カードを用いたペイメントシステムや金融分野の業界標準に準拠した IC カードを利用したペイメントシステムへの攻撃が可能であることを実験により示した研究、②新たな脅威に対しても情報システムに大幅な修正を加えることなく対応可能とする技術に関する研究、③一定の条件が満たされる限り、計算機性能の向上や攻撃手法の高度化等の影響を受けずに安全性が保証される技術に関する研究が挙げられる。ただし、過去に類似の事例がないまったく新しい脅威が登場する可能性もあり、新たに対応方針を検討していかなければならないケースも考えられる。

(3) 求められる攻めの姿勢

金融機関ではさまざまなセキュリティ技術が導入されているが、競合他社が利用しているから乗り遅れないようにするために自社でも同じセキュリティ技術を利用するといった「受け身」の姿勢ではなく、金融機関がビジネスを展開するうえで自らの情報システムに必要とされると考えられるセキュリティ要件を学界や産業界に積極的に発信し、要件を満たす新しいセキュリティ技術を研究開発してもらったうえでそれらを活用するという「攻め」の姿勢を期待したい。

3. 講演 1「スマートフォンのセキュリティ」

竹森は、スマートフォンのセキュリティや金融サービス用のアプリケーションを開発する際の留意点等について次のとおり発表した。

(1) スマートフォンのセキュリティ

近年、個人や企業から注目を集めているスマートフォンは、電話機能を搭載したパソコンといっても差し支えない情報機器といえる。スマートフォンは、誰もがアプリケーション（「アプリ」と呼ぶ）の開発に携われるほか、インストールが容易という長所がある反面、OS の脆弱性や悪意のある動作を行うアプリ（「マルウエア」と呼ばれる）等のリスクが存在するためセキュリティ対策が必要である。スマートフォン用 OS は複数存在するが、多くの OS では実行中のアプリが他のアプリやデータをユーザの許可なく操作することを防ぐために、隔離した領域（「サンドボックス」と呼ばれる）内でアプリを実行するという対策

を講じている。そのため、サンドボックスの仕組み等に脆弱性が存在しない限りは、マルウエアが外部から侵入したとしてもその影響はサンドボックス内に留まり、OS が感染したり、他の正常なアプリの動作に影響を与えることはないと考えられている。しかしながら、アプリがマルウエアであるとは気付かずにユーザ自身がインストールしてしまう場合には、セキュリティ上の問題が生じる。以下では現在仕様が公開されておりオープンに議論し易い「Android[1]」を取り上げ、その安全性について説明する。

マルウエアは、次の 2 種類のマルウエアに大別できる。

1 種類目は、Android のサンドボックス独自の仕組みを悪用するマルウエアである。Android では、アプリをダウンロードする際、当該アプリが利用する端末の個々の機能や各内部データへのアクセスに関する許可（「パーミッション」と呼ばれる）をユーザに問い合せ、同意が得られた場合にインストールするという仕組みとなっている。このタイプのマルウエアは、こうした仕組みを悪用し、まず、利用目的を明示せずに個人情報へのアクセスやインターネット接続等のパーミッションをユーザに要求しておき、インストール後に当該パーミッションに基づく機能を利用し、端末内の個人情報の漏えい等を行っている[2]。

2 種類目は、必ずしもパーミッションを求めずにインストールされるが、OS の脆弱性を利用して当該端末の管理者権限の奪取を行うマルウエアである。このマルウエアにおいては、端末内のデータへのアクセスや端末のすべての機能（インターネット接続、メール送信等）の利用が可能になるほか、別のマルウエアを秘密裏にインストールすることも可能になる。こうしたタイプのマルウエアは、ユーザが通常利用するデータ領域（「ユーザ領域」と呼ばれる）ではなく「管理領域」にインストールされることもあり、元のマルウエアのアンインストールやユーザ領域のデータ初期化でも駆除が困難という特徴がある。

こうしたマルウエアに対して、Android の開発元である Google は、発見された脆弱性に対応したセキュリティパッチ（修正プログラム）を提供しているほか、同社が運営するアプリ配信サイト「Android Market」に掲載されたアプリがマルウエアであると判明した場合には、当該サイトから速やかに削除するという対応や、ダウンロードしたユーザへは駆除ツールを提供するなどの対応が採られている。

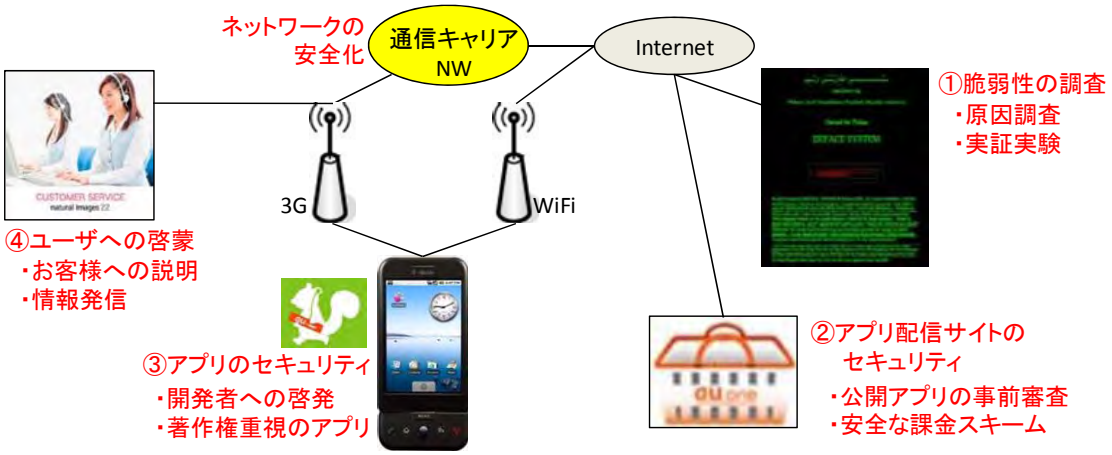
---

[1] Android は、Google が提供するスマートフォンやタブレット端末用のプラットフォームであり、厳密には、オープンソース系の OS である Linux、ミドルウェア、複数の主要なアプリケーションのパッケージから構成されている。

[2] 例えば、①インターネット・バンキング用のアプリやマルウエア対策アプリと見せかけて、個人情報や端末情報等を漏洩させるマルウエア、②通話内容を音声ファイルとして記録・漏洩させるマルウエア等が確認されている。

(2) セキュリティ向上に向けた取組み

例えば KDDI（株）では、ユーザがスマートフォンを安心して利用できるように、次のような取組みを行っている（図表 1 の①～④参照）。



図表 1. KDDI（株）の取組み（発表資料を基に作成）

① Android OS の脆弱性やマルウエアの状況について継続的に調査している。

② KDDI（株）が提供しているアプリ配信サイトでは、掲載前に各アプリのセキュリティを検証しているほか、開発者から検証の申請があったアプリについては個別により厳密な検証を行ったうえで合格証を当該アプリに与えている。

③ アプリ開発者への啓発活動として、安全なアプリを開発する際の留意点や上記のアプリ検証結果について情報提供を行っているほか、アプリが個人情報等を外部に送信する際はユーザに承認を求めるよう推奨している。

④ ユーザへの啓発活動として、アプリ配信サイト等においてアプリ（マルウエアのケースを含む）のインストールは自己責任であることを注意喚起するとともに、そうした説明をユーザが理解したことを確認するプロセスを設けるといった手順を経るように努めている。

このほか、通信事業者を含むスマートフォン・ビジネスにおけるサービス提供者とその利用企業、関連団体等が協調し、スマートフォンの安全な利活用を図り普及を促進するために「日本スマートフォンセキュリティフォーラム」を設立し（2011 年 5 月）、アプリ開発やスマートフォンの業務利用に関するセキュリティ・ガイドラインの作成や端末の安全性向上のための検討等を行っている。

(3) スマートフォンを利用する際の留意点

こうした状況において、ユーザがスマートフォンを安全に利用するうえでの留意点と金融機関が金融サービス用アプリを開発する際の留意点について説明する。

まず、ユーザに対しては、①OS ベンダや通信事業者等が提供する信頼できるアプリ配信サイトに掲載されたアプリの利用、②アプリの注意書き等に基づいたリスク判断の実施、③端末やアプリへの迅速なセキュリティパッチの適用といった点に留意する必要がある。

スマートフォンを用いたバンキングサービスを提供する金融機関に対しては、次の 3 つの留意点が挙げられる。①管理者権限を奪取された端末では、アプリの動作や処理データはすべてモニタされる可能性があるため、スマートフォン自体の ID（「端末 ID」と呼ばれる）やユーザ ID 等の認証子が盗聴・改ざんされるリスクに注意を払う必要がある。例えば、認証子の暗号化、アプリの解析を困難にする実装方法の採用、あるいは管理者権限が奪取されている端末においてはアプリを起動させないようにする措置の導入といった対応が考えられる。また、②複数のユーザによる端末の共同利用や紛失・盗難端末の第三者による利用への対応も課題となる。対策としては例えば、アプリ使用の度に暗証番号を入力する等のユーザ操作を求めるという対策や生体認証等の別の認証手段を併用するという対策等が考えられる。このほか、③スマートフォンはパソコンに比べると物理的に表示画面が狭く、接続したサーバのアドレス（URL[3]）が長い場合には URL の一部分しか一画面に表示されないため、一画面に表示される部分が正規サーバの URL に見えるような偽サーバにアクセスさせるというフィッシング詐欺への対策が課題となっている。そこで、URL 全体の表示や暗号を利用したサーバの正当性確認技術の利用といったサーバ認証を安全に実施するための配慮が求められる。しかし、既存の技術でこうした課題の全てを解決することは難しく、限界を踏まえた運用に留意する必要がある。

4. 講演 2「IPv6 の導入におけるセキュリティ上の影響と対策」

衛藤は、インターネットの根幹をなす仕様の次世代版「IPv6（Internet Protocol version 6）」の安全性や導入時の留意点について次のとおり発表した。

[3] URL（Uniform Resource Locator）は、インターネット上に存在するデータの場所を示す記述方法（例：http://www.○○○.co.jp）。

(1) IP アドレスの枯渇問題とその対応

インターネット・バンキング等におけるインターネット上の通信では、送信者（例：ユーザのパソコン）や受信者（例：金融機関のサーバ）を識別するために各々に割り当てられたインターネット上の住所（「IP アドレス」と呼ばれる）が用いられる。現在主流の IP アドレスは、「IPv4（Internet Protocol version 4）」において規定されているものであるが、パソコンや携帯電話等の普及に伴い、利用されている IP アドレスの数は年々大幅に増加している。IPv4 で扱うことが可能な IP アドレスの数は約 43 億個であり、仮に、すべての IP アドレスをパソコンやサーバ等に割り当て終わると、新規のパソコンやサーバ等に対し新たに IP アドレスを割り当てることができず、これらの機器がインターネットに接続することができないという状況に陥る。

こうした問題（「IP アドレスの枯渇問題」と呼ばれる）は 10 年以上前に指摘されており、技術面や運用面の対策が検討・実施されてきた。例えば、IPv4 の延命策として、1 つの IP アドレスを複数のパソコン等で共同利用する技術や利用しなくなった IP アドレスを回収し再割当てを行うという運用が行われているほか、根本的な解決策として、340 澗[4]（約 3.4×10^{38} 個）の IP アドレスが利用可能な新たな仕様である IPv6 の策定・導入が行われている。これまでは、通信相手との相互接続性の確保のハードルが低い IPv4 の延命策が主に利用されてきたが、近年、IP アドレスの枯渇が一部で現実化し、その影響が無視できなくなりつつあることから、IPv6 の導入が徐々に本格化してきているという状況である。

(2) IPv6 の安全性

これまで IPv6 を導入すれば IPv4 よりも安全性が向上するという認識が一般的であったが、現時点ではそうした認識が必ずしも正しいとは言えないことが明らかになっている。独立行政法人情報通信研究機構が実施した IPv6 の安全性評価によれば、IPv4 と IPv6 の両仕様に共通の脆弱性だけでなく IPv6 の仕様に固有の脆弱性が存在することがわかったほか、IPv6 の特定の実装方法にも脆弱性が存在することがわかった[5]。こうした脆弱性の中には、サービス妨害攻撃や通信の盗聴が IPv4 の場合よりも容易になるものも存在する。そこで、IPv6 に関する技術検証を行うために、通信機器メーカやパソコンメーカ等が参加する「IPv6 技術検証協議会」が 2010 年 7 月に設立された。

---

[4] 澗（かん）は、数の単位であり 10^{36} を表す。

[5] こうした IPv6 の脆弱性のほかに、IPv4 よりも安全性が向上する根拠の 1 つとされてきた「IPsec（Security Architecture for Internet Protocol）」への対応が、省リソースの機器への配慮から、必須項目からオプションに変更になった点も挙げられる。なお、IPsec は、SSL よりも物理層に近い層における暗号化通信を行うための仕様である。

同協議会のこれまでの活動では、深刻な影響を及ぼすおそれのある 24 通りの攻撃シナリオを抽出したうえで、市販の製品を用いて構築した検証用ネットワークにおいて検証実験が行われたほか、成功した攻撃シナリオへの対策の検討とその有効性の確認が行われている。各攻撃シナリオの検証結果は、①攻撃を防止する仕組みが存在する、あるいは、実装方法や運用により攻撃が回避可能であり、検討対象のすべての製品で攻撃を防止できたケース（6 シナリオ）、②実装方法によっては攻撃が成功する可能性があり、検討対象の一部の製品で攻撃が成功したケース（13 シナリオ[6]）、③実装方法の如何に関わらず必ず攻撃が成功するため、検討対象のすべての製品で攻撃が成功したケース（5 シナリオ[7]）となっている。同協議会の今後の活動としては、より大規模な検証用ネットワークを用いた検証実験の実施や IPv6 の脆弱性に関する更なる検証が考えられている。

(3) IPv6 導入における留意点

上述したように、IPv6 には IPv4 と同様の脆弱性のほかに IPv6 に固有の脅威も存在しており、IPv6 自体や IPv4 との相違点を把握したうえで運用することが重要である。また、IPv6 への移行期には、IPv4 と IPv6 の両方を併用するネットワークを構築・運用する必要がある。IPv4 と IPv6 の併用期間は想定以上に長期化することも考えられるが、こうした環境下での運用ノウハウが十分に蓄積されていない点にも留意が必要である。さらに、最近では IPv6 に対応した端末やネットワーク機器が広まりつつあり、IPv4 のみのネットワークのつもりで管理していても、各端末やネットワーク機器の設定によっては管理者が意図しないかたちで IPv6 の通信が行われ、そうした通信を攻撃に利用される可能性があることにも留意が必要である。

このように IPv6 の安全性上の検討事項は残っているものの、企業等が IPv6 を導入する必要性についてみると、対外接続するシステムについては、IP アドレスの枯渇に伴い IPv6 の導入が避けられない状況になりつつあるといえる。他方、対外接続しないシステムについては、当面、IPv4 のまま運用される可能性がある。しかし、長期的にみれば、調達可能な製品の制約等もあってすべてのネッ

---

6 例えば、元のデータを細かく分割して送信し受信者が再構築するという処理においては、特定のデータのみを大量に送信すると受信者（サーバ等）はデータの再構築のために大量のリソース（メモリや計算資源）を消費し、OS 等が正常に動作しなくなる可能性がある。対策としては、再構築のために割くリソースに上限を設けるという方法が検討されている。

7 例えば、経路情報をネットワーク上の機器に伝えるメッセージ（「RA＜Router Advertisement＞」と呼ばれる）を悪用することで、通信データが攻撃者の端末を必ず経由するように経路を改ざんし、通信データを盗聴するという攻撃が挙げられる。対策として、RA を送信した端末を認証するという方法や第三者端末が送信した RA を受け付けないという方法が検討されている。

トワークやシステムが IPv6 に移行すると考えられるため、どのように移行を進めるかについてあらかじめ検討しておくことが有用である。

5. 講演 3「暗号の世代交代や利用をめぐる話題から」

神田は、暗号アルゴリズムの世代交代の状況や効率的なセキュリティ対策について次のとおり発表した[8]。

(1) 暗号アルゴリズムの世代交代の最新状況

暗号アルゴリズム（「暗号」と呼ぶ）は、計算機の性能向上や解読技術の進展により安全性が経年劣化するため、時の経過に伴ってより安全な暗号への移行が求められる。しかし、移行した場合のメリットや移行しなかった場合のデメリットを情報システムの管理者が実感しづらいため、安全性が低下したという学界の警鐘だけでは移行が進みにくい。こうしたなか、米国立標準技術研究所（NIST：National Institute of Standards and Technology）は、2005 年に、当時主流であった暗号（具体的には、2-key TDES、鍵長 1,024bit の RSA、SHA-1）の安全性低下を受けて、政府系情報システムにおけるこれらの使用期限を 2010 年末と設定した。この NIST の決定を受け、暗号の利用企業等は、2010 年末までに利用する暗号を移行すべきではないかという認識を強めた（「暗号アルゴリズムの 2010 年問題」と呼ばれる）。その結果、国際標準や規格の次世代暗号への対応や、国際標準化団体等における移行計画策定、次世代暗号に対応した製品の開発の本格化につながった。

他方、2011 年現在、次世代暗号への移行が完了していない情報システムも多数存在する。こうしたなか、NIST は、暗号の安全性が低下する速度が 2005 年時点の予測ほどは速くはなかったことを受けて、アプリケーションによっては利用を継続しても実害が発生するリスクが少ないとして、暗号の使用期限を暗号の用途に応じて一部修正した。例えば、使用期限を 2010 年末と設定されていた 2-key TDES は、別の対策を併用する等により解読リスクを自ら制御できるのであれば、データ暗号化の用途には 2015 年末まで利用可能であり、過去に生成されたメッセージ認証子[9]を検証する用途には 2015 年以降も利用可能であると修正されている。なお、わが国では、2008 年に、政府系情報システムにおける暗号の利用について、2013 年度までに鍵長 1,024bit の RSA と SHA-1 のほかに、次世代暗号（鍵長 2,048bit の RSA や SHA-256 等）にも対応させるという指針が策定されている。

---

[8] 詳細は、独立行政法人情報処理推進機構[2011]と CRYPTREC[2011]を参照。
[9] メッセージの改ざんの有無を検証するためのデータ、または、その暗号技術。

次世代暗号への移行は、安全性の低下した暗号の解読リスクを管理する問題であり、解読リスクを踏まえて移行完了時期を設定することが重要である。

(2) わが国の電子政府推奨暗号リストの改訂

暗号に関するもう 1 つの動向として、わが国における「電子政府推奨暗号リスト」の改訂が挙げられる。同リストは、電子政府での利用が推奨されている暗号（「電子政府推奨暗号」と呼ばれる）を掲載しており、2003 年に 10 年間は安心して利用可能であると期待されるという基準をもとに作成された。現在、2012 年度中に次期リストを完成させるスケジュールで CRYPTREC[10]が改訂作業を行っている。

次期リストの特長は、次世代暗号への移行を意識した構成になっている点である。現行リストが電子政府推奨暗号を掲載した単一のリストであるのに対し、次期リストは、①十分な安全性と利用実績がある暗号を掲載する「電子政府推奨暗号リスト」のほかに、②十分な安全性はあるものの利用実績がなく、今後、電子政府推奨暗号に昇格する可能性のある暗号を掲載する「推奨候補暗号リスト」、③安全性低下により用途が互換性維持に制限される暗号を掲載する「運用監視暗号リスト」、④上記①～③のリストに関する参考情報や推奨事項を提供する「リストガイド」から構成される予定である。

なお、次期リストについては、関係者へのアンケート結果等を基に国産暗号の利用促進という観点も踏まえて検討が進められている。

(3) 効率的なセキュリティ対策

次世代暗号への移行のような先端的な対策だけでなく、システム全体の安全性を向上させるためには足元の課題への対策も重要である。具体的には、インターネット・バンキング等において被害が発生しているフィッシング詐欺への対策を優先することが望ましい。

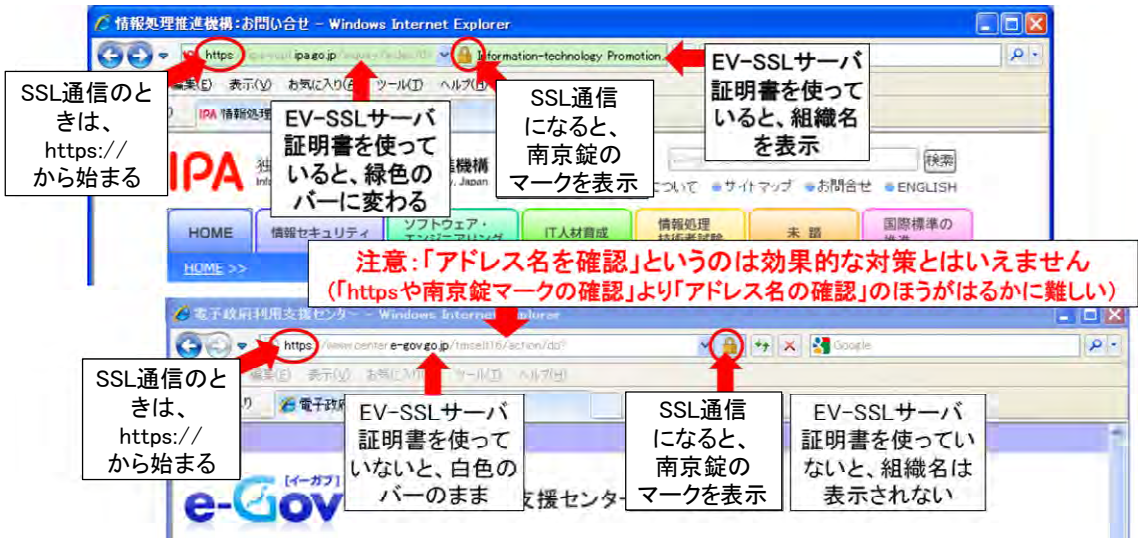
フィッシング詐欺等への対策として、サーバの正当性確認等を行うためのデータ（「サーバ証明書[11]」と呼ばれる）を金融機関のサーバは提供しているが、ユーザサイドの知識不足から必ずしもこれが活かされていないケースがあることがわかっている。例えば、サーバの設定ミスにより当該サーバの正当性を確認できない状態にあったにも関わらず多数のユーザがこれを気にすることなく当該サーバを利用したという事例が発生している。そこで、ユーザへの啓蒙活動を一層充実させるために、次の点に留意することが考えられる。

---

10 CRYPTREC（Cryptography Research and Evaluation Committees）は、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装方法・運用方法を調査・検討する委員会。

11 インターネット・バンキング用のサーバ等の正当性確認のほかに、当該サーバとの暗号通信用の鍵を共有するためのデータ。

まず、サーバ証明書の 1 つである「EV SSL 証明書」を利用する際に、同証明書は企業等の実在確認が行われている点で信頼性が高いことから、ブラウザでの表示でも、通常のサーバ証明書を利用した場合とは信頼性が異なることを強調して説明することが有用である。また、ユーザ端末とサーバが暗号通信（「SSL 通信」と呼ばれる）を行う際は、URL の先頭が「https://」となるほか、「南京錠」が表示されることを説明することも重要である（図表 2 参照）。また、インターネット・バンキング用サーバにおいて、委託企業宛てに発行された EV SSL 証明書を利用している金融機関が存在するが、当該金融機関宛ての証明書を利用することが望ましい。仮に、委託企業宛ての証明書を利用する場合には、その旨を明記することが求められる。こうした説明をインターネット・バンキングのログインページ内に掲載することで、ユーザの目に触れる機会が高まり、啓蒙の効果が大きくなると考えられる。このほか、金融機関による技術的対策としては、ワンタイム・パスワード[12]や乱数表の導入、サポート切れの OS やブラウザからの接続の拒否等も有用であると考えられる。



図表 2. サーバの正当性確認のポイント（発表資料を基に作成）

6. 研究発表「IC カード等利用システムにおける情報セキュリティ」

(1) 発表①「システムとしての新旧課題と対策」

廣川は、IC カードやモバイル機器を利用するペイメントシステムにおける新旧課題とその対策について、次のとおり発表した。

12 ワンタイム・パスワードは、パスワードの漏えいへの対策技術であり、本人確認において 1 度しか利用できないようにした使い捨てのパスワード。例えば、1 分毎に更新される 6 桁の数字を表示するハードウエア・トークンをユーザに配付しておき、ユーザがログインを行う際に、同トークンに表示されている値をワンタイム・パスワードとして入力させる方法がある。

イ．リテールペイメント・システムにおけるICカード等の利用

預貯金者等のユーザが所持するICカードやモバイル機器と、加盟店や金融機関の支店等に設置された端末を利用したリテール向けのペイメントシステム（「IC カード等利用システム」と呼ぶ）が普及してきている。そもそもICカードは、磁気カードの偽造や不正使用への対策として導入された。磁気カードと比較した場合のICカードの特長として、内部で暗号処理を実行可能であるため、カードの真正性確認や本人確認をより厳格に実施可能であることと、当該取引にカードが関与したことを示す暗号情報（「AC：Application Cryptogram」と呼ばれる）の生成が可能であることが挙げられる。

また、ICカード等と端末間のインタフェースには、ICカードと端末の端子を直に接触させる接触型と無線通信を利用する非接触型がある。非接触インタフェースを利用する場合、取引時にICカード等を取り出して端末に挿入する必要がなくなるため、接触インタフェースよりもユーザの利便性が向上する。しかし、非接触インタフェースは、通信を盗聴される可能性が相対的に高くなるほか、IC カード等の所持者が意図しない状態で第三者に当該カード等を利用される可能性があるなど、固有のリスクが存在する。海外をみると、そうしたリスクによる被害を抑えるために、1回の取引の上限金額を2,000～3,000円程度に設定しているケースや、接触インタフェースの場合よりも安全性の高い暗号アルゴリズムを採用しているケースがある。

ロ．システムの安全性

ICカード等利用システムの安全性を考えるうえでは、ICカード等と端末間のインタフェースに応じたリスクのほかに、利用する暗号アルゴリズムの安全性と、当該アルゴリズムをハードウエアやソフトウエアに実装した「暗号モジュール」の安全性に依存したリスクも存在する。暗号アルゴリズムに起因するリスクに対しては、IC カード等利用システムに関する業界標準の策定・管理を行っているEMVCoの取組みが参考になる。EMVCoは、推奨する暗号アルゴリズムや鍵長を示しており、例えば、接触インタフェースを利用する場合には、安全性の高い暗号アルゴリズムであるAESをオプションとして追加しているほか、RSA の鍵長の使用期限について毎年見直しを行っている。また、非接触インタフェースを利用する場合には、より短い鍵長でRSAと同等の安全性を達成可能な楕円曲線暗号やSHA-1よりも安全性が高いと期待されているSHA-3の導入について検討を行っている。暗号モジュールに起因するリスクに対しては、EMVCoの型式認定や「暗号モジュール試験及び認証制度」等の暗号モジュールの安全性を試験・認定する既存の制度を利用することが考えられる。

ハ．中間者攻撃の顕現化

上述したリスクのほかに、近年、IC カード等利用システムにおいて新たな攻撃が顕現化する可能性があることが複数の研究グループによって指摘されている。これらの攻撃はいずれも、IC カードと端末の間に「攻撃用装置」を挿入し、通信路上のデータを盗聴・改ざんすることで、不正な取引を試行するというもの（「中間者攻撃」と呼ばれる）である。

こうした中間者攻撃を防止するために、例えば、1980 年代前半にフランスで利用されていた公衆電話における偽 IC カードへの対策を利用することが考えられる。当時フランスでは、外部の装置と通信するためのケーブルが付いた偽 IC カードを排除する目的で、公衆電話内部に IC カードを取り込んだ後にカード挿入口をシャッターで閉じるという構造を採用していた。こうした偽 IC カードによる攻撃が顕現化しなかったためにこの構造は普及しなかったが、指摘された中間者攻撃への対策として、このような技術的対策を講じることが考えられる。また、仮に技術的な対策が不十分な状況で運用を続ける場合には、取引金額の上限を下げる等の運用面での対策を講じることが考えられる。

ニ．より広い視点からの情報セキュリティ対策

IC カード等利用システムには、さまざまなリスクが存在しうるが、広い視点から情報セキュリティ対策を考えていく必要がある。その際に参考となりうる情報として、IC カードの利用で先行する欧州の事例を紹介する。欧州の単一ユーロ決済地域（SEPA：Single Euro Payments Area）では、IC カードの普及率が 8 割を超えており、ATM 関連の不正使用やスキミング被害の大幅な縮小に成功している。そのうえで IC カード化進展後の課題を「Mature Chip Environment における課題」として検討している。そこでは、同地域で発行された磁気併用 IC カードの磁気情報を利用して同地域以外で行われる不正利用の防止やインターネット環境における不正取引の防止等が課題とされている。

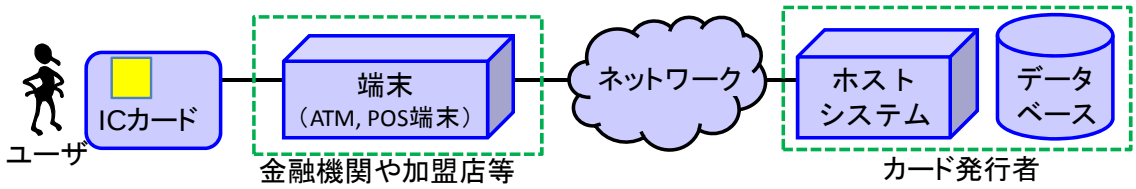
不正取引への対策には、技術的なものと運用によるものがあるが、技術的対策については技術進歩に対応してアップデートできるよう移行計画を検討することが求められる。他方、運用による対策については、技術的対策によって確保できるセキュリティ・レベルの実情に合わせて考えることが求められる。IC カード等利用システムを含め金融情報システムは、ビジネスの要件や社会ニーズの変化や技術進歩といった環境変化の影響を受けるため、そうした変化に対応して利便性と安全性のバランスを常に確保していくことが重要である。

(2) 発表②「新たに顕現化した攻撃（中間者攻撃）とその対策」

鈴木は、鈴木・廣川・古原[2010]に基づき、IC カード等利用システムへの中間者攻撃とその対策について、次のとおり発表した。

イ．EMV 仕様における取引

金融取引用 IC カードを利用したペイメントシステムには IC カードと端末に関する業界標準「EMV 仕様」が存在し、国内外において広く利用されている。同仕様では、ユーザが所持する IC カードと加盟店等に設置された端末が取引時に通信を行い、必要に応じて IC カードが端末経由でカード発行者のホストシステムと通信を行うというシステムを想定している（図表 3 参照）。



図表 3．EMV 仕様が想定する IC カード利用システムの全体像

同仕様が用意しているセキュリティ機能を利用した取引では、まず、取引に利用される「IC カードの真正性確認」とカードを提示した「ユーザの本人確認」が行われる。そのうえで、これらの結果や取引金額・日付といった「取引データ」等を基に当該取引を承認するか否かが決定される。この決定に際しては、取引時にホストシステムがリアルタイムに決定を下す「オンライン取引照会」とホストシステムに照会せずに端末が取引の可否を決定する「オフライン取引照会」の 2 つの方法が用意されている。

また、本人確認については、複数の方法が用意されている。例えば、暗証番号（PIN：Personal Identification Number）を利用する方法には、ユーザが端末に暗証番号を入力した後、当該入力値を受信したカードが照合を行う「オフライン PIN 認証」と、当該入力値を受信したホストシステムが照合を行う「オンライン PIN 認証」がある。

ロ．中間者攻撃の研究事例と対策

こうした EMV 仕様が想定するシステムに対する 3 種類の中間者攻撃（「中間者攻撃 1～3」と呼ぶ）が海外の研究者により指摘されている。いずれの攻撃も正規の IC カードと端末間に攻撃用装置を挿入し、通信路上のデータを盗聴・改ざんするタイプであり、各攻撃の概要とその対策は次のとおりである。

（イ）中間者攻撃 1 とその対策

中間者攻撃 1 は、本人確認としてオフライン PIN 認証を想定し、攻撃者は盗取した正規の IC カードと攻撃用装置を用いる。本人確認の際、攻撃者は、端末に任意の PIN を入力した後、カードに送信される当該入力値を攻撃用装置で遮断したうえで認証成功のメッセージを偽造し端末に返信する。同メッセージを受信した端末は、認証が成功したと判断するため攻撃が成功する可能性がある。

同攻撃では、カード内で本人確認が行われていないにも関わらず、端末はカードが本人確認を実施したと認識しており、カードの認識と端末の認識の間に齟齬が生じている。そのため、カードと端末内に記録された本人確認のログを利用して、こうした齟齬の有無を確認する仕組みを導入することで同攻撃を防止可能となる。なお、この対策を実施するためには、ログ自体や確認結果の改ざんを防止するために、高度な暗号処理が可能な IC カード、または、取引時にホストシステムへの接続が必要となる。

（ロ）中間者攻撃 2 とその対策

中間者攻撃 2 は、攻撃用装置が取り付けられた正規の端末を正規のユーザが利用する状況を想定している。同攻撃では、ユーザが入力する PIN を盗取した後（フェーズ 1）、当該ユーザの IC カードも盗取したうえで本人になりすまして不正な取引を試行する（フェーズ 2）。フェーズ 1 では、IC カードと端末が本人確認方法の決定を行う際、PIN が暗号化されずに IC カードに送信されるタイプのオフライン PIN 認証が選択されるように攻撃用装置で通信路上のデータを改ざんする。その後、ユーザが入力した PIN が暗号化されずに IC カードに送信されるため、攻撃用装置を用いて通信路上で当該 PIN を盗取する。フェーズ 2 では、盗取した IC カードと PIN でなりすますため、攻撃用装置は不要となる。

同攻撃ではデータの改ざんが行われるため、データの改ざんを検知した場合には本人確認を実施せずに取引を中止する等の取引フローを追加することが対策となる。

（ハ）中間者攻撃 3 とその対策

中間者攻撃 3 は、ある店舗（店舗 1）に設置された偽端末を正規のユーザが利用し、そのタイミングで、別の店舗（店舗 2）に設置された正規の端末で攻撃者が偽カードを使用するという状況を想定している。この攻撃は、偽端末と偽カードを利用して、店舗 1 に居るユーザのカードを店舗 2 の正規の端末と通信させており、ユーザは店舗 1 への支払いを意図しているにもかかわらず、実際には店舗 2 に居る攻撃者の取引への支払いを行うという状況になる。

同攻撃では、店舗 2 の端末から出力されるレシートに印字されたカード番号と偽カードの券面に印字されたカード番号が一致しない可能性が高いことから、店舗 2 のスタッフがこれらのカード番号を突合すること等で同攻撃を防止可能になる。

ハ．金融機関への留意点

上述したように、学界等では IC カード等利用システムに対する攻撃の可能性が指摘されていることから、金融機関は、少なくともこうした攻撃が自社システムに影響を与えるか否かを評価することが求められる。また、今後も金融機関が利用する情報システムに対する新たな攻撃が現れてくると予想されるため、学界等からの情報収集やそうした情報を基にした自社システムへの影響評価や対策の検討を継続的に行うことが重要である。

7．主な質疑応答

スマートフォンのセキュリティについて**フロア参加者 A** から、金融向けのアプリにおいて、利便性向上のためにスマートフォンの端末 ID を利用する場合、セキュリティ上の問題は発生するかとの質問が寄せられた。これに対して、**竹森**は、そうしたアプリが解析され、偽造された端末 ID で使用される場合には問題が発生する可能性があると説明したうえで、アプリを開発する際は、アプリの動作等の解析を困難にする実装方法を採用することが望ましいこと、同時に、攻撃者が時間を掛ければいずれ解析してしまうという脅威は無くならないことを補足した。また、**フロア参加者 B** から、スマートフォンにおいてもウイルス対策ソフトを利用すれば、パソコンと同程度の安全性を確保できるのかとの質問が寄せられた。これに対して、**竹森**は、スマートフォンではウイルス対策ソフトも他のアプリと同様にサンドボックス上で動作するため、他のアプリの監視に制約があり、マルウエアを検知できるとは限らないと説明した。そのうえで、仮にマルウエアを検知したとしても自動的に削除することはできず、検知したマルウエアの削除をユーザに促す画面を表示するにとどまり、ユーザが削除を指示するまでの一瞬のタイミングで個人情報が漏えいする可能性があると補足した。

暗号アルゴリズムの移行について**フロア参加者 A** から、現在、電子政府推奨暗号リストの改訂作業が行われているが、改訂版のリストがさらに改訂される時期はいつ頃になるのかとの質問が寄せられた。これに対して、**神田**は、改訂版の作成作業は前回同様 10 年間は安心して利用可能という考えが前提となっているため、その次の見直しは 10 年後と予想されるが、仮に、10 年経つ前に新し

い解読手法が発見され、リストに掲載された暗号の安全性が急激に低下した場合には当該暗号の扱いを見直す可能性もあると説明した。また、フロア参加者Ｃから、EMVCo ではどのような方針で RSA から楕円曲線暗号への移行を行う予定かについて質問が寄せられた。これに対して、廣川は、非接触インタフェースを利用したシステムに先行して普及している接触インタフェースを利用したシステムでは、RSA が利用されているという現状を紹介したうえで、EMVCo では、まず、楕円曲線暗号を普及させるために、これから新規システムの構築が進む非接触インタフェースを利用したシステムにおいて楕円曲線暗号を採用し、ある程度楕円曲線暗号が普及した段階で、接触インタフェースを利用したシステムにおいても楕円曲線暗号に対応させるという方針が示されていると説明した。

IC カード等利用システムへの中間者攻撃 1 についてフロア参加者Ｄから、本人確認の結果を容易に偽造することができるのかとの質問が寄せられた。これに対して、鈴木は、端末から IC カードに対して送信されるオフライン PIN 認証の実行命令に対して、命令が正常に終了したという固定のメッセージを偽造して端末に返信すればよいだけであり、IC カード内の暗号鍵を盗取する等の処理は不要であると説明した。

8. 総括コメント

今井は、シンポジウムの内容を振り返ったうえで次のとおりコメントを行い、シンポジウムを締め括った。

今回のシンポジウムでは、「金融分野における情報セキュリティ技術の最新動向と今後の方向性」というテーマに基づき、金融機関が利用する可能性がある新しい技術、あるいは、従来から利用している技術ではあるが注目される新たな動向が生じているものが取り上げられた。各技術の第一人者の講演により、それぞれの動向や金融分野への影響を把握することができ有益であった。

最近のサイバー攻撃の傾向として、①定義ファイルが存在しない新種のウイルス等を用いるためウイルス対策ソフトによる検知が困難であること、②対外接続しないネットワーク・システムであっても攻撃対象になりうることが挙げられる。こうした傾向を踏まえれば、既知の攻撃への対策を適切に実施するだけでなく、新たな攻撃が顕現化した場合の対応を事前に検討し「想定外」にしないことが重要である。

また、攻撃サイドが情報共有や技術移転等の連携を行っており、防衛サイドも情報共有や人材交流等で対応していくことが求められる。日本銀行金融研究所情報技術研究センターには、今後も情報セキュリティ・シンポジウム等を通

じて、わが国の金融業界における情報セキュリティの一層の向上に資する活動や、金融業界・産業界・学界の人材交流の場を提供する取組みを期待したい。

参考文献

CRYPTREC、「CRYPTREC Report 2010 暗号運用委員会報告書」、CRYPTREC、2011 年

鈴木雅貴・廣川勝久・古原和邦、「IC カード利用システムにおいて新たに顕現化した中間者攻撃とその対策」、日本銀行金融研究所 DPS 2011-J-16、2011 年

独立行政法人情報処理推進機構、「IPA テクニカルウォッチ『暗号をめぐる最近の話題』に関するレポート」、独立行政法人情報処理推進機構、2011 年

以　上