IMES DISCUSSION PAPER SERIES

多様化するリテール取引の安全性
—モバイル化を支える情報セキュリティ技術を中心に
—第14回情報セキュリティ・シンポジウムの模様—

Discussion Paper No. 2013-J-3

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 2013-J-3
2013 年 3 月

多様化するリテール取引の安全性
―モバイル化を支える情報セキュリティ技術を中心に
―第 14 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、2012 年 12 月 20 日、「多様化するリテール取引の安全性　―モバイル化を支える情報セキュリティ技術を中心に」をテーマとして、第 14 回情報セキュリティ・シンポジウムを開催した。

金融機関における預金引出や振込等のリテール取引では、窓口における対面取引から ATM 等を通じた非対面取引が中心になって久しい。また、最近では、パソコンや様々なモバイル端末を使ったバーチャルな環境での取引への対応が進むなど取引の形態が多様化してきている。一方で、多種多様なサービスが提供されるのに伴い、様々なセキュリティ上の脅威が顕現化しており、こうしたサービスに用いられる情報セキュリティ技術は常に進化が求められている。

こうした問題意識に基づき、今回のシンポジウムでは、①キャッシュカードシステムにおける IC カード対応の意義や今後の課題、②公開鍵暗号として今後中心的な役割を担うことが期待されている「楕円曲線暗号」の概要と利用上の留意点、③スマートフォンのアプリケーションを用いたモバイルバンキングに対して想定される攻撃とその対策、④ウイルスを用いたインターネットバンキングに対する新たな攻撃（Man-in-the-Browser 攻撃）とその対策の安全性評価について、専門家や当研究所スタッフによる講演が行われた。

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、4 件の講演、総括コメントの概要を紹介する。

キーワード：キャッシュカード、IC カード、楕円曲線暗号、スマートフォン、モバイルバンキング、Man-in-the-Browser、ウイルス
JEL classification: L86、L96、Z00

目　次

1. はじめに

日本銀行金融研究所は、2012 年 12 月 20 日、「多様化するリテール取引の安全性　――モバイル化を支える情報セキュリティ技術を中心に」をテーマとして、第 14 回情報セキュリティ・シンポジウムを開催した（プログラムは下記のとおり）。

●キーノート・スピーチ「多様化するリテール取引の安全性：
モバイル化を支える情報セキュリティ技術を中心に」
松本 勉（横浜国立大学大学院教授）

●講演 1「リテール取引システムにおける IC キャッシュカード機能の活用と将来の発展」
廣川勝久（日本銀行金融研究所テクニカル・アドバイザー）

●講演 2「次世代公開鍵暗号『楕円曲線暗号』とその適切な活用に向けて」
清藤武暢（日本銀行金融研究所）
※ 四方順司（横浜国立大学准教授）との共同研究に基づく講演。

●講演 3「スマートフォン向けアプリのセキュリティ
～バンキングサービスの安全性について～」
竹森敬祐（株式会社 KDDI 研究所主任研究員）

●講演 4「ウイルス感染した端末によるオンラインバンキングの安全性
―― Man-in-the-Browser 攻撃とその対策に焦点を当てて」
鈴木雅貴（日本銀行金融研究所主査）
※ 古原和邦（独立行政法人産業技術総合研究所研究グループ長）との共同研究に基づく講演。

●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講師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。

金融機関における預金引出や振込等のリテール取引では、窓口における対面取引から ATM 等を通じた非対面取引が中心になって久しい。また、最近では、パソコンや様々なモバイル端末を使ったバーチャルな環境での取引への対応が進むなど取引の形態が多様化してきている。一方で、多種多様なサービスが提供されるのに伴い、様々なセキュリティ上の脅威が顕現化しており、こうしたサービスに用いられる情報セキュリティ技術は常に進化が求められている。

こうした問題意識に基づき、今回のシンポジウムでは、①キャッシュカードシステムにおける IC カード対応の意義や今後の課題、②公開鍵暗号として今後中心的な役割を担うことが期待されている「楕円曲線暗号」の概要と利用上の留意点、③スマートフォンのアプリケーションを用いたモバイルバンキングに対して想定される攻撃とその対策、④ウイルスを用いたインターネットバンキングに対する新たな攻撃（Man-in-the-Browser 攻撃）とその対策の安全性評価について、専門家や当研究所スタッフによる講演が行われた。

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 100 名が参加した。

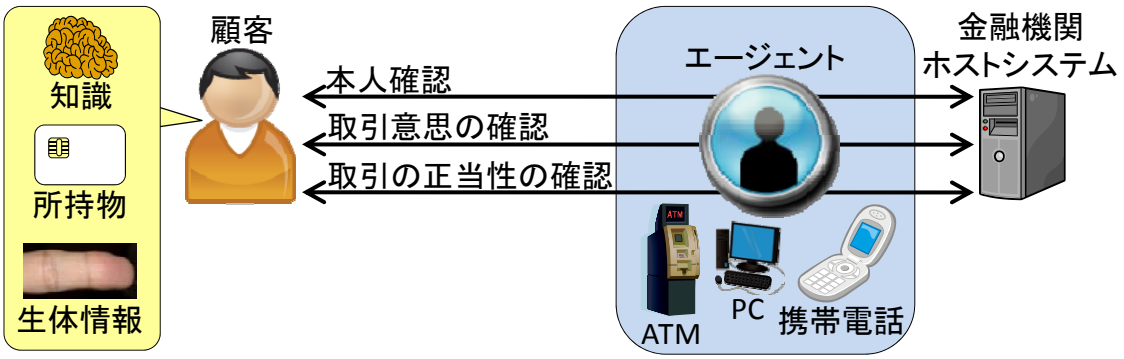
以下では、プログラムに沿って、本シンポジウムの概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）。

2. キーノート・スピーチ「多様化するリテール取引の安全性」

松本は、多様化するリテール取引の安全性に関する現状や検討課題を把握するうえでのポイントについて次のとおり発表した。

(1) 対面取引から様々な非対面取引へ

リテール取引の形態は、金融機関窓口における対面取引だけでなく、ATM 取引、インターネットバンキング、モバイルバンキングといった非対面取引に多様化してきた。こうした非対面取引は、顧客が金融機関ホストシステムとやり取りを行う際に、自分の代理あるいは同システムへのインタフェースとなる装置（以下、「エージェント」）を利用した取引として捉えることができる。金融機関は、こうしたエージェントの利用を前提に、本人確認、取引意思の確認、取引の正当性確認を適切に実施できるようにすることが求められる（図表 1 参照）。



図表 1．モデル化した非対面認証

(2) ATM 取引の動向

ATM をエージェントとして利用する ATM 取引では、偽造キャッシュカードによる預金不正払出し問題への 1 つの対策として、わが国では 2004 年から IC カードが発行されるようになった。そして、昨年、キャッシュカードシステム全体がようやく IC カード対応したという状況である。リスク管理を行ううえでは、システム全体が IC カード対応した意義について改めて確認しておくことが有用であろう。

また、欧州をみると、既に IC カード対応を終えて次の課題に取り組んでいる。具体的には、IC カード非対応の地域での利用を想定して、通常 IC カードには磁気ストライプも搭載されているが、この磁気ストライプを狙った不正取引が欧州域外で発生しており、こうした不正取引に対する新たな運用ルールを導入する動きがある。この動きを踏まえて、国内金融機関がどのように対応していくべきかを検討する必要があろう。

(3) インターネットバンキングの動向

顧客の PC をエージェントとして利用するインターネットバンキングについては、本人のログイン時に「偽画面」を表示して乱数表等の情報を全て盗取する手口が昨年後半より国内において発生している。海外では、さらに巧妙化された手口が確認されており、顧客の取引内容をリアルタイムで改ざんすることによる不正な資金移動が行われている。こうした攻撃は、ブラウザの中に通信に割り込んで不正行為を行っている人がいるかのように振舞われる（実際にはウイルスであるが）ことから「Man-in-the-Browser（MitB）攻撃」と呼ばれている。

同攻撃は、本人によるログイン後を狙うケースもあり、サーバ認証や本人確認の強化では防止することが難しい。また、PC の管理は顧客に委ねられており、ウイルス感染を完全に防止することも難しいといえる。このため、ウイルス感

染していても MitB 攻撃を防止可能な対策が求められており、例えば、PC と携帯電話のように 2 台の端末を利用して取引を行い、一方の端末がウイルス感染していなければ攻撃を防止可能という対策が提案されている。こうした対策の導入が急務と考えられるが、その際、安全性を評価し、何に留意すべきかを把握しておくことが望ましい。

(4) モバイルバンキングの動向

顧客のモバイル端末、特に、スマートフォンをエージェントとするモバイルバンキングは、2010 年頃から始まった比較的新しい取引形態である。このため、①スマートフォンの OS 自体の安全性、②ウイルス対策、③スマートフォン紛失時の対策、④スマートフォンのアプリケーション（以下、「アプリ」）の安全性等の多面的な観点から安全性を検討することが必要である。いずれも重要であるが、金融機関が直接管理できるのはモバイルバンキング用のアプリ（④）であり、脆弱性のないアプリの開発・実装、正規アプリの配信や解析防止といった検討が求められる。

(5) 暗号技術の動向

上記の各取引形態では、データの保護や認証等の用途に暗号技術を利用している。現在主流の暗号技術の 1 つとして RSA 暗号が知られているが、同暗号に対して、①必要な安全性を確保するための鍵長が長くなり過ぎ、将来使い続けていくうえで暗号処理上の制約が問題となりつつあることや、②暗号鍵の生成処理における不適切な運用等により、第三者に暗号鍵を推定されるリスクがあることが指摘されている。このため、こうしたデメリットが相対的に少ない暗号技術として「楕円曲線暗号」が注目を集めている。今後、金融業界においても同暗号の利用が進む可能性があるが、その際、同暗号の特徴や利用上の留意点を把握したうえで活用していくことが望ましい。

(6) まとめ

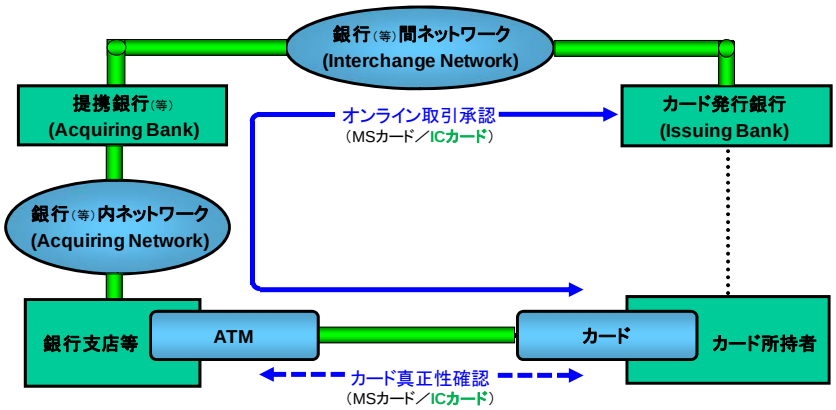
多様化するサービスを安全に提供していくためには、上記のポイントを含め、様々な点に留意する必要がある。今回のシンポジウムにおける各報告でそれぞれのテーマの現状や検討課題について報告が行われるが、これらが金融リテール取引における情報セキュリティ面での安全性向上に向けた取組みの一助となることを期待する。

3. 講演 1「リテール取引システムにおける IC キャッシュカード機能の活用と将来の発展」

廣川は、IC カード対応の意義と今後の課題について次のとおり発表した。

(1) わが国のキャッシュカードシステムの IC カード対応とその意義

昨年夏にかけて、わが国のキャッシュカードシステムの IC カード対応が進展した。同システムは、全国銀行協会の「全銀協 IC キャッシュカード標準仕様」（以下、「全銀協仕様」）に基づいており、キャッシュカードを発行するカード発行銀行のホストシステム、同銀行との提携銀行のホストシステム、銀行の本支店内に設置された ATM、キャッシュカードの所持者といった構成主体および、これらの主体をつなぐネットワークからなるシステムとして表現できる。カード所持者が提携銀行 ATM を利用して取引する場合の流れは以下（図表 2 参照）のとおりとなる。



図表 2. キャッシュカードシステム（提携銀行 ATM を利用する場合）

このようなシステム全体を一度に IC カードに対応させることは困難なため、わが国では、大きく 2 段階に分けて IC カード対応が進められた。1 段階目は、ATM の IC カード対応である。IC カードは、内部に格納された暗号鍵を用いて暗号処理を行う機能を有しており、ATM は同機能を利用したカードの真正性確認を実施することで偽造カードを排除できるようになった。ただし、同段階では、ATM からカード発行銀行までの全てのネットワークやホストシステムが IC カードに対応しているとは限らないため、カードの真正性確認後は IC カードであっても磁気カードと同様の扱いで取引処理が行われた。

2 段階目は、ATM から発行銀行までの全てのネットワークやホストシステムの IC カード対応であり、2012 年 8 月に対応が完了した。その結果、各取引に固有の暗号情報を IC カードが生成し、同情報を発行銀行のホストシステムが検証するといった End-to-End（IC カードと発行銀行のホストシステム間）での取引の正当性確認が実施できるようになった。

(2) IC カード対応後の課題

既にリテール取引システムにおける IC カード対応を完了させた欧州 SEPA[1]（単一ユーロ決済圏）では、偽造カードによる被害を大幅に削減することに成功しており、現在、IC カード対応後の課題として次の 2 つに取り組んでいる。

1 つ目の課題は、SEPA 域内で発行されたカードを偽造して域外で使用する不正への対策である。域内発行 IC カードは、IC カードに対応していない域外の国での利用も想定し、磁気ストライプを搭載した磁気併用 IC カードとなっている。IC カードとしての処理が行えず磁気カードとして利用された場合、同カードの磁気情報を偽造した不正取引のリスクが高くなる。そこで、SEPA は、IC カード対応がなされていないために発生した SEPA 域内発行 IC カードに対する不正取引の損害は、そうした環境を整備できていない金融機関や加盟店の責任であるとして、当該金融機関等に損害の負担を求める運用ポリシー（「債務責任の移行」と呼ばれる）を 2015 年 10 月から実施する方針を明らかにしている。

SEPA の運用ポリシー実施後は、わが国の ATM や POS 端末、ネットワークが IC カード対応となっていない場合には、わが国の金融機関等に対して SEPA から不正取引にかかる債務責任を求められることになる。さらに「債務責任の移行」ルールが他地域に広まる場合、SEPA 以外の国からも同様に債務責任を求められる可能性がある。逆に、国内発行 IC カードが海外で磁気カードとして利用される場合に生じる不正取引のリスクに対しては、わが国から当該国へ債務責任を求めていくことも考えられる。なお、米国では、磁気カード取引が主流であるが、SEPA の運用ポリシー等を受けて IC カード対応の強化を表明している。

SEPA の 2 つ目の課題は、インターネット取引における不正への対策である。インターネット取引では、カード券面の情報（口座番号、有効期限等）が漏えいすると、カード自体が盗取されなくとも不正取引が発生する可能性があり、SEPA 域内ではこうした不正取引が増加傾向にある。こうした状況下、SEPA は、インターネット取引の安全性を向上させるための方針を打ち出しており、同方針では、IC チップのようなハードウエアを用いた認証が対策の 1 つとして取り上げられている。わが国においてもインターネット取引がますます活発化していくと予想されるが、そうした中で IC チップ等を用いた不正取引への対策も検討していくことが望ましい。

---

[1] Single Euro Payment Area。EU 加盟国を含めた 32 カ国において、国内外の区別なくユーロ建ての小口決済が行える地域、および、それを実現するスキーム。また、SEPA 域内の IC カード対応状況については、IC カードはカード全体の 87.2%、IC カードに対応した ATM は 96.7%、同 POS 端末は 94.2%となっている（2011 年末現在）。

4. 講演 2「次世代公開鍵暗号『楕円曲線暗号』とその適切な活用に向けて」

清藤は、公開鍵暗号として今後中心的な役割を担うことが期待されている「楕円曲線暗号」の安全性や利用上の留意点について次のとおり発表した。

(1) 現在主流の公開鍵暗号「RSA」の課題と楕円曲線暗号の利点

金融機関は、ATM 取引やインターネットバンキング等において、データ保護や通信相手の認証等のために暗号を利用している。こうした暗号のカテゴリの 1 つに公開鍵暗号がある。公開鍵暗号は、公開鍵を公開しても秘密鍵を求めることが困難であるという仕組みを用いて安全性を保証しているが、この際、ある種の「数学的な問題」を利用してこの仕組みを実現している。現在主流である公開鍵暗号 RSA では、「2 つの素数の積から元の素数を求めることは難しい」という数学的な特徴（「素因数分解問題」と呼ばれる）を利用しており、かかる素数の桁数（鍵長）が大きいほど安全性が高くなる。

暗号の安全性は、攻撃の高度化や計算機性能の向上といった技術進歩により経年劣化するため、適切な安全性を維持するには鍵長を伸長していく必要がある。しかし、RSA では、比較的長い鍵長が必要になるため暗号処理の負荷が特に大きくなる傾向があり、鍵長を伸長していくことに限界があると指摘されている。また、RSA においては、異なるユーザの鍵生成時に同じ素数を使い回した場合、第三者が当該ユーザの秘密鍵を容易に導出できるという運用上の問題等も指摘されている。このため、これらの指摘の影響を受けにくい楕円曲線暗号が注目されている。同暗号は、インターネットバンキングの暗号通信等で利用可能になっているほか、既に地上波/BS/CS 放送等の映像コンテンツの保護用途等で利用が進んでいる。

楕円曲線暗号は、楕円曲線上の 2 点の間で「計算は容易」だが「逆演算は困難」という数学的な特徴を利用した暗号方式である。同問題を効率良く解く方法が考案されておらず、素因数分解問題よりも難しい問題であることから、楕円曲線暗号は RSA よりも鍵長が短くなる。現在 RSA では約 600 桁（2,048 bit）の鍵長が推奨されているが、楕円曲線暗号では約 10 分の 1 の鍵長（約 60 桁＜195 bit＞）で同等の安全性を確保することができると評価されている。また、楕円曲線暗号は、鍵生成の仕組みが RSA とは本質的に異なるため、RSA のような鍵生成にかかる運用上の問題は生じにくい。

(2) 楕円曲線暗号の安全性

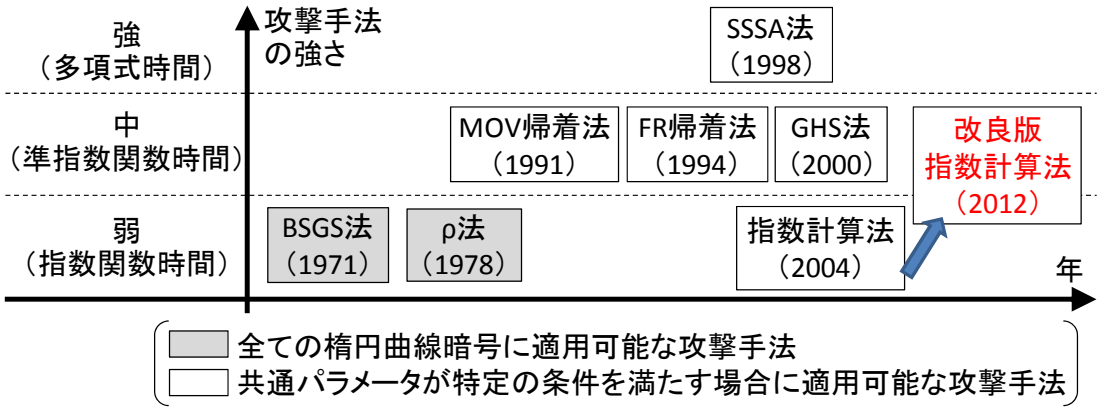
楕円曲線暗号では、まず、①楕円曲線のタイプと同曲線上の基準点をユーザ共通のパラメータとして決定したうえで、②各ユーザの秘密鍵と公開鍵のペアを生成する。楕円曲線暗号の安全性は、前述のとおり、公開鍵から秘密鍵を求

める難しさに依存しているが、この問題を解く方法（以下、「攻撃方法」）として、2 つのアプローチがある。1 つは、解の候補を 1 つずつしらみ潰しに試していくアプローチであり、全ての楕円曲線暗号に適用できる。同アプローチにおいて現在最も効率の良い攻撃方法は「ρ（ロー）法」と呼ばれている。もう 1 つは、共通パラメータが特定の条件を満たすことを前提に、楕円曲線上の数学的問題をより簡単な問題に変換し、変換後の問題を解くというアプローチである。

共通パラメータを設定する場合には、(a) ρ 法でも解読できない長さ（ρ 法による解読記録は 2009 年現在で鍵長 34 桁＜112 bit＞）の鍵長にすることと、(b)楕円曲線上の数学的問題をより簡単な問題に変換できないようなパラメータを選ぶことの 2 つの要件に留意する必要がある。米国立標準技術研究所等では、これらの要件を満たす共通パラメータを公表しており、金融機関等が参照することができる。

(3) 新たな攻撃の影響と利用上の留意点

特定の共通パラメータを用いる楕円曲線暗号に対する新たな攻撃「改良版指数計算法」が 2012 年に提案された。同攻撃は、従来の攻撃手法と比べて適用可能なパラメータの範囲が広いという特徴があり、注目を集めている（図表 3 参照）。



図表 3. 楕円曲線暗号への攻撃手法

もっとも、同攻撃手法は、今後の研究の進展の可能性も考慮すると潜在的には脅威ではあるが、当面は影響が限定的との評価が可能である。すなわち、改良版指数計算法を指摘した研究グループは、鍵長が約 600 桁以上の時に同攻撃が ρ 法よりも効率が良くなると報告している。したがって、鍵長が 600 桁以下の時は ρ 法への耐性に留意すればよいことになるが、米国立標準技術研究所等が公表している共通パラメータの鍵長は 49～172 桁（160～570 bit）となっているため、同パラメータを利用している間は改良版指数計算法の影響を受けない

ことになる。また、鍵長約 600 桁の楕円曲線暗号は、ρ 法を用いると西暦 3000 年頃に漸く解読可能となる。

したがって、少なくとも現行は、米国立標準技術研究所の公表情報等を参照して共通パラメータを適切に設定することにより、楕円曲線暗号は RSA より短い鍵長で同程度の安全性を確保できるといえる。

5. 講演 3「スマートフォン向けアプリのセキュリティ」

竹森は、モバイルバンキングに焦点を当てて、スマートフォン向けアプリケーション（以下、「アプリ」）に対して想定される攻撃とその対策について次のとおり発表した。

(1) 邦銀のモバイルバンキング

スマートフォンを利用してモバイルバンキングを行うためのアプリ（以下、「バンキングアプリ」）を提供する銀行が増加している。こうしたサービスを提供する形態は、Web 型とアプリ型に大別できる。Web 型サービスは、HTTP[2]等の標準化された情報通信手順を前提に Web ブラウザ（汎用アプリ）経由で提供されるサービスである。これまで PC 向けに提供してきたインターネットバンキングシステムも HTTP 等を前提としているため、同システムの設計・開発における安全性確保に関する知見等を活用できるというメリットがある。また、スマートフォンの OS や機種への依存度が低いことから、システムの開発やメンテナンスに要するコストも従来の PC 向け Web 型サービスと同程度になると考えられる。一方、アプリ型サービスは、Web ブラウザにはない独自の機能を備えた専用アプリを前提に提供されるサービスである。スマートフォン OS が提供する細かい制御機能も利用できるため、Web 型サービスよりも高い利便性や安全性を実現できる余地がある。ただし、アプリ開発の歴史は浅く安全性確保に関する知見等が十分に蓄積されていないことから、初歩的な脆弱性への対応がなされていない事例が多くみられ、アプリの脆弱性を悪用した攻撃が急増している。また、OS の種類やバージョンあるいは機種毎にアプリを開発する必要があり、開発・メンテナンスに要するコストが高くなるという課題もある。なお、アプリ型をベースとしつつ、振込等の重要な処理についてはアプリ内で Web 型サービスに切り替えるというハイブリッド型も考えられる。

以下では、アプリ型のモバイルバンキングサービスに焦点を当てて、想定される攻撃とその対策についてみていく。

---

[2] HyperText Transfer Protocol。Web ページを表示するために利用される情報通信手順。

(2) モバイルバンキングへの攻撃

スマートフォンでは、①OS の管理者権限は通信キャリアが保有し利用者には開放していないこと、②実行中のアプリがユーザの許可なく他のアプリやデータにアクセス出来ない仕組みとなっていること、③PC に比べマルウエア（ウイルス）の数が少ないほか PC のような自動感染はないこと等の理由から PC より安全性が高いといえる。ただし、スマートフォンがマルウエアに感染している場合やバンキングアプリに脆弱性がある場合には、次の攻撃が想定される。

① 偽のログインページによるパスワードの盗取等

マルウエアが偽のログインページを表示し、ユーザが騙されて入力したパスワード等の認証情報を盗取することが考えられる。攻撃手口としては、ユーザに正規のバンキングアプリと類似したマルウエアを起動させ偽のログインページを表示するケースや、予めインストールされたマルウエアがユーザによる正規ログインページへのアクセスを監視し、アクセス時に偽のログインページ（いわゆる、「偽画面」）を表示するケース（後述講演 4 における MitB 攻撃）等が考えられる。

② 正規アプリを改造したマルウエアによるパスワードの盗取等

正規のバンキングアプリにパスワードを盗取するなどの不正な機能を追加するかたちで改造されたマルウエアを用いる攻撃である。ユーザが正規のバンキングアプリと勘違いして同マルウエアを利用すると、一見正規アプリと同様に動作するものの、密かにパスワードの盗取等が行われる。解析が容易なプログラミング言語を用いて正規アプリが開発されている場合には、こうしたマルウエアを作成する手間が低くなるため注意が必要である。

③ アプリや OS の脆弱性を悪用したパスワードの盗取や不正取引等

バンキングアプリや OS に脆弱性がある場合には、前述したスマートフォンの安全性上の利点が失われ、攻撃につながる可能性がある。例えば、バンキングアプリに脆弱性がある場合には、マルウエアが同アプリの脆弱性を悪用し、パスワードの盗取や不正取引の試行を行うことが考えられる。また、スマートフォン OS の脆弱性を悪用してマルウエアが同 OS の管理者権限を奪取している場合、モバイルバンキングアプリを利用中にユーザが入力したパスワードの盗取や不正取引の指示等が可能になると考えられる。

なお、こうしたマルウエア（アプリ）をユーザにインストールさせるために、同アプリを配信サイト（「Market」と呼ばれる）に掲載してインストールを誘う方法や、同アプリのダウンロード先のリンクを記したメールをユーザに送信する方法等が採られる。

(3) 各攻撃への対策と留意点

上記の攻撃のように、ひとたびマルウエア感染した場合の影響が大きいことから、次のような対策を検討することが重要である。

(a) 端末認証の高度化

スマートフォンには、SIM（Subscriber Identity Module）と呼ばれる通信事業者が管理する IC チップが搭載されている。SIM は、電話番号や暗号鍵を安全に格納し、暗号処理が可能な一種の IC カードであり、従来は通信事業者のみが SIM を使った端末認証（「SIM 認証」と呼ばれる）を利用可能であった。今般、一部の通信事業者が一般のアプリ提供者向けに SIM による端末認証サービスを開放する旨の発表を行った。SIM 認証は、IC カードと同様に暗号技術を利用する安全性の高い認証方法であり、同認証をパスワード認証と併用することで、パスワード等が漏えいしても不正取引の防止が可能になる。

(b) 取引内容の通知（処理の見える化）

モバイルバンキング取引後に、取引があったという事実だけでなく、取引内容（送金先、金額等）もユーザに通知することにより、事後ではあるが不正取引の検知が可能になる。こうした通知は、E-mail のような遅延が許容される手段ではなく、リアルタイムにユーザに送付される方法（例えば、SMS[3]）を利用することが望ましい。

(c) 信頼できるアプリ配信方法の確立

ユーザがマルウエアを入手することを防止するために、正規アプリを配信する方法を確立することが望ましい。具体的には、予め正規アプリを公式 Market に掲載すると伴に、暗号によりサイト認証が行われている銀行の Web ページに同アプリへの直接のリンクを載せる方法である。この場合、ユーザは、信頼できる銀行の Web ページ経由で公式 Market 上の正規アプリを入手することができる。このほか、現在の Market では、アプリ開発者の厳格な身元確認を行っていないため、こうした確認をユーザが検証できるかたちで実施すること（「アプリ認証」と呼ばれる）も有用である。

(d) アプリの難読化

正規アプリを解析して偽アプリを作成する攻撃を防止するために、認証等の重要な処理については、解析が困難なプログラミング言語を用いて実装したり、「難読化」と呼ばれる解析が困難となるような処理を施すことが望ましい。

---

[3] Short Message Service。回線交換型のメールのため、リアルタイムにスマートフォンに配信することが可能。

(e) 脆弱性の排除

アプリ設計上の致命的な脆弱性を排除するために、設計段階からセキュリティ技術者と連携することが望ましい。また、アプリの実装時に脆弱性への対応が適格に行えるように、日本スマートフォンセキュリティフォーラムの「セキュアコーディングガイド」等を参照することが有益である。

(f) アプリ起動時のスマートフォン本体の安全性検査

「スマートフォン本体の管理者権限の奪取の有無やマルウエア感染の有無等をアプリ起動時に検査する機能」をバンキングアプリに搭載し、安全性が確認された場合にのみ同アプリ本体を起動するという方法である。一部の邦銀のバンキングアプリにおいて導入されている。

こうした対策の中には、実際にユーザに協力してもらわないと機能しないものが多く、ユーザにセキュリティ対策の重要性について啓蒙を図るとともに、金融業界内で仕様等の統一を図り操作手順等を標準化することを通じ、ユーザが対策を適切に利用できる環境を整備することが重要である。

6. 講演 4「ウイルス感染した端末によるオンラインバンキングの安全性」

鈴木は、インターネットバンキングに対する「Man-in-the-Browser（MitB）攻撃」とその対策について次のとおり発表した。

(1) Man-in-the-Browser 攻撃の概要

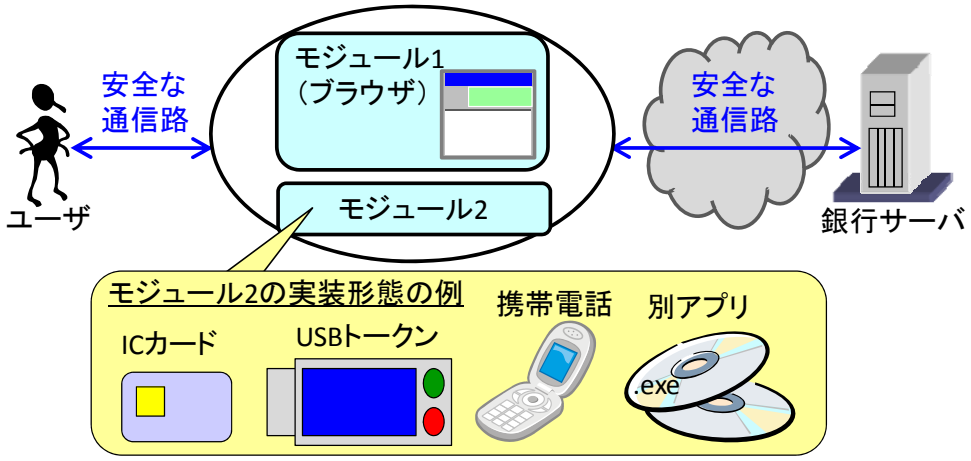
ウイルスを利用した金融犯罪はこれまでも発生してきたが、国内インターネットバンキングでは、2012 年 10 月下旬から MitB 攻撃と呼ばれる新しいタイプの攻撃が確認されている。同攻撃では、正規のサイトへログイン後、ウイルスによって秘密の質問への答えや乱数表の情報の入力を求める「偽画面」が表示される。偽画面は、金融機関のロゴ画像等を悪用して巧妙に作成されているため、ユーザは騙され易く、入力された情報はログイン時の ID、パスワード等の認証情報と共に攻撃者に盗取され、不正取引につながる。

海外では、さらに巧妙な MitB 攻撃が確認されている。具体的にはインターネットバンキングでユーザが入力した取引内容（送金先、金額）をウイルスが密かに改ざんして銀行のサーバに送信する攻撃である。サーバからの応答結果である取引確認画面においても、ウイルスが表示内容を改ざんして、ユーザがもともと意図した取引内容を表示するため、ユーザは取引が正常に受け付けられたと誤認する可能性が高い。

(2) 注目される対策「取引認証」

MitB 攻撃に対しては、ウイルス対策ソフトや OS 等のセキュリティパッチの利用といった PC をウイルスに感染させない対策が不可欠である。しかし、ウイルス対策ソフト等を利用していないユーザや新種のウイルスの存在を考慮すると、ウイルスに感染していても不正取引を防止可能な対策が重要になる。こうした対策として、取引時に取引内容（送金先、金額）をユーザ本人が認証する「取引認証」が知られており、多種多様な方式が提案されている。英 Barclays 等の一部の金融機関では既に導入しており、今後、不正取引対策等として普及していくと見込まれる。しかし、取引認証方式の安全性を統一的に評価する枠組みは、情報セキュリティ研究者の間ですら確立していないのが実情である。そこで、以下では、取引認証方式を用いたインターネットバンキングにおける MitB 攻撃への対策について整理・評価を試みた。

既存の取引認証方式をみると、PC 等の Web ブラウザのほかに、ソフトウエアまたはハードウエア（携帯電話、IC カード、USB デバイス等）により実現される別の要素（モジュール）を取引で併用し、ブラウザがウイルスに乗っ取られても同モジュールが安全であれば攻撃を防止できるというアイデアに基づいている。そこで、ユーザが 2 つのモジュールを併用して金融取引を行うシステムを対象に対策を整理したうえで安全性を評価した（図表 4 参照）。



図表 4. 想定するシステム

安全性評価にあたっては、こうしたシステムを前提とする取引認証方式を取引処理およびシステム構成の観点からそれぞれ評価した。

取引処理の観点では、各取引内容をユーザが認証するために使い捨て番号（「TAN : Transaction Authentication Number」と呼ばれる）を利用する場合としない場合、さらに取引指図等のやり取りを2つのモジュールのうちどちらのモジュールで行うかによって取引認証方式を評価した。この結果、TANを利用することで、MitB攻撃を防止可能な方式の選択肢が増加し、設計の自由度が高まるほか、

モジュールの一方に求める機能(ユーザインタフェース、通信機能、TAN生成機能)を軽減できるケースが多いことがわかった。

システム構成の観点からは、各モジュールを実装する際に同一端末上に実装するか、各モジュールとサーバとの通信路が電気信号的に分離されているかという違いに着目して評価した。この結果、一方のモジュールを乗っ取ったウイルスが他方のモジュールも乗っ取ることができるかという観点から安全性評価を行うと、PC（のブラウザ）と携帯電話を併用する方式のように、各モジュールが異なる端末上に実装され、かつ、各モジュールとサーバの通信路が電気信号的に分離されている方式の安全性が、そうでない方式の安全性よりも高いことが確認された。

(3) 運用上の留意点

取引認証方式の導入にあたり、事前作業として端末やメールアドレス等の登録やアプリケーションのインストール等の作業が必要となるケースが想定される。一方、ユーザの PC がウイルスに既に感染している状況も想定されるため、そうした PC を前提にしても適切に取引認証方式を導入可能な方法を検討することが望ましい。例えば、登録やインストール時に PC のウイルススキャンを行うツールを提供する方法や PC 以外の安全性を確保できる他の手段（郵便、電話等）を利用して登録作業を行う方法等が考えられる。

また、取引認証方式を適切に導入できたとしても、ユーザが同方式を適切に活用できなければ期待した効果が得られないため、ユーザに継続的な啓蒙を行うことも重要である。

このほか、本研究では、MitB 攻撃を防止する対策として取引認証に焦点を当てたが、同攻撃を事後的に検知可能な対策についても検討することが望ましい。例えば、サーバからユーザに取引結果を伝える際に、具体的な取引内容（送金先、金額）を含めるという方法が考えられる。

7. 主な質疑応答

米国における IC カード対応について**フロア参加者 A** から、現在対応が遅れている理由について質問が寄せられた。これに対して、**廣川**は、米国内ではオンラインでの取引承認が低コストで行えるため、IC カードを用いて取引の安全性を高めるニーズが高くなかったことが背景にあると説明した。そのうえで、SEPA における新たな運用ポリシー（債務責任の移行）の実施や、主要な国際決済ブランドによる IC カード対応の推進と債務責任の移行実施に関する表明を受けて米国においても IC カード対応を強化する方向である点を改めて強調した。

スマートフォンの安全性について**フロア参加者 B** から、バンキングアプリの起動時にスマートフォン本体の安全性検査を行うという対策が紹介されたが、本体の管理者権限が奪取されていることを前提とした場合でも、こうした検査は有効に機能するのかとの質問が寄せられた。これに対して、**竹森**は、アプリ起動時に本体の管理者権限が奪取されているか否かを確認する方法があり、こうした検査は有効に機能すると考えられると説明した。そのうえで、アプリ起動時の検査だけでなく、OS 等の改ざんの有無を検査しながらスマートフォン本体を起動する仕組みも存在し、既に一部のスマートフォンには導入されていると補足した。また、**フロア参加者 C** から、サイト認証が行われていない Web ページに正規アプリへの直接のリンクを載せる方法に問題があるかとの質問が寄せられた。これに対して、**竹森**は、サイト認証が行われていない Web ページの場合には、同ページの内容（正規アプリへのリンク先）が通信路上で改ざんされるリスクが残ると説明した。

MitB 攻撃への対策について**フロア参加者 D** から、PC（のブラウザ）と携帯電話のように 2 台の端末を用いた取引認証方式では、利便性が低下するのではないかとの質問が寄せられた。これに対して、**鈴木**は、ブラウザと当該 PC にインストールした別のアプリを併用することで、1 台の端末（PC）で取引認証を実施する形態を選択することが考えられると説明した。また、こうした形態の製品が既に利用可能になっているものの、同形態においてはブラウザと同アプリが同時にウイルスに乗っ取られないようにするための追加的な対策が重要であり、例えば、スマートフォン OS が提供するアプリとデータを保護するセキュリティ機構が参考になると補足した。

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のテーマ「多様化するリテール取引の安全性　―モバイル化を支える情報セキュリティ技術を中心に」は、最近の情報セキュリティを巡る動向を踏まえており、金融機関等にとって有益な情報が豊富であった。世間で問題となった「偽画面（ポップアップ型フィッシング詐欺）」の進化形である取引内容改ざん型 MitB 攻撃のように攻撃は日々高度化しており、単一の対策に頼るのではなく、本人認証の強化、取引認証、不正取引の即時または事後の検知、リスクに応じた限度額の設定、ユーザの啓蒙等、多面的に対策を検討していくことが重要である。

情報セキュリティの分野では、「理論的に可能性が指摘されている攻撃は必ず

発生する」と言われているため、日頃からセキュリティの動向をフォローし、具体的な対応を早めに検討していくことが望ましい。もっとも、金融機関が個別にこうした取組みを行うことには限界があるため、金融業界として情報を共有し、一体となって対処していくことが必要であろう。日本銀行金融研究所情報技術研究センターにはそうした活動をサポートしていく役割が一層強まっているように思う。また、同センターには、時代の潮流を適切に捉えた有効な取組みを今後も期待したい。

以　上