2014 年 12 月 26 日
日　本　銀　行
金　融　機　構　局
金融高度化センター

ITを活用した金融の高度化に関するワークショップ
第2回「金融取引チャネルとセキュリティ」の模様

Ⅰ．はじめに

日本銀行では、IT を活用した金融の高度化に関するワークショップを随時実施している。2014 年 11 月 26 日に、その第 2 回となる「金融取引チャネルとセキュリティ」を、以下のプログラムで開催した。

＜プログラム＞

▼ 開会挨拶　岩下 直行（日本銀行 金融機構局 金融高度化センター長）

▼ プレゼンテーション

「ネットバンキングのセキュリティ」

中山 靖司（日本銀行 金融研究所 制度基盤研究課 情報技術研究センター 情報技術研究グループ グループ長）

「セブン銀行の ATM 戦略とセキュリティ」

石黒 和彦　氏　（株式会社セブン銀行 取締役 常務執行役員）

▼ 自由討議

― 参加者については別添を参照。

― ワークショップにおける議論のポイントは、以下のとおり。

【今回ワークショップのポイント】

① キャッシュカードにおける磁気ストライプからICへの切替について、海外で急速な進展がみられている結果、わが国の遅れが目立ってきている。このため、わが国が国際的な犯罪の標的になるのではないかとの懸念の声が聞かれた。こうした中、導入が予定されているマイナンバー制度を活用してキャッシュカードのICカード化を図るとのアイデアが示された。

② インターネットバンキングにおけるセキュリティの強化策として、「取引認証」の必要性が強調された。

③ 金融機関の参加者からは、古いシステム環境にある顧客への配慮等から、一律に新しいセキュリティ対応に切替ることの難しさが示された。これに対し、脆弱なセキュリティ環境をそのままにしておくことの問題を指摘する声も聞かれた。また、「顧客のセキュリティリテラシーレベルを踏まえた対応」、「顧客に対する複数の選択肢の提供」、「補償基準の明確化」等の重要性が指摘された。

④ セキュリティ情報の共有化等の金融機関同士の協力が重要である、との意見が示された。

Ⅱ．開会挨拶（日本銀行 岩下 直行）

１．取引チャネルの拡大とセキュリティ

前回の第1回ワークショップでは、「金融ITが一般のIT技術の進歩に取り残されてしまった現状とその対策」について議論を行った。その中で、銀行システムに高い安全性を要請されていることが、そうした現状の背景にあるとの視点が提示された。そこで今回は、特に対顧客チャネルであるインターネットバンキングとATM取引について取り上げ、セキュリティの観点から、金融ITのあるべき姿を考えてみたい。

最初に申し上げたいのは、ATMやインターネットバンキングは、金融ITがもたらした大きな成果ということである。24時間、どこからでも現金の引出や振替指図をできるようになったことは、金融取引の顧客利便性を大きく向上させ、金融機関側でも、人件費コスト、出店コストの削減に寄与している。厳密な統計はないが、実感として、ATMとかインターネットバンキングは、既に金融機

関の主要な取引チャネルであり、店頭での紙ベースの取引に戻ることはもはや不可能であるということは、誰もが認めることである。

その一方で、ATM もインターネットバンキングも、様々な攻撃の対象となっている。かつて 2000 年代前半に偽造カード事件が世間を騒がし、預貯金者保護法の制定に繋がったことがあった。当時、金融機関は預金者を保護する努力を怠ったのではないかと、世間から厳しい指弾を浴びることとなった。ここ数年ではインターネットバンキングが攻撃の対象となっているが、どちらのチャネルも、攻撃が収まる様子はない。

詳しくは本日のプレゼンテーションに譲るが、攻撃者は預金者の認証情報を盗み取り、不正な送金や預金引出を行っている。攻撃手口は年々高度化しており、金融機関がいかに対策を講じても、その裏をかく手口が編み出される現状にある。

こうした現状を踏まえ、ATM やインターネットで提供するサービスの水準を再考すべきとの声も聞かれている。引出限度額、送金限度額の引き下げは既に実施されているほか、一部の地域金融機関がインターネットバンキングによる都度指定振込を制限する動きもある。

店頭での紙ベースの取引に戻ることはできないとしても、こうしたサービスをどう提供していくべきかについて悩む金融機関の声も聞かれている。しかし、せっかく IT を駆使して利便性の向上を図ってきた中で、リスク回避のために顧客サービスを低下させるのは、割り切れない思いがある。

２．外部からの隔離とその境界線の拡大

そもそも、ATM もインターネットバンキングも、金融機関の情報システムの外部との境界線にあることに注意する必要がある。

ATM やインターネットが出現する以前から、銀行システムは「外部からの隔離」をセキュリティの基本設計としてきた。これは、銀行の内と外とを隔離し、外部からの攻撃を困難にする作戦ともいえる。一旦銀行の内側に入った利用者や職員に対しては、利便性、効率性を重視する傾向にある。内部は性善説、外部は性悪説、などとも言われている。

こうした中で、 ATM（特に店外 ATM）やインターネット経由の取引は、このような隔離の境界線を利用者側に押し広げようというものであった。それは、顧客利便性などのためには必要な拡張であった。もっとも、セキュリティ技術的には、暗証番号やパスワードのような素朴な対策だけで、外部を内部のように扱おうとすると、攻撃側に付け込まれる隙が生まれる。そうして生じた隙が、過去の様々な事件に繋がったとも言える。

金融機関が採用してきたセキュリティの基本設計が「外部との隔離」であった以上、その矛盾が生じやすい部分である外部との境界線に問題が集中するのは当然のこととも言える。

こうした問題にどう対応すれば良いかだが、まず、 利用者の預金を犯罪者から守り、不正な送金、引出をさせないことは金融機関の責務であり、安全対策のさらなる充実が必要である。特にインター―ネットバンキングについては、安全性への懸念から取引を行わないとする利用者が多数存在する。せっかく IT 投資をしても、それが利用されないのでは、効果はない。そうした用心深い利用者にも信頼されるために、利用者に受け入れられやすく、実効性のある安全対策を講じていく必要がある。

とはいえ、セキュリティ対策に無限のコストをかけられない以上、ビジネスとして提供する預金サービスにおいて、どの水準までの対策を講じるべきかが問題となる。また、利用者に安全で適切な利用を促すための方策についても、様々な選択肢が存在する。利便性とセキュリティとコストのトレードオフ関係を意識したうえで、どのような選択を行うべきか、本日のセッションで議論していきたいと思う。

Ⅲ. プレゼンテーション要旨

1. 「ネットバンキングのセキュリティ」（日本銀行 中山 靖司）

(1)ネットバンキングを使った不正払出の増加

ネットバンキングを使った不正払出の被害額を警察庁の資料でみると、26/上期で 1,852 百万円に達し、前期比急増している。被害金融機関数では、最近地銀が狙われつつあるほか、法・個人別区分では、法人の増加が目立つものの、被

害全体でみると、大手行の個人口座が大きなターゲットになっている状況に変わりはない。この被害額の規模は、偽造キャッシュカードによる不正な現金の引出が社会問題となった 2005 年の 8 億円を上回る金額である。ただし、金融機関が補償に応じているため、大きな社会問題としてマスコミに騒がれるには至っていない。

(2)不正払出手口の変化

不正払出の手口としては大きく分けて従来型と最新型と 2 つあり、最新型へと移行してきている。

従来型とは、ID とパスワードを入手した犯罪者が本人に成り済まして、犯罪者のパソコンで送金の操作を行うものである。ID やパスワードの不正入手の手口には 3 つあり、①フィッシング、②ウイルス（キーロギングとか画面のスクリーンショットを送るとか、通信を傍受してそのまま送る等)、③ウイルスとフィッシングの融合（利用者が正規のネットバンキングにアクセスすると、ウイルスがポップアップで偽の画面を出し、そこで乱数表や秘密の質問等の入力を求める手口）である。

ところが、最近になって最新型による不正が行われるようになっている。最新型とは、ウイルスが利用者のパソコンを乗っ取り、本人の意思に反して送金の操作等を行うもので、MitB 攻撃（Man in the Browser 攻撃）と言われている。

その攻撃パターンは 2 つ存在し、1 つは、本人が ID とパスワードを入力して正規のサイトにログインすると、ウイルスが活動を開始し、裏で気付かれないように勝手に送金の操作を行うものである（取引偽造型 MitB 攻撃)。その際、乱数表の入力が必要となるとユーザに入力を求めることになる。

もう 1 つは一番高度な手口で、ウイルスがユーザの取引を改ざんする仕組みである（取引改ざん型 MitB 攻撃)。例えば、ユーザがインターネットバンキングにログインし「口座 A に 1 万円」と送金指図すると、ウイルスが勝手に裏側で「口座 X に 100 万円」と、口座番号、金額を変えて銀行サーバへ送信する。銀行から確認画面が戻ってくるが、その画面も改ざんし、元の指図通り「口座 A に 1 万円」と表示されるため、ユーザは攻撃に気付かないことになる。

海外では 2008 年頃から全てのタイプの攻撃が確認されている。米、独、伊、

蘭等で大規模発生した「Operation high roller」と呼ばれている一連の事件では、被害総額が 2 千億円にも上ったと試算されている。一方、国内をみると、取引偽造型 MitB 攻撃が 2014 年春頃から発生しているが、取引改ざん型 MitB 攻撃については確認されていない。

(3)被害急増の背景と海外動向

日本で被害が広がってきた背景は、攻撃ツールがインターネット上に流通し、簡単に使えるようになったことのほか、日本独自の理由として、不正送金した資金を現金で引出す方法等が確立していることがあげられる。これは、「振り込め詐欺」や「オレオレ詐欺」等の犯罪で使われるアルバイトの「出し子」を使った方法が、ネットバンキングの不正送金後の現金引出でも活用され始めたことや、日本の ATM の現金引出限度額が海外に比べ高いことが一因となっている。また、これまで、日本語の壁があると言われてきたが、日本語に堪能な協力者が犯罪組織に加わるようになったことによって、壁が無くなってきていることも要因としてあげられる。ただ、最大の理由は、日本のセキュリティが海外に比べて相対的に甘くなっていることかもしれない。海外において不正送金対策が進んできたため、ターゲットが海外から日本へ移行しつつある可能性がある。

英国におけるインターネットバンキングの被害額をみると、2012 年で 67 億円と、大きな金額が、それも恒常的に発生している。こうした中で、対策も進んでおり、英国の大手 5 行では、従来の時刻同期型 OTP（One Time Password）では不十分なため、振込先等の情報に紐付いた取引認証コードを生成する専用機器を導入している。

こうした中、アジアの対応をみると、シンガポールにおいて、シンガポール銀行協会（ABS)、シンガポール金融管理庁（MAS）が、取引認証の導入を強く求めたため、比較的対策が進んでいる。

また、中国については、遅れているようなイメージがあるが、必ずしもそうではない。中国人民銀行が、トランザクション署名[1]を基本機能として要求したため、中国 4 大銀行では、対話型 USB トークンといった、取引認証を行う専用

[1] トランザクション署名とは、ネットバンキングなどにおいて、送金などの処理情報（トランザクション）の内容（送金先の口座番号や金額など）をデジタル署名により暗号化し、トランザクションの内容が改ざんされていないかをサーバ側で確認できる仕組みのこと。

機器を導入している。中国では、金融機関の支店網が充実していないことから、インターネットバンキングのニーズが高く、2 千兆円ともいわれる額が、インターネットバンキングで取引されている。利用者側でも自分の預金は自分で守るといった意識が高いため、銀行による専用機器の導入指導に応じているといった背景がある。

中国 4 大銀行の 1 つ、中国工商銀行では、複数の認証方式を提供し、利用する方式により送金の上限額を変えている。一番セキュリティが高いタイプの対話型 USB トークン・トランザクション電子署名のケースでは、1 百万元（日本円で約 19 百万円）まで操作が行える。OCRA[2]仕様・トランザクション OTP 署名のケースでは 20 万元（日本円で約 380 万円）まで操作ができる。スクラッチカードによるワンタイム認証しか使用しないユーザは 2 千元（日本円で約 38 千円）までしか操作ができない。

(4)不正払出への対処

不正払出への対処として、キャッシュカードを使った ATM 取引であれば、自行のみならず提携行分も含め全て金融機関が管理する範囲にあるが、インターネットバンキングでは、ユーザが管理するパソコンを操作端末として使用するため、そのセキュリティの確保が難しい。MitB 攻撃という新しい攻撃に対し、ユーザの啓蒙とか、ウイルス対策ソフトの利用等様々な対策が考えられるが、結局はユーザのパソコンにおける対策であるため限界が存在する。こうした中、金融機関の対応として考えられるのが取引認証である。ユーザが行った取引に間違いがないことを署名で確かめる、あるいは、サーバで受付けた取引について、ユーザに確認してもらう必要がある。併せて、被害軽減とか事後検知といった観点からの対策も求められる。

①金融機関が採用すべき不正送金対策

日本における不正送金対策をみると、これまでは二要素認証あるいは多要素認証を導入することで、「本人認証」を強化する対策が中心となっている。これらは、ID、パスワード盗取型の攻撃には、ある程度有効な対策であった。しかしながら、MitB 攻撃に対しては無力であることが分かった以上、取引の内

[2] OATH(Open Authentication) Challenge-Response Algorithm. ワンタイムパスワードの規格の一つ。

容が正規のユーザの意図したものかどうかを確認する「取引認証」を速やかに導入する必要がある。「取引認証」の方法として、ここでは 3 つの事例を紹介する。

（方法 A）TAN 生成

1 つ目は、独立したデバイスで、取引内容に応じた TAN（Transaction Authentication No.＜確認コード＞）を生成し、取引認証として使用するものである。口座番号と取引額を入力すると、時刻情報も併せた OTP のようなものが表示される。それをインターネットバンキングを行っている際に入力すると、仮にその取引が書き換わった場合、TAN と不整合が生じることから、不正な取引であることが分かる仕組みとなっている。英国やシンガポールではこのタイプを採用している。

（方法 B）TAN 受信

2 つ目は、銀行サーバで取引を一旦受け取った後に、携帯電話の SMS（ショートメッセージサービス）等に取引内容とそれに合わせた TAN を送信し、それを確認したユーザがインターネットバンキングで入力すると取引が成立する方法である。

（方法 C）別端末で取引承認

3 つ目は、取引自体はパソコンを使用するが、スマートフォンの専用アプリで銀行サーバが受付けた取引内容を確認し、スマートフォンの確認画面で「OK」を出すと取引が成立する方法である。

国内における「取引認証」の導入状況をみると、取引認証機器を顧客に提供する先が出てきている。しかしながら、センター側のバンキングシステムが未対応なことから現時点では OTP としてしか使用していない。また、3 つ目に紹介した別端末で取引承認を行っている先が、ネット専業バンクに存在する。いずれにしても、一部において取引認証を導入したり、導入の準備を始める金融機関が出て来たことは評価できるが、こうした対応をより一層進めないとセキュリティは高まらないものと思われる。

一方で、取引認証機器を導入すればセキュリティは高まるものの、各行がそれぞれ対策を始めると、預金者は保有する金融機関の口座の数だけ機器を持つ

必要が生じ煩雑化するといった問題が発生する。この点、IC カードを使うタイプ（TAN 生成）で取引認証方法の共通化ができると、カードリーダーライターを共有できるメリットがある。ベルギーやオランダでは多くの銀行がこの IC カードを使うタイプにしているため、銀行毎にカードリーダーライターを揃える必要がない。また、ここで使用する IC カードについて、キャッシュカードとして配れば、キャッシュカードの IC カード化を同時に進めることができる。日本では、ATM の IC カード対応はかなり進んでいるが、キャッシュカードの IC 化は進んでいない。この背景には、昔発行したカードが永遠に使用できるといった問題が存在する。IC カードに強制的に切替えるためには、どうしたらよいかを考える時期になっていると思われる。

②金融機関の預金補償

金融機関の預金補償について、現時点では、金融機関は経営判断としてセキュリティ対策を採用するより、被害を補償することで預金者に迷惑をかけない道を選択している。また、金融機関は預金者に（重）過失がないと認められる場合、必ずしも保護対象ではないが、預貯金者保護法の趣旨に則って、不正払出の被害について補償している。この預金者に（重）過失がないと認められるかどうかについては、補償要件、補償基準を満たすかどうかで判断しているが、全銀協の資料をみると、補償要件は明確に記されているものの、補償基準については、明確に定めることが難しいとして個別判断としている。こうした中、一歩踏み込んで、全額補償が受けられない場合がある過失の具体例を示す金融機関も存在する。ただ、殆どの金融機関では注意喚起を行っているが、何を怠ると（重）過失に相当するのか分からない状況にある。

預金補償基準を分かりやすくするために、（重）過失となり得る場合とはどんな場合なのかを利用者に具体的に示すべきである。ただし、預金者に（重）過失がないと判断される状況は、世間の常識や社会通念によって変わっていく可能性がある点には留意が必要である。また、最近、インターネットバンキングの推奨環境を示している金融機関が殆どであるが、稼働保障の観点からであり、必ずしもセキュリティを意識したものにはなっていない。なお、さすがにセキュリティリスクが高いと考えられる Windows XP では非推奨環境に指定するだけでなく、サービスが稼働しないといった対応も必要ではないか。

こうした対応によって、預金者は、不正払出の被害者となるという万が一の

時に備え、補償が受けられるよう、（重）過失がないと認められる最低限の対策を行うようになることが期待される。

③リスクを下げるための他の対策例

その他、不正払出のリスクを下げるための対策として、3 点あげてみたい。1 つ目は「被害にいち早く気付かせる」工夫である。預貯金者保護法では、補償対象期間は、被害を金融機関に通知した日から遡って 30 日までと定められており、まず、その期間内に気付かせ、被害の拡大を抑えるためにも、残高や取引履歴を簡単に確認できる仕組みが必要となる。また、パソコンへのログインの際、前回ログイン履歴を示している金融機関は多いが、失敗履歴も含めて簡単に確認できる仕組みとし、ログイン日付に心当たりがなければ、金融機関にすぐに連絡してもらうといった仕掛けも考えられる。さらに、何らかの取引があった際に、事前に登録したメールアドレスに通知するサービスを提供している金融機関があるが、こうした対策も有効である。

2 つ目は「必要以上にリスクを負わせない」ということである。振込・振替等の限度額を必要な範囲内で、できるだけ低く設定してもらう、使わないユーザはゼロにすることも必要である。この点、最近残高照会のみで資金移動ができないサービスを提供する金融機関が増えており有効である。また、預金の全てをリスクに晒さないように、ネットバンキングで扱える預金を、口座の中で別段管理する方法も取れればよいと考えられる。

3 つ目は「パスワードの管理方法について」で、推測されにくいよう適切に設定させることである。具体的には、パスワードのログイン試行回数には制限があることから、例えば試行回数 5 回であれば、5 回で思いつくような、預金者の個人情報から容易に類推されるパスワードにさせないことが必要である。また、リバースブルートフォース攻撃[3]への対策として、パスワードは安易に設定されがちなものには設定できないようにシステム的に制限する考え方もある。さらに、どの金融機関もホームページをよく読むと「漏えいして 2 年以上経ったパスワードを使っている場合は補償対象外とする」旨の注意喚起がされているが、ユーザは承知していない。「2 年経つ前にパスワードを変更しな

[3] リバースブルートフォース攻撃とは、不正ログインを目的とするアカウント突破手法のうち、特定のパスワードとユーザ ID に使用される文字列の組み合わせを用いて、総当り的にログインを試みる手法。

いと不利益を得る可能性があること」を宣伝することも必要である。この他、パスワード等を自分だけがアクセスできる状態のメモに記録したりパソコンの中に保存することは止むを得ないが、少なくともパスワードそのものをそのままの形で記録しないよう推奨すること、一部にログイン ID を自由に設定できる金融機関が存在するが、パスワードリスト攻撃[4]を受ける可能性が高まるだけに、こうした対応はしないこと等が必要である。

（5）最後に

①金融機関にとってのバランス

金融機関は、セキュリティ対策は利便性とリスクとコストのバランスを考えて経営判断していると言うが、個々の前提が変わると結論も変わる可能性がある。

例えば、セキュリティ対策にかかるコストについては、販売促進費用（宣伝費）等から捻出する等の工夫の余地がある。ベルギーやオランダの事例では、ノベルティグッズとして自行名入りの取引認証用の IC カードリーダーライターを配布しているが、自行名が入っているので、それが宣伝になっている。

また、一律に被害を補償すると、対策を適切に行っている個人が相対的に不利益を被っているのではないかといった疑問が生じる。

さらに、コンプライアンスの観点であるが、やるべき対策をやらないために、反社勢力に金銭が流れる状況を放置しているとの見方も可能である。この他にも、都度振込の即時処理停止等にみられるように、利用者の利便性を著しく低下させることで対応している面が存在しているかもしれない。

②預金者にとってのバランス

金融機関は、利用者の利便性を損なうことに繋がる対策には慎重だが、一方で不安を感じて利用を控えている預金者が存在することも事実である。利用者が、サービスの利用や対策の導入の有無を自分で判断できるようにすること、すなわち、利用者が、利便性とリスクとコストのバランスを判断できるように

[4] パスワードリスト攻撃とは、攻撃対象とは別のサイトから得た ID とパスワードの一覧（リスト）を用い、攻撃対象のサイトでログインを試行する攻撃方法のこと。

正しく情報を提供するとともに、対策の選択肢を提供すべきである。

また、利用者のセキュリティリテラシーに応じたレベルのサービスの提供という考え方もある。預金者を不必要なリスクに晒すべきではなく、ユーザに応じて対応を変えるということである。

具体的な対応を 3 点あげると、1 つ目は、金融機関が提供する認証機器の利用有無、利用者のパソコンのセキュリティ対策の状況に応じて振込上限金額を変えるという発想がある。

2 つ目は、利用者にセキュリティリテラシーのテストを行い、結果に応じて提供するサービスを変えることも考えられる。この点、先日ある銀行のインターネットバンキングにログインしたところ、普段の注意喚起画面とは異なりチェックテストのようなものが出てきたことがあった。当該銀行では、こうした発想にあったのかもしれない。

3 つ目は、預貯金者保護法の存在が利用者に自分の預金は自分で守るというインセンティブを削いでいるといった意見もあるが、金融機関はそのインセンティブを持たせる方法を考えるべきである。これは、結果的に、セキュリティより利便性を重視する利用者にも配慮したことになる。

2.「セブン銀行の ATM 戦略とセキュリティ」（セブン銀行　石黒　和彦氏）

（1）会社概要

当社は 2001 年に開業して以来、ATM を中心とした経営を行っており、今年の夏には ATM の台数が 2 万台を超えた。2007 年以降は、海外で発行されたキャッシュカードやクレジットカードにも対応する ATM サービスを開始している。

当社の事業は大きく 2 つに分けられる。ひとつは、2 万台を超える ATM でお客さまに入出金を行って頂く「ATM サービス」であり、年間 7 億件を超える利用件数に達している。もうひとつは、預金、振込、融資といった「金融サービス」であり、最近は個人向けの海外送金なども手掛けている。経常収益の 9 割以上は「ATM サービス」からの収益が占めているが、個人の顧客から手数料を直接受け取っているのではなく、提携している金融機関やノンバンクから受け取っている ATM の利用手数料である。

当社はATM設置場所の拡大に注力しており、当社のグループ企業であるセブンイレブンやイトーヨーカドーの店舗に加えて、空港、駅（地下鉄を含む）、家電量販店、大型商業施設などにもATMを設置している。また、証券会社など、自社ATMの保有を望まない金融機関が、その代替として当社のATMを使うといったケースが出てきており、例えば、大手証券会社、新生銀行などは、支店内に当社のATMを設置している。また、岐阜県飛騨高山市には外国人観光客が多く訪れているが、十六銀行のATMは海外発行カードに対応していないため、同行飛騨高山支店内に当社のATMを設置している。

（2）外国人向けサービス

当社のATMでは、2007年から海外で発行されたカードの利用が可能となった。最近、わが国では外国人観光客が増加しており、本年は既に10月時点で1,000万人を超えたというニュースが報道されていた。こうした訪日観光客が最も不便に感じていることは、無料公衆無線LAN環境（WiFi）が使いにくいことであったが、最近、この問題は解消されつつある。残された訪日観光客の不満のひとつとして、日本のATMで海外発行カードが使用できないことが指摘されているが、当社のATMでは国際ブランドが網羅されており、海外発行のキャッシュカードおよびクレジットカードが24時間365日利用できる。

当社のATM画面とレシートは、日本語のほか、4か国語（英語、韓国語、中国語、ポルトガル語）で対応されている。また、お客さまがコールセンターと話すためのATM備え付けの電話でも英語対応を行っている。現在、言語対応のさらなる拡充を準備中である。

海外発行のカードが当社のATMで使われた場合には、当社センター、CAFIS[5]、日本のクレジットカード会社を経由して、海外のネットワークへと接続する仕組みになっている。海外発行カードについては、こうした取引電文の対応に加え、暗号化したテンキー（encryption pinpad）の実装が義務付けられているため、ATMの改造も必要となる。こうした海外カードサービスについては、日本のクレジットカード会社との資金決済、取引フローや明細票の多言語化、外国語でのコールセンター対応など、相応の投資が必要となっている。

[5] Credit And Finance Information System.　NTTデータが運営するカード決済のネットワーク。

当社 ATM での海外発行カードの取扱件数は、2011 年度が 150 万件、2012 年度が 220 万件、2013 年度が 240 万件、2014 年度上期は 180 万件となっており、2014 年度は 380 万件と見込んでおり、かなり急激に増加している。当社では、2020 年のオリンピックに向けて、海外発行カードの取扱件数がさらに一段と伸びていくとみている。このように海外発行カードの利用実績は伸びているが、一方で、セキュリティ対応や初期対応などに相応のコストを要しているため、期間損益は黒字化したものの、まだ累損解消に至っていない。

(3)セキュリティ強化策

当社では、開業当時からコンビニエンスストアに ATM を設置しているため、ATM を使うお客さまと店舗の安全を最優先する仕組みを採用している。具体的には、警察庁の基準などを参照し、ATM への警報ボタンの設置、店舗外周へのパトライト設置、店内の画像監視などを行っている。

当社の ATM は、日本自動販売機工業会が定めた防犯筐体の最高レベルをクリアしている。

当社は「全銀 IC 基本形[6]」への移行を 2012 年に完了している。当社の提携先金融機関は 121 行であり、このうち 112 行が当社 ATM での IC 取引に対応済みとなっているが、当社 ATM での IC 取引の割合は一定の割合にとどまっており、残りは、従来からの磁気ストライプによる取引で占められている。磁気ストライプによる取引の多さは、キャッシュカードにはクレジットカードのような有効期限が無いため、IC カード化されていないものでも、ずっと使い続けることができることによる。

(4)セキュリティ強化策(海外発行カード関連)

[6] 平成 13 年 3 月、全国銀行協会では、IC カードの新しい標準仕様である「全銀協 IC キャッシュカード標準仕様」を取り纏めたが、金融機関のホストシステムの更改に要する時間を考慮して、平成 17 年度末までを「経過期間」として設定し、端末・ホスト間の通信は従来と同一の電文形式で行い、IC カード認証はオフラインで行う扱いとした。その後、平成 24 年には、統合 ATM ネットワークの更改に伴って経過期間が終了し、「基本形」(ホストシステムで IC カードの認証を実行する形態)に移行した。従来の全銀協仕様は国際規格 ISO9992 に準拠していたが、「全銀協 IC キャッシュカード標準仕様」は、クレジットカードの国際的な共通仕様である EMV 仕様を採用している。

①ATM を取り巻く犯罪の傾向

海外発行カードと国内発行カードを比較すると、取扱件数では国内発行カードの方が多いが、偽造件数は海外発行カードの方が圧倒的に多い。犯罪傾向としては、「グローバルで偽造カードを作成し、他国で不正利用する」という手口が主流となっている。当社やゆうちょ銀行は海外発行カード対応を行っているため、こうした犯罪のターゲットにされやすい。

犯罪で最も多い手口はスキミングである。海外でスキミングを行って磁気ストライプの情報を盗み取り、そのデータを別の国に持ってきて偽造カードを作成し、その国の ATM で資金を引き出す、という手口である。

②スキミングの被害実績

当社も 2013 年 2 月にスキミングの被害に遭った。5 か所で犯行が行われたが、いずれもコンビニ店内の ATM ではなく、「店舗の近くにあるものの、外側を向いている ATM」や人気の少ない所に置かれている ATM が狙われた。この事件では、ATM のカード挿入口の上からスキマーを取り付けられたが、ATM と殆ど同じ色の素材で作られていたため、外観からは分かりにくかった。また、ATM の両脇に設置されている「バイザー」と呼ばれる目隠し用の壁に、ゴミ箱を装ったカメラ内蔵の箱を取り付けられており、お客さまが暗証番号をボタンで押している様子が撮影されていた。

このスキミング装置（スキマー）は、カード裏面に磁気ストライプのある海外発行タイプのカードしか読み取れない仕組みになっていたため、海外の犯罪者集団の手口だと考えられる。カード表面に磁気ストライプのある日本発行タイプのカードを使っても被害を受けなかったのが不幸中の幸いであった。

③スキミング対策

この事件を受けて、当社では約 1 年で犯罪対策を完了した。当社の講じた主な犯罪対策は、「ジッタコントロール」、「不審カード検知」、「盗撮カメラ検知」、「スキマー検知」などである[7]。

[7] 機能の詳細はセキュリティに関わる情報のため記載していない。

当社 ATM の監視カメラは、異常を検知すると過去に遡って画像を保存する機能を持っている。不審カード、盗撮カメラ疑い、スキマー疑いなどは、監視係の職員が 24 時間駐在しているコールセンターに通知される。

④ATM のセキュリティ対策のトレンド把握

ATM のセキュリティ対策のトレンドを把握するため、当社では様々な情報収集を行っている。その中で非常に有効だと感じているのが、2004 年に欧州で結成された「EAST」への加入である。この団体に加入したことにより、犯罪速報やセキュリティ会議のレポートの入手、各種フォーラムへの参加など、ATM 犯罪に対する最新の情報収集が可能となっており、年会費も 10 万円程度とさほど高くない。

スキミングのトレンドとしては、スキマーや盗撮カメラなど装置の小型化・精巧化が進んでいる。とくに EMV[8]（後述）にまだ対応していない北米、南米、アジアといった地域での被害が増加している。カード挿入口に取り付けられるスキマーについては、挿入口の内部に完全に入り込んでしまうような内部隠蔽タイプも現れてきている。

⑤海外偽造カード対策

スキミングで奪われたデータから作成された偽造カードについて、当社は 2013 年 3 月から 2 回に亘って対策――本格的な EMV 準拠の対策は準備中であるため、当社では「暫定対策」[9]と呼んでいるが――を講じ、被害が激減した。

⑥海外偽造カード事案の具体例

これまでに最も被害の大きかった偽造カード事件が「バンクマスカット事案」である。オマーンに本拠を持つ銀行が狙われ、全世界で約 40 億円が同時に引き出された事件である。狙われたのは当該銀行のプリペイドカードの口座であり、犯人は口座の決済管理を委託されている企業のシステムに不正侵入し、口座残高を積み上る操作をしたうえで、世界各国で同時に資金を引き出した。

---

[8] Europay, MasterCard,Visa により統一された IC カードの仕様。
[9] 機能の詳細はセキュリティに関わる情報のため記載していない。

この事案の発生後、当社では大量不正出金対策を講じた。具体的には、一定期間内に同一口座から多額の出金が繰り返し行われるケースなど、不審が疑われる事例を類型化したうえでネガ登録し、当該口座の取引を行おうとしたカードがあれば、ATM に吸い込んで回収してしまうわけである。

(5)取り組み中の対応

現在、偽造カードによる被害は、カード発行会社（イシュアー）の責任とされるが、今後は、IC 未対応の ATM 運営会社[10]に、上限なしで被害金を負担させる「ライアビリティシフト」の導入が予定されている[11]。この国際標準規格は 2016 年頃に本格的に導入される予定であるため、当社では 2015 年 12 月を目途として本格的な IC 化に取り組んでいる。

現行対応との違いは、IC チップに格納されている情報を海外のイシュアーに照会して真偽を確認するという点であり、取引電文なども複雑化されるため、クレジットカード会社や NTT データを含めた対応が必要となる。

当社では第三世代の ATM が最新機種となっているが、2020 年の東京オリンピック開催を展望して、第四世代の検討に着手している。この検討においても、とくにセキュリティに力を入れて対応したいと考えている。

Ⅳ. 自由討議要旨

1. キャッシュカードにおける磁気ストライプから IC への切替

(1)海外の状況

・　欧州は比較的経済規模が小さな国が多く、例えば英国では 2003～04 年頃、1 年間で磁気ストライプから IC カードと PIN[12]による認証方法に切替えることができた。一方、北米では、経済規模が大きいため、未だに IC カードが普及していないようである。わが国は、相応に大きな経済規模であるほか、金融機関数も多いため、協調して IC カードに切替えていくことが難しい。

---

[10] 日本では銀行に限られるが、海外では銀行以外の運営会社が含まれる。
[11] 国をまたがった取引のみが対象となる。国内で発行されたクレジットカードの国内利用について、当該ルールは適用されず、発行者の負担となる。
[12] Personal Identification Number. 個人認証番号。

・　米国では、現時点での IC カードの普及率は低いが、足もと急速に追い上げており、早晩わが国を上回ると言われている。海外では、銀行本体によるクレジットカードの発行が可能であるので、クレジットカードとキャッシュカードの機能を 1 枚に集約できる。このため、海外では、クレジットカードの切替タイミングに、キャッシュカードの IC カード化が可能となる。気がついたら、わが国だけ取り残され、他の国々は IC カード化が完了していた、ということもあり得る。

・　米国 FRB[13]が今年 9 月に公表した Federal Payment Survey によれば、ACH[14]関連での詐欺の被害額（2012 年度）は、件数 3,100 万件、金額 60 億ドル程度となっていた。米国は、磁気ストライプから IC カードへの切替を急ピッチで行っている。このため、締め出された犯罪者が日本に狙いを変える可能性がある。わが国の銀行界は 3,000～4,000 億円規模の損害を受けるかもしれない。

・　アジア各国のキャッシュカードの状況をみると、シンガポールでは 2014 年度から IC カード化が進んでいる。マレーシアでも来年から IC カードを導入予定である。ASEAN の主要 5 か国[15]のほか、ベトナムでも 2017 年くらいを目途として、銀行発行カードの EMV 仕様への対応を進める計画である。

・　前述の EMV 化とともに、ASEAN では 2015 年に経済統合を行うこともあって、「ASEAN Integration card」というクロスボーダーの EMV カードの発行について意思決定された。例えばインドネシアで発行されたカードが、シンガポールでも利用できるというものだ。カード以外のデバイスについても統合を進める方針にある。最近開催された ASEAN の銀行協会の集まりでこうした方針が決議された。わが国でも何らかの対策を講じないと、セキュリティ後進国になりかねない。

（2）わが国の状況

・　わが国は以前からセキュリティ後進国である。ただ、犯罪発生率が低いと

[13] Federal Reserve Board. 連邦準備制度理事会。
[14] Automated Clearing House. 連邦準備銀行等で運営されている小口取引の資金決済ネットワーク。
[15] インドネシア、マレーシア、フィリピン、シンガポール、タイ

か、金融機関のネットワークが閉鎖的であるなどにより、結果としてセキュリティ犯罪の被害額はそれほど大きくなかった。顧客の利便性を優先するあまり、新しいシステムへの切替を進めなかったため、結果的にセキュリティレベルが低くなってしまっているのが、わが国の現状だと思う。

・　磁気ストライプのキャッシュカードは累計 10 億枚発行されている。これらのカードの中には、かなり昔に発行され、持ち主の住所が変わったもの等が含まれているが、現在も使用は可能となっている。金融機関では、ATM 側で IC カードに対応できるようになっても、顧客が現在使っている磁気ストライプの継続使用に配慮している。セキュリティ上脆弱なものでも、そのまま使えるようにしておくことは、顧客にとってもプラスにならないと思われる。

・　当行では、生体認証カードを発行している。手続きが煩雑だと、顧客が受入れにくいことに配慮し、店頭即時発行のサービスを行っているが、普及はさほど進捗していない。

・　信用金庫は、IC カードを発行している。一部では生体認証にも対応している。

・　セブン銀行の石黒さんに質問したい。欧州のユーザが持ち込んだ IC カードを、わが国の ATM で利用する場合、IC チップの内容を読んで、取引認証に利用しているのか。

――　本質問に関し、石黒氏から以下の説明があった。
　現状では欧州で発行された IC カードについても、磁気ストライプによる取引認証を行っている。

(3)マイナンバー制度導入の活用

・　キャッシュカードの IC カード化については、2016 年から開始されるマイナンバー制度の活用が考えられる。マイナンバーが通知された後、個人の任意によって、マイナンバーの IC カードが発行される予定にある。これをキャッシュカードの IC カード化を進めていく上で活用できると思う。例えば、運転免許証がマイナンバーの IC カードになれば、それとキャッシュカードを統合するといったことである。

・　現時点では金融機関が個人のマイナンバー情報を、法定業務以外で利用することを禁じられている。ただ、今年4月に政府税調のワーキンググループから出された答申[16]によれば、将来的には金融機関の預金口座にもマイナンバーを付番していくべきとされている。

・　実際にマイナンバーを付番するには大きなコストを伴うため、10億以上の個人預金口座への対応をどうするのかという問題がある。また既に発行されている 10 億枚の磁気ストライプカードの切替をどうするのかという問題もある。一方で、マイナンバー、預金口座およびICカードがリンクされれば、こうした問題を同時に解決し得る可能性がある。

2. インターネットバンキングにおける認証方法の高度化

・　インターネットバンキングでは、毎回の取引に対して認証入力を行うべきとの話があった。毎回の作業が必要となることに関し、顧客の理解は得られるのかお聞きしたい。

――　本質問に対し、金融研究所の中山から以下の回答があった。

顧客の利便性に配慮すると、例えば新規の振込時に、その都度認証入力を求める一方、2回目以降の振込では、振込口座の確認ができているため認証入力を省略するなどの対応もあり得る。実際、海外事例をみると、導入当初は毎回の認証入力を求めていたが、その後、新規振込先のみに認証入力を求めるように対応を変えたケースもある。

・　毎回の認証入力を求められるようになったベルギーやオランダでは、顧客の新たな対応負担への苦情や、金融機関が顧客側の古いシステムに対応しないことを「サービスの低下」と捉える議論はなかったのか。

――　本質問に対し、金融研究所の中山から以下の回答があった。

海外では、セキュリティ被害が多いことから顧客の危機意識が高く、金融機関が提供するセキュリティレベル向上の働きかけにも積極的に応じている。ICカードの利用比率が9割以上であるなどセキュリティリテラシーも高い。

[16] 「論点整理」マイナンバーDG（内閣府、平成26年4月8日）

・　当行のインターネットバンキングでは、取引毎の認証が可能なパスワードカードを取り入れている。

・　トランザクション毎の認証は、現段階では効果的ではあると思うが、将来に亘って有効であるとは限らない。

・　当行でインターネットバンキングを利用している顧客は、全体の 8%程度であり、その多くは残高照会の利用である。インターネットで経常的に資金移動を行っている顧客は、インターネットバンキング利用者の 3 分の 1 程度であり、顧客全体の 2～3 %に過ぎない。この範囲の顧客のために、どこまで投資を行うのかが、地域金融機関の共通の悩みである。

3. 顧客側のシステム環境の問題

・　法人インターネットバンキングに関し、顧客側で、古い PC 環境から新しい PC 環境へどう移行してもらうか、は難しい問題である。当行のサービスの変更により、Windows XP を利用している顧客の端末で動作しない、といった事象が起きた際に、Windows XP でも利用できるようにソフトの変更を行った。このような社内の IT 環境をすぐには変えられないとの事例は、中小企業に限らず、大企業でもみられている。

・　顧客がサポート期限の切れた Windows XP を使用しているから、金融機関も古い OS をサポートしなければならないとなると、マイクロソフトが使用を止めるようにアナウンスしていることと正反対のことを行うことになる。このあたりは金融機関のシステムというよりも、サービスのスタイルの在り方自体が追いついていないということだ。

・　未だ Windows XP を使用している企業が多いとの話があったが、大手企業を含めてこうした状況がみられている。一般的なパッケージソフトウエアなら新 OS 対応も簡単だが、独自に組み上げたシステムの場合はなかなか移行できない。

4. 顧客のセキュリティリテラシーを踏まえた対応

・　顧客が求めるセキュリティと利便性のバランスが変わってきている、と思う。従来以上にセキュリティに手間がかかり、顧客に実害が出始めている中、

利便性を求める顧客においては、銀行が求めるセキュリティ上の要求に応えていく方向にあると思う。

・　日本の金融機関は顧客を一律に捉えがちだが、顧客のセキュリティリテラシーのレベルには相当の差がある。その違いに応じてセキュリティに関するサービスを提供していくべきである。例えば、顧客の財産を守るために銀行が高度なセキュリティを提供する場合には、それに見合った手数料を取る、としても良いのではないか。

・　セキュリティに関する顧客の理解向上は重要である。稚拙な文面のフィッシングメールであるにもかかわらず、銀行によるものと信じて反応している顧客が一定数いる。我々は、顧客への注意喚起のためのテストも実施している。

・　当行では、様々なセキュリティ対策を用意して、顧客の事情に応じて選んでもらうようにしている。例えば、「複数の承認者による取引ができないのであれば、セキュリティ対策ソフトを導入してください」とする一方、「セキュリティ対策ソフトが導入できない PC 環境であれば、複数の承認者で対応してください」といったように対策のバラエティを増やす取組みを行っている。

・　当行でも、顧客にとってのセキュリティ対策の選択肢を増やしていこうとしている。

・　当社グループはメーカーであるため技術を守る意識が高く、情報セキュリティに関し親会社のチェックが行われている。如何に高品質の製品を生産していても、情報セキュリティ水準が親会社の求める基準を下回ると、取引停止のペナルティが課せられる。そのため、システム対応のほかに社員のセキュリティリテラシー教育も行っている。

・　わが国の場合、ユーザ側の啓蒙と同時に、銀行側への啓蒙が相当難しい。銀行経営者が IT やセキュリティを自身の問題としてみていないことが一番の問題である。

5. 損害発生時の責任分担

・　顧客によって、一律のセキュリティに追随できない先もいる。従って、補

償基準を打ち出すことはやむを得ないと思っている。信用金庫業界では、統一的な補償基準の策定について検討している。

・　インターネットバンキング被害により損失が発生した場合、金融機関とユーザで、どのような損失分担ルールを設定すればよいのかを論じた米国の論文がある。ルールの 1 つ目は、損失を負うことで最も影響が少ない人に損失を負わせるべきというものである。金融機関と個人では、体力のある金融機関に損失を負わせることになる。ルールの 2 つ目は、より少ないコストで損失を削減できる人に損失を負わせることである。実際は、なかなか金融機関、ユーザの一方だけに損失を負わせること難しい。例えば、「ユーザにシステムを Windows XP から更新してもらえないと十分なセキュリティを確保することは難しい」との話があったとおり、金融機関にもユーザにも応分の損失負担を求めることになる。ルールの 3 つ目は、損失分担ルールは明確であることが重要ということである。そういう点では、信用金庫業界で、ルールを共通化・明確化するということも、この考え方に沿ったものと思う。

・　米国では､カードの変造や偽造に関して 50 ドルルール[17]というものがある。ユーザが早く被害に気付いて通報すると、その損失は 50 ドルの範囲内に留められる。一方で、何も対応を図らないとユーザの負担割合が増していく形で、ユーザにある程度のインセンティブを与える仕組みとなっている。何が何でも補償するやり方は、ユーザのセキュリティ向上意識を削ぐことになるため、こうしたバランスが重要となる。

6. 金融機関同士の協力

(1)金融機関同士での情報共有等の協力

・　セキュリティ犯罪の手口が次第に高度化している。海外で事件が発生し防止策が取られた結果、対策が手薄な日本が狙われるとすると、いち早く海外事例をキャッチすることが重要になってくる。海外の金融機関で発生したセキュリティ犯罪に関する情報共有を図る仕組みの整備は有効な施策である。国内の金融機関でも個別に CSIRT[18]などを導入しているが、アンテ

[17] 米国の連邦電子資金移動法（Electronic Fund Transfer Act）909 条。
[18] Computer Security Incident Response Team.

ナを高くし海外事例をいち早く収集するなどの態勢面での整備は重要と思う。

・　個別の金融機関がセキュリティ対策で差別化を図るといった考え方と業界全体で連携してセキュリティ対応力を高めていくといった考え方があるが、どちらの方向で対応すべきか、皆さんの意見を伺いたい。

・　基本的には業界全体でセキュリティレベルの底上げを図りたい。IC カード対応のほか、生体認証などの認証方法も業界で統一できれば良い。また、インターネットバンキングについては、あまり有効な対策ができていない。取引認証も検討しているが、スマホでアプリをダウンロードする方法だと、普通の携帯電話しか持っていない人はどうするのかなど苦労している。このあたりも業界一体の取組みができないか検討したい。

・　当行では他行とのセキュリティ事例の情報交換を進めており、かなり細かい点まで共有している。各行におけるシステムの違いもあり、全てが同じ足並みにはなってないが、目指す方向は同じである。また補償基準については、海外事例をみても各国の法制度の違いから全てを理解できているわけではない。こうしたことは個別に確認していくことは負担となるため、知見のある先と情報共有を図りたい。

・　海外のセキュリティ事例については、例えばインターネットバンキングの不正の手口に対する教育や各行が想定している対策内容など、金融機関の間である程度情報交換が始まっており、結果的に各行の対応策が同じような方向に向かっている。セキュリティ対応が不十分な顧客についても、相応に移行期間を設けて、例えばワンタイムパスワードが無いと振込ができないなどの啓蒙活動を通して対応していく方向にある。こうした取組みを進めるなかで、銀行業界はもちろんのこと、官民や産官学で情報共有の場が設けられることは重要かと思う。

・　モニタリングについて業界全体で取組むという考え方もあると思う。例えば、ユーザへの通知という点では、送金を取組んだ時に、仕向け先だけでなく、被仕向け先からの通知もあればクロスチェックが可能となる。

・　情報共有という点では、日本銀行金融研究所もセキュリティの観点から、様々な場を設けている。情報セキュリティのシンポジウムやセミナーで金融

機関に最新技術に関して情報還元を図っている。

（2）セキュリティ対策の技術標準

- 全ての金融機関が個別に同じような対応を考えるのは非効率であるので、統一された指針が出されれば取組み易いと思う。一方、技術的な問題では金融機関以外にシステムベンダーが関係してくる。例えば静脈認証の方法をみても、ベンダー毎に検知方法が指や手のひらなど仕様が異なる。セキュリティ業務に対しては、柔軟な選択肢を設定するなどある程度の幅を持たせた指針が必要かと思う。

- 金融機関のセキュリティ対策の技術標準を作成することについては、過去に、旧大蔵省銀行局の局長通達（所謂、「機械化通達」）があった。ところが金融機関のシステムインフラや ATM やインターネットバンキングなどのサービスの実態に追い付かなくなったこともあり、通達が廃止になったという経緯がある。セキュリティ対策の技術標準策定について、未だセキュリティに関するリテラシーが高くなかった 1990 年代では、多少無理があったと思う。ただ、米国では ANSI X9 Committee[19] や NACHA[20]、英国では APACS[21]が様々な技術標準を出しているので、こうした取組みを進めることも必要かと思う。

- 韓国では、金融監督法で必要な IT 投資額やセキュリティ投資額を定めており、金融監督院の検査でチェックを行っている。

７．その他

- セキュリティ対策については、犯罪者が割に合わないようにするのがポイントである。怪しい口座の凍結のほか、韓国で行われているような資金移動後の一定時間、現金の引出ができないようにする、といった対策が必要であると思う。

---

[19] 米国国内の標準化機関である ANSI (American National Standards Institute) の下で金融業界の標準化を行っている標準化委員会。

[20] National Automated Clearing House Association. 米国自動決済協会。

[21] Association for Payment Clearing Services. 銀行共同支払決済機構。現在は UK Payments Administration Ltd (UKPA) に名称変更。

・　当行では、サーバ側での自動検知のほか、有人のモニタリングも行っている。有人モニタリングについては、不正防止の効果が上がっている。

・　いろいろな情報を共有化することで対策コストの削減を図るということ、セキュリティ対策そのものを差別化要因として、金融機関の競争力として活用していくという議論があったが、例えばアジア各国における EMV の導入に関して、EMVCo[22]を構成する VISA や銀聯が技術的な供与を行っている。つまり、セキュリティ技術が貿易財になっている。わが国のセキュリティ技術の高度化も、将来的にはインフラ輸出により開発コストを回収することまで展望して取組むことが重要かと思う。

以　上

[22] EMV 仕様の策定、承認等を行う機関。

（別 添）

ワークショップ参加者（敬称略）

（プレゼンテーター）

石黒　和彦　　株式会社　セブン銀行　取締役　常務執行役員

松橋　正明　　株式会社　セブン銀行　執行役員　ATM ソリューション部　部長

深澤　孝治　　株式会社　セブン銀行　ATM ソリューション部　副部長

水村　洋一　　株式会社　セブン銀行　ATM ソリューション部　主任調査役

中山　靖司　　日本銀行　金融研究所　制度基盤研究課　情報技術研究センター　情報技術研究グループ　グループ長

（招待参加者）

梅崎　富雄　　株式会社　三菱東京 UFJ 銀行　リテール事業部　インターネットバンキング・セキュリティ対策室　室長

加藤　毅　　株式会社　横浜銀行　営業企画部　マーケティンググループ　グループ長

兼子　邦彦　　小嶋プレス工業株式会社　総務統括部　参事

島田　直貴　　株式会社　金融ビジネスアンドテクノロジー　代表

瀬田　和則　　株式会社　みずほ銀行　e - ビジネス営業部　部長

中山　知章　　株式会社　三井住友銀行　決済企画部　部長

三澤　敏幸　　朝日信用金庫　理事　システム部　部長

山上　聰　　株式会社　NTT データ経営研究所　金融戦略コンサルティング部門　パートナー

（日本銀行）

鈴木　淳人　　金融研究所　制度基盤研究課長

田口　哲也　　金融機構局　金融データ課長

志村　秀一　　金融機構局　考査企画課　システム・業務継続グループ長

岩下 直行　　金融機構局　金融高度化センター長

山口 省蔵　　金融機構局　金融高度化センター 副センター長