第17回
情報セキュリティ・シンポジウム「金融取引を安心安全に実現するための認証技術：FinTech時代も意識して」の模様

要　旨

日本銀行金融研究所は、2016年3月2日、「金融取引を安心安全に実現するための認証技術：FinTech時代も意識して」をテーマとして、第17回情報セキュリティ・シンポジウムを開催した。

インターネット・バンキングに関わる脅威と不正対策への関心は、近年高まる傾向にある。また、「FinTech」と呼ばれ、注目を集めている新しい金融サービスも、主にインターネット経由で提供されるため、同様のセキュリティ問題に晒されている。新旧いずれのサービスにおいても、利用者や取引内容を確認することで安心安全な金融取引を実現する「認証」が重要な役割を担っており、同技術を巡る最新動向を継続的に把握し、活用方法を検討することが重要である。その際、技術の発展・普及の観点から、セキュリティ（安全性）、利便性、網羅性の3つの要素をバランスよく満たす認証技術の開発が望まれる。

本シンポジウムでは、認証技術に関わる研究開発の最新動向を紹介する講演を当研究所スタッフと外部研究者が行った。また、外部の専門家を招いて、「インターネット・バンキングのさらなる発展に向けて」と題するパネル・ディスカッションを行い、セキュリティ・利便性・網羅性の間でバランスを取るためには、いかなる方法が有効かといった点について議論した。本稿では、キーノート・スピーチ、4つの講演、パネル・ディスカッションの概要を紹介する。

キーワード：異常検知、インターネット・バンキング、生体認証、取引認証、認証プロトコル、FinTech、TEE

本稿に示されている意見はすべて発言者たち個人に属し、その所属する組織の公式見解を示すものではない。

1. はじめに

インターネット・バンキングに関わる脅威と不正対策に対する関心は、近年、益々高まる傾向にある。また、金融分野においては、ネットワークやモバイル端末（スマートフォン等）をはじめとする最新の情報技術を活用したサービスが相次いで登場しており、これらは「FinTech」と呼ばれ、俄かに注目を集めている。これらの金融取引の多くは、インターネット等のオープンなネットワークを介して実施されるものであり、新旧いずれのサービスにおいても、利用者や取引内容を確認するための「認証」が重要な役割を担う。したがって、インターネット上で安心安全な金融取引を実現していくためにも、認証を巡るセキュリティ上の課題やその克服に資する研究開発の動向を継続的に把握し、それらの活用について検討していくことが重要である。その際、セキュリティ（安全性）を強調するばかりでは、技術の発展・普及を阻害することになりかねず、利便性（サービス利用者にとっての使いやすさ）、網羅性（適用可能なサービス利用者の範囲の広さ）という 3 つの要素をバランスよく満たす認証技術の開発が望まれる。

こうした問題意識に基づき、日本銀行金融研究所は、2016 年 3 月 2 日、「金融取引を安心安全に実現するための認証技術：FinTech 時代も意識して」をテーマとして、第 17 回情報セキュリティ・シンポジウムを開催した（プログラムは以下のとおり[1]）。当日は、金融機関の実務者や官公庁関係者、暗号学者、システム開発・運用に携わる実務者等、計 160 名が参加した。以下では、本シンポジウムの概要をプログラムに沿って紹介する（以下、敬称略、文責：日本銀行金融研究所）。

【第 17 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「金融取引を安心安全に実現するための認証技術：FinTech 時代も意識して」
  横浜国立大学大学院　教授　松本勉
- 講演 1「次世代認証技術を金融機関等が導入する際の留意点：FIDO を中心に」
  日本銀行金融研究所　企画役補佐　井澤秀益
- 講演 2「生体認証システムのセキュリティ評価：人工物を用いた攻撃に焦点を当てて」
  日本銀行金融研究所　企画役　宇根正志
- 講演 3「暗号ハードウェア等に対するセキュリティ評価および留意点」
  日本銀行金融研究所　清藤武暢

1 文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。

- 講演 4「情報セキュリティのための異常検知技術」
  東京大学大学院　教授　山西健司
- パネル・ディスカッション「インターネット・バンキングのさらなる発展に向けて」
  モデレータ：横浜国立大学大学院　教授　松本勉
  パネリスト：金融 ISAC 理事／ FS-ISAC Regional Director　鎌田敬介
  セコム株式会社 IS 研究所　マネージャー　松本泰
  産業技術総合研究所　研究戦略部連携主幹　高木浩光

2. キーノート・スピーチ「金融取引を安心安全に実現するための認証技術：FinTech 時代も意識して」

松本（勉）は、本シンポジウムのテーマとその背景について次のとおり報告した。

(1) 前回のシンポジウムで示された課題

今回のシンポジウムでは、認証技術に焦点を当てる。前回のシンポジウムでは、インターネット・バンキングの脅威と対策に関する講演やパネル・ディスカッションを行い、今後のセキュリティ対策を考える際には、次の 2 点について、検討していくことが必要であるとの意見がパネリストから示された。すなわち、①セキュリティの観点だけでなく利便性や網羅性とのバランスを考慮する必要がある、②金融分野や情報技術分野における今後の環境変化に伴うリスクも考慮しておくこと、が肝要である。今回のシンポジウムでは、これらの意見を課題として捉え、認証技術について、より踏み込んだ議論を行いたい。

(2) 金融分野や情報技術分野における環境変化

最近の金融業界において、情報技術と関連が深い動きとして、FinTech が挙げられる。FinTech は、「情報通信技術を活用した革新的な金融サービスやビジネス」を指す用語（日本カードビジネス研究会［2015］）であり、個人財務管理、オンライン融資、クラウド・ファンディング、スマートフォンによる送金等、スタートアップ企業によってネットワーク経由で提供される新しいサービスが代表的である（日

経 BP 社［2015］）。FinTech が登場してきた技術的背景としては、①サービス利用者側の環境変化（スマートフォン、SNS 等の普及）、②サービス提供者側の環境変化（クラウドサービスの活用等）、③情報解析技術の進化（リアルタイムでのデータ解析、機械学習等）が挙げられる。

また、従来から金融機関が提供しているインターネット・バンキングに関しては、わが国では預金等の不正払戻し金額が増加傾向にあることが注目される（全国銀行協会［2015］）。海外では、MitB（Man-in-the-Browser）攻撃[2] に加え、不正送金取引を DDoS（Distributed Denial-of-Service）攻撃[3] と組み合わせた攻撃の事例も報告されるなど（Kuhn [2015]）、手口が一段と巧妙化してきている。

各種の金融サービスを安心安全に実現するうえで重要なのが認証である。認証にかかる基本的なセキュリティ要件を挙げると、（a）サービスの利用者と提供者がネットワークを介してお互いの正当性を確認すること（サービス利用者認証／提供者認証）と（b）MitB 攻撃に対抗するために、サービス提供者が金融取引の正当性（取引内容がサービス利用者の意思に基づくものであること）を確認すること（取引認証）の 2 点である。金融機関等のサービス提供者は、当該サービスにおける業務リスクを把握し、セキュリティ・利便性・網羅性の間のバランスを勘案しつつ、上記の要件等を満たす認証技術を選択することが望まれる。

(3) 今次シンポジウムで取り上げるトピック

今回のシンポジウムでは、認証技術を巡る最新の動向について、4 つの講演が用意されている。講演 1 では、スマートフォン等においてサービス利用者認証や取引認証を実現する認証プロトコルとして最近注目を集めている FIDO（Fast IDentity Online）を紹介し、それをインターネット・バンキングに適用した場合のセキュリティを評価する。講演 2、3 では、FIDO で活用される生体認証や暗号ハードウェア等の技術動向や利用上の留意点について説明する。また、講演 4 では、データマイニングによる異常検知技術を取り上げ、金融取引のデータ等に異常検知技術を適用し、「異常」と判定されるデータを手掛りに不正な取引を検知するという手法の可能性について報告する。

後半のパネル・ディスカッションでは、インターネット・バンキングに焦点を当てつつ、認証技術を活用する際の留意点や実務上の課題について議論する。主な論点は、①認証を正確に行うためにはいかなるユーザインタフェース設計が有効なの

2 マルウエアに感染した端末（PC やスマートフォン）のブラウザを不正に操作し、ブラウザの表示内容やサーバとの通信内容を改ざんする攻撃。

3 複数の攻撃者から攻撃対象のシステム（サーバ等）に対して、一斉にパケットを送信する攻撃。この攻撃を受けたシステムは、処理能力が飽和状態となりサービスを提供できなくなってしまう。

か、②新しい認証技術を導入する際に既存の技術（レガシー技術）との棲分けや移行をどのように進めていけばよいのか、③セキュリティ・利便性・網羅性の間のバランスをどのようにとっていけばよいのか、という 3 つである。それぞれの論点について、パネリストに意見を求めるとともに、フロアからの質問や意見も交えて、議論を深めていければと考えている。

金融機関は、外部環境が激しく変化するなかで、複雑化するリスクに対処していかなければならない。攻撃者は常に新たな攻撃の手法を編み出している。金融機関は、そうした動きに対し、休むことなく対策を講じていく必要がある。そのためには、攻撃手法を含めた様々なリスクを幅広くフォローしておくことが望ましいことは言うまでもない。加えて、脅威の発生が予見された場合、インシデントを未然に防ぐために、プロアクティブなセキュリティ向上策を迅速に企画することができるよう、組織力を強化しておくことも必要である。金融機関は、金融分野のみならず、様々な分野で生じたインシデントを観察・分析することによって、新たな攻撃手法が自社（自業界）に対していかなる悪影響を及ぼし得るかを想像する力を強化していくことが肝要である。

3. 講演 1「次世代認証技術を金融機関等が導入する際の留意点：FIDO を中心に」

井澤 は、井澤・五味［2016］に基づき、次世代認証技術の 1 つとして注目されている FIDO をインターネット・バンキングに適用するケースを想定し、そのセキュリティ評価の結果と導入時の留意点について、次のとおり報告した。

(1) FIDO を適用したインターネット・バンキングの安全性評価

FIDO は、サービスの利用者と提供者の間で、ネットワーク越しの認証に、生体認証等を利用するための手順（プロトコル）を定めた技術仕様である。FIDO は、FIDO アライアンス（Alliance）によって 2014 年 12 月に策定された。既に、一部のスマートフォンで、FIDO を活用したサービスが利用可能になっており、海外では FIDO を利用したサービスの提供を開始した金融機関もある。

FIDO における認証手順は、主に「登録フェーズ」と「認証フェーズ」から構成されている。登録フェーズでは、従来使っていた ID・パスワード等の認証情報（レガシー認証情報）と、FIDO で使用するサービス利用者情報の紐付けを行う。また、

認証フェーズでは、サービス提供者がサービス利用者を認証するほか、取引認証（「Transaction Confirmation」と呼ばれる）の実施も可能である。サービス利用者の認証には生体認証等を活用することができる。その際、プライバシーに配慮し、生体情報等がサービス提供者に送信されない仕組みとなっている（端末内で検証処理が行われ、検証結果のみがサービス提供者に送信される）。

ここで、FIDO の Transaction Confirmation の仕組みをインターネット・バンキングに適用することを想定し、不正送金を企図した MitB 攻撃に対するセキュリティ評価を、登録フェーズと認証フェーズそれぞれについて実施した（井澤・五味［2016］）。その結果、登録フェーズでレガシー認証情報を攻撃者に盗取された場合、当該情報と攻撃者の端末を使って、攻撃者への不正送金が可能になってしまうことが判明した。また、認証フェーズでは、①攻撃者がサービス利用者の認証用端末（スマートフォン）に物理的にアクセスして生体認証でのなりすましに成功した場合、または、②攻撃者がネットワーク経由で認証用端末にアクセスしてルート（root）権限を悪用するマルウエアを当該端末に感染させた場合、攻撃者への不正送金が可能になってしまうことが判明した。一方、フィッシングやルート権限を持たないマルウエアへの脅威に対しては、一定の耐性を有していることがわかった。

（2） 金融機関等が FIDO を導入する際の留意点

以上の議論をまとめると、金融機関等が FIDO を導入する際の留意点は以下の 3 つである。

第 1 に、登録フェーズにおいてレガシー認証情報が盗取されるリスクに留意することが必要である。レガシー認証情報が盗取されると、攻撃者が自分の端末で登録フェーズを実施し、不正送金を実施することが可能となる。これはレガシー認証情報の使用にかかる問題であり、FIDO に固有の問題ではない。対応策としては、レガシー認証情報盗取の原因となるマルウエアへの対策を講ずるように、顧客に注意喚起するとか、普段使わない端末からの登録フェーズの処理を制限するといった方策が考えられる。

第 2 に、認証用端末がマルウエアに感染することによって、サービス利用者が目視確認する取引内容と異なる取引内容がシステムによって実行されるリスクに留意することが必要である。サービス利用者が取引内容のメッセージを端末の画面で確認する際、マルウエアが、サービス利用者の意図しない不正な取引メッセージの上に、ユーザの意図した取引メッセージを被せて表示すれば、ユーザの意図しない不正取引が実行されてしまい、利用者による確認は全く意味をなさなくなる。対応策としては、こうした 1 つのメッセージの上に別のメッセージを被せて表示すること

を困難にするインタフェース「Trusted UI（Trusted User Interface）」の活用を検討することが考えられる。

第 3 に、生体認証でのなりすましに留意することが必要である。攻撃者が端末に物理的にアクセスして生体認証でのなりすましに成功すれば、認証フェーズにおいて端末のロックを解除し、取引認証を実施することが可能となる。対応策としては、生体認証でのなりすましの検知精度（誤受入率等）について、当該端末が第三者による評価を受けていることを確認しておくことが考えられる。

4. 講演 2「生体認証システムのセキュリティ評価：人工物を用いた攻撃に焦点を当てて」

宇根 は、宇根［2016］に基づき、人工物を用いた攻撃に対するセキュリティ評価の現状、第三者機関によるセキュリティ評価・認証の実現に向けた検討の状況、金融機関が同評価・認証を活用する際の留意点について、次のとおり報告した。

(1) 人工物を用いた攻撃に対するセキュリティ評価の現状と取組み

生体認証システムは、身体的特徴や行動的特徴（以下、総称して「生体特徴」という）を利用して個人を認証するシステムである。金融分野では、既に ATM における取引時の本人確認手段として採用されている。今後は、FIDO を利用した金融サービスでも活用される可能性がある。こうした生体認証システムでは、「第三者によるなりすまし」を一定の確率で排除することが求められる。なりすましを企図した攻撃としては、攻撃者が自分の生体特徴を提示してなりすましを試みる「ナイーブな攻撃」と、なりすまし対象の個人の生体特徴を何らかの手段で入手し、人工物を用いて提示する「人工物を用いた攻撃」が知られている。

ナイーブな攻撃に対する生体認証システムのセキュリティについては、誤受入率等を評価尺度とする標準的な評価手法が既に確立されている。一方、人工物を用いた攻撃に対するセキュリティに関しては、評価手法の確立に向けて、現在活発に議論が進められているところである。具体的には、当該セキュリティをコモン・クライテリア[4] に則った方法で評価するための手法や枠組みが、わが国の産官連携プロ

4 コモン・クライテリア（Common Criteria）は汎用的な情報システム・製品のセキュリティを第三者機関が評価・認証する制度的な枠組みであり、その評価手法や手続等は ISO/IEC 15408 シリーズ等の国際標準となっている。コモン・クライテリアの枠組みは各国で制度化されており、わが国では、2001 年から、「IT セキュリティ評価及び認証制度」として運用されている。

ジェクト[5]において2014年度から検討されている。本プロジェクトでは、攻撃に用いられる人工物を模した「テスト物体」による評価手法の開発やその成果を国際標準に反映するための検討等が進められている。具体的には、テスト物体の作製やその費用等の算出、評価尺度（攻撃成功確率）の定義、評価用の試験環境等について、検討が行われている。2016年度には、静脈のパターンを用いたシステムの評価が試行される予定である。

(2) 金融分野における標準的なセキュリティ評価手法の活用

上記プロジェクトをはじめとする取組みが進展し、人工物を用いた攻撃に対するセキュリティ評価の標準的な手法が確立すれば、金融機関は、国際標準に基づいた生体認証システムの評価結果を活用できるようになる。同時に、異なる生体認証システム間で、評価結果を比較することも可能になる。評価結果の確認については、ベンダーの協力を得ながら、評価対象システムの「セキュリティ設計仕様書（Security Target）」やテスト証拠資料等を参照し、当該システムの用途や想定する脅威、運用時の前提条件、評価尺度等を確認するという方法が考えられる。

今後、生体認証システムを金融サービスにおいて利用する際には、わが国の産官連携プロジェクトや国際標準化等の動向をフォローし、それらの成果を活用することによって、セキュリティ・ガバナンスの向上を図ることが望ましい。こうした取組みが、ひいては、顧客の安心感を高めることにつながっていくと考えられる。

5. 講演3「暗号ハードウェア等に対するセキュリティ評価および留意点」

清藤は、スマートフォン等の内部に安全な実行環境を実現する技術であるTEE（Trusted Execution Environment）の主な機能とセキュリティ評価、TEEの活用を検討するうえでの留意点等について次のとおり報告した。

5 本プロジェクトの名称は、「平成26年度工業標準化推進事業委託費　戦略的国際標準化加速事業　国際標準共同研究開発・普及基盤構築事業：クラウドセキュリティに資するバイオメトリクス認証のセキュリティ評価基盤整備に必要な国際標準化・普及基盤構築」である。

(1) インターネット・バンキングのセキュリティと取引認証

インターネット・バンキングの利用者にとって最大のリスクは、意図していない取引が、サービス提供者（金融機関等）によって実施されてしまうことである。例えば、サービス利用者の端末（PC やスマートフォン等）がマルウエアに感染すると、MitB 攻撃等によってサービス利用者・提供者間でやり取りする取引内容が改ざんされ、不正送金等が発生するリスクが高まる。

こうしたリスクへの対策の 1 つが取引認証である。取引認証とは、サービス提供者が正当な取引（サービス利用者の意図に基づいた取引内容）であることを確認することである。複数の端末を利用し、取引内容等の送信と確認を異なる端末上で行うという方式が代表的である。送信端末がマルウエアに感染し、取引内容等が改ざんされたとしても、取引内容の確認に用いる端末がマルウエアに感染していない限り、改ざんを検知することができる。もっとも、こうした方式は、複数の端末を利用することが前提となっている。そのため、利便性や網羅性とのバランスを考慮すると、MitB 攻撃等へのセキュリティを確保しつつ、1 つの端末（例えばスマートフォン）で取引認証を実現するのが理想である。そうした観点から現在注目されているのが、TEE と呼ばれる技術である。

(2) TEE の主な機能とセキュリティ評価

TEE は、通常のアプリケーション実行環境（通常領域）と、そこから隔離された「安全なアプリケーション実行環境」（セキュア領域）の 2 つを、1 つの端末上に並存させるための技術仕様である。TEE の仕様は、IC カードにかかる技術の標準化を推進するグローバル・プラットフォーム（Global Platform）によって策定され、ハードウェアとソフトウェアを組み合わせてセキュア領域を実現するためのアーキテクチャや各種 API（Application Programming Interface）が規定されている。TEE で実現可能なセキュリティ機能として、①セキュア領域内で動作するアプリケーション等の完全性の確保、②セキュア領域内に格納されるデータ（暗号鍵等）の機密性・完全性の確保の 2 つが挙げられる。このほか、オプションの機能として、③セキュア領域とユーザインタフェースとの間の入出力の完全性の確保等が挙げられる。

TEE を活用するには、その機能が実際の製品において適切に実装されているか否かを、第三者の評価・認証等を利用して事前に確認しておくことが望ましい。そうした枠組みとして、コモン・クライテリアに基づく評価・認証制度が存在する。TEE においても、同枠組みに則った評価・認証を実施するための「セキュリティ要求仕様書（Protection Profile）」がグローバル・プラットフォームによって 2014 年に

公表されている。2016 年 3 月初の時点では、同要求仕様書に基づく評価・認証プロセスが複数の製品において進行中であり、今後、第三者の評価・認証を得た TEE の製品が提供されるようになるとみられる。

(3) TEE の活用を検討するうえでの留意点

TEE を用いた取引認証として、例えば、セキュア領域のデータの入出力を安全に実行するインタフェースである Trusted UI を活用するとともに、デジタル署名生成用の暗号鍵を安全に保管する機能（secure storage）と署名生成を行う機能をセキュア領域内で実装することが考えられる。サービス利用者は、取引内容にかかるデータをその確認結果とともに、デジタル署名を付して、サービス提供者に送信する。これらのデータを受信したサービス提供者は、署名検証に加え、当該取引内容がそれまでに交信した取引にかかる情報と整合的か否かを検証する。仮に通常領域上にマルウエアが存在し、通信データが改ざんされたとしても、サービス提供者側で署名検証と取引内容の整合性確認が行われる際に、攻撃を検知することが可能になる。

TEE を活用した取引認証の普及に当たっては、①想定される利用環境やアプリケーションに応じてセキュリティ要件を適切に設定しておくこと、②それらの要件が TEE を搭載する製品において充足されていることの確認手段を提供することが肝要である。特に②の点については、今後、コモン・クライテリアに則った評価・認証の結果を活用することが可能になるとみられることから、TEE を含め、暗号ハードウェア等の動向をフォローしていくことが有用であろう。

6. 講演 4「情報セキュリティのための異常検知技術」

山西は、データマイニングによる異常検知の手法や事例、情報セキュリティを確保するための異常検知技術の研究動向や留意点等について、次のとおり報告した。

(1) データマイニングと異常検知

データマイニングの目的は、機械学習の技術を利用して、大量のデータに潜在している知識を獲得し、将来に向けて活用することである。同手法を用いた異常検知

は、確率モデルの学習に基づいてデータの異常度合いを数値化することによって行われる。主な応用分野としては、セキュリティ（攻撃検知等）、システム保全・ネットワーク監視（障害・故障検知等）、マーケティング（トレンド発見等）、SNS ／ウェブ分析（話題潮流発見等）、ライフログ・フォレンジクス（法的証拠発見等）が挙げられる。金融分野に焦点を当てると、システムへの不正侵入の検知、ネットワークの障害とその予兆の検知、金融時系列データにおける変化の兆候の検知のほか、インターネット・バンキングにおけるなりすましの検知への適用が考えられる。

(2) 異常検知にかかる各種の手法

異常検知の手法としては、「外れ値検知」と「変化点検知」が代表的である。外れ値検知は、統計的なパターンから外れたデータ（外れ値）を抽出し、異常を検知する手法である。例えば、同手法をネットワークのパケットデータに適用し、外れ値を抽出することによって、ネットワークへの不正侵入を検知する手法が提案されており、実データを用いた性能評価実験の結果が報告されている。また、同手法をネットワークの障害検知に応用する研究等も活発に行われている。

変化点検知は、時系列データにおける異常の兆候（変化点）を捉える手法である。大きく分けて、時系列データの変化点をリアルタイムに検出して異常の兆候を早期に検知するタイプ（リアルタイム変化点検知）と、変化が徐々に起こる場合に時系列データから変化の兆候を検知するタイプ（変化予兆検知）の 2 種類があり、マルウエア等の攻撃兆候の検知に応用する研究が知られている。また、検知対象となる事象のモデル（変数や状態の数等）の変化を捉えて異常を検知する手法も盛んに研究されており、システムにおけるなりすましの検出やシステム・ログからの障害検知に応用した研究が知られている。障害検知への応用では、障害箇所の特定や障害の予兆の検出が可能となってきている。

(3) 異常検知技術を活用する際の留意点

異常検知技術を活用するには、実データを用いた研究が必須となる。第 1 に、異常を判断するためには正常な取引やデータを学習する必要がある。第 2 に、モデルの精度を高めて誤検知の確率を一定水準以下に抑える必要がある。これらの目標を達成するには、大量の実データを不断に収集・解析することが必要である。

7. パネル・ディスカッション「インターネット・バンキングのさらなる発展に向けて」

パネル・ディスカッションの冒頭、モデレータの松本（勉）は、インターネット・バンキングのさらなる発展に向けて、「インターネット・バンキングの認証においてセキュリティ・利便性・網羅性のバランスをどのように考えるべきか」という問題提起を行った。

(1) セキュリティ・利便性・網羅性のバランスについて

イ. 業務リスクに応じた認証技術

松本（泰）は、セキュリティ・利便性・網羅性のバランスを取るためには、「業務リスクに応じた認証技術を適用する」という観点が重要であると指摘し、そうした取組みの事例として、エストニアにおけるインターネット・バンキングを取り上げた。エストニアでは、政府主導で電子証明書が格納されたIDカードが国民に配付されている。当該IDカードは、これを用いて電子政府ポータルにログインできるほか、インターネット・バンキングにもログインすることができる。また、IDカードに加えて、電子証明書をスマートフォンのSIM（Subscriber Identity Module）に格納する「モバイルID」と呼ばれる認証技術も用意されている。かつてエストニアでは、インターネット・バンキングを行う際、パスワードカード（ペーパートークン）による旧型の認証技術が利用されていたが、IDカードやモバイルIDといったよりセキュアな認証技術に誘導するため、政府主導でパスワードカードの取引限度額が引き下げられていった。こうした取組みは、業務リスクに応じた認証技術の適用と電子証明書の利用によってセキュリティを確保しつつ、PCやスマートフォンでの利用を可能にすることによって網羅性を確保し、さらに国民が有するIDカードを用いてログインできるという利便性を確保したものと解釈することができるとした。そのうえで、わが国のマイナンバー制度を取り上げ、今後、銀行口座との紐付けが行われれば、エストニアと同様の枠組みをわが国で展開できる可能性があることを指摘した。今後、犯罪収益移転防止法の対応等も含め、国全体としてマイナンバー制度を活用していく必要があることを踏まえると、エストニアの事例は大変参考になると述べた。金融業界も、こうした機を捉え、積極的にマイナンバー制度に対するニーズや要件等を整理し、政府に提言していくという姿勢が必要であると指摘した。

高木は、インターネット・バンキングでは、ログイン認証（本人認証）のセキュ

リティ・レベルに関わらず、MitB 攻撃や偽造されたアプリケーション（以下、偽アプリという）を使った攻撃による利用者の取引情報の改ざんというリスクが常に存在するため、ログイン認証を強化することは適切とはいえないと指摘した。そのうえで、インターネット・バンキングの機能を重要なものとその他のものに分け、認証方法を使い分けるべきであると述べた。産業技術総合研究所では、送金や住所変更といった重要機能を利用する場合には、電子ペーパーで取引内容を目視確認するという手法を提案していることを述べた。その一方で、残高照会といった重要性が低い機能を利用する際には、効率性を重視してより簡便な手法（サービス利用者の特別な操作を必要としない認証、後述）を採用するといった対応が考えられると述べた。

鎌田 は、松本（泰）と高木が述べた内容は、いずれもセキュリティを確保するために、「業務リスクに応じた認証技術を適用する」という点で大いに参考になるとし、これに加えて、利便性と網羅性を合わせて追及するならば、サービス利用者自身が使いやすい認証技術を選択するというアイデアもあるのではないかと述べた。その際には、セキュリティ確保の観点から、認証技術を選択するためのアドバイスを金融機関が提供することが必要になるだろうと付け加えた。また、松本（泰）の「金融業界からニーズや要件等を整理し、政府に提言すべき」というアイデアに賛同し、認証技術の専門家は、各種の標準化を進めていく際、技術的な面で金融業界をサポートすることが可能であり、そうした対応がより有意義な結果につながるはずであるとコメントした。ただし、金融業界は認証技術のセキュリティ確保のほかにも多くの課題を抱えており、そのなかで認証技術の課題にどの程度のリソースを割くことができるかは、別の問題としてあり得ると付言した。

ロ. スマートフォンと PC

松本（泰） は、昨今のスマートフォンを前提とした認証の議論に関連して、網羅性を考えれば、スマートフォンだけではなく、PC を使った取引にも目を向ける必要があると指摘した。すなわち、法人向けサービスは個人向けサービスとは状況が異なり、前者の場合には、社内業務システムと連動してインターネット・バンキングを行う必要があるため、PC が必須となる場合があるのではないかとコメントした。

鎌田 も、将来的には個人向けサービスはスマートフォンの利用を前提としてもよいと思うが、法人向けサービスでは引き続き PC の利用を前提とすべきであろうと松本（泰）の意見に賛同した。

ハ. スマートフォンにおけるログイン認証と TEE

高木 は、先に述べた利便性に配慮したログイン認証の手法について、スマートフォンを使う場合を例に次のように説明した。まず、スマートフォン・アプリと金

融機関の間で SSL（Secure Sockets Layer）/TLS（Transport Layer Security）通信路を使って、トークン（サービス利用者と紐付けられた本人確認用のデータ）を共有しておく。次に、サービス利用者がアプリを利用する際に、当該トークンを使った「リモート認証」をアプリがバックグラウンドで行う。ここまでは、一般的なスマートフォン・アプリで行われていることである。これでは、スマートフォンを攻撃者に盗取された場合、不正な操作が行われるおそれがある。この問題への対処法としては、別途、スマートフォンのロックを解除するプロセス（ローカル認証）を付け加えることが考えられる。リモート認証にトークン、ローカル認証には生体認証や PIN（Personal Identification Number）認証等を利用すればよい。このリモート認証とローカル認証を分離する方法は、利用者にとって極めて簡便な認証手続きであり、利便性という観点からも評価できると考えられる。なお、この手法のリモート認証では、必要とされるセキュリティ・レベルという点からみて、電子証明書と PKI（Public-Key Infrastructure）は必ずしも必要ではないと付言した。さらにリモート認証の留意点として、同認証はスマートフォンの OS のサンドボックス機能[6] を利用しており、同機能の脆弱性に起因する不正が行われた場合には不正取引の防止が困難となることから、サンドボックス機能にかかる脆弱性に関して配慮する必要があると指摘した。また、高木 は、スマートフォンを利用する際には、偽アプリからの接続か正規アプリからの接続かを金融機関側で見分けることが困難であり、偽アプリを使用して取引が改ざんされるというリスクに注意する必要があると説明し、トークンを利用したリモート認証の利用は残高照会等に限定し、送金や住所変更等の重要機能については、前述した電子ペーパーを用いた取引内容の確認等、別途対策を講じる必要があると述べた。

ここで フロア参加者 から、スマートフォンの中のセキュア領域（SIM 等）においてスマートフォン・アプリのハッシュ値を検証して偽アプリを検出する手法が存在するとしたうえで、それを使って偽アプリを識別することが可能ではないかとの発言があった。

松本（勉） は、スマートフォンといっても多種多様なものが世の中に存在するため、何らかの前提を置いて議論することが必要であり、フロアからのコメントを考慮すると、スマートフォンの中にセキュア領域があるか否かがポイントになり得ると述べた。そのうえで、スマートフォン内に TEE というセキュア領域を置き、それを使った取引認証の仕組みによりセキュリティを確保するという講演 3 について、①そもそも TEE 内にマルウエアは入ってこないと考えてよいのか、また、② TEE 内で稼働するアプリがもともと不正なものである可能性はないのか、という論点を提示した。

6 トークンの機密性・完全性やアプリケーションの完全性をソフトウェアのみで確保する機能。スマートフォンの OS（Android や iOS 等）に標準搭載されている。

これに対して、清藤（講演 3 の講演者）は、上記①について、TEE はマルウエアがセキュア領域内のアプリには影響を及ぼさないことを前提としているが、実装上、その前提が満たされているか否かは、コモン・クライテリア等の第三者評価による検証が必要であると述べた。さらに廣川（日本銀行金融研究所テクニカルアドバイザー）は、上記②について、TEE のセキュア領域内で稼働するアプリ（Trusted Application）が正当なものか否かは、セキュア領域内で実行されるというだけで担保できるものではなく、別途確認する必要があると述べた。例えば、IC クレジットカードの場合は、何らかの形で認定された製品の使用を前提として、取引が実施される仕組みとなっている。具体的には、IC チップ、カード内 OS のセキュリティ、搭載されるペイメント・アプリ（Trusted Application に該当）については、カードの各ブランド（ペイメントスキーム）が、対応端末（IC カードが差し込まれる端末）については、EMVCo[7] が、それぞれ確認・認定を行っている。利用者が所有するスマートフォン内の TEE に搭載されるアプリについても、IC クレジットカードと同様に、誰かがその正当性を確認する必要があると補足した。

これを受け 松本（勉）は、インターネット・バンキング用の（確認・認定済の）正当なアプリがスマートフォンのセキュア領域にプリインストールされ、世に提供される状況になればよいのではないかとコメントした。

これに対して、高木 は、そのようなアプリの提供は良い考えではあるものの、将来的にアプリの機能を追加するニーズが出てくる可能性があり、アプリの追加時に攻撃者に狙われるリスクがあると指摘した。また、仮にアプリの機能を最小限に絞り、機能追加をあきらめたとしても、どのような機能を TEE 内に配置するかという点が問題になるだろうと述べた。

鎌田 は、セキュリティの向上を企図した新しいアプリや新技術の導入時の論点として、システムの安定稼働をどのように確保するかという別の視点も考慮する必要があると問題提起した。金融機関にとっては、インターネット・バンキングの不正送金リスクよりも、むしろ、サービスの安定稼働が阻害されるリスクの方が重視される傾向にあると指摘した。したがって、セキュリティ上有効な技術が登場したとしても、その技術の採用は、そのもとでシステムが安定的に稼働することが大前提となるとコメントした。

松本（勉）は、以上の討論を総括して、今後は、業務リスクに応じた認証技術を適用するという考えや、スマートフォンの普及という状況の変化を取り入れた認証技術が重要なポイントになろうと述べ、パネル・ディスカッションの前半を締めくくった。

7 EMVCo とは、国際的なクレジットカード・ブランドである Europay International、Visa International、MasterCard International により設立された組織であり、国際クレジットカード・デビッドカードの業界標準である「EMV 仕様」の管理を行っている。

(2) ユーザインタフェース、レガシー対応等について

イ. レガシー対応について

松本（勉）は、パネル・ディスカッション後半の論点として、「認証に当たってユーザインタフェース設計やユーザ教育等でどのような方策があるか」、「デバイスの多様化や新しいセキュリティ対策が台頭するなかでレガシー対応問題（レガシー技術を切り捨てるべきか否か）をどのように進めればよいのか」という論点を提起した。

鎌田は、レガシー対応問題は難しい問題であり、金融機関の内部でも、新しいものを導入する際には、必ずと言ってよいほど、レガシー技術に対応すべきであるという議論が出てくると指摘した。多くの場合、様々な立場の関係者（業務部門、システム部門、一般の顧客等）の意見をきくということになるが、法律や各種規制に基づく要請であればそれらに準拠するために対応が迅速に進むとコメントした。この問題にどう対処すべきかは、各金融機関によって状況が異なるため、1つの答えを出すことは難しい。まずは、何が考慮すべき観点なのかという点について、研究者、技術者、業界団体の間で議論していくことが肝要であるとコメントした。

これに対し、松本（泰）は、レガシー対応問題は金融業界全体で取り組まなければまとまらないと指摘した。金融機関内部でレガシー技術を切り捨てるという判断を行えば、鎌田が言うように、レガシー技術に対応すべきという議論が内部の別の部門から必ず出てきて最終的な結論が出ない。金融業界全体としてレガシー技術への対応を決断し、各金融機関はそれに従うというポリシーで進めるべきではないかとコメントした。

ロ. ユーザインタフェースについて

鎌田は、ユーザ教育について、一言でインターネット・バンキングといっても、法人向けと個人向けとで状況が異なると発言した。法人向けであれば、比較的容易に顧客とやりとりできるため、ユーザ教育ができる。一方、個人向けでは、それが難しいのが現状であると述べた。

高木は、ユーザインタフェース設計にしても、レガシー対応問題にしても、スマートフォン主流の時代にどのような認証が必要かを留意することが大切であり、それを踏まえた全体最適という観点が必要であると述べた。個人向けサービスについては、PCを前提とした設計思想は改めるべきであり、今一度過去を振り返って見直しを行うことが重要であると述べた。その際、過剰な技術を採用していないかに注意しつつ、ユーザフレンドリーなユーザインタフェース設計を志向すべきであろうと補足した。

松本（勉）は、パネル・ディスカッションの前半で述べられた認証技術をサービ

ス利用者が選択するという話を取り上げ、これと同様にして、好みのユーザインタフェースをサービス利用者が選択するということも案として考えられるのではないかとコメントした。

これに対して、鎌田 は、良い考えかもしれないが、コスト面が最も大きな課題になると述べた。利用者の接続環境ひとつとっても、ブラウザ経由での接続や専用アプリ経由での接続があり、利用端末も PC やスマートフォン等、種々多様な環境がある。こうしたなかで、さらにユーザインタフェースのバリエーションを増やすことは、金融機関側の対応コストが膨大になるリスクがあると述べた。

高木 は、発想を転換し、重要操作である送金と住所変更の不正を別の方法で防止する一方、残高照会等のユーザインタフェースを含むバンキング・アプリについては、金融機関が作成するのではなく FinTech 企業が専ら作成を担当し、複数のアプリ（複数のユーザインタフェース）からサービス利用者が選択するようにすればよいのではないかとコメントした。そうすれば、金融機関側の対応コスト増大を抑えられるうえに、FinTech 企業間の競争によりユーザインタフェースの利便性向上を促進できる。FinTech 企業にとっても、金融機関とウィン・ウィン（win-win）の関係を築けるのでメリットではないかと指摘した。

これに対して、鎌田 は、金融機関の側からすると、身元の分からない人が作ったアプリを顧客に使わせるという点について、抵抗感があるかもしれないと述べた。

高木 は、別の観点として、インターネット・バンキングの取引認証に関わるユーザインタフェース設計に関連して、サービス利用者が騙されにくくする工夫が必要なのではないかとコメントした。すなわち、インターネット・バンキングの取引認証の仕組みとしては、① TAN[8] 利用方式（サービス利用者は、振込先口座番号等を専用デバイスに入力して TAN を生成し、TAN と振込指図を金融機関に送信する手法）と、②取引内容確認方式（取引内容をサービス利用者が目視確認する手法）の大きく 2 通りがある。上記①の方式では、攻撃者の「〇〇を専用デバイスに入力せよ」という指示に利用者が従ってしまうと、たとえ取引認証が正しく行われたとしても不正送金が成り立ってしまう。一方、上記②の方式では、サービス利用者が視覚的に振込先を確認できるため、攻撃者に騙されにくいと考えられる。セキュリティの観点から、2 つのユーザインタフェース設計を考えると、②の方がよいとコメントした。

ハ. 証券業界における新たな脅威

ここで、松本（勉）がフロア参加者に意見を求めたところ、フロア参加者 から、証券業界における新たなリスクに関して、次のような問題提起があった。証券会社において不正アクセスを受けることは、これまでもあったが、最近は被害が大きく

8 Transaction Authentication Number：取引に紐付いた認証コード。

なっている。従来は、不正に株を売却されるということはあったが、売却代金は被害者のもとに残っているということが多かった。しかし、最近では、インターネット・バンキングと証券会社が連動していることもあって、両者のパスワードが同じで、当該パスワードが攻撃者に搾取された場合、攻撃者に株式を不正に売却されたうえに、売却代金が攻撃者の口座に不正送金されるという事例が頻発していると述べた。

これを受けて、鎌田は、金融 ISAC では、インターネット・バンキングにおける不正送金への対策に関し、ベストプラクティス集を作成している。同資料は、証券会社の方にとっても参考になるのではないかと述べた。

高木は、証券業界における新たな脅威への 1 つの対策として、証券取引にも取引認証を導入することが考えられると述べた。そのうえで、この方法では株式の高頻度取引に対応できない。そこで、不正送金を防ぐための水際対策として、証券会社からの出金やインターネット・バンキングにおける資金移動の際に限って、取引認証を実施することでもよいのではないかと補足した。

こうした議論を踏まえ、松本（泰）は、認証はインターネット・バンキングを含むネットワーク経由での金融サービス提供において重要なトピックであり、金融機関が今後も安心安全なサービスを提供し続けるためには、業界全体で認証にかかるニーズや要件について積極的に検討・整理を進める必要があると改めて指摘した。これは、FinTech についてもあてはまることであり、金融業界が FinTech を本気で進めていくためには、認証の将来像に関する議論を業界全体で深めていくべきであるとした。

松本（勉）は、こうしたパネル・ディスカッション後半の議論を次のように総括した。レガシー対応やユーザインタフェース設計等、様々な課題があるなかで、FinTech のような新しいサービスが次々と登場している。また、証券業界においても新しい脅威が出現しているようである。金融実務家や情報技術の専門家は、そうした環境変化を敏感に感じ取り、共同して議論を深めていくことが重要である。

参考文献

井澤秀益・五味秀仁、「次世代認証技術を金融機関が導入する際の留意点：FIDO を中心に」、『金融研究』第 35 巻第 4 号、日本銀行金融研究所、2016 年、21〜54 頁〈本号所収〉

宇根正志、「生体認証システムにおける人工物を用いた攻撃に対するセキュリティ評価手法の確立に向けて」、『金融研究』第 35 巻第 4 号、日本銀行金融研究所、2016 年、55〜90 頁〈本号所収〉

全国銀行協会、「『インターネット・バンキングによる預金等の不正払戻し』等に関するアンケート結果」、2015 年

日経 BP 社、「FinTech 金融を変えるのは銀行ではない」、『日経コンピュータ』No. 892、2015 年

日本カードビジネス研究会、「Fintech Report 2015」、2015 年

Kuhn, John, “The Dyre Wolf Campaign: Stealing Millions and Hungry for More,” Security Intelligence, 2015 (https://securityintelligence.com/dyre-wolf/).