IMES DISCUSSION PAPER SERIES

情報セキュリティ・シンポジウム（第22回）の模様：スマートフォンの利用にかかるセキュリティ

Discussion Paper No. 2021-J-12

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

１．はじめに

日本銀行金融研究所・情報技術研究センター（Center for Information Technology Studies : CITECS）は、2021 年 9 月 10 日、「スマートフォンの利用にかかるセキュリティ」をテーマとして、第 22 回情報セキュリティ・シンポジウムを開催した。

近年、金融サービスを提供する手段として、スマートフォンの存在感が一段と増しており、これを利用した新しいサービスが次々と展開されている。店頭での決済、個人間送金、資産管理、証券投資等、さまざまなサービスがスマートフォン・アプリとして提供されており、金融サービスがこれまで以上に身近なものになりつつある。こうした多くの金融サービスがスマートフォンに搭載されるようになると、それらを狙った犯罪も増えてくることが懸念される。実際に、他人のクレジットカードや銀行口座をスマートフォン・アプリに登録し、取引や決済が不正に行われた事件も発生している。こうした不正は、スマートフォン OS の脆弱性を悪用したり、スマートフォンをマルウェアに感染させたりするなどの手口によって行われており、その手口は巧妙かつ高度化している。

金融サービスを安全に利用してもらうためには、当該サービスを提供する金融機関や決済事業者は、想定されるリスクを把握し、それに合わせたセキュリティ対策を事前に講じておく必要がある。その際、足許のセキュリティ対策に止まらず、今後生じ得る問題に対応すべく中長期的な視野をもって、スマートフォンのセキュリティに関連する最先端の研究動向をフォローしておくことが重要である。

こうした観点から、今次シンポジウムでは、スマートフォンのセキュリティに関連する分野の第一線で活躍している専門家や実務者を招き、スマートフォンの利用にかかる足許の脅威、スマートフォンを巡るセキュリティの最新の研究動向、今後のセキュリティ対応のあり方に関して、講演とパネルによる議論を行った。当日は、情報セキュリティ技術に関わる金融機関関係者、スマートフォンを活用した金融サービスを提供する事業者等の実務者、研究者、システム開発・運用に携わる技術者等、約 200 名がオンラインで参加した。本稿では、以下のプログラムに沿って、シンポジウムにおける講演とパネルにおける議論の概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

---

1 文中の講演者やパネリストの所属と肩書きは、シンポジウム開催時点のものである。また、本稿に示された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。また、本シンポジウムでの講演の資料等については、日本銀行金融研究所の当該サイト（https://www.imes.boj.or.jp/jp/conference/citecs/22sec_sympo. html）を参照されたい。

【第 22 回情報セキュリティ・シンポジウムの講演・パネル】

●イントロダクション　日本銀行金融研究所　企画役補佐　田村裕子
●講演１「デジタル・トラスト時代の生体認証基盤」
　　株式会社日立製作所　研究開発グループ　主管研究員　高橋健太
●講演２「スマホ・マルウェアなどの脅威とその対策」
　　KDDI 株式会社　サービス統括本部　エキスパート　本間輝彰
●講演３「スマートフォンのセキュリティ機構」
　　情報セキュリティ大学院大学　教授　大塚玲
●講演４「スマホ時代のリスク管理」
　　セコム株式会社　IS 研究所　研究員　磯部光平
●パネル・ディスカッション「セキュリティの高い金融サービスの提供に向けて」
　・パネリスト：高橋健太、本間輝彰、大塚玲
　　一般社団法人金融 ISAC　専務理事／CTO　鎌田敬介
　・モデレータ：日本銀行金融研究所　企画役　宇根正志

２．イントロダクション

田村は、導入部として「スマートフォンを利用した金融サービスにおける脅威と対策」を展望したうえで、4 つの講演を以下のように位置づけた。

情報処理推進機構による「(個人向け) 情報セキュリティ 10 大脅威 2021」[2]をみると、「スマホ決済の不正利用」が 1 位となっている。その他にもスマートフォン関連の脅威が多く含まれており、情報セキュリティの問題が多発していることがわかる。

スマートフォンによる金融サービスで不正利用を防止するためには、少なくとも、ユーザ認証をしっかりと行う必要がある。利用者のパスワードとスマートフォンの端末情報がユーザ認証に用いられるケースがある。ここで、利用者のパスワードと端末情報が何らかの方法で盗取されると、なりすましによる不正な取引が行われてしまう。パスワードは、①利用者を巧みに騙すことによって盗まれやすく、②その悪用も容易であるほか、③端末情報が暗号処理を行わずに通信されていると、それを盗取することも比較的容易となる。

パスワードのようなテキスト入力による認証に代わる方法として、利用者の顔画像や指紋パターンのような生体情報による認証 (生体認証) が考えられるため、これを講演 1 で取り上げていただく。また、パスワードを盗むための各種攻

[2] 情報セキュリティ 10 大脅威 2021 は、2020 年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、情報処理推進機構が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等からなる「10 大脅威選考会」が審議・投票を行って決定される。個人が主に対象となる脅威と組織が主に対象となる脅威に分けて決定される。

撃（フィッシングやマルウェア）の防止策について、講演 2 で取り上げていただく。

更に、より高度なセキュリティの確保が必要となるサービスにおいては、スマートフォンのプラットフォーム（OS〈Operating System〉、ファームウェア、ハードウェア等）が提供するセキュリティ機能を積極的に活用する対応も有効である。そうした観点から、講演 3 では、スマートフォン内蔵のセキュア・エレメント[3]等を活用し、マイナンバーカード[4]の機能をスマートフォンに搭載する取組みの事例を紹介していただく。最後に、講演 4 では、スマートフォンのプラットフォームを活用する際のセキュリティ評価の現状と課題を紹介していただく。

３．講演１「デジタル・トラスト時代の生体認証基盤」

高橋は、スマートフォンを用いた決済サービスにおける最近の不正行為と、その原因となった本人確認・認証の不備、二要素認証における問題、生体認証の課題、安全性・利便性の向上に資する手法の動向について、次の通り発表した。

（１）スマートフォンによる決済サービスにおける不正行為と認証

近年、スマートフォン決済において、銀行口座から不正にチャージを行って金銭をだまし取る事件が発生している。攻撃者は、（被害者となった）ユーザの氏名・口座番号・暗証番号等を不正に入手した後、ユーザになりすまして自分のアカウントと（被害者の）銀行口座を紐付けし、当該銀行口座からアカウントに不正にチャージを行ったと報じられている。

こうした不正行為の発生源は主に 2 つある。1 つは、決済事業者によるユーザの本人確認[5]が不十分であった点である。具体的な事例では、個人のメールアドレスのみによって本人確認が行われたケースもあったようである。もう 1 つは、

---

3 セキュア・エレメントとは、暗号処理等のセキュリティ機能を有するとともに、外部からの物理的な攻撃に対しても高い安全性を有するモジュール（IC チップ）の総称である。

4 マイナンバーカードは、券面に氏名、住所、マイナンバー等が表示されたプラスチック製の IC カードであり、市区町村から交付される身分証明書である。対面での本人確認のほか、IC チップ内の電子証明書によって、公的個人認証サービス（JPKI）にも利用することができる。

5 本人確認とは、個人が特定のサービスに登録する際等に、その個人が当人によって主張されている個人であることを、公的機関が発行した身分証明書等を用いて確認することである。本人確認が成功すると、その個人のアカウントが開設され、そのアカウントを使用する際の認証（後述）のために、パスワードや暗号鍵（クレデンシャル）が設定される。これに対し、認証とは、登録済みの個人がサービスを利用する際にクレデンシャル（予め設定したパスワードや暗号鍵）を用いて一定の処理を行い、その結果に基づいて当該個人であることの確認を行うものである。ここでは、「当該銀行口座の所有者であるという申請」に対して、確かに所有者であることを確認する行為にあたる。なお、本人確認を認証の意味で使用するケースもある。

スマートフォン決済のアカウントと銀行口座を紐付ける際に行われる認証が不十分であった点である。不正行為の事例では、口座番号と暗証番号のみで認証が成功し口座振替の登録を行うことができたケースもあったようである。

（２）「二要素認証だから安全」とは限らない

認証の手法は、知識認証（パスワード、暗証番号等）、所有物認証（スマートフォン、IC カード、ワンタイム・パスワード・トークン等）、生体認証に分けて整理されることが多い。知識認証は、導入コストが相対的に低く、ユーザの意思確認に利用しやすい反面、失念する、推測されやすいパスワードが存在するといった欠点がある。所有物認証は、スマートフォンや IC カード等のハードウェア内部に暗号鍵を安全に格納することで暗号を用いた認証を実装できるものであるが、紛失や盗取のリスクがある。生体認証は、失念や紛失のリスクがないだけでなく、ユーザ本人でないと実行できないという利点もあるが、取替えができない点や、個人情報である生体情報の管理に十分配慮する必要がある。

オンライン・バンキング等では、2 つの手法を組み合わせる「二要素認証」が採用されるケースが多い。もっとも、「二要素認証であれば安全」とは必ずしもいえず、ユーザのスマートフォンと銀行のサーバの間で交わされる通信に介入する「中間者攻撃」が知られている。

例えば、パスワード（知識認証）とワンタイム・パスワード・トークン（所持物認証）の組合せによる認証に対して、次のような攻撃が想定される。まず、攻撃者が、フィッシング・メールを送信してユーザを自分の偽サイトに誘導し、オンライン・バンキング用の ID やパスワードを入力させる。次に、攻撃者は、銀行のサーバにアクセスして（ユーザから得た）ID とパスワードを入力しつつ、送金を指示する。銀行のサーバは、取引実行の確認のために、ユーザに対してワンタイム・パスワードの送信を要求する。これに対して、攻撃者は、ワンタイム・パスワードの（攻撃者への）送信をユーザに要求し（不審に思わなかったユーザが対応してしまった場合に）これを入手し、銀行のサーバに送信して取引を実行させる。

こうした攻撃に対抗するためには、暗号を用いた高度な認証プロトコルが必要である。例えば、ユーザとスマートフォンの間で認証を行うとともに、スマートフォンと銀行のサーバの間で公開鍵暗号に基づく認証プロトコルを実行することが考えられる。

（３）生体情報の保護と利便性の向上を実現可能な手法～PBI の提案

生体認証を用いる場合、サービス提供者側で生体情報をどのように安全に保護し続けるかが大きな課題となる。対応法の 1 つとして、サービス提供者側で

は生体情報を管理せず、ユーザのデバイス側で管理するという方法が考えられる。ユーザ認証の代表的なソリューションの 1 つである FIDO（Fast Identity Online）は、こうした考え方に基づいている。FIDO は、生体情報や暗号鍵をユーザが所有するデバイス内部で安全に管理することで、デバイスがユーザを認証しつつ、サーバがデバイスを暗号学的に認証する仕組みである。ただし、あらかじめデバイスの登録が必要であり、デバイスを利用しないいわゆる「手ぶら認証」には使用できないほか、デバイスの紛失時や買替え時に再度登録作業が必要になるという利便性上の課題が残る[6]。

ユーザによるデバイスの所有を不要とし、ATM のような共通のデバイスを使用する手ぶら認証を可能にするとともに、認証サーバや共通デバイスにおける生体情報等の管理に伴うリスクを最小化する方法として、「認証の都度、共通デバイス内部で生体情報から暗号鍵を生成する（認証時以外は生体情報、暗号鍵ともに保存しない）」手法である PBI（Public Biometric Infrastructure）を弊社において開発した。これは、鍵生成アルゴリズムに生体情報と乱数を入力することで公開鍵と秘密鍵を一意に生成し、この鍵ペアによって公開鍵認証基盤（PKI : Public-Key Infrastructure）と同様の機能を有するインフラを実現するものである。認証については、ユーザが秘密鍵によってデジタル署名を生成し、認証者がそれを公開鍵によって検証する方法を採る。また、生体情報を変更することはできないが、鍵ペア生成に用いる乱数を変更することによって、鍵ペアの失効・更新を行うこともできる。

PBI は、既に、手ぶら（IC カード等が不要）での銀行取引やキャッシュレス決済のサービスの一部で運用されており、今後、安全性と利便性を両立・向上する金融・決済サービスへの活用が期待される。

４．講演２「スマホ・マルウェアなどの脅威とその対策」

本間は、スマートフォンを対象としたマルウェア（スマホ・マルウェア）による攻撃手段、金融サービス等への攻撃のパターン、主な対策手法と課題について以下の通り発表した。

（１）スマートフォンにおけるマルウェアによる攻撃手段

スマートフォンの OS は、サンドボックス機能[7]等、各種セキュリティ対策が

---

6 FIDO は、生体情報や暗号鍵を格納したデバイスを用いるため、生体認証と所有物認証の 2 要素認証となっている。

7 サンドボックスとは、隔離された領域でプログラムを実行し、問題発生時においてもほかのプログラムに影響を及ぼさないようにする仕組みを指す。

施されており、マルウェアがアプリを直接乗っ取ることは困難である。そのため、スマホ・マルウェアは、スマートフォンのユーザをだましてダウンロードさせるケースが多い。

例えば、SMS（Short Message Service）によるフィッシング[8]（スミッシング）の場合、攻撃者が、①マルウェアをダウンロードさせるサイトの URL（Uniform Resource Locator）を含む SMS メッセージを送信し、②ユーザを当該 URL へ誘導してマルウェアをダウンロードさせる。その際、③ダウンロードが正規のアプリ・ストアから実行されるものではないことから、OS の機能によって警告画面が表示されるほか、インストールの際も警告画面が現れる。④ユーザが警告を重く受け止めず、これらを無視してインストールを許可すると、スマートフォンがマルウェアに感染する。その後、当該マルウェアが最初に起動される際に、⑤マルウェアがユーザに対して各種機能（アドレス帳へのアクセス、電話の発信等）の権限（パーミッション）の承認を要求するが、ユーザがそれらを承認すると、マルウェアに対して攻撃の手段を与えることとなる。

このように、マルウェアがインストールされても、ユーザがマルウェアに各種機能の権限を付与しなければ、マルウェアは活動できない。しかし、近年のマルウェアは正規のアプリを巧みに模倣するなど、ユーザがマルウェアと気づかずインストールしてしまうケースが少なくない。

（２）スマホ・マルウェアによる攻撃のパターン

スマホ・マルウェアによって情報を盗取する攻撃は、主に 3 つのパターンに分けられる。すなわち、①利用者の脆弱性を悪用するパターン、②サービスの脆弱性を悪用するパターン、③悪意のあるサード・パーティの SDK（Software Development Kit）[9]を用いるパターンである。

利用者の脆弱性を悪用する例としては、フィッシング・メールやスミッシング SMS を送信してフィッシング・サイトに誘導し、（被害者）ユーザが入力した ID やクレジットカード情報を盗取し悪用するケースが該当する。サービスの脆弱性の悪用については、スマートフォン決済のアカウントと銀行口座を連携する際の本人確認や認証が十分に行われず、なりすましによって銀行口座からアカウントに不正なチャージが実行されるといったケースが当てはまる。悪意のあるサード・パーティの SDK を用いるパターンは、攻撃用のプログラムを埋め込んだ SDK をアプリ開発者に配付し、それを用いて作製されたアプリをユーザに

---

8 SMS Phishing もしくは、Smishing（スミッシング）と呼ばれる。

9 SDK は、特定のシステムを開発する際に用いられるプログラムやドキュメントをパッケージ化したものであり、アプリ等のソフトウェア開発を効率的かつ安定的に進めることが可能となる。SDK は、開発対象のソフトウェアが動作するシステムの提供元が配付するだけでなく、そうした提供元以外の主体（サード・パーティ）が配付するケースもある。

使用させてスマートフォン内部のデータを盗取するといった攻撃である。

（３）スマホ・マルウェアへのセキュリティ対策

スマホ・マルウェアへの対策として、主に次の 3 つが挙げられる。すなわち、①アプリのマーケットから不審なアプリを検知・排除する、②不審なサイトをブラックリスト化してブラウザに適用し、当該サイトにアクセスした際に警告を表示する（セーフ・ブラウジング）、③ユーザがアプリをインストールする際にその機能を検査する（例えば、Google Play プロテクト）。もっとも、マーケットにおける審査によってすべてのスマホ・マルウェアを検知できるわけではないほか、不審なサイトのブラックリストの作成からブラウザへの適用にタイム・ラグが存在するなど、万全の対策とはいえない。したがって、スマホ・マルウェアがインストールされることを前提とした対応が求められる。

スマホ・マルウェアがインストールされた場合、上記の攻撃の各パターンに沿った対応が求められる。ID やクレジットカード情報等の盗取に対しては、ユーザが不審なメールや SMS に気づくことや最新の攻撃手法を認識することが重要である。もっとも、情報処理推進機構による情報セキュリティの脅威に対する意識調査結果をみると、フィッシング等一部を除き、最新の攻撃手法への認知度が低く、ユーザへの啓発活動を継続的に行うことが必要であるといえる。また、ID 等の漏洩を想定したサービス仕様の策定も有効である。例えば、①多要素（あるいは多段階）認証の導入、②事前に登録したデバイス以外の使用制限、③複数の手段による取引通知機能の提供が挙げられる。

また、サービスの脆弱性の悪用に対しては、脆弱性につながりうる不備を生じさせないための配慮がサービス提供者に求められる。具体的には、サービスの企画・開発の段階において、情報資産やリスクの定義、リスク分析、必要な対策の検討を実施する「セキュリティ（あるいはプライバシー）・バイ・デザイン」の考え方を導入することが挙げられる。また、アプリの開発の段階では、攻撃に耐えうる堅牢なプログラミングとして「セキュア・コーディング」の実践[10]や、脆弱な実装を検知するためのセキュア・コーディング診断の実施が推奨される。

さらに、悪意のあるサード・パーティの SDK に対しては、アプリの開発者が SDK やアプリの動作を確認し、設定不備等がないかをチェックすることが重要である。例えば、アプリの動作が仕様どおりであるか、予期せぬ通信が発生していないか、不要なアクセスを許容していないかなどがチェックポイントとなる。

10 例えば、日本スマートフォンセキュリティ協会では、アプリの開発者向けにセキュア・コーディングのノウハウをまとめたガイドを公開している。

５．講演３「スマートフォンのセキュリティ機構」

大塚は、マイナンバーカードの機能のスマートフォン搭載に向けた検討状況、IC カードとしてのマイナンバーカードとスマートフォン搭載ケースとの差異、スマートフォンの主なセキュリティ機構について次のように発表した。

（１）マイナンバーカードの機能概要とスマートフォン搭載

マイナンバーカードによって公的個人認証サービスを利用する際には、マイナンバーカードの IC チップに格納されている公開鍵と秘密鍵のペア、および、これらの鍵のペアが正規に発行された有効なものであることを確認するための「電子証明書」[11]が用いられる。

政府では、マイナンバーカードの電子証明書をスマートフォンに搭載できるようにするプロジェクトが進められている。現在も、スマートフォンやコンビニエンスストアの専用端末にマイナンバーカードをかざすことによって、オンラインで各種行政手続きを実行することなどが可能であるが、今回のスマートフォンへの搭載が実現すれば、利便性のさらなる向上が期待できる。

今次プロジェクトは、2020 年 11 月、総務省の「マイナンバーカードの機能のスマートフォン搭載等に関する検討会」が発足してスタートした。12 月には、「第 1 次とりまとめ～電子証明書のスマートフォン搭載の実現に向けて～」が公表され、スマートフォンへの搭載のためのシステムの概要等が公表された。現在、技術検証のための実証実験が行われている。

（２）マイナンバーカードとスマートフォン搭載の形態の差異

マイナンバーカードとスマートフォンはセキュア・エレメントを搭載しているという点で共通している。ただし、スマートフォンの場合、同一端末上の他のアプリと連携して動作させることができるという点で拡張性がある。

ユーザ・インタフェースに関しては更に大きな利点がある。スマートフォンでは、画面表示やタッチパネルによる入力機能を使用可能であるため、ユーザが「自分が署名しようとしている電子文書」を目視で確認することができる[12]。一方、マイナンバーカード単体ではこの機能を実現することができない[13]。

---

11 電子証明書として、署名用電子証明書と利用者証明用電子証明書が用いられる。署名用電子証明書は、電子文書をインターネットで送信する際等に、それにデジタル署名を付与することで改変の有無を後から確認可能にする。利用者証明用電子証明書は、インターネット上のサイトを閲覧する際等に、利用者本人であることのみを相手に証明することを可能にする。

12 この機能は「WYSIWYS」（What you see is what you sign.）と呼ばれる。

13 IC カードの場合、カードリーダに接続されたディスプレイ上で電子文書を確認し、カードリーダに IC カードをかざして署名を生成するという方法が考えられる。ただし、「一見適切にみえる（が実は偽物の）画面」を「実際の画面」の上にかぶせて表示し、不適切な文書に対し

通信機能に関しても、スマートフォンでは、モバイル通信機能等によってネットワークへの常時接続が可能である点でマイナンバーカードより拡張性がある。このため、万一スマートフォンを紛失した際でも、その内部の電子証明書等をリモートで消去できる。ただし、ネットワークへの常時接続が前提であることから、スマホ・マルウェアへの対策を講じる必要があるといえる。

（３）スマートフォンのセキュリティ機構

スマートフォンの主なセキュリティ機構として、①セキュア・エレメント、②OS を保護するセキュア・ブート、③セキュア・エレメントへのアクセス制御が挙げられる。

マイナンバーカード機能のスマートフォン搭載では、フェリカネットワークス製のセキュア・エレメント（FeliCa-SE）の使用が想定されている。FeliCa-SE は、IC カード技術の標準化を推進する GlobalPlatform の技術仕様に準拠しており、スマートフォンへの搭載も進展している。FeliCa-SE 搭載スマートフォンのプラットフォームは、フェリカネットワークスのセキュリティ認証プログラム（FeliCa Approval for Security and Trust）に基づくセキュリティ評価が行われ、マイナンバーカードの場合[14]とほぼ同様にセキュリティ認証が実施されていることから、高いセキュリティの実現が期待される。

セキュア・ブートは、スマートフォンの OS を保護する機構である。スマートフォンの起動時、ブートローダ（Bootloader）という信頼できるプログラムが最初に動作し、スマートフォンの状態（lock／unlock）を確認しつつ、OS が改変されていないことを（OS に付された署名の検証によって）確認する。署名検証が成功すれば OS が起動するが、そうでなければ警告が表示される。

セキュア・エレメントへのアクセス制御については、不審なアプリによるアクセスを防ぐために、プラットフォーム事業者（フェリカネットワークス）に登録されているアプリか否かを電子証明書等で確認する機構が備わっている。確認に成功してはじめて、当該アプリを安全に利用することが可能となる。

これらのほか、生体認証によるパスワードの代替・排除が可能であることや、スマートフォンの盗難・紛失・譲渡時のリモートでの対応や運用についても整備されている。

今回のマイナンバーカード機能のスマートフォンへの搭載によって、公共

て署名させるという攻撃が知られている（ディスプレイ・オーバーレイ攻撃）。したがって、IC カードの外部環境において上記の攻撃への対策が別途求められる場合がある。

14 マイナンバーカードのセキュリティ評価は、国際標準 ISO/IEC 15408 シリーズで規定されている枠組みに基づいて行われており、第三者評価機関による（実機を用いて脆弱性の有無を確認する）脆弱性分析を含む、高度なテストが実施されている。さらに、評価プロセスが適切であったことが認証機関（公的機関）によって確認されている。

サービスに加えて、今後、金融・決済サービスでの利用も展望される。例えば、eKYC（electronic Know Your Customer）、キャッシュカードやクレジットカードによる取引、CBDC（Central Bank Digital Currency）のプラットフォームとしても活用の余地がある。

６．講演４「スマホ時代のリスク管理」

磯部は、スマートフォンを用いた金融サービスのアーキテクチャと内在するリスク、リスクを管理する際の留意点、リスク管理の高度化に資する取組みについて以下の通り発表した。

（１）金融サービスのアーキテクチャとリスクの変化

スマートフォンを用いた金融サービスのアーキテクチャは、PC を前提とした場合とは異なる。オンライン・バンキングの場合、ユーザが PC を用いるケースでは、銀行のサーバが PC にウェブ・サービスを提供する形態が主流である（多くの場合、ブラウザを通じてサービスが提供され、専用のソフトウェアを立ち上げるケースは少ない）。一方、スマートフォンを用いるケースでは、銀行がアプリを開発してユーザに提供し、銀行のサーバがアプリとの間で通信や処理を行う。このとき、アプリは、自身が有する機能に加えて、スマートフォンの OS、SDK、デバイス（生体認証用センサやカメラ等）の機能も使用することが多い。

こうしたサービスのアーキテクチャの変化はリスクの変化をもたらしている。銀行のサーバがウェブ・サービスを提供する形態の場合、リスクの源は（銀行が制御できない）ユーザの PC であり、銀行は「PC が脆弱である」との前提でリスクを分析し、それに基づいてウェブ・サービスを自ら設計することでリスクを制御できる。スマートフォンの場合も、アプリが使用するプラットフォームの機能を銀行が適切に把握できるのであれば、PC の場合と同様にリスクに合わせて適切なアプリを設計することができる。しかし、近年、スマートフォンのプラットフォームのブラックボックス化が進んでおり、銀行は、プラットフォームのリスクを分析・評価し、その結果に基づいてアプリを適切に設計するという対応が困難となっている。

（２）外部リスク管理と求められる視点

上記のようなリスクは、サービス提供者が直接関与できない部位に関係しているという意味で「外部リスク」といえる。スマートフォンの場合には、こうした部位が多岐にわたり、それぞれのメーカーが異なることから、外部リスク管理の難易度が高まっている。また、プラットフォームの脆弱性を発見できたとして

も、それを直ちに解消させることが常に可能というわけではない。

例えば、スマートフォンへの標準装備が進められている TEE（Trusted Execution Environment）[15]に関して、製品の一部に各種の脆弱性が存在していることを示す研究成果が報告されている[16]。また、TEE は、SoC（System on a Chip）[17]の内部に実装されるなど、ハードウェアとの結び付きが強く、脆弱性を解消するための改修等が容易でない場合がある。

サービス提供者は、こうしたリスクを認識し、特定のデバイスやプラットフォームを対象にサービスを提供しても問題ないかを見極める必要がある。特に、暗号や認証の処理をプラットフォームに依存する場合にこうした見極めが重要となる。

（３）外部リスクの管理・評価に資する取組み

最近、リスク管理の文脈において「特定の部位に暗黙的な信頼を置かず、常時必要な検証を行うことが必要である」という「ゼロ・トラスト・アーキテクチャ」（Zero Trust Architecture）の考え方が注目されている。これはスマートフォンのサービスにおいても当てはまる。ただし、スマートフォンのプラットフォームがさまざまなデバイス等から構成されているため、人手ですべて検証することは実務上困難であり、自動化された仕組みや管理・評価を前提とした環境整備が必要である。

自動化の仕組みとして、アテステーションの活用が挙げられる。アテステーションは、アプリやデバイスが安全な状態か否かを検証する機能である。例えば、スマートフォンの「安全な状態」（工場出荷時点の状況等）を事前に登録した後、実際のサービス提供時にスマートフォンの状態を計測し、登録したものと照合するという運用が想定される。こうした考え方に基づく手法が、プラットフォームの一部を対象とするものに限られてはいるが既にいくつか実装されている[18]。また、アテステーションのプロトコルやデータのフォーマットの標準化に向けた検討が、IETF（Internet Engineering Task Force）[19]において進められている。

---

15 TEE は、暗号処理等高いセキュリティが要求される処理のための実行環境（TEE 空間）を提供する機能である。TEE 空間は、通常のアプリが動作する空間（Rich Execution Environment）と分離され、両空間の間の通信は厳格なアクセス制御のもとで実行されるように設計される。

16 詳細については、磯部光平・宇根正志、「スマートフォン等のスマート・デバイスにおけるセキュリティ：プラットフォーム化によるリスクの現状と展望」、『金融研究』第 40 巻第 3 号、日本銀行金融研究所、2021 年、77～102 頁を参照されたい。

17 SoC は、1 つの物理的な IC チップの内部に複数の IC チップの機能を回路として集約したものを指す。

18 例えば、OS やアプリ配信サービスの API 応答によって正規アプリ経由でのアクセスを検証するもの（Apple App Attest）や、セキュア・ブート等の状況からデバイスの改変の有無を検証するもの（Android SafetyNet Attestation）が挙げられる。

19 IETF は、インターネットにおいて使用される情報通信技術の標準仕様の策定を主たる目的と

また、プラットフォームのブラックボックス化への対応として、第三者による評価が可能となるように、公開された技術に基づいてプラットフォームを設計・構成する取組みが進められている。例えば、セキュアオープンアーキテクチャ・エッジ基盤技術研究組合[20]では、RISC-V[21]等のオープン・ソースの技術を用いてSoC や TEE の設計・開発を進めており、透明性が高いプラットフォームの実現が期待されている。

とはいえ、「こうすればプラットフォームを安心して使用できる」といったものは現時点では存在しない。サービス提供者は、プラットフォームの状況やアテステーション等の効果・限界を考慮しつつ、リスク評価をアップデートしながらアプリやサービスの提供について随時検討・判断していく必要がある。

７．パネル・ディスカッション

パネル・ディスカッションでは、スマートフォンを利用して安全な金融サービスを提供していくにあたっての課題や留意点について議論を行った。その概要は以下のとおりである。

（１）PC の利用を前提としたサービスとのセキュリティ対策の違い

まず、モデレータの宇根は、主に PC を利用した従来の金融サービスに加えて、近年、スマートフォンを利用した金融サービスが普及している状況を説明した。そのうえで、利用者の端末の違い(PC とスマートフォン)によってセキュリティ・リスクや対策にどのような差異が生じうるか問題提起した。

高橋は、PC とスマートフォンの違いとして、可視光カメラを利用した顔認証を例に、認証精度に差が出る可能性があることを説明した。すなわち、スマートフォンで顔認証を実行する場合、室内で使用されることが多い PC に比べて、可視光カメラによる画像が外光によって影響を受け、その結果、認証精度に影響が生じる可能性がある。また、スマートフォンでは、OS、ファームウェア、ハー

する技術者団体であり、標準仕様は「RFC（Request for Comments）」と呼ばれている。アテステーション・プロトコルの標準化は RATS（Remote Attestation Procedures）WG において検討されている。

20 セキュアオープンアーキテクチャ・エッジ基盤技術研究組合は、IC チップのセキュリティを検証できるようにするために、オープン・アーキテクチャを活用したセキュリティ技術の試験・研究を目的とする研究組合であり、2019 年 8 月に設立された（http://trasio.org/home/、2021 年 9 月 15 日）。

21 RISC-V は、オープン・ソースによって開発された命令セット・アーキテクチャ（Instruction Set Architecture : ISA）であり、RISC ISA の 5 番目のバージョンとして、最初の仕様が 2011 年にリリースされている。ISA とは、概していえば、IC に内蔵されるプロセッサ等で使用される各種処理やデータ形式の体系を意味する。代表的な ISA としては、x86 や Arm が挙げられる。

ドウェア等が一体となってセキュリティ機能が提供されている旨を紹介し、そうした事情から、生体情報等の秘密の情報をハードウェア内部等で安全に取り扱うことが可能になっている点を指摘した。

本間は、スマートフォンの利用者を巧みに騙してマルウェア感染やパスワードを盗取する犯罪が増えている現状を説明したうえで、利用者が騙されないようにするために、犯罪の手口を紹介するといった啓発活動の重要性を取り上げた。スマートフォンは幅広い年代に利用されており、各年代のユーザの嗜好等に応じた啓発活動のあり方を検討するとともに、アプリやサービスを提供するさまざまな業界が足並みを揃えて啓発活動に取り組むことが重要であると強調した。

大塚は、スマートフォンの転売に着目し、マイナンバーカード機能をスマートフォンに搭載すると内部の機能を無効化しないまま転売されることによって生じるリスクを指摘した。このリスクへの対応として、転売先のキャリア・ショップや中古端末取扱業者において、スマートフォン内部（セキュア・エレメント）の秘密情報を消去する運用が検討されていると説明した。また、データを消去せずに個人間で転売した場合でも、遠隔からの操作によって秘密情報を消去する機能を使用することによって当該リスクを低く抑えることができるとした。

（２）利便性とセキュリティのバランス

スマートフォンは瞬時に起動してアプリを動作させることができるという高い利便性を有している。アプリによって提供されるサービスにも同じレベルの利便性が期待されている。一方、セキュリティは利便性とトレードオフの関係にあり、セキュリティ対策のために煩雑な操作を利用者に要求すると、利用者はサービス自体を敬遠することになりかねない。**宇根**は、こうした利便性とセキュリティのバランスについてパネリストに意見を求めた。

鎌田は、金融機関におけるアプリ開発の現場では、主に利便性を重視するビジネス部門とセキュリティ部門との間の関係性によって、利便性とセキュリティのバランスが決まる傾向にあり、現場における部門間での適切な関係性が両者のバランスをとるうえで重要であるとの見方を示した。また、外部事業者とのサービス連携の場面において、情報共有と認識の擦合せが適切に行われず、「相手がセキュリティ対策を担ってくれる」とお互いに誤解したままシステム開発を進めた事例を紹介し、関係者が情報を共有し認識を揃えながらシステム開発を進めることが重要であると指摘した。さらに、グローバルに利用されているサービスには一定のセキュリティを維持しつつ、高い利便性を実現しているものが多く、それらを参考にバランスのあり方を検討することが有用であると説明した。

高橋は、生体認証について、認証処理そのものの利便性は高くなってきているが、事前に行う生体情報の登録作業等に本人確認を伴う煩雑な手続きが必要であり、利便性を向上させるうえで、そうした手続きを、セキュリティを損なうことなく改善することが求められるとの見方を示した。また、スマートフォンの機種変更時に必要となるアカウント・リカバリーに触れ、リカバリー作業が容易なサービスは機種変更時には便利だが、第三者によってアカウント乗っ取りのリスクがあることから、セキュリティと利便性のバランスに留意する必要があると指摘した[22]。そのほか、認証の利便性を高める技術研究として、利用者の行動履歴等を用い、スマートフォンを持っているだけで本人であると認証してくれるような研究について紹介した。

（３）サービス連携に伴うリスク

近年、フィンテック企業によるサービスとインターネット・バンキングのサービス連携など、複数の事業者が既存のサービスを連携させて新しいサービスを提供する動きが広がっている。こうした状況は、既存のサービスの運用環境が変化することを意味しており、既存サービスにおいて想定されていたリスクの形態が変化する可能性が考えられる。こうした観点から、**宇根**は、サービス連携に伴うリスクについて意見を求めた。

鎌田は、サービス連携を行う事業者間でセキュリティ対策にかけられるリソースに差異がある場合、一方にとっては「実施して当たり前」のセキュリティ対策が、もう一方にとってはそうでないという事例も発生していると紹介した。そのうえで、サービス連携を検討する際には、必要なセキュリティ対策のレベルを事業者間でしっかり擦り合わせることが求められるとした。

また、**宇根**は、スマートフォン上のサービスを使用する際に必要なユーザの本人確認の手段として eKYC が活用されようになってきている状況を説明したうえで、スマートフォン搭載されたマイナンバーカード機能における本人確認のセキュリティについて意見を求めた。

大塚は、マイナンバーカード機能における本人確認について、対面での本人確認と同等の安全性を確保するという方針で設計されている旨を説明したうえで、インターネット取引で想定されるリスクについても十分に考慮されていると回答した。

---

22 機種変更した後、ID・パスワードの入力だけでアカウントにログインできるサービスでは、ID・パスワードさえあればどの端末からでもログインできるということであり、ID・パスワードが漏洩したときのリスクが高い。そのため、アカウント・リカバリー時には、複数の手段でユーザ認証を行うことが望ましい。例えば、事前に登録されているメールアドレスや電話番号を利用してその保有者であることを確認する方法などがある。

（４）アジャイル開発におけるセキュリティの確保

従来のシステム開発では、セキュリティ対策に関する検討は要件定義のプロセスの中で行われ、これに従って開発やテストが進められるケースが多かった。一方、現在注目されているアジャイル型[23]の開発では、開発を進めながらテスト・評価を実施し、要件を必要に応じて見直しながら完成度を高める手法が採用されている。**宇根**は、こうしたアジャイル開発においてセキュリティ機能を適切に開発・実装するための留意点についてパネリストに見解を求めた。

本間は、スマートフォン用のアプリに関しては、アジャイル型での開発事案が増える中で、それに合わせたセキュリティ機能の実装方法が課題となっていることに同意した。そのうえで、理想的には、アジャイル開発チームにセキュリティ技術に精通するスタッフを加えるべきであり、その常駐が難しい場合であっても、要所ごとにセキュリティ技術者に確認を求めていくことが必要との見解を示した。また、アプリをデザインする段階からセキュリティを意識しておくことが必要であり、アプリ設計に携わる技術者にはそうしたトレーニングが必要であると指摘した。

高橋は、システム開発の現場では、仕様上問題ないと判断していた箇所に脆弱性が潜んでおり、運用後にその脆弱性が顕現化するケースも少なくないことから、セキュリティ機能を実装する際にはアジャイル開発の考え方が向いているとの見方を示した。そして、OODA（Observe〈観察〉、Orient〈状況判断、方向付け〉、Decide〈意思決定〉、Act〈行動〉）サイクルを頻繁にまわし、臨機応変に柔軟な対応を講じる体制を整備することが必要であり、開発部隊は、セキュリティの専門家で構成される専門部隊[24]と連携することが必要であると説明した。

以　上

---

23 迅速にソフトウェアを開発するための技法の 1 つ。従来から行われてきたウォーターフォール開発が、予めソフトウェアなどの全機能に関する要件定義や設計を綿密に行ってから開発に入るのに対し、アジャイル開発では、機能単位の小さなサイクルで、計画から設計・開発・テストまでの工程を繰り返すことにより開発が進められる。

24 サイバー攻撃の検出・分析を行い、対応策のアドバイスなどを行う SOC（Security Operation Center）や CSIRT（Computer Security Incident Response Team）がその一例。また、CSIRT が情報システムのセキュリティ・インシデントの対応を行う組織であるのに対し、製造／販売製品のセキュリティ・インシデントに対応する組織は PSIRT（Product Security Incident Response Team）と呼ばれる。