2019年1月24日

各　　位

東京都港区虎ノ門四丁目1番 28 号
日本通信株式会社
代表取締役社長　福田　尚久
（コード番号：9424）
問合せ先　広報室長　堀江　祐子
電話 03-5776-1700

日本通信、金融庁の結果公表を受け FinTech 実証実験の概要および結果を公開 ～インターネット金融取引、世界最高の安全性を実現～

日本通信株式会社（「当社」という）は、金融庁の「FinTech実証実験ハブ」に選定された、FinTechプラットフォーム（FPoS（エフポス）（Fintech Platform over SIM））を利用したスマートフォンでの安全・安心な金融取引に係る実証実験の結果を金融庁が本日公表したことを受け、FPoSおよび実証実験に関する概要及び結果を公開しましたので、お知らせいたします。

FinTech分野でのオープン・イノベーションに対する期待が高まっている中、オンラインバンキングサービスの不正利用等、セキュリティに関する問題が注目されています。近年の犯罪手口の高度化・巧妙化（中間者攻撃やマン・イン・ザ・ブラウザ攻撃、端末の乗っ取り（ハイジャック）など）は深刻な問題であり、新たな脅威に対する解決方法の登場が強く望まれています。

当社のFPoSは、このような背景をもとに考案されたプラットフォームですが、金融機関がFPoSを商用導入する場合、金融庁の「主要行向けの総合的な監督指針」並びに「中小・地域金融機関向けの総合的な監督指針」の規定に従う必要があります。監督指針の当該セクションには、全国銀行協会の申し合わせ等において記載されている「現行方法」によるセキュリティ対策事例が挙げられていますが、サブSIM等を用いたFPoSによるセキュリティ向上の仕組みが、監督指針に記載されている要請を忠実に実現しているか否かが論点となっていました。

このような背景のもと、参加金融機関・企業として株式会社群馬銀行、株式会社千葉銀行、株式会社徳島銀行、株式会社マネーフォワード、及びサイバートラスト株式会社に協力を頂き（詳細は、2018年5月31日付け「日本通信のFinTechプラットフォームが金融庁の「FinTech実証実験ハブ」の支援案件として決定」をご参照ください）、FPoSの法令への適合、金融取引の安全性や利用者の利便性、銀行及びフィンテック企業における導入・運用の容易さ等を検証してまいりました。

今回の実証実験を通じ、監督指針及び実証結果における金融庁からの見解は、以下のとおりとなります。

＜金融庁からの見解＞

・本人認証方法へのサブSIMの利用は、それが適切に運営されているのであれば、監督指針で示されている「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」などの高度化・巧妙化する犯罪手口への対策にかかる着眼点も充足するものと考えられ、本実証実験の手法は、インターネット等の通信手段を利用した非対面取引を行う場合の本人認証の観点で特段の問題はないと考えられる。

・実証実験の結果、サブSIMを用いた新たな本人認証方法は、ワンタイムパスワード等を使用する現行方法と同等以上のセキュリティ（取引内容の改ざん防止を含む）を確保しつつも、利便性を損なわずに本人認証等が実現可能であることを確認でき、本人認証等へのSIMカードの活用が金融取引の安全性の確保や利便性の向上に資する可能性があることが示された。

・今後、こうした新たな本人認証方法の実現により、金融機関等による、よりセキュリティの高いサービスの実現や利用者の利便性の向上等が期待される。

（本件に関する金融庁の発表資料：https://www.fsa.go.jp/news/30/20190124.html ）

本実証実験の詳細な報告書は、下記よりご覧いただけます。

FPoS (FinTech Platform over SIM)を利用したFinTech実証実験に係る報告書

https://www.j-com.co.jp/ir/pdf/press_190124.pdf

当社は、このFPoSによる金融取引セキュリティ技術を、これからも国内外に向け展開します。

■日本通信について

日本通信は 1996年５月24日、モバイルが実現する次世代インターネットを活用して日本の次世代経済の基盤を構築する総務省の方針を実現する会社として設立されました。当社ビジネスモデルはのちにMVNOと命名され、2009 年３月、総務省の携帯市場のオープン政策のもとNTTドコモとの相互接続を実現しました。これにより「格安SIM」が生まれ、携帯事業者以外から携帯通信（SIM）が買える市場が誕生しました。次は、携帯電話以外の産業が、自社サービスにモバイルを組み込み、産業全体がモバイルを活用し成長する番です。MVNO ルールメーカ、世界初のMSEnabler としての強い技術ビジョンと高い遂行力によって、日本発の経済創出の一翼を担うべく次世代プラットフォームの構築に取り組んでいます。東京、米国コロラド州およびフロリダ州、アイルランドダブリンに拠点を置き、東京証券取引所市場第一部に上場（証券コード：9424）しています。当社のコーポレートガバナンスのポリシーとして、社外役員が 過半数で、全社外役員は独立役員です。

FPoS (FinTech Platform over SIM)を利用したFinTech実証実験に係る報告書

平成31年1月24日

日本通信株式会社
株式会社群馬銀行
株式会社千葉銀行
株式会社徳島銀行
株式会社マネーフォワード
サイバートラスト株式会社

目次

1. はじめに

1980 年代から急速に普及し始めたインターネットは、SNS やネットショッピングなどを多くの人が日常的に利用するに至り、今や生活に不可欠な存在となった。当初、インターネットは、低速のダイアルアップ方式によりサービスが開始され、その後、ADSL の普及や光回線の登場により高速通信が可能となり、ネットショッピング、動画・音楽提供サービス等が登場し、急速に普及が始まった。

一方、2001 年には第 3 世代携帯電話（3G）サービスが開始され、携帯電話やスマートフォンからでも高速のインターネット接続が可能となった。現在、日本国内における携帯通信サービスの契約数は約 1 億 7 千万契約 [1)]にも及んでおり、携帯電話・スマートフォン利用者向けの様々なサービスが登場し続けている。

その中で、スマートフォンを利用した金融サービスも急速に発展している分野の一つである。市場におけるサービス展開と相俟って、銀行から電子決済等代行業者へのオープン API 導入が努力義務として規定されるなど、本格的な FinTech 時代に向けた基盤整備も進展している。

このように FinTech 分野でのオープン・イノベーションに対する期待が高まっている中、オンラインバンキングサービスの不正利用等、セキュリティに関する問題が注目されるようになってきた。近年の犯罪手口の高度化・巧妙化 [2)]（中間者攻撃やマン・イン・ザ・ブラウザ攻撃、端末の乗っ取り（ハイジャック）など）は深刻な問題であり、新たな脅威に対する解決方法の登場が強く望まれている。

Fintech Platform over SIM（以下、「FPoS」と略記、エフポス)は、このような背景をもとに考案されたプラットフォームである。特に、スマートフォンを利用した金融サービスを安全に、かつ利便性高く行うことをその狙いとしている。スマートフォンには、SIM カードと呼ばれる IC カードを読み取るための IC カードリーダが内蔵されている。この点に着目し、高度なセキュリティを備える IC カードに暗号鍵と電子証明書等を搭載し、これらを用いることで安心・安全な金融サービスをスマートフォンで実現することが可能となる。

この FPoS について、その安全性、利用者の利便性、銀行及び Fintech 企業における導入・運用の容易さ等を検証するため、日本通信株式会社、株式会社群馬銀行、株式会社千葉銀行、株式会社徳島銀行、株式会社マネーフォワード並びにサイバートラスト株式会社の 6 企業が金融庁 FinTech 実証実験ハブの枠組みに参加し、実証実験を行った。

本報告書では、FPoS の原理、実証実験のねらい、実験システムの構成、実験内容及び評価結果を述べる。

---

1) 電気通信事業者協会「2018 年度 携帯電話・PHS の事業者別契約数」より引用。

2) 金融庁「主要行向けの総合的な監督指針 Ⅲ-3-8-2-(2)セキュリティの確保」より引用。

2. 概要

2.1 FPoS の位置づけ

オンラインバンキングサービスにおける不正利用の変化は、アクセス方法変遷の歴史でもある。図 2.1 に示すように、オンラインバンキングが普及し始めた当初は PC での利用が一般的であり、ID とパスワードを用いて第三者による不正アクセスを防止していた。近年は、これに加えて第 2 要素認証、たとえば、ワンタイムパスワードトークン（発行器）などを利用するのが一般的となってきた。しかし、スマートフォンが普及した現在、PC での利用を前提としていたワンタイムパスワードトークンは、利用する金融サービスごとに所有する必要があり、利用者の利便性を損ねてしまう。そのため利便性を考慮したワンタイムパスワードアプリが登場し、普及しているが、スマートフォン 1 台で利用できてしまうことは、セキュリティの観点から、真に 2 要素認証であるかどうかが問題となる。

これに加えて、中間者攻撃やマン・イン・ザ・ブラウザ攻撃、端末の乗っ取り（ハイジャック）などの新たな攻撃手法が出現するに至って、第 2 要素認証のみでは不正アクセスを防御できない事例が多数発生するようになり、犯罪手口の高度化・巧妙化に堪え得る不正利用回避手段の開発・適用が強く望まれるようになってきた。

このような状況を鑑み、利便性にも配慮しながら開発したのが FPoS である。FPoS の基本技術は、SIM カードに格納した電子証明書と暗号化機能、そしてこれらを活用した認証及び署名手続きである。この SIM カードは銀行の ATM カードやクレジットカード等として金融サービスにおいて幅広く使われている IC カードと同一種のカードである。2016 年 1 月から交付が開始されたマイナンバーカードも IC カードであり、電子証明書と暗号化機能を搭載することで、本人確認や電子文書の送信等を安心・安全に行うことができる。

これら技術を適用することにより、スマートフォン上のアプリケーションソフトウェアが乗っ取られたり、取引経路上での中間者攻撃などを排除することができ、仮に取引電文が盗聴され、改ざんされた場合でも、それを金融機関及び利用者に即時に通知することが可能になる。

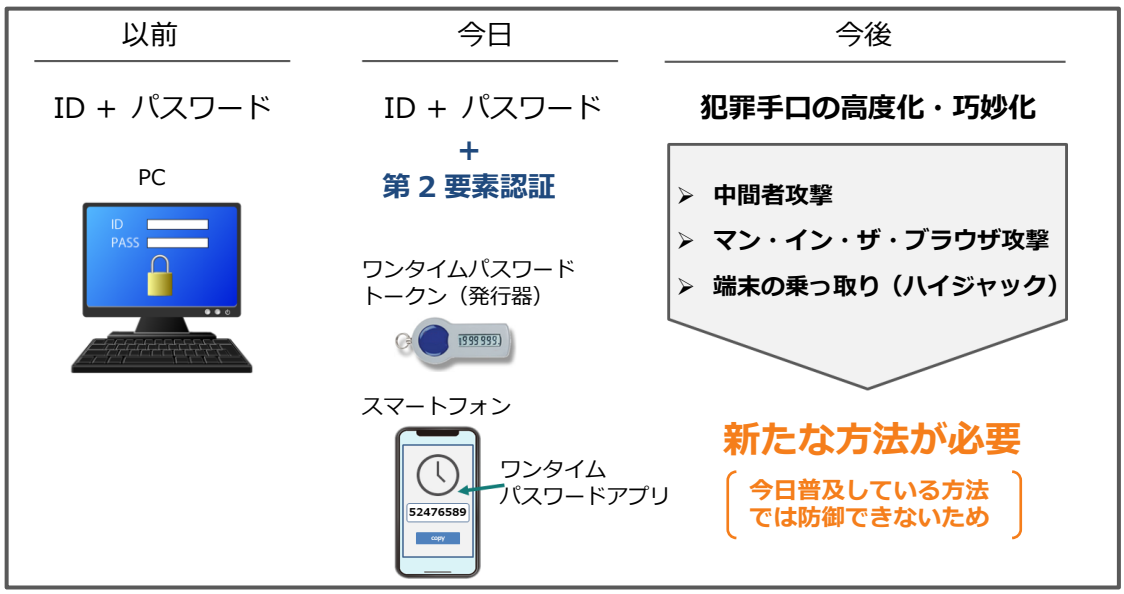

図 2.1　オンラインバンキングにおけるアクセス方法の変遷

FPoS の基本的な考え方は、「利用者が正しい利用者であること」の本人性確認と「取引電文が改ざんされていないこと」の保証にある。FPoS は、これら 2 つの要件を満たすプラットフォームとして設計された。その考え方を図 2.2 に、セキュリティリスクと対応手段の対応関係を図 2.3 に示す。

前者の本人性の確認については、FPoS は、一般的に言われる 3 つの要素のうち「利用者のみが知っている知識」及び「利用者のみが保有している物」を認証に利用することを基本としている。FPoS の場合、「利用者のみが知っている知識」とは SIM カードなどのセキュアなデバイスをアクセスする際のパスワードであり、「利用者のみが保有している物」とは、SIM カードなどのセキュアなデバイスそれ自身である。これに「利用者が生まれつき備えているもの」による認証（いわゆる生体認証）を組み合わせることも容易である。FPoS はこれらの要素を組み合わせ、本人性を確認する。即ち、利用者は SIM カードのパスワード入力と生体認証を行うことで、SIM カードなどのセキュアなデバイスにアクセスすることができ、SIM カードなどの内部で認証情報を生成する。生成した認証情報は FPoS サーバへ送信され、利用者の認証を行う。

また、後者の情報改ざん検知・防止については、電子証明書による認証及び署名を利用している。即ち、暗号鍵（公開鍵及び秘密鍵）、アクセス認証用及び署名用の電子証明書、並びに認証情報生成及び署名の演算プロセスを SIM カード内部に格納し、SIM カード内部でこれらの演算を行うことで漏洩リスクを排除し、認証情報作成及び電子署名を行う構成としている（図 2.4）。RSA2048 などの暗号方式を採用した場合、現在の計算機処理能力では 10 年程度以上の演算時間がかかることから、この方法を採ることにより、有意な時間内での解読が困難であり、また、仮に解読された場合でも改ざんをリアルタイムに検知することが可能であることから、端末乗っ取りや中間者攻撃、マン・イン・ザ・ブラウザ攻撃などの不正操作を防御することが可能になる。

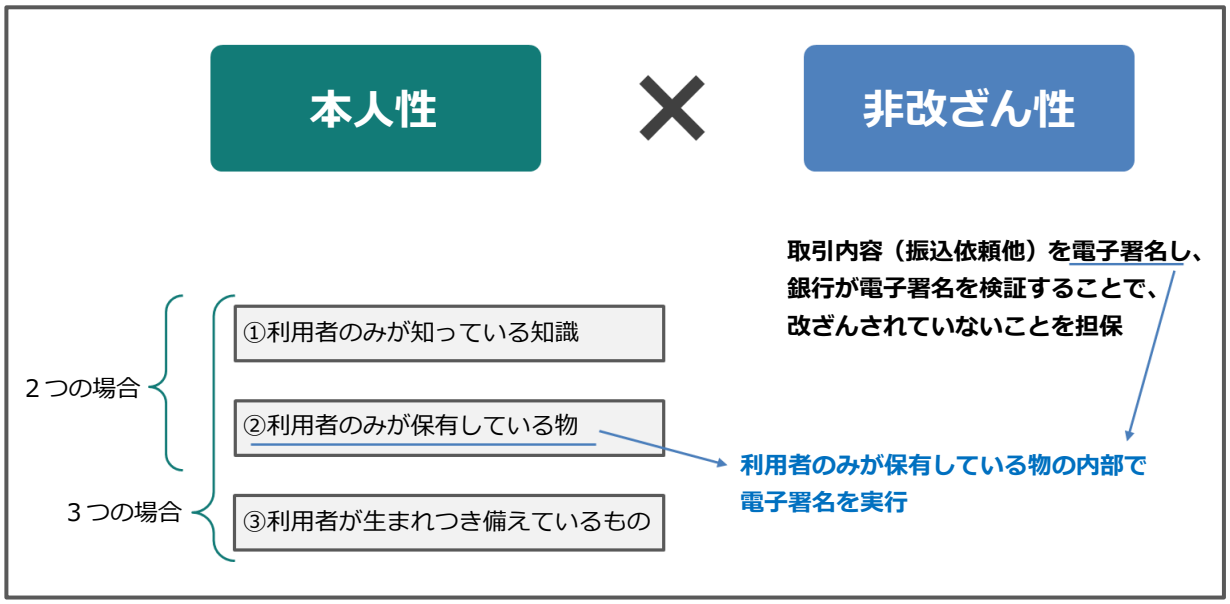

図 2.2　本人性と非改ざん性に対する FPoS の考え方

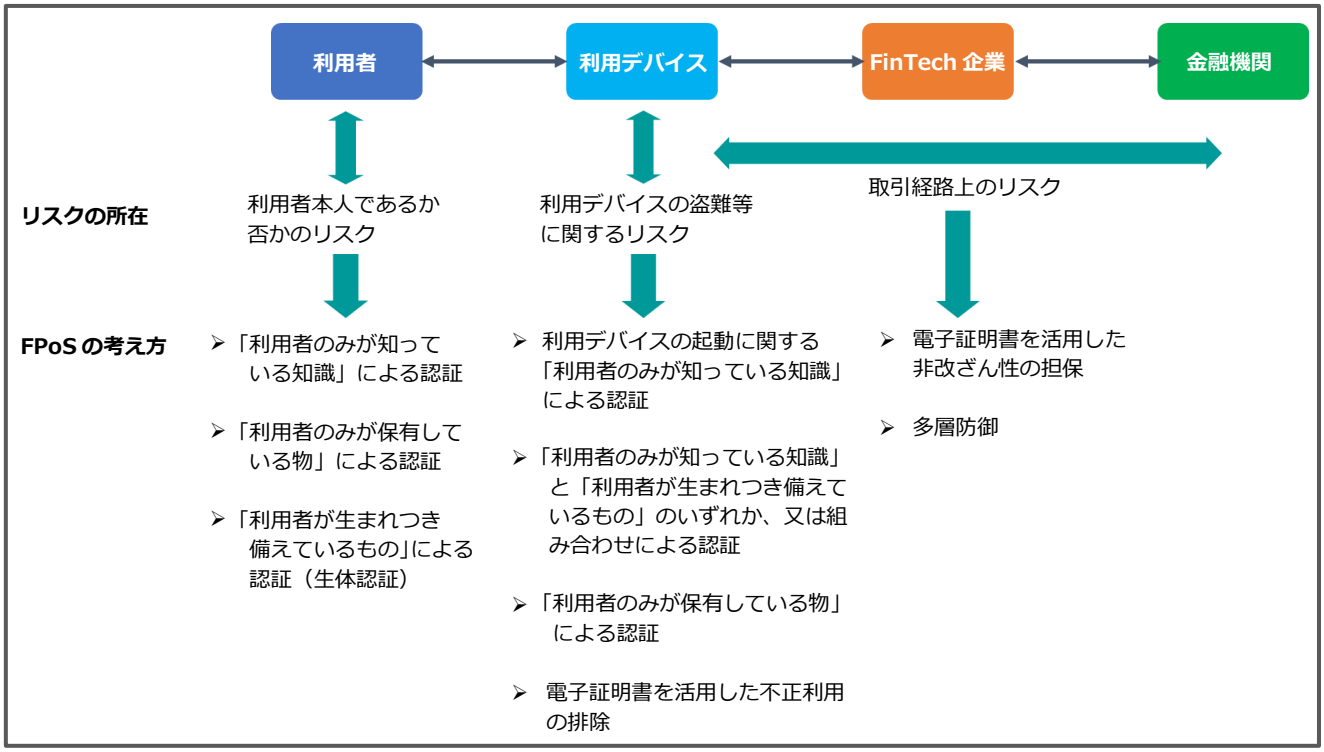

図 2.3　本人性と非改ざん性に係るセキュリティリスクの所在と FPoS での対応

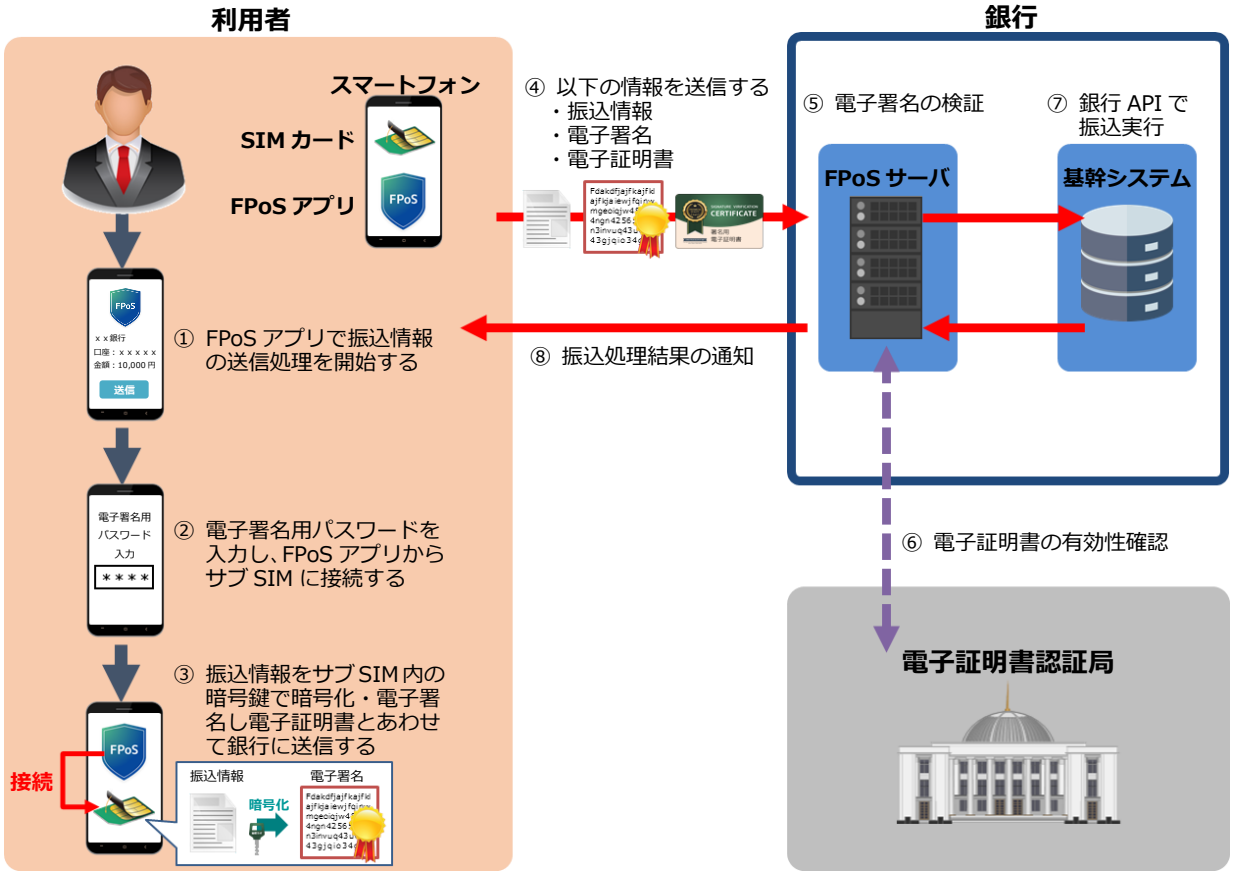

図 2.4　SIM カードを用いた電子署名の流れ

以上のような特徴を有する FPoS は、各種の金融取引に利用できる汎用プラットフォームである。その特徴を図 2.5 に示す。複数の銀行口座を保有すると、その数だけ第 2 要素認証の手段、例えばワンタイムパスワードトークンを持たざるを得ないことは誰もが経験することである。これは便利とは言えない。共通に利用できるプラットフォームであれば、このような煩雑さを回避できるところ、FPoS では、電子証明書と暗号鍵の仕組みで煩雑さを回避している。さらに、スマートフォンのようなモバイルデバイスを利用する場合、ワンタイムパスワードトークンをスマートフォンと共に持ち歩くことさえ不便であるから、常にスマートフォンに格納されている SIM カードに電子証明書や暗号鍵を内蔵させておけば便利である。この点も考慮して、FPoS を設計した。

FPoS のさらなる特徴は、サブ SIM と呼ばれるフィルム状の SIM を活用することにある。その理由は、今日の携帯電話サービスの提供事業者は 900 社を超えており [3)]、各事業者が個別に発行する SIM カードに電子証明書を搭載して FPoS サービスを均一に提供することが困難であるためである。サブ SIM は通常のプラスティック製通信用 SIM（以下、メイン SIM という）の上に貼り付けて利用し、SIM カードスロットが 1 つしか搭載されていないスマートフォンでも、メイン SIM とサブ SIM を同時に搭載することができる。サブ SIM は、海外各国で利用が始まっている新たな形状の SIM であり、この SIM の利用を通して、どの携帯事業者と契約していても、FPoS サービスの利用が可能となる。

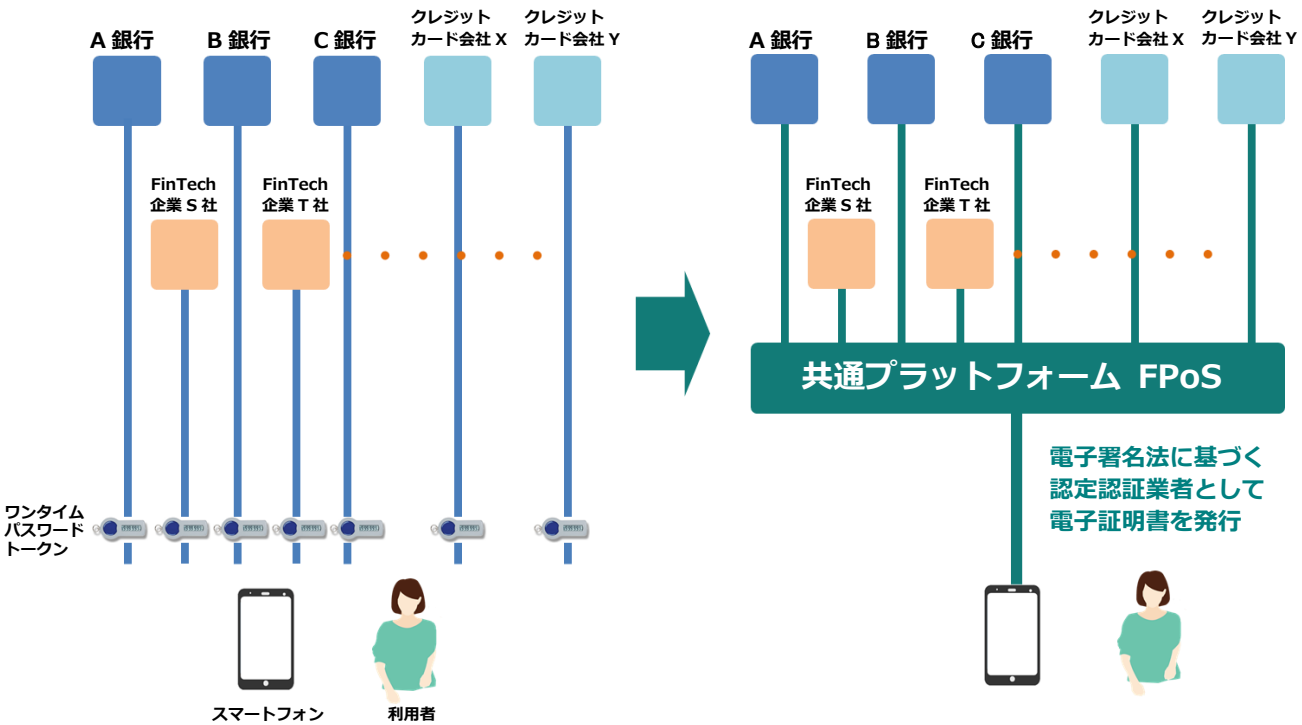

図 2.5　共通プラットフォームとしての FPoS のイメージ

3) 総務省 「電気通信サービスの契約数及びシェアに関する四半期データの公表（平成 30 年度第 1 四半期（6 月末））」より引用。

実証実験では、Android スマートフォンを利用し、サブ SIM を搭載した。iPhone の場合は、Secure Enclave というセキュアエレメントを用いることでサブ SIM 利用時と変わらない FPoS 機能の実装が可能になる。このように、サブ SIM に証明書等を実装する場合を含めて、複数種類の実装が可能である。図 2.6 に、スマートフォンの OS 種別毎の好ましい実装方法を整理した。

セキュリティ機能運用の観点からは、FPoS は「発生予防」、「発生防止」及び「早期発見」の 3 段階を幅広くカバーする（図 2.7）。その根源は、電子証明書と暗号化技術による不正利用防止と早期発見にある。特に従来、対策が手薄であった取引自体の改ざん検知並びに防止に対する効果は大きいと考えられる。加えて、FPoS を採用していること自体、宣伝効果として発生予防にも有用であると考えられる。

	Android スマートフォン	iPhone
秘密鍵と公開鍵の生成を受け持つハードウェア	サブ SIM	Secure Enclave （iPhone に内蔵されているコプロセッサ）
秘密鍵を保管するハードウェア	サブ SIM	Secure Enclave
電子署名処理を実行するハードウェア	サブ SIM	Secure Enclave

図 2.6　FPoS 機能の実装方法

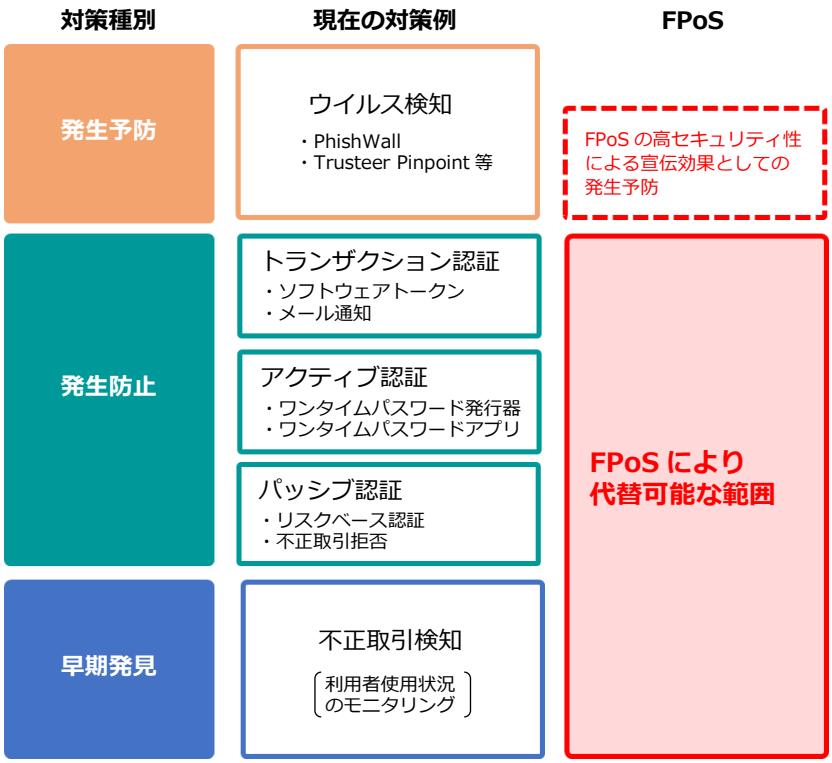

図 2.7　セキュリティリスク対策と FPoS の適用範囲

2.2 実証実験の狙い

前節に記載したとおり、FPoS によるセキュリティ向上の原理は明確であることから、実証実験では、原理の実証よりはそれが正しく動作することや利用者の利便性検証など、以下の各点を明らかにすることを主眼した。

1) FPoS の仕組みを確実に実装できるか
2) FPoS の利便性は高いか
3) 銀行にとって、FPoS の運用性に問題はないか
4) FinTech 企業にとって、FPoS の運用性に問題はないか
5) FPoS の導入に際し、関連法令・規則等についての検討事項があるか

3. 実証実験の概要

3.1 サービス

実証実験は、銀行が行っているサービスのうち参照系サービスとして預金残高照会を、また更新系サービスとして振込（自行内及び他行宛て）及び住所変更（個別及び一括)を選択し、2.2 節で述べた項目の評価を行うこととした。

これらのサービスは、銀行自体が直接利用者にサービスを提供する場合と FinTech 企業がサービスを提供する場合の二種類に分かれる。実証実験では、前者を徳島銀行が提供するサービスとして、また、後者を群馬銀行・千葉銀行と接続されるマネーフォワードが提供するサービスとして検証することとした。

3.2 システム構成

上述のサービスを実現するためのシステム構成を図 3.1 に示す。実証実験システムは、端末、FPoS 機能サーバ、仮想銀行機能サーバ、FinTech 企業サーバ及び電子証明書認証局から構成される。利用者端末は無線ネットワークを介して、徳島銀行を模擬する仮想銀行機能サーバと FinTech 企業を模擬する FinTech 企業サーバに接続される。FinTech 企業サーバは、さらに千葉銀行を模擬する仮想銀行機能サーバと群馬銀行を模擬する仮想銀行機能サーバに接続される。これらの仮想銀行機能サーバの前段に設置された FPoS 機能サーバは、電子証明書認証局と接続される。各ノードの主たる機能と特徴は以下のとおりである。

(1) 端末

端末には、メイン SIM、サブ SIM、FPoS 設定アプリ、徳島銀行サービス用アプリ若しくはマネーフォワードサービス用アプリのどちらか一方、若しくは両方を実装した。サブ SIM には 2 種類の電子証明書、2 種類の暗号鍵及び暗号演算等の機能を実装した。メイン SIM、サブ SIM 及びスマートフォンは、それぞれの固有 ID（メイン SIM に格納されている電話番号など）で紐づけ、紐づけされた ID 以外の組み合わせでの利用を禁止して、SIM 抜き取りなどの行為を防ぐ構成とした。

(2) 仮想銀行機能と FPoS 機能

各銀行の基幹システムを模擬した仮想銀行機能の前段に FPoS 機能サーバを設置し、電子証明書や電子署名を扱う処理は、この FPoS 機能サーバで処理して、銀行システム側とは各仮想銀行機能サーバが発行する API で接続する構成とした。また、両者を標準的な認可プロトコルである OAuth2.0 で連携させ、情報アクセスの認可手続きを明確化した。サーバの実装に際しては、サーバ及び伝送装置類をファイアウォール、IDS 及び IPS 等が設置されたデータセンタに設置し、IP アドレス監視制御を含む多層防御の仕組みを併用する形態で実験を行った。

(3) FinTech 企業

端末に実装されるマネーフォワードサービス用アプリと FinTech 企業（マネーフォワード）サーバ間はマネーフォワードが提供する API を利用して通信を行い、FinTech 企業サーバと FPoS 機能間は FPoS が提供する FPoS API を利用して通信を行う構成とした。また、両者を標準的な認可プロトコルである OAuth2.0 で連携させ、情報アクセスの認可手続きを明確化した。

(4) 電子証明書認証局

電子証明書認証局は、サブ SIM に格納する 2 種類の電子証明書を発行する機能、及び FPoS サーバの認証機能を管理する機能（例えば、発行した電子証明書を失効させる機能）を有する。認証局と FPoS 機能間の電子証明書の有効性確認処理については、電子証明書失効リスト（CRL: Certificate Revocation List）を利用した確認方法を用いた。

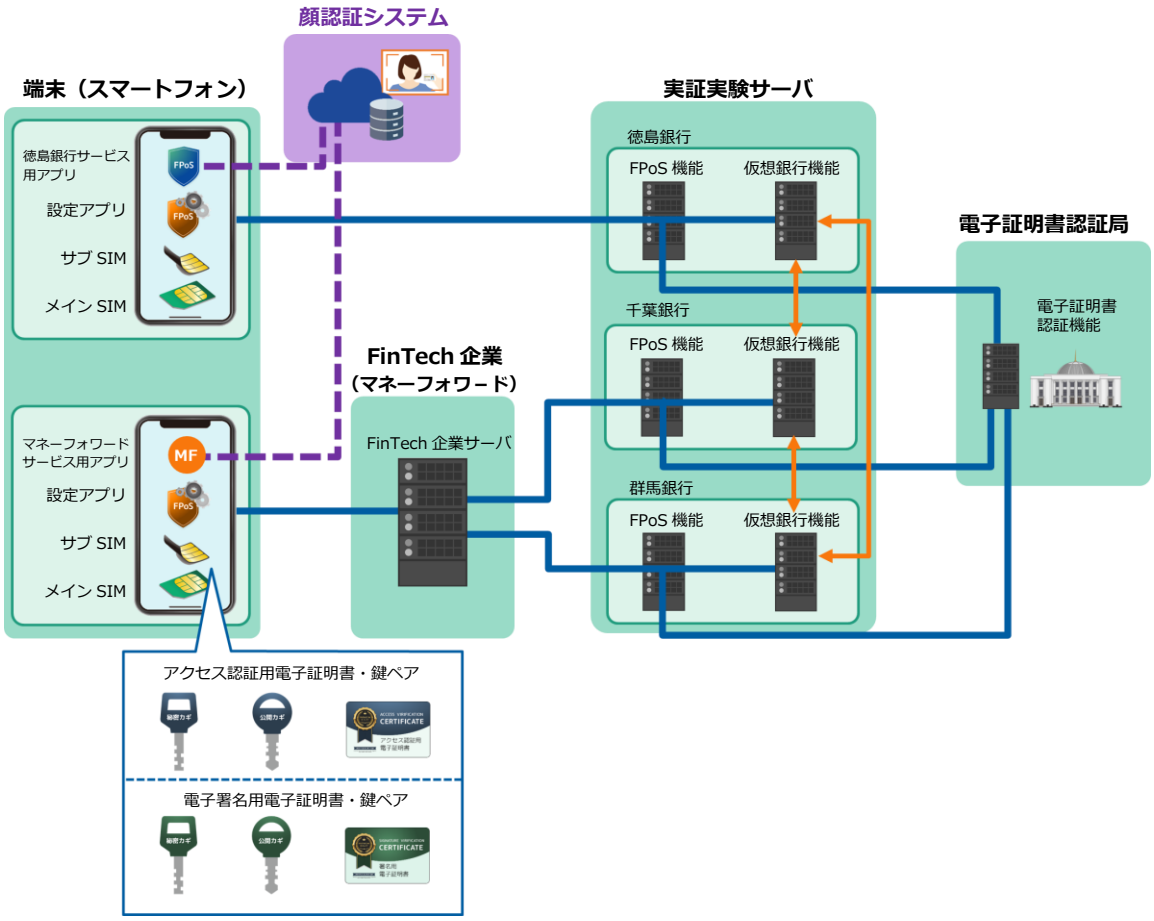

図 3.1　システム構成

3.3 実験方法等

実証実験の概要を表 3.1 に示す。

表 3.1 実証実験の概要

参加者	日本通信・千葉銀行・群馬銀行・徳島銀行の社員及び行員
実験端末	➢ 参加者自身が利用しているスマートフォン端末 (Android OS バージョン 5.0 以上の端末) ➢ メイン SIM（参加者が契約中の携帯電話会社の SIM カード） ➢ サブ SIM
実験内容	参加者の任意の時間帯に下記の実験を行った。 ➢ アクセス認証 ➢ 預金残高照会 ➢ 振込 ➢ 住所変更

参加者は日本通信の社員、千葉銀行、群馬銀行、徳島銀行の行員であり、参加者総数は 69 名であった。実験に利用する端末は利用者自身が所有している Android OS バージョン 5.0 以上を搭載したスマートフォン端末とし、参加者自身が契約している携帯電話会社の SIM カード上にサブ SIM を装着し、実験を行った（設定作業簡素化等のため、一部の参加者には試験用スマートフォン端末を貸し出した）。

実験の開始に際しては、参加企業毎に説明会を実施し、FPoS サービス申込窓口を開設して、重要事項説明や犯罪による収益の移転防止に関する法律に基づく本人確認手続きなどを模擬的に実施した。

実証実験を行う時間帯は任意の時間帯とし、参加者に預金残高照会、振込、住所変更の試験を依頼した。また、正常系の試験に加えて、振込または住所変更処理中の中断処理（取引処理中に意図的に機内モードにすることでエラーを発生させ、取引が正常に中断されるかを確認する実験）を行うこととした。

4. 実験結果

参加者には、参加申込み時に配布した実証実験結果記入表に試験日時、試験結果、試験失敗時の詳しい状況を記入するよう依頼した。同時に、実証実験サーバ及び端末アプリにおいても各種取引の履歴を保存し、実証実験サーバ上の履歴と参加者の申告する実証実験結果記入表に基づいて、実証実験結果の取りまとめを行った。

(1) 試験回数と成功率

各参加者の実証実験結果記入表の記載内容、実証実験サーバにおいて取得された履歴をもとに、マネーフォワードアプリ及び徳島銀行アプリでの取引試行回数、取引成功回数、不完了回数を算出した。表 3.2 にその結果を示す。なお、振込における口座番号誤入力など、利用者操作に起因するものは不完了取引として扱っていない。

表 3.2　マネーフォワードサービス用アプリ及び徳島銀行サービス用アプリによる試験結果

	試行回数	成功回数	不完了回数
アクセス認証	2,326	2,326	0
預金残高照会	12,327	12,324	3
振込	1,845	1,845	0
住所変更	851	848	3
合計	17,349	17,343	6

総試行回数 17,349 回のうち、17,343 回で取引が成功している。また、6 回の不完了試行は、取引処理中の電波状態等による通信エラーによるものであり、FPoS システム自体の動作に問題はなかった。

(2) 処理時間

各取引における処理時間を徳島銀行アプリ利用時において計測した。

処理時間は、アクセス認証に関して平均して 4.6 秒、振込に関して平均 8.3 秒、住所変更に関して平均 8.1 秒の処理時間であった。

(3) 利便性の評価

実証実験参加者に対して、5 段階評価（利便性が高い、利便性がやや高い、利便性は変わらない、利便性がやや低い、利便性が低い）でアンケートを実施した。結果の要点は以下のとおりであった。

- 現在オンラインバンキングまたは FinTech サービスを利用している参加者の 81%から、FPoS のログイン手続きについて利便性が高い、またはやや高いという評価を得た。
- 金融サービスを利用していない参加者の 45%から、FPoS のログイン手続きについて、利便性が高い、またはやや高いという回答を得た。同様に、46%の参加者が利便性は変わらないと回答したことから、全体として、金融サービスを使い慣れていない参加者も利便性の低下は感じていないという結果を得た。
- 現在オンラインバンキングまたは FinTech サービスを利用している参加者の 70%から、FPoS の振込手続きについて利便性が高い、またはやや高いという結果を得た。
- 金融サービスを利用していない参加者の 50%から、FPoS の振込手続きについて、利便性が高い、またはやや高いという回答を得た。同様に、参加者の 37%が利便性は変わらないと回答したことから、全体として、金融サービスを使い慣れていない参加者も利便性の低下は感じていないという結果が得られた。
- 一括住所変更機能については、現在オンラインバンキングまたは FinTech サービスを利用している参加者の 93%から利便性が高い、またはやや高いという評価を得た。

5. システムの高度化

本実証実験期間中に、実証実験とは別に以下の開発を並行して進め、FPoS システムに組み入れた。各機能が正常に動作することを確認した。

(1) 顔認証機能

生体認証の応用例として顔認証を取り上げ、利用申込時に顔写真を撮影してクラウド上の認証サーバへ登録し、アプリを利用する都度、顔認証を行う機能を実現した。

(2) iPhone への FPoS 機能搭載

図 2.6 の整理に従い、iPhone 内の Secure Enclave に FPoS 機能及び次項のランダムキーボード機能を搭載し、振込などを行った。

(3) ランダムキーボード機能

サブ SIM 内部でランダムに配列したキーボードを端末画面に直接表示することにより、端末が乗っ取られた際の盗聴の可能性を非常に小さくすることができる。この機能を実現した。

6. 考察

FPoS の仕組み、実証実験システムの設計・構築・運用過程、実験結果並びに参加者の意見を考慮して評価した結果を以下に述べる。

6.1 運用性

FPoS システムの運用性についての評価は以下のとおりである。

(1) システム構築及び運用

システム構築並びに運用に際して困難な点は存在せず、安定的な運用を図ることができた。これは、電子証明書関連技術やセキュアエレメントなどの FPoS 機能構成要素のそれぞれが既に確立された技術であり、特段の技術的困難性なくシステムを構築できた点にあると考えられる。

FPoS では、銀行システムの前段に FPoS 機能を配備し、証明書処理などの各種処理を銀行システムと独立に行う構成を採る。さらに、FPoS 機能と銀行システム間をオープン API を利用して接続する。この構成により、FPoS 導入の際の銀行システムへの影響を最小限に留めることが可能になる。また、FPoS サーバが銀行間のインターフェースや通信プロトコルの差異を吸収できるので、FinTech 企業やモバイルデバイスに対して発行する API の差異がなくなり（若しくは小さくなり）、統一されたインターフェース条件の下、FinTech 企業サーバや端末アプリを設計できるというメリットも生じる。

なお、実証実験においては銀行システムそれぞれに FPoS サーバを設置する構成を採用したが、FPoS サーバを一つにまとめて設置する形態を採ることも可能である。

(2) FPoS サービス申込窓口

本人確認やサブ SIM 貼付などを行う FPoS サービス申込窓口を、必ずしも金融機関の本支店に設置する必要はない。FPoS サービス運用会社が提携する他業種の企業（例えば家電量販店）等を主体として運用する形態もあり得る。

実証実験においては、参加者が自らメイン SIM を取り出し、サブ SIM を貼付してこれらをスマートフォンに再挿入すると共に、自らがアプリケーションソフトウェアのダウンロード等を行った。実験結果から、参加者やスマートフォン機種によってはこの操作に時間がかかることが判明したため、商用時には窓口の係員が治具等を利用してこれら作業を行うのが好ましい。

6.2 利便性

４章（3）で述べたように、参加者によるアンケートでは FPoS システムの利便性について総じて高い評価が示された。一般的にセキュリティレベルが上がると利便性が落ちる中、FPoS では両者が共に改善されることが分かる。これは、セキュリティを高めるための処理（暗号化など）に利用者が直接関わらないことに起因していると考えられる。また、モバイルデバイス利用の場合でもワンタイムパスワードトークンのような「利用者のみが保有している物」を個別に持ち歩かなくて良い点（SIM カードなどがスマートフォンに内蔵されている点）も高評価の一要素であると考えられる。

なお、これらの評価に当たっては、例えば参加者が FPoS サービス申込窓口を自らの足で訪れていない点や、現状の制度・銀行の基準に依っては融資口座や投資信託口座などで遠隔からの振込・住所変更サービスの提供ができない場合がある点までは考慮されていない可能性もある。利便性評価に当たっては、実運用に向けてさらなる考察が必要である。

また、４章（2）で述べたとおり、振込などの処理時間については平均 8.1 秒乃至 8.3 秒の時間を要した。この時間について、若干名の参加者から長すぎるとの指摘があった。一方で、例えば、現行のワンタイムパスワードを使う方式では、ワンタイムパスワードトークンが手元にあったとしても、通常、一連の作業に 10 秒以上の時間がかかるものと思われる。従って、現行のワンタイムパスワード方式の所要時間と比較すれば、FPoS 処理時間が長いとは言えない、とも考えられる。いずれの場合にも、証明書取得及び署名処理についてはサブ SIM へのアクセス方法の最適化により一定の改善が可能であることがわかってきたため、継続して検討を行う予定である。

6.3 セキュリティ性

前章までで述べたとおり、実証実験を通して、FPoS のセキュリティ原理を困難なく実装できることが確認できた。セキュリティに関連して確認できた具体的な項目は以下のとおりである。

- 利用者端末の紐付けにより、登録した組合せ以外の端末及び SIM カード類によるアクセスを防止できること。
- 「利用者のみが知っている知識」及び「利用者のみが保有している物」による本人性の確認によりサブ SIM にアクセスして FPoS を起動させること。

- 「利用者が生まれつき備えているもの」の例として顔認証技術を併用した場合でも FPoS が正常に動作すること。
- 電子証明書技術を用いてアクセス認証時の本人性確認機能が正常に動作すること。
- 同様に、電子署名の仕組みを利用して送信情報改ざんを検知できること。
- サブ SIM に電子証明書、暗号鍵、暗号演算機能等を実装し、スマートフォンに内蔵した状態で暗号化演算ができること。
- OAuth2.0 による認可機能が正常に動作すること。
- サーバ装置実装に伴い、多層防御機能が併用実装できること。
- 設計した API の下、FPoS サーバと仮想銀行機能サーバが通信を行い、依頼された取引の処理ができること。
- 同様に、設計した API の下、FinTech 企業サーバと FPoS サーバが通信を行い、認証及び署名処理が正常に行われること。
- FPoS による電子証明書の有効性確認が電子証明書認証局と連携して正常に実施できること。
- サブ SIM 内部で生成したランダムキーボードをスマートフォンの画面に表示し、文字入力を正常に行えること。

今後は、これらの検討結果をもとに、さらに端末盗難時の対応など本実証実験では検証しなかった付随的な項目についても検討を進める必要がある。

7. 制度面に関する検討

(1) 金融庁の監督指針

FPoS を商用導入する場合、その適格性の評価や運用方法は、金融庁の「主要行向けの総合的な監督指針」並びに「中小・地域金融機関向けの総合的な監督指針」の規定に従う必要がある。

FPoS は、SIM などの Hardware Security Module や電子証明書を積極的に採用したプラットフォームであるが、その技術的な特質に起因して、現行の監督指針に準拠できない、若しくは現行の監督指針の変更を必要とする事項は存在しない。むしろ、FPoS は、監督指針に記載されている要請を忠実に実現したプラットフォームであると考えられる。例えば主要行向けの総合的な監督指針Ⅲ-3-7 のシステムリスク及び Ⅲ-3-8 のインターネットバンキングには、コンピュータシステムやインターネットバンキングに関するセキュリティ確保について各種の要件が技術的な観点からも記載され、その一例として、監督指針Ⅲ-3-8-2-(2)セキュリティの確保において「犯罪手口の高度化・巧妙化等（「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」など）を考慮しているか」という記載がある。電子証明書技術に基づく本人認証や電子署名機能を具備した FPoS は、この要件を満たすものと考えられる。

このような技術的側面に加えて、FPoS サービス商用化に際しては、システムリスク、情報セキュリティ、サイバーセキュリティの管理態勢に関する要件を整備し充足する必要があるが、これら要件は、基本的に金融機関等が現在運用しているサービスやコンピュータシステムに対する対策と同一または類似の対策を必要とする要件であり、商用時までに要求される基準を満たす体制を整えることは可能であると考えられる。

また、FPoS は利用者の利便性を確保しつつ、より強固な金融取引のセキュリティ性を提供するプラットフォームであるから、上述のⅢ-3-7 及びⅢ-3-8 以外の指針についても、それらの適合性を高めることはあれ、毀損させるとは考えにくい。

(2) 金融情報システムセンター（FISC）の指針

FISC は、FPoS に関連して二つの指針を発行している。一つは「金融機関コンピュータシステムの安全対策基準・解説書（2018 年 3 月、第 9 版）」であり、もう一つは「金融機関と API 接続先のための API 接続チェックリスト解説書（2018 年度 10 月版）」である。

前者については、幾つかの項目は商用開始時までに運用ルールの策定等を必要とするが、技術的な課題については、実証実験自体若しくは実証実験中に行った付随的な開発において実証された事項であり、その他の一般的な課題も含めて、今後の一定の準備により、この安全対策基準の要件を充足できると考えられる。

後者についても上述の安全対策基準と同様で、確認済の技術的要件の下、管理運用ルールの制定整備及びそれに従った運用準備を行うことにより、商用開始時期までにすべての要件を充足することは十分可能であると考えられる。

8. おわりに

金融庁の FinTech 実証実験ハブを活用した FPoS（FinTech Platform over SIM）にかかる実証実験を日本通信株式会社、株式会社群馬銀行、株式会社千葉銀行、株式会社徳島銀行、株式会社マネーフォワード及びサイバートラスト株式会社の 6 社で行い、携帯端末を利用した銀行振込みや住所変更などのサービスを安全かつ利便性高く実現できることを確認した。

FPoS の事業化に向けては、実証実験で取り上げた利便性やセキュリティに関する課題、運用性についての課題などの更なる検討に加えて、以下の検討が必要になる。

・顧客ニーズの調査
・各事業者で発生するコスト及び費用対効果の検討
・銀行サービス全体としてのセキュリティ評価（他のセキュリティ対策との複合的な評価）
・事業モデルの確立及びその詳細化
・事業会社の設立
・必要な資格の取得（電子署名法に基づく電子証明書認証業務の認定取得など）
・事業開始のための各種準備（所要設備等の調達、運用ルールの制定など）

これらの課題を解決し、FPoS 運用の仕組みを整えると、銀行向けサービス以外にも FPoS の適用範囲が広がる。

例えば、信用金庫やネット証券企業、電子商取引企業（ネット通販サービスやフリーマーケットアプリサービス等）においても不正利用や中間者攻撃の被害は存在するため、FPoS により、これらの被害を最小化することが可能になる。また、仮想通貨分野においては、安全な仮想通貨の保管方法としてコールドウォレットがあるが、通常、スマートフォンや PC とは別のハードウェア媒体での保管が必要なため、利用者の利便性は高くない。サブ SIM をコールドウォレットとし、FPoS で本人認証を行うことで、セキュリティ性を保ったまま、利用者の利便性を向上させることができる。

FPoS サービスの適用分野が何であれ、FPoS の実用化に際しては、まず FPoS サービスを提供する企業の誕生が必要である。この FPoS 運用会社は、上述の各課題への取り組みの一環として、サービス利用者である金融機関を顧客にすべく活動を展開することになる。その過程において、本実証実験の成果は有用であると共に、実証実験を通して明らかになった個別課題の検討も進むものと思われる。参加 6 社は、これらの検討が継続して行われ、FPoS サービスの早期実用化が図られることを期待する。

—