2024 年６月７日
日本銀行決済機構局

ＣＢＤＣフォーラム ＷＧ３
「ＫＹＣとユーザー認証・認可」
第７回会合の議事概要

１．開催要領

（日時）2024 年４月 16 日（火）14 時 00 分～16 時 00 分
（形式）対面形式およびＷｅｂ会議形式
（参加者）別紙のとおり

２．プレゼンテーション

ＮＲＩセキュアテクノロジーズ株式会社、株式会社マネーフォワードよりプレゼンテーションが行われた。概要は以下のとおり。

（１）認証・認可の現状および最新動向の整理①（ＮＲＩセキュアテクノロジーズ株式会社）

―― プレゼンテーション資料の要旨は別添１を参照。

ＡＰＩを用いたＣＢＤＣのシステム間連携の整理と海外事例を紹介し、続いて認可によるＡＰＩの保護、認可・ＡＰＩセキュリティの最新動向、責任分界について言及を行い、最後にＣＢＤＣの認可に関する示唆を述べる。

日本銀行のパイロット実験では、家計簿サービス等のＣＢＤＣの利便性を向上させる追加サービスの提供事業者や仲介機関、中央システムといった各関係者のシステムが連携して、ＣＢＤＣに関連するサービスを提供するユースケース（ＣＢＤＣの発行・環収や払出・受入等）を踏まえた検討がされていると理解している。また、ＢＯＥ（Ｂａｎｋ ｏｆ Ｅｎｇｌａｎｄ／イングランド銀行）のＣＢＤＣへの考察文書（Ｔｈｅ ｄｉｇｉｔａｌ ｐｏｕｎｄ： Ｔｅｃｈｎｏｌｏｇｙ Ｗｏｒｋｉｎｇ Ｐａｐｅｒ）では、仲介機関と中央システム間の連携においてＡＰＩの利用が検討されたほか、ＢＩＳ（Ｂａｎｋ ｆｏｒ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｓｅｔｔｌｅｍｅｎｔｓ／国際決済銀行）の「Ｐｒｏｊｅｃｔ Ｒｏｓａｌｉｎｄ」というＣＢＤＣの実証実験においては、ＡＰＩが用いられた。このような海外事例は、日本におい

ても参考になると考えている。

ＡＰＩを活用すると、ユーザーから権限移譲を受けた事業者がユーザーの残高情報等のリソースへアクセスが可能となる。ＡＰＩを適切に保護する認可の標準技術としてＯＡｕｔｈ２．０があり、ＣＢＤＣにおいてもこのような技術を用いてＡＰＩを保護することは重要であろう。

ＯｐｅｎＩＤ　Ｆｏｕｎｄａｔｉｏｎ（以下、ＯＩＤＦ）が策定したＦＡＰＩ（Ｆｉｎａｎｃｉａｌ－Ｇｒａｄｅ　ＡＰＩ）という高いセキュリティ水準が求められるＡＰＩ向けの技術仕様があり、ＦＡＰＩへ準拠することで、なりすましやデータ改竄、認可コード・アクセストークンの漏洩等への技術的観点からの対策が可能となる。また、ＢＩＳの「Ｐｒｏｊｅｃｔ　Ｒｏｓａｌｉｎｄ」では全てのＡＰＩがＦＡＰＩに準拠するようにと言及があるほか、ＢＯＥのＣＢＤＣへの考察文書ではＦＡＰＩによって最高標準のセキュリティ管理が可能になると言及されている。

イギリスやブラジル、オーストラリア等、各国の金融機関でＦＡＰＩが採用されている事例があるが、技術面における要求事項を満たしても、当該ＡＰＩの利用が進まないケースもある。一例として、ＦＡＰＩに準拠した英国の中小企業の給与支払いにおいて、実際にはＡＰＩが使われていない理由を紹介すると、責任分界の整理においてＡＰＩの呼び出し元が大きな責任を負うとされていることや、更新系ＡＰＩへのアクセスコストが挙げられている。

以上を踏まえ、ＣＢＤＣの認可に関する示唆を挙げる。まず、ＣＢＤＣにおいて、様々な追加サービス提供事業者に参加してもらうにあたり、付加価値を提供しやすい仕組みが重要であり、そのためにはＡＰＩと認可の実装が必要になると考える。

次に、ＣＢＤＣという重要度が高い金融資産に対しては高いセキュリティが要求されるため、ＦＡＰＩへの準拠は検討すべき事項と考える。最後に、ＡＰＩ利用における責任分界の整理は、各関係者が連携してサービスを提供するためには重要な観点であり、ＣＢＤＣにおいても、各関係者に起因して発生しうるインシデントを検討し、どのように責任分界を整理すべきか検討が必要であると考える。

参考として、欧州決済サービス指令第２版（ＰＳＤ２）では、利用者保護のため、ユーザーに求める責任は限定的な金額にするべきとされており、ユーザーに詐欺または重過失がある場合を除き、ユーザーに請求する損害の上限額

は５０ユーロが適切であると言及されている。また、米国のＯＩＸ（Ｏｐｅｎ　Ｉｄｅｎｔｉｔｙ　Ｅｘｃｈａｎｇｅ）では、損害を発生させた当事者が、枠組みのルールに全て従っていたことが証明できれば、その当事者に責任が発生しない、過失ベースの考え方がされている。

（２）認証・認可の現状および最新動向の整理②（株式会社マネーフォワード）

――　プレゼンテーション資料の要旨は別添２を参照。

当社は電子決済等代行業者（以下、電代業者）であり、家計簿サービスや会計サービスを提供している。これらのサービスを提供する上で銀行とＡＰＩ連携を行い、ユーザーの預金口座情報の取得などを行っており、ＡＰＩ連携がＵＸ（ユーザーエクスペリエンス）に対して重要な役割を担うと考えている。ＣＢＤＣにおいては、電代業者は追加サービス提供者の位置づけにあり、こうした視点からＡＰＩ連携によるＵＸ向上に向けた課題について説明を行う。

まずは現状のオープンバンキングの基本的枠組について説明する。オープンバンキングとは、銀行の預金口座の取引情報などの顧客データなどをＡＰＩ経由で、電代業者等の第三者の企業と連携することにより、新たなサービスを生み出す試みのことである。電代業者と銀行間の関係は、電代業者がユーザーからＩＤとパスワードを預かって、ユーザーに代わってインターネットバンキングにログインし、画面上の口座残高等の情報を抽出するスクレイピングから、オープンバンキングの進展によりＡＰＩを介した連携へ変遷している。現在では、参照系ＡＰＩは普及している一方で、更新系ＡＰＩはほとんど普及していないのが実情のため、更新系ＡＰＩの普及にかかる課題について説明をする。

更新系ＡＰＩを活用した振込時は、現在、銀行から提供されているＡＰＩでは電代業者のサービスから直接振込指示を出すことはできず、ユーザーは電代業者のサービスへログインするために認証をし、振込予約の認証を行った後に、銀行のインターネットバンキングへログインし直すために認証を行い、振込実行の認証をする必要がある。このように、更新系ＡＰＩの利用には認証の回数が多いなどＵＸ向上の課題があり、ＣＢＤＣにおいても追加サービス提供者と仲介機関の連携がＡＰＩ経由で行われるのであれば同様の課題が出ると想定される。

ＣＢＤＣの導入は、これまでの前提条件をゼロベースから再検討できる良

い機会と捉えており、課題への対応案として①認証の一部省略・簡略化、②一連のＵＸ上での認証回数の制限、③一連のＵＸ上での追加サービス提供者と仲介機関間の情報連携、④追加サービス提供者と仲介機関間での責任分界の考え方の整理、の４点について海外事例を踏まえながら説明する。

①認証の一部省略・簡略化は、ユースケースと不正率の２点から説明する。まず、ユースケースについては、リスクの低いユースケースであれば認証を省略する余地はあると考えており、例えば、自身の口座間の資金移動、税公金収納、公益企業への支払などが挙げられる。英国の事例では、電代業者に相当するＰＩＳＰ（Ｐａｙｍｅｎｔ Ｉｎｉｔｉａｔｉｏｎ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ）と銀行に相当するＡＳＰＳＰ（Ａｃｃｏｕｎｔ Ｓｅｒｖｉｃｉｎｇ Ｐａｙｍｅｎｔ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ）がＡＰＩ連携で行う決済のうち、同一名義人間の資金移動は銀行を跨ぐ送金であっても送金元の銀行で当初１回の認証を行えば、その後は当該銀行での認証を不要とし、ＰＩＳＰの認証のみで定期的に送金することが許容されている。さらに、公的機関等への支払についても同様に省略化が検討されている。このほか、欧州の事例では決済履行時にＳＣＡ（Ｓｔｒｏｎｇ Ｃｕｓｔｏｍｅｒ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）と呼ばれる多要素認証が義務化されているが、交通運賃の支払やパーキングメーターの支払など、リスクが低いと考えられる一部のユースケースについては、必ずしもＳＣＡを適用しなくてもよいとされている。

次に、不正率については、欧州の事例ではリアルタイムで取引の監視を行う条件のもと、義務化されているＳＣＡを不要とできる不正率の基準値を定めている。例えば、オンライン取引におけるクレジットカードやデビットカード決済では 500 ユーロを超えない取引額の範囲において 0.01%同等または以下の不正発生率であれば、ＳＣＡを不要とすることができる。同様に銀行送金においては、500 ユーロを超えない取引額の範囲において 0.005%同等または以下の不正発生率であればＳＣＡを不要とすることができる。

②一連のＵＸ上での認証回数の制限については、欧州の事例では、ＰＩＳＰを介した決済の認証時には、ＰＩＳＰから必要な情報連携を受けたＡＳＰＳＰによる一度の多要素認証で決済を開始するように義務付けし、全体として一定のセキュリティ強度を担保しつつ、認証回数を抑えることを検討している。日本でもこのような考え方は参考になるだろう。

③一連のＵＸ上での追加サービス提供者と仲介機関間の情報連携について、英国では、ユースケースごとにＰＩＳＰと銀行間の情報連携を法令および公的機関であるＯＢＬ（Ｏｐｅｎ Ｂａｎｋｉｎｇ Ｌｉｍｉｔｅｄ）によるガイドラインで規定しており、参考になるだろう。このガイドラインでは、Ｐ

ＩＳＰが提供する決済サービスの支払プロセスにおいて、ＰＩＳＰと銀行の法令による義務範囲、ガイドラインによる要請範囲が詳細に定められている。例えば、ＰＩＳＰの画面から銀行の画面に遷移する際にＰＩＳＰはユーザーに対して銀行の画面に遷移する旨の通知を行わなければならない、などが挙げられる。このようなガイドライン整備は、役割が明確になるため事業者間の連携がスムーズになり、ＵＸも改善されることが期待されるため有効な取り組みであると考える。

④追加サービス提供者と仲介機関間の責任分界について、欧州では、ＥＰＣ（Ｅｕｒｏｐｅａｎ　Ｐａｙｍｅｎｔｓ　Ｃｏｕｎｃｉｌ）と呼ばれる自主規制機関によって一つの参考になる考え方が示されている。法令ではないため強制力があるものではないが、電代業者が自らのモニタリング結果に基づいて取引のリスク判断を行い、それによってパターンが３つに分けられる。低リスクと判断する取引はＳＣＡの非適用を銀行に要請し、不正利用時に電代業者が責任を負担する。高リスクと判断する取引はＳＣＡの適用を銀行に要請し、不正利用時に銀行が責任を負担する。電代業者が判断に迷う場合は、銀行側でＳＣＡの要否を判断し、不正利用時には銀行が責任を負担すると定めている。このように責任を分担する考え方も存在している。

以上を踏まえて、ＣＢＤＣにおける検討課題を挙げる。①認証の一部省略・簡略化に関しては、ＣＢＤＣにおいても同一名義人間の資金移動や税公金収納、公益企業への支払といった低リスクのユースケースの場合や、取引をリアルタイムで監視しつつ不正率が一定の基準を下回る場合には、認証の省略・簡略化が検討できるのではないだろうか。また、不正率などのデータは、複数の民間事業者が横断的に取りまとめるよりも、公的・中立的な機関によって蓄積される方が望ましい可能性もあると考えている。②一連のＵＸ上での認証回数の制限に関しては、ＣＢＤＣにおいても全体として一定のセキュリティ強度が担保できるのであれば、追加サービス提供者と仲介機関間の連携時に求められる認証の回数を抑える方法が検討できるのではないだろうか。あわせて、仲介機関システムや中央システムそれぞれの認可内容や認可範囲についても議論する必要があるだろうと考えている。③一連のＵＸ上での追加サービス提供者と仲介機関間の情報連携および④追加サービス提供者と仲介機関間の責任分界に関しては、ＣＢＤＣにおいても情報連携のガイドラインや責任分界の考え方について整備が必要であり、海外では公的、中立的な機関が整備している事例もあることから、日本でも同様に検討することが考えられるのではないだろうか。

３．ディスカッション

プレゼンテーションに引き続き、参加者によるディスカッションが行われた。モデレータは、ソニー株式会社が担当した。概要は以下のとおり。

【ＦＡＰＩの準拠】

（参加者）ＦＡＰＩに準拠しているかを、どのような機関がどのような方法で判断しているか。

（参加者）複数のテストケースを一括りにしたテストスイートをＯＩＤＦが提供しており、それを用いて自ら準拠できているかを検証し、そのテスト結果をＯＩＤＦに申請し、認められればＦＡＰＩ準拠の認定が取得できる。ＯＩＤＦのウェブサイト上では、ＦＡＰＩ準拠の認定を得た組織等の一覧があり、確認が可能である。

（参加者）ＦＡＰＩ準拠はユーザーと銀行などの間では重要だと思うが、本ＷＧにおいて、なぜＡＰＩの活用やＦＡＰＩの準拠を議論する必要があるのか、意図を確認したい。

（日本銀行）ご紹介のあった海外のＣＢＤＣの検討事例では、関係者間をつなぐ認可の仕組みとしてＡＰＩに言及し、その中でもＦＡＰＩの準拠について示唆があったと認識している。日本では、既に銀行サービスをＡＰＩによって繋ぎ、様々なサービスが提供されているが、さらにＣＢＤＣという要素が加わった場合、認可の仕組みがどのように変わりうるのかという観点で、海外事例も参照しながら議論をいただければと考えている。

（参加者）ＦＡＰＩの準拠の必要性は、ＣＢＤＣに限った話ではないと認識している。あくまでも安心安全な仕組みを構築し、関係者を守るための認可の仕組みの一つとして、ＣＢＤＣにおいてもＦＡＰＩの準拠が検討・推奨されたと理解している。

【ＡＰＩ仕様の共通化の度合い】

（参加者）ＣＢＤＣにおいて仲介機関が提供するＡＰＩの仕様は、共通化するのか、それとも独自性を持つのか、ＣＢＤＣフォーラムの他のワーキンググループで議論されていたら教えてほしい。

（参加者）ＷＧ２（追加サービスとＣＢＤＣエコシステム）で、ＡＰＩの仕様がどの程度共通化されるべきかについて議論になったが、結論は出ていないと認識している。また、程度の考え方も、様々な観点がありうる。例えば、詳細なシステム仕様も含めて同じように動くという観点や、セキュリティやプライバシーに関する考え方や要求が同じという観点などがあげられ、その程度は様々にありうると認識している。これまで各金融機関がＡＰＩの提供を進めた中では、連携するサービスを作る側は、各金融機関のＡＰＩの仕様の差異に対応するのが大変だったという話がある一方で、そうした個別の対応をした結果、独自性のあるサービスが打ち出せたといった良い面もあるとの意見があった。ＷＧ２では、このように様々な議論がされていると認識している。

（日本銀行）同様の認識である。ＡＰＩの仕様の共通化により外部連携が容易になり、結果的にサービスの質も高まるというメリットを強調する意見が多いが、その程度については様々な考えがあると認識している。

【ＦＡＰＩとＡＰＩ設計の拡張性】

（参加者）ＦＡＰＩの準拠は、高いセキュリティを実現できると理解したが、ＦＡＰＩの準拠によって、追加サービスは画一的になりがちとなるのか、それとも特に影響はなくニュートラルなのだろうか。各国の議論も含め、意見や見解があれば伺いたい。

（参加者）ＦＡＰＩの準拠が、追加サービスに与える影響は、ニュートラルと考えている。ＦＡＰＩは、ＡＰＩで接続される関係者同士が、お互いを守るためのセキュリティの基礎となるものであり、これにより追加サービスの柔軟性が損なわれることはないと考えている。実際に、ＦＡＰＩの準拠について言及しているＰｒｏｊｅｃｔ　Ｒｏｓａｌｉｎｄの実証実験の示唆として、シンプルで基本的なＡＰＩの機能群は、様々なユースケースに対応可能と言及されている。ただし、ＡＰＩ設計における拡張性の高さとエンドユーザーのＵＸの一貫性はトレードオフの関係にあるとも述べられている。例えば、送金のプロセスにおいて、各仲介機関が提供するＡＰＩ設計の拡張性が高ければ、追加サービス毎に全く異なる送金のプロセスとなる可能性があり、結果としてエンドユーザーのＵＸは一貫しない可能性を示している。ＦＡＰＩの準拠とＡＰＩ設計の拡張性の高低が追加サービスに与える影響は、また別の論点と考えている。

【責任分界と仕様の共通化】

（参加者）英国の事例であげられたＡＰＩのリクエスト元が大きな責任を負うという責任分界の整理に関して、詳しく伺いたい。

（参加者）ＡＰＩを通じて権限を委譲した後、委譲先のサービスでシステム上のトラブルやサイバー攻撃により事故が発生した場合には、原因となったＡＰＩのリクエスト元として大きな責任を負うという責任分界の整理の一例の紹介である。責任分界に関しては、技術的な観点というよりもむしろ社会的な観点によって形作られていくと考えており、まさに論点のひとつと考えている。

（参加者）金融犯罪対策を重視する立場からは、これまで議論のあったＡＰＩの接続方式等は単にシステム間をどのようにセキュアに繋げるかに過ぎず、むしろＫＹＣや認証・認可、その中でもとりわけ当人認証が重要と考えている。その上で、最終的には責任分界をどのように設定するかが肝要となるだろう。

銀行と更新系ＡＰＩのリクエスト元の関係性を、既存の仕組みに当てはめると、ユーザーと予め取り決めを行い、ユーザーが指定した第三者からの要求によってユーザーの口座から引落しを行う点が、口座振替の仕組みと類似していると感じる。現状の口座振替においては、ユーザーが指定した収納企業の指示に基づく口座振替の引落しが不正だったと判明した場合、基本的には収納企業が責任を負う。ただし、ユーザーから見れば銀行が管理している口座から本人の意思に関わらず残高が減ったと見えることから、苦情等の窓口となってしまう傾向にある。

こうした現状を踏まえて、仮に更新系ＡＰＩにおいてユーザーに何らかの不正被害が発生した場合を想定すると、口座振替と同様に更新系ＡＰＩのリクエスト元が大きな責任を負うのも当然であろう。ただし銀行も口座を管理する当事者として、更新系ＡＰＩ接続を許容してよいのかを慎重に判断する必要がある。この点、銀行は更新系ＡＰＩのリクエスト元が行う当人認証の強度やセキュリティ対策が適切なものであるかを把握することが困難かつコントロールもできないことを考えると、リスクが増える銀行にとって更新系ＡＰＩを許容するインセンティブはあるのだろうか。

さらにＣＢＤＣでの導入を想像すると、そもそもの前提の一つとして、一部の大手やネット系の金融機関等にユーザーが集中し、規模の小さい金融機関等は、ユーザーが少ない可能性がある。そうした中で、全ての仲介機関に対して、高い水準での共通化を推し進めると、特に規模の小さい金

融機関にとっては対応負担が大きく、そもそも仲介機関になることのインセンティブが不明瞭であることも相まって、仲介機関としては参加をしないと判断する可能性がでてくるだろう。

ＣＢＤＣの普及においては、ユーザーに利便性や高いＵＸを提供することは重要であるものの、仲介機関側に生じる負担も考慮していく必要がある。

（参加者）ブラジルなどの海外の一部の国においてＦＡＰＩの準拠が進んだ理由は、国としてＦＡＰＩの準拠を義務化したからと考えている。

日本においては、銀行法の改正に伴い、銀行のオープンＡＰＩの実装が努力義務となり、多くの銀行が対応したものの、クオリティの高いＡＰＩを実装している銀行は少ないと認識している。ＦＡＰＩに準拠している銀行は数行にとどまるため、異なる仕様のＡＰＩが増えただけに映る。電代業者が提供するサービスと連携する容易さの観点からは、同じ仕様のＡＰＩが幅広く実装されることが重要である。

なお、仕様の共通化は、海外事例等も踏まえると、国として強制力をもって主導することが成功のモデルと考えるものの、その裏付けに大義名分がなければ、あまり上手くいくことはないだろう。

（参加者）仮に、ＣＢＤＣにおいて仕様の共通化を強制したとしても、そもそも各金融機関が仲介機関としての役割を担うか否かを独自に判断するのであれば、どのような基準で判断をするのだろうか。そうした観点では、ＣＢＤＣが参入したい魅力的なサービスであることや、仲介機関になることによって何らかのインセンティブが得られる設計であることが重要であり、こうした検討が必要と考える。

【認証と責任分界】

（参加者）プレゼンテーションで紹介された「欧州の自主規制機関による責任分界の考え方」の事例（別添２．14 頁）では、電代業者相当と銀行相当の間の責任分界について、電代業者相当の判断に基づき銀行相当に認証を要請した場合、当該認証における責任は銀行相当が負うということを示しているか。

（参加者）ご理解の通り。このように整理されているのであれば、資金移動を含む更新系ＡＰＩを活用した追加サービスを検討し易くなるだろう。

（参加者）金融犯罪対策の観点では、各銀行は自らがセキュリティをコントロールできる範囲にサービスを限定して、その範囲内で責任を取ると考えているのではないか。資金移動を含む更新系ＡＰＩに関しては、仮に組み込まれた先の電代業者のサービスのセキュリティが突破されたことを起因とする犯罪被害が発生した場合には、電代業者の責任はさることながら、当該口座を管理している銀行として対応を取る必要がある。銀行としては、電代業者のサービスのセキュリティに関して直接的にコントロールする立場ではないため、インシデント発生時の対応負担等も考えれば更新系ＡＰＩの提供には慎重になるだろう。なお、税金や公共料金などの口座振替のように支払い先が限定されるのであれば、リスクが低いと考えられ、銀行としては更新系ＡＰＩを提供しやすくなるかもしれない。このように、ユーザーの属性ではなく、更新系ＡＰＩで行う取引そのもののリスクの高低に着目することは留意すべき点と考える。

【口座振替の将来性】

（参加者）銀行が提供する口座振替は３０年後にどうなっているだろうか。

（参加者）管理負担の軽減という観点からはクレジットカードでの支払いといった方法もあるが、口座振替での支払いは、今後も必要とされるのではないだろうか。口座振替は既に社会インフラとなっているほか、口座振替は指定された銀行の口座が必要であることから、当該銀行にとってはそれをきっかけに口座開設をしていただく新たな顧客との接点という営業的側面もある。口座振替契約を行っている収納企業が悪意者に乗っ取られた場合などのリスクを考えれば、口座振替の仕組みが悪用される可能性も考えられるものの、収納企業は銀行の法人営業担当等によって審査を行い管理されているケースが多いので、そうしたリスクは高くないだろう。

（参加者）詳しく説明できていないが、本日のプレゼンテーションにあったＶＲＰ（Ｖａｒｉａｂｌｅ　Ｒｅｃｕｒｒｉｎｇ　Ｐａｙｍｅｎｔ／変額定期支払）は口座振替をデジタル化したものに近いと認識している。海外ではユースケースや、認証を含めたＵＸをどうするかについて議論がなされている。将来的には日本でも同様の議論になるかもしれないと考えている。

【ＣＢＤＣにおける新たなアイデアの検討】

（参加者）プレゼンテーションにあったように、ＣＢＤＣではこれまでの前提条

件をゼロベースから再検討ができる機会と考えられるので、例えば、そのエコシステムへの参加者に対して、定期的にデューデリジェンスを行う厳格な仕組みや、参加者全体で保険をかけて被害発生時の補償を分担する仕組み等のアイデアも考えられるのではないだろうか。

（日本銀行）新たなアイデアについては現時点で特にお答えがあるわけではないが、仮にＣＢＤＣを導入していくとなれば、その実現すべき目的に沿って、様々なアイデアを新しく検討できる機会となるであろうと考える。

【欧州の事例について】

（参加者）欧州の事例として、不正率やユースケースによる認証の緩和など、興味深い事例があったが、ＳＣＡとこれまでの会合で議論に出てきたＮＩＳＴ等のガイドラインにおける当人認証保証レベル２は同じ考え方か。

（参加者）多要素認証を求める点など共通する部分はあるが、直接的にリンクしているものではないと認識している。

（参加者）欧州では、このような決済における認証関連の法令、ガイドライン等はどのような時間軸で見直しがされるものか。

（参加者）数年をかけて更新していく法令や、細部であれば細かく改定されるものもある。頻繁に更新されると対応する事業者の負担が大きいため、基本的には必要に応じて徐々に変えているイメージである。

（参加者）欧州での事例では、多要素認証を必ずしも適用しなくても良い例外的ユースケースがあるとあったが、その場合においても最低限の認証の基準は定められているのか。

（参加者）送金や決済では基本的にＳＣＡの適用が求められるが、例外的なユースケースの場合には必ずしもＳＣＡを適用しなくても良いと認識している。

（参加者）ＳＣＡを基準として、例外的なユースケースにおいては省略・簡略化も可能である一方、ＳＣＡより強い認証を求めることも可能と理解した。

【ＡＰＩにかかるコスト負担と仕様統一】

（参加者）銀行がシステム対応を行う際には、大きなコストがかかる。特に、規

模の大きくない銀行では、単体で対応することが困難なケースがある。このようなケースでは銀行同士で連携をして、同じシステム基盤を使い、共同利用をすることでコストを抑えることが非常に多い。ＡＰＩにおいて、仮にＦＡＰＩを導入するとなると、高額のコストがかかることが考えられ、加えて銀行として必要なセキュリティ対応を行うと、さらにコストがかかることが予想される。このような際に、統一した仕様の定めがないと、どのような仕様とすべきか等について開発を担うベンダー側の意向が働きやすくなる可能性もある。コスト負担削減、検討負担削減の観点から仕様を統一いただきたいと考えている。

（参加者）米国におけるＡＰＩ仕様統一についての議論を紹介すると、銀行の資産規模に応じて、対応期限の段階を分けて導入していく案が提示されている。同様の段階的導入事例は豪州でもあり、実際に仕様を統一する際の政策対応として参考になるかもしれない。

４．次回予定

次回の会合は５月 24 日（金）に開催予定。

以　上

別紙

ＣＢＤＣフォーラム ＷＧ３
「ＫＹＣとユーザー認証・認可」
第７回会合参加者

（参加者）※五十音・アルファベット順
株式会社イオン銀行
セコム株式会社
ソニー株式会社
大日本印刷株式会社
株式会社千葉銀行
日本電気株式会社
日本マイクロソフト株式会社
日立チャネルソリューションズ株式会社
フェリカネットワークス株式会社
株式会社ふくおかフィナンシャルグループ
株式会社マネーフォワード
株式会社みずほ銀行
株式会社三井住友銀行
株式会社三菱ＵＦＪ銀行
株式会社ゆうちょ銀行
株式会社りそなホールディングス
ＮＲＩセキュアテクノロジーズ株式会社
株式会社ＮＴＴドコモ
ＰａｙＰａｙ株式会社

（事務局）
日本銀行

CBDCフォーラム WG3　第7回会合　APIセキュリティ・認可における動向

エグゼクティブサマリ

CBDCにおけるAPIの利用	• CBDCでは追加サービス提供事業者・仲介機関・中央システムが連携してサービスを提供する。 • システム間の連携方法については、イングランド銀行の考察文書やProject Rosalindによる検証ではAPIが利用されている。
API セキュリティ・認可における動向	• イングランド銀行の考察文書では、利用者のプライバシー保護の必要性にも言及しておりOAuth 2.0のような標準技術を用いた認可の実施が重要である。 • 高い水準のセキュリティが求められる重要度が高いAPI向けの仕様としてFinancial-Grade API (FAPI)という規格が存在し、他国のCBDCに関する検討でもAPIのセキュリティとして言及されており、日本におけるCBDCにおいても検討することは必要と考える。
認可における考慮事項	• 各事業者が連携してサービスを提供する際には、責任分界の整理が必要となる。 • APIを用いたシステム連携は、疎結合性を高める点で責任分界の議論に有益と思料。 • また事業者において高い水準のセキュリティを具備することは、事業者が負う責任にも影響を及ぼし得る重要な観点と考えられる。

別添２
株式会社マネーフォワード

CBDCフォーラム WG3 第7回会合
追加サービス連携時の課題検討

2024/4/16 株式会社マネーフォワード

マネーフォワードについて

マネーフォワードは、「お金を前へ。人生をもっと前へ。」をミッションに2012年に創業しました（東証プライム上場）

Vision　すべての人の、「お金のプラットフォーム」になる。

Values　User Focus　Tech & Design　Fairness

主な提供サービス

事業者向け

経理・財務
- Money Forward クラウド会計
- Money Forward クラウド確定申告
- Money Forward クラウドインボイス
- Money Forward クラウド債務支払

HR
- Money Forward クラウド給与
- Money Forward クラウド勤怠
- Money Forward クラウド人事管理
- Money Forward クラウド社会保険

その他バックオフィス
- Money Forward クラウド契約
- Money Forward Pay for Business
- Admina
- HiTTO
- Manageboard
- V-ONEクラウド

SaaSマーケティング支援

BOXIL SaaS　ADXL　BALES CLOUD

個人向け

- Money Forward ME

Fintech

- Money Forward Early Payment
- Money Forward Kessai
- Money Forward 請求書カード払い for Startups
- Money Forward トランザクションファイナンス for Startups

金融機関向け

- Money Forward Fintech Platform

ハイライト（2023年11月期末）

課金顧客数（事業者） 301,233 （前年同期比+27.8%）	ME利用者数（個人） 1,530万	連携金融関連サービス数*1 2,540以上
SaaS ARR （年間定期収益） 231.5億円	SaaS ARR成長率 前年同期比 +42%	売上高成長率 前年同期比 +41%
連結従業員数 2,130名	エンジニア/デザイナー比率 約４割	エンジニアnon-JP比率 約４割

*1　連携できる金融関連サービス。自社調べ、2023年5月末現在。

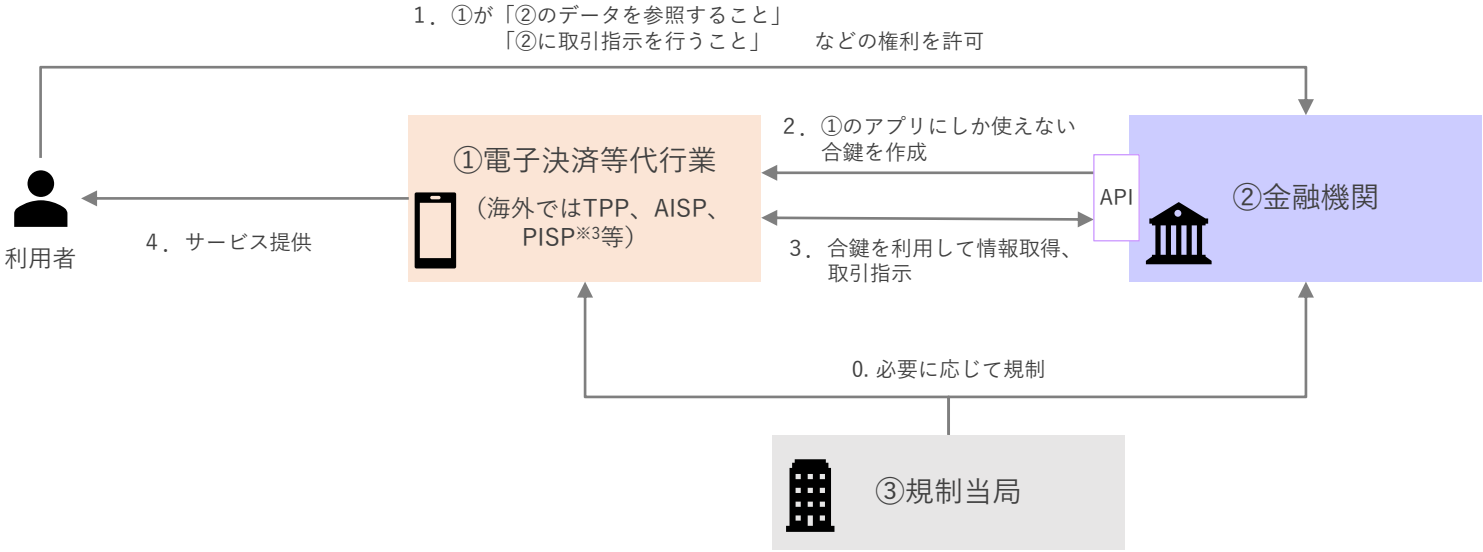
本日の内容

CBDCにおいて、追加サービスと仲介システムが連携する際のUX（ユーザー体験）向上に向けた課題の整理

1．オープンバンキングの基本的枠組
2．追加サービスとの連携について
3．追加サービス連携時の課題
　①認証の一部省略・簡略化
　②認証回数の制限
　③追加サービス提供者⇔金融機関間の情報の連携
　④追加サービス提供者と金融機関間での責任分解
4．追加サービス連携時の課題（まとめ）
5．【参考】電子決済等代行事業者協会のStudy Group

1. オープンバンキングの基本的枠組

- 電子決済等代行業者と金融機関の連携については、スクレイピングからAPI※1連携に移行※2
- 更新系（送金、振込）APIはほとんど普及していない



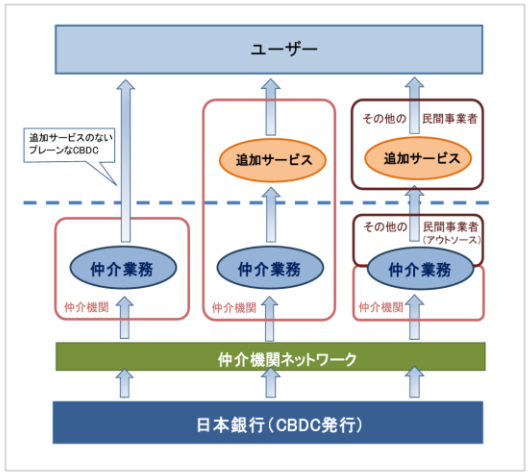
※1　API: Application Programming Interface
※2　都市銀行、第一地方銀行、第二地方銀行についてはほとんどがAPI接続を実現
※3　TPP: Third Party Provider
AISP: Account Information Service Provider
PISP: Payment Initiation Service Provider

（出典）各種資料より当社作成

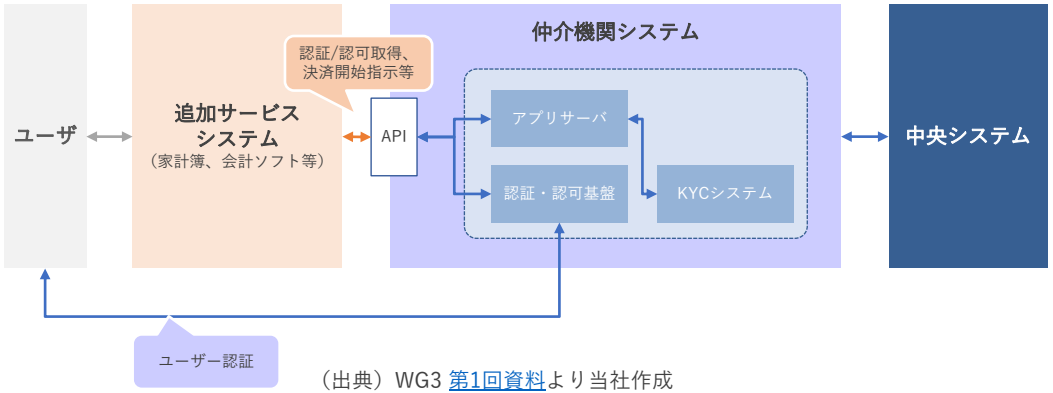
2. 追加サービスとの連携について

CBDCエコシステムで想定されている追加サービスを視野に入れた場合、右図の構成が想定される

- 仲介機関と追加サービスがAPIで連携
- 認証・認可取得、決済開始指示などもAPI経由で実行
- 決済開始指示の場合、最終的には中央システムの台帳更新とも連携



（出典）「中央銀行デジタル通貨（CBDC）に関する取り組み」より

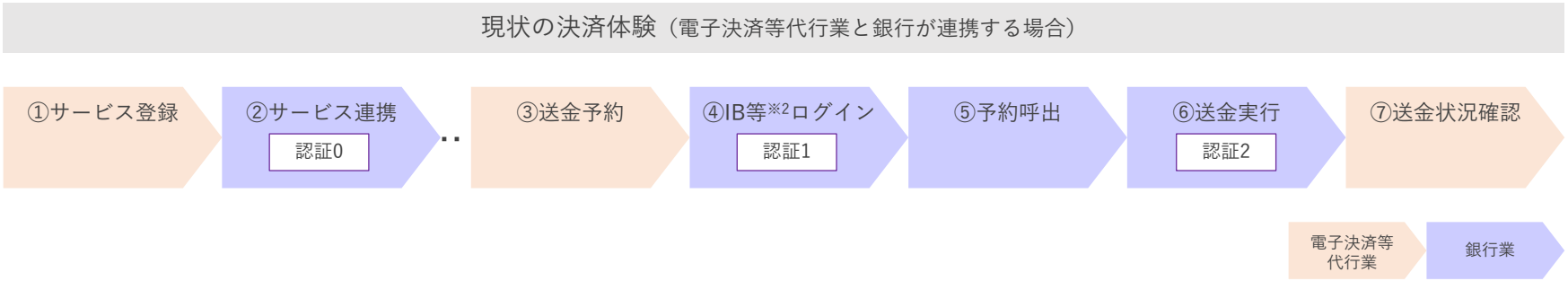


（出典）WG3 第1回資料より当社作成

3. 追加サービス連携時の課題

決済時のUX※1向上が課題となる

※1　UX: User Experience、ユーザー体験
※2　IB: Internet Banking



- ②のサービス連携（電子決済等代行業との「紐づけ」）時に、銀行側による認証0が行われる。
  ・送金予約機能、送金状況確認機能：銀行側が認可
  ・送金実行　　：認可無し
- ③送金の「予約」しか電子決済等代行業からは行えない
- ④IB等の画面にログインし直す必要がある（銀行側が認証1を実行）
- ⑥送金実行時に再度、認証が求められる（銀行側が認証2を実行）

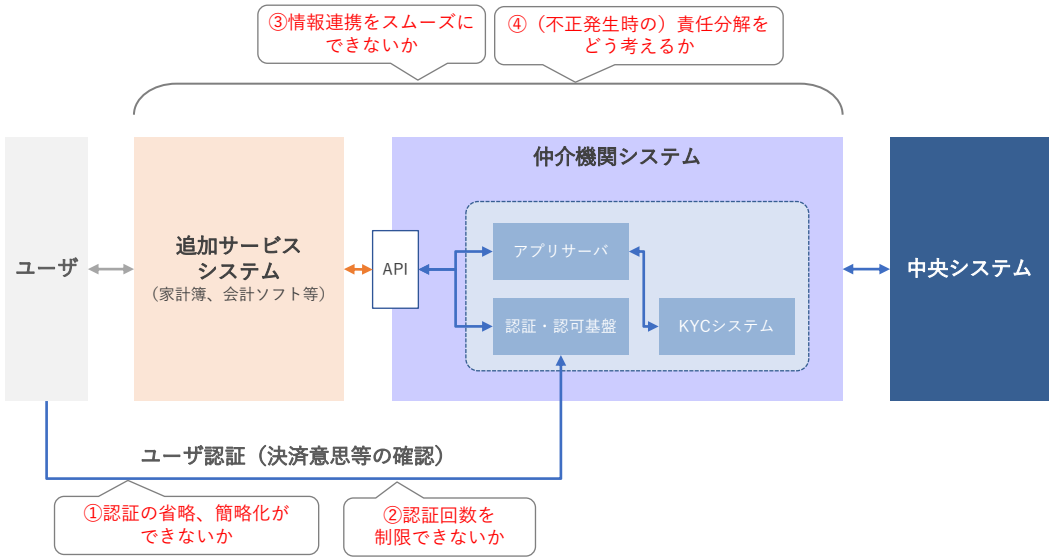
（出典）当社作成

3. 追加サービス連携時の課題

・CBDCの導入は、これまでの前提条件をゼロベースから再検討できる好機

・決済時のUX向上のため以下の対応が検討できないか

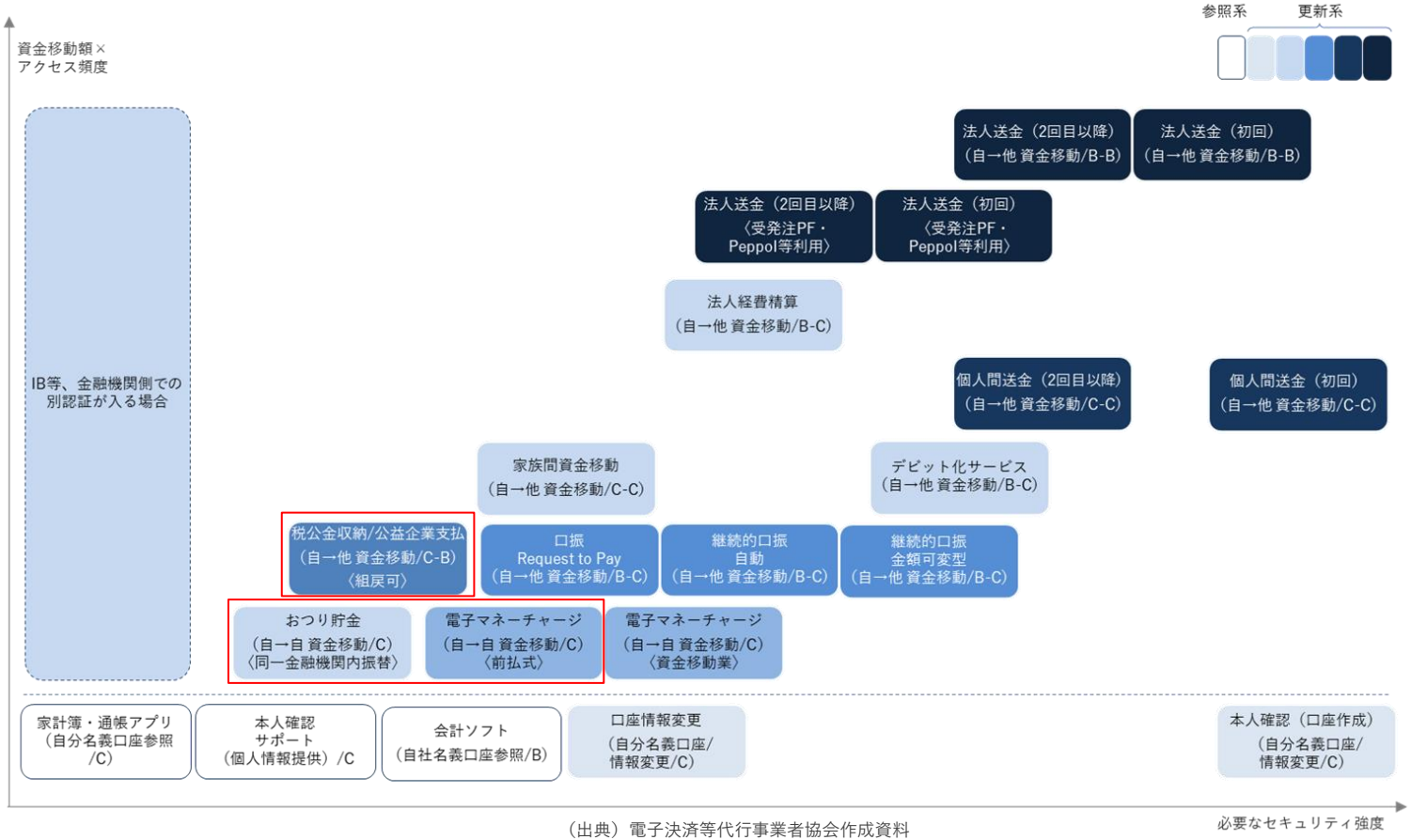
①認証の一部省略、簡略化
②（一連のUX上での）認証回数の制限
③（一連のUX上での）追加サービス提供者⇔金融機関間の情報の連携
④追加サービス提供者と金融機関間での責任分解の考え方の整理



（出典）当社作成

3. ①認証の一部省略、簡略化

CBDCでも、低リスクユースケースについては認証の一部省略が考えられないか

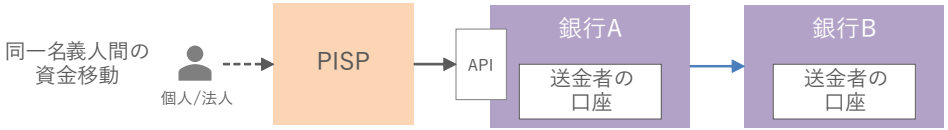


（出典）電子決済等代行事業者協会作成資料

3. ①認証の一部省略、簡略化（海外情報１）

英国では同一名義人間、政府組織等への資金移動（VRP：変額定期支払）について規制を緩和

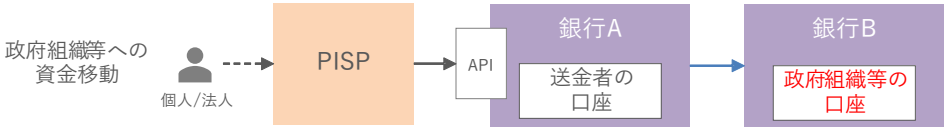
大手9行に義務付済（2022年）



・個人/法人の同一名義の「当座預金口座」への資金移動について、VRPを義務付け
・VRPに関する認証は当初1回のみ、銀行（ASPSP）で必要。SCA適用
・上記認証後は、定期的にPISPから資金移動を指図。金額は毎回変動
・上記以降の認証は、PISP側で90日毎に取得すればよい（銀行（ASPSP）への再認証は不要）

（出典）https://assets.publishing.service.gov.uk/media/610029a8d3bf7f044ee52336/Letter_to_the_Open_Banking_Implementation_Entity.　pdf
Developments in Open Banking: Variable Recurring Payments and Sweeping　- Bird & Bird (twobirds.com)

合同規制監視委員会提案中



・上記と同様のVRP

【英語略称】
VRP: Variable Recurring Payment、変動定期支払
SCA: Strong Customer Authentication　強力な顧客認証。欧州等で義務化された多要素認証
PISP: Payment Initiation ServiceProvider、決済開始サービス提供者
（日本で言う電子決済等代行事業者の1号業務）
ASPSP: Account Servicing Payment Service Provider　口座サービス提供者（銀行等）

（出典）電子決済等代行事業者協会作成資料

3. ①認証の一部省略、簡略化（海外情報２）

欧州では下記ユースケース時には、多要素認証※を**必ずしも適用しなくてもよい**

※　欧州では決済履行時にSCA（Strong Customer Authentication: 強力な顧客認証）と呼ばれる多要素認証が義務化されている

PSR: Payment Service Regulation、現在提出中のPSD3関連法案
RTS: Regulatory Technical Standard、欧州銀行監督局が定めるハイレベル標準

条項	内容	備考
PSR案85条2.	受取人のみが開始する決済	Debit、Request to Pay
RTS第11条	店頭での非接触決済	50ユーロ未満等の条件付
RTS第12条	交通運賃支払、パーキングメーター支払	
RTS第13条2.	信頼できる受取人リストへの支払	リスト改訂にはユーザー認証が必要
RTS14条2.	同一の受取人への二回目以降の定期的な支払	
RTS15条	同一の決済口座サービス提供者内にある同一の自然人又は法人間の送金	いわゆる同行内振替
RTS第16条	低額取引	30ユーロ未満等の条件付
RTS第17条	専用の決済プロセス又はプロトコルによる企業決済	当局による事前の了承要（Peppol利用時等に相当すると考えられる）
RTS18条	取引監視により一定の不正率以下と見なされる場合	不正率の計算方法等は詳細に規定。監視方法等には監査が求められる
（参考）参照系		
PSR案86条3.	口座情報サービス提供者による決済口座への2回目以降のアクセス	
RTS第10条a 1.	決済口座の残高参照、90日以内の過去の決済取引の情報参照	

（出典）電子決済等代行事業者協会作成資料

3. ①認証の一部省略、簡略化（海外情報３）

欧州では多要素認証※を**適用しない場合の基準となる不正率を定めている**

※　欧州では決済履行時にSCA（Strong Customer Authentication: 強力な顧客認証）と呼ばれる多要素認証が義務化されている

規制技術標準第18条「取引監視により一定の不正率以下と見なされる場合」

免除基準値	参照する不正率（%）	
	遠隔での電子的なカードベース決済	遠隔での電子的な送金
500ユーロ	0.01	0.005
250ユーロ	0.06	0.01
100ユーロ	0.13	0.015

この金額を超えない範囲　／　この率と同等又は以下の不正発生率

＋

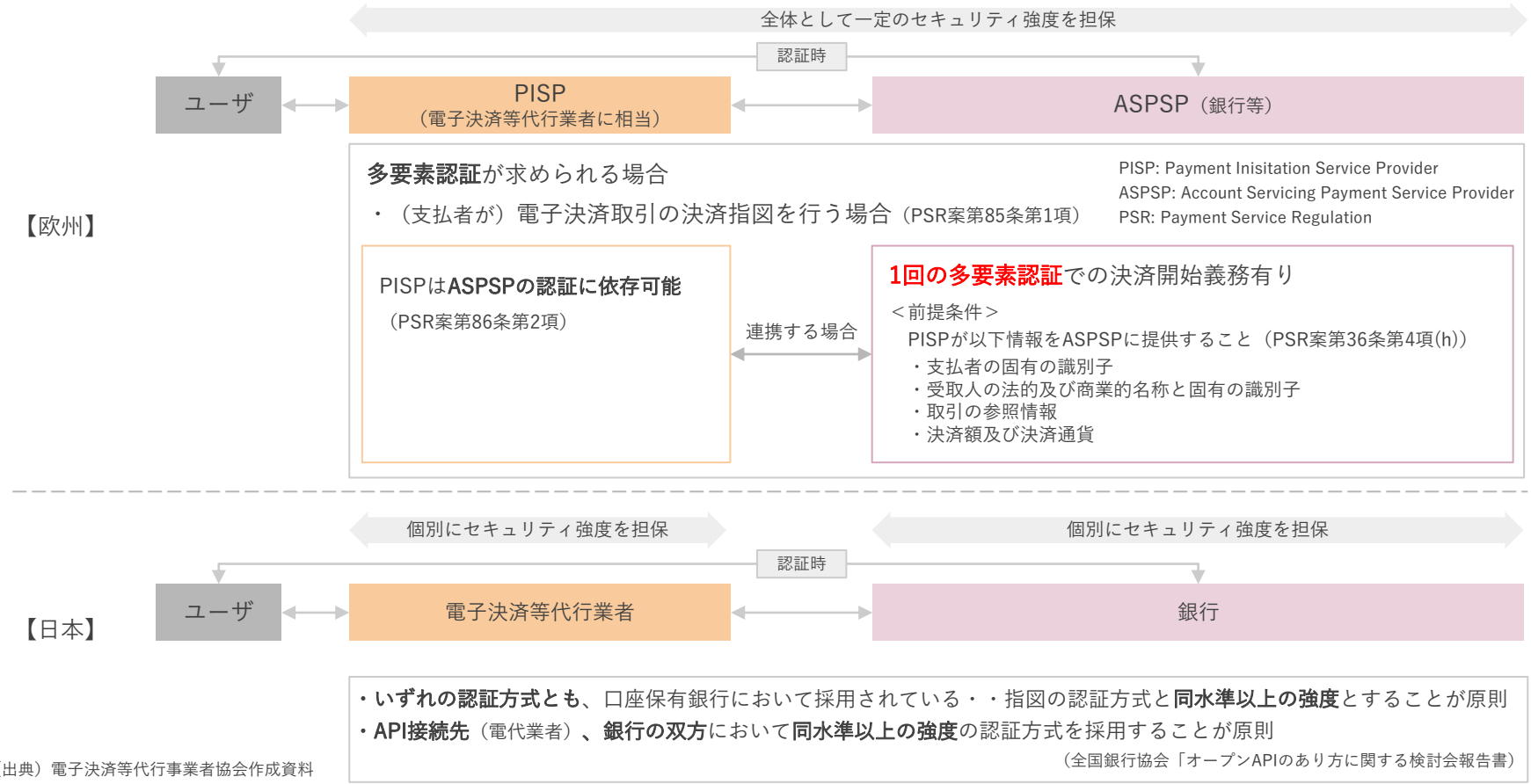
怪しい送金パターン、不正シナリオ、高リスクの所在地などでないことが
リアルタイムで監視可

多要素認証を不要とできる

（出典）欧州の規制技術標準（RTS）附属書より当社作成

3. ②（一連のUX上での）認証回数の制限（海外情報４）

欧州では決済時認証について、金融機関側に「1回」の多要素認証での決済開始を義務付け

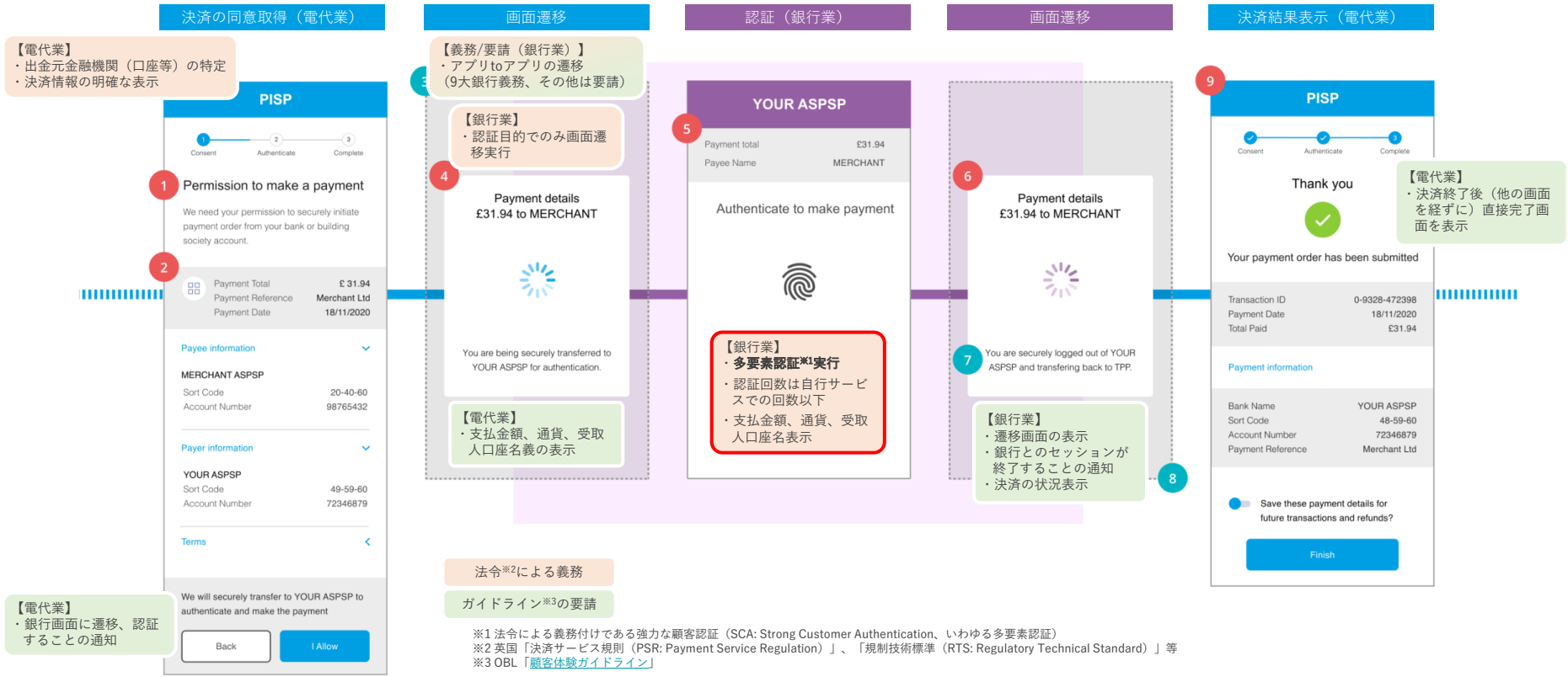


（出典）電子決済等代行事業者協会作成資料

3. ③（一連のUX上での）追加サービス提供者⇔金融機関間の情報の連携（海外情報５）

英国ではユースケース毎に、PISP（電代業1号事業者に相当）と銀行間の情報連携を法令＋ガイドラインで詳細に規定

国内送金（一回のみ決済）のユースケース



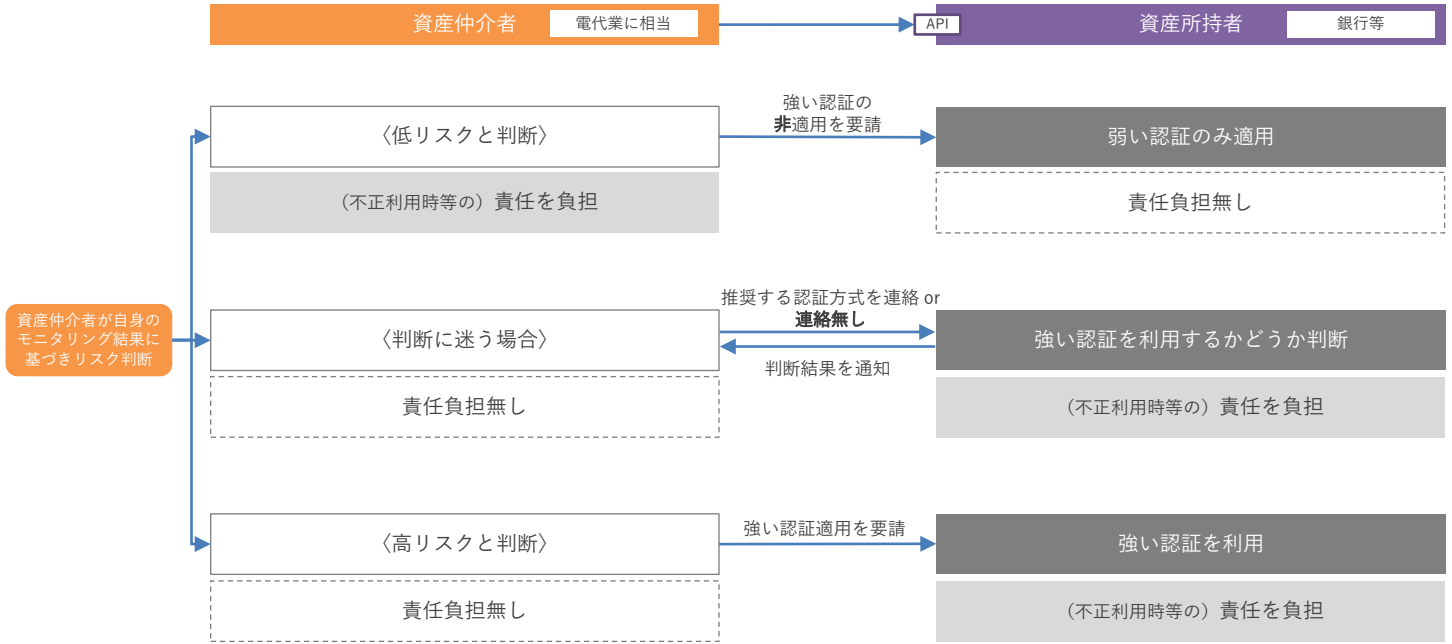
※1 法令による義務付けである強力な顧客認証（SCA: Strong Customer Authentication、いわゆる多要素認証）
※2 英国「決済サービス規則（PSR: Payment Service Regulation）」、「規制技術標準（RTS: Regulatory Technical Standard）」等
※3 OBL「顧客体験ガイドライン」

（出典）上記ガイドラインより当社作成

3. ④追加サービス提供者と金融機関間での責任分解（海外情報６）

欧州の自主規制機関による、電子決済等代行業⇔金融機関間の、認証及び責任分解の考え方

規制技術標準18条（リスクベース判断）適用時の顧客認証の分担と責任分解の考え方



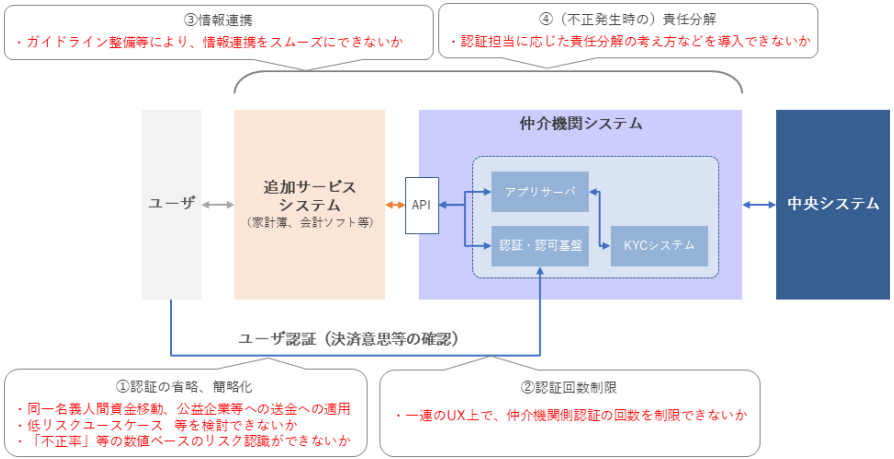
※ SPAA（SEPA Payment Account Access）スキーム：EPCが定める決済口座アクセスに関するルール、標準、ガイドライン等の総体
※ EPC（European Payments Council）：欧州の主要な銀行等が参加する自主規制組織

（出典） EPCサイト https://www.europeanpaymentscouncil.eu/document-library/rulebooks/sepa-payment-account-access-spaa-scheme-rulebook-v11 より電子決済等代行事業者協会作成

4. 追加サービス連携時の課題（まとめ）

・ CBDCの導入は、これまでの前提条件をゼロベースから再検討できる好機

・決済時のUX向上のため、海外動向なども参考に以下の対応が検討できないか



課題	考えられる対応	CBDCの場合の視点
①認証の省略・簡略化	・同一名義人間資金移動、公益企業等送金への適用 ・低リスクユースケースの検討 ・「不正率」等の数値ベースのリスク認識	・公共的なユースケース検討と連携 ・不正率データ、不正関連情報の公的、中立的機関による蓄積
②認証回数制限	・仲介機関側認証の回数制限	・仲介機関側の認可内容、中央システム側の認可内容にも依存
③情報連携	・ガイドライン整備	・公的、中立的機関による整備の可能性※ ※英国ではOBL、EUではEPC、米国ではFDXなどが整備
④（不正発生時の）責任分解	・認証担当に応じた責任分解	

（出典）当社作成

本資料に記載された情報は株式会社マネーフォワードが信頼できると判断した情報源を元に株式会社マネーフォワードが作成したものですが、その内容および情報の正確性、完全性等について、何ら保証を行っておらず、また、いかなる責任を持つものではありません。

本資料に記載された内容は、資料作成時点において作成されたものであり、予告なく変更する場合があります。株式会社マネーフォワードの許可なく、本資料を第三者に提示し、閲覧させ、また、複製、配布、譲渡することは堅く禁じられています。

本文およびデータ等の著作権を含む知的所有権は株式会社マネーフォワードに帰属し、事前に株式会社マネーフォワードの書面による承諾を得ることなく、本資料に修正・加工することは堅く禁じられています。