2024 年 1 月 22 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３回会合の議事概要

１．開催要領

（日時）2023 年 12 月 11 日（月）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

事務局から、「本ＷＧに関連する海外の議論（デジタルユーロ調査フェーズ報告書）」（別添１。以下、海外動向紹介資料）に基づいて説明を実施。その後、株式会社イオン銀行、株式会社三菱ＵＦＪ銀行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）既存の資金決済サービスの現状①（株式会社イオン銀行）

―― 提供している資金決済サービスにおいて、ＫＹＣと当人認証に関連するユーザーアクションや実施状況の整理を行った。プレゼンテーション資料の要旨は別添２を参照。

既存の資金決済サービスの現状整理として、当社が提供中の資金決済サービスおよび身元確認と当人認証の取組について説明を行う。

当社グループでは後払い決済サービス（以下、クレジット）、即時払い決済サービス（以下、デビット）、前払い決済サービス、銀行預金口座など複数の決済サービスを提供。また、預金口座は他社の電子マネーチャージなどに使える預金口座振替機能を提供している。それぞれの決済サービス機能が付与されたカードを大きく分けて４種類（クレジット機能のみ、クレジット機能＋預金口座機能、デビット機能＋預金口座機能、預金口座機能のみ）発行している。

これらの決済サービスは、Ｗｅｂ（非対面取引）による申込も受付しており、その際の身元確認は、決済サービスごとに取り扱いに差異があるが、①本人確

認方法の特例（犯罪収益移転防止法施行規則第１３条）による確認、②カード受取時確認（配達員による本人確認書類の確認）、③顔写真なし本人確認書類２点アップロード＋転送不要郵便による確認、④ｅＫＹＣのホ方式（本人確認書類の撮影＋容貌の撮影）による確認の４種類を揃えている。ホ方式は、本人確認書類の撮影が簡単ではないことや操作手順が煩雑であること等から申込途中での離脱率が高いことが課題。そうした課題を踏まえ、現在ｅＫＹＣのワ方式（マイナンバーカードのＩＣチップ読取＋暗証番号入力）の導入を検討している。ワ方式は、マイナンバーカード保有者のみが対象であることがデメリットであったが、マイナンバーカードの普及率が高まっており、そのデメリットが薄まりつつある。加えて、ＩＣチップの偽造が困難であること、ホ方式と比較してシンプルな手続きであること、容貌画像や本人確認資料の真贋判定が不要でその分１件あたりのコストが低く判定に要する時間も少ないこと等のメリットがあるため、導入検討対象として考えている。

預金口座については、Ｗｅｂブラウザからアクセスするインターネットバンキング、スマートフォンアプリ（以下、アプリ）の２種類のツールを提供しており、認証強度に応じて、利用できる機能に差異を設けている。残高確認など取引照会機能であれば、インターネットバンキングもしくはアプリへログイン（ＩＤとパスワードによる認証）することで利用可能であるが、定期預金預入や投信購入、送金、登録情報の変更等は、インターネットバンキングのみで利用ができる。インターネットバンキングにおける取引では、定期預金預入や投信購入等は別途定めた取引パスワードの追加認証が必要となり、振込や登録情報変更等は、取引パスワードに加え、メールにて受け取るワンタイムパスワードを用いた認証が更に必要となる。なお、インターネットバンキングにおいては、ログインする利用端末を予め登録し、登録された端末とは別の端末でログインした場合には合言葉を入力する必要が生じるなど、リスクに応じて認証を追加するリスクベース認証の対応も行っている。

他社の電子マネーにチャージするための口座振替登録においては、他社アプリ等より当社Ｗｅｂページに遷移し、ＩＶＲ認証（自動音声応答による本人認証）およびキャッシュカードの暗証番号にて認証を行う。

現状の当社決済サービスにおける課題は、①認証レベルとユーザビリティの観点でのガイドラインや基準、②属性情報の取得、③非対面（非対人）の限界、④ユーザビリティとセキュリティの４点が挙げられ、ＣＢＤＣを検討する上でも論点になると考えられる。①認証レベルとユーザビリティの観点でのガイドラインや基準は、明確にはないものの、当社が提供する決済サービスに

おいては、当該取引のリスクとユーザビリティを踏まえ、セキュリティ部門と相談の上、認証方式の判断を行っている。一方、他社が提供する電子マネー等の決済サービスにおいて、当行口座を引落口座として紐づけることを許容する際の提携可否判断は、当該事業者のセキュリティレベルを測る必要があるため、独自の評価基準を作り、絶対評価と相対評価の両面で総合的に判断を行っている。自社と他社での決済サービスにおけるこうした対応のガイドラインや基準を今後どのようにしていくかは、重要な点と考えている。②属性情報の取得については、預金口座開設やクレジット申込の時期により、当社に電話番号・メールアドレスの登録がない場合があり、電話番号やメールアドレスを用いた認証ができないお客さまがいる。このようなお客さまへの対応が課題である。③非対面（非対人）の限界については、年々Ｗｅｂ経由の各種申込が拡大している中、高齢者の多くは手続き自体の高度化も相まって、非対面のＷｅｂブラウザ等を通じた手続きを自己完結させることが難しく、非対面だけでは全てのお客さまに対応ができないことが課題となっている。ユニバーサルアクセスの観点を踏まえ、店舗対応やコールセンターなど人によるサポートが引き続き必要になると考えている。④ユーザビリティとセキュリティについては、営業的な観点ではユーザビリティは高ければ高いほど良いと考えるが、セキュリティの観点では手続きが簡素化されることでリスクが高まることは望ましくなく、そのバランスが難しいと考えている。あえて手続きを煩雑にするなど、悪意者に不正利用されない仕組みを検討することも必要と思われる。

（２）既存の資金決済サービスの現状②（株式会社三菱ＵＦＪ銀行）

―― 提供している資金決済サービスにおいて、ＫＹＣと当人認証に関連するユーザーアクションや実施状況の整理を行った。プレゼンテーション資料の要旨は別添３を参照。

オンラインにおける既存の資金決済サービスの現状整理として、スマートフォンのアプリを用いた口座開設から振込までの流れにおける当行の身元確認および当人認証の取組を説明し、ＣＢＤＣシステムを検討する上で想定される論点出しを行う。

当行は、口座開設を担う「スマート口座開設」アプリ（以下、口座開設アプリ）、インターネットバンキング機能を有した資金決済サービスとして、Ｗｅｂブラウザを利用する三菱ＵＦＪダイレクト（以下、インターネットバンキング）、スマートフォンのアプリを利用する「三菱ＵＦＪ銀行」アプリ（以下、

ＩＢアプリ）を提供している。

口座開設アプリにおける口座開設時の身元確認では、ｅＫＹＣのホ方式とヘ方式を選択でき、運転免許証もしくはマイナンバーカードを用いることができる。口座開設が完了すると、口座開設アプリ上で、インターネットバンキングの利用登録としてログインパスワードやメールアドレス等の登録を行う。その後、不正な口座開設申込を防止する観点、具体的には１つのスマートフォンで複数回申込むようなスマートフォンの使いまわし防止も含めて、ＳＭＳ認証が行われる。

登録したログインパスワードを用いて、ＩＢアプリに初回ログインをすると、生体認証（ＦＩＤＯ）の利用登録が案内される。登録は任意だが、登録することで生体認証を用いて簡単にＩＢアプリへのログインが可能となる。ＩＢアプリのログイン後、振込の際に必要となるワンタイムパスワードの利用登録を行うが、利用登録に際してはＩＶＲ認証またはヘ方式によるｅＫＹＣ認証を選択できる。ワンタイムパスワード利用登録後は、ワンタイムパスワード認証（スマートフォンのアプリを用いたソフトウェアトークン）を利用することで、振込ができる流れとなる。以上のように、当人認証においては、各種認証を組み合わせ、取引ごとに必要と考えるセキュリティの認証強度を確保している。

また、身元確認および当人認証における改善事例として２点紹介する。１点目は、口座開設アプリにおける不正な口座開設申込への対策として、過去の申込時の容貌画像を活用し、一定水準以上で不正な申込が疑われる場合、事務センターにおいて人手で重点的にチェックを行う仕組みとしている。２点目は、ＩＢアプリにおけるお客さまの利便性向上として、前述のとおり、ヘ方式によるｅＫＹＣ認証を導入した点。ＩＶＲ認証のみだった時期には、お客さまが電話番号を変更した際にはアプリ上でワンタイムパスワードの利用登録ができず、コールセンターとの問診または店頭での手続きを行う必要があった。ｅＫＹＣ認証導入後はオンラインで完結できるようになり、お客さまの利便性向上を実現した。このように、不正利用対策や利便性向上の観点による機能改善は、いずれも重要と考えている。

こうした現状を踏まえ、ＣＢＤＣシステムを検討する上で想定される論点として、①身元確認や当人認証に係る仕様、②不正利用への対策を挙げる。①については、３点ある。１点目は、ＣＢＤＣシステムにおいて共通の仕様を導

入するか、各仲介機関で個別に決定するか、という点。各仲介機関に判断が委ねられた場合、ＣＢＤＣシステムにおける各取引において、仲介機関ごとに認証強度の差分が生まれることが想定される。一方、共通仕様とする場合は、いわゆる競争領域と非競争領域の考え方があるため、非競争領域として１つの認証基盤を活用することも検討の余地があると考えられる。２点目は、当人認証の強度を共通化する１つの選択肢として、公的個人認証の導入が検討に値するのではないかという点。３点目は、上述のとおり、電話番号が変更になった場合への対応としてｅＫＹＣ認証を導入した経験より、ＣＢＤＣユーザーがパスワードの失念等により利用できなくなった際など、オンラインで復旧する仕組みは利便性を高めるために必要であるという点。②については、２点ある。１点目は、ＣＢＤＣ口座は、預金口座や資金決済アカウントに紐づけられると認識しているが、預金口座や資金決済アカウントの身元確認や当人認証の強度に差がある場合、差を許容するか、許容しないかは論点になりうるという点。不正利用防止の観点からは、より強度の高い方式に揃えることが望ましいが、ユーザビリティとのバランスも重要になる。２点目は、残念ながら不正利用が発生した場合において、関係者間の責任分界点が論点となりうるという点。関係者として、仲介機関、ＣＢＤＣシステムの運営機関、日本銀行などが想定されうるが、不正利用のケースを想定しながら議論をしていく必要があると考えている。なお、一例としての紹介であるが、振込に関しては、全国銀行協会において申し合わせを行っており、補償に関してはお客さまに寄り添った形で対応していくという統一的な目線はある。ＣＢＤＣシステムにおいても、このような指針を踏襲するか否か含め、論点となりうると考えている。

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、株式会社千葉銀行が担当した。概要は以下のとおり。

【海外動向】

（参加者）海外動向紹介資料の７ページ目「支払いの流れ」において、「決済の指図にユーザーを特定できるデータは含まれない」と記載がある。ユーザーを特定できないが、決済が可能であることについての補足説明をお願いしたい。

（日本銀行）決済の指図のデータに個人を特定しうる個人情報が含まれないが、

支払いの相手先を特定するための番号なり識別子等を用いることによって決済が可能となるものと理解している。

【ユーザビリティとセキュリティのバランス】

（日本銀行）これまでの発表や議論から、ユーザビリティとセキュリティのバランスが重要かつ課題が多いと感じた。身元確認における課題を解決するためにワ方式の導入が挙げられているが、このワ方式はユーザビリティとセキュリティのバランス上、満足がいくものか、改善の余地があるものか、意見を伺いたい。

（参加者）ワ方式は、マイナンバーカードを読み取った後に、暗証番号を入力する流れだが、暗証番号を覚えているユーザーが少なく、ワ方式による身元確認を完結出来ないユーザーが一定数いるという問題がある。ユーザーの利便性を高める観点からは、ヘ方式など、他の方式との併存も必要と考える。

（日本銀行）利便性を追求し、セキュリティが弱い方式を併存させると、悪意者がセキュリティの弱い箇所を中心に攻撃してくる可能性は否めないと思われる。こうしたことを踏まえて、ホ方式も含め、セキュリティの観点からご意見あれば伺いたい。

（参加者）ワ方式およびヘ方式に対して、ホ方式は大きく異なるものと理解している。ワ方式およびヘ方式は、ＩＣチップの中の電子証明書を読み取る必要があるが、電子証明書を悪意者が偽造することは現時点では難しい。一方で、ホ方式は、本人確認書類を偽造されるリスクへの対応が課題である。ワ方式およびヘ方式であれば、本人確認書類の偽造という観点におけるリスクは、一定程度に抑えられると考えている。

（参加者）一般論として、新たなセキュリティ対策を出したとしても、すぐに陳腐化が始まるというのが基本的な考え方のため、例えば「ワ方式を導入すれば大丈夫」といった考え方は、不正利用防止の観点では危険だと考える。どの方式が良いということではなく、例えば、ワ方式を使いつつ、追加で本人の容貌画像や動いた姿の撮影も行う、というように、犯収法上の本人確認では求められていないものの、民間事業者が不正利用の実態を踏まえた上で、追加的に対策を行っていく必要があると考える。導入当初は最新技術であっても、時間が経過すれば突破されることが十分にありう

る。悪意者にとって経済的な利益が大きければ、セキュリティを突破する技術を開発してくることが想定される。また、根本的には、所持認証と知識認証の組み合わせでしかないので、不正にワ方式による本人確認が突破されるリスクは既に存在している。こうしたリスクも加味して考える必要があり、セキュリティの面で満足することはないと考えている。

【生体認証および端末認証の課題】

（日本銀行）ユニバーサルアクセスの観点からも、セキュリティとユーザビリティは非常に重要と認識している。例えば、生体認証における知見や懸念点があれば伺いたい。

（参加者）生体認証というよりも、ヘ方式やワ方式にも共通する話ではあるが、非対面における口座開設の共通の課題の１つとして、対面であれば得られる付加的な情報により本人確認の精度を上げられる場合を指摘できる。

（参加者）対面であれば目の前にいるので追加の確認ができるが、非対面だと追加の確認が難しく、どのように対応すべきかは、当社においても常に議論になっている。

（参加者）端末認証に関して、端末自体に依存してしまうことが課題と考えている。つまり、端末を変更すると、端末認証を取り直す必要が生じるが、取り直し易いユーザビリティの観点と、悪意者が別端末でなりすますことを防ぐセキュリティの観点とのバランスをどう考えるかといった点である。加えて、セキュリティの観点からは、端末認証による認証の結果、どの程度の取引を許容するかも検討事項になると考えている。

（日本銀行）端末を変更した際に、端末認証を取り直す必要があるのはなぜか。

（参加者）ＦＩＤＯ認証の場合、端末にセキュリティトークンが保存されていることから、端末変更時にはトークンを別端末に引継ぐ必要があると理解している。引継ぎ方法は、ＦＩＤＯ認証においても用意されているが、引継ぎする行為自体がセキュリティの面で穴になりうる。

（参加者）生体認証の懸念点として、新しく登録をする、または端末変更があれば、再登録をする、といった際の登録処理において、何をもってユーザーと認証器の紐づけを行うかが重要。ＩＶＲ認証やキャッシュカード暗証番号認証なども考えられるが、こうした最初の紐づけをする際の認証をどう設計するかが、セキュリティの観点からは大きな影響があると認識している。

（参加者）ＦＩＤＯ認証はＢａａＳや組み込み型金融においても、有効な認証方法と認識しているが、端末変更時の取り扱いは整理していく必要があると考える。

（参加者）ＦＩＤＯ認証に関し、端末変更時や端末を無くした場合のリカバリ方法としては、Ｓｙｎｃｅｄ　Ｐａｓｓｋｅｙｓ（同期型パスキー）という新しい規格が出てきている。これにより、端末変更時等においても、再登録するのではなく、認証資格情報を引継ぐことが可能となる。問題点としては、これまでの議論と同様ではあるが、端末変更時の移行手続きにおける追加認証を突破された場合、認証資格情報が不正利用されてしまうリスクがあることである。

（参加者）誰もがスマートフォンといった端末を紛失することはない、端末が自分のものであると証明されているということを前提しがちだが、そうではない場合もありうることを踏まえて議論する必要がある。

【責任分界点】

（参加者）海外動向紹介資料の５ページにおいて、デジタルユーロにおける個人ユーザーは、「デジタルユーロ口座は一つしか保有できない」と紹介いただいたが、日本のＣＢＤＣにおいても同様の制度設計となった場合には、犯収法上の特定事業者がＫＹＣを行い、ＣＢＤＣの口座開設が行われると考えられる。金融庁のガイドラインを踏まえれば、ＫＹＣは犯収法上の本人特定事項の確認、つまり本人の存在の確認に留まらず、自社のプロファイルに基づいてお客さまの情報を追加的に知る必要があると認識している。そうして、お客さまのプロファイルを充実させて管理することで、不正の疑いのある取引に気づくことができる。ＣＢＤＣにおいては、仲介機関の役割として行った口座開設やその後の取引モニタリングなど、様々なシチュエーションにおいて、誰がどのような責任を持つのかという責任

分界点について明確にしていく必要があると考えている。また、「個人ユーザーはＣＢＤＣ口座を複数保有できる」という制度設計となった場合は、１つの口座では少額の振込しか行っておらずとも、口座を多数開設することで、全体としては多額の振込を行っている、などの問題の発生が考えられるため、名寄せの要否を含め、どのように確認を行うかを考える必要がある。いずれの場合においても、異常値の検知方法や、そのためのコストおよび責任の所在などについて検討する必要があると考える。今後もデジタルユーロの進捗は参考にしたい。

（参加者） 今後もデジタルユーロの進捗を見ていくことに賛同する。例えば、オープンＡＰＩ、オープンバンキングの促進が始まった際に、ＥＵでは各国の所管官庁が、オープンバンキングやＯＡｕｔｈ２．０の認証方式などについて、細かく定めてスタートしていた印象がある。おそらくＣＢＤＣにおいても、同様に情報セキュリティ面を含めて検討を進めていくのではないかと期待されるため、海外の情報は引き続き共有をいただきたい。

（参加者）当社では、欧州決済サービス指令第３版（ＰＳＤ３）の調査をしており、その調査において、銀行とサードパーティ事業者間の責任分界点について整理されていた覚えがある。本ワーキンググループにおける議論においても有益な情報と感じているため、改めて共有させていただく。

（参加者）端末認証、セキュリティ、名寄せ等様々な論点が挙げられたが、今後の会合の中で整理を進め、議論を深めていきたい。

４．次回予定

次回の会合は１月 24 日（水）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３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

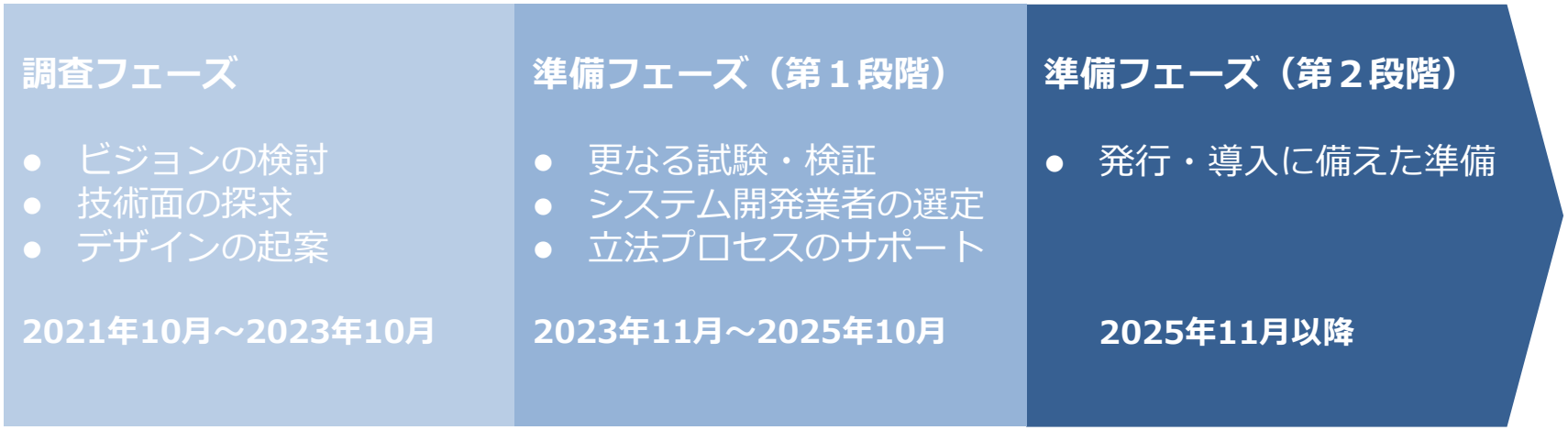
CBDCフォーラム
【KYCとユーザー認証・認可】WG（WG3）
第3回会合　事務局説明資料

本WGに関連する海外の議論
（デジタルユーロ調査フェーズ報告書）

2023年12月11日
日本銀行 決済機構局

ECB「デジタルユーロ調査フェーズ報告書」

- ECBは本年10月に、デジタルユーロ（ユーロ圏版リテールCBDC）の**調査フェーズ（investigation phase）を完了**し、調査フェーズを通じて得られた主な知見を要約した報告書を公表



- 報告書の内容は以下のとおり多岐にわたるが、本資料では、**本WGに関連する箇所を抜粋**して紹介する
  - 第1章 デジタルユーロの意義
  - 第2章 エンドユーザーからみたデジタルユーロ
  - 第3章 PSP・中央銀行の役割
  - 第4章 投資手段としての制限
  - 第5章 デジタル・金融包摂
  - 第6章 プライバシーおよびデータ保護
  - 第7章 ステークホルダーとの協業
  - 第8章 準備フェーズに向けて

第2章（エンドユーザーからみたデジタルユーロ）①

利用主体

- **ユーロ圏の居住者**（個人・事業者）がデジタルユーロを利用できる
  - ✓ **非居住者や旅行者による利用は、デジタルユーロの導入時点では想定していない**

ユーザーの属性	ユーロ圏内	ユーロ圏外
個人	• デジタルユーロの保有と、それによる支払が可能	• ユーロ圏外居住者のデジタルユーロへのアクセスは、デジタルユーロ導入後、次の段階（next step）として検討 • ユーロ圏外の国におけるデジタルユーロ利用可否は、常に当該国当局との合意（agreement）に基づく
事業者 (businesses)	• デジタルユーロの受取が可能 • 他のデジタル決済手段を受け入れている事業者は、デジタルユーロによる支払を許容しなければならないことを想定	• ユーロ圏の居住者にサービスを提供した場合、ユーロ圏のPSP（決済サービス提供者）を通じてデジタルユーロによる支払を受入可能
公共部門	• デジタルユーロの支払・受取が可能	（記載なし）

第2章（エンドユーザーからみたデジタルユーロ）②

口座開設

- 顧客と適切な契約関係を結ぶことは、PSP (Payment Service Provider)の責任である
- **口座開設（onboarding）はできる限り簡便**であるべき
  - ✓ PSPは、既に取引関係にある顧客の口座開設にあたっては、自身の保有するデータをエンドユーザーに再度要求するべきではない
  - ✓ PSPは、既存顧客以外の口座開設を行う場合、**KYCを実施**する
  - ✓ KYCのプロセスは、**既存の法律や規則に服する**
  - ✓ EU規則案では、デジタルユーロ以外の口座の保有や開設をデジタルユーロ口座開設の条件とすべきではないとされている

第3章（PSPの役割）①

口座開設

- **口座開設手続、関連するデューデリジェンスおよびKYCの実施は、PSPの責任**である

個人ユーザー

- 口座開設において、PSPは個人ユーザーに以下を提供する
  - ✓ ユーザー資格情報（user credentials）
    - —— **デジタルユーロ口座番号**（**DEAN**: Digital Euro Account Number）等
  - ✓ デジタルユーロへアクセスするためのアプリ
  - ✓ DEANと紐づけされた電話番号など個人を識別する情報（エイリアス）の登録機能
  - ✓ （ユーザーの要望に応じて）物理カード
- デジタルユーロ口座は一つしか保有できないため、口座開設を申し込んだユーザーが他PSPに既に保有していた場合、口座移管要求（portability request）を通じて既存保有額を移管する

第3章（PSPの役割）②

口座開設（続）

事業者ユーザー

- 口座開設において、PSPは事業者ユーザーに以下を提供する
  - ✓ 1つまたは複数のデジタルユーロ口座番号（DEAN）
  - ✓ POSまたは仮想端末のアップデート（デジタルユーロの受入機能の追加）
  - ✓ PSPが提供する既存の資金管理アプリケーションへのデジタルユーロ管理機能の追加
- 同一のエンドユーザーが、同一のPSPで、個人ユーザーとしても事業者ユーザーとしても口座開設することはありうる
  - ✓ その場合、２種類のKYC手続きが別々に実行され、２つのデジタルユーロユーザー（個人と事業者）が登録される

返金

- マネーロンダリング防止などの理由により、市場慣行に倣い、デジタルユーロによる支払はデジタルユーロによってのみ返金可能とする

第3章（PSPの役割）③

支払の流れ

- ユーザーは（ECBの）デジタルユーロアプリ、PSPの自社アプリ、PSPのオンライン・インターフェース、または支払カードを経由して、PSPを通じて、支払を指図する
- PSPは**ユーザーに認証を求め**、必要なチェック（**AML/CFT**や詐欺リスクのチェック）を行い、確認後、決済（settlement）が行われる
  - ✓ 決済の指図は、支払人と受取人のいずれのPSPからも送信されうる
  - ✓ **決済の指図にユーザーを特定できるデータは含まれない**
- 認証とは、個人や法人のアイデンティティを確認するセキュリティ・メカニズムを指すが、デジタルユーロのスキームは、認証方法そのものを提供するわけではなく、**既存の認証方法の活用にオープン**である

アクセス権限の付与

- 個人ユーザーはサードパーティの事業者（口座情報サービス提供者、決済指図伝達サービス提供者など）に対し、PSP経由でデジタルユーロ残高にアクセスする権限を与えることができる

第6章（プライバシーおよびデータ保護）

- プライバシーおよびパーソナルデータ保護は個人の重要な権利であり、**デジタルユーロの重大な目的の一つ**である
- 適切なレベルのプライバシーとデータ保護を保証することは、デジタルユーロへの信頼を育むことにおいて重要である
- **ユーロシステム（中央銀行）は、エンドユーザーを特定するいかなる情報にも直接アクセスすることはない**
- プライバシーおよびパーソナルデータ保護は、**AML/CFT**や脱税対策といった、**他の政策目的とのバランス**をとる必要がある
- 欧州規則案では、デジタルユーロ口座開設にあたっての本人確認は、**既存のデジタル決済サービスと同様**に扱われる

サマリ

別添２
（イオン銀行発表要旨）

■ KYCおよび認証・認可にかかる現状

✓ KYCでは、カード受取時確認や本人確認書類の厚みなどの特徴の撮影と容貌画像で確認するホ方式を活用しているが、セキュリティやコスト面が難あり。コスト面で有利であり、最近のマイナンバーカードの普及やそのICチップを読み取り本人確認するセキュリティの高い確認方法(ワ方式)の採用を検討中。

✓ 認証・認可では、WEBブラウザ・アプリで照会・取引の際に認証が必要であるが、多要素認証を導入し、特に送金や属性変更については、もう一段階、認証を追加する仕組みを導入しセキュリティを高めている。クレジットカードの属性変更時にはマイナンバーカードの用いたワ方式による認証を採用済み。

■ 現状の課題

課題	内容
認証レベルとユーザビリティの観点でのガイドライン/基準	自社の決済サービスにおける認証方式や他社の決済サービスへの口座紐づけ可否は、それぞれ判断を行っている。こうした対応のガイドラインや基準を今後どのようにしていくかが重要。
属性情報の取得	口座開設時期により携帯番号・メールアドレスが未登録である口座があり、共通した認証を行うことが難しい。
非対面(非対人)の限界	WEB普及、ペーパーレス化など自社の省力化によりWEBを活用した非対面での対応範囲が拡大しているが、高齢層の多くはWEB完結させることに難しい面が多く、また手続自体が高度化していることから、店舗設置やコールセンターでの人による対応が引き続き必要。
ユーザビリティとセキュリティ	犯罪行為自体が高度化する中でより高セキュリティの認証方法が求められている。逆に営業面からは簡素であればあるほど良い。営業的側面で負荷が発生しているケースも見られる。

サマリ

- オンラインにおいて、弊行での口座開設を担う「スマート口座開設」アプリ、
  資金決済サービスを提供する「三菱UFJ銀行」アプリ・三菱UFJダイレクトが対象
  - 「スマート口座開設」アプリで口座開設申し込み時にKYCを対応
    - eKYC認証（ホ方式とヘ方式を選択可能）、社内システムによるリスク評価を実施
    - 偽造の本人確認書類を用いた口座開設申し込みへの対策として、過去の申込時の容貌画像を活用することで、
      事務センターにおいて人手で重点的に点検。また、端末使いまわしへの対策として、SMS認証を導入済
  - 「三菱UFJ銀行」アプリでの振込にあたっては、口座情報を元に当人認証の上、三菱UFJダイレクトの利用登録、
    ワンタイムパスワードの利用登録を実施。当人認証では、各種認証を組み合わせ、取引毎に必要と考えるセキュリティ強度を確保
- CBDCシステムを検討する上で想定される論点
  - 認証・KYCに係る仕様の観点
    - 第2回会合の内容も踏まえると、CBDCにおいて、認証・KYCに係る仕様を共通にするか、各仲介機関で個別に決定するかは論点となりうる。共通仕様とする場合は、認証アプリや認証APIを中央システムで用意し、仲介機関システムが呼び出す仕様も想定される
    - 政府が官民ともに利用促進を続けている公的個人認証は、検討スコープに入れるのがよいと考える
    - 認証情報を忘れた場合にオンラインで復旧できる仕組みの整備により、利便性を高めることが望ましい
  - 不正利用への対策の観点
    - CBDC口座は、既存の銀行預金口座や既存の決済アカウントに紐づける想定。決済事業者と銀行の認証・KYCに関する強度に差分がある場合、平仄を合わせる必要があると考える
    - CBDC口座の不正利用（だまされた本人が送金操作したケース、ハッキングによる資金詐取のケースなど）への対策、
      補償についての責任分界点は論点となりうる。想定される登場人物は、仲介機関、CBDCシステム、日銀など

MUFG