2024 年６月 26 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８回会合の議事概要

１．開催要領

（日時）2024 年５月 24 日（金）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

大日本印刷株式会社、フェリカネットワークス株式会社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）ＣＢＤＣシステムにおけるＫＹＣおよび認証・認可のあり方①（大日本印刷株式会社）

――　プレゼンテーション資料は別添１を参照。

本プレゼンテーションでは、第７回会合まで整理してきた現状のｅＫＹＣの各方式をもとに、リスク、ユーザビリティ等を踏まえて、ＣＢＤＣシステムにおけるｅＫＹＣの実施方式やその特徴、留意点、あり方等について整理する。

日本銀行が公表している「中央銀行デジタル通貨に関する連絡協議会 中間整理」（2022 年５月）によると、ＣＢＤＣが具備すべき基本的な特性として、ユニバーサルアクセス、セキュリティ、強靭性、相互運用性、即時決済性が挙げられている。この中で、本ＷＧに関係が深いユニバーサルアクセスおよびセキュリティの観点から説明を行う。

まず、ｅＫＹＣの代表的な４つの方式であるホ方式（本人確認書類の撮影＋容貌の撮影）、ヘ方式（本人確認書類のＩＣチップ読み取り＋容貌の撮影）、ト（１）方式（本人確認書類の撮影またはＩＣチップ読取＋金融機関の保有する顧客情報の照会）、ワ方式（公的個人認証・マイナンバーカードのＩＣチップ

読み取り＋暗証番号）について改めて確認すると、これらは今後も基本的な身元確認方法として位置づけられると考える。

次に、ＣＢＤＣにおいて身元確認を実施する場面を整理すると、①口座開設時のほか、②払出・受入および送金、③登録された個人情報変更、④スマートフォンの機種変更後の当人認証の再設定といったリスクが高い取引や手続きを行う時が想定できる。①は、不正な口座開設を防ぐ観点から原則身元確認が必要と考えるが、サービス設計によっては、身元確認を行わなくともよいケースも考えられるだろう。②は金額や送金先などにリスクや懸念がある場合に、③④は重要な項目等が変更される場合に、身元確認を改めて実施することが考えられる。

一方、身元確認は、操作の煩雑さや本人確認書類の審査時間などから、その実施回数が増えるほどＣＢＤＣ利用時のユーザビリティの低下につながることが懸念される。そのため、各取引や各手続きにおけるリスクについて、不正発生時の「被害の程度」、「責任の所在明確化」、「サービスとしての信用低下」等を踏まえた評価を行い、身元確認の実施要否、実施方式を適切に決めることが必要だろう。

続いて、ＣＢＤＣが具備すべき基本的な特性のうち、ユニバーサルアクセスの観点からｅＫＹＣを考える。現行のｅＫＹＣの各方式には、それぞれ課題があり、「誰でも使える」ユニバーサルアクセスを実現することは簡単ではない。例えば、ｅＫＹＣを実施するためには、ヘ方式やワ方式の場合はＩＣチップの読み取りが可能なスマートフォン端末を持つ必要があるし、ト（１）方式の場合は銀行口座を持つ必要がある。他にも、ｅＫＹＣに利用できる主要な本人確認書類を保有していることや、自らスマートフォン等の端末を操作しｅＫＹＣを実施できるＩＴリテラシーがあることなどが挙げられる。より多くのユーザーがｅＫＹＣを利用できるようにするためには、ｅＫＹＣで使える本人確認書類の網羅性を高めることや、ユーザーに対するサポート体制を充実させることが考えられるだろう。なお、マイナンバーカードはデジタル庁が利用を促進しており、関係省庁の方針・動向を注視することは重要だろう。また、ＵＩ／ＵＸも重要であり、情報をわかりやすく視覚化したインフォグラフィックスや、あらゆる人が利用しやすいユニバーサルデザインによってユーザーが直感的に使えることも重要だろう。

さらに、ＣＢＤＣが具備すべき基本的な特性のうち、セキュリティの観点からｅＫＹＣを考える。ＣＢＤＣを「安心して使える」ようにするためには、Ｃ

ＢＤＣの機能とリスクを踏まえて、適切な強度の身元確認方法を定める必要がある。例えば、セキュリティを高めるためには、ワ方式に容貌撮影を加えることも考えられる。こうした身元確認方法は、犯罪収益移転防止法（以下、犯収法）など関連しうる法令や不正利用の動向などを見ながら、適時適切に見直していく必要がある。また、不正利用による具体的な影響は何があるのかの検証をもとに、リスクの評価方法やその基準について検討が必要だろう。

最後に、これまでの会合での議論を踏まえると、ＣＢＤＣにおける身元確認方法の共同化のあり方については、①共同化せずに仲介機関ごとに個別に決定、②仲介機関のためのガイドライン等により仕様や基準を統一、③共同センター化、の３パターンが大きく考えられる。①共同化せずに仲介機関ごとに個別に決定する場合は、仲介機関が従前から利用する既存システムが活用可能であるものの、仲介機関間で身元確認レベルに差が出ることによるセキュリティリスクが課題となりうる。②仲介機関のためのガイドライン等により仕様や基準を統一する場合は、各仲介機関における開発内容が明確になるものの、（既存システムにはない機能の追加が必要な場合には）追加開発コストが必要になることに加え、ガイドライン制定にかかる検討が必要になるだろう。③共同センター化の場合は、仲介機関各社のコストが抑えられ参入しやすくなる可能性があるが、仲介機関を跨ぐ個人情報の取り扱いをどうするかや、責任の所在を明確化することなどが課題となりうる。それぞれに良い面と悪い面があるが、ユニバーサルアクセスやセキュリティの観点を踏まえつつ、検討していくことが必要になると考える。

（２）ＣＢＤＣシステムにおけるＫＹＣおよび認証・認可のあり方②（フェリカネットワークス株式会社）

―― プレゼンテーション資料の要旨は別添２を参照。

ＣＢＤＣにおける認証・認可について、認証を中心に過去７回の会合の議論を振り返り、考慮事項をまとめた上で、標準化やガイドラインの方向性について、いくつかの想定パターンを整理・提示し、議論に繋げていきたい。

ＣＢＤＣは安心安全に誰にでも使えることが求められ、仲介機関、追加サービス事業者等からの追加サービス連携も含めた多様なサービスの提供が想定される。そのため、ＣＢＤＣには様々な認証パターンが考えられることから、認証方式を一律とすることは難しく、各サービスの内容・リスクに応じて、セキュリティとユーザビリティのバランスを考慮した上で、認証方式を適切に

選択し、正しく実装することが必要と考える。

説明の前提として、認証・認可の定義と分類を行う。認証は、ユーザーの登録済み情報を用いて、サービスの利用を行う対象がユーザー当人であることを確認する当人認証（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を指し、認可（Ａｕｔｈｏｒｉｚａｔｉｏｎ）は、あるサービスのリソースに対して、別のサービスがアクセスできる権限を与えることを指す。次に、ＣＢＤＣにおいて当人認証がどのエンティティ間で実施されるかについて４つのケースに分類した。当人認証は、①「仲介機関のサービスを利用する際のユーザーと仲介機関間」、②「追加サービスを利用する際のユーザーと追加サービス提供事業者間」、③「追加サービス連携（登録）にあたっての、ユーザーと仲介機関間」で行われ、認可は、④「追加サービス利用にあたっての、追加サービス事業者と仲介機関間」で実施される。また、スマートフォンアプリの利用を前提に当人認証のタイミングを整理すると、口座開設時に認証方式の設定を行った後のアプリへのログイン時、残高照会時、送金等の取引時、追加サービスへの連携やログイン時、端末変更時、口座解約時等、様々なタイミングが想定される。スマートフォンアプリの利用以外のケースとしてＰＣからの利用時や対面時での対応等を考慮すると、更に検討すべき当人認証のバリエーションは広がると考える。

次に、過去７回の会合での議論を振り返り、各回で行われた認証・認可に関する議論を整理した結果、①セキュリティの重要性、②セキュリティとユーザビリティのバランス、③標準化・ガイドラインの必要性、④システム共同化の可能性、の４つを重要な観点として改めて共有する。①セキュリティの重要性では、ＣＢＤＣは安全なサービス・システムの提供にあたり、認証におけるセキュリティ確保のために適切な認証保証レベルと認証方式を選択・利用することが求められるとの意見のほか、フィッシング耐性の強い認証方式の適用の必要性や、多要素認証が必要となる当人認証保証レベル２の適用について言及があった。②セキュリティとユーザビリティのバランスでは、ユニバーサルアクセスの観点で、あらゆる属性の人が利用することを考えた場合、ユーザビリティも重要であり、サービス内容に応じてセキュリティとユーザビリティの適切なバランスが求められるが、どのレベルが適切か判断することが難しく課題である、との意見があった。③標準化・ガイドラインの必要性では、仲介機関や追加サービス提供事業者等の間で、一定のセキュリティレベルを確保したり、サービスやユーザビリティとセキュリティのバランスを確保するために、何らかのガイドラインを作成し、継続的にメンテナンスすることが

望ましいという意見があった。④システム共同化の可能性では、ユーザーの当人認証を主として行うことが想定される仲介機関にとって、認証関連のシステムやサービスの導入・運用コストの負担は課題であり、コスト負担軽減の観点から認証関連のシステムを共同化することも選択肢として考えられるとの意見があった。

これらを踏まえ、本日の議論の論点として、「ＣＢＤＣの当人認証に関する標準化・ガイドラインの位置づけと記載レベル」、及び「標準化・ガイドラインの発行主体の考え方」の２点を挙げる。

議論に先立って、参考事例や、考慮事項・見解を含めて説明する。まず、参考事例としてモバイルＦｅｌｉＣａサービスにおける標準化・ガイドラインの事例を共有する。当該サービスの提供にあたっては、駅等に設置してあるリーダ・ライタ端末のシステム開発者向けや、スマートフォン等の端末開発者向け、スマートフォン搭載ＩＣチップ開発者向け、サービス事業者向けに、それぞれに標準仕様・ガイドラインを制定している。これらが互換性を保つ上で重要な役割を担っていると考えている。ただし、標準仕様・ガイドラインの作成とその後のメンテナンスには多くのリソースを必要とするものの、直接収益を生むものではないため、作成の意図・目的が果たされるように意識して取り組む必要があると考えている。

次に、標準化・ガイドラインの作成における考慮事項・見解として４点挙げる。①記載内容が抽象的になれば個社・実装依存の部分が多くなり、共通化という本来の目的が果たされなくなる可能性がある一方で、具体的に定めると内容や仕様についての関係者間の意見が分かれ、合意形成が難しくなる可能性がある。記載内容の具体性の度合いについて、どのようなバランスとすべきかが課題となるだろう。②作成した標準仕様とガイドラインを多くの関係者が利用するための取り組みとして、実際のサービスやシステムが準拠して開発・運用されるように、法的・制度的な強制や業界自主規制、明確な準拠メリット等が必要になると考える。③正しく準拠しているかを確認・検証するためのスキームとしてチェックリスト等の何らかの確認手段とその確認結果をステークホルダーや第三者が検証する枠組みが必要だろう。④標準仕様・ガイドラインのリリース後に見つかった改善・修正すべき点や、技術進歩・市場環境変化を踏まえた見直し等によって、定期的なメンテナンスは必要であるが、作成・メンテナンスに関わる団体の体制の維持、知識・ノウハウの継承が課題になるだろう。

続いて、システム共同化関連での考慮事項・見解を挙げる。システム共同化は、一般的にはコストメリットや、仕様・実装が統一されるメリットがあると

考えられるが、メリットの最大化を図るには関係者の多く、できれば全員の利用が望ましいだろう。ただし、共同化の範囲や仕様次第では、参加企業の既存システムや業務仕様への影響が大きくなる場合もあるため、バランスを考慮する必要がある。また、利用者が多いと、各種の合意形成が課題となるケースが多いため、利用者間でのコスト負担の配分の根拠や、機能追加や拡張等の仕様変更における合意・決定プロセスを予め定めておくことが望ましいと考えている。

さらに、ＣＢＤＣにおける当人認証の特徴と考慮事項、ガイドラインの目的について整理する。高い安全性が求められるＣＢＤＣにおいて、各取引の起点となる当人認証は不正利用等の攻撃対象として狙われやすい箇所であり、高いセキュリティが必要である。幅広い人々に広く利用されるためには、当人認証によるユーザビリティ・ＵＸの低下をできるだけ軽減することが重要である。ＣＢＤＣは、複数の仲介機関や追加サービス提供事業者等が、それぞれ多様なサービスを提供することが想定され、求められる当人認証のレベルや、認証方式も多様になる可能性があるだろう。次に、想定するガイドラインの目的については、大きく３点に整理した。１点目は、ＣＢＤＣ全体のセキュリティレベルの維持のためである。ＣＢＤＣには、多様な仲介機関や追加サービス提供事業者の参加が想定される中、セキュリティの弱い部分を作らずに全体のセキュリティレベルを維持するために必要と考えている。２点目は、サービスレベルとユーザビリティについて一定の共通化を図るためである。例えば、一定額以上の取引の際には、追加の当人認証が必要になり、その際の認証方法はどうするかといったユースケースやその際のセキュリティとのバランスについての考え方を揃えるためである。３点目は、各仲介機関・追加サービス提供事業者の負荷軽減のためである。業界や有識者の知見や検討結果を共有し、個々での検討や対応を減らす意義があると考える。

最後に、本日の議論の論点について整理する。１つ目の論点の、「標準化・ガイドラインの位置付けと記載レベル」における「位置付け」は、順守する要求度合いの強い順に「必須要求事項」、「推奨事項」、「参考情報」と分類し、「記載レベル」は、具体性の高い順に「技術仕様レベル」、「要件レベル」、「考え方レベル」と分類する。これらを組み合わせると、マトリクス上は９つのパターンに分けられる。議論においては、どの組み合わせのパターンを目指すのかによっても大きく方向性が異なるため、目線を合わせた上で議論を進められるよう組み合わせパターンで実際に考えられる例を提示させていただいた。次に、２つ目の論点の「標準化・ガイドラインの発行主体の考え方」について整理する。発行主体の候補は大きく３つ考えられ、一つ目の候補は公共機関であ

る。政府や日本銀行、その他公共機関が発行主体となり、民間の組織・団体や有識者の協力の下、作成・改定を実施していくことが考えられる。二つ目の候補は、民間の組織・団体である。ＣＢＤＣの仲介機関となりうる企業が主な構成者である業界団体や、キャッシュレスやセキュリティ等に関する民間の団体・組織が発行主体となることが考えられる。最後の候補は、ＣＢＤＣに関する新組織・団体である。ＣＢＤＣは新たなサービスであり、ステークホルダーも多岐に亘るため、新たにＣＢＤＣに関する新組織・団体を組成し、発行主体となることも考えられるだろう。

なお、今回提示した想定やパターン等はあくまでも例であり、標準化・ガイドラインの方向性等を決定付けるものではないが、今後、各サービスのユースケースごとに、セキュリティとユーザビリティのバランスを考慮した認証保証レベル、認証方式についてＣＢＤＣとして求められる要件について議論を進めていくにあたり、ＣＢＤＣとしての当人認証に関する要件のあり方・方向性について関係者の認識を合わせておくことで、より効果的に議論を行うことができると考える。

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、セコム株式会社が担当した。概要は以下のとおり。

【セキュリティとユーザビリティを考慮した身元確認】

（参加者）セキュリティを重視するあまり、必ずしも必要ではない取引や手続きにおいて身元確認を改めて実施し、結果としてユーザビリティの低下を招く可能性があると認識している。このような事態を避けるためには、身元確認のあり方をどのように考えるべきか。

（参加者）ユーザビリティとセキュリティは表裏一体の関係にある中で、身元確認のプロセスを安易に増やせばユーザーの使い勝手が悪くなり、サービスを利用してもらうという本来の目的を失ってしまう可能性がある。こうした事態を避けるために、取引や手続きごとに不正発生時のリスクを評価した上で、セキュリティを重視し過ぎていないか、ユーザーの使い勝手が悪化しすぎていないかを踏まえて、身元確認が追加で必要かを判断すべきと考えている。

【ｅＫＹＣにおけるリスクと対策】

（参加者）現状、リスクに応じて身元確認の要否を変更しているケースはあるか。また、ｅＫＹＣの各方式は、なりすましリスクに差があると理解しているが、各方式のリスクに応じて提供する方式を切り替えることはあるか。

（参加者）例えば、送金では一定以上の金額の場合にリスクが高いと判断し、改めて身元確認を行うケースがありうるだろう。また、ｅＫＹＣの各方式の提供にあたっては、事業者がリスクに応じて切り替えるのではなく、事業者が提供する複数のｅＫＹＣの方式の中から、ユーザーが自由に選択している印象である。ｅＫＹＣの各方式が不正に突破されるリスクに対しては、追加の確認や最新技術などを駆使しながら対策を行う必要があるだろう。

（参加者）ｅＫＹＣによる身元確認について、必ずしも全ての不正を見抜けているわけではない現状を踏まえると、セキュリティ水準の高低を考える上では、ＣＢＤＣを不正に利用された際にユーザーにどの程度の被害が生じうるかが、重要なポイントになると考えている。本ＷＧにおけるこれまでの議論でも触れられてきたが、例えばＣＢＤＣでの取引は５万円など少額取引に限るとするのであればリスクは限定的であり、ＣＢＤＣの利用にあたっては身元確認がそもそも不要といった整理も考えうる。このように、ＣＢＤＣの提供のあり方次第で、セキュリティの適切な水準は大きく変わりうると考えている。

【ＣＢＤＣの払出・受入・送金時のリスクや留意点】

（日本銀行）第７回会合で本人の口座間の取引であれば、低リスクとして当人認証を簡略化できるかもしれないと意見があったが、例えばＣＢＤＣの払出・受入が仮に自身の預金口座と自身のＣＢＤＣ口座間の価値移転だとした場合は、どのように考えるか。また、ＣＢＤＣの送金において、実務的な観点からリスクがどこにあるのか、現状での各社の取引実態を踏まえて、留意点を伺いたい。

（参加者）１点目について、同一の銀行に預金口座とＣＢＤＣ口座を持つ場合の払出・受入であれば、同一の銀行に複数の口座を持つ同一人の口座間の振替と近いと思われるので、同様に低リスクとして取り扱いを検討できるだろう。

（参加者）２点目について、取引金額の観点では、犯収法において 10 万円を超える現金による振込時には本人確認を含む取引時確認が必要とされていることから、ＣＢＤＣでの送金においても同額が本人確認等を行う目線の一つになるだろう。同一名義人間の取引の観点では、同一名義人であるかの一致確認が課題となるだろう。銀行振込においては、振込先が他行の同一名義人口座の場合でも、振込元の銀行が全銀システムを介して確認できるのは振込先の名義人のカナ氏名であるため、同姓同名の別人の可能性も残り、基本的には通常の他行宛て振込と同様に取り扱う必要がある。ＣＢＤＣにおいても、送金元と送金先の仲介機関が異なる際に、名義人が同一人であるかが確認できないのであれば、他人宛ての送金と同様に対応することが基本的な考え方になるだろう。

また、ＣＢＤＣは、その公的な位置づけからユニバーサルアクセスは重要だと考えるが、かといって全ての人が全く同じサービスにアクセスする必要はないのではないか。例えば、最近ではＳＮＳ型投資詐欺で騙される方、特に高齢者が多くなっている現状を踏まえると、お客さまの資産を守るために、高額振込ができる機能を誰でも簡単に利用できるユニバーサルアクセスとする必要があるかは考えるべきで、犯罪被害を防ぎ、ユーザーを守るためには簡単にはアクセスさせないことも重要な視点だろう。

ＣＢＤＣが目指し、提供するものが何か次第ではあるが、機能別に段階を分けて提供するのも一案と考える。例えば、デビュー、ノーマル、プロと段階を分けて、１段階目のデビューでは身元確認不要だが 10 万円以下の少額取引に限るとし、小学生や高齢者を含めて幅広い人々が使えるようにする。２段階目のノーマルでは、上限金額の引き上げなど機能が拡張されるが、段階を上げるには身元確認が必要となる。３段階目のプロでは、一定の経験や基準を超えてプロに相応しいと認められることによって、機能が一層拡張する。ただし、どのような人であれば問題が生じないかの基準を見極めることは難しいだろう。一案ではあるが、このようにして全ての機能を全てのユーザーが使えるようにするのではなく、段階に応じて機能を限定して提供すると割り切ることは、犯罪被害を防ぐためには重要な観点の一つだろう。

【共同センター化の課題】

（参加者）共同センターを設立し、共同センターがｅＫＹＣによる身元確認を集中して担うとした場合の課題について意見を伺いたい。

（参加者）共同センター化は、各社が個別に取り組みをすることに比べ、一般的にはコスト面でのメリットがあると考えるが、責任分界をどう整理するか、運営主体をどのようにするかが課題になると考える。責任分界の整理については、関係者間でのリスクの範囲が明確になることによって、各社がどのようにリスクを取りながら事業を運営していくかを検討する上で重要になるだろう。運営主体については、共同出資など様々なやり方が考えられるが、どのような主体が主導するのか、民間だけでやるのか、多数の関係者がいる中で合意形成はどのようにしていくのか等が課題になると考える。

（参加者）共同センター化については、コストを抑えつつ集中して処理することで情報の蓄積が進み、不正検知の精度を高められるのであれば、大きなメリットがあると捉えられるだろう。

（参加者）ユーザーの情報の取り扱いに関しては、プライバシー保護を念頭に、事前にユーザーの同意を得るなどのルール作りが必要と考える。

（参加者）ｅＫＹＣを共同化して共同センターのような機関が集中して実施する場合の課題を考えると、当該ｅＫＹＣを不正に潜り抜けた事例のデータ収集が簡単ではないことが挙げられる。ｅＫＹＣサービス提供事業者とそのサービスの提供先は別のエンティティであることから、サービスの提供先がｅＫＹＣを不正に潜り抜けた事例として認識した後に、そのデータをフィードバックとしてｅＫＹＣサービス提供事業者に対して、どの段階でどのように情報共有できるかは、個人情報でありプライバシーにも配慮した整理が必要だろう。また、積極的にフィードバックが進む仕組みやどのような機関が共同センターを運営するかについても、検討が必要になると考えている。

【ｅＫＹＣのユーザーインターフェース】

（参加者）ｅＫＹＣのユーザーインターフェースの見易さやわかりやすさは、ユーザーに対してどのような影響を与えるだろうか。

（参加者）ｅＫＹＣの手続きの中では、ユーザーに対して特定の動作を実施してもらう必要が生じる場合があり、わかりやすく伝えられないと、ユーザーが手続きを断念する要因となりうる。例えば、本人確認書類の厚みを撮影する動作は、ユーザーが日常的に行うことがほとんどないために、手続

きを理解した上で正しく撮影ができるかは、難易度が非常に高いと認識している。こうした案内をユーザーに直感的に理解してもらえるように伝えられるかが重要であり、各社は常日頃から工夫を凝らしている。インフォグラフィックスやユニバーサルデザイン（別添１、９頁）もその一例として参考になるだろう。

（参加者）仲介機関ごとの実装によって操作画面や手続きの案内が異なれば、ユーザーに混乱をきたす可能性があるため、こうしたユーザーインターフェースについても一定の標準化が進むと良いのではないだろうか。

【ユニバーサルアクセスを考慮した身元確認】

（日本銀行）本ＷＧでは非対面でのｅＫＹＣによる身元確認の手続きを優先的に議論してきたが、ユニバーサルアクセスを踏まえた際に、ｅＫＹＣでの手続きが様々な事情により難しい人々も一定数いると考えられる。そうした人々に対して、どのように身元確認を実施するかについて、各社の実務に照らし合わせてフィージビリティがあるのか、ご意見を伺いたい。

（参加者）金融機関は窓口での手続きを非対面でもできるようにデジタル化を進め、実店舗のあり方を見直して来た経緯がある。また、仲介機関を担いうるインターネット専業銀行や資金移動業者等は、そもそも店舗を構えていない。こうした現状では、ユニバーサルアクセスとして、誰でも対応できるように対面での手続きを含むサービス設計とすることは簡単ではなく、何らかの割り切りを検討する必要があるのではないか。加えて、仮に金融機関が対面での手続きに対応したとしても、金融機関が近くにない地域も想定されることから、ユニバーサルアクセスが全ての地域において必ずしも実現されるわけではないだろう。以上を踏まえた上でもなお、仲介機関に対面での手続きに対応することを求める場合には、対面での手続き対応のコストを賄う何らかのインセンティブや意義を提示することが重要だろう。

（参加者）仲介機関に対面での手続きに対応することを求める場合は、仰るとおりの何らかのインセンティブ等がなければ、仲介機関が対応することは大変厳しいだろう。そもそも、国内においては、厳格化されたとはいえ身元確認ができれば比較的容易に銀行口座は開設でき、また資金移動業者のアカウント開設も容易な中、ユニバーサルアクセスの観点も含めて、ＣＢＤＣがどこを目指して何を目的に利用されるかについて議論を深める必要

があるだろう。先程も言及されたが、例えば 10 万円以下であれば身元確認も行わずに誰でも使えるようにし、それ以上の金額を利用するのであれば一定水準の身元確認としてｅＫＹＣが求められる設計とすることは、ユニバーサルアクセスを一定程度確保しながら、ＣＢＤＣを提供できるシンプルな解決策の一つであると考える。

【標準化・ガイドラインのデメリット等】

（参加者）これまでの会合では、標準化・ガイドラインが必要という意見が多い認識だが、デメリットや作成したことでむしろ苦労した経験等があれば伺いたい。

（参加者）標準化・ガイドライン自体は役立つものとして作成されている認識だが、実際には適切に活用されていないケースは往々にしてありうるだろう。

（参加者）ＣＢＤＣの検討が各国で進められる中、海外で国際的な標準仕様が制定されれば、日本も準拠せざるをえなくなる可能性もある。過去にもＦｅｌｉＣａ方式の採用を巡ってＩＣカードの国際標準が成立していたかが問題になった事例もあり、予め国際的な標準化の動向を見据えて、国際協調や、時には日本としての意見を纏めて提言することも重要と考える。

（参加者）国際的な標準化の話もあったが、本ＷＧでの議論における「ＣＢＤＣ」や「認証の標準化・ガイドライン」とは、国内または国際的な標準のどちらを指すだろうか。

（参加者）どちらも国内に限ったものと認識している。また、標準化は認証の技術面に関する部分が主となり、ガイドラインはサービスの提供品質のような業務的な内容も含まれるとイメージしている。

【標準化・ガイドラインに付属するチェックリストの留意点】

（参加者）標準化やガイドラインを策定した際に、順守しているかをわかりやすく確認するために、チェックリストが制定されることがある。こうした際に、チェックリストを埋めることが目的化してしまう経験が往々にしてあるので留意が必要である。本当のリスクはどこにあるのかを考えて対応をしなくてはならない。また、技術的なセキュリティをどれほど高めたとしても、結局は人間が使うものであるために、技術的な要因ではない詐欺

等により犯罪被害が生じうる。標準化で定める技術的なセキュリティのレベルを徒に高める必要はないものの、技術的なセキュリティが優先的に狙われない程度の水準で高い必要があるだろう。技術は発展するので、状況に応じた見直しを関係者間での合意形成を進めながら、常に行っていく必要があるだろう。

【標準化・ガイドラインの作成上の留意点】

（参加者）現在の認証における標準仕様のパターンは非常に多く、各事業者が全ての標準仕様へ対応することは困難だろう。ＣＢＤＣにおいては、標準仕様やガイドラインを作成した場合は、それらを踏まえた上で、各事業者がどのように実装していくかも合意形成をした方が良いと考える。そうしなければ、各社はそれぞれ標準に沿う形で対応していたものの、実際には微妙な実装上の差異が生じ、結果として齟齬が生じる事態がありうる。特に、アプリの仕様や、利用者の認証情報の連携をする場合に留意が必要と考えている。

（参加者）海外のとあるサービスにおけるガイドラインでは、ユースケースに応じて、例えばＯｐｅｎＩＤ　Ｃｏｎｎｅｃｔ等への参照を具体的に記載しているケースがあり、こうしたやり方は実装上の差異を防ぐのに有効な工夫であろう。

【標準化・ガイドラインの発行主体】

（参加者）日本銀行は、標準仕様やガイドラインの作成の主体となりうるか。

（日本銀行）ＣＢＤＣが発行される場合、日本銀行はその発行主体となるため、関連したガイドライン等が作成される際には何らかの形で関与することも想定されるだろう。ただし、どのような形でどういった関与度合いが適切かは、関係者の皆さまのご意見を是非伺いたいと考えている。

（参加者）米国では、民間団体が標準仕様を作成し、後から政府がお墨付きを与えることで、標準仕様に準拠することへの強制力を持たせつつ、技術の進歩や状況の変化に応じて、民間ならではのスピード感や柔軟性をもって対応するという、官民の良いところをうまくバランスさせた事例があるので、こうしたやり方もありうる事例として、参考までに共有させていただく。

４．次回予定

次回の会合は７月５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８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

別添1
大日本印刷株式会社

Confidential

CBDCフォーラム WG3 第８回

DNP
未来のあたりまえをつくる。

2024/5/24
大日本印刷株式会社
情報イノベーション事業部
第1PFサービスセンター
デジタルトラストプラットフォーム本部
企画開発第１部

目次

Confidential DNP

第８回のテーマ

現状整理したKYCおよび認証・認可の各方式をもとに、リスク、ユーザビリティ等を踏まえて、CBDCシステムにおけるKYCおよび認証・認可の実施方式やその特徴、留意点、あり方等を整理する

CBDCシステムが具備すべき基本的な特性について

Confidential

DNP

CBDCが具備すべき基本的な特性

ユニバーサルアクセス
ＣＢＤＣを「誰でも使える」ものとするためには、送金・支払を行う際に用いる端末、カード等の利用対象者を制限することがないよう、簡便性や携帯性に関する設計面での工夫が必要となる。

「誰でも使える」
未成年者、高齢者、
利用可能端末など

セキュリティ
ＣＢＤＣを「安心して使える」ものとするためには、偽造抵抗力を確保し、各種不正を排除するよう、セキュリティを高める取り組みが必要である。

「安心して使える」
AML/CFT、なりすまし不正、
個人情報の保護など

「中央銀行デジタル通貨に関する日本銀行の取り組み方針」より

犯収法に則った代表的なeKYCの手法について

Confidential

DNP

『ホ方式』　本人確認用画像情報+本人確認書類の画像

当該顧客等の容貌の写真　＋　写真付本人確認書類の画像情報

『ヘ方式』　本人確認用画像情報+ICチップ情報

当該顧客等の容貌の写真　＋　写真付本人確認書類のICチップ情報

『ト方式』　本人確認書類の画像またはICチップ情報と銀行等への照会

本人確認書類の画像又はICチップ情報送信

銀行・クレジットカード会社

銀行等による顧客情報を照会

『ワ方式』　マイナンバーカードのICチップ情報（公的個人認証サービス）

マイナンバーカードの電子署名用証明書の暗証番号

PF事業者、J-LIS

J-LISへの照会

身元確認の実施が想定されるケースについて

一般的には、身元確認と当人認証は活用場面が異なるものであるが、取引や手続のリスクによっては改めて身元確認を実施（併用含む）するケースが考えられる。

取引/手続き	想定される状況
口座開設	不正な口座開設を防ぐため、原則身元確認が必要。 CBDCの利用用途、匿名での利用形態によっては不要な場合も考えられる。
払出/送金/受入	送金金額、送金先などにリスク・懸念がある場合に実施。
属性の変更 （継続的顧客管理）	姓、住所等の変更時には、入力された情報が正しいかどうかの確認のために実施することが考えられる。
登録された 個人情報の変更	当人認証に用いる認証方法によっては、変更時に身元確認を行う場合があり得る。 ※個人情報の変更によって、設定された認証方式や認証の通知先が変更となる場合など
機種変更や 当人認証の再設定	当人認証方法やそのセキュリティレベルによっては、なりすまし操作のリスクがあるため。

身元確認の実施におけるデメリットとして、操作の煩雑さ、本人確認書類の不携行、審査に要する時間などにより、CBDC利用時のユーザビリティが損なわれることが挙げられる。CBDCシステムが持つ機能を踏まえて各取引/手続きにおけるリスクの評価が重要となる。

不正発生時の「被害の程度」、「責任の所在の明確化」、「サービスとしての信用低下」等を踏まえリスクの評価を行い、身元確認実施要否、実施内容を決める必要がある。

「誰でも使える」

現行eKYC手法の採用にあたっての課題として以下のようなことが挙げられ、「誰でも使える」のは難しい。

・ヘ方式、ワ方式を検討する場合、ICチップの読み取り可能なスマホ端末が必要になる。

・ト方式を検討する場合、口座やアカウントを持たないユーザー（未成年等）のCBDCシステムの利用について考慮が必要。

＜利用できないユーザーとして考えられる例＞

項目	利用できないユーザー
銀行口座	口座を持たない（持てない）ユーザー
エンドポイントデバイス	スマホを持っていないユーザー、IC情報を読み取れないスマホを持っているユーザー
身元確認書類	代表的な本人確認書類（マイナンバーカード・運転免許証）を持たないユーザー
ITリテラシー、セキュリティ	操作方法を理解できないユーザー、個人情報の取扱いを気にするユーザー
操作UI	個別のサポートを必要とするユーザー

「誰でも使える」

eKYC手法採用において考慮すべき点について

・運転免許証（16歳以上）やマイナンバーカードにしても、普及率は十分とはいえず、代表的な本人確認書類を持たないユーザーが存在する中で、CBDCシステムとして、どこまで網羅するべきか、議論が必要。

・デジタル庁がマイナンバーカードの取得・利用拡大を促進。法令に準拠する場合、マイナンバーカードの利用が必須となる可能性がある。CBDCシステムにどこまで機能（送金先）・制約（保有残高、送金限度額など）を持たせるかにも関わるものとなるため、関係省庁の方針・動向のキャッチアップが重要となる。

・個別のサポートを必要とするユーザーへの対応方針（音声、KYC等）の検討要否について議論が必要。

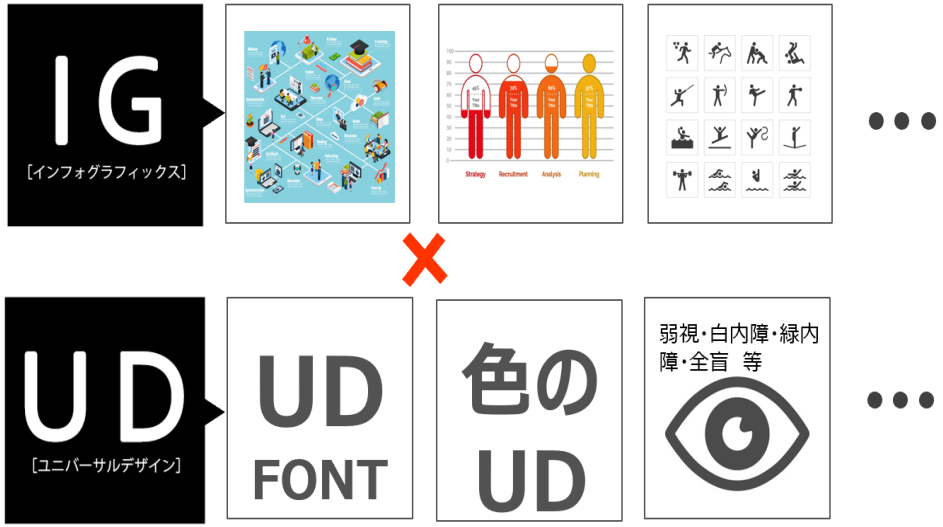
ディスカッションポイント

CBDC口座開設や開設後の利用時における身元確認操作において、採用する身元確認方法、準拠する法律、操作を非対面のみとすることによって、利用者が限られてしまう。
カバー（採用）が必要な本人確認書類、対面取引の有用性などをどのように考えるか。

「誰でも使える」

eKYC手法１つとっても、その実装方法によってユーザビリティ、ユニバーサルアクセスのレベルは異なる。
例：容貌撮影で顔を傾ける or まばたきする、操作画面の色合いやレイアウトなど

※ユーザーデバイスのUI/UXに関しては、別のWGで議論



IGUD

インフォグラフィックス × ユニバーサルデザイン

IGUDは、インフォグラフィックス（情報を視覚化したデザイン）とユニバーサルデザイン （あらゆる人が利用できるデザイン）を掛け合わせたDNP独自のメソッドです。

「安心して使える」

・CBDCシステムに持たせる機能とリスクを鑑み、身元確認・当人認証の方法を決定する必要があると考えるが、安心して利用するには、相応の確認・認証が必要と考える。

・当人認証の方法は不正等の動向を見つつ、身元確認方法は、変更・追加していく必要がある。

・身元確認方法は、犯収法への準拠が基準になるが、セキュリティとして万全ではない。
例えば、ホ方式は、運転免許証の偽造による不正利用、ワ方式はマイナンバーカード紛失による不正利用の懸念があるため、安全面からは犯収法＋αの実装も十分に考えられる。（ワ方式＋容貌撮影など）

・申込等身元確認操作時における問い合わせサポート体制の検討。対面窓口の検討。

・一定の水準のセキュリティレベルを持ったシステムの構築。

ディスカッションポイント

不必要な身元確認の実施（ユーザビリティの低下）を避けるため、CBDCシステムにおける操作/手続きにかかるリスクの評価をする必要がある。
不正による具体的な影響には何があるかをもとに、リスク評価方法、基準について、議論する必要がある。

「安心して使える」

・身元確認手法としてのセキュリティ性以外で考慮すべき「安心して使える」観点としては、システム（身元確認審査業務含む）としてのセキュリティ性があげられる。

【個人情報保護】 

【情報セキュリティ(ISMS)】 

【事業継続(BCMS)】 

【品質】 

【環境】 

❶信頼性

- 24時間365日対応
- BCMSにもとづく速やかな業務継続
- 実績（例：国策レベル）

❷高品質

- サービスレベルの向上
  品質管理システムなどの完備
- 業務効率化／品質向上
  AIやRPAなどの高度な技術の導入

❸対応力

- 設備・スペースや人材確保
  事業内容やボリュームに柔軟に対応
- トータルサポート体制
  業務マニュアル作成など
  各専門作業者が連携

CBDCシステムにおける身元確認方法の共同化

身元確認方法	利点	課題
仲介機関個別で決定	既存システムが活用可能	身元確認レベルの差によるセキュリティリスク、ユニバーサルアクセス
仲介機関で同一基準（ガイドライン）	身元確認の開発内容が明確	追加開発コスト、ガイドラインの策定
共同センター（システム）	コストが抑えられる、参入しやすさ、取引モニタリングの共同化にもつながる可能性	個人情報の取扱、責任の所在

・ガイドライン策定については、外部公表されているガイドラインが参考になるが、各種身元確認方法によるリスク、ユニバーサルアクセス、ユーザビリティの評価が重要。

・セキュリティリスク、ユニバーサルアクセスの観点から共同化が望ましいと考えるが、共同センター化した場合、最終的な身元確認の責任の所在（審査業務の運営主体等）については議論の余地がある。
また、共同センターが特定事業者となるのか、や、犯収法に準拠する際のリスク（準拠ではセキュリティやユニバーサルアクセスの観点で不十分である可能性）について、検討が必要。

ディスカッションポイント：

ユニバーサルアクセス、セキュリティ観点も含めて、採用する身元確認方法を検討する必要がある

まとめ

・不正防止観点で身元確認方法の選定をするべきであることは前提ではあるものの、採用する身元確認方法、準拠しなければならない法律によって、CBDC口座開設可能者（利用者）が決まってしまう点に留意する必要がある。CBDC口座開設が非対面のみの場合は特に重要となる。

・不必要な身元確認の実施（ユーザビリティの低下）を避けるため、CBDCシステムにおける操作/手続きにかかるリスクの評価をする必要がある。

・最低限の身元確認のレベルが、犯収法への準拠となる。セキュリティリスク、法改正などの動向を踏まえて、導入後に身元確認方法が変更されることも考慮した仕組み・運営（※）にする必要がある。
※仲介業者の身元確認方法の違いによる影響（セキュリティ低下、コスト負担による対応遅延など）を極小化

Confidential

DNP

大日本印刷株式会社

情報イノベーション事業部
第1PFサービスセンター
デジタルトラストプラットフォーム本部
企画開発第1部

別添2
フェリカネットワークス株式会社

CBDCフォーラム WG3 第8回会合
CBDCにおける認証・認可の整理

2024年5月24日

フェリカネットワークス株式会社

FeliCa Networks

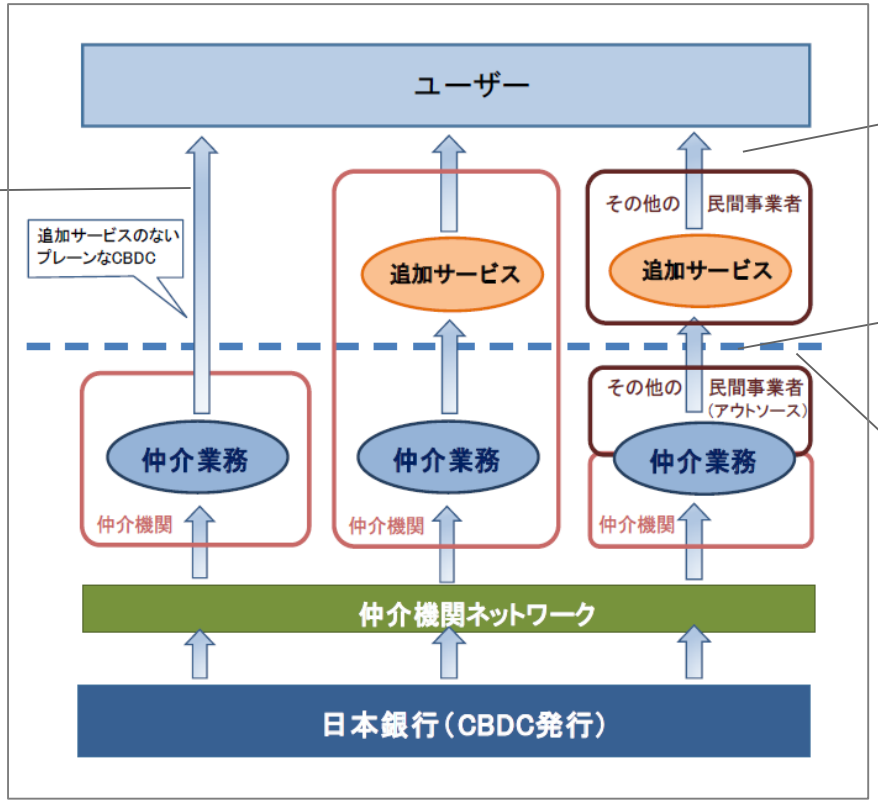
認証・認可の定義と分類

本資料における認証・認可の定義

- 認証：ユーザの登録済み情報を用いて、サービスの利用を行う対象が、ユーザ当人であることを確認する、当人認証（Authentication）を指すものととする
  - 【KYCとユーザ認証・認可】に関するWG第6回会合の内容に基づく
- 認可：追加サービス提供事業者が、仲介機関のリソースに対するアクセスの権限を与えるえる、認可（Authorization）が、CBDCにおける認可の１つと考えられる
  - 【KYCとユーザ認証・認可】に関するWG第7回会合の内容に基づく

前提：CBDCにおける認証・認可のケース

①ユーザと仲介機関の間での“当人認証“



②ユーザと 追加サービス提供事業者の間での“当人認証”

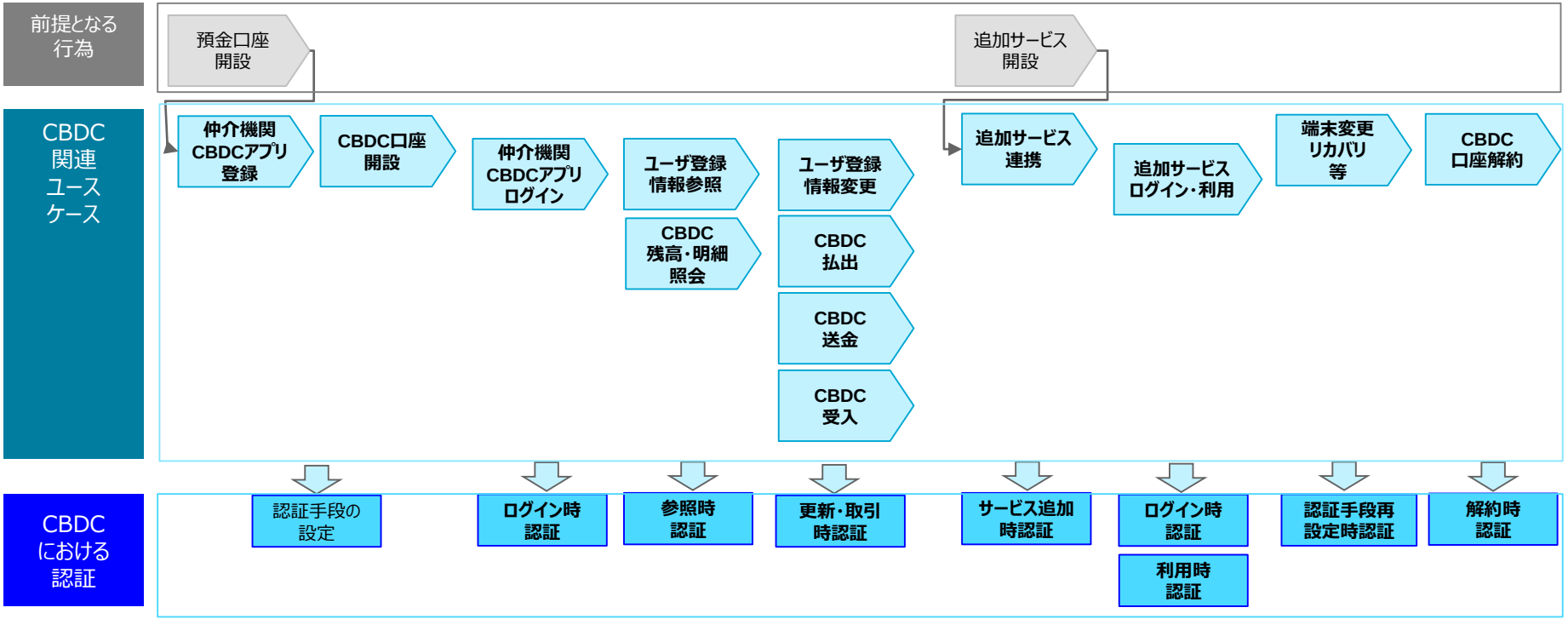
③追加サービス連携(登録)にあたっての、ユーザと仲介機関の間での“当人認証”

④追加サービス利用にあたっての仲介機関と追加サービス事業者の間での“認可”

出典：第1回CBDCフォーラム全体会合 日本銀行様資料より引用

CBDCの想定ユースケースと認証タイミング

CBDCの想定ユースケースとユースケース実行時に行われる認証の整理を行った
CBDCにおいては様々なユースケースにおいて認証が行われると想定される



WG3 第1～7回会合 認証・認可の議論振り返り

WG3での認証関連コメントのまとめ

WG3の第1回～第7回会合における認証に関連するコメントのまとめを行った
・第7回を除く各回の議事録から認証・認可に関すると思われるコメントをピックアップ
・ピックアップしたコメントをユーザビリティ観点、ガイドライン等の観点別に分類

- **WG3 第１回～第7回 認証関連コメントのサマリとまとめ**
  - **セキュリティの重要性：**CBDCとして安全なサービス・システムを提供するにあたり、セキュリティは重要であり、認証におけるセキュリティ確保のために適切な認証レベルと認証方式を選択、利用することが求められる
  - **セキュリティとユーザビリティのバランス**：CBDCのユニバーサル性の観点で、あらゆる属性の人が利用することを考えた場合に、ユーザビリティも重要であり、サービス内容に応じて、セキュリティとユーザビリティのバランスを適切にとることが求められるが、どのレベルが適切かを判断することは難しく、課題である
  - **標準化・ガイドラインの必要性**：仲介機関や追加サービス連携事業者等の間で広く一定のセキュリティレベルや、サービス性・ユーザビリティとセキュリティのバランスを確保するために、何らかのガイドラインを作成し、メンテナンスしていくことが望ましい
  - **システム共同化の可能性**：ユーザの認証を主として行う仲介機関にとって、認証関連のシステム・サービスの導入・運用等のコストを負担することは課題であり、コスト負担の軽減の観点で、認証関連システムの共同化も選択肢として考えられる

WG3における認証・認可の論点と本日のディスカッションポイント

[第1-7回会合における認証・認可に関わる論点]

・認証・認可をどのように実施すべきか

・標準化・ガイドラインの要否

・共同化によるメリット・デメリット

・当人認証の保証レベル

・セキュリティとユーザビリティのバランス

・ユニバーサルアクセス

・最新の技術動向

【本日のディスカッションポイント】

CBDCの認証に関する

・標準化・ガイドラインの位置づけと記載レベル

（システム共同化の可能性も考慮）

・ガイドラインの作成主体と準拠確認の方法

※上記ポイントを選んだ意図：認証レベルや方式、セキュリティとユーザビリティのバランス等について、今後議論していくにあたり、目指す方向性や決定主体について認識を合わせておくことがよいのではないか、という考え

CBDCの認証の標準化・ガイドラインの方向性（ディスカッション）

CBDCにおける認証に関する標準化・ガイドラインの目的

- **CBDCにおける認証の特徴と考慮すべき事項**
  - 高い安全性が求められるCBDCにおいて、各取引の起点となる認証は、不正利用等の攻撃対象として狙われやすい箇所であり、高いセキュリティが必要である
  - CBDCのユニバーサル性として、あらゆる人に広く利用されるためには、認証によるユーザビリティ・UXの低下をできるだけ軽減することが必要である
  - CBDCは、複数の仲介機関や追加サービス事業者等がそれぞれ多様なサービスを提供することが想定され、求められる認証のレベルや認証方式も多様になる可能性がある

- **ガイドラインの目的（想定）**
  - CBDC全体でのセキュリティレベルの維持
    - 多様な仲介機関、連携サービスセキュリティの弱い部分を作らない
  - サービスレベル・ユーザビリティの（一定の）共通化
    - サービスレベル・ユーザビリティとセキュリティのバランスの考え方の具体例を示す
  - 各仲介機関、追加サービスの負荷軽減
    - 業界や有識者の知見や検討結果をを共有し、個々での検討や対応を減らす

論点1：標準化･ガイドラインの位置付けと記載レベル

- **標準化･ガイドラインの位置付けに関する３つの方向性**
  - A：必須要求事項
    - 仲介機関等が対応すべき要件の位置づけ（対応が義務付けられる）
  - B：推奨事項
    - 仲介機関等が対応することが望ましい内容を推奨事項としてまとめた位置づけ
  - C：参考情報
    - 各仲介機関がガイドラインを見て自ら検討し、対応するための参考情報の位置づけ
- **標準化･ガイドラインの記載レベルに関する３つのレベル案**
  - 1：技術仕様レベル
    - 記載レベル例：送金時の認証の保証レベルはAAL2相当とし、FIDO等の多要素認証を利用する
  - 2：要件レベル
    - 記載レベル例：送金時の認証の保証レベルはAAL2相当とし、多要素認証を利用する
  - 3：考え方レベル
    - 記載レベル例：サービス内容のリスクに応じて仲介機関は適切に認証レベル、認証方式を判断、選択する

組み合わせパターンで実際に考えられる例

強 ← 要求度 → 弱

具体的 ↑ 記載レベル ↓ 抽象的

	A：必須要求事項	B：推奨事項	C：参考情報
1：技術仕様	必須技術要件 例：送金時の当人認証の保証レベルはAAL2相当とし、FIDO等の多要素認証を利用すること **必須技術要件（仕様と実装の共通化が主目的）**	推奨技術要件 例：送金時の当人認証の保証レベルはAAL2相当とし、FIDO等の多要素認証を利用することを推奨する	参考技術要件 例：送金時の当人認証の保証レベルとしては、AAL2相当でFIDO等の多要素認証が利用される事例がある
2：要件	必須要件 例：送金時の当人認証の保証レベルはAAL2相当とし、多要素認証を利用すること	推奨要件 例：送金時の当人認証の保証レベルはAAL2相当とし、多要素認証を利用することを推奨する **推奨要件（サービスごとの認証とユーザビリティの整理が主目的）**	参考要件 例：送金時の当人認証の保証レベルとしては、AAL2相当で多要素認証が利用される事例がある
3：考え方	必須の考え方 例：送金時の当人認証についてはリスクを踏まえて適切な認証を実施すること	推奨の考え方 例：送金時の当人認証についてはリスクを踏まえて適切な認証を実施することが推奨される	参考の考え方 例：送金時の当人認証についてはリスクを踏まえて適切な認証を実施することが一般的である **考慮すべき情報（仲介機関等の検討・対応すべき事項の整理が主目的）**

注1：送金時に想定される脅威を分析し、脅威分析に基づく適切な保証レベルと認証方式を記載することが望ましい
注2：要件・推奨として多要素認証を定義し、技術仕様の参考情報としてFIDOを記載するやり方も考えられる

論点2：標準化・ガイドラインの発行主体の考え方

- **1) 公共機関が発行主体**
  - 政府や日本銀行等その他公共機関が発行主体となる。
  - 仮にCBDCが発行される場合は、日本銀行が発行し、国が提供するサービスであるため国や関連公共機関が発行するのが望ましい、という考え方。
  - 民間の組織・団体や有識者の協力の元で、作成、改定を実施していく。
    - 例：デジタル庁 行政手続におけるオンラインによる本人確認の手法に関するガイドライン
    - 例：金融庁　マネー・ローンダリング及びテロ資金供与対策に関するガイドライン

- **2) 民間の組織・団体が発行主体**
  - 全国銀行協会等仲介機関が主な構成者である団体、もしくはキャッシュレスやセキュリティ等に関する民間の組織・団体が発行主体となる
  - 実際にCBDCの認証を実施する機関が作成し、随時見直しを行っていくという考え方。
    - 例：全国銀行協会　資金移動業者等との口座連携に 関するガイドライン
    - 例：OpenID ファウンデーション・ジャパン 民間事業者向けデジタル本人確認ガイドライン

- **3) CBDCに関する新組織・団体が発行主体**
  - CBDCは新しいサービスであり、ステイクホルダーも官民多岐に渡るため、CBDCに関係する公共機関や民間組織が参画する新しい組織・団体を設立し、作成、改定を実施していくという考え方

認証に関する標準化･ガイドラインの方向性のパターン例

	概要	ガイドラインの位置付け	ガイドラインの記載レベル	ガイドラインの発行主体	メリット、デメリット等の考察
1	公共機関が発行する必須技術要件	必須要件	技術仕様	公共機関	・公共機関が定める必須技術要件として統一化が図りやすい ・対応が難しい仲介機関が出る可能性が高まる ・技術仕様が共通であれば共同システム化も検討しやすい。
2	新しいCBDC関連団体が発行する推奨要件	推奨事項	要件	新しいCBDC関連団体	・幅広い参加者により多くのケースをカバーする網羅性の高い内容になることが期待される ・まとまらない可能性もある ・新団体設立を前提とすべきかも論点である
3	民間組織・団体が発行する考え方/要件の整理	参考情報	考え方/要件	民間組織・団体	・各仲介機関の検討負荷は大きい ・仲介機関の状況により柔軟に対応できる可能性がある ・セキュリティレベルやサービス性は個々に異なる可能性が高い。

注：上記の表のパターンは議論用の組み合わせであり、これに限定されるものではない。

まとめ

- 本資料では、CBDCにおける認証・認可について、認証を中心にWG3の第１回～第７回の議論を振り返り、論点をまとめた上で、標準化・ガイドラインの方向性についていくつかの想定パターンを提示した。
- 今回提示したのは例であり、標準化・ガイドラインの方向性を決定づけるものではない。今後、各サービスのユースケースごとに、セキュリティとユーザビリティのバランスを考慮した認証レベル、認証方式についてCBDCとして求められる要件について議論を進めていくにあたり、CBDCとしての認証に関する要件のあり方・方向性について関係者の認識を合わせておくことで、より効果的に議論が行うことができるのではないかと考えられる。