2024 年８月 30 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９回会合の議事概要

１．開催要領

（日時）2024 年７月５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

日本マイクロソフト株式会社、日本電気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（日本マイクロソフト株式会社）

――　プレゼンテーション資料は別添１を参照。

ＣＢＤＣの口座開設や各取引時の本人確認として、スマートフォン内の安全なウォレットに、マイナンバーカードの情報を基に生成されるＶＣ（Ｖｅｒｉｆｉａｂｌｅ　Ｃｒｅｄｅｎｔｉａｌ）を格納して活用することを想定した場合の実現性、現状の課題、その解決方法の有無について、検討や考察を行う。

はじめに、マイナンバーカードの利用状況について整理する。総務省の発表によれば、人口に対するマイナンバーカードの保有者の割合は約 73.8%である（2024 年５月３１日時点）。また、マイナンバーカードのＩＣチップに搭載された電子証明書を利用して本人確認を行う公的個人認証サービス（ＪＰＫＩ）は、金融や携帯電話業界等の多くの民間企業で採用され、口座開設時や契約時の本人確認に活用されている。

マイナンバーカードの沿革を振り返ると、様々な形でマイナンバーカードの利活用が模索されてきたことが分かる。2023 年からは、マイナンバーカードの電子証明書がＡｎｄｒｏｉｄスマートフォン上に搭載できるようにな

り、ｉＰｈｏｎｅ端末への対応や券面記載事項（氏名、住所、生年月日等）の搭載等、更なる機能の拡充も今後検討されている。また、2024 年６月 24 日からは、マイナンバーカードを利用したオンライン本人確認サービスとして、「デジタル認証アプリ」がデジタル庁よりリリースされた。デジタル認証アプリはｉＯＳ／Ａｎｄｒｏｉｄ両方に対応しており、アプリをインストールしたスマートフォン端末をマイナンバーカードへかざすことにより、対応する行政機関や民間事業者でオンラインでの本人確認を行うことができる。デジタル認証アプリの認証ＡＰＩや署名ＡＰＩは無料で利用することができ、開発者向けのドキュメントや実装ガイドラインはデジタル庁のウェブサイトから閲覧できる。

次に、ＣＢＤＣシステムにおけるＶＣの利用可能性について検討する。ＶＣは「検証可能な資格情報」または「検証可能な資格証明書」と訳されることが多く、「発行者（Ｉｓｓｕｅｒ）」「所有者（Ｈｏｌｄｅｒ）」「検証者（Ｖｅｒｉｆｉｅｒ）」の三者の間でやり取りが行われ、その手順は以下のようになるだろう。①ＶＣの所有者となるユーザーは、発行者に対して「メタデータ（発行者や所有者に関する情報）」「クレーム（氏名・住所・性別・生年月日からなる基本４情報等の情報）」「発行者の署名」等の情報が含まれたＶＣの発行をリクエストする。発行されたＶＣは、所有者の持つスマートフォン端末のウォレットに保存される。②所有者は、身元確認または当人認証時に必要なクレームを選択し、ＶＰ（Ｖｅｒｉｆｉａｂｌｅ　Ｐｒｅｓｅｎｔａｔｉｏｎ）として検証者に提示する。これにより、所有者は提供する個人情報の範囲を自らの意思で決めることができる。③検証者は信頼できる第三者が管理するデータベースである「信頼されたデータレジストリ」に予め登録された公開鍵を使用して、ＶＰの署名を検証する。

上記の手法の場合、マイナンバーカードのＩＣチップ情報読取と同等の身元確認・当人認証保証レベル３相当となるだろう。仲介機関に提示する個人情報の範囲をユーザーが選択できることや、スマートフォン内に保存されたＶＣの提示のみで認証が完結させられること等、ＶＣならではの利点も期待できる。

最後に、検討すべき課題とディスカッションポイントとして①認証強度、②有効期限、③事故対応、④検証者の実装コスト、⑤「信頼されたデータレジストリ」の管理とプライバシー保護の５点を挙げる。①は、取引の重要度に応じて変えるため、マイナンバーカードのパスワード入力やライブネスチェック等の要否について判断する必要があるだろう。②は、ＶＣとマイナンバーカー

ド内電子証明書の有効期限を一致させる仕組みが求められると考えている。③は、例えば、所有者がマイナンバーカードを紛失した場合等に備えて、ＶＣの無効化プロセスを設計する必要があると考えている。④は、ＩＤセレクターとの連携等により、実装コストの低減が期待できるのではないかと考えている。⑤は、管理主体をどうするかだが、パブリックなブロックチェーンの活用も含めて、様々に考えられるだろう。

（２）ＣＢＤＣシステムにおけるＫＹＣおよび認証・認可のあり方②（日本電気株式会社）

――　プレゼンテーション資料の要旨は別添２を参照。

前回までの会合を踏まえ、ＣＢＤＣシステムにおける仲介機関の機能・システムを共同化した場合、これまでに挙げられた課題が解決できるか、もしくは新たな課題があるか等について考察する。

なお、本プレゼンテーションで展開する議論の前提として、ＣＢＤＣシステムにおける共同化を決定付けるものではないこと、本ＷＧテーマのＫＹＣ、ＡＭＬ／ＣＦＴ、認証・認可を中心とした考察であること、共同化しない場合も比較対象とすること、共同化における法的な見解は除外すること、があることに留意いただきたい。また、令和６年（２０２４年）４月に財務省にて公表された「ＣＢＤＣ（中央銀行デジタル通貨）に関する関係府省庁・日本銀行連絡会議　中間整理」に記載されている仲介機関・日本銀行・政府の役割、プライバシーの確保、不正利用対策等の内容をもとに考察を行った。

まず、共同化のモデルを検討する。前提となるモデル図は令和４年（２０２２年）５月に日本銀行により公表された「中央銀行デジタル通貨に関する連絡協議会　中間整理」より引用した。なお、本プレゼンテーションにおいて「顧客管理業務」は、ユーザーの身元確認や顧客情報を管理する業務を、「ユーザー口座管理業務」はユーザーのＣＢＤＣ口座の管理を行う業務を意味する。

１つ目のモデルは、共同化しない場合の「共同化なしモデル」である。共同化しない場合、仲介機関の業務は仲介機関毎に運用されるため、基本的に仲介機関間の情報共有は行われないと想定する。

２つ目のモデルは、顧客管理業務のみを共同化する場合の「顧客管理共同化モデル」である。本人確認に特化した共同システムで顧客管理業務を行い、認証・認可やＡＭＬ／ＣＦＴは各仲介機関で行う。なお、ＡＭＬ／ＣＦＴも共同システムで行う方法もありうるが、他モデルとの棲み分けを明確化する観点から各仲介機関が行うものとする。また、顧客管理業務にはＶＣを利用するこ

とも考えられるだろう。

３つ目のモデルは、仲介機関の業務すべてを共同化する場合の「セントラルモデル・フルサービス型」である。ｅＫＹＣ、ＡＭＬ／ＣＦＴ、認証・認可等の仲介機関の業務全般を共同システムが担い、仲介機関はＳａａＳ（Ｓｏｆｔｗａｒｅ　ａｓ　ａ　Ｓｅｒｖｉｃｅ）におけるマルチテナントのように複数のテナント（企業等）で論理分割しつつ同一のサービスを利用する。顧客情報やＣＢＤＣ口座情報は共同システム内で一元管理されるため、技術的には名寄せ等が簡単に行えると考える。

４つ目のモデルは、仲介機関の業務をＢａａＳ（Ｂａｎｋｉｎｇ　ａｓ　ａ　Ｓｅｒｖｉｃｅ）で共同化する場合の「セントラルモデル・ＣＢＤＣａａＳ（ＣＢＤＣ　ａｓ　ａ　Ｓｅｒｖｉｃｅ）型」である。仲介機関の業務すべてを共同化する点はフルサービス型と同様だが、仲介機関は公開されたＡＰＩセットより必要な機能を選択して利用できるため、独自のサービス提供を行い易くなり、サービスの画一化を避けることが可能となる。

次に、仲介機関の業務の共同化のメリット・デメリットを整理する。

メリットは大きく４点考えられる。１点目は「効率性の向上」。共通プラットフォームの使用により取引・事務・システム運用コストが削減できる可能性が考えられる。２点目は「互換性の確保（標準化の導入）」。各仲介機関間での情報共有やシステム連携がスムーズになる可能性が考えられる。３点目は「負荷分散のコントロール」。各仲介機関に過度な負荷がかかることを防ぎ、システム全体の安定性が向上する可能性が考えられる。４点目は「高度化」。共同化によって集められたデータの利活用が可能となることで、処理が高度化できる可能性が考えられる。

デメリットは大きく３点考えられるが、見方によってはメリットにもなりうる。１点目は「セキュリティリスクの増大」。共同システムに攻撃を受けた場合、影響が大きくなる可能性がある。ただし、共同化されていることで対策が打ちやすい側面もあるだろう。２点目は「運用の複雑性の増大」。複数の仲介機関が共同で運用するため、調整や管理が複雑になる懸念がある。ただし、適切に運用ができれば、むしろメリットにできる可能性もあるだろう。３点目は「競争の抑制」。共同化により、各仲介機関が提供するサービスが画一化し、競争が阻害される懸念がある。ただし、セントラルモデル・ＣＢＤＣａａＳ型であれば、仲介機関が選択するＡＰＩの組み合わせにより、フルサービス型対比でサービスの自由度を上げることも可能だろう。

続いて、各モデルのメリット・デメリットの整理を行う。共同化なしモデルは、各仲介機関が独立していることから、共同化による恩恵としての業務効率

化、コスト削減、データの利活用による高度化は得られない。また、仲介機関間の互換性の考慮は不要だが、インターフェースの標準化は最低限必要であること、システム負荷は分散されているが全体のコントロールが困難であること、個社毎にセキュリティリスクの検討が必要であること等が特徴と言える。

顧客管理共同化モデルは、顧客管理部分は共同化されているため、一定の効率化やコスト削減、データの利活用による高度化は望めるが、顧客情報の集中によるセキュリティリスクの増大は懸念となる。

セントラルモデルは、全モデルの中で最も効率的な運用やコスト削減が見込まれ、互換性の検討も要さず、データ利活用による高度化も期待できる。しかし、処理集中時のシステム影響や顧客情報等の集中によるセキュリティリスクの増大、関係者間の要望を取り入れた結果として運用が逆に複雑化してしまう懸念がある。ただし、システム負荷分散のコントロール、リスク対策、関係者間での合意等により、懸念を解消できる可能性があると考えている。

続いて、共同化における考察ポイントを３点挙げる。考察ポイントの１つ目は、「どこまで何を共同化すべきか」で、以下６つの課題があると考えている。①機能と業務に関し、共通化部分と仲介機関個社部分の機能や業務の明確化。②データに関し、データの共有化範囲の十分な検討。③役割と責任分担に関し、日銀・仲介機関・ユーザーの責任範囲の明確化。④セキュリティリスクに関し、データを集中して持つことによるリスク増加への対策。⑤ガバナンスコントロールに関し、チェック機関のような第三者評価の仕組みづくりの必要性の検討。⑥事務コスト・システムコストに関し、システムの複雑化によるコスト増加懸念への対応および運用コストの按分方法の明確化。なお、運用コストの按分方法は、例えばＳａａＳではＡＰＩのコール数で従量課金を行っているなど、既存のサービスの考え方を参考にできるだろう。

考察ポイントの２つ目は、「ガイドラインの必要性とセキュリティレベル」である。一般的には、攻撃者はセキュリティレベルの低い箇所から侵入を試みるため、セキュリティレベルの目線を各仲介機関で合わせる必要がある。その際、ガイドラインやチェックリストで目線を合わせても解釈の違い等でセキュリティレベルを一定に維持できない可能性に留意が必要と考える。

考察ポイントの３つ目は、「プライバシー保護、インシデント発生時の影響度」である。プライバシー保護については、共同化に伴いデータが集中することで、個人情報の収集と追跡、目的外利用、政策の乱用等へのユーザーからの懸念が増大する可能性がある。また、情報漏洩等のインシデント発生時の影響度については、大量のデータが集中するため社会的な影響が増大する可能性

がある。
　ここで、参考として金融業界における共同化の検討や取り組みを２つ紹介する。１つ目は、証券コンソーシアムのＫＹＣ共通化ワーキンググループである。公表されたホワイトペーパーには、共同化はコスト低減と高度化がポイントである旨が記されており、それらの検討結果は参考になるだろう。もう１つは、マネー・ローンダリング対策共同機構の取り組みである。金融機関毎にデータを分割管理し、金融機関間でデータが混ざることはない構成とされており、このように、データを分ける方法も参考になるだろう。

　最後に、ディスカッションポイントとして、「共同化の是非と選択すべきモデル」「セキュリティおよびプライバシーの担保」「コスト目線」「共同化による業務の効率化・高度化」の４点を挙げる。この点について、各参加者の意見やコメントがあれば伺いたい。

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、株式会社ふくおかフィナンシャルグループが担当した。概要は以下のとおり。

【マイナンバーカードとＶＣの差異やＶＣを利用する上で整理すべき事項等】

（参加者）現行の犯罪収益移転防止法上におけるワ方式では、マイナンバーカードの署名用電子証明書とその暗証番号の入力によって本人確認を行っている。ＶＣを利用した本人確認の場合は、法律やセキュリティの観点で、現行方式と比べてどのような違いが生じうるかは整理が必要だろう。

（参加者）ＶＣについては、ＤＩＤ／ＶＣ共創コンソーシアムが立ち上がるなどビジネスでの利用に向けた議論が一部で進みつつあるが、個人的には本人確認は公的個人認証サービス（ＪＰＫＩ）の利用が良いのではないかと考えている。健康保険証のマイナンバーカードへの一本化等によりマイナンバーカードの利用がさらに浸透すれば、個人が本人確認の際にマイナンバーカードによる公的個人認証サービス（ＪＰＫＩ）を利用することへの意識は変わっていくだろう。ＶＣは、マイナンバーカードには含まれない様々な情報の保持や住み分けが可能と思われるが、ＶＣの使い道については何か考えがあるか。

（参加者）相手先に渡す個人情報を選択できるＶＣの仕組みを使うことで、ユーザーが必要以上に個人情報を渡さなくてもよくすることが使い道の一つと考えている。

（参加者）本人確認は、マイナンバーカードによる公的個人認証サービス（ＪＰＫＩ）を利用するほうがよいことに同意する。ただし、ＥＵのデジタルアイデンティティウォレットなどで、金融機関や携帯キャリア等のサービス提供者が保有する様々な属性情報をデジタルアイデンティティウォレットに集めていくという考え方があり、そうした観点でもＶＣが今後必要とされる可能性はあるだろう。

【デジタル認証アプリとの連携】

（参加者）デジタル認証アプリによる本人確認について、どのような考えを持っているかを伺いたい。

（参加者）デジタル認証アプリを、オンラインにおける口座開設等のサービス利用開始時の本人確認プロセスに組み込むことで、ｅＫＹＣ（ホ方式、ヘ方式）に比べてセキュリティを高められる可能性がある。例えば銀行アプリでの口座開設で実際に利用する場合には、口座開設手続きの途中でデジタル認証アプリという別のアプリを間に挟むことになる。そのため、操作方法をユーザーに理解いただけるよう、サービス提供者としては、アプリのわかりやすいＵＩ／ＵＸ設計や丁寧な説明を考える必要があるだろう。また、デジタル認証アプリは、デジタル庁が認証機能を無償で提供することから、社会全体での本人確認のコスト削減に寄与する可能性があるのは喜ばしい点。ただし、本人確認の関連サービスを提供している民間企業においては、ビジネスモデルへの影響の可能性も考えられる。デジタル認証アプリの導入を検討する際は、本人確認プロセスのユーザビリティの高さと、既存の本人確認の関連サービスへの影響を含めたコスト抑制の両面への目配りが必要だろう。

【パブリックブロックチェーンの利点と留意点】

（事務局）ＶＣのデータレジストリにパブリックブロックチェーンを活用する利点は何か。

（参加者）パブリックブロックチェーンは、取引データを見ようと思えば誰でも見ることができ、そうした衆人環視による監視によって安全が担保され

ている仕組みであることが利点と考えている。書き込まれたデータの改ざんが困難であることだけでなく、こうした改ざん検知の仕組みがあることは利用者に安心感を与えるだろう。

（参加者）仮に、ＶＣのデータレジストリにパブリックブロックチェーンを利用する場合を考えると、保存されるアイデンティティの情報を誰がどのように書き込むか等のアイデンティティ管理のあるべき姿を考える必要がある。また、身元確認や当人認証等のＶＣが使われるシチュエーションによっても考慮事項は変わるため、検討すべき内容は多岐にわたるだろう。

【様々な立場から見た共同化の可能性】

（参加者）規模の大きくない仲介機関の立場とすれば、自前で全てのシステムを用意することは難しいと想定され、何かしらの共同化は必要だろう。また、同一人物が異なる名義を用いて不正に口座開設を申し込む事例があるが、ｅＫＹＣの共同化によって顔写真データの集約が可能になれば、仲介機関を跨いだ不正検知の高度化等が期待できると考える。

（参加者）共同化については、各企業の中においても、例えば第１線の事業部門、第２線の管理部門、データを利活用する部署等の立場の違いによって様々な意見がありうると考えている。

　第２線の立場からは、共同機構が提供する共通のプラットフォームのセキュリティを突破された場合に、共同機構が何らかの対策を打たない限りは、プラットフォームの利用者である仲介機関としては手の打ちようがなく、被害が出続ける可能性を危惧している。また、仲介機関としては、共同機構から提供されたデータを利用しているだけであって、共同機構に対策と補償の責任があるとの主張がありうる。共同機構はユーザーとの接点が直接ないゆえに対策をとることが難しい局面も考えられる中、ユーザーと直接の接点を持つ仲介機関が当事者意識をもって解決を図っていくことは簡単ではないだろう。

　共同化によりデータが集約されれば、データの利活用のメリットが大きくなる一方で、セキュリティを突破された場合のリスクも大きくなるため、どのようにして適切なバランスをとるかは難しい。また、共同化したがゆえに、セキュリティリスクが大きくなり、インシデントからの復旧等の対応が難しくなれば、トータルのコストは実際には増える可能性も考えられるため、そうした点も留意して検討する必要があるだろう

　また、現在の決済領域における競争が、ユーザーをいかに自社の経済圏

に囲い込むかが重要になっていることを踏まえると、第１線の立場からは、第２線での業務効率化やコスト削減のみを鑑みて共同化を進めることが、他社との競争優位を築く上で正しいかは疑問が残る。

　コスト面だけを考えれば、法的な整理は必要かもしれないが、マイナンバーの代わりにある個人を一意に特定できる情報としてＶＣ（Ｖｅｒｉｆｉａｂｌｅ　Ｃｒｅｄｅｎｔｉａｌ）を活用し、マネー・ローンダリング対策等に必要な情報をＶＣの情報をキーにして各仲介機関同士で照会し、情報共有を行うことも考えられる。いずれにしても、ＣＢＤＣがどのように使われるかによって、求められる対策は異なるだろう。

（参加者）別添１の課題とディスカッションポイント（26 頁）のなかに「ＶＣの有効期限と、それに伴う口座等の有効期限の考慮」とあったが、既存の銀行口座に有効期限という概念はないため、興味深い論点だと感じた。また、仮にユーザーが仲介機関ごとに口座を持てるとした場合、システムの共同化を一つの理由として、ユーザー単位で顧客情報が一元管理されていれば、顧客情報の更新の申し出があった場合に、更新作業が一度で済むため効率的になると考える。

【共同化の実情、課題、留意点】

（参加者）様々な自治体が地方金融機関と連携してデジタル地域通貨を提供しているが、地方金融機関は自治体向けに個別にシステムを構築しているのか。

（参加者）自治体によって使用しているシステムが異なるため、金融機関側はそのシステムに合わせて対応する必要がある。この点、メガバンク等の規模の大きい金融機関であれば、デジタル地域通貨のシステムを自前で構築し、自行のシステムと連携することも可能だろうが、地方銀行では自前でのシステム構築は難しいため、大部分はデジタル地域通貨のサービス提供者等が提供する共通基盤を使用し、自行システムとの連携部分に関して、システム連携が難しい場合は、手作業やＲＰＡ等も活用して個別対応を行うことが多いと認識している。

（参加者）共通基盤の利用には相応のコストが発生するケースが多いが、ＡＰＩの繋ぎ方、勘定系システムへの接続有無等によってコストが増減するため、共通基盤を使用しない方がコストを抑えられるケースも存在する。また、昨今、自治体では、クラウドサービスを基盤としたシステム構築を行

ったり、標準化された仕様・規格を活用することが増えているため、共同化するための仕様・規格の統一へのハードルは下がってきていると感じている。そのため、今後はセントラルモデル・フルサービス型、セントラルモデル・ＣＢＤＣａａＳ型のような方向性になることも考えられる。ただし、共同化によってリスクは増加する場合もあるため、十分な検討が必要だろう。

（参加者）標準化された仕様・規格を活用することは、ベンダーロックインを避ける点でも有益だろう。

（参加者）全ての仲介機関ではなく、一部の仲介機関のみが共同化する考え方はあるか。

（参加者）銀行界では勘定系システムがまさにその流れになっており、一部の仲介機関のみで共通基盤を作ってグループで運用を行うことも考えられるだろう。

（参加者）仮に共同化を進めるとなった場合、関係者が多岐にわたるため、どのような主体が主導し、どのようなモチベーションで推進されるかによって、実現可能性、実現に至るスピード、予算の確保のハードルの高さ等が変わるため留意が必要だろう。

４．次回予定

次回の会合は９月 11 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９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

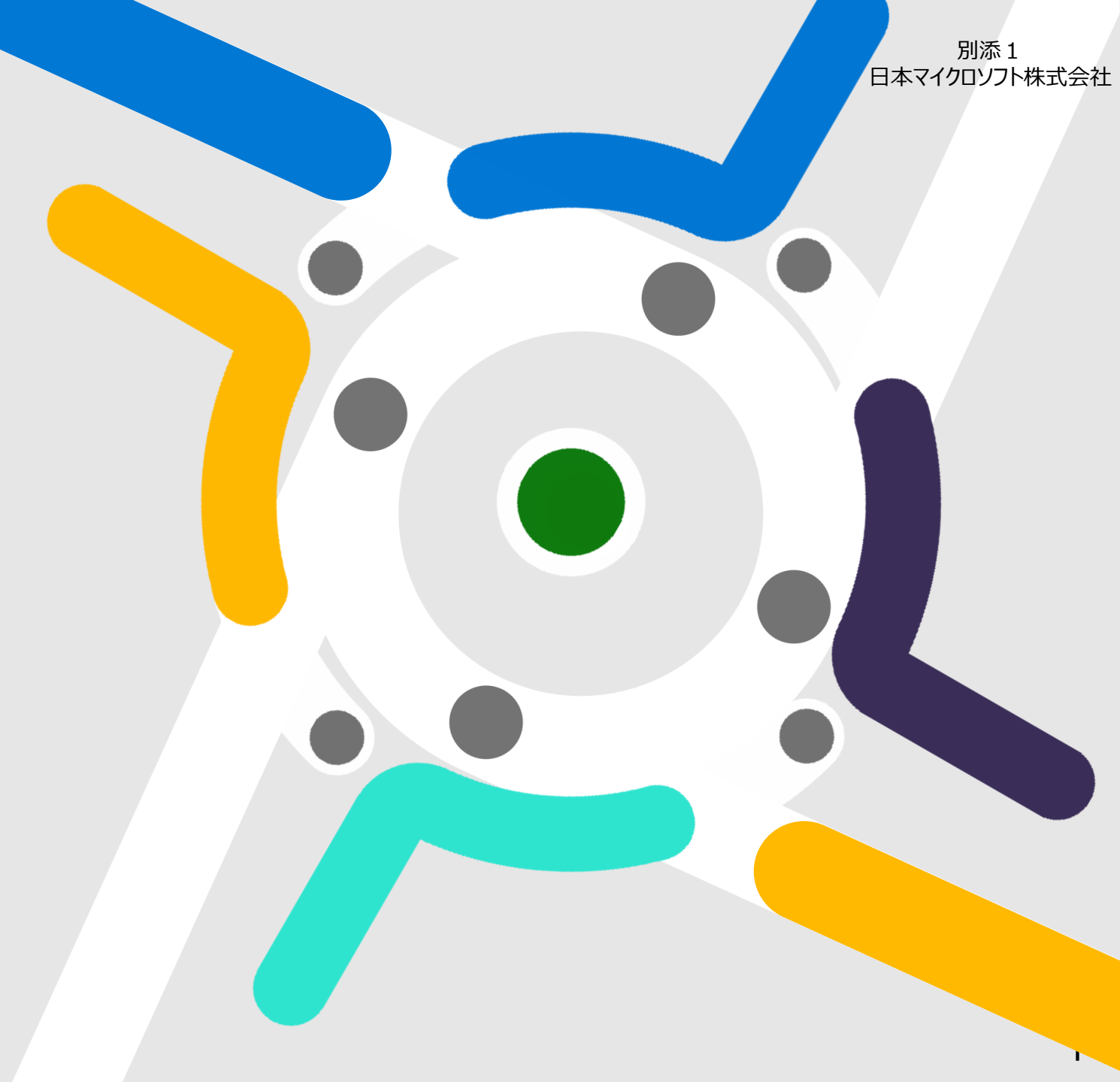
別添１
日本マイクロソフト株式会社

Microsoft Security

CBDC フォーラム WG3
第9回会合

# 認証と認可の整理
# ～ スマートフォンを使用した VC による認証/認可の可能性

2024.07.05
日本マイクロソフト株式会社



# 本日のテーマ

第8回、第9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、ユーザー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、認可の実施方法やその特徴、留意点、あり方などを整理する。

を踏まえて

CBDC 口座の開設や各種取引業務に使われる認証や認可方式として、スマートフォンに搭載されたマイナンバーカードを活用することを想定した場合の実現性、現状の課題、その解決方法の有無などについて、直近のマイナンバーカードに関連する動向を踏まえ考察する。

# 過去の議論より

今回のテーマは、過去の発表や議論を踏まえ、スマートフォンに格納された「マイナンバーから生成された VC」を使用した認証/認可が、以下に示す課題とどのように関わるのか、何が解決できて解決できないのかについて考察するものである。

- 本人確認手法の保証レベル
- 仲介機関が保持するアカウント情報の信頼性
- 仲介機関等の運用にかかわるコスト
- プライバシー保護
- ユーザビリティ

# この考察で想定する最終的な姿

- スマートフォン内の安全なウオレットに、マイナンバーカードから生成された Verifiable Credential（以降 VC）を格納する。
- 仲介機関は上記方式による認証結果をもって口座開設等を行う
- 仲介機関は上記を基盤とし、VC を使用して取引にかかわる認証と認可を行う
- 前ページの課題が“ある程度のレベルで”解決できる

Microsoft Security

# マイナンバーカードの利活用状況の整理

# マイナンバーカードの申請、交付、保有状況（2024年6月23日時点）

| | 合計（※1） | 人口に対する割合（※2） |
|---|---|---|
| 有効申請受付数（累計）<br>【令和6年6月23日（日）時点】 | 101，424，702 | 約80．9% |
| 交付枚数（累計）<br>【令和6年6月23日（日）時点】 | 99，880，620 | 約79．6% |
| 保有枚数<br>【令和6年5月31日（金）時点】 | 92，575，353 | 約73．8% |

有効申請受付件数・交付枚数 ： 再交付、更新を含むこれまでに有効に申請受付された又は交付されたカードの累計枚数
保有枚数 ： 現に保有されているカードの枚数（交付枚数から死亡や有効期限切れなどにより廃止されたカードの枚数を除いたもの）

※1　国外利用分含む
※2　令和5年1月1日時点の住基人口（125,416,877人）に対する割合（国外利用分除く）

参照元 総務省｜マイナンバー制度とマイナンバーカード｜マイナンバーカード交付状況について (soumu.go.jp)

# マイナンバーカードの公的個人認証サービスの民間利用

## 公的個人認証サービス（JPKI）利用事業者数

| 2022.3.31時点 | | 2023.8.1時点 |
|---|---|---|
| **144社** | → | **465社** |

※利用事業者数は、PF事業者（大臣認定事業者）とSP事業者（PF事業者に署名検証を委託してサービスを提供する事業者）の合計

## JPKI導入済の民間ビジネス（業界別）

●金融業界　　ワ方式の採用率は増加中
資金移動、銀行、証券、損害保険・生命保険、クレジットカード、暗号資産取引　など
●携帯電話業界
●不動産業界
●シェアリングエコノミー業界

→主に口座開設時や契約時の本人確認に活用されている。
→金融業界を中心に、その他の様々な業界、サービスにおいても、利用が広がりつつある。

参照元 デジタル庁 マイナンバーカードの普及・利活用拡大 (digital.go.jp)

# マイナンバーカード活用に関する歴史とロードマップ


2015年10月 マイナンバー通知開始
2016年01月 マイナンバー制度開始、マイナンバーカード配布開始
2017年11月 マイナポータル運用開始
2019年11月 各種証明書のコンビニ交付サービス開始
2020年01月 e-Tax 送信サービス開始
2021年10月 マイナンバーカードと健康保険証の一体化の運用開始
2023年02月 マイナポータルでの引っ越し手続きオンラインサービス開始
　　05月11日 マイナンバーカードの電子証明書を Android スマートフォンに搭載開始
　　12月20日 スマートフォンを使用した各種証明書のコンビニ交付サービス開始
2024年06月18日 携帯電話の契約の際に券面の目視ではなく、IC チップの読み取りを義務づける方針を発表
　　06月24日 スマホ用デジタル認証アプリの提供開始（マイナンバーカードのスマホ搭載とは別物）
　　08月　　婚姻関係を含む戸籍関係情報との連携がスタート予定
　　末　　運転免許証との一体化
2025年春　iPhone に電子証明書、券面記載事項（審議中）格納開始予定（Apple Wallet 内）
今後　　健康保険証のスマートフォン搭載、
　　Android への券面記載事項の搭載

# マイナンバーカード機能のスマートフォンへの搭載について

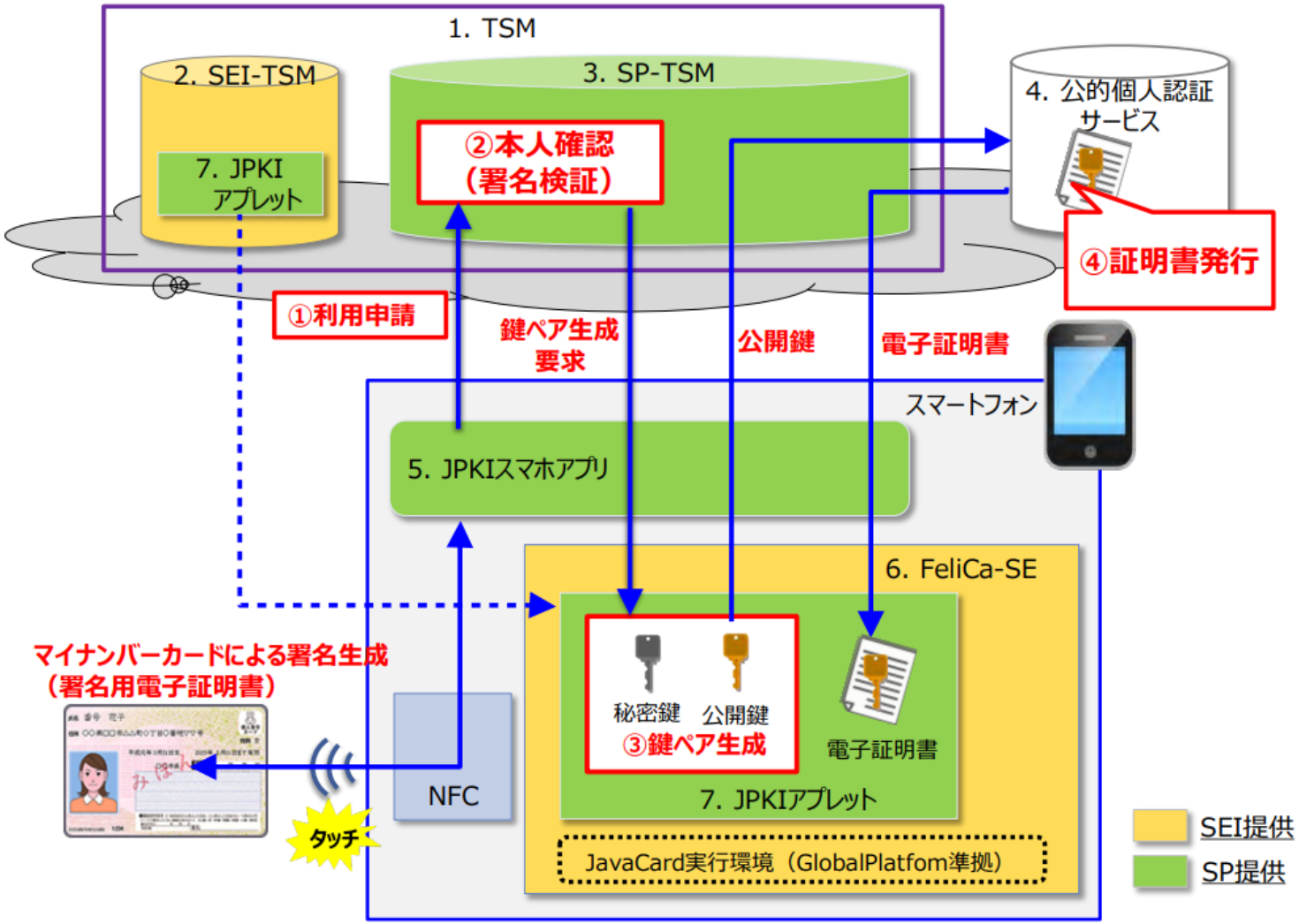
2024年5月31日 デジタル庁 マイナンバーカード機能のiPhoneへの搭載について｜デジタル庁 (digital.go.jp)

- スマートフォンだけでマイナンバーカードでできることを実現する
- 4桁の暗証番号に代わり、携帯電話の持つ 生体認証機能を活用することも可能
- [審議中] 属性証明機能（氏名、住所、生年月日、性別、マイナンバー、顔写真の証明の機能）

| | Android 端末 | iPhone |
|---|---|---|
| 電子証明書 | 2023年5月11日 提供済 | 2025年 春 予定 |
| 券面記載事項（審議中） | 検討中 | |

# （参考）電子証明書のスマートフォン発行の流れ

000721286.pdf (soumu.go.jp)

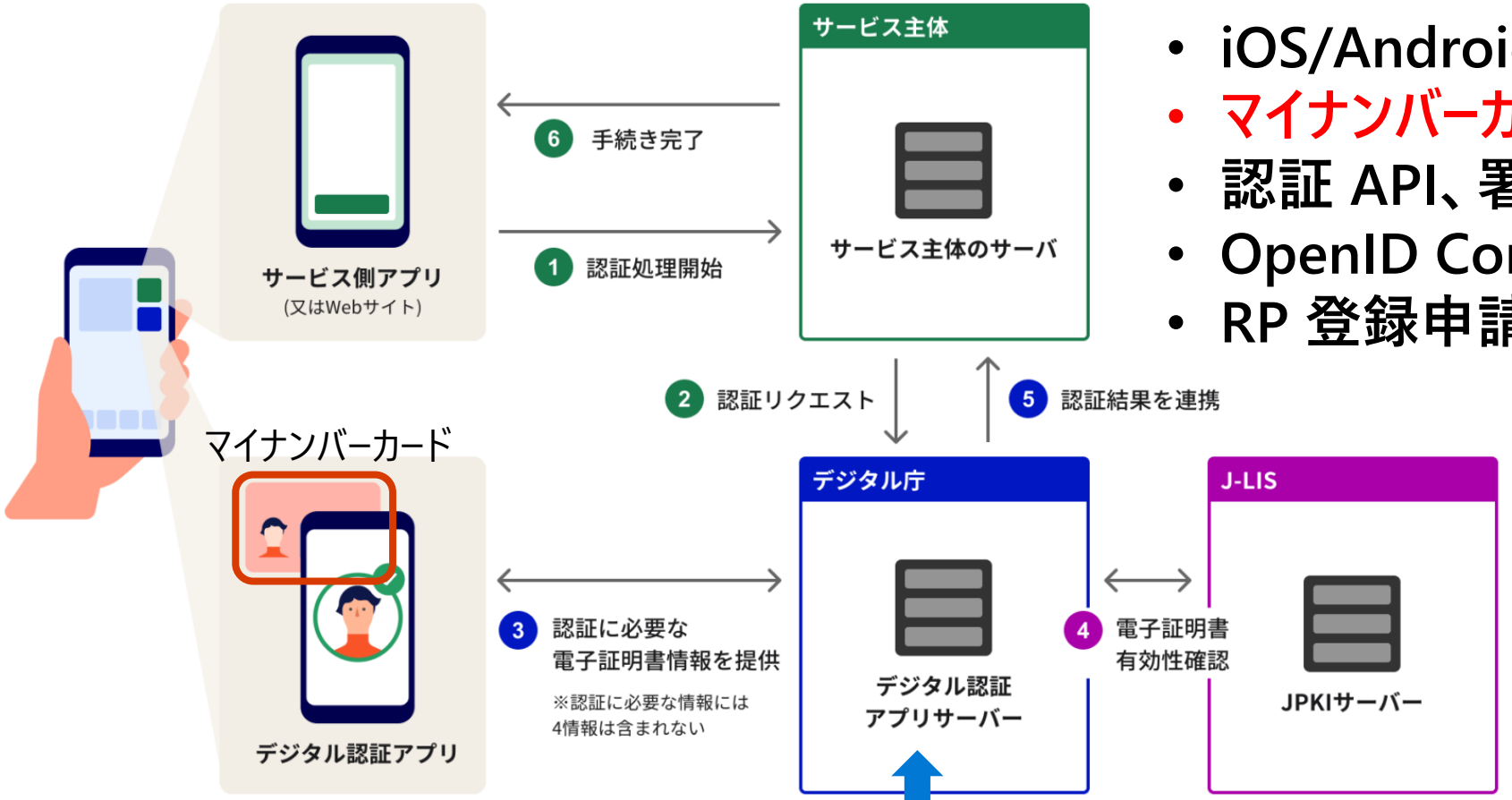



総務省 “電子証明書のスマートフォン搭載に関するシステム構成と初期発行フロー” より

# デジタル認証アプリ（2024年6月24日 提供開始）

デジタル認証アプリについて (digital.go.jp)

行政機関等・民間事業者向け実装ガイドライン | デジタル認証アプリ | ドキュメント | デジタル庁 開発者サイト (digital.go.jp)




- iOS/Android に対応
- マイナンバーカードを使って認証等を行う
- 認証 API、署名 API の利用料はタダ
- OpenID Connect 準拠
- RP 登録申請が必要

デジタル庁のサーバーに保存される情報

- 電子証明書の発行番号
- サービス提供者を識別するコード
- 認証日時
- 認証結果 など

参照　デジタル庁 デジタル認証アプリについて より

# デジタル認証アプリ 実装ガイドライン


| | |
|---|---|
| ス | デジタル認証アプリのサービス全体を示す。 |
| デジタル認証アプリサービスAPI | デジタル認証アプリサービスが行政機関等及び民間事業者向けに開発するAPI。 |
| 利用者識別子 | デジタル認証アプリサーバがRPへ発行する識別子（PPID）。RP内で利用者を特定することができる。RPごとにユニークな識別子を発行する。 |
| 同一端末 | デジタル認証アプリがインストールされている端末内でRPのアプリケーション、もしくはRPのWebサービスが実行されている状態。 |
| 別端末 | デジタル認証アプリがインストールされている端末とは別の端末でRPのアプリケーション、もしくはRPのWebサービスが実行されている状態。 |
| クライアントID | RPを特定するID。<br>デジタル認証アプリサービスにRPを登録した時、デジタル庁から発行される。<br>OAuth 2.0 認可コードフローにおける用語定義「Client Identifier」に基づく。<br>参考：RFC6749 The OAuth 2.0 Authorization Framework - 2.2 Client Identifier |
| 署名対象データ名 | 署名するデータの名称。 RP側で自由に設定可能。<br>利用者が署名対象を識別するために、署名時に表示する項目。<br>※文字や文字数などの制限はAPIリファレンスを参照のこと。 |
| 署名対象識別コード | 署名するデータを識別するために、RPが発行するコード。 RP側のサイトで表示された署名対象識別コードと、デジタル認証アプリに表示された署名対象識別コードの一致を確認することで、利用者は、RP側で発行された電子署名対象に対して署名することを確認する。<br>※文字や文字数などの制限はAPIリファレンスを参照のこと。 |
| 属性情報 | 利用者個人に関わる基本的な情報群を示す。<br>例えば、基本４情報は属性情報として分類される。 |

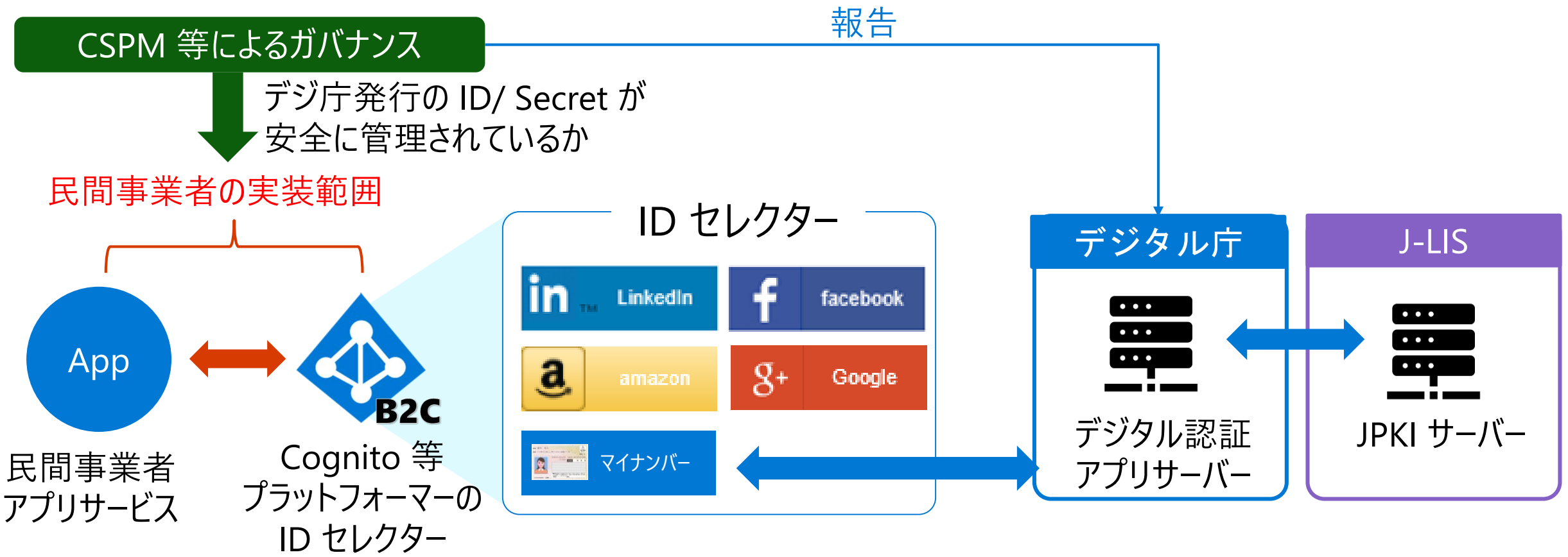
行政機関等・民間事業者向け実装ガイドライン | デジタル認証アプリ | ドキュメント | デジタル庁 開発者サイト (digital.go.jp)

# デジタル認証アプリに対するパブリックコメント（抜粋） PcmFileDownload (e-gov.go.jp)

- **プライバシーへの懸念**
  - 国民がいつどんなオンラインサービスを使っているのか、政府が網羅的に把握できるおそれがある（名寄せ）
  - デジタル庁は発行者（Issuer）に専念すべき
- **ダンピングへの懸念**
  - API 利用が無料であり、民間事業者のサービスを圧迫する可能性
- **事業者側のコスト、スピード感**
  - Client ID の発行に必要な審査の手続きが面倒でハードルが高い
  - 署名の検証、有効性確認機能が提供されていないため独自に実装が必要
  - サービスの実装が複雑
- **使い勝手の悪さ**
  - マイナンバーカードの読み取りが必要
- **プラットフォーマーが提供し幅広く利用されているIDセレクターとの連携性への考慮**
  - Auth0 や Cognito 等との連携が望まれる

# （参考）プラットフォーマーが提供する ID セレクター機能

- 民間事業者アプリと直接接続するのではなく、IDセレクターと連携させることで民間事業者の実装コストを低減させることが可能
- Client ID および Secret の管理方法やガバナンスの報告義務については要検討



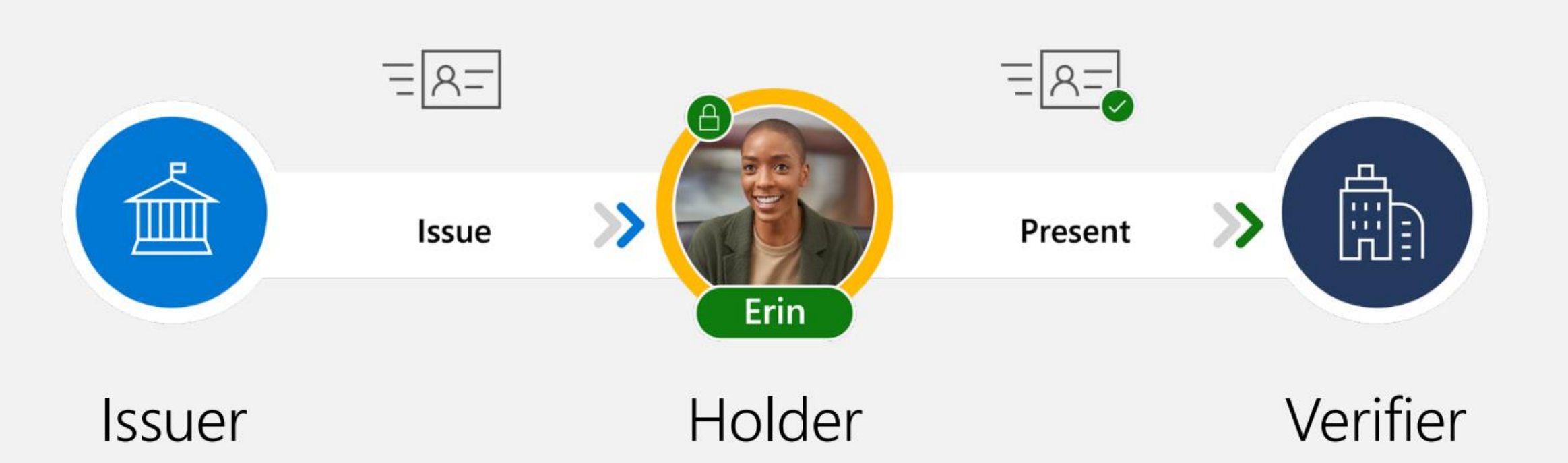
Microsoft Security

# Verifiable Credentials の可能性

ここでは、マイナンバーカードから生成された VC がスマートフォンに搭載された場合、どのようなメリットとデメリットが考えられるか考察する

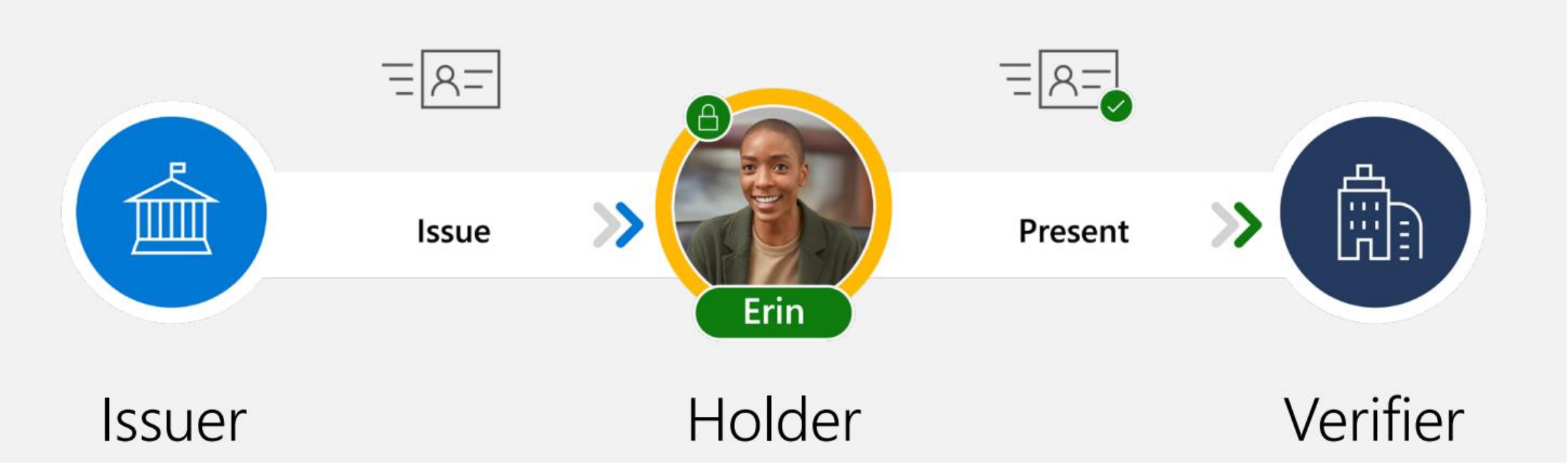
# Verifiable Credentials(VC) とは

- **発行者(Issuer)**が署名した資格情報であり、**検証者(Verifier)**が真正性を検証可能である
- 日本語では「**検証可能な資格情報**」または「**検証可能な資格証明書**」と訳されることが多い
- 異なる検証者の異なる要求に応じた柔軟な情報交換が可能



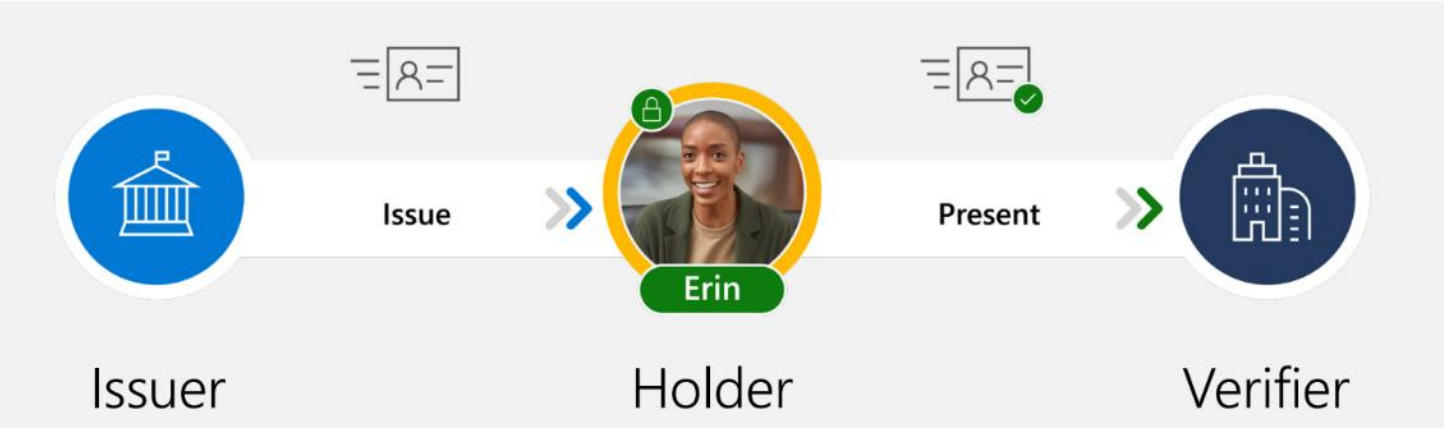
# Verifiable Credentials(VC) とは

- **発行者(Issuer)**が署名した資格情報であり、**検証者(Verifier)**が真正性を検証可能である
- 日本語では「**検証可能な資格情報**」または「**検証可能な資格証明書**」と訳されることが多い
- 異なる検証者の異なる要求に応じた柔軟な情報交換が可能




| 発行者 | 所有者 | 検証者 |
| --- | --- | --- |
| デジタル庁/J-LIS | 国民 | 仲介機関 |

# 言葉の定義




**Issuer（発行者）**
信頼された企業またはエンティティ。ユーザの身元に関するクレームを確認し、そのユーザに電子署名付きクレデンシャルを発行する。発行者は、ID 検証ベンダー、政府機関、雇用主、大学、またはその他の組織である。

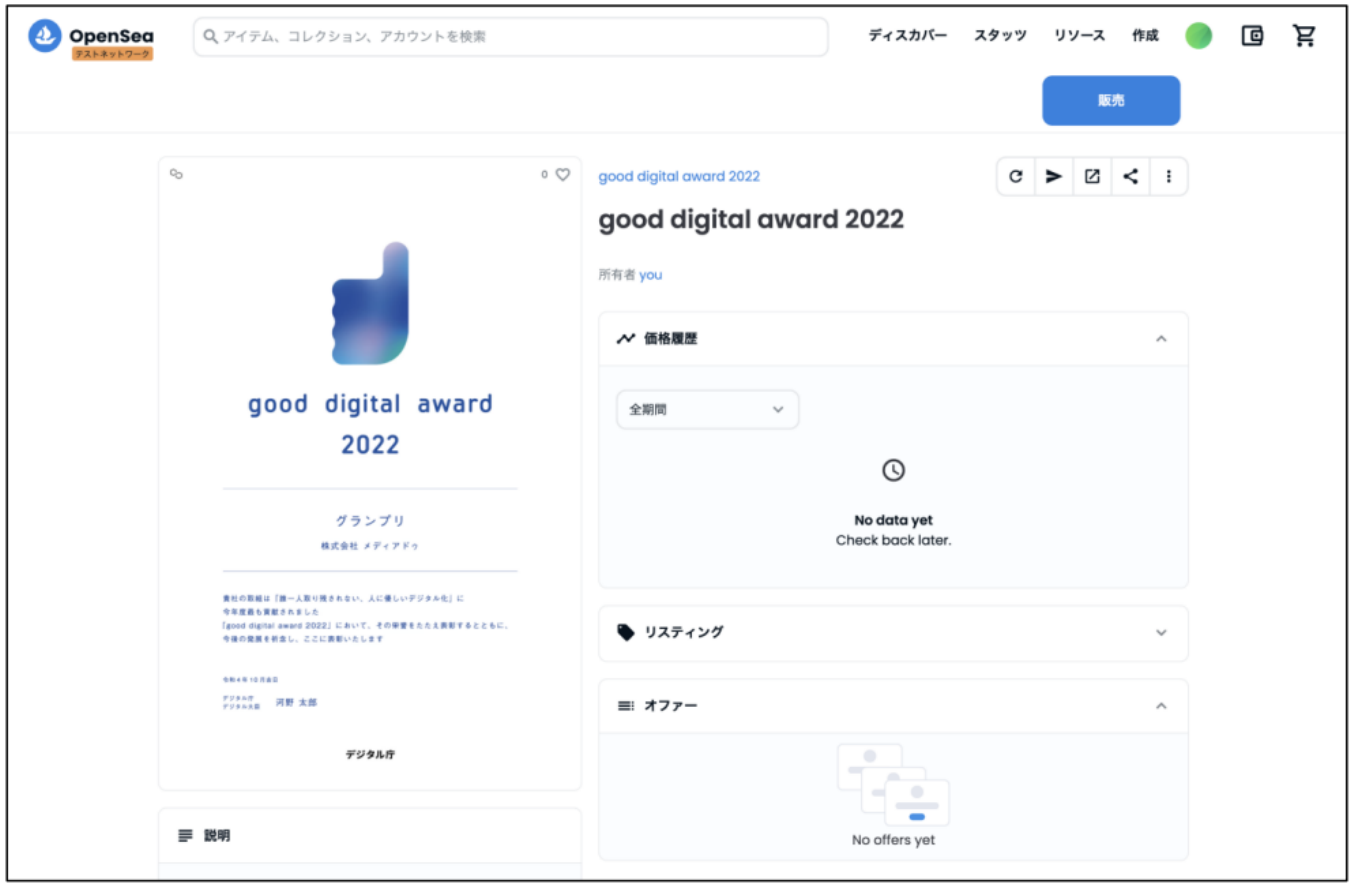
**Holder（所有者）**
発行者に検証可能なクレデンシャルの発行をリクエストし、発行者から検証可能なクレデンシャルを受け取る。
デジタル・ウォレットでクレデンシャルを管理し、クレデンシャルから検証可能なプレゼンテーションを作成し、検証者に提示する。ユーザーのウォレットは一般に、PIN または生体情報のいずれかを介してその ユーザーのみがアクセスできるアプリケーションである。

**Verifier（検証者）**
信頼された企業またはエンティティ。ユーザのクレデンシャルの検証を要求する。Holder からクレデンシャルを受領すると、クレデンシャル内のクレームが要件を満たしていることを検証する。検証者は、新しい雇用主、航空会社、住宅ローン会社など、クレデンシャルの証明を要求するあらゆる組織である。

# デジタル庁での VC の活用事例（2022年度）

## Verifiable Credentials と 譲渡不可NFTを組み合わせた デジタル賞状の発行

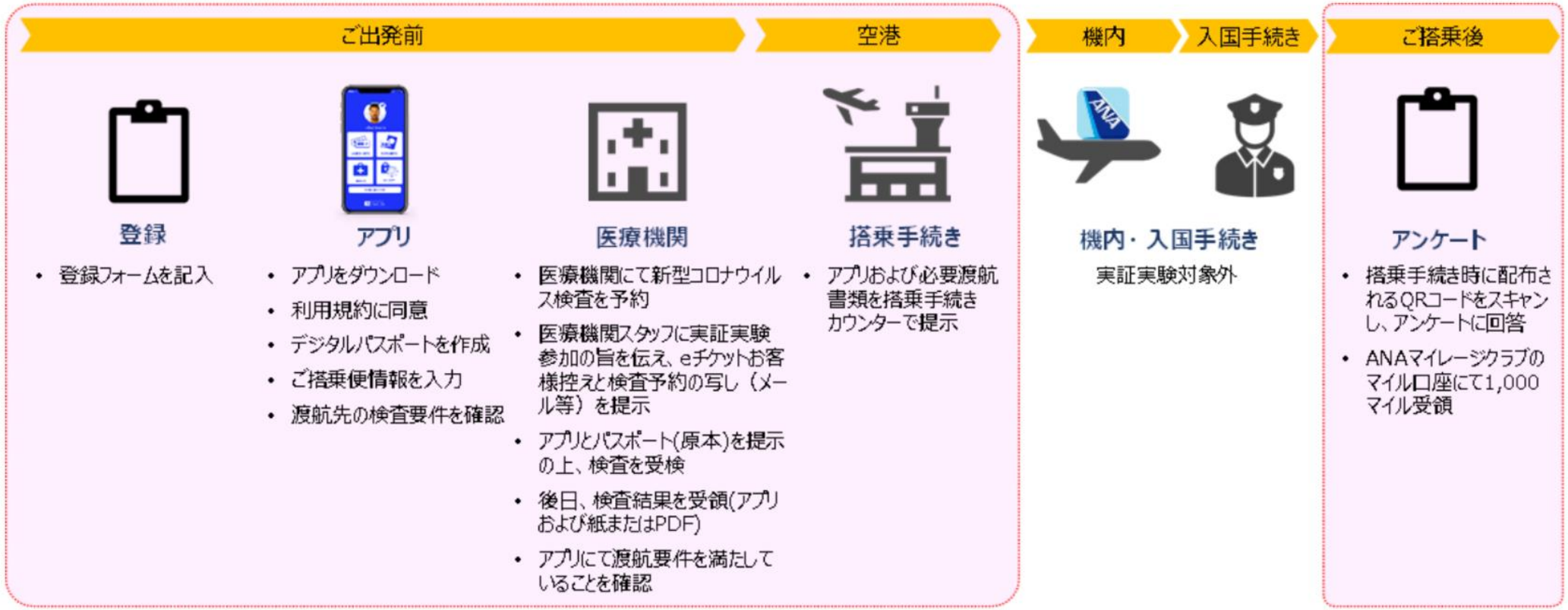
Verifiable Credentials と 譲渡不可NFTを組み合わせたデジタル賞状の発行について (digital.go.jp)

# 民間での VC の活用事例（2021年）

## IATA（国際航空運送協会）Travel Pass（実証実験）

- パスポートだけでは検証不可能な渡航要件の検証
- ANA、JAL など世界32の航空会社で実証実験（特定路線）
- 主目的は COVID-19 検査結果やワクチン接種証明書の提示




＝ 実証実験対象範囲

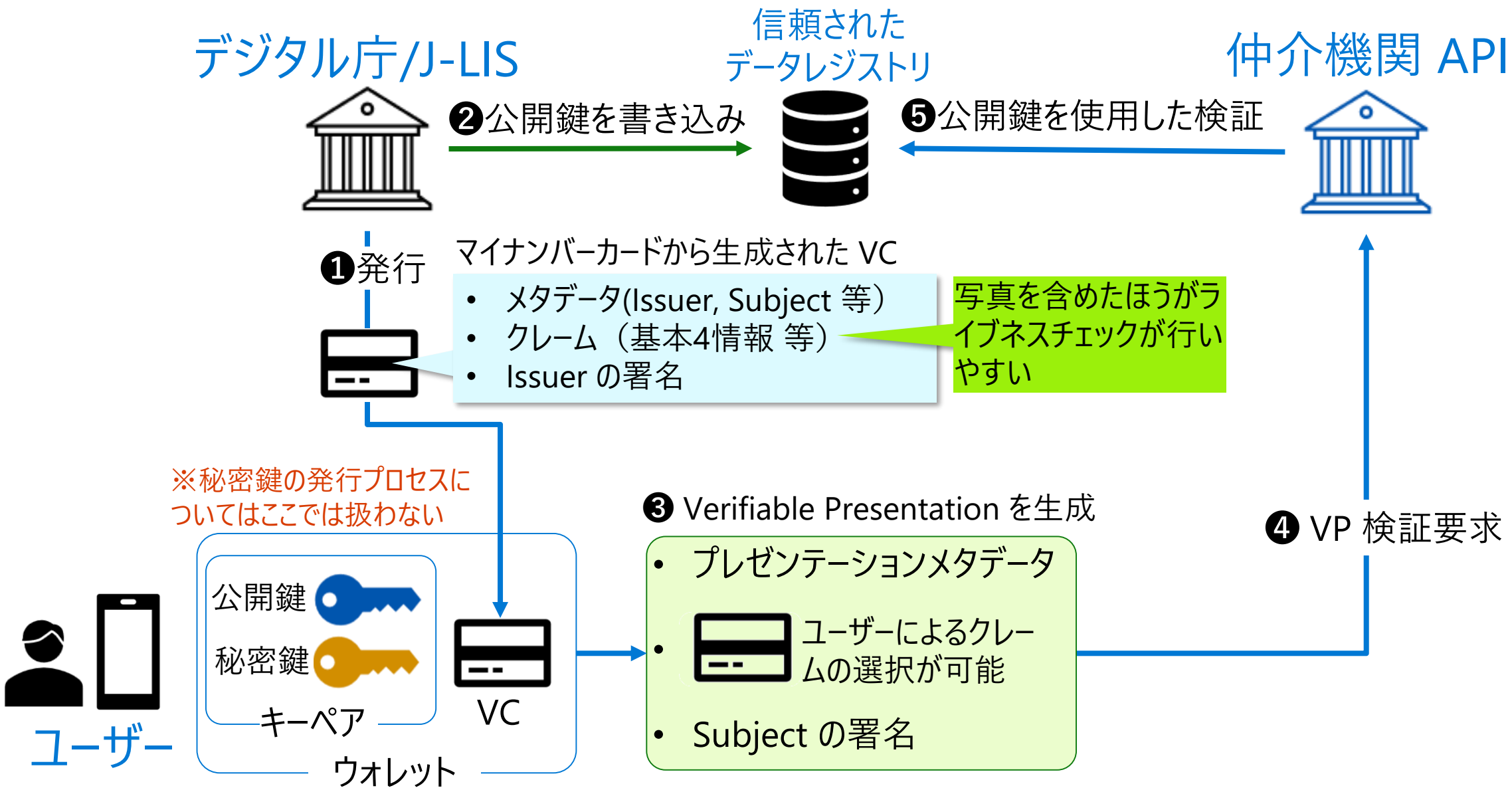
デジタル証明書アプリ「IATAトラベルパス」の実証実験を羽田＝ホノルル・ニューヨーク線にて実施します｜プレスリリース｜ANAグループ企業情報 (anahd.co.jp) より

# 政府主導 VC の例

## EU Digital Identity

- 2023年11月8日 EU理事会と欧州議会で合意
- 想定用途：公的サービス、銀行口座の開設など幅広い活用を目指す
- 認証に関する技術要件
  - Person Identification Data（PID）
    - **ISO/IEC 18013-5:2021で規定されたデータモデルおよび、W3C で標準化されている VC（Verifiable Credentials）データモデル1.1に準拠**
  - PID 認証
    - 属性情報の選択的情報開示がデータモデルに応じて JWT（SD-JWT）とモバイルセキュリティオブジェクト（ISO/IEC18013-5）スキーマを用いて利用できるようにしなければならない。
  - 認証交換プロトコル（Attestation exchange Protocol-1）
    - **欧州デジタル ID ウォレットは、Type1（顔写真などの高い身元確認レベルを要求される認証）では OpenID4VP をサポートしなければならない。**仮名認証が求められた際には、リクエストパラメーターに OpenID SIOPv2 に準拠して指定されるとよい。

# VC の発行と、VC を使用した認証（検証）



# Verifiable Credentials に関連する標準

| テクノロジ スタック コンポーネント | オープン標準 | 標準化団体 |
|---|---|---|
| データ モデル | Verifiable Credentials Data Model v1.1 | W3C VC WG |
| 資格情報の形式 | JSON Web Token VC (JWT-VC) - JSON としてエンコードされ、JWS として署名されます (RFC7515) | W3C VC WG /IETF |
| エンティティ識別子 (発行者、検証者) | did:web | W3C CCG |
| エンティティ識別子 (発行者、検証者、ユーザー) | did:ion | DIF |
| ユーザー認証 | Self-Issued OpenID Provider v2 | OIDF |
| プレゼンテーション | OpenID for Verifiable Credentials | OIDF |
| クエリ言語 | Presentation Exchange v1.0 | DIF |
| DID (分散化識別子) 所有者の信頼 | Well Known DID Configuration | DIF |
| 無効化 | Verifiable Credential Status List 2021 | W3C CCG |

# 参考 ～ OpenID4VP とは

- 分散型 ID 環境で検証可能なクレデンシャルを交換するためのプロトコル。
- OAuth 2.0 の上に構築され、検証可能なクレデンシャルを検証可能なプレゼンテーションとして提示するためのメカニズムを定義している。
- OpenID4VP は、エンドユーザーがウォレットを使用して検証者に検証可能なプレゼンテーションを提示するためのコンテナとして VP トークンを導入し、VP トークンには、同じまたは異なるクレデンシャル形式の1つ以上の検証可能なプレゼンテーションが含まれる。
- この仕様は、OpenID Connect Working Group の成果物であり、Decentralized Identity Foundation (DIF) や ISO のワーキンググループと連携して標準化作業が行われている。
- 略語として「OID4VC」、「OID4VCI」、「OID4VP」が使われることがあるが、これらはすべて「OpenID for VC」、「OpenID for VCI」、「OpenID for VP」と発音する。

# 当初の課題とその解決策

- **本人確認手法の保証レベル**
  - マイナンバーカードの IC チップ情報のみによる本人確認
    （身元確認 IAL レベル3、当人確認 AAL レベル3 相当）
- **仲介機関が保持するアカウント情報の信頼性**
  - マイナンバーカードの IC チップ情報のみを信頼する
- **仲介機関等の運用にかかわるコスト**
  - プラットフォーマーが持つ VC や ID セレクター機能の活用が活路か？
- **プライバシー保護**
  - 提供される情報はワ方式と同等ではあるが、今後のユースケースの拡大に伴い VC により提示する情報をユーザーが選択可能ではあることのメリットは大きい
- **ユーザビリティ**
  - スマートフォン内に保存された VC の提示で完結

# 課題とディスカッションポイント

- **取引の重要度に応じた認証強度の変更**
  - マイナンバーカードのパスワード入力の有無
  - ライブネスチェックの有無　等
- **VC とマイナンバーカード内電子証明書の有効期限の一致**
  - マイナンバー更新時の VC 更新
  - 転居時の VC 再発行プロセス
  - VC の有効期限と、それに伴う口座等の有効期限の考慮
- **事故対応**
  - マイナンバーカード紛失時の VC 無効化プロセス
  - スマートフォンやウォレットの破損
  - スマートフォン紛失
- **検証者の実装コスト**
  - プラットフォーマーの既存 VC 製品との接続性
- **「信頼されたデータレジストリ」の管理とプライバシー**
  - 共同化センターによる運用
  - パブリックなブロックチェーンの活用


Microsoft

Orchestrating a brighter world NEC

別添２
日本電気株式会社

【CBDC フォーラム】
WG3）テーマ:KYCとユーザー認証・認可

第9回会合 プレゼン資料

# CBDCにおける認証・認可の整理
# ～仲介機関の共同化について～

2024/07/05 日本電気株式会社

# Agenda

1. 本日のテーマ
2. 前提事項の確認
3. 共同化のモデルケース検討
4. Pros&Cons
5. 考察ポイント
6. ディスカッションポイント

# 1. 本日の議論テーマ

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。

# 本日の議論テーマ（第9回目）

| | 開催（予定）日 | 議論テーマ |
|---|---|---|
| 第1回 | 2023年10月25日 | 日本銀行よりWGの概要、議論の前提、進め方等を説明 |
| 第2回 | 11月21日 | （プレゼンテーション）提供している資金決済サービスにおける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<br>（ディスカッション）身元確認方式のセキュリティとユーザビリティのバランス、当人認証における課題、AML取引モニタリング上の留意点 |
| 第3回 | 12月11日 | |
| 第4回 | 2024年1月24日 | AML/CFT業務実施状況の現状および最新動向の整理 |
| 第5回 | 2月15日 | KYCの現状および最新動向の整理 |
| 第6回 | 3月下旬頃 | 当人認証の現状および最新動向の整理 |
| 第7回 | | 認証・認可のユースケース、システム実現方式の現状および最新動向の整理 |
| 第8回 | 4月以降 | 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 |
| 第9回 | | |
| 第10回以降 | | 必要に応じて追加テーマを設定 |

全体の
まとめを行う会

# 仲介機関の共同化についての仮説考察

## 「本日の議論テーマ」

前回までの議論を踏まえて、CBDCシステムにおける※「仲介機関の共同化」を行った場合、これまで出された課題が解決できそうか、もしくは新たな課題がありそうか等を仮説を立てて考察する

※「仲介機関の共同化」＝仲介機関機能・システムの共同化の意味合い

# 2. 前提事項の確認

# 議論の展開前提

・本仮説はCBDCの共同化について決定づけるものではなく、あくまでも仮説である

・KYC/AML/認証・認可における部分を中心に考察し、その他周辺部分は深く考察しない

・共同化しない場合も比較対象とする

・共同化における法的な見解は除外する

# 第8回会合の論点まとめから

ガイドラインの是非、身元確認の強度など各仲介機関バラバラの懸念、コスト面の課題などのコメントを頂いた

| カテゴリ | ご意見 |
|---|---|
| ユニバーサルアクセス | ・誰でも同じように使える必要は必ずしもない。使いやすくすると事故の起こる可能性は背反なので一定の線引きはあった方が良い |
| 不必要な身元確認 | ・過度に本人確認し過ぎるとUXが下がる<br>・送金パターン（本人宛口座）や金額ベース（10万円以下）での線引きなどリスクに応じた確認が重要<br>・名寄せの考え方で見て同一判断できるかはハードルが高い<br>・対面チェックはコスト面から不合理 |
| ガイドラインの是非 | ・国際標準は見ておくべき。チェックリストは形骸化しやすい<br>・どこが出すか（お墨付き機関の有無）<br>・順守状況の確認と罰則は必要？<br>・テクノロジー面だけのチェックでよいか？ |
| 共同化 | ・地銀の目線では共同化で実施できる形が良い<br>・不正利用されたことに気づくのは銀行から連絡あってから、責任を取ろうにも「正解データ」がない。サービス事業者を使うのであれば不正利用、黒かどうかってわからないから、グレーの段階で止めないといけない。このあたりの責任をどうするのか、そこもハードルになるはず。「正解データ」を募る仕組みが必要だがインセンティブが無いと協力はされないと考えられる。 |

# CBDC関係府省庁・日本銀行連絡会議 中間整理（令和6年4月17日）（概要）より

**【利用者情報・取引情報の取扱い】**

○ **プライバシーの確保が前提**。その上で、**情報の利活用を通じた利便性の向上や公共政策上の要請への対応とのバランスを図る**必要。

– **仲介機関**は、個人情報保護法など**関係法令を踏まえ、適切に情報を取り扱う**ことが基本。

– **日銀**は、**取り扱う情報の範囲は必要最小限**とすることが基本。例えば、可能な限り取得・保有することがないよう設計。仮に取得・保有する場合も、匿名化などの措置や、不要になれば消去。

– **政府**は、現在の仕組みと同様、AML/CFTをはじめ**公共政策上の目的に基づき、必要に応じて情報提供を受ける**ことが基本。その目的や対象を事前に明確にしておく必要。

○ **不正利用対策**の観点からは、既存の決済手段と同様、**本人確認等を行う必要。マネロン事犯・サイバー事案の取締**の観点からは、利用者が特定され、CBDCの犯罪収益等としての移転や不正アクセスによる情報流出等の痕跡が追跡できることが望ましい。その上で、

– 例えば、**取引額上限の多寡に応じて、利用者の提供するべき情報の範囲を設定することも選択肢**と考えられるが、**今後の国際動向も見ながら検討**を深めていく必要。

– **非居住者による利用**は、本人確認等は困難と想定される一方、他の決済手段を国内で容易に利用可能。利用者の範囲は、**当面国内居住者**としつつ、**非居住者は今後の検討課題**。

○ 仮に非居住者との取引における利用を認める場合、経済制裁措置の実効性確保など**外為法の法益を確保**できる制度設計とする必要。

【プライバシー確保】
・情報の利活用と公共政策上の要請バランス
・仲介機関は適切な情報の取り扱いが必要
・日銀は必要最低限の情報のみを取り扱う
・政府は公共政策上の目的により情報提供を受ける

【不正利用対策】
・本人確認等を行う必要性
・マネロン事案・サイバー事案の取り締まり（利用者の特定や追跡が可能な状況）
・取引額の上限の多寡に応じた利用者情報の取得範囲の設定

# CBDC関係府省庁・日本銀行連絡会議 中間整理（令和6年4月17日）（概要）より

**（１）日本銀行と仲介機関の役割分担**

○ **現金同様、仲介機関が日銀と利用者の間に立ち、CBDCの授受を仲立ちする「二層構造」**が適当。

**【日銀の役割】**

○ 日銀が一元的に発行するため、**CBDCの記録・確認を正確に行うための仕組み（台帳等）の管理**を行うことが適当。**民間決済サービスの高度化を図るといった「触媒」**としての役割も求められうる。

○ 技術面のあり方は、トークン型や分散型台帳技術といった技術を活用するかも含め、引き続き検討。

**【仲介機関の役割】**

○ **利用者に基礎的な決済手段を提供**する観点から、

① 日銀との間において、**発行・還収に関する業務**

② 利用者との間において、**流通に関する業務**（例：取引の開廃手続・顧客管理、スマートフォンアプリ・カードなどの提供、払出・移転・受入依頼への対応）

を担う想定。それぞれの経営実態や意思・能力に応じて業務を行うことができるよう、柔軟で幅広い選択肢が認められることが望ましい。

○ **追加サービス**（例：家計簿サービス、条件付き決済サービス）は、民間の創意工夫を促す観点から、公正な競争条件を確保しつつ、**他の民間事業者も参入できる方向で検討。**

**【仲介機関の範囲と規制のあり方】**

○ **仲介機関の範囲**は、**求められる業務内容を整理していく中で検討。**現在決済サービスを提供している**銀行をはじめとする預貯金取扱金融機関やその他の事業者は、その役割を担いうる。**

○ **仲介機関への規制のあり方**は、**制度設計の具体化に併せ議論**を進めていくべき。

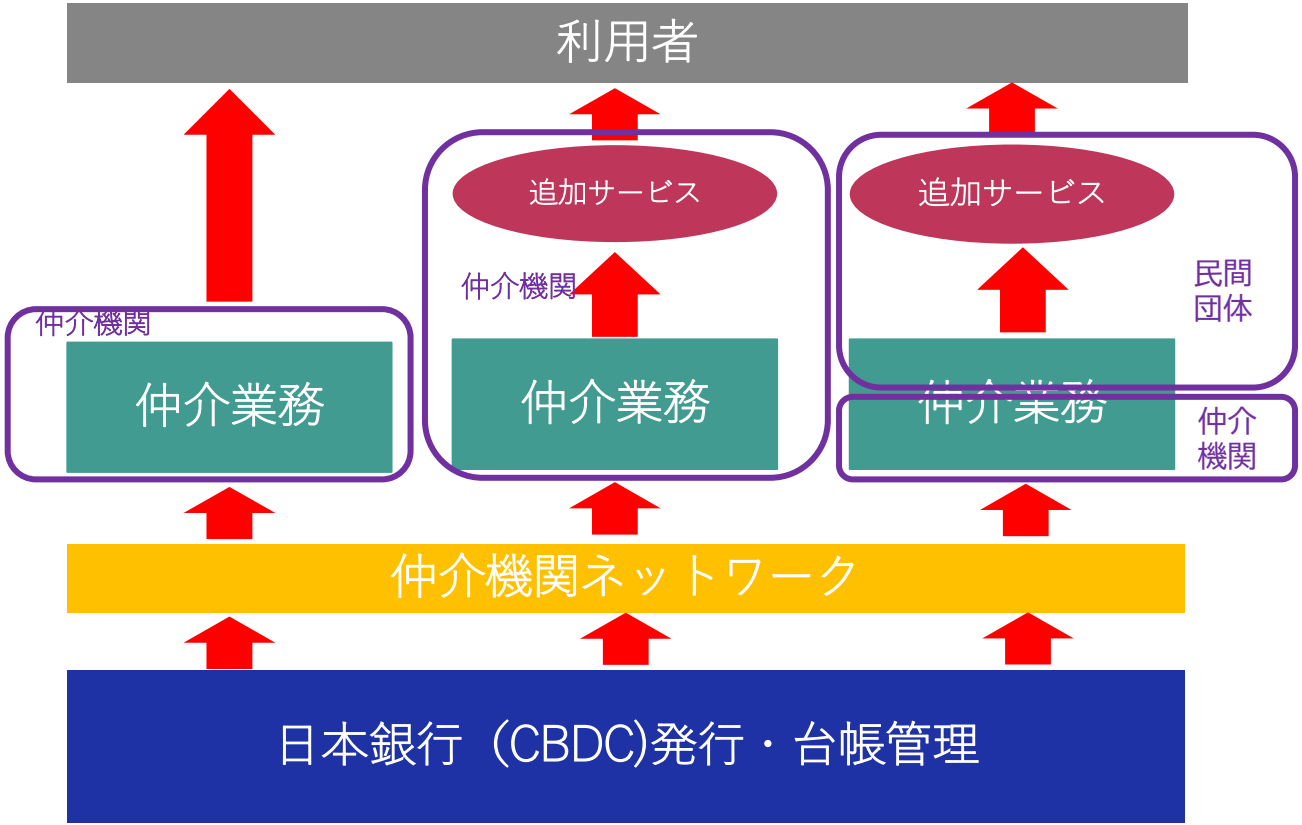
【日銀の役割】
・CBDCの台帳管理
・民間の高度決済サービスの高度化への触媒

【仲介機関の役割】
・日銀との間の発行・還収に関する業務
・利用者への決済手段の提供
・利用者間の流通をするための業務
・追加サービス

【仲介機関の範囲】
・銀行をはじめとする決済サービス事業者

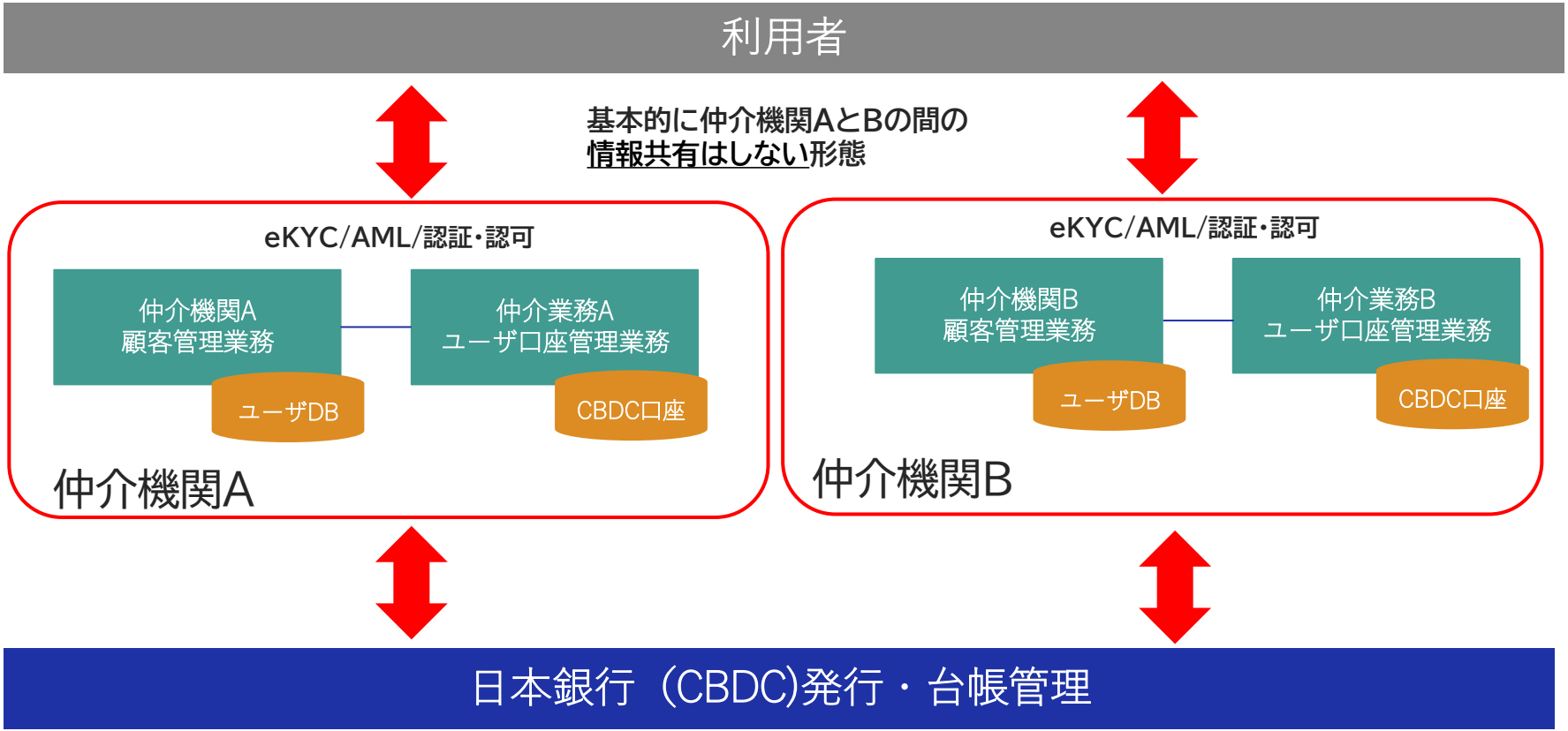
# 3. 共同化のモデルケース検討

# 前提モデル（連絡協議会「中間整理」（2022年5月））



# 1)共同化しない場合

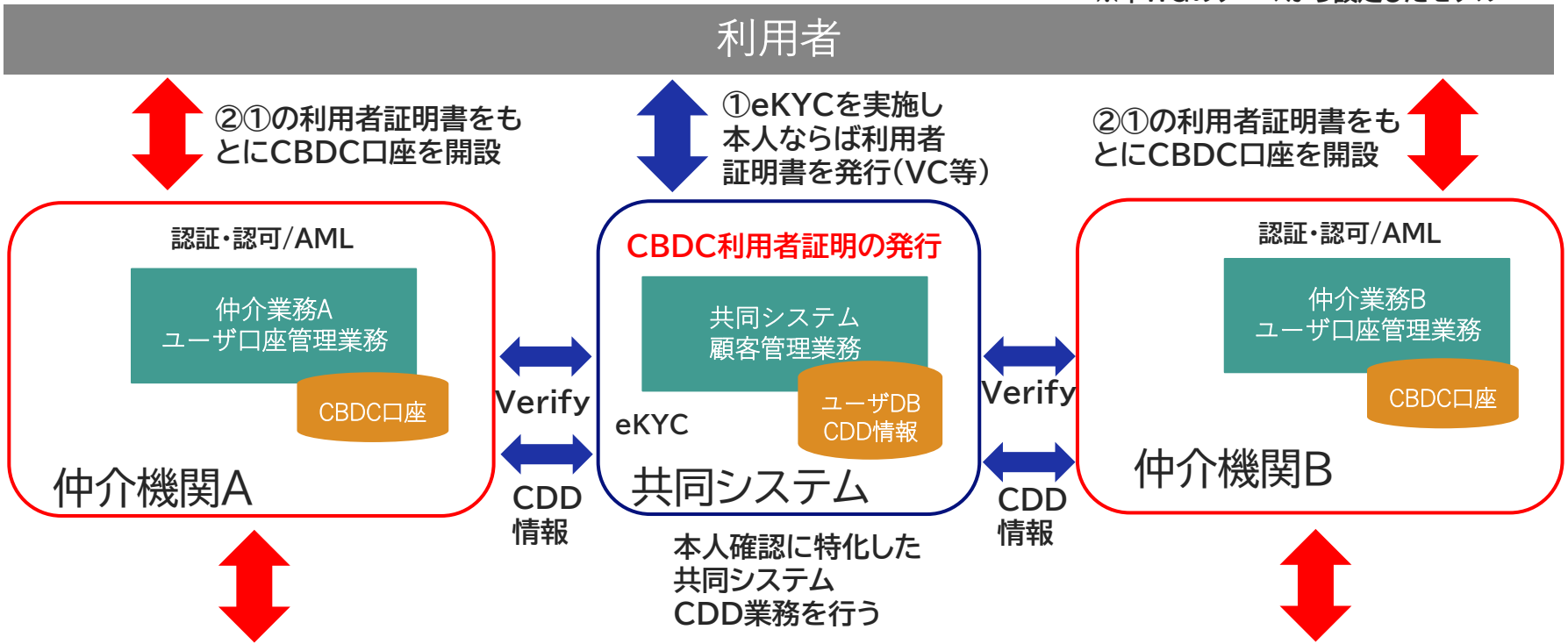
共同化なしモデル



# 2)顧客管理業務を共同化する場合

顧客管理共同化モデル

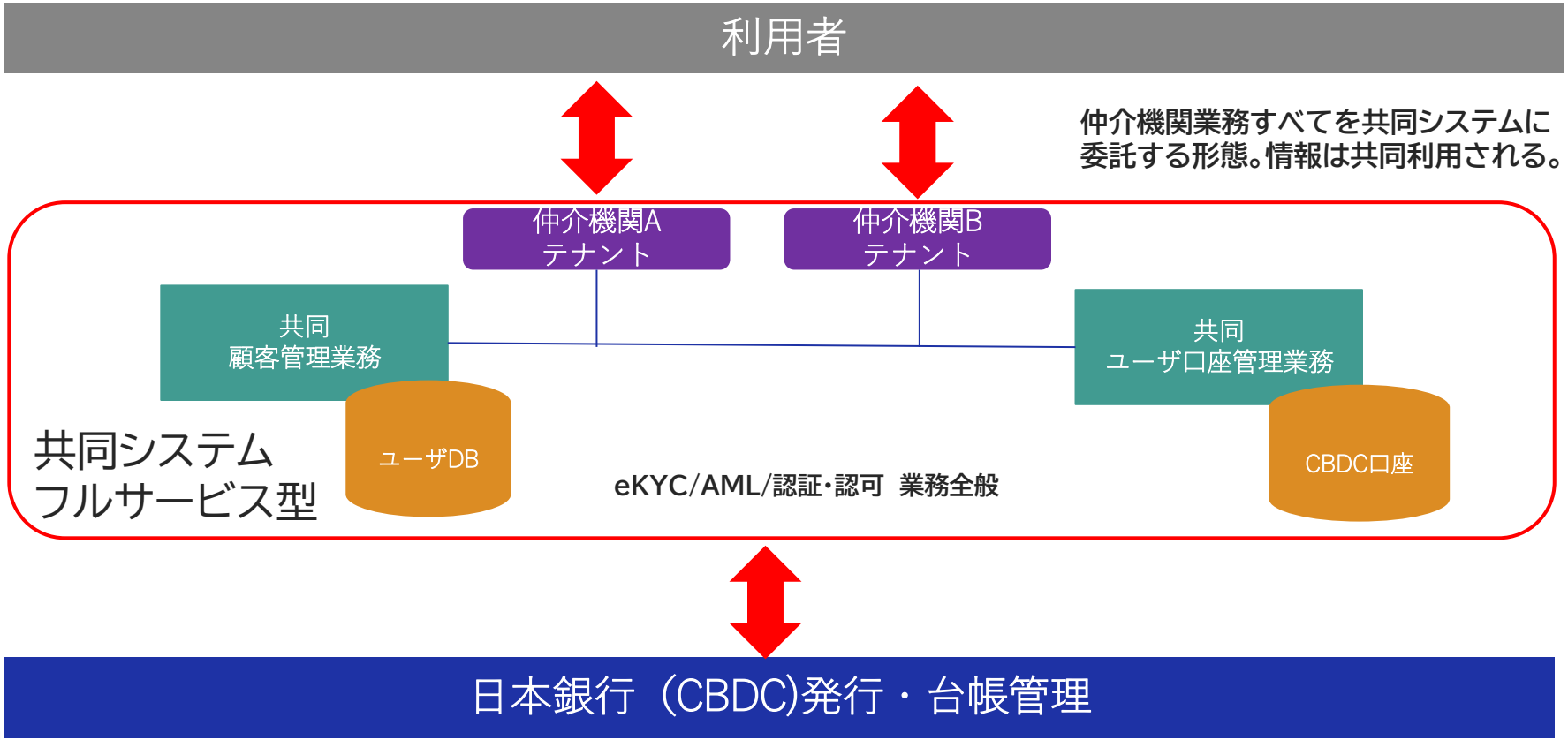
※本WGのテーマから設定したモデル




※CDD: Customer Due Diligence(顧客管理)

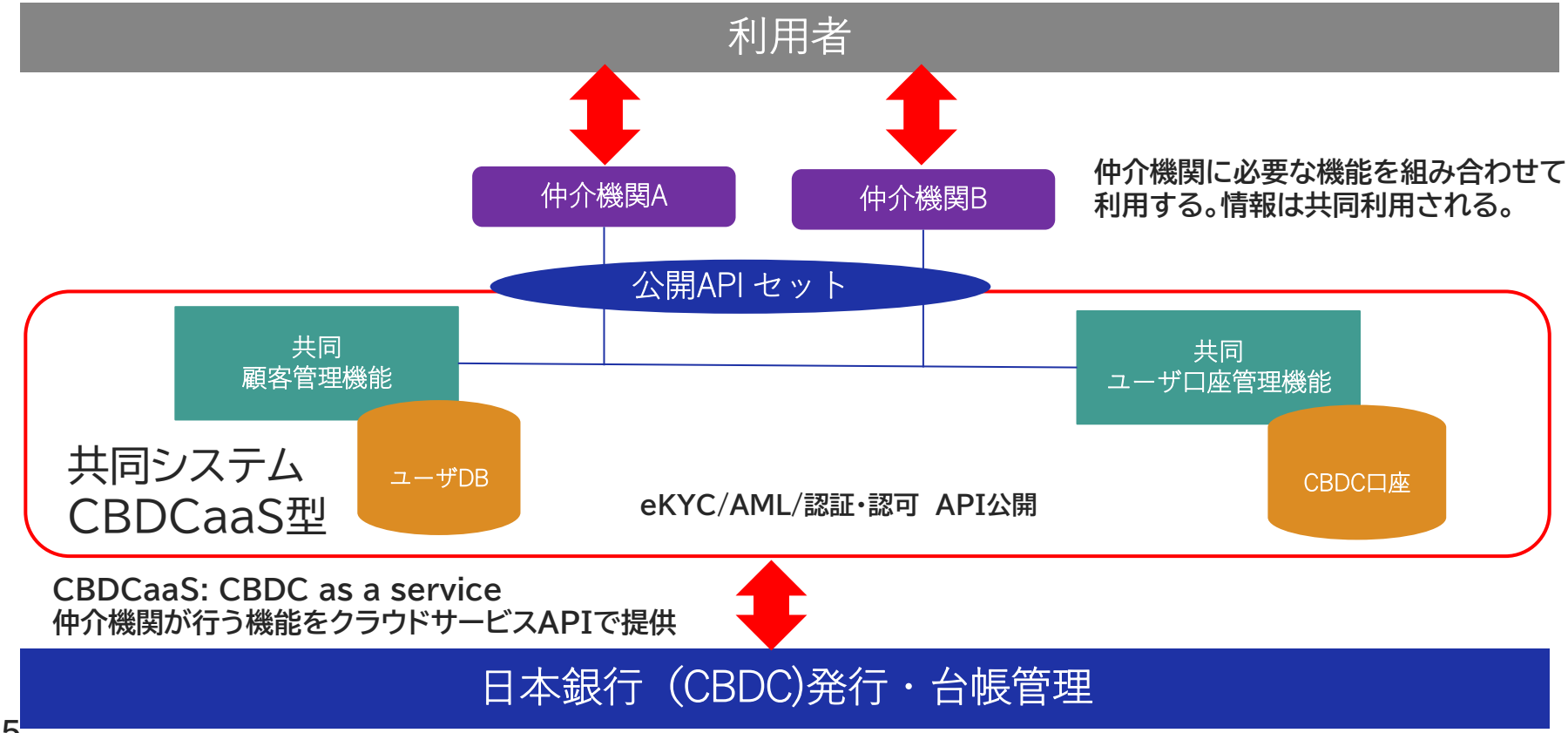
# 3)仲介機関業務すべてを共同化する場合

セントラルモデル
フルサービス型



# 4)仲介機関業務をBaaSで共同化する場合

セントラルモデル
CBDCaaS型



# 4. Pros&Cons

# 仲介機関の共同化のメリット・デメリット

| メリット | 説明 |
|---|---|
| 効率性の向上 | 共通のプラットフォームを使用することで、取引コストや事務コスト、システム運用コストが削減できる可能性<br>また、共同化により他領域（競争領域など）へのリソース配分が可能になる |
| 互換性の確保（標準化の導入） | 異なる仲介機関間でのデータ交換やシステム連携がスムーズになる可能性<br>（国際間取引にも有効） |
| 負荷分散のコントロール | 各々の仲介機関に過度の負担がかからず、システム全体の安定性が向上する可能性<br>負荷分散を集中的にコントロール可能 |
| 高度化 | 共同化によって集められたデータの利活用が可能になり処理が高度化する可能性<br>（AMLの高度化など） |

| デメリット | 説明 |
|---|---|
| セキュリティリスクの増大 | 共通のインフラが攻撃を受けた場合、影響が大きくなる可能性<br>ただし、共同化により対策が打ちやすい側面もあり（P23参照） |
| 運用の複雑性の増大 | 複数の仲介機関が共同で運用するため、調整や管理が複雑になる可能性<br>ただし、ガバナンスコントロールがきちんとできれば共同化のメリットにもなる |
| 競争の抑制<br>（イノベーションの抑制） | 共通プラットフォームの利用により、各仲介機関間の競争が減少する可能性（差別化が困難）<br>ただし、CBDC as a Service 型によりAPIの組み合わせによる自由度は上がる |

# 各仮定モデルの比較整理（Pros＆Cons）

| | メリット | | デメリット | |
|---|---|---|---|---|
| 共同化なしモデル | 効率性 | 仲介機関毎の業務のため効率的ではない | セキュリティリスク | 個社毎のリスク |
| | 互換性 | データや機能の互換性の必要はない<br>（I/Fの標準化は必要） | 運用の複雑性 | なし |
| | 負荷分散 | 仲介機関が分散していることで負荷分散されているが、全体としてのコントロールはできない | 競争の抑制 | なし |
| | 高度化 | 全体でのデータの利活用ができない | コスト | 事務コスト、システムコストが仲介機関毎に発生 |
| 顧客管理共同化モデル | 効率性 | 顧客管理部分は効率化される | セキュリティリスク | 顧客情報が集中することのリスクあり |
| | 互換性 | データや機能の互換性を保つための標準化が必要 | 運用の複雑性 | 運用の複雑性が増大する |
| | 負荷分散 | 共同化部分がボトルネックになる可能性はある | 競争の抑制 | ほぼ抑制されない |
| | 高度化 | 顧客管理部分のデータの利活用が可能 | コスト | 顧客管理部分を共同化することで一部分は下がる可能性あり |
| セントラルモデル<br>（フルサービス型）<br>（CBDCaaS型） | 効率性 | 効率的<br>共同化により他領域（競争領域など）へのリソース配分が可能になる | セキュリティリスク | すべての情報が集中することでリスクが増大するが対策は打ちやすい側面もあり |
| | 互換性 | 統合化された機能を提供できる | 運用の複雑性 | 運用の複雑性が最大となるが、ガバナンスコントロールがうまく働けばメリットとなる可能性もあり |
| | 負荷分散 | 処理が集中的に発生しシステムへの影響が大きくなる可能性があるが、負荷分散のコントロールはしやすい | 競争の抑制 | 機能が固定化（共通化）する懸念があり、競争が抑制される懸念があるが、CBDCasS モデルでは問題にならない可能性もある |
| | 高度化 | データの利活用が可能 | コスト | 事務コスト、システムコストが大きく下がるが、運用が複雑化しコストが下がらない可能性もあり |

# ご参考：共同化や統合化によりコストが増加してしまった事例

**事例1: アメリカ合衆国のヘルスケア企業**
　ある大手ヘルスケア企業は、複数の病院やクリニックを運営していた。コスト削減のために、電子カルテ（EHR）システムを統合するプロジェクトを実施した。しかし、各施設が独自のワークフローとプロセスを持っていたため、統合後のシステムは非常に複雑になった。医療従事者は新しいシステムに慣れるまでに時間がかかり、トレーニングコストが大幅に増加した。また、システムのカスタマイズやメンテナンスも複雑化し、結局は運用コストが当初の予想を大幅に上回る結果となった。

**事例2: 日本の地方自治体**
　日本のある地方自治体は、複数の市町村で使われている行政システムを統合しコスト削減を図った。
しかし、各市町村が異なるニーズと要件を持っていたため、統合されたシステムは非常に複雑で、運用が難しくなった。結果として、システムの障害が頻発し、住民サービスの質が低下しました。さらに、システムのトラブル対応や追加のカスタマイズが必要となり、当初の予算を大幅に超えるコストが発生した。

**事例3: 国際的な金融機関**
　ある国際的な金融機関は、各国の支店で使われているバンキングシステムを統合することで、コスト削減を目指した。しかし、各国の規制や業務プロセスが異なるため、システムの統合が非常に複雑化した。
システムのトラブル対応や法規制対応に多大なコストがかかり、さらにシステムの運用と保守にかかる費用も予想以上に増加した。結果として、統合後のシステムは当初の目標であったコスト削減を達成できず、逆にコストが増加した。

# 5. 共同化における考察ポイント

# 考察ポイント1： どこまで何を共同化すべきか

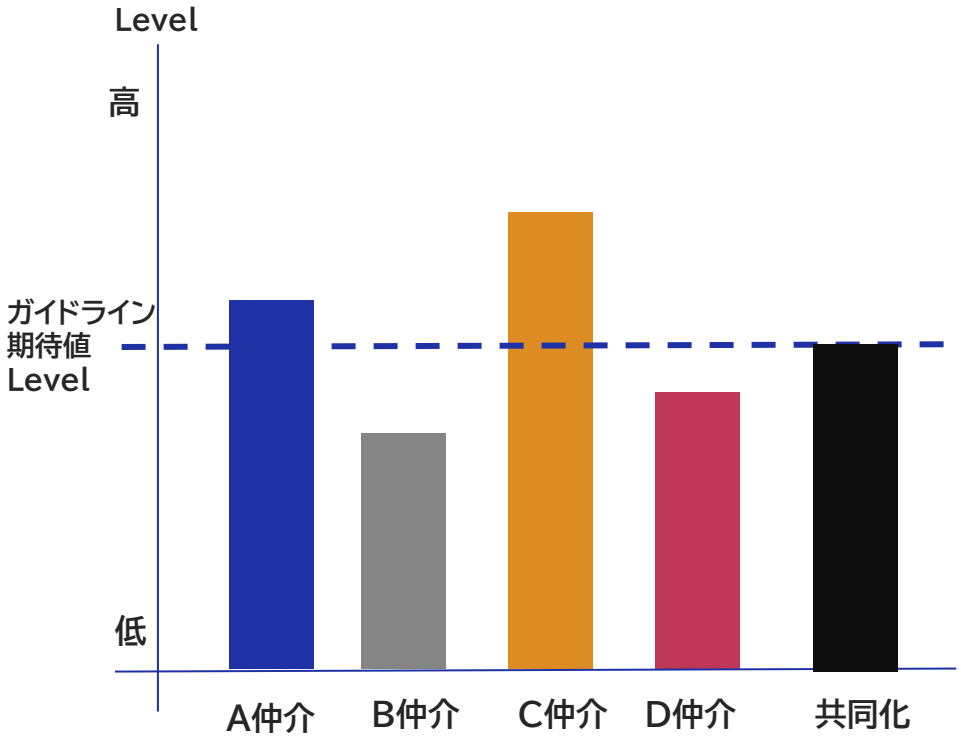
| 共同化の課題 | 懸念事項 |
| --- | --- |
| 機能と業務 | 共通化部分と仲介機関個社部分の機能や業務の明確化 |
| データ | どこまでのデータを共有化するのか十分な検討が必要 |
| 役割と責任分担 | 日銀、仲介機関、利用者の責任範囲の明確化 |
| セキュリティリスク | データを集中で持つことによるリスクの増加 |
| ガバナンスコントロール | チェック機関が必要。第三者評価の仕組みを作る必要あり |
| 事務コスト<br>システムコスト | ・共同化することで下がりそうだが、システムが複雑化することでコスト増の可能性もある<br>・運用コストの按分方法や割合も課題<br>（例：CBDC as a Service で APIのコール数での課金もあり） |

# 考察ポイント2： ガイドラインの必要性とセキュリティレベル

・仲介機関毎にセキュリティレベルを合わせる必要がある

・ガイドラインやチェックリストで目線を合わせても解釈の違いなどにより一定にはならない

・攻撃者はセキュリティレベルの低いところから侵入を試みる



# 考察ポイント3： プライバシー保護、インシデント発生時の影響度

**【プライバシー保護】**
共同化することで利用者の懸念が増大する可能性（意識の高い人の意見）

・**個人データの収集と追跡**： 共同化により収集と追跡がよりしやすくなる
・**目的外利用への懸念**： 別な利用用途に利用される可能性がより増大する
・**政策の乱用**： 政府機関等がCBDCのデータを利用して、特定の個人やグループを監視したり、制限をかけたりする可能性（共同化により監視や規制がしやすくなる）
（法規制と合わせての検討が必要）

**【インシデント発生時の影響度】**
大量のデータが漏洩するリスクが大きくなる可能性

・情報漏洩インシデントが発生時の社会的な影響の大きさが増大
・情報漏洩やなりすまし等が発生した場合の利用者への金銭的補償の検討が必要
金融ADR制度（金融分野における裁判外紛争解決制度）等の活用などの検討
共同化したほうが対応しやすい側面あり

# 参考1:証券コンソーシアム　KYC共通化ワーキンググループ

## 共同化はコスト低減と高度化がポイント

**図5-1：AML/CFTの共通化･高度化のコンセプト**

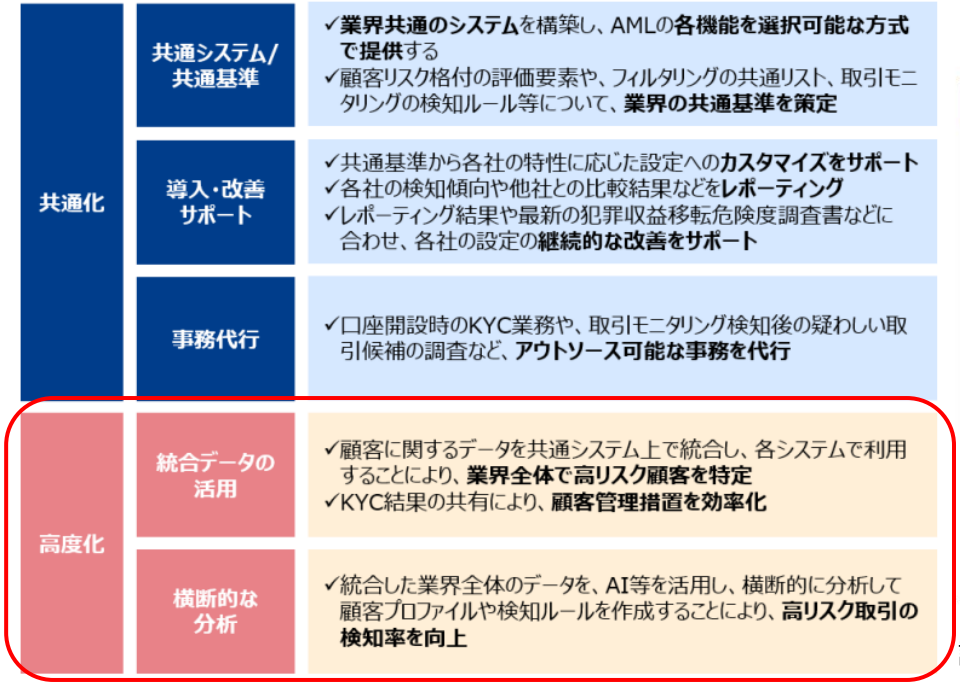



**表5-1：共通システムで実施する事務代行（例）**

| 業務 | 説明 |
|---|---|
| 本人確認 | 口座開設時の本人確認書類の真贋確認（画像/映像を目視）を実施。 |
| フィルタリング<br>（リスト照合） | 本人特定事項を基に、反社DBや民間DB、共通システム管理リスト、個社リスト等への照会を実施する。<br>※RPA･AIで自動化が可能<br>※反社DB照会代行は金融商品取引業者のライセンス取得が前提 |
| 顧客に対しての<br>本人情報確認 | 継続的顧客管理措置における顧客への確認を実施する。<br>（電子メール、郵送等） |
| EDD（追加情報取得） | EDD（追加情報取得）が必要となった際、顧客へコンタクトをとり、情報収集を実施する。（電子メール、電話、追加調査等） |
| 疑わしい取引候補の<br>初期調査 | 検知された疑わしい取引候補について、AIを活用し、取引のリスクスコア･予想届出確率･判定理由等を提示する。 |
| 疑わしい取引の報告 | 疑わしい取引の届出書を作成し、届出報告を代行する。 |

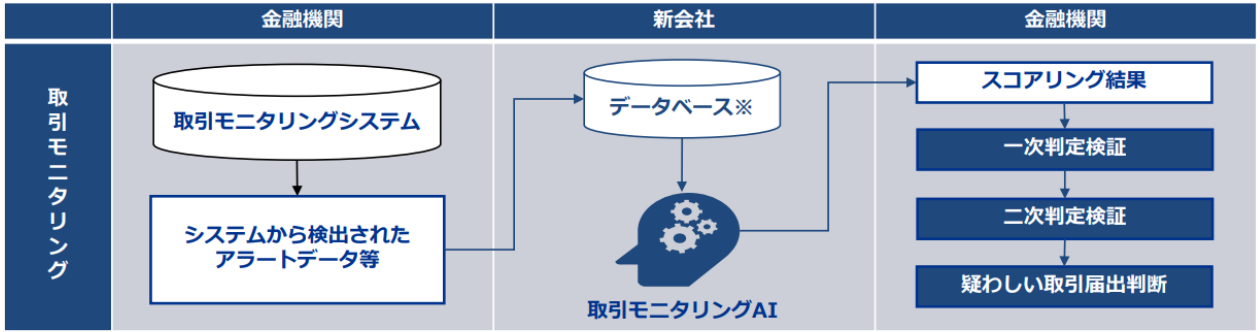
証券コンソーシアム KYC共通化ワーキンググループ　ホワイトペーパーより
https://jpn.nec.com/fintech/kyc/pdf/white_paper.pdf

# 参考2：株式会社マネー・ローンダリング対策共同機構

**AIモニタリング**
**＋**
**業務高度化支援**

| サービス名称 | 提供サービス内容（想定） | 対象と効果 |
|---|---|---|
| **AIスコアリング機能（取引モニタリング）（ネームスクリーニング）** | ● 取引モニタリングシステム・ネームスクリーニングシステムから出力されるアラート・ヒット情報の**リスク度合いをスコア付けするAI機能**を提供<br>● 上記に伴い、AIの処理対象となる**データの品質管理**、**AIシステム自体の有効性検証**を実施 | ● 大量のアラート・ヒット誤検知の対応の効率化<br>● 上記の効率化に伴い、利用金融機関はより幅広いアラートやヒットの検出へのリソース配分が可能に |
| **業務高度化支援（実務基準、FAQs、ヘルプデスク）** | ● 業界共通の取り組むべきテーマ・課題について、**リーディングプラクティス、実務上の実践的な対応事例を策定し、実務基準およびFAQsとして提供**（**ヘルプデスク・研修**を通じた理解促進も補完的に実施）<br>● AML/CFTに係る法制度やガイドライン等の**海外事例調査**、および**中長期的な課題の調査研究**等を行う。 | ● 自行のリスクに応じ、AML/CFTに係る法令およびガイドライン等に基づく態勢の確立・維持が求められている金融機関に対し、対応水準の検討や実効性向上のための効率的な検討を可能とする。 |

**ご参考：AIスコアリングサービスのイメージ**（下図：取引モニタリングの例）




※ 金融機関ごとにデータを分割管理し、金融機関間でデータが混ざることはない構成。

出典：https://www.zenginkyo.or.jp/news/2022/n101302/

# 6. ディスカッションポイント

# ディスカッションポイント

1. 共同化の是非と選択すべきモデル
   それぞれの立場から

2. セキュリティおよびプライバシーの担保
   追加でご意見あれば

3. コスト目線
   それぞれの立場から

4. 共同化による業務の効率化・高度化
   追加でご意見あれば

   その他さまざまな観点からのご意見あれば


Orchestrating a brighter world
NEC