2024 年４月１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５回会合の議事概要

１．開催要領
（日時）2024 年２月 15 日（木）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
日本電気株式会社、株式会社三井住友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）ＫＹＣ業務の現状および最新動向①（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１を参照。

ＫＹＣ業務の現状および最新動向の整理として、一般的なｅＫＹＣの方式とその現状について説明し、想定されるリスクや課題、その対応等を説明する。

代表的なｅＫＹＣには、ホ方式（顔写真付き本人確認書類の撮影＋容貌の撮影）、ヘ方式（顔写真付き本人確認書類のＩＣチップ読取＋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（マイナンバーカードのＩＣチップ読取（暗証番号入力要））がある。
ｅＫＹＣでの確認は、①容貌の一致確認（容貌の撮影画像と顔写真付き本人確認書類の顔画像の一致確認）、②本人確認書類券面の真贋性確認（本人確認書類の券面や厚み等の特徴を撮影した画像から真贋性を目視で確認）、③本人特定事項の一致確認（氏名、住所、生年月日等の一致確認）の３要件に大別できる。ホ方式は①と②、ヘ方式は①、ト（１）方式は②と③を実施している。ワ方式は、ＩＣチップ読取により、署名用電子証明書の有効性の確認を行うだけのため、目視等の人手による確認作業は発生しない。金融機関等の業務量か

ら考えると、最も簡便と言える。

続いて、①～③の確認業務の自動化の可能性について見解を述べる。①容貌の一致確認は、容貌の撮影画像と本人確認書類の顔画像を比較し、その一致度の定量化を行い、各金融機関等によって任意に設定した閾値を超えない場合は不一致と判定することで一定の自動化ができる。②本人確認書類券面の真贋性確認は、人手による目視での確認を要している。③本人特定事項の一致確認は、本人確認書類と金融機関の保有する顧客情報における表記の差異（丁目、番地の記載方法等）を予め加工・整理しておくことで、データの突合が自動化できる。いずれの自動化においても、どの範囲でどの程度まで自動化をするかは、各金融機関等が十分に技術的な評価を行った上で、責任をもって判断する必要がある。

次に、想定されるリスクと不正関連事例・技術を紹介する。ｅＫＹＣの各方式で、様々な不正手段が想定されるが、その中でも本人確認書類の偽造が最も発生しうる不正手段であり、代表的に使われる免許証、マイナンバーカード、在留カードは、いずれも偽造事例がニュースになっている。ＩＣチップの読取を用いる方式でも、不正は起こりうるため、一定の不正リスクは潜在している。例えば、マイナンバーカードとそのパスワードを一緒に付帯している場合、紛失・盗難に伴う不正リスクが大幅に上がる。また、容貌の撮影においても、ディープフェイクを用いた容貌偽装等、新たな技術発展に伴う不正リスクが今後増加していく可能性があると考える。

これらの不正に現行技術を用いて対策する場合の事例を２つ紹介する。

１つ目は、ワ方式とヘ方式を組み合わせる方法である。マイナンバーカードとそのパスワードが一緒に悪意者に渡った場合においても、顔写真付き本人確認書類のＩＣチップから読み取った顔画像と、容貌の撮影画像の一致確認をすることで、所持、知識、生体の３要素を組み合わせた身元確認となり、なりすましへの対策が可能と考える。しかし、手続きのプロセスが増えることで、ユーザビリティの低下に繋がるため、リスクの高いサービスに限定する等、セキュリティとユーザビリティのバランスへの配慮は重要になってくると考える。

２つ目は、一般的にはあまり普及はしていないが、ト（１）方式において開示される金融機関の保有する顧客情報の一部にマスキングを施すことで、悪意者が完全な情報を取得できないようにし、本人確認書類の偽造を防ぐことができると考える。

そのほか、現時点では問題が大きく顕在化していないが、ディープフェイクを用いた不正への対策を考えた場合、米国の独立系評価機関ｉＢｅｔａによって、なりすまし攻撃に対する国際的な評価手法の基準があるため、参考として紹介する。当該基準でレベル２であれば、３Ｄマスク・マネキン等によるディープフェイクが通ってしまう確率が１％以下であり、ディープフェイクに一定程度は対応ができる水準と評価できるのではないか。また、本人がカメラの目の前にいるか否かを判定するライブネス判定において、首を傾ける等の簡易的な動作では、本人確認資料の顔写真を複製し動かすだけで判定を突破される懸念があるため、ウインクや笑顔といった表情の変化を求めることで、不正防止効果が大きくなる。

こうした現状を踏まえ、ＣＢＤＣにおけるｅＫＹＣを検討する上で、①法令、②ユーザビリティ、③最新の技術動向、④システム仕様・コストの４点を留意すべき点や論点として挙げる。①法令は、犯罪収益移転防止法（以下、犯収法）の改正があれば、ｅＫＹＣの各方式にも影響がでる可能性があるため、ＣＢＤＣにおける身元確認を検討する上でも、動向を注視しておく必要があるだろうと考える。②ユーザビリティは、使い勝手が悪く、利用までの手続きが煩雑なサービスは使われない傾向があるため、セキュリティとの間で適切なバランスをとることが重要と考えている。③最新の技術動向は、各金融機関が不正事例への対策として行っている犯収法準拠＋αの対応や、ＡＭＬ／ＣＦＴ対策に対して、どのような技術を採用していくかは、論点となりうる。また、各金融機関において、本人確認書類の偽造などの不正利用に対する対応状況が異なることは、留意しておく必要がある。④システム仕様・コストは、ＣＢＤＣにおけるｅＫＹＣを誰がどうやって実施するかがポイントとなる。仮に各金融機関が実施するとした場合、各金融機関が独自のシステムで実施をするよりも、共同化したシステムで実施をする方が全体的な負担を減らせる可能性があるだろう。また、現時点でｅＫＹＣを実施していない金融機関もあるため、そのような金融機関がすぐに共同化に参加することは、難易度が高いと思われる。そのため、段階的な対応等により、導入までを支援していくことも重要な点と考えている。

（２）ＫＹＣ業務の現状および最新動向②（株式会社三井住友銀行）

―― プレゼンテーション資料の要旨は別添２を参照。

当行が取り組んでいるｅＫＹＣ、および銀行業務におけるＫＹＣの現状を

説明の上、ＣＢＤＣにおいて検討が必要と考えるＫＹＣの論点を説明する。なお、ｅＫＹＣはデジタル技術を活用した非対面（オンライン）での身元確認を指し、ＫＹＣは自らのビジネスモデルが持つリスクに応じた顧客のプロファイリング全般（身元確認を含む）を指すと認識している。

当行では、居住者は国籍に関わらずｅＫＹＣを行うことで、非対面の口座開設申込ができる。日本国籍の居住者は、ｅＫＹＣのホ方式、またはワ方式が選べ、外国籍の居住者は、ホ方式として在留カードおよび特別永住者証明書の２点の撮影＋容貌の撮影のみが対象となる。なお、例外としてＦＡＴＣＡ（外国口座税務コンプライアンス法）による米国税務当局への報告対象者（米国籍保有者、米国居住者等）は、別途確認手続きが必要なため、対面のみで口座開設を受け付けている。

一方、非居住者は、非対面の口座開設申込ができない。非居住者が口座開設後に振込をしようとした場合、その振込は、日本国内間での振込でも外為法（外国為替及び外国貿易法）に則った外国送金の手続きが必要となる。そのため、国内振込用のサービスを主とした個人用インターネットバンキングの仕様では、外為法上許容できない。こうした事情から、非対面の口座開設申込も受付していない。

銀行によるＫＹＣの実施に際しては、顧客が誰で、何をしていて、なぜ銀行の商品・サービスを使用するのか等を理解するために、顧客本人の顧客属性や取引目的等を申告いただいた上で、これらの情報が正しいことを可能な限り調査することが求められる。具体的には、①ＣＤＤ（Ｃｕｓｔｏｍｅｒ　Ｄｕｅ　Ｄｉｌｉｇｅｎｃｅ：標準的な顧客管理）、②リスク格付、③ＥＤＤ（Ｅｎｈａｎｃｅｄ　Ｄｕｅ　Ｄｉｌｉｇｅｎｃｅ：厳格な顧客管理）、④継続的顧客管理と取引モニタリングの４つに分類される。

①ＣＤＤとは、ＫＹＣを行う事業者の目線においては、リスク格付のために必要な情報を収集する行為そのものを指す。当行では、犯収法上の取引時確認である本人特定事項等の確認に加え、国籍、在留資格・期間、経済制裁対象国等の取引・資産の有無等の確認を行っている。

②リスク格付とは、ＣＤＤで得た顧客情報をリスク要因（顧客の属性・事業、提供する商品・サービス、取引の対象となる国・地域）に当てはめてマネロン等リスクの高い顧客を洗い出す行為である。ＡＭＬ／ＣＦＴの観点ではリスクに応じて高・中・低の３段階に分けることが一般的である。

③ＥＤＤとは、リスク格付により高リスクと判断された場合に、実施される追加的な顧客管理措置である。ＥＤＤでは、リスク要因に応じて追加的に情報収集を行い、リスクを許容できるか否か、あるいは許容できる程度に低減でき

るか否かを判断する。
④継続的顧客管理と取引モニタリングとは、取引開始以降に行う、取引状況の確認と顧客毎の継続的なマネロンリスクの把握・評価である。取引開始以降は、顧客属性がライフイベント等に応じて変化すると想定され、合わせてリスクも変動する可能性がある。このため、属性変更の有無を継続的に確認する必要がある。収集する情報はＣＤＤ、ＥＤＤと同じだが、属性変更があった場合、変更によるリスクの増減を見極め、取引方針の見直しを適切に判断することが求められる。また、送金等取引が行われると、プロファイリングした顧客情報と比較して異質な取引が行われていないか、取引モニタリングをする必要もある。取引モニタリングではシステムによる検知および店頭等による気付きで、不自然な取引を抽出する仕組みを構築することが重要である。なお、取引モニタリングにより疑わしい取引に該当した場合は当局あて報告を行うこととなる。

ＣＢＤＣにおいて検討が必要と考えるＫＹＣの論点として、①ＫＹＣ手法、②ＫＹＣ対応の業務負担、③取引モニタリングの課題、の３点を挙げる。

①ＫＹＣ手法は、各事業者が実施している既存の手法を流用してもよいのか否か。例えば、銀行は提供するサービスのリスクの高さから、より強固なＫＹＣが求められている。ＣＢＤＣがどのようなサービスを実現できるか次第ではあるが、ＣＢＤＣの不正リスクやマネロン等リスクを、銀行の既存サービスと同等か、よりリスクが低いとした場合は、既存の手法を流用できるだろう。ＣＢＤＣのリスクは、誰をユーザーと想定し、どのような利便性を提供するか等によるため、ＫＹＣの実施方法やその強度を考えるうえでは、こうしたビジネスモデルが重要な点になると考えている。

②ＫＹＣ対応の業務負担は、口座開設から口座解約まで継続的に発生している。ＣＢＤＣが社会のインフラとして、全ての国民が使えることを前提とするならば、そのＫＹＣコストを銀行から顧客に転嫁することは容易ではないだろう。ただし、ＣＢＤＣで求められるＫＹＣ対応が、仲介機関となる各事業者が行っているＫＹＣ対応の範囲内であれば、追加的なコストは限定的と考えられる。これは、①と同様にＣＢＤＣが誰に、どのような利便性を提供するか次第である。各事業者に追加的なリスク低減策の実施が求められ、追加負担が発生する可能性もあると考えており、こうしたコストに関しては、論点となりうると考えている。

③取引モニタリングの課題は、送金先情報をどのようにして把握するか。第４回会合で説明のあったとおり、顧客情報や決済情報を紐付けてネットワーク化し、包括的に関係性を把握することで精度の高い顧客管理とマネロン等

対策を実現できると考えるが、そのためにも取引日や取引金額のほかに、送金先情報が必要になる。仮に、これらの情報を一元的に管理するのであれば、この課題は解決し、高精度なモニタリングが可能と考える。あるいは、ＣＢＤＣが図書カードのように、保有上限額が少額であることや使途が限定的である等、マネロンや不正利用に向かないサービス設計となるのであれば、最小限のモニタリングに留めることも案としては考えられるだろう。

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、日立チャネルソリューションズ株式会社が担当した。概要は以下のとおり。

【ｅＫＹＣの方式を組み合わせた不正対策】

（参加者）マイナンバーカードを用いてへ方式を実施する場合、ＩＣチップの読み取りに必要なセキュリティコード等の情報は券面に記載されているため、マイナンバーカードの現物があれば誰でも入力できる。その後、ＩＣチップ内に保存されている顔画像と容貌撮影による顔画像の照合を行うが、ディープフェイク等による容貌偽装によって、へ方式単体では突破されるリスクが残る。ワ方式の場合は、マイナンバーカードとその署名用電子証明書の暗証番号が一緒に悪意者に渡ると、不正が可能となる。プレゼン内で紹介のあったワ方式とへ方式を組み合わせる方法あれば、マイナンバーカードの券面記載のセキュリティコード等の情報とマイナンバーカードの暗証番号が必要となり、その上で容貌撮影による顔認証があるため、不正対策が組み合わさって強固になる。ユーザビリティは下がるが、セキュリティを重視する場合の一例としては、有用なものだと考える。

（参加者）昨今、ｅＫＹＣを目にする機会が増え、スマートフォンを使用して銀行口座等を作成する際には容貌撮影が必要、という認識が世の中に定着してきていると感じる。ワ方式とへ方式を組み合わせる方法は、本人が紛失・盗難の被害に遭うケース以外にも、意図的に他人に譲渡したケース等、幅広な不正対策になると考えられる。

【ディープフェイクを用いた不正】

（参加者）ｅＫＹＣの容貌撮影やライブネス判定は金融機関等が提供するスマートフォンのアプリを用いて撮影をすることが多いと思うが、その場合もディープフェイクを用いた不正の対象となりうるのか。

（参加者）対象となりうるだろう。

（参加者）数年前、ディープフェイクを用いてｅＫＹＣが突破される、という論文があったと記憶しているが、ディープフェイクへの対応について考えを伺いたい。

（参加者）ディープフェイクを用いた不正は、今後顕在化する懸念があると考えており、それを防ぐ技術の研究・開発が重要だと考えている。ｉＢｅｔａのレベル２水準の技術であれば、簡易なディープフェイクは看破できるが、１００％防げるわけではないので、ホ方式などの容貌の撮影を行う方式からＩＣチップ読取を行う方式への切り替えを検討していくことも一案と考えている。

【容貌を用いた生体認証】

（参加者）金融機関の中には、生体認証だけ、もしくは生体認証＋暗証番号で一部取引が行える金融機関もあり、災害時での利用を考えた際には、重要なポイントになると考えている。その中でも、容貌は本人確認資料に載っている場合も多いことから、容貌を用いた生体認証は、今後も使用され続けられるのではないかと考えているが、技術的な面での課題はあるか。

（参加者）容貌を用いた生体認証は便利であるが、部屋の明るさや、撮影の角度に影響を受けやすい特徴もある。そうした中、生体認証の精度を高める方法は多角的に研究されており、最近では、容貌＋虹彩といった、複数の生体認証を組み合わせることで、認証の精度を上げる方法もある。ＣＢＤＣの検討では、取引内容やリスクに応じて認証強度を変えることも必要と考えており、そのためには保証レベルを整理することが重要だと思う。

【保証レベルについて】

（参加者）ｅＫＹＣによる身元確認や当人認証の保証レベルを定量化している事例があれば伺いたい。

（参加者）定量化はされていないが、国内におけるｅＫＹＣ方式の身元確認や当人認証の保証レベルは、独立行政法人情報処理推進機構（ＩＰＡ）のデジタルアーキテクチャ・デザインセンター（ＤＡＤＣ）で整理された内容もあり、こうした資料は参考にできると思う。ＣＢＤＣの検討では、保証レベルの整理が十分でなかったり、各仲介機関に保証レベルの判断を任せたりしてしまうと、対応に差異が生じてしまうため、留意が必要だと考えており、その対策として、ｅＫＹＣシステム等の共同化は一つの方法だと思う。

（参加者）共同化した際には、マルチベンダーで開発・運用を行う可能性も考えられるので、その場合は、技術的な設計や運用をどのように実装していくかは、各社の特徴も踏まえた検討が必要だろう。

【仕向先・被仕向先の情報】

（参加者）ＣＢＤＣを扱う事業者でコンソーシアムを形成し、取引情報を一元管理するプラットフォームを作ることも一案と考える。ＣＢＤＣの移転をコンソーシアム内で管理されるＣＢＤＣ口座間に限定すれば、仕向先（送金元）および被仕向先（送金先）の情報がコンソーシアム内で共有されることになり、不正取引のリスクを低減する効果が期待できるだろう。

（参加者）コンソーシアムを形成して、プラットフォームを作る必要性には基本的に同意する。

（参加者）送金を受ける被仕向先の請求に基づき行われるＲＴＰ（Ｒｅｑｕｅｓｔ　ｔｏ　ｐａｙ）型の送金は、被仕向先の情報を一定程度把握することが可能であるが、こうしたＲＴＰ型の送金が当たり前になった場合は、マネロン等対策は容易になるか。

（参加者）ＲＴＰ型の送金では、ビジネス上の取引に基づく請求として取引情報を確認できるため、確認すべき項目が減り、マネロン等対策がし易くなる可能性はあるだろう。ただし、仕向先、被仕向先の双方ともに悪意者である場合、正常なビジネス上の取引と見せかけた不正取引であるため、この点に注意が必要と考える。

（日本銀行）被仕向先の顧客情報の把握が進むことによって、実務的な観点ではどの程度の影響があるのか意見を伺いたい。

（参加者）外国送金は仕向先の銀行において、被仕向先の顧客情報の把握ができる。一方で、全銀ネットを介した国内送金は、被仕向先の顧客情報の限定的な把握に留まる。外国送金は、仕向先から被仕向先の顧客情報や送金目的を受け入れるため、被仕向先を一意に特定でき、予め必要な確認作業を行うことができることから、リスク低減策として効果がある。しかし、収集する情報が多いために確認の手間が増えるとともに、それらが適切かを判断する必要も生じる。結果として、ユーザーの利便性が低下し、銀行の確認体制の維持コストが嵩むことになる。他方、国内送金は仕向先の銀行が把握できる情報は、口座番号・カナ氏名・取引金額のみとなるために、被仕向先を一意に特定することはできず、確認作業も限定的となる。リスク低減の観点からは、外国送金のように把握できる情報が多いことが望ましいものの、国内送金は海外送金と比しても膨大なトランザクションが発生していることから、仮に国内送金でも被仕向先の顧客情報を受け入れて、それとともに確認の手間が増えるとなれば、現在の体制では運営が成り立たないほどの負担が生じることになるだろう。ＣＢＤＣを検討するにあたっては、リスク低減効果と負担のバランスを取るとともに、利便性が低いサービスはユーザーから使われなくなるという視点を持ちながら検討を進めることが重要であろう。

【プライバシー保護と顧客情報】

（日本銀行）仮に事業者間で顧客情報を共有するのであれば、プライバシー保護の観点からユーザーからの同意が前提であると考えるが、その場合、どのようにして同意を得るのか。

（参加者）ＣＢＤＣにおける場合、金額上限や使途制限等によってリスク低減策が講じられていれば取引時ではなく、銀行預金口座とＣＢＤＣ口座間の交換である払出や受入時にモニタリングをする整理もありうるのではないかと考える。
その上で、取引モニタリングを行う必要があるとした場合を考えると、個人情報保護を踏まえた方法は大きく２つ考えられる。１つ目は、第三者に顧客情報を提供することについて顧客から同意をとる方法で、この場合はＣＢＤＣの利用開始時に同意を得る仕組みを考える必要がある。ただし、

同意を求めることがＣＢＤＣ利用促進の阻害要因になることも懸念されるため、ＣＢＤＣのユーザーに対して何らかのインセンティブも合わせて検討する必要があるかもしれない。２つ目は、個人情報保護法の例外規定（個人情報保護法第 27 条）に基づき、顧客同意を得ずに第三者に提供をする方法が考えられる。ただし、正常な取引が大半を占める中、異常取引を検知するために例外規定を用いて、顧客同意を得ずに正常取引を含む顧客情報を共有するという整理は困難ではないか。

【ＡＩ技術活用の課題】

（参加者）ＡＩ技術等を活用することで取引モニタリングにかかる負担は変化するか。

（参加者）現状では、不正が疑われるか否かを判断する必要があり、ＡＩ技術によって効率化できるかもしれないが、ＡＩの判断根拠がブラックボックスである場合は、その結果だけをもって不正取引であるとは判断できない。ＡＩ技術を調査効率化のための補助的な位置付けとして利用し、コスト削減を実現することは可能であっても、人による判断は引き続き必要であるため、一定の負担は残ると考えられる。

【身元確認の実施方法】

（日本銀行）プレゼンテーションでは身元確認の共通化を一つのディスカッションポイントとして示されたが、ご意見を伺いたい。

（参加者）身元確認の共通化は、各社によって様々な考え方があるだろう。例えば、身元確認方法の共通化の場合、自社が既に対応している方法が採用されれば良いが、そうでない場合は新たな開発負担等が生じる可能性があるため、望ましくないと考えることもあるだろう。また、身元確認の共同実施の場合、そもそも他の事業者が行った身元確認済情報をもって身元確認完了とすることは、他の事業者の身元確認済情報が、実際は不正に手続きされたものであると判明した場合の対応に苦慮することが想定されるため、ハードルが高いと考えている。

（参加者）各事業者が個別に対応する労力と、共同センター等が集約して対応する労力を比較すると、後者の方が効率的であり、ひいては社会全体のコ

ストを抑えられることから、身元確認のプロセス自体の共同化はした方が良いだろうと考えている。ただし、プライバシーを保護する観点から個人情報の取扱いには課題も考えられる。
仮に、共同センター等が一括して身元確認を実施するとした場合も、取得した個人情報を仲介機関に共有する際には、ユーザーから予め第三者への情報提供として同意を得るか、もしくは個人情報保護法 27 条５項１号委託提供の場合として整理するか等の検討を行う必要があると考える。そのほか、取得した情報を目的外で利用していると見られるレピュテーションリスクも考えられ、身元確認の実施主体そのものを共同化するとしても慎重に検討を行う必要があると考えている。

（参加者）ＣＢＤＣ口座の管理を行う観点では、オンボーディング時の身元確認のみならず、取引モニタリング等の管理についても合わせて共同化することは望ましい方法の一つと考える。ただし、共同化した場合は、仲介機関や口座を紐づけしている銀行との間での責任の所在や、不正な取引を検出した際の対応について、予め基準や仕組みを検討する必要があるだろう。

（参加者）デジタル庁が、デジタル認証アプリを開発中で、2024 年度中に提供予定としている。現状、事業者が公的個人認証サービス（ＪＰＫＩ）を提供するには、事業者のアプリを作り込む必要があるが、こうした開発負担が軽減される可能性がある。このような公的機関の動きも視野に検討を進めると良いだろう。

（参加者）各事業者は既存の決済サービスにおいて身元確認を実施しているが、仮にＣＢＤＣの身元確認における手続きとしてｅＫＹＣが共通化された場合は、既存の決済サービスとＣＢＤＣは別々に身元確認を求められるという理解か。別々に行う必要がある場合は、ユーザーに不便な印象を与える可能性がある。

（参加者）共通化といっても、これまでの議論で出ているｅＫＹＣの実施主体そのものを共同化して実施する方法とｅＫＹＣの方式や手続きについて共通のルールを定めた上で各仲介機関が個別に実施する方法の２種類が考えられる。いずれにしても、既存の資金決済サービスで身元確認が完了していれば、当該事業者においてＣＢＤＣをオンボーディングする際には身元確認を改めて行う必要はないと考える。ただし、ＣＢＤＣの方が既存の資

金決済サービスとの関係でよりリスクが大きい場合には、リスクに応じた身元確認を別途行う必要があるとの議論はありうると考えている。

４．次回予定

次回の会合は３月 25 日（月）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５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

Orchestrating a brighter world NEC

別添1
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5回会合 プレゼン資料

KYCの現状および最新動向の整理

2024/02/15 日本電気株式会社

Agenda

1. 一般的なeKYCと実施業務概要
2. 想定リスクと不正関連事例・技術
3. 現行技術での対応例
4. 不正対応技術例

1. 一般的なeKYCと実施業務概要

代表的なeKYC手法(準拠法)

一般的に「eKYC」は、犯収法施行規則第6条1項1号の下記4手法が該当

1 6条1項1号【ホ】

本人の顔画像

＋

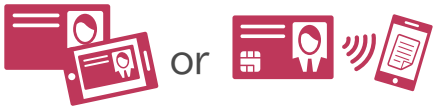
本人確認書類(顔写真付き)
の画像情報

3 6条1項1号【ト(1)】

銀行の保有する情報

＋

本人確認書類(1枚限の発行)
の画像情報 or ICチップ情報



2 6条1項1号【ヘ】

本人の顔画像

＋

本人確認書類(顔写真付き)
のICチップ情報

4 6条1項1号【ワ】

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

必要となる本人確認業務の概要

確認業務は、全手法通して3要件の確認事項を適宜実施

1 6条1項1号【ホ】

【1. 容貌の一致】
・身分証と容貌撮影の顔の一致
【2. 券面の真贋性】
・厚み等の特徴を撮影した画像から真贋性を目視で確認

2 6条1項1号【ヘ】

【1. 容貌の一致】
・身分証と容貌撮影の顔の一致

3 6条1項1号【ト(1)】

【3. 本人特定事項の一致】
・氏名／住所／生年月日の一致
【2. 券面の真贋性】(ICチップ使用時は不要)
・厚み等の特徴を撮影した画像から真贋性を目視で確認

4 6条1項1号【ワ】

特になし

※送信画像が改竄不可である等のシステム的な要件および確認記録等は割愛

本人確認業務の自動化可能性

1. 容貌の一致

- 容貌の一致度を定量化し、閾値以下をNG判定とする自動化が可能
- OK判定を自動判定するための閾値は、事業者により設定される

2. 券面の真贋性

- 撮影画像から真贋性を自動判定することは現状難しい（後述）
- ICチップ読取の方式であれば本要件相当部分の自動化が可能となるが、読取に必要なパスワードのユーザビリティが課題（方式により桁数が異なる）

3. 本人特定事項の一致

- 表記の差異（丁目、番地など）を前処理することで、自動化が可能
- 身分証の本人特定事項をOCR読取する場合は性能評価が必要

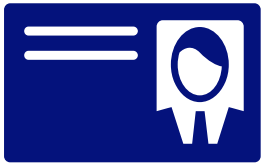
※自動化（＝機械処理）は認められているが、その性能について具体的な基準は定められておらず、性能について特定事業者が責任を持って確認する必要がある

【参考】犯罪収益移転防止法におけるオンラインで完結可能な本人確認方法に関する金融機関向けQ&A No.49, 51
https://www.fsa.go.jp/common/law/guide/kakunin-qa.html

券面撮影画像の真贋判定

券面の画像情報から犯収法レベルの真贋判定を機械的に実施することは技術的に困難
本人確認業務では目視判断を要しているのが実情

真贋判定補助の技術例



【券面情報に対する判定例】
・テキストフォントのチェック
・デザイン(罫線、色、等)のチェック

【厚み情報に対する判定例】
・身分証の角度から厚みを
推定しチェック

実態

精巧に偽造された場合
看破が難しい場合が多い

⇒稚拙な偽造の判定が限界

【参考】資金移動業と「口振依拠」に関して

施行規則第13条で定められる本人確認に関する特例（口振依拠 or 銀行依拠と呼ばれる方法）に関し、資金移動業は適用不可となっている

- ✓ 資金移動業者については原則、公的個人認証やeKYC等による本人確認を事業者側で実施することについて明記（＝規則13条による口振依拠は原則×）
- ✓ 口振連携時の銀行情報との同一性の確認についても氏名、生年月日に加え、住所や電話番号等について確認することが望ましい旨明記
- ✓ パブリックコメント68番*資金移動業者以外の犯収法対象事業者とのイコールフッティングの観点から同様の対応は必要なものと考えている旨が明記

*事務ガイドライン（第三分冊：金融会社関係）、2021年2月26日パブコメ68番

2. 想定リスクと不正関連事例・技術

各手法で想定される不正手段

想定手段のうち、身分証偽造が最も発生しうる不正手段と考えられる

1 6条1項1号【ホ】

【**身分証偽造**】
・券面情報だけでなく、物理的にも精巧な偽造身分証を作成／使用

【**ディープフェイクなどによる容貌偽造**】
・現状表立った問題化はしていないがAI技術の高度化に伴い精巧な偽造の可能性

2 6条1項1号【ヘ】

【**ディープフェイクなどによる容貌偽造**】
・同上

3 6条1項1号【ト(1)】

【**銀行情報の不正取得**】
・不正入手した認証情報による銀行情報提示

【**身分証偽造**】
・同左

4 6条1項1号【ワ】

【**PINコード情報＋マイナンバーカード不正取得**】
・署名用電子証明書のPINコードごと盗難したマイナンバーカードを使用

身分証偽造

身分証偽造は近年より顕在化しており券種問わず事例がある状況だが
機械的な真贋判定は難しく、目視による判定など人的対応による不正検出が主となる

主な身分証として使用される「免許証・在留カード・マイナンバーカード」
はいずれも偽造事件の事例が確認されている


介護送迎車で２人を死亡させた７５歳運転手、運転免許証を偽造した疑いで追送検…「採用が有利になる」と生年月日欄を書き換え

11/8(水) 16:18 配信 17

讀賣新聞 オンライン

さいたま市見沼区の通所介護施設駐車場で９月、送迎車で３人をはね、８０歳代の利用者２人を死亡させたとして自動車運転死傷行為処罰法違反（過失運転致死傷）でさいたま地検に起訴されたアルバイトの被告の男（７５）について、埼玉県警は８日、生年月日欄を偽造した運転免許証のコピーを採用時に提出していたとして、偽造有印公文書行使容疑で同地検に追送検した。

埼玉県警察本部


《ニュース追跡》外国人の在留カード偽造、販売　不法滞在での就労が横行　当局は事業所啓発を強化

公開：2023/9/23 11:30

シェアする ツイート B! ブックマーク この記事をクリップ

外国人が日本に滞在するために必要な在留カードを偽造したとして、群馬県太田市のベトナム人2人が9月に逮捕された。本国に指示役がおり、製造して全国の販売先に郵送していたとみられる。関係者によると、群馬県内でも不法滞在者が偽造カードを使って職を得ている。偽造を見破れなかったふりをして雇い入れる日本人事業者まで存在し、違法状態で生活が成り立ってしまう環境がつくられている。


外国人向けの身分証「偽造工場」を摘発、マイナンバーカードも　警視庁

2023/12/4 11:40

社会 | 事件・疑惑 | 地方 | 関東 東京

外国人向けにマイナンバーカードを偽造したなどとして、警視庁国際犯罪対策課は４日、入管難民法違反の疑いで、中国籍の無職、周桜婷容疑者（２６）＝大阪市大正区泉尾＝を逮捕した。調べに対し、容疑を認めているという。

逮捕容疑は１１月１２日ごろ、自宅でベトナムやインドネシアなどの国籍の男女の在留カード１３枚、マイナンバーカード９枚を偽造したとしている。

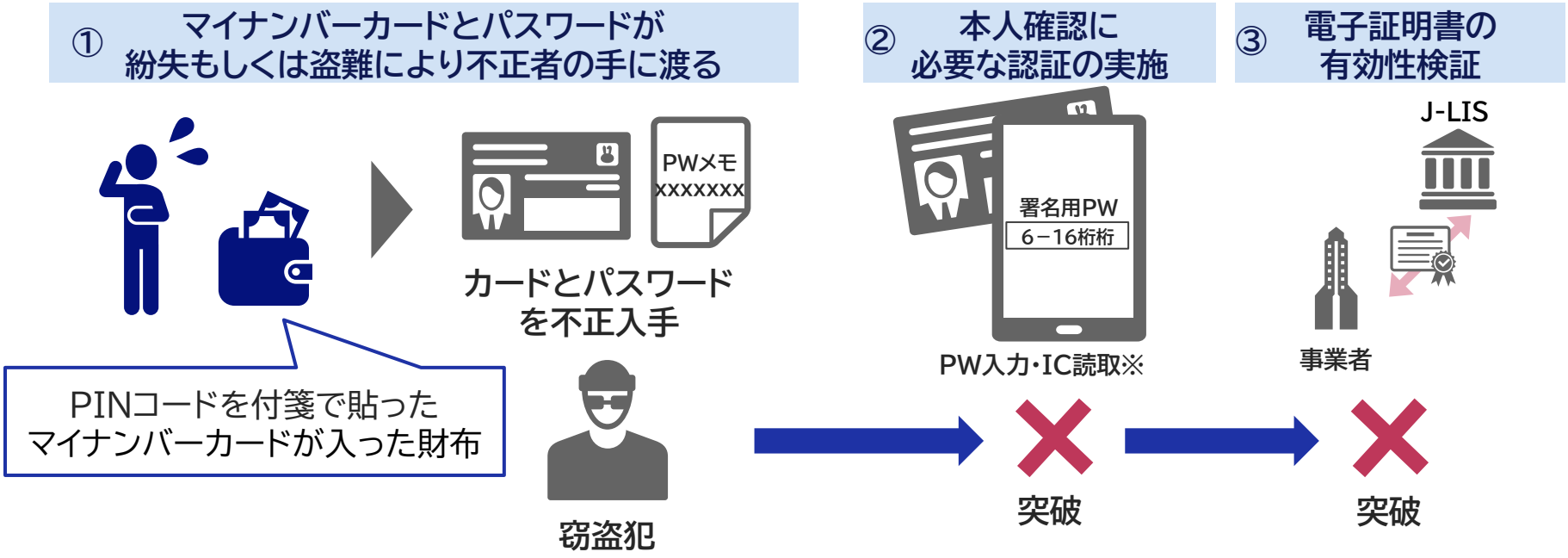
警視庁

先述のとおり偽造身分証を券面画像から検出することは困難、
人的対応による詳細な方法もセキュリティ観点からあまり公開されていないのが実情

読売新聞オンライン(2023/11/8)https://news.yahoo.co.jp/articles/4694bcf088ffd6b2d749e8c572cc43bce4a33bc1
朝日新聞デジタル(2021/5/6) https://www.asahi.com/articles/ASP565752P3TOIPE022.html
産経新聞(2023/12／4)https://www.sankei.com/article/20231204-LV4AXVIV7NJOXC2SIVA4DODDTA/

ワ手法の不正利用で考えられるケース

PINコードを付箋でカードに付帯している場合、紛失・盗難に伴う不正リスクが大幅に上がることが懸念される



ディープフェイク

ディープフェイクによる不正はまだ大きく顕在化していないがAI技術の高度化により今後リスク増となる可能性がある

ディープフェイクとは

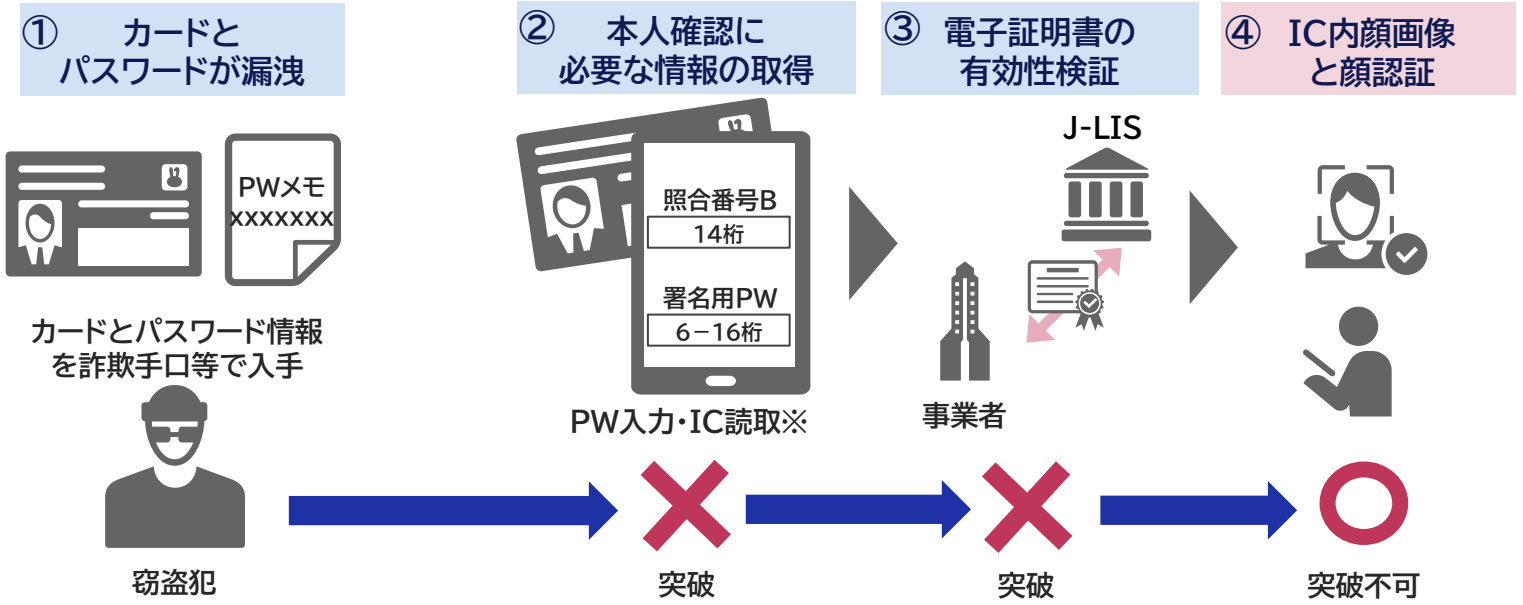
- 「ディープラーニング」と「フェイク」を組合せた造語、AIを用いて人物の映像や音声を人工的に合成する処理技術を指す
- 静止画だけでなく動画の生成も容易化しており、著名人や政治家のネガティブキャンペーンなどの不正が近年問題視されている

出典：FNNプライムオンラインhttps://www.fnn.jp/articles/-/1070

3. 現行技術での対応例

公的個人認証＋顔認証

公的個人認証に顔認証を加えた多段階認証により、不正利用による**なりすまし対策**が可能。（顔認証はICチップに含まれるものを利用するのが望ましい）

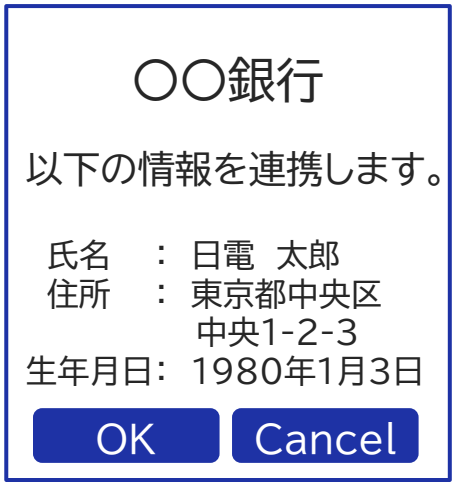


※照合番号Bは券面記載の為、OCRで自動入力も可

ト方式における身分証偽造対策例

使用する銀行情報を一意に特定不可とする表現(マスキング)を施し、
銀行情報に合わせた身分証偽造を防止することが可能

操作者が銀行情報を全て認識できる場合

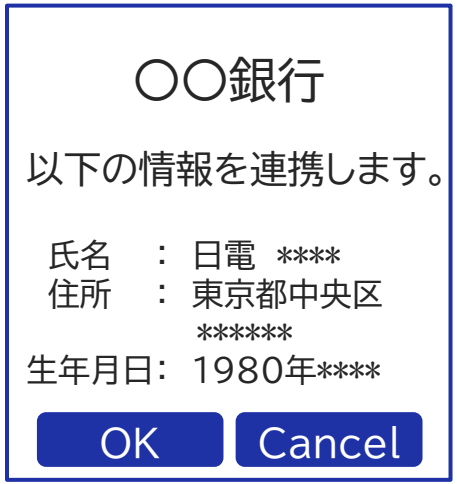


同一情報の身分証が偽造可能

▼

なりすまし可能

操作者が銀行情報を全て認識できない場合



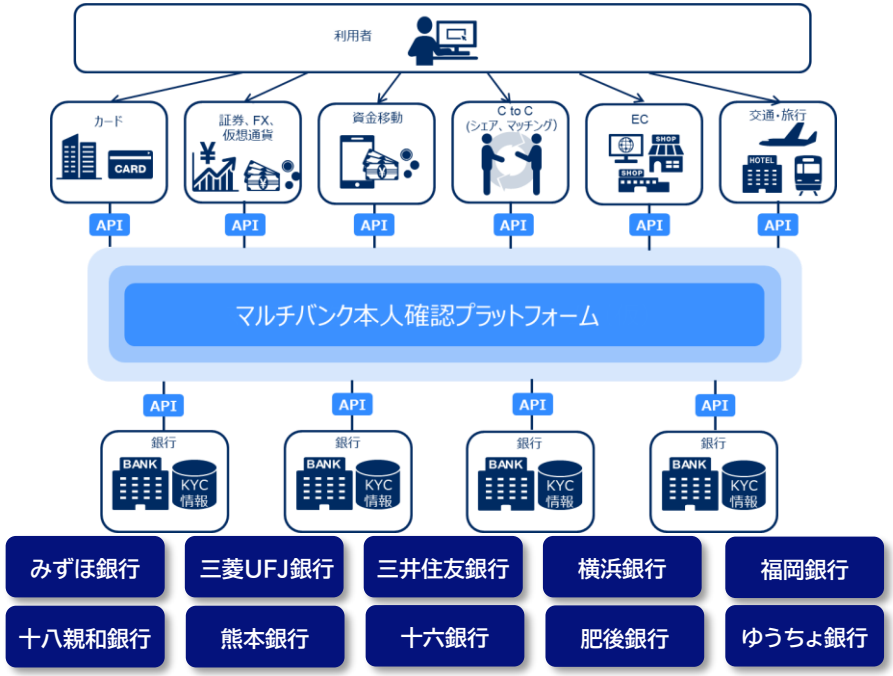
同一情報の身分証は偽造不可

▼

なりすまし不可

【参考】ト方式の提供事例

銀行情報との突合を行うト方式は、個別行ごとの提供では非効率。複数行のAPI接続を束ねるPFerが存在することで解決が可能。（事例：NEC提供のマルチバンク本人確認プラットフォーム）



上記の他、大手銀行、ネット銀行、地方銀行も参加を検討中

本プラットフォームの特長

複数銀行との接続を実現するプラットフォームサービス

- ✓本プラットフォームとの契約およびAPI接続で、接続する全ての銀行の情報が利用可能
- ✓犯収法（規則6条1項1号ト）に準拠したオンライン完結型の本人確認を実現

身分証を用いない本人確認としても利用可能

- ✓本人確認済みのデータであるため、身分証の画像アップロード等に代わる手段として利用可能
- ✓銀行の反社チェックに該当する口座は連携されないため、簡易なネガティブチェックも可能

4. その他の不正対策技術例

ディープフェイク自動検知に向けて

iBetaレベル2相当の技術によりディープフェイクによる不正を検出することが期待できる

iBetaとは

なりすまし攻撃に対する国際的な評価手法として標準化されている
「ISO30107-3,4」への準拠度合を検証する生体認証認定機関（本社：米国・コロラド州）

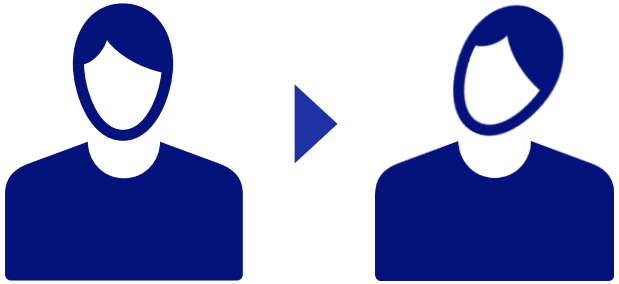
レベル	品質保証内容	iBeta基準値
レベル1	顔写真・ディスプレイによるディープフェイクが通ってしまう確率	通過率0%
レベル2	3Dマスク・マネキンによるディープフェイクが通ってしまう確率	通過率1%以下
その他	本人の顔が本人でないと誤認識される確率	誤認識率15%以下

【参考】https://www.ibeta.com/iso-30107-3-presentation-attack-detection-confirmation-letters/

表情によるライブネス判定

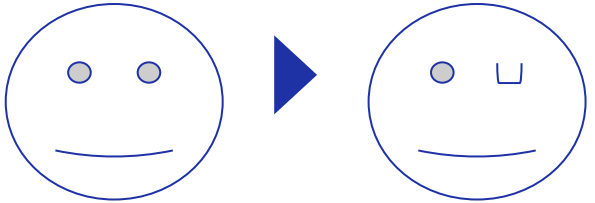
簡易な顔の動作によるライブネス判定は写真等を用いた不正を防止しきれない可能性があるが、顔の表情変化による判定は偽造難度が高く一定の不正防止効果がある

顔の動作のみから判定する場合



身分証の顔写真を複製し指示動作に
併せて動かすことで突破する懸念がある

表情の動作から判定する場合



一枚の写真等では表現困難な指示により
一定の不正抑止効果が可能

総括およびディスカッションポイント

■ 法令
- 犯収法改正の動き：今後eKYC手法の変更可能性あり

■ ユーザビリティ
- デジタルユーロ調査報告書によると“口座開設はできる限り簡便であるべき”と記載あり。日本においても口座開設を簡便にすべきか、簡便にする際の手段を検討すべきか。

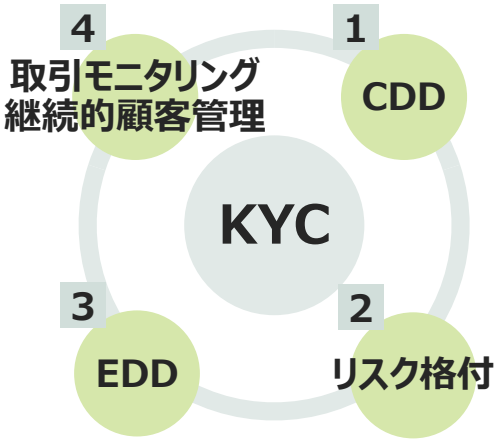
例：
- 既に預金口座を持っている銀行でのCBDC口座開設はKYC情報の名寄せをし、ユーザーアクションを簡便にする（案：ト方式の自行口座情報の参照 等）
- eKYC手法の統一により各仲介機関間でのユーザリティの違いを防ぐ　等

■ 最新の技術動向
- 現在、各金融機関が各自行っている犯収法準拠＋αのKYC、AML/CFT対策をどこまで実施するか
- 身分証偽造など最新不正事例への対策アップデートについて各金融機関対応状況の違い

■ システム仕様、コスト
- CBDCシステムをどう検討するかでKYC共同化システムを検討する際のコストは大きく変動する
- コストの兼ね合い等で現状eKYCを導入していない金融機関の負担

サマリ

1．KYC(Know Your Customer)とは？



1	CDD(Customer Due Diligence/標準的な顧客管理) リスクに関係なく全顧客に対して実施(犯収法上の**取引時確認**等)
2	リスク格付 顧客毎にマネロンリスクを把握するために格付を実施
3	EDD(Enhanced Due Diligence/厳格な顧客管理) CDDを超えて実施される顧客管理措置。より高いリスク特性を示す顧客に対して実施
4	取引モニタリングと継続的顧客管理 取引状況の確認と顧客毎の継続的なマネロンリスクの把握・評価

2．CBDCにおけるディスカッションポイント

（CBDCにおいて事業者がKYCを実施する前提）

- KYCは事業者が行う、**自らのサービスを前提**とした、顧客に係るプロファイリング。
  各事業者のKYC手法を流用してよいのか？もしくは共通の手法を検討するのか？
- KYCは継続的な実施が必要であり、**コストが発生**。
  少なくとも、積極的に実施すべきインセンティブ等が必要ではないか？
- KYC（特に取引のモニタリング）には取引の頻度や額に加えて、相手方（送金先等）の情報も必要。
  金融機関と同定度の強度を前提とした場合、取引相手方の情報はどのように把握するのか？