

2025年7月15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14回会合の議事概要

1. 開催要領

(日時) 2025年5月27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

株式会社三菱UFJ銀行、セコム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) 法人におけるKYC、認証・認可について③(株式会社三菱UFJ銀行)  
—— プレゼンテーション資料は別添1を参照。

三菱UFJ銀行における法人名義の預金口座(以下、法人口座)について、法人向けインターネットバンキング(以下、法人IB)の概要と認証認可のフローや機能を紹介したうえで、個人と法人ではどのような点で取り扱いが異なるかを整理し、CBDCに関するグループディスカッションへと繋げたい。

法人IBについては、大きく分けて内国為替、外国為替、融資、市場リスク管理、為替予約の5つのサービスを提供している。

これらのサービスを利用する際の認証については、まず、お客さまはブラウザで当行の法人向けのポータルサイトにアクセスし、契約者番号、利用者ID、ログインパスワードを入力し、同サイトにログインを行っていただく。ログイン後のメニューから法人IBにアクセスすると、追加の認証として、①予め取得した電子証明書の提示と、②当行が予め配布した物理的なカード型デバイスであるハードウェアトークンが生成するワンタイムパスワードの入力の両方が必要となる。

操作できる範囲、権限等を決める認可については、法人のお客さまは、一つの法人IB契約に対して利用者が複数になることが一般的であるために、お

客さまが登録した管理権限を持つ管理者が利用者ごとの操作権限を設定できる機能を提供している。管理者は、利用者ごとに「取引種類（申請、承認、実行、照会）」、「取引金額の上限」、「利用口座」の操作権限を設定できるとともに、利用者の操作履歴の確認もできる。こうした権限設定を行うことで、例えば、担当者が振込データの申請を行い、上司が承認を行うといった社内権限に合わせたワークフローの組み立てができる仕組みとなっている。

このほか、セキュリティ向上の観点から、①ソフトウェアキーボードの導入によるキーロガー対策、②悪意のあるソフトウェアを検知してコンピュータを保護するマルウェア対策ソフトの提供、③電子証明書をパソコンと別媒体のICカードに格納することで不正に詐取されるリスクの低減、④電子証明書の署名アルゴリズムの高度化、⑤最新のアルゴリズムの利用による暗号化通信の強化、⑥DDOS等のサイバー攻撃対策等を行っている。

最後に、法人IBにおいて、CBDCを送金する機能が組み込まれると前提を置いた場合のディスカッションポイントを5点挙げる。1点目は、既存の法人IBの当人認証機能に加え、CBDC特有の新たな認証要素を加える必要があるか。2点目は、認可についても同様にCBDC特有の要素を加える必要があるか。3点目は、既存の法人IBと同様に、必要に応じて複数のCBDC口座の開設を認め、送金の予約機能や大量に一括で送金を行う総合振込に類似した機能を提供する必要があるか。4点目は、CBDCを利用する場合の企業側のメリットは何か。5点目は、システムトラブルや不正な払戻しが発生した場合、ユーザー、仲介機関、台帳管理者等の関係者間の責任分界点をどのように整理すべきか。

以上について、各参加者の意見を伺いたい。

## （２）法人におけるKYC、認証・認可について④（セコム株式会社）

—— プレゼンテーション資料は別添2を参照。

本プレゼンテーションでは、OpenIDファウンデーションジャパン（以下、OIDF-J）のKYCワーキンググループにて報告書作成中の事業者を対象とした本人確認（以下、事業者本人確認。本人確認は身元確認および当人認証をさす）について、要点を紹介したうえで、CBDCに関する論点を挙げる。

足許、自然人を対象とした本人確認の議論に比べ、事業者本人確認は整理が進んでいないとの問題意識のもと、報告書の作成を進めている段階にあり、今

後修正されうるものにご留意いただきたい。なお、本発表においては、「事業者確認」は事業者本人確認に加え、取引判断に必要となる事業者の事業内容や実態、実績、取引意思等も含めた様々な情報を確認することとし、「事業者の範囲」には、株式会社や一般社団法人等の法人に加え、マンション管理組合等の任意団体や個人事業主も含めるものとした。

まず、事業者本人確認について考察する。事業者は、法律上の権利義務の主体であるが、①現実世界で実体のある自然人と異なり、現実世界で実体が存在しない、②主体を構成する要素が複雑、③第三者が事業者の内部情報について完全な確認をすることが困難であることから、「複数の信頼できる情報を複合的に確認することにより、確からしさを高める」という、自然人の本人確認とは異なる考え方が必要となる。

次に、事業者との取引開始にあたり行う事業者確認について考察すると、大きく3つの確認要素に分けられると考える。1つ目は、「事業者を対象とした身元確認（以下、事業者身元確認）」であり、本人確認書類の検証や信用情報調査会社等への確認を通じて申請者を一意に識別するとともに実在性の確認を行う。2つ目は、「事業者の取引に関わる意思の確認」であり、押印された紙の申込書や、電子署名を付した電子文書の提出を受ける等で、当該事業者の取引の意思を確認する。3つ目は、「顧客管理」であり、取引開始または継続的な取引について、どのようなリスクが存在するのか、取引リスクに見合った価値があるのか等を、各社の社内基準に基づき、適切かつ相応の注意や努力を払って調査を行い、管理していくことである。

続いて、これら3つの確認要素を、本人確認の規定が存在する犯罪収益移転防止法等の法令や、事業者間の取引行為・申請等における業務運用を参考に整理した。1つ目の「事業者身元確認」は、「法人格に対する確認」と、「事業者に関連する自然人に対する確認」に分けられ、前者は「法的実在性確認」、「物理的実在性確認」、「内部組織の実在性確認」の要素があり、後者には「所属確認」、「(取引の任に当たっていることの)権限確認」、「事業者に関連する自然人の個人としての本人確認」の要素がある。2つ目の「事業者の取引に関わる意思の確認」には、「法人格の当該行為自体に関わる意思の確認」の要素がある。3つ目の顧客管理には、「事業内容の確認」、「事業活動の実態有無の確認（当該事業者や組織の運営状態を確認）」、「実質的支配者の確認」、「反社会的勢力でないことの確認」、「資産および収入状況の確認」、「信用情報の確認」の要素がある。

上述の事業者確認で行う要素はリスクに応じて変わりうるため、C B D Cにおいても、どのようにすべきか検討することは重要だろう。また、事業者確

認をデジタル上で効率的に完結するためには、各種確認事項のデータフォーマットの標準化を行う等のデジタルデータの表現に関する多くの課題があると考えている。

次に、信頼できる情報源について考察として、課題を3点挙げる。①個人事業主を含む様々な形態の事業者における、法人名、所在地、事業内容・活動等を一元的に照会できる公的機関が存在しないことや、事業者の形態によって必要な実在性確認方法が異なるため、実在性確認に関わる基本情報の取得負担が大きいこと、②代理権限者や事業活動の実態有無等の事業者内部に属する情報の確認が難しいことや、法人に関係する自然人、組織、事務所レベルの本人認証において信頼できる情報源が明確でないこと、③本人確認に関わる情報を最新状態に維持する動機づけも含めた仕組みが不足していること、が考えられる。

続いて、事業者を対象とした本人認証（以下、事業者本人認証）について考察する。様々な事業者向けデジタルサービスを調べると、本人認証の際のアカウント管理のモデルは、①事業者単位で共通のアカウントを用いる方法と、②操作者個人単位のアカウントを用いる方法の2つに大別でき、②はアカウントの管理権限をサービス提供者側が持つのか、サービス利用者側の管理権限者が持つのか等によって細分化できる。このように、事業者向けデジタルサービスでは、アカウント管理の方法はサービスによって異なりうるため、事業者本人認証を検討する際には保証レベルを規定するだけでなく、アカウント管理のモデルについても、あわせて検討する必要があるだろう。

以上が、O I D F - Jでの検討中の報告書の概要であるが、目指すべき次世代の事業者本人確認のあり方については、現在のところ解には辿り着いていない。一つの案としては、事業者の情報に関して一箇所に集約する基盤を誰かが整備するとよいのではないか、といった考えもあるが、①事業者が自社の持つ情報を当該基盤に提供するには、事業者に対してどのようなインセンティブが必要か、②集約された情報を最新の状態で維持するにはどうすべきか等が課題になると考えている。また、別の案として、官民も含めた複数の組織が保有する鮮度の高い情報を連携する方法も挙がり、O I D F - Jでの検討においてOpenID Connectのプロトコルを応用した組織間の情報連携方法の可能性について期待する声もあった。

最後に、CBDCに関する論点を5つ挙げる。①CBDCにおける事業者本

人確認の基準を検討するにあたり、どのような事項が要求されるか。②事業者本人確認においては、デジタル化が進んでいない確認方法もあり、そうした状況を踏まえた上で、デジタル化の実現可能性があるか。以降は、事業者間のC B D C利用のユースケースやアカウント管理のモデルの整理をした上で議論をした方がよいが、③事業者間でI D連携を行う場合にどのようにデータの定義を行うべきか。④当人認証のアカウント管理のモデルは様々にありうるため、どのように区別すべきか。また、仮にI D連携が必要となる場合は、アカウント管理のモデル間の差異をどのように吸収すべきか。⑤事業者本人確認を通じて得た事業者の属性情報を活用できないか（プログラマブルマネー等）。

以上について、各参加者の意見やコメントを伺いたい。

### 3. 質疑応答とグループディスカッション

参加者による質疑応答の後、グループディスカッションが行われ、各グループ代表者からの発表が行われた。概要は以下のとおり。

#### 【法人I Bのセキュリティおよび法人口座の保有上限数】

(参加者) 2点質問がある。1点目、法人の規模やお客さまのニーズに応じて、セキュリティのカスタマイズを行えるか。2点目、法人口座に関して、保有上限数はあるか。

(参加者) 1点目については、重要度が高いため、法人の規模等に関係なく、一定の高いセキュリティレベルを維持した上で、申請・承認ワークフロー設定等はお客さまに選択いただけるようにしている。2点目については、法人のお客さまからは、部署間で口座を切り分けて管理したいという業務上の必要性から複数口座開設のご要望をいただくこともあり、法人のお客さまの必要性を踏まえた上で、対応している。

#### 【不正対策の費用負担】

(参加者) 法人I Bの当人認証に用いるハードウェアトークンの費用は誰が負担しているか。C B D Cに置き換えた場合、同じような仕組みでハードウェアトークンを配布する場合には、費用負担のあり方が論点になるかもしれない。

(参加者) 現状、ハードウェアトークンは、法人I Bを提供している銀行が費用

を負担している。

#### 【法人 I B の外部連携】

(参加者) 法人 I B と会計ソフト等との連携はどのように行っているか。

(参加者) 会計ソフト等を提供する電子決済等代行業者との連携には、提供している API サービスにて、OAuth 2.0 を用いて必要なデータのやり取りを認可している。このほか、主に大企業向けではあるが、お客さまのサーバと銀行のサーバを直接繋いでデータのやり取りを行うサービスも提供している。

#### 【各グループ代表者からの発表】

(参加者) プレゼンで説明のあった事業者の範囲について、番号法（行政手続における特定の個人を識別するための番号の利用等に関する法律）に基づき法人番号が付与されている事業者に加え、法人番号が付与されていない任意団体や個人事業主も含めた形として提示を頂いたが、法人番号がなく公的な証明がない任意団体や個人事業主の本人確認をどのように行うかは、難しい問題との意見があった。

このほか、個人との違いの観点では、法人は新規設立が容易にできる点が挙げられる。仮に法人の口座に対して凍結等の制限がされたとしても、別の法人を設立することで、過去に制限を受けたことのない口座開設の主体を次々に生み出すことが可能である。そのため、法人の場合は登記情報等の客観的な情報だけでなく、その実体の確認を行うことで、実体のない法人による口座開設を防止することが重要であるが、実務の中ではその難しさを感じている。このほか法人は、本社や支社ごとに複数の口座を作成する場合があるため、名寄せ管理機能も必要となる等、個人とは異なる難しさがある、といった議論があった。

(参加者) どのように C B D C の制度設計がされるか次第であるが、仮に C B D C は基本的には円の機能の一部を代替しうるものに過ぎないのであれば、取扱金額に上限のない銀行は、認証・認可のセキュリティ水準を大きく変える必要はないと思われるが、資金移動業者は、取扱金額に上限がある先、ない先があるので、認証・認可のセキュリティ水準を強化する必要がある先も出てくるかもしれない、との意見があった。

ただし、法人の C B D C の利用範囲を個人からの支払いの受領のみに限定するのであれば、個人から支払われた C B D C を法人の C B D C の口座

で受領後に、同一法人の預金口座に対する振替しか発生しないと思われる。そのため、①仲介機関と預金口座の銀行が同一の場合は、同一の主体が管理するシステム内での同一法人間の振替であり、認証・認可の強度はログイン時に十分な水準であれば、実質的に事足りるのではないかと、との意見があった。次に、②仲介機関と預金口座の銀行が異なる場合は、預金口座の銀行としては、仲介機関経由でどのような背景の取引か不明な多額の資金が流入するため、マネー・ローンダリング対策の観点から懸念が生じうるだろう。こうした懸念を受けて、預金口座の銀行が②の場合を認めず、①の場合のみを認めるとすると、C B D Cの仲介機関となれるのは事実上預金口座のある銀行のみとなる。これは、仲介機関は銀行以外の多様な主体にも担われうるといふ趣旨に反するため、マネー・ローンダリング対策とのバランスをどのように取るべきか、は検討事項になる、との議論があった。

また、仲介機関は円滑なオペレーションを維持するために一定のC B D Cを残高として保有し、流動性を管理しなければならない可能性がある。こうした場合に生じうる仲介機関の資金の負担をどのように考えるべきか、についても検討事項、との議論があった。

議論の中でグローバルベースでのIDの取り組みであるLEI（取引主体識別子）<sup>1</sup>が活用されているとの話が出て、日本においても法人がこのような識別子を積極的に取得することのインセンティブがあってもよい、との意見があった。これに関連して、銀行の外国送金における相手先のユーザーは、相手先の外国金融機関にて本人確認が行われていることを前提に、主に自行側では制裁対象者リストに掲載されていないかを確認するフローとなっており、銀行としては相手先の調査まで求められていないことから、LEIのような仕組みの導入必須化までを銀行が求めることはないだろう、との意見があった。

（参加者）リスクに合わせて本人確認を検討する必要があるとの観点から、資金移動業の加盟店審査における本人確認について議論になり、基本的には対面で実施しているとの実情の説明があった。この議論の中では、本人確認を銀行の本人確認に依拠してはどうかとの意見もあったが、責任分界をどうするかがネックになるため、自社で本人確認を行うことが重要との意見があった。

本人認証に関しては、個人の場合は、昨今ではワンタイムパスワードの方

---

<sup>1</sup> <https://www.gleif.org/ja/organizational-identity/introducing-the-legal-entity-identifier-lei> を参照

式ではフィッシングで破られることがあるため、基本的には生体認証である F I D O 認証へ移行する流れがあるものの、法人の場合は複数人が利用するような利用シーンも想定されるので、どのような認証方式が適切かは考えていく必要がある、との意見があった。

認可に関しては、内部不正をどのように防ぐかが、重要なテーマになるとの意見があった。

(参加者) 当グループでは、三菱UFJ銀行が提示した議論のポイント①～⑤に沿ってディスカッションを行った。

①および②の「既存の決済サービスに追加してCBDCを取り扱う場合に、認証・認可についてプラスアルファの要素が必要か」については、基本的に円の機能の一部を代替しうるものに過ぎず、リスクが高まらないのであれば、認証・認可についてプラスアルファの要素は必要ない、との意見があった。ただし、CBDCは「お金の流れがトレースしやすい」といった特徴を持つことにより、何らかのデータが付加されることでリスクが高まるのであれば、プラスアルファの要素が必要となることもありうるのではないか、との意見もあった。

③の「複数口座の開設を認めるか」については、CBDCと円預金をどのように管理するかに議論が及び、CBDCと円預金を別々の口座で管理する方法だけではなく、単一口座の中でCBDCと円預金の混在を認めて管理する形態もありうるかもしれないとの意見があり、どのようなアーキテクチャになるかに依存するのではないかと議論があった。

④の「CBDCを利用する企業のメリット」については、例示があった「お金の流れがトレースしやすい」という点は、企業側のメリットというよりは、日本全体としてのマネー・ローンダリング対策に資する社会的意義はあるものの、個別の企業としては事務負担が増加する可能性もあり、企業に対するインセンティブとのバランスも含めた設計がないと、導入の推進を促すことは難しいのではないかと、との意見があった。

⑤の「責任分界点をどのように考えるか」については、現在の法人口座は、過失割合に応じて、補償が減額されうる基準として全銀協申し合わせがあるとのプレゼンがあったが、CBDCも基本的に同様の基準で考えるべき、との意見があった。ただし、CBDCは「お金の流れがトレースしやすい」という特徴を持つのであれば、例えば台帳管理者が持つ情報をもとに事業者間での責任分界を巡る紛争を仲裁する機能を持つようなことができれば、責任分界がより明確になるのではないかと、といった意見もあった。

(参加者) 金融犯罪対策の観点から、一般的に法人のアカウント・口座の作成は煩雑化していく方向性にあると認識していたが、セコム株式会社のプレゼンテーションからは、事業者本人確認をオンラインでデジタル完結することで簡素化していく方向性も示され、参考になったとの意見があった。日本としては、こうした仕組みを統一的に整えていく必要があり、デジタル庁が提供する認証サービス「GビズID<sup>2</sup>」は候補の一つ、との意見があった。

(参加者) 当グループでも、法人の認証・認可に関し、CBDCの導入による特別な対応は不要であろう、との議論があった。このほか、仮にCBDCは「お金の流れがトレースしやすい」という特徴を持ち、送金元、送金先といった情報が明確化されるのであれば、消込の業務がスムーズになるかもしれないといったアイデアがあった。

#### 4. 次回予定

次回の会合は未定。

以 上

---

<sup>2</sup> <https://gbiz-id.go.jp/top/> を参照

CBDCフォーラム WG3  
「KYCとユーザー認証・認可」  
第14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  
株式会社野村総合研究所  
日立チャネルソリューションズ株式会社  
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  
株式会社りそなホールディングス  
株式会社NTTドコモ  
PayPay株式会社

(事務局)  
日本銀行

# 法人向けインターネットバンキング (IB)における認証・認可

2025年5月27日

三菱UFJ銀行

世界が進むチカラになる。



# 法人IBのサービス

# サービス例

サービス一覧		サービス概要
内為サービス	基本サービス	残高・明細照会、振込・振替、税金・各種料金の払込(ペイジー収納)
	振込送金組戻訂正サービス	振込の組戻し・訂正・再振込の依頼
	24時間サービス	土日・祝日でも当日付の振込が24時間即時
	総合／給与振込サービス	総合・給与賞与振込の依頼
	取引通知サービス	入出金データや振込入金データをまとめてダウンロード
	振込入金メール通知サービス	通知履歴および振込入金明細の確認
	口座振替サービス	口座振替の依頼、結果の照会・ダウンロードや再依頼
	APIサービス	外部サービス会社が提供するサービスと連携
	etc	
外為サービス	仕向送金	外国送金の依頼
	被仕向送金	到着した被仕向送金の明細照会や、入金指図
	外貨預金	外貨預金の振替や、残高・入出金明細
	輸出ドキュメンタリ	輸出L/Cの到着状況に加え、輸出手形の買取・取立に関する計算明細や決済状況の照会
	輸入ドキュメンタリ	輸入L/Cの発行・条件変更の依頼や、L/C発行結果・L/C残高の照会
	外為取引通知	外貨預金入出金明細・外為取引明細・外国為替関連情報のダウンロード
融資サービス		当座貸越(専用)借入申込
		借入明細照会
		計算書・返済予定表照会
市場リスク管理サービス		各種デリバティブ商品の残高や時価評価額を日次で照会
FOREXサービス		為替予約取引

認証

# 認証①: PCからのログイン方法

- 利用者ID・ログインパスワード、電子証明書、ワンタイムパスワード等を利用した厳重な本人確認

〈ホームページトップ〉

電子証明書を取得したPCからのアクセスであることを確認します。

1. 電子証明書を選択
2. ワンタイムパスワードを入力

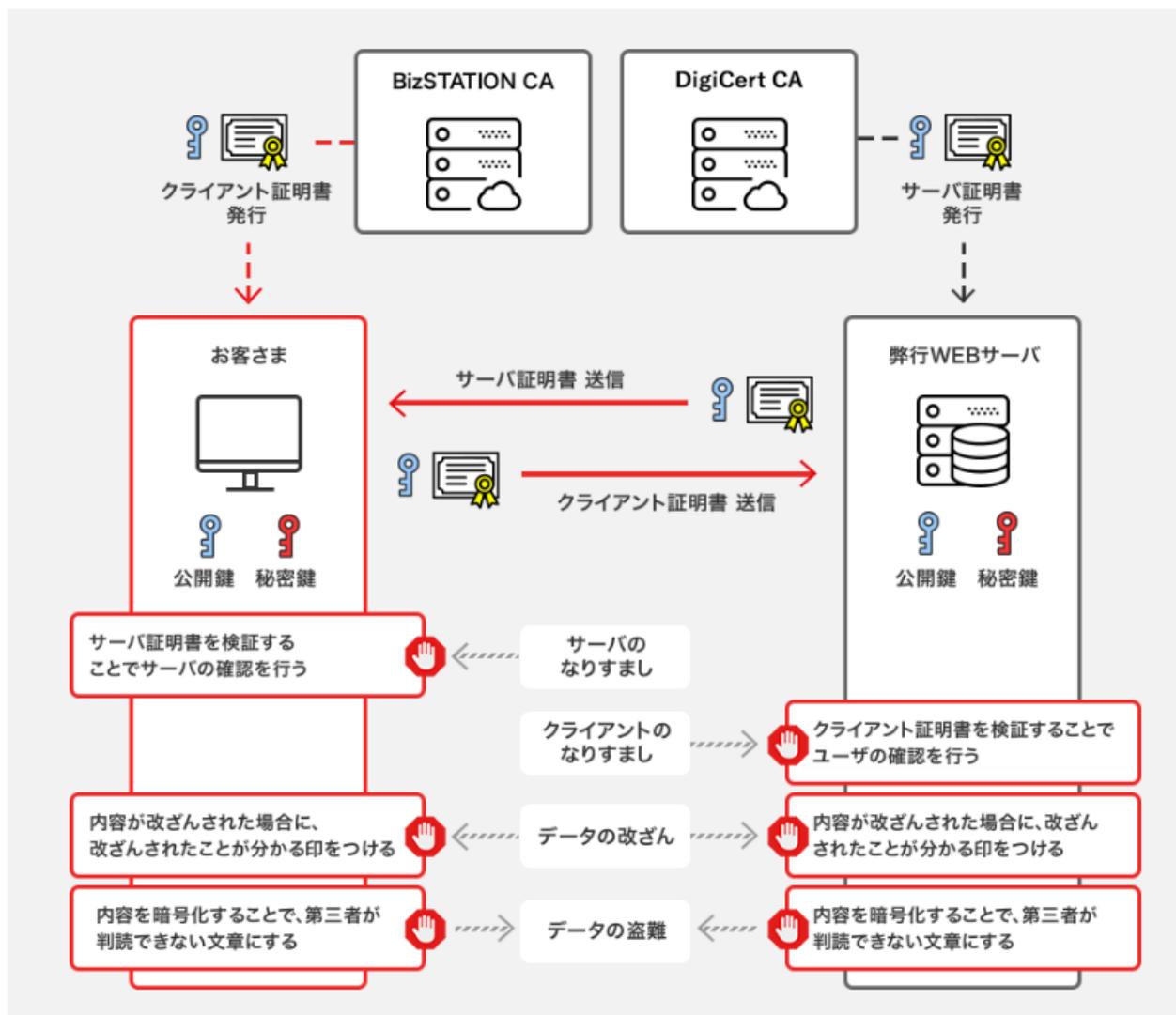
ご利用の前に・・・

「電子証明書」を取得します。

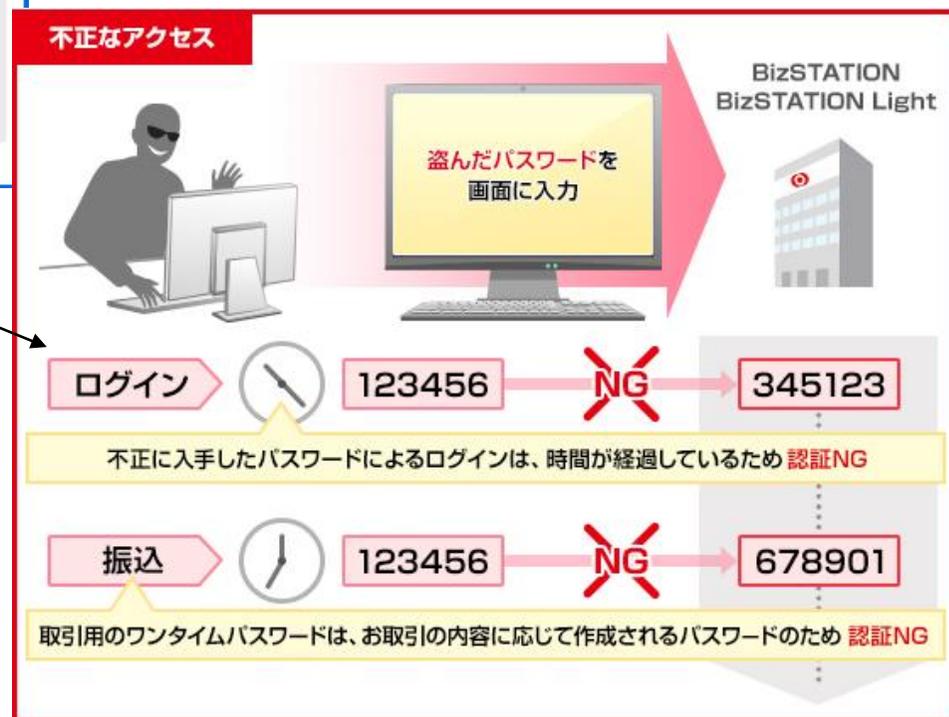
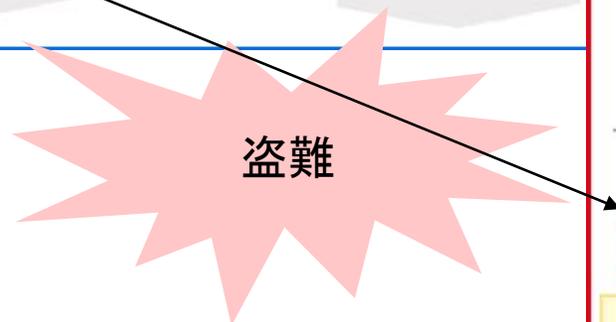
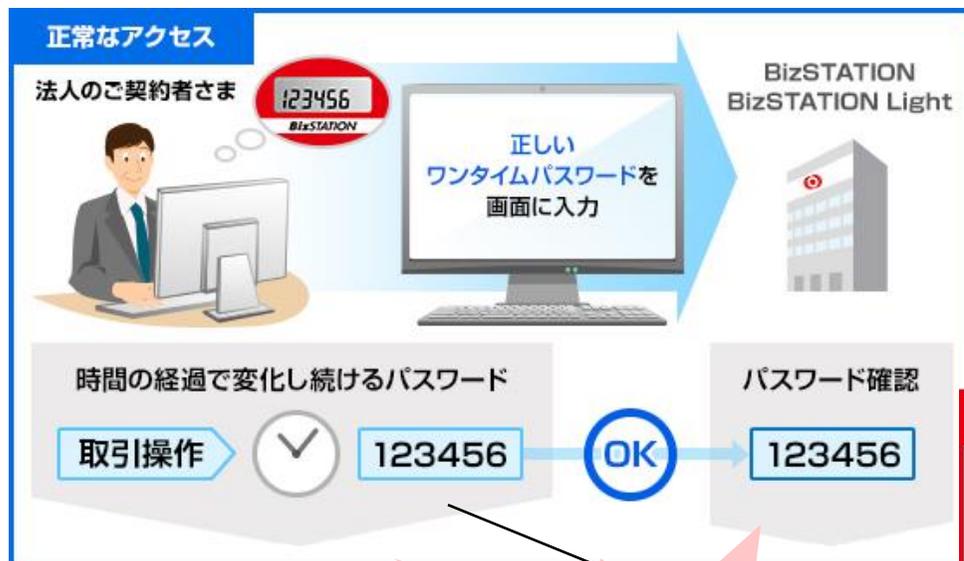
《電子証明書》  
現実の世界では、個人を証明するために免許証やパスポートといった本人確認資料を提示することで、相手に自分自身の証明を行うことができます。しかし、インターネット上では、そのような本人確認資料を相手に見せるといったことが難しく、また、信用させようとする相手に、本人確認資料の複写を送るといったことは現実的ではありません。そこで、インターネット上で自分を証明する手段として電子証明書による本人を確認する手段が考えられました。

《ワンタイムパスワード》  
ワンタイムパスワードは、パソコンからログイン振込等のお取引を実行、または承認する際に使用する1回限り有効な使い捨てパスワードです。一定時間を経過すると無効になり、同じパスワードを再利用できないため、第三者による不正利用等のリスクを軽減させることが可能です。

## 認証②: 電子証明書による認証の概要



# 認証③: ワンタイムパスワードによるセキュリティ強化



# スマートフォンからのログイン～取引

## スマートフォンアプリのセキュリティ

- スマートフォンアプリでは、FIDO (※)認証を採用。個人情報をネットワーク上に流さず本人認証を行う安全性の高い規格であり、利用者のIDやパスワードの漏洩リスクを低減させることが可能

(※)Fast Identity Onlineの略称。オンライン認証の国際標準規格。

**ログイン認証**

**取引認証**

スマートフォンアプリ利用登録の際に設定した、**アプリパスワード** または **生体情報** で認証

**FIDO認証のメリット**

- 個人情報のインターネット上への流出無し
- ログイン認証も取引認証も統一した操作で可能

認可



## 認可②

### 操作(申請・承認)権限設定例

- 申請権限や承認権限は、業務上の社内権限に合わせてご利用者ごとに設定することが可能。以下代表例。

#### 設定例1 申請と承認を分ける

例えば、担当者が申請し、上司が承認を行う



#### 設定例2 申請と承認を一人で行う

一人の利用者に承認権限と申請権限を両方登録して、振込の依頼を一人で行う



#### 設定例3 異なる二人で承認を行う(複数承認)

一次承認と二次承認の二重の承認を必要とさせる。  
例えば、担当者が申請し、上司①、上司②がそれぞれ承認を行う。



## その他のセキュリティ対策

---

項目	概要
ソフトウェアキーボード	キーロガー対策
マルウェア対策ソフト	悪意のあるソフトウェアを検知してコンピューターを保護する
ICカード	電子証明書をパソコンから分離されたICチップに格納することで、不正に詐取されるリスクを低減
電子証明書の強化	署名アルゴリズムの高度化(SHA2など)
暗号化通信の強化	SSL3.0、TLS1.0～1.1暗号化通信を遮断
その他	DDoS等のサイバーアタック対策

ディスカッション

法人IBのメニューに、円・「CBDC」・ドル・ユーロ・etcと並んだ場合、

- ①、既存のIB認証を利用することでよいか？  
CBDC取扱い用に、プラスアルファの「認証」要素を加える必要があるか？
- ②、①同様、プラスアルファの「認可」要素を加える必要があるか？
- ③、複数口座、予約・大量明細に相對する機能は必要か？
- ④、CBDCを利用するユーザ(企業)のメリットは？  
(不正な払戻しがあった場合に、お金の流れがトレースしやすい等)
- ⑤、システムトラブルや不正な払戻しが発生した場合、責任分界点はどこにおくべきか？  
⇒ユーザ ~ 仲介機関 ~ 台帳管理者

# CBDCフォーラム WG3 事業者確認に関する現状整理と課題

2025年5月27日

セコム株式会社  
IS研究所 主幹研究員  
佐藤 雅史

# 本発表について

- OpenIDファウンデーションジャパン KYC WGにて法人KYC（事業者本人確認）の現状と課題を議論してきました。現在、その成果を報告書としてまとめています。
- 本発表ではその要点を紹介し、CBDCでの論点を議論します。
- 本資料は報告書のドラフトから引用しており、報告書の最終版では内容が修正される可能性がありますので、留意ください。

# 本発表における用語定義

報告書ドラフトより一部抜粋

用語	定義
身元確認 (*1) (Identity Proofing)	申請者を一意に識別するとともに、実在性を確認すること。 具体的には、申請者の属性情報を収集することで申請者を一意に識別するとともに、収集した属性情報が真正かつ申請者自身のものであることを本人確認書類により検証することで、申請者が実在かつ生存する人物であることを確認する。
当人認証 (*1) (Authentication)	申請者の当人性を確認すること。 具体的には、対象手続を利用しようとする者が、身元確認時に登録された者と同一の人物であることを、申請者と紐づけて登録した認証器を用いて確認する。
本人確認	身元確認及び当人認証を実施すること。
事業者身元確認	事業者を対象とした身元確認。
事業者当人認証	事業者を対象とした当人認証。
事業者本人確認	事業者を対象とした本人確認。
事業者確認	事業者本人確認に加え、取引判断に必要な事業者の事業内容や実態、実績、取引意思なども含めた様々な情報を確認すること。
顧客管理 (Customer Due Diligence)	事業者の身元確認や事業内容、取引内容、関連情報などを調査し、リスク評価を行い、講ずるべきリスク低減措置を判断し実施すること。

(\*1) デジタル庁「行政手続等での本人確認におけるデジタルアイデンティティの取扱いに関するガイドライン（案）」の用語定義より引用

# 【背景】

自然人に対する身元確認や当人認証の議論は整理されつつあるが、事業者に関する議論は共有されていない傾向がある。

報告書ドラフトより抜粋

自然人を対象とした本人確認方法は確立されつつあり<sup>※1</sup>、セキュリティや利便性の向上において一層の改善が図られている状況にある。デジタル化を前提とした自然人に対する認証や属性の連携によるサービス向上の議論は今後も目覚ましい発展が期待される。

一方で、事業者の本人確認に関わる現状の整理や将来的なデジタル化における課題は自然人の議論に比べ共有されていない現状がある。

## 自然人の本人確認に関する報告書やガイドライン(国内)の例

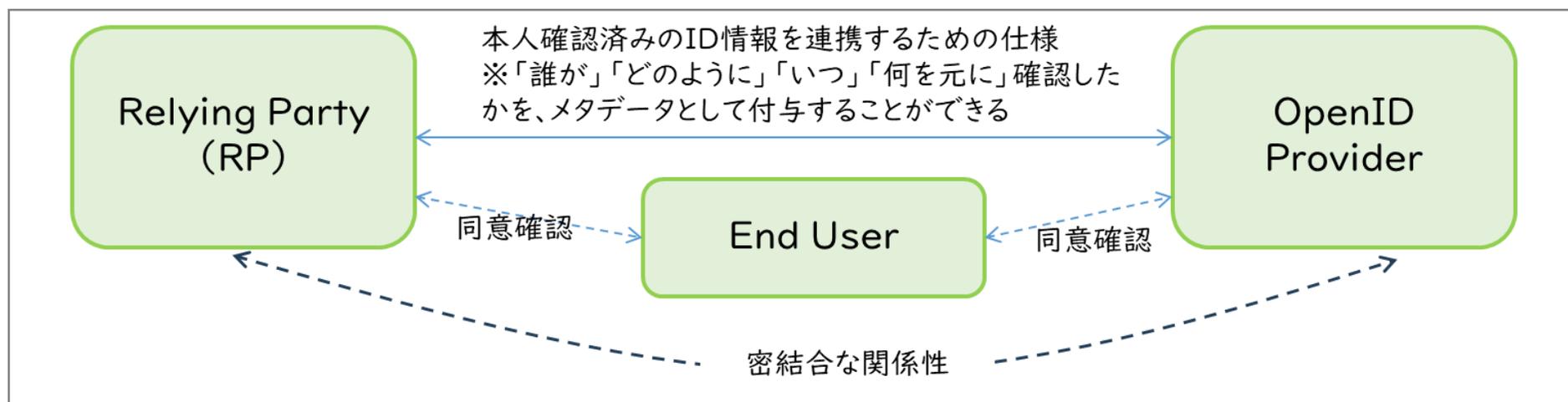
- 経済産業省
  - 「オンラインサービスにおける身元確認手法の整理に関する検討報告書」 2020年3月31日
- 各府省情報化統括責任者(CIO)連絡会議決定
  - 「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」 2019年2月25日
- 一般社団法人 OpenID ファウンデーション・ジャパン KYC WG
  - 「民間事業者向けデジタル本人確認ガイドライン」 2023年3月
  - 「デジタル本人確認の国内での普及に向けたツール・ルールの検討レポート」 2022年12月
  - 「サービス事業者のための、継続的顧客確認に関する調査レポート」 2021年9月
  - 「次世代におけるKYCの方向性に関するレポート」 2021年9月
  - 「サービス事業者のための本人確認手続き(KYC)に関する調査レポート」 2020年1月

# 事業者の身元確認に関するデジタル化と情報の連携は可能か？

## 【参考】OpenID Connect for Identity Assurance (IDA) の概要

報告書ドラフトより抜粋

- OpenID Connectの仕組みを使い、本人確認済みのID情報を連携するための仕様  
(ユーザーの本人確認が、どのように行われたかを伝達するインターフェースの標準化)
- ✓ OpenID Connectでサポートされている各種個人情報に対して、「誰が」「どのように」「いつ」「何を元に」確認したかを、メタデータとして付与することができる
- ✓ Verified Claims というオブジェクトを新たに定義
- ✓ RPは、Claims Parameterで細かい条件を指定も可能  
例:「日本の犯収法に基づかない結果であれば不要」など、結果を受領する条件を規定することができる
- ✓ 例えば、「20歳以上」「東京都か千葉県在住かどうか」など、個人情報本体ではなく、その条件をTrue/Falseで返却する事もできる
- ✓ RPとOP (IDP) が密結合な関係性のデータ連携が基本思想



# 報告書の内容（予定）

- 事業者確認の全体の整理
- 事業者の身元確認に関する考察
- 信頼できる情報源に関する考察
- 事業者の当人認証に関する考察
- 付録：調査内容の詳細、海外動向の紹介

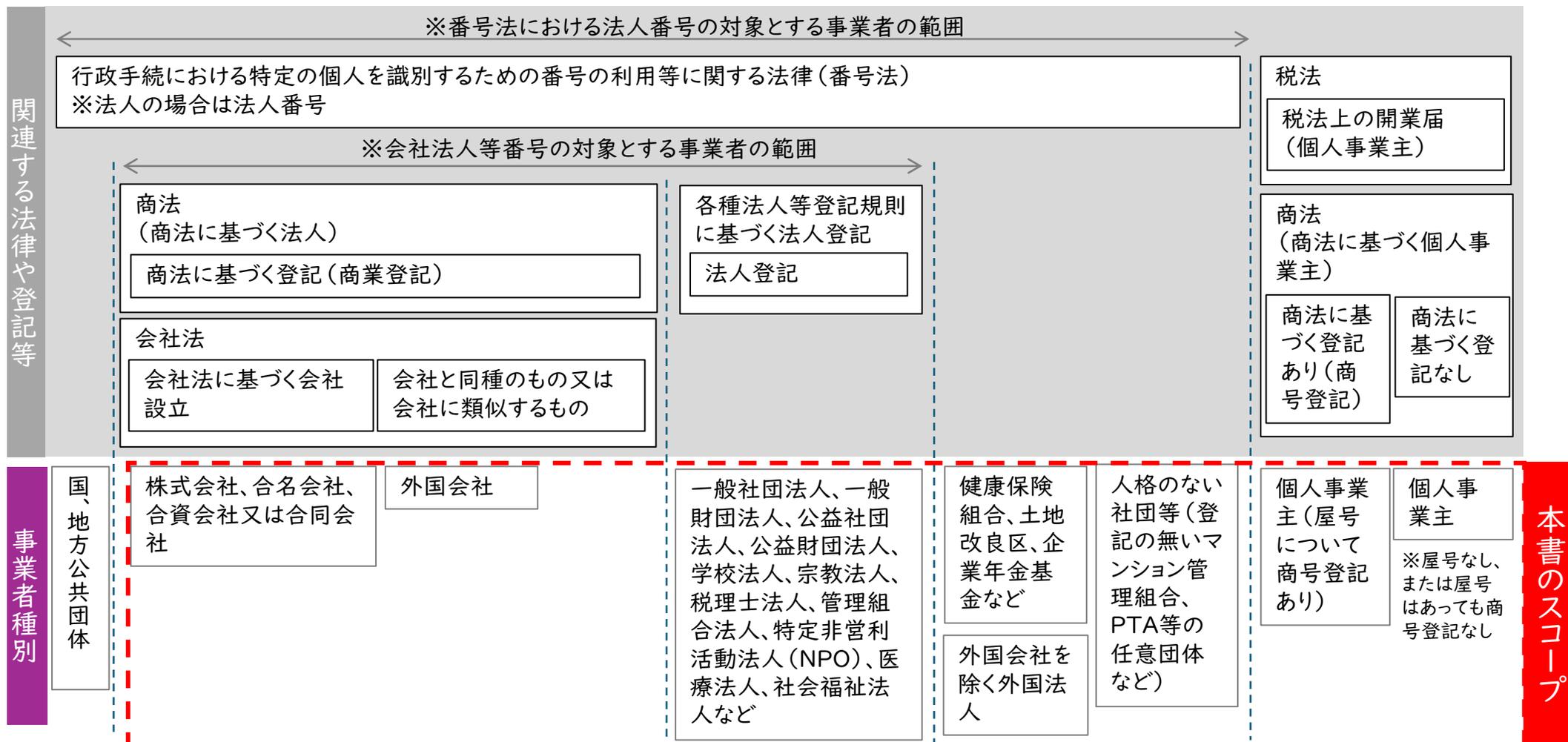
# 報告書のスコープ（予定）

- 一般的な事業者間の取引業務や申請等における本人確認を主に焦点をあてる。ただし、事業者の本人確認（身元確認＋本人認証）の共通事項の整理については、犯収法なども参考にしている。
- 以下はスコープ外
  - 事業者の識別子の番号を発行・管理を行う機関で行われる内部の手続きやシステムの詳細
  - 本人確認書類を証明する機関で行われる内部の手続きやシステムの詳細
  - 法令への適合性

# 検討対象とする事業者（確認対象）の範囲

- 前述の、本書の検討対象とする事業者の対象について、以下の通りイメージを補記する。
- 各々の法律等は、個別の目的に対し対象の事業者の定義を行っている。事業者全般に対して、網羅性・整合性のある定義がなく、対象事業者の範囲の相関について、独自見解としてイメージの作成を行った。

図2-1:検討対象とする事業者の範囲



# 事業者の身元確認に関する考察

## ➤ 事業者を本人確認する場合には、自然人の本人確認とは異なる考え方が必要となる。

- ✓ 事業者は、法律上の権利義務の主体であるが、現実世界で実体のある自然人（個人）と異なり、現実世界で実体があるわけではない。
- ✓ また、主体を構成する要素が、自然人よりも複雑であり、第三者が「完全な確認」をする事が困難である。

図3-1:事業者本人確認の特徴

リアルに存在する自然人



自然人

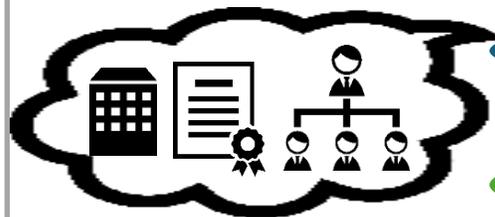
- ✓ 現実の世界に実体が存在する

信頼性の高いエビデンス(※)を軸にしたProofingをするという考え方がとりやすい

※例:本人確認書類 (Identity Document)など



法律上の権利義務の主体となる法人(/事業者)



法人格

法人と自然人  
の関係性

事業者に関する自然人

- ✓ 現実の世界に実体が存在しない

- ✓ 主体を構成する要素が複雑

- ✓ 第三者が法人内部情報について「完全な確認」をする事が困難

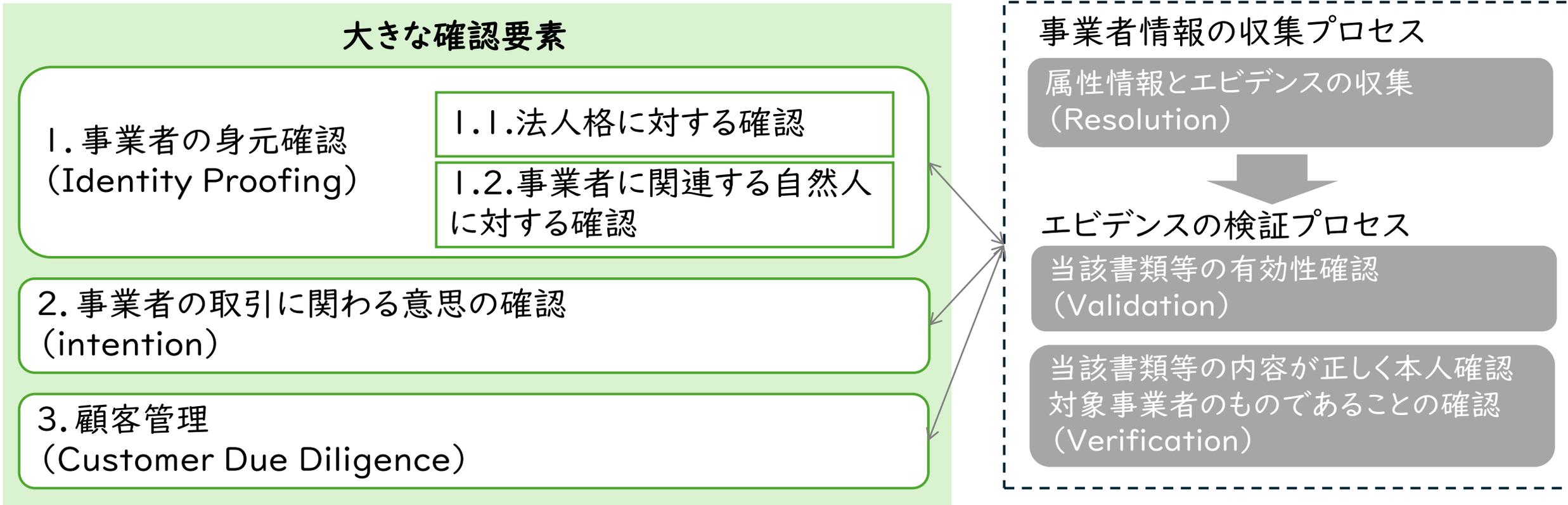


完全な確認 (Proofing) が困難

⇒ 複数の参考となる信頼できる情報を「複合的に確認」により、確からしさを高める (Trustを高める) 考え方

- ✓ 事業者との取引を開始するにあたり、対象の事業者に関する様々な情報を確認することになる。
- 事業者との取引時の事業者確認において、一般的に以下の大きな確認要素を含むものと考えられる。

図4-1：事業者本人確認における大きな確認要素



# 取引時の事業者確認の概要（事業者の身元確認）

図4-2:事業者本人確認における2つの類型と確認イメージ

## 1. 事業者の身元確認 (Identity Proofing)

1.1. 法人格に対する確認

1.2. 事業者に関連する自然人に対する確認

### A. 本人確認対象事業者によって提示された証拠書類等に基づき行うケース



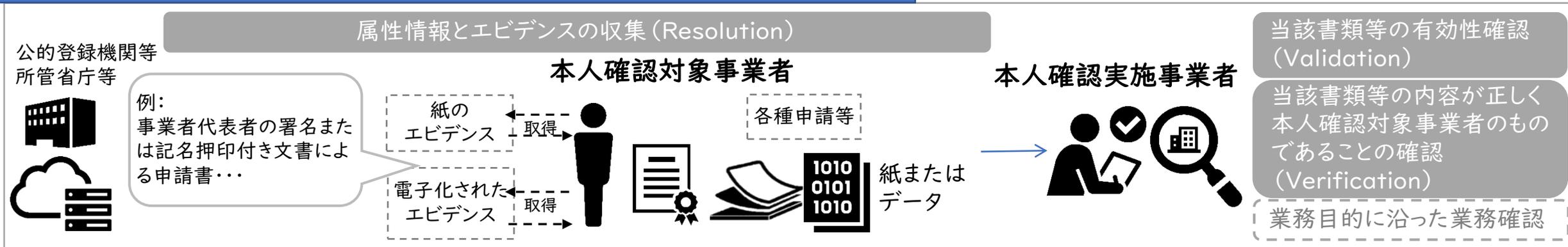
### B. 本人確認実施事業者が主体的に情報を収集して行うケース



(次頁続く)

## 2. 事業者の取引に関わる意思の確認 (intention)

### A. 本人確認対象事業者によって提示された証拠書類等に基づき行うケース



## 3. 顧客管理 (Customer Due Diligence)

### B. 本人確認実施事業者が主体的に情報を収集して行うケース



- この章では、本人確認の規定が存在する法令等（例：犯罪収益移転防止法）や、一般事業者間の取引行為や申請等における業務運用のサンプル分析を参考に、確認事項の要素を分類整理した。

表4-1：確認要素の分類整理におけるサンプル分析対象

本書のサンプル分析対象
犯罪収益移転防止法
一般事業者間の取引リスクが大きい新規取引における取引与信
EDI等のアカウント申請等
インターネットのドメイン取得
商業登記電子証明書の取得申請

- 分類整理において、事業者に対する確認事項を洗い出すことを目的に、本人確認と顧客管理を区別せず両者を含めて考察した。
- また、確認事項の考察に際しては、紙文書とデジタルデータ、対面と非対面を区別なく分析した。

- ✓ 本章では、サンプル分析結果のサマリーのみを記載する。

※個別のサンプル分析の具体的な内容は、別添資料

## 4. 事業者本人確認に関わる要素や属性

### 4.3 事業者確認事項における確認要素の分類

事業者確認事項の大きな分類	要素 ※補足説明は後頁
1. 事業者の身元確認 (Identity Proofing)	
1.1. 法人格に対する確認	法的実在性確認、または公的情報等に基づく実在性確認 物理的実在性確認 法人等に属する内部組織の実在性確認
1.2. 事業者に関連する自然人に対する確認	所属確認 (代表者等、従業員、代理人等) 取引の任に当たっている事の確認 (権限確認) (代表者等取引の任に当たっている自然人の) 事業者に関連する自然人の「個人」としての本人確認
2. 意思の確認 (intention)	法人格の当該行為自体に関わる意思の確認 (内容確認をしている事の確認含む)
3. 顧客管理 (Customer Due Diligence)	事業の内容の確認 事業活動の実態有無の確認 (当該事業者や組織の運営状態を確認) 実質的支配者 (BO) の確認 反社確認 資産及び収入の状況の確認 信用情報確認

## 4. 事業者本人確認に関わる要素や属性

### 4.3 事業者確認事項における確認要素の分類

前頁の確認要素の補足説明

要素	補足説明
法的実在性確認 または公的情報等に基づく実在性確認	法令に従った登記情報等に当該事業者や組織が存在することを確認。 例：商業登記や法人登記されていることを確認 例：適格請求書発行事業者登録番号が有効であることを確認 例：個人事業主の場合に、実印押印と印鑑登録証明書の照合と、屋号や開業届などを確認 個人事業主の実在性確認は個人に対してであり、事業性に係る実在性については確認が難しく、別途、確定申告書や納税証明等の公的情報等に基づく事業性に係る実在性確認を行うケースも存在。
物理的実在性確認	当該事業者や組織の所在を確認。 例：商談プロセス等における対面確認 例：郵送やり取りなどにおける非対面確認 例：企業信用調査会社の企業調査書等の確認（現地調査含む）
法人等に属する内部組織の実在性確認	部門や事業所等を確認
所属確認（代表者等、従業員、代理人等）	法人格と事業者に関連する自然人の「関係性」の確認。 例：代表者、従業員、代理人等 例：所属組織
取引の任に当たっている事の確認（権限確認）	適切な権限や資格をもって、当該行為を執り行っているかどうかの確認

（次頁続く）

## 4. 事業者本人確認に関わる要素や属性

### 4.3 事業者確認事項における確認要素の分類

(前頁続き)

要素	補足説明
(代表者等取引の任に当たっている自然人の) 事業者に関連する自然人の「個人」としての本人確認	Identity Document等の確認をもって、当該本人自身である事の確認(本人特定事項の確認)
法人格の当該行為自体に関わる意思の確認(内容確認をしている事の確認含む)	申請代表者等取引の任に当たっている自然人の行為を介しての、法人としての当該行為に対する意思の確認。 例: 契約書や申請書等の代表者等の押印の確認 例: (取引リスク等の必要に応じて) 押印の印影と印鑑登録証明書の照合 例: 対面で、所属確認や取引の任にあたっている事の確認(権限確認)等を併せて確認 例: 電話等や、電子証明書による電子署名の確認など非対面確認
事業の内容の確認	一般事業者間の取引行為等においては、各事業者の取引判断等に際し、当該取引先事業者との取引開始または継続的取引について、どのようなリスクが存在するのか、取引リスクに見合った価値があるのか等、主に各事業者の社内基準に基づき、適切かつ相応な注意や努力を払って調査を執り行う事などが含まれる。(多くの一般事業者においては、新規取引時や継続的取引における途上管理における取引与信プロセス等や企業M&A等の一部で執り行われる事が多い。なお、Customer Due Diligenceに対する日本語記載を「顧客管理」としたのは、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等に依るものである)
事業活動の実態有無の確認(当該事業者や組織の運営状態を確認)	
実質的支配者(BO)の確認	
反社確認	
資産及び収入の状況の確認	
信用情報確認	なお、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や犯罪収益移転防止法等においては、Identity Proofingは顧客管理(Customer Due Diligence)の一部扱いとなり明確に区分された記載にはなっていないが、本書においては、Identity ProofingとCustomer Due Diligenceを区分した

## 4. 事業者本人確認に関わる要素や属性

### 4.2 事業者確認の目的

- 事業者確認において、事業の内容や当該行為等におけるリスクの大きさが影響を及ぼす。
  - ✓ 事業者の事業内容は多種多様であることから、リスクも同様に多種多様にある。
  - ✓ リスクに応じて、必要となる本人確認事項の要素や属性が異なる。
- 
- 事業の内容に応じて、例えば、以下のようなリスクの大小がある。
    - サービス提供先への連絡手段など必要最小限の情報のみを必要とし、取引リスクがそれほど大きくないもの
    - 個人との取引と事業者との取引でリスクが大きく変わらないもの
    - 事業者との取引が比較的大規模であるなど、自社の経営に影響を与えうるもの
    - 事業者との取引が自社が提供する製品やサービスの供給や品質に影響を与えるもの（サプライチェーン）
    - 事業者のなりすまし等により社会的に影響を与えうるもの（例：企業が発信する情報、公式SNSアカウント、Webサイト等）
    - 取引が犯罪組織、テロ組織、制裁国への利益供与に結びつくもの（金融、兵器転用可能な部品など）

## 4. 事業者本人確認に関わる要素や属性

### 4.3 事業者確認事項における確認要素の分類

表4-5: サンプル分析のサマリー

分類		要素	犯罪収益移 転防止法	一般事業者の 取引与信(リ スク大)	EDI等のアカ ウント申請	インターネット ドメイン取得申 請	商業登記電子 証明書の取得 申請
1. 事業者 の身元確 認 (Identity Proofing)	1.1. 法人 格に対する 確認	法的実在性確認 または公的情報等に基 づく実在性確認	○	○	○	○	○
		物理的実在性確認	○	○	○	△	
		法人等に属する内部組 織の実在性確認		○	○	△	
	1.2. 事業 者に関連す る自然人に 対する確認	所属確認(代表者等、従 業員、代理人等)		○	○	△	○
		取引の任に当たっている 事の確認(権限確認)	○	○	○	△	○
		(代表者等取引の任に当 たっている自然人の) 事 業者に関連する自然人 の「個人」としての本人 確認	○				

(次頁続く)

## 4. 事業者本人確認に関わる要素や属性

### 4.3 事業者確認事項における確認要素の分類

(前頁続き)

分類	要素	犯罪収益移 転防止法	一般事業者の 取引与信(リス ク大)	EDI等のア カウント申請	インターネットド メイン取得申請	商業登記電子 証明書の取得 申請
2. 意思の確認 (Intention)	法人格の当該行為自体 に関わる意思の確認(内 容確認をしている事の確認 含む)	○	○	○	○	○
3. 顧客管理 (Customer Due Diligence)	事業の内容の確認	○	○			
	事業活動の実態有無の 確認(当該事業者や組織 の運営状態を確認)		○			
	実質的支配者(BO)の確認	○	△			
	反社確認		△			
	資産及び収入の状況の 確認	△	△			
	信用情報確認			○		

## 4. 事業者本人確認に関わる要素や属性

### 4.4 事業者確認の手法に関する現状分析

#### 4.4.1 現状の手法の整理(説明)

表4-6:事業者本人確認に関わる手法例

デジタル手法	(参考)アナログ手法	AS ISユースケースの例
商業登記電子証明書(電子認証登記所発行の電子証明書)を用いた電子署名を用いた電子申請や取引に関わる情報の確認	商業登記の登記事項証明書(対面or書留等)	例) 犯収法の対象事業者の特定業務(例:口座開設)における「法人の本人特定事項の確認」 <ul style="list-style-type: none"> <li>電子署名が行われた特定取引等に関する情報(口座開設申込書等)と商業登記電子証明書</li> <li>登記・供託オンライン申請システム</li> </ul> 例) 不動産登記のオンライン申請、商業・法人登記のオンライン申請など 例) e-TAX 例) 電子調達システム 例) 特許のインターネット申請 例) 電子自治体の各種申請・届け 例) 電子証明書の発行電子申請
登記情報提供サービスの照会	商業・法人登記事項証明書(対面or書留等)	例) 犯収法の対象事業者の特定業務(例:口座開設)における「法人の本人特定事項の確認」 例) 以下、法人番号公表サイトやgBizINFO照会等と同じ(ただし、有償コストを許容する事業者の場合)
法人番号公表サイトやgBizINFOの照会等	商業・法人登記事項証明書(対面or書留等)	例) 犯収法等の法令に基づかない一般事業者の取引与信業務等の一部として必要に応じて確認(法人の実在性確認)。ケースによっては(例:リスクの低い取引など)、TBDやTSRの企業情報調査などに基づくCDDを行わず、実在性確認のみで良しとする事業者によっては業務運用ケースも存在。

## 4. 事業者本人確認に関わる要素や属性

### 4.4 事業者確認の手法に関する現状分析

#### 4.4.1 現状の手法の整理(説明)

(前頁続き)

デジタル手法	(参考)アナログ手法	AS ISユースケースの例
企業信用調査会社(例:TBDやTSR等)の企業情報照会サービス	企業信用調査会社(例:TBDやTSR等)の企業情報調査書	例) 犯収法等の法令に基づく特定業務であろうが、一般事業者の取引与信業務の一部であろうが、ある程度の取引リスクの存在するCDDにおける情報照会
公的個人認証他	取引の任に当たる代表者または担当者の自然人の本人特定事項の確認書類	例) 犯収法の対象事業者の特定業務(例:口座開設)における「取引の任にあたる自然人の本人確認」
電子委任状	取引の任に当たっている事の確認の為の委任状または本店や事業所などへの架電など	例) 犯収法の対象事業者の特定業務(例:口座開設)における「取引の任にあたっている事の確認(取引の任の委任に関する法人の意思の確認)」 例) 一般事業者における、非常に取引リスクの高い取引(例:不動産取引など?)における取引の任に当たっている事の確認で求められるケース
電子証明書を用いた電子署名を用いた取引に関わる情報の確認	契約書面、請求書面など	例) 事業者に所属する特定の自然人(取引の任にあたる自然人)による署名・捺印などでの契約書面締結
電子証明書を利用した電子署名の確認	印鑑証明書(対面or書留等)と印影の照合確認に類似	例) 一般事業者における、比較的取引リスクの高い取引における契約書面の法的な推定効を強化する上の確認で求められるケース
EDI等を介した取引に関わる情報	契約書面、請求書面など	例) EDI等を介した電子的記録を伴う電子取引を活用する一般事業者間の取引など

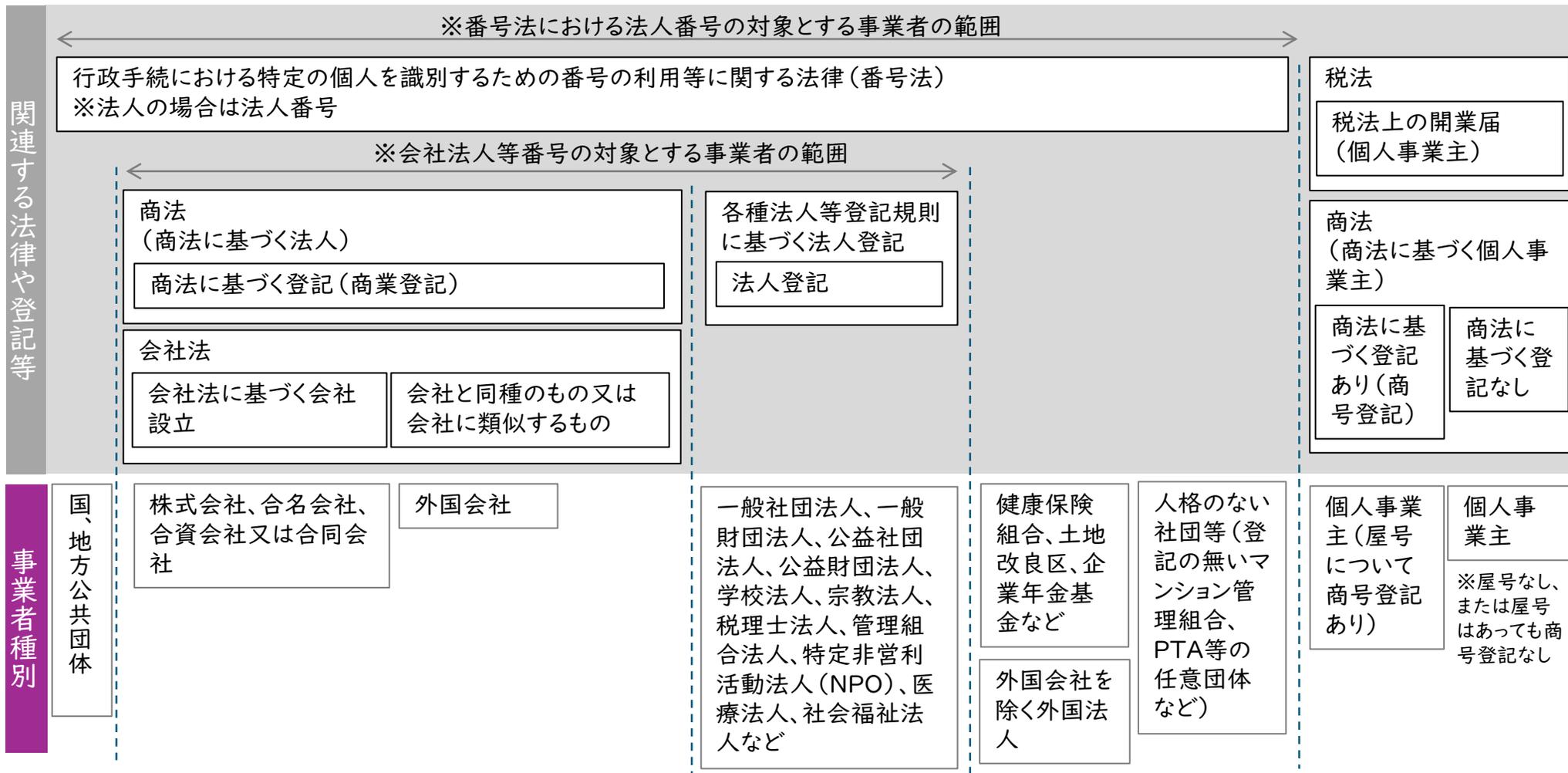
# 信頼できる情報源に関する考察 (本発表では整理の内容は省略)

# 5. 信頼できる情報源に関する考察

## 5.2 信頼できる情報源に関する課題の背景

- 公的なレジストリに関しては、関連する法律等の目的が異なる事を背景に、対象範囲の事業者の相違や保有情報の相違が大きく、情報鮮度に係る課題も存在する。

【再掲】図2-1: 検討対象とする事業者の範囲



## 5. 信頼できる情報源に関する考察

### 5.3 信頼できる情報源に関する課題の現状分析

- 現状、“官民の信頼できる情報源”において、「事業者のカバー範囲」「事業者確認事項の要素」「情報鮮度」の3つの観点で、確認可能な範囲のばらつきが大きく、情報取得の負担が大きい。

#### ✓ 課題1: 様々な形態の事業者に対する、実在性確認に関わる基本情報の取得負担が大きい

- 個人事業主を含む様々な形態の事業者に対して、「法人名」「所在地」「事業内容」を、一元的に照会できる公的機関の環境が存在しない。(個人事業主は登記情報で、事業者としての実在性を確認できない)
- 個人事業主の実在性確認は個人に対してであり、事業性に係る実在性については確認が難しく、別途、確定申告書や納税証明等の公的情報等に基づく事業性に係る実在性確認を行うケースや、現地調査等を行うケースも存在する。

#### ✓ 課題2: 事業者に関係する自然人や組織や事業所などの実在性確認、法人との関係性の確認、事業内容や事業活動の実態有無の確認に関わる情報の取得負担が大きい

- 事業者内部に属する情報の確認が難しい(代表者・代理権限者や、事業所や社内組織、事業活動の実態有無など)
- 法人に関係する自然人や、組織や事業所レベルの当人認証において信頼できる情報源が明確でない

#### ✓ 課題3: 最新状態の情報の取得負担が大きい

- 本人確認に関わる情報の最新状態を維持する仕組みがない(法人名、所在地、業務内容、代表者・代理権限者や、事業所や社内組織など)

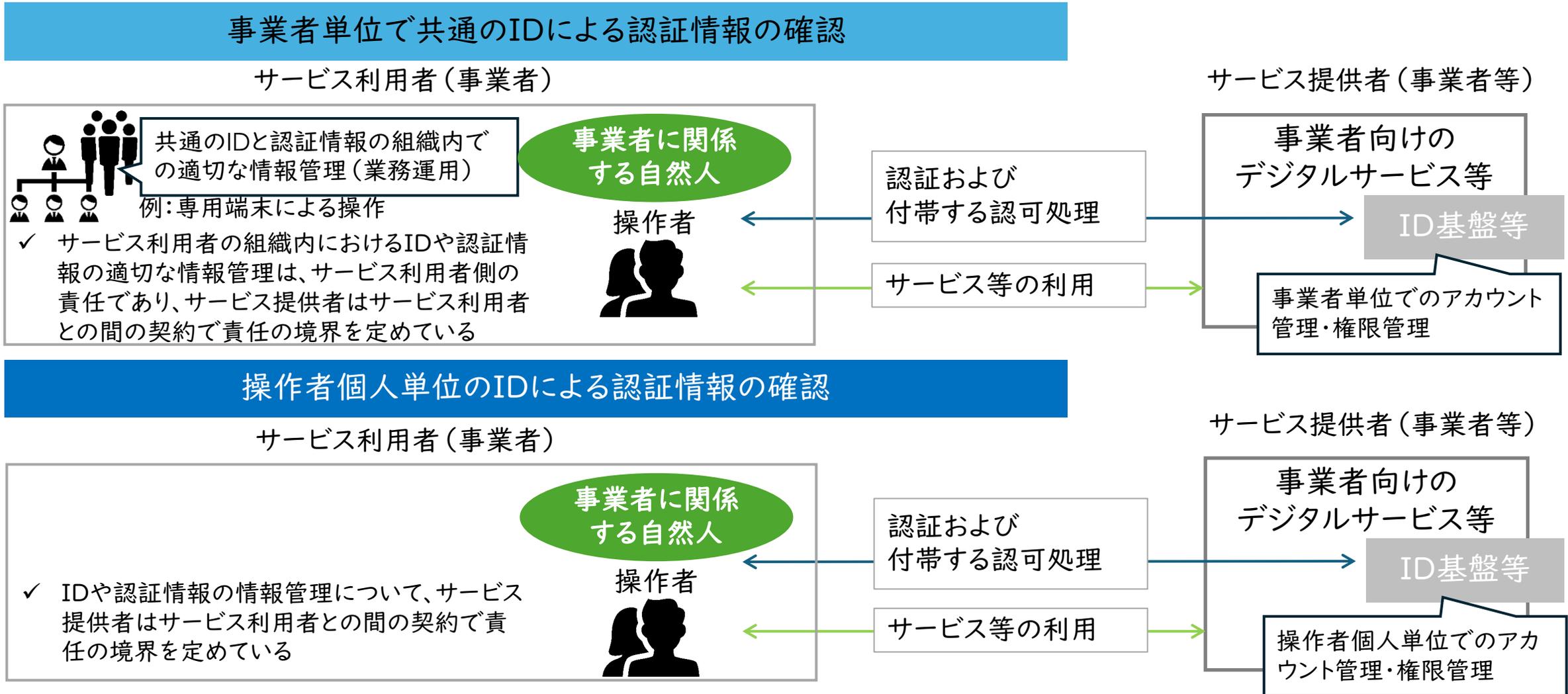
# 事業者の当人認証に関する考察

# 6. 事業者本人確認における当人認証

## 6.3 事業者向けのデジタルサービス等における当人認証の現状

➤ 実際の当人認証においては、以下のような当人認証の単位の相違がある。

図6-2: 事業者向けの当人認証の単位の相違



## 6. 事業者本人確認における当人認証

### 6.3 事業者向けのデジタルサービス等における当人認証の現状

- 当人認証および認可に係るアカウント管理の業務運用の在り方としては、以下のようなケースがある。

表6-1: アカウント管理の業務運用の在り方の相違

当人認証の単位の相違	アカウント管理の業務運用の在り方の相違(例示)	
A. 事業者単位で共通のIDによる認証情報の確認	A	<ul style="list-style-type: none"> <li>✓ サービス提供者側のアカウント管理者により、事業者単位のアカウント管理を行うケース</li> </ul>
B. 操作者個人単位のIDによる認証情報の確認	B-1	<ul style="list-style-type: none"> <li>✓ サービス提供者側のアカウント管理者により、サービス利用者側の管理権限者のアカウント管理のみを行う。</li> <li>✓ その上で、サービス等を利用する事業者側の管理権限者により、サービス提供者側のアカウント管理機能を利用し、当該事業者の操作者個人単位のアカウント管理が行われるケース (≒操作者単位のアカウント管理の業務運用は、サービス利用者側の管理権限者に権限移譲) 例) 請求書電子化サービス事業者や中小企業向けEDIサービス事業者の提供サービス</li> </ul>
	B-2	<ul style="list-style-type: none"> <li>✓ (契約等は事業者や組織単位であるが) サービス提供者側のアカウント管理者または機能により、サービス利用者側の操作者個人単位のアカウント管理も行うケース 例) 名刺管理サービス事業者や企業向け福利厚生サービス事業者の提供サービス</li> </ul>
	B-3	<ul style="list-style-type: none"> <li>✓ 操作者個人単位で利用申請(または契約)が必要であり、サービス提供者側のアカウント管理者により、操作者個人単位のアカウント管理を行うケース 例) 府省共通研究開発管理システム(e-RAD)への民間事業者に所属する民間研究員として登録と利用</li> </ul>

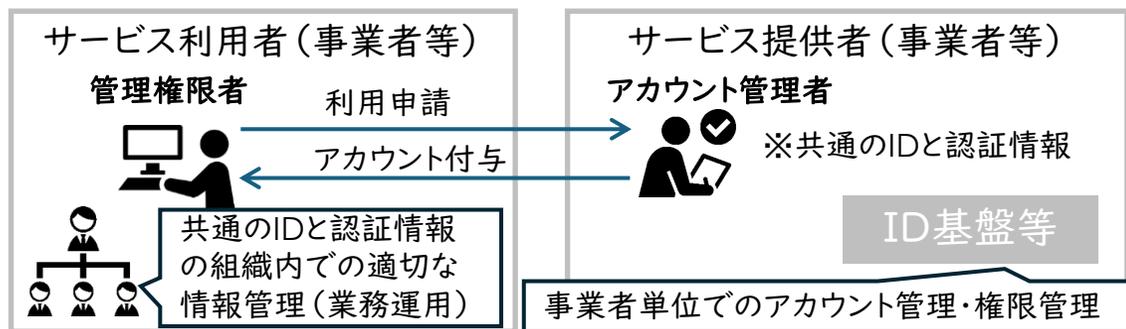
# 6. 事業者本人確認における当人認証

## 6.3 事業者向けのデジタルサービス等における当人認証の現状

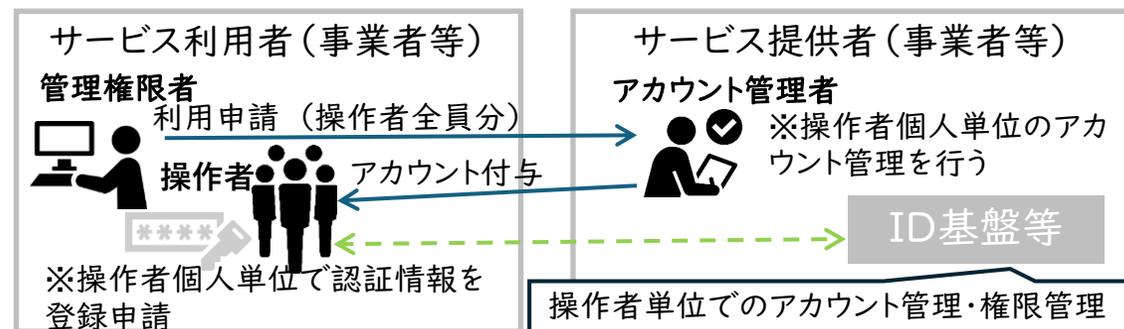
図6-4:アカウント管理の業務運用の在り方の相違(イメージ)

### アカウント管理の業務運用の在り方の相違(例示)

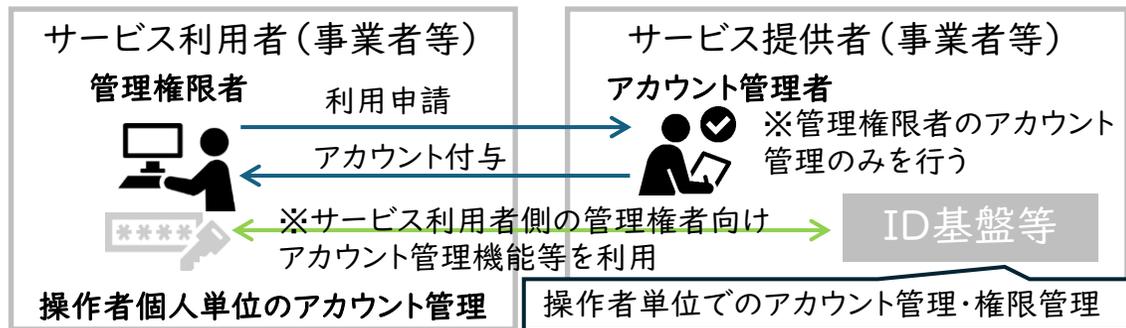
#### <A>



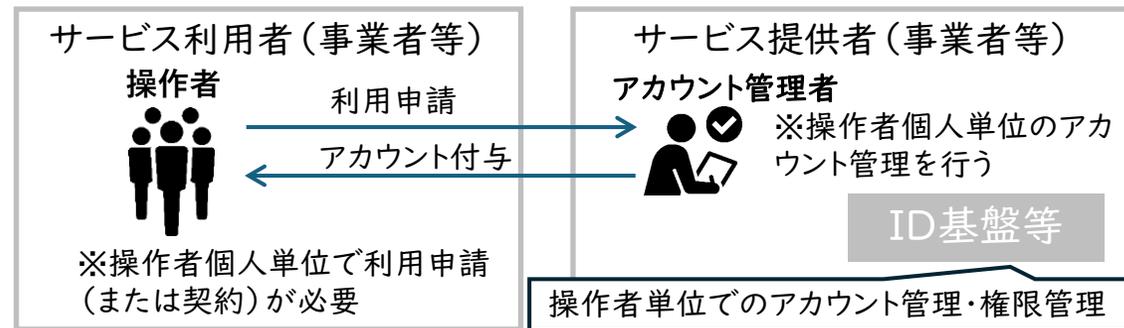
#### <B-2>



#### <B-1>



#### <B-3>



# 事業者確認の全体の課題

## 8. 次世代の目指すべき事業者本人確認に向けて

### 8.1 事業者本人確認の課題の振り返り

➤ 4章、5章、6章の現状分析をもとに、現状の課題を振り返る。

#### 4.4 事業者本人確認の手法に関する考察

※参照:4.4.1 現状の手法の整理(表4-7)

✓ 現状、事業者確認事項の要素を、“一元的に円滑に確認できるデジタル手法”が存在せず、情報取得の負担が大きい

※現状のデジタル手法は、各々の目的に対応するものであり、確認可能な要素の範囲は限定的である。

複数の手法を使い分けする必要がある場合がある事や、確認要素の一部については、現状では確認が困難である事がある。

#### 5.3 信頼できる情報源に関する課題の現状分析

※参照:5.2 信頼できる情報源に関する課題(表6-1)

✓ 現状、“官民の信頼できる情報源”において、「事業者のカバー範囲」「事業者確認事項の要素」「情報鮮度」の、3つの観点で確認可能な範囲のバラつきが大きく、情報取得の負担が大きい

※特定のエビデンスの確認やデータベース等(公的なレジストリや、民間の企業信用調査会社の企業情報調査書等)に対する参照だけでは、実態の把握が困難であり、複数の情報源からの取得や、場合によっては個別現地調査等が必要となるケースがある。

#### 6.4 事業者の当人認証の課題

✓ 近年の外部環境の変化から、事業者の当人認証について、より安全かつ適切な制御が求められていく際に、派生的に、“アカウント管理の業務運用の負担の増大”が課題感として取り上げられるケースも多くなっていくのではないかと想定される

## 8. 次世代の目指すべき事業者本人確認に向けて

### 8.1 事業者本人確認の課題の振り返り

#### ➤ 現状の課題の背景を振り返る。

#### 4.3 事業者確認事項における確認要素の分類

※参照:4.3 事業者確認事項における確認要素の分類(表4-2)

#### ✓ “事業者確認事項の要素”は多岐にわたり、各要素の確認に際して有益となる情報も様々となる

※法的実在性確認または公的情報等に基づく実在性確認、物理的実在性確認、法人等に属する内部組織の実在性確認、所属確認、取引の任に当たっている事の確認、(代表者等取引の任に当たっている自然人の)事業者に関連する自然人の「個人」としての本人確認、法人格の当該行為自体に関わる意思の確認、事業の内容の確認、事業活動の実態有無の確認 など

#### 5.2 信頼できる情報源に関する課題の背景

※参照:2.1 検討対象とする事業者の範囲(図2-1)

#### ✓ 事業者の種別や形態も様々である

※公的なレジストリに関しては、関連する法律等の目的が異なる事を背景に、対象範囲の事業者の相違や保有情報の相違が大きく、情報鮮度に係る課題も存在する。

※特に、個人事業主含む小規模事業者については、全体的に情報不足といえる。

#### 3.1 事業者本人確認の特徴

※参照:3.1 事業者本人確認の特徴(図3-1)

#### ✓ 事業者本人確認は、完全な確認(Proofing)が困難であり、複数の参考となる信頼できる情報を「複合的に確認」により、確からしさを高める(Trustを高める)考え方が必要になる

※事業者を本人確認する場合には、自然人の本人確認とは異なる考え方が必要となる。

# 8. 次世代の目指すべき事業者本人確認に向けて

## 8.1 事業者本人確認の課題の振り返り

【背景】“事業者確認事項の要素”は多岐にわたっている

事業者確認事項の大きな分類	要素
1. 事業者の身元確認 (Identity Proofing)	
1.1. 法人格に対する確認	法的実在性確認、または公的情報等に基づく実在性確認
	物理的実在性確認
	法人等に属する内部組織の実在性確認
1.2. 事業者に関連する自然人に対する確認	所属確認 (代表者等、従業員、代理人等)
	取引の任に当たっている事の確認 (権限確認)
	(代表者等取引の任に当たっている自然人の) 事業者に関連する自然人の「個人」としての本人確認
2. 意思の確認 (intention)	法人格の当該行為自体に関わる意思の確認 (内容確認をしている事の確認含む)
3. 顧客管理 (Customer Due Diligence)	事業の内容の確認
	事業活動の実態有無の確認 (当該事業者や組織の運営状態を確認)
	実質的支配者 (BO) の確認
	反社確認
	資産及び収入の状況の確認
	信用情報確認

【背景】事業者の種別や形態も様々 (例: 登記有無、個人事業主)

### 現状の課題

“官民の信頼できる情報源”において、「事業者のカバー範囲」「事業者確認事項の要素」「情報鮮度」の、3つの観点で確認可能な範囲のバラつきが大きい



現状、事業者確認事項の要素を、“一元的に円滑に確認できるデジタル手法”が存在しない



※商業登記電子証明書、登記情報提供サービス、法人番号公表サイト、gBizINFO、企業信用調査会社の企業情報照会サービス、電子委任状など

## 8. 次世代の目指すべき事業者本人確認に向けて

### 8.2 次世代の事業者本人確認とは？

次世代に求められる事業者本人確認の在り方とは？

例えば、

- 確からしさの向上
  - 鮮度の高い、より確かな情報に基づいた事業者本人確認を実施できる
  - 大規模な事業者でなくても、より確度の高い事業者本人確認に対応でき、リスクを軽減できる
- より容易で効率的・効果的な事業者本人確認
  - デジタルエビデンスに基づいた、より信頼でき効率的な事業者本人確認
  - 確認手法の違いによる確認に関わる業務負担の軽減



様々な本人確認実施事業者が持つ鮮度の高い確認情報や、信頼できる機関が持つ確度の高い事業者の情報との連携

## 8. 次世代の目指すべき事業者本人確認に向けて

### 8.3 次世代の事業者本人確認を検討するための論点とは？

次世代の事業者本人確認に向けて以下の論点が含まれる

- 事業者確認事項の要素の整理  
今回考察した対象以外の様々なユースケースを想定することが必要
- 事業者情報連携のモデルの整理
  - 事業者間連携のアーキテクチャ(システムのモデル)
  - 事業者間の連携を促進するビジネスモデル・インセンティブ
- 事業者確認情報のデジタルデータ表現
  - データフォーマット、事業者確認事項のデータ表記の標準化
  - デジタルインタフェース(プロトコル)の標準化
  - デジタルエビデンスの実現可能性・利用可能性
- 事業者当人認証のモデルの整理
- 事業者本人確認 保証レベルの規定
  - 明確なレベル分けができなくてもトラストフレームワークの区別ができること。
  - どの視点や粒度(例:要素のセットのレベル)での保証レベルの規定が可能か検討する必要がある。
  - 総合的な保証レベルは多次元になりえる。事業者確認要素のレベルではアシュアランスレベルが必要ではないか。

# CBDCでの論点

- 事業者本人確認に関するベースラインとなる要求事項の整理の必要性。
  - **OIDF-Jの報告書へのフィードバックもお待ちしています！**
- 事業者本人確認のデジタル化の可能性。
  - デジタルエビデンスの実現可能性（CBDCの範疇を超えるが）。
  - デジタルエビデンスがカバーする証明内容の違いにも注意が必要（例：eシール vs 法人代表者電子証明書）。

## 【事業者間のCBDC利用のユースケースやモデルの整理をしたうえで…】

※検討全体としてユースケースを限定する必要はないが、議論のきっかけや意識合わせとしてあったほうがよい。

- 事業者に関するID連携モデルの可能性。ありえる場合には、上記の要求事項の整理に基づくデータの定義が必要。
- 当人認証のアカウント管理の形態も含めたモデルの区別の必要性。（管理負担の軽減も両立する必要がある）
- 事業者に関する属性情報による柔軟な認可の可能性（プログラマブルマネー等）。