Digital Architecture Design Center

IPA Better Life with IT

インキュベーションラボ第二回成果報告

対象テーマ：「サービスに応じたデジタル本人確認ガイドラインの検討」

2022年7月

独立行政法人情報処理推進機構（IPA）
デジタルアーキテクチャ・デザインセンター（DADC）

本資料・本活動の位置づけ

本資料は、第二回インキュベーションラボテーマの活動成果報告（概要版）の詳細を説明する資料である。

本活動では、「サービスに応じたデジタル本人確認ガイドラインの策定」に向けた、事前検討を行った。

エグゼクティブサマリ

背景

Society5.0の進展や、新型コロナ感染症対策による非接触・非対面のライフスタイルの急速な定着などの影響もあり、様々な業種や業界に次々とオンラインサービスが提供され始めている。しかし、事業者向けの共通指針等がないため、事業者の多くがビジネスやサービスに適したデジタル本人確認手法の選択に苦慮し、法令に定められた手法を選択して過剰な本人確認が行われる等の事態が起きている。

経済産業省の検討会の報告書(*1)においては、「現状、身元確認は自己申告もしくは公的身分証の確認のいずれか」である現状が明らかになっており「身元確認の厳格化とあわせて手間・コストのハードルが大きく上がることが課題である」と示された。また、法令等の規制や指針がない場合にどういった強度の身元確認を実施すべきかについて、レベル感の考え方や考慮すべき要素が整理されているものが有用ではないか、と提唱されていた。

テーマ

民間事業者と個人間でオンライン上で行うデジタル手段による本人確認について、その導入や点検等に資するガイドライン策定を目標とし、現状把握を中心に、ガイドラインに必要な基礎情報収集、分析を行う。

活動の成果

本活動では、現状の本人確認手法を、IAL（身元確認保証レベル）とAAL（当人認証保証レベル)※のマトリクスに配置することで、特定のレベルに認証強度の異なる手法が混在し集中していることを可視化した。ニュージーランドにて先進的に取り組まれていたBA※の概念を取り入れてIALを細分化し、保証強度レベルの境界線を可視化した（※IAL、AAL、BAの説明はp5、p25参照）。その結果、法令に定めがない手法も、一定の技術要件が確保されれば犯収法等に定められた手法と同等の保証レベルと見做せるなど、事業者がサービスに応じた手法を選択しやすくなることが確認できた。

また、14の団体および事業者に対して、本人確認の適用の現状とそのリスクや課題等についてのヒアリングを実施した結果、事業者の手法の選択は、リスクだけでなく、ユーザビリティやコスト等総合的に勘案して決定されており、手法選択を円滑に行うためにも事業者向けのガイドラインの策定が強く望まれていることを改めて確認することができた。

デジタル庁「トラストを確保したDX推進サブワーキンググループ」が2022年3月22日に取りまとめた報告書にも、DADCでの検討成果も踏まえて、マルチステークホルダーで検討を進めていくことが明記され、引き続き官民多様な主体で連携して検討される案件として位置付けられている。今後は、デジタル庁等関係機関と連携しながら、OpenIDファウンデーション・ジャパンと協力して検討の場を探索していき、早期のガイドラインの策定を推進する。

*1「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」　2020/3/31　https://www.meti.go.jp/press/2020/04/20200417002/20200417002-3.pdf

Digital Architecture Design Center

目次

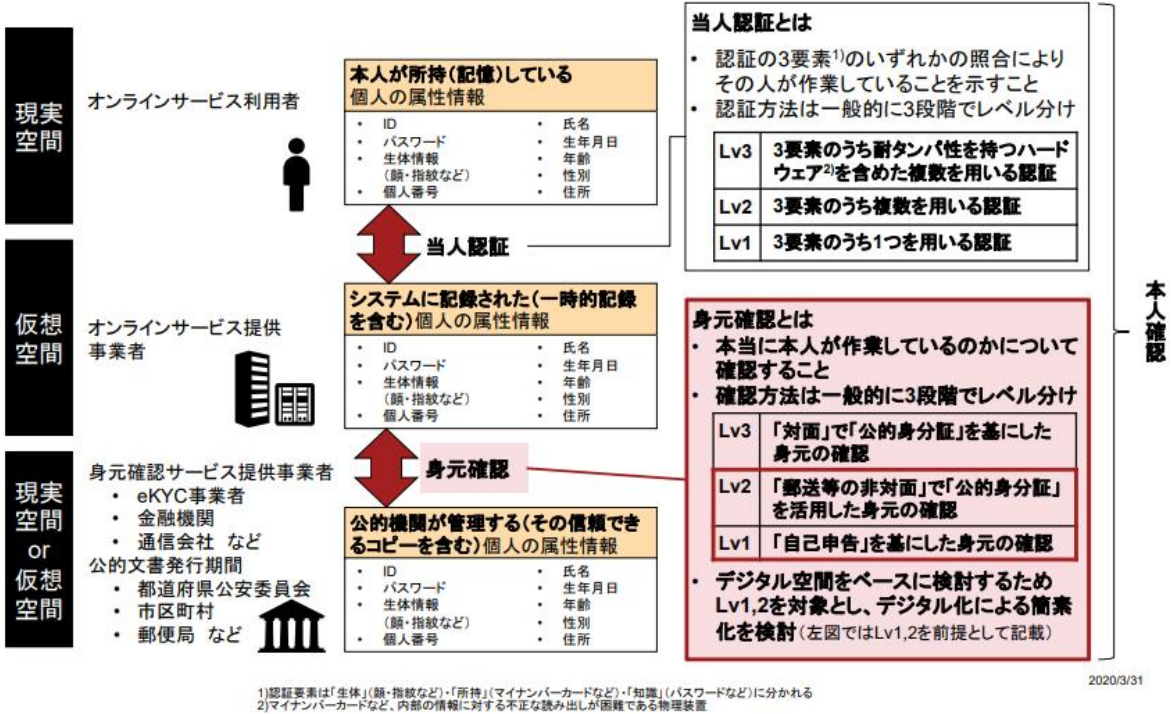
Digital Architecture
Design Center

目次

（前提）本人確認とは

「身元確認」および「当人認証」を合わせて、本人確認という。
またそれぞれのアシュアランス（保証/確保/担保）のレベルを、IAL、AALという（＊）。

＊ 世界規模でデファクトスタンダードとなっている米国立標準技術研究所（NIST）の認証に関するガイドライン「Digital Identity Guidelines（電子的認証に関するガイドライン）」による定義。当プロジェクトでも参照し、検討や議論を進行。



当人認証の保証レベル
＝ **AAL**
（Authenticator Assurance Level）

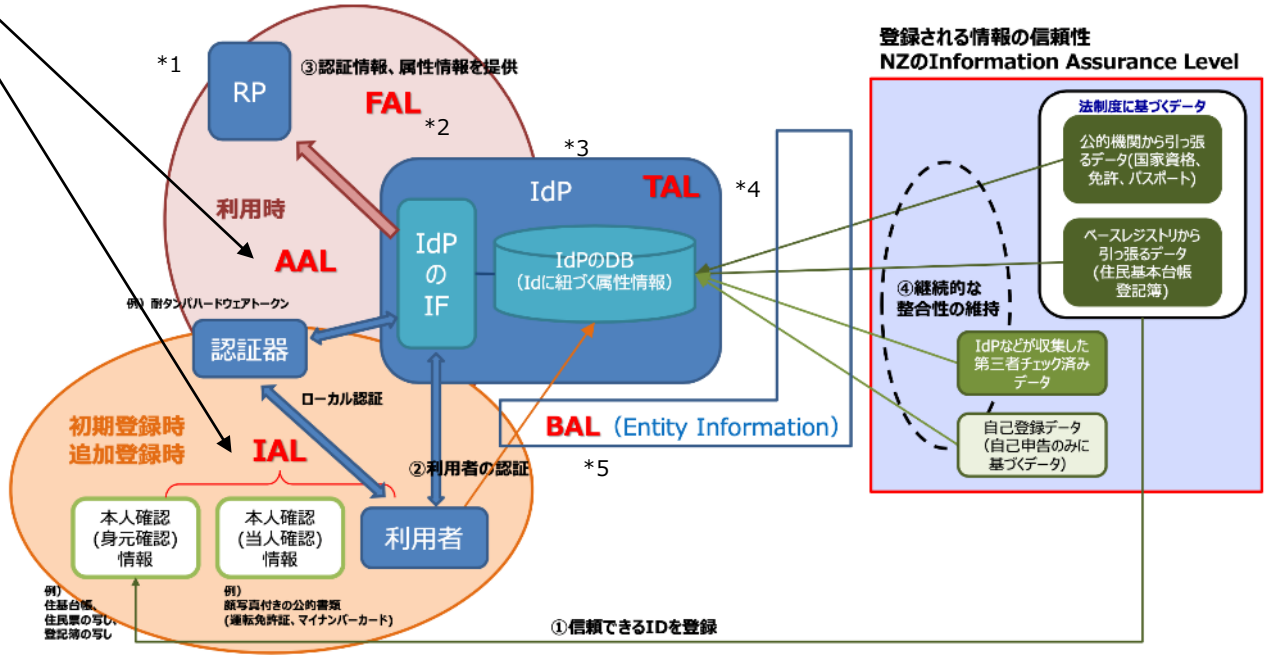
身元確認の保証レベル
＝ **IAL**
（Identity Assurance Level）

［引用元］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（経済産業省）

（前提）トラストサービスのアシュアランスレベルの考え方

IALはアカウントの初期登録、追加登録時に、AALはアカウントの利用時に重要となる。

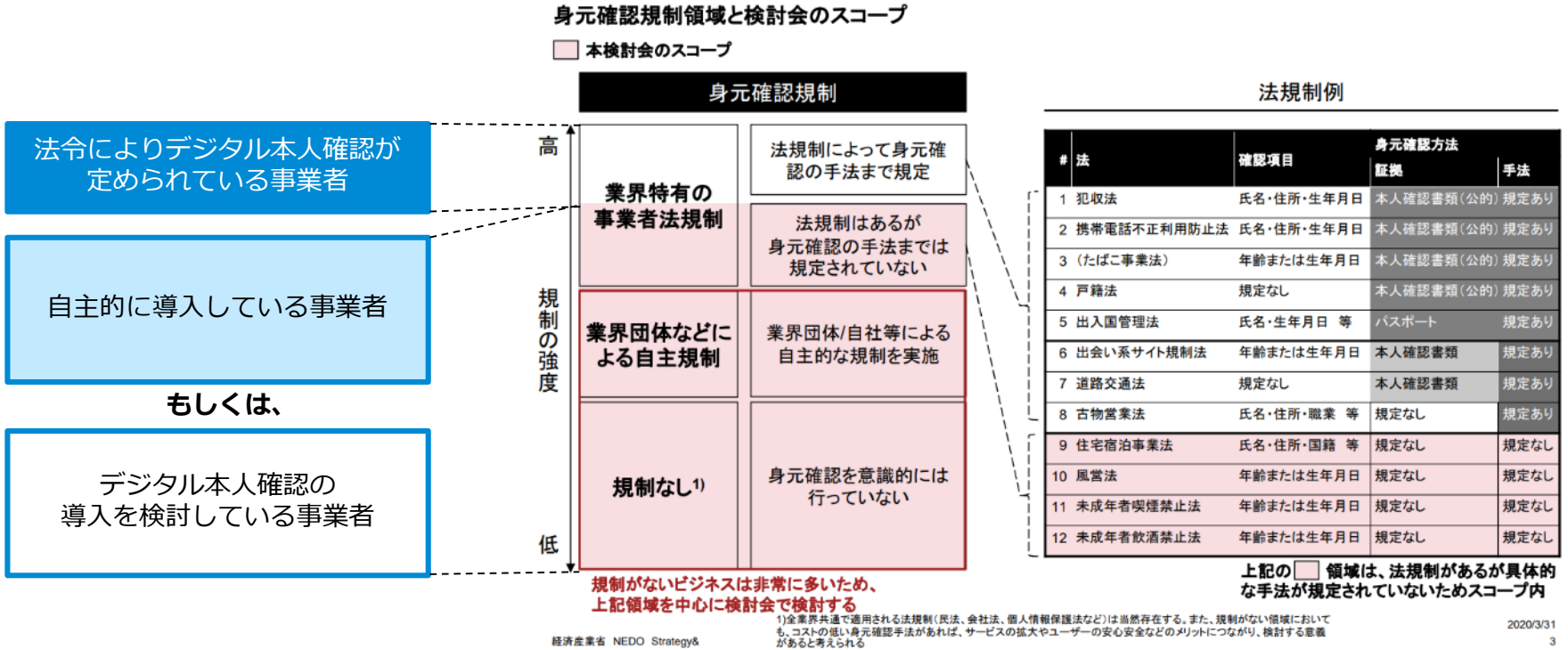
［引用元］第5回トラストを確保したDX推進サブワーキンググループ　資料2　手塚氏提出資料（トラストサービスのアシュアランスレベルの考え方）（デジタル庁）



*1　RP　：Relying Partyの略。IDでログインするサイト、サービス。
*2　FAL　：Federation Assurance Levelの略。IDトークン等、Assertionのフォーマットやデータやり取りの仕方の強度。
*3　IdP　：Identify Providerの略称。クラウドサービスなどにアクセスするユーザーの認証情報を保存・管理するサービス。
*4　TAL　：Trust Assurance Levelの略。トラストサービスの信頼度。
*5　BAL　：Binding Assuarance Levelの略。被検証者とIDの紐づけの強度。

（前提）本人確認に関する規制の有無

ビジネスの内容によっては本人確認の手法が規定されているものの、大部分のビジネスでは規制されていない。



#	法	確認項目	身元確認方法	
			証拠	手法
1	犯収法	氏名・住所・生年月日	本人確認書類（公的）	規定あり
2	携帯電話不正利用防止法	氏名・住所・生年月日	本人確認書類（公的）	規定あり
3	（たばこ事業法）	年齢または生年月日	本人確認書類（公的）	規定あり
4	戸籍法	規定なし	本人確認書類（公的）	規定あり
5	出入国管理法	氏名・生年月日 等	パスポート	規定あり
6	出会い系サイト規制法	年齢または生年月日	本人確認書類	規定あり
7	道路交通法	規定なし	本人確認書類	規定あり
8	古物営業法	氏名・住所・職業 等	規定なし	規定あり
9	住宅宿泊事業法	氏名・住所・国籍 等	規定なし	規定なし
10	風営法	年齢または生年月日	規定なし	規定なし
11	未成年者喫煙禁止法	年齢または生年月日	規定なし	規定なし
12	未成年者飲酒禁止法	年齢または生年月日	規定なし	規定なし

［引用元］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（経済産業省）

プロジェクトのテーマ・内容（採択時）

【テーマ名】
サービスに応じたデジタル本人確認ガイドラインの検討

【内容】
海外のビジネスや標準化の動向も踏まえ、将来のデジタル本人確認（身元確認・当人認証）によって実現すべき社会や産業構造の将来像を具体的に描くとともに、その実現に向けたアーキテクティングを行うことで、様々なサービスやインフラが広く準拠できるデジタル本人確認の協調領域の検討に注力し、ガイドラインとして整理する。

【採択条件】
- 既存の本人確認（身元確認・当人認証）の手法の標準化や、サービスごとのレベル分けに関する基準などのルールメイキングの検討だけでなく、Identificationや認証（Authentication、Certification）が、本人の信頼性をどうもたらすのかも含めて、将来的にどうあるべきか、それにより社会がどうなっていくべきかという将来像を具体的に描き、その実現のためのアーキテクティングを行った上で、本人確認に関係する様々なサービスやインフラが準拠する協調領域の検討を行いガイドラインとして整理すること。
- 多様な企業や個人が協調領域として活用できるものにしていくために、提案事業者にとって競合となるプレイヤー（例えば分散型IDなど、デジタルIDについて異なる考え方を持つ者）や、本人確認の周辺領域のステークホルダーの考えを取り込みながら、協調領域の検討に注力すること。なお、本テーマをワーキンググループにする場合には、競合となるプレイヤーを体制として取り込むこと。

【留意事項】
- 既に海外でのビジネス実装や標準化が進む分野でもあり、日本独自ではなく、海外動向を踏まえながらグローバルに通用する内容を目指すこと。
- DADCとして取り組む際の前提ではあるが、設計したアーキテクチャの実装には政府など公的機関の関与が必要と考えられることから、そうした関係者と検討初期段階から密に連携すること。

採択時の目的

- 目的

日本の産業や生活を、グローバルに通用するデジタル本人確認のガイドラインが普及した、サービス提供者と利用者双方の安全性、利便性が両立した環境にする。このことにより、Society5.0に根差した市場拡大及び国際競争力に資する。

- 目標

サービスに応じたデジタル本人確認のガイドライン及び技術を、世界の動向を踏まえて整備し、広く普及させる。

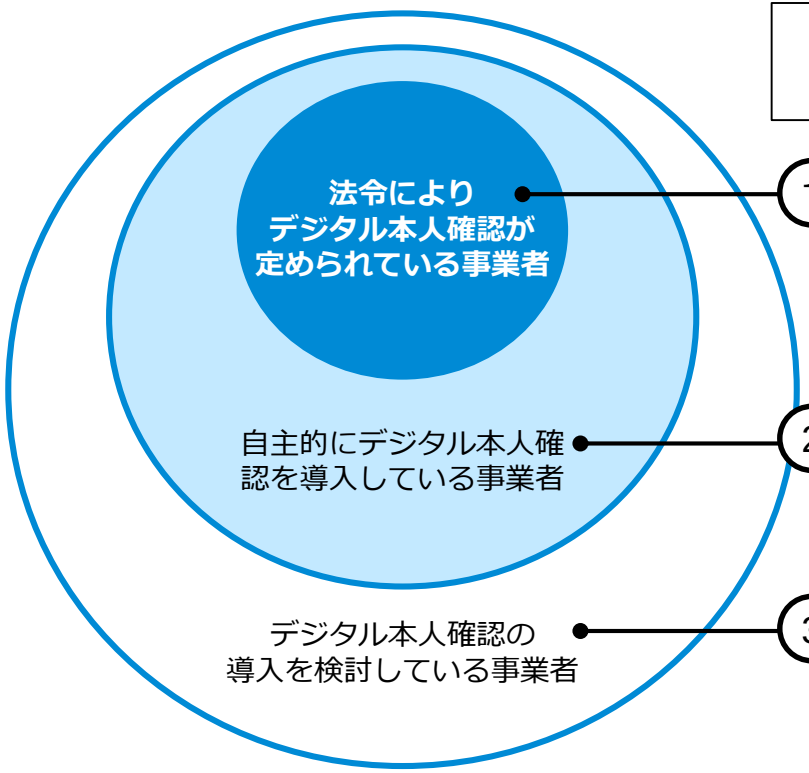
- 活動のスコープ
  - 個人の民間サービスを対象とする。
  - 既にガイドラインが定められている「行政手続き」は取り扱わない。

【活動のスコープ（赤枠内）】

サービスの種類	サービス提供者の種類		利用	ガイドラインの現状
	管理責任	実行責任		
行政サービス、 行政手続	行政機関、自治体・省庁 及び関連組織	行政機関、自治体・省庁 及び関連組織	個人 法人	あり 「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」
民間委託、 コラボレーション	行政機関、自治体・省庁 及び関連組織	企業、個人事業主	個人 法人	なし 但し「行政手続き～」に従うことが適当。管理責任者の基準において、実行責任者が実行するため。
民間サービス	企業、個人事業主	企業、個人事業主	個人 法人	**大部分に存在しない** **身元確認/当人認証の保証レベル判定方法、保証レベルに応じた手法例が必要**

ガイドラインを策定する趣旨

規制の有無に関わらず「本人確認手法が分からない」（下図①～③）ことが事業者共通の課題となっている。
ガイドラインを策定し普及させることで、各種本人確認手法の保証レベルが整理でき、自社サービスの特性に応じた本人確認の選択が可能になると想定。



＊ 円の大きさは事業者数の規模を表現

	本活動のメンバーが把握している本人確認手法に関する事業者の課題
①	法令に多くの手法が定められているが、安全性や利便性の**違いが分からない。**
②	導入済みの手法が自社のサービスに**最適な手法か分からない。**
③	対面手続に代わる手続となるデジタル本人確認の手法を、**どのように選択すべきか分からない。**

ガイドラインの主な役割

①本人確認手法の保証レベルの整理

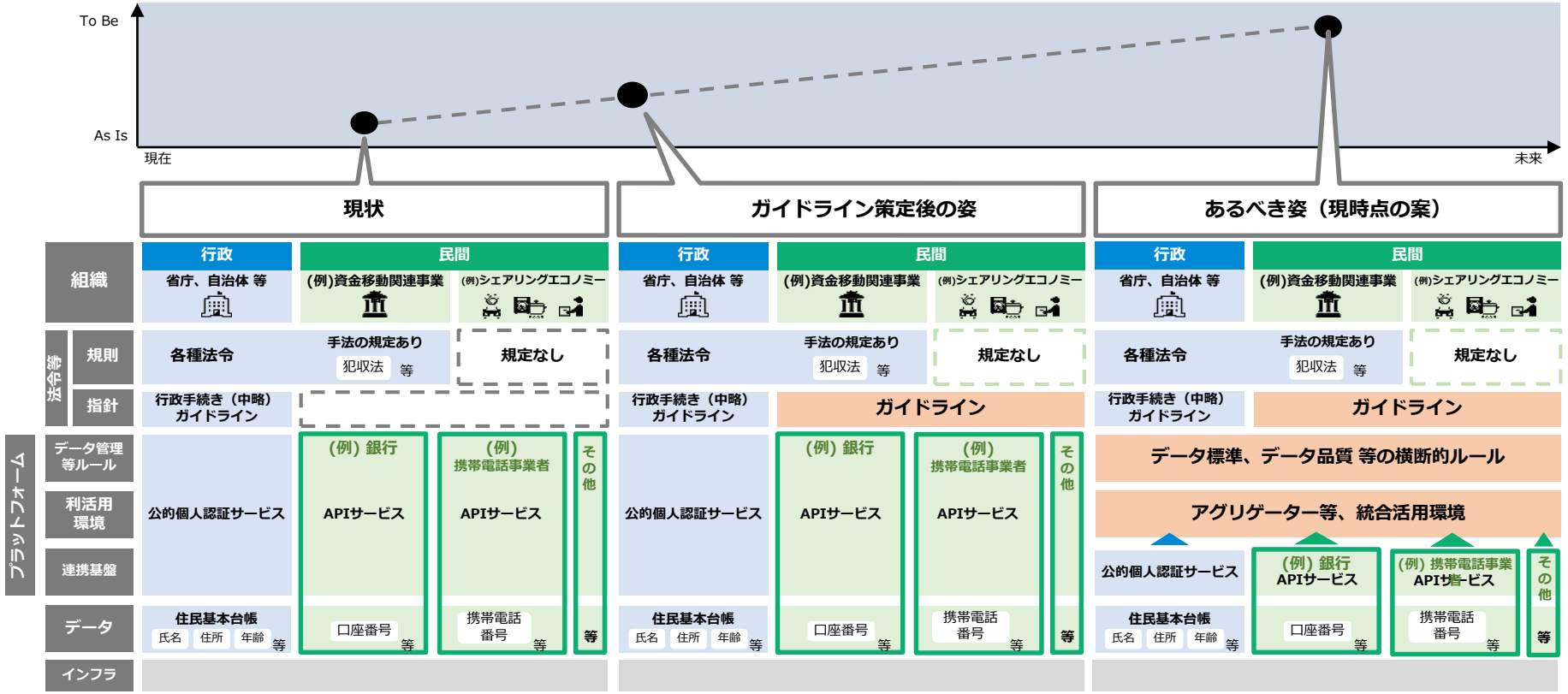
②サービスに応じた本人確認手法の選択

Digital Architecture Design Center

目次

デジタル本人確認の現状、あるべき姿と、ガイドラインを策定する趣旨

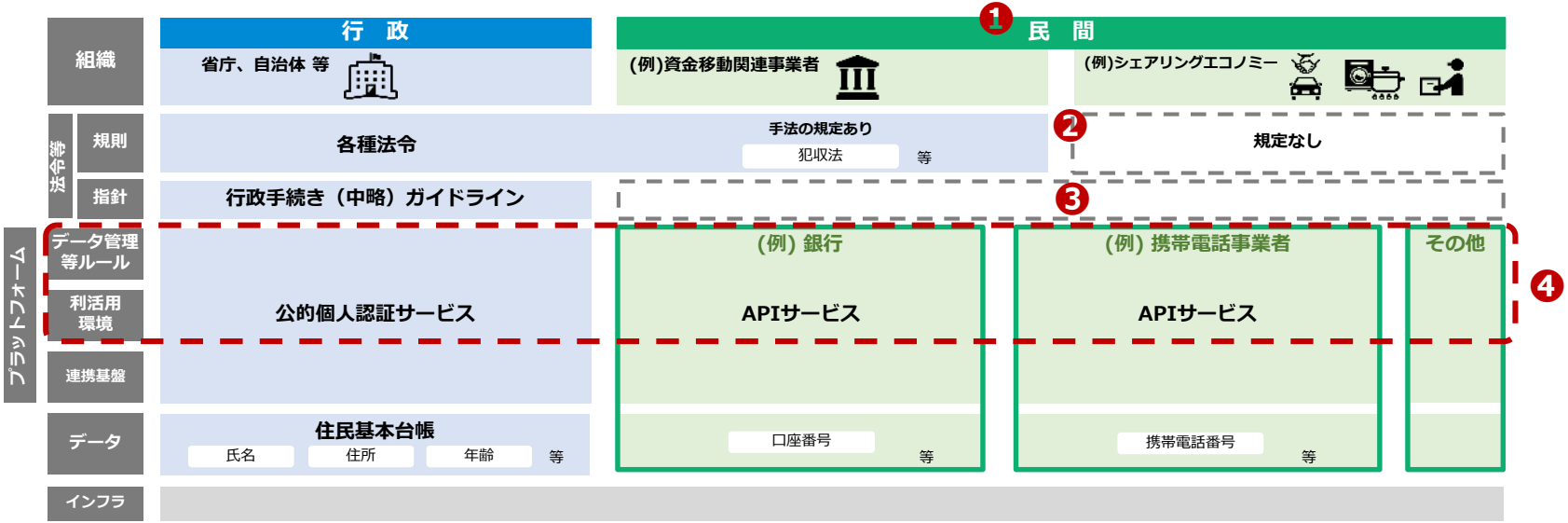
ガイドライン策定により、安心安全なデジタルサービスが普及し、データの利活用が促進される。



上記図は「包括的データ戦略のアーキテクチャ」（https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/576be222-e4f3-494c-bf05-8a79ab17ef4d/210618_01_doc03.pdf）を参考として、デジタル本人確認に関して表現。

デジタル本人確認の現状

本プロジェクトがラボ活動を通して把握したデジタル本人確認への事業者のニーズ、および現状の課題は、主に以下の通り。



❶ 民間事業者におけるデジタル本人確認へのニーズは、主に以下の通り。
- 事業リスクへの対策として**一定の保証レベルを確保したい**
- ユーザーやサービスに応じた手法にしたい（**コスト、UX等への配慮**）

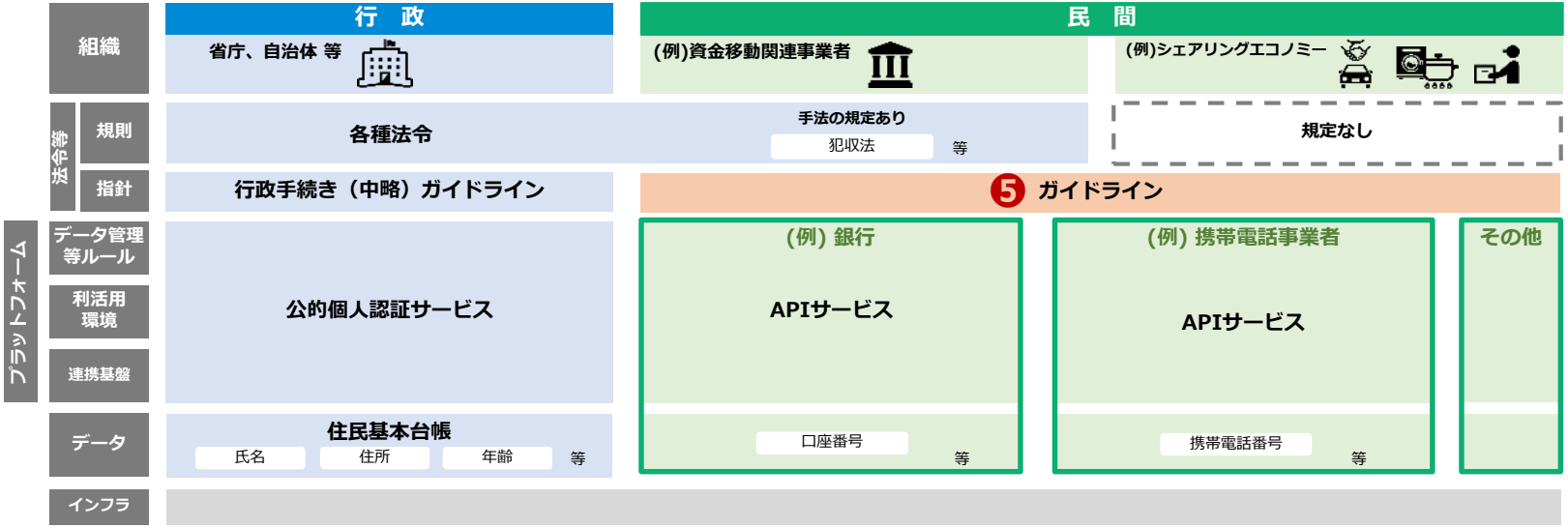
❷ 導入検討時に、**拠り所になるルールがなく**、事案発生後に対策する／強化している。

❸ **本人確認の各手法の違いが不明瞭で比較しにくく**、自社に最適な手法か分からない。

❹ 組織ごとに属性情報のデータ仕様、品質に対する考え方や、利活用環境が異なっており、**統合的な活用を行いにくい。**

ガイドライン策定の意義、狙い

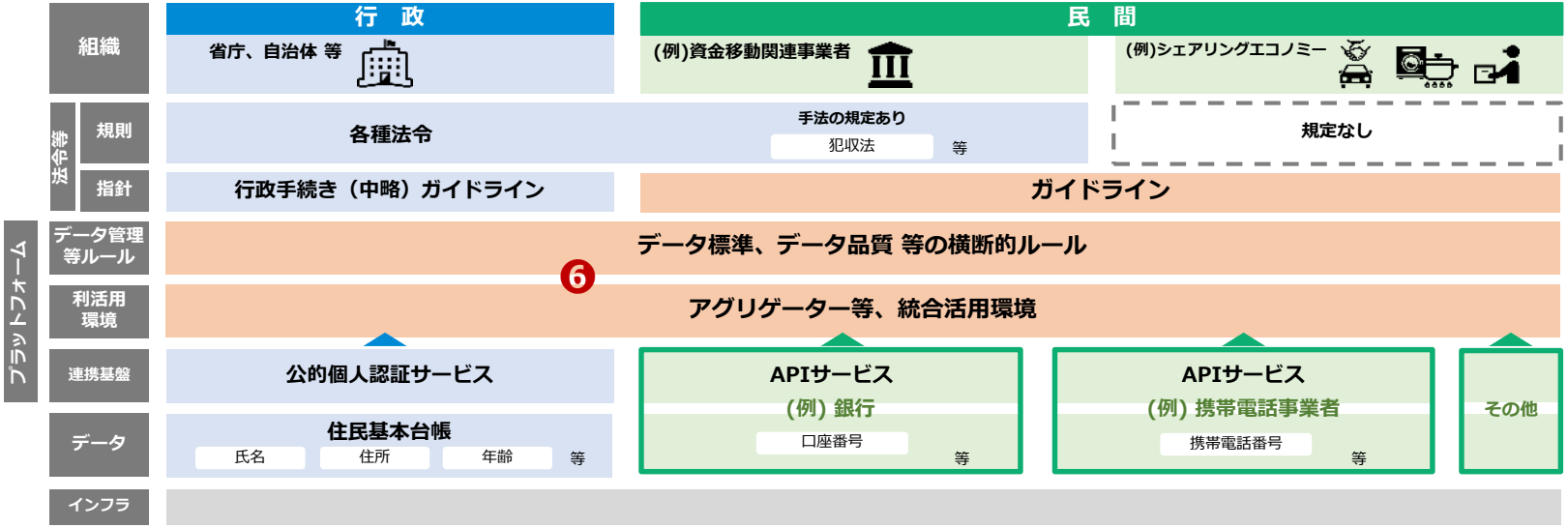
あるべき姿とのギャップに対する方策として、まず「ガイドライン策定」が必要であると認識。



❺ ガイドライン策定、およびその普及により、**デジタル本人確認の各手法、エビデンスの特徴や違いが明確になり、現状の課題**（前述の**❷、❸**）**が解消**される。
また、民間手続きにおけるデジタル本人確認のプラットフォームに求める要件が明らかになる。
（例）どのようなサービスでどんな手法が必要とされるか。その場合、どういった属性情報が必要か。
プラットフォームへの要件が明確になることは、**プラットフォームを横断するルール、およびPDS（Personal Data Store)等統合活用環境の具体的かつ、統制の取れた検討の進展に資する。**

デジタル本人確認のあるべき姿（現時点の案）

現在想定するデジタル本人確認の「あるべき姿（現時点の案）」は以下の通り。



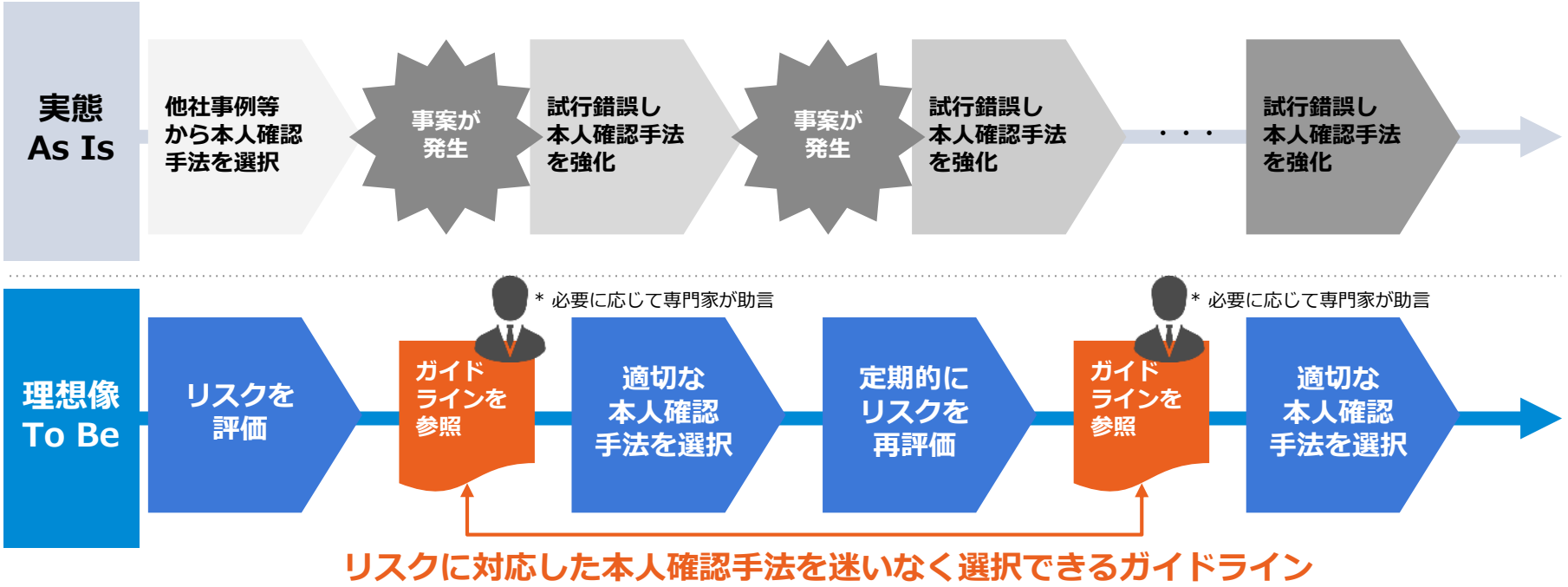
❻ デジタル本人確認の**各プラットフォームを横断したデータ標準やデータ品質に関する共通ルールが整備され、統合活用環境が整備される。**

（例）ユーザーはアグリゲーターを通じて氏名、住所、マイナンバー、口座番号、携帯電話番号等、属性情報の連携や更新等の制御を統括して行うことができる。事業者はアグリゲーターから連携される情報であることを拠り所にすることで、その他の身元確認をせずとも、ユーザー情報の取得やサービスの提供を行うことができる。

ガイドライン普及によるビジネスプロセスの変化（現在の想定）

ガイドラインが普及することにより、各事業者が試行錯誤をせずとも、各事業者のリスク評価結果に対応したデジタル本人確認手法を選択できるようになる。

リスクに応じた本人確認手法選択の実態と理想像

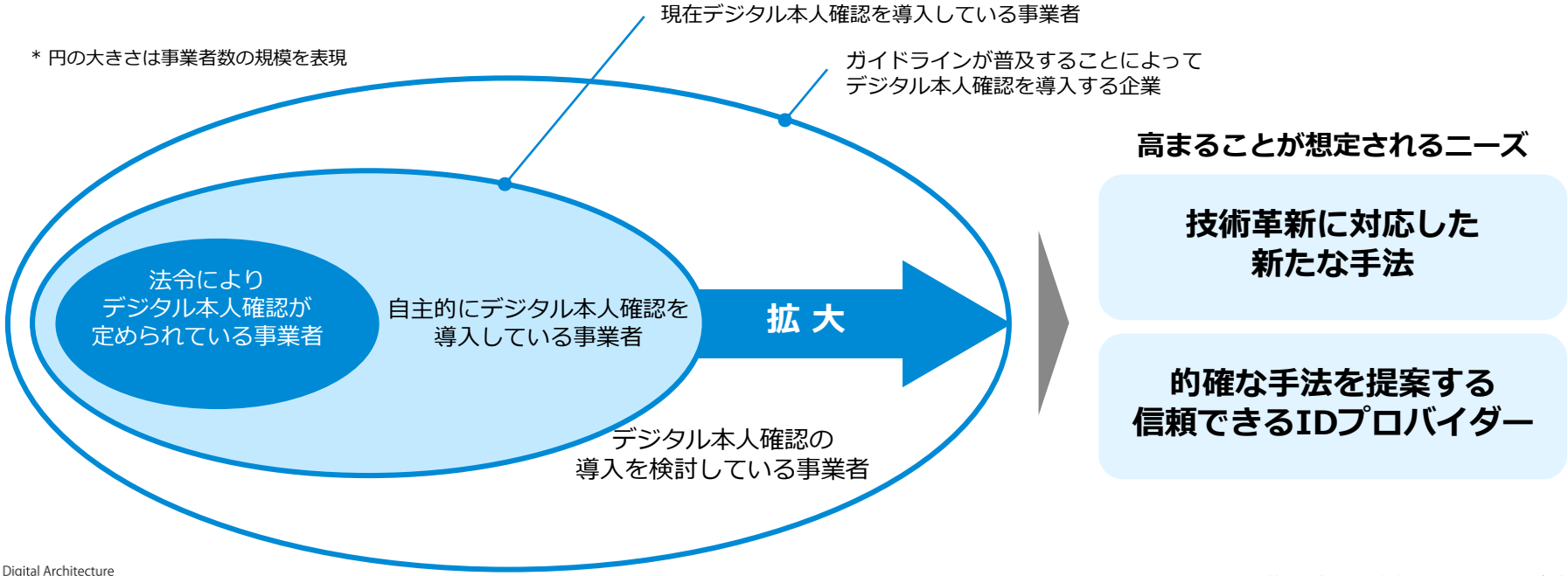


ガイドラインの普及が社会に与える影響（現在の想定）

ガイドラインが普及することで、デジタル本人確認を導入する事業者が増え、以下のニーズが高まることを想定。

- ガイドラインに基づいた、技術革新に対応した新たな手法
- ガイドラインに沿って的確な手法を提案する「信頼できるIDプロバイダー」

トラストサービス関連の市場規模が拡大し、日本におけるトラストサービスの醸成やイノベーションが促され、サービスを提供する側、利用する側の両者の利便性、安全性が向上することを期待。



Digital Architecture
Design Center

目次

インキュベーションラボにおける活動

- 活動期間
  2021年8月～2022年1月
- 活動
  主に以下4点の活動を通し、デジタル本人確認の現状とあるべき姿について考察。

1	本人確認手法の保証レベルの整理	現状、多くの民間サービスにおいて指針のない本人確認手法の保証レベルについて整理することで、ガイドラインとして示す保証レベルがどうあるべきかを考察。
2	事業者・関係団体に対する本人確認等に係るヒアリング調査	各事業者が抱えているリスク、実施している本人確認の具体的手法、当該手法を選択した理由や方法、その他本人確認に関する課題等の実態調査を目的に、オンラインサービス提供事業者や業界団体に対してヒアリングを実施。
3	リスクに応じた本人確認手法選択の現状と課題	リスクに関して、事業者等へのヒアリングから得た情報や示唆等から、事業者が捉えているリスクの事例や当該リスクへの対応等について整理。
4	海外動向調査	海外におけるデジタルID、および本人確認の現状について、Webを中心に情報収集し、整理。

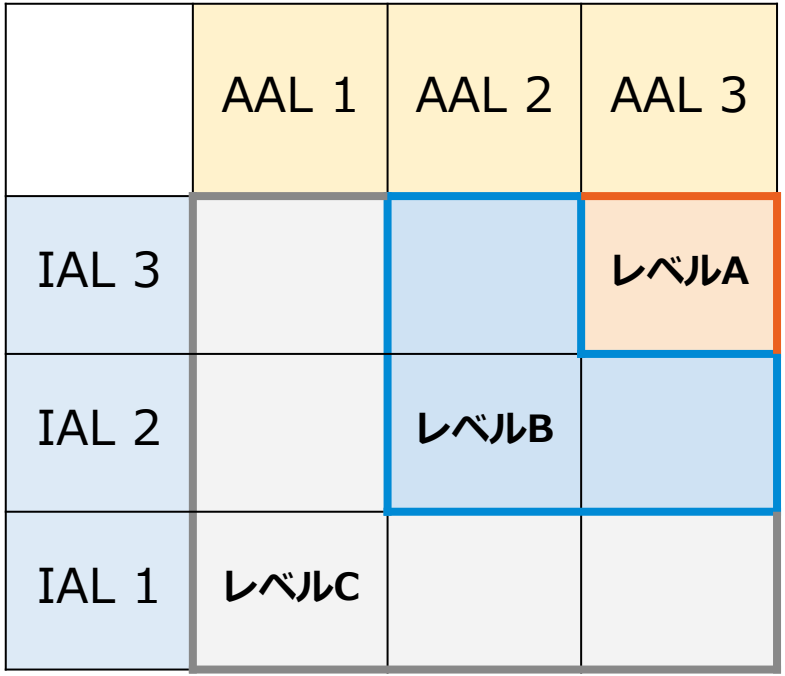
Digital Architecture
Design Center

目次

本人確認手法の保証レベル分類方法

IAL・AALの両観点で本人確認手法を分類し、レベルの低い方が本人確認手法のレベルと判断。

保証レベル	
IAL	AAL
レベル３ 対面での身元確認	**レベル３** 耐タンパ性が確保された ハードウェアトークン
レベル２ 遠隔又は対面での身元確認	**レベル２** 複数の認証要素
レベル１ 身元確認のない自己表明	**レベル１** 単一又は 複数の認証要素



［引用元］行政手続き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（各府省CIO連絡会議）

本人確認の現状　本人確認手法について

本人確認手法をマトリクスに配置したところ「レベルB」に集中しており、法令内でもばらつきがみられる。

身元確認レベル（IAL） ＼ 当人認証レベル (AAL)	認証なし	レベル1 単要素認証	レベル2 2要素認証	レベル3 2要素認証 (耐タンパを含む)
レベル3 対面確認				・犯収法ワ (犯収法規則6条1項1号) ・公的個人認証
レベル2 郵送・リモート確認		・公的身分証以外の身分証のアップロード ・公的身分証のアップロード ・犯収法ホ (犯収法規則6条1項1号) ・口座連携(犯収令13条1項1号)	・公的身分証以外の身分証のアップロード ・公的身分証のアップロード ・犯収法ホ (施行規則6条1項1号) ・口座連携(犯収施行令13条1項1号) (* 1) ・身元確認のAPI連携 （銀行API/携帯電話事業者API) (* 1) ・犯収法ヘ (犯収法規則6条1項1号) ・犯収法ト（施行規則6条1項1号） ・犯収法ヲ (犯収法規則6条1項1号) ・民間APIサービスB (* 1)	・犯収法ヘ (犯収法規則6条1項1号) ・犯収法ヲ (犯収法規則6条1項1号) ・身元確認のAPI連携 （携帯電話事業者API）（SIM利用) (* 1)
レベル1 自己申告		・身分証に基づかない自己申告での登録	・身分証に基づかない自己申告での登録	

凡例	レベルC	レベルB	レベルA

＊1　アカウント作成後は身分証不要

本人確認の現状　オンラインサービスにおける本人確認について

本人確認を実施しているオンラインサービスについてもマトリクスの「レベルB」に集中。

身元確認レベル（IAL） ＼ 当人認証レベル (AAL)	認証なし	レベル1　単要素認証	レベル2　2要素認証	レベル3　2要素認証 (耐タンパを含む)
レベル3 対面確認			・古物商A (* 1) ・犯収法の特定事業者 (* 1) ・携帯電話事業者 (* 1) ・シェアリングエコノミーA社 (* 2)	・犯収法の特定事業者 ・携帯電話事業者(* 1) ・電子サインA (* 1)
レベル2 郵送・リモート確認		・マッチングアプリ ・シェアリングエコノミーB社	・犯収法の特定事業者 (* 1) ・携帯電話事業者 (* 1) ・古物商B (* 1) ・シェアリングエコノミーB社 (* 2) ・マッチングアプリ (* 3) ・たばこ会員登録 (* 3) ・公営ギャンブル (* 3) ・eMAFFプライム (オンライン本人確認) (* 4) ・gBizプライム (郵送) (* 4) ・引越し (* 4)	・電子サインA (* 1) ・口座開設 (ネット完結) (* 2) ・たばこ会員登録 (* 3) ・公営ギャンブル (* 3)
レベル1 自己申告		・gBiz・eMAFF (エントリー) ・電子サインC (* 1)	・電子サインB (* 1)	

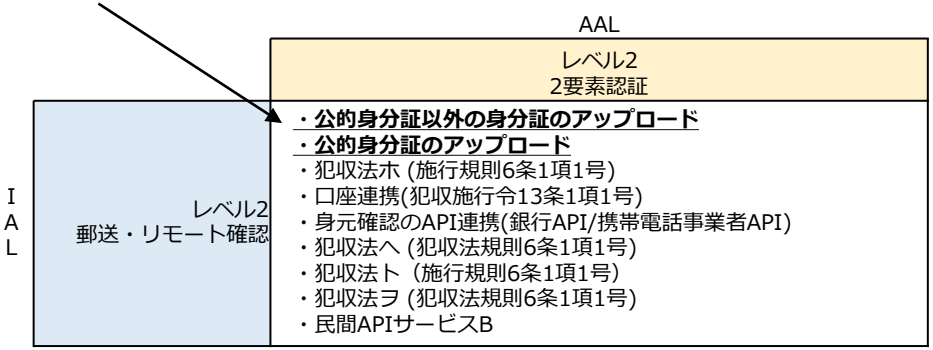
凡例　レベルC　レベルB　レベルA

＊1　法令に基づく
＊2　自主的取組
＊3　自主的取組 (年齢確認のみ)
＊4　行政

IALの細分化

本人確認手法をIALとAALのマトリクスへ配置したところ、以下が明らかになった。

- 本人確認手法および本人確認を実施しているオンラインサービスのいずれもが「レベルB」に集中していた。
- 「レベルB」の中には、認証強度が異なる手法が混在していると考えられる。
  （例）公的身分証画像のアップロードと、公的身分証以外のアップロードの両方が「レベルB」



事業者が自社サービスの特性に応じた適切な本人確認手法を選択するためには、本人確認レベルを細分化し、各手法の保証レベルの差をより明示的にする必要がある。

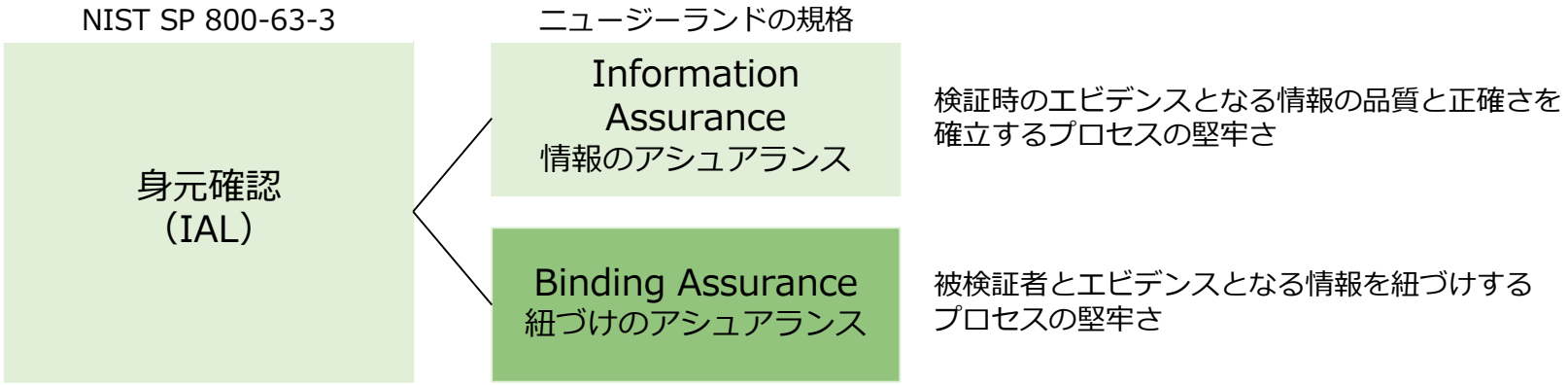
本人確認の段階において、**初期のアカウント作成・登録時に重要なIALを優先**して検討。

ニュージーランドにおける本人確認規格を導入し、細分化を実施。
細分化後のIALを、本書では便宜上「DADC・IAL」とする。

（参考）ニュージーランド規格における身元確認の細分化（概要）

ニュージーランドの本人確認に係る管理規格である「Identification Management Standards」は、世界規模でデファクトスタンダードとなっている米国立標準技術研究所（NIST）の認証に関するガイドライン「Digital Identity Guidelines（電子的認証に関するガイドライン）」（＊）の考え方を基にした上で、**身元確認を2つの観点に細分化**。
Binding Assuranceを取り入れて形にしたという点において、世界的な先例となっている。

身元確認のアシュアランスに関する世界の議論の状況



＊ 日本における「行政手続き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」でも参照されている。
2022年2月現在、第3版（NIST SP 800-63-3）が最新。

［参照元］
- NIST SP 800-63-3「Digital Authentication Guideline」・Identity Assurance Level（IAL）（SP 800-63A）・Authenticator Assurance Level（AAL）（SP 800-63B）
  https://pages.nist.gov/800-63-3/sp800-63-3.html
- ニュージーランドスタンダード　「Identification Management Standards」
  https://www.digital.govt.nz/standards-and-guidance/identification-management/identification-management-standards/overview-of-the-identification-management-standards

（参考）ニュージーランドのInformation Assuranceの概要

IAレベル	要求事項(レベルごとに差分があるもののみ抜粋)
4	情報の正確性 ・RP（Relying Party、IDでログインするサイト、サービス）は、**権威ある情報源**であるか、または**権威ある情報源と連続的に同期したリンクを持つエビデンス**を選択しなければならない エビデンスの質 ・信頼できる通信チャネルを介してシステム的に識別され、アクセスされる証拠に基づいて品質を設定しなければならない コントロール ・RP は詐欺対策技術を適用しなければならない
3	情報の正確性 ・RP は、**少なくとも権威のあるソースのコピーである証拠**を選択しなければならない エビデンスの質 ・RPは、手動で特定された証拠に基づいて品質を決定しなければならず、また、 **再現するために独自の知識を必要とする物理的なセキュリティ機能**を含まなければならない コントロール **・RPは詐欺対策技術を適用すべきである**
2	情報の正確性 ・RPは、少なくとも作成時に権威あるソースのコピーを参照した証拠を選択すべき エビデンスの質 ・RP は証拠を「額面通り」に受け取らなければならない
1	情報の正確性 ・RPはエンティティを証拠として用いるべき エビデンスの質 ・RPはそのエンティティを証拠として受け入れなければならない

（参考）ニュージーランドのBinding Assuranceの概要

BAレベル	要求事項(レベルごとに差分があるもののみ抜粋)
4	エンティティと情報との関係の確立 **・RP は、バイオメトリクス要素を、知識または所有のいずれかのバインディング要素タイプで使用するか、または同等以上の保証レベルの既存の認証機関またはクレデンシャルを使用しなければならない。** 詐欺対策技術 ・RPは不正防止技術を適用しなければならない エンティティバインディングの再確認 ・認証イベントに生体認証要素が含まれていない限り、少なくとも5年に1回RPはこの管理を実施しなければならない。
3	エンティティと情報との関係の確立 ・RP は、**最低でも 2 種類の結合要素、**または保証レベルが同等以上の既存の認証機関やクレデンシャルを使用しなければならない。 詐欺対策技術 **・RP は詐欺対策技術を適用すべきである。** エンティティバインディングの再確認 ・認証イベントに生体認証要素が含まれていない限り、少なくとも5年に1回RPはこの管理を実施しなければならない。
2	エンティティと情報との関係の確立 ・RP は、**最低でも 1 種類の結合要素**を使用するか、同等以上の保証レベルの既存の 認証子またはクレデンシャルを使用しなければならない。 エンティティバインディングの再確認 ・少なくとも5年に1回行うべき
1	エンティティバインディングの再確認 ・少なくとも5年に1回行うべき

ニュージーランド規格のInformation Assurance要件を参考にした本人確認手法のInformation Assurance Level分類結果

ニュージーランド規格上の項番	1	2	3			4		
	IA3.03	IA3.03	IA3.03	IA4.02	IA4.03	IA3.03	IA4.02	IA4.03
ニュージーランド規格における Information Assurance要件	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、使用できないような登録状態（一時停止、取り消し等）の証拠があるかを確認すること	依拠当事者が、可能な限り不正行為対策技術を適用すること	依拠当事者が、各情報の検証に必要な情報アシュアランス（IA）のレベルに合った適切な証拠を選択すること	依拠当事者が、使用できないような登録状態（一時停止、取り消し等）の証拠があるかを確認すること	依拠当事者が、可能な限り不正行為対策技術を適用すること
・[MUST]　必須要件 ・[SHOULD]　推奨	依拠当事者はエンティティーを証拠として使用すべき	[SHOULD]権威ある情報源のコピーを参照した証拠	[SHOULD]権威ある情報源のコピーである証拠	[SHOULD]証拠発行者又は同等のサービス・プロバイダーに登録状態を確認	[SHOULD]不正行為対策技術を適用	[MUST]権威ある情報源である証拠、又は権威ある情報源と継続的に同期したリンクを持つ証拠	[MUST]証拠発行者又は同等のサービス・プロバイダーに登録状態を確認	[MUST]不正行為対策技術を適用
本プロジェクトで検討した補足条件（暫定） 手法					以下のいずれかを満たせば〇 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する			以下のいずれかを満たせば〇 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する
公的個人認証による署名用電子証明書＋電子署名付契約書						〇	〇	〇
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影			〇	×	〇	×	×	〇
認定認証事業者による電子証明書＋電子署名付契約書			〇	×	〇	×	×	〇
1枚限り発行される顔写真のある公的身分証のICチップ読み取り、もしくは1枚限り発行される顔写真のある公的身分証の撮影（表・裏・厚み）＋法律に基づく身元確認済のAPI連携			〇	〇	〇	×	〇	〇
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影			〇	×	〇	×	×	〇
公的身分証のリアルタイム撮影		〇	〇	×	×	×	×	×
法律に基づく身元確認のAPI連携（銀行API、携帯電話事業者API等）			×	〇	〇	×	〇	〇
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	〇	×	×	×	×	×	×	×
身分証確認なし（自己申告＋eメール、SNSログイン等）		×	×	×	×	×	×	×

Information Assurance Level の分類結果
4
3
3
3
3
2
3
1
0

［出典］ニュージーランドスタンダード　「Identification Management Standards」

ニュージーランド規格のBinding Assurance要件を参考にした本人確認手法のBinding Assurance Level分類結果

ニュージーランド規格上の項番	1	2	3		4	
		BA3.02	BA3.02	BA3.06	BA3.02	BA3.06
ニュージーランド規格における Binding Assurance要件	なし	依拠当事者が、紐づけ要素(*)を用いて、要求される紐づけのアシュアランスのレベルと整合する紐づけ方法を選択すること	依拠当事者が、紐づけ要素(*)を用いて、要求される紐づけのアシュアランスのレベルと整合する紐づけ方法を選択すること	依拠当事者が、可能な場合に詐欺対策技術を適用すること	依拠当事者が、紐づけ要素(*)を用いて、要求される紐づけのアシュアランスのレベルと整合する紐づけ方法を選択すること	依拠当事者が、可能な場合に詐欺対策技術を適用すること
・[MUST] 必須要件 ・[SHOULD] 推奨		[MUST]最低でも 1 種類の紐づけ要素を使用するか、同等以上のアシュアランスレベルの既存のオーセンティケーター又はクレデンシャルを使用	[MUST]最低でも 2 種類の紐づけ要素を使用するか、同等以上のアシュアランスレベルの既存のオーセンティケーター又はクレデンシャルを使用	[SHOULD]不正行為対策技術を適用	[MUST]バイオメトリクス要素を、知識又は保有のいずれかの紐づけ要素タイプで使用するか、又は同等以上のアシュアランスレベルの既存のオーセンティケーター又はクレデンシャルを使用	[SHOULD]不正行為対策技術を適用
本プロジェクトで検討した補足条件（暫定） 手法				以下のいずれかを満たせば〇 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する	対面で証明書を渡してる事が保証でき、それが確実に確認出来る場合（ICチップ読取り）に〇。	以下のいずれかを満たせば〇 1.認定事業者による電子署名 2.犯収法要件に準拠 3:キャリア網+暗証番号認証 / FIDO認証等を利用する
公的個人認証による署名用電子証明書＋電子署名付契約書					〇	〇
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影					〇	〇
認定認証事業者による電子証明書＋電子署名付契約書			〇	〇	×	×
1枚限り発行される顔写真のある公的身分証のICチップ読み取り、もしくは1枚限り発行される顔写真のある公的身分証の撮影（表・裏・厚み）＋法律に基づく身元確認済のAPI連携					〇	〇
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影					〇	〇
公的身分証のリアルタイム撮影		〇	×	×	×	×
法律に基づく身元確認のAPI連携（銀行API、携帯電話事業者API等）			〇	〇	×	〇
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）		〇	×	×	×	×
身分証確認なし（自己申告＋eメール、SNSログイン等）		×	×	×	×	×

＊紐づけ要素は次のいずれか。
- 公的で、容易に判断できない、かつ予測できない知識要素
- 真正であると評価するのに十分な特徴を持つ保有要素
- なりすましを検出するための適切な手段を用いたバイオメトリクス要素（例：録音、マスク、化粧、義足など）

Binding Assurance Level の分類結果
4
4
3
4
4
2
3
2
0

Digital Architecture Design Center

［出典］ニュージーランドスタンダート 「Identification Management Standards」

身元確認手法の細分化結果

手法	Information Assurance Level	Binding Assurance Level	DADC・IAL
公的個人認証による署名用電子証明書＋電子署名付契約書	4	4	**4**
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	3	4	**3**
1枚限り発行される顔写真のある公的身分証のICチップ読み取り、もしくは1枚限り発行される顔写真のある公的身分証の撮影（表・裏・厚み）＋法律に基づく身元確認済のAPI連携	3	4	
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影	3	4	
認定認証事業者による電子証明書＋電子署名付契約書	3	3	調整中 （* 39ページ参照）
法律に基づく身元確認のAPI連携（銀行API、携帯電話事業者API等）	3	3	
公的身分証のリアルタイム撮影	2	2	**2**
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	1	2	**1**
身分証確認なし（自己申告＋eメール、SNSログイン等）	0	0	**0**

今回の整理における IAL間の外形的な違い

- **・現況確認の有無**
- **・エビデンス確認対象の有無**
- **・偽造等不正対策の有無**
- **・身分証保有確認の有無**
- **・身分証の有無**

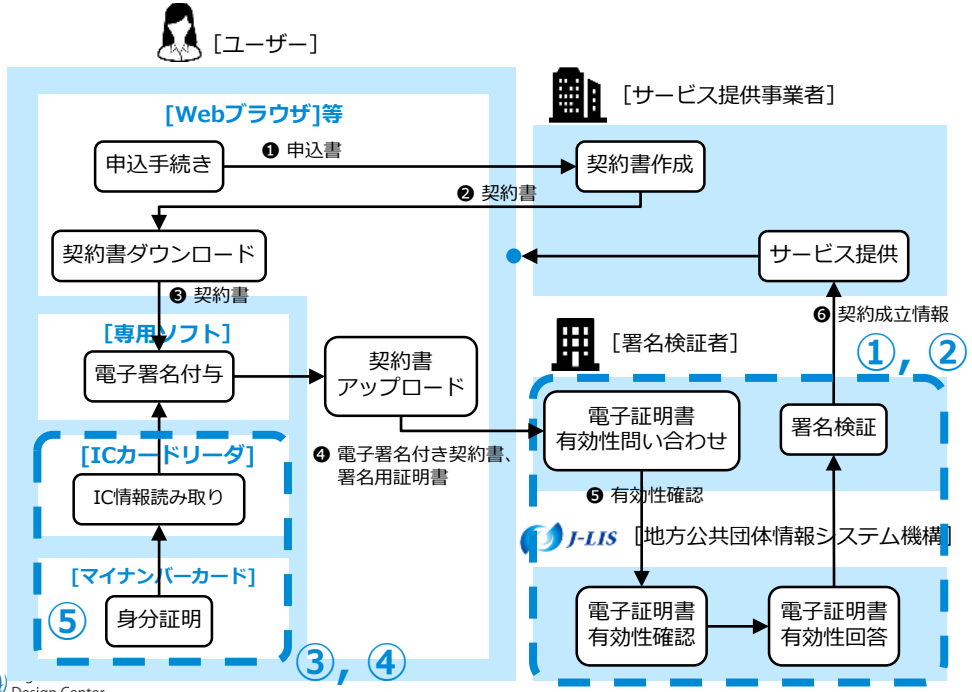
今回の整理におけるIAL間の外形的な違いについて

DADC・IALレベル４における、他のレベルとの外形的相違点を以下に例示。

（例）公的個人認証による署名用電子証明書＋電子署名付契約書の一例

<前提>
- ユーザーはサービス提供事業者へサービスの利用を申し込む段階。
- ユーザーは既にマイナンバーカードを保有している状態。

<凡例>
：機能　：プロセス、情報の流れ　（白色青字オブジェクト含む）：責任範囲



今回の整理におけるIAL間の外形的な差異項目	有/無	有無の理由等、備考
① 現況確認	有	総務省認定事業者経由でJ-LISへ電子証明書の有効性を確認。
② エビデンス確認対象	有	総務省認定事業者経由でJ-LISへ電子証明書の有効性を確認。
③ 偽造不正対策	有	マイナンバーカードのICチップに耐タンパ性あり。
④ 身分証保有確認	有	電子証明書の利用に際して、マイナンバーカードをICカードリーダーで読み取り、暗証番号を入力する必要あり。
⑤ 身分証	有	マイナンバーカードを使用。

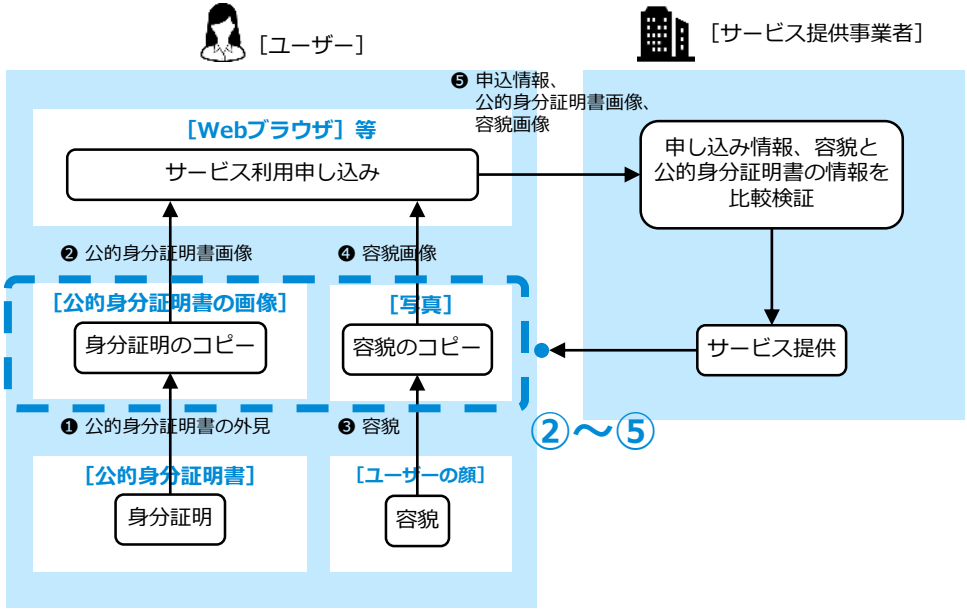
今回の整理におけるIAL間の外形的な違いについて

DADC・IALレベル３における、他のレベルとの外形的差異を以下に例示。

（例）顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影

<前提>
- ユーザーがサービス提供事業者へサービスの利用を申請するフェーズ。
- ユーザーは既に公的身分証明書を保有。

<凡例>
：機能　：プロセス、情報の流れ　（白色青字オブジェクト含む）：責任範囲



今回の整理におけるIAL間の外形的な差異項目	有/無	有無の理由等、備考
① 現況確認	無	
② エビデンス確認対象	有	顔写真と容貌画像を比較検証することで、公的身分証とユーザーの紐づけを確認。
③ 偽造不正対策	有	容貌確認、公的身分証の表裏、厚み確認等、犯収法要件に準拠し対策。
④ 身分証保有確認	有	公的身分証の表裏、厚み確認により、保有を確認。
⑤ 身分証	有	公的身分証のコピーで確認。

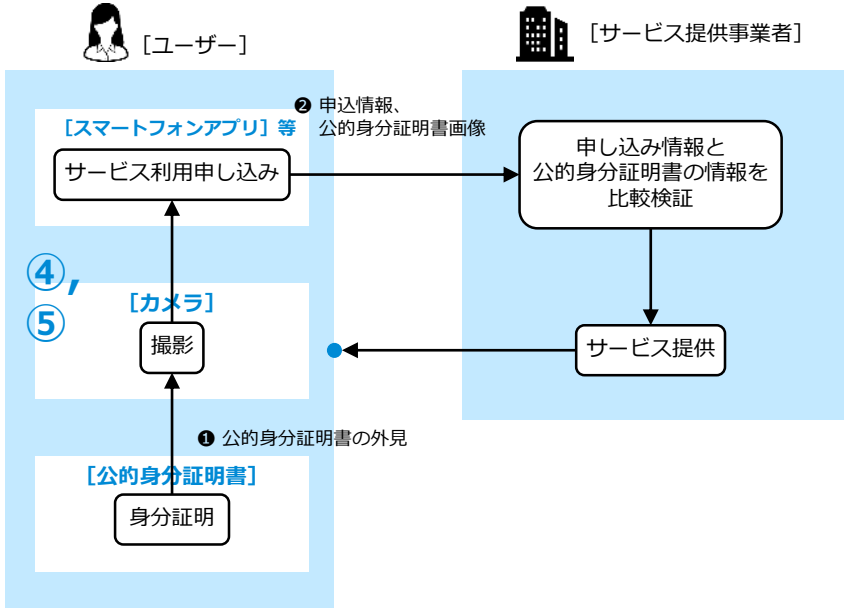
今回の整理におけるIAL間の外形的な違いについて

DADC・IALレベル２における、他のレベルとの外形的差異を以下に例示。

（例）公的身分証のリアルタイム撮影

<前提>
- ユーザーがサービス提供事業者へサービスの利用を申請するフェーズ。
- ユーザーは既に公的身分証明書を保有。

<凡例>
：機能　：プロセス、情報の流れ　（白色青字オブジェクト含む）：責任範囲



今回の整理におけるIAL間の外形的な差異項目	有/無	有無の理由等、備考
① 現況確認	無	
② エビデンス確認対象	無	
③ 偽造不正対策	無＊	＊ 罫線位置等、身分証の外見的特徴を検査することにより、対策を実施している場合もあり。
④ 身分証保有確認	有	リアルタイム撮影により、ユーザーが今保有していることを確認。
⑤ 身分証	有	公的身分証の画像による確認。

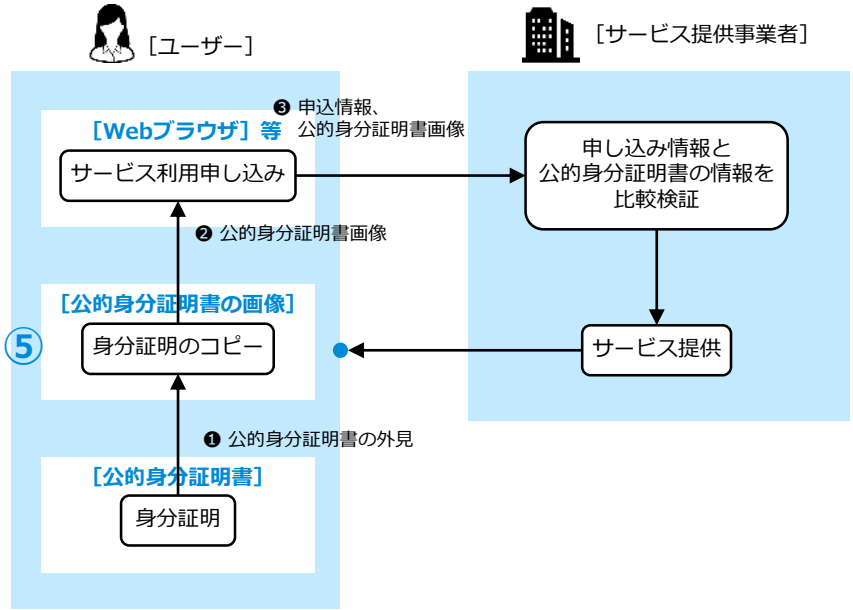
今回の整理におけるIAL間の外形的な違いについて

DADC・IALレベル１における、他のレベルとの外形的差異を以下に例示。

（例）公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）

<前提>
- ユーザーがサービス提供事業者へサービスの利用を申請するフェーズ。
- ユーザーは既に公的身分証明書を保有。

<凡例>
：機能　：プロセス、情報の流れ　（白色青字オブジェクト含む）：責任範囲



今回の整理におけるIAL間の外形的な差異項目	有/無	有無の理由等、備考
① 現況確認	無	
② エビデンス確認対象	無	
③ 偽造不正対策	無＊	＊ 罫線位置等、身分証の外見的特徴を検査することにより、対策を実施している場合もあり。
④ 身分証保有確認	無	
⑤ 身分証	有	公的身分証のコピーによる確認。

DADC・IAL策定作業の成果（その１）

手法	DADC・IAL	犯収法等 根拠になる 規定の有無	行政手続 ガイドライン のIAL
公的個人認証による署名用電子証明書＋電子署名付契約書	4	あり	3
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	③	あり	
1枚限り発行される顔写真のある公的身分証のICチップ読み取り、もしくは1枚限り発行される顔写真のある公的身分証の撮影（表・裏・厚み）＋ 法律に基づく身元確認済のAPI連携	3	あり	
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影		あり	2
認定認証事業者による電子証明書 ＋電子署名付契約書		あり	＊ 個別に確認が必要
法律に基づく身元確認のAPI連携 （銀行API、携帯電話事業者API等）		なし	
公的身分証のリアルタイム撮影	2	なし	
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	1	なし	
身分証確認なし（自己申告＋eメール、SNSログイン等）	0		1

①

Binding Assurance の概念を取り入れて Identity Assurance Levelを再整理

②

犯収法等法令に同列で**規定されている身元確認手法であってもIALが異なる**ことを確認、明示

③

「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」において**不明確であったIAL2を細分化**

DADC・IAL策定作業の成果（その２）

手法	DADC・IAL	犯収法等根拠になる規定の有無	行政手続ガイドラインのIAL
公的個人認証による署名用電子証明書＋電子署名付契約書	4	あり	3
顔写真のある公的身分証のICチップ読み取り＋容貌の撮影	3	あり	2 ＊ 個別に確認が必要
1枚限り発行される顔写真のある公的身分証のICチップ読み取り、もしくは1枚限り発行される顔写真のある公的身分証の撮影（表・裏・厚み）＋法律に基づく身元確認済のAPI連携		あり	
顔写真のある公的身分証の撮影（表・裏・厚み）＋容貌の撮影		あり	
認定認証事業者による電子証明書＋電子署名付契約書		あり	
法律に基づく身元確認のAPI連携（銀行API、携帯電話事業者API等）	④	なし	
公的身分証のリアルタイム撮影	2	なし	
公的身分証のアップロード（1点で情報が不足する場合、2点（例）保険証等＋公共料金）	1	なし	
身分証確認なし（自己申告＋eメール、SNSログイン等）	0		1

④

法令に定めがない手法も、公的身分証が用いられ、不正行為対策、詐欺対策等の技術要件が確保されれば、**犯収法等に定められた手法とDADC・IALが同じになる**

技術要件が確保されたAPI連携手法の導入を促進

＊ 発行元の真正性、本人性の確認等について今後検討する必要あり

法令に定めのない手法の多様化とIALの明確化（例：券面事項入力補助AP）

デジタル庁が提供する「新型コロナワクチン接種証明アプリ」は、これまであまり利用されることのなかった身元確認手法（マイナンバーカードの「券面事項入力補助AP」）を採用している。

この手法は法令に定めはないものの、DADC・IAL3に相当し、犯収法等に定める手法と同じレベルであることが確認できる。

新型コロナワクチン接種証明アプリ

券面事項入力補助AP

×

4桁PIN入力による ICチップ読み取り

【概要】
- 法令等に定めのない手法
- 暗証番号等の入力によりマイナンバーカードのICチップの情報のうち、基本4情報や個人番号を読み取る（＊）
- 犯収法等の手法と同等のDADC・IAL３に相当

＊ 利用可能な情報は以下の3種存在し、それぞれに応じたアクセスコントールをしている。
尚、個人番号の取り扱う①・②は、個人番号の利用ができる事業者のみが行うことができる。

	利用可能な情報	アクセスコントロール
①	個人番号と基本4情報とその電子署名データ	券面事項入力補助用暗証番号(数字4桁)
②	個人番号とその電子署名データ	照合番号A(数字12桁：個人番号)
③	基本4情報とその電子署名データ	照合番号B(数字14桁：マイナンバーカード裏面に記載の生年月日6桁、有効期限西暦年、セキュリティコード4桁)

DADC・IALの期待効果

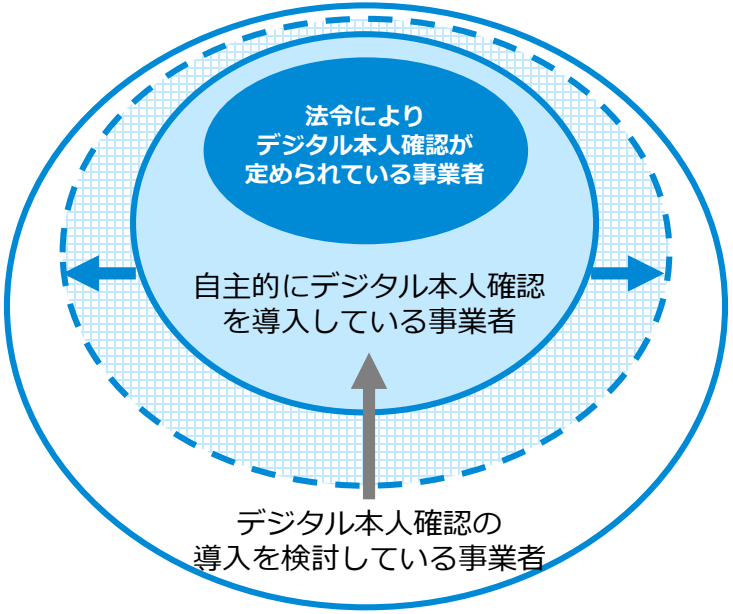
法令に定めがない手法であっても、公的身分証が用いられ、不正行為対策・詐欺対策等の技術要件が確保された手法であれば、犯収法等に定められた手法と同等の保証レベルと見做せることが明確になった。
民間事業者、特に自主的に本人確認を導入する事業者にとって、レベルが可視化され、選択肢が増えることで、サービスに応じた手法を安心して選択しやすくなり、デジタル本人確認の導入が広がる。

自主的に本人確認を導入する事業者の課題

- ユーザーやサービスに応じた手法を利用したいが一定の保証レベルは確保したい
- 法令に定めのない手法の保証レベルが分からないので利用を控えてしまう

DADC・IALにより解決

デジタル本人確認の導入拡大



＊ 円の大きさは事業者数の規模を表現

今後の検討課題

- 細分化後のIALに本人確認手法をマッピングすると、DADC・IALのLv3に集中した（30ページ参照）更に外部有識者等から意見を収集した上で、他の観点の導入等、細分化の要否、検討を継続する。
- 外部有識者との意見交換の中で、手法からのアプローチではエビデンス（身分証等）の真贋判定の強固さが観点の中心になるが、その真贋判定の前提条件として、エビデンスに対する支配権、管理権限を被検証者が実際に持っているかどうかの観点が必要である旨の指摘を受け、ガイドラインではこの内容を補記することとした。今後、ガイドラインとしてどのように記載するか、説明文章等の具体的な検討が必要。

＜記載案の一例＞
　想定し得る脅威を例示し、ニュージーランド規格のBinding Assurance（紐づけのプロセスの堅牢性）に基づく検証でリスク対策できることと、できないこと＝別途対策を行わないといけないことを示す。

Digital Architecture
Design Center

目次

ヒアリング概要

「サービスに応じたデジタル本人確認ガイドライン」策定の検討に資するため、民間事業者に対して、
事業者が抱えているリスク、実施している本人確認の具体的手法、当該手法を選択した理由や方法、
その他本人確認に関する課題等の実態を聴き取る、ヒアリング調査を実施した。

ヒアリング調査の概要

目的	● 各事業者が抱えているリスク、実施している本人確認の具体的手法、当該手法を選択した理由や方法、その他本人確認に関する課題等の実態を収集する ● ガイドライン策定等に関するビジネス現場からの意見等を収集する
方法	● ビデオ会議システムによるリモート調査 ● 1社当たり約60分実施
期間	● 2021年11月～2022年1月
対象	● 全14事業者・団体等を対象に実施 ● 法令等で本人確認が求められていない業種や、サービスの提供者・利用者の双方に対して本人確認が行われる可能性のあるシェアリングエコノミー事業者を中心に、業界団体の紹介等に基づき選定 ● その他、本ラボでの検討に資する技術標準化団体等にも、聴き取りや資料照会を実施した
質問事項	● ビジネスの具体的内容・サービスモデル ● 本人確認手法や選択理由 ● 本人確認に関わるリスク ● リスクに応じた本人確認手法の選択について ● 本人確認に関わる課題 ● その他本検討へのご意見やご要望

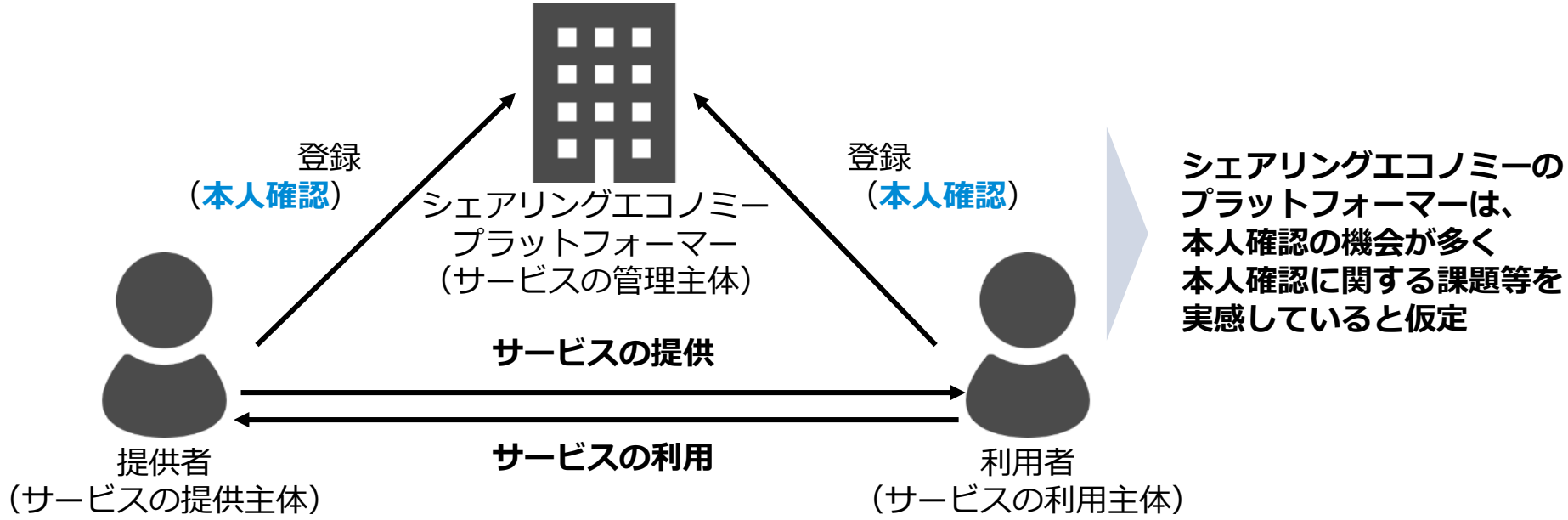
（参考）ヒアリング対象一覧

#	ヒアリング対象事業者・団体	事業の対象等	実施日時	ヒアリング内容
1	業界団体A	個人向け・個人間プラットフォーム	2021/11/12	業界としてのオンライン本人確認に関する現状や課題等
2	個人間プラットフォーム事業者１	シェアリング・オフライン	2021/11/15	本人確認の実践及び本人確認で対応しているリスク等
3	個人間プラットフォーム事業者２	シェアリング・オフライン	2021/11/16	本人確認の実践及び本人確認で対応しているリスク等
4	個人間プラットフォーム事業者３	シェアリング・オフライン	2021/11/19	本人確認の実践及び本人確認で対応しているリスク等
5	業界団体B	決済関連	2021/11/19	業界としてのオンライン本人確認に関する課題等
6	個人間プラットフォーム事業者４	シェアリング・オフライン、一部オンライン	2021/11/30	本人確認の実践及び本人確認で対応しているリスク等
7	技術標準化団体C	—	2022/01/07	IAL細分化に関する考え方の確認等
8	流通事業者（個人向け、リアル店舗中心）	個人向け・オフライン中心	2022/01/07	本人確認の実践及び本人確認で対応しているリスク等
9	フィンテック事業者１	法人向け・オンライン中心	2022/01/11	取引先のオンライン本人確認に関する現状や課題等
10	フィンテック事業者２	法人向け	2022/01/12	取引先のオンライン本人確認に関する現状や課題等
11	フィンテック事業者３	個人向け	2022/01/14	本人確認の実践及び本人確認で対応しているリスク等
12	フィンテック事業者４	個人向け・オンラインのみ	2022/01/25	本人確認の実践及び本人確認で対応しているリスク等
13	技術標準化団体D	—	2022/01/27	本人確認手法に関連した驚異事例等の資料提供依頼
14	業界団体E	個人向け・オンライン	2022/01/30	業界としてのオンライン本人確認に関する課題等

（参考）シェアリングエコノミーのビジネスモデル

シェアリングエコノミーでは、プラットフォーマーが仲介役となり、提供者が利用者へ直接サービスを提供している。そのため、シェアリングエコノミーのプラットフォーマーは、サービスの提供主体と利用主体の双方に対して本人確認を行う可能性があり、本人確認に関する課題等を実感していると仮定し、調査対象とした。

シェアリングエコノミーのビジネスモデル (イメージ)



出所：総務省 (2015)「平成27年版　情報通信白書」等を参考により作成

ヒアリング結果のサマリ

	項目	ヒアリング結果概要
本人確認	本人確認の実施理由	法令で求められているため。また、リスクの防止・予防のためという意見が中心。
	本人確認手法の選択方法	犯収法の手法を選択するほか、他社事例やeKYC事業者からの提案を参考に決定。
	本人確認手法の選択時に重視した点	利用者の確認、偽造身分証の排除、コスト、ユーザーの負担、リアルタイムでの確認等。
	本人確認の推進施策と導入後の状況	キャンペーンや検索順位でのインセンティブを設定。また、マイナスの影響は無かった。
	本人確認手法の選択に係る課題	①手法を選択するための指針の不在に加え、②身分証等に固有の課題等が存在。
	本人確認に係る課題	①適用の柔軟性、②ユーザーの理解 、③本人確認を行わないニーズ、④個人情報の取扱い等。
リスク	リスクの事例	ヒト、モノ、カネ、情報に加え、その他複数のリスク事例を収集した。
	リスクへの対応	ヒトに関するリスクへは本人確認を中心、その他のリスクに対しては保険を含む複数手法で対応。
	リスクに応じた本人確認手法の選択	柔軟な手法選択及びリスク評価が必要。ただし、特にリスク評価に困難さが存在。
	リスクに応じた本人確認の事例	実態としては、必ずしもリスクに応じたIALレベルにはなっていない。
	リスクに応じた本人確認に係る課題	対応するリスクの特定、評価及びユーザーの負担になりすぎない対応方法の設定等が課題。
その他	ラボ活動に対するご意見	各主体が役割分担をしながら、統一的に議論を進めていく必要性についての指摘等があった。
	ガイドラインの位置づけ・要望	指針が設定されることへの期待と、その指針が強制されることに対する不安の両面の意見があった。
	マイナンバーカードについて	マイナンバーカードの積極活用のためには、普及率及びユーザの理解醸成が課題。
	その他課題・要望等	柔軟な制度検討、依拠の推進、不正事例のタイムリーな発信等の意見・要望等が存在。

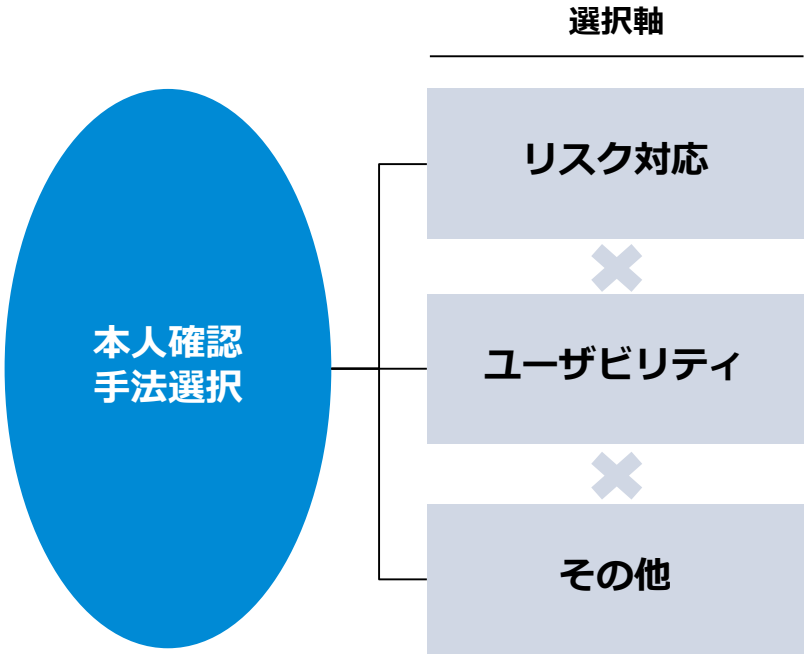
Digital Architecture Design Center

目次

事業者は、どのように本人確認手法を選択しているか

ヒアリングから各事業者は、
①リスク対応と②ユーザビリティを重視した上で、コストやeKYC提供事業者の信頼度も踏まえ、
本人確認手法を選択していることが分かった。

本人確認手法の選択軸



ヒアリングでの事業者からの主なコメント

- オンラインで完結できる手法を選択した
- 依頼者が起こすトラブルを回避したい
- 偽造身分証を防ぎたい

- セキュリティを強化すると利用者のハードルが上がるが、サービスが使われないと意味がない。本人確認を強固に行うことで、利用者のハードルがどれだけ上がるかのバランスで手法を決めた

- コストとのバランスを見ながら（身分証の偽造を検知するという）目的を達成できる手法を選択した
- 当社の求める目的に過不足ない適切な手法を提示してくれた(eKYCサービス事業者の信頼度)

インキュベーションラボにおける検討事項

「リスクに応じた本人確認手法を選択できる」という目的を踏まえ、まずはリスクに関して、事業者が捉えているリスク事例や当該リスクへの対応等について調査・整理した。

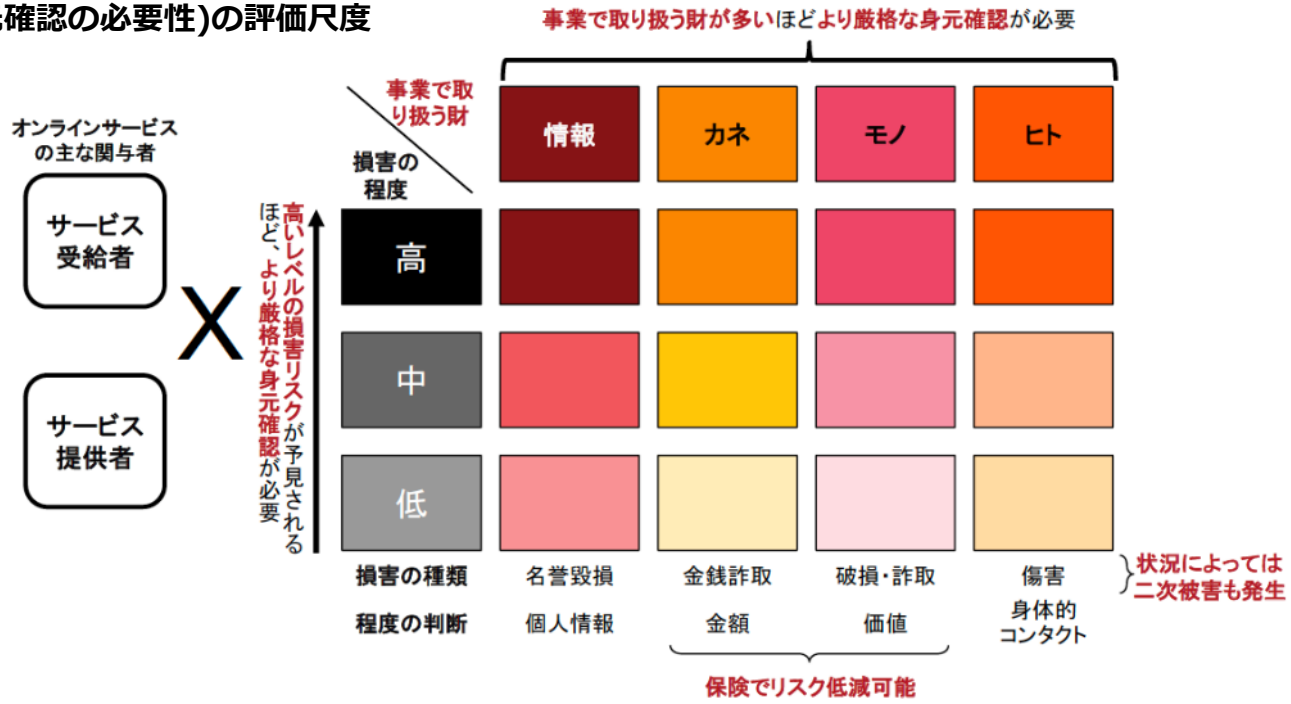
検討事項の整理

本人確認手法の選択軸	論点	検討の方向性
リスク対応	● 事業者がどのようなリスクを抱えて、本人確認で対応しているか ● 本人確認で対応できている点、できていない点 等	**本検討活動の対象**
ユーザビリティ	● ユーザにとっての負荷をどう整理するか ● 既存の手法をユーザビリティの視点でどう整理するか	ガイドライン策定に当たって、今後議論すべき論点
その他	● コストについては、各eKYC事業者の競争領域で、ガイドライン等では対象外 ● eKYC事業者の信頼度については、認証制度等も考えられるが、本ラボのスコープ外と思料	コストは、各事業者判断。事業者の認証等は将来的な課題

過去の検討会におけるリスクの整理

経済産業省「オンラインサービスにおける身元確認に関する研究会」では、リスク評価の際には、事業で扱う財とその内容や関与者、保険/補償の有無、二次被害の可能性、等を踏まえた被害程度を見積る必要性が指摘された。

事業リスク(身元確認の必要性)の評価尺度

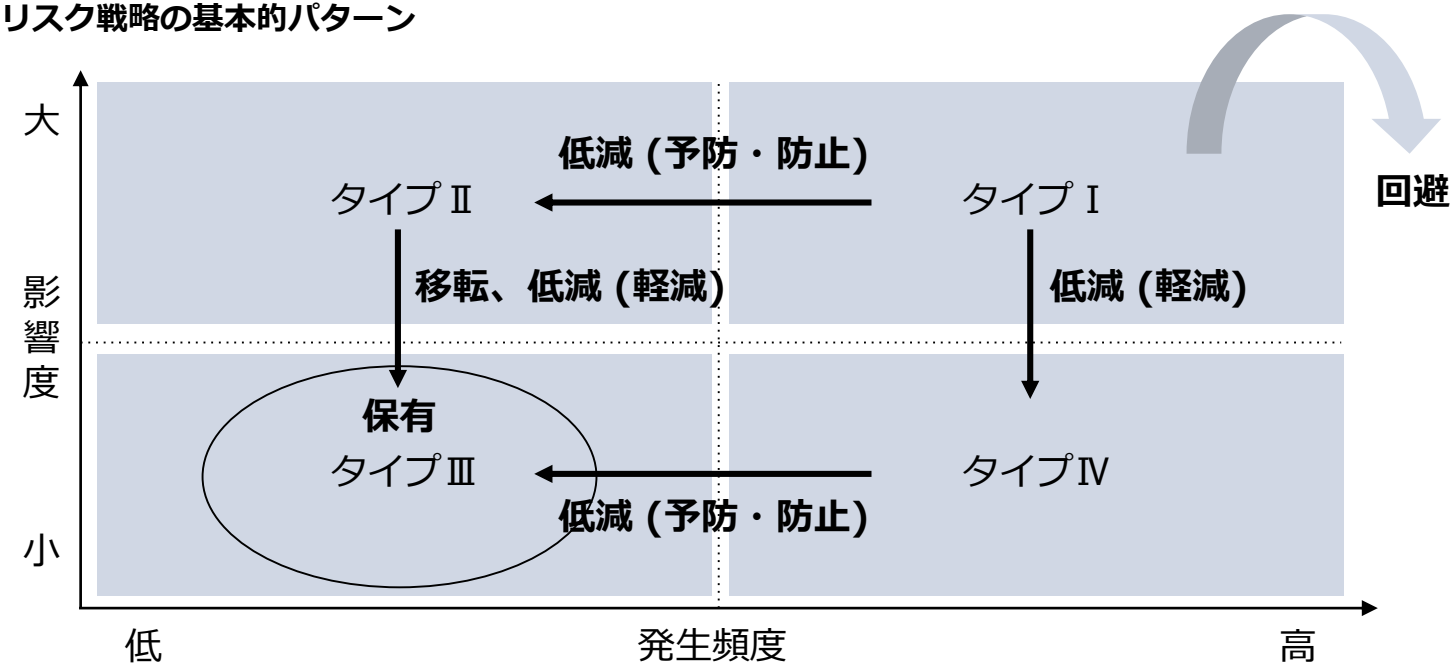


出所：経済産業省 (2020)「オンラインサービスにおける身元確認手法の整理に関する検討報告書」より

（参考）リスクマネジメントにおけるリスク評価の基本的考え方

一般的にリスクマネジメントでは、各リスクを影響度と発生頻度のリスクマップ上にプロットし、各社が優先順位をつけて適切なリスク戦略を選択している。「リスクに応じた本人確認手法の選択」をガイドライン化するためには、リスク評価・リスク戦略等の手法を参考に「リスクの標準化」が課題となる。

リスク戦略の基本的パターン



リスク戦略の例

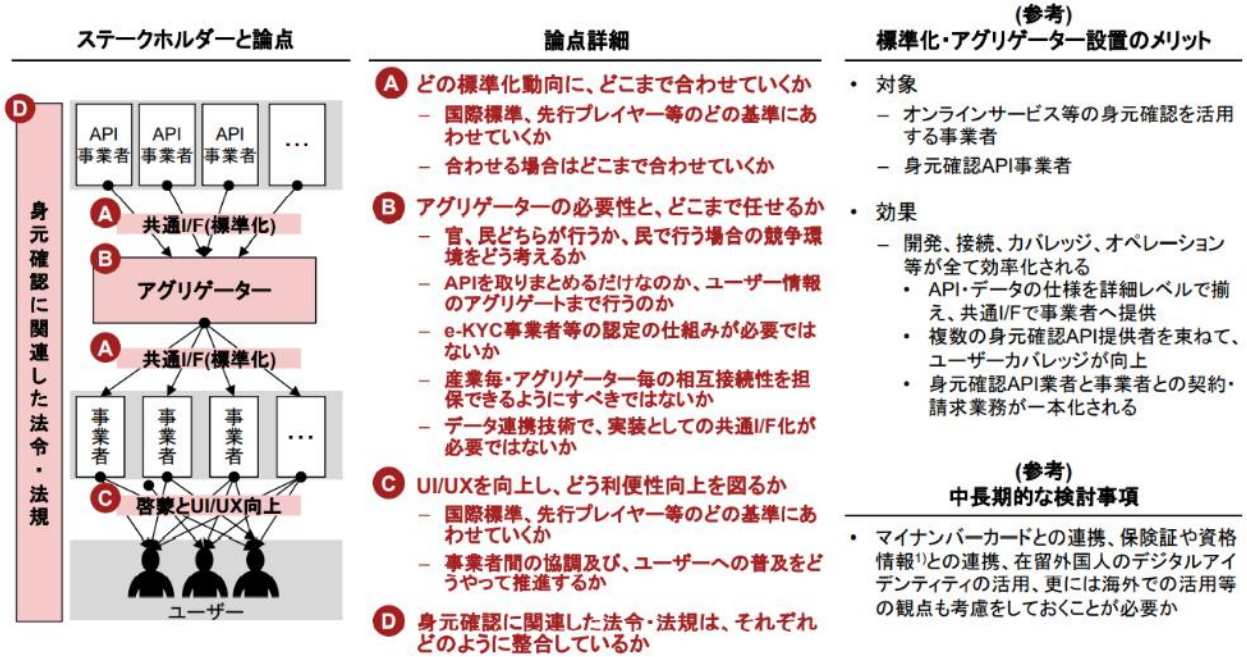
- 移転:
  損害保険
- 低減(予防・防止):
  本人確認
- 低減(軽減):
  サービスごとに立案
- 回避:
  事業撤退

出所：経済産業省 (2005)「先進企業から学ぶ事業リスクマネジメント実践テキスト－ 企業価値の向上を目指して －」より

その他、リスクに応じた本人確認手法選択に係る事業者の懸念点

本人確認を実施することによるUXの悪化を懸念する意見も得られた。
リスク対策とユーザビリティ確保を両立するためには、アグリゲーター等が事業者が抱えるリスクを考慮し、最適な本人確認手法を提案する仕組み等が考えられる。

（参考）「オンラインサービスにおける身元確認に関する研究会」で提示されたアグリゲーターを設置する案

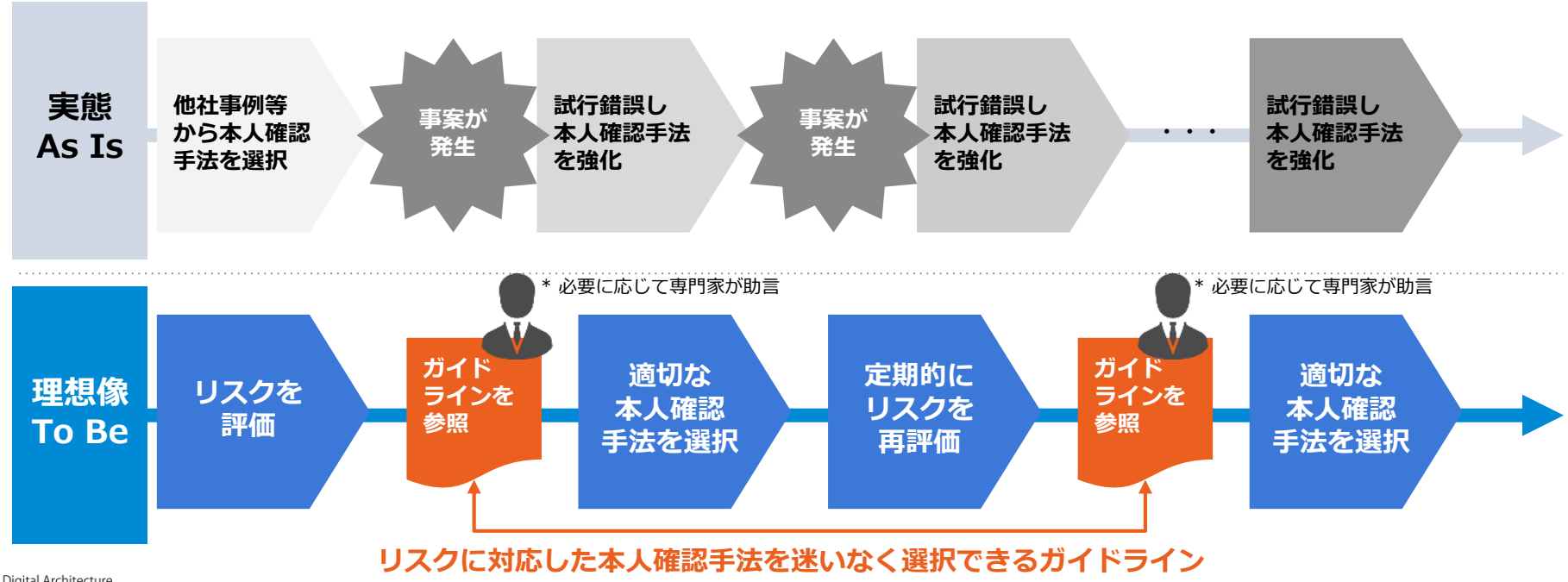


出所：経済産業省 (2020)「オンラインサービスにおける身元確認手法の整理に関する検討報告書」より

ヒアリングから得られた示唆

事業者は自社が抱えているリスクに対応する手段の1つに本人確認を位置づけており、事案の発生等を受けて試行錯誤的に本人確認を強化している実態が明らかになった。理想像としては、試行錯誤をせずとも、各事業者のリスク評価結果に対応した本人確認手法を選択できるガイドラインの策定が必要である。

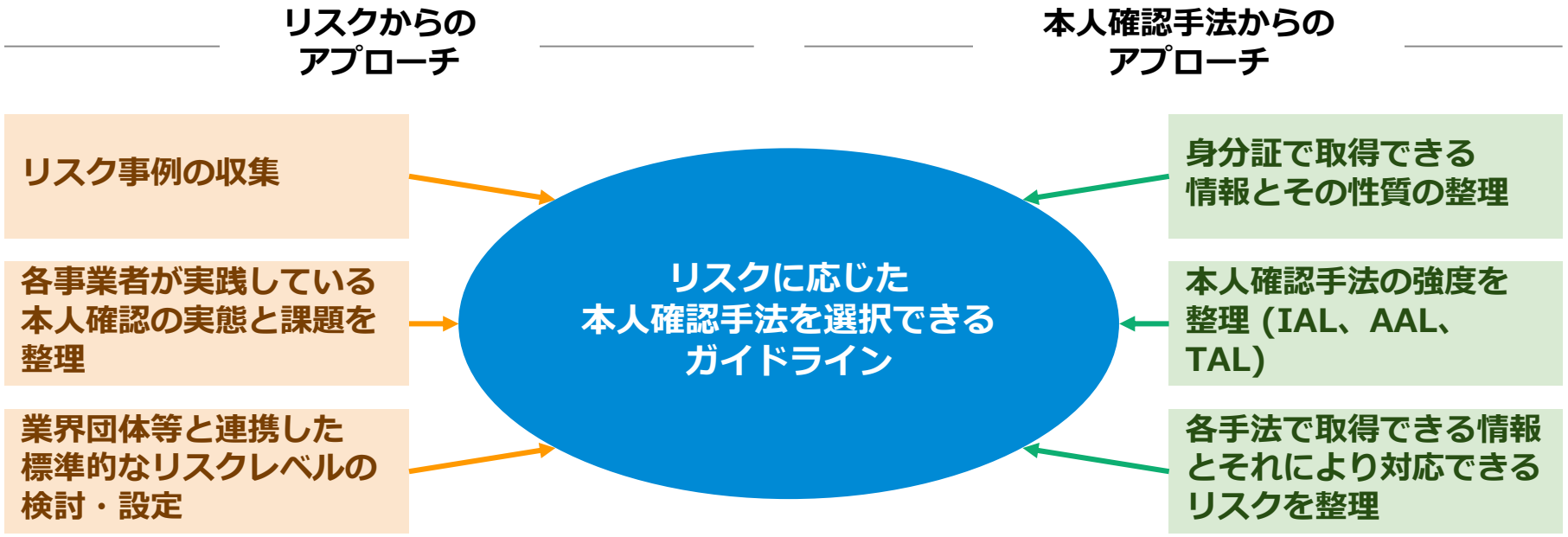
リスクに応じた本人確認手法選択の実態と理想像（イメージ）



ヒアリングから導出される今後の課題

本活動で整理した事例は限られたものであり、より広範なリスクおよび本人確認の実践例の収集が必要。また、ガイドラインの策定には、事例調査等を踏まえたリスク側からの検討に加え、本人確認手法や身分証等の特徴から導き出した、「対応できるリスク」等を踏まえた検討が必要と考えられる。

リスクに応じた本人確認手法を選択できるガイドラインの検討イメージ



Digital Architecture Design Center

目次

海外動向調査について

- 実施内容
  - 主に本人確認に利用されるデジタルIDに対しての取り組み状況を確認。
  - Webページを中心に調査。

- 調査結果
  - スウェーデン、シンガポール、英国（グレートブリテン及び北アイルランド連合王国）、エストニア、インドの5ヵ国を対象に調査。

件名	内容	示唆を得た調査
UXの向上を契機とした普及	デジタルIDがスマートフォンに搭載され物理的なカードを使わずに本人確認が行えることでユーザーの利便性が高まり、一気にデジタルID、およびデジタル本人確認が普及。 **デジタル本人確認の普及には、UXへの配慮が重要**であり、ガイドラインにおいても安全性やコストだけではなく、UXへの考慮が必要であることを、事業者に提示する必要がある。	• スウェーデン • シンガポール • エストニア
デジタルIDや本人確認サービスの一極集中への指摘	1. 単一IDプロバイダーへの過度の依存がリスクになり得る。 2. イノベーションや品質、価格面での競争が不在。 3. 移民や銀行口座のない個人などが排除。 ガイドラインは**手法を限定せず、多様な手法を許容しつつ、分類できるものであるべき**。	• 英国 • スウェーデン • インド
国民の了解と普及	厳格に本人確認できる手段として個人識別番号制度や共通認証プラットフォームが議論され、導入が進められたものの、国民から費用対効果への疑問や、プライバシー侵害等の批判を受け、普及の阻害要因となったケースもあった。英国では普及が進まず、代替となる新たなデジタルIDの検討が進んでいる。インドでは最高裁にて個人識別番号制度が違憲判定を受けた後、制度改正がなされた。一方、スウェーデンでは早くから番号制度が運用されており、センシティブと考えられている個人情報の範囲認識も狭く、デジタルID等への抵抗感は低い。 **デジタル本人確認の普及には、日本の国民性や状況を踏まえ、ユーザーの理解醸成に働きかけることが必要。**	• 英国 • インド • スウェーデン

- 今後の課題

時間的な制約もあり、調査方法や調査範囲が限られた。デジタルIDに対しての取り組みに限らないデジタル本人確認手法のアシュアランスレベルや導入理由等について、広範かつ詳細、特にフォーカスした調査が必要。海外動向調査によって得られた情報から、グローバルにも通用するデジタル本人確認ガイドラインの要件を明らかにする。

各国の取り組みに関する主な情報

- スウェーデン

国の情報 **(外務省基礎データ)**	• 人口：約1,022万人（2018年11月，スウェーデン統計庁） • 面積：約45万平方キロメートル（日本の約1.2倍）		
名称	Bank ID	**取り組みの主体**	民間（銀行７行のコンソーシアム）
概要	• 口座開設時に付与。IDはパーソナルナンバー（日本のマイナンバーに相当）と紐づく。 • 2004年、電子政府のオンライン申告や申請手続きに使用するデジタルIDに選定される。パーソナルナンバー（日本のマイナンバーに相当）に紐付けられており、オンラインで各種申請や手続きを行う際の本人認証手段として、Bank IDが利用されている。 • 2009年、国税庁がBankID利用者の優遇税制を設け利用拡大。BankIDによる電子署名には、法的拘束力がある。		
利用状況	• 登録者数：820万人（2019年）人口普及率80%以上。 • 対応可能なサービス：公共サービス：確定申告、各種行政手続、病院関連の手続き等。民間サービス：銀行取引、決済サービス、電子商取引、ポイントサービス等。 • BankIDの電子署名は、eIDASのルールを遵守する電子署名法に基づく法的効力のある署名。		
普及状況の背景	• 2010年にモバイルBank IDが導入され利便性が高まり、普及。 • 2012年にはモバイルP2P決済サービス「スウィッシュ(Swish)」の認証手段にBank IDが使われたことで、一気に利用が広がる。 • パーソナルナンバーは1947年に開始しており、元々ナンバーを使う機会が多く、国民の抵抗感が低い。 • 高い透明性が確保されており、国民の国への信頼度も高い。公的機関における個人情報の取り扱いの適正性については、独立機関が監督。希望者に対しては公的機関の保有する自己に関する情報を毎年提供し、官庁間や官から民への情報提供ルールが法令で規定されているなど、透明性の高い仕組みが構築されている。 • 国民の プライバシー意識として、センシティブと捉える情報の対象範囲が狭い。収入や納税額もオープン。		
備考	—		

各国の取り組みに関する主な情報

- シンガポール

国の情報 **(外務省基礎データ)**	• 人口：約569万人（うちシンガポール人・永住者は404万人）（2020年） • 面積：約720平方キロメートル（東京23区と同程度）		
名称	National Digital Identity（NDI：国家デジタル認証）	**取り組みの主体**	政府
概要	• 国が主導してNDIと呼ぶ官民共通のデジタルIDスキームの開発・普及を推進。 • NDIは、識別子となる個人登録番号（NRIC番号）と既存の公的認証システム「SingPass」、および個人情報の登録・利用の一元化サービス「MyInfo」を基盤とし、市民が単一のデジタルIDで官民のサービスを利用できる共通認証プラットフォームの構築を目指すプロジェクト。		
利用状況	• SingPass/My Infoという既存のサービスは、70の政府機関が提供する160のデジタルサービスの認証基盤として活用されている。今後は民間企業も個人認証のためにNDIプラットフォームを利用できるようになる予定。 • SingPassに実装されたクラウドベースの顔認証は、生体認証スキャンによって得られたユーザーの顔データを政府に保管されたデータベースと照合することで、本人確認を行う。政府機関だけでなく、銀行・保険などの民間企業に対しても開放しており、インターネットバンクの新規利用申し込みに必要な本人確認手続きにも利用されている。		
普及状況の背景	• 2018年にスマートフォンの生体認証を利用するSingPass Mobileが始まり、2019年には公的身分証明書（NRICカード）を見せなくても本人確認と必要な個人情報を提供可能とするSG Verifyが導入された。 • 企業は、独自のインフラやシステムを構築しなくても、政府が提供するNDIの共通APIや各種ツールを使って認証基盤を導入することが可能となり、コスト削減や安全性の強化に繋がる。		
備考	• NDIはシンガポールのスマートネイション構想の下、進められている。スマートネイション構想は、日本が推進するSociety5.0との類似点が多く、先行事例として位置づけられる。		

各国の取り組みに関する主な情報

- 英国（グレートブリテン及び北アイルランド連合王国）

国の情報 **(外務省基礎データ)**	• 人口：6,708万人（2020年） • 面積：24.3万平方キロメートル（日本の約3分の2）		
名称	GOV.UK Verify	**取り組みの主体**	政府
概要	• 2016年に公共サービスの共通認証プラットフォーム「GOV.UK Verify」（以下、Verify）が導入された。 • オンラインで公共サービスを利用するにあたり、政府の認定を受けた複数のIDプロバイダーのなかから、利用者自身が使用する認証サービスを選択する仕組み		
利用状況	• 当初の計画通りに普及が進んでいない。		
普及状況の背景	• 普及が進んでいない理由として、①UXの考慮が不十分である、②関係する省庁が必ずしも協力的ではない、③民間サービスプロバイダーの求める要件を満たすものではないこと等が指摘されている。 • 政府は、2019年に省庁横断的にデジタルIDを推進する組織を設置し、Verifyに代わる新たなデジタルIDの在り方を検討している。		
備考	• 識別子となる統一的な国民番号がないことが課題として指摘されている。		

各国の取り組みに関する主な情報

- エストニア

国の情報 **(外務省基礎データ)**	• 人口：約133万人（2021年） • 面積：4.5万平方キロメートル（日本の約9分の1）		
名称	Mobile-ID（SIMカード）、Smart-ID（アプリ）	**取り組みの主体**	政府
概要	• Mobile-IDは身分証明書法で本人確認手段として定められているモバイル端末を利用するSIMカード。SIM契約時、およびMobile-ID証明書アクティベーション時に、対面による本人確認が必要。 • Smart-IDはモバイル端末で利用するアプリ。初回登録時にe-IDカードを認証（生体認証、NFC認証）して紐付けることで、公的身分証による本人性を担保する。		
利用状況	• 2002年エストニア政府はエストニア版マイナンバーカード「e-IDカード」を国民に配布し、従来は役所に訪問しなければ不可能だった本人確認をオンライン上で可能にした。 • 現在エストニアでは99%の行政申請がオンラインで可能（Mobile-ID利用の場合。Smart-IDでは一部）であり、連携したサービスも2,700を超える。結婚、離婚、不動産の手続き以外は全てオンラインで可能。		
普及状況の背景	• 普及率は、Mobile-IDで19%、Smart-IDで42%（2020年時点） • e-IDカードで認証を行うためには、カードリーダーを持ち歩き、物理的なカードで認証させなくてはならず、導入当初は利用者からの不満も多かった。		
備考	• 日本、および今回の調査対象国と比較し、人口や面積が小規模である。		

各国の取り組みに関する主な情報

- インド

国の情報 **(外務省基礎データ)**	• 人口：13億8,000万人（2020年世銀資料） • 面積：328万7,469平方キロメートル（インド政府資料：パキスタン、中国との係争地を含む）（2011年国勢調査）		
名称	Aadhaar（アドハー）、India Stack	**取り組みの主体**	政府
概要	• Aadhaarは、インドの固有識別番号庁（UIDAI）によって登録が進められている国民識別番号制度であり、国民の名前や住所、生体情報（指紋、顔、および虹彩）を収集して管理する。 • India Stackは、そのAadhaarをベースに開発された各種オープンAPIの集合体。eKYCの機能「Aadhaar eKYC」を含む。行政機関や民間企業が利用し、自組織のアプリケーションに組み込むことができる。 • Aadhaarをベースとする機能は複数の中央政府組織や公的組織が開発・管轄し、 India Stackを構成するオープ ンAPIも別々の組織によって所有されているが、開発には、専門家のボランティアからなる民間シンクタンク、iSPIRT（アイスピリット）が深く関与している。		
利用状況	• 既に12.3億人以上が登録し、公共福祉サービスが効率的に支払われるようになり、不正行為も激減した。 • India Stackを最も頻繁に活用する業種は、銀行および通信キャリア。主にAadhaar eKYCを活用。紙書類による手続きに比べ、大きく効率化され、大幅なコストダウンにつながっている。		
普及状況の背景	• Aadhaarの普及割合は銀行口座保有者の割合と比例して増加。口座を保有できることが1つの要因と考えられる。2008年時点では人口の4%程度しかIDを持っていなかったが、2018年には10億人以上がIDを保有するようになった。 • ボランタリーなファイナンシャル／ソーシャルインクルージョン実現に貢献したと高く評価される向きがある一方、実際は社会保障を得るための必須要件にすることで、半ば強制的に進められたという指摘もある。 • Asdhaarの導入以来、プライバシー侵害等の批判に晒されている。最高裁による差し止めや利用制限命令がなされた。現在はAadhaar法を制定、改正し、本人同意の下で、民間の事業者もAadhaarを本人確認に利用することが可能に。 • iSPIRTは、企業がユーザーデータから利益を得ていることが問題なのではなく、ユーザーが自分のデータから恩恵を得られないことが問題であると主張。銀行口座とデジタルIDの紐づけやデータ接続を個人に管理できる環境を提供し、ユーザーが自分のデータを適切に生かしてメリットを得やすくしている。		
備考	• 10億人をこえる市民に対していかに効率的に行政サービスを提供するかという観点からデジタルテクノロジーの導入を進めた。 • 今後整備が必要なのは、市民が行政に対して提供したデータを、どの機関に、どこまで共有するかを確認する機能や、行政側からの通知を一元的に受ける機能の提供。個人情報の保護とワンスオンリーを同時に実現するには、自己データの共有先を管理できる機能が不可欠。		

海外動向調査 参考ソース

文書名、書籍名	発行者	URL
デジタル時代の社会基盤「デジタルID」	日本総合研究所	https://www.jri.co.jp/MediaLibrary/file/report/jrireview/pdf/11717.pdf
エストニアの電子証明書等について	総務省	https://www.soumu.go.jp/main_content/000731090.pdf
デジタルガバメント先進に関する諸外国に事例の実態調査	経済産業省	https://www.meti.go.jp/meti_lib/report/2019FY/000247.pdf
India Stack：インドのデジタル化促進策にみる日本のマイナンバー制度への示唆	日本総合研究所	https://www.jri.co.jp/MediaLibrary/file/report/rim/pdf/11416.pdf
行政をハックしよう	著者：吉田 泰己 出版社：ぎょうせい	（書籍）

Digital Architecture
Design Center

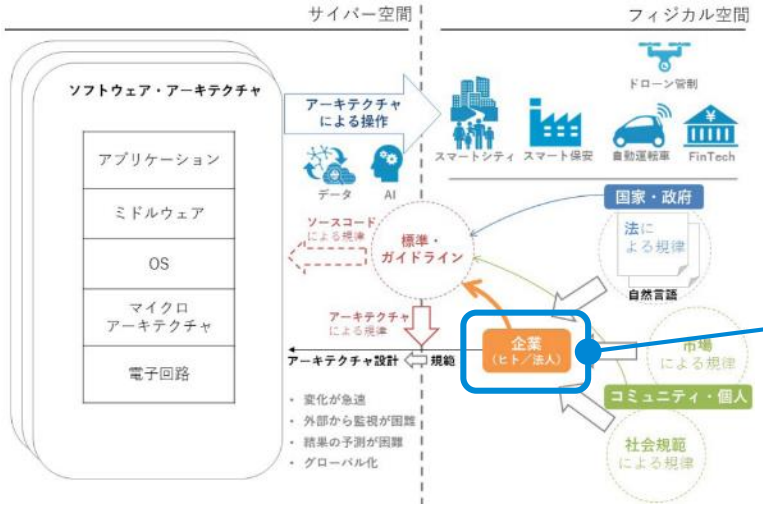
目次

IPA Better Life with IT

ガイドライン策定のための体制、ステークホルダー（現在の想定）

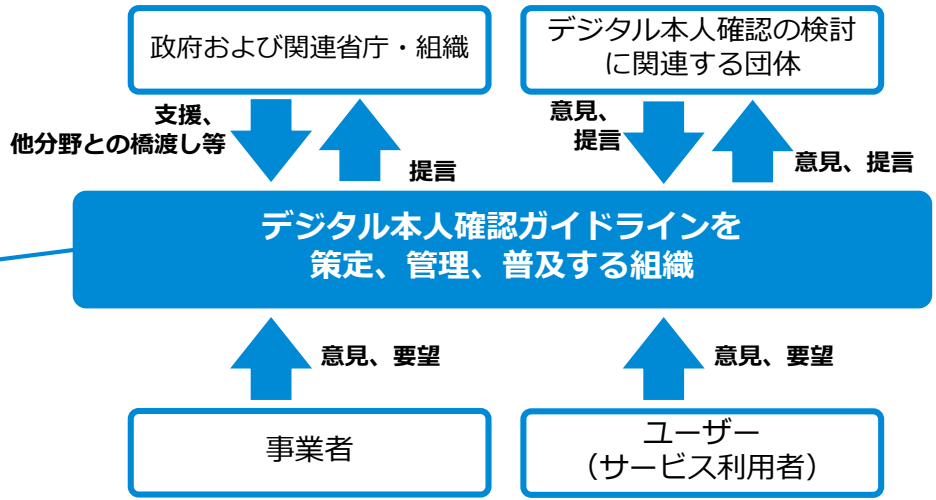
- 方針
  引き続き複数事業者からなる組織において、統一的な議論を進め策定することが望ましい。
  OpenIDファウンデーション・ジャパンと協力して検討の場を探索していくものとする。

1. 経済産業省より、Society5.0を実現するガバナンスモデルとして「サイバー空間及びフィジカル空間を融合したアーキテクチャを設計・運用している企業や、これらを利用するコミュニティ・個人による、ガバナンスへの積極的な関与」が提唱されている。
2. 事業者や団体に行ったヒアリングにおいて、本人確認については様々な場所で検討・議論がされているが、各主体が役割分担をしながら、いち事業者だけではなく、統一的に議論を進めていく必要性について指摘があった。



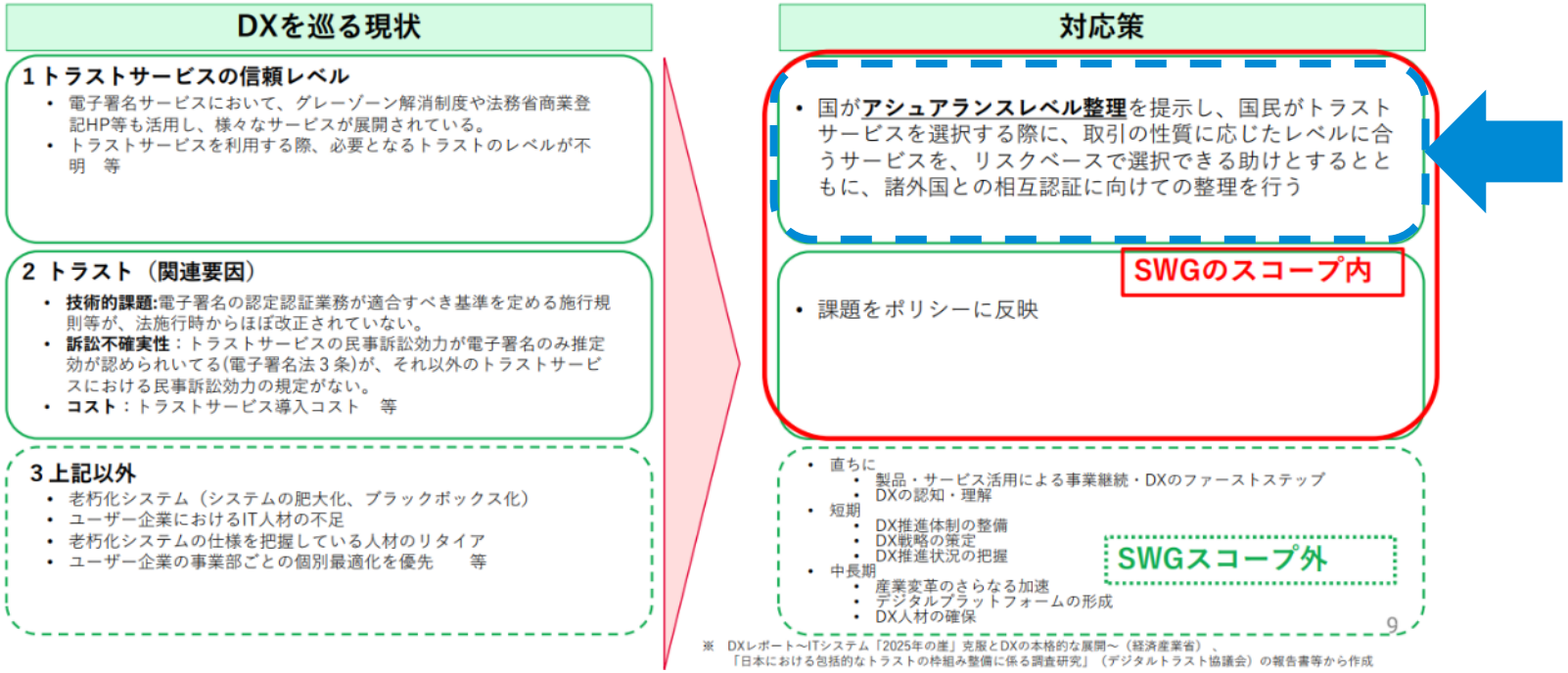
［引用元］経済産業省「GOVERNANCE INNOVATION： Society5.0の実現に向けた法とアーキテクチャのリ・デザイン」報告書

ガイドライン策定のための組織と周辺のステークホルダーの関連



ガイドライン策定のための体制、ステークホルダー（デジタル庁との連携）

ガイドラインの主要素である本人確認のアシュアランスレベル整理は、デジタル庁データ戦略推進ワーキンググループ内のトラストを確保したDX推進サブワーキンググループ（以下「SWG」という。）においてスコープの一部に位置付けられる。
当プロジェクトは第4回のSWGにて成果を発表し、以降オブザーバーとして参加。
今後もデジタル庁を始めとした関係省庁との連携を継続。



［引用元］第1回トラストを確保したDX推進サブワーキンググループ　資料1　トラストを確保したDX推進サブワーキンググループについて（デジタル庁）

マイルストーン（現在の想定）

現在の案は以下の通り。これをベースに各所との協議の上、調整を行う。