Digital Trustをめぐる最近の課題とデジタル庁の取組

2025/10

デジタル庁統括官 デジタル社会共通機能グループ長 楠 正憲

デジタル庁
Digital Agency

1. 自己紹介
2. DS-500 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の改定
3. Verifiable Credentials, Digital Identity Walletを活用した属性情報のデジタル活用の高度化

自己紹介

楠 正憲（くすのき・まさのり）

政府における取組

デジタル庁統括官 デジタル社会共通機能グループ長

マイナンバー法、自治体システム標準化、預貯金口座法、
トラスト政策（Trusted Web、電子署名法、電子委任状法）
ベースレジストリ、新技術（Web3、AI実装等）を担当

これまで構築に従事してきた主なシステム等

特定個人情報保護評価制度 評価書受付システム、
情報提供ネットワークシステム、マイナポータル、
マイナポイント、接触確認アプリCOCOA、
ワクチン接種記録システム、公金受取口座登録システム、
預貯金付番システム、ベースレジストリ関連システム、
給付支援サービス、行政事務標準文字、
ガバメントAI・デジタル庁生成AI利用環境「源内」等

主な経歴

1996年 神奈川大学経済学部 入学 2001年 卒業
1997年 Benefit Online嘱託 ECサイト再構築に従事
1998年 インターネット総合研究所 入社
1999年 CBook24.com 設立、電脳隊、P.I.M. 参画
2002年 マイクロソフト 入社 CTO補佐、国際標準化責任者など
2011年 内閣官房 番号制度推進管理補佐官 任用
2012年 ヤフー 入社 ID本部長 CISO-Boardなど
2016年 ISO/TC307 国内審議委員会 委員長（現任）
2017年 Japan Digital Design 設立 CTOとして参画
2018年 Cryptoassets Governance Task Force 設立
2021年 デジタル庁設立に統括官として参画（現任）
2025年 内閣官房 外国人との秩序ある共生社会推進室 次長（現任）

本人確認ガイドラインの改定について

DS-500 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の改定

本人確認ガイドラインの改定について

- 各府省が行政手続をデジタル化する際に従うべき**本人確認に関する基準、手法例、リスク評価の手順等**をとりまとめた**標準ガイドライン**※として2019年に発効。
- 技術革新や国内外の関連制度の状況、フィッシング攻撃や身分証偽造等による被害増加等を受けて2025年10月に改定（予定）。
- 本人確認の基本的枠組みを定めるほか、攻撃手法の高度化を踏まえた各種保証レベルやリスク評価プロセス等を大きく見直し。
- 今後、各保証レベルを満たすために使うことが想定される**主要な手段を示す解説編を策定し2025年度中に公表予定**。

本人確認ガイドラインの主な変更内容

基本的な考え方や枠組みの定義

基本的な考え方

- リスクに応じたレベルの本人確認手法の選択が必要。
  単に保証レベルの高い手法を選べばよいわけではない
- 本人確認手法によって事業目的の達成や公平性の確保を阻害したり、プライバシーを毀損したりしてはならない　等

基本的な枠組み

身元確認	当人認証	フェデレーション
		
主に窓口手続時やオンラインサービス利用開始時に、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。	主にオンラインサービス利用時に、申請者の当人性を確認すること。	身元確認や当人認証を、他者（信頼できるIDプロバイダ）に依拠して実現すること。

保証レベルやリスク評価プロセスの見直し

身元確認や当人認証の保証レベル

	（例）身元確認保証レベルの位置づけ（概要）	
	本人確認書類の検証手法	申請者の検証手法
レベル3	 ・ICチップ等による**デジタルな検証**を必須とし**偽造や改ざんに対する厳格な耐性**を確保	 ・本人確認書類の盗用に対し、**対面での容貌の確認、非対面での容貌の確認**又は**暗証番号による検証**を必須
レベル2	 ・本人確認書類の**対面での物理的な検査**等も許容	
レベル1	 ・**非対面での物理的検査（カメラ撮影、複写物の郵送等）**も許容	 ・**住所への到達確認による検証**も許容

リスク評価や保証レベル判定のプロセス

観点	評価の基準	影響度
申請者の権利権益	権利権益を長期間にわたって行使又は享受できなくなる	高位
	本来有する権利利益を一時的に行使又は享受できなくなる	中位
	一時的な不便等	低位
プライバシー	大量の個人情報漏洩など容易には回復できないプライバシー面の影響	高位
犯罪や攻撃	犯罪や他の行政サービス・民間サービスへの攻撃に悪用	高位

※本ガイドラインはデジタル社会推進標準ガイドライン群の１つとして整備。同ガイドライン群において標準ガイドライン（Normative）とは「政府情報システムの整備及び管理に関するルールとして順守する内容を定めたドキュメント」とされている。

本人確認ガイドラインの改訂

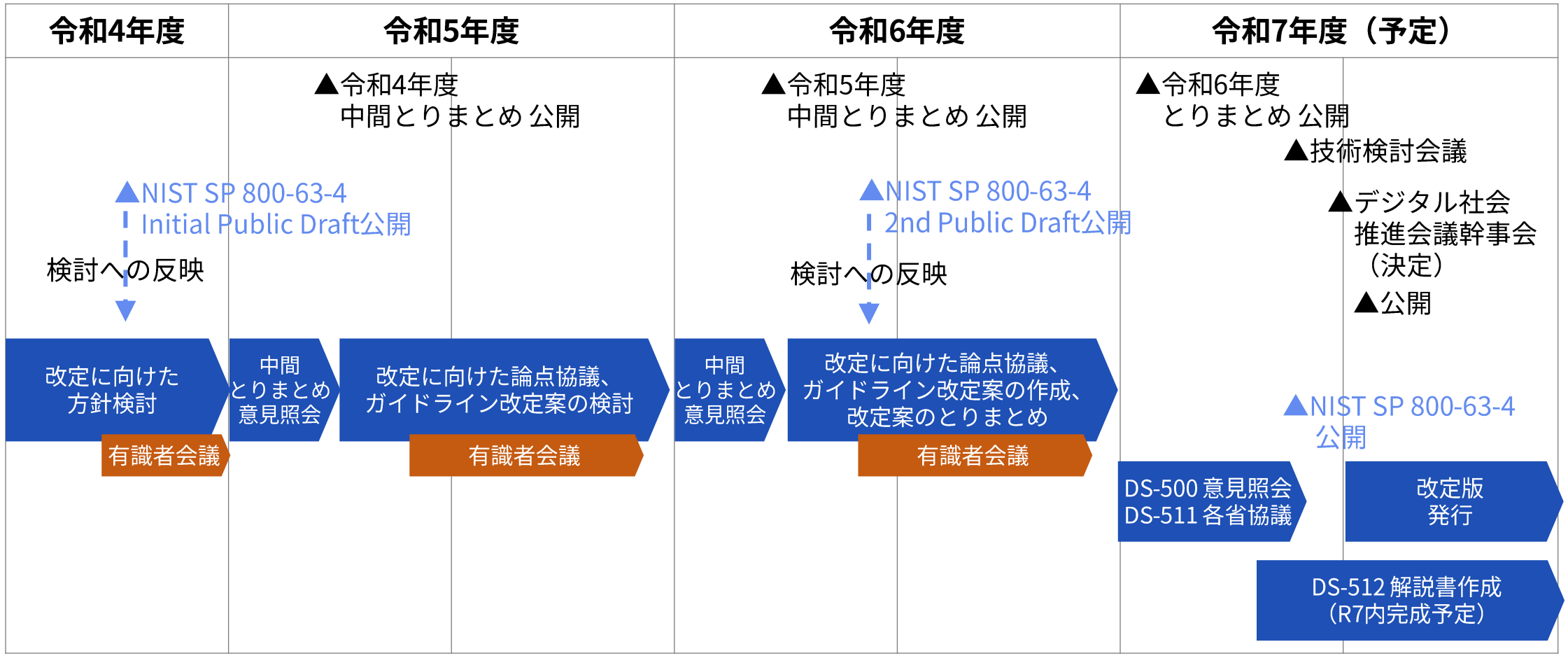
- 「DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン*1（以下「本人確認ガイドライン」という。）」は、デジタル社会推進標準ガイドラインの一つとして、各府省が行政手続をデジタル化する際に従うべき本人確認に関する基準、手法例、リスク評価の手順等をとりまとめ、**2019年に発効されたガイドライン（Normative）**である。
  - 米国国立標準技術研究所（NIST）が発行するSP 800-63 Digital Identity Guidelines等を参考としつつ、公的個人認証など我が国特有の本人確認手法を掲載している。
- 発効後の本人確認に係る情勢の変化等を踏まえ、ガイドラインの改定に係る有識者会議*2を開催し、本人確認に関する諸観点につき議論のうえ、改定案を取りまとめた。

技術・制度的な変化
- 米国NIST SP800-63-4の改定
- マイナンバーカードの普及
- GビズID、デジタル認証アプリ等認証基盤の普及
- パスキーなど強固な認証機能の登場　等

脅威の変化
- IDに関するサイバー攻撃の激化
- フィッシング攻撃による被害の増加
- 身分証明書の偽造攻撃の増加　等

*1 https://www.digital.go.jp/resources/standard_guidelines#ds500
*2 https://www.digital.go.jp/councils/identification-guideline-revise-experts-meeting

改定の経緯


令和4年度
令和5年度
令和6年度
令和7年度（予定）
▲令和4年度
中間とりまとめ 公開
▲令和5年度
中間とりまとめ 公開
▲令和6年度
とりまとめ 公開
▲技術検討会議
▲デジタル社会
推進会議幹事会
（決定）
▲公開
▲NIST SP 800-63-4
Initial Public Draft公開
検討への反映
▲NIST SP 800-63-4
2nd Public Draft公開
検討への反映
改定に向けた
方針検討
有識者会議
中間
とりまとめ
意見照会
改定に向けた論点協議、
ガイドライン改定案の検討
有識者会議
中間
とりまとめ
意見照会
改定に向けた論点協議、
ガイドライン改定案の作成、
改定案のとりまとめ
有識者会議
▲NIST SP 800-63-4
公開
DS-500 意見照会
DS-511 各省協議
改定版
発行
DS-512 解説書作成
（R7内完成予定）

本人確認ガイドライン解説書の新規整備

- 今回の改定にあわせ、本編とは別に「本人確認ガイドライン解説書」を整備する方針とする。
- Normative である本編に対し、「解説書」はInformativeとする。変化のサイクルの速い情報（具体的な技術、手法、事例等）を「解説書」にとりまとめることで、今後の動向変化にも柔軟に対応できる構成とする。
- 解説書は現在作成中。

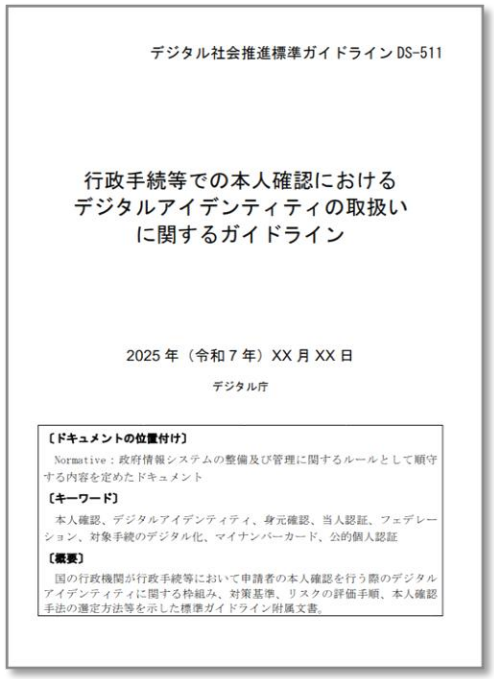
本人確認ガイドライン 本編(DS-511)

位置づけ：Normative
（遵守する内容）

本人確認の概念、基本的な枠組み、検討のプロセスなど、原則的・普遍的で陳腐化しにくい情報をとりまとめる

読み手の負担を軽減するため、本編はできる限りシンプルな内容に留めてページ数を抑え、参考情報は「解説書」に移動する

比較的長期間の改定サイクルを想定する


デジタル社会推進標準ガイドライン DS-511

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

2025 年（令和 7 年）XX 月 XX 日

デジタル庁

〔ドキュメントの位置付け〕
Normative：政府情報システムの整備及び管理に関するルールとして順守する内容を定めたドキュメント
〔キーワード〕
本人確認、デジタルアイデンティティ、身元確認、当人認証、フェデレーション、対象手続のデジタル化、マイナンバーカード、公的個人認証
〔概要〕
国の行政機関が行政手続等において申請者の本人確認を行う際のデジタルアイデンティティに関する枠組み、対策基準、リスクの評価手順、本人確認手法の選定方法等を示した標準ガイドライン附属文書。

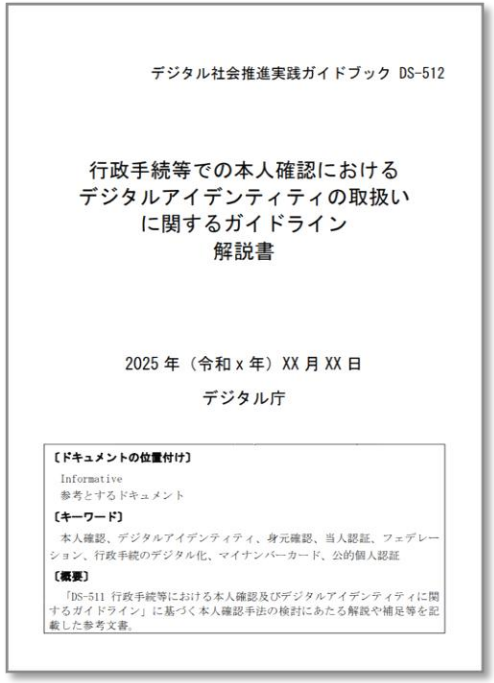
本人確認ガイドライン 解説書 (DS-512) *1

位置づけ：Informative
（参考情報）

本人確認ガイドライン本編の参考資料として、
- 採用候補となる具体的手法
- 実際の事例、留意点
- 検討用ワークシート

などの情報をとりまとめる

技術や脅威の動向等を踏まえつつ、比較的短期間のサイクルでの継続的な改定を行う運用を想定する


デジタル社会推進実践ガイドブック DS-512

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
解説書

2025 年（令和 x 年）XX 月 XX 日

デジタル庁

〔ドキュメントの位置付け〕
Informative
参考とするドキュメント
〔キーワード〕
本人確認、デジタルアイデンティティ、身元確認、当人認証、フェデレーション、行政手続のデジタル化、マイナンバーカード、公的個人認証
〔概要〕
「DS-511 行政手続等における本人確認及びデジタルアイデンティティに関するガイドライン」に基づく本人確認手法の検討にあたる解説や補足等を記載した参考文書。

*1 R7(FY2025)作成、公開予定。

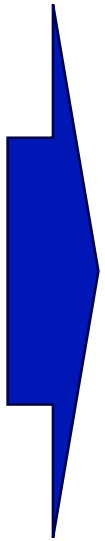
DS-511 行政手続等での本人確認における デジタルアイデンティティの取扱いに関するガイドライン

- 「DS-511 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」は現行DS-500の実質的な改訂版。本人確認の概念、基本的な枠組み、検討のプロセスなどある程度普遍的な内容を記載したもの(Normative)。
- 「DS-500 行政手続等におけるトラストおよびデジタルアイデンティティに関するガイドライン群(Informative)」は文書体系、バージョン管理の考え方などを記載するドキュメントに変更。

現在：

DS-500 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

DS-531 処分通知等のデジタル化に係る基本的な考え方



改訂後：

DS-500 トラスト及びデジタルアイデンティティ関連

- DS-510 デジタルアイデンティティ関連（未）
  - **DS-511 本人確認に関するガイドライン本編**
  - DS-512 本人確認に関するガイドライン解説書（作成中）
  - …
- DS-520 プライバシー関連（未）
- DS-530 トラスト関連（未）
  - DS-531 処分通知（既存）
- DS-540以降別テーマにて利用予定

本人確認ガイドラインの主要な改定ポイント

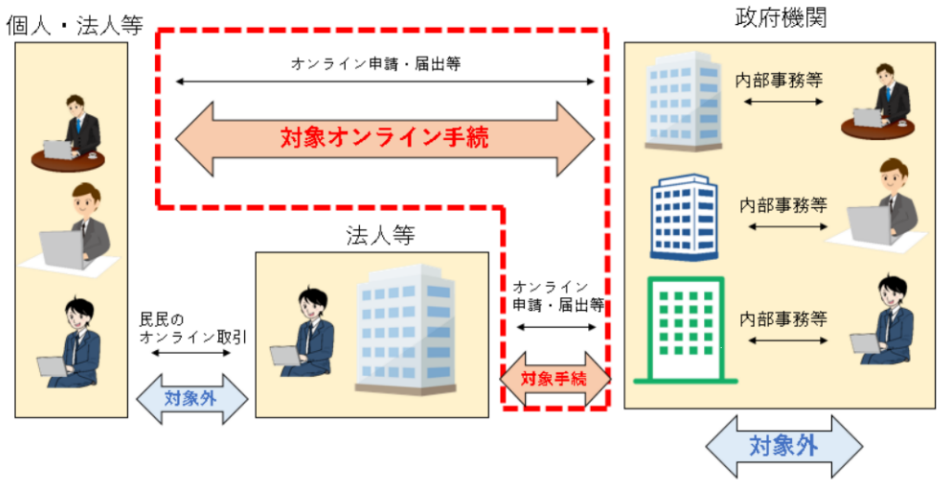
1章 はじめに	**① ガイドラインの適用対象と名称の見直し** • デジタルによる本人確認の機会がオンラインだけでなく対面にも拡大していることなどを踏まえ、対面の本人確認も適用対象に含める。これにあわせてガイドライン名称も変更する。
	② 検討にあたる「基本的な考え方」を定義 • 対象とする手続等の特性に応じた手法が選択できるよう、「事業目的の遂行」「公平性」「プライバシー」「ユーザビリティ及びアクセシビリティ」「セキュリティ」の5つの観点から「基本的な考え方」を定義。
2章 本人確認の枠組み	**③ 本人確認の基本的な枠組みを定義** • 身元確認や当人認証などの基本概念を説明する2章を新設し、「フェデレーション」の概念を新たに盛り込む。さらに、本人確認の実装モデルとして「連携モデル」及び「非連携モデル」を定義する。
3章 本人確認における 脅威と対策	**④ 脅威と対策の最新化、保証レベルの見直し** • 国内外の脅威の動向、最新の技術動向、米国NIST SP 800-63-4（2pd）での改定内容等を踏まえ、身元確認、当人認証及びフェデレーションにおける想定脅威と手法例を最新化する。 • 身元確認保証レベル及び当人認証保証レベルの位置づけと対策基準を脅威への耐性の観点から見直す。
4章 本人確認手法の 検討方法	**⑤ リスク評価プロセスの全面的な見直し** • 「基本的な考え方」の5つの観点から採用する手法の評価、調整、例外措置の検討等を行うプロセスを追加する。あわせて複雑な判定フローは廃止し、保証レベル判定までのプロセスをできる限り単純化する。

本人確認ガイドラインの適用対象の見直し

- 前述の背景を踏まえ、「対面による手続」及び「行政手続以外の行政サービス」についても適用対象に含める方針とする。

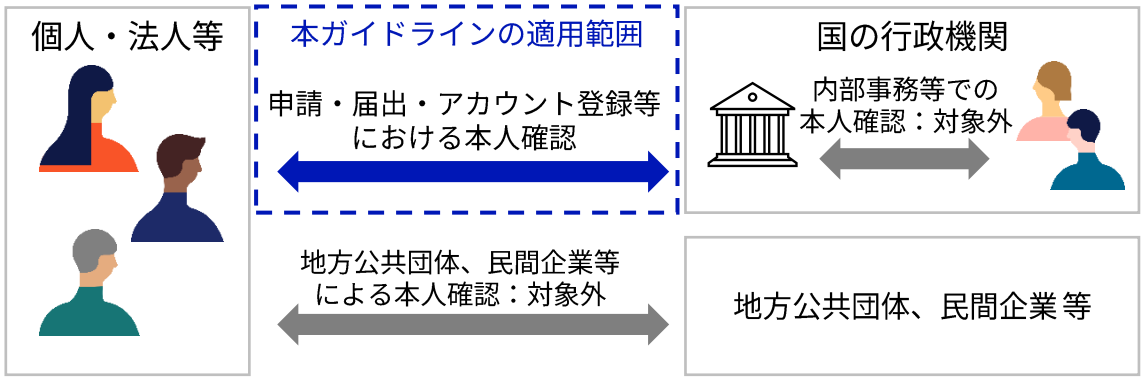
現行ガイドラインの適用対象（概要）

- 個人又は法人等に対するオンラインによる本人確認が必要であると見込まれる行政手続を対象とする
- 政府機関内の内部事務は対象外
- 民間企業による本人確認は対象外



改定後の適用対象（概要）

- 個人又は法人等に対する本人確認が必要であると見込まれる行政手続及び行政サービスを対象とする
- 政府機関内の内部事務は対象外（変更なし）
- 民間企業による本人確認は対象外（変更なし）



※ここでの「行政手続」とは、国の行政機関が行う行政手続を指す。地方公共団体は対象には含まれない。

本人確認手法の検討にあたる「基本的な考え方」を定義

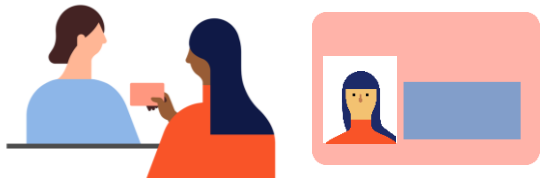
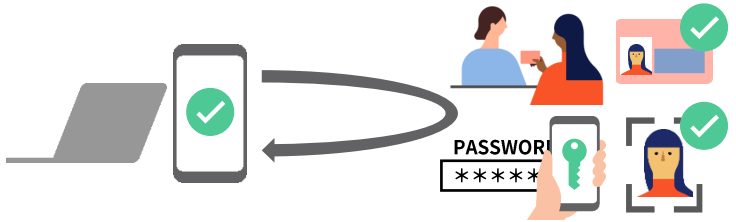
- 行政手続等における本人確認の手法は、その行政手続等が達成しようとする目的、対象となる利用者層、想定リスク等を考慮したうえで、様々な観点から検討されるべきであり、「単に厳格であればよい」という訳ではない。
- 今回の改定では、検討にあたり考慮すべき5つの観点を「基本的な考え方」として定義することとする。

「1.5　基本的な考え方」として定義する５つの観点（概要）

1) 事業目的の遂行	• 本人確認が障壁となって行政手続が達成しようとする事業目的が阻害されてはならない。採用しようとする本人確認手法に事業目的の遂行を阻害する懸念がある場合には、代替手段や例外措置を検討する。
2) 公平性	• 本人確認手法によって対象手続の公平性が損なわれてはならない。例えば、スマートフォンの所持を前提とする当人認証手法は、その採用によって対象手続の申請や利用における公平性が損なわれないか、慎重な検討が必要である。
3) プライバシー	• 利用者のプライバシーを毀損しない本人確認が必要である。収集目的を明示する、目的外の利用を行わない、取り扱うデータを必要最小限に留めるなどプライバシー保護の観点で必要な措置を検討し講じることが必要である。
4) ユーザビリティ及びアクセシビリティ	• ユーザビリティやアクセシビリティが悪いと、利用者が手続きを断念したり、誤操作したりする原因になるため、事業目的の遂行や公平性などにも影響を与えうる重要な要素である。
5) セキュリティ	• 単にセキュリティレベルの高い手法を選べばよい訳ではない。事業目的の遂行、公平性、プライバシー、ユーザビリティ及びアクセシビリティへの影響も考慮しながら、リスクに応じたレベルの本人確認手法を選択することが必要である。

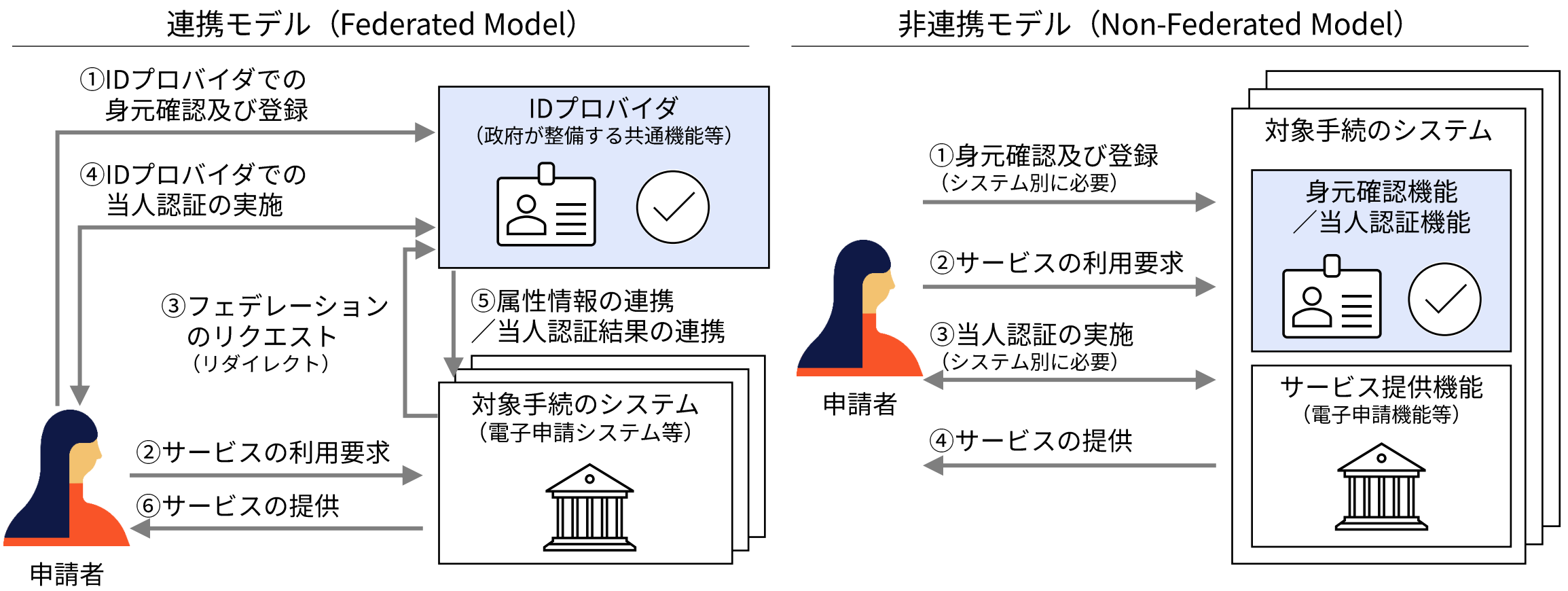
本人確認の基本的要素を定義

- 本人確認の構成要素である「身元確認」と「当人認証」を明確に定義し、概念図を示す。
- また、身元確認や当人認証を他者に依拠して実現する「フェデレーション」という概念を、今回の改定において新たに定義する。

身元確認 (Identity Proofing)	**当人認証** (Authentication)	**フェデレーション** (Federation)
		
申請者を一意に識別するとともに、その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。	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。	身元確認や当人認証を、他者に依拠して実現すること。 具体的には、信頼できるIDプロバイダと連携し、IDプロバイダによって行われた身元確認や当人認証の結果に関する情報を入手することで、対象手続における本人確認を実現する。

システムの実装モデルを定義

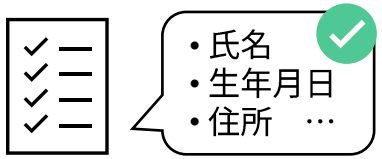
- 本人確認を行うシステムの実装モデルとして「連携モデル」と「非連携モデル」を新たに定義する。
- ユーザの利便性や政府情報システムにおける共通機能の活用の方針に基づき、本ガイドラインではフェデレーションを活用した「連携モデル」の採用を第一候補として扱う。



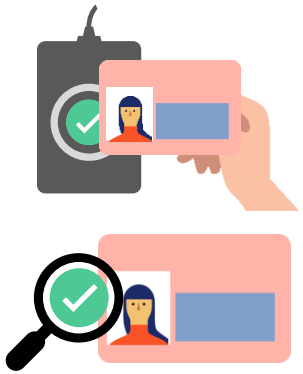
身元確認のプロセスの定義

- 身元確認の具体プロセスとして「属性情報の収集」「本人確認書類の検証」「申請者の検証」を定義し、それぞれのプロセスで対策すべき想定脅威を整理。また、関連するプロセスとして身元確認完了後の「登録」プロセスについても定義する。

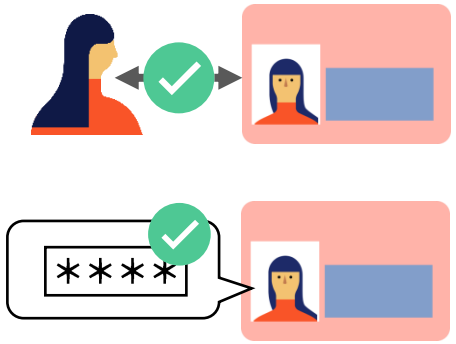
属性情報の収集 → **本人確認書類の検証** → **申請者の検証** → **登録**



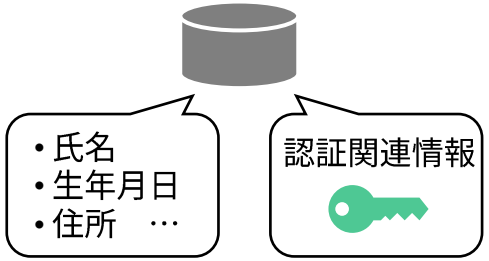
氏名、生年月日、住所等の属性情報を申請者から収集し、申請者を対象となる母集団の中で一意に識別する。



申請者から提示された本人確認書類が、偽造・改ざん・複製等された不正なものでないことを、物理的又は電子的に検証する。



本人確認書類が備える顔写真や暗証番号等を用いて、提出された本人確認書類が確かに申請者自身のものであることを検証する。



身元確認の結果をもとに、利用者の属性情報や当人認証のための認証関連情報を登録する。

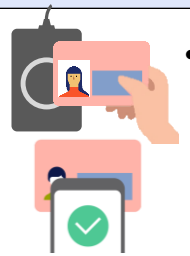
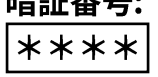
身元確認手法例の体系化

- 身元確認手法例は、国内に普及している技術・方式等を踏まえ、手法の類型を体系的に整理して最新化する。
- ただし、これらに該当する具体的な手法名（例えば「マイナンバーカードの署名用電子証明書」など）については、本編には詳細は記載せず、「解説書」にて技術仕様や留意点等を解説する方針とする。

属性情報の収集手法例	×	本人確認書類の検証手法例	×	申請者の検証手法例
a) 電子的な読取り • スマートフォンやICカードリーダーを用いて、本人確認書類のICチップから電子データを読み取る **b) 物理的な読取り** • OCR等を用いて本人確認書類の券面の記載情報を物理的に読み取る **c) 申請者自身による記入・入力** • 紙の申請書やWebフォームに申請者自身による記入や入力を求める **d) IDプロバイダからの情報取得** • IDプロバイダとの連携により身元確認済みの属性情報を取得する		**a) デジタル署名の検証** • 本人確認書類から読み取った電子データのデジタル署名を検証する **b) 信頼できる情報源への照会** • 参照番号やQRコードなどにより発行元等に情報を照会する **c) 対面での物理的検査** • 本人確認書類の券面を、対面にて目視・触覚等で検査する **d) 非対面での物理的検査** • 本人確認書類の券面を、カメラ映像や複写物等によって検査する		**a) 対面での容貌確認** • 本人確認書類の顔写真と申請者の容貌を目視にて比較する **b)非対面での容貌確認** • 本人確認書類の顔写真と申請者の容貌をカメラ映像等で比較する **c) 暗証番号等による検証** • 本人確認書類が備える暗証番号等の認証機能によって、申請者が本人確認書類の持ち主であることを確認する **d) 住所への到達確認による検証** • 本人確認書類に記載された住所に確認コードを郵送するなどして申請者へと到達できることを確認することで、申請者が本人確認書類の持ち主であることを確認する

身元確認保証レベル（IAL*）の見直し　―　全体概要

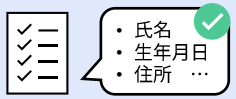
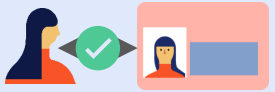
- 昨今の脅威動向を踏まえ、身元確認保証レベルは「ICチップ等によるデジタル的な検証の有無」を、保証レベルの差として表現できるように改定する。また低リスクの手続・サービス向けの保証レベルとして「レベル1」を定義※する。（※現行ガイドラインの「レベル1」は「身元確認なし」の位置づけであったが、今回の改定で簡易的な身元確認を行うレベルとして再定義する。）

保証レベル	保証レベルの位置づけ	
	本人確認書類の検証手法	申請者の検証手法
身元確認 保証レベル3	 • ICチップ等による**デジタル的な検証を必須**とし、**偽造や改ざんに対する厳格な耐性**を確保するレベルとする。 （「デジタル的な検証」：発行者によって付与されたデジタル署名等による暗号学的な検証を行うこと。）	  • 本人確認書類の盗用に対し、**対面での容貌の確認、非対面での容貌の確認**又は**暗証番号による検証**を必須とする。 • 本人確認書類の貸し借りに対しては、対象手続のリスクに応じた個別検討※を行うこととする。 ※ 暗証番号のみでは本人確認書類の貸し借りを検知できないため、貸し借りのリスクを許容できない場合は「容貌の確認」の追加実施等を検討する。
身元確認 保証レベル2	 • 本人確認書類の**対面での物理的な検査等も許容**する。ただし検証強度を考慮しカメラ越しや複写物による検査（非対面で物理検査）は不可とし、一定の耐性を確保する。	
身元確認 保証レベル1	 • 保証レベル2までの手法に加えて、**非対面での物理的検査（カメラでの撮影、複写物の郵送等）も許容**する。偽造・改ざんへの簡易的な耐性をもつレベルとして位置付ける。	 • 保証レベル2までの手法に加えて、**住所への到達確認による検証**も許容する。 （本人確認書類に記載されている住所に居住していることの確認をもって、本人確認書類との紐づきを検証する手法）

* Identity Assurance Levelの頭文字

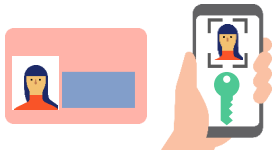
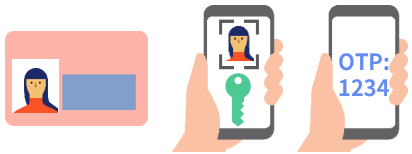
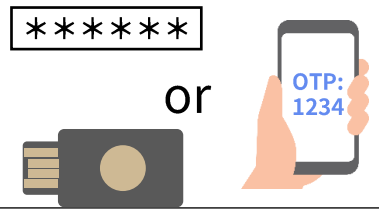
身元確認保証レベル（IAL）の見直し　—　各レベルの対策基準

- 前述の「位置づけ」に基づき、各レベルの対策基準を以下のとおり定義する方針とする。
  ※対策基準はあくまで基準であり、同等の脅威耐性を確保できる場合は他の手法等により代替してもよいものとして定義する。

保証レベル	対策基準（**青字：上位レベルとの相違点**）		
	属性情報の収集 	**本人確認書類の検証** 	**申請者の検証** 
身元確認 保証レベル3	電子的な読取り	デジタル署名の検証	以下のいずれか • 対面での容貌確認 • 非対面での容貌確認 • 暗証番号等による検証
身元確認 保証レベル2	（収集手法は任意とする）	以下のいずれか • デジタル署名の検証 • **信頼できる情報源への照会** • **対面での物理的検査**	
身元確認 保証レベル1	（収集手法は任意とする）	以下のいずれか • デジタル署名の検証 • 信頼できる情報源への照会 • 対面での物理的検査 • **非対面での物理的検査**	以下のいずれか • 対面での容貌確認 • 非対面での容貌確認 • 暗証番号等による検証 • **住所への到達確認による検証**

当人認証保証レベル(AAL*1)の見直し

- 当人認証保証レベルについては大幅な変更は行わないが、フィッシング攻撃など最新の脅威動向、技術動向、国民向けの行政手続等において想定されるリスク等を考慮し、脅威耐性の観点から各レベルの対策基準を一部見直す。

保証レベル	対策基準	
	認証要素	脅威への耐性要件
当人認証 保証レベル3	**公開鍵認証を含む多要素認証** 例） • 暗証番号付きのICカード • パスキー 	• **フィッシング耐性（必須）** 「必須」：全ての利用者に対してフィッシング耐性をもつ認証方式を適用する ＋ • 保証レベル2の耐性
当人認証 保証レベル2	**多要素認証** 例） • 暗証番号付きのICカード • パスキー • パスワード ＋ワンタイムパスワード 	• **フィッシング耐性（推奨）** 「推奨」：フィッシング耐性をもつ認証方式を利用者に対して提供し、その利用を推奨するが、他の認証方式についても選択可能とする • **認証器等の盗用に対する耐性** ※ICカードやパスワード等の認証要素のうち一つが盗用された場合の耐性 ＋ • 保証レベル1の耐性
当人認証 保証レベル1	**単要素認証**（又は多要素認証） 例） • パスワード • ワンタイムパスワード • USB接続型セキュリティキー • 又は保証レベル2以上の手法 	• 盗聴 • リプレイ攻撃 • オンライン上での認証情報の推測

*1 Authentication Assurance Levelの頭文字

フェデレーションの対策基準（概要）

- 本ガイドラインでは、フェデレーションについての保証レベルは定めず、一律の対策基準を定義する方針とする。
- 対策基準の内容はNIST SP 800-63-4 2pdのFAL 2の要件を参考としつつ、以下の方針によって定義する。

No.	項目	対策基準の定義方針	NIST SP 800-63-4 2pdのFAL要件との対応
1	信頼関係の確立	• フェデレーションによる連携にあたる信頼関係の確立は事前に行うこと。	“Trust Agreement Establishment”のFAL2に相当
2	設定・登録及び鍵管理	• 識別子や暗号鍵の設定・登録・鍵管理は、静的な方法を基本とするが、動的な方法についても採用可とする。	“Identifier and Key Establishment”のFAL2に相当
3	アサーションに関する対策	• フェデレーショントランザクションは原則として依拠当事者側から開始されること。 • IDプロバイダから連携されたアサーションに対して以下の検証を行うことで、インジェクション攻撃等への耐性を備えること。 ① 想定するIDプロバイダから発行されたものであること ② 第三者により偽造・改ざんされたものでないこと ③ 自身が要求したリクエストに対して発行されたものであること ④ 自身に向けて発行されたものであること ⑤ 再利用されたものでないこと ⑥ 有効期限内であること	“Injection Protection”のFAL2に相当 （NISTよりも要件を具体化して定義）

リスク評価プロセスの見直し方針

- 4章のリスク評価プロセスは、保証レベル判定までのプロセスを簡略化しつつ、事業目的の遂行、公平性、プライバシー等への影響を考慮したテーラリングの考え方を取り入れる形で全面的に見直し。

検討プロセスの全体像	今回の改定における見直し方針
4.1 対象手続の保証レベルの判定 1) リスクの特定 2) リスクの影響度の評価 3) 保証レベルの判定	**❶保証レベル判定プロセスの改善と単純化** • 円滑なリスク評価が行われるよう、影響度の評価の前段に「リスクの特定」プロセスを新設 • 影響度や保証レベルの複雑な判定フローは廃止し、よりシンプルで行政手続等に適した判定基準へと見直し
4.2 本人確認手法の評価と決定 1) 本人確認手法の評価 2) 補完的対策等の検討 3) 例外措置の検討	**❷本人確認手法の評価プロセスを新たに定義** • 保証レベルに対応する手法を採用した際の影響を、事業目的の遂行や公平性、プライバシーなど様々な観点から評価し、本人確認手法とあわせて検討すべき補完的対策や例外措置の検討プロセスを新設 （NIST SP 800-63-4における”テーラリング”のプロセスに相当）
4.3 継続的な評価と改善 1) 評価のための情報収集 2) 評価と改善の実施	**❸継続的な評価と改善プロセスの具体化** • 継続的な改善のために実施すべきプロセスを新たに定義 ※現行ガイドラインにおいても記載があった内容をプロセスとして明文化

保証レベル判定プロセスの改善と単純化

- リスク影響度の評価は、リスクのカテゴリーや複雑な判定フローを廃し、本ガイドラインの主な適用対象が行政手続であることを踏まえ、「利用者の権利権益の侵害」を軸とした評価の基準とする。
- ただし、プライバシー面での深刻な影響、犯罪や攻撃への悪用が想定される場合については、権利権益の侵害の度合いによらず「高位」とする。

検討プロセスの全体像

4.1 対象手続の保証レベルの判定
1) リスクの特定
2) リスクの影響度の評価
3) 保証レベルの判定

4.2 本人確認手法の評価と決定
1) 本人確認手法の評価
2) 補完的対策等の検討
3) 例外措置の検討

4.3 継続的な評価と改善
1) 評価のための情報収集
2) 評価と改善の実施

観点	評価の基準	影響度	想定例
対象手続によって得られる権利権益等の侵害	特定の利用者や関係者が、**本来有する権利権益を長期間にわたって行使又は享受できなくなる**など、深刻かつ長期的な影響を受ける	**高位**	なりすましの被害者が長期間にわたって補助金を受け取れなくなり、遡及等の原状回復にも時間を有する
	特定の利用者や関係者が、**本来有する権利利益を一時的に行使又は享受できなくなる**が、短期間での回復や復旧ができる	**中位**	なりすましの被害者が本来有する資格を一時的に行使できなくなるが、短期間で復旧できる
	特定の利用者や関係者の権利権益は侵害しないが、**一時的な不便等**の影響を与える	低位	なりすましの被害者はアカウント再発行が必要となり一時的な不便を被る
プライバシーの侵害	特定の利用者や関係者に関する要配慮個人情報が侵害されるなど、**容易には回復できないプライバシー面の影響**を受ける	**高位**	不正アクセスによって利用者の要配慮個人情報等を攻撃者に閲覧・窃取される
犯罪や攻撃への悪用	対象手続におけるなりすましや不正アクセスの結果が、**犯罪や他の行政サービス・民間サービスへの攻撃に悪用**される	**高位**	攻撃者に対して対象手続から証明書が発行され、民間サービスに対するなりすましに悪用される

Verifiable Credentials, Digital Identity Wallet を活用した属性情報のデジタル活用の高度化

属性情報のデジタル活用の高度化について

■ 課題

- データ利活用推進に向け、**デジタル上でやりとりする相手を信頼するための属性情報※1(身元・資格等)の証明が重要**。
- デジタル庁では、行政手続のデジタル完結や官民でのデータ利活用推進等に向け、様々な**証明書等のデジタル化を推進**。

- 現在の証明書のデジタル化のアプローチは**「PDF等で発行・提供」することが多い**が、以下のような課題がある。
  - ✓ **PDF等は文書の編集・偽造が容易**であり、なりすましリスク等が高い

    例）住民票の写しをPDFで発行すると複製しやすく、ローンや口座開設のなりすまし可能。
  - ✓ 人の目で確認できるが**機械による自動データ処理が困難**

    例）電子申請を受けてもPDFを目視してデータを手入力し、電話等で検証。AIを用いたデータの利活用にも課題。

■ 政策の方向性

- デジタルで属性情報(デジタル・アイデンティティ)※2を、偽造防止・機械処理可能な形で扱うための新たな技術、特にベリファイアブル・クレデンシャル(VC)及びデジタル・アイデンティティ・ウォレット(DIW)という技術・仕組みでの証明書の活用が期待され、各国で利活用や国際相互運用の議論が活発化している。
- 我が国においても**各種の証明書（身分証明書、資格証明書、その他の属性証明書等）のVC・DIWを用いた電子化及び高度化をすることで、上記課題の解決につなげる**。

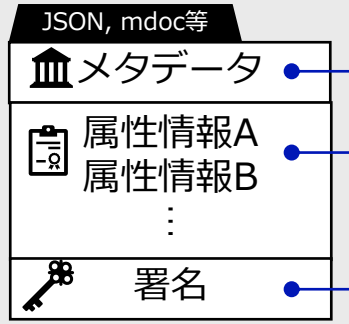
※1：ある個人に紐づく情報（保有する資格や役職、経歴等の主体を構成する情報）を属性情報と呼ぶ
※2：デジタル庁ホームページ（トラスト政策）：トラスト（デジタル・アイデンティティ等）｜デジタル庁

基礎情報：VC (Verifiable Credential)とは

■ VC（Verifiable Credential）とは

- **デジタル署名による真正性確保・改ざん防止**等の機能を有する、**目視しやすく**また**機械可読**かつ**汎用的なデータ形式、**及びデータ流通の形態。
  ※W3C VCDMやISO18013-5(mdoc)等、様々なデータフォーマットが存在する

VCの構造



■ VCが行政で試行的に利用された例：新型コロナワクチン接種証明書

- ただし、接種証明は対面でしか提示できない等、VCの効果として期待される手続のデジタル完結やシステムでの自動検証に必要な使用方法・仕様をカバーしていなかった。

1. VCを発行

マイナンバーカードで本人確認を行い、ワクチン接種証明書（VC）を発行する

2. VCを管理

ワクチン接種証明書アプリ（DIW）でワクチン接種証明書（VC）を管理する

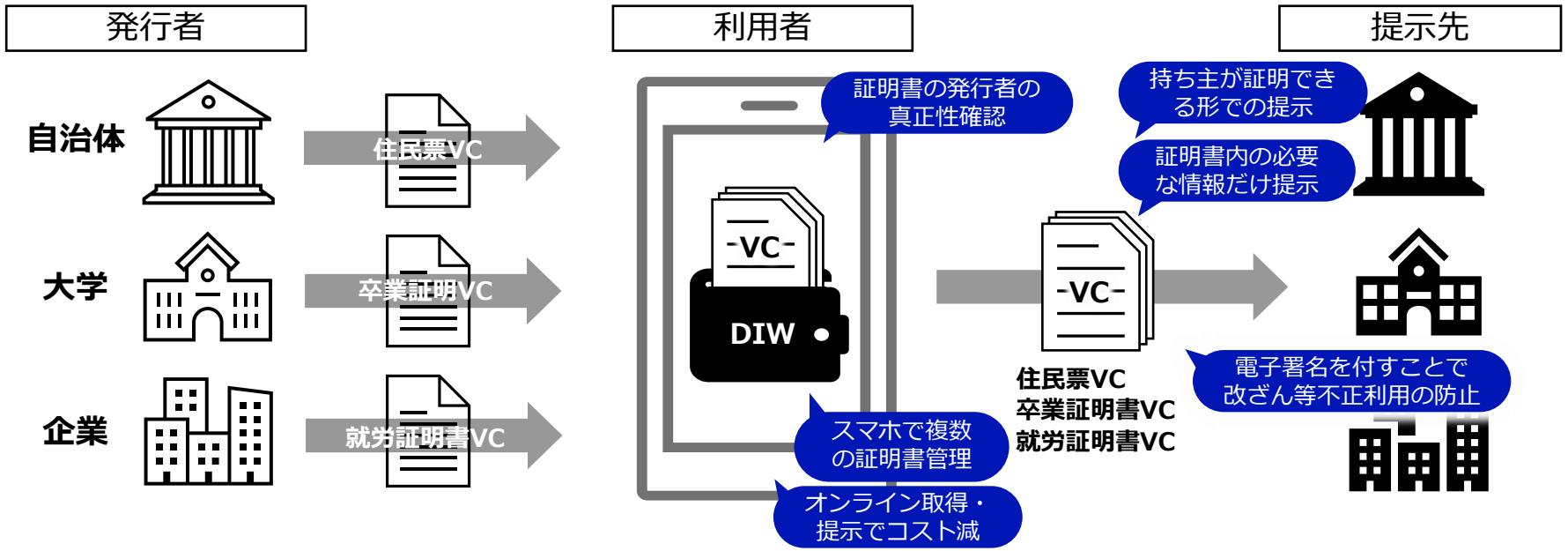
3. VCを提示

ワクチン接種証明書（VC）を各検証者に提示する

基礎情報：DIW (Digital Identity Wallet)とは

■ **DIW(Digital Identity Wallet)の一般的な概念**

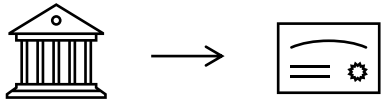
- 端的には**VCを入れる入れ物**（財布の中に身分証、資格証等をまとめて持ち歩くことから）。
- ユーザーは、自分の証明書等を**スマートフォン等に保存・管理し、第三者に提示**出来る。
- 第三者への証明書の提示に際し、**持ち主本人だと証明した形での提示**、証明書の必要な情報のみを選択的に提示することでの**プライバシー向上**、属性情報取得に要する**コストの削減**、**セキュリティ強化**等が謳われている。



VC・DIWを用いた証明書の効果

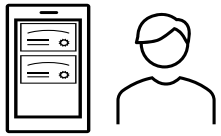
VC・DIW等の「電子的かつ標準化された証明書の発行・管理・提出」や「機械可読性・検証可能性の確保」等の特徴を活かし、**自治体等での発行コスト低減、証明書の不正・偽装の防止**とその検証易化による**省力化**が実現するほか、利用者の**利便性向上やプライバシー保護、AI時代の高度なデータ活用の拡大**等にもつながり、**デジタル社会の発展に資する大きなメリットをもたらす。**

発行者のメリット



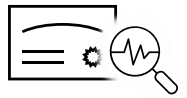
- ✓ 書面の証明書の発行手続に係る職員の所要コストを削減
  例：住民票(写)は最大年間5500万件程度
- ✓ 民間の発行する証明書を中心に、非改ざん性をはじめとする流通に関するリスクを低減
  例：未登録事業者が無効な「技能講習終了証」を発行・販売する刑事事件が発生

利用者のメリット



- ✓ 行政手続き等における利便性向上（発行申請等の簡便化）
- ✓ 証明書の受取コスト・管理コスト・提示コストの削減
  例：国家資格システムで取扱う資格者証は将来的に最大120資格程度
- ✓ 検証者に提示する情報の最小化によるプライバシーの確保
  例：酒類・タバコ購入時の年齢確認等
- ✓ 標準化の進展による国を跨いだ活用、他分野間における証明書利用拡大

検証者のメリット



- ✓ (発行者の真正性確保による)提出時の発行者への確認コストの削減
  例：保育所の入所・更新時に確認する就労証明書は最大年間270万件程度
- ✓ 機械可読による、職員の目視確認・転記作業等の事務処理コスト削減
  参考：自治体からは分野としては子育て、福祉、介護、生活保護、手続としては申請の適格性確認のコストが大きいとの声も
- ✓ 行政手続等における個人情報の提供に関して、本人の同意を厳密に確認可能

※例に挙げた証明書に関してはVC・DIWを用いることが既に決定しているものではなく、関係省庁と調整中である。

VC・DIWによる属性証明の電子化・高度化の将来展望

将来展望（ありたい姿）

❶デジタル完結の観点：
便利で効率的なデータ連携を推し進める

VC・DIWが様々な証明書をデジタルで活用し、官民で連携するためのインフラとなり、行政手続のデジタル完結や国を超えた相互運用による利便性向上・業務効率化等を推進

❷消費者保護の観点：
安心してデジタル証明書を利用できる

プライバシーやセキュリティが適切な技術や制度等によって保護され、安心してVC・DIWを利用できる

❸エコシステム維持発展の観点：
新たな価値を創出する

多様な事業者が参入することで、既存のユースケースに囚われない新たな価値や顧客体験が創出される

利用者にとってのメリット

利便性の向上　**手続の簡略化**　**プライバシーの保護**

行政機関・民間企業にとってのメリット

業務効率化　**信頼性の向上**
情報活用の推進　**新たな顧客体験の創出**

証明書の電子化及び高度化に向けて取り組むべきこと

資格証明・属性証明用途は、ニーズ・期待が明確に示されつつあるものの採用すべき技術標準や実装方式の選定指針が体系的に整理されておらず、代表的な証明書のVC化が進んでいない状況である。

各証明書共通で考慮が必要な項目に関して、**採用すべき技術面・運用面の対策を促す手法の整理やその示し方等の必要な検討**をデジタル庁が担い、**各証明書のVC化の推進環境を整える**必要がある。

		公的に発行される属性証明書			民間が発行する属性証明書	
		身元証明書		資格証明書・属性証明書	資格証明書・属性証明書	
電子化・高度化状況		○	スマートフォンのマイナンバーカード搭載（カード代替電磁的記録）	△ 住民票(写)や国家資格者証など、VCによる高度化が期待される証明書が紙・PDFのまま	△	民間企業がVC・DIWを提供しはじめているが、非推奨な利用形態もあるため、VCの適切な活用方法を明確化する必要
利活用に向けた措置	技術面の対応	○	ISO/IEC 18013-5に準拠した構造	× 公的VC証明書のリスクへの対策の推奨要件が未整理	×	行政の信頼性確保や消費者保護の観点での推奨要件が未整理
	運用面の対応	○	利用申請手順を規定 本人確認ガイドラインを規定			
	制度等の対応	○	マイナンバー法で法定化しており、送信用・確認用プログラムの大臣認定を定めている	× カード代替電磁的記録のように、公的機関が発行する証明書であれば、発行方法・格納方法・提示方法等、満たすべき基準を規定する必要がある可能性	×	源泉徴収票や診断書等、法令で交付義務が規定されている証明書や悪用リスクが高い証明書をVC化する場合、満たすべき基準を規定する必要がある可能性

要対応

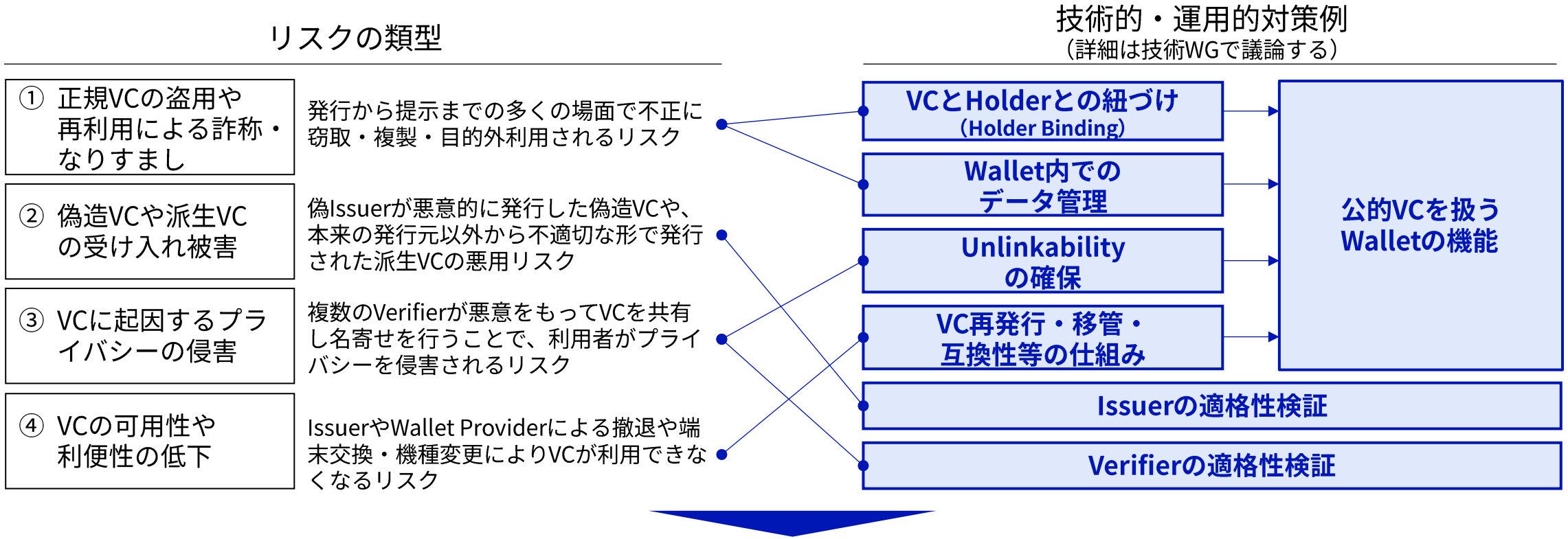
令和７年度　属性証明の課題整理に関する有識者会議

- 昨年度の「DIWアドバイザリーボード」及び「VC/VDCの活用におけるガバナンスに関する有識者会議」を統合・再編する形で、属性証明の課題整理に関する新たな会議体を立ち上げます。

会議体	論点	論点の概要
属性証明の課題整理に関する有識者会議（本体会議）	論点１ 適切な技術面・運用面の対策を促す手法	VC・DIWによる証明書の電子化・高度化における各種リスクへの対策について、既存のガバナンスによる規律も踏まえ、論点２で整理される技術面・運用面の対策をどのように示し、促すか、必要な手法などを公的かつリスクの高いユースケースを念頭に検討する。 今年度目指したい議論結果 **適切な技術面・運用面の対策を促す手法**
技術ワーキンググループ（技術WG）	論点２ 技術面・運用面の対策	VC・DIWによる証明書の電子化・高度化にあたり考慮が必要な各種リスクに対し、特にリスクの高いユースケースを中心に技術面・運用面の対策を検討すると共に、VCフォーマットの利用方針をはじめ、今後の社会実装に向けた技術要件の選択指針についても併せて検討する。 今年度目指したい議論結果 **推奨する技術面・運用面の対策の整理**

各リスクに対する適切な対策を促すために必要な手法

- VC・DIWの健全な利活用のためには、各リスク対策として採るべき手段を明らかにしておくべきであると考えられる。この**適切な技術面・運用面の対策を促すために必要な手法は何か？**



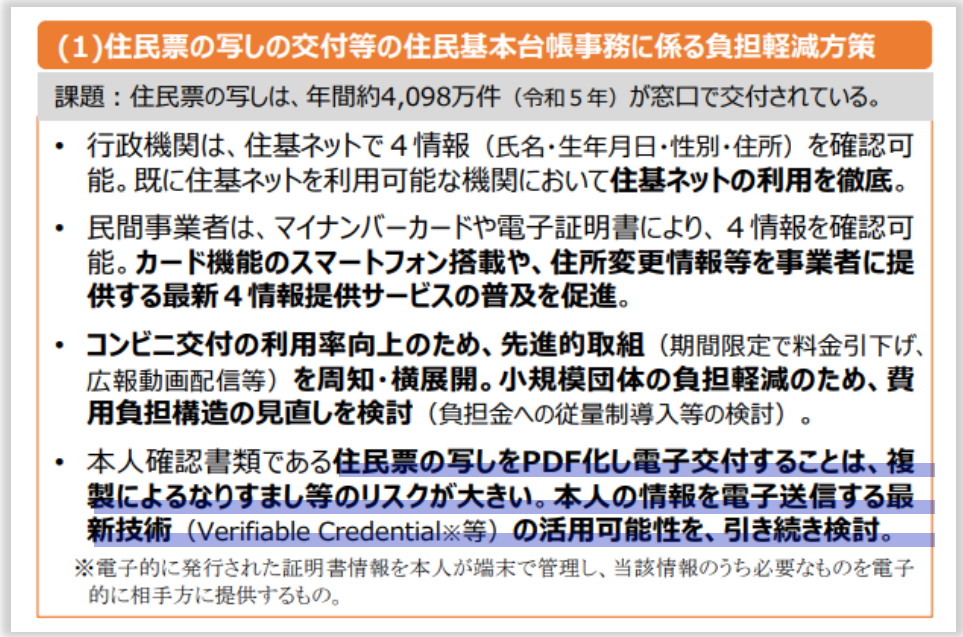
適切な技術面・運用面の対策を促すために必要な手法は何か？

（参考）直近のVC活用への期待の高まり

期待例①：住民票の写し

総務省の「デジタル技術を活用した効率的・効果的な住民基本台帳事務等のあり方に関するワーキンググループ」では、住民票の写しの電子化を検討しているが、同証明書は行政手続や民間取引で「提出」する性質を有することから、単純なPDF形式では複製によるなりすまし等、個人情報保護の観点で看過し得ないリスクが懸念されるところ、**Verifiable Credential等の活用が期待されている。**

総務省における住基WGの検討状況



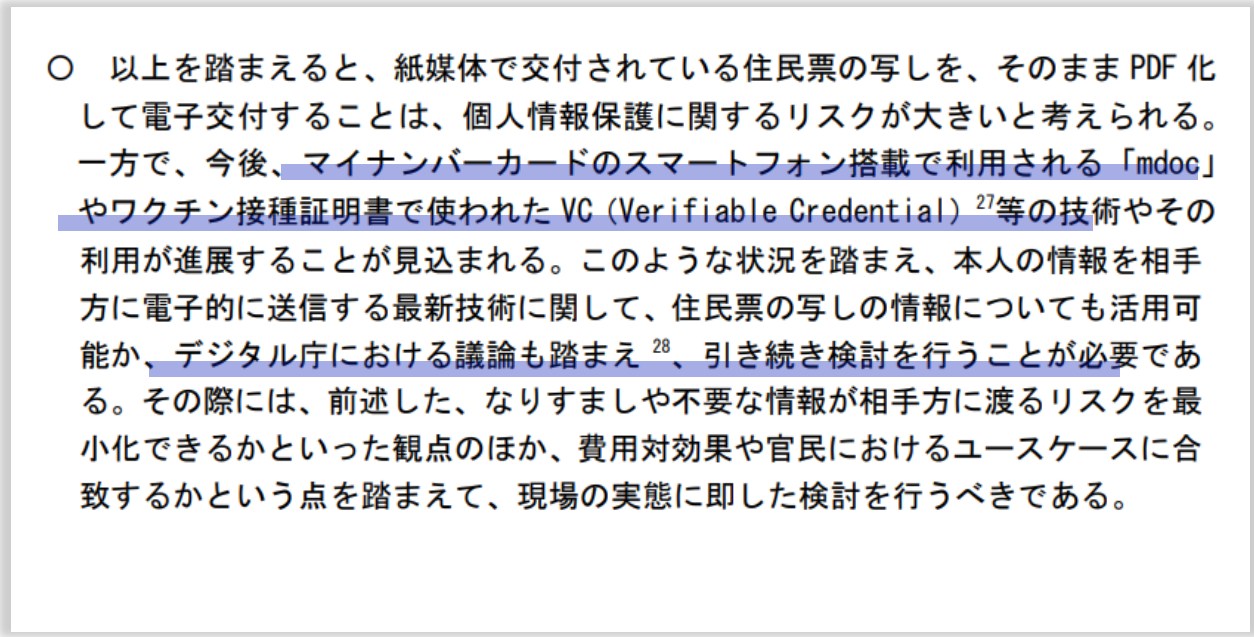
(1)住民票の写しの交付等の住民基本台帳事務に係る負担軽減方策

課題：住民票の写しは、年間約4,098万件（令和５年）が窓口で交付されている。

- 行政機関は、住基ネットで４情報（氏名・生年月日・性別・住所）を確認可能。既に住基ネットを利用可能な機関において**住基ネットの利用を徹底。**
- 民間事業者は、マイナンバーカードや電子証明書により、４情報を確認可能。**カード機能のスマートフォン搭載や、住所変更情報等を事業者に提供する最新４情報提供サービスの普及を促進。**
- **コンビニ交付の利用率向上のため、先進的取組**（期間限定で料金引下げ、広報動画配信等）**を周知・横展開。小規模団体の負担軽減のため、費用負担構造の見直しを検討**（負担金への従量制導入等の検討）。
- 本人確認書類である**住民票の写しをPDF化し電子交付することは、複製によるなりすまし等のリスクが大きい。本人の情報を電子送信する最新技術**（Verifiable Credential※等）**の活用可能性を、引き続き検討。**

※電子的に発行された証明書情報を本人が端末で管理し、当該情報のうち必要なものを電子的に相手方に提供するもの。

デジタル技術を活用した効率的・効果的な住民基本台帳事務等のあり方に関するワーキンググループ 中間とりまとめ（概要）



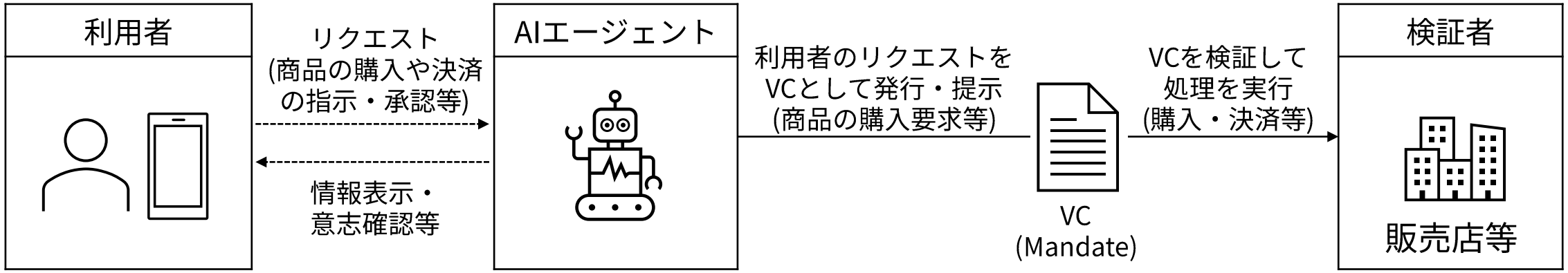
○　以上を踏まえると、紙媒体で交付されている住民票の写しを、そのまま PDF 化して電子交付することは、個人情報保護に関するリスクが大きいと考えられる。一方で、今後、マイナンバーカードのスマートフォン搭載で利用される「mdoc」やワクチン接種証明書で使われた VC（Verifiable Credential）[27]等の技術やその利用が進展することが見込まれる。このような状況を踏まえ、本人の情報を相手方に電子的に送信する最新技術に関して、住民票の写しの情報についても活用可能か、デジタル庁における議論も踏まえ[28]、引き続き検討を行うことが必要である。その際には、前述した、なりすましや不要な情報が相手方に渡るリスクを最小化できるかといった観点のほか、費用対効果や官民におけるユースケースに合致するかという点を踏まえて、現場の実態に即した検討を行うべきである。

デジタル技術を活用した効率的・効果的な住民基本台帳事務等のあり方に関するワーキンググループ 中間とりまとめ（令和7年6月）（全体版）

期待例②：AIエージェント

- **AIエージェントによるVCの活用の可能性も注目されている**（現時点では発展途上）
  - Googleは2025年9月、主要な決済・テクノロジー企業と共同開発した、AIエージェントによる安全な決済取引を実現するオープンプロトコル「Agent Payments Protocol (AP2)」※1を発表した。
  - 旅行・施設の予約やECサイトでの商品購入等、日常的で複雑なタスクをAIエージェントが自動的に代行する場面で、ユーザーはAIエージェントに対し「△△の商品を購入してほしい」等の指示を与えるとともに、指示の正当性を証明する「マンデート（Mandate）」をVCとして発行する。
  - サービス提供者側は、VCの提示を受けて、AIエージェントの行為がユーザーに正当に許可されていると検証でき、取引における安全性と信頼性を確保することができる。

AP2（Agent Payments Protocol）を用いたVC活用例の簡略図



（参考）直近のVC活用への期待の高まり

DIW・VCに関する諸外国の動向

- EUでは2024年4月にEuropean Digital Identity Framework （eIDAS 2.0）が公布された。また、米国では州発行の運転免許証をスマートフォンに保存できる「モバイル運転免許証（mDL）」の導入が進められている。
- DIWの実装に関係する技術要素は、一部がISO化されるなど、各標準化団体等における取組※が進められている。

EUでの主な動向

EU DIWの取組が進行

- EU DIWはEU域内でのデジタルIDの相互認証による利便性・効率性の実現などを目指すもの
- 2024年4月にEuropean Digital Identity Frameworkが公布、全ての加盟国に対してDIWの提供等が義務付けられた
- 既にDIWの展開を複数の国において開始している
- 技術実装リファレンスであるARFや、実施規則案であるImplementing Actsが順次公開
- 2023年よりLSP（Large Scale Pilots）が行われ、デモ動画などが公開

米国での主な動向

モバイル運転免許証の導入が進む

- 顧客体験の向上や不正の減少などのメリットの享受を目指し、2025年3月時点で少なくとも15の州にてモバイル運転免許証（mDL）の導入が進んでいる
- 政府機関（NCCoE)と15の企業等で金融サービスでのmDL活用に関する共同研究プロジェクトが2024年より始動

その他の動向

英国、GOV.UK Walletを今年導入予定

- デジタル運転免許証と退役軍人カードを政府の新たなスマートフォンアプリであるGOV.UK Walletに保管できるようになる
- 運転免許の提示や、年齢制限のある商品購入時の年齢証明が容易にできるようになる
- デジタルパスポートの導入も検討

画像出典：UK government reveals mDL pilot, Gov.uk digital wallet plans | Biometric Update

※代表例として、ISO/IEC 18013-5:2021（mDL）、W3C Verifiable Credentials Data Model、OpenID for Verifiable Credential Issuance　等

Educational Credentialsの日・EU相互運用実証の背景と期待

政策背景

- データの連携・利活用の基盤として、やりとりをする相手やそのデータについての「トラスト」、例えば**主体の本人性・実在性やデータの非改竄性・真正性に関する検証可能性**を向上する仕組み・ツール等が求められている。
- 「トラスト」の論点の中でも、個人・法人等の主体については、本人性や実在性だけでなく、**属性情報（どのような主体か）が多くのデータ利活用の場面で必要**。
- デジタルにおいて主体の属性を確立・証明するデジタル・アイデンティティの利活用は、デジタル社会におけるトラストを確保・向上するための基礎であり重要な要素である。

デジタル・アイデンティティの国際互運用実証に関する経緯と期待

- 本実証は、**デジタル・アイデンティティの国際相互運用を実現する、我が国として初のユースケース創出**を目指し、2024年日EUデジタルパートナーシップの下で結んだMoCに基づき、将来的な実装を目指して行うものである。

> デジタル・アイデンティティとトラストサービスに関するMoC[1]　抜粋
> Both sides intend to explore use cases on business activities and student exchanges in cooperation with the European Commission and Ministry of Education, Culture, Sports, Science and Technology, Japan. This work would be initiated in the course of 2024.

- また現在、データ連携・利活用における「トラスト」に関する国際相互運用の必要性やその実現方法が議論されている。
- そこで**異なるガバナンス（法令・制度）および技術的構造をもった国同士でも、デジタル・アイデンティティの相互運用性が確保可能と示すことを目指す**本実証の成果は、「トラスト」に関する国際相互運用の議論全体にも資することが期待される。

[1]河野デジタル大臣はブルトン欧州委員と会談を行い、 欧州連合（EU）とデジタル・アイデンティティに関する協力覚書を交わしました｜デジタル庁

令和7年度重点計画及び2025年日EU閣僚級会合共同声明

- 本年の日EU閣僚級会合における共同声明において、本実証を開始する予定であることを、
  電子署名もしくはeシールが付与されているVCとウォレットを実証で使用する旨、
  異なるガバナンスや技術的構造を持つ国同士でも国際的な相互運用性を確保できる方法を示すことを目指す旨と共に明記

（参考）第 3 回 日 EU デジタルパートナーシップ閣僚級会合における共同声明[3]　抜粋
To pave the way for interoperability and mutual recognition of academic credentials through digital identity and trust services, both sides welcome the formulation of a scoping document based on which **a pilot project could be launched to assess the technical feasibility**. The scoping document involved that the project would use wallet infrastructures and verifiable credentials signed or sealed electronically in accordance with respective regulations. **Through the project, both sides aim to demonstrate how cross-border interoperability could be ensured among countries with different governance and technological architectures**.

- また、令和7年度重点計画において、**国際的なデータ連携において求められるトラストについては、日 EU等の様々な政府間対話の機会を捉えて国際的にも通用するものにする**こと等を記載

（参考）令和7年度　デジタル社会の実現に向けた重点計画[2]　抜粋
産業界からの要請が強いトラストについても、データ連携で必要となるトラストについて体系的に考え方・在り方を整理したフレームワークとしてトラスト基盤を整備して、トラストを確保するための手法の体系化を図るとともに適切に選択して組み合わせられるようにする。公的な法人認証が必要となるケースに対応するためにGビズ ID の認証機能の活用を候補の1つとして検討することや、新たな手法を柔軟に取り入れる等、最適な形での制度的技術的な整備を進め、トラスト基盤を更新する。国際的なデータ連携において求められるトラストについては、日 EU、日 ASEAN 等の様々な政府間対話の機会を捉えて国際的にも通用するものにする。また、Digital Identity Walletや Verifiable (Digital) Credential等のデジタル・アイデンティティの新しい仕組みの社会実装に向けたガバナンスの在り方を検討するとともに、例えば行政におけるユースケースの創出に取り組むなど、トラストを確保できる環境を充実させる。

※いずれも下線は本資料用に追記

[2]日EUデジタルパートナーシップ閣僚級会合（第3回会合）を開催しました｜デジタル庁
[3]デジタル社会の実現に向けた重点計画｜デジタル庁

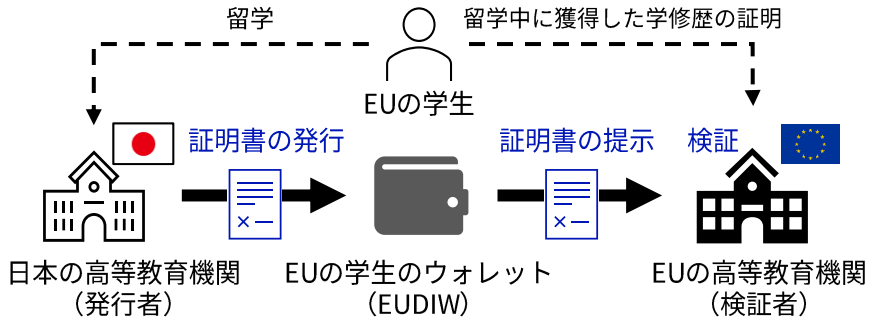
実証対象とする具体なユースケース（イメージ）

- 相互運用実証として、具体には**交換留学などの場面を想定した以下のようなユースケース**について実証することを想定。
  - 日本側が実証する主なアクションは、
    ①のうち、日本の高等教育機関（発行者）がEUDIW（ウォレット）に教育クレデンシャルを発行すること
    ②のうち、日本の学生（所有者）の持つ日本側のウォレットから、日本の高等教育機関へ教育クレデンシャルを提示し、
    日本の高等教育機関（検証者）が提示されたクレデンシャルを認証し、教育クレデンシャルの有効性を検証すること

- EUDIWとの相互運用性の実証によって、**異なるガバナンス（法令・制度）や技術的構造を持つ国同士でも相互運用性が確保可能であることを示す**

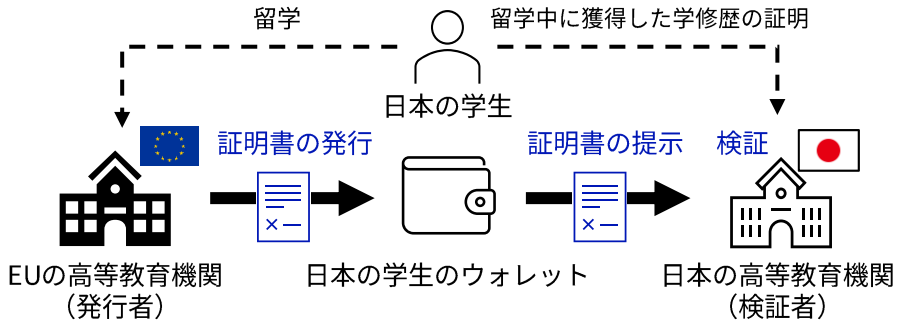
❶日⇒EUのユースケース

- 日本の高等教育機関が、日本の高等教育機関に留学に来たEUの学生のウォレット（EUDIW）に教育クレデンシャルを発行
- EUの学生はEUの高等教育機関に戻り、その教育クレデンシャルをEUの高等教育機関に提示し、EUの高等教育機関が証明書や発行元を検証



❷EU⇒日のユースケース

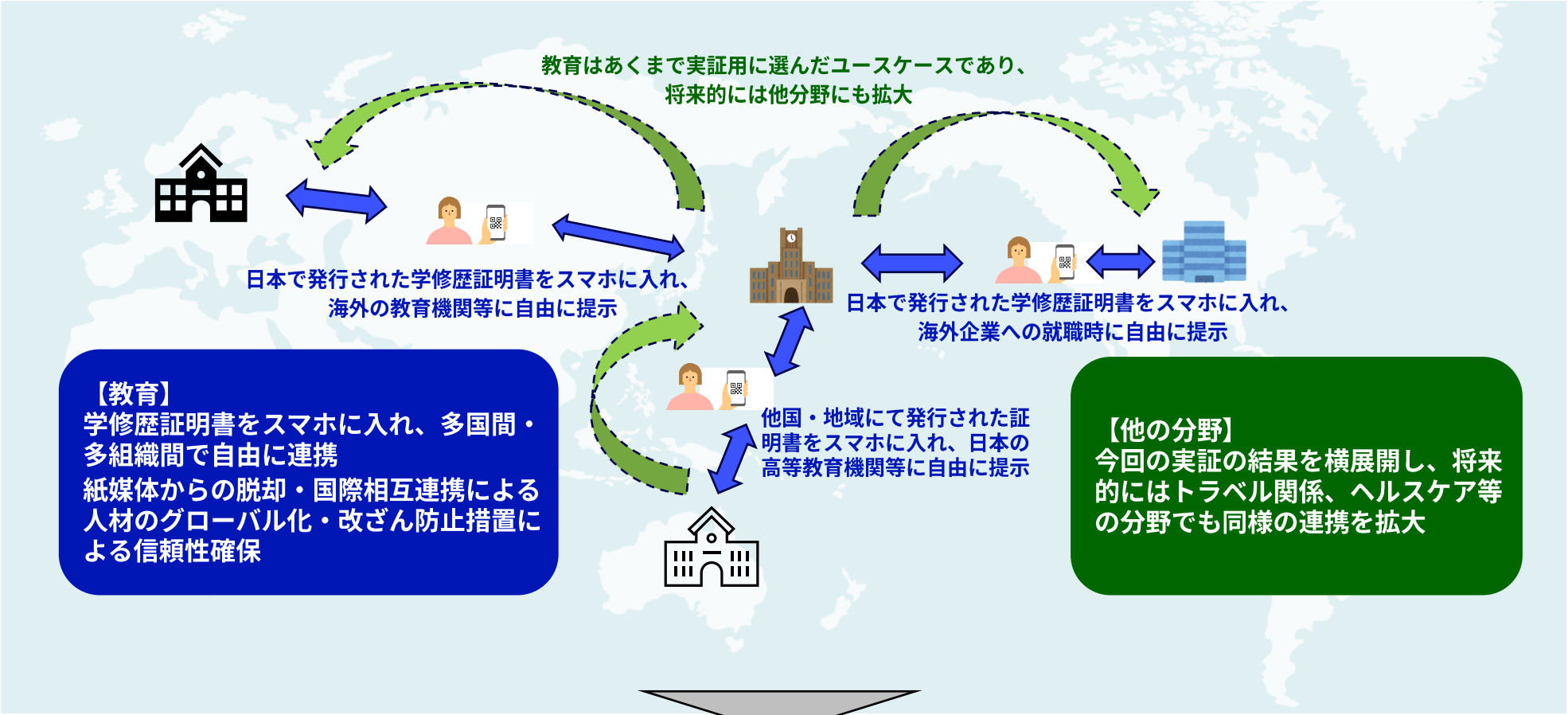
- EUの高等教育機関が、EUの高等教育機関に留学に来た日本の学生のウォレットに教育クレデンシャルを発行
- 日本の学生は日本の高等教育機関に戻り、その教育クレデンシャルを日本の高等教育機関に提示し、日本の高等教育機関が証明書や発行元を検証



※　あくまでも概要のイメージであり、ユースケースの具体は日EU間で議論中であり、変更の可能性がある。

将来的な理想像

- 日EUに留まらず、他国・地域間におけるデジタル・アイデンティティの相互運用性を確保し、各国で進められているDIWなどの取組と協調しつつ取り組むことで、**行政・民間の証明書を国境を越えて相互運用できる環境を作り、国を跨いだ移動・活動の利便性の向上を目指す**。



デジタル庁
Digital Agency