DS-511/512 政府機関における本人確認ガイドライン

2026年6月17日 デジタル庁　アイデンティティユニット　アイデンティティスペシャリスト
山田　達司

デジタル庁
Digital Agency

自己紹介:山田　達司

デジタル庁　アイデンティティユニット　アイデンティティスペシャリスト(2021/10～)
- 政府機関における本人確認ガイドラインの改定(DS-500→DS-511/512)
- 法人共通認証基盤Gビズ IDの機能改善

先進ITデバイス と セキュリティ による 働き方改革 が専門

物理世界の私

先進ITデバイス(AR/VR)
- 2000年頃の電子手帳ブームにPalm用日本語化ソフトの開発、書籍執筆、開発コミュニティ支援により「Palmの神様」と呼ばれる。ネット用語「神降臨」の元祖と言われる
- FY2017～ VRによるビジネスメタバース「フルデジタルオフィス」の開発

セキュリティ(Identity Management)
- NTTデータ/データグループにおける認証基盤の開発と運用
- 上記をVANADISとしてソリューション化、企画、販売、PM
- Kantara Initiative, JNSA Digital Identity WGなどで活動

働き方改革(テレワーク)
- 総務省「テレワークセキュリティガイドライン」委員等テレワーク普及に尽力
- 経団連と連携し「研究開発における技適の適用緩和」を提言し実現。これにより、発売直後のApple Vision Pro/Ray-ban Meta等が日本で利用可能に

オンライン
ビジネスの私

オンライン
オフの私

自己紹介:山田　達司

デジタル庁　アイデンティティユニット　アイデンティティスペシャリスト(2021/10～)

- 政府機関における本人確認ガイドライン
- 法人共通認証基盤GビズIDの機能改善

先進ITデバイス と セキュリティ による 働き

ネット用語「神降臨の元祖」

物理世界の私

先進ITデバイス(AR/VR)

- 2000年頃の電子手帳ブームにPalm用日本語化ソフトの開発、書籍執筆、開発コミュニティ支援により「Palmの神様」と呼ばれる。ネット用語「神降臨」の元祖と言われる
- FY2017～ VRによるビジネスメタバース「フルデジタルオフィス」の開発

セキュリティ(Identity Management)

- NTTデータ/データグループにおける認証基盤の開発と運用
- 上記をVANADISとしてソリューション化、企画、販売、PM
- Kantara Initiative, JNSA Digital Identity WGなどで活動

働き方改革(テレワーク)

- 総務省「テレワークセキュリティガイドライン」委員等テレワーク普及に尽力
- 経団連と連携し「研究開発における技適の適用緩和」を提言し実現。これにより、発売直後のApple Vision Pro/Ray-ban Meta等が日本で利用可能に

オンライン
ビジネスの私

オンライン
オフの私

IPAによるセキュリティ10大脅威2026

IPAによるセキュリティ10大脅威2026（個人）

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	7年連続10回目
インターネット上のサービスへの不正ログイン	2016年	11年連続11回目
インターネットバンキングの不正利用	2016年	4年ぶり8回目
クレジットカード情報の不正利用	2016年	11年連続11回目
サポート詐欺（偽警告）による金銭被害	2020年	7年連続7回目
スマホ決済の不正利用	2020年	7年連続7回目
ネット上の誹謗・中傷・デマ	2016年	11年連続11回目
フィッシングによる個人情報等の詐取	2019年	8年連続8回目
不正アプリによるスマートフォン利用者への被害	2016年	11年連続11回目
メールやSNS等を使った脅迫・詐欺の手口による金銭要求	2019年	8年連続8回目

大多数がデジタルアイデンティティ関係！

デジタルアイデンティティの正しい理解なくして、セキュリティは守れない！

デジタルアイデンティティに対する脅威

デジタルアイデンティティに関連する脅威

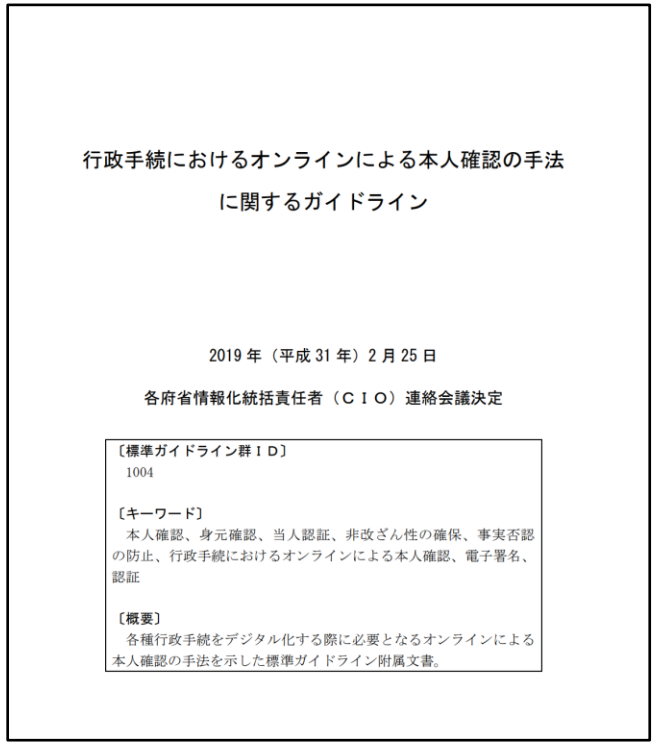
※IPAによるセキュリティ10大脅威2026をもとに作成：
https://www.ipa.go.jp/security/10threats/10threats2026.html

1. 本人確認ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
4. 解説書における追加内容

前版　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-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」（以下「本人確認ガイドライン」という。）は、各府省が行政手続をデジタル化する際の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文書。米NISTによるSP 800-63-3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（身元確認及び当人認証）手法を掲載し、**2019年**に発行。（以降前版）

近年の本人確認を取り巻く環境変化を踏まえ、**2022年度**から改定の検討を開始し、**2025年度**に改訂。



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（平成 31 年）2 月 25 日

各府省情報化統括責任者（ＣＩＯ）連絡会議決定

〔標準ガイドライン群ＩＤ〕
1004

〔キーワード〕
本人確認、身元確認、当人認証、非改ざん性の確保、事実否認の防止、行政手続におけるオンラインによる本人確認、電子署名、認証

〔概要〕
各種行政手続をデジタル化する際に必要となるオンラインによる本人確認の手法を示した標準ガイドライン附属文書。

サービス・技術の変化

- 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のIDプロバイダの登場
- パスキーなど強固な認証技術の登場　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（本人確認書類）の偽造攻撃の増加　等

本人確認ガイドライン：本編と解説書

- 「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に関するガイドライン 解説書」（以下「ガイドライン解説書」又は「解説書」といいます。）は、本人確認に関する最新動向、本人確認ガイドライン本編の記載内容の解説、採用候補となる手法の具体例、検討にあたる留意点等をまとめた文書。
- 本編が記載内容への順守を求める「Normative」であるのに対し、解説書は参考情報「Informative」の位置づけとし、本編よりも短期間での改定を行うことで、今後の動向変化にも柔軟に対応可能。

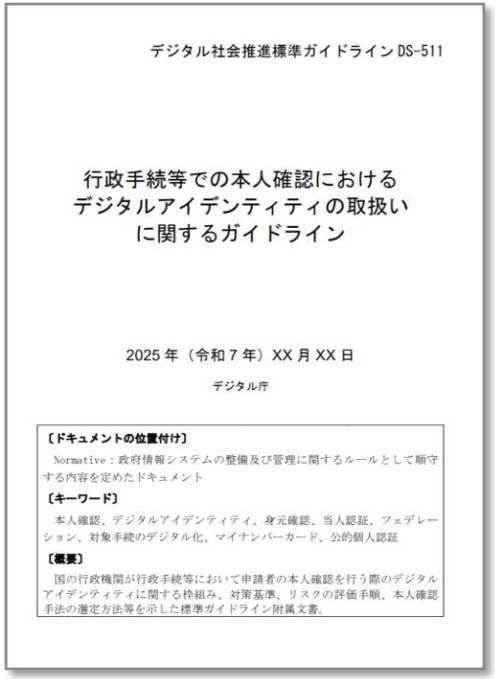
DS-511 本人確認ガイドライン 本編

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、原則的な情報をとりまとめる

本編はできる限りシンプルな内容に留め、詳細情報、状況が短期的に変わり得る具体手法、その他の動向等に関する情報は「解説書」として別途とりまとめる

比較的長期間の改定サイクルを想定


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。

DS-512 本人確認ガイドライン 解説書

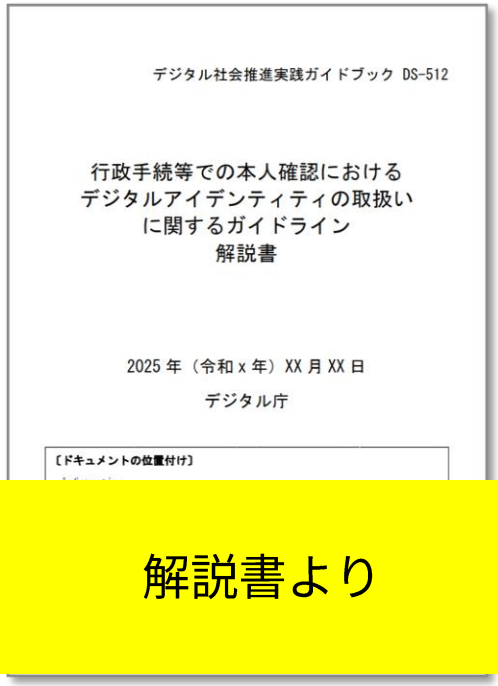
位置づけ：Informative
（参考情報）

本人確認ガイドライン本編の参考資料として、

- 本人確認に関する最新動向
- 本編の記載内容の解説
- 採用候補となる具体的手法
- 検討にあたる留意事項

等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


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

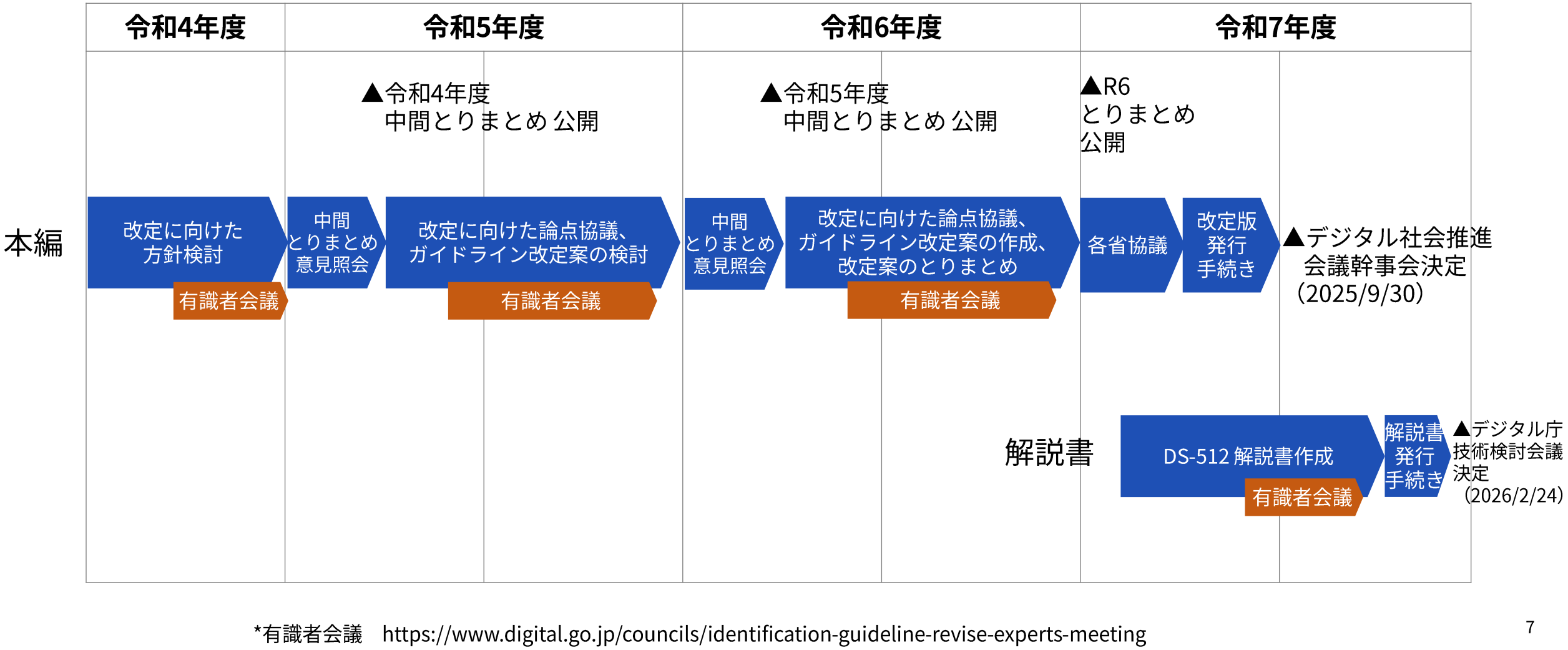
2025 年（令和 x 年）XX 月 XX 日

デジタル庁

【ドキュメントの位置付け】

解説書より

ガイドライン本編及び解説書策定スケジュール



*有識者会議　https://www.digital.go.jp/councils/identification-guideline-revise-experts-meeting

本人確認ガイドライン本編に関する有識者会議メンバー

（敬称略・五十音順。所属は2024/9時点のもの）

勝原 達也	アマゾン ウェブ サービス ジャパン合同会社 Specialist Solutions Architect, Security
後藤 聡	TOPPANエッジ株式会社 事業推進統括本部 DXビジネス本部 RCS開発部 部長
﨑村 夏彦	OpenID Foundation Chairman
佐藤 周行	国立情報学研究所アーキテクチャ科学研究系 教授
新崎 卓	株式会社Cedar 代表取締役
肥後 彰秀	株式会社TRUSTDOCK 取締役
富士榮 尚寛	OpenIDファウンデーションジャパン代表理事
満塩 尚史	順天堂大学 健康データサイエンス学部 健康データサイエンス学科　准教授 理学博士
南井 享	株式会社ジェーシービー イノベーション統括部 市場調査室 部長代理
森山 光一	株式会社NTTドコモ チーフセキュリティアーキテクト FIDOアライアンス執行評議会・ボードメンバー・FIDO Japan WG座長 W3C, Inc.理事（ボードメンバー）

本人確認ガイドライン解説書に関する有識者会議メンバー

（敬称略・五十音順。所属は2025/9時点のもの）

狩野 達也	株式会社メルカリ Foundation and Identity Principal Engineer
後藤 聡	TOPPANエッジ株式会社 データマネジメント統括本部 DXビジネス本部 RCS開発部 部長
﨑村 夏彦	NATコンサルティング合同会社 代表社員
佐藤 周行	国立情報学研究所 教授（トラスト・デジタルID基盤研究開発センター センター長）
新崎 卓	株式会社Cedar 代表取締役
肥後 彰秀	株式会社TRUSTDOCK 取締役
富士榮 尚寛	OpenIDファウンデーションジャパン代表理事
満塩 尚史	順天堂大学 健康データサイエンス学部 健康データサイエンス学科　准教授
南井 享	株式会社ジェーシービー イノベーション統括部 市場調査室 部長代理
森山 光一	株式会社NTTドコモ チーフセキュリティアーキテクト FIDOアライアンス執行評議会・ボードメンバー・FIDO Japan WG座長 W3C, Inc.理事（ボードメンバー）

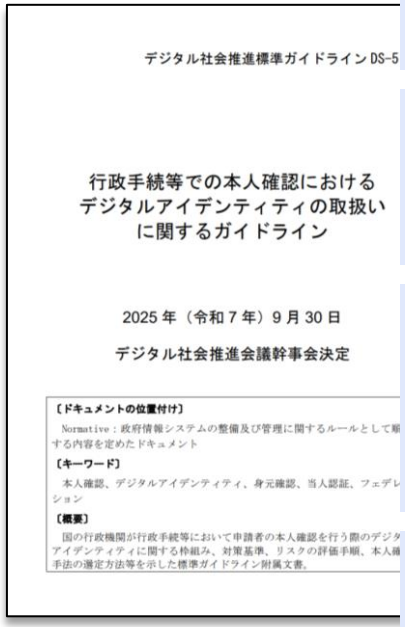
1. 本人確認ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
4. 解説書における追加内容

解説書より

全体構成

本編の目次構成及び記載内容は以下の通り。

DS-511 本人確認ガイドラインの全体構成


デジタル社会推進標準ガイドライン DS-5

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）9 月 30 日

デジタル社会推進会議幹事会決定

【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
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
ション
【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
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
手法の選定方法等を示した標準ガイドライン附属文書。

1 はじめに
1.1 背景と目的／1.2 適用対象／1.3 位置づけ／1.4 用語／1.5 基本的な考え方

2 本人確認の基本的枠組み
2.1 本人確認の構成要素
2.2 本人確認の実装モデル

3 本人確認における脅威と対策
3.1 身元確認（Identity Proofing）
3.2 当人認証（Authentication）
3.3 フェデレーション（Federation）

4 本人確認手法の検討方法
4.1 対象手続の保証レベルの判定
4.2 本人確認手法の評価と決定
4.3 継続的な評価と改善

各章の記載内容のポイント

- 本人確認ガイドラインの**改定の背景**
- 検討にあたる**「基本的な考え方」**

- 本人確認を構成する**３つの要素**（身元確認、当人認証、フェデレーション）
- システムでの**実装モデルのパターン**

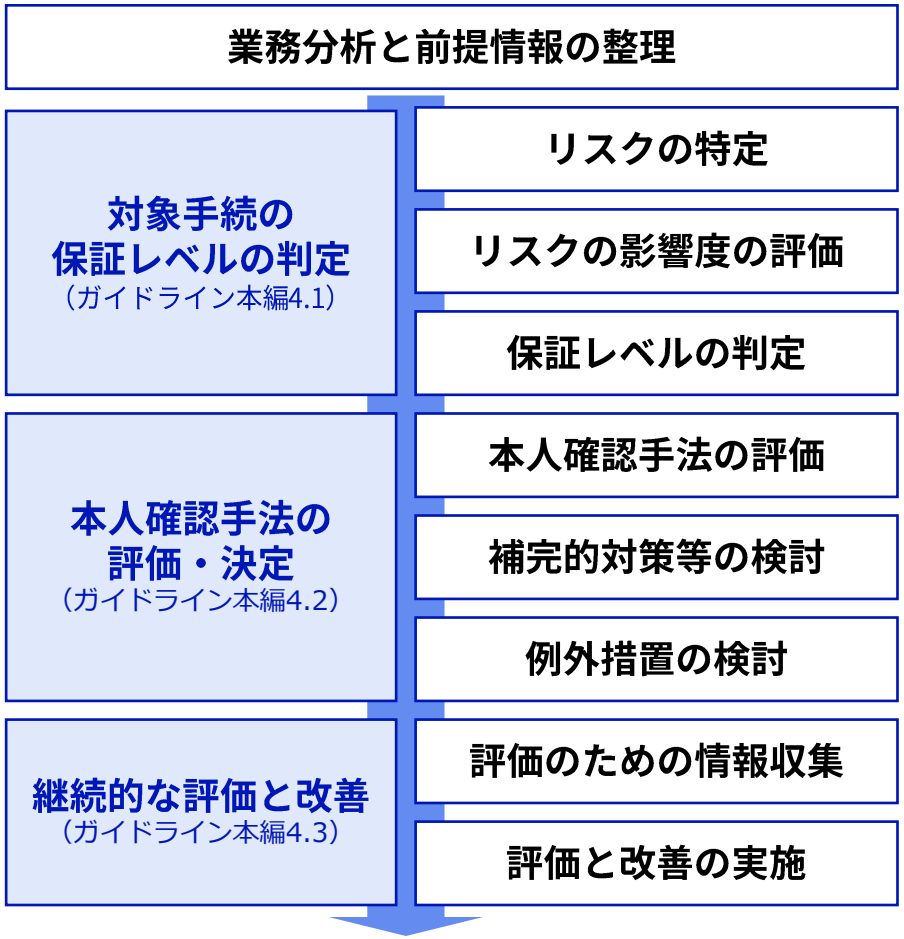
- 身元確認、当人認証、フェデレーションのそれぞれで**想定されるリスクと対策**
- ３段階の**保証レベルと対策基準**の定義
- 検討すべき**「個別検討事項」**

- リスク評価による**保証レベルの判定手順**
- 「基本的な考え方」の5つの観点を踏まえた**本人確認手法の選定手順**

解説書より

本人確認手法の検討プロセスの全体像

- 解説書の４章では、ガイドライン本編の４章の全体フローと各検討プロセスについて、検討にあたる基本的な考え方や、検討の参考となる情報を掲載している。



業務分析を行い、一連のリスク分析に必要となる情報を収集・整理・明文化する。

対象手続の機能やサービス等を踏まえつつ、本人確認のリスクを特定する。

特定したリスクが顕在化した場合の影響 度の大きさを3 段階で評価する。

影響度の評価結果に基づき、対象手続に 求められる保証レベルを判定する。

採用候補とする本人確認手法を選定し、事業目的の遂行、公平性等の観点での影響を評価する。

手法の評価結果を踏まえ、懸念される影響を軽減するための補完的対策を検討する。

本人確認における例外ケースを想定し、 必要な例外措置を検討する。

本人確認手法の評価と改善に必要となる 情報を検討し、運用期間中における情報収集を行う。

収集した情報を基に本人確認手法の評価 を行い、必要に応じて改善措置を講じる。

FY2025版ガイドラインにおける主な改訂内容

ガイドラインの目次

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

1　はじめに
- 1.1　背景と目的
- 1.2　適用対象
- 1.3　位置づけ／1.4　用語
- 1.5　基本的な考え方

2　本人確認の基本的枠組み
- 2.1　本人確認の構成要素
- 2.2　本人確認の実装モデル

3　本人確認における脅威と対策
- 3.1　身元確認（Identity Proofing）
- 3.2　当人認証（Authentication）
- 3.3　フェデレーション（Federation）

4　本人確認手法の検討方法
- 4.1　対象手続の保証レベルの判定
- 4.2　本人確認手法の評価と決定
- 4.3　継続的な評価と改善

主な改定ポイント

① ガイドラインの適用対象と名称の見直し
- 適用対象の拡大
- ガイドライン名称の変更

② 検討にあたる基本的な考え方を定義
- 5つの観点：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、セキュリティの定義

③ 本人確認の基本的な枠組みを定義
- 身元確認、当人認証、フェデレーションの概念の定義
- 実装モデル：連携モデル／非連携モデルの定義

④ 脅威と対策の最新化、保証レベルの見直し
- 脅威と手法例の最新化
- 保証レベルの位置づけと対策基準の見直し

⑤ リスク評価プロセスの見直し
- 本人確認手法を5つの観点から評価するプロセスを追加
- リスク評価プロセスの単純化

1. ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
   - **① ガイドラインの適用対象と名称の見直し**
   - ② 検討にあたる「基本的な考え方」を定義
   - ③ 本人確認の基本的な枠組みを定義
   - ④-1 保証レベル見直し－身元確認
   - ④-2 保証レベル見直し－当人認証
   - ④-3 保証レベル見直し－フェデレーション
   - ⑤ リスク評価プロセスの見直し
4. 解説書における追加内容

3. ガイドラインの主な改正点
① ガイドラインの適用対象と名称の見直し

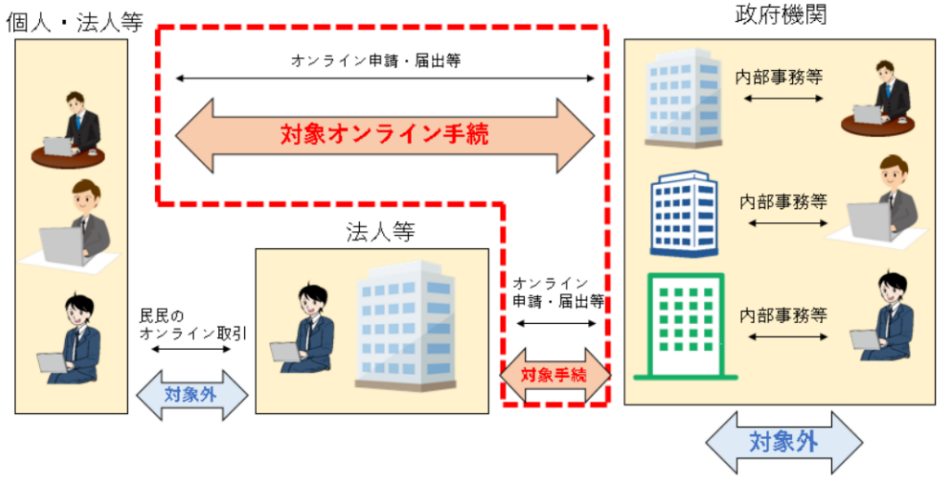
適用対象

- 前編※は「オンラインによる本人確認」のみを対象としていたが、対面での本人確認における脅威の高度化の傾向や、デジタル技術を活用した本人確認手法が対面の手続においても広く利用可能となっている状況等を考慮し、令和7年の改定において適用対象を見直し、対面及び郵送での手続き・サービスを追加。

※ 従前の本人確認ガイドライン：DS-500-1 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

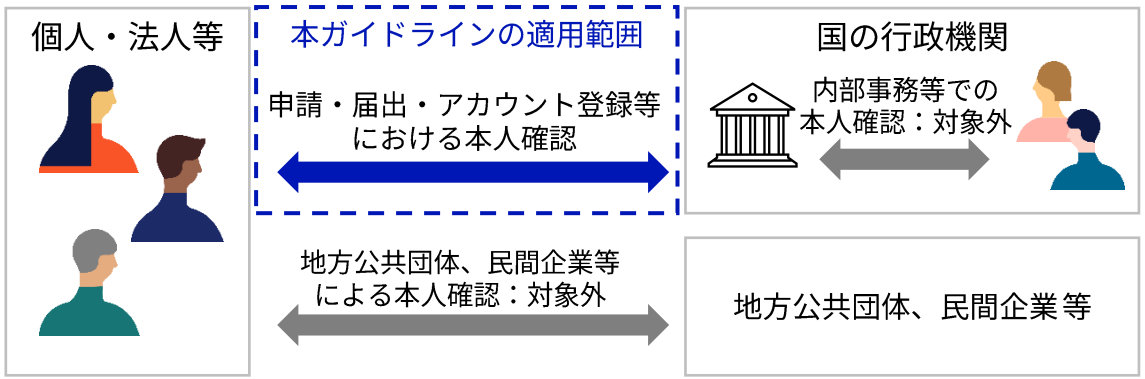
従前の本人確認ガイドラインの適用対象（概要）

- 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



改定後の本人確認ガイドラインの適用対象（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）



3. ガイドラインの主な改正点
① ガイドラインの適用対象と名称の見直し

ガイドライン名称の見直し

- ガイドラインの名称は、改定後の内容に合致するよう以下のとおり変更した。
- あわせてトラスト関連ガイドライン群の採番体系を見直し、文書番号もDS-500からDS-511へと変更。

旧版：「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-500 → 採番体系の見直し
- 行政手続 → 行政手続以外のサービスにも拡大
- オンラインによる → 対面を適用対象に含めるため削除
- 本人確認の手法 → フェデレーションなどの新規導入を踏まえ、より広い概念を示す名称に変更

改定後：
「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-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」

500 番台	トラストおよびデジタルアイデンティティ関連ドキュメント全般
510 番台	デジタルアイデンティティに関するドキュメント
520 番台	プライバシーに関するドキュメント
530 番台	トラストに関するドキュメント

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 より

1. ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
   - ① ガイドラインの適用対象と名称の見直し
   - **② 検討にあたる「基本的な考え方」を定義**
   - ③ 本人確認の基本的な枠組みを定義
   - ④-1 保証レベル見直し－身元確認
   - ④-2 保証レベル見直し－当人認証
   - ④-3 保証レベル見直し－フェデレーション
   - ⑤ リスク評価プロセスの全面的な見直し
4. 解説書における追加内容

「基本的な考え方」の解説

- 本人確認手法は、単にセキュリティレベルの高い手法を選べばよいというものではない。事業目的の遂行、公平性、プライバシー、アクセシビリティ及びユーザビリティといった多角的な視点からの検討が必要。

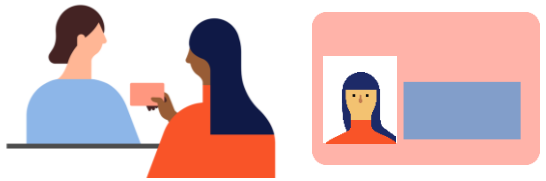
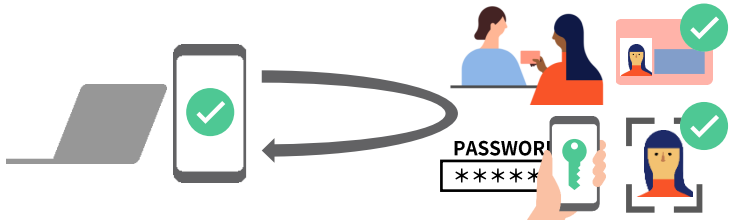
「1.5　基本的な考え方」として定義する５つの観点（概要）

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) アクセシビリティ及びユーザビリティ	• アクセシビリティやユーザビリティが悪いと、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。

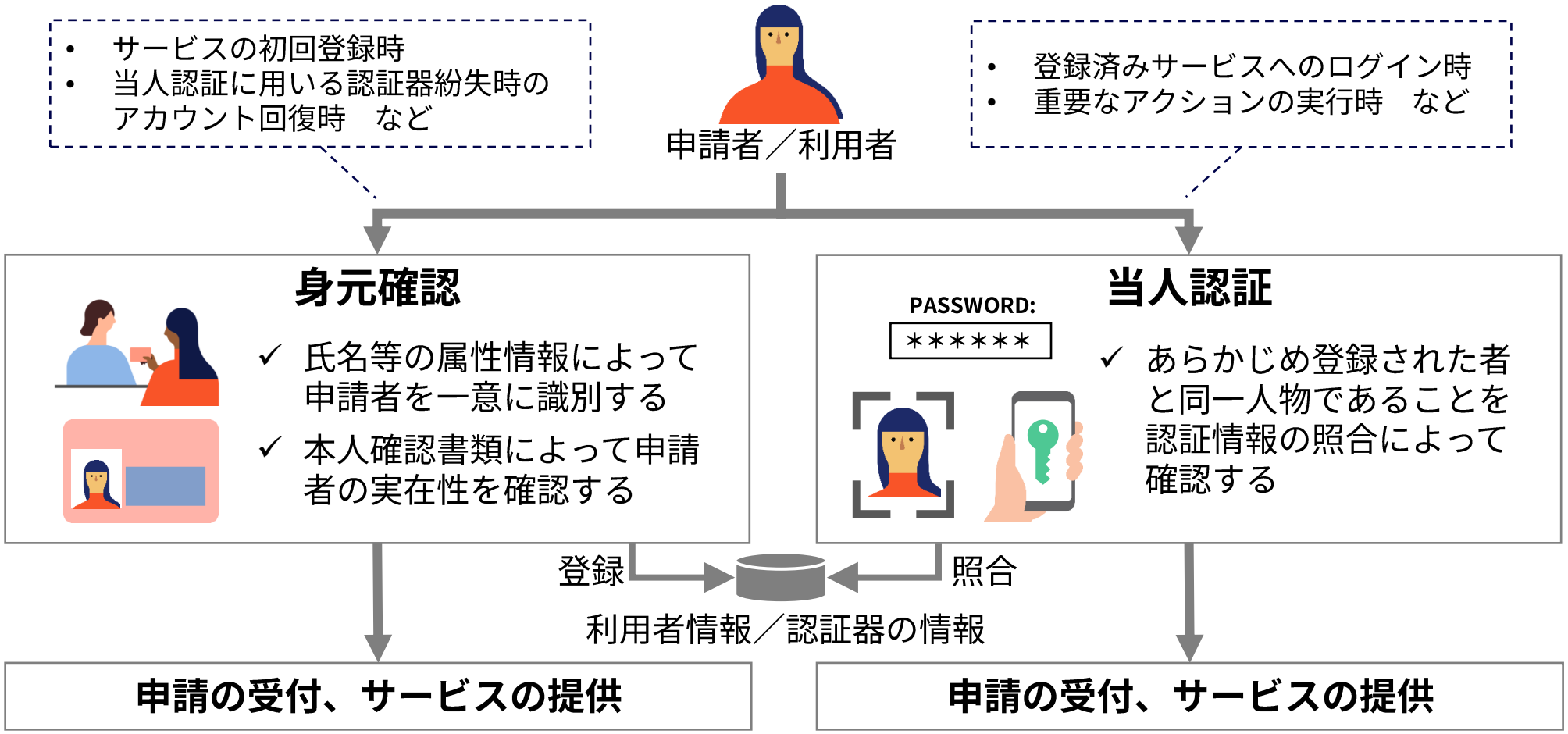
1. ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
   ① ガイドラインの適用対象と名称の見直し
   ② 検討にあたる「基本的な考え方」を定義
   ③ 本人確認の基本的な枠組みを定義
   ④-1 保証レベル見直し－身元確認
   ④-2 保証レベル見直し－当人認証
   ④-3 保証レベル見直し－フェデレーション
   ⑤ リスク評価プロセスの全面的な見直し
4. 解説書における追加内容

本人確認の基本的要素を定義

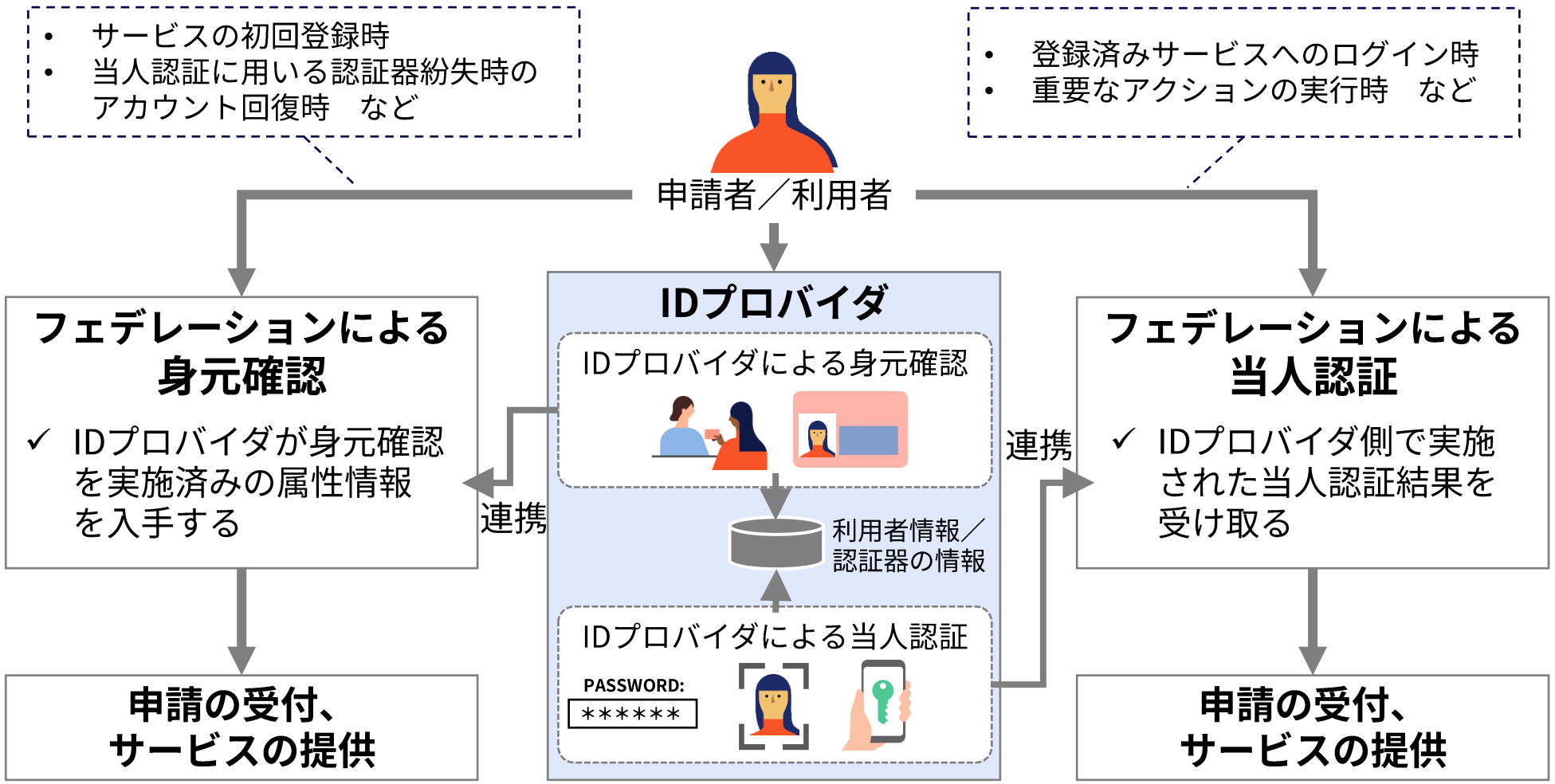
- 本人確認の構成要素である「身元確認」と「当人認証」を明確に定義し、概念図を示す。
- また、身元確認や当人認証を他者に依拠して実現する「フェデレーション」という概念を、今回の改定において新たに定義する。

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。

身元確認及び当人認証の概念図

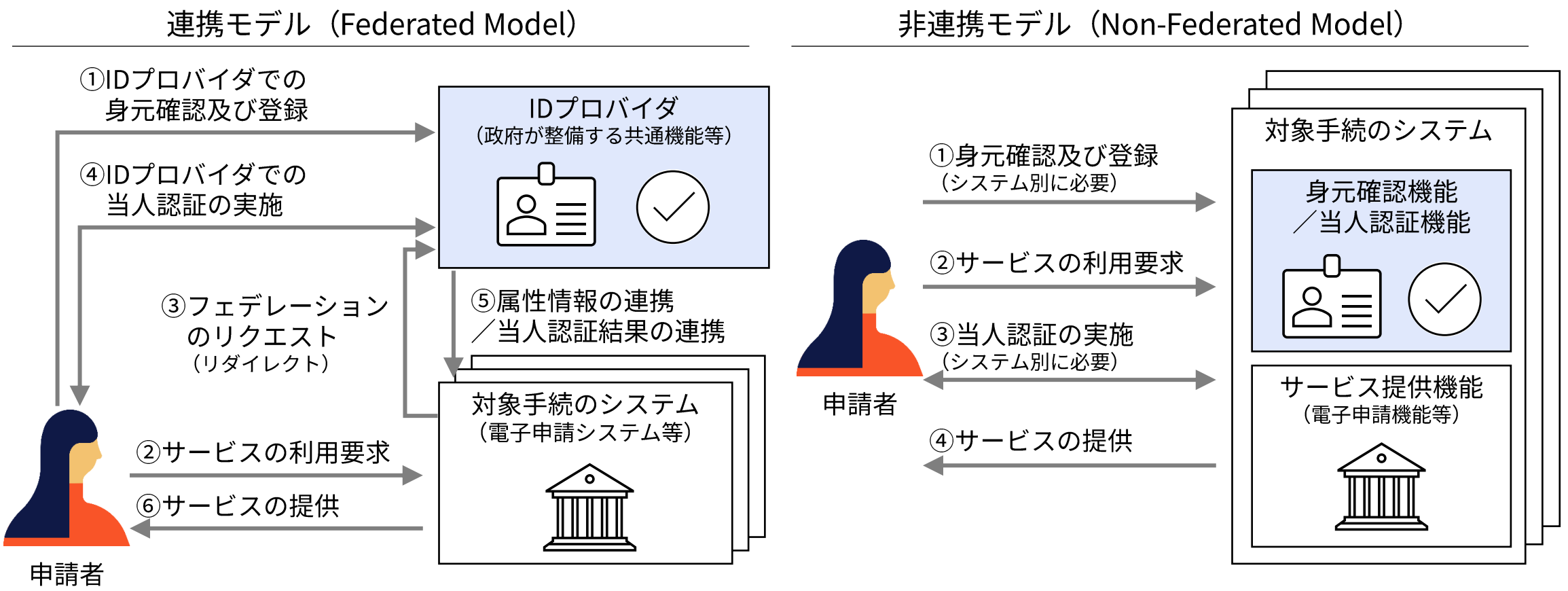


フェデレーションによる本人確認の概念図



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。

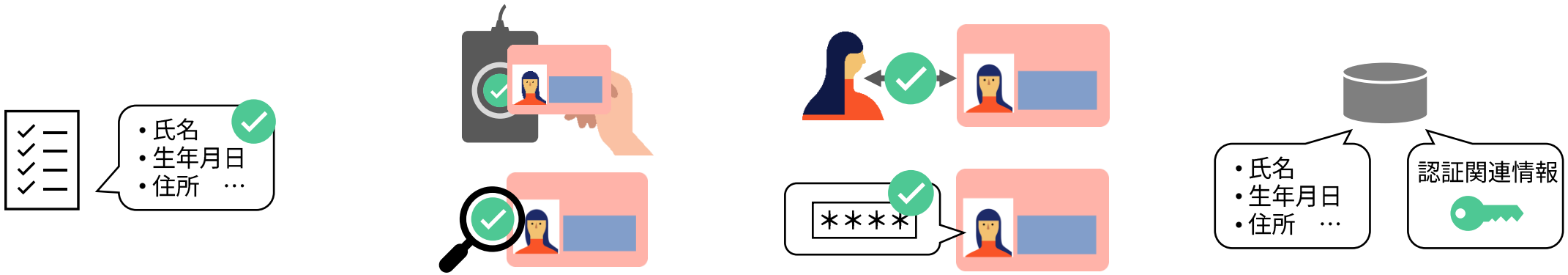


1. ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
   ① ガイドラインの適用対象と名称の見直し
   ② 検討にあたる「基本的な考え方」を定義
   ③ 本人確認の基本的な枠組みを定義
   ④-1 保証レベル見直し－身元確認
   ④-2 保証レベル見直し－当人認証
   ④-3 保証レベル見直し－フェデレーション
   ⑤ リスク評価プロセスの全面的な見直し
4. 解説書における追加内容

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。

身元確認における脅威の定義

- 身元確認における脅威を各プロセスと紐づけて定義。

No.	主な脅威	脅威の概要	対策プロセス
1	**重複登録**	申請情報の不足や誤り等によって、同一の申請者による重複申請を検知できずに受け付けてしまう	属性情報の収集
2	**別人との誤紐づけ**	申請情報の不足や誤り等によって、申請者と別の人物とを区別できなくなり、誤った人物の情報と紐づけてしまう	
3	**本人確認書類の偽造・改ざん**	偽造又は改ざんされた本人確認書類によって、実在する別の人物や架空の人物になりすまされる	本人確認書類の検証
4	**本人確認書類の複製**	電子的又は物理的に複製された本人確認書類によって、実在する別の人物になりすまされる	
5	**本人確認書類の盗用**	盗まれた本人確認書類によって、実在する別の人物になりすまされる	申請者の検証
6	**本人確認書類の貸し借り**	貸し借りされた本人確認書類によって、実在する別の人物になりすまされる	

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。

属性情報の収集手法例

a) 本人確認書類の電子的な読取り
- 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) 本人確認書類の物理的な読取り
- 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

本人確認書類の検証手法例

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) 券面の物理的検査（対面）
- 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) 券面の物理的検査（非対面）
- 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

申請者の検証手法例

a) 容貌の確認（対面）
- 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

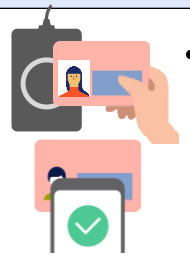
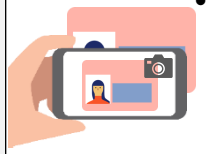
b) 容貌の確認（非対面）
- 本人確認書類の顔写真と申請者の容貌をカメラ映像等で比較する

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) 確認コードの送付による検証
- 本人確認書類に記載された住所等に確認コードを送付し、その入力をも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

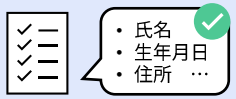
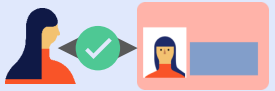
身元確認保証レベルの見直し　―　全体概要

- 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。）	 暗証番号: ＊＊＊＊ • 本人確認書類の盗用に対し、**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**物理的な券面の検査等も許容**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（非対面での券面検査）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、**非対面での券面検査（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、**本人確認書類に記載された住所等に確認コードを送付することでの間接的な検証**も許容する。 （例：当該住所に居住していることをもって、本人確認書類との紐づきを確認する 等）

身元確認保証レベルの見直し　―　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。
  ※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	本人確認書類の電子的な読取り	デジタル署名の検証	以下のいずれか • 容貌の確認（対面） • 容貌の確認（非対面） • 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** • **券面の物理的検査（対面）**	
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 • 券面の物理的検査（対面） • **券面の物理的検査（非対面）**	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 • **確認コードの送付による検証**

解説書より

身元確認に関する主な解説

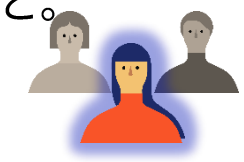
- 以下に示す「1) 身元確認において収集する属性情報の考え方」や「2) 身元確認において利用可能とする本人確認書類の考え方」は、身元確認の保証レベル、事業目的の遂行、公平性等に大きく影響する。

解説書における身元確認に関する解説 （一部抜粋・要約）

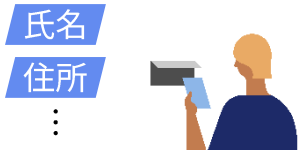
1) 身元確認において収集する属性情報の考え方

身元確認において収集する属性情報を検討する際の考え方として、以下の3つの条件を明示。

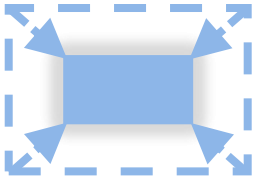
- その手続や行政サービスが扱う母集団の中で、申請者を一意に識別できる属性集合であること。
- その手続・サービスを提供するために必要な属性が含まれていること。
- プライバシー保護等の観点から、必要最小限であること。



母集団の中で申請者を一意に識別できること



手続やサービスの提供に必要な属性であること

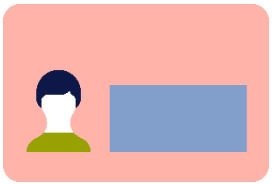
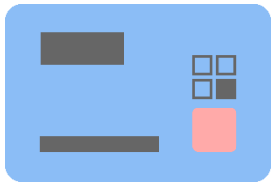


必要最小限であること

2) 身元確認において利用可能とする本人確認書類の考え方

身元確認においてどのような本人確認書類を利用可能とすべきかについて、以下の検討の観点を明示。

- **利用者層**：想定する利用者層における所持率・普及率
- **必要な属性情報**：身元確認に必要な属性が含まれているか
- **求められる保証レベル**：求められる身元確認保証レベルを満たすことができるか
- **信頼可能な発行元**：発行できる組織・機関から発行されたものであるか
- **対象手続の根拠法令**等：根拠法令上利用可能であるか

解説書より

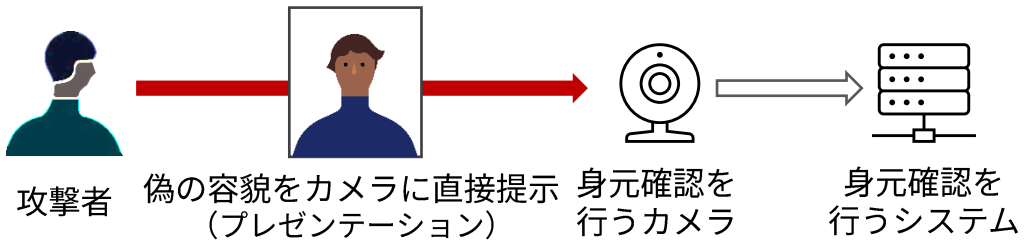
身元確認に関する主な解説

- カメラを利用したビデオベースの身元確認手法に関する特有の脅威として、「プレゼンテーション攻撃」と「ビデオインジェクション攻撃」を解説。ビデオベースの身元確認手法を利用する際は、これらの脅威に十分留意し、必要な対策を検討することが重要。

解説書における身元確認に関する解説 （一部抜粋・要約）

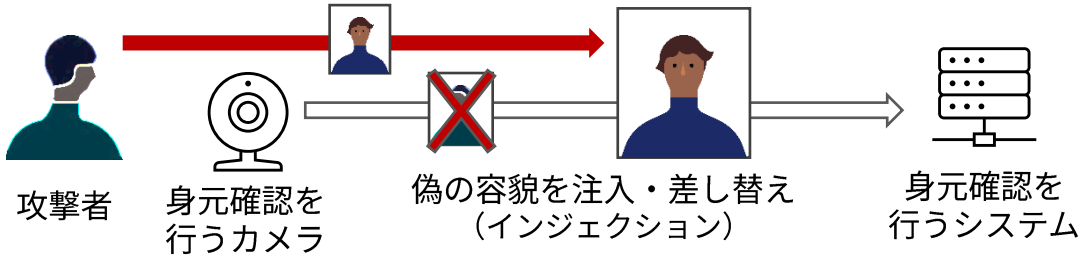
3) ビデオベースの身元確認手法における脅威

プレゼンテーション攻撃



- 印刷した写真、タブレット端末に映した映像等を身元確認時にカメラに映すことで、攻撃者が自身の容貌を偽装する攻撃。静止画や事前に撮影された動画だけでなく、AI 技術を活用しリアルタイムに顔を入れ替えられた映像が用いられる場合もある。
- 攻撃手法が単純であり、映像の不自然さ（光の反射等）によって検知できる場合があるが、身元確認を行うデバイス側は正常であるためセキュリティ機能による防止・検知が難しい。

ビデオインジェクション攻撃



- 攻撃者が身元確認を行うカメラやデバイスに対して偽の映像データを注入することで、本来撮影した映像ではない別の映像データを送信する攻撃。プレゼンテーション攻撃と同じく、AI 技術を活用しリアルタイムに顔を入れ替えられた映像が用いられる場合もある。
- デバイス側のセキュリティ機能による防御や検知による対策が可能な場合があるが、入れ替えられた映像の不自然さによる検知はプレゼンテーション攻撃よりも難しい。

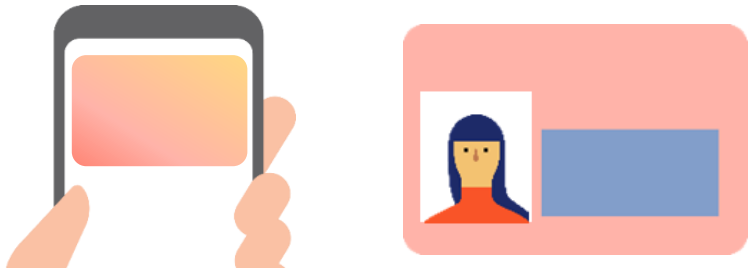
解説書より

身元確認手法の選定の考え方（本編４．２関連）

- 保証レベルの判定後は、採用すべき手法を検討する。本編では原則的なプロセスを定義しているが、解説書４．３節では多くの行政手続等において採用候補であるマイナンバーカードを基本とした考え方を解説している。
- 身元確認手法については、いずれの保証レベルにも対応可能であるマイナンバーカードの活用を第一候補としつつ、事業目的の遂行、公平性等の観点から、必要に応じてマイナンバーカード以外の代替手法を併用する構成を、多くのケースに共通する「身元確認手法の基本的な考え方」として示している。

マイナンバーカードを用いた身元確認手法

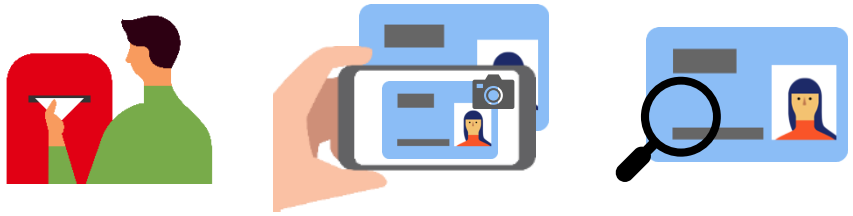
- マイナンバーカードによる身元確認は、保証レベル1～3のいずれにも利用可能。
- 身元確認に利用する機能によって実現できることが異なるため、対象手続に求められるアクセシビリティ、ユーザビリティ、脅威耐性等の観点から、最適な機能を選択する。



＋

マイナンバーカード以外による代替手法

- 対象手続の利用者層、事業目的の遂行、公平性等の観点から、必要な場合にはマイナンバーカード以外による身元確認手法を併用する。
- 採用可能な手法は保証レベルによって異なるため、保証レベルに応じた手法を選択する。保証レベルを満たさない手法を採用せざるを得ない場合は、リスク軽減のための補完的対策を検討する。

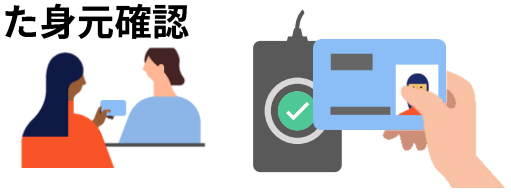
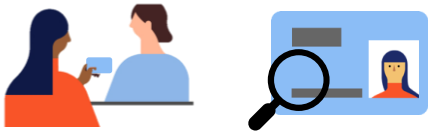
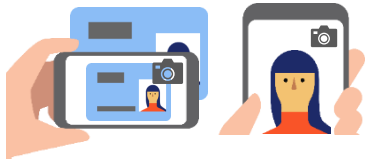
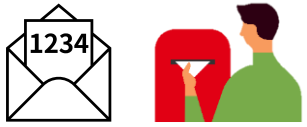


注）上記の「基本的な考え方」は、多くのケースに共通する考え方を示すものであり、ここで示す手法の採用を必須とするものではない。例えば、外国人観光客向けの行政サービスにおいてはマイナンバーカードによる手法は適しておらず、代替手法を中心とした手法の検討が必要であると考えられる。

解説書より

マイナンバーカード以外による身元確認手法（例）

- マイナンバーカード以外による身元確認手法は、保証レベルのほか、どのような場面で、本人確認書類を利用可能とするかによっても異なる。解説書では、代替手法のレベル別の例についても示している。

保証レベル	オンラインによる手法	郵送による手法	対面による手法
身元確認 保証レベル3	マイナンバーカード以外の **ICチップ付き本人確認書類を用いたオンライン身元確認** （電子署名不要の場合のみ） 	（該当手法なし）	マイナンバーカード以外の **ICチップ付き本人確認書類を用いた身元確認** 
身元確認 保証レベル2	レベル3と同様	**本人限定受取郵便（特定事項伝達型）** 	**写真付き本人確認書類を用いた身元確認**（券面の物理的検査＋容貌確認） 
身元確認 保証レベル1	本人確認書類と申請者の容貌を撮影する **ビデオベースの身元確認** （電子署名不要の場合のみ） 	**本人確認書類の郵送＋住所への到達確認** 	レベル2と同様

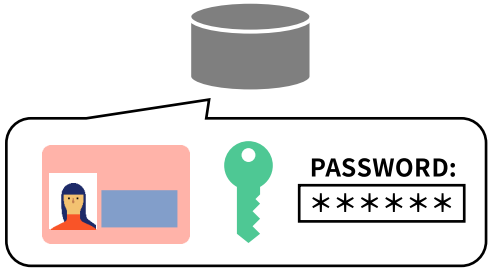
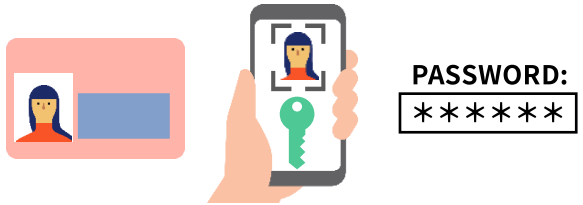
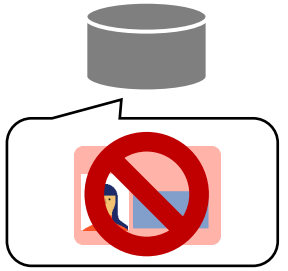
※上記は代表的な手法の一例。これら以外の手法であっても各保証レベルの対策基準を満たす手法であれば採用可能。

1. ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
   ① ガイドラインの適用対象と名称の見直し
   ② 検討にあたる「基本的な考え方」を定義
   ③ 本人確認の基本的な枠組みを定義
   ④-1 保証レベル見直し－身元確認
   ④-2 保証レベル見直し－当人認証
   ④-3 保証レベル見直し－フェデレーション
   ⑤ リスク評価プロセスの全面的な見直し
4. 解説書における追加内容

当人認証の概要　―　目的とプロセス（本編より）

- 当人認証は、対象手続を利用しようとする申請者が、あらかじめ登録されている者と同一の人物であること（当人性）を確認することを目的とした行為。
- 本編では、認証器※のライフサイクルに沿った当人認証のプロセスとして「認証器の登録」「当人認証の実施」「盗難・紛失等への対応」「アカウントの回復」を定めている。

※認証器：当人認証に用いるために申請者が所持し管理する情報、機器、ソフトウェア等の総称。パスワードや認証用デバイス等。

認証器の登録	当人認証の実施	盗難・紛失等への対応	アカウントの回復
			
アカウント登録時等の身元確認プロセスにおいて認証器を登録するなどして、当人認証に用いる認証器を利用者と紐づけて登録する。	手続やサービスを利用しようとする申請者が、あらかじめ登録されている利用者と同一の人物であることを、認証器によって確認する。	利用者から認証器の盗難や紛失の報告を受けた際に、認証器の無効化やアカウントの停止等の対応を行う。	認証器の盗難・紛失、故障による交換、パスワードの忘失などによって利用者がアカウントにログインできなくなった状態を回復する。

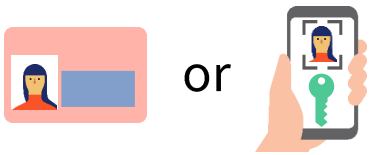
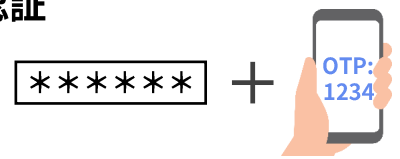
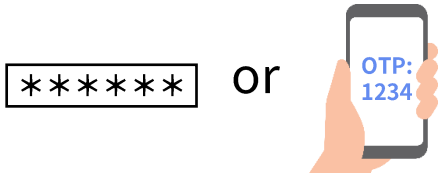
当人認証における脅威の最新化

- 当人認証における脅威についても、リアルタイム中継型のフィッシング攻撃など、昨今の脅威動向等を反映した最新化を行った。

No.	主な脅威	脅威の概要	対策例
1	オンライン上でのパスワードの推測	総当たりやパスワードリスト等により繰り返しログインを試行することで、なりすましを行う	パスワードの複雑性の確保、一定時間あたりの認証回数の制限、多要素認証の採用
2	盗聴・リプレイ攻撃	通信を盗聴し、パスワード等の認証情報を窃取することでなりすましを試みる、同じ内容を再送信することでなりすましを行う	通信の暗号化、チャレンジレスポンス方式の採用、nonceの導入、ワンタイムパスワードの採用
3	パスワードや認証器の盗用	他サービスから漏えいしたパスワード、盗難したICカード等を用いてなりすましを行う	多要素認証の採用
4	フィッシング攻撃	利用者を偽のサイトに誘導し、入力されたパスワード等を攻撃者が窃取したり、**正規のサイトにリアルタイムに中継**したりすることで、なりすましを行う	**フィッシング耐性**を有する認証技術の採用 ※ ワンタイムパスワードはリアルタイム中継型のフィッシング攻撃への耐性を有さない点に留意
5	暗号鍵の不正な取り出し・複製	秘密鍵が格納されたデバイスに対し、物理的な解析やサイドチャネル攻撃等を行うことにより、秘密鍵を不正に取り出そうとする	耐タンパ性を有するハードウェアの利用等

当人認証の概要　―　身元確認保証レベル

- 身元確認と同様、対象手続のリスクの影響に応じた適切な本人確認手法が選択されるよう、昨今の脅威動向を踏まえ以下に示す３段階の当人認証保証レベルを定義。

保証レベル	脅威への耐性要件	該当する手法例 （代表的な手法の一例）
当人認証 保証レベル3	**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	**フィッシング耐性を有する多要素認証** 例） • マイナンバーカードの利用者証明 • パスキー 
当人認証 保証レベル2	**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	**フィッシング耐性を有さない多要素認証** 例） • パスワード認証 ＋ワンタイムパスワード認証 
当人認証 保証レベル1	盗聴、リプレイ攻撃への耐性 オンライン上での認証情報の推測への耐性	**単要素認証**（又は多要素認証） 例） • パスワード認証 • ワンタイムパスワード認証 • USB接続型セキュリティキー 

解説書より

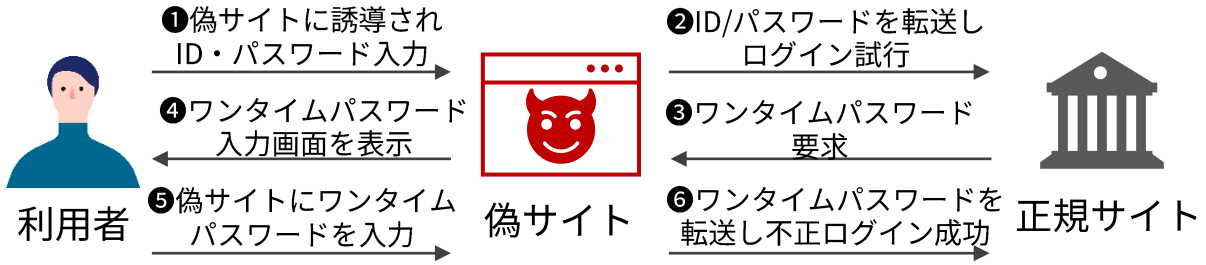
当人認証に関する主な解説（解説書より）

- 当人認証に関する解説、補足、参考情報を示している。
- 「本人確認に関する直近の動向」でも言及した「リアルタイムフィッシング」や、その対抗手段となる「フィッシング耐性の実現手段」の現実的な選択肢について解説。

当人認証に関する解説 （一部抜粋・要約）

1) リアルタイムフィッシングについて

- リアルタイムフィッシングでは、利用者が偽サイトに入力したパスワードがリアルタイムに中継され、ログインが試行される。
- ワンタイムパスワードも中継され得るため、パスワードとワンタイムパスワードを組み合わせた二要素認証では防ぐことができない。

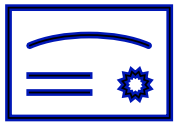


2) フィッシング耐性を実現できる手段

- 現時点でフィッシング耐性を有する手段の現実的な選択肢は「パスキー」と「PKI（公開鍵基盤）をベースとした認証」が現実的な選択肢。

パスキー

- パスキーはドメインに紐づけられており、偽サイトのドメインで利用することができないよう制御されること等により、フィッシング耐性のある当人認証を実現。



PKI（公開鍵基盤）をベースとした認証

- 利用者に紐づくクライアント証明書を用いて正規サイトとクライアント間での相互認証（相互TLS）を行うことで、フィッシング耐性のある当人認証を実現。

解説書より

パスワード認証に関する留意事項

- 解説書では、パスワード認証に関する留意事項をとりまとめている。パスワード認証は従来広く用いられてきた当人認証手法だが、現在では多くの留意事項がある手法。
- パスワード認証を安易に採用すると、様々なセキュリティ面の対処が必要となり、結果として将来的なコスト増の要因となることも懸念される。採用に当たっては慎重な検討が求められることを解説。

パスワード認証に関する留意点

フィッシングへの脆弱性	パスワード認証はフィッシング攻撃への耐性を有さず、対策については利用者側の判断や注意に依存せざるを得ない。
パスワードの使い回しへの対応の難しさ	利用者が複数のサービスでパスワードを使いまわしていた場合、他のサービスから漏えいしたパスワードにより不正アクセスを受けるリスクがある。パスワードの使い回しをサービス提供側でのコントロールすることは難しい。
パスワードマネージャーの利用の考慮	フィッシング対策の観点からは、パスワードマネージャーを利用できるようにすべき。以下のようなパスワードマネージャーの利用を阻害するような実装は避けるべきである。 • 一般的なパスワードマネージャーが生成するパスワードの文字種・文字長に対応していない • 入力フォームでオートフィル機能が起動しない、貼り付け（ペースト）が禁止されている

（参考）米国NISTのガイドラインにおける要求事項

- パスワードの長さは、**単要素認証として利用する場合は15文字以上、多要素認証の一要素として利用する場合は8文字以上**としなければならない。また、設定可能なパスワードの最大長は少なくとも64文字とすべきである。
- パスワード設定時に**異なる文字種を混在させることを強制してはならない**。
- 利用者に対して、**定期的なパスワードの変更を求めてはならない**。ただし、パスワードが侵害された証拠がある場合には、パスワードの変更を求めなければならない。
- パスワードを思い出すための**「ヒント」や「秘密の質問」は実装してはならない**。
- パスワードマネージャーや**自動入力機能（オートフィル機能）を利用できるようにしなければならない**。
- パスワードの**「貼り付け」についても、自動入力ができない場合を考慮して許可すべき**である。

（NIST SP 800-63B-4 「3.1.1. Passwords」より抜粋・要約）

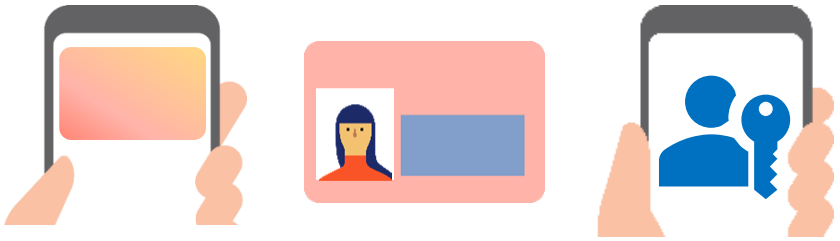
解説書より

当人認証手法の選定の考え方（本編４．２関連）

- 当人認証手法についても身元確認と同様に、当人認証手法の選定にあたる基本的な考え方を示している。
- 昨今の技術動向・脅威動向等を踏まえ、いずれの保証レベルにおいてもマイナンバーカード又はパスキーによる当人認証を第一候補として検討することを基本とし、そのうえで、必要に応じて保証レベルに応じてその他の手法の採用・併用についての検討を行うこととしている。

マイナンバーカード又はパスキー

- マイナンバーカード（利用者証明用電子証明書）及びパスキーはいずれも脅威耐性に優れ、すべての保証レベルにおいて採用候補となる。
- 保証レベル2又は3ではフィッシング耐性を有する手法の提供が必要となるが、採用可能な手法は限られており、マイナンバーカード／パスキーのいずれかの手法の採用が実質的に必須となると考えられる。



＋

その他の当人認証手法

マイナンバーカード/パスキー以外の当人認証手法の採用・併用が必要と考えられる場合には、保証レベルに応じた手法の採用を検討する。

- **保証レベル2の場合**：フィッシング耐性手法との併用を前提として、その他の手法の採用を検討する。
- **保証レベル1の場合**：フィッシング耐性のない手法の採用も可能。ユーザビリティ等の観点から採用を判断する。

なお、保証レベル3はフィッシング耐性が必須であるため、「その他の手法」として採用可能な手法は想定されない。

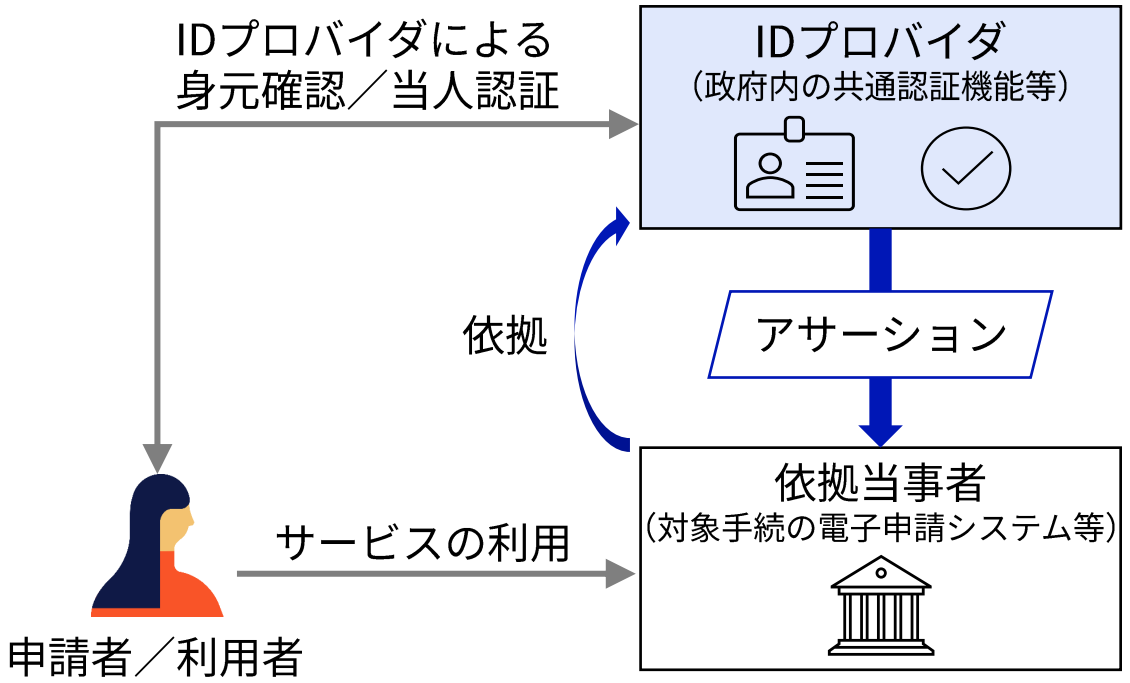
注）身元確認と同様、上記の「基本的な考え方」は、多くのケースに共通する考え方を示すものであり、ここで示す手法の採用を必須とするものではない。

1. ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
   ① ガイドラインの適用対象と名称の見直し
   ② 検討にあたる「基本的な考え方」を定義
   ③ 本人確認の基本的な枠組みを定義
   ④-1 保証レベル見直し－身元確認
   ④-2 保証レベル見直し－当人認証
   ④-3 保証レベル見直し－フェデレーション
   ⑤ リスク評価プロセスの全面的な見直し
4. 解説書における追加内容

フェデレーションの概要　―　フェデレーションとは

- フェデレーションは、対象手続における身元確認や当人認証を、信頼できる他者に依拠して実現するという概念。令和７年９月のガイドライン本編の全面改定において、新たに定義した要素。
- 依拠元となる対象手続を「依拠当事者」、依拠先を「ID プロバイダ」といい、連携のために ID プロバイダから発行される情報を「アサーション」と呼ぶ。

フェデレーションの概念図と用語



「IDプロバイダ」
申請者や利用者に対する身元確認／当人認証を行う主体

「アサーション」
身元確認／当人認証の結果を依拠当事者に連携するためにIDプロバイダから発行される情報

「依拠当事者」
身元確認／当人認証をIDプロバイダへ依拠する主体

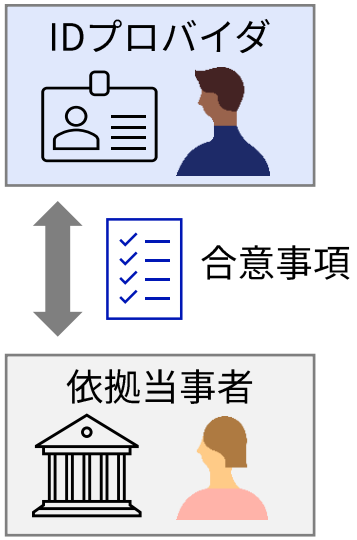
解説書より

フェデレーションの概要　―　目的とプロセス

・フェデレーションを実現するためのプロセスは、本編において「信頼関係の確立」、「設定・登録及び鍵管理」、「アサーションの連携」及び「定期的な確認と見直し」を定義。

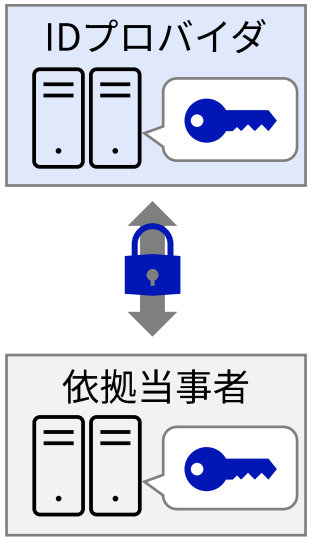
信頼関係の確立

IDプロバイダと依拠当事者との間で、フェデレーションにおいて連携する属性情報や保証レベル等の条件を事前に調整し、合意・確立する



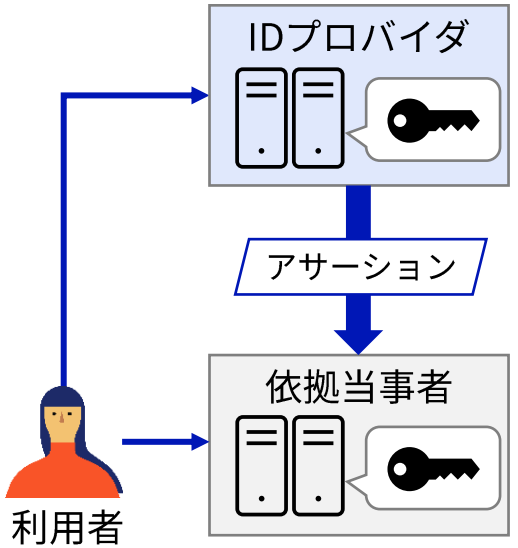
設定・登録及び鍵管理

IDプロバイダと依拠当事者のシステム間で安全な連携を実施するため、ドメイン名やURIの設定、暗号鍵の交換と登録処理等を行う



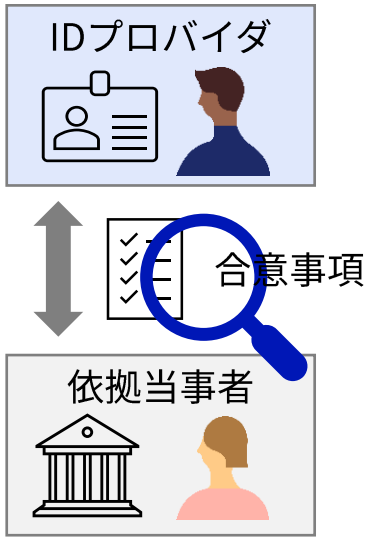
アサーションの連携

IDプロバイダと依拠当事者のシステム間でアサーションの授受を行い、アサーションが再利用や偽造・改ざんされたものでないか等の検証を行う。



定期的な確認と見直し

IDプロバイダとの合意事項が確かに実施されていることを定期的に確認し、技術や脅威の動向等を踏まえ、必要に応じて合意事項を見直す。



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。
- 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）

解説書より

フェデレーションに関する解説　―　考慮すべき脅威

- フェデレーションには様々なメリットがあり、本編の「２.２ 本人確認の実装モデル」においても、フェデレーションを活用した「連携モデル」を推奨している。その一方で、フェデレーションで特有の脅威にも考慮が必要。
- 解説書３．３節では、フェデレーションを利用する際に考慮すべき脅威として「保証レベルの齟齬」と「アサーションに関する攻撃」について解説。

フェデレーションの脅威に関する解説 （一部抜粋・要約）

1) 保証レベルの齟齬について

脅威の概要

- 依拠当事者が本来必要とする保証レベルと、ID プロバイダ側の保証レベルとの間に不一致が生じること。
- ID プロバイダが提供する本人確認手法の仕様や保証レベルを依拠当事者側が十分に把握できていなかったり、運用開始後にID プロバイダ側の仕様や運用が変更されたりすることで生じる可能性があり、攻撃の起点として悪用されるリスクがある。

必要な対策

- 保証レベルの一致を「信頼関係の確立」プロセスによって確認・合意するとともに、IDプロバイダ側の実装や運用を定期的に確認することが必要。

2) アサーションに関する攻撃

脅威の概要

- ID プロバイダから依拠当事者に対して発行されるアサーションに対し、盗聴・ 窃取・偽造・改ざん・再利用等の攻撃が行われること。
- アサーションに含まれる利用者の個人情報を窃取されたり、不正に取得したアサーションを使って依拠当事者に対するなりすまし等が行われたりするリスクがある。

必要な対策

- ID プロバイダと依拠当事者との間で安全な連携のための設定等を行う。詳細な対策については、利用するフェデレーションプロトコル（OpenID Connect、SAML等）の技術標準に則って実装する。

1. ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
   ① ガイドラインの適用対象と名称の見直し
   ② 検討にあたる「基本的な考え方」を定義
   ③ 本人確認の基本的な枠組みを定義
   ④-1 保証レベル見直し－身元確認
   ④-2 保証レベル見直し－当人認証
   ④-3 保証レベル見直し－フェデレーション
   ⑤ リスク評価プロセスの全面的な見直し
4. 解説書における追加内容

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

解説書より

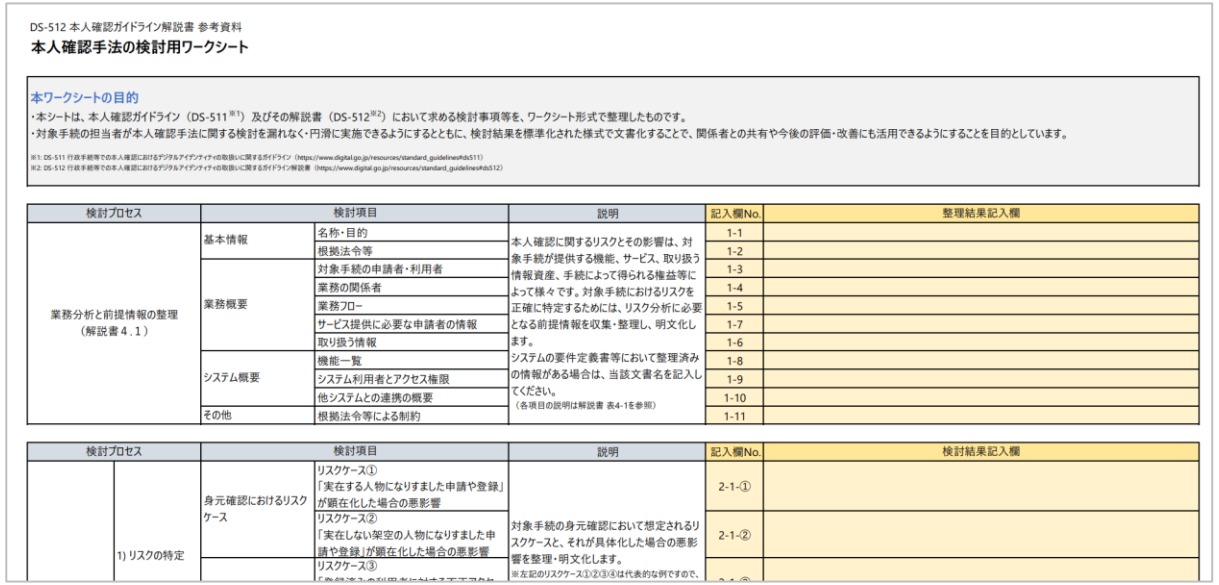
業務分析と前提情報の整理

- 本人確認に関するリスクの大きさは対象手続の性質によって様々であり、本人確認手法もその性質を考慮した検討が必要。解説書４．１節ではこれを踏まえ、対象手続におけるリスク評価（４．２節以降）を検討するための前段プロセスとして、対象手続の業務分析と前提情報の整理について解説。

「4.1 業務分析と前提情報の整理」において整理すべき前提情報の項目（例）

- 本人確認に関するリスクとその影響は、対象手続が提供する機能、サービス、取り扱う情報資産、手続によって得られる権益等に依存するため、検討にあたって整理すべき前提情報を例示。
- また、解説書の参考資料として、これらの情報をとりまとめる「検討用ワークシート」についても公開。

分類	リスク分析に向けて整理すべき項目
基本情報	名称・目的
	根拠法令等
業務概要	対象手続の申請者・利用者
	業務の関係者
	業務フロー
	サービス提供に必要な申請者の情報
	取り扱う情報
システム概要	機能一覧
	システム利用者とアクセス権限
	他システムとの連携の概要
その他	根拠法令等による制約



DS-512 本人確認ガイドライン解説書 参考資料

本人確認手法の検討用ワークシート

本ワークシートの目的

・本シートは、本人確認ガイドライン（DS-511※1）及びその解説書（DS-512※2）において求める検討事項等を、ワークシート形式で整理したものです。
・対象手続の担当者が本人確認手法に関する検討を漏れなく・円滑に実施できるようにするとともに、検討結果を標準化された様式で文書化することで、関係者との共有や今後の評価・改善にも活用できるようにすることを目的としています。

※1: 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（https://www.digital.go.jp/resources/standard_guidelines#ds511）
※2: 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（https://www.digital.go.jp/resources/standard_guidelines#ds512）

検討プロセス	検討項目		説明	記入欄No.	整理結果記入欄
業務分析と前提情報の整理（解説書４．１）	基本情報	名称・目的	本人確認に関するリスクとその影響は、対象手続が提供する機能、サービス、取り扱う情報資産、手続によって得られる権益等によって様々です。対象手続におけるリスクを正確に特定するためには、リスク分析に必要となる前提情報を収集・整理し、明文化します。 システムの要件定義書等において整理済みの情報がある場合は、当該文書名を記入してください。 （各項目の説明は解説書 表4-1を参照）	1-1	
		根拠法令等		1-2	
	業務概要	対象手続の申請者・利用者		1-3	
		業務の関係者		1-4	
		業務フロー		1-5	
		サービス提供に必要な申請者の情報		1-7	
		取り扱う情報		1-6	
	システム概要	機能一覧		1-8	
		システム利用者とアクセス権限		1-9	
		他システムとの連携の概要		1-10	
	その他	根拠法令等による制約		1-11	

検討プロセス		検討項目		説明	記入欄No.	検討結果記入欄
	1) リスクの特定	身元確認におけるリスクケース	リスクケース① 「実在する人物になりすました申請や登録」が顕在化した場合の悪影響	対象手続の身元確認において想定されるリスクケースと、それが具体化した場合の悪影響を整理・明文化します。 ※左記のリスクケース①②③④は代表的な例ですので、	2-1-①	
			リスクケース② 「実在しない架空の人物になりすました申請や登録」が顕在化した場合の悪影響		2-1-②	
			リスクケース③			

解説書より

対象手続の保証レベルの判定

- 解説書４．２節では、本編で示す影響度評価の基準に基づき、実際の保証レベル判定を行う際の参考情報として、架空の手続の判定（例）を掲載。リスク判定については今後事例を追加予定。

ガイドライン本編で示す影響度評価の基準

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、本来有する権利権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

解説書「4.2 対象手続の保証レベルの判定」における架空の手続の（例）

- 解説書４．２では、架空の手続における検討結果例として、本編４．１節に沿ってリスク評価を行う際の「影響度」の判定の例などを例示。

表　4-3　リスク顕在化時における影響度の判定（例）

顕在化時の悪影響の特定（例）（「リスクの特定」の結果より抜粋）	影響度の判定結果と判断根拠（例）
なりすましを検知できなかった場合、攻撃者に対して給付金が不正に支給される可能性があり、組織は金銭的な被害を受ける。 *攻撃者になりすまされた個人がその後に申請を行った場合は二重申請として検知されるが、なりすまされた個人に対する給付金の支給が最大●●か月程度遅延する可能性がある。*	*【高位】* *なりすまされた個人に対する給付金の支給遅延は長期間にわたるおそれがあり、高位の基準の一つである「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。」に該当すると判断。*

解説書より

継続的な評価と改善　―　評価に必要な情報の例

- 本人確認手法の評価と改善に必要な情報としては、例えば次のような情報が考えられる。システムの設計に組み込まないと収集が難しい情報も多いことから、要件定義時点において必要情報を検討・明確化することが望ましい。

分類	評価のための情報（例）	概要
身元確認	身元確認の完了率 身元確認の失敗発生率 身元確認の離脱率	申請者が身元確認プロセスを開始してから最後まで完了できた割合 ／身元確認プロセスにおいて検証の失敗が発生した割合 ／身元確認プロセスを最後まで完了できず申請者が途中離脱した割合
	身元確認の失敗原因	身元確認が失敗したプロセス、失敗の原因等の記録
	身元確認完了までの時間	身元確認プロセスの平均完了時間
	身元確認手法の利用率 （複数の手法を併用する場合）	申請者がどの手法によって身元確認を行ったかの割合
	本人確認書類の利用率 （複数を利用可能な場合）	申請者がどの本人確認書類を用いて身元確認を行ったかの割合
	身元確認に関する問合せ履歴	身元確認に関する問い合わせ件数／その内容、対応結果等
当人認証	当人認証の成功率 当人認証の失敗率	利用者が当人認証に成功した割合 ／利用者が当人認証に失敗した（認証エラーとなった）割合
	当人認証手法の利用率 （複数の手法を併用する場合）	利用者がどの当人認証手法を用いて当人認証を行ったか
	当人認証に関する問合せ履歴	当人認証に関する問い合わせ件数／その内容、対応結果等
全般	不正・不正疑い	不正あるいはその疑いのあったイベント及びインシデントの件数／内容

1. ガイドライン改定の背景
2. ガイドラインの全体像
3. ガイドラインの主な改正点
4. 解説書における追加内容

本人確認ガイドライン：本編と解説書(再掲)

- 「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に関するガイドライン 解説書」（以下「ガイドライン解説書」又は「解説書」といいます。）は、本人確認に関する最新動向、本人確認ガイドライン本編の記載内容の解説、採用候補となる手法の具体例、検討にあたる留意点等をまとめた文書。
- 本編が記載内容への順守を求める「Normative」であるのに対し、解説書は参考情報「Informative」の位置づけとし、本編よりも短期間での改定を行うことで、今後の動向変化にも柔軟に対応可能。

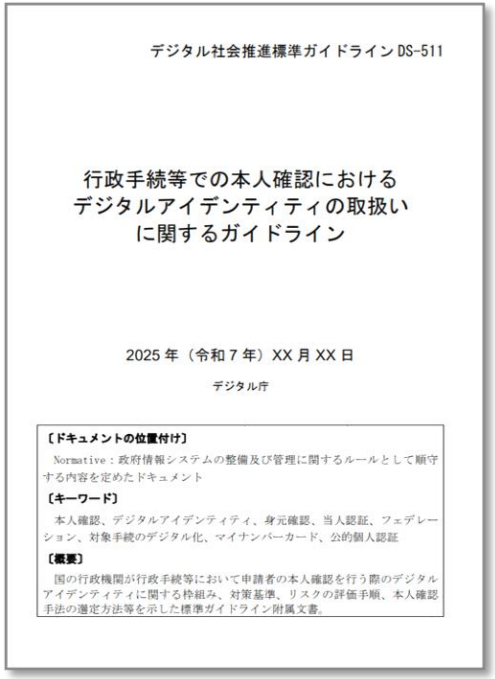
DS-511 本人確認ガイドライン 本編

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、原則的な情報をとりまとめる

本編はできる限りシンプルな内容に留め、詳細情報、状況が短期的に変わり得る具体手法、その他の動向等に関する情報は「解説書」として別途とりまとめる

比較的長期間の改定サイクルを想定


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。

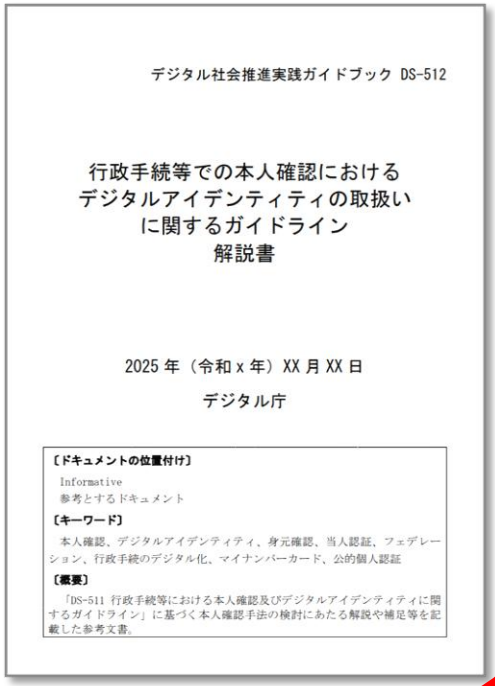
DS-512 本人確認ガイドライン 解説書

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、
- 本人確認に関する最新動向
- 本編の記載内容の解説
- 採用候補となる具体的手法
- 検討にあたる留意事項

等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


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。

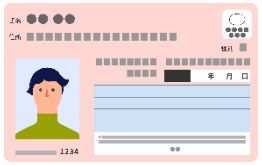
解説書より

本人確認に関する直近の動向（2026 年初頭時点）

- 解説書２．１節では、本人確認ガイドラインを利用する方に特に把握いただきたい動向を解説。
- 特に「本人確認書類の偽造・改ざんの高度化」や「リアルタイムフィッシング」といった脅威の動向は、行政機関に限らず様々な業界において攻撃事例が拡大している脅威である。本人確認手法を検討する際の重要な情報なので、一読を勧める。

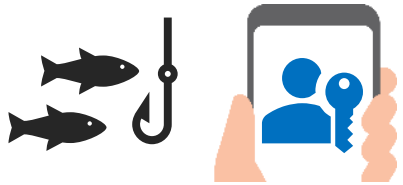
本人確認に関する動向（一部抜粋・要約）

本人確認書類の偽造・改ざんの高度化



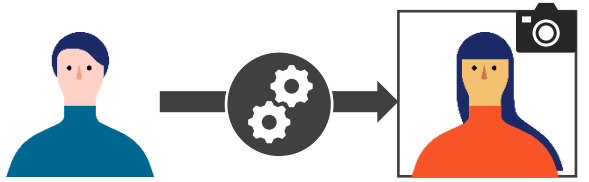
- ✓ 本人確認書類の偽造・改ざん技術はますます高度化しており、目視での厳密な検査は困難となりつつある
- ✓ 精巧な偽造・改ざんを厳密に検知するためには、IC チップを具備した本人確認書類等による、デジタル署名を用いた電子的な検証が必要

リアルタイムフィッシングとパスキー



- ✓ 偽サイトに入力させたパスワードを正規サイトにリアルタイム中継するタイプのフィッシング攻撃が増加
- ✓ ワンタイムパスワードでも防げないため、「パスキー」などのフィッシング耐性を有する当人認証手法の必要性が高まっている

生成 AI を悪用したディープフェイク



- ✓ カメラで撮影中の画像や映像を生成AIで加工・差し替える「ディープフェイク」がビデオベースの身元確認手法での新たな脅威となっている
- ✓ ビデオベースの身元確認手法を用いる場合には、その利用環境に応じた対策の検討が必要

解説書より

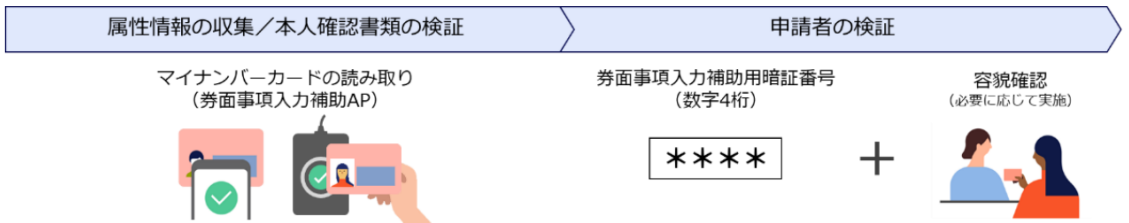
別紙１ 身元確認手法の具体例

- 別紙１では、身元確認手法の選定時の参考情報として、主要な身元確認手法 の概要、脅威耐性、採用時の留意事項についての解説を手法別に掲載している。また、身元確認において重要な要素となる本人確認書類についても、主要な本人確認書類の概要や留意点を説明。
- 本編４章に沿って身元確認手法を検討する際の参考情報として活用いただくことを想定。

身元確認手法の具体例の解説（一例）

解説書の別紙１の１章では、行政手続等での採用候補となる主要な身元確認手法の概要説明、概要図、脅威耐性、保証レベル、採用時の留意事項等を解説。

図　1-1　実物のマイナンバーカード（券面事項入力補助 AP）による身元確認の概要図



本人確認書類の解説（一例）

解説書の別紙１の２章では、我が国において広く流通している 主要な本人確認書類の具体例を、３段階の区分に分けて概要や留意事項等を解説。

区分	概要	該当例
区分A	デジタル署名を備える本人確認書類	実物のマイナンバーカード、スマートフォンのマイナンバーカード、運転免許証、パスポート、在留カード、特別永住者証明書
区分B	顔写真を備える本人確認書類	運転経歴証明書、顔写真付きのその他の国家資格証（小型船舶操縦免許証 等）、顔写真付きの福祉手帳（身体障害者手帳、精神障害者保健福祉手帳、療育手帳）
区分C	その他の本人確認書類	住民票の写し、顔写真なしの福祉手帳（身体障害者手帳、精神障害者保健福祉手帳、療育手帳）

解説書より

別紙２ 当人認証手法の具体例

- 別紙２では、当人認証手法の選定時の参考情報として、主要な当人認証手法 の概要、脅威耐性、採用時の留意事項についての解説を掲載している。
- こちらも別紙１とあわせて、本編４章に沿って当人認証手法を検討する際の参考情報として活用いただくことを想定している。

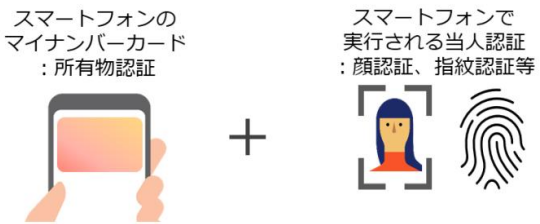
当人認証手法の具体例の解説（一例）

解説書の別紙２では、行政手続等での採用候補となる主要な当人認証手法の概要説明、概要図、脅威耐性、保証レベル、採用時の留意事項等を解説。

ア　手法の概要

スマートフォンに搭載されたマイナンバーカード機能のうち、スマートフォン用の利用者証明用電子証明書（移動端末設備用利用者証明用電子証明書）を用いることで、実物のマイナンバーカードと同じく、公開鍵認証による当人認証を行うことができます。実装において適切なフィッシング対策を講じることで、当人認証保証レベル３の当人認証を実現できます。

図　1-2　スマートフォンのマイナンバーカード（利用者証明用電子証明書）による当人認証の概要図



解説書より

別紙１及び別紙２に掲載している具体手法例の一覧

- 別紙１及び別紙２に掲載している具体手法例は以下のとおり。
- 今後も技術動向や行政手続等における採用動向の変化に応じて、掲載手法の随時追加・見直しを行い、解説書を改定することを予定。

身元確認手法 一覧

マイナンバーカードによる身元確認手法

1) 実物のマイナンバーカード（券面事項入力補助AP）
2) スマートフォンのマイナンバーカード（属性証明機能）
3) 実物のマイナンバーカード（署名用電子証明書）
4) スマートフォンのマイナンバーカード（署名用電子証明書）

マイナンバーカード以外による身元確認手法

1) IC チップ付き本人確認書類を用いた身元確認
2) 顔写真付き本人確認書類を用いた身元確認（対面）
3) 顔写真付き本人確認書類を用いたビデオベースの身元確認
4) 本人確認書類の郵送＋住所への到達確認

当人認証手法 一覧

フィッシング耐性を有する当人認証手法

1) 実物のマイナンバーカード（利用者証明用電子証明書）
2) スマートフォンのマイナンバーカード（利用者証明用電子証明書）
3) パスキー

その他の当人認証手法

1) パスワード認証＋ワンタイムパスワード認証
2) パスワード認証

解説書より

コラム

- 用語説明、最新情報、ガイドラインには含まれないが、理解しておくことが有用な概念等をコラムとして記載。随時内容の修正、追加を予定している。

参考情報：段階的な身元確認について

ガイドライン本編では、本人確認を次の三つの要素で構成すると定義し
ています。一つ目は「身元確認」です。これに
ともに、その実在性を確認するプロセスで、申
その真正性を本人確認書類により検証すること
ムを利用するうえで必要な利用者の属性を収集
証」です。身元確認済みの本人が再度システム
にその人であることを確認するプロセスで、申
証器（パスワードやパスキー、スマートフォン
れます。三つ目は「フェデレーション」で、身
きる ID プロバイダと連携して実現する仕組みで
標準的な流れは、まず公的証明書などを利用
利用する、併用することも可能です）必要な属
確認することで身元確認を実施し、確認が完了
同時にパスワード、パスキーなどの認証関連情
す。この方法は、すべての ID の身元確認保証
め、システムの構築が容易であるという利点が
一方、コンシューマ向けサービスでは、「段階
first flow 等と呼ばれます)」という方法が広
式では、例えば、まずメールアドレスを入力し
時点で ID と認証器を発行し、サービス利用を
請者が当該メールアドレスへのアクセスが可能

（用語解説）アクセシビリティとユーザビリティ

アクセシビリティとは、製品やサービスを
る人々が利用できるように設計・開発され
ルにおけるアクセシビリティは「ウェブ
WCAG 2.2 という国際的なガイドラインも
ISO/IEC 40500:2025 として国際標準規格に
8341-3:2016 についても一致規格としての
ェブアクセシビリティの対象はウェブサイ
ンのアプリ等も含まれており、iOS アプリや
ンも WCAG を参照して作られています。
ユーザビリティとは、製品やサービスを
の効果・効率・満足度、そして利用目的を
9241-11:2018（日本産業規格では JIS Z 8
アクセシビリティが確保されていないと、
くなってしまうことから、アクセシビリ
ティを考慮した設計・開発を行うことが、
方であると言えます。

（参考情報）「フェデレーション」という用語について

令和７年９月のガイドライン本編の改定では、身元確認や当人認証を、他者に依拠して実現することを表す概念である「フェデレーション（Federation）」という用語を追加しました。

参考としている NIST SP 800-63-4 においては、フェデレーションを実現するための代表的な技術として OpenID Connect、あるいは SAML（Security Assertion Markup Language）が言及されています。我が国においては、フェデレーション及びこれを用いて当事者間のアイデンティティ情報が結びつく概念を示すフェデレーテッドアイデンティティ（Federated Identity）※を単純に翻訳しただけの「連合（連合アイデンティティ）」、あるいは、一般的にフェデレーションの過程で行われる当人認証をイメージした「認証連携」という言葉が用いられがちです。

しかしながら、フェデレーションはユーザの識別子や属性情報、その他のメタデータ等も含めた情報を「アサーション」と呼ばれる保護されたデータとして流通させるものであり、「連合」はその概念の理解を助ける訳語とは言いがたく、また「認証を連携する」ものではありません。

これを踏まえ、ガイドライン本編では「連合」や「認証連携」といった用語は用いずに、Federation を片仮名で表記した「フェデレーション」という用語を用いることとしました。本解説書もこの表現に沿っております。

※文書によっては「ID 連携」と記載しているものも同様の概念です。

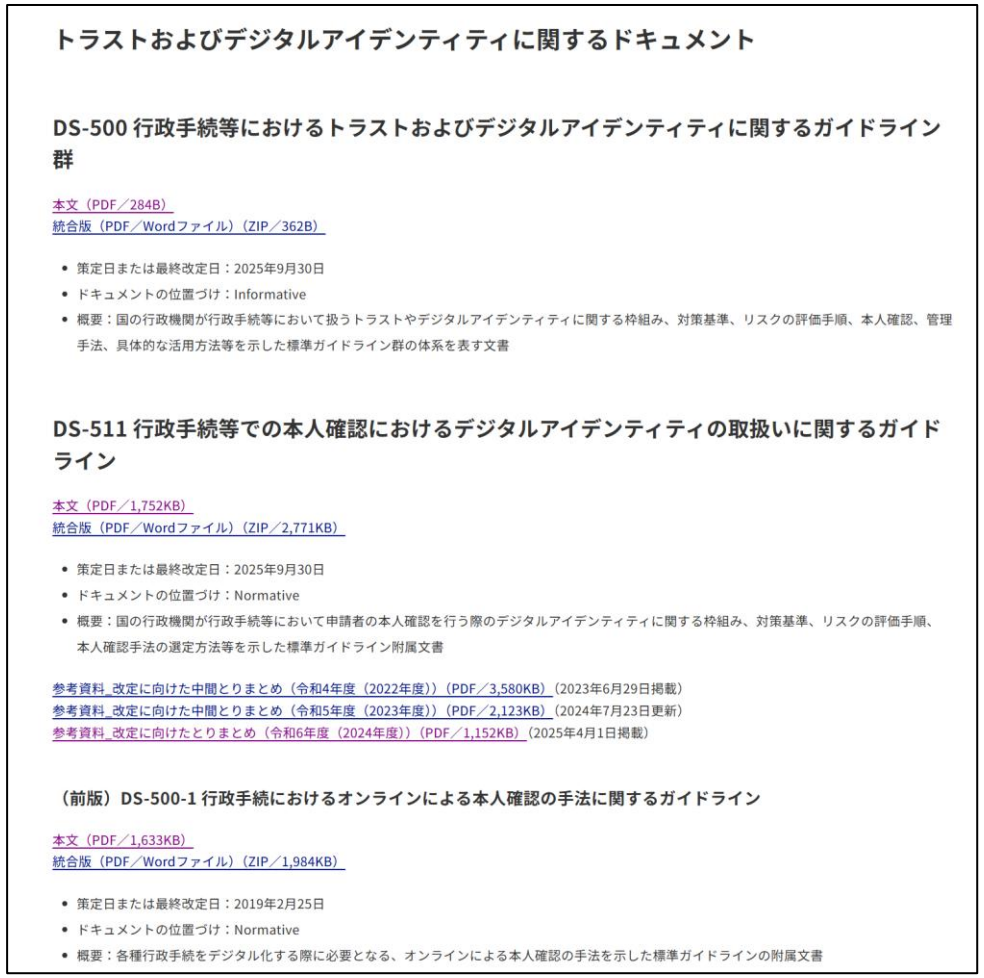
終わりに

ご参考

- 本ガイドラインは主に政府機関向けのものだが、それに限らない。ぜひご活用を！

デジタル社会推進標準ガイドライン

https://www.digital.go.jp/resources/standard_guidelines



トラストおよびデジタルアイデンティティに関するドキュメント

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

本文（PDF／284B）
統合版（PDF／Wordファイル）（ZIP／362B）

- 策定日または最終改定日：2025年9月30日
- ドキュメントの位置づけ：Informative
- 概要：国の行政機関が行政手続等において扱うトラストや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、管理手法、具体的な活用方法等を示した標準ガイドライン群の体系を表す文書

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

本文（PDF／1,752KB）
統合版（PDF／Wordファイル）（ZIP／2,771KB）

- 策定日または最終改定日：2025年9月30日
- ドキュメントの位置づけ：Normative
- 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

参考資料_改定に向けた中間とりまとめ（令和4年度（2022年度））（PDF／3,580KB）（2023年6月29日掲載）
参考資料_改定に向けた中間とりまとめ（令和5年度（2023年度））（PDF／2,123KB）（2024年7月23日更新）
参考資料_改定に向けたとりまとめ（令和6年度（2024年度））（PDF／1,152KB）（2025年4月1日掲載）

（前版）DS-500-1 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

本文（PDF／1,633KB）
統合版（PDF／Wordファイル）（ZIP／1,984KB）

- 策定日または最終改定日：2019年2月25日
- ドキュメントの位置づけ：Normative
- 概要：各種行政手続をデジタル化する際に必要となる、オンラインによる本人確認の手法を示した標準ガイドラインの附属文書

本人確認ガイドラインの改定に関する有識者会議

https://www.digital.go.jp/councils/identification-guideline-revise-experts-meeting

本人確認ガイドラインの改定：本人確認実務の課題・事例・手法とそのガイドラインに関する有識者会議

最終更新日:2026年1月5日

デジタル社会推進標準ガイドラインの一つとして整備された「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」の改訂版である「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」及びその関連文書の作成及び改訂を行っています。
令和7年度（2025年度）は「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」の解説編である「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」作成のための有識者会議を開催します。

※2025年9月30日より「本人確認ガイドラインの改定に向けた有識者会議」から「本人確認実務の課題・事例・手法とそのガイドラインに関する有識者会議」へ、本活動の名称を変更しました。

新着情報

- 2026年1月5日 本人確認実務の課題・事例・手法とそのガイドラインに関する有識者会議（令和7年度 第2回）（2025年11月26日開催）の議事録を掲載しました。

開催状況

令和5年度（2023年度）

- 本人確認ガイドラインの改定に向けた有識者会議（令和5年度 第1回）（2023年10月31日開催）
- 本人確認ガイドラインの改定に向けた有識者会議（令和5年度 第2回）（2023年11月16日開催）
- 本人確認ガイドラインの改定に向けた有識者会議（令和5年度 第3回）（2023年12月26日開催）
- 本人確認ガイドラインの改定に向けた有識者会議（令和5年度 第4回）（2024年1月30日開催）
- 本人確認ガイドラインの改定に向けた有識者会議（令和5年度 第5回）（2024年2月27日開催）

令和6年度（2024年度）

- 本人確認ガイドラインの改定に向けた有識者会議（令和6年度 第1回）（2024年9月17日開催）
- 本人確認ガイドラインの改定に向けた有識者会議（令和6年度 第2回）（2024年11月5日開催）
- 本人確認ガイドラインの改定に向けた有識者会議（令和6年度 第3回）（2024年12月5日開催）
- 本人確認ガイドラインの改定に向けた有識者会議（令和6年度 第4回）（2025年1月16日開催）
- 本人確認ガイドラインの改定に向けた有識者会議（令和6年度 第5回）（2025年3月4日開催）

令和7年度（2025年度）

- 本人確認実務の課題・事例・手法とそのガイドラインに関する有識者会議（令和7年度 第1回）（2025年9月30日開催）
- 本人確認実務の課題・事例・手法とそのガイドラインに関する有識者会議（令和7年度 第2回）（2025年11月26日開催）

IPAによるセキュリティ10大脅威2026（再掲）

デジタルアイデンティティの正しい理解なくして、セキュリティは守れない。ぜひ連携を！

IPAによるセキュリティ10大脅威2026（個人）

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	7年連続10回目
インターネット上のサービスへの不正ログイン	2016年	11年連続11回目
インターネットバンキングの不正利用	2016年	4年ぶり8回目
クレジットカード情報の不正利用	2016年	11年連続11回目
サポート詐欺（偽警告）による金銭被害	2020年	7年連続7回目
スマホ決済の不正利用	2020年	7年連続7回目
ネット上の誹謗・中傷・デマ	2016年	11年連続11回目
フィッシングによる個人情報等の詐取	2019年	8年連続8回目
不正アプリによるスマートフォン利用者への被害	2016年	11年連続11回目
メールやSNS等を使った脅迫・詐欺の手口による金銭要求	2019年	8年連続8回目

大多数がデジタルアイデンティティ関係！

デジタルアイデンティティによる脅威

デジタルアイデンティティに関連する脅威

※IPAによるセキュリティ10大脅威2026をもとに作成：
https://www.ipa.go.jp/security/10threats/10threats2026.html

デジタル庁
Digital Agency

別紙２　法人等の手続における身元確認の考え方について

- 法人等の手続における身元確認では、個人に対する身元確認とは異なる考え方や手法が必要となることを考慮し、この考え方を本編の「別紙２」にとりまとめた。

法人等の手続における身元確認の概念図