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（2024年度））

本人確認ガイドライン改定方針
令和6年度とりまとめ（案）

令和7年3月　　デジタル庁　トラストタスクフォース

本資料の位置づけについて

- 本資料は、有識者会議での協議・レビューを行うことを目的として、本人確認ガイドライン改定方針の現時点案をとりまとめたものです。
- 本資料の内容については、有識者からのご意見、関係各所との調整等を踏まえ、今後見直しを行うことを予定しています。

デジタル庁
Digital Agency

本資料について

「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、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た文書である。米国国立標準技術研究所（NIST）が発行するSP 800-63-3 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。

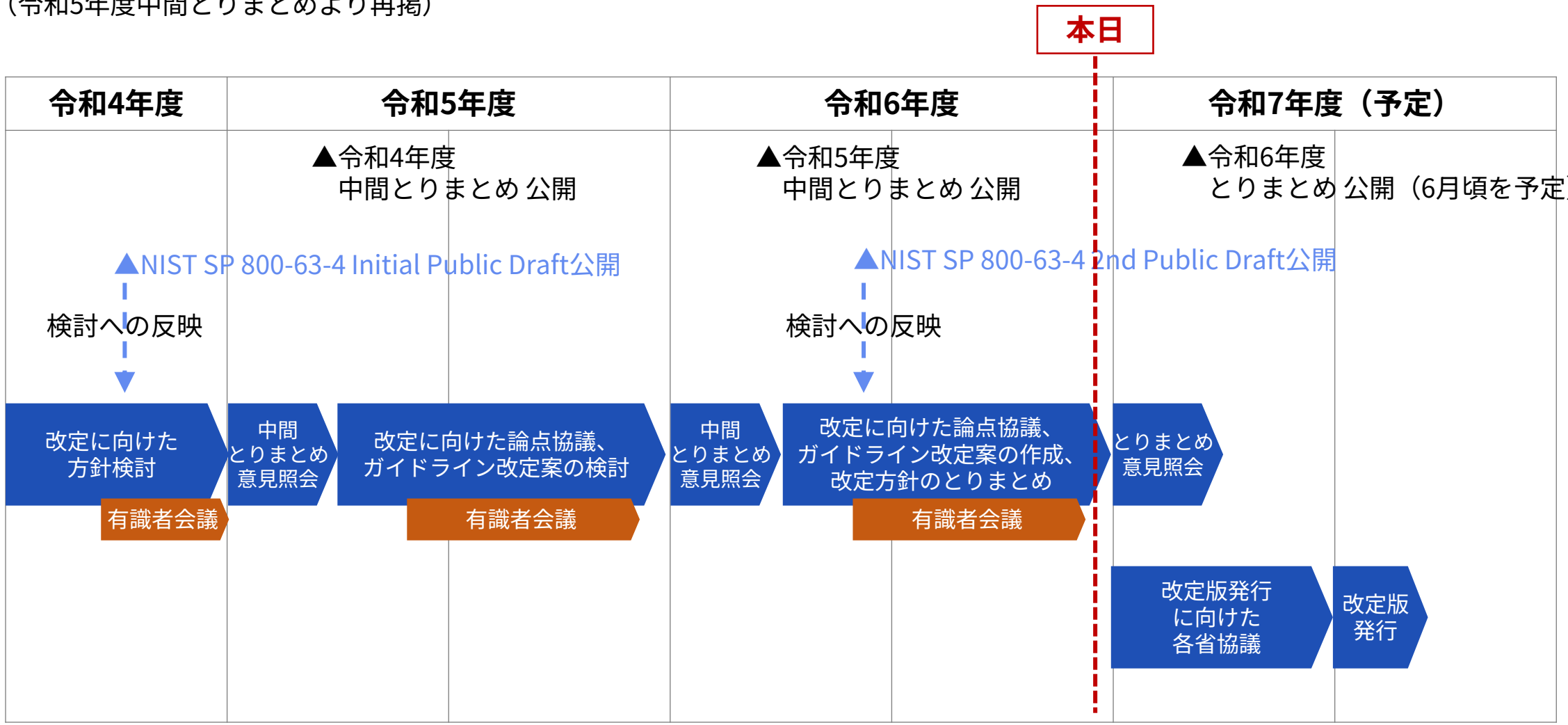
一方、近年の本人確認を取り巻く環境は、行政手続のオンライン化の推進、マイナンバーカードの普及、フィッシング攻撃の高度化、本人確認書類の偽造事件の増加などによって大きく変化している。
米国ではNIST SP 800-63 Digital Identity Guidelinesの改定が進められており、2024年8月には改定案の二次ドラフトが公開された。欧州ではデジタルIDをスマートフォンに格納して利用する仕組みであるEuropean Digital Identity Walletの導入も進められている。

こうした背景を踏まえ、デジタル庁トラストタスクフォースではデジタルアイデンティティ領域の専門家による「本人確認ガイドラインの改定に向けた有識者会議」を開催し、現状課題や国内外の動向等を踏まえつつ、本人確認ガイドライン改定に向けた検討を進めている。

本資料は令和6年度に実施した有識者会議の結果を基に、本人確認ガイドラインの改定方針（案）をとりまとめた文書である。

参考：改定に向けたスケジュール（予定）

（令和5年度中間とりまとめより再掲）



本人確認ガイドライン改定方針（案）の全体像

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。

ガイドライン改定案の目次

ガイドライン改定案の目次（現時点案）

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

主要な改定ポイント（概要）

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解説
- 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全面的な見直し
- 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

「本人確認ガイドライン解説書」の新規整備について

- 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。
  （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）
  （Informative: 参考情報をとりまとめたドキュメント）

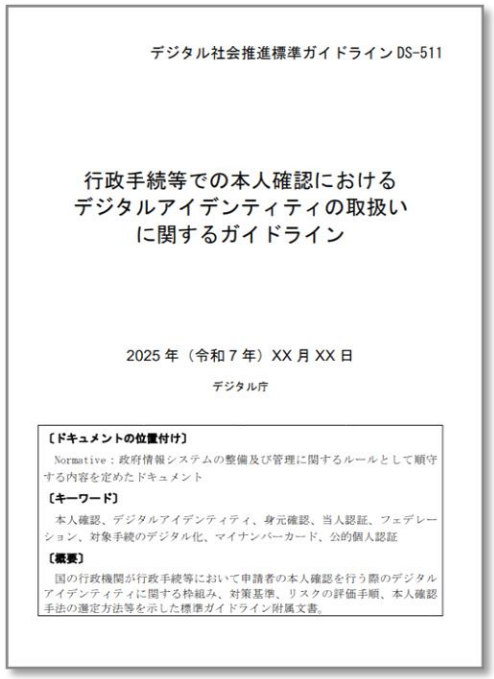
本人確認ガイドライン 本編

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・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

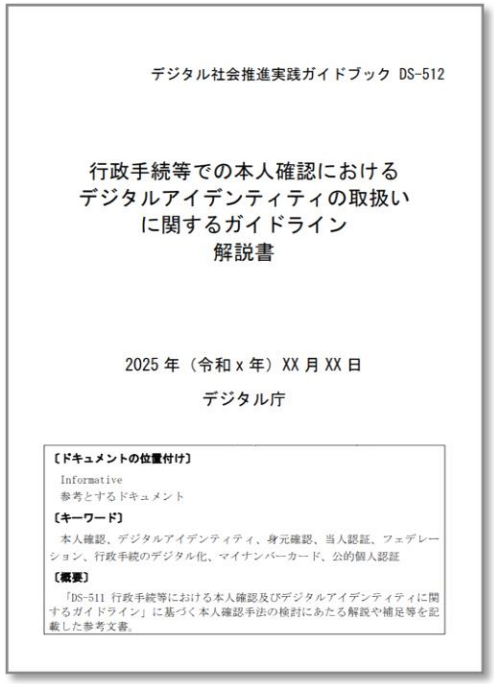
【ドキュメントの位置付け】
Normative：政府情報システムの整備及び管理に関するルールとして順守する内容を定めたドキュメント
【キーワード】
本人確認、デジタルアイデンティティ、身元確認、当人認証、フェデレーション、対象手続のデジタル化、マイナンバーカード、公的個人認証
【概要】
国の行政機関が行政手続等において申請者の本人確認を行う際のデジタルアイデンティティに関する枠組み、対策基準、リスクの評価手順、本人確認手法の選定方法等を示した標準ガイドライン附属文書。

本人確認ガイドライン 解説書

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。

主要な改定のポイント
① ガイドラインの適用対象と名称の見直し

ガイドライン改定案の目次

ガイドライン改定案の目次（現時点案）

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

主要な改定ポイント（概要）

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全面的な見直し
- 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

改定の背景　―　適用対象と名称

- デジタル技術を活用した本人確認の機会が対面や行政手続以外にも拡大していることを踏まえ、本ガイドラインの適用対象を拡大する方針とする。
- 改定にあわせ、内容に合致した名称となるようガイドライン名称も変更する。

見直しの背景

適用対象

デジタルによる本人確認機会の拡大

- 現行ガイドラインは電子申請システム等への適用を想定していた経緯から「オンラインによる本人確認」を適用対象としているが、昨今はマイナンバーカードの普及等に伴い、デジタル技術を活用した本人確認手法（ICチップの読み取り等）が対面の手続においても利用され始めている。
- 様々な行政サービスのデジタル化・オンライン化に伴い、政府が本人確認を行う機会が行政手続以外にも拡大している

名称

ガイドラインの記載内容との乖離

- 今回の改定により、適用対象を変更し、本人確認の枠組みなどの内容も追加することに鑑み、ガイドラインの改定後の内容に合致した名称へと変更する

トラスト関連ガイドライン群の採番体系の見直し

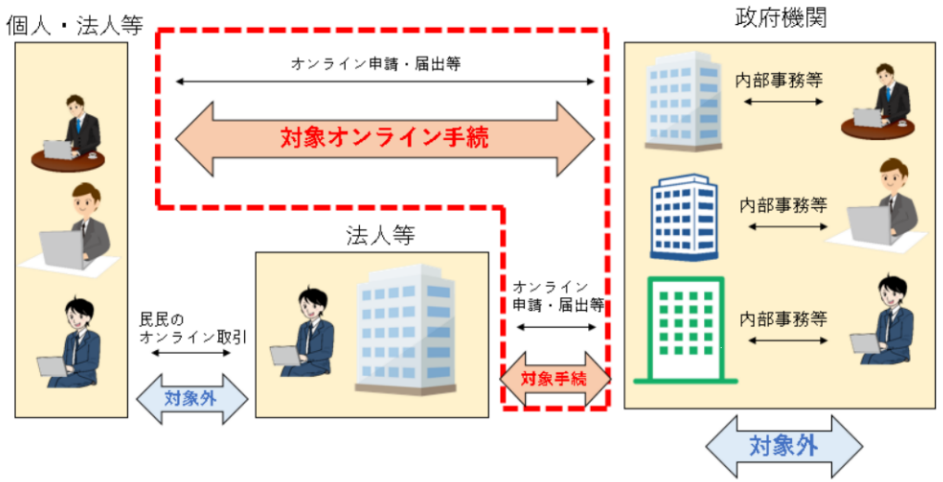
- トラスト関連ガイドライン群の今後の整備予定を考慮し、今回の改定のタイミングでDS-500以下の採番体系の見直しを行う

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。

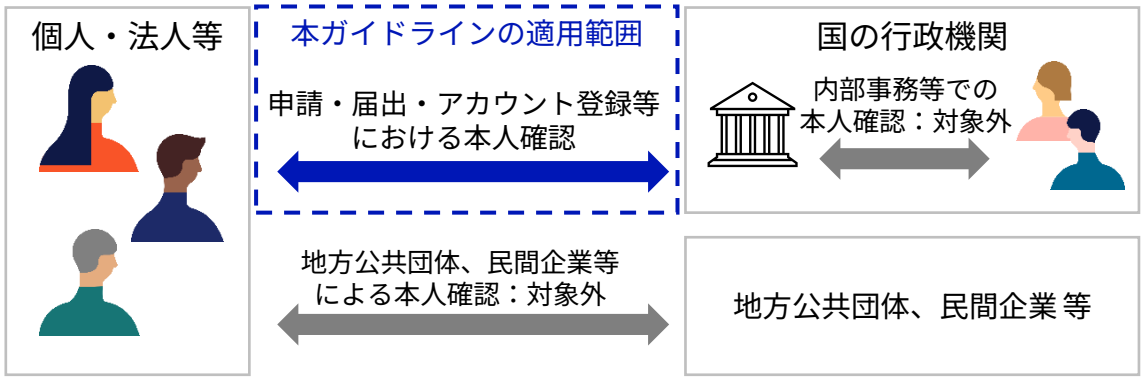
現行ガイドラインの適用対象（概要）

- 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。

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する。
- 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へと変更する。

現行：「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」

- 採番体系の見直し
- 行政手続以外のサービスにも拡大
- 対面を適用対象に含めるため削除
- 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

改定案：「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」

主要な改定のポイント
② 検討にあたる「基本的な考え方」を定義

ガイドライン改定案の目次

ガイドライン改定案の目次（現時点案）

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

主要な改定ポイント（概要）

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全面的な見直し
- 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

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。

主要な改定のポイント
③ 本人確認の基本的な枠組みを定義

ガイドライン改定案の目次

ガイドライン改定案の目次（現時点案）

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

主要な改定ポイント（概要）

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

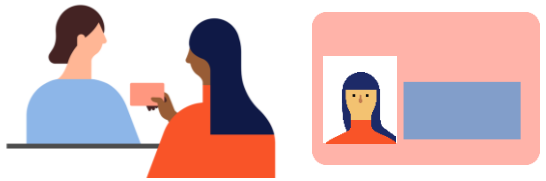
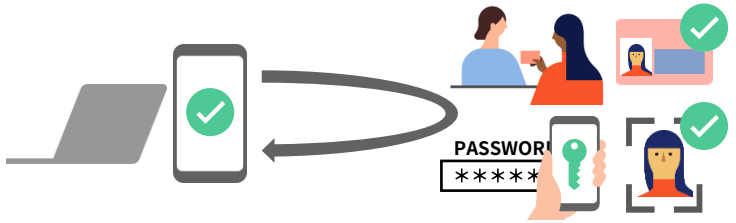
③ 本人確認の基本的な枠組みを定義
- 身元確認、当人認証、フェデレーションの概念の定義
- 実装モデル：連携モデル／非連携モデルの定義

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

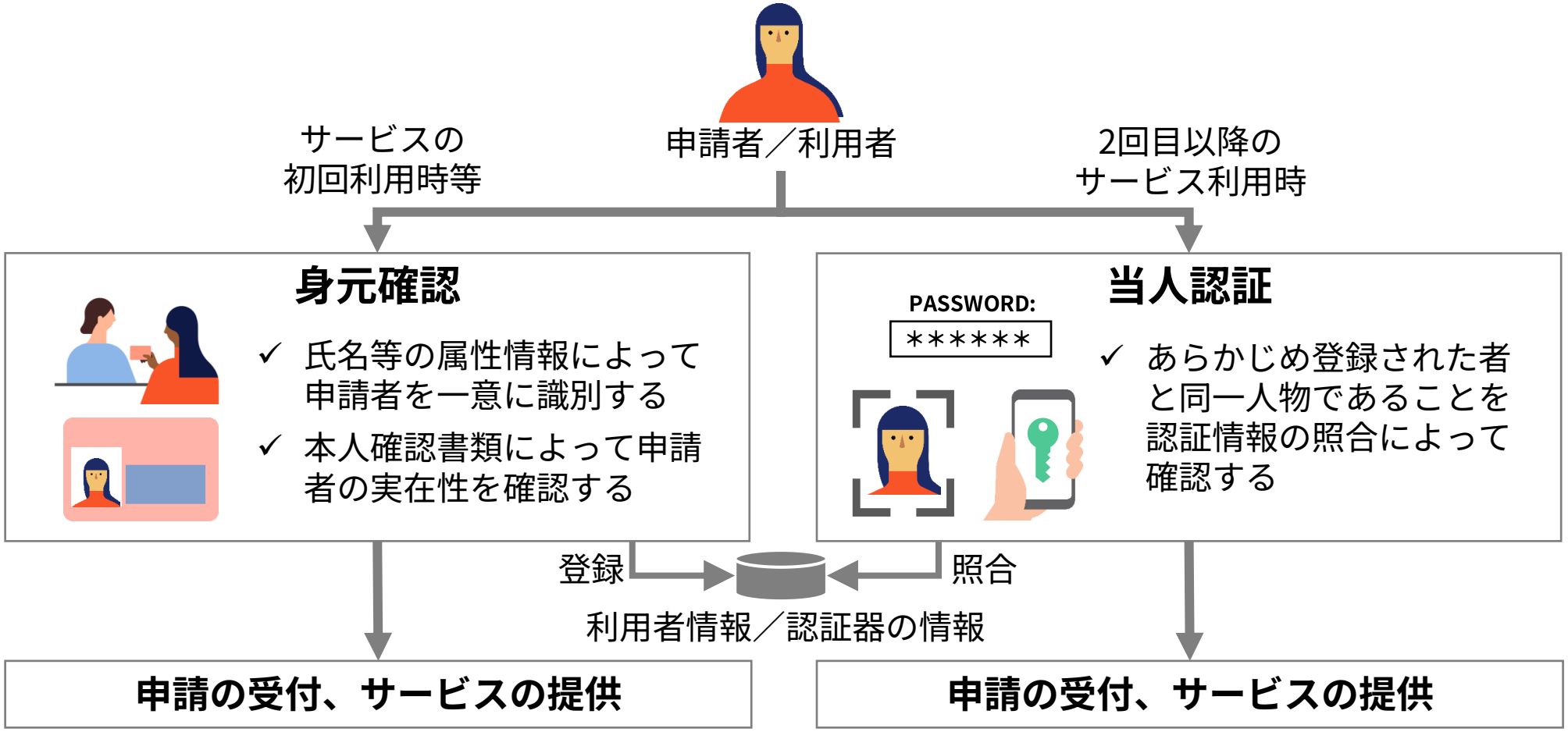
⑤ リスク評価プロセスの全面的な見直し
- 本人確認手法を5つの観点から評価するプロセスを追加
- リスク評価プロセスの単純化

本人確認の基本的要素を定義

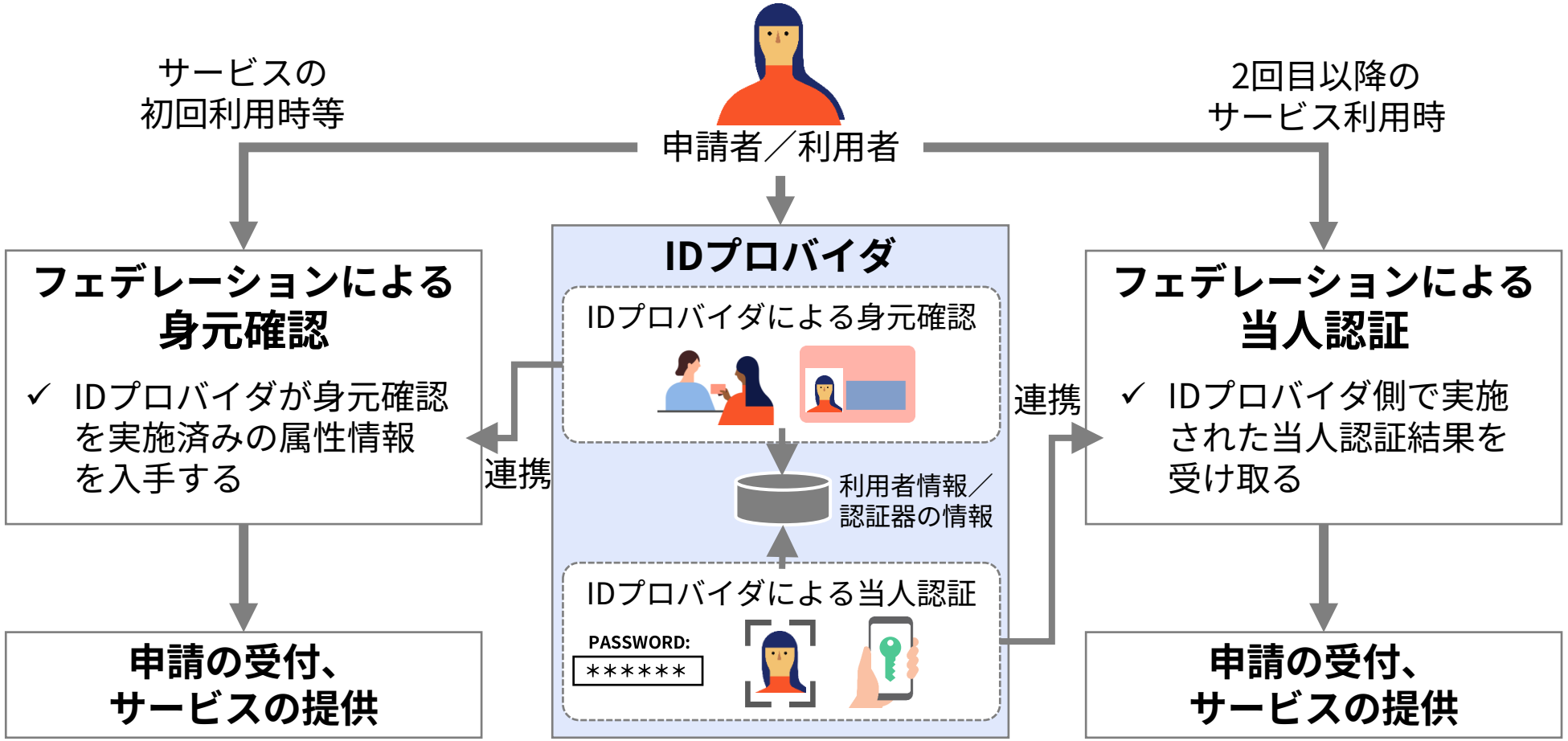
- 本人確認の構成要素である「身元確認」と「当人認証」を明確に定義し、概念図を示す。
- また、身元確認や当人認証を他者に依拠して実現する「フェデレーション」という概念を、今回の改定において新たに定義する。

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

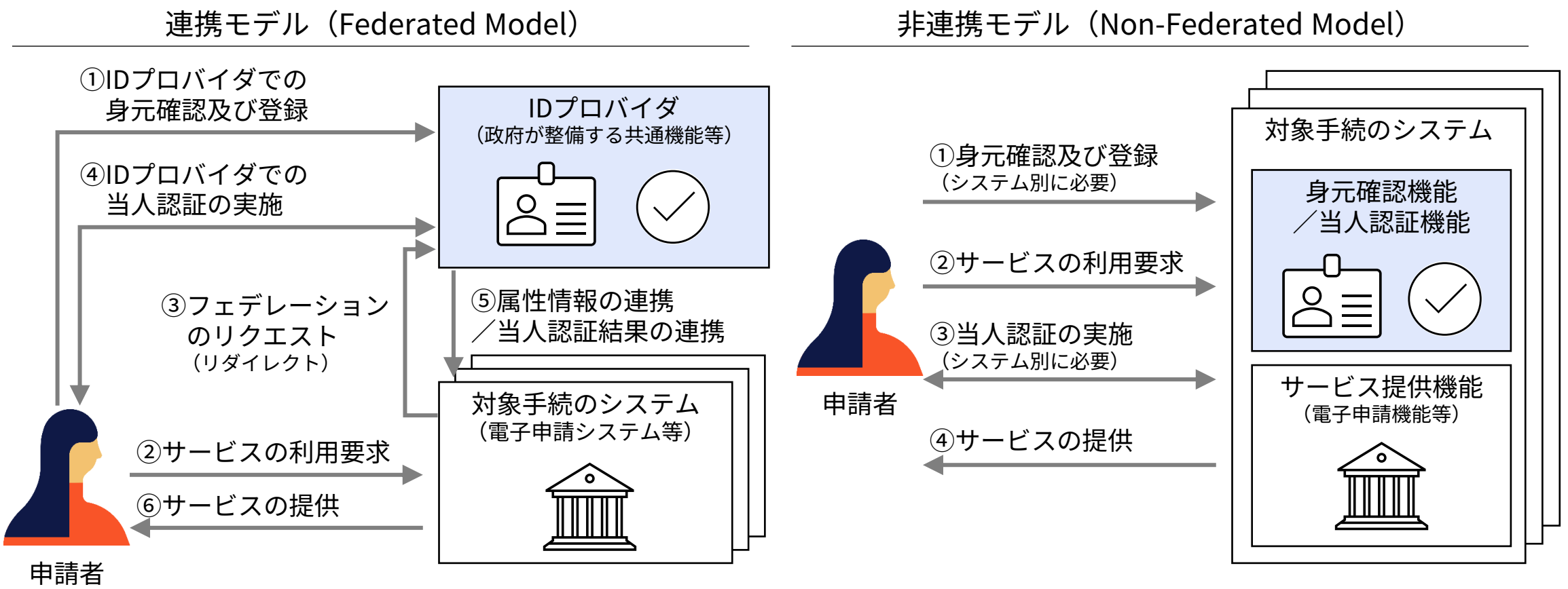


フェデレーションによる本人確認の概念図



システムの実装モデルを定義

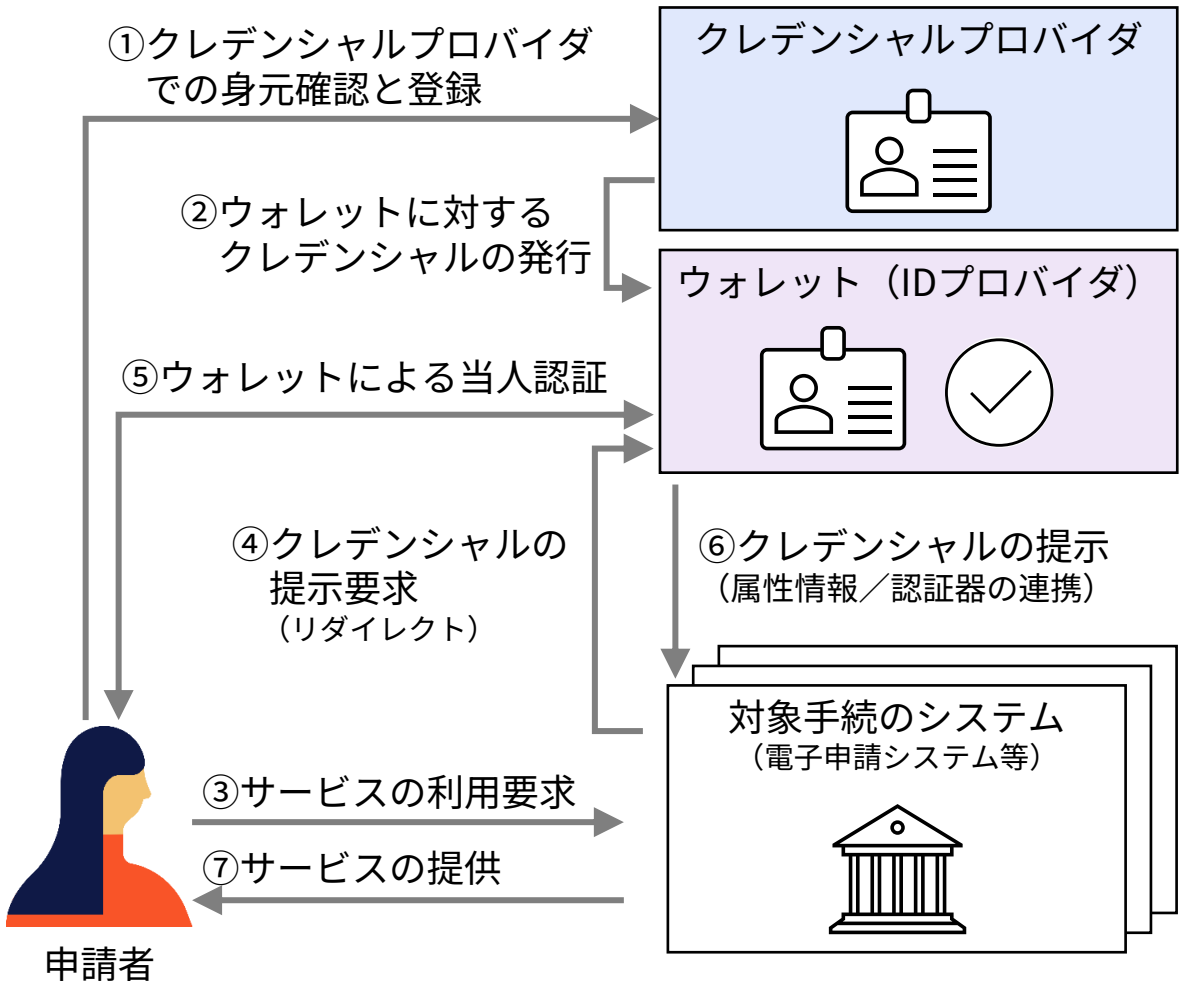
- 本人確認を行うシステムの実装モデルとして「連携モデル」と「非連携モデル」を新たに定義する。
- ユーザの利便性や政府情報システムにおける共通機能の活用の方針に基づき、本ガイドラインではフェデレーションを活用した「連携モデル」の採用を第一候補として扱う。



補足：ウォレットモデル（仮称）の定義の見送りについて

- 令和5年度の有識者会議において検討候補とした「ウォレットモデル（仮称）」については、次の理由により今回のガイドライン改定案への盛り込みを見送る方針とする。
  - ウォレット（デジタルIDウォレット）に関する技術やモデルは現在も標準化やモデルの議論が盛んに進められている段階にあること
  - 本ガイドラインは比較的長期間のサイクルでの改定を想定しているため、未成熟のモデルを掲載した場合の情報の陳腐化等のリスクが大きいこと
- ウォレットに関するモデル定義や対策基準については、今後必要になった段階で、参考資料や別冊等で補足することを検討する。

参考：ウォレットを想定したモデル図（案）



主要な改定のポイント
④ 脅威と対策の最新化、保証レベルの見直し
3.1 身元確認（Identity Proofing）

ガイドライン改定案の目次

ガイドライン改定案の目次（現時点案）

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

主要な改定ポイント（概要）

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

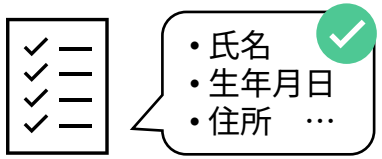
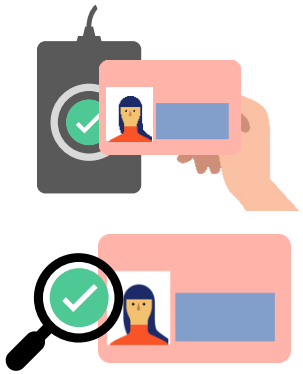
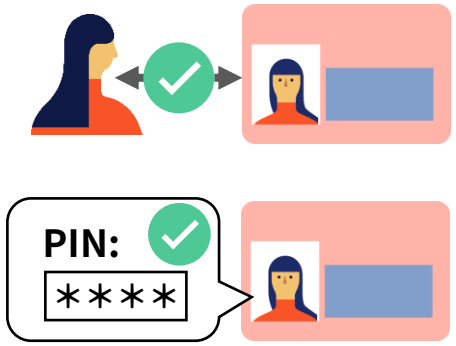
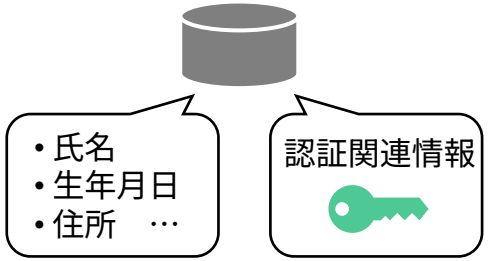
③ 本人確認の基本的な枠組みを定義
- 身元確認、当人認証、フェデレーションの概念の定義
- 実装モデル：連携モデル／非連携モデルの定義

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全面的な見直し
- 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

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

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

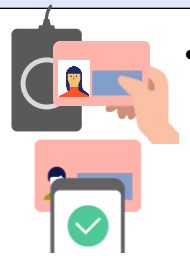
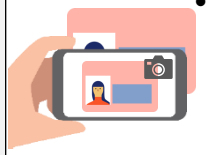
b) 容貌の確認（非対面）
- 本人確認書類の顔写真と申請者の容貌をカメラ映像等で比較する

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

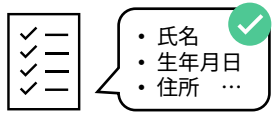
身元確認保証レベルの見直し　―　全体概要

- 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。）	 • 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への対策は必須とはせず、対象手続のリスクに応じた個別判断とする。
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。	**暗証番号:** ＊＊＊＊
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。

プロセス	対策基準（**青字：上位レベルとの相違点**）		
	身元確認保証レベル1	**身元確認保証レベル2**	**身元確認保証レベル3**
属性情報の収集 	（収集手法は任意とする）	（収集手法は任意とする）	本人確認書類の電子的な読取り
本人確認書類の検証 	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 • 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）**	デジタル署名の検証
申請者の検証 	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 • **確認コードの送付による検証**	レベル3と同じ	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

その他の改定ポイント

❶身元確認において収集する属性情報について

- プライバシーの観点等も踏まえ、必要な属性情報の検討を求める記載の追加
  （NIST SP 800-63-4 2pdにおける “Core Attributes” の項目に相当）

❷身元確認において利用可能とする本人確認書類について

- デジタル署名の要否など、検証手法に応じた本人確認書類の条件を検討する際の考え方を明記

❸本人確認手法の貸し借りへの対策について

- 対象手続における貸し借りリスクについての考慮事項

❹身元確認の実施担当者に対する訓練等について

- 券面の物理的検査や容貌の確認を行う場合の手順の整備、担当者に対する教育・訓練等の必要性について

❺カメラに対する攻撃への対策について

- カメラを用いる非対面の身元確認における脅威と対策についての留意事項を明記
- ディープフェイク等の生成AIを悪用した攻撃についても明記

主要な改定のポイント
④ 脅威と対策の最新化、保証レベルの見直し
3.2 当人認証（Authentication）

ガイドライン改定案の目次

ガイドライン改定案の目次（現時点案）

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

主要な改定ポイント（概要）

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

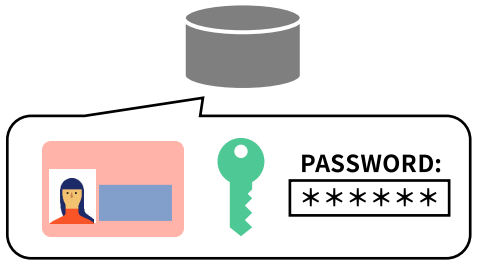
④ 脅威と対策の最新化、保証レベルの見直し
- 脅威と手法例の最新化
- 保証レベルの位置づけと対策基準の見直し

⑤ リスク評価プロセスの全面的な見直し
- 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

当人認証のライフサイクルに沿った対策の定義

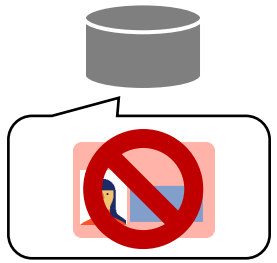
- 当人認証におけるプロセスとして「認証器の登録」、「当人認証の実施」、「盗難・紛失時の対応」、「アカウント回復」を定義し、認証器のライフサイクルに沿って必要となる対策や留意事項を定義する。

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

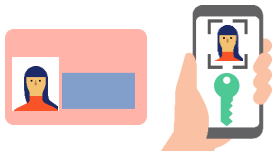
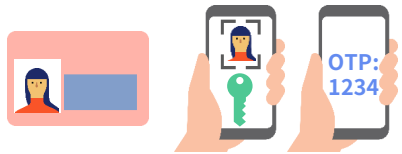
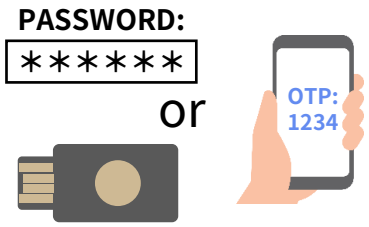
当人認証における脅威の最新化

- 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う。

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

当人認証保証レベルの見直し

- 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	**「公開鍵暗号に基づく認証器」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

主要な改定のポイント
④ 脅威と対策の最新化、保証レベルの見直し
3.3 フェデレーション（Federation）

ガイドライン改定案の目次

ガイドライン改定案の目次（現時点案）

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

主要な改定ポイント（概要）

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

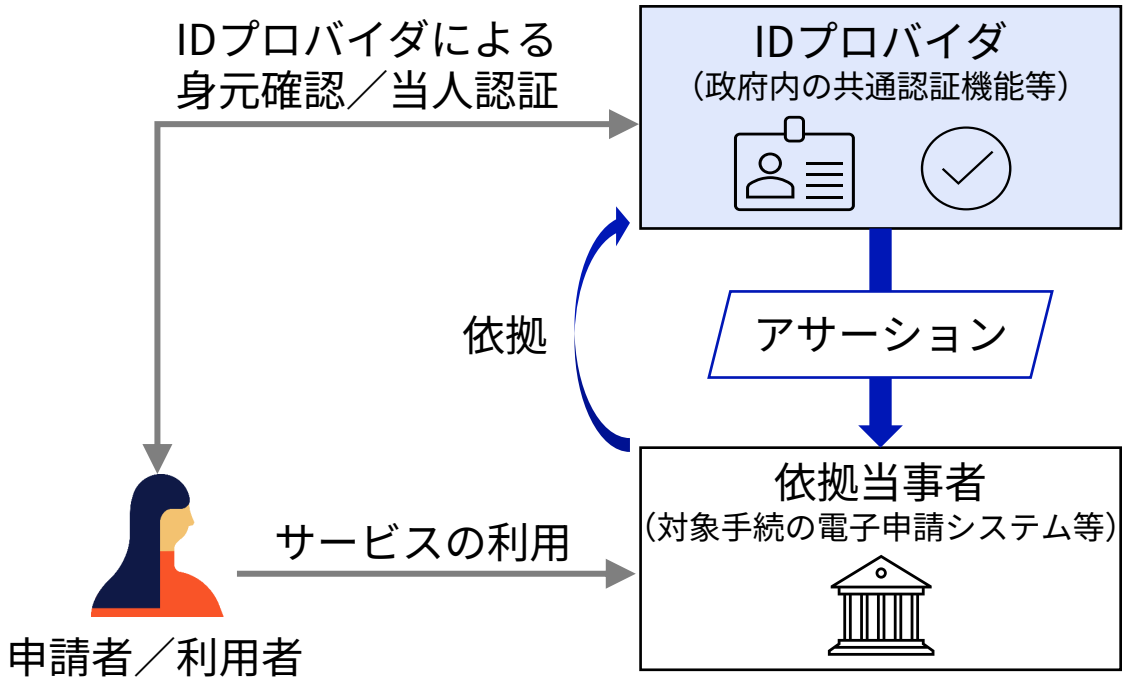
④ 脅威と対策の最新化、保証レベルの見直し
- 脅威と手法例の最新化
- 保証レベルの位置づけと対策基準の見直し

⑤ リスク評価プロセスの全面的な見直し
- 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

フェデレーションの概念

- フェデレーションとは、身元確認や当人認証を他者に依拠して実現する概念である。本人確認ガイドラインとしては第2章の「連携モデル」とあわせて新たに定義する。
- 本ガイドラインでは、フェデレーションにおいて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」、連携に用いられる情報を「アサーション」という。

フェデレーションの概念図



「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

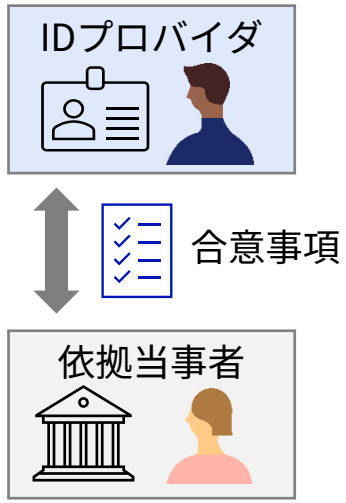
「依拠当事者」
身元確認／当人認証をIDプロバイダへ依拠する主体

フェデレーションに関するプロセスの定義

- フェデレーションを行う場合のプロセスは、以下の4つのプロセスによって定義し、それぞれのプロセスに対して対策基準を定める。

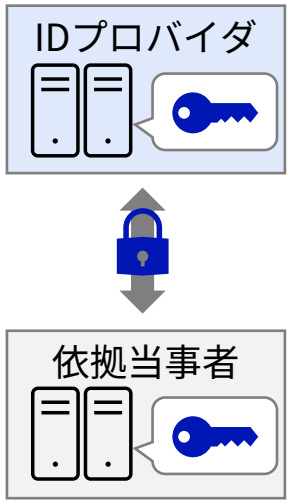
信頼関係の確立

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



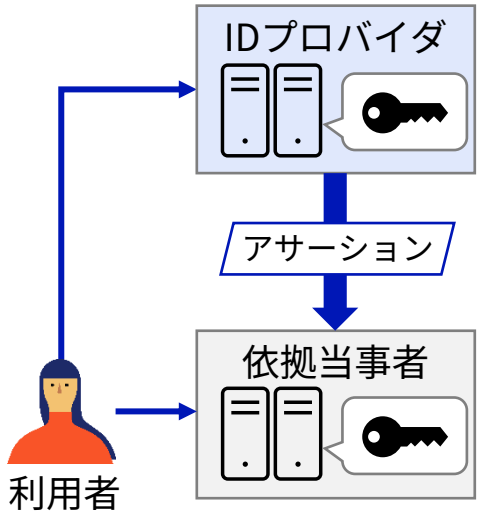
設定・登録及び鍵管理

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



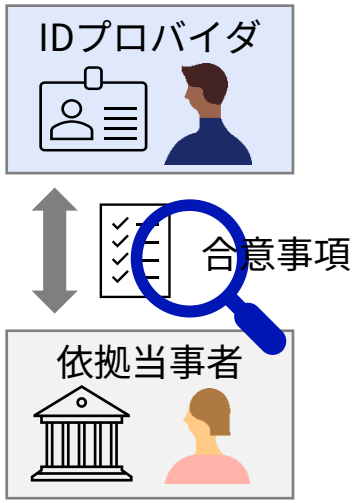
アサーションの連携

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）

主要な改定のポイント
⑤ リスク評価プロセスの全面的な見直し

ガイドライン改定案の目次

ガイドライン改定案の目次（現時点案）

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

主要な改定ポイント（概要）

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全面的な見直し
- 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

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

❶ 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

❷ 本人確認手法の評価プロセスを新たに定義　―　評価の観点

- 新設した「本人確認手法の評価」のプロセスでは、採用しようとする手法による悪影響やリスクを評価する。
- ガイドラインでは、「1.5 基本的な考え方」で定義した5つの観点に基づく評価の考え方を定義する。

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

評価の観点	評価の観点の具体内容
事業目的の遂行	事業目的の遂行に適した手法であるか。 具体的には、対象手続の目的、根拠法、緊急性、本人確認を行う環境、想定される利用者層などに対して適した手法であり、**事業目的の遂行を阻害する懸念がないか**。
公平性	当該手法によって公平性が損なわれないか。 具体的には、想定される利用者の一部にとって障壁となる懸念がなく、当該事業が対象とする**利用者全員に対して、公平な利用機会を提供できる手法であるか**。
プライバシー	当該手法によるプライバシー面の懸念がないか。 例えば、対象手続のサービス提供に必要な範囲以上の個人情報を収集してしまうなど、**プライバシーの原則に抵触するような制約がないか**。
ユーザビリティ及びアクセシビリティ	十分なユーザビリティ及びアクセシビリティを確保できる手法であるか。 ユーザビリティについては、想定する利用者にとって**理解しやすく、間違いにくく、効率的なユーザビリティを提供できる手法であるか**。 アクセシビリティについては、利用者の怪我、障害、視力や聴力の低下など、**利用者の様々な条件や制約を考慮したうえで、採用可能な手法であるか**。
セキュリティ	対象手続が求める保証レベルに該当する手法であり、**必要以上の強度を有する過剰な手法となっていないか**。また、耐性を有さない脅威によるリスクは受容可能であるか。

❷ 本人確認手法の評価プロセスを新たに定義　―　補完的対策の検討

- このプロセスでは、前述の評価結果をもとに、本人確認手法を補完するための対策を検討する。
- 取り得る対策の考え方として「複数の手法の併用」、「追加の対策」、「より高い保証レベルの手法の採用」、「より低い保証レベルの手法の採用」を挙げ、解説する。

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

補完的対策	概要
複数の手法の併用	採用しようとする手法の制約によって事業目的の遂行や公平性の阻害が懸念される場合には、複数の手法を併用することで制約を緩和することが検討できる。
追加の対策	採用しようとする手法だけではプライバシーやセキュリティの要求事項を満たせない場合には、追加的な対策を講じることでリスクを軽減することが検討できる。
より高い保証レベルの手法の採用	採用しようとする手法にセキュリティ面の懸念がある場合などには、対象手続に求められる保証レベルよりも高いレベルの手法を採用することも検討できる。ただし、それによって事業目的の遂行や公平性など他の観点へ与える影響を考慮する必要がある。
より低い保証レベルの手法の採用	事業目的の遂行、公平性、ユーザビリティ及びアクセシビリティ等の観点から、対象手続に求められる保証レベルよりも低いレベルの手法を採用することも検討できる。この場合、本来必要とされる保証レベルとの差によるセキュリティ面のリスクを「追加の対策」によって補完するか、リスクを受容する判断が必要となる。

❸ 継続的な評価と改善プロセスの具体化

- 本人確認手法の継続的な評価を行うためのプロセスを新たに定義する。
- このプロセスでは、対象手続における利用者からの問合せ、セキュリティイベントやインシデント、脅威の動向等を収集し、手法の評価と改善を継続的に行う。

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

ガイドライン改定案の記載案

1) 評価のための情報収集

対象手続において採用した本人確認手法について、評価に必要となる情報を定義し、それらの情報を収集・蓄積すること。

評価に必要な情報には、対象手続における利用者からの問合せ履歴、セキュリティ監視によって検知したイベントやインシデントの履歴、本人確認に関する脅威やインシデントの動向など様々なものが考えられる。

これらの情報収集には、システムの運用・監視等の仕組みの構築が必要となるものも含まれるため、情報システムの要件定義時点から、このような情報収集を見据えた要件定義を行うことが必要である。

2) 評価と改善の実施

収集した情報をもとに本人確認手法の評価を行い、必要に応じて手法の見直し、追加対策の導入、本人確認担当者に対する教育・訓練等の改善措置を講じること。

デジタル庁

Digital Agency