

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)

# 本人確認ガイドライン解説書の記載内容（案）について

令和7年11月 デジタル庁 トラストタスクフォース

はじめに

はじめに

## 本資料の位置づけ

本人確認ガイドラインの改定にあわせ、具体的な手法例等を取りまとめた「解説書」を準備中。

本資料は「[解説書](#)」に掲載予定の「[本人確認手法を選定するための具体的な検討方法](#)」の案を、有識者会議での協議用資料として取りまとめたものである。

### 本人確認ガイドライン 本編

(改定版の発行に向け現在手続中)

#### 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

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遵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、本人認証、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 (仮称)

(2025年度内の発行に向け執筆中)

#### 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

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、本人認証、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を記載した参考文書。

はじめに

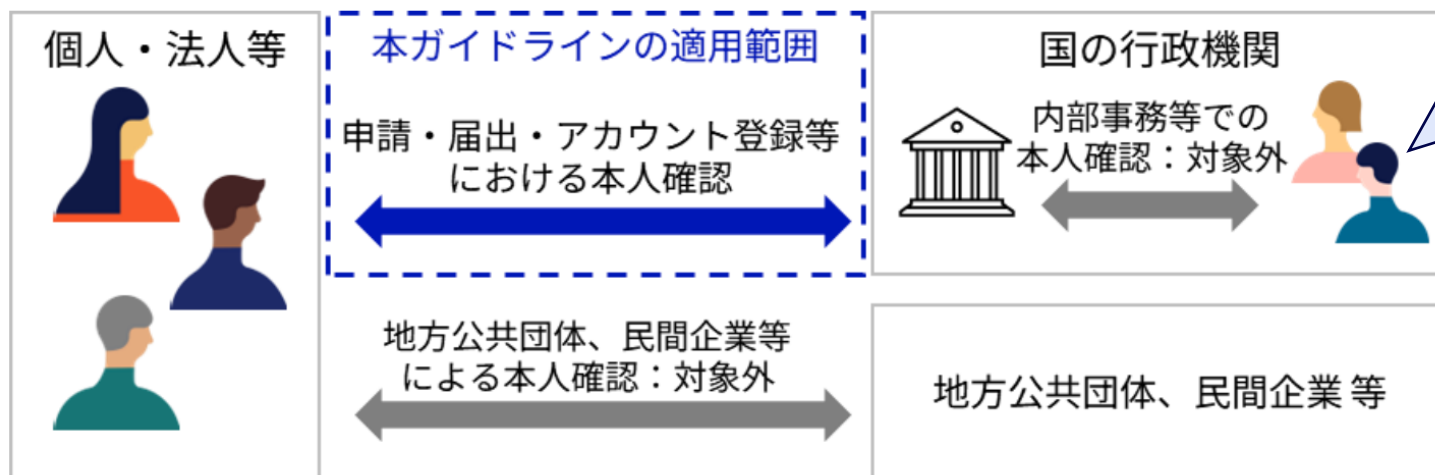
## 本人確認ガイドラインの適用対象について（議論の前提に関する補足）

本人確認ガイドラインの適用対象は「国の行政機関が提供する行政手続又は行政サービス（以下「対象手続」という。）において、個人又は法人等が申請・届出・アカウント登録・ログイン等を行う際の本人確認」としており、**行政機関の内部事務等を担当する政府職員や請負事業者に対する本人確認は対象外**である。

他方、米国NIST SP 800-63-4は政府職員や請負事業者も対象に含めており、なりすましや不正アクセスが行われた場合のリスクが比較的大きいケースも対象としている。

本人確認ガイドラインは、NIST SP 800-63-4を参考としているものの、あくまで**行政手続等の申請者向けに実施する本人確認を対象とした保証レベルや対策基準を定義している**点をご認識いただきたい。

図 1-1 本ガイドラインの適用対象の範囲



DS-511 本人確認ガイドラインでは、**内部事務等を実施する職員向けの本人確認は対象外**（別ガイドラインを整備予定）

（本人確認ガイドライン本編 図1-1より抜粋）

# 1. 本人確認ガイドライン解説書の目次（案）

## 1. 本人確認ガイドライン解説書の目次（案）

# 本人確認ガイドライン解説書の目次（案）

本人確認ガイドライン解説書（仮称）の目次構成は以下を検討中。本日の会議では、このうち「**3 本人確認手法の選定の考え方**」に掲載予定の内容をご確認いただきたい。

### 本人確認ガイドライン解説書（仮称）の目次案

### 主な記載内容

#### 1 はじめに

- 1.1 本解説書について
- 1.2 適用対象／1.3 位置づけ／1.4 用語

#### 2 本人確認ガイドラインの概要

- 2.1 本人確認に関連する技術や脅威の動向（本編全般）
- 2.2 本人確認ガイドラインの概要と全体構成（本編全般）
- 2.3 本人確認ガイドラインの適用対象（本編1.2関連）
- 2.4 検討に当たる基本的な考え方（本編1.5関連）

#### 3 本人確認手法の選定の考え方

- 3.1 対象手続の保証レベルの判定（本編4.1関連）
- 3.2 身元確認手法の選定の考え方（本編4.2関連）
- 3.3 当人認証手法の選定の考え方（本編4.2関連）
- 3.4 継続的な評価と改善（本編4.3関連）

#### 別紙1 本人確認の具体手法例

- 1. 身元確認の具体手法例
- 2. 当人認証の具体手法例

#### 別紙2 参考資料一覧

#### 本人確認ガイドラインの概要解説（本会議での議論対象外）

- ガイドライン本編の読者に特に認識してほしいポイントとして、昨今の脅威の動向、ガイドラインの全体構成、適用範囲、5つの基本的な考え方について解説する

#### 本人確認手法を選定するための実務的な検討フローの解説（本日議論）

- 各手続が手法を選定する際の実務的な手引きとして、保証レベルを踏まえて採用すべき本人確認手法を円滑に選定・調整できるように、基本的な考え方、推奨手法と検討フロー、検討すべき事項などを示す。

（※第1回会議での委員コメントを踏まえ、内容を拡充）

#### 本人確認手法の具体例と参考資料一覧（別紙）

- 採用候補となる具体手法の概要、特徴、保証レベル、採用に当たる留意事項などを、手法別に示す。
- 本人確認に関連する外部文書や、実装時の参考とできる技術標準などの参考文献一覧を示す。

## **2. 本人確認手法の検討方法の全体像**

(本人確認ガイドライン本編4章の概要解説)

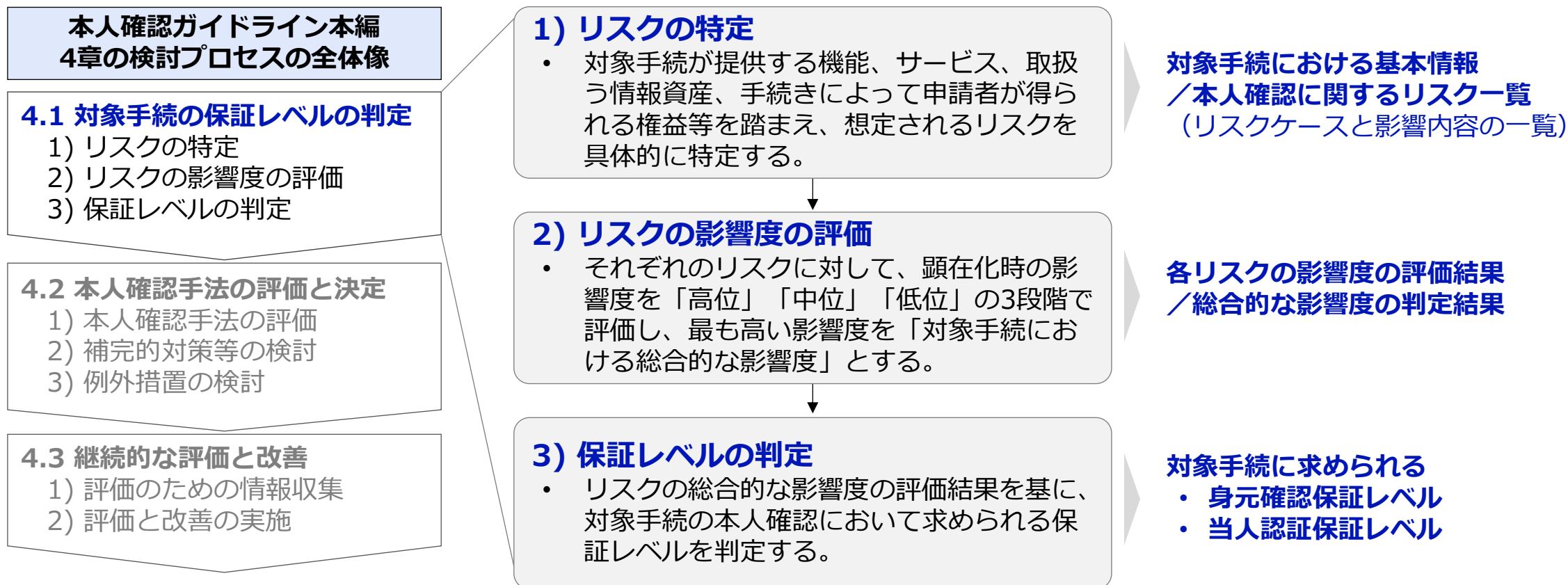
## 2. 本人確認手法の検討方法の全体像

### 4.1 保証レベルの判定 — 検討プロセス

本人確認ガイドライン本編では、本人確認手法の選定に先立って、まずは**対象手続に求められる「保証レベル」を判定すること**としている。具体的には、対象手続におけるリスクケースを特定し、各リスクの顕在化時の影響度を3段階で評価し、最も高い影響度に対応する保証レベルを判定する。

本人確認手法の検討方法の全体像（本編より要約）

各プロセスの検討結果



## 2. 本人確認手法の検討方法の全体像

### 4.1 保証レベルの判定 — 検討結果のイメージ（一例）

前述のプロセスの検討結果は、例えば以下のような内容を想定している。

ここで、リスクケースは多くの対象手続で類似となると考えられるが、「顕在化時の影響内容」は対象手続が提供する機能、取り扱う情報資産、申請によって得られる権益などによって大きく異なるため、**対象手続の特性等を踏まえ、影響内容を具体化・明確化したうえで、影響度を判定することが重要**である。

プロセス	リスクケース	顕在化時の影響内容	影響度の判定結果	総合的な影響度と保証レベル
身元確認	実在する人物になりすました申請や登録	<ul style="list-style-type: none"> <li>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る。</li> <li>また、なりすまされた個人がその後申請を行った場合は二重申請と判定される。不正は検知されるが、<b>当該個人に対する給付金の支給が一時的に遅延する可能性</b>がある。</li> </ul>	中位	総合的な影響度：中位 ↓ <b>身元確認保証レベル2</b>
	実在しない架空の人物になりすました申請や登録	<ul style="list-style-type: none"> <li>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る。</li> </ul>	低位	
当人認証	登録済みの利用者に対する不正アクセス	<ul style="list-style-type: none"> <li>申請システムへの不正アクセスが行われた場合、システム上に表示される氏名や申請受理状況等が攻撃者に閲覧される。</li> <li>システムの仕様上、申請の変更や取り消し等を行うことはできないため、申請そのものへの影響は懸念されない。</li> </ul>	低位	総合的な影響度：低位 ↓ <b>当人認証保証レベル1</b>
	フィッシングサイトに対する情報入力	<ul style="list-style-type: none"> <li>（パスワード認証を採用する場合）登録者のメールアドレスやパスワードが攻撃者に漏洩する。</li> </ul>	低位	

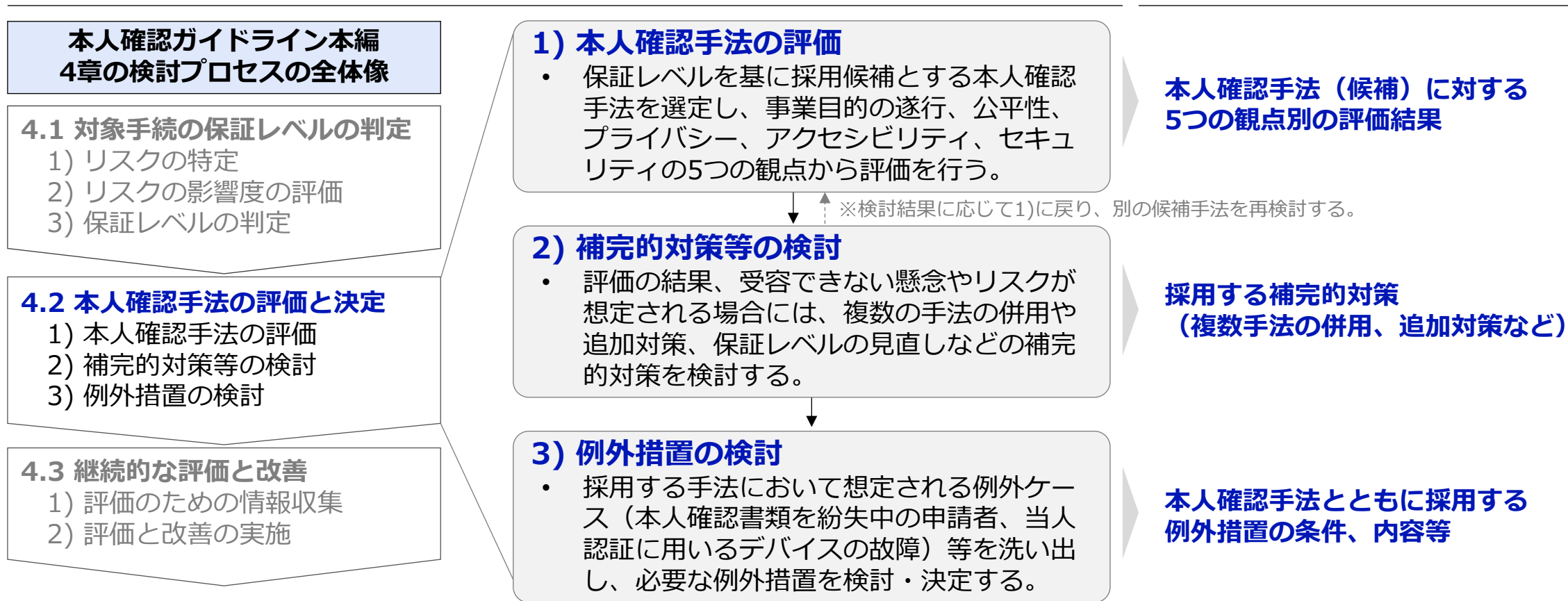
## 4.2 本人確認手法の評価と決定 — 検討プロセス

保証レベルの判定後、対象手続の保証レベルに基づき、採用候補とする本人確認手法を評価し決定する。

具体的には、採用候補となる手法が対象手続にとって適する手法であるかを5つの観点から評価し、必要に応じて補完的対策や保証レベルの見直し、例外措置の検討を行ったうえで、最終的に採用する手法を決定する。

本人確認手法の検討方法の全体像（本編より要約）

各プロセスの検討結果



## 2. 本人確認手法の検討方法の全体像

### 4.2 本人確認手法の評価と決定 — 検討プロセス

本人確認手法の評価と決定については、**マイナンバーカードやパスキーなど現在採用可能な具体手法例を踏まえつつ、基本的な構成、考え方、検討のフローやポイントなどを解説書において詳細に記載することを予定。**

この記載内容（案）については、本資料の3章にてご説明する。記載内容の妥当性等について有識者の皆様からのご助言をいただきたい。

#### 本人確認手法の評価と決定のための解説（本資料の3章にて詳細をご説明）

身元確認手法の基本的な考え方（案）

##### 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

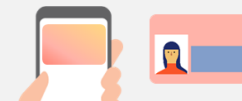
- 対象手続の利用者層、事業目的の遂行、公平性等の観点から、必要な場合にはマイナンバーカード以外による身元確認手法を併用する。
- 採用可能な手法は保証レベルによって異なるため、保証レベルに応じた手法を選択する。保証レベルを満たさない手法を採用せざるを得ない場合は、**リスク軽減のための補完的対策を検討する。**



#### リスク評価による保証レベル判定

##### 1) マイナンバーカードを用いた手法の検討

- 1-a) 電子署名の要否の検討
- 1-b) アクセシビリティ及びユーザビリティに関する検討
- 1-c) セキュリティに関する検討



##### 2) マイナンバーカード以外による手法の検討

- 2-a) マイナンバーカード以外による手法の要否の検討
- 2-b) 採用する代替手法と補完的対策の検討



##### 3) 実装モデルと実現手段の検討

- 3-a) システムの実装モデルの検討
- 3-b) その他の実現手段に係る検討



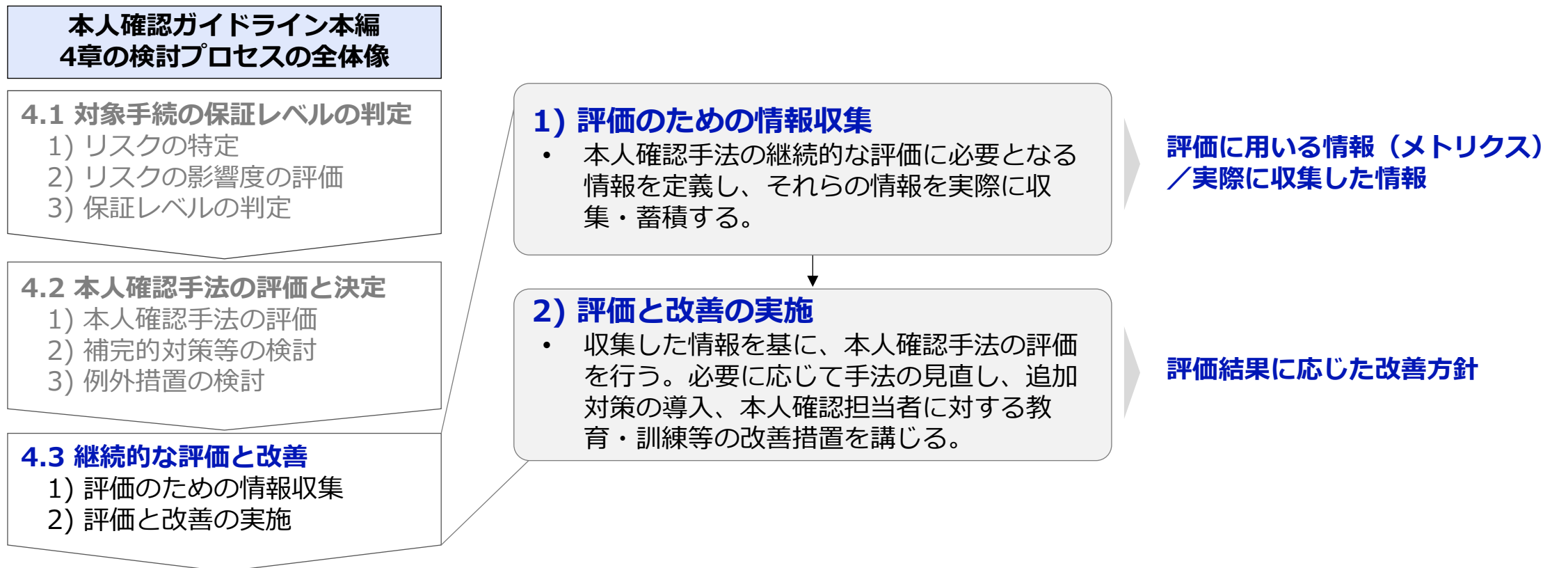
## 2. 本人確認手法の検討方法の全体像

### 4.3 継続的な評価と改善 — 検討プロセス

本人確認手法の決定後は、**継続的な評価と改善を見据えた評価情報（メトリクス）**を定義し、実際の情報収集、評価と改善を行う。

本人確認手法の検討方法の全体像（本編より要約）

各プロセスの検討結果



## 2. 本人確認手法の検討方法の全体像

### 4.3 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

### **3. 身元確認手法の選定の考え方**

— **身元確認手法の基本的な考え方**

— 身元確認手法の検討フロー

— ご議論いただきたいポイント

## 身元確認手法の基本的な考え方 — 基本構成

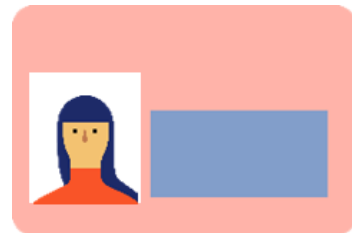
身元確認手法は、いずれの保証レベルにも対応可能であるマイナンバーカードの活用を第一候補としつつ、事業目的の遂行、公平性等の観点から、**必要に応じてマイナンバーカード以外による代替手法を併用**することを基本とする。

(ここでは、多くのケースに共通する「考え方」を示すものであり、この構成を必須とするものではない。在留外国人向けの手続きなど、この考え方には合致しない行政手続等も想定される。)

### 身元確認手法の基本的な考え方 (案)

#### マイナンバーカードを用いた 身元確認手法

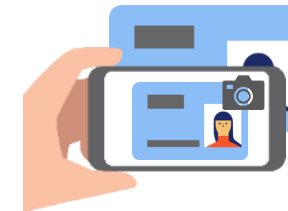
- マイナンバーカードによる身元確認は、保証レベル1~3のいずれにも利用可能。
- 身元確認に利用する機能によって実現できることが異なるため、対象手続に求められるアクセシビリティ、ユーザビリティ、脅威耐性等の観点から、最適な機能を選択する。



+

#### 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。

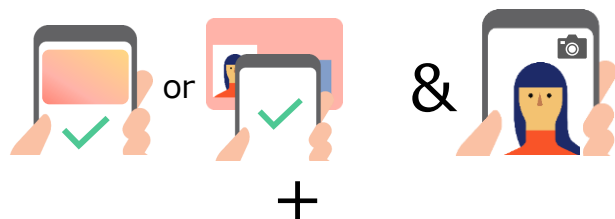


## 身元確認手法の基本的な考え方 — 検討結果（例）

身元確認では、**マイナンバーカードを軸としつつも、郵送や対面による代替手法を併用**することが典型的な採用例の一つとなると考える。

### 身元確認保証レベル3 の検討結果例

- マイナンバーカードによる**電子署名**  
**+オンライン容貌確認**  
を基本とする。



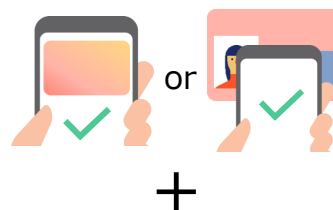
- マイナンバーカードを保有していない  
方向けの代替手段として、**窓口等での  
対面の身元確認**を受け付ける。



※ 保証レベル3では、対面で身元確認を行う場合においても、ICチップを備える本人確認書類を用いたデジタル署名による検証が必要。

### 身元確認保証レベル2 の検討結果例

- マイナンバーカードの券面情報による  
**身元確認**（スマートフォンのマイナンバーカードの属性証明機能 又は 実物のマイナンバーカードの券面事項入力補助AP）



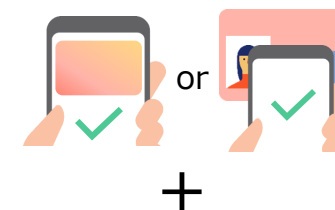
- マイナンバーカードを保有していない  
方向けの代替手段として、**本人限定受  
取郵便（特定事項伝達型）**を利用する。



※ 本人限定受取郵便（特定事項伝達型）は、様々な制約に考慮する必要があるが、ガイドライン上の「対面による身元確認」に相当する手法としてみなせる。

### 身元確認保証レベル1 の検討結果例

- マイナンバーカードの券面情報による  
**身元確認**（スマートフォンのマイナンバーカードの属性証明機能 又は 実物のマイナンバーカードの券面事項入力補助AP）



- マイナンバーカードを保有していない  
方向けの代替手段として、**郵送による  
申請（本人確認書類の郵送+住所への  
到達確認）**を利用する。



※ 郵送による本人確認書類の郵送は、それだけでは「申請者の検証」に相当プロセスを満たさないため、住所等への到達確認を併用することが必要である点に留意。

注：上記は「採用する手法の検討結果」を例示したものである。上位の保証レベルの手法を採用する例も含んでおり、各手法と保証レベルの関係を示すものではない。

### **3. 身元確認手法の選定の考え方**

- 身元確認手法の基本的な考え方
- **身元確認手法の検討フロー**
- ご議論いただきたいポイント

## 身元確認手法の基本的な考え方 — 検討フロー

解説書では、前述の構成を決定するための検討フローを以下のように示し、それぞれのプロセスで検討すべき事項、検討における考え方、判断基準の例などを示す予定である。

### 身元確認手法の検討フロー



## 1) マイナンバーカードを用いた身元確認手法の検討事項

マイナンバーカードを用いた身元確認手法の検討においては、「電子署名の要否」、「スマートフォンのマイナンバーカードの利用」、「複数機能の組み合わせの回避」、「容貌確認の要否」等が主な検討事項となると考えられる。

### 1-a) 電子署名の要否の検討

#### 基本的な考え方

- マイナンバーカードによる身元確認の手法は「電子署名」を行うかどうかで利便性が大きく変わる。
- ユーザビリティ等の観点では、電子署名は用いず券面情報による身元確認を行うことが望ましいため、電子署名については真に必要な場合のみ選択するという考え方で検討する。

#### 検討のポイント

- 対象手続において**厳格な否認防止が必要かどうか**（⇒対象手続が否認された場合のリスクの大きさから判断）
- **根拠法等により電子署名が求められているかどうか**

### 1-b) アクセシビリティ及びユーザビリティに関する検討

#### 基本的な考え方

- 券面情報/電子署名のいずれを用いる場合も「スマートフォンのマイナンバーカード」を利用可能とすることが望ましい。
- また、特に実物のマイナンバーカードでは**複数回読み取る機能の組み合わせ**はできる限り避けることが望ましい。

#### 検討のポイント

- スマートフォンのマイナンバーカードに関して、**実現技術や根拠法等の制約**がないか
- マイナンバーカードの複数の機能を組み合わせず、**単一の機能によって必要な属性情報を収集できないか**

### 1-c) セキュリティに関する検討

#### 基本的な考え方

- 対象手続において貸し借り攻撃の検知が必要な場合は、マイナンバーカードによる手法に加えて、容貌確認の実施が必要となる。
- **貸し借りが行われた場合のリスクの大きさ**を踏まえ、容貌確認の追加実施の要否を検討する。

#### 検討のポイント

- 対象手続において**貸し借りの検知が必要かどうか**（⇒貸し借りが行われた場合のリスクの大きさから判断）
- ビデオベースの容貌確認を行う場合の**特有の脅威への対策**  
（特有の脅威：プレゼンテーション攻撃、インジェクション攻撃）

## 2) マイナンバーカード以外による手法の検討

マイナンバーカード以外の手法の検討については、まずは**事業目的の遂行や公平性の観点から代替手法の要否を検討**する。代替手法が必要な場合は、**対象手続の保証レベルに応じた手法と補完的対策の採用**を検討する。

### 2-a) マイナンバーカード以外による手法の要否の検討

#### 基本的な考え方

- 前述のマイナンバーカードを用いた身元確認に加えて、マイナンバーカード以外による身元確認手法が必要かどうかを、対象手続の**事業目的の遂行や公平性の観点から検討**する。

#### 検討のポイント

- 対象手続の特性（事業目的、想定される利用者層、申請等を行う環境条件、緊急性など）や、マイナンバーカードの普及状況、新規交付にかかる期間等の制約を考慮したうえで、**マイナンバーカード以外による手法を受け付ける必要があるかどうか**。

### 2-b) 採用する代替手法と補完的対策の検討

#### 基本的な考え方


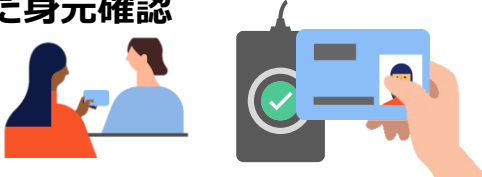


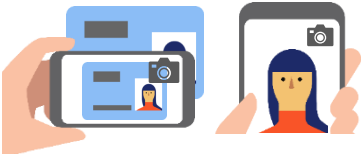

- 採用可能な代替手法は**対象手続の保証レベルによって異なる**。保証レベルを満たす代替手法を確認し、採用する手法を検討する。
- やむを得ず保証レベルを満たさない手法を採用せざるを得ない場合は、**当該手法によって想定されるリスクを低減するための補完的対策**を併せて検討する。

#### 検討のポイント

- マイナンバーカード以外に、どのような本人確認書類を利用可能とする必要があるか。
- 対象手続の保証レベルを踏まえ、どのような手法を採用すべきか。
- （保証レベルを満たさない手法を採用する場合は）リスクを低減するためにどのような補完的対策を講じる必要があるか。

## 2) マイナンバーカード以外による手法の検討 — 保証レベル別の手法例

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、どのような本人確認書類を利用可能とするかによっても異なる**。代表的な手法の一例を以下に示す。

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 <b>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</b> <small>(電子署名不要の場合のみ)</small> 	(該当手法なし)	マイナンバーカード以外の <b>ICチップ付き本人確認書類を 用いた身元確認</b> 
身元確認 保証レベル2	レベル3と同様	<b>本人限定受取郵便 (特定事項伝達型)</b> 	<b>写真付き本人確認書類を用いた 身元確認</b> (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 <b>ビデオベースの身元確認</b> <small>(電子署名不要の場合のみ)</small> 	<b>本人確認書類の郵送 + 住所への到達確認</b> 	レベル2と同様

※上記は代表的な手法の一例である。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。

## 3) 実装モデルと実現手段の検討

マイナンバーカードによる手法、マイナンバーカード以外による手法のそれぞれについて、実装モデルと実現手段を検討する。**実装モデルは本人確認ガイドライン本編にも記載のとおり「連携モデル」を第一候補とする。**

### 3-a) システムの実装モデルの検討

#### 基本的な考え方

- 本人確認ガイドライン本編に基づき「連携モデル」を第一候補として検討する。採用しようとする手法に対応したIDプロバイダが存在するかどうかを確認し、該当するIDプロバイダが存在する場合には、その利用是非を検討する。
- 「非連携モデル」により実装する場合は**完全な独自開発は原則避け、既存の製品、サービス、OSS等の活用を検討する。**

#### 検討のポイント

- 採用する手法に適したIDプロバイダが存在するかどうか。  
(例：デジタル認証アプリ等)
- 候補となるIDプロバイダが提供する機能、連携仕様、保証レベル、制約、リスク等を踏まえたうえで、実際に連携モデルを採用可能であるか。
- 非連携モデルにおいて利用可能な既存の製品等があるか。  
(例：民間企業が提供するeKYCサービス等)

### 3-b) その他の実現手段に係る検討

#### 基本的な考え方

- 対面での身元確認を行う場合は、**身元確認に必要な環境、機器、設備等（例えば窓口の端末やICカードリーダー等）**についての検討が必要である。
- 「本人確認書類の物理的検査」など、人手による検証手法を採用する場合には、**身元確認担当者に対する訓練、マニュアルの整備**など、身元確認を適切に実施するための環境整備についても検討が必要である。

#### 検討のポイント

- 窓口での身元確認の検証強度を確保するために、どのような環境、機器、設備、マニュアル等を整備する必要があるか。
- ICカードの読み取り環境（PC端末、ICカードリーダー等）の準備が難しい場合には、ICカード読み取り用のスマートフォンアプリの活用を検討できないか。  
(例：マイナンバーカード対面確認アプリ等)

### **3. 身元確認手法の選定の考え方**

- 身元確認手法の基本的な考え方
- 身元確認手法の検討フロー
- **ご議論いただきたいポイント**

## 身元確認手法の選定方法に関してご議論いただきたいポイント

前頁までの記載内容（案）を踏まえ、その妥当性、考慮事項、追加で記載を検討すべき事項などについて、委員の皆様からのご意見をいただきたい。

### ご意見・ご議論をいただきたいポイント

---

#### 1. 身元確認手法の基本的構成について

⇒ 「マイナンバーカードを用いた身元確認+マイナンバーカード以外による代替手法」という構成を基本として示すことの妥当性、考慮事項などについて。

（前提：あくまで多くのケースに共通する「考え方」を示すものであり、この構成を必須とするものではない。）

#### 2. 各保証レベルの検討結果（例）について

⇒ あくまで一例ではあるものの、ガイドライン解説書の読者にとっての参考情報となることを踏まえ、適切な例を示せているかどうか。

#### 3. 検討フローにおける考え方、検討ポイントについて

⇒ それぞれの手法の検討における基本的な考え方、検討ポイントなどと言及すべき内容は充足できているか。追加で記載すべき観点やポイントはないか。

## **4. 当人認証手法の選定の考え方**

— **当人認証手法の基本的な考え方**

— 当人認証手法の検討フロー

— ご議論いただきたいポイント

## 本人認証手法の基本的な考え方 — 基本構成

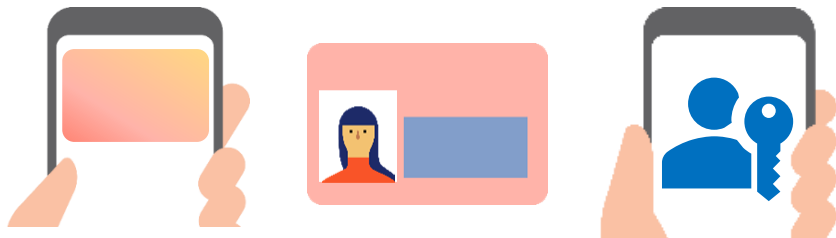
本人認証手法は、昨今の技術動向・脅威動向等を踏まえ、いずれの保証レベルにおいても**マイナンバーカード又はパスキーによる本人認証を第一候補として検討**することを基本とする。そのうえで、必要に応じて保証レベルに応じてその他の手法の採用・併用についての検討を行う。

(ここでは、多くのケースに共通する「考え方」を示すものであり、この構成を必須とするものではない。)

### 本人認証手法の基本的な考え方（案）

#### 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。



+

#### その他の本人認証手法

マイナンバーカード/パスキー以外の本人認証手法の採用・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。

## 本人認証手法の基本的な考え方 — 検討結果（例）

身元確認手法の検討結果の想定例（一例）を示す。本人認証手法は**マイナンバーカード又はパスキーのいずれかを基本としつつ、ワンタイムパスワード等を代替手法として提供する**ことが典型的な採用例の一つとなると考える。

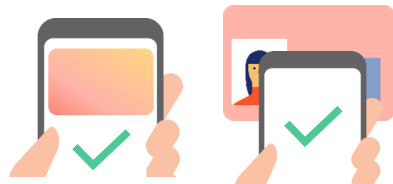
### 身元確認保証レベル3 の検討結果例

- パスキーによる本人認証を基本とし、利用者への利用を推奨する。



+

- パスキーと併せて**マイナンバーカード（利用者証明用電子証明書）**も利用可能とする。



※ この例におけるマイナンバーカードは、パスキーを利用できない方向けの代替手段としてだけでなく、アカウント回復用の本人認証手法としての役割も想定。

### 身元確認保証レベル2 の検討結果例

- パスキーによる本人認証を基本とし、利用者への利用を推奨する。

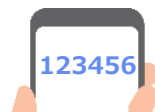


+

- パスキーを利用できない方向けの代替手段として、**パスワード+ワンタイムパスワード**（スマートフォンのTOTPアプリ等）による本人認証を提供する。

\*\*\*\*\*

&



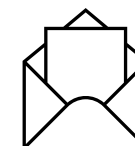
### 身元確認保証レベル1 の検討結果例

- パスキーによる本人認証を基本とし、利用者への利用を推奨する。



+

- パスキーを利用できない方向けの代替手段として、**ワンタイムパスワード**による本人認証を提供する。（電子メールでのコード送付等）



code:  
**999999**

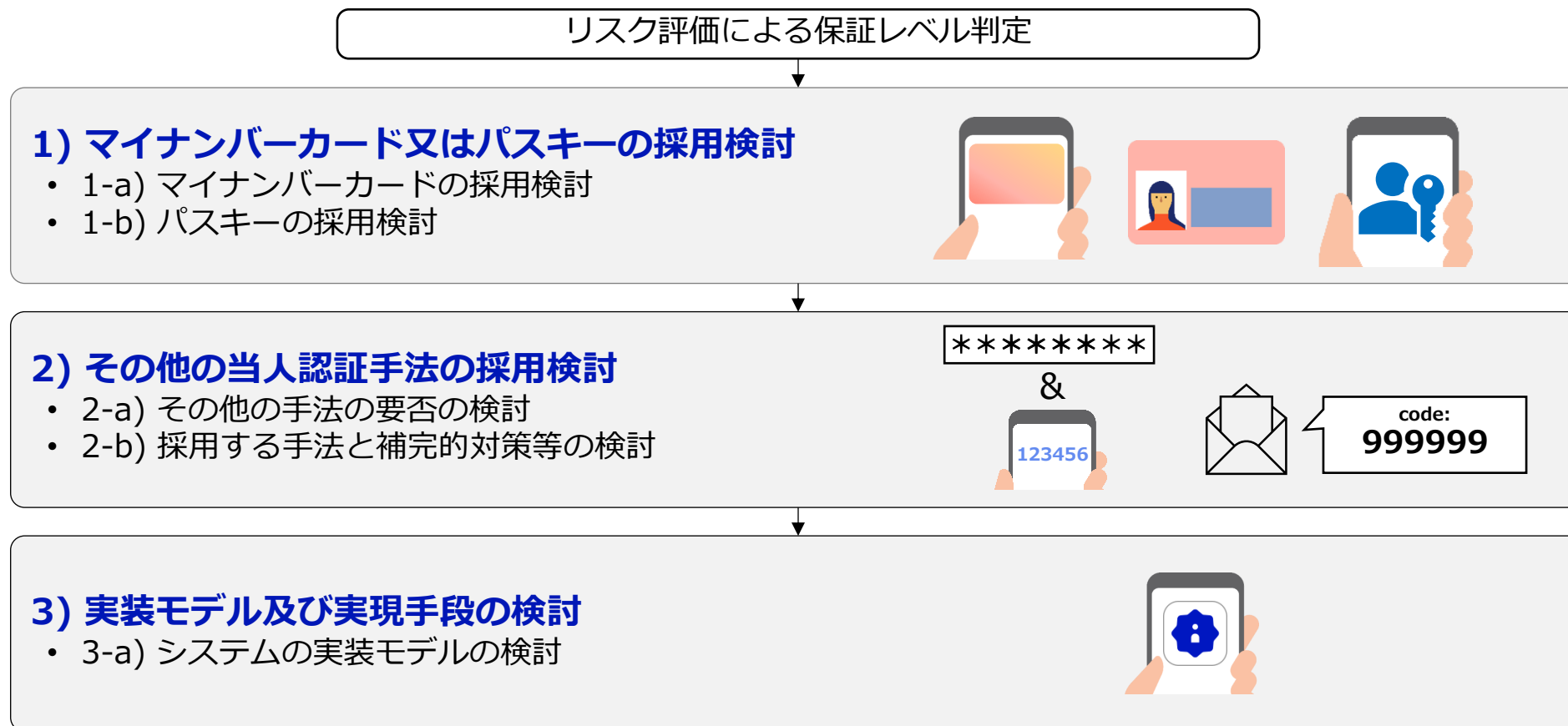
## 4. 当人認証手法の選定の考え方

- 当人認証手法の基本的な考え方
- **当人認証手法の検討フロー**
- ご議論いただきたいポイント

## 当人認証手法の基本的な考え方 — 検討フロー

解説書では、前述の構成を決定するための検討フローを以下のように定め、それぞれで検討すべき事項、検討における考え方、判断基準の例などを示す。

### 当人認証手法の検討フロー



## 1) マイナンバーカード又はパスキーの採用検討

いずれの保証レベルにおいても、まずはマイナンバーカード又はパスキーの利用を第一候補として検討する。保証レベル2以上では**フィッシング耐性を有する手法の提供が必要であるため、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。

それぞれ特徴やメリット・デメリットが異なるため、対象手続の利用者層等に応じて採用する手法を検討する。

### 1-a) マイナンバーカードの採用検討

#### 基本的な考え方

- マイナンバーカードの利用者証明用電子証明書は、適切に実装することでフィッシング攻撃を含む幅広い脅威への耐性をもつ本人認証を実現できる。
- スマートフォンのマイナンバーカード（スマホ搭載電子証明書）を利用可能とすることでユーザビリティも確保できるため、**いずれの保証レベルでも採用候補**となる。

#### 検討のポイント

- 対象手続の根拠法等において、スマートフォンのマイナンバーカードが利用可能かどうか
- デジタル認証アプリをIDプロバイダとした連携モデルの実現可能性（3-aにて後述）

### 1-b) パスキーの採用検討

#### 基本的な考え方

- パスキーは、フィッシング攻撃を含む幅広い脅威への耐性を持ち、ユーザー体験についても従来手法より優位とされるため、**いずれの保証レベルでも採用候補**となる。
- マイナンバーカードを保有しない方でも利用できる手法であるため、対象手続の利用者層等を考慮しつつ採用を検討する。なお、**マイナンバーカードとの併用も検討余地がある**。

#### 検討のポイント

- パスキーを利用可能なデバイスやブラウザなど、パスキー特有の制約や考慮事項についての対応方針の検討（考慮事項については解説書3章に記載）
- マイナンバーカードとの併用の必要性（アカウント回復手段の確保等の観点から）

## 2) その他の本人認証手法の採用検討

1)の検討結果を踏まえつつ、その他の本人認証手法の必要性を検討し、**必要と判断さ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。

### 2-a) その他の手法の要否の検討

#### 基本的な考え方

- マイナンバーカード又はパスキーの採用検討結果を踏まえつつ、対象手続における事業目的の遂行や公平性等の観点から、その他の本人認証手法の採用（併用）の要否を検討する。
- 注）保証レベル3の場合はフィッシング耐性が必須となるため「その他の手法」は採用できない。

#### 検討のポイント

- マイナンバーカード／パスキーを利用しない／できない利用者向けの代替手法を提供する必要があるかどうか。
- マイナンバーカード／パスキーを採用せず、その他の手法のみを採用すべき理由があるか  
（※保証レベル1の場合）

### 2-b) 採用する手法と補完的対策等の検討

#### 基本的な考え方

- その他の手法の採用・併用が必要な場合は、**保証レベルに応じた手法を検討**する。

#### 検討のポイント

- **保証レベル2の場合：**  
パスワード認証＋ワンタイムパスワード認証の組み合わせを基本として考える。  
マイナンバーカード又はパスキーとの併用が前提となる。
- **保証レベル1の場合：**  
ワンタイムパスワード認証（電子メールによる送信等）を基本として考える。  
マイナンバーカード又はパスキーとの併用が望ましいが、対策基準上は併用は必須ではない。

### 3) 実装モデルと実現手段の検討

実装モデルと実現手段の検討については、身元確認の同様の考え方により**連携モデルを第一候補**として検討する。また、非連携モデルを採用する場合でも、**独自開発は原則避け、既存の製品等の活用を検討**することが望まれる。

#### 3-a) システムの実装モデルの検討

##### 基本的な考え方

- 本人確認ガイドライン本編に基づき「**連携モデル**」を第一候補として**検討**する。採用しようとする手法に対応したIDプロバイダが存在するかどうかを確認し、該当するIDプロバイダが存在する場合には、その利用是非を検討する。
- 「非連携モデル」により実装する場合は**完全な独自開発は原則避け、既存の製品、サービス、OSS等の活用を検討**する。

##### 検討のポイント

- 採用する手法に適したIDプロバイダが存在するかどうか。  
(例：デジタル認証アプリ等)
- 候補となるIDプロバイダが提供する機能、連携仕様、保証レベル、制約、リスク等を踏まえたうえで、実際に連携モデルを採用可能であるか。
- 非連携モデルにおいて利用可能な既存の製品等があるか。  
(例：民間企業が提供する認証ソリューション等)

## 4. 当人認証手法の選定の考え方

- 当人認証手法の基本的な考え方
- 当人認証手法の検討フロー
- **ご議論いただきたいポイント**

## 当人認証手法の選定方法に関してご議論いただきたいポイント

前頁までの記載内容（案）を踏まえ、その妥当性、留意事項、追加で記載を検討すべき事項などについて、委員の皆様からのご意見をいただきたい。

### ご意見・ご議論をいただきたいポイント

---

#### 1. 当人認証手法の基本的構成について

⇒ マイナンバーカードとパスキーを軸とした構成を基本として示すことの妥当性、考慮事項などについて。

（前提：あくまで多くのケースに共通する「考え方」を示すものであり、この構成を必須とするものではない。）

#### 2. 各保証レベルの検討結果（例）について

⇒ あくまで一例ではあるものの、ガイドライン解説書の読者にとっての参考情報となることを踏まえ、適切な例を示せているかどうか。

#### 3. 検討フローにおける考え方、検討ポイントについて

⇒ それぞれの手法の検討における基本的な考え方、検討ポイントなどと言及すべき内容は充足できているか。追加で記載すべき観点やポイントはないか。

**デジタル庁**  
**Digital Agency**