資料X

本人確認ガイドライン改定方針
令和5年度中間とりまとめについて

令和6年6月　　トラストTF

本資料について

- 本資料は令和5年度時点のガイドライン改定方針（案段階のものを含む）について今後の検討事項とともに中間的にとりまとめた資料であり、改定方針として確定されたものではありません。
- 最終的な改定方針については今後有識者意見を踏まえた見直しを行ったうえで、関係各所と調整の経て最終化することを予定しています。

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、身分証の偽造技術やフィッシング攻撃の高度化などによって大きく変化している。NISTではSP 800-63-3の改定が進められており、2023年12月には改定案の初期ドラフトが公開された。また、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認証・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の改定に向けた検討を進めている。

本資料は令和5年度に実施した有識者会議の結果を基に、現段階での本人確認ガイドラインの改定方針（案）と今後の検討事項を中間的にとりまとめた文書である。

本資料中の用語・表記について

- NISTと本人確認ガイドラインとの類似用語を区別して議論できるよう、本資料では以下の用語・表記を用いる。
- これら以外のNIST SP 800-63に関する用語等は、原則としてOpenID Foundation Japanによる翻訳版に準拠する。
  ※ここで示す用語は本資料内の定義であり、改定後の本人確認ガイドラインにおける用語を定義するものではない。

用語・表記	本資料中の定義
本人確認ガイドライン ／本ガイドライン	改定検討中の「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」のこと。 現行版のガイドラインのみを指す場合は「現行ガイドライン」のように表記する。
身元確認保証レベル 当人認証保証レベル 認証連携保証レベル	本人確認ガイドラインで定義する各保証レベルのこと。NIST SP800-63のAssurance Levelとの混同を防ぐため、本資料中ではこのように日本語で表記する。また、3種類の保証レベルをまとめて「本人確認保証レベル」と表記する。
NIST IAL NIST AAL NIST FAL	NIST SP800-63 Digital Identity Guidelinesで定義される各Assurance Levelのこと。 本人確認ガイドラインの保証レベルとの混同を防ぐため、明示的に「NIST xAL」と表記する。
対策基準	各保証レベルにおいて求める対策の要求事項のこと。NIST SP800-63 のRequirementsに相当。
本人確認書類の真正性の確認	身元確認時に、提出された本人確認書類の真正性や有効性を検証する行為のこと。 NIST SP800-63A-4の”Evidence Validation”に相当。
申請者と本人確認書類の 紐づきの検証	身元確認時に、申請者が本人確認書類の正当な持ち主であることを検証する行為のこと。 NIST SP800-63A-4の”Verification”に相当。
容貌の照合	申請者と本人確認書類の紐づきの検証のために、本人確認書類の顔写真等と、申請者の容貌等を比較する行為のこと。 NIST SP800-63A-4の”Biometric Comparison”に相当。
リアルタイム型フィッシング	SMS OTP等では防ぐことが難しい、リアルタイムで認証情報を中継するタイプのフィッシング攻撃のことを指す。 （従来型のフィッシング/ファーミングと区別するため、このような表記をする。）

今後の検討事項　―　用語定義について

No.	概要	今後の検討事項
1	“Validation” に対応する訳語の再検討	• 本資料の用語定義では、NISTの“Evidence Validation”に対応する行為を「本人確認書類の真正性の確認」と表記していたが、「確認」という言葉は”Identity Proofing”（身元確認）の訳語としても用いられているため、より適切な訳語や表現がないかを再検討する。
2	“Federation”に対応する訳語の再検討	• 本資料の用語定義では、NISTの”Federation”を当初は「認証連携」と表記していたが、正確には「認証を連携する」というものではないため、より適切な訳語がないか再検討する。 ※本資料中においては仮置きで「認証連携」と表記している。改定度のガイドラインにおいてどのような訳語を用いるかについては今後継続検討する。
3	“Biometric Comparison”に対応する訳語の再検討	• 本資料の用語定義では、NISTの”Biometric Comparison”に対応する行為を「容貌の照合」と表記していたが、この表現のスコープには顔以外の生体情報（指紋等）を用いた方法が含まれない表現となっているため、より適切な表現がないかを再検討する。
4	現行ガイドラインの用語定義全般の見直し・最新化	• 現行ガイドラインの用語定義はNIST SP 800-63-3（一部は63-2）を基にしたものが含まれているため、現在も通用する内容であるかを全面的に確認し、必要に応じて用語の置き換えや定義の見直しを行う。

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を変更** • デジタルによる本人確認がオンラインだけでなく対面にも拡大していることや、改定後のガイドラインの内容・位置づけ等を踏まえ、ガイドラインの適用対象と名称を変更する。
	② ミッション遂行などの基本的な考え方を解説 • 「1.5 基本的な考え方」を新たに設け、ミッション遂行、公平性とアクセシビリティ、プライバシー、ユーザビリティなど、リスク評価プロセスにおいて考慮すべき新たな観点を解説する。
２章 本人確認の枠組み	**③ 本人確認の枠組みを定義・解説** • 2章を新設し、身元確認や当人認証の概念を説明する。現行ガイドラインでは言及のない認証連携についても新たに盛り込み、IDプロバイダを利用する実装モデルとして「認証連携モデル」の解説を追加する。
	④ 保証レベルと対策基準の一部を見直し • NIST SP 800-63-4 におけるxALの改定を参考としつつ、身元確認保証レベルと当人認証保証レベルの位置づけや対策基準を見直す。
３章 本人確認手法の 検討方法	**⑤ リスク評価プロセスを全面的に見直し** • 公平性やプライバシー等の観点も考慮した手法選択が行われるように検討プロセス全体を見直す。 • ガイドライン利用者がリスク評価や本人確認手法の選定を円滑に実施できるよう参考資料を拡充する。

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 政府機関におけるデジタル本人確認に関するガイドライン（仮称）

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　本人確認の基本的要素

2.2　政府機関における本人確認のモデル

2.3　保証レベルと対策基準

3　本人確認手法の検討方法

3.1　デジタル化を念頭に入れた対象手続の業務改革（BPR）

3.2　本人確認に係るリスクの特定

3.3　保証レベルの判定

3.4　本人確認手法の選択

3.5　検討結果の文書化

3.6　継続的な評価と改善

本人確認ガイドライン参考資料

参考資料1　本人確認に係るリスク評価ワークシート

参考資料2　保証レベルに対応する本人確認手法例　等

主要な改定ポイント

①ガイドラインの適用対象と名称を変更

- 「1.2　適用対象」を見直し、本ガイドラインが対象とする本人確認の範囲を一部変更

②ミッション遂行などの基本的な考え方を解説

- ミッション遂行、公平性、アクセシビリティ、プライバシー等の基本的な考え方の解説を冒頭に追加

③本人確認の枠組みを定義・解説

- 身元確認、当人認証、認証連携などの定義と解説を追加
- 認証連携を用いる場合の一般的なモデルの解説を追加

④保証レベルと対策基準を見直し

- 最新の脅威動向等を踏まえ、各保証レベルの区分と対策基準を見直し

⑤リスク評価プロセスを全面的に見直し

- 公平性やプライバシー等の観点も考慮した手法選択が行われるように検討プロセス全体を見直し
- 一連の検討を補助する参考資料を拡充

本人確認ガイドラインの主要な改定ポイント

① ガイドラインの適用対象と名称を変更

本人確認ガイドラインの主要な改定ポイント
① ガイドラインの適用対象と名称を変更

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 政府機関におけるデジタル本人確認に関するガイドライン（仮称）

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　本人確認の基本的要素
- 2.2　政府機関における本人確認のモデル
- 2.3　保証レベルと対策基準

3　本人確認手法の検討方法
- 3.1　デジタル化を念頭に入れた対象手続の業務改革（BPR）
- 3.2　本人確認に係るリスクの特定
- 3.3　保証レベルの判定
- 3.4　本人確認手法の選択
- 3.5　検討結果の文書化
- 3.6　継続的な評価と改善

本人確認ガイドライン参考資料
- 参考資料1　本人確認に係るリスク評価ワークシート
- 参考資料2　保証レベルに対応する本人確認手法例　等

主要な改定ポイント

①ガイドラインの適用対象と名称を変更
- 「1.2　適用対象」を見直し、本ガイドラインが対象とする本人確認の範囲を一部変更

②ミッション遂行などの基本的な考え方を解説
- ミッション遂行、公平性、アクセシビリティ、プライバシー等の基本的な考え方の解説を冒頭に追加

③本人確認の枠組みを定義・解説
- 身元確認、当人認証、認証連携などの定義と解説を追加
- 認証連携を用いる場合の一般的なモデルの解説を追加

④保証レベルと対策基準を見直し
- 最新の脅威動向等を踏まえ、各保証レベルの区分と対策基準を見直し

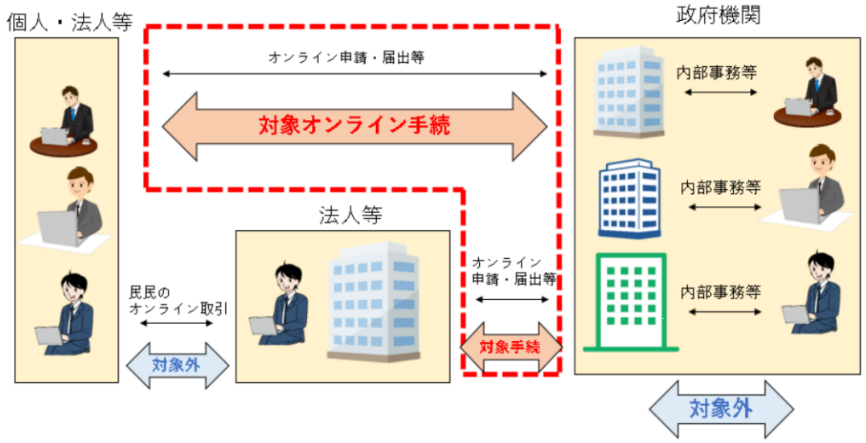
⑤リスク評価プロセスを全面的に見直し
- 公平性やプライバシー等の観点も考慮した手法選択が行われるように検討プロセス全体を見直し
- 一連の検討を補助する参考資料を拡充

本人確認ガイドラインの主要な改定ポイント
① ガイドラインの適用対象と名称を変更

ガイドラインの適用対象の見直し方針

- 本人確認を取り巻く環境の変化等を踏まえ、適用対象の見直しを行う。

現行ガイドライン
１．２　適用対象
　各府省が法令等に基づき行う行政手続をデジタル化する際に、個人又は法人等の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ものであり、そのうち、個人・法人等と政府との間の申請・届出等のオンライン手続の全て（以下「対象オンライン手続」という。）とする。代理人による申請について、代理権の付与の確認は手続ごとの要件に従い、利用者として代理人が申請する場合の本人確認については本ガイドラインを参考にできるため利用されたい。



適用対象の見直し方針（案）

❶「オンラインによる本人確認」 → 対面等も含める

- マイナンバーカードを活用した本人確認はオンラインだけでなく対面にも広まっていることなどを考慮し、オンラインだけでなく対面等での本人確認も適用対象に含める。

❷「個人又は法人等の」 → 個人向け／法人向けで分冊化

- 法人の本人確認は、個人（自然人）の本人確認とは異なる検討事項が多いため、個人向けと法人向けでガイドラインを分冊化する方針とする。法人向け部分は、将来的には別文書として管理することも検討する。

❸「行政手続」 → 内部事務への将来的な拡大を検討

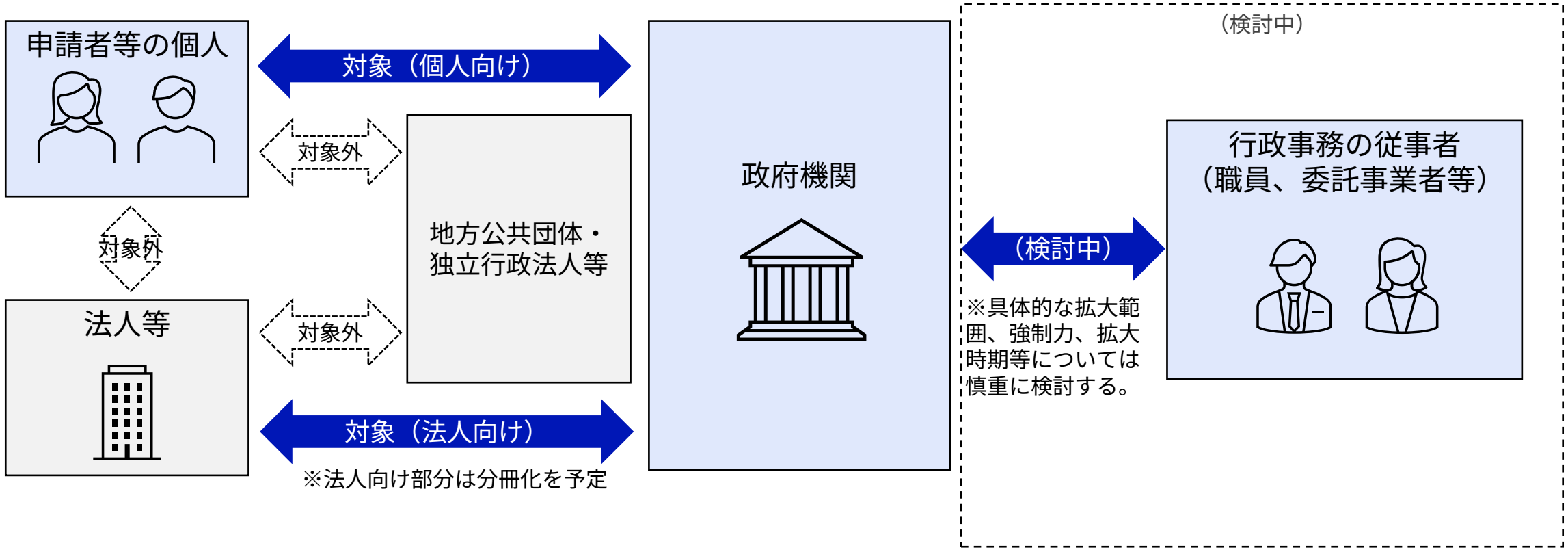
- 行政の内部事務においても情報システムの利用時などで職員等を認証する機会は多くあるため、本ガイドラインを内部事務にも適用すべきでないか検討する。
- ただし影響範囲が非常に広い変更となるため、具体的な拡大範囲、強制力、拡大時期等については慎重に検討する。

本人確認ガイドラインの主要な改定ポイント
① ガイドラインの適用対象と名称を変更

ガイドラインの適用対象の見直しイメージ

- 適用範囲の見直しイメージは以下のとおり。
- 「行政事務の従事者」への適用拡大については影響が非常に大きいため、拡大の可否も含めて検討する。

適用範囲の見直しイメージ



本人確認ガイドラインの主要な改定ポイント
① ガイドラインの適用対象と名称を変更

今後の検討事項　―　適用対象の見直しについて

No.	概要	今後の検討事項
1	法人と個人の関係性に着目した整理について	• 法人の本人確認に関するガイドラインの分冊化については、個人と法人の関係性をどのように表現して認証するかという観点に立った整理を行う。 • 分冊化の議論では、身元確認と当人認証を分けて考える。法人に所属する自然人の当人認証については個人向けと共通する部分が多いため、本ガイドラインの対象に残すことも含めて検討する。
2	法人向けガイドラインの分冊化の方法・タイミングについて	• 法人の本人確認に関するガイドラインを分冊化する場合においても、改定のタイミングで空白期間が生じないよう、現行ガイドライン相当の対策基準が最低限維持されるような方法での分冊化を検討する。
3	内部事務への拡大方針について	• 内部事務への拡大方針については、有識者会議での以下の意見も踏まえつつ、引き続き拡大範囲、強制力、拡大時期等の検討を行う。 （有識者会議での主な意見） – 対象を拡大する場合、国民向けサービスと内部向けサービスではリスクや影響範囲が明らかに異なるため、これを考慮した記載とすべきである – 内部事務に従事する委託事業者を対象とする場合、法人向けガイドラインを別冊化することとの整合性の確保が必要である

本人確認ガイドラインの主要な改定ポイント

② ミッション遂行などの「基本的な考え方」を解説

本人確認ガイドラインの主要な改定ポイント
② ミッション遂行などの「基本的な考え方」を解説

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 政府機関におけるデジタル本人確認に関するガイドライン（仮称）

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　本人確認の基本的要素
- 2.2　政府機関における本人確認のモデル
- 2.3　保証レベルと対策基準

3　本人確認手法の検討方法
- 3.1　デジタル化を念頭に入れた対象手続の業務改革（BPR）
- 3.2　本人確認に係るリスクの特定
- 3.3　保証レベルの判定
- 3.4　本人確認手法の選択
- 3.5　検討結果の文書化
- 3.6　継続的な評価と改善

本人確認ガイドライン参考資料
- 参考資料1　本人確認に係るリスク評価ワークシート
- 参考資料2　保証レベルに対応する本人確認手法例　等

主要な改定ポイント

①ガイドラインの適用対象と名称を変更
- 「1.2　適用対象」を見直し、本ガイドラインが対象とする本人確認の範囲を一部変更

②ミッション遂行などの基本的な考え方を解説
- ミッション遂行、公平性、アクセシビリティ、プライバシー等の基本的な考え方の解説を冒頭に追加

③デジタル本人確認の枠組みを定義・解説
- 身元確認、当人認証、認証連携などの定義と解説を追加
- 認証連携を用いる場合の一般的なモデルの解説を追加

④保証レベルと対策基準を見直し
- 最新の脅威動向等を踏まえ、各保証レベルの区分と対策基準を見直し

⑤リスク評価プロセスを全面的に見直し
- 公平性やプライバシー等の観点も考慮した手法選択が行われるように検討プロセス全体を見直し
- 一連の検討を補助する参考資料を拡充

本人確認手法の検討にあたる「基本的な考え方」を５つの観点から解説

- 今回の改定では「ミッション遂行」、「公平性」、「プライバシー」といった現行ガイドラインでは言及されていない観点を取り入れるため、これらの解説を第１章の「1.5　基本的な考え方」として追加する。

「1.5　基本的な考え方」として解説する５つの観点（概要）

“基本的な考え方”	**1) ミッション遂行**	• 本人確認が障壁となって行政手続が達成しようとするミッションが阻害されてはならないと考える。採用しようとする本人確認手法にミッション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	• 利用者の人種、性別、年齢、住む地域などによらず誰もが利用できる行政手続としなければならないと考える。採用しようとする本人確認手法に公平性の懸念がある場合には、代替手段や例外措置を検討する。
	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と考える。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、ミッション遂行や公平性、プライバシーなどにも影響を与えうる重要な要素であると考える。
	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と考える。公平性、プライバシー、ユーザビリティ等への影響も考慮しながら、リスクに応じたレベルの本人確認手法を選択することが必要である。

本人確認ガイドラインの主要な改定ポイント
② ミッション遂行などの「基本的な考え方」を解説

今後の検討事項　―　「基本的な考え方」の記載方法について

No.	概要	今後の検討事項
1	「セキュリティ」に関する記載内容の明確化	• 単に「セキュリティ」と書くだけでは範囲が広い。ここで言及しているセキュリティが何を指しているのかを明確に定義し、達成を目指すセキュリティゴールが明確になるような記載案を検討する。 • 資料では、セキュリティと他の概念が対立することが前提のような書き方になっている。実際にはトレードオフになる「場合もある」が正しいため、表現を見直す。
2	「プライバシー」に関する記載内容の見直し	• 現在の案はOECDの8原則のうちいくつかを抜粋しているが、抜粋は妥当であるのか、その他の原則に言及する必要はないのか等を再検討する。
3	「公平性」「アクセシビリティ」「ユーザビリティ」の関係の整理	• 「ユーザビリティ」と「アクセシビリティ」は内容の一部が重複するようにも見えるため、それぞれの定義の明確化、項目の統合などを検討する。 • 「公平性を確保するためにアクセシビリティやユーザビリティに配慮する」といった関係性にも思えるため、これらを横並びに示すことが適当かどうかを再検討する。
4	デジタル以外の手段も含めた公平性の確保について	• 公平性をデジタルだけで満たす必要があるように受け取られかねないため、「対面や郵送での本人確認なども含めて公平性が確保されるべき」という趣旨が正しく伝わるような記載案を検討する。
5	その他の見直し	• NISTの”Trusted Referees”に相当する概念を盛り込むことができないか検討する。 • NISTでは社会保障番号（SSN）にも言及されている。同じような言及が必要ないかを検討する。 • 一度きりの検討ではなく継続的な評価と改善が重要であるという点を盛り込むことを検討する。 • 「発見的統制」などの用語はガイドラインの読者にも理解できる表現へと見直す。

本人確認ガイドラインの主要な改定ポイント

③ 本人確認の枠組みを定義・解説

本人確認ガイドラインの主要な改定ポイント
③ 本人確認の枠組みを定義・解説

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 政府機関におけるデジタル本人確認に関するガイドライン（仮称）

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　本人確認の基本的要素
2.2　政府機関における本人確認のモデル
2.3　保証レベルと対策基準

3　本人確認手法の検討方法
3.1　デジタル化を念頭に入れた対象手続の業務改革（BPR）
3.2　本人確認に係るリスクの特定
3.3　保証レベルの判定
3.4　本人確認手法の選択
3.5　検討結果の文書化
3.6　継続的な評価と改善

本人確認ガイドライン参考資料
参考資料1　本人確認に係るリスク評価ワークシート
参考資料2　保証レベルに対応する本人確認手法例　等

主要な改定ポイント

①ガイドラインの適用対象と名称を変更
- 「1.2　適用対象」を見直し、本ガイドラインが対象とする本人確認の範囲を一部変更

②ミッション遂行などの基本的な考え方を解説
- ミッション遂行、公平性、アクセシビリティ、プライバシー等の基本的な考え方の解説を冒頭に追加

③デジタル本人確認の枠組みを定義・解説
- 身元確認、当人認証、認証連携などの定義と解説を追加
- 認証連携を用いる場合の一般的なモデルの解説を追加

④保証レベルと対策基準を見直し
- 最新の脅威動向等を踏まえ、各保証レベルの区分と対策基準を見直し

⑤リスク評価プロセスを全面的に見直し
- 公平性やプライバシー等の観点も考慮した手法選択が行われるように検討プロセス全体を見直し
- 一連の検討を補助する参考資料を拡充

本人確認ガイドラインの主要な改定ポイント
③ 本人確認の枠組みを定義・解説

本人確認の基本的要素の定義・解説

- 「身元確認」と「当人認証」に加えて、NISTのFederationに相当する「認証連携」（アイデンティティ連携）を新たに定義する。また、各要素の解説を2章に新設する。

身元確認
→現行ガイドラインの記載を基に定義・解説

手続やサービスの利用者を一意に識別するために必要となる氏名等の属性情報を確認・検証し、手続/サービスの利用者として登録するプロセス。

本人確認書類の真正性の確認、申請者と本人確認書類の申請者の紐づきの検証等を行うことで、次のような事項を確認することを目的とする。

- 本人確認書類に記載された人物と同一の人物であること
- 現実に存在している人物であること（架空の人物でないこと）
- 生存している人物であること
- 当該手続/サービスにおいて同一人物が既に登録されていないこと　等

当人認証
→現行ガイドラインの記載を基に定義・解説

手続やサービスを利用しようとする者が、身元確認プロセスで登録した者と同一人物であること（当人性）を、認証情報の照合によって確認するプロセス。

以下のような脅威に対策するため、認証の3要素である知識・所有物・生体の1つ又は複数の組み合わせた認証情報を用いる。

- 認証情報の推測・盗聴・分析
- 中間者攻撃
- リプレイ攻撃
- フィッシング／ファーミング
- リアルタイム型フィッシング
- 多要素認証疲労攻撃　等

認証連携
→NISTの定義等を参考として新たに定義

身元確認時の属性情報の収集や当人認証における認証処理を、IDプロバイダ（IdP）と連携して処理すること。

認証連携によりサービス利用側・提供側それぞれに以下のようなメリットが期待できるため、適切なIDプロバイダが存在する場合には認証連携の採用を検討することが望ましい。

サービス利用側のメリット：
- サービス申請・登録の負担軽減
- サービスごとに認証情報（パスワード等）を管理する負担の解消
- 当人認証時のユーザ体験の統一

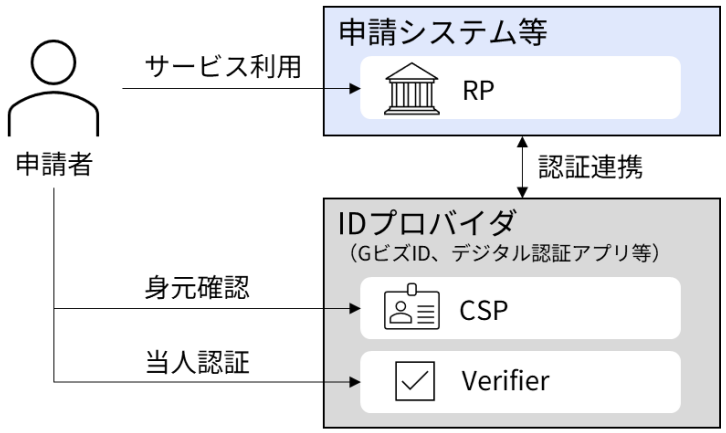
サービス提供側のメリット：
- IDプロバイダ機能の構築、運用等に要するコストの低減

本人確認ガイドラインの主要な改定ポイント
③ 本人確認の枠組みを定義・解説

政府機関における本人確認のモデル（案）

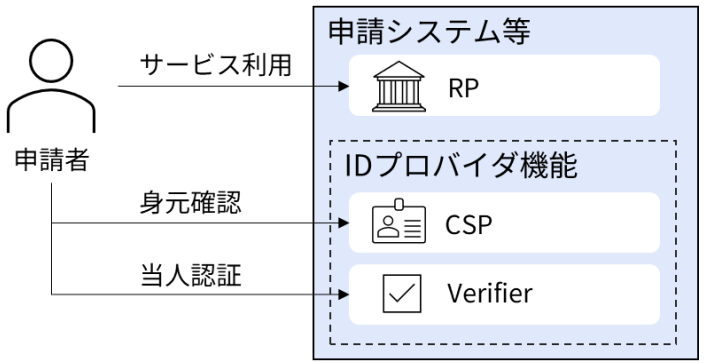
- 政府機関における典型的な本人確認モデルを定義し、解説を記載する。
- NIST SP 800-63-4を参考としつつ、GビズIDやマイナポータル等の政府のIDプロバイダの整備状況を踏まえた本人確認モデルを検討中。現段階でのモデル案は以下のとおり。

❶ 認証連携モデル
（NIST Federated Model相当）



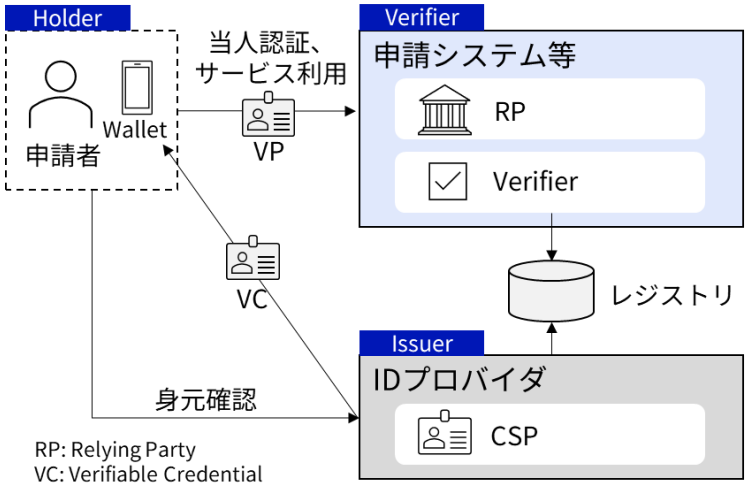
RP: Relying Party
CSP: Credential Service Provider

❷ 非認証連携モデル
（NIST Non-federated Model相当）



RP: Relying Party
CSP: Credential Service Provider

❸ ウォレットモデル（仮称）

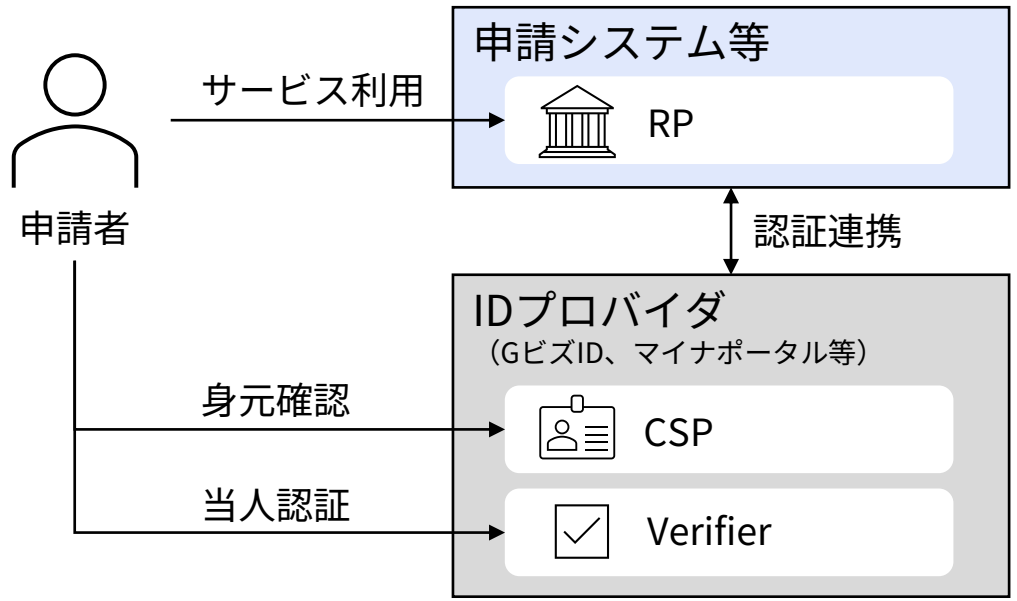


RP: Relying Party
VC: Verifiable Credential
VP: Verifiable Presentation

モデル案❶ 認証連携モデル（Federated Model）

- IDプロバイダと連携して身元確認や当人認証を行うモデル。適切なIDプロバイダを活用できれば、利用者側・サービス提供側の双方にとってメリットが期待できる。
- 行政手続において利用可能なIDプロバイダとしては、 GビズIDやマイナポータル等を想定。

❶ 認証連携モデル（Federated Model）



RP: Relying Party
CSP: Credential Service Provider

メリット・デメリット

- 利用者にとってはシステムごとのアカウントや認証情報を管理する必要がなくなるメリットがあり、認証時のユーザ体験も統一される。
- 各システムにとってはIDプロバイダ機能を既存システムによって実現できるため、構築コストや運用コストの削減、システム品質の均一化が期待できる。

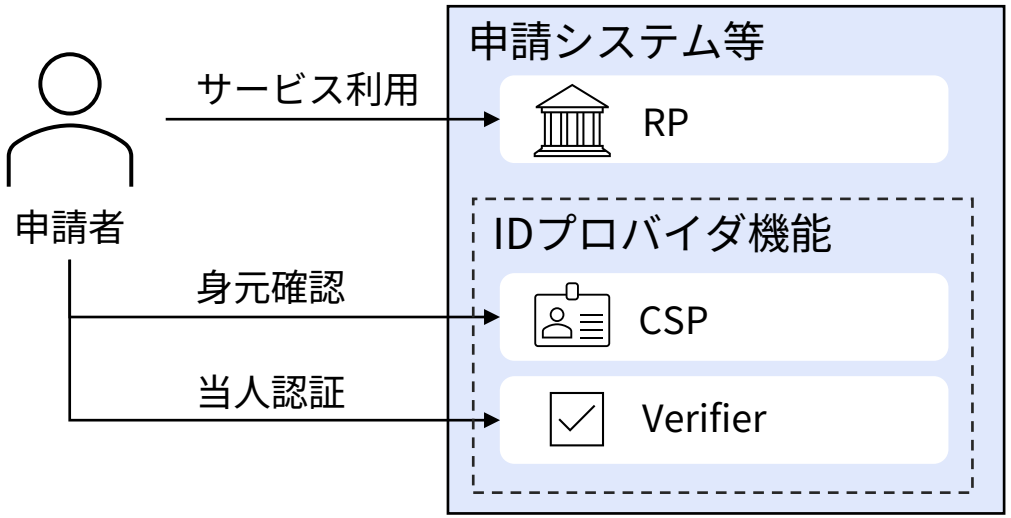
留意点等

- 各システムが必要としている保証レベルを満たすIDプロバイダの存在が前提となる。
- 認証連携に関する脅威への対策が必要。

モデル案❷ 非認証連携モデル（Non-federated Model）

- IDプロバイダ機能とRPとを一体として構築し、認証連携を行わないモデル。システム自らがIDプロバイダ機能の構築・運用を行う必要がある。

❷ 非認証連携モデル（Non-federated Model）



メリット・デメリット

- 利用者にとっては、システムごとにアカウントを管理する手間が生じる。
- 各システムにとっては、自システムの要求に応じたIDプロバイダ機能を構築できるメリットがあるが、独自のIDプロバイダを構築・運用するためのコストが生じる。

留意点等

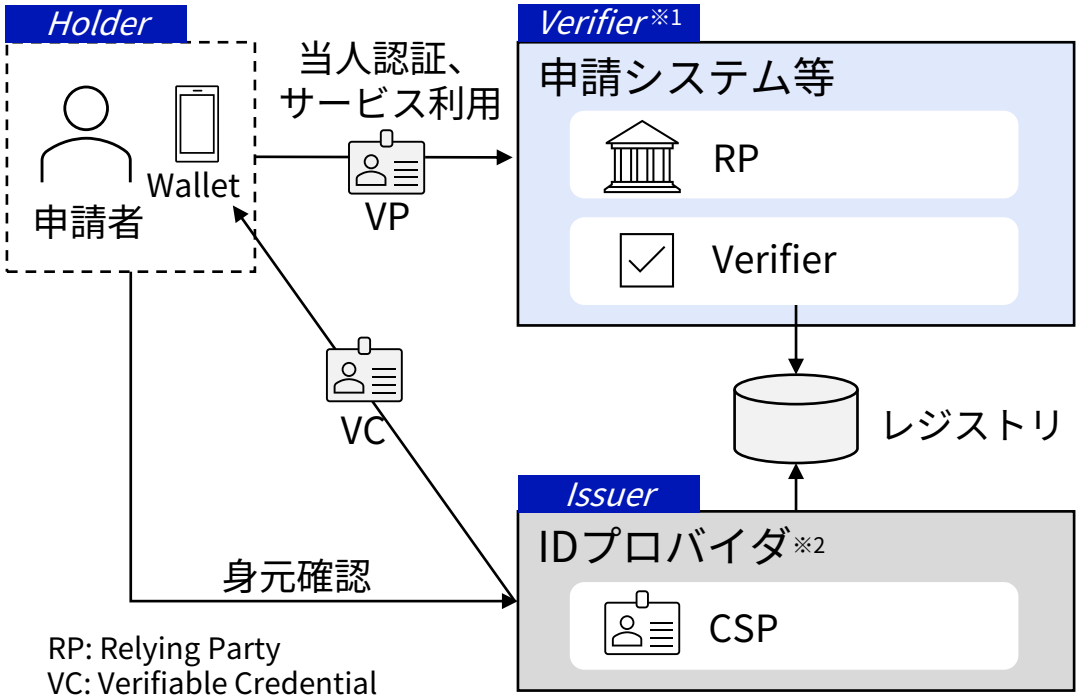
- 自システム内にIDプロバイダ機能を構築する場合であっても、認証連携プロトコルを介した連携を行う場合には「認証連携モデル」としてリスク分析が必要。

RP: Relying Party
CSP: Credential Service Provider

モデル案❸ ウォレットモデル（仮称）

- 証明書等をVC（Verifiable Credential）として申請者に発行し、申請システム側は申請者から提示されたVP（Verifiable Presentation）を検証することで身元確認や当人認証を行うモデル。
- モデル案❶、❷と横並びに扱うことの妥当性も含めて継続検討する。

❸ ウォレットモデル（仮称）



メリット・デメリット

- *Issuer*と*Verifier*※1の間に直接的なシステム接続関係がなくとも、提示された身元確認情報の真正性を検証可能となる。
- 認証連携モデルにおけるプライバシー面での留意事項（RPの利用状況をIDプロバイダが把握可能になる）を解消できる。

留意点等

- まだ普及前のモデルであるが、NIST SP 800-63-4にも盛り込まれる予定※3とされているため、我が国の行政手続でも将来的に採用され得るモデルとして検討中。

※1　本頁中の斜体の *"Verifier"* はIssuer-Holder-Verifierモデルに準じたものであり、他のモデル案にある「Verifier」とは異なる概念である。
※2　他のモデル案との比較のため便宜上「IDプロバイダ」と表記しているが正確な呼称ではないため、今後用語を見直す予定。
※3　A Note on progress…NIST's Digital Identity Guidelines. | NIST より

今後の検討事項　―　本人確認の枠組みについて

No.	概要	今後の検討事項
1	ウォレットモデル（仮称）に関する継続検討	• NIST SP 800-63-4 second public draftにおいてIssuer-Holder-Verifierモデルの盛り込みが予定されているため、NISTの動向を確認しつつウォレットモデルに関して継続検討する。 • 現在のウォレットモデルの案は「Verifier」「IDプロバイダ」「CSP」など、的確ではない用語の使い方が含まれているため、他のモデルとの整合を考慮しつつ用語を見直す。 • 「属性プロバイダ」の存在を明示して整理することで、ウォレットモデルを他のモデルと統合的に扱うことができないか検討する。 • ウォレットモデルは「検証可能な資格情報」に着目したものであるため、他のモデルとは並列には扱わず、別の枠組みとして整理することも検討する。
2	認証連携モデルと非認証連携モデルのハイブリッドモデルの必要性の検討	• 一部の行政手続では、認証連携モデルを基本としつつ非認証連携モデルを代替手段として併用することで、複数の認証方式に対応しようとするケースも想定される。 • このようなケースを想定したハイブリッドモデルを本ガイドラインにおいて定義する必要がないか検討する。
3	認証連携モデルにおける政府以外のIDプロバイダとの連携について	• 民間企業や大学など、政府以外のIDプロバイダとの認証連携を想定したモデルを本ガイドラインで定義すべきかどうか検討する。トラストフレームワーク等の考え方についても、どこまで本ガイドラインに盛り込むべきか検討する。
4	認証連携モデルに関連する脅威やインシデント事例の整理	• 認証連携モデル特有のリスクに関して、過去のインシデント事例等を踏まえながら想定脅威をマトリクス形式などで整理し、ガイドラインに掲載することを検討する。

本人確認ガイドラインの主要な改定ポイント

④ 保証レベルと対策基準の一部を見直し

本人確認ガイドラインの主要な改定ポイント
④ 保証レベルと対策基準の一部を見直し

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 政府機関におけるデジタル本人確認に関するガイドライン（仮称）

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　本人確認の基本的要素
2.2　政府機関における本人確認のモデル
2.3　保証レベルと対策基準

3　本人確認手法の検討方法
3.1　デジタル化を念頭に入れた対象手続の業務改革（BPR）
3.2　本人確認に係るリスクの特定
3.3　保証レベルの判定
3.4　本人確認手法の選択
3.5　検討結果の文書化
3.6　継続的な評価と改善

本人確認ガイドライン参考資料
参考資料1　本人確認に係るリスク評価ワークシート
参考資料2　保証レベルに対応する本人確認手法例　等

主要な改定ポイント

①ガイドラインの適用対象と名称を変更
- 「1.2　適用対象」を見直し、本ガイドラインが対象とする本人確認の範囲を一部変更

②ミッション遂行などの基本的な考え方を解説
- ミッション遂行、公平性、アクセシビリティ、プライバシー等の基本的な考え方の解説を冒頭に追加

③デジタル本人確認の枠組みを定義・解説
- 身元確認、当人認証、認証連携などの定義と解説を追加
- 認証連携を用いる場合の一般的なモデルの解説を追加

④保証レベルと対策基準を見直し
- 最新の脅威動向等を踏まえ、各保証レベルの区分と対策基準を見直し

⑤リスク評価プロセスを全面的に見直し
- 公平性やプライバシー等の観点も考慮した手法選択が行われるように検討プロセス全体を見直し
- 一連の検討を補助する参考資料を拡充

本人確認ガイドラインの主要な改定ポイント

④ 保証レベルと対策基準の一部を見直し

A. 身元確認保証レベルの見直し

本人確認ガイドラインの主要な改定ポイント
④ 保証レベルと対策基準の一部を見直し

身元確認保証レベルの見直し（案）概要

	身元確認保証レベルの位置づけ	改定のポイント
身元確認 保証レベル3	**対面での身元確認を原則とする保証レベル** • 対面での身元確認を原則として位置付ける。 • 本人確認リスクが極めて大きい一部の行政手続のみが該当し、一般的な行政手続は該当しないレベルとして想定。	• NIST IAL3相当となるよう対策基準を厳格化する （トラストタスクフォースで別途検討中の「政府機関における個人アイデンティティの検証（Personal Identity Verification）」等での活用を想定。）
身元確認 保証レベル2	**オンラインでの身元確認も可能な保証レベル** • 対面又はリモートでの身元確認が可能な保証レベルとして位置付ける。 • 多くの行政手続が該当する保証レベルとして想定。	• 多く手法がレベル2に該当することを考慮しレベル2を細分化する
身元確認 保証レベル１	**登録コードによる身元確認も可能な保証レベル** • 「登録コード」（電子メールや郵送等で送付した番号等）を使った身元確認を認める保証レベルとして位置付ける。 （登録コードの入力確認は対面又はオンラインで行う。）	• レベル2よりも簡易的な保証レベルとして「レベル1」を新たに定義する
身元確認 保証レベル0	**身元確認を必要としないレベル** • 身元確認を行わない場合のレベル。行政手続は基本的に該当しないと想定しているが、形式上定義する。	• 現行ガイドラインのレベル1（身元確認なし）は「レベル0」に繰り下げる

本人確認ガイドラインの主要な改定ポイント
④ 保証レベルと対策基準の一部を見直し

身元確認保証レベルの対策基準（案）

<table>
<tr><th colspan="2" rowspan="2">対策基準</th><th colspan="3">各保証レベルの要求事項</th></tr>
<tr><th>レベル3</th><th>レベル2</th><th>レベル1</th></tr>
<tr><td colspan="5">身元確認の実施場所（Presence）</td></tr>
<tr><td colspan="2">対面</td><td>✓</td><td rowspan="2">✓
いずれか</td><td rowspan="2">✓
いずれか</td></tr>
<tr><td colspan="2">リモート</td><td>△※1</td></tr>
<tr><td colspan="5">申請者と本人確認書類の紐づきの検証方法（Verification）</td></tr>
<tr><td rowspan="2">生体情報や
容貌の比較</td><td>a) 申請者の容貌等を対面で確認し、本人確認書類と比較する</td><td>✓※2</td><td rowspan="3">✓
いずれか</td><td rowspan="3">✓
いずれか</td></tr>
<tr><td>b) 申請者の容貌等をリモート（カメラ越し）で確認し、本人確認書類と比較する</td><td>—</td></tr>
<tr><td rowspan="2">暗証番号等
による認証</td><td>c) 本人確認書類の認証機能（暗証番号等）により認証する</td><td>—</td></tr>
<tr><td>d) 住所等に送付した登録コードにより検証する</td><td>—</td><td>—</td></tr>
<tr><td colspan="5">本人確認書類の真正性の確認方法（Validation）</td></tr>
<tr><td rowspan="2">電子的な
検証</td><td>e) ICチップ内のデータの電子署名を検証する（※有効性確認を含む）</td><td>✓</td><td rowspan="5">✓
いずれか</td><td rowspan="5">✓
いずれか</td></tr>
<tr><td>f) ICチップ内の券面画像と券面を比較する</td><td>—</td></tr>
<tr><td rowspan="3">物理的な
検証</td><td>g) 券面の真正性を目視等による外観検査で確認する</td><td>—</td></tr>
<tr><td>h) 券面の真正性をリモート（カメラ越し）で確認する</td><td>—</td></tr>
<tr><td>i) 券面の真正性を券面の写し（コピー）で確認する</td><td>—</td><td>—</td></tr>
</table>

※1 保証レベル3における統制環境下のリモート身元確認（Supervised Identity Remote Proofing相当）については具体条件を検討中
※2 保証レベル3においてはVerification時に生体情報（顔写真等）の記録を行うことを想定

本人確認ガイドラインの主要な改定ポイント
④ 保証レベルと対策基準の一部を見直し

身元確認保証レベルの対策基準（案）　―　レベル2の細分化（案）

対策基準		各保証レベルの要求事項						
		レベル3	レベル2					レベル1
			2A	2B	2C	2D	2E	
身元確認の実施場所（Presence）								
対面		✓	✓	—	—	✓	—	✓ いずれか
リモート		△※1	—	✓	✓	—	✓	
申請者と本人確認書類の紐づきの検証方法（Verification）								
生体情報や容貌の比較	a) 申請者の容貌等を対面で確認し、本人確認書類と比較する	✓※2	✓	—	—	✓	—	✓ いずれか
	b) 申請者の容貌等をリモート（カメラ越し）で確認し、本人確認書類と比較する	—	—	✓	—	—	✓	
暗証番号等による認証	c) 本人確認書類の認証機能（暗証番号等）により認証する	—	—	—	✓	—	—	
	d) 住所等に送付した登録コードにより検証する	—	—	—	—	—	—	
本人確認書類の真正性の確認方法（Validation）								
電子的な検証	e) ICチップ内のデータの電子署名を検証する（※有効性確認を含む）	✓	✓ いずれか	✓ いずれか	✓ いずれか	—	—	✓ いずれか
	f) ICチップ内の券面画像と券面を比較する	—				—	—	
物理的な検証	g) 券面の真正性を目視等による外観検査で確認する	—	—	—	—	✓	—	
	h) 券面の真正性をリモート（カメラ越し）で確認する	—	—	—	—	—	✓	
	i) 券面の真正性を券面の写し（コピー）で確認する	—	—	—	—	—	—	

※1 保証レベル3における統制環境下のリモート身元確認（Supervised Identity Remote Proofing相当）については具体条件を検討中
※2 保証レベル3においてはVerification時に生体情報（顔写真等）の記録を行うことを想定

今後の検討事項　―　身元確認保証レベルの見直しについて

No.	概要	今後の検討事項
1	保証レベル3の対策基準の詳細検討	• 厳格化を予定している身元確認保証レベル3の対策基準に関して、次の事項を検討する。 – 統制環境下でのリモート身元確認（NIST Supervised相当）の具体的な条件 – 必要な本人確認書類の点数（NISTは最低でも2点が必要） – 申請者の顔写真等の収集（NIST Biometric Collection相当）の目的と必要性の再整理
2	保証レベル1の対策基準の詳細検討	• 保証レベル1はNIST SP 800-63-4 initial public draftのIAL1を参考として検討中のレベルであるが、現在の案ではレベル2との差があまりなく、ユースケースも明確でない。 • IAL1はSP 800-63-4 second public draftで見直し予定とされているため、今後のNISTの改定動向も参考としながらレベル1の対策基準を継続検討する。
3	郵送による手法の位置づけの整理	• 本人確認書類のコピーを郵送するタイプの手法が、現在の対策基準（案）のどこに該当するのかが明確となるよう整理する。 • 本人受取型郵便を活用する場合の手法についても、どのレベルに該当するのか整理する。
4	デジタル署名を必須とする方針とブートストラップ問題の整理	• 保証レベル3のValidationにおいて、本人確認書類のデジタル署名による検証を必須とした場合のブートストラップ問題（クレデンシャル紛失時などに再発行する手段がなくなる問題）を整理し、実現性や例外措置などを検討する。
5	本人確認書類に対する要求事項の整理	• 各保証レベルで必要な本人確認書類の条件（写真付き、ICチップ付き、暗証番号の有無等）を整理し、対策基準としてとりまとめる。 • 券面の物理的の真正性については、真贋判定機を使用有無についても考慮した検討を行う。

本人確認ガイドラインの主要な改定ポイント

④ 保証レベルと対策基準の一部を見直し

B. 当人認証保証レベルの見直し

本人確認ガイドラインの主要な改定ポイント
④ 保証レベルと対策基準の一部を見直し

当人認証保証レベルの見直し（案）概要

	当人認証保証レベルの位置づけ	改定のポイント
当人認証 保証レベル３	**耐タンパ性ハードウェアを含む２要素認証** • 耐タンパ性ハードウェアによる認証を含む２要素以上の多要素認証を必須とする保証レベルとする。 • なりすまし等のリスクが大きく厳格な当人認証が求められる行政手続向けのレベルとして想定。	• リアルタイム型フィッシング攻撃への耐性を「必須」とする
当人認証 保証レベル２	**２要素認証** • ２要素以上の多要素認証を必須とする保証レベルとする。多くの行政手続が該当する、中程度のリスクに対応する保証レベルとして想定。	• リアルタイム型フィッシング攻撃への耐性は「推奨」とする • 多く手法がレベル2に該当することを考慮しレベル2を細分化
当人認証 保証レベル１	**単要素認証** • 単要素での認証を認める保証レベルとする。 • なりすまし等のリスクが小さいとみなせる行政手続向けの保証レベルとして想定。	• 大きな変更なし （リアルタイム型フィッシング攻撃への耐性は不要）

本人確認ガイドラインの主要な改定ポイント
④ 保証レベルと対策基準の一部を見直し

当人認証保証レベル２の細分化（案）

青字：主な改定ポイント

対策基準項目		対策基準（案）				
		当人認証保証レベル3	当人認証保証レベル2			当人認証保証レベル1
			レベル2A	レベル2B	レベル2C	
認証要素		耐タンパ性が確保されたHWトークンを含む２要素	２要素			単要素
脅威耐性（新規）	リアルタイム型フィッシング ：ユーザの入力をリアルタイムに中継することでSMSOTP等の2段階認証を突破するタイプのフィッシング攻撃	必須	必須	不要	不要	不要
	多要素認証疲労攻撃 ：大量の認証要求（プッシュ通知）を送り付けることでユーザを疲れさせ認証ボタンを押させる攻撃	必須	必須	必須	不要	不要
	誤ったログイン ：ユーザが意図せず他のアカウントへの認証に成功しログインしてしまうこと	必須	必須	必須	必須	不要
脅威耐性（現行ガイドライン定義済み）	フィッシング／ファーミング※	必須	必須			不要
	リプレイ攻撃※	必須	必須			不要
	中間者攻撃※	必須	必須			必須
	オンライン上の推測※	必須	必須			必須
	盗聴による認証情報の取得※	必須	必須			必須

※現行ガイドラインに掲載されている脅威については具体的な定義を見直し予定

本人確認ガイドラインの主要な改定ポイント
④ 保証レベルと対策基準の一部を見直し

今後の検討事項　―　当人認証保証レベルの見直しについて

No.	概要	今後の検討事項
1	脅威耐性の見直し	• 「中間者攻撃」「リプレイ攻撃」など現行ガイドラインから定義されている脅威について、最新の脅威動向やNISTでの定義を確認し、必要に応じて定義を見直す。「セッションハイジャック」については厳密にとらえると防ぐことが難しいため、脅威から除外するか、身元確認保証レベル3でも防げない部分があるという旨が伝わるようにする。 • レベル3でしか防げない脅威（チップの解析、クレデンシャルの複製等）を対策基準に含め、脅威耐性としてレベル3とレベル2Aの差が表現されるようにする。 • 現在の脅威耐性案は、現行ガイドライン、NIST SP 800-63-4、米国CISAガイドライン等の複数の文書を参考として組み合わせたものであるため、ISO/IEC 29115等を参考としながら基準や粒度が揃うよう全体的な見直しを行う。
2	認証器の認定制度等を考慮した対策要件の追加について	• 認証器の認定制度を考慮した対策基準の追加を検討する。 （第三者的な認定を受けていることを対策基準の条件とするなど。）
3	保証レベル3のHWトークンの要件の明確化	• 保証レベル3で求めるHWトークンに関する要件の明確化を検討する。例えばNIST AAL3においてはFIPS 140のレベル2以上を求めている。 • 他方、NIST AAL3を厳密に満たさないセキュアエレメントも世の中では多く活用さえているため、こうした技術の取扱いをどこに含めるかについてもあわせて検討する。
4	認証要素数と認証強度の関係性について	• 例として、タップのみで動作するFIDOセキュリティキーは、パスワードとSMS OTPの組み合わせよりもフィッシング耐性の観点では優れている。このように認証要素の数が認証強度の優劣に必ずしも反映されなくなってきている点を、保証レベルや対策基準にどのように反映すべきかを検討する。
5	保証レベルの段階の見直し（名づけ方の見直し）	• 保証レベル2の細分化については現在の方針で進めるが、3段階を維持したまま「2A」「2B」「2C」と細分化するのではなく、レベル1～5のように単純な5段階とすべきかどうか検討する。

本人確認ガイドラインの主要な改定ポイント

⑤ リスク評価プロセスを全面的に見直し

本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し

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 政府機関におけるデジタル本人確認に関するガイドライン（仮称）

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　本人確認の基本的要素
2.2　政府機関における本人確認のモデル
2.3　保証レベルと対策基準

3　本人確認手法の検討方法
3.1　デジタル化を念頭に入れた対象手続の業務改革（BPR）
3.2　本人確認に係るリスクの特定
3.3　保証レベルの判定
3.4　本人確認手法の選択
3.5　検討結果の文書化
3.6　継続的な評価と改善

本人確認ガイドライン参考資料
参考資料1　本人確認に係るリスク評価ワークシート
参考資料2　保証レベルに対応する本人確認手法例　等

主要な改定ポイント

①ガイドラインの適用対象と名称を変更
- 「1.2　適用対象」を見直し、本ガイドラインが対象とする本人確認の範囲を一部変更

②ミッション遂行などの基本的な考え方を解説
- ミッション遂行、公平性、アクセシビリティ、プライバシー等の基本的な考え方の解説を冒頭に追加

③デジタル本人確認の枠組みを定義・解説
- 身元確認、当人認証、認証連携などの定義と解説を追加
- 認証連携を用いる場合の一般的なモデルの解説を追加

④保証レベルと対策基準を見直し
- 最新の脅威動向等を踏まえ、各保証レベルの区分と対策基準を見直し

⑤リスク評価プロセスを全面的に見直し
- 公平性やプライバシー等の観点も考慮した手法選択が行われるように検討プロセス全体を見直し
- 一連の検討を補助する参考資料を拡充

本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し

「3　本人確認手法の検討方法」の全体概要

- 本人確認手法の検討プロセスは、NIST SP 800-63-4で追加された「テーラリング」や「文書化」などの要素を取り入れつつ、全面的に見直しを行う予定。本書ではこのうち3.2～3.4の改定方針を示す。

	検討プロセス	ガイドライン改定版の目次案	概要
	業務の見直し	3.1　デジタル化を念頭に入れた対象手続の業務改革（BPR）	• 業務改革（BPR）における本人確認に関連する見直しポイントなどの参考情報を追記する。
本書で改訂方針を示す範囲	リスク分析と手法の選択	3.2　本人確認に係るリスクの特定	• 本人確認において想定されるリスクケースにおいて「誰に」「どのような影響が生じる可能性があるか」を特定する。
		3.3　保証レベルの判定	• 特定したリスクの影響度を評価し、必要な保証レベルを判定する。身元確認と当人認証で別々の保証レベルを選択できるプロセスへと見直す。
		3.4　本人確認手法の選択	• 保証レベルを基に、公平性やプライバシーへの影響を分析しながら採用すべき手法を検討する。代替管理策や例外措置なども同時に検討する。
	文書化と継続的な改善	3.5　検討結果の文書化	• 上記の一連の検討結果の文書化を求める。
		3.6　継続的な評価と改善	• 一連のリスク分析や手法選択について、継続的な評価と改善を行う。

リスク評価プロセスの全体像

- 「1.5 基本的な考え方」で示す公平性やプライバシー等の影響を考慮した手法選択が行われるよう、リスク評価プロセスは全面的な見直しを行う。プロセスの全体像は以下のとおり。

3.2　本人確認に係るリスクの特定

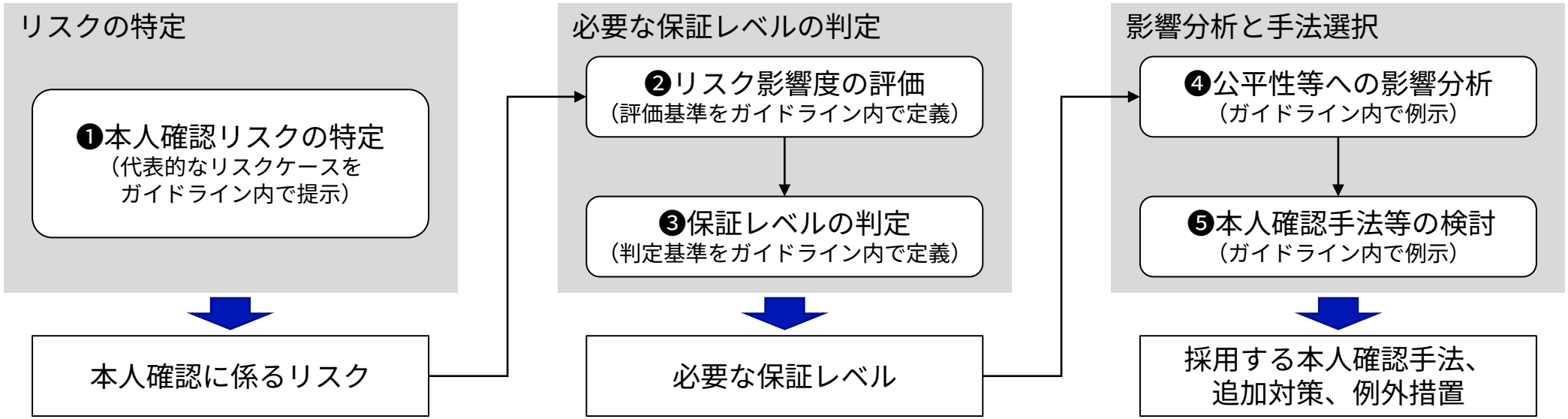
- 身元確認、当人認証、認証連携のそれぞれにおけるリスクケースを想定し、具体的にどのような本人確認のリスクがあり、顕在化時に誰が影響を受けるのかを特定する。

3.3　保証レベルの判定

- 3.2で特定したリスクを基に、リスクが顕在化した場合の影響度を６つのカテゴリーから評価する。
- 影響度の評価結果を基に、対象手続に必要な保証レベルを判定する。

3.4　本人確認手法の選択

- 保証レベルに対応する手法について公平性やプライバシー等への影響を分析する。
- 分析結果をもとに本人確認手法を決定するとともに、必要に応じて追加対策や例外措置を決定する。



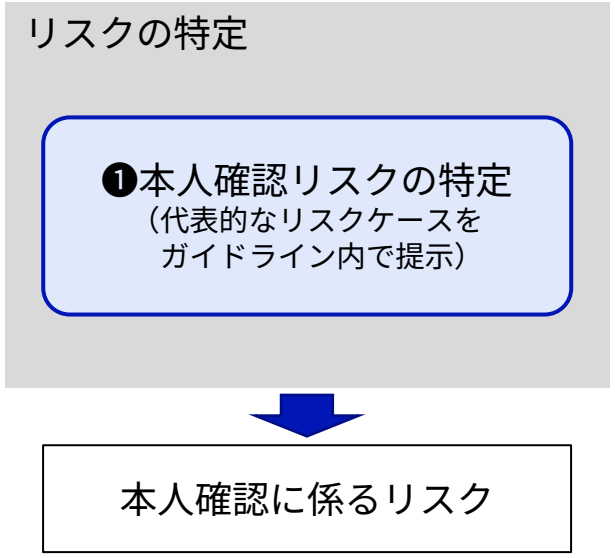
本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し

❶本人確認リスクの特定

- 新たに「本人確認リスクの特定」プロセスを追加する。ガイドラインで代表的なリスクケースを示し、対象手続においてこれらのケースが生じたとき、具体的にどのようなリスクが生じるかを特定・文書化する。

3.2　本人確認に係るリスクの特定

- 身元確認、当人認証、認証連携のそれぞれにおけるリスクケースを想定し、具体的にどのような本人確認のリスクがあり、顕在化時に誰が影響を受けるのかを特定する。



代表的なリスクケース

本人確認要素	想定脅威	代表的なリスクケース	リスクの例
身元確認	なりすまし	• 他人になりすました攻撃者からの申請を受け付けてしまった場合	• なりすまされた個人が本来受けとれるはずの給付金を受け取れなくなる
	重複登録	• 申請・登録を二重に受け付けてしまう	• 給付金が二重給付されてしまい、返還を求めるための説明や手続きが必要となる
当人認証	なりすまし	• 他人になりすました攻撃者を当人として認証してしまった場合	• なりすまされた個人の申請情報等の個人情報が攻撃者に漏えいする
認証連携	（今後整理予定）		

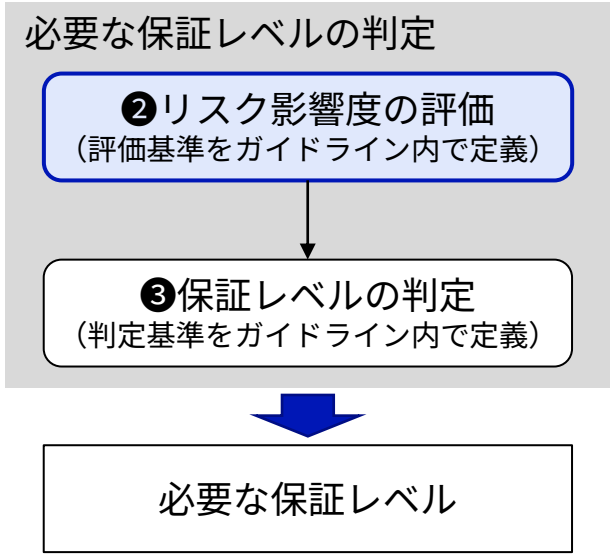
本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し

❷リスク影響度の評価

- リスク影響度評価のカテゴリー（評価の観点）は、SP 800-63-4の改定内容を参考とし、個人への影響と組織への影響を区別して記載するよう修正する。また「ミッション遂行」に関する記載などを取り入れる。

3.3　保証レベルの判定

- 3.2で特定したリスクを基に、リスクが顕在化した場合の影響度を６つのカテゴリーから評価する。
- 影響度の評価結果を基に、対象手続に必要な保証レベルを判定する。



影響度カテゴリー（改定案）

影響度カテゴリー	概要
①ミッション遂行に対する影響	個人が本来受けられるはずの行政サービスを受けられなくなる、組織が果たすべきミッションや機能を遂行できなくなる
②信用や評判への影響	個人や組織の信頼関係、イメージ、評判が悪化する
③個人情報等の漏えい	個人情報やその他の機微な情報等が漏えいする、組織の知的財産や要機密情報が漏えいする
④金銭的被害、財務上への影響	個人が資産や収入源を喪失するなどして金銭的な被害を受ける、組織が資産の喪失や賠償責任等により財務上の影響を受ける
⑤生命や安全への影響	個人が死亡する又は肉体的・精神的な健康被害を受ける、組織の労働力や安全な労働環境が損なわれる
⑥法律等への違反	民事上又は刑事上の法令、その他の契約等に違反する可能性がある

❸保証レベルの判定

- 保証レベルの判定については、身元確認と当人認証で別々の保証レベルを判定できるように見直す。保証レベルは最大の影響度に対応するレベルを判定するプロセスとし、現行ガイドラインの判定フローは削除する。

3.3　保証レベルの判定

- 3.2で特定したリスクを基に、リスクが顕在化した場合の影響度を６つのカテゴリーから評価する。
- 影響度の評価結果を基に、対象手続に必要な保証レベルを判定する。

必要な保証レベルの判定

❷リスク影響度の評価
（評価基準をガイドライン内で定義）

↓

❸保証レベルの判定
（判定基準をガイドライン内で定義）

↓

必要な保証レベル

最大の影響度に対応する保証レベルの判定（イメージ）

身元確認リスクの影響度評価	
①ミッション遂行に対する影響	中位
②信用や評判への影響	低位
③個人情報等の漏えい	中位
④金銭的被害、財務上への影響	低位
⑤生命や安全への影響	なし
⑥法律等への違反	中位

影響度評価（最大のもの）	必要な身元確認保証レベル
高位	レベル３
中位	**レベル２**
低位	レベル１
なし	レベル０

当人認証リスクの影響度評価	
①ミッション遂行に対する影響	低位
②信用や評判への影響	低位
③個人情報等の漏えい	中位
④金銭的被害、財務上への影響	中位
⑤生命や安全への影響	なし
⑥法律等への違反	低位

影響度評価（最大のもの）	必要な当人認証保証レベル
高位	レベル３
中位	**レベル２**
低位	レベル１

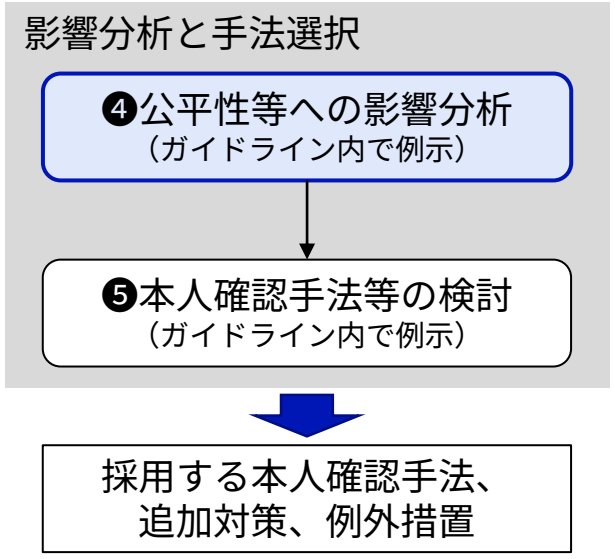
本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し

❹公平性等に対する影響分析

- 判定した保証レベルに対応する手法を確認し、「1.5　基本的な考え方」で示す公平性やプライバシー等の観点から採用可能なものであるか、影響分析を行う。

3.4　本人確認手法の選択

- 保証レベルに対応する手法について公平性やプライバシー等への影響を分析する。
- 分析結果をもとに本人確認手法を決定するとともに、必要に応じて代替手段や例外措置を決定する。



「1.5　基本的な考え方」の観点に基づく影響分析

影響分析の観点	影響を分析すべき内容
ミッション遂行と公平性	• 採用しようとする本人確認手法によって対象手続の目的達成が阻害されないか • 手続の対象者が公平に利用可能な手法であるか
プライバシー	• 採用しようとする手法によって、利用者のプライバシーに影響を及ぼす恐れがないか
ユーザビリティ及びアクセシビリティ	• 採用しようとする手法は、ミッション遂行や公平性の確保の観点から十分なユーザビリティ・アクセシビリティが確保できるものであるか
セキュリティ	• 採用しようとする手法は、対象手続において必要な脅威耐性を備えているか （例えば、マイナンバーカードの貸し借りによる不正を許容できない手続であれば、貸し借りを検知できる本人確認手法を選択する必要がある）

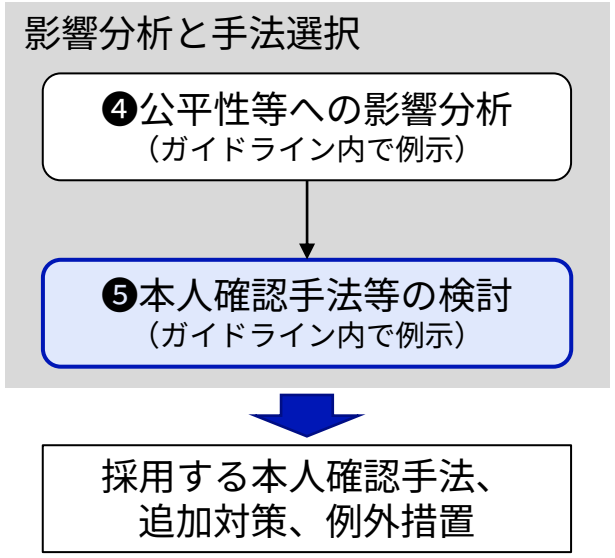
本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し

❺本人確認手法等の検討

- 影響分析の結果に基づき、本人確認手法を選択するとともに、必要に応じて必要に応じて複数の本人確認手法の併用、追加対策、例外措置の設定等の対応を検討する。

3.4　本人確認手法の選択

- 保証レベルに対応する手法について公平性やプライバシー等への影響を分析する。
- 分析結果をもとに本人確認手法を決定するとともに、必要に応じて追加対策や例外措置を決定する。



影響分析に基づく対応方針（例）

対応方針の区分	具体例
複数の本人確認手法を併用する	• マイナンバーカードを持たない利用者や海外からの渡航者に対しても広くサービスを提供する必要があるため、マイナンバーカードによる本人確認を基本としつつ、別の認証方式も選択可能とする
異なる保証レベルの手法を採用し、必要な追加対策を講じる	• 身元確認保証レベル2に該当する手続であるが、早急な給付金の支給が必要な状況であるため、保証レベル1に該当する手法を採用する • これにより生じる不正申請のリスクに対して、追加対策として事後的な監査を行うことで対応する
例外措置を設ける	• 申請に必要なマイナンバーカードが紛失中のケースを想定し、紛失中の場合には例外的に事後の本人確認を認める運用とし、マイナンバーカードの再発行後に本人確認を行う運用とする

本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し

参考資料「リスク評価ワークシート」の整備

- リスク影響度の評価を行うための参考資料としてワークシートを整備する予定。ワークシートでは各保証レベルに該当するリスクを列挙し、「対象手続において、そのようなリスクが存在するかどうか」を判定することでリスク影響度を評価できるようにする。

ガイドライン本編で示すリスクの内容や具体例を解説

検討項目	リスク影響度の基準 ※説明文はOIDF-J翻訳版or現行ガイドラインの表現で仮置き。 →今後わかりやすい表現に見直す。	解説・具体例	該否	該当する場合、具体的なリスクを記入
1-1.身元確認保証レベル３の該否判定 ・当該手続において身元確認が失敗した場合に想定される影響が、右の①～⑥に該当するかどうかを判定する。 ・いずれか1つ以上に該当する場合は、当該手続の身元確認保証レベルを「レベル３」と一次判定する。いずれにも該当しない場合は次項の「レベル２の該否判定」に進む。 ※「身元確認の失敗」とは、例えば他の人物へのなりすまし、実在しない人物へのなりすまし、同一人物による重複登録などが挙げられる。	**①ミッション遂行の阻害（高位）**：個人が平等な行政サービスを享受できなくなるような構造的な格差を生む。組織が1つ以上の主要機能を果たせなくなる。または、組織の資産や公共の利益に深刻な損害を及ぼす。		該当	
	②信頼や評判の棄損（高位）：深刻又は長期間の不便、苦痛又は利用者や機関等の地位や評判に対する影響を及ぼす。この影響は、特に深刻な影響や多くの利用者に影響する状況をいう。		非該当 該当	
	③機密情報の損失（高位）：公開許可のない個人情報、政府の機密情報又は企業秘密の公開により、機関等の活動や資産、又は利用者に致命的又は壊滅的な機密性損失の悪影響をもたらす。			
	④経済的安定の損害又は損失（高位）：個人又は組織に対して深刻または破滅的な金銭的損失を及ぼす。			
	⑤生命の損失，安全・健康・環境的安定に対する損害（高位）：深刻な負傷又は死亡の影響を与える。			
	⑥法律，規制，契約上の義務のすべて，または一部の不履行（高位）：法執行の計画で、特に重要とされている民事上又は刑事上の法律違反のリスクがある。			
1-2.身元確認保証レベル２の該否判定 ・当該手続において身元確認が失敗した場合に想定される影響が、右の①～⑥に該当するかどうかを判定	**①ミッション遂行の阻害（中位）**：行政サービスを受益できる個人とそうでない個人との間での結果的な格差を生む。組織の主要な機能が大幅に低下した状態が継続し、業務能力の大幅な劣化が生じる。また			

ワークシートの活用イメージ
- レベル３に該当するリスクの該否を回答させることで、当該手続がレベル３に該当するかどうかを判定。
- 該当しない場合はレベル２のリスクの該否→レベル１のリスクの該否へと進む。

本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し

参考資料「保証レベルに対応する本人確認手法例」の整備

- 影響分析のための参考情報として、各保証レベルに対応する代表的な本人確認手法の脅威耐性、公平性、プライバシーへの影響等をとりまとめた資料をガイドライン参考資料として整備する予定。

本人確認手法の選択に関する参考資料（イメージ）

身元確認 保証レベル		身元確認手法例	脅威耐性に係る 考慮事項	プライバシーに係る 考慮事項	公平性に係る 考慮事項	…
レベル3		…	…	…	…	
レベル2	2A	**マイナンバーカードによる対面での身元確認** ・電子証明書の検証により真正性を確認 ・対面での目視により本人確認書類と申請者との容貌を照合	―	―	…	…
	2B	**マイナンバーカードによるオンラインでの身元確認（容貌照合）** ・電子証明書の検証により真正性を確認 ・ビデオ撮影等により本人確認書類と申請者との容貌を照合	• オンラインでの容貌照合においては、プレゼンテーション攻撃への対策が必要	• 容貌比較のために取得した写真・ビデオ等の取扱いについて、必要なくなった段階でデータを削除する等の検討が必要	…	…
	2C	**マイナンバーカードによるオンラインでの身元確認（暗証番号）** ・電子証明書の検証により真正性を確認 ・暗証番号により本人確認書類と申請者との紐づきを検証	• 容貌照合を行わないため、カードの貸し借りは検知できない点に留意する	• 券面入力補助APには個人番号が含まれるため、利用可能な手続が限定される点に留意する	…	…
	…	…			…	…

本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し

今後の検討事項　―　リスク評価プロセスの見直しについて

No.	概要	今後の検討事項
1	フェデレーションに関する検討プロセスの継続検討	• フェデレーションに関するリスク分析や手法選択を、リスク評価のどのプロセスに盛り込むべきかを継続検討する。 • 当初は「3.4 本人確認手法の選択」に盛り込む案を検討していたが、有識者会議で得られた意見を踏まえ、認証連携に関するリスク評価が行われる箇所へ盛り込む方針で再検討する。
2	フェデレーションに関するスコープやモデルの再検討	• 以下の有識者意見を踏まえつつ、フェデレーションに関するリスク評価の方法や手法選択等の詳細プロセスを検討する。 　• 組織外との連携については分けて定義すべき。組織をまたぐ認証連携については難易度が非常に高くなるはずである。 　• システム内でIdPとRPを分離する場合にも認証連携のリスクや保証レベルの検討が必要である。また、身元確認や当人認証においては、外部から得られた結果に依拠することの判断を行う必要があるため、3.4での検討では遅いのではないか。 　• フェデレーションにはいくつかパターンがあり、外部に100%依拠する以外にも、既存のアカウントと紐づけたり、身元確認時の属性を取り寄せるために使うだけに使ったりするケースがある。こうしたケースを前提としてリスク評価が行われるべきである。 　• RPの保証レベルとIdPの保証レベルに差異がある場合など、過去の事例等を踏まえ特に注意が必要なリスクについて読者に伝わるようなガイドラインとすべき。
3	検討用ワークシートのトライアルと最終化	• 参考資料として準備予定のリスク評価の検討用ワークシートを作成し、実際の行政手続を想定したリスク評価の試行等を行う。

デジタル庁
Digital Agency