資料1

令和5年度
本人確認ガイドラインの改定に向けた有識者会議
論点協議資料（第4回分）

令和6年1月　　トラストタスクフォース

デジタル庁
Digital Agency

協議対象論点

協議対象論点

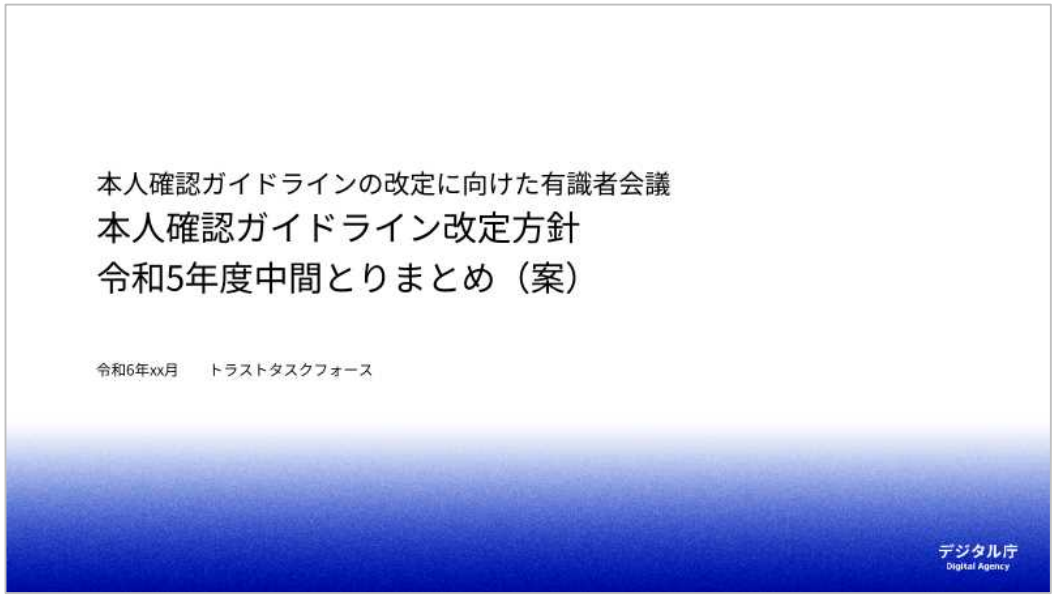
- 第1回、第2回での論点協議結果を踏まえ、トラストタスクフォースでは「本人確認ガイドライン改定方針　令和5年度中間とりまとめ」を作成中。
- 第3回以降では、この「令和5年度中間とりまとめ」の案を検討資料としながら、論点の再協議、追加協議、ガイドライン改定案の記載案レビューを実施いただきたい。

✓ 第1回・第2回において協議を行った論点

大項目	論点の概要
身元確認保証レベルの見直し	論点1-1.「身元確認保証レベル３」をNIST IAL3基準に見直すべきではないか
	論点1-2. リモート身元確認において生体情報の比較を必須とすべきか
	論点1-3.「身元確認保証レベル１」における登録コードの扱いをどうすべきか
当人認証保証レベルの見直し	論点2-1.「当人認証保証レベル２」においてフィッシング耐性を必須とすべきか
リスク評価プロセスの見直し	論点4-1. NISTで改定されたリスク評価プロセスをどのように反映すべきか
	論点4-2. 適切なリスク評価のためにどのような検討支援や統制が必要か

※当初予定していた論点3については内容精査が必要になり附議を保留中

✓ 第3回以降：「令和5年度中間とりまとめ」として改定方針を整理しつつ、その内容を協議・レビュー（本資料 P4以降）



本人確認ガイドラインの主要な改定ポイント（現在検討中の案）

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考え方を「基本的な考え方」として解説 • 「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 デジタル本人確認の枠組み	**③ デジタル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、IdP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 • 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。あわせてNISTのFALに相当する「認証連携保証レベル」を新設する。
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** • SP 800-63-4 におけるリスクマネジメントプロセスの全面改定を参考としつつ、保証レベルの一次判定やテーラリング等のプロセスを導入してリスク評価プロセスを全面改定する。
参考資料（別冊）	**⑥ リスク評価と手法選定のための参考資料やツール群の拡充** • 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などを的確かつ円滑に実施できるよう、リスク評価のためのワークシートや各種本人確認手法に関する参考情報を拡充して整備する。

本日の協議対象

本人確認ガイドラインの主要な改定ポイント（現在検討中の案）

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考え方を「基本的な考え方」として解説 • 「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 デジタル本人確認の枠組み	**③ デジタル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、IdP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 • 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。あわせてNISTのFALに相当する「認証連携保証レベル」を新設する。
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** • SP 800-63-4 におけるリスクマネジメントプロセスの全面改定を参考としつつ、保証レベルの一次判定やテーラリング等のプロセスを導入してリスク評価プロセスを全面改定する。
参考資料（別冊）	**⑥ リスク評価と手法選定のための参考資料やツール群の拡充** • 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などを的確かつ円滑に実施できるよう、リスク評価のためのワークシートや各種本人確認手法に関する参考情報を拡充して整備する。

論点協議資料

本人確認ガイドラインの改定に向けた有識者会議

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（案）

令和x年xx月　　トラストタスクフォース

本資料は令和5年度の有識者会議における議論を目的とした検討用資料です。

- 令和5年12月時点で検討中の事項を含む案であり、本資料の内容は何ら確定されたものではありません。
- 本人確認ガイドラインの改定方針は、有識者会議における今後の議論、NIST SP 800-63-4の最終改定版の内容、関係者間との調整、その他の関連動向等を踏まえつつ、引き続き検討を継続する予定です。

デジタル庁
Digital Agency

※第3回会議でのご指摘を踏まえ、今後見直し予定

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、本資料中では以下の用語・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。

赤字：第1回・第2回からの変更点

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。
身分証明書の真正性の確認	NIST SP800-63A-4のValidationに相当する行為のこと。※用語表記を第1回・第2回から一部変更
身分証明書と申請者の紐づきの検証	NIST SP800-63A-4のVerificationに相当する行為のこと。※用語表記を第1回・第2回から一部変更
容貌の照合	NIST SP800-63A-4のVerification時のRequirementsとして示される”Biometric Comparison”に相当する行為のこと。 身分証明書等のEvidenceに含まれる顔写真と、申請者の顔（リモートの場合は写真又はビデオ）を比較して、身分証明書と申請者との紐づき（バインディング）を検証する。
登録コード	NIST SP800-63A-4のVerification時のRequirementsとして示される”Enrollment Code”のこと。 Validation済みの住所、電話番号、メールアドレス等に対して送信した登録コードによってVerificationを行う行為のこと。
リアルタイム型フィッシング	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。）

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考え方を「基本的な考え方」として解説 • 「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 デジタル本人確認の枠組み	**③ デジタル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、IdP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 • 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。あわせてNISTのFALに相当する「認証連携保証レベル」を新設する。
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** • SP 800-63-4 におけるリスクマネジメントプロセスの全面改定を参考としつつ、保証レベルの一次判定やテーラリング等のプロセスを導入してリスク評価プロセスを全面改定する。
参考資料（別冊）	**⑥ リスク評価と手法選定のための参考資料やツール群の拡充** • 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などを的確かつ円滑に実施できるよう、リスク評価のためのワークシートや各種本人確認手法に関する参考情報を拡充して整備する。

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　デジタル本人確認の枠組み

2.1　身元確認、当人認証及び認証連携

2.2　デジタル本人確認のモデル

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　リスク影響度の評価

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

ガイドライン参考資料（Informative）

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　本人確認手法の選定にあたる脅威等の考慮事項

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、対象とする本人確認の範囲を一部変更する

②ミッション遂行などの考え方を解説

- 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

- 身元確認保証レベル、当人認証保証レベルの見直し
- 認証連携保証レベルを新たに定義

⑤リスク評価プロセスを全面的に見直し

- 保証レベルの一次判定後のテーラリング、検討結果の文書化、継続的な評価と改善などのプロセスを新たに定義

⑥参考資料やツール群の拡充

- リスク評価のためのワークシート等の参考資料を別文書として拡充。

本日の協議対象ポイント

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　デジタル本人確認の枠組み
2.1　身元確認、当人認証及び認証連携
2.2　デジタル本人確認のモデル
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　リスク影響度の評価
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

ガイドライン参考資料（Informative）
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　本人確認手法の選定にあたる脅威等の考慮事項

主要な改定ポイントとの関係

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、対象とする本人確認の範囲を一部変更する

②ミッション遂行などの考え方を解説
- 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
- 身元確認保証レベル、当人認証保証レベルの見直し
- 認証連携保証レベルを新たに定義

⑤リスク評価プロセスを全面的に見直し
- 保証レベルの一次判定後のテーラリング、検討結果の文書化、継続的な評価と改善などのプロセスを新たに定義

⑥参考資料やツール群の拡充
- リスク評価のためのワークシート等の参考資料を別文書として拡充。

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

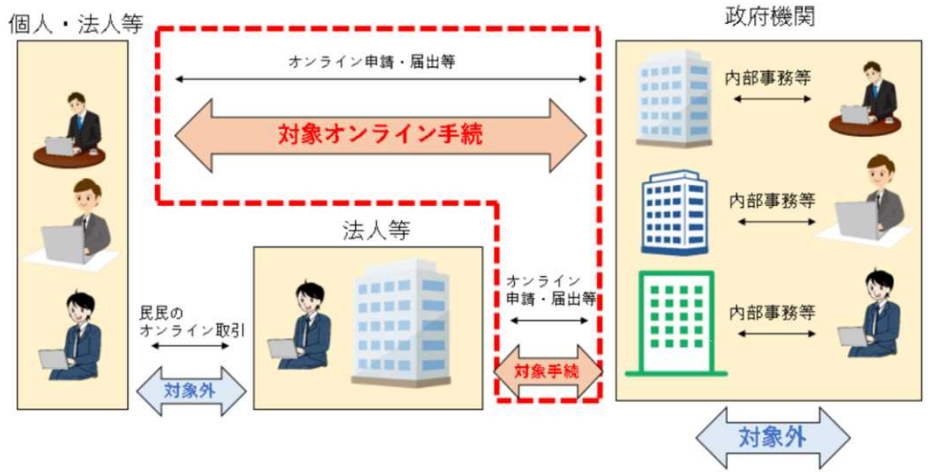
ガイドラインの適用対象の見直し方針

- 本人確認を取り巻く情勢の変化等を踏まえ、今回の改定にあわせて適用対象の見直しを検討中。

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」 → 「本人確認」

- 対象範囲を「オンラインによる本人確認」から、対面等も含めた単なる「本人確認」へと拡大する。
- マイナンバーカードを活用した本人確認が、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。

❷「個人又は法人等の」 → 「個人の」

- 今回の改定版より「個人の本人確認」のみを対象とする。
- 「法人の本人確認」は固有の考慮事項が多くあることから、別ガイドラインとして別途整備することを検討中。

❸「行政手続」 → 「行政手続及び内部事務」 （検討中）

- 行政手続だけでなく行政事務の従事者（職員、委託事業者等）に対する本人確認も対象に含めるべきでないか検討中。
- 影響範囲が非常に大きい変更となるため、対象拡大の是非、適用時期、強制力などについては今後も継続検討予定。

参考：地方公共団体への適用について

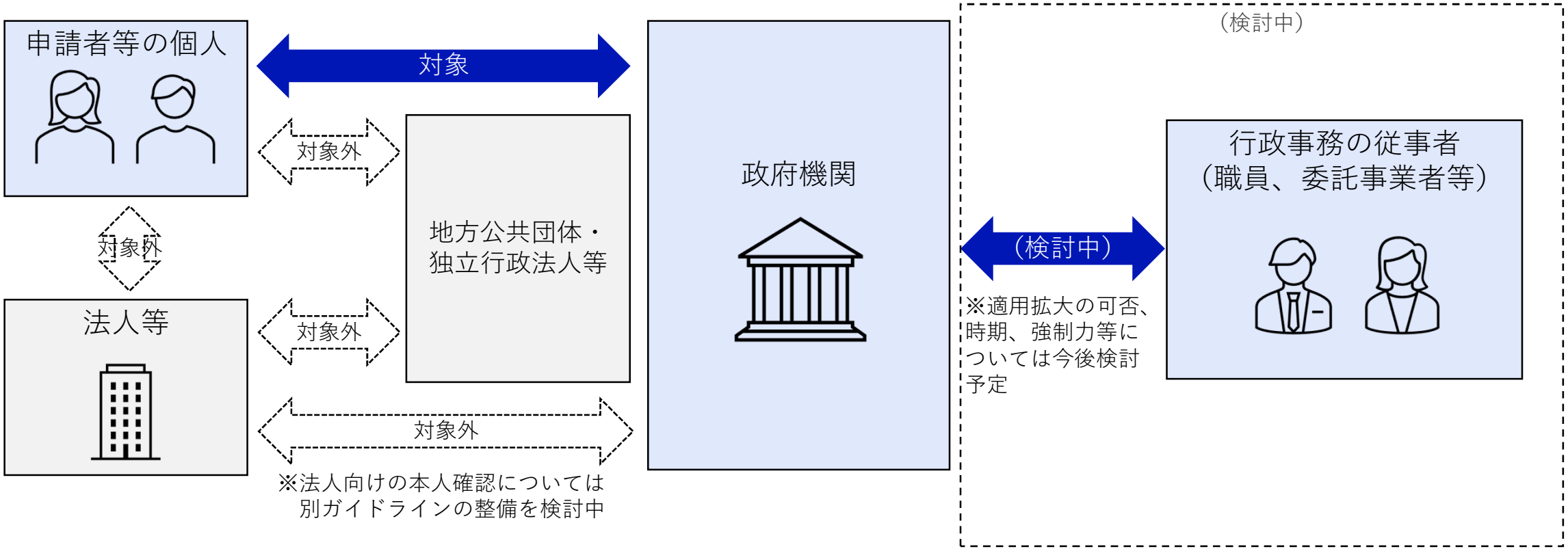
- 標準ガイドライン群は政府情報システムを対象とするドキュメント群であるため、地方公共団体等については現行ガイドラインと同様、適用対象外となる。
- ただし、地方公共団体から参照されるケースも多くある現状を踏まえ、記載内容の見直しや補足等を検討する。

本人確認ガイドラインの主要な改定ポイント
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中。

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

参考：ガイドライン名称の見直し案

- 適用対象の見直し、その他の改定に伴うガイドラインの内容変更等に伴い、本ガイドラインの名称についても変更を検討中。

現行：　「**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**」

↓

改定案１：「**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**」

改定案２：「**政府機関における本人確認に関するガイドライン**」

改定案３：「**政府機関におけるデジタルアイデンティティに関するガイドライン**」

改定案４：「**政府機関におけるデジタルアイデンティティ及び本人確認に関するガイドライン**」

有識者の皆様にご意見・議論いただきたいポイント

適用対象の変更に対するご意見

- 前述の適用対象の拡大方針について、妥当性や懸念事項などのご意見をお伺いしたい。
- 特に「行政事務の従事者」への拡大については実現可否も含めて検討中の段階であるものの、現時点でのご所見をいただきたい。

本日の協議対象ポイント
（第3回会議で議論予定であった内容を繰り越し）

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

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　デジタル本人確認の枠組み
2.1　身元確認、当人認証及び認証連携
2.2　デジタル本人確認のモデル
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　リスク影響度の評価
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

ガイドライン参考資料（Informative）
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　本人確認手法の選定にあたる脅威等の考慮事項

主要な改定ポイントとの関係

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、対象とする本人確認の範囲を一部変更する

②ミッション遂行などの考え方を解説
- 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
- 身元確認保証レベル、当人認証保証レベルの見直し
- 認証連携保証レベルを新たに定義

⑤リスク評価プロセスを全面的に見直し
- 保証レベルの一次判定後のテーラリング、検討結果の文書化、継続的な評価と改善などのプロセスを新たに定義

⑥参考資料やツール群の拡充
- リスク評価のためのワークシート等の参考資料を別文書として拡充。

本日の協議対象ポイント
（第3回会議で議論予定であった内容を繰り越し）

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

④-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）

	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（マイナンバーカード等）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。（現行ガイドラインから変更なし） • なりすまし等によるリスクが大きく、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。	• 対策基準に「リアルタイム型フィッシング攻撃への耐性」等の多要素認証に対する攻撃を追加し、保証レベル３においてはこれらを必須として求める。
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。（現行ガイドラインから変更なし） • 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必須としないが「推奨」とする。ただし、今後の認証技術の動向によっては「必須」とすることも検討する。 • 同じレベル２の手法であっても対策可能な脅威には様々な差異があるため、脅威と手法の関係を参考資料（改定ポイント⑥）に掲載する。
当人認証 保証レベル１	**単要素認証** • 多要素認証は必須とせず単要素認証を認める保証レベルとする。（現行ガイドラインから変更なし） • なりすまし等による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。	• リアルタイム型フィッシング攻撃への耐性は不要とする。

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

当人認証保証レベルの対策基準（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１	当人認証保証レベル２	当人認証保証レベル３
認証要素		単要素	２要素	耐タンパ性が確保された ハードウェアトークンを含む ２要素
脅威への耐性	オンライン上の推測 ※辞書攻撃など	必須		
	盗聴による認証情報の取得	必須		
	セッションハイジャック	必須		
	中間者攻撃 ※定義は一部見直し予定	必須		
	リプレイ攻撃 ※定義は一部見直し予定	不要	必須	
	フィッシング／ファーミング	不要	必須	
	リアルタイム型フィッシング	不要	推奨	必須
	多要素認証疲労攻撃	不要	推奨	必須
	SIMスワップ	不要	推奨	必須

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の細分化について（議論用のたたき台）

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1	当人認証保証レベル2			当人認証保証レベル3
			レベル2C	レベル2B	レベル2A	
認証要素		単要素	２要素			耐タンパ性が確保されたHWトークンを含む２要素
脅威への耐性	オンライン上の推測 ※辞書攻撃など		必須			
	盗聴による認証情報の取得		必須			
	セッションハイジャック		必須			
	中間者攻撃 ※定義は一部見直し予定		必須			
	リプレイ攻撃 ※定義は一部見直し予定	不要	必須			
	フィッシング／ファーミング	不要	必須			
	リアルタイム型フィッシング	不要	不要	不要	必須	必須
	多要素認証疲労攻撃	不要	不要	必須	必須	必須
	SIMスワップ	不要	不要	必須	必須	必須

有識者の皆様にご意見・議論いただきたいポイント

1. 当人認証保証レベル２の細分化の意義について

- リアルタイム型フィッシング、疲労攻撃、SIMスワップへの耐性を軸として保証レベルを細分化することは可能であるが、この細分化を定義する意義はあるか。あるいは、細分化を行うことによる弊害や懸念は想定されるか。
    - 新たな脅威の出現によるレベル定義の陳腐化等

※ 今回のガイドライン改定タイミングが、リアルタイム型フィッシング耐性を有する技術（パスキー等）の普及過渡期となるであろうことを踏まえつつご議論いただきたい。

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

フィッシング耐性を有する当人認証手法の例

- 現時点で普及している当人認証手法を踏まえると、レベル２においてリアルタイム型フィッシングへの耐性を必須とした場合、行政手続において採用できる手法が極めて限定的になってしまうことが懸念される。

NIST AAL		主要な当人認証手法（括弧内：SP 800-63B-4のAuthenticator Type）	行政手続における留意事項等
NIST AAL3（HWベース多要素）	フィッシング耐性あり（注１）	生体認証でアクティベートされるFIDOセキュリティキー（Multi-Factor Cryptographic Devices）	• 物理デバイスの準備が必要であるため不特定多数が利用する行政手続では採用しにくい
		PINでアクティベートするスマートカードによる証明書認証（Multi-Factor Cryptographic Devices）	
NIST AAL2（多要素）		生体認証でアクティベートされるFIDO認証（パスキー含む）（Multi-Factor Cryptographic Software）	• フィッシング耐性を備えるAAL2の手法として有力となり得ると期待できるが、普及動向への考慮が必要
		生体認証でアクティベートされるAuthenticatorアプリによる証明書認証（Multi-Factor Cryptographic Software）	• 証明書の配付が必要となるため不特定多数が利用する行政手続では採用しにくい
		パスワード ＋ 端末にインストールされた証明書認証（Memorized Secret + Single-Factor Cryptographic Software）	• 証明書の配付が必要となるため不特定多数が利用する行政手続では採用しにくい
	フィッシング耐性なし	パスワード ＋ Authenticatorアプリでのプッシュ通知・番号選択等（Memorized Secret + Out-of-Band Devices）	
		パスワード ＋ AuthenticatorアプリでのTOTP（Memorized Secret + Single-Factor OTP Device）	
		パスワード ＋ SMS認証コード（Memorized Secret + Out-of-Band Devices）	
NIST AAL1（単要素）		パスワードのみ（Memorized Secret ）	

（注１）最終的なリアルタイム型フィッシングへの耐性有無は、上記の認証器の種別だけでなくバックチャネルの実装（相互認証の有無等）にも依存する点に留意。

本日の協議対象ポイント

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

⑥ リスク評価と手法選定のための参考資料やツール群の拡充

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　デジタル本人確認の枠組み
2.1　身元確認、当人認証及び認証連携
2.2　デジタル本人確認のモデル
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　リスク影響度の評価
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

ガイドライン参考資料（Informative）
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　本人確認手法の選定にあたる脅威等の考慮事項

主要な改定ポイントとの関係

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、対象とする本人確認の範囲を一部変更する

②ミッション遂行などの考え方を解説
- 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
- 身元確認保証レベル、当人認証保証レベルの見直し
- 認証連携保証レベルを新たに定義

⑤リスク評価プロセスを全面的に見直し
- 保証レベルの一次判定後のテーラリング、検討結果の文書化、継続的な評価と改善などのプロセスを新たに定義

⑥参考資料やツール群の拡充
- リスク評価のためのワークシート等の参考資料を別文書として拡充。

「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。検討中の改定案の全体概要は以下のとおり。

検討プロセス	ガイドライン改定版の目次案	概要（青字：主な改定方針）
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）の具体的手法等は本ガイドラインの範囲外であるが、電子申請や本人確認に関連する見直しポイント（ワンスオンリー、プッシュ型サービスなど）などの参考情報を追記する。
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	• 後続のリスク分析を円滑に検討できるよう、リスクの特定プロセスを追加する。本人確認に関する想定脅威をガイドラインで示し、「誰に対して」「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　リスク影響度の評価	• 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。影響度評価のカテゴリーは一部見直し、解説等を拡充する。
	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プロセスとして追加する。代替管理策や例外措置なども同時に検討されるようにする。
文書化	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。
継続的な改善	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求める。現行ガイドラインにおいても言及されている事項であるが、プロセスとして明確に定義する。

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／⑥ リスク評価と手法選定のための参考資料やツール群の拡充

「3.1　デジタル化を念頭に入れた対象手続の業務改革（BPR）」の記載案

- 現行ガイドラインからの大幅な変更はないが、軽微な見直し・加筆を行う。

ガイドライン改定版の記載案（検討中の素案）

3.1　デジタル化を念頭に入れた対象手続の業務改革（BPR）

各府省は、法令等に基づき行政手続をデジタル化する場合には、当該手続の事務フローを作成し、デジタル化を念頭に入れて当該手続の事務フローを抜本的に見直す業務改革（BPR）を検討するものとする。

1）　業務改革（BPR）における検討事項

業務改革（BPR）では、「デジタル社会の実現に向けた重点計画」で定められる政府方針及び「政府方針及びデジタル社会推進標準ガイドライン群」の各種ガイドラインに基づき、利用者のニーズ、利用状況及び現場の業務を詳細に把握・分析した上で、あるべきプロセスを法令・体制・手法を含めて一から検討する。

この検討においては、デジタルアイデンティティ及び本人確認に関連する見直しとして、以下に示すような事項についても検討する。

- そもそも当該手続において申請行為や本人確認が必要であるか。プッシュ型サービスとして行政サービスを提供することで、申請行為を不要とすることができないか。
- 申請行為が必要な場合でも、府省内の情報連携、マイナンバーによる行政機関間での情報連携により、申請時の入力項目や添付書類を削減できないか。

2）　本人確認を行う必要のある属性情報の特定

対象手続において本人確認が必要であると判断した場合には、本人確認においてどのような情報を確認・検証する必要があるのかを特定する。確認すべき情報は対象手続の特性や関連法令等によって異なるが、例えば、個人番号、氏名、住所、連絡先、銀行口座情報などが考え得る。

なお、プライバシーの観点からは、本人確認において収集する情報は最小限とすべきであることに留意する。

主な見直しポイント

BPRの関連文書の最新化
- 業務改革（BPR）の検討において参照すべき上位文書を最新化

※BPRそのものは本人確認ガイドラインの対象範囲ではないため、他のガイドライン等を参照させる

BPRの検討ポイントの例示
- 電子申請や本人確認に関連する見直し事項として、プッシュ型サービスやワンスオンリー等を例示

その他の補足の追記
- 「必要な属性の特定」においては、プライバシーの観点からの留意事項を追記

リスク分析から本人確認手法の選択までの検討プロセス

- NIST SP 800-63-4の改定内容や有識者会議での議論内容を踏まえ、検討プロセスを全面的に見直す。
- また、プロセスの複雑化に伴う検討負担を軽減するため、**各プロセスに対応する検討用ワークシートを整備**し、本ガイドラインの参考資料として公開する方針とする。
- この検討用ワークシートを作成することで、「3.5　検討結果の文書化」についても満たすことができるようにし、「3.6　継続的な評価と改善」のインプット情報としても活用できるようにする。

第2回有識者会議での議論を踏まえて3.2を追加

認証連携の検討をこのプロセスに盛り込むことを検討中

3.2　本人確認に係るリスクの特定 ：リスク影響度評価の前段として追加	3.3　リスク影響度の評価 ：現行ガイドラインのリスク評価に相当	3.4　本人確認手法の選択 ：SP 800-63-4のテーラリングに相当
• 対象手続が実施する身元確認、当人認証のそれぞれにおける脅威を想定し、どのような本人確認のリスクがあるのか、顕在化時には誰が影響を受けるのかを整理・特定する。	• 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。 • 影響度の判定結果を基に、対象手続における保証レベルを判定する。	• 公平性、プライバシー、ユーザビリティ等への影響を分析しつつ、保証レベルに対応する本人確認手法や外部IdPの活用可否を検討する。 • 必要に応じて、代替管理策や例外措置の採用を検討する。
文書化	文書化	文書化
リスク特定ワークシート	リスク評価ワークシート	本人確認手法の検討ワークシート

ガイドライン参考資料

3.5　検討結果の文書化／3.6　継続的な評価と改善

「3.2　本人確認に係るリスクの特定」の概要

- リスク影響度評価の前段として、本人確認に係るリスクの特定プロセスを追加することを検討中。あらかじめリスクを特定・明文化しておくことで、後続の検討作業の円滑化や検討結果の妥当性向上を狙う。
- 具体的には「**本人確認に関するリスクを特定すべきケース**」**をガイドライン内で示し**、これを基に対象手続におけるリスクの特定を行うことを想定。

本日ご意見をいただきたいポイント

「リスクを特定すべきケース」の案（NISTの「障害モード」に相当）

身元確認	なりすまし	• 本人確認書類の偽造等により、 – **実在する他の人物**として申請や登録を受け付けてしまった場合のリスク（当人性の詐称） – **現実には存在しない架空の人物**からの申請や登録を受け付けてしまった場合のリスク（存在性の詐称） – **現在は生存していない人物**からの申請や登録を受け付けてしまった場合のリスク（生存性の詐称）
	重複申請	• 既に登録済みの者からの申請や**登録を重複**して受け付けてしまった場合のリスク
	本人確認書類の貸し借り	• 本人確認書類の貸し借りによって、**本人とは異なる者**によって手続や申請・登録が行われた場合のリスク
当人認証	なりすまし	• ICカードやパスワード等の窃盗・詐取によって、**本人ではない者を本人として認証**してしまった場合のリスク（当人性の詐称）
	認証器の貸し借り	• パスワードやICカード等の共有や貸し借りによって、**本人ではない者を本人として認証**してしまった場合のリスク

リスクの特定結果

- 対象手続の本人確認において左記のケースが生じたとき「誰に対して」「どのような影響が生じるか」を特定し、文書化する

対象手続における身元確認リスク
・組織のリスク
・個人のリスク
・その他の関係機関のリスク

対象手続における当人認証リスク
・組織のリスク
・個人のリスク
・その他の関係機関のリスク

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／⑥ リスク評価と手法選定のための参考資料やツール群の拡充

「3.2　本人確認に係るリスクの特定」の記載案

３．３　本人確認に関するリスクの特定

対象手続等において、どのような本人確認に関するリスクが想定されるかを特定する。具体的には、身元確認、当人認証の各プロセスにおける想定脅威を整理し、それぞれの脅威に対応するリスクを特定、文書化する。

リスクを特定すべき代表的なケースの例を以下に示す。

表 2　本人確認に係るリスクを特定すべきケース（例）

プロセス	想定脅威	リスクを特定すべきケース
身元確認	なりすまし（当人性の詐称）	本人確認書類の偽造等により、実在する他の人物として申請や登録を受け付けてしまった場合
	なりすまし（存在性の詐称）	本人確認書類の偽造等により、現実には存在しない架空の人物からの申請や登録を受け付けてしまった場合
	なりすまし（生存性の詐称）	本人確認書類の偽造等により、過去に存在していたが現在は生存していない人物からの申請や登録を受け付けてしまった場合
	重複申請	既に登録済みの者からの申請や登録を重複して受け付けてしまった場合
	本人確認書類の貸し借り	本人確認書類の貸し借りによって、本人とは異なる者によって手続や申請・登録が行われた場合（正当な手続きを経た代理人等を除く）
当人認証	なりすまし（当人性の詐称）	パスワードや IC カード等の詐取によって、本人ではない者を本人として認証してしまった場合
	認証器の貸し借り	パスワードや IC カード等の共有や貸し借りによって、本人ではない者を本人として認証してしまった場合

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／⑥ リスク評価と手法選定のための参考資料やツール群の拡充

「3.3　リスク影響度の評価」の概要

- リスク顕在化時の影響度を６つのカテゴリーで評価し、対象手続で必要となる保証レベルを判定する。
- 今回の改定では、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。また、保証レベルの判定フロー図を削除し、**最大の影響度に対応する保証レベルを判定するプロセス**へとする。
- その他、NISTの改定を参考としたカテゴリー定義の修正、影響度定義の解説の拡充等を行う。

リスクの特定結果（3.2より）

対象手続における身元確認リスク
・組織のリスク
・個人のリスク
・その他の関係機関のリスク

対象手続における当人認証リスク
・組織のリスク
・個人のリスク
・その他の関係機関のリスク

リスク影響度の評価

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

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

保証レベルの判定

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

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／⑥ リスク評価と手法選定のための参考資料やツール群の拡充

「3.3　リスク影響度の評価」のカテゴリーの見直し

- 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。

現行ガイドラインのカテゴリー	改定版でのカテゴリー定義の修正案
機関等の活動計画や公共の利益に対して影響を与える	**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
オンライン手続サービスの利用において国民等の利用者に不便、 苦痛を与える、又はオンライン手続サービスを所管する機関等が信頼を失う	**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
国民等の利用者の個人情報等の機微な情報が漏えいする	**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
国民等の利用者に金銭的被害を与える、機関等に賠償責任が生じるなど、財務上の影響を与える	**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
国民等の利用者の身の安全に影響を与える	**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
法律に違反する	**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

※現行ガイドラインのカテゴリーは、改定案と対応するように順序を並べ替えて掲載している。

※上記は現時点の改定方針を示すための素案であり、詳細な定義については今後検討を行う。

本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し／⑥ リスク評価と手法選定のための参考資料やツール群の拡充

「3.3　リスク影響度の評価」の影響度定義の解説等の拡充

- リスク評価の際の「影響度の定義」は現行ガイドラインの内容を踏襲するが、ガイドライン利用者が理解しやすいよう解説や補足等を拡充する予定。

リスク影響度の定義
（内容は現行ガイドラインを踏襲）

影響度	定義
高位	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に致命的又は壊滅的な悪影響を及ぼすと予想される
中位	当該リスクの影響による損失が、組織の運営、組織の資産、又は個人に重大な悪影響を及ぼすと予想される
低位	当該リスクの影響による損失が、組織の運営、組織の資産、又は 個人に限定的な悪影響を及ぼすと予想される

解説等の拡充方針（案）

①定義内の表現の解説・補足

- 定義内で用いられている「致命的な」「重大な」「限定的な」などの表現についてはFIPS 199を参考としたものであるが、判断基準が読み手の解釈によって異なるという課題がある。
- これを踏まえ、後述する検討用ワークシートにおいて解説や例示等の補足説明を拡充することで、影響度の判断基準を明確化する。

②各行政手続のリスク影響度の事例等の整理

- 将来的に、政府内の各手続のリスク影響度を収集し、参考事例として蓄積・共有することで、類似の手続を参考としたリスク評価が行えるようにすることを検討。
- 典型的なパターンの行政手続については、リスク影響度のサンプルを参考資料等で整備できないか検討中。
    - 例：「個人向けの給付金の支給申請」における標準的なリスク影響度など

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／⑥ リスク評価と手法選定のための参考資料やツール群の拡充

「3.3　リスク影響度の評価」検討用ワークシート案

- リスク影響度の評価用ワークシートでは、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される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。 一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。

「3.4　本人確認手法の選択」の概要

- NIST SP 800-63-4で追加された「テーラリング」に相当するプロセスとして新たに定義する。このプロセスでは、**採用しようとする本人確認手法がミッション遂行や公平性などへ及ぼす影響を分析し、代替管理策や例外措置の必要性を検討・決定**する。
- また、外部IdPの活用によるフェデレーションの検討も、このプロセスに含めることができないか検討中。

保証レベルの判定結果

必要な 身元確認保証レベル
レベル３
レベル２
レベル１
レベル０

必要な 当人認証保証レベル
レベル３
レベル２
レベル１

本プロセスでの検討事項

本日ご意見をいただきたいポイント（赤字部分）

観点	検討内容
①採用する本人確認手法	• 同じ保証レベルの手法であっても細かな脅威耐性は異なるため、**当該手続に必要な脅威耐性や法令等との制約を考慮して手法を選択**する。 ※この際の検討に資するよう、一部の保証レベルは脅威耐性に応じた細分化を行う。
②外部IdPの活用可否	• 採用しようとする本人確認手法を提供するIDプロバイダが存在する場合には、**当該IDプロバイダとの連携による本人確認の実現を検討**する。 ※必要な認証連携保証レベルの扱いについては検討中。
③代替管理策	• 採用しようとする本人確認手法によって、**ミッション遂行や公平性が阻害される恐れがないか、プライバシーが侵害される懸念はないか、ユーザビリティやアクセシビリティは十分に確保できるか**を確認する。 • 必要に応じて別の本人確認手法を併用する、保証レベルを見直して他のリスク軽減措置を講じるなどの代替管理策を検討する。
④例外措置	• 対象手続の利用者が、**認証に必要なICカード等を紛失している場合**、災害等によって**本人確認書類を喪失している場合**などの例外的なケースを想定し、対応の必要性や方法等の例外措置を検討する。

本人確認ガイドラインの主要な改定ポイント
⑤ リスク評価プロセスを全面的に見直し／⑥ リスク評価と手法選定のための参考資料やツール群の拡充

「3.4　本人確認手法の選択」の検討のための参考資料（案）

- 各行政手続が本プロセスを検討する際の参考情報として、代表的な本人確認手法の脅威耐性、公平性や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	…	…
	…	…			…	…

有識者の皆様にご意見・議論いただきたいポイント

1.「3.2　リスクの特定プロセス」の追加について

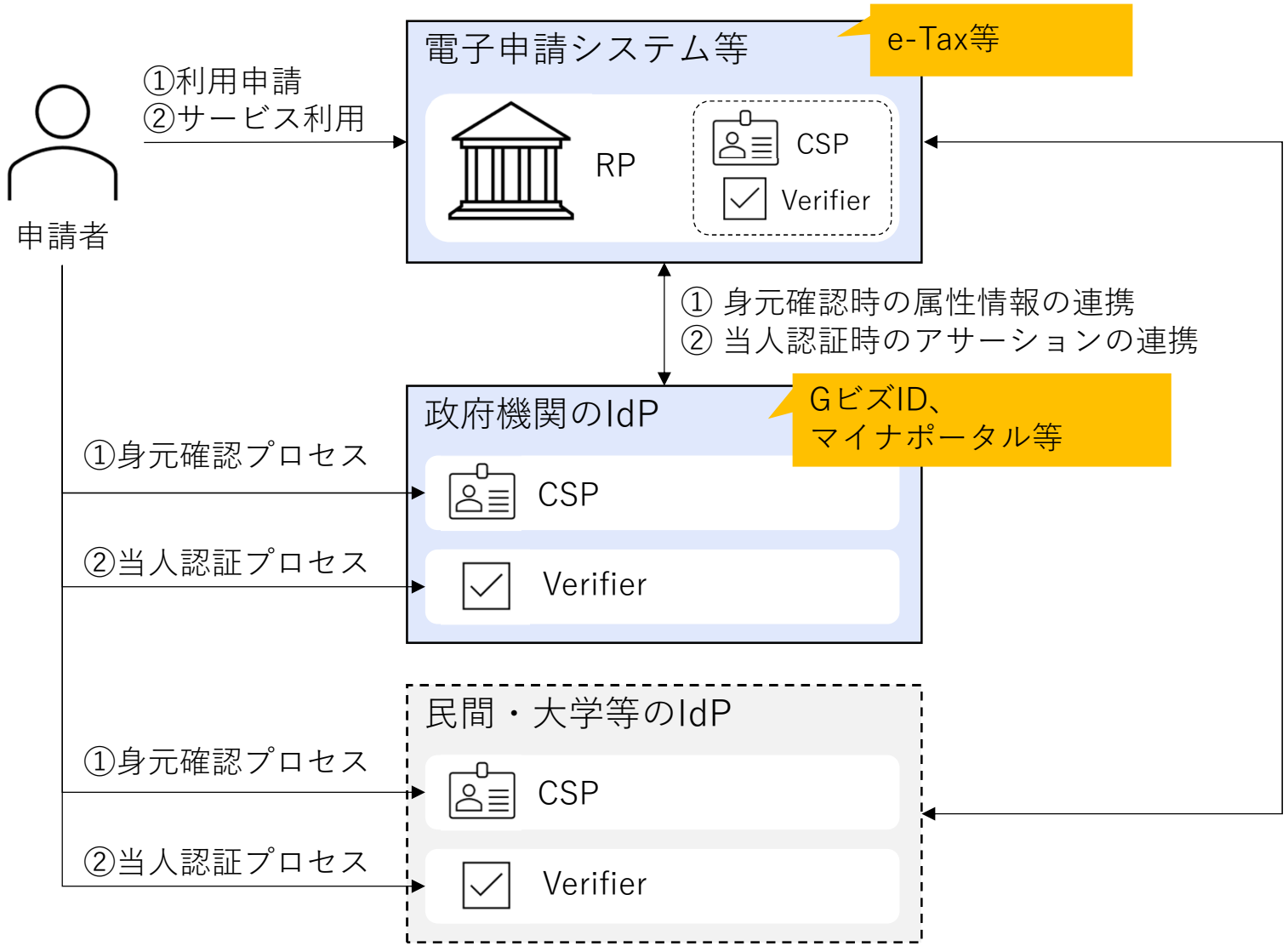
- NISTでは明文化されていないプロセスではあるが、リスク影響度評価や脅威耐性の要否判断には必要不可欠であると考え追加を検討中。
  （第2回会議での「障害モード別のリスクは明文化すべき」とのご意見をベースに案を作成）
- このプロセスの追加について疑義、追加すべき例、見直すべきポイント等ご意見をいただきたい。

2. 外部IdP活用（フェデレーション）の検討プロセスについて

- フェデレーションの検討は「3.4　本人確認手法の選択」（NISTのテーラリングプロセスに相当）に盛り込む方向で検討中。NISTとは異なるプロセスとなるため、妥当性をご意見をいただきたい。

（フェデレーションについての検討経緯）
- 当初はフェデレーションについても3.2の「リスクの特定」や3.3の「影響度評価」を行うべきと考えていたが、フェデレーションに起因するリスクは結局のところ「身元確認のリスク」「当人認証のリスク」のリスクケースとほとんど同じになってしまう。
- フェデレーション固有の脅威やリスクの考慮は必要であるが、それであれば詳細な脅威耐性の検討を行う予定の「テーラリング」のプロセスに盛り込むことが適当ではないかと考え、3.4の「本人確認手法の検討」に盛り込むこととした。

参考：政府の本人確認モデル案（ディスカッション用）



民間・大学等のIdPとの連携については将来的な実現を想定

① 身元確認時の属性情報の連携
（政府機関が有していないもの）
- 口座番号
- 電話番号
- 就労情報
- 在籍情報
- 卒業情報　等

② 当人認証時のアサーションの連携

デジタル庁
Digital Agency