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3回分）

令和5年12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

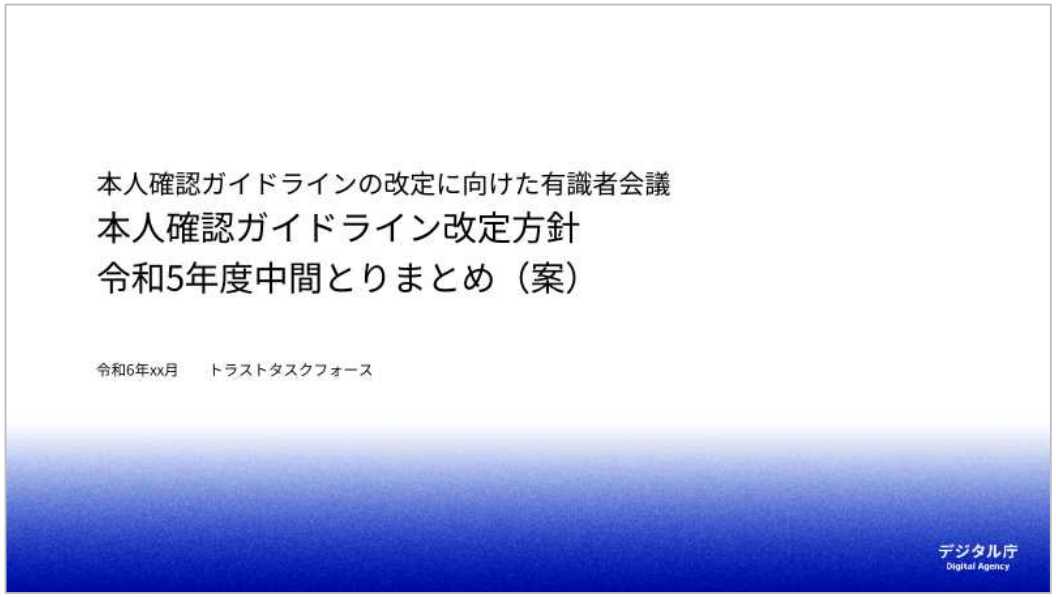
- 第1回、第2回での論点協議結果を踏まえ、トラストタスクフォースでは「本人確認ガイドライン改定方針　令和5年度中間とりまとめ」を作成中。
- 第3回以降では、この「令和5年度中間とりまとめ」の案を検討資料としながら、論点の再協議、追加協議、ガイドライン改定案の記載案レビューを実施いただきたい。

✓ 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。

本人確認ガイドラインの主要な改定ポイント

本日の協議対象

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

赤字：第1回・第2回からの変更点

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。

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 行政手続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　デジタル本人確認における認証連携モデル
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　デジタル化を前提とした対象手続の業務改革（BPR）
3.2　本人確認を行う必要のある属性の特定
3.3　リスク評価に基づく保証レベルの一次判定
3.4　保証レベルの調整及び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、対面におけるデジタル本人確認等も対象とする

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。

（本テーマは第4回有識者会議にて議論予定）

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

（本テーマは第4回有識者会議にて議論予定）

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　デジタル本人確認における認証連携モデル
- 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　デジタル化を前提とした対象手続の業務改革（BPR）
- 3.2　本人確認を行う必要のある属性の特定
- 3.3　リスク評価に基づく保証レベルの一次判定
- 3.4　保証レベルの調整及び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、対面におけるデジタル本人確認等も対象とする

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

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

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考え方を「基本的な考え方」として解説

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 行政手続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　デジタル本人確認における認証連携モデル
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　デジタル化を前提とした対象手続の業務改革（BPR）
3.2　本人確認を行う必要のある属性の特定
3.3　リスク評価に基づく保証レベルの一次判定
3.4　保証レベルの調整及び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、対面におけるデジタル本人確認等も対象とする

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つの観点の概要

本人確認手法の検討において考慮すべき観点	**1) ミッション遂行**	• 本人確認が障壁となって当該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。
	2) 公平性とアクセシビリティ	• 利用者の人種、性別、年齢、住む地域などによって行政手続の利用しやすさにできる限り差が生じないように、誰にとっても利用可能な本人確認手法を採用しなければならない。
	3) プライバシー	• 本人確認において収集する情報はプライバシーの観点からは必要最小限にしなければならない。また、情報の収集目的を明示しなければならない。
	4) ユーザビリティ	• ユーザビリティは単なる「使いやすさ」だけでなく、申請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、公平性、プライバシー、セキュリティなどにも影響す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。前述の公平性とアクセシビリティ、プライバシー、ユーザビリティとのトレードオフを考慮しつつ、リスクに応じた本人確認手法の選択が必要である。

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」に記載予定の内容（素案）

- 具体的には以下のような記載案を検討中。
  ※以下は検討中の素案。今後関係各所との調整や推敲等を行ったうえでガイドライン改定案に反映予定。

1）ミッション遂行

- **基本的な考え方**：本人確認の障壁によって、必要な行政サービスの遂行が阻害されてはならないと考える。例えば生活に直結するような緊急を要する支援金等の給付において、本人確認が障壁となって給付が行えなくなるようなことがあってはならない。
- **代替手段や例外措置の考え方**：厳格な本人確認手法を採用することでミッション遂行を阻害してしまう場合においては、ミッション遂行を優先するための代替手段や例外措置を設けておかなければならないと考える。また、利用者が身分証を紛失中であったり、手続きに必要な暗証番号を覚えていないようなケースについても考慮し、ミッション遂行の観点で身分証の再発行や暗証番号の再設定を待つことができるのか、それとも例外措置を設けるべきなのかなどについても検討が必要である。
- **発見的統制の考え方**：提供しようとする行政サービスの緊急度によっては、本人確認は簡易な方式としつつ不正やなりすましにを事後的に検証可能な情報を記録しておき、監査等によって不正等を検知するといった「発見的統制」の考え方を取り入れることも検討する。

2）公平性とアクセシビリティ

- **基本的な考え方**：本人確認の手法によって、行政サービス提供の公平性が損なわれてはならないと考える。例えば人種、宗教、性別、年齢、住む地域、時間帯、障害の有無、職業などによって、当該手続の利用のしやすさにできる限り差が生じないような本人確認手法を採用しなければならない。
- **代替手段や例外措置**：単一の本人確認手法によって公平性を確保することが難しい場合は、代替手段や例外的な措置を設けておくべきである。

（次頁へ）

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考え方を「基本的な考え方」として解説

（前頁の続き）

3) プライバシー

- **基本的な考え方**：本人確認のうち特に身元確認においては個人に関する情報を収集することになるが、プライバシーの観点からは収集する情報は最小限としなければならない。身元確認が目指すところは「最小限の属性情報の組み合わせによって、申請者を一意に識別する」であると考える。
  また、身元確認において申請者の属性情報を収集する際には、その目的を明示的に通知しなければならない。

4) ユーザビリティ

- **基本的な考え方**：本人確認のユーザビリティは、ミッション遂行、公平性、セキュリティ、プライバシーなどにも影響する重要な要素である。ユーザビリティが悪い場合、利用者が手続を完結できずに断念してしまう懸念がある。また、意図しない入力や操作によってセキュリティやプライバシーの問題に繋がる可能性も考慮すべきである。

5) セキュリティ

- **基本的な考え方**：本人確認のセキュリティレベルは、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の他の観点とトレードオフとなるため、単にセキュリティレベルの高い手法を選べばよいというものではない点を心得る。
  適切なセキュリティレベルの本人確認手法を選択するためには、当該手続におけるリスクを評価することで保証レベルを一次判定し、その後に当該行政手続の特性も踏まえながら、具体的な脅威への耐性、公平性、プライバシー、ユーザビリティ等の観点も考慮しながら採用すべき本人確認手法を選択することが必要である。

有識者の皆様にご意見・議論いただきたいポイント

1.「基本的な考え方」として示す５つの観点について

- 前述の５つの観点について、ご意見をいただきたい。
  - ５つの観点の粒度は適切か。ほかに言及すべき観点はないか
  - 記載順はこの並びが妥当か　等

2. 各観点の記載内容（素案）について

- 前頁までのガイドライン記載案について、ご意見をいただきたい。
  - 各観点で言及すべき内容に不足はないか
  - 例示を示すなどしてガイドライン読者の理解のしやすさを改善すべき点はないか　等

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

③ デジタル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 デジタル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 行政手続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　デジタル本人確認における認証連携モデル
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　デジタル化を前提とした対象手続の業務改革（BPR）
3.2　本人確認を行う必要のある属性の特定
3.3　リスク評価に基づく保証レベルの一次判定
3.4　保証レベルの調整及び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、対面におけるデジタル本人確認等も対象とする

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
③ デジタル本人確認の枠組みを定義・解説

デジタル本人確認の構成要素

- 「身元確認」と「当人認証」に加えて「認証連携」を新たに取り入れる。2章において定義と解説を記載する。
- 認証連携についてはメリットを訴求し、適切なIDプロバイダがある場合には積極的な活用を推奨する。

身元確認

（現行ガイドラインの記載等を元に定義・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。

身分証明書の真正性の確認、身分証明書と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。

- 提出された本人確認書類と同一の人物であること（当人性）
- 現実に存在している人物であること（存在性）
- 生存している人物であること（生存性）
- 同一人物が当該手続/サービスにおいて既に登録されている者でないこと（唯一性）

当人認証

（現行ガイドラインの記載等を元に定義・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
- セッションハイジャック
- 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
- SIMスワップ

認証連携

（今回の改定版より新規定義・解説）

身元確認時の属性情報や当人認証における認証処理を、別のシステム（IdP：IDプロバイダ）と連携して処理すること。

認証連携を活用することで次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。

利用者側のメリット：
- 申請・登録時の入力負担の軽減
- 複数の認証情報の管理負担の解消
- 認証時のユーザ体験の統一・向上

手続/サービス提供側のメリット：
- 認証機能の構築、運用等に要するコストの低減
- 管理・保護しなければならない認証関連データの最小化
- これらによるミッション遂行への専念

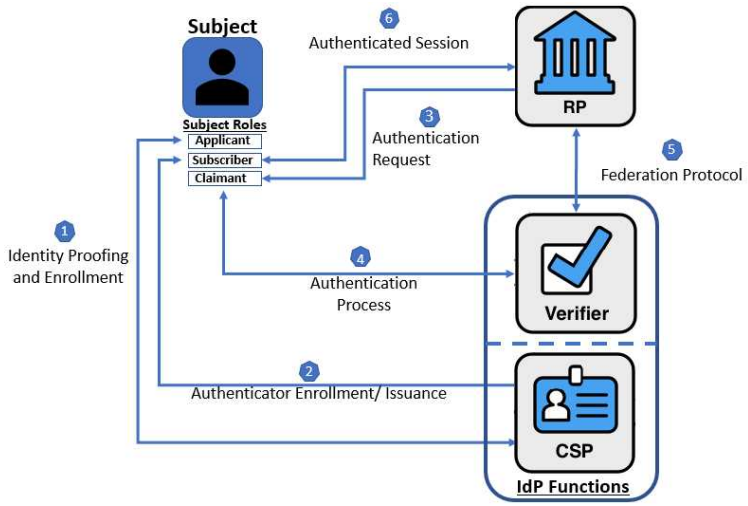
本人確認ガイドラインの主要な改定ポイント
③ デジタル本人確認の枠組みを定義・解説

デジタル本人確認の枠組み

- 基本的なモデルとして「認証連携モデル」と「非認証連携モデル」を図示・解説し、政府の各種認証基盤を活用した「認証連携モデル」の採用を促す。
- Digital Identity Walletを想定したモデルについての必要性は現在検討中。

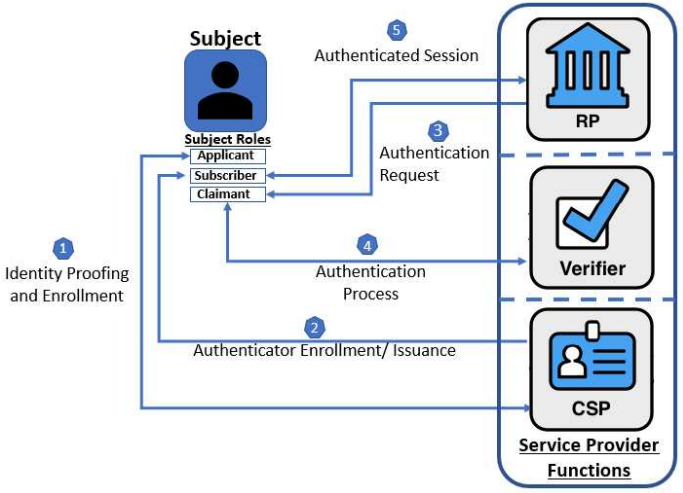
デジタル本人確認の枠組みのイメージ
（改定案のモデルは以下のNIST SP 800-63-4 ipdの”Digital Identity Model” 等を参考として今後作成予定）

認証連携モデル
(Federated Model)



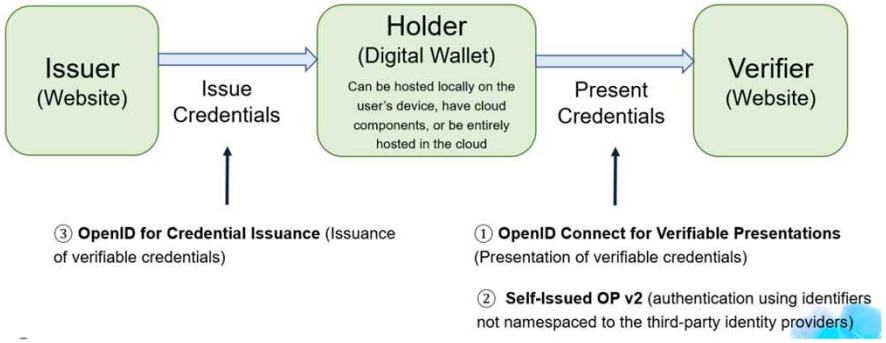
（図の出典：NIST SP 800-63-4 ipd）

非認証連携モデル
(Non-federated Model)



（図の出典：NIST SP 800-63-4 ipd）

Walletモデル（仮称）



（図の出典：OpenID Foundation
“OpenID for Verifiable Credentials”

有識者の皆様にご意見・議論いただきたいポイント

1. 認証連携モデル/非認証連携モデルの考え方や留意点について

- マイナンバーカード等の国内特有の動向、その他の技術動向等を踏まえ留意すべき点、変更・見直しを検討すべき点があればご意見をいただきたい。
  - ❶ Identity Proofing and Enrollmentよりも❷ Authenticator Enrollmentを先にすべき

2. 認証連携モデル（Federated Model）の推奨方針について

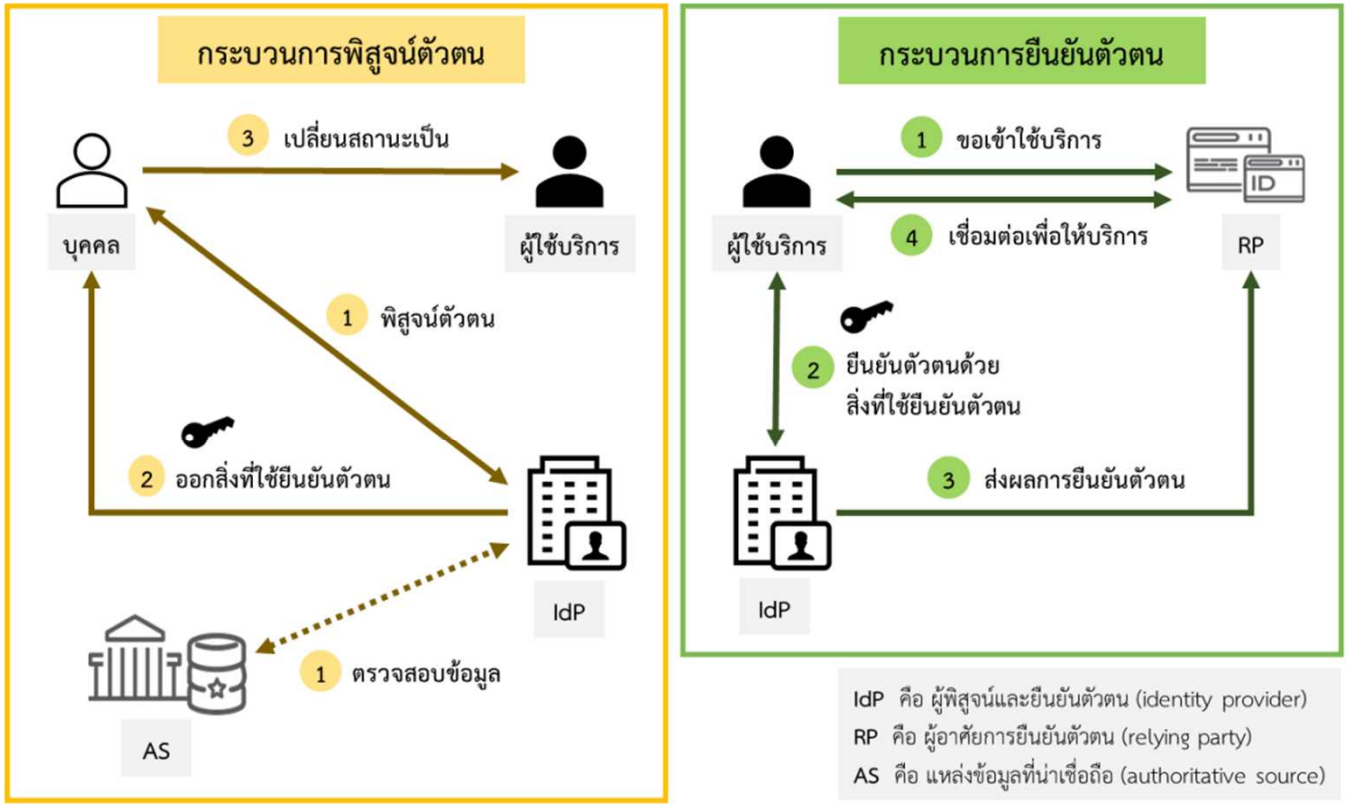
- 本人確認ガイドラインにおいて「認証連携モデル」を推奨することは妥当か。懸念点はないか。
  - 非認証連携モデルを推奨すべきケースがあるとすれば、どのような手続か。

3. Walletモデル（Issuer-Holder-Verifierモデル）について

- 本人確認ガイドラインの次回改定に盛り込むべきか。盛り込むにあたってどのような検討や留意が必要と想定されるか。
  ※SP 800-63-4ではSecond Public DraftでIssuer-Holder-Verifierモデルが盛り込まれる予定とのこと。
  （12/12公開のNIST blogより）

参考：タイ王国のデジタルアイデンティティガイドラインの例

- タイのガイドラインでは、IdPとRPが明示的に区別されたFederatedモデルが記載されている。
  （その上で「ただし、RPとIdPが同一の組織であってもよい」と書かれている。）

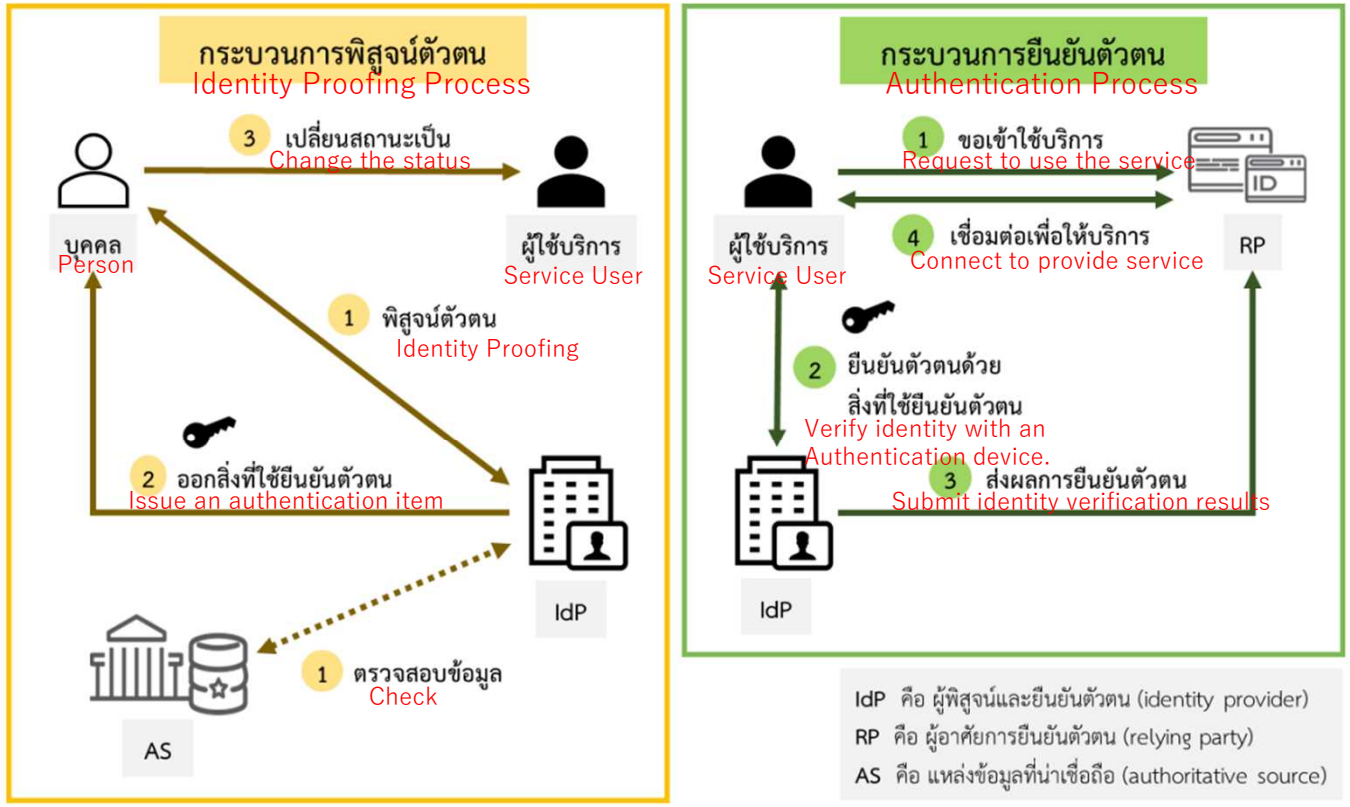


รูปที่ 1 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องในการพิสูจน์ตัวตนและยืนยันตัวตน

出典：ETDA Digital Identity - Framework

参考：タイ王国のデジタルアイデンティティガイドラインの例

- タイのガイドラインでは、IdPとRPが明示的に区別されたFederatedモデルが記載されている。
  （その上で「ただし、RPとIdPが同一の組織であってもよい」と書かれている。）



รูปที่ 1 ความสัมพันธ์ระหว่างผู้ที่เกี่ยวข้องในการพิสูจน์ตัวตนและยืนยันตัวตน
Figure 1. Relationship between people involved in identity Proofing and Authentication

画像出典：ETDA Digital Identity – Framework （赤字部分：仮訳を補記）

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

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 行政手続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　デジタル本人確認における認証連携モデル
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　デジタル化を前提とした対象手続の業務改革（BPR）
3.2　本人確認を行う必要のある属性の特定
3.3　リスク評価に基づく保証レベルの一次判定
3.4　保証レベルの調整及び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、対面におけるデジタル本人確認等も対象とする

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
④ 保証レベルと対策基準の一部を見直し

保証レベルと対策基準の見直し（サマリー）

青字：主な改定ポイント
黄色マーカー：継続検討中の事項

各保証レベルの位置づけと改定方針（現時点案）

身元確認	• **身元確認保証レベル３**：対面での身元確認。NIST IAL3相当となるように対策基準を厳格化する。 • **身元確認保証レベル２**：対面又はオンラインでの身元確認。大きな変更はない。レベルの細分化を検討中。 • **身元確認保証レベル１**：登録コードによる身元確認を認める保証レベル。今回の改定で新設する。 • **身元確認保証レベル０**：身元確認を行わないレベル。現行ガイドラインの「レベル１」から格下げ。
当人認証	• **当人認証保証レベル３**：耐タンパ性HWを含む２要素認証。リアルタイム型フィッシング耐性を「必須」とする。 • **当人認証保証レベル２**：２要素認証。リアルタイム型フィッシング耐性を「推奨」とする。レベルの細分化を検討中。 • **当人認証保証レベル１**：単要素認証。リアルタイム型フィッシング耐性は不要。
認証連携	• **認証連携保証レベル３** • **認証連携保証レベル２** • **認証連携保証レベル１** ：いずれも今回の改定版で新たに定義する。対策基準はNIST FALをベースとして検討中。 （現行ガイドラインでは「認証連携保証レベル」は未定義。） →詳細なレベル定義はNISTの改定動向も踏まえつつ今後検討予定。

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

④ 保証レベルと対策基準の一部を見直し

④-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）

	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** • 現行ガイドラインと同じく、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。	• 対策基準はNIST SP 800-63-4のIAL3相当となるよう厳格化する。 （将来的に「政府機関における個人アイデンティティの検証（Personal Identity Verification: PIV）」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** • 現行ガイドラインを同じく、対面又はオンライン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。	• NIST SP 800-63-4の改定内容やその他の動向等を踏まえ、対策基準の定義を見直す。
身元確認 保証レベル１	**郵送等での身元確認も可とする保証レベル** • 「登録コード」（電子メールや郵送等で送付した6桁の番号等）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位置付ける。	• レベル２よりも簡易的な身元確認手法を認める保証レベルとして新たに定義する。 – 補足：現行ガイドラインにおいて「身元確認を行わないレベル」として定義されている保証レベル１は、改定後はレベル０とする。これにより、改定後の保証レベル１は新設扱いとなる。
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保証レベル１を繰り下げ、保証レベル０として定義する。

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

身元確認保証レベルの対策基準（案）

青字：主な改定ポイント
黄色マーカー：継続検討中の事項

対策基準項目 （括弧内：NIST SP 800-63-4の該当要件/プロセス）	対策基準（案）		
	身元確認保証レベル１（新設） ※SP 800-63-4 second public draftで見直される予定	身元確認保証レベル２	身元確認保証レベル３
身元確認の実施環境 （Presence）	対面又はオンライン （登録コードの送付には郵送や電子メール等を用いる）	対面又はオンライン	対面を原則 リモートの場合：NISTの”Supervised Remote Identity Proofing” 相当の監視環境下を条件とする ※具体的な条件は今後検討する。
必要な 身分証明書 （Evidence）	公的な顔写真付きの身分証を１つ	公的な顔写真付きの身分証を１つ	公的な顔写真付きの身分証を２つ（仮） ※ 必要な身分証明書の点数については、マイナンバーカードへの身分証明書の一元化方針も踏まえながら継続検討中。
身分証明書の 真正性の確認 （Validation）	物理的な身分証の場合： • 券面の目視検査等による真正性の確認 ICカード等の場合： • 耐タンパ性ICチップによる改ざん防止＋デジタル署名の検証による完全性の確認	物理的な身分証の場合： • 券面の目視検査等による真正性の確認 ※物理は非推奨とすべきでないか検討中。 ICカード等の場合： • 耐タンパ性ICチップによる改ざん防止＋デジタル署名の検証による完全性の確認	ICカード等の耐タンパ性ICチップによる改ざん防止＋デジタル署名の検証による完全性の確認 ※ レベル３の身分証明書はICチップ等によるデジタルでの真正性確認を必須とする方向で検討中。
身分証明書と申請者の紐づきの検証 （Verification）	以下のいずれかによる検証 a. 申請者の容貌と身分証の顔写真を比較 b. 身分証に紐づいた暗証番号の入力 c. 事前に確認済みの住所やメールアドレス等に送付した登録コードの入力	以下のいずれかによる検証 a. 申請者の容貌と身分証の顔写真を比較 b. 身分証に紐づいた暗証番号の入力	以下による検証 a. 申請者の容貌と身分証の顔写真を比較 b. 身分証に紐づいた暗証番号の入力
生体情報の収集 （Biometric Collection）	なし	なし	申請者の生体情報（顔写真、指紋等）の情報を収集・記録する

有識者の皆様にご意見・議論いただきたいポイント

1. 身元確認保証レベル3で「ICチップ等によるデジタルでの真正性確認」を必須とすることについて

- 「身元確認保証レベル3」はPIV等での活用を見据えて厳格化する方針であり、ICチップ等を有した身分証明書によるデジタルによる真正性確認を必須とすることを検討中。この方針について、妥当性、懸念、留意事項等についてご意見をいただきたい。

2. 身元確認保証レベル2における「物理券面の確認による真正性確認」について

- レベル2においても「物理券面の確認による真正性確認」は非推奨とし、原則としてデジタルによる真正性確認を推奨すべきではないかと検討中。
- この場合、あらゆる対面窓口においてICカードリーダ等が必要となるといった影響も踏まえつつ、将来的に目指すべき姿についてもご議論いただきたい。

3. 身元確認保証レベル2の細分化について

- 第1回会議での「レベル2の解像度が不足するのでは」という旨のご意見を踏まえ、ValidationとVerificationを軸としたレベル細分化の是非を検討中。レベル細分化の是非について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

参考：身元確認保証レベル２の細分化について（議論用のたたき台）

- 例えばVerificationとValidationの強度に応じて保証レベル2を細分化することが検討できるか。

				身分証明書の真正性の確認（Validation）	
				物理的な確認 券面の目視検査等による真正性の確認 （対面又はリモート）	**デジタルでの確認** 耐タンパ性ICチップ等による改ざん防止 ＋デジタル署名での真正性の確認
身分証明書と申請者の紐づきの検証（Verification）	容貌照合 **あり**	**対面**	身分証の顔写真と申請者の**容貌の照合** ＋**生体情報を記録**	厳格化したレベル３では デジタルでの真正性確認を必須とするため 該当手法なし	**保証レベル3**
			身分証の顔写真と申請者の**容貌の照合**	**保証レベル2D** • 券面偽造への耐性はデジタルに劣る • 現在多くの対面窓口で採用	**保証レベル2A** • 券面偽造に対して強い耐性 • 対面手続でもカードリーダ等が必要
		リモート	身分証の顔写真と申請者の**容貌の照合** （カメラ越しの照合）	**保証レベル2E** • 券面偽造への耐性はデジタルに劣る • Verification強度は2Dよりも劣る	**保証レベル2B** • 券面偽造に対して強い耐性 • Verification強度は2Aよりも劣る
	容貌照合 なし	リモート又は対面	身分証に紐づいた**暗証番号**による検証	暗証番号を用いる場合は デジタル身分証が前提となるため 該当手法なし	**保証レベル2C** • 券面偽造に対して強い耐性 • カードの貸し借りは検知できない
			妥当性確認済みの住所等に送付した登録コードによる検証	保証レベル1	

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

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	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。

参考：第1回会議資料より再掲

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。

（本テーマは第4回有識者会議にて議論予定）

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

④-C 認証連携保証レベルの新設

（本テーマは第4回有識者会議にて議論予定）

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

（本テーマは第4回有識者会議にて議論予定）

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　デジタル本人確認における認証連携モデル
- 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　デジタル化を前提とした対象手続の業務改革（BPR）
- 3.2　本人確認を行う必要のある属性の特定
- 3.3　リスク評価に基づく保証レベルの一次判定
- 3.4　保証レベルの調整及び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、対面におけるデジタル本人確認等も対象とする

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。

（本テーマは第4回有識者会議にて議論予定）

本人確認ガイドラインの主要な改定ポイント

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

（本テーマは第4回有識者会議にて議論予定）

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　デジタル本人確認における認証連携モデル
- 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　デジタル化を前提とした対象手続の業務改革（BPR）
- 3.2　本人確認を行う必要のある属性の特定
- 3.3　リスク評価に基づく保証レベルの一次判定
- 3.4　保証レベルの調整及び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、対面におけるデジタル本人確認等も対象とする

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。

デジタル庁
Digital Agency