資料1

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

本人確認ガイドラインの改定に向けた有識者会議
令和6年度（2024年度）第4回

ガイドライン改定案の妥当性に関する協議資料

令和7年1月　　デジタル庁　トラストタスクフォース

デジタル庁
Digital Agency

各回の検討テーマ

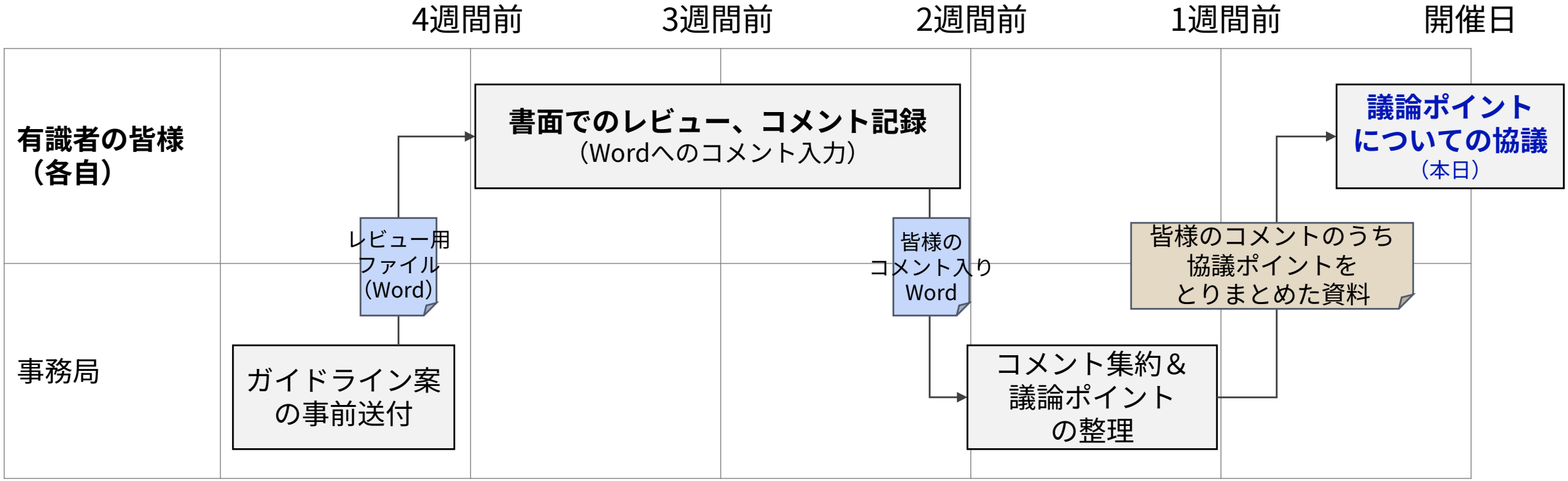
- 本日は「ガイドライン改定案の妥当性に関する協議」の第1回目として、作成中のガイドライン改定案の記載をご確認いただき、見直すべき記載、追加検討すべき論点などについてご議論をお願いします。

開催回	議題予定
第1回 令和6年9月17日（火） 18:00～20:00	• **開催要綱説明** • **ガイドライン改定に向けた論点協議（1）** – 論点1. NIST SP 800-63-4 2pdから反映を検討すべき事項について
第2回 令和6年11月5日（火） 18:00～20:00	• **ガイドライン改定に向けた論点協議（2）** – 論点2. 身元確認保証レベル１の位置づけと本人確認書類の対策基準について – 論点3. フェデレーション保証レベルと対策基準について
第3回 令和6年12月5日（木） 18:00～20:00	• **ガイドライン改定案の妥当性に関する協議（1）** – ガイドライン改定案に対するコメント、指摘、意見交換
第4回 令和7年1月16日（木） 18:00～20:00	• **ガイドライン改定案の妥当性に関する協議（2）** – ガイドライン改定案に対するコメント、指摘、意見交換
第5回 令和7年3月4日（火） 18:00～20:00	• **本人確認ガイドライン改定に向けた最終とりまとめ** – ガイドライン改定案の修正結果の確認 – 最終とりまとめ（案）についての意見交換、内容合意

ガイドライン改定案の妥当性に関する協議の進め方について（再掲）

- 委員の皆様におかれましては、ガイドライン改定案の事前レビューに対応いただき、ありがとうございました。
- 本資料では、皆様からいただいたコメントのうち特にご議論いただきたいポイントを抜粋・整理しておりますので、そのポイントを中心としたご議論やご助言をいただきたくお願いします。

※本資料内で抜粋していないコメントにつきましても、事務局にてガイドライン改定案への反映を検討いたします。



本日の協議対象範囲

第4回会議におけるレビュー・協議の範囲

ガイドライン改定案の目次（現時点案）

1　はじめに
（省略）

2　本人確認の枠組み
2.1　本人確認の基本的要素
2.2　本人確認モデル

3　本人確認における脅威と対策
3.1　身元確認（Identity Proofing）
3.2　当人認証（Authentication）
3.3　フェデレーション（Federation）

4　本人確認手法の検討方法
4.1　検討プロセスの全体像
4.2　リスク評価と保証レベルの判定
4.3　本人確認手法の評価と決定
4.4　継続的な評価と改善

主なレビュー対象範囲

「3.1 身元確認（Identity Proofing）」

第2回・第3回会議でのご意見をもとに、以下の点を見直し

- 身元確認の目的と3つのプロセスの概観図を追加
- 身元確認に関する脅威を詳細化して定義
- 身元確認保証レベルの対策基準を脅威ベースで再整理

「4. 本人確認手法の検討方法」

NISTで取り入れられたテーラリングの考え方などを取り入れつつ、リスク評価プロセスを以下の方針で全面的に見直し

- 従前からのプロセスである「4.2 保証レベルの判定」は判定基準を単純化し、保証レベル判定までの検討負担を軽減
- 今回の改定で追加する「4.3 本人確認手法の評価と決定」において、公平性やプライバシーの観点を含めたテーラリングや例外措置の考え方を導入

※目次は2023年度の中間とりまとめ時点の案をベースに一部修正。
また、別紙の記載は省略しています。

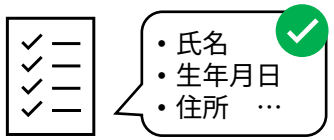
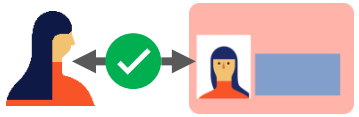
ガイドライン改定案に対するコメント、意見交換

3.1 身元確認（Identity Proofing）
- **身元確認保証レベルの見直し方針について**
- ガイドライン改定案に対する委員からのコメント紹介、意見交換

4. 本人確認手法の検討方法
- リスク評価プロセスの見直し方針について
- ガイドライン改定案に対する委員からのコメント紹介、意見交換

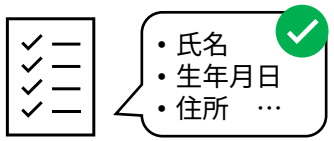
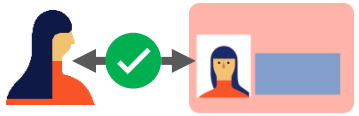
身元確認プロセスの全体像（概観）

- 昨年度までの中間とりまとめ、今年度の第2回会議での議論を踏まえつつ、現在作成中のガイドライン改定案においては身元確認プロセスと各手法を次のように整理・定義した。

身元確認プロセス	プロセスの概要	主な手法
属性情報の収集  	• 申請者から氏名、生年月日、住所等の属性情報を収集し、申請者を一意に識別できる状態とする。 （SP 800-63A-4の ”Resolution” に相当）	a) 本人確認書類から電子データを読み取る b) 本人確認書類の券面から機械的に読み取る c) 申請者自身に記入・入力を求める d) IDプロバイダから取得する
本人確認書類の検証 	• 申請者から提示された本人確認書類が偽造・改ざんされたものでないことを物理的又は電子的に検証する。これにより、収集した申請者の属性情報が正確かつ真正なものであることを確認する。 （SP 800-63A-4の ”Validation” に相当）	a) デジタル署名の検証 b) 対面での券面の検査 c) 非対面での券面の検査
申請者の検証 	• 本人確認書類が備える顔写真や暗証番号等を用いて、提示された本人確認書類が確かに申請者自身のものであることを検証する。 （SP 800-63A-4の ”Verification” に相当）	a) 対面での容貌確認 b) 非対面での容貌確認 c) 暗証番号等による検証 d) 確認コードの送付による検証

身元確認における脅威の整理

- 前述の身元確認の3つのプロセスを軸として、身元確認において想定される主な脅威を以下の8つに区分して定義。

身元確認プロセス	想定される主な脅威		
属性情報の収集  	**❶ 重複登録** • 属性情報の不足や誤り等により、申請者が既に登録済みの人物であると検知できず、重複申請を受け付けてしまう	**❷ 別人との誤紐づけ** • 属性情報の不足や誤り等により、申請者を別の人物と区別できず、別人の情報と紐づけてしまう	
本人確認書類の検証 	**❸ 本人確認書類の偽造・改ざん** • 偽造又は改ざんされた本人確認書類によって、実在する別の人物や架空の人物になりすまされる	**❹ 本人確認書類の複製** • 複製された本人確認書類によって、実在する別の人物になりすまされる	**❺ 本人確認書類の不正な発行** • 不正な手続によって発行された本人確認書類により、実在する別の人物や架空の人物になりすまされる
申請者の検証 	**❻ 本人確認書類の盗用** • 盗まれた本人確認書類によって、実在する別の人物になりすまされる	**❼ 本人確認書類の貸し借り** • 貸し借りされた本人確認書類によって、実在する別の人物になりすまされる	**❽ カメラ映像の偽造・改ざん** • カメラの映像を不正に加工されたり、差し替えられたりすることで、別の人物になりすまされる

脅威に対する対策手法の大まかな強度

- 脅威耐性の観点から保証レベルを定義すべく、前述の脅威に対して想定される手法の強度を大まかにマッピング。

想定される主な脅威	対策手法の大まかな強度 弱 → 強 注：ここで示す強弱関係はあくまで大まかな基準であり、実際の強度は様々な条件によって変化する。			
❶ 重複登録 ❷ 別人との誤紐づけ	申請者自身に 記入・入力を求める	本人確認書類の券面から OCR等で機械的に読み取る	本人確認書類から 電子データを読み取る	
❸ 本人確認書類の偽造・改ざん	非対面での券面の検査	対面での券面検査	デジタル署名の検証	
❹ 本人確認書類の複製	複製対策なし	本人確認書類の複製対策 （複製検知印刷技術等）	本人確認書類の複製対策 （耐タンパー技術等）	
❺ 本人確認書類の不正な発行	信頼できる機関から発行された本人確認書類の利用 （信頼できる機関：本人確認書類の発行プロセスが明らかであり、かつ対象手続に十分な水準で実施されていると信頼できる機関。）			
❻ 本人確認書類の盗用	確認コードの送付	暗証番号等による検証	非対面での容貌確認	対面での容貌確認
❼ 本人確認書類の貸し借り	耐性なし			
❽ カメラ映像の偽造・改ざん	対策なし	ライブネスチェック等の 不正検知技術の採用	統制環境下での リモート身元確認	対面での身元確認

対策基準（案）　―　身元確認保証レベル3

- 保証レベル3は、電子的な検証と対面又は統制環境下での身元確認を求める厳格な対策基準とする。

想定される主な脅威	対策手法の大まかな強度（弱 → 強）			
❶ 重複登録 ❷ 別人との誤紐づけ	申請者自身に 記入・入力を求める	本人確認書類の券面から OCR等で機械的に読み取る	本人確認書類から 電子データを読み取る	
❸ 本人確認書類の偽造・改ざん	非対面での券面の検査	対面での券面検査	デジタル署名の検証	
❹ 本人確認書類の複製	複製対策なし	本人確認書類の複製対策 （複製検知印刷技術等）	本人確認書類の複製対策 （耐タンパー技術等）	
❺ 本人確認書類の不正な発行	信頼できる機関から発行された本人確認書類の利用 （信頼できる機関：本人確認書類の発行プロセスが明らかであり、かつ対象手続に十分な水準で実施されていると信頼できる機関。）			
❻ 本人確認書類の盗用	確認コードの送付	暗証番号等による検証	非対面での容貌確認 注：統制環境下のみ可	対面での容貌確認
❼ 本人確認書類の貸し借り	耐性なし			
❽ カメラ映像の偽造・改ざん	対策なし	ライブネスチェック等の 不正検知技術の採用	統制環境下での リモート身元確認	対面での身元確認

注：ここで示す強弱関係はあくまで大まかな基準であり、実際の強度は様々な条件によって変化する。

対策基準（案）　―　身元確認保証レベル2A

- レベル2Aは、電子的な検証についてはレベル3と同水準としつつ、統制環境以外でのリモート身元確認を許容する。
  （レベル3と比較すると、脅威❻❼❽に対する耐性要件を緩和したレベルとして位置付けられる）

想定される主な脅威	対策手法の大まかな強度（弱 → 強） 注：ここで示す強弱関係はあくまで大まかな基準であり、実際の強度は様々な条件によって変化する。			
❶ 重複登録 ❷ 別人との誤紐づけ	申請者自身に 記入・入力を求める	本人確認書類の券面から OCR等で機械的に読み取る	本人確認書類から 電子データを読み取る	
❸ 本人確認書類の偽造・改ざん	非対面での券面の検査	対面での券面検査	デジタル署名の検証	
❹ 本人確認書類の複製	複製対策なし	本人確認書類の複製対策 （複製検知印刷技術等）	本人確認書類の複製対策 （耐タンパー技術等）	
❺ 本人確認書類の不正な発行	信頼できる機関から発行された本人確認書類の利用 （信頼できる機関：本人確認書類の発行プロセスが明らかであり、かつ対象手続に十分な水準で実施されていると信頼できる機関。）			
❻ 本人確認書類の盗用	確認コードの送付	暗証番号等による検証	非対面での容貌確認	対面での容貌確認
❼ 本人確認書類の貸し借り	耐性なし			
❽ カメラ映像の偽造・改ざん	対策なし	ライブネスチェック等の 不正検知技術の採用	統制環境下での リモート身元確認	対面での身元確認

対策基準（案）　―　身元確認保証レベル2B

- レベル2Bでは、本人確認書類の物理的な検証についても許容するレベルとする。
  （レベル2Aと比較すると、脅威❶❷❸❹に対する耐性要件を緩和したレベルとして位置付けられる）

想定される主な脅威	対策手法の大まかな強度（弱 → 強） 注：ここで示す強弱関係はあくまで大まかな基準であり、実際の強度は様々な条件によって変化する。			
❶ 重複登録 ❷ 別人との誤紐づけ	申請者自身に 記入・入力を求める		本人確認書類の券面から OCR等で機械的に読み取る	本人確認書類から 電子データを読み取る
❸ 本人確認書類の偽造・改ざん	非対面での券面の検査		対面での券面検査	デジタル署名の検証
❹ 本人確認書類の複製	複製対策なし		本人確認書類の複製対策 （複製検知印刷技術等）	本人確認書類の複製対策 （耐タンパー技術等）
❺ 本人確認書類の不正な発行	信頼できる機関から発行された本人確認書類の利用 （信頼できる機関：本人確認書類の発行プロセスが明らかであり、かつ対象手続に十分な水準で実施されていると信頼できる機関。）			
❻ 本人確認書類の盗用	確認コードの送付	暗証番号等による検証	非対面での容貌確認	対面での容貌確認
❼ 本人確認書類の貸し借り	耐性なし			
❽ カメラ映像の偽造・改ざん	対策なし	ライブネスチェック等の 不正検知技術の採用	統制環境下での リモート身元確認	対面での身元確認

対策基準（案）　―　身元確認保証レベル1

- 保証レベル1は、非対面での券面検査などを許容し、必要最低限の脅威への耐性を求めるレベルとする。

想定される主な脅威	対策手法の大まかな強度（弱 → 強）			
	注：ここで示す強弱関係はあくまで大まかな基準であり、実際の強度は様々な条件によって変化する。			
❶ 重複登録 ❷ 別人との誤紐づけ	申請者自身に 記入・入力を求める	本人確認書類の券面から OCR等で機械的に読み取る	本人確認書類から 電子データを読み取る	
❸ 本人確認書類の偽造・改ざん	非対面での券面の検査	対面での券面検査	デジタル署名の検証	
❹ 本人確認書類の複製	複製対策なし	本人確認書類の複製対策 （複製検知印刷技術等）	本人確認書類の複製対策 （耐タンパー技術等）	
❺ 本人確認書類の不正な発行	信頼できる機関から発行された本人確認書類の利用 （信頼できる機関：本人確認書類の発行プロセスが明らかであり、かつ対象手続に十分な水準で実施されていると信頼できる機関。）			
❻ 本人確認書類の盗用	確認コードの送付	暗証番号等による検証	非対面での容貌確認	対面での容貌確認
❼ 本人確認書類の貸し借り	耐性なし			
❽ カメラ映像の偽造・改ざん	対策なし	ライブネスチェック等の 不正検知技術の採用	統制環境下での リモート身元確認	対面での身元確認

補足：対策基準の位置づけについて

- ここで定義する「対策基準」はあくまで「基準」であり、同等と考えられる対策での代替や、テーラリング時の個別リスク評価に応じた個別判断も許容される位置づけのものとする。
  - 例：対象手続のリスクに応じて、特定の脅威に対して上位レベルor下位レベルの手法を採用するなど

- この位置付けは現行ガイドラインも同様である。（以下、現行ガイドラインより抜粋）

> “本ガイドラインの対策基準は絶対的なものではなく、同等の代替基準で あれば他の対応策による代替が許容されるものとする。そこで、各手続の事情に より、対策基準の一部を満たさなくても同等のセキュリティが確保されると判断 される場合には、対策基準の該当部分を見直しても差し支えない。”

参考：ValidationとVerificationのマトリクス

- 前述の案を「本人確認書類の検証手法」と「申請者の検証手法」のマトリクスで表現すると以下のようになる。
  （このマトリクスでは全ての脅威耐性は表現できていないため、参考として掲載）

※上図の点線枠：「❸×①」「❷×②」の組み合わせは、対面と非対面の手法の組み合わせとなるため、実際に採用されることは想定されない。

ガイドライン改定案に対するコメント、意見交換

3.1 身元確認（Identity Proofing）

- 身元確認保証レベルの見直し方針について
- **ガイドライン改定案に対する委員からのコメント紹介、意見交換**

4. 本人確認手法の検討方法

- リスク評価プロセスの見直し方針について
- ガイドライン改定案に対する委員からのコメント紹介、意見交換

ガイドライン改定案　―　1) 身元確認における脅威と対策

３．１　身元確認（Identity Proofing）

身元確認の目的は、申請者から収集した属性情報によって申請者を一意に識別し、その申請者が実在することを確認するとともに、申請された属性情報が正確・真正かつ申請者自身のものであることを確認することである。

本節では、身元確認において想定される脅威を踏まえ実施すべきプロセスと手法を解説し、身元確認における保証レベルと対策基準を定義する。

1)　身元確認における脅威と対策

身元確認において想定される代表的な脅威と対策プロセスとの関係を示す。

No.	代表的な脅威	脅威の概要	対策プロセス
1	重複登録	属性情報の不足や誤り等により、申請者が既に登録済みの人物であると検知できず、重複申請を受け付けてしまう	属性情報の収集
2	別人との紐づけ	属性情報の不足や誤り等により、申請者を別の人物と区別できず、別人の情報と紐づけてしまう	
3	本人確認書類の偽造・改ざん	偽造又は改ざんされた本人確認書類によって、実在する別の人物や架空の人物になりすまされる	本人確認書類の検証
4	本人確認書類の複製	複製された本人確認書類によって、実在する別の人物になりすまされる	
5	本人確認書類の不正な発行	不正な手続によって発行された本人確認書類により、実在する別の人物や架空の人物になりすまされる	
6	本人確認書類の盗用	盗まれた本人確認書類によって、実在する別の人物になりすまされる	申請者の検証
7	本人確認書類の貸し借り	貸し借りされた本人確認書類によって、実在する別の人物になりすまされる	
8	カメラ映像の偽造・改ざん	カメラで撮影した申請者の容貌を不正に加工されたり、差し替えられたりすることで、別の人物になりすまされる	

1) 身元確認における脅威と対策　―　委員の皆さまよりいただいた主なコメント（1/2）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3.1 身元確認（Identity Proofing）	3.1 身元確認（Identity Proofing） 「身元確認の目的は、申請者から収集した属性情報によって申請者を一意に識別し、その申請者が実在することを確認するとともに、申請された属性情報が正確・真正かつ申請者自身のものであることを確認することである。」	「実在すること」は「実在かつ生存すること」ではないでしょうか。ただし生存については、いま生存しているかどうかは問わない業務もあるかと思いますので、その点の記述と合わせて差し支えない表現にすると良いと思います。
		ここの記載は、以下のように整理をしてはいかがでしょうか。 ・身元確認の目的は、申請者が真に申請者であるかを確認することである。 ・身元確認には、対面によるもとのと非対面によるものがある。 ・身元確認には、身元確認を必要とするサービスの特性に応じて、保証レベルを設ける。 ・身元確認のために属性情報を収集し、申請者を一意に識別するなどの方法がとられる。 ・より厳格な身元確認のためには、複製がきわめて困難なICチップを持ちいるなどの方法もとられる。
	表 3-1　身元確認における代表的な脅威と対策プロセス 全般	脅威の記載だけでなく、それによって生じる具体的な影響や被害も明記すると、読み手にとって教育的な意味を持つので良いと考えます。 （例） ・No1: 補助金給付において、同一人物から複数の申請を受けつけ、給付を重複して行ってしまう ・No6: 闇バイトなどによって本人確認を正当に実施し、アカウント登録後に、悪意あるサービス利用者によってアカウントを操作されてしまう

1) 身元確認における脅威と対策　―　委員の皆さまよりいただいた主なコメント（2/2）

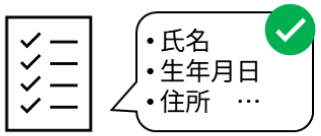
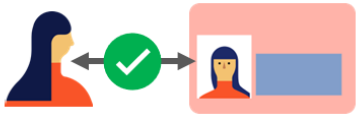
該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3.1 身元確認（Identity Proofing）	表 3-1　身元確認における代表的な脅威と対策プロセス「代表的な脅威」	本人確認を正当に通過したあと、アカウントを売却されてしまう脅威についても掲載しておきたいです。 この脅威はブートストラップでは対処できないため、このリスクを考慮する必要があると判断したビジネスについては、継続的カスタマーデューデリジェンスや、サービス開始後にユーザーが成り代わっていることを想定した後続・継続的な身元確認が求められることにも触れておくとよいのでは。
		本人確認書類の窃盗の他に最近では「売買」もあり対策が必要ですので、記載してはどうでしょうか？
	「本人確認書類の窃盗」	「窃盗」は「盗む行為」そのものなので、ここで用いるべき表現は「盗用」でしょうか。

2) 身元確認のプロセスと手法　―　プロセスの全体像

2)　身元確認のプロセスと手法

前述の脅威へ対抗するため、身元確認は「属性情報の収集」、「本人確認書類の検証」及び「申請者の検証」の3つのプロセスによって実施する。プロセスの全体像と各プロセスの概要を以下に示す。

図　3-1　身元確認プロセスの全体像

	属性情報の収集	本人確認書類の検証	申請者の検証
身元確認プロセス	 氏名、生年月日、住所等の属性情報を申請者から収集し、申請者を一意に識別できる状態とする。	 申請者から提示された本人確認書類が、信頼できる機関から発行されたものであり、偽造・改ざんされたものでないことを、物理的又は電子的に検証する。	 本人確認書類が備える顔写真や暗証番号等の認証機能を用いて、提出された本人確認書類が確かに申請者自身のものであることを検証する。
主な脅威	● 重複登録 ● 別人との誤紐づけ	● 本人確認書類の偽造・改ざん ● 本人確認書類の複製 ● 本人確認書類の不正な発行	● 本人確認書類の盗用 ● 本人確認書類の貸し借り ● カメラ映像の偽造・改ざん

2) 身元確認のプロセスと手法　―　ア　属性情報の収集

2）身元確認のプロセスと手法

ア　属性情報の収集

このプロセスでは、申請者の属性情報（氏名、生年月日、住所等）を収集することで、申請者を一意に識別できる状態とする。

この属性情報が正確に収集できないと、重複登録や別人との誤紐づけの原因となるため、できる限り誤記や表記揺れが発生しにくい方法による収集が望ましい。また、当該情報を取り扱うシステムにおける異体字や外字に関する仕様・制約にも留意する必要がある。

属性情報の収集における主要な手法は以下のとおりである。

a）　本人確認書類から電子データを読み取る

本人確認書類に搭載されたICチップ等から、必要な属性情報を電子データとして読み取る手法。手書きや手入力を伴う手法と比べて、誤記や表記揺れのリスク低減が期待できる。

b）　本人確認書類の券面からOCRで読み取る

OCR（Optical Character Recognition：光学式文字認識）等を用いて、本人確認書類の券面から必要な属性情報を読み取る手法。申請者自身に記入・入力を求める手法と比べて誤記や表記揺れのリスク低減が期待できるが、OCRの読取精度に応じた一定のリスクは残存する。

c）　申請様式や申請フォームへの記入・入力を求める

申請様式や申請フォームを用意し、申請者自身による記入・入力を求める方式。誤記、表記揺れ、入力ミスなどのリスクが存在する。

d）　IDプロバイダから取得する

連携モデルでは、IDプロバイダに身元確認を依拠し、IDプロバイダから必要な属性情報を取得することができる。この場合、後続の「本人確認書類の検証」や「申請者の検証」を実施済みのものとして扱うことができる。

IDプロバイダから取得した属性情報がどの程度の正確性を有しているのか（どの程度の誤記や表記揺れ等のリスクを含んでいるのか）については、IDプロバイダが採用している身元確認手法に依存する。

※第3回会議でいただいたコメントについては順次反映中。全体の構成には大きな変更予定なし。

2) 身元確認のプロセスと手法　―　イ　本人確認書類の検証

イ　本人確認書類の検証

身元確認におけるなりすまし等の不正を防ぐため、申請者から提示された本人確認書類に対して、それが偽造・改ざんされたものでないこと、失効したものでないこと等を検証する。

主要な検証手法は以下のとおりである。手法により検証の強度は大きく異なる。

a)　デジタル署名の検証

本人確認書類に格納された電子データに発行元のデジタル署名が付与されている場合、デジタル署名を検証することで、データの発行元と、データが発行後に改ざんされていないことを検証できる。デジタル署名のもつ暗号学的な性質に基づき、厳密な検証が可能である。

また、公的個人認証制度に基づく電子証明書を格納している本人確認書類を用いる場合、当該電子証明書の有効性確認によって住所や氏名の変更等が行われていないことを検証することもできる。

b)　対面での券面の検査

対面において、本人確認書類の券面を物理的（視覚的・触覚的）に検査することで、偽造・改ざんがされていないことを検証する手法。

この手法による検証の強度は、検査を行う環境（照明の明るさ等）、検査に利用できる道具、本人確認書類が備える偽造対策技術（ホログラムやパールインキ等の印刷技術等）、検査担当者の経験・技能、マニュアルや訓練の有無など、様々な要因によって左右される。

c)　非対面での券面の検査

カメラによる画像・動画の撮影、複合機等による複写・スキャン等によって、本人確認書類の券面を非対面で検証する手法。

手法により強度の差はあるが、この手法による精巧な偽造・改ざんの検知は難しく、対面の場合と比べて検証の強度は低くなる。

※第3回会議でいただいたコメントについては順次反映中。全体の構成には大きな変更予定なし。

2) 身元確認のプロセスと手法　―　ウ　申請者の検証

ウ　申請者の検証

「本人確認書類の検証」によって本人確認書類が真正かつ有効であることを確認できた場合でも、窃盗や貸し借りによって正規の本人確認書類が悪用されている可能性がある。そのため、本プロセスによって本人確認書類が確かに申請者自身のものであることを検証する。

主要な手法は以下のとおりである。手法によって検知可能な攻撃や強度が異なる点に留意が必要である。

a)　対面での容貌比較

対面において、本人確認書類に含まれる顔写真と申請者の容貌とを見比べ、本人確認書類が確かに申請者のものであることを検証する手法。

この検証の強度は、検証を行う環境（照明の明るさ等）、検証時の条件（帽子やマスク等の着脱等）、本人確認書類の顔写真の品質や媒体（券面に印刷されたものか、ICチップに格納された電子データか）、検証を担当する者の経験・技能、マニュアルや訓練の有無など、様々な要因によって左右される。

b)　非対面での容貌比較

オンラインでの手続において、カメラで撮影された映像・画像等を観察することで、本人確認書類に含まれる顔写真と申請者の容貌とを見比べ、本人確認書類が確かに申請者のものであることを検証する手法。

この検証の強度は、カメラでの撮影を行う環境（照明の明るさ等）、カメラの解像度、本人確認書類の顔写真の精度、検査を担当する者の経験・技能、マニュアルや訓練の有無など、様々な要因によって左右される。顔照合技術等を用いて検査担当者を介さずに行う場合は、当該技術の精度によっても左右される。

また、カメラに偽の映像・画像を流し込む、通信途中にデータを差し替える、AI技術等を用いてリアルタイムに加工するなど、この手法で特有の攻撃への対策が必要となる。

c)　認証機能による認証

ICチップを備える本人確認書類やスマートフォンに搭載された本人確認書類等において、それらが備える暗証番号や生体認証等の認証機能を利用することで、申請者が本人確認書類の持ち主であることを検証する手法。

この検証の強度は、認証に用いる要素、認証機能の精度や仕様（暗証番号の桁数、生体認証の本人拒否率や他人受入率等）等に左右されるが、検証の環境や担当者の技能等に左右されにくく、一定の強度が期待できる。ただし、暗証番号を用いる場合、暗証番号が共有され得るため本人確認書類の貸し借りは検知できない。

d)　確認コードの送付による検証

本人確認書類に記載された住所等の連絡先に対して「確認コード（4桁の番号等）」を送付し、申請者がそのコードを受け取り、入力できることをもって申請者と本人確認書類との紐づきを検証する手法。顔写真を含まない本人確認書類にも適用できる特徴がある。

この検証の強度は、検証の環境や担当者の技能等に左右されにくく、対面・オンラインのいずれにおいても一定の強度が期待できるが、確認コードが攻撃者に不正取得されるリスクが存在する。また、確認コードが共有され得るため本人確認書類の貸し借りは検知できない。

なお、本人確認書類に紐づかない連絡先（電話番号、電子メールアドレス等）に確認コードを送付しても、本プロセスが目的とする「申請者と本人確認書類の紐づきの検証」はできない点に留意が必要である。

※第3回会議でいただいたコメントについては順次反映中。全体の構成には大きな変更予定なし。

2) 身元確認のプロセスと手法　―　委員の皆さまよりいただいた主なコメント（1/2）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3.1 身元確認（Identity Proofing） 2) 身元確認のプロセスと手法	表 3-2　身元確認プロセスの概要 No.1 属性情報の収集 氏名、生年月日、住所等の属性情報を申請者から収集し、申請者を一意に識別できる状態とする。	資格の確認においては、生年月日と日付から年齢を計算する例が知られ始めており、身元確認書類に含まれる属性情報の収集だけに留まらない点を触れるかどうかについて確認をしておきたいです。
	イ　本人確認書類の検証 全般	手法が丁寧に分解して定義されていて良い面もあると思うのですが、例えば世の中に存在する「マイナンバーカードの真贋判定器」では、券面情報とICチップの中身を突合し、装置によってICチップ内の写真と所持者の容貌確認ができます。そうした具体例についても明記してはどうでしょうか。
	イ　本人確認書類の検証 削除した「信頼できる情報源への照会」の手法について	属性を検証する観点が抜けているように思えます。券面記載事項についてはIdentity Evidenceが検証されれば裏付けられるということで良いですが、申請者が自らClaimした属性については、reference番号からauthoritative sourceに対して問い合わせを行って裏付けるなどの手段もここに含まれるのではないでしょうか。 将来的にはIdentity Evidenceに署名付きのQRコードを介した問い合わせなども実現しうるものであり、ソースに問い合わせて検証すること自体は含めるべきと考えました。
		「信頼できる情報源への照会」は、属性の収集と検証にもなると思うのですが、エビデンスの有効性がリアルタイムで検証できるという意味ではEvidence Validationにもなるように思います。 マイナンバーカードの場合は、有効性に属性が最新かを含んでいるので、両者にまたがっていますが、PKIを考えるとそもそもはevidenceのvalidationの意味合いが濃いようにおもいました。 つまり項目は残しても良いように思います。

2) 身元確認のプロセスと手法　―　委員の皆さまよりいただいた主なコメント（2/2）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3.1 身元確認（Identity Proofing） 2) 身元確認のプロセスと手法	イ　本人確認書類の検証 a) デジタル署名の検証	デジタル署名の検証と公的個人認証の有効性確認は、別の手法として記載したほうがよいのではないでしょうか。その方が拡張性があり、かつ対策基準を書きやすいように思えます。
		前の段落がデジタル署名の検証、この段落が証明書の有効性確認ということで、一緒にするのは違和感があります。「有効性確認」はデジタル署名の検証の一環と考えてよいでしょうか。

3) 身元確認保証レベルと対策基準　―　ア　身元確認保証レベルの位置づけ

ア　身元確認保証レベルの位置づけ

身元確認の保証レベルは、表　3-3に示す4段階で定義する。また、身元確認の各保証レベルと対策基準の全体概要を表　3-5に示す。

表　3-3　身元確認保証レベルの定義

身元確認保証レベル	保証レベルの位置づけ
レベル 3	極めて厳格なレベル。身元確認が失敗したとき、組織の活動が停止する、関係者の財産に甚大な影響を及ぼすなど、影響度が極めて大きい対象手続のみが該当する。
レベル 2A レベル 2B	厳格な強度をもつレベル。身元確認失敗時の影響度が比較的高い対象手続が該当する。 原則としてレベル 2A を推奨するが、受入可能な本人確認書類を広くとる必要がある場合にはレベル 2B を選択する。
レベル 1	一定の強度をもつレベル。身元確認失敗時の影響度が比較的低い対象手続が該当する。

表　3-5　身元確認保証レベルの対策基準（全体概要）

対策分類	対策基準	身元確認保証レベル			
		3	2A	2B	1
本人確認書類の検証	デジタル署名の検証	○	○	○	○
	対面での券面の検査	×	×		
	非対面での券面の検査	×	×	×	
申請者の検証	対面での容貌確認	○	○	○	○
	非対面での容貌確認	※			
	暗証番号等による検証	×			
	確認コードの送付による検証	×	×	×	
その他	顔写真の収集・保管	○	―	―	―

○：必須（複数の欄にまたがる場合は、いずれか 1 つの実施が必須）
―：要件なし（任意）
×：採用不可
※：非対面での容貌確認は「対面に準ずる統制環境下」でのみ可

※ P6-13までの見直し方針は、本日の議論を踏まえて本頁に反映を予定。

3) 身元確認保証レベルと対策基準　―　イ　身元確認保証レベルの対策基準

イ　身元確認保証レベルの対策基準

a)　身元確認保証レベル3の対策基準

身元確認保証レベル3は、以下の全ての対策基準を満たすこと。なお、身元確認保証レベル3は対面での身元確認を原則とするが、表　3-6に示す「対面の準ずる統制環境下」を満たす環境においては非対面での身元確認も実施可とする。

表　3-5　身元確認保証レベル 3 の対策基準

対策分類	想定脅威	対策基準
本人確認書類の検証	本人確認書類の偽造・改ざん 等	a.　デジタル署名の検証により、本人確認書類の真正性の検証を行うこと
申請者の検証	本人確認書類の窃盗	b.　以下のいずれかの手法により、提示された本人確認書類が窃盗や貸し借りされたものでなく、申請者自身のものであることを検証すること ・　対面での容貌確認 ・　表　3-6 に示す「対面に準ずる統制環境下」での非対面での容貌確認
	本人確認書類の貸し借り	
その他	アカウント回復手続に対する攻撃	c.　身元確認完了後のアカウント回復が必要となった場合に備え、申請者の顔写真を収集・保管すること

表　3-6　「対面に準ずる統制環境下」の対策基準

対策分類	想定脅威	対策基準
統制された環境と設備	カメラに対するプレゼンテーション攻撃	a.　複数のカメラを備えるなど、カメラに対するプレゼンテーション攻撃を検知できる環境であること
	侵害された端末によるビデオインジェクション攻撃	b.　適切に管理・制御された専用の端末を用いることで、カメラ映像の改ざんが行われることを防ぐこと
	不明瞭なカメラ映像による不正検知の失敗	c.　十分な照度の照明、適切な解像度を有するカメラを備え、カメラ越しであっても申請者を明瞭な画質で監視できること
	本人確認書類の電子的な改ざん	d.　本人確認書類の読取装置（IC カードリーダー等）は外部から持ち込まれたものではなく、組織に管理され取り外しのできない状態であること
	通信の改ざん、不正な中継	e.　全ての通信は、相互に認証され、かつ暗号化によって保護された通信経路で行われること
訓練されたオペレータによる監視	不正行為全般	f.　不正行為を検出するための訓練を受けたオペレータが遠隔で参加し、身元確認の開始から終了までの申請者の行動についてビデオカメラ等を通じて監視すること。

※ P6-13までの見直し方針は、本日の議論を踏まえて本頁に反映を予定。

3) 身元確認保証レベルと対策基準　―　イ　身元確認保証レベルの対策基準

b)　身元確認保証レベル2Aの対策基準

表　3-7　身元確認保証レベル 2A の対策基準

対策分類	想定脅威	対策基準
本人確認書類の検証	本人確認書類の偽造・改ざん 等	a.　デジタル署名の検証により、本人確認書類の真正性の検証を行うこと
申請者の検証	本人確認書類の窃盗	b.　以下のいずれかの手法により、提示された本人確認書類が申請者自身のものであることを検証すること ・　対面での容貌確認 ・　非対面での容貌確認 ・　暗証番号等による検証

c)　身元確認保証レベル2Bの対策基準

表　3-8　身元確認保証レベル 2B の対策基準

対策分類	想定脅威	対策基準
本人確認書類の検証	本人確認書類の偽造・改ざん 等	a.　以下のいずれかの手法により、本人確認書類の真正性の検証を行うこと ・　デジタル署名の検証 b.　対面での券面の検査
申請者の検証	本人確認書類の窃盗	c.　以下のいずれかの手法により、提示された本人確認書類が申請者自身のものであることを検証すること ・　対面での容貌確認 ・　非対面での容貌確認 ・　暗証番号等による検証

d)　身元確認保証レベル1の対策基準

表　3-9　身元確認保証レベル 1 の対策基準

対策分類	想定脅威	対策基準
本人確認書類の検証	本人確認書類の偽造・改ざん 等	a.　以下のいずれかの手法により、本人確認書類の真正性の検証を行うこと ・　デジタル署名の検証 ・　対面での券面の検査 b.　非対面での券面の検査
申請者の検証	本人確認書類の窃盗	c.　以下のいずれかの手法により、提示された本人確認書類が申請者自身のものであることを検証すること ・　対面での容貌確認 ・　非対面での容貌確認 ・　暗証番号等による検証 ・　確認コードの送付による検証

※ P6-13までの見直し方針は、本日の議論を踏まえて本頁に反映を予定。

3) 身元確認保証レベルと対策基準　―　ウ　本人確認書類の対策基準

ウ　本人確認書類の対策基準

本人確認書類に求めるべき対策基準は、対象手続の利用者層や、採用する本人確認手法によっても異なるため、本人確認手法の検討段階において採用する手法とともに対策基準を個別に検討すること。参考として、想定される対策基準の例を以下に示す。

対策分類	想定脅威	対策基準（例）
共通	本人確認書類の不正発行	a. 信頼できる機関により、適切な本人確認を経たうえで発行された本人確認書類を用いること
	全般	a. 本人確認書類に一意な参照番号が付与されており、不正の発覚時等に発行元への照会が可能であること
本人確認書類の検証のための機能	本人確認書類の偽造・改ざん	（デジタル署名の検証を行う場合） a. 属性情報には発行元によるデジタル署名が付与されており、発行元の検証及び真正性の検証が可能であること b. 格納されたデータの電子的な複製が困難な仕組み（耐タンパ技術等）を備えていること
		（公的個人認証の有効性確認を行う場合） a. 公的個人認証に基づく電子証明書が格納されており、発行元に対する有効性確認が可能であること。
		（対面での券面の検査を行う場合） a. 券面の偽造や改ざんを防止するための技術（ホログラム、パールインキ、顔写真のシェーディング等）を備えていること
		（非対面での券面の検査を行う場合） a. 非対面において改ざんを防止又は検知するための技術（オンラインでの情報照会等）を備えていること
	最新でない本人確認書類の悪用	（最新情報の照会を行う場合） a. 発行元への照会等により、本人確認書類の属性情報が最新であるかを確認できること
申請者の検証のための機能	本人確認書類の窃盗・貸し借り	（対面又は非対面での容貌確認を行う場合） a. 適切な品質の顔写真を券面に含むこと b. 適切な品質の顔写真を電子データに含むこと
		（暗証番号等による検証を行う場合） a. 暗証番号等による認証機能を備えること
		（確認コードの送付による検証を行う場合） a. 確認コードの送付先となる住所等の連絡先情報を含むこと

※ P6-13までの見直し方針は、本日の議論を踏まえて本頁に反映を予定。

2) 身元確認のプロセスと手法　―　委員の皆さまよりいただいた主なコメント（1/3）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3.1 身元確認（Identity Proofing） 3) 身元確認保証レベルと対策基準	ア　身元確認保証レベルの位置づけ 表 3-3　身元確認保証レベルの定義 レベル2A レベル2B	2Aと2Bを明確に区別する必要がなくなってきているように思います。「レベル2A」を「レベル2」とし、「レベル2B」はレベル2の亜種のような表記（レベル2+、レベル２’など）の扱いとしてはいかがでしょうか。
		2Bを「誰一人取り残さない」という観点で残すのか、2Bでも十分なサービスがあるために残すのか、で表現のしかたが変わってくると思いました。2Bを残すことで攻撃者が紛れ込みやすくなるという懸念もあるので、いま一度考え方と表現をていねいに検討すべきかと思います。
		ここの段階で、2A/2Bの違いは受け入れる本人確認書類の違いであることを書いてしまった方がわかりやすいかと思います。
	表 3-4　身元確認保証レベルの対策基準（全体概要）	この条件ですと、犯収法ホ方式（いわゆるeKYC）がレベル2ではなくレベル1に該当します。中間とりまとめではレベル2（2E）でしたので、念のための確認です。
		「Identity evidenceの検証手段によって振れ幅がある」ことに対する方針の記載がない点が引き続き気になります。 現在の案では基本的にはIdentity evidenceは１枚のみ（実質的にマイナンバーカードか免許証かパスポート）であると読み手は理解します。それで良いのかどうかの議論があると良いです。 ベースラインとして「このレベルの検証はできるだろう」というものを基準として、別のIdentity evidenceを組み合わせて提出を求め、複数枚の検証で攻撃者に手間をかけさせる、ミスを誘発させるなどの概念を導入するかの議論が十分ではないと感じます。

2) 身元確認のプロセスと手法　―　委員の皆さまよりいただいた主なコメント（2/3）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3.1 身元確認（Identity Proofing） 3) 身元確認保証レベルと対策基準	表3-5　身元確認保証レベル3の対策基準 その他 c. 身元確認完了後のアカウント回復が必要となった場合に備え、申請者の顔写真を収集・保管すること	アカウント回復に備えた顔写真の収集・保管については、例えば正面の顔画像だけでなく側面の顔画像も保管しておくと識別性能は高くなります。
		アカウント回復に関する対策基準がここにあるのは違和感があります。アカウント回復については「登録時と同等レベル以上の身元確認保証レベルを要求する」くらいでいいのでは？と思います。
		保管の期間についてガイダンスが必要と思います。 また、このときのすり替えなどを考慮し、本人確認書類の検証、申請者の検証とワンストップでシステム化されていることが望ましいことについても記載があると良いと思います。
	表3-6　「対面に準ずる統制環境下」の対策基準 「f. 不正行為を検出するための訓練を受けたオペレータが遠隔で参加し、身元確認の開始から終了までの申請者の行動についてビデオカメラ等を通じて監視すること。」	ここでは、定期的な研修を受けることが望ましいことについて記載があると良いと思います。
	表3-8　身元確認保証レベル2Bの対策基準	レベル2Aではデータとして取得した顔写真を使う必要があるが、レベル2Bでは券面の顔画像も使える、という違いを明確化すべきと思います。

2) 身元確認のプロセスと手法　―　委員の皆さまよりいただいた主なコメント（3/3）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
3.1 身元確認（Identity Proofing） 3) 身元確認保証レベルと対策基準	ウ　本人確認書類の対策基準 本人確認書類に求めるべき対策基準は、対象手続の種類とその利用者層、想定される脅威に応じて、以下の対策基準を満たすこと。	身元確認に必要な本人確認書類に対する真正性の確認などを求める一方で、その本人確認書類に求めるべき対策基準が「個別に検討すること」となっています。対策基準が「例」となってしまっては、依拠するところがあいまいになってしまって、本ガイドラインの役割を小さくしてしまうことを強く憂慮します。
		ここは、本当に「例」でいいのか、例えば、現状のa.とb.は、全て必須なような感じがしてc.以降が条件文がついているように思えるので、例として「個別に検討」ではなく、想定している対策基準の組み合わせがあるように思えます。
	表3-5　本人確認書類の対策基準（例） 全般	前提として、物理的な本人確認書類が念頭にありますか？スマホ搭載されたものは対象として考えますか？ もし対象とする場合、複数スマホへ同じ書類を入れているケースなどへの対応（発行状態の管理が行われているかどうか？）なども論点になると思っています。
	表3-5　本人確認書類の対策基準（例） 「信頼できる機関により、適切な本人確認を経たうえで発行された本人確認書類を用いること」	という記載の「信頼できる機関」とは、もし定義するとなんでしょうか？ authoritative sourceの所以は何？という話にも繋がって明示しずらい所ではありますが
		「適切な本人確認」の定義も必要だと思いますが、難しいですね。

特に協議いただきたいポイント

❶ 身元確認における脅威の整理結果について	• 「身元確認における脅威」の再整理結果について、網羅性・妥当性の観点からのご意見をいただきたくお願いします。 ※事前にいただいた「身元確認後のアカウントの売却」の脅威については、「4) 身元確認に関する考慮事項」において言及する方針で検討中です。
❷ 本人確認プロセスの概観図について	• 新たに作成した「身元確認の3つのプロセスの概観図」の案について、改善点があればご意見をお願いします。
❸ 本人確認書類の「非対面での券面の検査」をレベル1とする方針について	• 身元確認保証レベルの再検討結果のうち「非対面での券面の検査」による手法を保証レベル1へと変更する方針について、妥当であるかどうかの観点からご意見をいただきたくお願いします。
❹ 保証レベル2Bの位置づけについて	• 電子的な検証を必須とするレベル2Aを「レベル2」とし、物理的な検証を許容するレベル2Bは例外的な扱いとすべきか、ご意見をいただきたくお願いします。 （例えば「電子的な検証ができない場合の代替手段」のような手法をガイドライン上で設けておくなど））|
❺ 本人確認書類に対する対策基準の定め方について	• 本人確認書類の対策基準は、採用する手法によって様々なバリエーションが考えられるため「例」としての記載に留めています。この方針についてのご意見、ご懸念がありましたらいただきたくお願いします。

ガイドライン改定案に対するコメント、意見交換

3.1 身元確認（Identity Proofing）
- 身元確認保証レベルの見直し方針について
- ガイドライン改定案に対する委員からのコメント紹介、意見交換

4. 本人確認手法の検討方法
- **リスク評価プロセスの見直し方針について**
- ガイドライン改定案に対する委員からのコメント紹介、意見交換

リスク評価プロセスの見直し方針（概要）

- 4章のリスク評価プロセスは、4.2の保証レベル判定までのプロセスを簡略化しつつ、4.3に公平性やプライバシーへ当への影響を考慮したテーラリングの考え方を取り入れる形で全面的に見直し。

検討プロセスの概要		今回の改定における見直し方針
4.2 リスク評価と保証レベルの判定	• 対象手続の概要、利用者や関係者を明確化したうえで、本人確認のリスクを具体的に特定し、5つのカテゴリーから影響度の大きさを判定する。 • 最も高い影響度を基準として、対象手続に求められる保証レベルを判定する。	**保証レベル判定プロセスの簡略化** • 複雑な判定フローは取りやめ、「最も高い影響度に対応した保証レベルを判定」する方式に。 （NIST SP 800-63-4においても当該フローが廃止される見込みであることを考慮。）
4.3 本人確認手法の評価と決定	• 保証レベルを踏まえ、採用候補となる本人確認手法について、事業目的の遂行、公平性、プライバシー等の観点から手法を評価し、必要な補足的対策、対策基準の見直しなどを検討する。 • 本人確認書類の紛失などの例外ケースを想定した例外措置の必要性を検討する。	**本人確認手法の評価プロセスを新たに定義** （NIST SP 800-63-4のテーラリングプロセスに相当） • 保証レベルに対応する手法を採用した際の影響を様々な観点から評価し、対策や調整を講じるプロセスを4.3として新たに定義。
4.4 継続的な評価と改善	• 継続的な評価に必要となる情報を定義し、収集を行う。 • 収集した情報をもとに本人確認手法の評価を行い、必要に応じて改善措置を講じる。	**継続的な評価と改善プロセスの具体化** • 継続的な改善については現行ガイドラインにおいても記載があったものであるが、1つのプロセスとして定義したうえで記載内容を具体化。

補足：リスク評価ワークシート（案）による検討支援

- リスク評価を円滑に行えるよう、4章のリスク評価プロセスに沿った「リスク評価ワークシート」を参考資料として別途作成し、ガイドラインとともに公開予定。

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機械的に判定。
- 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。

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。 →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する。 ・いずれか1つ以上に該当する場合は、当該手続の身	**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。または、組織の資産や公共の利益に重大な損害を及ぼす。			
	②信頼や評判の棄損（中位）：深刻かつ短期間又は限定的かつ長			

（令和5年度 第2回会議資料より）

ガイドライン改定案に対するコメント、意見交換

3.1 身元確認（Identity Proofing）
- 身元確認保証レベルの見直し方針について
- ガイドライン改定案に対する委員からのコメント紹介、意見交換

4. 本人確認手法の検討方法
- リスク評価プロセスの見直し方針について
- **ガイドライン改定案に対する委員からのコメント紹介、意見交換**

ガイドライン改定案　―　4. 本人確認手法の検討方法

４．１　検討プロセスの全体像

本人確認手法の検討プロセスは、表 ４-1のとおりとする。各プロセスの検討結果は文書化して管理し、継続的な評価と改善に活用するものとする。

No.	検討プロセス	概要
1	リスク評価と保証レベルの判定	1)　対象手続における本人確認のリスクを特定する。 2)　特定したリスクが顕在化した場合の影響度の大きさを評価する。 3)　影響度の評価結果に基づき、対象手続に求められる保証レベルを判定する。
2	本人確認手法の評価と決定	1)　保証レベルの判定結果を踏まえ、採用候補となる本人確認手法を選定し、事業目的の遂行、公平性、プライバシー等の観点から手法を評価する。 2)　手法の評価結果を踏まえ、補足的対策の採用、複数の手法の採用、対策基準の見直し等を検討する。 3)　本人確認における例外ケースを想定し、必要な例外措置を定義する
3	継続的な評価と改善	1)　本人確認手法の継続的な評価と改善に必要となる情報を定義し、継続的な情報収集を行う。 2)　収集した情報をもとに本人確認手法の評価を行い、必要に応じて改善のための措置を講じる。

なお、対象手続における本人確認手法の検討前には、対象手続の事務フローを抜本的に見直す業務改革（BPR）を行うものとする。業務改革（BPR）の具体的な手法等については本ガイドラインの対象範囲外であるため、他のガイドライン等を参照すること。

4.2　リスク評価と保証レベルの判定

４．２　リスク評価と保証レベルの判定

1)　リスクの特定

対象手続において本人確認が失敗した場合のリスクを具体的に特定する。少なくとも次の事項を明確化し、文書化する。

表　4-2　リスクの特定において明確化する事項

項目		説明
基本情報	手続・サービスの概要	当該手続・サービスの背景、目的、提供機能の概要等
	取り扱う情報資産	当該手続・サービスにおいて取り扱う情報資産の内容
	利用者の概要	利用者の種類、範囲、人数、考慮すべき特徴や性質
	利用者以外の関係者・関係組織	利用者以外に対象手続に関係する組織（リスクの影響を受ける可能性のある組織）
	採用する本人確認モデル	身元確認の要否、当人認証の要否、フェデレーションの活用有無、フェデレーションで連携する ID プロバイダ名
本人確認のリスク	身元確認において想定されるリスク	身元確認において想定される脅威とリスクの一覧（例えば、身元確認書類が偽造され、なりすましによる不正な申請を受け付けてしまうなど）
	当人認証において想定されるリスク	当人認証において想定される脅威とリスクの一覧（例えば、フィッシングサイトに誘導されるなどして認証情報を窃取され、不正にログインされるなど）

2)　リスクの影響度評価

特定したリスクに対して、以下の①から⑤に示す観点ごとに影響度を評価し、最も高い影響度を「対象手続における総合的な影響度」として判定する。

なお、対象手続によっては身元確認と当人認証で影響度が異なる場合も想定される。そのような場合には、身元確認と当人認証のそれぞれに対して影響度を個別に判定するものとする。

評価結果は文書化して管理する。

※表4-3：次頁に掲載

3)　保証レベルの判定

影響度の評価結果を基に、対象手続における保証レベルを以下の基準に基づき判定する。判定の結果は文書化する。

表　4-4　保証レベルの判定基準

プロセス	影響度	該当する保証レベル
身元確認	高位	身元確認保証レベル 3
	中位	身元確認保証レベル 2A
	低位	身元確認保証レベル 1
	なし	―（身元確認を行う必要がない）
当人認証	高位	当人認証保証レベル 3
	中位	当人認証保証レベル 2A
	低位	当人認証保証レベル 1
	なし	―（当人認証を行う必要がない）

4.2　リスク評価と保証レベルの判定　―　影響度の判定基準

表4-3　影響度の判定基準

影響度	判定基準
高位	①　事業遂行への影響：サービス提供の長期的な中断など、事業遂行に致命的な影響を及ぼす ②　信頼や評判への影響：関係者の信頼、地位、評判に関して、容易には回復できない長期的かつ深刻な影響を及ぼす ③　機密性の侵害：多数の機密情報を閲覧・窃取・改ざんされるなど、容易には復旧できない広範囲の悪影響を及ぼす ④　経済的な影響：個人の生活水準の低下や組織活動の縮小などにつながる甚大な経済的損失を及ぼす ⑤　生命や安全への影響：生命の危険、住居の喪失、安全な労働環境の喪失などの重大な影響を及ぼす
中位	①　事業遂行への影響：複数の利用者に対するサービス提供の中断など、事業遂行に対して広範囲の影響を及ぼす ②　信頼や評判への影響：関係者の信頼、地位、評判に関して、回復可能な影響を及ぼす ③　機密性の侵害：攻撃や侵害を受けた当事者に関する機密情報を閲覧・窃取・改ざんされるなど、限定的な悪影響を及ぼす ④　経済的な影響：個人の生活水準や組織活動への影響は軽微であるが、補償や補填を要する程度の経済的な損失を及ぼす ⑤　生命や安全への影響：関係者の安全に軽微な影響を及ぼす可能性がある
低位	①　事業遂行への影響：影響範囲は攻撃や侵害を受けた当事者のみに限定される ②　信頼や評判への影響：関係者の信頼、地位、評判に対して、回復可能な軽微な影響を及ぼす ③　機密性の侵害：攻撃や侵害を受けた場合でも、機密情報の侵害は生じない又は軽微な範囲に留められる ④　経済的な影響：補償や補填を要しない程度の軽微な影響に留められる ⑤　生命や安全への影響：関係者の生命、安全には影響を及ぼさない
なし	上記のいずれにも該当しない場合

4.3　本人確認手法の評価と決定（1/3）

４．３　本人確認手法の評価と決定

1）　採用候補とする本人確認手法の評価

保証レベルの判定結果を基に、採用候補となる本人確認手法を評価する。評価の観点は「1.5基本的な考え方」で示す5つの観点を基本とする。

本人確認手法には様々な種類・方式が存在し、対象手続の事業目的、想定利用者などによって適する手法は異なる。また、同じ保証レベルの手法であってもセキュリティ面の脅威耐性等には差がある。したがって、採用候補とする手法は複数を選定し、比較評価を行うことが望ましい。

影響度の評価結果を基に、対象手続における保証レベルを以下の基準に基づき判定する。判定の結果は文書化する。

評価の観点	評価の観点の具体内容
事業目的の遂行	事業目的の遂行に適した手法であるか。当該事業に求められる特性、本人確認を行う環境、想定される利用者層などに適した手法であり、事業目的の遂行を阻害する懸念がないか。
公平性	十分な公平性を確保できるか。一部の利用者にとって障壁がある手法ではなく、当該事業が対象とする利用者全員ができる限り公平な条件で利用できる手法であるか。
プライバシー	プライバシー面の懸念や考慮事項がないか。例えば利用に当たって必要以上の個人情報を収集してしまうなど、プライバシーの原則に抵触するような制約がないか。
ユーザビリティ及びアクセシビリティ	高いユーザビリティを確保できるか。利用者にとって理解しやすく、間違いにくく、効率的・合理的なユーザビリティを提供できる手法であるか。 十分なアクセシビリティを確保できるか。怪我、障害、視力や聴力の低下などの様々な条件や制約を考慮したうえで、誰もが利用しやすい手法であるか。
セキュリティ	本ガイドラインで示す「対策基準」を満たしているか。また、対象手続において想定される脅威とリスクを踏まえ、必要な脅威耐性を有しているか。耐性を有さない脅威については、当該リスクを受容可能であると判断できるか。

4.3　本人確認手法の評価と決定（2/3）

４．３　本人確認手法の評価と決定

2)　本人確認手法を補完する対策等の検討

前項の評価の結果、採用候補とする本人確認手法が実際に採用可能であるかを検討する。

本ガイドラインで示す対策基準を満たせない場合や、対象手続における要求事項の全てを満たせない場合も想定される。そのような場合には、リスクを低減するための補完的対策の採用、複数の本人確認手法の採用などを検討し、本人確認手法と要求事項とのギャップを解消することを検討する。必要な場合には、保証レベルの見直しについても検討する。

ア　対策基準を補完する対策の採用

採用しようとする本人確認手法が本ガイドラインで示す対策基準の一部を満たしていない場合には、それによるリスクを低減するための補完的な対策を講じたうえで、当該手法を採用する方法が考えられる。

対策基準はあくまで基準であるため、補完的な対策によって同等の脅威耐性を確保できると判断できる場合には、このような方法での調整を行うことができる。

イ　保証レベルの見直し

リスク受容の判断を行ったうえで、対象手続の保証レベルを引き下げ、対応する手法を選択する。例えば、保証レベル2Aと判定された対象手続が、リスク受容の判断のもので保証レベルを2Bに引き下げるなどが考えられる。

本来は対策基準を満たした手法の採用が望ましいが、事業目的の遂行や公平性の確保の観点から、このような方法をとることも検討できる。

ウ　複数の本人確認手法の採用

複数の本人確認手法を採用することで、公平性やアクセシビリティを確保することを検討する。例えば、当人認証において複数の認証手法を提供し、利用者側が選択できるようにするなどの方法が考えられる。

対象手続に高い公平性やアクセシビリティが求められる場合には、このような方法の検討余地がある。

4.3　本人確認手法の評価と決定（3/3）　／　4.4　継続的な評価と改善

3)　例外措置の検討

申請者が本人確認書類を紛失した場合や、当人認証に用いるデバイスが故障した場合など、本人確認手法には様々な例外ケースが発生しうる。対象手続の事業目的や特性によっては、こうした例外ケースが発生した状況においても、代替の手段による申請や手続の受付けを可能としなければならない場合も想定される。

こうした例外ケースへの対処方法の設計を誤ると、なりすまし等の攻撃の起点に悪用される場合があるため、対象手続の保証レベルや採用する本人確認手法と併せて、適切な例外措置をあらかじめ検討・定義する。

また、例外措置は攻撃者の標的となる場合もあるため、例外措置の詳細な方法や手順については原則として公開しないこと。

4.4　継続的な評価と改善

1)　継続的な評価のための情報収集

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

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

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

2)　評価と改善の実施

収集した情報をもとに本人確認手法の評価を行い、必要な場合には改善措置を講じる。

4. 本人確認手法の検討方法　―　委員の皆さまよりいただいた主なコメント（1/4）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
４.２　リスク評価と保証レベルの判定	表4-2　リスクの特定において明確化する事項 「身元確認の要否、当人認証の要否、フェデレーションの活用有無、フェデレーションで連携するIDプロバイダ名」	外部IdPの活用を前提とするのであれば、準拠しているトラストフレームワーク（法令など）についても確認事項とした方が良いかと思います。
1) リスクの特定	表4-2　リスクの特定において明確化する事項 「身元確認において想定される脅威とリスクの一覧（例えば、身元確認書類が偽造され、なりすましによる不正な申請を受け付けてしまうなど）」 「当人認証において想定される脅威とリスクの一覧（例えば、フィッシングサイトに誘導されるなどして認証情報を窃取され、不正にログインされるなど）」	リスク一覧は別に示すのでしょうか。それとも表３－１を意味していますか。 ガイドラインの利用者がこの「リスク一覧」をゼロから作成することは難しいと想定されますので、表３－１と関連させるなど、何かしらのガイダンスが必要ではないでしょうか。
2) リスクの影響度評価	表4-3　影響度の判定基準	影響度ごとに記載されていますが、実務で判定していくときは、①～⑤それぞれで高～低を考えていくように思えます。 書き方だけの問題で好みもあろうかと思いますが、NISTのように ①事業遂行への影響 　高：XXXX 　中：XXXX 　低：XXXX という書き方の方が良いかもしれません。
		運用できるのか、判断できるのか、の議論はこの先も出てくるかとは思いますが、このような記載にせざるをえない部分は理解します。
		「⑤ 生命や安全への影響」の基準が「低位」と「なし」が同じになっています。 とはいえ、低位＝生命や安全への影響がないというのはアリだと思います。

4. 本人確認手法の検討方法　―　委員の皆さまよりいただいた主なコメント（2/4）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
４.２　リスク評価と保証レベルの判定 3) 保証レベルの判定	表4-4　保証レベルの判定基準	「初期判定では、必ず2Aを選択し、2Bは初期判定には含めない」という補足説明は、本文中にも補足として書いておいた方が良いのではないでしょうか。
		見通しと一貫性のために、ここに2Aなどレベル内の階段で表現しなくてよいのではと思います。 ※で細分化しているので上位から採否をテーラリングすることをどこかに明記しておけば良いのでは。
		ここではレベル2Aではなく、単に「レベル2」でいいと思います。 レベル2Bのことを書きたければ、注釈で「受入可能な本人確認書類を広くとる必要がある場合のみ... といったような書きぶりでも良いのではないでしょうか。

4. 本人確認手法の検討方法　―　委員の皆さまよりいただいた主なコメント（3/4）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
４.３　本人確認手法の評価と決定 1)　採用候補とする本人確認手法の評価	表4-5　採用候補とする本人確認手法の評価観点 全般	評価の観点が複数にわたるとき、それぞれの観点における実際の評点のバランスに関する考え方を記載しておいた方が良いのではないでしょうか。 例えば、公平性は高レベルだがプライバシーは０点、とかいうケースにならないようにするために、リスク評価をした結果を受けて最低限中レベルが必要と判断したら全ての観点で中レベルを取ることが必要、など。
	表4-5　採用候補とする本人確認手法の評価観点 プライバシー	集めるか集めないかは重要な観点ですが、日本人がプライバシーと聞くと「集めない、伝えない、隠す」ことだけを強調しがちであるため、サービス提供のために必要な範囲を超える、などもうその先にある観点を補足すると良いと思います。
	表4-5　採用候補とする本人確認手法の評価観点 ユーザビリティ及びアクセシビリティ 「…十分なアクセシビリティを確保できるか。怪我、障害、視力や聴力の低下などの様々な条件や制約を考慮したうえで、誰もが利用しやすい手法であるか。」	そもそも論ですが、「全面的に誰もが利用しやすい」のが良いのか、それとも適した手法を選択できることが良いのでしょうか。 すべての人に高いユーザービリティを確保することは理想ですが、「誰もが利用しやすい（画一的）な手法であるか」ではなく、「それぞれの条件や制約を考慮して代替的な手法や救済を目的とした手段を講じることを含む」というニュアンスが含まれていると良いと考えます。
	表4-5　採用候補とする本人確認手法の評価観点 セキュリティ 「本ガイドラインで示す「対策基準」を満たしているか。また、対象手続において想定される脅威とリスクを踏まえ、必要な脅威耐性を有しているか。耐性を有さない脅威については、当該リスクを受容可能であると判断できるか。」	リスク対応戦略の回避、緩和、移転、受容の観点で記載するほうが、思考を狭めないと思います。耐性を有さないのではなく、リスク対応戦略を取った結果、残存リスクが受容できるかです。 例えば「回避」では、業務をそもそも変えたり、緩和では実現できることを制約したり、移転ではそれこをIdPを利用したり、と様々な選択肢があることを意識させることを意図しています。

4. 本人確認手法の検討方法　―　委員の皆さまよりいただいた主なコメント（4/4）

該当目次	記載内容	コメント（赤字：本日特にご議論いただきたいポイント）
４.３　本人確認手法の評価と決定 2)　本人確認手法を補完する対策等の検討	採用しようとする本人確認手法が本ガイドラインで示す対策基準の一部を満たしていない場合には、それによるリスクを低減するための補完的な対策を講じたうえで、当該手法を採用する方法が考えられる。	ここでは、発見的統制など、補完的な対策の例を記載すると親切かと思います。
	例えば、当人認証において複数の認証手法を提供し、利用者側が選択できるようにするなどの方法が考えられる。	例としてはここでは身元確認のものを何等か記述しておくとよいと思います。「本人確認手法」と記載しているところで、わかりやすい認証手法を挙げていますが、公平性・アクセシビリティで難易度がより高いのは身元確認であると考えるためです。 例えば、初回の身元確認が対面で行われており、マイナカードで確認が取れているのであれば、ハードウェアOTPを郵送で送って仮パスワードでアクティベーションするのも合理的なプロセスです。 一方、初回の身元確認が郵送やオンラインで行われている場合は、マイナンバーカードの受取のとき対面要素とエビデンスの検証を入れるようなバリエーションについて検討できると思います。 そうした記載が本書にはないため、どこかに考え方を記載できると良いと考えます。
４.４　継続的な評価と改善	全般	ここでは研修等による担当者のスキル改善についても触れると良いと思います。

特に協議いただきたいポイント

❶ 保証レベル判定の簡略化について	• リスク評価と保証レベルの判定は、従前のような複雑なフローではなく、「5つのカテゴリーのうち、最も高い影響度に対応する保証レベルを選択する」方式へと見直しました。（※従前のフロー図はNISTを参考としたものであったが、NISTでも-4で削除される見通し） • 後続にテーラリングプロセスを追加したことを考慮した簡略化ですが、この簡略化の妥当性についてご意見があればいただきたくお願いします。
❷ 本人確認手法の評価方法、リスク対応の考え方について	• テーラリングを行う「4.3 本人確認手法の評価と決定」では、5つの評価観点に基づく評価を行うこととしていますが、前半のリスク評価ほどの具体的な基準は示せていません。 • ここは対象手続の個別判断によるところも大きいプロセスであり、全ての観点に対して明確な基準を示すことは難しいと考えておりますが、参考となる基準や指標があればご助言いただきたくお願いいたします。
❸ その他のご意見	• その他、4章全般に対するご意見・コメントがありましたらお願いいたします。

デジタル庁
Digital Agency