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２回分）

令和5年11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

大項目	論点の概要
1. 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
2. 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
3. マイナンバーカードを用いた本人確認の保証レベルの再整理	論点3-1. マイナンバーカードを用いた各保証レベルはどのような位置づけとなるか （※NIST SP 800-63-4における保証レベル定義の見直し等を踏まえた位置づけの確認など）
	論点3-2. マイナンバーカード機能のスマートフォン搭載の保証レベルはどう整理できるか
4. 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

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	本人確認ガイドラインにおいて、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。
妥当性確認（Validation）	NIST SP800-63A-4のValidationに相当する行為のこと。
検証（Verification）	NIST SP800-63A-4のVerificationに相当する行為のこと。
生体情報の比較 （Biometric comparison）	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。 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、申請者と証明書とのバインディングを検証する。
登録コード （Enrollment code）	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。
フィッシング耐性 （Phishing resistant）	本資料中では特に明記しない限り、OTP等では防ぐことが難しいリアルタイムフィッシング攻撃に対する耐性のことを指す。

4. 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

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

- SP 800-63-4 ipdではRisk Managementの章が全面改定された。NISTの改定内容をどのように本人確認ガイドラインに反映していくべきか、現時点の方針の妥当性をご議論いただきたい。

論点概要

- SP 800-63-4 ipdの改定内容を踏まえ、本人確認ガイドラインのリスク評価プロセスをどのように見直すべきか。（NISTの改定ポイントのうち、どのような点を我が国のガイドラインにも取り込むべきか。）
- SP 800-63-4 ipdの主な改定ポイント：
  - ① 個人やコミュニティも含めたリスクの評価
  - ② xALの一次判定後のテーラリングプロセスの追加
  - ③ リスク評価結果の文書化
  - ④ 継続的な評価と改善のプロセスの明文化

現時点の方針

- NISTの改定内容は、いずれも我が国の行政手続においても考慮されるべき事項であると考えられる。
- リスク評価プロセスの複雑化には留意が必要であるが、NISTのいずれの改定ポイントも反映する方向で本ガイドラインを改定する。

  ※ リスク評価プロセスの複雑化に対する対応方針については、論点4-2.で別途協議する 。

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
参考資料

SP 800-63-4 ipdにおけるRisk Managementの改定ポイント

63-4 ipd 5. Risk Managementの目次（青字：主な変更点）

5.1. Conduct Initial Impact Assessment
- 5.1.1. Identify Impacted Entities
- 5.1.2. Identify Impact Categories and Potential Harms
- 5.1.3. Identify Potential Impact Levels
- 5.1.4. Impact Analysis

5.2. Select Initial Assurance Levels
- 5.2.1. Assurance Levels
- 5.2.2. xAL Descriptions
- 5.2.3. Initial Assurance Level Selection

5.3. Tailor and Document Assurance Levels
- 5.3.1. Assess Privacy, Equity, Usability and Threats
- 5.3.2. Identify Compensating Controls
- 5.3.3. Identify Supplemental Controls
- 5.3.4. Document Results - The Digital Identity Acceptance Statement

5.4. Continuously Evaluate and Improve

5.5. Cyber, Fraud, and Identity Program Integrity

※5.5についてはリスク評価プロセスとは別途に反映検討中。

SP 800-63-4 ipdでの主な改定ポイント

① 個人やコミュニティも含めたリスクの評価
- 自組織だけでなく、影響を受ける主体として個人やその他のコミュニティなどを特定し、それらに対するリスクの評価が求められるようになった。（※改定前の63-3でも個人のリスクについては言及されていたが、組織のリスクと明確に区別されるようになった。）

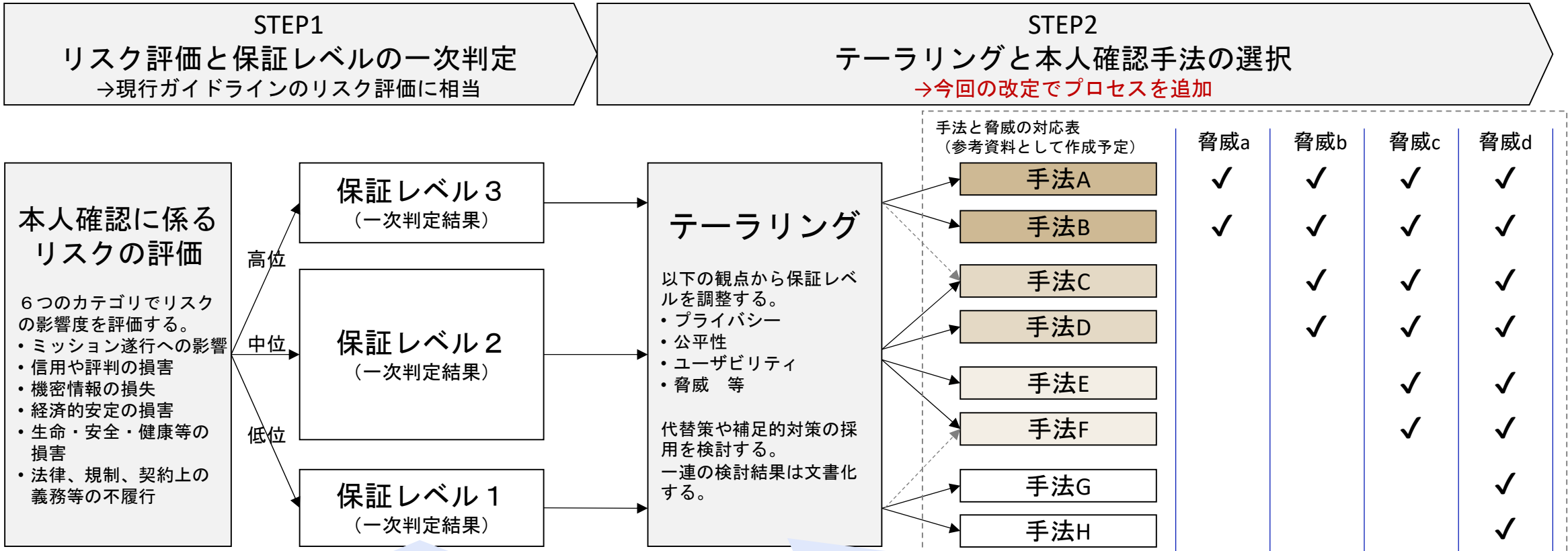
② xALの一次判定後のテーラリングプロセスの追加
- 5.1のリスク評価結果をもとに5.2において初期のxAL（Initial Assurance Level）を選択した後、5.3としてプライバシー、公平性、ユーザビリティ、脅威等の観点からテーラリングを行うプロセスが追加された。

③ リスク評価結果の文書化
- 初期のリスク評価とxALの判定結果、その後のテーラリング結果、代替策を採用する場合の検討結果と残存リスク、その他の補足的対策など、一連のリスク評価結果を文書化することが必須の要求事項として定義された。

④ 継続的な評価と改善のプロセスの明文化
- 脅威の動向やユーザニーズの変化に対応するため、継続的な評価と改善を実施すべき（SHOULD）と明記された。

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
参考資料

リスク評価プロセスの改定案（イメージ）



課題（第１回会議より）

- 特に身元確認保証レベル３を厳格化した場合、多くの手続・手法がレベル２に集中することになり、保証レベルの解像度が不足してしまうのではないか。

解決の方向性（現時点の案）

- 新たに定義するテーラリングプロセスにおいて、プライバシーや公平性等の観点から保証レベルを調整しつつ、脅威ベースで手法を選択できるようなガイドライン参考資料を整備する。これにより、保証レベルの実質的な細分化として機能させることができるのではないか。

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
参考資料

参考：民間事業者向けデジタル本人確認ガイドラインにおけるIALの細分化

保証レベル別の身元確認手法マッピング

IAL	DADC IAL	主な手法例*	行政手続ガイドラインの定義
IAL3	DADC IAL4	• マイナンバーカードの公的個人認証（署名用電子証明書） • マイナンバーカードの機能のスマートフォン搭載の署名用電子証明書（予定）	身元識別情報が特定された担当者の対面で確認され、身元確認の信用度が非常に高い。
IAL2	DADC IAL3	• 犯収法ホ方式 • 犯収法ヘ方式 • 犯収法ト方式 • ホ方式の自動化 • 身元確認結果の活用	身元識別情報が遠隔又は対面で確認され、身元確認の信用度が相当程度ある。
	DADC IAL2	• リアルタイム撮影 • 顔写真付き本人確認書類の裏表のリアルタイム撮影＋容貌の撮影	身元識別情報が確認される必要がなく、身元確認の信用度がほとんどない。身元識別情報は、自己表明若しくは自己表明相当である。
	DADC IAL1	• アップロード	
IAL1	DADC IAL0	• 自己申告	

注釈 ：掲載した手法例は一部であり、今後皆様からのご意見等を踏まえて継続的にアップデートしていきます。
出所：内閣官房 情報通信技術（IT）総合戦略室 (2019)「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」を参照。

167

出典：民間事業者向けデジタル本人確認ガイドライン（ https://www.openid.or.jp/news/kyc_guideline_v1.0.pdf）

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
参考資料

リスク評価プロセスの改定案（本人確認ガイドライン３章の目次案）

本人確認ガイドライン３章の改定案（青字：主な改定箇所）

3.1 デジタル化を前提とした対象手続の業務改革（BPR）（変更なし）

3.2 本人確認を行う必要のある属性情報の特定（変更なし）

3.3 リスク評価と保証レベルの一次判定

1) 影響を受ける主体（組織、個人、コミュニティ等）を特定する。
2) 各リスクカテゴリーに基づきリスク影響度を評価する。
3) 身元確認、当人認証、認証連携のそれぞれの観点から初期のリスク評価を行う。
4) 初期のリスク評価結果をもとに、対象となるオンライン手続きの認証強度として求められるレベル（保証レベル）を一次判定する

3.4 保証レベルの調整、本人確認手法の選択及び文書化

1) プライバシー、公平性、ユーザビリティ、脅威等の観点から一次判定した保証レベルを評価し、必要に応じて見直す。
2) 確定した保証レベルに対応する本人確認の手法を選択する。
3) 代替管理策、補足的対策の必要性を検討する。
4) 検討結果を文書化する。

3.5 継続的な評価と改善

1) 定期的な見直し

SP 800-63-4 ipdでの主な変更点（青字：主な改定箇所）

（NISTには該当プロセスの定義なし）

5.1. Conduct Initial Impact Assessment
- 5.1.1. Identify Impacted Entities
- 5.1.2. Identify Impact Categories and Potential Harms
- 5.1.3. Identify Potential Impact Levels
- 5.1.4. Impact Analysis

5.2. Select Initial Assurance Levels
- 5.2.1. Assurance Levels
- 5.2.2. xAL Descriptions
- 5.2.3. Initial Assurance Level Selection

5.3. Tailor and Document Assurance Levels
- 5.3.1. Assess Privacy, Equity, Usability and Threats
- 5.3.2. Identify Compensating Controls
- 5.3.3. Identify Supplemental Controls
- 5.3.4. Document Results - The Digital Identity Acceptance Statement

5.4. Continuously Evaluate and Improve

4. 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

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

- SP 800-63-4 ipdの改定内容を反映すると、リスク評価プロセスはどうしても複雑化してしまう。これに対して、どのような検討支援や統制の仕組みが考えられるか、議論いただきたい。

論点概要

- SP 800-63-4 ipdではリスク評価プロセスが複雑化したうえ、リスク評価結果をもとに保証レベルを判定するためのフロー図も削除されたため、リスク評価の難易度や検討負担は上がっている。
- これを本人確認ガイドラインに反映した場合、検討時に求められる専門性のレベルも上がると想定される。 これは行政手続の担当職員の負担増を招くだけでなく、ガイドラインの内容が十分に理解・実践されなくなり、適切なリスク評価が行われなくなってしまう事態も懸念される。
- したがって、リスク評価プロセスの見直しとあわせて、リスク評価の検討負担を軽減するための仕組みや、適切なリスク評価が行われていることを確認・統制するような仕組みを検討すべきではないか。

現時点の方針

- リスク評価の負担軽減のための「リスク評価ワークシート」のようなツールを参考資料として整備することで、現場の負担を軽減しつつ、リスク評価結果のレビュー、統制、文書化が図れるのではないかと検討中。
- 他方、こうしたツールの整備によって、SP 800-63-4 ipdで削除された”リスク判定フロー図”と同じような弊害を招くことにならないか、継続検討中。

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
参考資料

63-4 ipdにおけるリスク評価プロセスの複雑化のイメージ

想定される障害モードの特定

身元確認の障害モード
- サービスを異なるSubjectに提供してしまうことによる影響
- 身元確認の過程でSubjectが受ける偏見を含む障壁のために適格なSubjectにサービスが提供されないことによる影響
- 身元確認プロセスをサポートするための過剰な情報収集と保持の影響

当人認証の障害モード
- 誤ったSubjectを認証した場合の影響
- SubjectがAuthenticatorを提示する際に直面する偏見などの障壁により、正しいSubjectの認証に失敗した場合の影響

認証連携の障害モード
- 誤ったSubjectがアプリケーション、システム又はデータへのアクセスに成功した場合の影響
- Subscriber Attributeを誤ったアプリケーションやシステムに開示した場合の影響

リスクレベルの評価マトリクス×３

身元確認に関するリスク評価マトリクス

	組織	個人	その他	総合
①ミッション遂行に対する損害	M	M	L	M
②信用や評判に対する損害	M	L	L	M
③機密情報の損失	H	M	L	H
④経済的安定の損害又は損失		⋮		
⑤生命の損失, 安全・健康・環境的安定に対する損害				
⑥法律, 規制, 契約上の義務のすべて, または一部の不履行				

当人認証に関するリスク評価マトリクス

	組織	個人	その他	総合
①ミッション遂行に対する損害	M	M	L	M
②信用や評判に対する損害	M	L	L	M
③機密情報の損失	H	M	L	H
④経済的安定の損害又は損失		⋮		
⑤生命の損失, 安全・健康・環境的安定に対する損害				
⑥法律, 規制, 契約上の義務のすべて, または一部の不履行				

認証連携に関するリスク評価マトリクス

	組織	個人	その他	総合
①ミッション遂行に対する損害	M	M	L	M
②信用や評判に対する損害	M	L	L	M
③機密情報の損失	H	M	L	H
④経済的安定の損害又は損失		⋮		
⑤生命の損失, 安全・健康・環境的安定に対する損害				
⑥法律, 規制, 契約上の義務のすべて, または一部の不履行				

“全体的な影響度”に基づくxALの一次判定

“全体的な影響度”	対応するIAL
Low	IAL1
Moderate	IAL2
High	IAL3

“全体的な影響度”	対応するAAL
Low	AAL1
Moderate	AAL2
High	AAL3

“全体的な影響度”	対応するFAL
Low	FAL1
Moderate	FAL2
High	FAL3

テーラリングへ

（NIST SP 800-63-4 ipdを元に作成）

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
参考資料

リスク評価ワークシート（案）による検討負担の軽減（案）

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。 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			

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
参考資料

リスク評価ワークシートを用いた検討支援と統制（イメージ）

- 前述のリスク評価ワークシートを用いて、リスク評価やテーラリングに対する助言・レビューなどを行うことで、検討支援や統制を実現できないか。

本人確認ガイドライン
改定案の検討プロセス

3.1 デジタル化を前提とした業務改革(BPR)

3.2 本人確認を行う必要のある属性の特定

3.3 リスク評価と保証レベルの一次判定

3.4 保証レベルの調整、本人確認手法の選択及び文書化

3.5 継続的な評価と改善

当該手続の担当者による検討	リスク評価ワークシートを用いた検討支援・統制（案）
• デジタル原則や他のガイドライン等に基づき、BPRを実施する。 （※BPRは本ガイドラインのスコープ外であるため概要レベルのみ記載）	
• 業務目的や行政間での情報連携の可否等を踏まえ、本人確認を行う必要のある属性情報を特定する。	リスク評価ワークシート（仮）
• 影響を受ける個人等を特定し、6つの影響カテゴリー別に各主体への影響度を評価し、身元確認/当人認証/認証連携それぞれのリスクを評価する。 • リスク評価結果をもとに、身元確認、当人認証、認証連携の各保証レベルを一次判定する。	**①リスク評価の助言やレビュー** • 影響度評価の結果に対する助言 • 事例や参考情報等の提供 • リスク評価結果のレビュー
• 保証レベルに該当する手法を参照しながらプライバシー、公平性、ユーザビリティ、脅威等の観点から保証レベルの一次判定結果を評価し、必要に応じて保証レベルを見直す。 • 採用する手法を選択する。また、必要に応じて代替管理策や補足的対策の検討等を行い、その結果を文書化する。	**②テーラリングの助言・レビュー** • プライバシー、公平性、ユーザビリティ、脅威等の観点からのレビュー • 代替管理策、補足的対策の提案 • リスク評価の検討結果文書として管理
• 脅威の動向、公平性やプライバシーへの影響等の観点から継続的な評価を行い、必要に応じて改善や見直しを行う。	**③継続的な評価の支援** • リスク評価シートの定期的な見直し • 必要に応じた改善提案

リスク評価ワークシートについての懸念点と考え方

リスク評価が形式的になってしまう点について

- ワークシートではどうしてもリスク評価が機械的となってしまうため、SP 800-63-4 ipdで削除された“保証レベルの判定フロー” と同じような弊害を生む原因となってしまうのではないか。

  → 後続のテーラリングプロセスにおいて脅威ベースの手法選択や保証レベルの見直しが適切に実施されるのであれば、保証レベルの一次判定については大まかな機械的判定でもよいと考えられるのではないか。

「リスクの有無」の回答形式の有効性について

- リスク評価プロセスの検討負担を軽減するため、リスクレベル（高位/中位/低位）ではなく「リスクの該否（有無）」を回答させる形式としているが、現場でリスク評価を実施する際に有効に機能するか。

  → 有識者の皆様のご意見を伺わせていただきたい。

デジタル庁
Digital Agency