「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」

改定に向けた中間とりまとめ

令和5年6月　　トラストタスクフォース

デジタル庁
Digital Agency

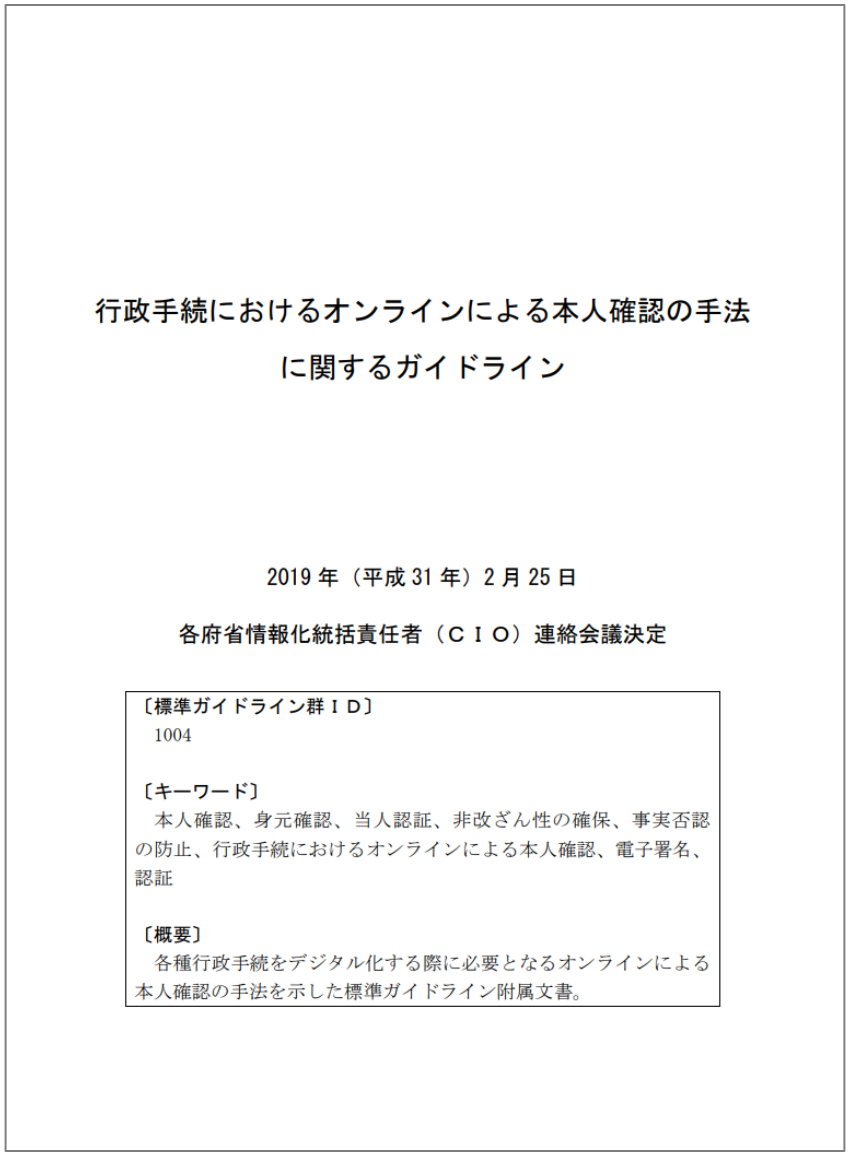
ご意見等連絡先

本ドキュメントについてのご意見等は trust-tf@digital.go.jp までお願いいたします。
なお、いただいたご意見について、必ずしもご返答できるものではない点はご留意ください。

検討の経緯

ガイドライン策定の経緯

行政の在り方そのものをデジタル前提で見直すデジタル・ガバメントを実現するため、平成 30 年 に「デジタル・ガバメント実行計画」が策定。
現行の本人確認ガイドラインは、同実行計画に基づき、行政手続をデジタル化する際に必要となるオンラインでの本人確認に対する考え方及び手法をまとめた文書として、平成31年に「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」として策定された。
現行ガイドラインは米国 NIST SP800-63-3 をベースとしており、オンライン手続に求められる「保証レベル」等を定義。
また、具体手法例についてはマイナンバーカードの公的個人認証等、国内特有の手法例が盛り込まれている。



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

2019 年（平成 31 年）2 月 25 日

各府省情報化統括責任者（ＣＩＯ）連絡会議決定

〔標準ガイドライン群ＩＤ〕
1004

〔キーワード〕
本人確認、身元確認、当人認証、非改ざん性の確保、事実否認の防止、行政手続におけるオンラインによる本人確認、電子署名、認証

〔概要〕
各種行政手続をデジタル化する際に必要となるオンラインによる本人確認の手法を示した標準ガイドライン附属文書。

本人確認ガイドラインを取り巻く状況の変化

状況が大きく変わっていることからガイドラインの改定を計画

NIST SP 800-63の改定

- ベース文書であるSP 800-63がRevision 4へと改定される動き。
  → 令和4年12月16日にInitial Public Draftが公開

国内の動向

- 民間事業者向け本人確認ガイドラインが制定（2023/3/20 OIDF-Jより公開）

マイナンバー関連の動向

- マイナンバーカードの普及と利活用の推進、スマホ搭載の開始（予定）
- マイナンバー法の改正（予定）

GビズID関連の動向

- GビズIDの普及と利活用の推進

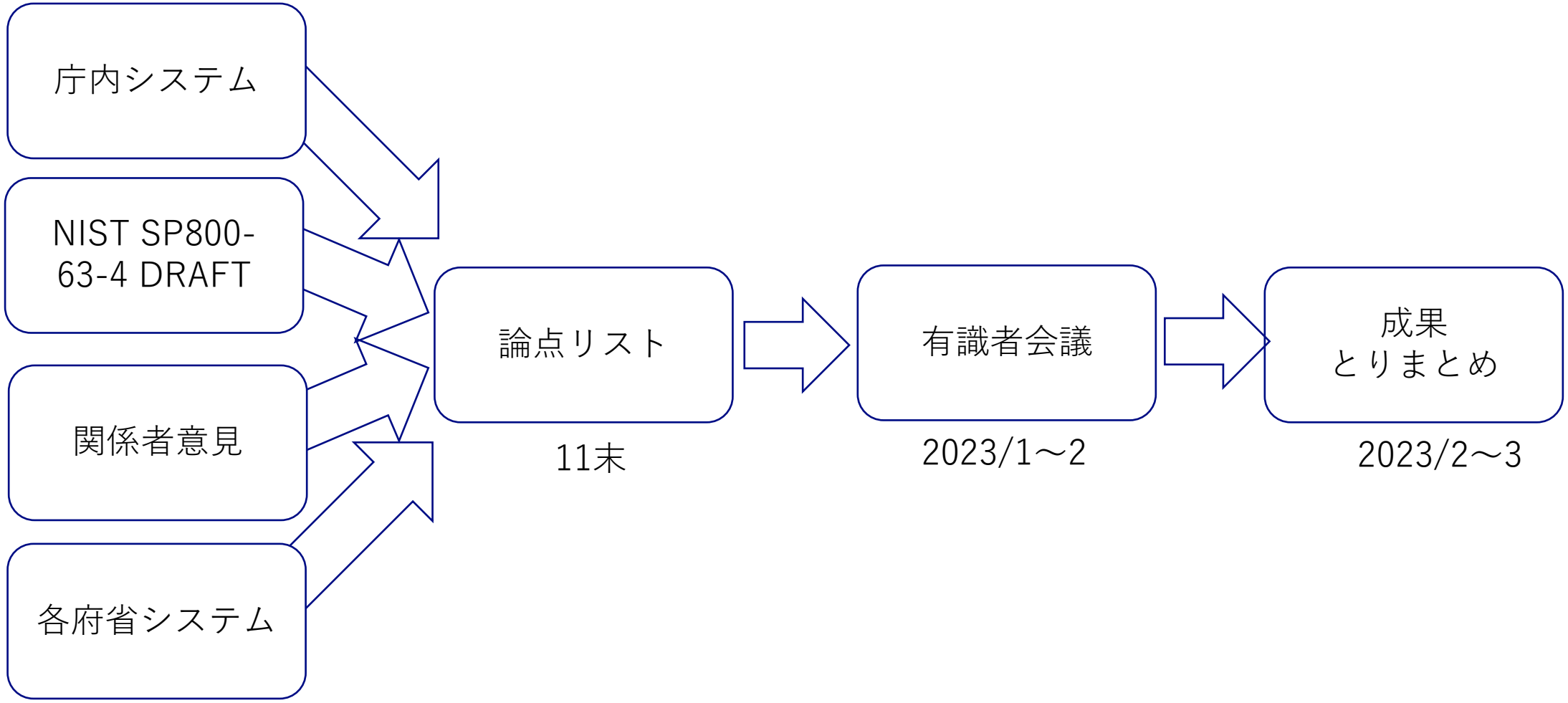
現行ガイドラインの課題

- 現行ガイドラインに内在する既知の課題、利用者からの意見・改善要望等

その他の諸外国の動向

- eIDAS 2.0 / eID / Digital Identity Wallet
- New Zealand Identification Management Standards
- CISA Phishing-Resistant MFA …

令和4年度は下記の活動を実施



有識者会議を２回実施し、とりまとめ

開催日時

- １回目：1/31 18:00-20:00
- ２回目：2/28 18:00-20:00

有識者（あいうえお順）

- **勝原 達也**　アマゾン ウェブ サービス ジャパン合同会社
Specialist Solutions Architect, Security
- **後藤 聡**　TOPPANエッジ株式会社
事業推進統括本部　DXビジネス本部　RCS開発部　部長
- **﨑村 夏彦**　OpenID Foundation Chairman
- **佐藤 周行**　東京大学情報基盤センター准教授・国立情報学研究所学術認証連携委員会
次世代認証連携作業部会/トラスト作業部会 主査
- **肥後　彰秀**　株式会社TRUSTDOCK 取締役
- **富士榮 尚寛**　OpenIDファウンデーションジャパン代表理事
- **南井 享**　株式会社ジェーシービー
イノベーション統括部 市場調査室 部長代理
- **森山 光一**　株式会社NTTドコモ チーフセキュリティアーキテクト
FIDOアライアンス執行評議会・ボードメンバー・FIDO Japan WG座長
W3C, Inc.理事（ボードメンバー）

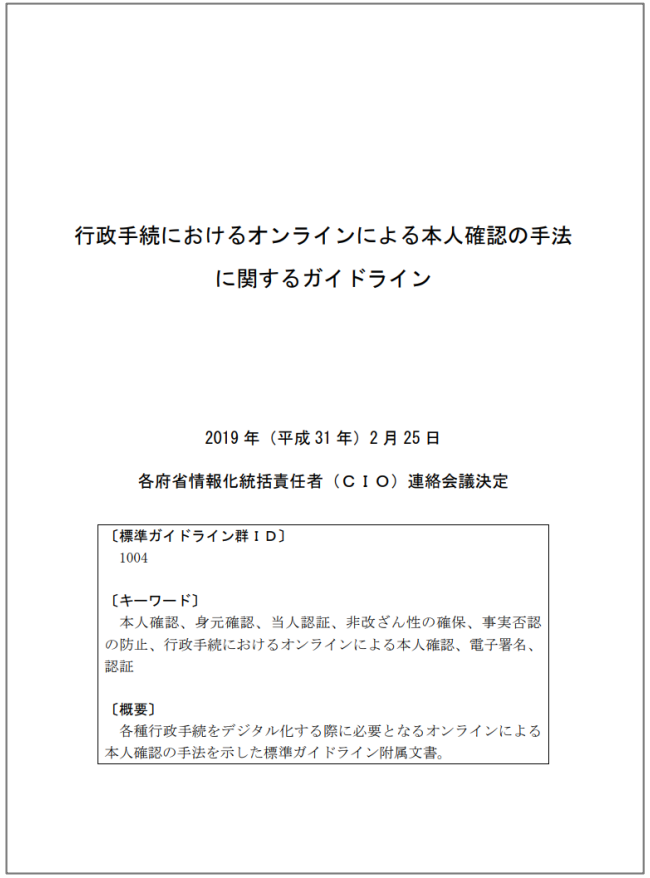
中間とりまとめ資料

目次

目次

「本人確認ガイドライン」
：行政手続のデジタル化にあたり必要となるオンラインでの本人確認に対する考え方及び手法をまとめた文書

「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（以下「本人確認ガイドライン」という。）は、行政手続のデジタル化にあたり必要となるオンラインでの本人確認に対する考え方及び手法をまとめた文書として、平成31年に標準ガイドライン関連資料として策定された。
米国 NIST*が発行する「SP 800-63-3 Digital Identity Guidelines」をベースとしつつ、マイナンバーカードの公的個人認証など我が国特有の手法を掲載している。



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

2019 年（平成 31 年）2 月 25 日

各府省情報化統括責任者（ＣＩＯ）連絡会議決定

〔標準ガイドライン群ＩＤ〕
1004

〔キーワード〕
本人確認、身元確認、当人認証、非改ざん性の確保、事実否認の防止、行政手続におけるオンラインによる本人確認、電子署名、認証

〔概要〕
各種行政手続をデジタル化する際に必要となるオンラインによる本人確認の手法を示した標準ガイドライン附属文書。

*NIST (National Institute of Standards and Technology)：アメリカ国立標準技術研究所。米国連邦政府のコンピュータシステムにかかる標準等を発行している機関。

本人確認ガイドラインを取り巻く状況は初版策定時から大きく変化

政府のオンライン対象手続の拡大、マイナンバーカードの急速な普及など、本人確認ガイドラインを取り巻く状況は平成31年の初版策定時から大きく変化している。
令和4年12月には、ベース文書であるSP 800-63-3の改訂案となるSP 800-63-4 DraftをNISTが公開。令和5年度末までに正式版の発行が予定されている。

国内の動向（一例）

- 政府のオンライン手続の拡大
- ワンスオンリー、コネクテッドワンストップの推進
- マイナンバーカードの普及と利活用の推進
- マイナンバーカード機能のスマートフォン搭載
- マイナポータル、GビズIDなど共通認証基盤の利用拡大
- 民間事業者向け本人確認ガイドラインの制定　等

諸外国の動向（一例）

- NIST SP 800-63の改定
- 欧州 eIDAS 2.0 / eID / Digital Identity Wallet
- New Zealand Identification Management Standards
- CISA Phishing-Resistant MFA ガイドライン　等

本人確認ガイドライン改定に向けた「検討の方向性」を検討

国内外の動向を踏まえ、本人確認ガイドラインを最新情勢に応じた内容へと見直すべく、令和4年度より改定に向けた検討に着手。
関係府省へのヒアリング調査等により課題・要望を調査した後、有識者会議により改定に向けた論点を議論。

これらの検討の中間状況を関係府省に共有するため、
本人確認ガイドラインの改定に向けた「検討の方向性」
として本資料を取りまとめ。

目次

主要な論点

身元確認保証レベル（IAL）の見直し

- SP 800-63-4 Draftでは身元確認の保証レベルの定義（IAL）が見直された。
- 民間ガイドライン等では保証レベルを細分化する動きもみられるため、本人確認ガイドラインへの反映検討が必要。

対策基準の見直し

- 現行ガイドラインの対策基準には共通認証基盤がなかった時代の思想が残っており、オンライン化やマイナンバーカードの普及が進んだ現在においては馴染まない対策が一部見受けられる。

その他

- 共通認証基盤の普及に応じて、フェデレーション（認証連携）に関する記載が必要ではないか。
- 民間ガイドラインとの相互運用性の確保が必要ではないか。

検討の方向性

- SP 800-63-4に盛り込まれた「ミッションデリバリー」「公平性」「プライバシー」「ユーザビリティ」などの観点を参考としつつ、マイナンバーカード等の国内のインフラを踏まえた見直しを行う。
- 保証レベルの細分化については、無用な複雑化を避けるためにも必要性を慎重に検討することとする。

- マイナポータルやGビズID等の共通認証基盤の活用も踏まえ、対策基準全般を見直す。
- マイナンバーカードを持たない利用者に対する代替管理策の考え方、プライバシー、ミッションデリバリーに基づく発見的統制などについても併せて検討する。

- 共通認証基盤の普及、民間や文教との認証連携を見据え、フェデレーションに関する記載を追加する。
- 民間ガイドラインとの相互運用性については、民間ガイドライン側の策定状況等も踏まえながら継続して検討する。

検討の方向性　①保証レベルの見直し　補足

「ミッションデリバリー」指向

- NIST SP 800-63-4では「ミッション遂行」の観点での記述が多く追加された。保証レベルの選定においては一度選択した保証レベルを、ミッション遂行等の観点から調整するプロセスが明記された。
  - 例えば「緊急を要する補助金給付」のようなケースでは「必要な人へ給付が行きわたること」がミッションであり、この遂行を妨げないように本人確認の保証レベルを緩和するような運用が考えられる。
  - 全ての不正受給を事前に防ごうとする「予防的統制」よりも、まずはミッション遂行を優先し、事後的なチェックにより不正を検知するような「発見的統制」の考え方も取り入れることが望まれる。

「公平性」への配慮

- 性別、年齢、人種、障害、その他の特性によらず、サービスを受ける資格や権利を持つすべての人に対して公平なサービスを提供するための配慮が求められている。
  - 例えば、名前入力欄が西洋の名前形式（ファーストネーム、ラストネーム、ミドルネーム）を前提としていたり、顔画像の撮影時において宗教上の理由で着用されている覆いが問題となるケースなどが、公平性への配慮が必要となる一例として挙げられている。
  - ほかにも、年齢層によって利用に障壁が出てしまう技術やプラットフォーム、地域や性別によってアクセスのしやすさに差が生じる運用方法（立地、受付時間）、指紋認証における特定の職業（指紋がなくなってしまうような仕事）への配慮などが、考慮すべきケースの一例として考えられる（有識者会議での議論等で挙がった例より）。

「プライバシー」への配慮

- 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とすべきであり、本人確認に必要のない情報の収集は可能な限り避けるべきである。
  - IAL（身元確認保証レベル）はレベルが高いほどセキュリティの強度が上がるが、プライバシーの観点からはレベルが低いほど望ましいとも言える。

主要な論点

リスク評価プロセスの見直し

- 現在のガイドラインのリスク評価は難解な用語が登場し、判断基準には曖昧な表現もあるため、ガイドラインを利用するPJMO等の職員側からは、より明確で簡易なリスク評価方法が望まれている。
- 一方、ベース文書であるSP 800-63-4においてはリスク評価プロセスが全面改定され、リスク判定のためのフローチャートが削除された。自組織だけでなく、「個人のリスク」や「コミュニティのリスク」の評価も求められるようになり、リスク評価の難易度は全体的に上がっている。
- 現状の課題とSP 800-63-4の改訂内容を踏まえながら、本人確認ガイドラインにおいてどのようなリスク評価を求めていくべきかの検討が必要。

検討の方向性

- 個別システム側の負担を軽減しつつ妥当なリスク評価を行うためのリスク評価のあり方を、デジタル庁や各府省PMOの役割等も含めて総合的に検討する。
  - SP 800-63-4で削除されたフローチャートは、本人確認ガイドラインからも削除する方針とする。有識者会議においても、フローチャートやチェックリストによる機械的・形式的なリスク評価には限界があるとの指摘が挙げられている。
  - 他方、フローチャートやチェックリスト等の形式的な手段なしにリスク評価を実施することは、PJMO職員の負担や専門性の観点からは困難と想定されるため、デジタル庁や各府省PMOの役割等も含めたリスク評価のあり方を総合的に検討する。
- SP 800-63-4において追加された個人やコミュニティ等のリスクの評価についても、本人ガイドラインのリスク評価プロセスへの反映を検討する。

検討の方向性　②リスク評価手法の見直し　補足

個人やコミュニティのリスク評価」について

- SP 800-63-4ではリスクマネジメントプロセスが全面的に見直され、組織（政府機関）自身への影響だけでなく、システムを利用する個人、コミュニティ、他の組織などについても影響度を評価をしたうえで文書化することが求められるようになった。
  - 一例として、個人への影響については「本来受けられるはずの行政サービスが受けられなくなる」、「それにより格差が生じる」、「経済的な損失を受ける」、「身体的・精神的・情緒的な健康への被害を被る」など、複数の観点から影響度分析を行うことが求められている。
  - 本人確認ガイドラインへの反映検討では、個人やコミュニティのリスクの受容判断が必要となるケースも想定されることから、有識者会議等を開催する際の人選にも留意する。

「デジタル庁や各府省PMOの体制・役割も含めた総合的な検討」について

- 令和4年度の有識者会議で挙げられた次のような意見を踏まえ、検討を行う。（一部抜粋・要約）
  - プライバシーも含めたリスク管理には専門的な知識が必要なので専門家を育てる雰囲気を醸成してほしい。リスク管理は素人がやっても上手くいかない。専門家をある程度配置して、機能する体制をデジタル庁が整備する必要があると思う。
  - 専門家については、専門性は兼ね備えながらサービスをよく理解して顧客の利益に繋がるような、かつ社会的に説明ができることに対して積み上げて判断していかなければならない、専門家の難しさがある。
  - 現場の担当者が目的やリスクを正しく理解した上でシステムを作っていくことを期待するのであれば、原則論を押し出した記述とすべき。そうでないのなら、一部の例外は許容して物差しを作ることも一案として考える必要がある。まずはそうした方針を検討すべきてはないか。
  - 英国ではGDS（日本でいうところのデジタル庁、現在はDCMS）にリスク判断を集約し、セキュリティや効率を高めた事例がある。これはひとつの事例であるが、参考とすべきではないか。
  - プライバシーについては、SAOP（Senior Agency Official for Privacy）のような役割も必要なのではないか。

主要な論点

本人確認手法例の最新化

- ガイドライン策定時から技術動向や脅威等が変化しているため、本人確認の手法例についても最新化が必要。

「身元確認」と「当人認証」の手法の分離

- 現在のガイドラインは「身元確認」と「当人認証」の保証レベルをひとまとめにして手法例を記載している。2つの保証レベルが異なる場合にも対応できるよう、手法を分けて記載することを検討する。

手法例の分冊化

- 本人確認の手法例は、技術や脅威の動向に応じて随時見直されることが望ましいため、柔軟な見直し・改訂を行えるように分冊化すべきか検討する。

検討の方向性

- マイナンバーカードの各種機能を使った手法例についての記載を最新化・拡充する。
（署名用電子証明書、利用者証明用電子証明書、券面入力補助AP、スマホ搭載など）
- 昨今の技術と脅威の動向等を踏まえ、フィッシング耐性の必要性などの観点から、各保証レベルに対応する手法例を見直す。
- IAL（身元確認レベル）とAAL（当人認証レベル）をまとめて扱わず、それぞれのレベルに対応した手法を選択できるよう、手法例は分けて記載する。
- 「本人確認の手法例」をガイドライン本編から分離し、Informative（参考情報）な位置づけの文書とする。
これにより情勢に応じた柔軟な改訂を行えるようにする。

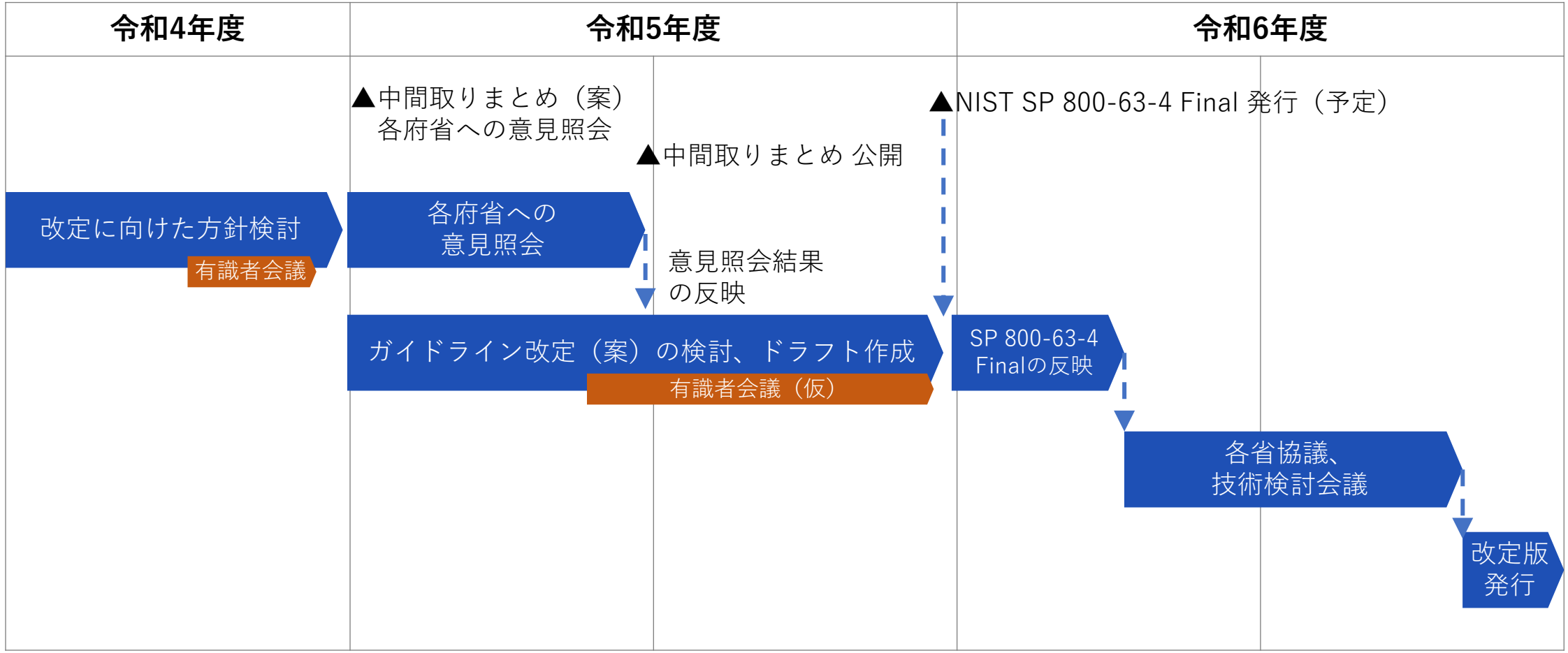
検討の方向性　③本人確認手法例の最新化と分冊化　補足

フィッシング耐性の要求について

- SP 800-63-4ではフィッシング耐性についての要件が追加され、当人認証保証レベル（AAL）がレベル3の場合には「必須」、レベル2の場合には「推奨」とされている。
- 昨今の脅威動向や国内で利用可能なインフラ等の状況を踏まえ、本人確認ガイドラインへの反映においてはレベル2においてもフィッシング耐性を「必須」とすべきかどうか、検討する予定である。

目次

令和6年度の改定を目標として各種検討を実施予定



デジタル庁
Digital Agency

参考資料1　各論点に対する検討の方向性

（有識者会議資料より抜粋）

テーマ１の論点一覧

1-1. IALの見直し	①	SP 800-63-4でのIALの見直しは本人確認ガイドラインにも素直に反映できるのか。
	②	より細やかな粒度で行政手続の特性に応じた身元確認手法を選択できるように、NZの例などを参考として、更なるIALの細分化を行うべきか。
	③	民間の本人確認ガイドラインにおいて細分化されたIAL（DADC・IAL）との相互運用性を、どのレベル、どの範囲で確保すべきか。
1-2. 身元確認の対策基準の見直し	①	昨今の主要な身元確認手法やSP 800-63-4でのIALの改訂内容を踏まえ、IAL2に求める対策基準をどのように見直すべきか。
	②	現ガイドラインでは、NIST SP800-63AのRequirementsを踏まえつつ、我が国の行政機関で採用されうる手法をある程度想定した対策基準を定めた結果、現実の手法との乖離が生じてしまっている。 次期改定時にはベース文書の要求事項を素直に列挙する形式とすべきか。
1-3. フェデレーションに関する内容の追加	①	昨今本人確認ガイドラインの次期改定時にフェデレーションの記載を追加すべきかどうか。またその際には、 NIST SP 800-63-4と同様にNon-Federated ModelとFederated Modelに分けた整理を行うべきか。
	②	将来的な認証連携のニーズや、GビズIDやマイナポータルの整備状況等を踏まえて、具体的にどのようなフェデレーションのユースケースを想定すべきか。

1-1. IALの見直し
― 検討の方向性について

論点	検討の方向性
① SP 800-63-4でのIALの見直しは本人確認ガイドラインにも素直に反映できるのか。	• 「ミッション指向」、「公平性」、「プライバシー」などの観点は参考としつつも**<u>我が国のインフラ※を考慮したIALの見直し</u>**を行う。 ※マイナンバーカードの存在、普及している身分証の種類、Validationの可否など
② より細やかな粒度で行政手続の特性に応じた身元確認手法を選択できるように、NZの例などを参考として、更なるIALの細分化を行うべきか。	• IALの細分化については**<u>必要性を慎重に検討</u>**する。 • むやみに細分化しすることで運用が複雑化してしまい、ガイドラインの実効性が損なわれるリスクを考慮する。
③ 民間の本人確認ガイドラインにおいて細分化されたIAL（DADC・IAL）との相互運用性を、どのレベル、どの範囲で確保すべきか。	• 3月にリリース予定の民間事業者向けガイドラインや論点1-3 のフェデレーションの議論も踏まえつつ、**<u>相互運用性を確保すべき範囲について引き続き検討</u>**する。

1-2. 身元確認の対策基準の見直し ― 検討の方向性について

論点

① 昨今の主要な身元確認手法やSP 800-63-4でのIALの改訂内容を踏まえ、IAL2に求める対策基準をどのように見直すべきか。

② 現ガイドラインでは、NIST SP800-63AのRequirementsを踏まえつつ、我が国の行政機関で採用されうる手法をある程度想定した対策基準を定めた結果、現実の手法との乖離が生じてしまっている。次期改定時にはベース文書の要求事項を素直に列挙する形式とすべきか。

検討の方向性

- 電子署名の部分に限らず、**対策基準は全面的に見直す。**
  - 現在のガイドラインの記載は紙の時代の名残が多い内容となっており、昨今の動向との乖離もみられる。
  - ワンスオンリー（マイナンバーによる行政間での情報連携）の取組みなども踏まえた見直しを行う。
- 見直し検討に当たっては、**プライバシーの観点**（情報のミニマイゼーション等）の考慮事項や、既定の本人確認手法を利用できない場合の**代替管理策の考え方**などについても盛り込む。
- ミッションデリバリーの観点から、予防的統制だけでなく**発見的統制の観点**を取り入れられないか検討を行う。

1-3. フェデレーションに関する内容の追加 ― 検討の方向性について

論点

① 昨今本人確認ガイドラインの次期改定時にフェデレーションの記載を追加すべきかどうか。またその際には、 NIST SP 800-63-4と同様にNon-Federated ModelとFederated Modelに分けた整理を行うべきか。

② 将来的な認証連携のニーズや、GビズIDやマイナポータルの整備状況等を踏まえて、具体的にどのようなフェデレーションのユースケースを想定すべきか。

検討の方向性

- 次期改定ではフェデレーションとFALについての内容を盛り込む。
  - 行政間の連携においては、ワンスオンリーの観点（一度行政が取得した情報を再取得しない）も踏まえた改定検討を行う。
  - サービスによって Core Attributes （そのサービスにおける身元確認のために必要な属性群）が異なるため、マイナンバーには紐づかない情報をどのように対応するのかなどについてもガイドラインでの明確化を検討する。

- 民間や文教との連携については、単なる認証連携（当人認証としての利用）と、属性を含めた連携を区別して検討を行う。
  - B2G、E2Gのケースについては、CSPやIdPによって身元確認のレベル・内容には差があるため、その差によるリスクを考慮した検討を行う。

テーマ２の論点一覧

2-1.「オンラインによる手法例」の見直し	①	IALとAALのレベルを「レベルA～C」とまとめて区分することを見直し、IAL、AALそれぞれに対応する手法例を独立して示すべきではないか。
	②	IALとAALのレベルに差があるケースとしては、具体的にどのようなケースが想定しうるか。 （ガイドラインの読者の理解を促すために例示できるようなケースはあるか。）
2-2. 身元確認の手法例の見直し	①	各省に対して拘束力をもつガイドラインとして、マイナンバーカードによる身元確認を、行政手続における身元確認手法の「原則として採用すべき手法」のような位置づけとすべきか。それとも、手法例の一つに留めるべきか。
	②	マイナンバーカードによる本人確認の保証レベルはどう位置づけられるべきか。
	③	身元確認の「手法例」としてガイドラインに新たに追記すべき手法、解説や注意喚起を掲載すべき手法としては、どのようなものが考えられるか。
2-3. 当人認証の手法例の見直し	①	マイナンバーカード活用を原則とすべきか、手法例の一つに留めるべきか。 （身元確認の手法例の論点と同様。ただし、身元確認と当人認証で位置づけを変えることも想定される。）
	②	当人認証の「手法例」としてガイドラインに追加すべき手法、解説や注意喚起を掲載すべき手法、見直すべき手法にはどのようなものがあるか。

2-1.「オンラインによる手法例」の見直し ― 検討の方向性について

論点

① IALとAALのレベルを「レベルA～C」とまとめて区分することを見直し、IAL、AALそれぞれに対応する手法例を独立して示すべきではないか。

② IALとAALのレベルに差があるケースとしては、具体的にどのようなケースが想定しうるか。
（ガイドラインの読者の理解を促すために例示できるようなケースはあるか。）

検討の方向性

- IALとAALは**<u>分けて検討できるように見直す</u>**。
  - ミッションデリバリーの観点、プライバシーの観点（ミニマイゼーションの観点）を踏まえ、独立して検討されるよう見直す。

- 次のようなケースの例示を検討する。
  - 児童手当などで二重申請させないことが目的であれば、その場でのIALは高くなくてもよく、二重申請を防ぐためにAALは高いレベルが求められる。
    （ミッションデリバリーの観点からは、受給資格の確認は事後的でもよいのでは。）

2-2. 身元確認の手法例の見直し ― 検討の方向性について

論点

① マイナンバーカードによる身元確認を、行政手続における身元確認手法の「原則として採用すべき手法」のような位置づけとすべきか。それとも、手法例の一つに留めるべきか。

② マイナンバーカードによる本人確認の保証レベルはどう位置づけられるべきか。

③ 身元確認の「手法例」としてガイドラインに新たに追記すべき手法、解説や注意喚起を掲載すべき手法としては、どのようなものが考えられるか。

検討の方向性

全般

- 手法例については**脅威ベースで記載する形**とできないか検討する。

個別の本人確認手法例について

- **マイナンバーカードの署名用電子証明書**
  - マイナンバーカード活用を原則とするにしても、必ず合理的な**代替手法とあわせて提示**する形とする。
  - マイナンバーカードによる身元確認の保証レベルについても、必要なAttributeにより異なることに留意する。
- **利用者証明用電子証明書、券面入力補助AP**
  - 手法例として追記することを検討する。
  - 利用者証明用電子証明書を用いて本人確認を実施している各種サービスについて、どのように属性情報の収集および確認がされているのか整理する。

2-3. 当人認証の手法例の見直し ― 検討の方向性について

論点

① マイナンバーカード活用を原則とすべきか、手法例の一つに留めるべきか。
（身元確認の手法例の論点と同様。ただし、身元確認と当人認証で位置づけを変えることも想定される。）

② 当人認証の「手法例」としてガイドラインに追加すべき手法、解説や注意喚起を掲載すべき手法、見直すべき手法にはどのようなものがあるか。

検討の方向性

全般

- 手法例については**脅威ベースで記載する形**とできないか検討する。

個別の当人認証手法例について

- 多要素認証については、**想定脅威に対応する手法（要素）を選択**できるような記載方法を検討する。
- -4Bの主要な変更点である**フィッシング耐性**の有無を考慮した反映を行う。
  - AAL2のフィッシング耐性はNISTどおり“Recommended”でよいのか、それとも本人確認ガイドラインでは ”Required” とすべきか、などについて継続して検討する。

テーマ３の論点一覧

3-1. オンライン本人確認のリスク評価のあり方	① 本人確認ガイドラインにおいて、リスク評価の手順や方法をどのように規定すべきか。63-4での変更内容を素直に反映できるのか。 ② 担当職員が実践できる内容に落とし込むという観点で、より簡易的な保証レベルの判定方法は考えられないか。 – 例えば、手続きの類型（補助金申請、許認可）別にベースラインを示す方法はどうか。 – 既存のIdP（GビズID、マイナポータル等）を利用する場合には、その保証レベルを受容可能かどうかを判定できるチェックリストのようなものを作れないか。
3-2. ガイドラインのドキュメント構成の見直し	① ガイドラインを ”Normative” と ”Informative” のコンテンツに分けて整備しようとする場合に、考慮・留意すべき点はあるか。 ※本論点については、反対意見やご懸念がある場合にご意見をお願いします。
3-3. 前述までの論点以外に検討・考慮すべきポイント	① 前述までの論点以外に、本人確認ガイドラインの次回改定に向けて検討・考慮すべきSP 800-63-4の変更ポイントはあるか。 ② また「NISTが特にコメントを求める点」として挙げられている事項に対して、どのような留意が必要となるか。

3-1. オンライン本人確認のリスク評価のあり方 ― 検討の方向性について

論点

① 本人確認ガイドラインにおいて、リスク評価の手順や方法をどのように規定すべきか。63-4での変更内容を素直に反映できるのか。

② 担当職員が実践できる内容に落とし込むという観点で、より簡易的な保証レベルの判定方法は考えられないか。

検討の方向性

- リスク評価を個別手続きの現場に任せられるようにするのか。それとも現場には最低限のチェックをさせて、リスクマネジメントはデジタル庁側で行うのか。デジタル庁として目指す姿を整理する。
  - 中央に集約するケースは、諸外国（英国）での事例等も参考にできるのではないか。
  - 完璧なフロー図のようなものと作るのは困難と考えた方がよい。
  - 組織だけでなく、個人やコミュニティのリスクも考慮が必要。また、個人やコミュニティのリスク受容判断は組織にはできないので、マルチステークホルダーモデルでの議論も必要ではないか。
- 他方、地方自治体などから参照されているガイドラインである、という点も考慮する必要がある。

3-2. ガイドラインのドキュメント構成の見直し ― 検討の方向性について

論点

① ガイドラインを ”Normative” と ”Informative” のコンテンツに分けて整備しようとする場合に、考慮・留意すべき点はあるか。

検討の方向性

- 「手法例」の内容はInformativeとして分離する方針とする。
- 分離に当たっては次の点に留意する。
  - Informativeを出した後にNormativeが他省庁からの意見で内容が変わるなど、不整合のリスクには考慮が必要。
  - このガイドラインの特性と考慮すると、NormativeとInformativeをそこまで明確に扱う必要はそれほど高くないかもしれない。（改訂プロセスの観点はあるにせよ。）
  - 他方、相互運用性の確保という観点では、Normativeの範囲は重要である。現時点では民間ガイドラインとの相互運用性を考慮する。

3-3. 前述までの論点以外に検討・考慮すべきポイント ― 検討の方向性について

論点

① 前述までの論点以外に、本人確認ガイドラインの次回改定に向けて検討・考慮すべきSP 800-63-4の変更ポイントはあるか。

② また「NISTが特にコメントを求める点」として挙げられている事項に対して、どのような留意が必要となるか。

検討の方向性

- 議論なし

参考資料2　有識者コメント一覧

有識者コメント一覧　本人確認ガイドラインの内容について
1-1. IALの見直し

①「SP 800-63-4でのIALの見直しは本人確認ガイドラインにも素直に反映できるのか。」について

- SP 800-63-4では、行政として何ができるかに着目している規格であり、ミッションを実行できるのかどうかを最重要ポイントとしている。コロナ禍において必要な人に必要な援助を届けることを実践した結果の影響もあるとのことである。災害の被害に遭った方は証明書を持っていないことも多く、精神的に追い詰められているため複雑な手続きを求められると諦めてしまうことがある。そういった点も考慮して対応を進めることを63-4は強く求めている。
- ミッションの実効性と公平性（手続きを求める場合、ある集団では簡単にできることが別の集団ではできないことがある）、個人とコミュニティに対するリスクマネジメントを意識することを打ち出している。これは行政として考えるときにとても重要だと思う。ガイドラインは民と官の間のインターフェースとしてのガイドラインなので、その辺の考え方は是非取り入れるべきだと考えている。
- 具体的にはベースラインを決めてテーラリングによって対応していくこととなる。細かいレベルについてはNISTでも検討中のためそのままガイドラインに取り込む必要はないし、置かれている状況も異なるのでこちらできちんと検討すべきである。アメリカにはマイナンバーカードに対応するようなものはなく、初期値としての状態が違うからその辺はきちんと考慮すべきである。
- IAL0の扱いを明確化するのは本ガイドラインでも参考にすべき点だと思う。公平性を担保しつつミッションを実行できるかどうかを考えるとやはりIAL0がポイントになると思う。災害時だけではなく、例えば複数回同じ人が申請をしないことを保証したい、という話であれば匿名であっても識別・特定ができればOKだと思う。
- 社会的弱者以外にTrusted Referee（当人によるプロセス実行が困難な場合に支援を行う者、日本でいうと成年後見人など）が63-3でも記載されていたが63-4でより重要な扱いとなったのが大きな変化と考えている。何も身元確認をやっていない状態を63-3ではIAL1としていたものが63-4ではIAL 0 となり、63-3でIAL2としていたものが細分化されて4段階となったことは自然な流れであると思う。これを鵜呑みにするかという点については現時点で日本のIDエビデンスとの不整合が数多く存在している。写真が重要視されているにも関わらず日本の証明書は写真付きのものがそれほど多くない。既に色々な法律（犯収法や携帯電話不正利用防止法）で認められている中に障害者手帳など写真が載っているかどうか規定されていないものが出てきているのでそういった整合性を考えると方針として参考にはするものの日本のインフラストラクチャと合わせたテーラリングをせざるを得ないというのが正直なところであると考えている。
- Validation（オーソリティティブソースやクレディブルソースに対しリファレンス番号で参照をかけにいくこと）について盛んに記載されており米国政府であれば可能なのかもしれないが、IDエビデンスを受け取るのが日本政府もしくは民間である場合にそのようなバックエンドの仕組みがどこまで整備されているかという問題があるため鵜呑みにしてはいけない。良いところは取り込めば良いと思うが、文字通り解釈してそれが一致している一致していないといった判断はしない方が良いのではないかと考えている。

有識者コメント一覧　本人確認ガイドラインの内容について
1-1. IALの見直し

（続き）

- ものすごく暴論だとは思うが、IAL0と2の2段階くらいでいいのではと思う。２の手法に関しても基本は公的個人認証、持っていない人は例外としてしまって、公的個人認証と同等レベルとなるAlternativeってなんだろうという議論で済ませるのも方法なんじゃないかと思ったりする。もちろん行政だから、という前提があるからではあるが。
- IALは、日本における身分証、authoritative sourceへの確認の可否など、日本における環境を意識する必要がある。そのため、IALについては日本版のレイヤーをしっかり作る必要があるかと思う。その場合に、800-63に沿って、または国という単位でのテーラリングとして取り組むのか、それとも独自の基準を作成したうえで、他国との調和を目指すのか、という点は分かれ道であると考える。
- 結局行政手続きにおける、という冠をつけるとほとんどのケースでは住民基本台帳上に記録されているレコードとの一致度合いをどうやって確認するか以外の論点はあまり存在しないのではないかと思う（例外が複数回申請をさせないことを保証したいIAL0のケース）。そういう意味では、基本はマイナンバーカード、持っていない人は代替手段、っていうのも考えられると思う。63-4でもテーラリングの中で合理的な代替手段を考える、という話があったはずなので同じ考え方だと思っている。
- リスク管理策ということでも組織としてのリスク管理はまぁまぁだが個人やコミュニティ、ポピュレーションに対すリスクやインパクトがどれほどのものがあるかについては意識が希薄な気がする。既に63-3に存在していた観点であり、プライバシーに対する考慮がされていることが63-3の目玉策であった。63-3の著者の一人に元FTCのプライバシーの専門家であるNaomi Lefkovitzという人がいるが、彼女が言うにはプライバシーの観点で言えばIALは低ければ低いほど良く、シビルアタック耐性があればIALをうんと下げても良いという話であった。そういう観点が現状の日本のものからは読み取れないので是非今回の改定に入れてもらいたい。
- マイナンバーカードを持っていない方もそうだが、災害時に（他の身分証も含めて）持ち出すかと言われると、結構難しいケースは出てくると思う。阪神大震災の時は、中学の周辺が盛大に火事になってそれどころではなかったようなので（実際逃げ遅れた方も）。
- ある金融機関からも、対面・目視確認の限界を感じており、全支店に身分証の真贋判定ができ、ICチップまで読める機器を導入する検討をしていると聞いた。オンラインのガイドラインなので対面の確認についてどこまで踏み込むかはあるが、重要な論点かと思う。

有識者コメント一覧　本人確認ガイドラインの内容について
1-1. IALの見直し

②「より細やかな粒度で行政手続の特性に応じた身元確認手法を選択できるように、NZの例などを参考として、更なるIALの細分化を行うべきか。」について

- アカデミアで似たようなことをやっているが、基準を複雑にすると絶対機能しないという経験がある。NZ規格のBinding Assuranceも興味深い内容ではあるが、パッケージ化して論じる方が良いだろうと考えている。NISTのIALが３＋１の4段階になる点についてはIAL1とIAL2の差は日本の事情を考えるとVerificationをきちんと行うかどうかの差しかない。Verificationが可能なIDドキュメントがどれくらいあるかというとそんなにないが、マイナンバーカードは政府がオーソリティになれるような高保証のIDドキュメントになり得る。現在マイナンバーカードに対して批判も多く存在する状況ではあるが、前に押し出してこれで行政手続きを進めるのだとした上で、そこから漏れた人をどうするのかということを真剣に考えてもらいたい。IALに限定した話ではないが、ベースラインをきちんと定めた上でテーラリングによりアシュアランスを確保するのが良い。
- （保証レベルの細分化については）行政側の見解として想定しているリスクをどこまで細分化しないといけないか、細分化しないといけない要求があるかの棚卸や現場からのヒアリングにより意見が得られているだろうか、というのが第一であると思う。そうでないと対応するIALを細分化すべきかざっくりで良いのかの議論ができないと思っている。関連して暴論ではあるものの行政手続きにおけるという冠がつく以上、申請に来た個人（自然人）で考えたときに住民基本台帳に載っている内容とどのくらい一致しているのか、存命なのか、死亡しているのか、行政手続きに閉じて言えばそれ以上の確認が必要なものはそんなにない気がする。であれば、どういう手段をもって住民基本台帳に載っている人物と目の前またはオンライン上の人物が一致しているのを確認できるのだろうか、もちろんそこでマイナンバーカードが大きな手段になるのは間違いないが、公平性や包括性の観点からマイナンバーカードを持っていない人や海外居住者に対して代替手段がどうあるべきなのかを議論していくべき。テーラリングの中で合理的な代替手段についても並行して考えていくべきである。基本はマイナンバーカードをベースとするが持っていない人は同等のレベルを持った本人確認手段が今あるものの中で何が該当するか、で議論が終えられるのではないかと。そう考えるとAALの方がより重要になってくるのではないか。

有識者コメント一覧　本人確認ガイドラインの内容について

1-1. IALの見直し

③「民間の本人確認ガイドラインにおいて細分化されたIAL（DADC・IAL）との相互運用性を、どのレベル、どの範囲で確保すべきか。」について

- 先日トラストSWGにおいて、DADCで作成した民間ガイドラインについて発表を行った。民間ガイドラインではニュージーランド規格（以下NZ規格）のBinding Assuranceを取り入れ、DADC・IALとして4段階に細分化した。レベル0を意識することとIAL2を細分化することを出発点としており、63-4との共通点も多いと考えている。民間ガイドラインは民間事業者向けとして3月にリリース予定で引き続き検討を進めており、ガイドラインともうまく平仄を合わせていきたいと考えている。
- 民間における本人確認・特定の目的と行政におけるものは異なると思うので、そこは明確にすべきだと思う。行政だとやはり住民基本台帳というDB上に存在していることを確認しないといけないというケースが民間に比較して多いと思うので、民間でやっている複数アカウントの作成を防止するために、という話とは少し重みが違うと思っている。
- IALの議論でFAL等にも関係すると思うが行政機関（独立行政法人等も含むかもしれないが）で運用されることを想定するのかそれとも例えばLINEの中の特に厳しい確認を経たもの等の民間のCSPやIdPのIDも受け入れるのかデジタル庁としてどういう方向に持っていこうとしているのか。CSPやIdPに対する統制を行うという意図が後ろに隠れているかもしれないと理解した。
- 民間のCSPを使って行政手続きをしてもらうB2GやE2Gという話と、GビズIDを使って民間の業務やサービスで利活用するG2BやG2Eという話は分けて考えないといけないと思う。

有識者コメント一覧　本人確認ガイドラインの内容について
1-1. IALの見直し

その他の議論

- 省庁ヒアリングで挙がったリスク評価については難しい。IT系でNIST RMFもにらみながらリスク分析をやりきれている例に出会ったことがないので、手段を求める傾向が強い（パッケージ）のは理解できる。自動車や医療など古くからフォールト分析をしているような業界や金融機関はセキュリティのリスク分析を行う素養のある人材がいるが、行政・自治体分野で「リスク分析」と記載して機能するのか、それを要求するガイドラインにするのか、という懸念は感じる。
- マイナンバーカードは決して100％にはならない。なぜなら紛失してしまう人がいてその場合再発行に時間を要するからである。また災害等を理由にマイナンバーカードが手元にない人に対しマイナンバーカードを所持していないので援助対象外とするといったことはあり得ない。ミッションに対するパフォーマンスというのは重要なクライテリアだと考えており、残念ながら今回用意された資料にはその観点の記述が見当たらないので是非追加してほしい。
- ミッション達成のための管理策であって管理策のための管理策であってはならない。63-4でこれほどミッションの遂行が強調されているのは63-3を参照して運用している中で管理策のための管理策となった現場が多かったからではないかと考えている。ミッションが達成されなければ管理策は無駄である。ハッキングされないことが重要なのではなく、サービスを提供した上でハッキングされないことが重要なのである。

- 相互運用性ということだと民間の話もあるが具体的な相互運用性というのもある程度考えてあげた方が良いと思われる。例えば欧州との相互運用性であるとかSingpassとの相互運用性であるとかを考える時期に来ているのではと考えている。そういった意味では国際基準や国際的な動向に配慮するのが良いのではないかなと思われる。
- IALの見直しについては相互運用性と話が逆にいくかもしれないが日本固有の風土やシステムを考慮して日本ではこれでOKなのだということをきちんと評価してほしい。63-4の直訳を適用してうまくいくはずもなく、日本での相互運用性を実現するのだということを明記すると利用者は安心するのではないか。その辺はまさしくリスク評価の出番である。デジタル庁がそのあたりの専門家とコンタクトをとることが非常に重要だと思う。

有識者コメント一覧　本人確認ガイドラインの内容について

1-2. 身元確認の対策基準の見直し

①「昨今の主要な身元確認手法やSP 800-63-4でのIALの改訂内容を踏まえ、IAL2に求める対策基準をどのように見直すべきか。」
②「現ガイドラインでは、NIST SP800-63AのRequirementsを踏まえつつ、我が国の行政機関で採用されうる手法をある程度想定した対策基準を定めた結果、現実の手法との乖離が生じてしまっている。次期改定時にはベース文書の要求事項を素直に列挙する形式とすべきか。」について

- 申請者に名前や住所を記載させる行為は昔からの名残と認識しているがリスク管理には寄与しないので考え直した方が良い。電子署名を利用するのであれば氏名を記載する必要はないはずである。申請者が申請してきた住所・氏名を公的な台帳に照らし合わせるというのはValidationの話であり問題ないが、受け取っているのが行政なのになぜ住民票を添付する必要があるのか。エストニアなどでは禁止している行為である。どこまでいっても申請書主義なのだなと思うが申請者が記載した申請書というのはVerificationもValidationもできないためほとんど意味がない。3Dセキュアなどで認証するという話であれば別だが。この辺りはきちんと見直した方が良いと思われる。
- 情報のミニマイゼーションの概念が割と希薄なので、その辺はきちんと盛り込んだ方が良いと思われる。また、代替的管理策が採用可能だということは明記するべきと考えている。
- 63-4でフローチャートがなくなったのはNISTが機械的な判断が適当でないと認識したからだと考えている。きちんとリスク（組織のリスクだけでなく、対象となる個人やコミュニティのリスク）を洗い出して検討をすべきであると。そういうところも含めて今回の改定で対応しなければいけない。民間であれば対象とする顧客でないことを理由に検討の対象外とすることも可能であると思うが、行政手続きにおいてはそういうわけにいかないと思う。
- 申請書主義というのは、本人が意思表明しなければなにもサービスしないという古来の「伝統」に則っていると思う。
- オンラインと郵送手続きは分けて考えた方が良いのではと思う。
- 書かせない行政手続きは必要なことではあると考える一方、書いていないのに色んな集めてこられて勝手に手続きが進んでしまうということに関する気持ち悪さをどのように解消していくかということも必要で、申請者が意思表明をしたということをどうやって判断するのか明文化するというのを手段と併せてガイドラインに盛り込んでもらうのが良いと感じた。
- 意思表明主義や同意主義は日本で蔓延しているが、それができるのは、それが何を意味するのかを十分に理解できる人だけだと思っている。
- （利用者にとっての省力化を含め）いかに省力化を進めるかと、自分が意識できないところで自動的に処理してくれることに対して感じる気持ち悪さの解消とをどうやって折り合いをつけていくか、何らかの答えを出さないといけない。

有識者コメント一覧　本人確認ガイドラインの内容について

1-2. 身元確認の対策基準の見直し

（続き）

- それは透明性の原則、処理の正当性の原則、処理される情報に関連性があり不足がない、これは日本の法律から全く落ちているところであるが、国際的には当然のこととして認められている。当然のこととしてプロアクティブに進めるけれどもオプトアウトできないといけない、またプロアクティブに進めることに対して害がないことを確認してからやらなきゃいけない。
- そういう意味だと現行のガイドラインはいかにして身元確認をするかという行政側の都合で書かれているところが多い。こんなことやらなくてもできるのだけれどもどういう風にやっているのか、やるべきなのか、情報開示の最小化や正当化のためのルールが明記されていないのが問題なんじゃないのかなと。
- 民間で身元確認がどうあるべきかを探求してきたので、例えばボクシングのタイトルマッチを見るのに犯収法レベルの身元確認が必要かと言われれば必要ないので、民間のサービスに身元確認について非常に高いレベルのものもあればそうでないものもある。
- しかし給付金は同じ人に重複して出してはいけない認識である。犯収法レベルの本人確認は不要であるが、その人には1回付与していて、なりすまして2回3回と申請できてはいけない、となるとシビル耐性が重要となる。身元確認ができれば受けられる行政サービスがあるというのは理解した。そういう意味だとレベルが3段階くらいあるのは良さそうである。
- ミッションが達成できているかという観点で言うと、多少重複や無駄があったとしても届けないといけない人に届くかどうかが重要になってくると思われる。
- その通りで、分かりやすい事例で言うと大地震発生時の補助金申請があるが、重複申請や本来対象外となる申請に対しても緊急性が高いという理由で目を瞑って給付しているようなケースがある。本来必要な身元確認のレベルに対し緊急性の有無により条件の緩和を認めるといった判断を併せて行う必要があると思っている。
- 緊急性が関わってくる点については承知している。普段から条件がゆるゆるだと税金払っている人からすると何なんだとなるためコンダクトリスクとしては押さえておくべきだと思う。
- フロントエンドで絞り切らなくても良い。アメリカでもトランザクションリスクをフォローアップしてみればフロントエンドは結構緩くても良いという考えがある。
- その例としてアメリカの銀行口座はよく止められるというのがある。申請すれば解除はされるが日本とは少し方針が違うのかなと思う。
- 行政サービスを受けるための前提条件があって、それに対して同意を取るというのは選択肢がなくほぼ拒否の余地がないので、行政サービスを別の手段で得る選択肢とのセットということ。一方、必須の属性というのは手段によっては変わらないように思う。ユーザービリティの議論なのか、サービス提供するうえで必要なものは必要という線引きの話は分けた方が良い。

1-2. 身元確認の対策基準の見直し

（続き）

- ガイドラインは発見的統制ではなく予防的統制なアプローチが多く趣旨としてはよくわかる。保証的な対応とか書かれている要件を外れるということもドキュメントに書いていれば良いではないとか理由があれば良いではないかという話があったので。後から取るリスクをさらって行政手続きであれば懲罰とかの手段もあると思うので視点が狭くならないように敢えて言及しておくみたいな話は行政ならではのものなのかなと思った。民間であれば行政の裏付けたる法律に記載されていれば良いのであろうが。発見的統制の観点もあって良いかなと感じた。NISTではあまり手厚くは記載されておらず少し触れられている程度であるが。
- その辺はNISTに対してもきちんと主張しなければいけないことであると思っているし、結構批判を受ける点だとは思っている。
- 予防的統制に関する記述が強いので、発見的統制でどうリスクのmitigationを図るか、という観点でNormativeな要件から外れるのを許容する、というようなことは良さそう。

有識者コメント一覧　本人確認ガイドラインの内容について

1-3. フェデレーションに関する内容の追加

①「本人確認ガイドラインの次期改定時にフェデレーションの記載を追加すべきかどうか。またその際には、NIST SP 800-63-4と同様にNon-Federated ModelとFederated Modelに分けた整理を行うべきか。」
②「将来的な認証連携のニーズや、GビズIDやマイナポータルの整備状況等を踏まえて、具体的にどのようなフェデレーションのユースケースを想定すべきか。」について

- 63-4の改定の中で自身が了解している限りではNISTが目指すものとして情報をいちいち利用者から取得するなと、どこかの省庁で情報を取得しているならそれをフェデレーション使って取得しろと主張している。フェデレーションをもっと使っていくことを考える必要があるように感じる。
- （政府の共通認証基盤を推奨することについて）良いとは思うが、Core Attributeとその他必要なAttributeはサービスごとに異なると思うので、マイナンバーカードに基づくものだけでなんとかなるかといえばならないということは予想がつく。その辺を柔軟に対応できるような形にガイドラインを記載してあげる必要があると思う。
- B2GやE2Gについて考える場合、行政側が必要としている情報が何であるかは身元確認とは少し違う議論になると思う。きちんとフェデレーションを利用して必要な属性だけ取得するような形でサービスを提供するというのは行政のあるべき一つの姿だと思う。民間や独立行政法人、私立大学も含めたアカデミアのIDというのは脇に見ながら考えてほしいと思う。
- 申請書に記載させている情報は行政側で保有していない情報であるから記載させているのだと思われる。民間がオーソリティティブソースのものもたくさんある。そういったものについては民間からフェデレーションすることも考えた方が良いと思う。
- 属性を民間から補完するという役割もそうであるがユーザーから見たときにあちらこちらにパスワードを作りたくないというのも含まれると思うので、フェデレーションについても属性を含めたID連携と単純な認証連携に閉じた世界とに分けても良いのではないかと思う。
- 賛成である。民間のオーソリティティブソースが持っている情報が必要だからあるいは利便だからというケースとCSPとして民間のIDを持っているから使えた方が良いというのは分けて考えた方が良い。後者はマイナンバーカードによる個人認証を原則としますかというところにぶつかってくるとは思うが、ユーザーがどこのCSPをメインで利用するかについては選択の余地があっても良いのではないかと思う。
- 63-4でもユーザーオプショナリティについては特に強調されているところである。
- 過去にフェデレーションに関して色々なトラブルを対処してきたが、CSPやIdPによってIDの質の違いがあって、連携をしたときに元のIdPでメンテナンスされているIDのレベルが低くて結果的に被害に遭うということが発生している。特に多いのはフェデレートされた側のポイントがIdPのポイントに紐づけられて被害に遭うといったケースである。そう考えるとフェデレーションの可能性を十二分に信じているからやっているが相手方がどういう状態であるかは大事なので少なくとも63C-3以上のことをやっていかないと問題が発生する。

有識者コメント一覧　本人確認ガイドラインの内容について
1-3. フェデレーションに関する内容の追加

（続き）

- いわゆる犯収法の依拠のパターンのあたりでフェデレーション出てくるが、単にプロトコルの話だけではない部分でビジネス的な結びつけ方の解釈に揺れがあるので、フェデレーションでIALxに代えるというのは、もう少しユースケースが明確化されると良いと思う。
- 民間のIdPは様々なレベルがあるのでB2Gが可能なものが一定以上いるとして、第三者評価を行うことでGと連携可能なIdPを絞るのではなく、民間のIdP側が宣言して（その宣言がテーラリングの一種として捉えられるかは分からないが）宣言がGのポリシーに合致するのかというのをポリシーベースで話せる、判断できるといいのかなと思う。
- 実態としてはGoogleやFacebookといったプラットフォーマーのIDがSNSのログイン時に利用されることが多いと思うが、それをどこまで信じてよいのか、あるいはプラットフォーム側で適切に管理されている場合もあるのでその辺が難しい部分だと思う。
- パフォーマンスモニタリングとかに繋がってくるところ。関係性を明示的に評価してから実施せよというのは63C-4にも記載されている。お互い相手がコントロールしているだろうと思い込んで接続し、実はそれが満たされていなかった、となると当然事故が発生する。その辺りについてドキュメントを作成して合意形成した上で進めるというのがあるべきである。逆に言うと双方がコントロールしていると負荷が大きくなってしまうのでフェデレーションオペレーターが入らないといけないといった話になってくる。
- アカデミアの場合はミッションを共通に持っているため非常に楽であるが、民間まで含めた非常に大きいフェデレーションを作成するとなると一つ一つ注意して問題点を潰していく必要がある。
- 手続きを長い目で見ると完了や不備、更新の通知等継続的なコミュニケーションが発生していくものと考えている。どのような手段で通知を受け取りたいかは当然ユーザーが決めることであり、郵送で受け取りたいなど色々あると思うが、携帯電話番号を用いたSMS等による通知は郵送と比較して費用も安く必要な期間も短くなり場所を問わず受け取ることが可能となるため良いと思っており、損保会社の人間と話をした際にも、災害により自宅に戻ることができない場合でも保険証券はないけど携帯は持っていたということがあったようでこれからのタッチポイントは携帯電話番号だといったような声も聞こえてきている。一方で携帯電話番号というのは契約解除後数か月で再利用され他の利用者の手に渡ってしまう可能性があるのでそのまま使えるかと言ったらそんなことはないが、携帯キャリアの身元確認結果を使うと手入力なしで正しい携帯電話番号か確認できるのでなかなかほかにないサービスかなと思っている。民間側の検討の中でも中間強度の身元確認手法として携帯キャリアや銀行における身元確認結果を利用するというのは議論に上がっており、検討に値するのではないかと感じた。

有識者コメント一覧　本人確認ガイドラインの内容について
2-1.「オンラインによる手法例」の見直し

①「IALとAALのレベルを「レベルA～C」とまとめて区分することを見直し、IAL、AALそれぞれに対応する手法例を独立して示すべきではないか。」
②「IALとAALのレベルに差があるケースとしては、具体的にどのようなケースが想定しうるか。」について

- IAL/AALを1軸にまとめたレベルA~Cは妥当性が下がっている。NISTに対し、日本版の解釈（レイヤー）を作ることも、メンテナンス性、マッピングの大変さなど難しくなっていると思う。A～Cは廃止した上で、IALは、先ほど書いたが日本版のレイヤーをしっかり作る必要があるかと思う。AAL/FALは技術要素が概して標準的なことも含め、NISTの要求事項を並べるシンプルな構成がありえるのではないかと考える。
- 結論から言うと（IALとAALは）分けて考えられる方が良いと思う。その理由としてはIAL 0 を利活用していくケースにおいてはAALを重視しなきゃいけないケースが出てくると思われ、IAL 0 に対しAAL 3 といったケースも発生しうる。そういう場合に対応できるような形にしていくのが順当であると思われる。現行のIALとAALを横に並べてA~Cでは少し粒度が足らないのではと想像する。ただし本当にそういうケースがあるのかといった点についてはどのくらい実際の現場から上がってきているかというところできちんと考えないといけない。ありもしないようなパターンを作ってもしょうがないのではと考えているところである。
- プライバシーの観点からすると分けないと絶対的にまずい。データミニマイゼーションとか。
- 例えば児童手当の申請など、二重申請をさせないことが目的であればその場でのIALはあまり高くなくても良く、二重申請でないことを保証するためにAALは高くないといけないといったケースが該当するのではないか。本当に子どもがいるかどうかはその場で確認する必要がありますか、という話だと思う。
- 昔からプライバシーコミュニティでよく言われる話で「ひなびた温泉の仲居さん問題」というのがあって、DVなどから逃げている人が田舎の温泉宿に逃げ込んで働いているケースがある。そこで厳格な身元確認をやるとそこから居場所が発覚して追いかけてこられるといった問題がある。保険証によりきちんと保険料が納入されていることだけ確認できればよいので、そういったケースではAALだけ高ければIALは低くても問題ないといった例もある。
- すべての手続に「ログイン」が必要なのか、と考えると良いのでは。たとえば日本入国手続のワクチン接種確認について、個人がログインをしてなにかのステータスの確認することがあるか、必要なのか。必要ないのであれば、むやみにID/パスワードを発行することはせず、書類提出をすれば良いのではないか。その場合、IALのみ、AALなし、の手続きが成立する(ちなみに、シンガポール入国の際はログインさせず、書類提出のみであった)。また、手法例のレベルAにも、2ポツ目に電子署名の例があるが、これはAALが必要ない事例とも言えるかと思う。
- 今回のNIST側の改定でもフロントローディングによったのはまずいと強く意識されている。処理全体として整合性が取れていれば良いという話になっている。ミッションをすごく強調しているのもその表れであると思う。安全に働いて生活ができるというのは住民保護のミッションなわけなので。
- マイナポイントの支給事業をやっていた際に他人のマイナンバーカードを利用して二重申請できないように振込先の口座をユニークにすることを担保していると思うのだが、検討した際のリスク、IALやAALの考え方はどのような整理がなされたものなのか。その辺りにヒントがあるような気がしている。

有識者コメント一覧　本人確認ガイドラインの内容について

2-2. 身元確認の手法例の見直し／ 2-3. 当人認証の手法例の見直し

全般

- 明らかに今回NISTが追加したのはフィッシング耐性のあるものをきちんと区別して使っていこうということである。フィッシング耐性のあるMFAとそうでないMFAには差があって、国内だと二段階認証と二要素認証で区別しているが英語ではマルチファクターオーセンティフィケーションと呼ばれる。二段階認証のためのセキュリティコードを入れてもフィッシング耐性があることにはならない。明らかにフィッシング耐性のある認証を採用しなければいくらIALのレベルを適切に判断したとしても意味がないものとなる。63-4に対するアライメントとしてもあるし、国内で起きている事象に対する対策としてもやるべきだと考える。
- 手段を書くのではなくスレット（脅威）とそれに対する管理策で書けというのをずっと言っている。今対応しなければならないスレットに全然対応していないものを二つ利用して二要素だ、二段階だ、というのは非常によろしくない。よってこの辺りはスレットベースで書いた方が良い。NIST SP 800-63は伝統的にスレットベースで記載されているしISO/IEC 29115もスレットベースであるので、それらを見習うべきである。
- 個人個人に対してサービスを提供する、というミッションということを考えると、トークンの盗難に対するクレデンシャルの漏洩という文脈よりも、フィッシング耐性がpracticalに効果がある、というのは言い切ってよいと思う。
- 現在はマイナンバーカードを使うとIALもAALも3だという議論が比較的多い状況であるが、63-4を参照するとそんなことはない状態となっている。本来どうあるべきか、というところはタスクフォース内でも議論になっており、悩んでいるところ。コメントをいただけるとありがたい。
- 必要なアトリビュートをまず決定せよと63-4にも記載されている。マイナンバーカードに入っている各種情報でコアアトリビュートが全て充足されるならいざ知らず、そうでない場合には当然単体では求められるIALのレベルは達成できない。
- 手法に寄ってしまってリスク検討を中断してしまうようなことは大変危険である。
- 利用者証明用電子証明書でのログインは実装例がほとんどないと思っていて、なぜ普及しないのかという点は一考の余地があると考えている。一方でコンビニ交付やマイナポータルのログインは利用者証明用電子証明書だけでやっている。これは国なり自治体なりがバックにあり、バックチャネルで本人を特定できるからそういう使い方なのだと思うがこれについての定義も全然なくて、利用者証明用電子証明書を使って身元確認ができていますというものが存在しますというのも全くどこにも触れられていなかったりするのでこちらも含めて整理がされるといいかなと思う。
- 利用者証明用電子証明書の件は高いレベルのIALでCSPに登録されたIDを使っているからという話だと思う。IALは必要なアトリビュートが充足されているか問題もあるので、一概にそれだけでどうのっていうのは言いにくいというのは分かるのだが。
- 利用者証明用電子証明書で署名されたシリアル番号を受け取れば住基のDBを参照して本人特定ができるという性質を使っていると思っているがIALの手段として存在していますよねという説明がどこにもないと感じている。

2-2. 身元確認の手法例の見直し／ 2-3. 当人認証の手法例の見直し

（続き）

- 今の議論は的を射ていると思っていて、署名用電子証明書を使った電子的な申請書で出されたものは正しいという考え方はコアアトリビュートの話と比べると書いてあるのに、署名していればたとえ行政がデータベースにあらかじめ身元確認をした上で保存したデータと違う差分が入っていたとしても正しいという解釈になりうるのかなというところもあって、それもちゃんとバリデートする書かれた情報が正しいのか署名用電子証明書で署名されたデータの中に適当に書いてある内容かもしれない、といったことに対する思慮が少し足りないかな。これがやりたいのは単に非否認性、あなたそう書いて送りましたよねということに対して否定できない事実を作ることであって、嘘をついて送っている可能性も当然ある。というところで建付けの整理みたいなのは必要なのだろうなというところと4PINで認証できる方のアプリケーションの活用も認証寄りに広げられると良いのかなと思いつつも、それだけだと民間側がアトリビュートを取れないという実情もあったりすると思うのでその辺りの整理がなされるとよりクリアになるのではないかと思う。
- PINなしで確認できる保険証利用とかも同じユースケースだと思うが窓口とか携帯電話のショップで本人確認をしたら、みたいなユースケースの拡大で追記されていくのはとても良い方向だと思う。
- やはり行政シナリオに閉じれば識別と認証さえできればバックチャネルで属性は取ってこられる前提でいいのであろう。不足属性がある場合は民間とのFederationを追加する、という考え方もありかと思う。
- NIST SP 800-63におけるAAL 3 でないといけないという議論の中でFIDOというよりは一つのアーキテクチャでやっているという理屈は、実態としては証明書の中に4情報が入っていて絶対に外に出てはいけないというような要求があったからであってFIDOの証明書の取り扱いはその必然性はなく実質的にTEEで扱っていたり、OSプラットフォームベンダーのクラウドを使って実質的には安全にフィッシング耐性が何よりも確保できるという良さがあったりもするので、マイナンバーカードの話はマイナンバーカードの話としてやって、認証のところは幅広の議論をするべきところがあるのではないかと思っている。
- 何度もお伝えしたがミッションオリエンテッドであるべし。ミッションの到達性、パフォーマンスが一番重要なのであって他のものというのはそれを達成するための手段に過ぎないのでそれをしっかり記載する。またプライバシーと公平性の観点が現在不足しているので追加する。手段でなくスレットで書く。以上である。
- 利用者証明用証明書（厳密にはシリアル）は、個人特定情報は含まないが、シビル攻撃耐性があるとも考えられるので、うまく活用できると良いなと思う。

有識者コメント一覧　本人確認ガイドラインの内容について

3-1. オンライン本人確認のリスク評価のあり方

①「本人確認ガイドラインにおいて、リスク評価の手順や方法をどのように規定すべきか。63-4での変更内容を素直に反映できるのか。」
②「担当職員が実践できる内容に落とし込むという観点で、より簡易的な保証レベルの判定方法は考えられないか。」について

- 現場の担当者に個別に判断してもらう要素をどこまで残すのかということについて、デジタル庁としてどう考えているかにも依存してくると思う。本質的に言うと63-3にあったフローが廃止されたことと同様のことと思われるが、モノサシを作りすぎると本質から外れてしまうというところがある反面、現場の担当者に正常に判断するためのリテラシーが備わっていることを要求してしまっている。正しく目的やリスクを理解した上で自分たちが管理策を考えてシステムを作っていくことができることを期待するのであれば、原則論を前面に押し出した記述とするべきであろう。そうでないのであれば、ある程度モノサシにはまってしまうことで柔軟性の低下や局所的には本来求められることから少し外れた結果となる可能性があることも受容して、８割救えばよいのではないかという考え方で最初にモノサシを決めてしまうという記載方針もあると思う。今回ガイドラインの改定をするにあたってどちらを基本的な考え方とするのかを示すべきと考える。
- ブレグジット以前、英国が政策を取っていた時に彼らが最初にやったことは、全てのリスク判断が現場でできるわけもないので、GDS（日本でいうところのデジタル庁、現在はDCMS）に集約した。その結果多数のシステムの重複を発見することでコスト削減にもなり、安全性の向上にもなったという事例がある。一つの事例ではあるが、個別にシステムを作らせないということはコスト削減の面からも非常に重要なことであると感じた。ちなみに、アメリカの場合は現場の力が強いので集約することは難しいため、NISTについても連邦政府向け基準であることを強調し、各部局で各自インプリするものだと強調している。
- このガイドラインがどのように行政の中で役立っていくかを考えた時に、難解であるとか曖昧であるというコメントがあるという意見はすごくよく理解ができる。社内では、63-3をもとに本質的なところに突き詰めたフローにした結果、サービスを設計する側のスキルや経験によっては良い判断ができるようになった。一方でそういったスキルやバックグラウンドがないチームがサービスを設計する際には分かりにくいという話になった。前回も議論されたようなテーラリング、本当にニーズに応えたところを考え抜いた結果としてガイドラインが活用される場合が期待される結果であると思うが、ガイドラインに書いてあるからということだけで実装が進むと本来のあるべき姿から離れてしまう可能性がある。

有識者コメント一覧　本人確認ガイドラインの内容について
3-1. オンライン本人確認のリスク評価のあり方

（続き）

- リスク分析が難しいものであるというのは誰も疑う余地がなく、経験を積んだ専門家が必要であり、それについてリソースの問題があるというのは前提条件として存在する。判定条件の基準の高・中・低の文言を詰めるとか、機密性1～3のように既に運用がうまく回っているものがもしあればそれに依拠するといったテクニックの話と、どう運用されるかをこの表を考えるときにはセットで考えないといけないと強く感じている。リスクマネジメントのコンサルティングをやっていた経験として、専門家を集めるといっても、数万人規模の会社に対してリスクマネジメントの専門家が10人程度しかいないような規模感になると、やはりある程度リスク分析を現場に委譲しなければならない。とはいえ重大なリスクを掬い上げる必要はあるため、チェックリストのようなものが運用されることが多い。そのチェックにおいて機密性が高いとか接続されているネットワークが内部向けであるということを理由にフラグが立って、専門家による確認が必要となるような形で運用を組み立てている。その観点で今回のガイドライン改定においても運用とセットで検討しなければならないと考えている。
- このガイドラインの本来のスコープでいう府省の手続ということであれば、リスク判断はデジタル庁に集約できるものは集約した方が良いと考えている。手続の類型ごとに振り分けられた必要レベルを示すぐらいまでできた方がリスク管理の面でも良いと考えているし、その後に府省ごとのシステムで管理策なり手法の選択・実装というところでデジタル庁がチェックやレビューを実施していくというのが、良いと考えている。本来のスコープからは外れるところではあるが、自治体が参照できるものが現状このガイドラインしかないということもあり、現行版ガイドラインについてどのように読み解けばいいか苦労している様子を知っている。自治体には3～4千種類の手続があると言われているが、自治体を横串で見るとほとんどが重複している。自治の観点もありバランスが難しいとは思うが、同じ種類の手続に対してそれぞれの自治体が判断し読み解いていくということになってしまうので本質を解説しにいくアプローチはなかなか難しいと考えている。この点が考慮に入ると良いなと思う。
- 民間のガイドラインにおいても同様の議論になって、民間企業へのヒアリングでもフローチャートが欲しいという意見が一定数あった。しかし民間でいうと事業内容や会社規模、ミッション、あるいはどのような方が手続をするかによって判断軸が変わってくるので、フローチャートの作成は難しいという結論になった。行政手続においては、それがデジタル庁になるかどうかは分からないが、リスク評価を集中させるのが良いと思っている。
- 誰にとってのリスクなのかを考えるのが非常に重要だと思っている。63-4ではコミュニティに対するリスクという考え方が出てきた。組織にとってのリスク、当該個人にとってのリスク、個人が属するコミュニティにとってのリスク、そういうことを明示して検討していく必要があるだろう。さらに重要なのは、個人にとってのリスク、個人が属するコミュニティにとってのリスクを許容するという判断は、組織にはできない（する権利がない）ことである。プライバシーリスクなどでは特に言われることであるが。本当はPIAの時にもあるようにマルチステークホルダーのエンゲージメントをして残存リスクを許容できるかを確認するプロセスを入れなければならない。非常に面倒ではあるが必要なことであり、特に行政機関がやる際には重要なことであると思うので、考慮してほしい。

有識者コメント一覧　本人確認ガイドラインの内容について
3-2. ガイドラインのドキュメント構成の見直し

①「ガイドラインを "Normative" と "Informative" のコンテンツに分けて整備しようとする場合に、考慮・留意すべき点はあるか。」について

- Normativeな部分とInformativeな部分とに分けることについてとてもよく理解できる反面、仕様書の中でNormativeな部分とInformativeな部分に分かれていること、これは標準化活動を行っている側からすれば当然のことではあるが、実際のガイドラインの利用者目線で考えるとそれでも不足する部分があるのではないか。つまり、考え方として重要・厳守すべきという部分に重層的に具体的な例を示すのが良いのではないかと考えている。
- 63-4は部分ごとにNormativeやInformativeと明記されているが、SHALLがあったらNormativeで、なければInformativeなことは明らかなのであまり意味がないと思っている。逆にInformativeのところは全部飛ばしていいかというとそんなことはないので、マーキングするのは逆に良くないのかなと思う。
- 分冊にするといってもこちらはInformativeに送っておいたつもりがこれはSHALLだろうと指摘された場合どうするのかということが気になる。プライバシー関係だと起きがちで、例えばISO/IEC 29184とJIS X 9252。これは経済産業省のガイドラインが基になっている。ガイドラインだったのでSHALLがなくて全てSHOULDだったのだがEDPB（European Data Protection Board）からSHALLに変更せよとの意見がたくさん寄せられSHALLだらけの文書になった。そういう事例があるためNormativeとInformativeでうまく分けられるのかという点に疑問がある。
- 国際標準化における仕様策定の中ではインターオペラビリティがとても重要となるのでNormativeかInformativeかは特に重要となる。今回は行政における本人確認のあり方に関するガイドラインであるため、国際標準化において策定される仕様書をベースに色んな実装や書物の作成がされるというようなことはなく、実際に本人確認をしていくために必要なガイドラインであるので63-4の中でここはNormativeであるとかInformativeであるということにあまりこだわりすぎなくてもいいのかなと個人的には思う。一方で、ガイドラインとして本質的なことをきちんと突き詰めてコンセンサスを取って、利用者が学びながら実行に移していくためのガイドラインの本体に対し、より多くの方が具体的にこのケースではこうするのだなという補足を別紙にすることは賛成であり、形式にとらわれすぎるよりは実を達成できるように再構成をするということであれば大賛成である。
- 相互運用性を担保していくということにおいてはNormativeの範囲が規定されていることの重要性は言わずもがなである。その中で今回のガイドラインが外部から参照される可能性がどのくらいあるかということを考慮しておくのが良いと思う。少なくとも現在OIDF-Jで検討している民間ガイドラインとの相互運用性については引き続き検討するという形で前回の結論になったと理解しており、対称性は低いと考えられあまり気にしすぎることはないとは思うが、民間から見た時にこのガイドラインに依拠するようなことが今後発生するのであれば整合性については考えておいた方が良いと思う。

有識者コメント一覧　本人確認ガイドラインの内容について

デジタル庁の役割、体制等について

デジタル庁の体制について

- プライバシーも含めたリスク管理には専門的な知識が必要なので専門家を育てる雰囲気を醸成してほしい。リスク管理は素人がやっても上手くいかない。専門家をある程度配置して、ちゃんと機能する体制をデジタル庁が整備する必要があると思う。
- 専門家という点についてコメントすると、（私の会社の）グループ会社にはセキュリティの専門家がたくさんいるが、セキュリティの観点でしか意見を言わないので実際のサービス運営や顧客が困っている時にそれを救うアドバイスが出てこないことが多い。専門性は兼ね備えながらサービスをよく理解して顧客の利益に繋がるような、かつ社会的に説明ができることに対して積み上げて判断していかなければならない、専門家の難しさがある。

リスク評価における政府内の役割分担について

- （現行ガイドラインにおいて個々のシステムでのリスク評価が難しいとされている点に関して）そういった事情であればデジタル庁発足を機会として、専門家をデジタル庁に集めて、一番難しいテーラリングなどの部分で主導してもらうのが良いと思う。

有識者コメント一覧　本人確認ガイドラインの内容について
「検討の方向性」について

- 改定の頻度で 5 年という話もあったが、実際やってみると少しずつでも良いのでタイムリーにしていった方が良いという実感を持っている。状況の変化も激しく、記載したものに対する訂正もしていくべき。マイナーなアップデートに関する頻度については検討をした方が良いのかなと。もう一つはガイドラインを作ること以上に運用していくことの難しさを実感している。改定後は府省などからこれをどう解釈すべきかといった質問を受けることになるので、ガイドラインを作った後にどう運用するかということについても良く検討するのが良いのではと感じた。
- フィッシング対策としてはフィッシング対策協議会がフィッシング対策ガイドラインを毎年出ている。総務省や金融庁、経済産業省がオブザーバーとして参加しているので、民間企業向けなので行政手続にどこまで適用できるのかというところはあるかもしれないが、参考にするのが良いのかなと思う。
- 63-4ではパフォーマンスエバリエーションを随時やってそれでフィードバックを入れなさいというのがすごく重要な点として強調されているのでそれは是非とも記載すべきではないかと思う。行政の文書というのはどこの国においてもそんなに簡単にアップデートできない。だから行政文書からスタンダードにリファーする。そしてNISTの人たちはスタンダードボディに出てくる。そういう建付けなのでそういったことも、フィッシング協議会のガイドラインをリファーするといったこともやっていいと思う。もちろんWTO的に大丈夫なちゃんとしたプロセスを持っていることが非常に重要であり、駄目なところをリファーするとWTOに指摘されてしまう。行政文書は 3 ～ 5 年に1度しかアップデートできないというのを補完してくということは考えてもいいのではないかなと。海外事例としてアメリカもブラジルもサウジアラビアとかオーストラリアもOpenID Foundationの規格を参照している。ISO/IECを参照しているところはもっと多いと思われる。レギュレーションから参照されるとそのスタンダードはレギュレーションとしての力を持つ。そういう事例はいくらでもあるので、検討しても良いかなと。
- NIST SP 800-63は色々と米国的な都合が入っていて妙に細かい。国際規格のISO/IEC 29115は本文25ページしかないがNIST SP 800-63は300ページある。ISO/IEC 29115はものすごくざっくりしているがそういうざっくり加減もそれなりに重要なのではと思う。国際規格というのは各国が議論し合って同意できたところだけが規格になっているので逆に言うとすごく煮詰まっているというか蒸留されているというか。そういうものなので是非参考にしてもらうのが良い。なお2012年に作成されて以来 1 行も変わっていない。
- 今の時代に耐えられなくなっているのではないかという議論があり、今までできたことをできなくする可能性も大いにはらんでいる状態だと思っている、非常にインパクトのあることだと思っているので、そこについて配慮し過ぎると今あるものが動くようにしたテーラリングした何かになるし、あるべき姿にするのであれば何かが落とされるというのが起きるのでその点を事前になるべく時間を空けてビジョンを示していく、あと今回の63-4の改定で入ったTrusted RefereeとApplicant Reference、要はプラスアルファの救い上げる手立てとセットで考えていかないといけないと強く考えている。

有識者コメント一覧　本人確認ガイドラインの内容について
「検討の方向性」について

（続き）

- 一つのやり方で全部をカバーしようというのは甘いと最近強く感じている。そうすると疎外される人たちが出てくる。先日インドでカンファレンスに参加した際に思ったこととしては、パスワードを使えるというのは仮定が強すぎることだということである。まさかアルファベット読めると思っていないよねと聞かれて、言われてみればその通りだなと。また、ジェンダーバイアスがかからないようにという話があって、認証の世界においてジェンダーバイアスなど存在するのだろうかと思っていたが、暗黙のうちに男性にとってやりやすい行動様式を本人確認や認証の中で要求してしまうことが多く、そうすると女性を排除することになる。あるいは都会にいる人にとってやりやすい手続を要求すると田舎にいる人を排除することになる。そういうことをきちんと考えてほしいということである。特にアジアなどでは深刻で、子育て中の女性が家を離れることが文化的にほとんど許されない。そうすると役所に来なさいとなった瞬間に彼女たちはアイデンティティがない人になってしまう。63-4に記載されているEquityというのはそういうことであり、気に留める必要がある。日本では昔から窓口の担当者がよしなにやってくれていた。それをガイドラインのように明文化するとそういった揺らぎの部分がなくなってそこで切り捨てられる人が出てくる可能性があるので、それを起こしてはいけない。それが63-4に記載されているミッションが遂行できていることを確認せよということである。その辺りは是非考慮してほしい。
- メイクや洗い物での手荒れなどの関係で、顔認証や指紋認証は女性にとっては使いにくかったりする。
- 郵便事情などは国の差が大きい。日本だと信用されているのでアクティベート済みのクレジットカードが届くが、海外だと信用されていないので「到着してから自分でアクティベート」が好まれたりする。
- 少し違う観点で、国内の状況と実際の現場での行政における本人確認に着目したときに実際にどうあるべきなのか考えた時に、今犯収法の中で本人確認に関する記載が多く存在する。そういったものをどう捉えるべきなのかという議論はこの2～3年ずっとあったと思われる。ミッション思考で考えるときにまさに厳格にその方であることを確認するというのは、JPKIにおける署名用証明書を使った本人確認であれば本当にそう言えるのか、個人的な意見としては、利用者証明用証明書でもマイナンバーカードを所持している人であるということが言えるので少なくとも厳格にその人であると判断していいのではないかとか。eKYCに関しては様々な議論があり、セルフィ型のものについては残念ながら色々なシーンでなりすましが発生しているので、そろそろ何かを示しをしていった方が良いと個人的には思っている。一方でeKYCでもICチップを使ったものは所持がセットになってくるので厳格さが増してくるという意味ではあるレベルで非常に有効に活用できるのではないか。考え方の部分に対して実装のところがある程度ついてこないと実際の現場ではうまく活用できないのではないかと思っている。さらに、プライバシーとの照らし合わせで言うと、法令の中で言われている本人確認というのはプライバシーの問題ではなくて本当にその人であるか何かしら確認しようというコンセプトになっていて、資格を持っているかどうかの確認にはなっていないと思う。免許証を所持していることだけ確認できれば運転できるという風に確認できるというような話もあり、身元確認としてある本人確認性に対して具体的に日本にどんなツールがあるのかということと、実際にプライバシーの保護というのを考え抜いたときに、まだまだ不十分なところもある中で資格を確認するという観点で、これで良いのだというやり方、それがIALでいうと 2 あたりのことかなとも思ったりするのでその辺りをもう少し深堀できるといいガイドラインになるのではないかと考えているがいかがか。

有識者コメント一覧　本人確認ガイドラインの内容について
「検討の方向性」について

（続き）

- そもそも NIST SP 800-63には上位ポリシーとしてOMB M-04-04が存在しているので。「情報のミニマイゼーション」にプライバシー対策を象徴させているのだと思うが、ミニマイゼーションだけでなくプライバシー原則全てに対する考慮が必要である。
- 欧米の政府はPIAが必須になっている。その過程の中でその情報がコレクションミニマイゼーション、あるいはその取扱いが過大でないのかを全て文書化して正当化することが求められ、当然情報がミニマイゼーションされる。63-4の中でもPIAをしなさいと書いてある。結局そういうことなので日本のガイドラインとしても国際的に平仄を合わせるのがいいのではないかなという気がしている。そうすることによって社会的にそっちの方向にもっていくという意味合いもあると思うので、是非検討してほしい。
- プライバシー原則に関しては JIS X 9250 を、PIA に関しては JIS X 9251 を参照するなどが考えられると思う。
- （対策基準の見直しについて）実際書くときにすごく難しいなと思ったのはこの項目である。例えば認証を行うときにこういう手段を使ってこのレベル以上の認証器を使って認証すべきであるというのを書いたとして、そうじゃない認証のパターンを通ってきたことを検知する仕組みを併せて入れなさいといったことをルールとして規定する話になってしまうだろうなと思っている。それを手段まで踏み込んで書くというのは現実的に不可能だと思うので、どの粒度まで踏み込んで書くかというのは少し検討しないといけない項目だと認識した。ただ方向性として、こういう視点・観点を入れていくというのは非常に重要なことだと思うので、書きぶりの部分で工夫をするのが非常に重要だと思った。
- 紙の時代の名残ということで、現行のガイドラインはオンラインの中に遠隔で郵送というのが含まれているがそこを今後も残していくのか、削除してしまうのかは分からないが、代替管理策として紙での手続というのは絶対に残ると思っている。紙の申請にもいくつかパターンがあって、役所に行って書いて出す、役所の窓口で渡されて家に持って帰って書く、はがきや封書で申請書が送られてきて書いて免許証のコピーを貼って送る、役所のHPから申請書をダウンロードする、などが存在する。そのどれかがだめだと言ってしまうとハレーションが大きいと思うので、きちんとそこを整理していく、オンラインに遠隔の要素を含むのであれば、代替策として整理するといいのではないかと思った。
- ミッションデリバリー、発見的統制という話で、前回の議論では、給付金を配布することが目的であるので9割の人に配るようにしたい、1割の邪なことを考えている人にも配ってしまうかもしれないが後から追跡して然るべき対応ができれば良いでしょうという話であったように記憶している。最近話題になったのが、マイナンバーカードの利用者証明用電子証明書の暗証番号が分かっていればコンビニで6～16桁の署名用電子証明書の暗証番号をリセットできるというのがあった。そういうのを想定しなければいけないのだろうと。利用者の明らかな失敗ではあるが、そういう人もいる。そういうのを発見的統制でどう適用するのかなというと、キオスクやコンビニで監視カメラがあってある程度の確度で記録が残されており、後で公的権力によって追うことができる、そういうことをセットで考えていくのも発見的統制なのかなと。認証におけるアカウントリカバリの身元確認ということになってきて、発見的統制について記載するのが大変だなと、記載するとしてもInformativeに書かないといけないと感じた。

有識者コメント一覧　本人確認ガイドラインの内容について
「検討の方向性」について

（続き）

- 利用者証明用証明書用の暗証番号で6～16桁の署名用電子証明書のやや複雑なPWをリセットできる問題というのは上位概念のこととかあまりきちんと整理されないまま議論が進んだように見えるので、ガイドラインを策定する過程で検討メンバーが気になる部分をリストアップしてガイドライン改定とともに実装部分についても整えていく必要があるのではと思いながら聞いていた。
- 郵送の点は、日本の事情を汲んだものにしたい。通知・配布・到達に利用するというところは一定残しつつ、郵送申請についてはできれば整理（強めに言うと妥当でないものは根絶）したい。郵送は通知・配布・到達などの片方向では（転送不要、到達確認や特定事項伝達型本人受取郵便など）引き続き使い道があると思っている。反面、もう片方向の、申請に利用するのは（発信者の身元確認も当人確認も定かではなく）曖昧だと思うところがある。アナログに近いというところで受容性が高いのも分かるが、証明書が郵送申請で取れるものもあり、本人確認レベルが実質アップグレードしてしまっているのではないかというところもあるので、整理ができるといいのではないかと思った。
- IALやAALを今後デジタル庁が中心となって決定する認識であるが、それを文教や民間が参照してデジタル庁の定めたIAL相当であるとかそういう使い方ができるものにしてもらえると助かる。行政用に使うため当然ではあるが、一般的な記載をしてもらえると文教としては助かる。それはOpenIDを含めた民間で運営されているIdPのレベルを評価する時も当てはまることだと思うので是非検討してほしい。
- IALとAALを分けるというのは大賛成。さらにフルリモートのことを考えるとクレデンシャルファーストフローでないと動かない。今のA/B/Cで、IALがある後にAALがあるのは連邦職員向けだからである。必ず事前にIALが確立している人たちなので。市民サービスで考えるとAALが先にあってそれを基にしてIALとかを加えていく方が現実的なのでそうやって分けて考えたらいいと思う。二重申請のところは色々難しい。アジア圏でもそうだしほかの地域でもそうなのだが他人になりすまして二重申請を申請するというのはよくある。そうするとそれを防ぐためにはAALだけでは不可能で、もっと言うと 4 情報を確かめてももまだ駄目で、結局バイオメトリクスという話になってしまう。写真を要求することの意味合いのひとつに、同一個人による別の人間になりすました多重登録という脅威に対応するということがある。そういった意味では書き方に少し工夫がいるかもしれない。
- あまり本質的な話ではないが、日本だとあまり起きないタイプのことを念頭に置いて書くべきか否かといった話はあるかなと思っている。身分の偽造みたいな話だとアメリカだとsyntheticクロールとか頻繁にやられているのでそこをどうするのだということが課題になると思うが日本だと移民も少なくてあまり問題にならないというのがあるので、その辺りの国情の違いをどこまで反映するかなというところはあるかなと。日本だと考慮しなくても良いようなものはいっそ書かないという選択肢もあると思う。

有識者コメント一覧　本人確認ガイドラインの内容について
「検討の方向性」について

（続き）

- 利用者証明用電子証明書をIALの手法例に掲載するのかAALの手法例に掲載するのかという素朴な疑問がある。行政においてはシリアルと住基データを突き合わせることで身元確認の手法にもなるということであれば、そうした解説が記載されていると望ましいと思う。
- 券面入力補助APが便利に使われているシーンも承知していて、コロナのワクチン接種のアプリなどはこれが使われている一方で、4情報をマイナンバーカードから取り出すという役割を持っているこの機能が身元確認になるかどうかは色々議論があると思うので、この辺りはどういう考え方でどういう方針にしようとしているか見解を教えてほしい。
- 利用者証明用電子証明書を使う点については少なくともマイナンバーカードを所持している方の一意性を確保するという役割は持てるので、単なる利用者証明ということを超えて身元確認保証レベルをあるレベルに確保できているのだという役割を果たさせることについては、すごく意味があると思う。
- 何に署名させるかを明示せずに署名させているという点は怖いなと思った。それを聞くとむしろ認証のために署名用電子証明書を使うのは禁止すべきではないかとすら思う。どういうアタックがあるのかを考えると本当に怖い。それは置いておいてISO/IEC 29115の表10-4というのがある。これはIALに当たるところではあるがThreatsとコントロールと書いている。署名用電子証明書とか券面入力補助APはコントロールの話である。Threatsを並べていってコントロールのところにマイナンバーカードをはめていって見てみると整理がよくされるのではないかなと思うので是非やってみてほしい。Impersonationというのがあってに対するコントロールとして本人確認をするにあたってどういうプロセスをしたか。窓口がちゃんとそのプロセスをフォローしているか。していなくて発行されてしまう事例もあったと思う。他の人に渡してしまうなど。これもImpersonationになってしまう。あとtamperingの話とかある。公的個人認証は電子証明書が付いているからtamperingは検出できる、券面入力補助APはどうなのであろう。そういう話が出てくると思うのでこういったものを一つ一つ見ていくといいかなと思う。
- AAL2のフィッシング耐性はRequiredで良いと思う。
- フィッシング耐性の確保に対して積極的な要請をしていくことが国民を守ることに繋がるのではないかなと考えるので、Requiredが良いと思う。最初から100点ということはないと思うが、そこに近づいていくことには意味があると思う。