本人確認ガイドラインの改定に向けた有識者会議（令和 5 年度 第 3 回）
令和 5 年 12 月 26 日（火）18:00～20:00

（出席者）

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
崎村夏彦	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）

議題（1） 開会・開催要綱説明

（挨拶・事務局説明）

- それでは本人確認ガイドラインの改定に向けた有識者会議の第 3 回を始めさせていただきます。お忙しいところをご参集いただきましてありがとうございます。
- NIST SP 800-63-4 の公開に向けた動きが本格化するという情報も入ってきており、国際的にはインターオペラビリティを確保していこうという流れになっている中、マイナンバーカード情報の紐づけ誤り問題や企業の内部犯行による情報の流出等が発生し、なかなか大変な一年となりました。また、クラウドサービスの普及によってセキュリティ問題に細やかに対応することができる環境も整いつつあり、身元確認や当人認証がどの程度正しく機能しているか等、検討すべきことが多くあると感じています。自治体のシステムの標準化も進んでいく中、本質に立ち返ってみなさまと本人確認ガイドラインの改定の検討ができることを喜ばしく思います。問題にきちんと向かい合って、世界に胸を張れるガイドラインを共に作ってまいりたいと思いますので、引続きご協力のほどよろしくお願いします。
- 本日議論いただきたい論点は 3 点ありまして、検討中の本人確認ガイドラインの 6 つの改定ポイントのうち 3 点を対象とした論点協議をお願いいたします。

議題（2） ガイドライン改定に向けた論点協議

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」について

事務局より、資料 1 に基づき改定ポイント②について現時点での検討結果を説明し、有識者による自由討議を行った。

（有識者意見）

- 前提の確認ですが、改定後の本人確認ガイドラインの対象は行政サービスに限定されるという理解で合っていますか。そうであるなら、「当該行政手続が」という表現は「対象手続が」という表現でも良いと感じました。
  - 事務局：適用範囲については現在見直し中ではありますが、基本的には現行ガイドラインと同じく、行政手続を対象としています。
- 改定ポイントそのものに対する意見ではありませんが、7 ページの用語定義に「容貌の照合」という表現がありますが、「容貌」という表現では顔以外の生体認証技術が使えなくなってしまうのではと思いました。
  - 事務局：ご指摘を踏まえて用語や表現を再検討いたします。
- 同様に、「身分証明書」というのも場合によってはセンシティブな表現となるため、再検討しても良いかもしれません。
- 身分証明書とは？といった別の議論が生まれてしまう可能性もありますね。
  - 事務局：このページの用語はあくまで本日の検討資料内の用語定義ではありますが、実際のガイドラインの用語定義においてどのような表現を用いるかについては、いただいたご意見を踏まえて再検討したいと思います。
- 改定ポイント②の項目についてですが、「2） 公平性とアクセシビリティ」と「4） ユーザビリティ」は一部の内容が重複しているようにも見受けられます。分けて記載するのであれば、それぞれに記載する内容をきちんと定義すると良いのではないでしょうか。次に「3） プライバシー」についてですが、マイナンバーカードを利用した 4 情報の取得が今後の標準的な考え方になる可能性が高い中で、どういう位置づけで記載するかについては少々工夫が必要なように思います。また、NIST SP 800-63-4 には社会保障番号についての言及がありますので、それを踏まえて日本ではどのような記載とすべきか、検討する必要があるように思いました。プライバシーと銘打つのであれば、当該業務における申請内容や関連情報が他の用途で利用されないようにしましょう、という記載の方が適当であるように思います。
- 「確認」と「検証」という言葉が用いられていますが、「確認」という言葉が適切であるのか、「検証」との使い分けはどのようにされているのか等を整理すべきではないかと思いました。
  - 事務局：用語の使い分けについて、Validation と Verification に対して別の言葉を当てる意図で使い分けていましたが、「確認」という言葉はガイドラインのタイトルにもある「本人確認」にも含まれている点を考慮できていませんでしたので、適切な表現を再検討したいと思います。
- Verification、Validation、Proof はどれも一対一で日本語に翻訳することは難しいですが、ニュアンスは異なる言葉であるため、うまく汲み取って成熟度を上げていく必要があるのかなと思います。
- NIST SP 800-63-4 でも、用語の使い分けがうまくいっていない部分がありますからね。
- 「2） 公平性とアクセシビリティ」と「4） ユーザビリティ」の内容が一部重複していることについては、公平性を全面に打ち出した上で、公平性を確保するためのユーザビリティとはこういうことである、と記載されていると分かりやすいのではないかと思いました。理念の話と実装における留意点の話のように分けるのが良いのではと思います。
- 「5） セキュリティ」に関してはその定義を記載すべきだと感じます。保証レベル 1～3 のこと、

本人確認に必要な情報をどう安全に管理するかということ、生体認証における他人受入率などの性能のこと、といったように、セキュリティという言葉だけですと色々な意味に捉えられてしまいます。

- 私も同意見です。セキュリティに関しては、セキュリティゴールを記載する必要があると思います。
- セキュリティに関しては公平性やアクセシビリティとトレードオフになると言い切っているように見えますが、そうなる場合がある、と捉えるべきではないでしょうか。
- 5)が 1)～4)の対立概念のように記載されている点は私も気になりました。
- 本人確認手法の検討において何を守るべきであるのかを明らかにして、相反する要素がある場合はどちらを優先するのか、というように、丁寧に記載すべき部分だと思います。
- NIST SP 800-63 にはセキュリティという項があって、そこでは CSP や IdP のシステムに対するセキュリティのことが記載されています。それを考慮すると現在の資料のような記載になるのも仕方ない気もしますが、ここで検討を行うことで NIST へのフィードバックにもつながるので良いと思います。本人確認手法については色々な攻撃の手法や脆弱性などの議論がありますが、そのことを言っている訳ではなさそうですので、私もセキュリティの定義を行うことについて賛成です。本人確認における脅威や手法の脆弱性については別ドキュメントにまとめることが求められるかもしれません。
- 資料においてこの 5 点が大事だと言っていて、5 点目の定義が分からないまま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と書かれているので、強い思いがあるようには感じられたのですが、それがどこにあるのかが見えにくい気がします。
- 身元確認保証レベルや当人認証保証レベルといったものがあり、それぞれの観点においてリスク評価をして本人確認手法を選択していく必要があることが、読み手に対するメッセージとして 1.3 の位置づけなどで記載されると思うのであれば、このままでもある程度意味は通じるものと思いますが、皆さんのご意見と同様に補足はした方がよいように思います。また、公平性とアクセシビリティのところで野心的だなと思って読んでいたのですが、「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」というのはかなり強い表現であるように思いました。ユニバーサルなものを採用せよと言っているように私は読み取ったのですが、過剰に解釈されるのではと少し気になりました。公平性やアクセシビリティが低くてもよいということではないのですが、99%の人をデジタルで便利にしながらも、あらかじめ残り 1%にも目を配って、現実的、かつ運用可能な救済手法を用意していこう、というのが元々の理念だったと理解しており、このドキュメントの位置付けに係わる部分だと思っています。
- 「基本的な考え方」のなかに「発見的統制」という表現がありますが、この会議内では通じても一般的には馴染みのない言葉かと思いますので、「後から見つけることが可能であるということ」が一般の読み手に通じる別の表現に置き換えるべきだと思います。
- 公平性とアクセシビリティについては、オンラインのみではなくオフラインも含めて考えてもよいのではないかと思っています。とある自治体でも、オンライン手続が可能な方向けには効率よく進めていただく方法を用意し職員のコストも節約し、その分オンライン手続きが難しい方にオフラインでの対応を手厚くサポートしたい、といった意見をいただいたことがあり、なるほどと思いました。そういった意味で基本的な考え方としても代替手段としてオフライン手法が選択肢として含まれるような記載にするのがよいと感じました。

- NIST SP 800-63-4 では Trusted Referees が強調されており、オフラインでサポートすることによってデジタルの仕組みに繋ぎ込むことを支援する役割の人が必要であると記載しています。日本において現実的なのかという問題はあるものの、そこに踏み込むか否かを検討することも有用なのではないかと思います。
- その点は日本のすごく弱いところであるので、今回の本人確認ガイドラインで踏み込むことで徐々に世の中がよくなっていくよう、踏み込むべきだと思います。
- デジタルで本人確認をやるときに求められる基本的な考え方の話と、行政手続をデジタル化するときに求められる基本的な考え方の話との両方が含まれる形で、スコープが広がっており、分量が多くなっている印象があります。
- 資料に記載いただいている内容は基本的にそのとおりだなと感じるところですが、評価して改善していくということが大事だと思っています。私自身が担当している Web サービスのユーザビリティ評価でも、作り手が想像もしないような意見が発見されることもあるので、作って終わりではなくて、利用者からフィードバックを受け取って改善していくということは重要な事項であるように思います。コストもかかる話なので簡単ではないとは思いますが。OpenID Foundation Japan による SP 800-63-4 の翻訳版に書かれていた「ユーザーが正しいことを行うことは簡単で、間違ったことを行うのは困難であり、間違ったことが起きたときに回復するのが簡単であるようにすべき」という言葉が印象に残っています。
- 少し話はずれるのですが 3)プライバシーのところで「取得情報の最小化」と「目的の通知」が記載されていますが、OECD は 8 原則、ISO は 11 原則とある中でこの 2 件だけを取り出した理由が気になりました。また、「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」と記載されていますが、もしこれが身元確認の目的なのであれば、もっと前段に記載されるべきだと考えますし、本当にこれが身元確認の目的であるかどうかという点においては疑義があるかもしれません。行政手続に利用するのであればマイナンバーがあれば問題ないという話に繋がるので。
    - 事務局：8 原則からの抜粋については事務局としても課題感を持っていますので本日のコメントを受けて再度検討したいと思います。身元確認の目的についてもご指摘のとおりと感じましたので再検討いたします。
- 1)ミッション遂行についてですが、ここに記載されている行政手続の本人確認というのは日本国民のみを対象としているのでしょうか。それとも在留外国人や渡航者も含めているのでしょうか。行政サービスの種類に応じて適切・的確な本人確認をすることが前提になっているとは思うのですが、代替手段や例外措置の考え方のところに「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」と記載があるので、こういった注釈的な内容が先行してしまうようだと後々利用者が困ってしまうかもしれないと思いました。
    - 事務局：在留外国人や渡航者も対象となり得ることを想定しています。
- 厳格な手続は使い勝手が悪いという assumption もあります。この部分についてはやりたいことをやれるようにしましょうという話だけでよい気がします。
- 皆さんトレードオフという表現に引っかかっているのだと思います。リスク評価を基にしたリスクの受容という意味合いを少し強調し過ぎている気もします。
    - 事務局：皆様からいただいたご指摘はごもっともと思われます。本日いただきましたご意見を反映し、よりよい文書にしていきたいと思います。

改定ポイント③「デジタル本人確認の枠組みを定義」について

事務局より、資料 1 に基づき改定ポイント③について現時点での検討結果を説明し、有識者による自由討議を行った。

（有識者意見）

- 「認証連携」という言葉についてですが、実際には認証を連携しているのではなくAssertionを流通しているのである、という指摘を有識者の方と議論したことがあります。本人確認ガイドラインにおいては、別の言葉を検討いただくべきだと思っています。また、NIST SP 800-63-4 の FAL では相互 TLS 認証等の足回りの話の記載が中心となっており、IAL や AAL と比較すると少し浮いているような印象を受けます。業務として連携した際に生じるリスクのような、サービス同士の連携まで視点を上げた方が良いとも考えており、月並みな表現ですが「サービス連携」のような言葉の方が適当なのではと考えています。
- 22 ページには「認証連携モデル」、「非認証連携モデル」、「Wallet モデル」と 3 つの図が掲載されていますが、ここで示されている CSP というのは内部的なものとなっています。外部の CSP を図に追加して RP・Verifier・CSP を囲む枠線を描き分ければ、1 つの図で各モデルを表現できるようになるのではないでしょうか。
- 誰の視点で図を描くかによって変わってくる話だと思っているので、読者が一番想像しやすい中央の「非認証連携モデル」を基準とした上で、外部の CSP とどのように連携していくかを追加することでまとめて表現できるのではないでしょうか。「Wallet モデル」も認証手段として Holder が登場する手法を当てはめているだけなので。
- 「Wallet モデル」の図で表現されている Verifier と「認証連携モデル」、「非認証連携モデル」の 2 つの図で表現されている Verifier は全く意味が異なっている点には注意が必要です。
- 「Wallet モデル」の図は資格を証明するための話で、本人かどうかということよりも保持しているクレデンシャルがそのサービスを受ける資格を有しているか否かという点がポイントだと考えられるので、私は他の 2 つの図と一緒にしなくても良いのではと思っています。
- NIST の関心がこのモデルの構成に集まっているのは確かなのですが、呼び方が変わっているだけで新しいトピックが追加されているものではないと思っています。
    - 事務局：今後公開が予定されている SP 800-63-4 の Second Public Draft でどのような記載がされるかという点も参考にしつつ、モデルの図自体を説明の対象にすることについては議論が必要だと思っています。また、実際にモデルの概念を整理する際に「認証連携モデル」、「非認証連携モデル」を別々の図として表現するか、役割が変化することについての説明を加えつつ 1 つの図にまとめてしまうのか、は悩ましい事項だと思っています。
- 「認証連携」とは呼ばない方がいいという意見が多数派だとしても、連携の話自体は入れた方がいいと感じます。私の所属先で社内用のデジタルアイデンティティガイドラインを作成する際にも、この連携をどう扱うかは有識者の方にご意見をいただきました。自システムが保持している ID や IdP としての身元確認保証レベル・当人認証保証レベルと連携先システムの各保証レベルを軸として、発生しうる脅威はマトリクス形式で整理することができるので、連携に関する議論は避けない方が良いと思います。

- 「非認証連携モデル」は 1 つのエンティティの中で完結しているので各オペレーションについて Verify できますが、「認証連携モデル」のように複数のエンティティになる場合はそれぞれのエンティティ間で相手がどのようなオペレーションをしているかを Verify できなくなってしまいます。そこにトラストの要素が出てくるので、エンティティを分割できるようにしておく、また分割したときにどのようなリスクが生じるかというのを論じておくことは非常に重要だと思います。
- 今回のガイドラインにおいて本人確認の主体は常に行政になるのでしょうか。
  - 事務局：必ずしもそうではない認識です。民間から属性を受け取る C2G のケースは今回の改定においては明示的に意識しないといけないと思っています。
- 民間から属性を受け取るケースが存在することはそのとおりだと思いますが、属性は受け取るものの本人確認をするのはあくまで行政側が行うのか、それとも完全に依拠をするのかで異なるため、その切れ目を作らないとこのモデルは書けないと考えています。「認証連携モデル」を有効にするのであれば、例えばある事業者の本人確認結果を盲目的に信用することとし、RP だけを行政側で用意することになると思いますが、それが行政において許容されるのかという点については若干疑問が残ります。そうではなく、事業者 A から提供される属性をメタデータとして受け取ることによって本人確認手続に対する補助属性として扱うのが本来の形であると私は認識していたのですが、いかがでしょうか。
  - その場合は G2G のユースケースが非常によく当てはまると思います。つまり府省を跨る連携の場合はどちらの府省も RP 側にも IdP 側にもなり得ると考えています。
- マイナンバーカードを使って公的個人認証を行うケースは「認証連携モデル」に該当すると思います。また NIST が記載している認証の連携においては、民間の CSP を受け入れることを実現しようとしていました。
- 22 ページに「政府の各種認証基盤を活用し」と書かれているので、民間はあまりターゲットに入っていないのかなと思っていました。
- テクノロジーとしてのフェデレーションの話と、フェデレーテッドなんだけど行政の認証基盤、とういう話は少し違うのかなと思っています。
- Federal PKI などでは、例えば航空機メーカーで機密情報を扱う職員を PIV-I で認証して受け入れるというのはごく普通のことになっています。日本でもそうしたことも考えていかなければいけないのではないでしょうか。そうした展開を考えると、IdP の部分は必ずしも政府でないというケースも想定しておくべきだと思います。
- 属性情報として民間がソースになるところは結構あると思います。
- 令和 6 年または 7 年に改定版ガイドラインを公開する予定であることを踏まえて「Wallet モデル」の話を含め、どういう可能性まで考慮しておくかという問題だと思っています。
  - 事務局：はい。公開から 5 年程度は利用されるガイドラインということは意識して検討を進めたいと考えています。
- 住民基本台帳がある日本国民だけに限定せず、外国人や海外からの渡航者を対象にすることを考えた場合には色々な連携を無視できなくなると思います。「Wallet モデル」については一旦置いておくとしても、「認証連携モデル」か「非認証連携モデル」か、ということについての分解能は持っておいて、それに当てはめていくという考え方は良いと思います。
- 分解してからエンティティを囲む枠線を自由に描けるようにしておいてあげるというのが重要

なのだと思います。

- この手の話をする際、専門家はきれいに整理された図を用いて説明する傾向がありますが、読み手にとって重要なのは、利用する際に馴染みのあるものをイメージしてマッピングできるかどうかだと思っています。実際のシステム開発では内部の IdP を利用して完結させる「非認証連携モデル」になるケースが大多数を占めますが、外部の IdP を利用してエンティティを明示的に分ける方法も存在するのだということを認識してもらうために、「認証連携モデル」の図があるのだと思っています。ただ、RP や IdP が誰であるかによってユースケースが変わるということは書いておいた方が良いと思います。大半の読者は、デジタル庁が IdP を用意し府省側のサービスが公的個人認証で認証結果を受け取る、というところまでしか想像しないと思うので、スコープとして想定しているのであれば、このモデルでは役割が変わることによりこのようなパターンが発生します、ということを書かないとおそらく理解されることはないと思います。
- 「認証連携モデル」を推奨することが妥当かという質問について、そのねらいは何になるのでしょうか。典型的なユースケースがセットになっていない状態で推奨されると読み手は困惑してしまうと思います。事務局のねらいを確認した上で議論することが適当であると感じました。
    - 事務局：元々のねらいは認証機構の乱立を回避することです。もちろん既存の認証機構で過不足が生じるケースは出現してくると思われるので、先ほどの公平性についての議論も踏まえ、この認証機構に限定するというところまでは書ききらないとは思っています。一方で、認証機構を独自に立ち上げるのは大変なので「認証連携モデル」を推奨することが、今回のガイドラインの記載として望まれている認識です。
- その考えは妥当だと思います。周囲を見渡して要件を満たす既存の IdP が存在するかどうかを確認してください、ということですよね。
    - 事務局：はい。中央省庁で利用可能な IdP については参考資料等で紹介することになるだろうと思っています。
- マイナンバーカード用の公的個人認証アプリのように、具体的な候補が記載される前提であればその方針で良いと思います。
- IdP を量産してほしくないというメッセージは非常によく分かるのですが、そうすると文書全体の記載の配分も変わってくるような気がしています。RP としてどの IdP は受け入れ可能であるかといった実践的な内容が必要になるので、身元確認保証レベルや当人認証保証レベルよりも認証連携保証レベルについての記載が多くなると感じたのですが、事務局でもそのように考えているのでしょうか。
    - 事務局：その点については今まさに悩んでいるところであり、タイの例のように、覚悟を持って一部の説明を省略した結果分かりやすくなった例もある、ということを踏まえて、我々がどこにフォーカスし、それ以外のところを削ぎ落していくのかということについて検討する必要は感じています。皆さんには認識いただいていると思うのですが、現行ガイドラインでは身元確認保証レベルと当人認証保証レベルの分離すらされておらず、併せてレベル A、B、C として扱っています。身元確認保証レベルと当人認証保証レベルについての理解が前提となって認証連携保証レベルの話になると考えているので、一定量の記述は必要なのかなと思っています。
- 身元確認保証レベルや当人認証保証レベルについての検討の大変さを冒頭で感じてもらっ

て最後に FAL に言及して、それを誰かにお願いできるという形になるわけですね。

- そういう意味では身元確認保証レベルと当人認証保証レベルをきちんと整理しましょう、その上で RP と IdP を分離してもいいよ、というような流れで書けば解決するのではないかと思いました。
- そうですね、身元確認保証レベルと当人認証保証レベルを一生懸命考えて作ったものがあって、それを使いまわすモデルがありますよ、という見方ですね。
- 少しずれるかもしれませんが、民間の IdP の参加を認めることになると、政府は何らかの形でその IdP の認定をしなければならないと思うのですが、その準備は進んでいるのでしょうか。
  - 事務局：現時点で確定した情報としてお伝えできるものはないですが検討はしており、民間事業者向けの本人確認ガイドラインとの平仄も考えないといけないと思っています。外部向けの整合についてはガイドライン的に考えていく必要があるというのは強く意識しています。
  - 事務局：モデルを考える上で多くのご示唆をいただけましたので、今後の検討の中でご意見を反映させていただけたらと思います。また、いくつか追加で検討が必要な事項も出てきたと思いますので、次年度になる可能性はあるものの、その点についても検討させていただくようにいたします。

<u>改定ポイント④「保証レベルと対策基準の一部を見直し」について</u>

事務局より、資料 1 に基づき改定ポイント④について現時点での検討結果を説明し、有識者による自由討議を行った。

（有識者意見）

- 身元確認保証レベルの細分化は RP がどこまで細分化した情報が欲しいかによって対応が変わってくると思っているのですが、細分化したレベルがないと困るという行政手続はどのくらいあるのでしょうか。
  - 事務局：どちらかというと、今回の再分類でレベル 2 に色々な手続が集中してしまい、レベル 2 だけでは整理が難しい要素が入り過ぎたので、細分化しようという意向が先に立っている認識です。RP の要望は行政手続の種類に合わせて整理すればよいという認識で検討を進めていました。
- なるほど。そうすると行政手続の多くが 2C は適当ではないということになると、そのレベルが対象外になる可能性もあるわけですね。
  - 事務局：理論上は、そうなる場合もあると思います。
- そういうこととしてどこに評価を引けばいいかということでやっているということですね。
  - 事務局：おっしゃるとおりです。
- 2A・2B と 2C の差は、貸し借りアタックに対応するか、そういう脅威を考えるか、ということですよね。また、2A と 2D の差は機械が検証するか人による目検かというものでしょうか。
  - 事務局：はい、そのように考えています。
- 32 ページに、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、とありますが、これを認めることになると、ブートストラップができないので身元確認保証レベル 3 のクレデンシャルを発行できなくなってしまうと思います。

- そういう意味では公平性の話をどうやって入れるかという観点が必要になってくると思います。ブートストラップの話はその典型かもしれませんが、何も持っていない、アクセスできない人に対しても手続自体は平等に提供しなければいけないことを考えると、代替手段がないものを作ってはいけないのではないでしょうか。
- 以前民間で既存の認証手法について分類をした際に、「本人確認書類のコピーを郵送する」「撮影済みの画像をアップロードする」といった手法は下位に分類しました。33 ページの表の中だと 2E よりも下位に位置することになると思うのですが、既存の手法を一部認めず切り捨てることも視野に入れてこの領域の分類を検討しているという理解で合っているでしょうか。
  - 事務局：その点は検討中でして、レベル 1 の登録コードの扱いと比較しながら検討が必要だと認識していますが、今回の細分化の案には考慮できていないのが現状です。
- 郵送による手法の強度は当然ながら対面よりは落ちますので、「数年後にこの手法は廃止する」といったような強い意志があるなら、そうした内容が反映されること自体は良いと思います。
- 住民基本台帳に登録されている住所に対してプレプリントした申込書を郵送し、署名・捺印・免許証コピーの貼付等を行って返送する、といったオペレーションが現在も多く残っています。今回の改定版ガイドラインで原則は対面またはオンラインとし、郵送を代替手段として記載する、ということであれば問題ないと思うのですが、それを一切認めないとするのはまだ少し厳しいのではないかなと思っています。本人限定受取郵便は追加費用が発生するため、郵送する数によってはあまり現実的でないというケースもあるかもしれませんが、対面で確認しているということでレベル 2 に該当するか否かという議論もあるのではないかと感じています。
- 誤解があるかもしれないので確認しておきたいのですが、SP800-63-4A で登録コードが身元確認保証レベル 1 であるという件はいわゆる居住地の意味の住所だけに限らない電話番号やメールアドレスも含むアドレスに登録コードを送付してアドレスの検証をすることができるということを示しています。アドレスの検証に使うことができないだけで、レベル 2 やレベル 3 でも登録コードを利用すること自体はでき、中断した Identity Proofing のセッションを再開するためのつなぎとして登録コードを使うことは可能だと言っています。日本における本人限定受取郵便は住所の Verification をするために行うのではなく、郵便局に出頭して対面で本人確認をせよという話であり、登録コードを Identity Proofing のセッション再開のために使っている話となります。なので、単にレベル 1 に登録コードを利用した身元確認と書いてしまうと、おそらく読み手の大半は誤解してしまうと思います。本人限定受取郵便という基本的には対面の写真付き証明書をチェックする別経路に繋ぎ込むために登録コードを使っているという話なので、そこを整理して認識しておくと迷いがなくなるのかなと思います。
- 本人限定受取郵便はここでいうところの 2D ですよね。
- はい、レベル 2 のものとして使って良いのだと思います。
- 携帯不正利用防止法で定めている中での郵送による本人確認手段である、特定事項伝達型本人限定受取郵便、それだったら良いと思います。
- 確か犯罪収益移転防止法とほぼ一緒で、特定事項伝達型だと登録コードだけ届いて指定された場所に行って見せないといけないと記憶しています。カード会社によっては本人確認書類を先にアップロードして簡易書留で転送不要で送ってくるながれなのですが、それは本人確認書類をアップロード済みなので住所に到達できれば最後の受取という一連のプロセスをつなぐために登録コードを利用しているという解釈だと思っているので、注意が必要です。た

だ、本人確認書類をアップロードするときに画像でいいのかという話を今度は議論していく必要があるのだと思います。

- 事務局：登録コードの利用については改めて事実を確認しておくようにいたします。また、郵送による身元確認については登録コードとは混同せず、対面の身元確認のどれに相当するのか、ということを整理する必要があると認識しました。

- マトリクスの軸の話についてですが、容貌の照合を実施したか否かで対面とリモートを分けていますが、本来はプレゼンテーションアタックへの耐性をどのくらい保持しているかの話だと思っています。Supervised Remote は Supervisor の存在だけでなく環境面での条件も指定がされていますが、その理由はプレゼンテーションアタック耐性の確保のためです。なので、対面かリモートかで分けるのはあまりよくない気がします。同様にこのレベル 2B と 2C は貸し借りへの耐性があるか否かで分けられる話だと思います。
- 海外だとクレジットカードは受取後にアクティベーションが必要なケースが一般的ですが、日本では一部の例外を除き送付されたカードはすぐに利用可能な状態です。その理由は郵便局に対する信頼度が高いからです。その信頼度が今後下がってしまう可能性まで考慮するならば、追加の検討が必要になってくると思います。
- 要素が揃っていれば順番が逆になっても OK とみなす傾向があると感じていて、簡易書留で送られてきたクレジットカードがすぐに利用可能となっているというのは前提として身元確認済みだから、順番が変わる場合はオペレーションも変化して受取後にオンライン等での身元確認が終わると利用可能となる、ということだと理解しています。その辺は注意深く検討が必要ですが、結構難しい部分だと感じています。
- それは郵便物を詐取する攻撃に対する耐性ということですか。
- 荷受け詐欺とかそういったものですね。
- 日本ではほとんどないと思いますが、可能性としては郵便物が捨てられてしまうなど、郵送事情がよろしくない地域というのも存在します。
- 33 ページの図について私はとてもよく考え抜かれているなと思っています。IC チップを確認することの重要性はものすごく実感しており、2A、2B、2C の後ろに 2D、2E があるのは、私の感覚とはとてもよく合っています。一方、冒頭にコメントのあったブートストラップの問題はそうだろうなと思っています。
- ブートストラップ問題は、例えばマイナンバーカードであれば、カードを落したときに誰でもひっかかってしまいますね。
- マイナンバーカード自体をなくしていても、マイナンバーカードの所持を前提として発行された別の物があればそれを根拠にアカウントリカバリが実施できる、といったように、いろいろやり方はあると思います。
- この図では 2B と 2D のような斜めに位置する関係についてはその強弱をあえて明示していないと思いますが、概ねとしては ABCDE の順に認証強度が高い印象を受けました。
    - 事務局：細分化したレベル 2 の表現については、強度が高い方を A にするのか、それとも逆にするのかという点について事務局内で議論した結果、暫定的にこのように整理することとなりました。
- 私も、認証強度は ABCDE の順となっている印象を受けました。金融機関でも窓口に IC チップを読み取る機器を導入するという話も聞きますので、民間もそういう流れになってきている

のかな、と私も実感しているところです。

- 31 ページの表の 3 段目のレベル 3 のところについて、デジタル署名の検証はすごく良いと思っており IC チップも是非というところではあるのですが、一方で運転免許証については住所変更をしたときに IC チップ内のデジタル署名が更新されないという話がありまして、制度やカード自体が変える必要のある話ではあるものの、現状デジタル署名を確実に使えるものはマイナンバーカードくらいしか存在しないはずです。ということをお伝えしておきたいと思います。
- 4 段目のレベル 1 のところですが、メールアドレスに登録コードを送って確認することはチャネルを確立するという点ではいいと思うのですが、メールアドレスがエビデンスに書かれていない状態でそこに送って確認しても、それが支配下にあるかどうかが分からないのではと思います。エビデンスに書かれている住所への郵送と書かれていないメールアドレスへの送信とでは品質が変わってくるのではないかと思います。
- 日本においてどうするかは別途検討が必要ですが、NIST IAL1 で言っているのは申請者が申告した住所を Verification に使用して良いということなので、本当にその住所に住んでいるかは別として、届いた荷物を受け取れるところまでは確認する、だからレベル 1 なのかなと感じていて、レベル 2 とレベル 3 はそれを許さないので単純に申告された住所は検証には使わない、あくまで IC チップに書かれている住所の署名の検証によってのみ Validate することになるので、レベル 2 とレベル 3 の場合登録コードは Proofing セッションのつながりを別経路に移すためだけに使えるのかなと思いました。そんなに違和感はなく、レベル 2 やレベル 3 で申告された住所が検証に使えるようだと少し雑に感じますのでその感覚はほぼ一緒なのかなと思います。
- 33 ページの容貌照合なしの対面確認というのはどのようなケースを想定されているのでしょうか。容貌照合なしの Verify を認めるのであれば、Evidence を顔写真付きの身分証明書に限る必要はないのでは。
    - 事務局：SP 800-63-4 の説明としては、容貌照合なく Verify できるレベルとして IAL1 を新設するという記述がありまして、これに相当する本人確認を想定しています。また、Evidence の部分はご指摘のとおり不整合が起きている可能性がありますので、確認させていただくようにします。
- 33 ページの表は、特に 2 行目が顕著ですが、全体的に選択肢が少ないと感じます。日本の現状にフィットするのかという点については確認が必要ではないでしょうか。米国民は写真付きの本人確認書類をみんなそんなに持っているのかなと疑問に思い調べてみると、SP 800-63-3 のインプリメンテーションガイドという詳細が記されている文書がありまして、その中に米国民は大体こういう身元確認用のドキュメントを持っていて Superior はこれ、Strong はこれ、というのが書かれています。NIST のガイドラインは政府職員向けなので 1 枚目は PIV カードが前提になっていまして、その辺りの差は注意が必要であると感じました。
    - 事務局：ありがとうございます。身元確認書類の種類や点数については現在検討中でして、まだ脅威ベースで整理できてないところもありますので、いただいたコメントを踏まえ再検討するようにいたします。
- 実際のリストを見ていただければわかると思いますが、持っていない方も結構いらっしゃるのではという感覚を持っています。
- 顔認証マイナンバーカードを新しいパターンとして考える必要があると思っていまして、電子

証明書を所持しないということになっている一方、券面事項入力補助などの IC チップの中の情報はあると思いますので、これがレベル 2 またはレベル 3 で使用可能なのか否かは検討が必要だと感じました。

- 事務局：顔認証マイナンバーカードについては今後に仕様を確認しながらどこに当てはまるかを整理しておくようにします。

- 参考情報ですが、12 月 8 日に日本銀行が開催した CBDC に関するフォーラムで、民間企業内でのデジタルアイデンティティガイドラインについての発表がされています。保証レベルの考え方はいろいろあると思うのですが、参考になるかと思いご紹介しました。
  - 事務局：ありがとうございます、参考とさせていただきます。

閉会・次回案内

（事務局）

- 本日議論させていただきたい事項は以上となります。次回は令和 6 年 1 月 30 日（火）を予定しており、改定ポイントのうち本日議論いただいていないものの協議を予定しております。本日は長時間にわたるご参加、加えて様々なご意見をいただき誠にありがとうございました。

（了）