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 2 回）
令和 6 年 11 月 5 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	国立情報学研究所・教授（トラスト・デジタル ID 基盤研究開発センター センター長）
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
満塩尚史	順天堂大学 健康データサイエンス学部 准教授
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）議題の一部変更について

事務局より、資料 1 に基づき議題予定の一部変更についての説明を行った。

議題（2）ガイドライン改定に向けた論点協議

「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」

事務局より、資料 2 P2～16 に基づき論点 2 についての説明を行い、有識者による自由討議を行った。

（有識者意見）

- 主に資料 2 に関してのコメントとなります。資料 2 P8 に関して、身元保証レベル 1 においてどういう本人確認書類を使用できるようにするのかといった議論になるかと思います。NIST SP 800 63-4 への改定で IAL0 がなくなったことで、昨年度 IAL0 に相当していた本人確認書類も IAL1 として使用できるのではないかといった議論がありました。少なくとも、匿名に近いが申請者と受取者が同一である、ということの識別・確認ができれば良い。IAL で担保できない分 AAL で申請者と受取者の連続性を担保できればよいという手続きもあるのではないだろうかといった議論を昨年度実施していたのではないかと思います。身元確認保証レベル 1 におい

て使用できる本人確認書類には、少し緩めのものを入れてもよいのではないでしょうかといった意見になります。次のページでも影響してくるのではないかと考えています。

- 資料 2 P10 に記載がある「在留カード」は、パスポートと同じレベルでよいのかといった議論が必要ではないかと考えています。パスポートには、住所の記載がないことはすでに確認していますが、在留カードにおいても住所の記載はされているのかといった点が懸念事項となっています。
- 資料 2 P10 に記載がある「FAIR-a/c」と「FAIR-b」の間には、少しレベルの差を感じました。FAIR-bは発行元の特定と確認が難しいのではないかと考えています。特に民間企業の社員証や学生証、特に海外の社員証などは、窓口を使用して確認ができるのだろうかというところが疑問であるように感じています。FAIR-c は、公共料金であり、発行元は限定されるため、可能だと考えられます。
- 資料 2 P12 に記載がある、FAIR-a と FAIR-b（顔写真付きの社員証・学生証など）を組み合わせた容貌比較も可とするのは問題ないと考えますが、2 つの書類が同じ人を指しているかの、確認をすることができるかどうかという疑問があるように感じました。紐づけをするには、氏名を確認するしかなく、行政に届けている氏名と会社に届け出ている氏名が必ずしも一致するとは限らず、組み合わせをすること自体に異論はありませんが、実際の運用を考慮する必要があると感じました。
- 資料 2 P24 に記載があるリード文の意図が良くわかりませんでした。かっこの中で例が「OIDC における Implicit Flow や SAML における artifact binding profile の採用要否を検討する等」と書かれていますが、これがインジェクション攻撃を受けやすい例として書かれているのであれば、もしかしたら誤解があるのかもという疑問を感じました。（注：指摘を受けて、公開資料では修正済）
- レベル1は「連続性・同一性の確認」とし、レベル2は「到達性の確認」、レベル3は「本人性の確認」のように、分類してしまった方が簡単な気がしてきました。
- 現状の保証レベル 1/2/3 の目標があまり明確ではなく、別の委員がおっしゃっていたように、レベル 1/2/3 でそれぞれ連続性・同一性の確認、到達性の確認、本人性の確認といったような大きな分け方の方がわかりやすいのではないかと考えます。また、何の脅威に対して耐性があるかといった観点での、資料 2 P13 記載のような整理の方が良いのではないかと考えています。
- また、脅威は陳腐化せず、手法が陳腐化していくと思います。脅威に関しては、現状それが受け入れ可能なレベルのリスクであるかどうかといったことで変化していくのではないかと考えます。
- 陳腐化しないようにというのは重要な点ではあると考えます。対策基準を中心に記載していくと、脅威ベースの記載と Evidence に対しての記載が組み合わさって記載されることとなり、混乱するのではないかと感じています。Evidence の区分については、公的な発行機関の書類に関しては、分類したほうが良いのではないかと考えています。公表するかしないかは置い

ておき、検討段階では脅威とマッピングすることは重要ではあると考えますが、最終的に Evidence は分類した形で提示したほうが良いのではないかと感じました。

- 別の委員もおっしゃっていましたが、FAIR-a と FAIR-b のエビデンスの性質に大きな差があるように感じます。その結果 FAIR-a のみを用いた確認と、FAIR-a と FAIR-b を組み合せた確認の間で有意な差があるように見えないと思います。今後、G ビズ ID や法人の Verification がデジタルな証明書で発行できるようになれば、このようなことを考えても良いのではないかと考えます。私は、現状 FAIR-b のようなものをこのガイドラインの中で記載しなくてもよいのではないかと感じています。一方で FAIR-c は、住所を含むと記載をしていることで現実世界との結びつきがあることを大切にしており、補助ドキュメントとして、他の本人確認書類と一緒に出すことに意味が見いだせるという点で重要なのではないかと考えます。
- テーラリングに含められるかもしれませんが、脅威の耐性は、本来は〇×ではなく Mitigation の程度で示されるべきではないでしょうか。
- 学生証は、適切に制御すれば、日本版 STRONG に該当する可能性があると考えています。
- 学生証は、検証者の立場としてどうやったら検証できるのかというのが問題です。
- 実務上、発行者である学校は有限ではありますが、各校が独自フォーマットなので真偽の判別がつきません。身元確認というよりは資格の確認の用途、かつクリティカルでないミッションで用いることが限界ではないかと感じており、例えば、自治体の施設予約で、体育館の学生利用料金の適用に利用する等が想定できます。Authoritative Source に対して問い合わせて Validation できるのであれば、本人確認の Evidence にはなり得るとも考えます。
- 資料 2 P14 の「❷ 本人確認書類の紛失時を想定した代替パターン」に関してですが、救済措置としての代替パターンは必要だと考えます。一方で、ガイドラインでパターンを示すと、攻撃者がそこを狙ってくる可能性も十分にあり得るのではないかと考えています。どこの範囲までであれば例外措置を許容するのか、例外措置があることによる具体的なリスクも記載をすべきではないかと感じています。
- 別の委員のおっしゃっていたとおり、最終的には、本人確認書類が分類され、わかりやすいラベルが張り付けられている状態が、利用者にとってはメリットが大きいと思います。例えば資料 2 P10 のように、本人確認書類の例が記載されていることに対しては賛成です。しかし、ガイドラインの中に記載されているのではなく、法律の施行規則のような形で、ガイドラインの外に取り出してある方が、脅威が顕在化した場合に、記載してある本人確認書類に追記等ができ、より望ましいのではないかと考えます。
- 本人確認書類の例を別冊化することは検討中であります。
- 本人確認書類を分類すると、詳細な条件に差が生まれ、脆弱性を突かれることも出てくると考えられますが、ガイドライン本文の記載を変更する大変さを考慮すると、別冊に記載することで良いのではないかと考えます。
- 今回の第 2 回有識者会議は身元確認がメインのアジェンダだと思いますが、身元確認をするというのはどういったことなのか、ということを改めて考えさせられました。身元を確認する

ということと、資格を確認することは明確に区別するべきだと考えています。身元確認、あるいは本人確認というのは「本当に実在する方なのかどうか」ということであり、脅威は、なりすましになると考えられます。かねてから民間では携帯電話不正利用防止法に基づく店頭での確認や金融サービスに求められる本人確認が実施されているものと思います。しかし、なりすましをされてはならないといった認識から一定レベルの対策を行ってきたにもかかわらず、攻撃手法は高度化しており、その結果、ある時には十分であると信じられていた対策が、現在では十分ではなくなったケースもあります。本人確認ガイドラインに書かれるべき本質的なこととして、本人確認とは何かという意味でいえば、なりすまされないことであり、脅威はなりすましであるといった記載をするべきだと考えます。また、どこまでの対策を実施するべきかといったことに関して言えば、ある時期は住民票をもっていれば問題なかった手続きも現在ではそうではなくなっているということなので、日本版 SUPERIOR か日本版 STRONG かといった件に加え、多くの場面でなりすましが発生しているといった脅威については、行政機関・民間企業を問わず受け止めるべきものとし、煩雑さなどは発生するにせよ、なりすましを防ぐにはどのようにするべきかというのを定める必要があると考えています。資料 2 P8 をどのように埋めるかといった件に関しては、保証レベル 3/2 においては、容貌の確認をするのは非常に重要であると考えており、容貌の確認を実施するのが難しいのであれば、その手続きは低いレベルに位置付けざるを得ないのではないかと考えます。容貌の確認の有無に加え、複製や偽造のしやすさ等から適切に説明できるようなレベルを設定すべきだろうと考えます。6 月に発表された「国民を詐欺から守るための総合対策」にも記載があるように、本人確認の際には、容貌の確認や IC チップの読み取りを確実に実施することが重要であると思います。容貌の確認等は、あくまでも手法の話ではありますが、現実的で実行可能ななりすましを防ぐ方法であることを示す必要があると考えます。それよりも下のレベルの手続きに関しては、目的が、本人確認なのか、資格の確認なのかを分けて考える必要があります。来た人が申請者と同一であることさえ分かればよい場合では、身元確認ではなく、当人認証でよい可能性があるのではないかと考えます。また、資格の確認を目的としている場合、現在はマイナンバーカード単体では確認できないものであり、学位等の資格を証明する書類と合わせて確認を行っていく必要があると考えます。

- 資料 2 P14 の「❸ガイドラインにおける本人確認書類の区分定義の必要性について」に、実際のガイドラインでは「日本版 SUPERIOR」のような区分は定義せず、前頁のように保証レベルごとの対策基準を直接定義する方が、基準が明確となり理解もしやすくなるのではないか。」と記載がありますが、全て網羅する必要はありませんが、具体的な本人確認書類名を記載したほうが、読み手側としては理解しやすいと思います。また、物理的な検証はどこまで求めるかというところは検討する必要があると考えます。資料 2 P12 では、日本版 FAIR-a と日本版 FAIR-b で Validation の際に物理的な検証が必要であると記載してありますが、日本版 FAIR-c で発行主体が電力会社等であった場合は物理的な検証がある程度可能ですが、日本版 FAIR-b の本人確認書類の物理的な検証は難しいのではないかと考えています。特

にオンラインでの確認を行う際や、本人確認書類の写真やコピーが提出される場合には、物理的な検証がほぼ不可能となります。身元確認保証レベル1で求める本人確認書類の基準をどこまで、緩めるか、あるいは強めるかといった検討はとても重要になると考えます。

- セキュリティだから厳格にしなければならないというわけではないですが、第三者が本人を装ってなりすました結果、本来の利用者が使えなくなることに加え、限定的ながら、本来の利用者の本人確認情報等を利用し、不正送金に使われることも想定できます。民間の事業者によっては、ビジネスの脅威のレベルがそこまでではないという場合には、緩和してもよいかもしれませんが、民間企業においても、本人確認において、相当の厳格性が必要であることを強く感じています。
- 同様の意見を持っています。先ほどの発言は、あくまでも身元確認保証レベル 1 の話をしておりました。
- 身元確認保証レベル 3 や 3 に近い 2 というのは大事でないかと感じています。それ以下のレベルは、あまり厳格さを求めないのではないかと考えています。レベル 1 は、目的に照らし合わせて的確な組み合わせを行って検証するといったような記載が良いのではないかと考えています。
- 身元確認保証レベル 1 で必要な本人確認書に対する物理的な検証は難しいため緩めるのか、レベル 1 であっても偽造対策印刷技術等の確認をしっかり行うのか、といった基準の動かし方が難しいところであると感じました。
- 「日本版 SUPERIOR」のように本人確認書類の分類は行うが、資料 2 P11 に記載されている、身元確認保証レベルとの対応関係は、ある程度の緩さを持たせる、もしくは、テーラリングとしてそれぞれの組織が決定するということになるのでしょうか。
- 各身元確認保証レベルにおいて、脅威だけではなくどのようなユースケースが該当するかを想定していますか。各身元確認保証レベルに対してユースケースをあてはめ、ユースケースに対応する脅威が決定し、最終的にレベルの定義が決まるというように理解しています。現行の本人確認ガイドラインを作成する際には、身元確認保証レベル 1 は「行政機関で図書館カードを作るにはどうすればよいか」というユースケースを想定していました。逆に言えば、確認コードを利用すること自体にも疑問を持っており、図書館カードのような施設を予約する程度であれば、自己主張だけでもよいのではないかと感じています。資料 2 P10 の日本版 FAIR では、印鑑登録証明書や住民票の写しの検証を窓口で行うことは難しいと考えます。その点では学生証や社員証などと変わらないと感じています。ただし、民事訴訟法第二百二十八条に公文書の真正性要件が2点記載されており、公が決めれば真正であるという旨の「文書は、その方式及び趣旨により公務員が職務上作成したものと認めるべきときは、真正に成立した公文書と推定する。」といった記載のほかに、「公文書の成立の真否について疑いがあるときは、裁判所は、職権で、当該官庁又は公署に照会をすることができる。」といった記載もあり、裁判所が問い合わせて確認することができると考えられます。住民票の写しも、その場で行政機関へ確認することは難しいかもしれませんが、最終的には裁判所では確認が可能とな

っている認識です。そのような意味では、住民票の写し等と学生証等とは別であると感じています。公共料金の領収書についても、番号が記載されているため、問い合わせができると思います。

- 公共料金の領収書は、お金が動いているため、トラッキングすることが可能であるというのも重要な観点だと思います。
- そのような観点では、資料に書かれている「公共料金の領収書」と「その他、住所の証明に利用される郵便物」は同等にはならないのではないかと感じます。
- 米国では、銀行口座を開設する際に、住所の証明に利用される郵便物を持参するよう求めていたので、日本の現状に合わせて、トラッキングできること等に修正する必要があると考えます。事務局に伺いたいのは、身元確認保証レベル 1 のレベル感は想定があるのでしょうか。ユースケースが決定していないのであれば、身元確認保証レベル 1 はある程度許容できる範囲を持っておく必要があると考えています。匿名である必要はないものの、仮名で活動できるような空間が必要ではないかと考えています。仮名で活動することすら禁じられた場合、シャドーIT 化する危険性もあり、位置づけを実施し、コントロールしたほうが良いのではないかと感じています。
- NIST SP 800-63-4 2pd の改定において取り入れられた「Attended か否か」（オペレーターが存在しているか否か）の概念がないと感じました。身元確認保証レベル 1 などで微妙な差を作るにあたって、考慮が必要ではないかと感じています。また、身元確認保証レベル 2B も Remote unattended の場合になるかと思いますので、Remote attended との差がつくところが丸められてしまっており、きちんと書き出した方が良いのではないかと思います。また、NIST SP 800-63-3 で、Supervised Remote Proofing の扱いが中途半端に記載されていたと記憶しており、Attended か否かは要素として追加が必要だと思っています。現状、リモートでの容貌の確認は、Remote unattended のみなのでしょうか。結果としては変わらないのかもしれませんが、場合分けを実施することで、読み手の納得感が醸成されるのではないでしょうか。
- リモートでの容貌の確認方法は、自動で認証するパターンと、後から目視で確認するパターンと 2 つあります。
- そもそも、身元確認保証レベル 1/2/3 として分けることができるのかといったことに疑問を感じています。単なるプラスチックカードとしての身分証は、偽造という観点では何の意味もないと感じます。脅威に対応する対策があり、それらのラベルの組み合わせでプロファイルを行った方が良いのではないでしょうか。現状の身元確認保証レベル 1/2/3 の基準であれば、各国との間で平仄が取れないのではないかと考えています。例えば、カラープリンタで簡単に作成できるような本人確認書類が使える身元確認保証レベル 2D を、身元確認保証レベル 2 としてまとめてしまうことに意味があるのかと感じています。また、別の委員が言及していた、仮名での活動という点は重要です。それを身元確認保証レベル 1 として位置づけてよいのかというのに疑問もあります。マイナンバーカードの利用者証明書用電子証明書のみを利用した確認は、それ自体には氏名等が含まれていませんが、強度的にはほとんど身元確認保証

レベル 3 に近いのではないかと感じています。さらに mdoc などを利用し、毎回 Applet の中でランダムに ID を発行するものの、同じ検証者に対しては、同じ Identifier を払い出すといったような運用は容易に想像できます。NIST SP 800-63-3 以来の基準である、レベル 1/2/3 という基準そのものが、多様化している認証強度の観点を限られた次元に押し込めようとしているがゆえに、このような議論が発生しているのではないかと感じています。むしろ、フィッシング耐性を有するのか、偽造可能なのか否かといったラベルだけつけていく方が良いのではないかと感じています。

- ISO 27002 などでは、軸を 1 個 2 個に決めてマッピングするのではなく、タグをたくさん作りマッピングしていくことが多くあります。ただ、グローバルスタンダードとの整合性を取る必要はあるのではないでしょうか。
- ラベルを決めていくと同時に、他国との整合性を取るためのマッピングテーブルは作るべきだと思います。マッピングエクササイズ用のドキュメントとして、米国におけるレベルは、日本におけるこのラベルの組み合わせにあたる、というドキュメントを作成すればよいのではないかと思います。国内でリスクアセスメントをする際にはラベルごとに要不要を判断していけばよいのではないかと思います。
- ガイドラインの書き方として、ラベルを付けていくような方法は良いと思います。ただ、専門家はタグで判断することができるかもしれませんが、一般の行政官が対策ごとの要否を判断できるのかは懸念が残ります。
- あらかじめ、典型的なラベルの組み合わせを用意しておくことになるのではないかと考えます。電子申請の場合やくじ引きの場合など、あまり多種な例はないのではないかと感じます。また、これまでの保証レベルとの互換性を考えると、Liveness Check を身元確認保証レベル 1 にするか 2 にするかは、政治的なプレッシャーを受けやすくなっていると思います。特定のユースケースに対して、基準を緩くしたり、上位の基準として認めたりすることによる、社会的な損失が無視できなくなってきています。本来は、NIST SP 800-63-4 に合わせに行くのではなく、NIST SP 800-63-5 が本人確認ガイドラインに合わせにくるような発想で検討することが望ましいと考えています。身元確認保証レベルとの対応関係で検討に行き詰っているとするならば、この概念自体に無理があるのではないかと感じます。
- 国内の動向を踏まえれば、この会議体に対する社会からの期待や要請はこれまで以上に強まるのではないかという認識があります。ここでいう身元確認や何のためにやるのか。身元確認や本人確認の実施する目的を突き詰めていくと、なりすましを防ぐことにあると考えます。行政サービスのみならず、民間事業者においても、例えば携帯電話事業者において新しい契約を結ぶ際や機種変更を行う際等で、間違えても違うお客様になりすました者と契約することがあってはなりません。まず、議論すべきことは、本人確認をする際に、厳格さを求める際にはどこまで求めるかどうかだと思います。身元確認保証レベル1の具体的な本人確認書類の組み合わせを議論することは、ユースケースがはっきりしていない中では難しいということは繰り返し申し上げたいと思います。例えば図書館カードの事例では、パスポートを持参さ

れてもどこに住んでいるかがわからないため使用できないと考えます。業務がはっきりすればレベル 1 の中で幅があり、テーラリングが適切にできます。身元確認保証レベル 3 や 2 といった高いレベルの議論されているところが大事になってくるため、明確な記載を行うことが、役に立つドキュメントとなるのではないかと考えます。資料 2 P11 に、これまで議論してきた身元確認保証レベル 3 や 1 は、想定される業務が明確にされておらず、身元確認保証レベル 2 には、複数の段階が存在しています。直感的に言えば、身元確認保証レベル 2B 以上は、厳格な本人確認を求める手続きに必要なレベルになっています。身元確認保証レベル 2A/2B には、電子的検証とリモート/対面での容貌比較が必要である旨が記載されていますが、身元確認保証レベル 3 にはその記載がありません。説明のみを見ると、身元確認保証レベル 3 と身元確認保証レベル 2A の区別がわかりません。身元確認保証レベル 2A 以上、もしくは身元確認保証レベル 2B 以上は、新しい身元確認保証レベル 3 のような区分にとらえられるのではないかと感じます。身元確認保証レベルが低いものに関しては、目的に応じてテーラリングすればよく、例えば住民票の写しを持っている方であるとすれば、それで十分だとするケースも存在するだろうと思います。

- また、資料 2 P10 に記載してある「公的機関」の定義は、はっきりとはしていないのではないかと感じており、例えば、国立大学行政法人は公的機関ではありますが、私立大学は公的機関ではないといったことも考えられます。先ほどあった議論のように、トラックできるか否かといった基準で選定することが落としどころになるのではないかと考えています。
- 今回改訂する本人確認ガイドラインが 3 年から 4 年は使われることを念頭に置くと、現状ですでに、マイナンバーカードは約 9500 万枚保有されており、今後はより多くの国民に保有されて利用されることが想定されます。事業者が日本版 SUPERIOR に該当するマイナンバーカードの確認を行う中で、日本版 SUPERIOR ではないとき、日本版 STRONG に該当する本人確認書類とは何が違うのか、どこが脆弱になり、どのようなリスクがあるのかを強調する必要があるのではないでしょうか。
- P10 において引っかかったのは、マイナンバーカードで認証できてさえいれば、他は何も考えなくてもいいといったような状況は、あと何年続くのでしょうか。日本国民であれば、だれでも持つようなことができる ID カードであるため、多くの人が持てば持つほど貸し借りやその他の問題が発生し、そういった知見が署名検証者の中で蓄積されるなかで、依拠する基準のテーラリングをどのように行うかといったことも視野に入れる必要があります。
- また、今の資料はリモートと対面の二極となっていますが、日本にはコンビニに置いてある ATM があり、これは、対面とリモートのどちらに該当するのでしょうか。当然、人が見ているといった状況も重要ではありますが、侵害されている可能性の高い個人のデバイスではなく、管理された端末で実行されているということは同じ以上に重要であると考えます。コンビニ ATM は様々なコンビニで展開されるでしょうし、すでに病院においては顔認証付きカードリーダーなどが存在しており、デバイスのプロファイルが均質なものが全国に展開しているというのは、米国にはない日本独自の状況になっているのではないかと感じています。日本だから

こそ、対面かリモートかではなく、デバイスが managed か否かと attended か否かといった議論は分けて考えることができると考えており、米国追従になりすぎると、日本では先に行っている部分が生かしにくいのではないかと感じています。

- 今仰られたことは、今までの我々の議論において欠けていたことであり、カバーすべき内容であると感じました。マイナンバーカードが広く使われてきたことに対しては良いことではありますが、カードをなくした方・交付を受けていない方・海外からきた方といった境界条件に対して、悪意をもった者が入り込んでくるだろうと考えます。そういった方々に対して、マイナンバーカードでできること以上の対策をやったほうがいいと思います。対面か否かにかかわらず、容貌の確認を行わない限り、悪意をもった者からの攻撃からは守ることができないと強く主張します。また、マイナンバーカードを紛失した方のブートストラップ問題も非常に重要だと考えます。突き詰めると、出生をしたタイミングから、なんらかをトラストアンカーとし、再度発行するのかといったことも考えられますが、様々なケースで日本国民となる方もいらっしゃり、そのような方がマイナンバーカードを持てる状況が想定されます。こういった様々な境界条件を洗い出して、対策を実施していくことが望ましいと考えます。
- マイナンバーカードを紛失した際に、再発行することが難しいのではないかといった件は私も気にしています。マイナンバーカードが免許証と一体化されると、どうやってマイナンバーカードを再発行するのかという点が、ブートストラップに引っかかってしまっていると思われるため、検討が必要なのではないかと思います。本人確認書類が完全一元化となるのは大変厳しくなると考えており、また本人確認書類が多数あっても仕方がない中で、再発行も考慮し複数あることは保証すべきであると考えています。
- 再発行に使える書類がないという話については、認証アプリや mdoc に Derived Credentials を入れるという話が使える可能性があります。マイナンバーカードしか使用できないといった状況は、数年後には改善されているのではないかと思います。
- Derived Credentials は、あくまでも資格であると思います。人とバインドされた本人確認と本人確認されたものにも紐づけられたクレデンシャルは異なるものではないでしょうか。
- 物理カードとしてのマイナンバーカードを紛失したとき、スマホにステータスが残っている場合、どうすべきかといったユースケースを詰めていかないといけないと思います。境界問題というのは多数あり、例えば戸籍は持ってらっしゃらない方なども存在します。再発行の方法と境界問題は慎重に検討する必要があると思います。
- 再発行に関しては、私も問題だと思っています。FIDO アライアンスで議論してきたアカウントリカバリーに関する議論が、貢献できる可能性があると思いました。伝統的に FIDO クレデンシャルはデバイスから出せないものとされていたため、デバイスを紛失した際にどうするかということが議論されてきました。その中で、ある身元確認をした結果を根拠として FIDO クレデンシャルを FIDO 認証器を作り、片方をなくした際に、もう片方の認証器を使用してアカウントリカバリーが可能になるといったことを提案しています。今でいうと、紙のマイナンバーカードとスマホ搭載マイナンバーカードの両方を所持することが許容されているため、スマホにマイ

ナンバーカードが残っていれば、リモートで再発行はできるのか、それとも、市役所に行かないと再発行できないのかといった議論ができるのではないかと考えています。

- NIST のような Evidence の種類と 3 段階になんとかマッピングしていくこと念頭に考えすぎているがゆえに、うまく当てはまらないことがあるのではないかと感じています。そもそも米国では SUPERIOR に該当するものが何かと考えてしまうほど SUPERIOR の Evidence を得ること自体の難易度が高いという状況になっています。一方で、別の委員がおっしゃっていたように Authoritative Source への問合せが、日本では簡単ではないと認識していますが、米国ではシステムで検証することが考えられており状況が違うと思います。現在、身元確認保証レベル 2A/2B/2C として記載されているのは、NIST に合わせようとした結果うまくいかなかった表れであると認識しています。今、日本にある手段から何の脅威が軽減されているのかを確認してみた結果、最終的にいくつかのパターンに集約されるといった検討のアプローチをしてもよいのではないかと感じています。以前に企業向けのリスクを整理した際は、細かいマトリックスで、生存性・実在性といったリスクを並べ、それぞれでプラスマイナスを評価しました。単純に評価結果を足し合わせてスコアにしてよいのかといった議論はありますが、一定の程度感を示すのもよいのではないかと感じています。この議論は、本会議の今年度の検討スコープに大きく影響を与えるため、改めてどのような方向性で考えるかを議論したいと考えています。
- NIST には、Authenticator を再発行するならば、同じ IAL で Identity Proofing をやり直すべきであるといった記載が書いてあります。しかし、マイナンバーカードに免許証が搭載された場合、免許証がなくなり、Authenticator が一つになってしまうのではないかといった問題が発生し、アカウントリカバリーは難しくなると考えています。スマホに搭載するマイナンバーカードは、紙のマイナンバーカードと同一の有効期限を持たなくてもよいのではないか、別の Authenticator として登録できるのではないかと理解しています。NIST の枠組みに引っ張られすぎているのではないかと感じています。

議題(2)ガイドライン改定に向けた論点協議

「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」

事務局より、資料 2 P17～25 に基づき論点 3 についての説明を行い、有識者による自由討議を行った。

（有識者意見）

- NIST の FAL は技術的な内容が多く、組み合わせのパッケージのようになっているため、そのパッケージングでよいのかは議論の余地があると考えています。ただし、IAL に比べて AAL や FAL は日本ならではという事情が少なく、NIST を参考にすること自体には違和感はありません。FAL2 でのアサーションインジェクション攻撃は、基本的には SAML での IdP initiated のアサーションを禁止しているものだと理解をしています。IdP initiated のアサーションはエン

タープライズでは広く使われており、SSO でログインをしたポータルにアプリケーション一覧がダッシュボードのように並んでいるところ、選択したアプリケーションに IdP initiated のアサーションを送ることでログインできてシームレスに使えるというものです。社内、あるいは庁内や省内で良く使われるユースケースであり既存のユースケースが自動的に FAL1 になってしまうが、IdP initiated のアサーションが禁止されることで、行政システムへどれほど影響があるのでしょうか。

- これまでは、調達自体が異なることなど等から、ポータル画面のようなものを作りにくく、結果的に疎結合でした。デジタル庁が設立されたことで複数のシステムがまとめられるような可能性がありますが、あくまでも新府省間ネットワークに閉じたものであることが想定されています。
- 現在は、ゼロトラストの概念を採用しているため、イントラかインターネットかといったことは関係ないと思います。現にインターネット経由で利用するサービスも増えてきており、ライセンスを一緒に買った場合等は、横に並べたくなるようなニーズは出てくる可能性があります。ただし、IdP initiated ではなく一度 SP を経由する実装とすれば SP initiated になり、一部のシステムでは対策もできていると認識しています。
- 多くのサービスがそのような対策ができているのであれば、今のところは大きく影響はなく導入できるのではないかと理解しました。
- OpenID Connect は IdP initiated は仕様上存在しませんので、本件については特に SAML の SP が今後対応しないといけない、あるいはすでに対応し始めていると考えられます。よって、資料 2 P24 e. アサーションインジェクション攻撃への保護対策を講じることといった要件が入ったとしても問題ないのではないかと思いました。
- レベル分けをしてどうするのかというのは感じます。設定を選択する方向であればレベル分けが必要かもしれないですが、結局正しく設定をする方向でしかありません。フェデレーション保証レベルを決めたとしても、行政官が、自分の事務を決定するときに選ぶものにならないように感じています。米国のように民間の IdP を使った行政手続が登場すればフェデレーション保証レベルの概念も必要になってくるのではないかと感じていますが、日本の状況を見ていても、すぐに民間の IdP を使用した行政手続が登場するとは思えません。本人確認ガイドラインにおいては、フェデレーションに言及する必要はあるかもしれないですが、レベル分けの必要性は低いかもしれません。
- ボトムラインを上げるところと、テーラリングの選択肢が脅威と対応して整理されていればよいと思います。これまでの議論を聞いて、フェデレーションのレベリングはあまり強く求められる状況ではなく、テーラリングの選択肢の平仄が他のガイドラインととれている必要があると感じました。
- 現行ガイドラインが策定された頃は、世の中がフェデレーションを新しく導入するタイミングだったため記載をしていませんでしたが、現在は、皆様がフェデレーションを利用したシステムを作り始めている状況になります。デジタル庁以外の人たちへの注意ということで周知するこ

とは大事だと感じました。

- 自治体では民間 IdP の受け入れが良くあると思います。プッシュ型行政いったコンセプトの取り組みで、民間 ID を利用して軽い IAL の人たちに情報発信や手続き案内を行っているが、そのまま申請を行うこともできるような手続きが多く発生してきています。これらは、本人確認ガイドラインの本来のスコープではないことは承知ですが、実態としては自治体からも多く参照されるドキュメントとして、FAL1 を記載するニーズはあるのではないかと感じます。
- 別の委員の発言とも重複しますが、民間企業の属性情報を参照する可能性があるのではないかと思います。携帯電話番号や銀行口座情報等、民間の方がより詳しい情報を持っている場合もあり、それを活用することは有用だと思っています。
- 本人確認ガイドラインは、あくまでも各省庁の行政手続のみをスコープにしています。しかし、実際には NISC のガイドラインなどと同様に自治体から参照されることも考慮が必要です。アメリカのエンタープライズでは、SAML が多く残っていたとしても、日本では 2015 年の銀行法改正をきっかけとして Attribute Provider となりうる主要銀行や主要プロバイダーが構築されており、2017 年以降に構築されたものが大半と想定されますので、OpenID Connect を利用し、相当しっかりとした IdP を構築いただいているのではないかと考えます。
- Shared Signal の概念が行政の中だけでしか使用されないはもったいないと思います。行政と民間で分断があった際に、Shared Signal に価値があるのかといった指摘をいただく可能性があります。行政機関も民間企業の情報が欲しい、民間企業も行政機関の情報が欲しい中でどのようにこれを解決していくかの答えはまだ出ていません。ただ、現在の Shared Signal には、個人の識別ができる情報が入っていないため、民間企業へ渡そうと思えば、渡すことも可能であるように思えます。
- 行政と民間をまたいだ Shared Signal を本人確認ガイドラインで現行法の下で実施できるか、踏み込んでやる必要があるのかという話と、海外と平仄をとり、脅威に対する Mitigation の手段として本人確認ガイドラインに記載したうえで、法の下で実施できるかどうかのアセスメントは別途行うといったことは考えられます。
- 確かに Shared Signal は難しいと思うことが多いです。また、エンタープライズでお客様によって、SAML は使っていますが、マス・コンシューマー向けは、全て OpenID Connect となっています。
- FAL3 は、現状実現する方法はあるのでしょうか。将来的に日本版 PIV やデジタル認証アプリが Holder-of-Key Assertion を利用することを見据えるのであれば、FAL3 自体はあっても良いように思います。FAL1,2,3 は normative ではなく、informative で初期 FAL 検討後のベースとして、実施の有無の理由の記録を残すような扱いでも良いかもしれないと感じました。

閉会

（事務局）

- 非常に実態を踏まえた議論ができたのではないかと感じています。国際的に耐える論点を出していければ望ましいと考えており、引き続き今後もよろしくお願いいたします。

（了）