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 4 回）
令和 6 年 1 月 30 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 4 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。
- デジタル庁内でもアイデンティティマネジメント関係も色々と具体的な動きがある中でして、本人確認の重要度は増しており、欧州と米国間で実施されたマッピング結果なども参考にしながら国際的な相互運用性を意識した検討を進めていく必要が高まっています。米国をはじめとした海外の動向を単純に取り込むだけではなく、技術の進歩や様々な取り組みをタイムリーに把握した上で自分事として議論を進めていくことが大切だと考えていますので引き続きご指導のほどよろしくお願いいたします。
- 本日議論いただきたい論点は大きく 3 点ございます。検討中の本人確認ガイドラインの改定ポイント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①「ガイドラインの適用対象と名称を変更」について

事務局より、資料 1 に基づき改定ポイント①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）

- 行政事務の従事者を対象に含める方針ということですが、それは行政手続の申請者と同等の本人確認を行うための統一的な基準を作成するということでしょうか。

- 事務局：完全に一致させられるかという点については検討中の部分ではありますが、同等の基準を適用できないかと検討中です。参考としている NIST SP 800-63-4 が同様の方針となっているので、本ガイドラインもそれにならう形にできないかと検討しています。

- 行政事務の従事者を対象とすることについて、想定されている RP はあるのでしょうか。
  - 事務局：内部事務のために利用する情報システムを主な RP として想定しています。
- 適用対象を拡大することは良いのかなと思うのですが、国民向けサービスと内部向けサービスでは想定されるリスクと影響範囲が明らかに異なりますので、その差を考慮した記載にする必要があると考えています。
- 行政事務に関わる委託事業者を対象としていることについては、改定版のガイドラインから法人を対象外としようとしている方針と若干ズレが生じているのではないかと感じました。法人が行政手続をする際の本人確認と、行政事務に従事する委託事業者に対して行う本人確認は似通ったものになることが想定されますので、職員と委託事業者についてはカテゴリーを分けた方が良いのではないかと思います。
  - 事務局：委託事業者に対する本人確認は、実際にシステムを利用する自然人としての作業者の本人確認を想定しています。委託事業者に対して法人としての本人確認が必要な場合には、別途整備する法人向けガイドラインを適用することを想定しています。
- 事業者を通して見た個人を対象とする場合、事業者がその個人を採用する際に一定のスクリーニングがされているということを前提として個人を見るはずなので、政府機関がゼロから本人確認を行うことにはならないと考えており、その部分は分けた方が良いのではないかと感じました。
  - 事務局：その点は今後検討が必要と考えておりますが、このガイドラインによって現在の委託事業者に対する身元確認を厳格化するといった意図や目的はございません。他方、委託事業者にシステムのアカウントを払い出すようなケースにおいて当該従事者の当人認証を行うケースは多いと認識しておりまして、そういったケースへの適用を想定しています。
- そういうことであれば賛成です。
- 当該部分については、米国の PIV 制度と同様のものを日本にも導入する前提で書かれているのかなと思って聞いていました。国民に対して一般的なサービスを提供する場合とはクリアランスの水準が異なる話だと思うので、そこが強調された記載となっていないところが少々気になりました。
- 私も PIV などの話がスコープに入ってくるのかなと感じておりました。極めて重要なユースケースでの採用を前提として身元確認保証レベル 3 が厳格化される方針とも整合が取れるものと思います。また、各府省・システムによって定められたアカウントの発行プロセス・権限管理といったセキュリティに関する内規の統一や強制を目的とすることを考えているのであれば、妥当であると感じました。
- このガイドラインを使って民間企業側が本人確認を行ってその結果を政府が受け入れるケースも想定しているのでしょうか。
  - 事務局：現状、そこまでは想定しておりません。
- サービスの提供においては個人と法人を分けられない部分はあると思っており、今回の改定で法人をスコープ外としようとしているという方針には唐突感がありました。何か理由がある

のでしょうか。
  - 事務局：誤解を招く説明となってしまいましたが、法人については別のガイドラインに切り出した上で整理することを想定しております。
- その場合、ガイドライン改定との時系列での関係はどのようになるのでしょうか。
  - 事務局：本人確認ガイドライン改定のタイミングに間に合うのかという点も含めて検討をしている状況ですが、仮に法人向けガイドラインの整備が間に合わない場合は、単純なスコープアウトはできないと考えています。
- サービスの利用者は個人の場合もあれば学校や団体といった法人であることもあって、それにより別の要素が入ってくることは当然理解しています。FIDO の Enterprise Attestation に関する考え方でも、会社や団体として身元確認を行った上で従業員となっていることを前提に、個人に対するプライバシーの問題と、企業がそれを管理するのだからという意味での違いが区別されています。ただ、何らかのボトムラインがないとなし崩しになってしまうので、同じタイムフレームでミニマムにきちんと押さえていくことが大事なのではと感じました。
  - 事務局：ご指摘のとおり、現行ガイドラインで存在していた既存の基準がなくなってしまうことは問題ですので、ガイドラインが途切れないよう、最低でも改定時に法人向け部分を別冊として残すなどの対応が必要と考えています。
- 法人の本人確認が難しい問題を含んでいるということは理解しているのですが、難しいことを理由に後回しにしてしまうのではなく、目標を定めてそのタイミングまでに結論を出すというアプローチが必要だと考えます。
  - 事務局：皆様からいただいたコメントは重要な示唆があるものと受け止めております。現行ガイドラインは G ビズ ID や商業登記認証局といったそれぞれの具体的な認証手段を強く意識したものとなっており、法人そのものを認証しているというよりは、企業の手続担当者という自然人に対する本人確認に近い内容になっていると認識しています。他国のガイドラインとの平仄を揃える意味でも、所属先などの属性の確認とあわせて検討すべきテーマであると考えております。また、ガイドラインから法人をスコープアウトすることで空白ができてしまうことが問題ではないか、というご指摘はそのとおりだと思います。法人の手続におけるマイナンバーカードの利活用や、特に中小企業などにおける多要素認証の導入ハードルなどの情勢も現行ガイドライン発行時から変化してきておりますので、そうした環境変化を整理したうえで、スコープを変更しようとする背景を丁寧に記載・説明する必要があると認識しました。
- 身元確認と当人認証というのはやはり別物でして、当人認証については個人でも従業員でも、その時に求められる認証強度の考え方はほとんど変わらないと思います。強いて言えばプライバシーに関する考え方は違いますが。一方、身元確認については、従業員であれば企業や団体が身元確認をして採用している前提があり、その上で所属との関係を確認する点が個人のものとは異なってきます。モダンな考え方を照らし合わせることで、残りの期間の中でもできそうなことはあると思うので、急に法人をスコープから外すのではなく、できる範囲で検討した方が良いと考えます。
- OpenID Connect for Identity Assurance の中でも Authority Claims というプロファイルがあります。この設計をする際に最初に話していたのが、認証している主体はあくまで個人であって、個人と法人の関係性をどのように属性として表現するのかというところです。その関係性をき

ちんと表現することができれば今回のスコープからも外すことなく自然と収まるのではないでしょうか。英国では Companies House というデータベースで法人の登記情報がオープンデータとして公開されていますが、そのデータと個人をどうやって紐づけるかというのが Authority Claims の設計思想です。法人そのものの真正性の確認は元々スコープ外だと思うので含めなくても良いと思いますし、個人と法人の関係性に範囲を絞ればスコープを外すという議論にならなくて済むのではと思います。

- 委託先目線で考えてみると、「所属先」が異なる再委託先や派遣社員の方にも対象を広げるとなると厳しそうな気がしました。どの人にどの作業までを認めるかという権限という意味であれば制御できるかもしれませんが。
- 日本では雇用規制の背景があるため、再委託先の社員が重要なオペレーションを担当しているケースもあります。本来であれば米国のようにバックグラウンドチェックやるべきところを、これまで重大な問題が発生していないことを理由に省略してしまっているというのが実情だと思っています。かといって、役務提供契約において相手の身元まで確認すること自体がコンプライアンス上問題であるという整理もあるので、とても難しい問題だと思います。
    - 事務局：法人の本人確認については G ビズ ID などから参照されているため、完全になくすことはできないと認識しております。最低でも現行ガイドライン相当の内容を別冊化する形でガイドラインとしては存続させたいと考えておりますが、本編との記載粒度が大きく異なってしまいますので、どのタイミングで更新を行っていくのかも含め継続して検討したいと考えます。

<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）

- 22 ページの表に記載されている脅威は、一般的なものからあまり見かけないものまで内容に幅があるように見えます。複数の出典元から集約した内容なのでしょうか。
    - 事務局：黒字部分が現行のガイドライン内で定義されているもの、青字部分が今回の改定に当たって NIST 文書や米国 CISA のフィッシングレジスタンスに関するガイダンスを参照しつつ、対策を検討すべき脅威として抽出したものとなります。
- ここに記載されているリアルタイム型フィッシング、多要素認証疲労攻撃、SIM スワップとはそれぞれどのような脅威を指しますか。また、レベル 2A～2C に分類する場合、具体的にどの手法がどのレベルに該当するかが記載されていませんのでそちらについて教えてください。
    - 事務局：リアタイム型フィッシングは、偽サイトを用意してそこに入力される認証情報をリアルタイムで中継するタイプ、これは一種の中間者攻撃に該当すると思いますが、プロキシのような形で情報を窃取して二要素認証を突破するタイプのフィッシング攻撃のことを指しています。多要素認証疲労攻撃は、Authenticator のアプリのうち OK ボタンの押下のみで認証してしまうタイプに対して大量のリクエストを送ることで正規ユーザーの誤ったログイン承認を狙うタイプの攻撃を指しています。SIM スワップは、SIM 紛失時の再発行手続などから他人の SIM を奪取するような攻撃全般を指しています。

- 事務局：レベル 2A～2C の具体的な手法例ですが、リアルタイム型フィッシングを防ぐことができる 2A の手法としては FIDO ベースの認証あるいは PKI ベースの証明書での認証を想定しています。多要素認証疲労攻撃を防ぐことができる 2B の手法としては、認証時に数字を入力させるタイプの Authenticator を、2C については SMS を使った OTP を想定しています。

- SIM スワップを防ぐためには、本質的には当人認証時ではなく身元確認時の対策が必要になるため、当人認証保証レベルを定義する表に掲載することには違和感を覚えました。
- 2A～2C の想定として説明いただいた手法は明らかに強度に差がありますので、当人認証保証レベルを細分化するという方針については賛成です。
- 22 ページ目の脅威の黒字部分に「中間者攻撃」と「リプレイ攻撃」がありますが、これらの対策ができるのにリアルタイム型フィッシングの対策ができない、という手法はないのでは？と思いました。また、「セッションハイジャック」を防ぐのは厳密には難しく、対応可能な Authenticator がなくなってしまうのではと思います。
- 民間からも参照されるガイドラインであることを考えたとき、レベル 2A～2C の 3 つの区分が採用可能性や負担を考えた細分化となっているのか、それとも単純に防御の必要性の観点で細分化しているのか、先ほどのセッションハイジャックの話も含めて基準や粒度が揃っていないのではという点が少し気になりました。
  - 事務局：表中の黒字部分は現行ガイドラインの記載ですが、定義の明確化・最新化が必要であると認識いたしました。また、黒字部分と青字部分（追加部分）の粒度が揃っていないというご指摘や記載内容に矛盾があるように見えるという点も課題と認識しましたので、ここで基準とする脅威の種類と定義は改めて整理・明確化するようにいたします。
- 黒字部分については NIST SP 800-63-3 が発行された当時は用語定義に幅があったため、中間者攻撃と記載されているものだと考えます。今回の目的はリアルタイム型フィッシングとそうでないフィッシングの違いを浮き彫りにして読み手に意識させることだと思うので、言葉の定義を見直すことで調整できればよいと考えています。
- NIST SP 800-63-3 が公開された頃と現在では、この領域に対する理解と対策の成熟度が明らかに違うと感じています。当時の文書では、耐タンパ性のあるデバイスであれば万全であるような記載がされていたりしますが、現在では当人認証が完了のセッション管理で Cookie が詐取されてしまうとアウトであるということは共通の理解になっていますし、NIST SP 800-63-4 でも Attacker-in-the-Middle という表現が取り入れられています。定義された身元確認保証レベルと当人認証保証レベルを達成しても、防ぎきれない攻撃が存在するという示唆もしていく必要はあるのではないでしょうか。認証の瞬間が重要であることは間違いないですが、この手法によって脅威が全て解決するように見えてしまうのは危険な気がします。
- プロプライエタリなチャネルであれば対策を実現できる場合もあると思いますので、対策について推奨とすることは問題ないですが、必須とするのは難しいと思います。
- 当人認証保証レベルを 2A～2C に細分化することについて論理的には整理するものの、Verifier の観点から見たとき、ある認証器が該当するレベルをどのように判定するのかという問題がおそらく発生します。FIDO の認証器でも指紋認証を必須にしているものとそうでないものとがありますし、Authenticator のアプリでも顔認証をした上でロックを解除しているものなのか、単純に番号が表示されているものなのかを区別ができないと思います。

- その点について私は違う意見を持っています。レベル 2A を達成するために生体認証でないといけないのかどうかという点については選択の幅があるはずで、詳細な認証要素の細分化までは入り過ぎている気がします。
- その場合には認証キーのレジストリが必要になってくると思っていて、どの認証キーがどのレベルにマッピングされているものかを利用者が確認できる状態にしておく必要があると考えました。
- その意見は理解できるのですが、どこまで理解する必要があるかであって、例えばパスキーは実装する企業ごとに仕様は異なりますし、利用者が認証手法として生体認証を登録して利用しているかどうかは分からないケースも多いです。それでも当人認証保証レベルはいずれも 2A が達成できるので、実装上必要かというとそうではないと考えています。
- FIDO の場合はそうかもしれないですね。一方、ソフトウェアベースの Authenticator となった場合には、色々なばらつきがあるなとも思っています。
- その認証がどのように行われるかレジストリを使って管理するのだとしたら、2A～2C も管理できるのではないかなと私は思いました。
- 関連して、レベル 3 のところに HW トークンの記載がありますが、品質の悪い HW トークンではダメだと思います。NIST が言っているのは FIPS 140 のレベル 2 またはレベル 3 の認証を取っている HW ということですよね。
- そのように縛りをかけるというのがまさに認定基準といった話になると思うのですが、本当にそれで認証されてきたかっていうのを RP がどうやってわかるのかという問題に行き着いてしまう気がします。
- それは CSP が保証するしかないと思います。
- クレデンシャルを登録する際に認証キーの関係は定義づけられるので、実装できると思うのですが。
- その際に基準を満たす HWトークンとそうでないものを判定する仕組みが必要だと思っています。
- このメタなコンセプトに加えて実装する際のガイダンスも必要です。この当人認証保証レベル 3 の HW トークンということでいうと、少なくとも FIDO のセキュリティキーにはセキュリティ認定レベルの 1～3+があって、米国政府が使っているのは 2+以上だったと思います。そこではメタデータサービスが利用できるため HW トークンを管理ができるようになっています。
- 2A～2C に細分化することも必要だと思うし、細分化したときに認証キーをそれぞれのレベルに区別することもできるし、レベル 3 についても認証キーに対する管理、認証、検証といったことが必要であると書いておくべきだと思います。
- きちんとマッピングできる状態で書かれていないと実装ができないということですよね。
- おっしゃるとおりです。
- 今の議論は、従来のトラストフレームワークの機能や要件の非常に大きい部分だと思います。それをきちんと記述する必要があります。また、参加する CSP について政府がコントロールできるものであれば Authenticator を管理・制限できると思いますが、民間の CSP を受け入れる場合には、トラストフレームワークの設計がとても重要になってくるはずです。アカデミアのような閉じた世界であれば推進しやすいのですが、政府ですと国民にサービスを提供することになるので、CSP をどうコントロールするかというのは実装面で大きな課題になると考え

ています。

- そういう意味ですと、レベル 2A の FIDO やパスキーにも幅があって、実装による差も出てきています。従来は OS プラットフォームベンダーやメーカーが実装しているものが中心だったのですが、最近はいわゆるパスワードマネージャーを提供するベンダーがパスキーを提供するようになり、利用者の選択の幅が広がったということが発表されています。
- この表の縦軸には、メタデータサービスに登録されていること、つまり Authenticator が管理されているという評価軸が必要になってくるのではないでしょうか。
- レベル 3 の HW の話が出ましたが、FIPS 140-2 でまぁ良いでしょう、コモンクライテリアの評価保証レベル 4+もまぁ良い線行っているでしょう。ただ FIDO とかはその議論がありますが、Restricted Operating Environment がどうなっているかはすごく重要でして、Arm のセキュアエレメントを使っていれば良いのか、専用のセキュアエレメントがないとダメなのか、あるいは Apple の Secure Enclave に裏付けられた実装だったらいいのか、といったような感じで、厳密に横並びで HW を語れないというのは悩ましいポイントだと思っています。ただ、実態として世の中の人はこれらを概ね最高レベルだと思って使っていたりするところもあるので、NIST の尺度には反映されないグレーゾーンをどのように扱うのか、ケアが必要だろうと思います。
- 同じ話がレベル 2 のところでも出てきていて、Authenticator が本当にローカルの認証をしたか分からない問題について NIST は悲観的にとらえることにしており、Authenticator にもタップのみで動作するものもあれば指紋の認証をするものもあり、それが何なのか分からない限りは、その Authenticator はローカルのパスワード認証や生体認証相当のものはしていないとみなす解釈になります。一方、リアルタイム型フィッシング耐性から考えると、2 要素である OTP でも防げない攻撃が、FIDO Authenticator なら Authentication Intent のタップのみで動作する 1 要素のタイプでも防げるケースもありますので、ローカル認証の議論においてはこうしたケースについても考慮して議論してもいいかと思いました。
- 単要素・2 要素という分け方も微妙なところがあるかもしれません。ダメな 2 要素よりも良い単要素の方が優れているというケースがありますので。
- タップだけのセキュリティキーは別ですが、スマホに搭載して PIN、パターン認証、生体認証などのシングルジェスチャーに紐づけられた FIDO クレデンシャルは、FIDO アライアンスとしてはシングルジェスチャーだけど 2 要素ということになります。知識だけではなくて利用者の操作または生体情報とクレデンシャル所持の組み合わせになりますので、単一要素ではないとはっきり言っていて、そこは区別した方がいいと思います。
- 今はもうそんな実装がないのかもしれませんが、スマホの Authenticator で PIN 入力なしで認証ができた時代があったはずで、今はどうなっているのでしょうか。PIN を入れないとキーストアが HW と連動して保護されないところまで縛ってくれていればそれで OK かなと思うのですが、現状はグレーだと思います。少なくとも NIST SP 800-63-3 のときは悲観的にとらえると明確に書いてあって、言いたいことは分かるけどこの尺度だとそう解釈するしかないのかなと思っていました。63-4 がどうなるかだとは思うのですが。
- ソリューション提供側の話が多かったと思っていて、ソリューション提供者は細分化されてクライテリアがあれば自身の提供するソリューションの保証レベルを名乗っていけると思うのですが、要求する側がレベル 2A、2B など細分化したものを指定する対応ができるのかなという点が気になりました。リスクを分析して要求する保証レベルを決定するという流れの中で、行政

手続を 2A～2C に区分けできる解像度が持てるかなというところが不安に思います。もちろん保証レベルとリスクは対応しているのでこのリスクは対応すべき、または受容できる、というところから各レベルが導かれるべきではあるのですが。

- SMS やメールの OTP を利用した 2 段階認証と FIDO を使った認証とでは、被害の出方が明らかに違うことが知られていますので、前向きに検討していただくのがよいと思います。
- レベル 2 なら良いよという運用はメジャーになると思っています。そこから細分化して色分けをするならば、効果を読み手に伝えないといけないと思います。現在の犯罪収益移転防止法のように業界的なコンセンサスが長い時間で形成される可能性もあると思いますが、今回のガイドラインでは「2A には効果があるのです」と訴えていくぐらい、前のめりになってもよいのではと思います。
- 効果の観点で読み手が理解できるレベル分けの書き方をしてあげることが重要だと思います。本日の資料で言うと、2A とそれ以外は同じレベル 2 ではなくてもいいと思います。極端な話、パスワードのみをレベル 0 として、2B と 2C をレベル 1 に落とすとか、あるいは全体で 4 段階のレベルにするとか、そうしても良いくらいだと思います。
- 2C であっても、誤ったログインを減らすという意味では効果があります。膨大な数のアカウントを持つサービスでは、似たような ID やパスワードを設定する人がいて、誤ってログインされることがあり得ます。2C のレベルであっても 2 段階認証を入れておくと、こうした誤ったログインを防ぐことができます。
- 誤ったログインについては、ぜひとも脅威として追加していただくのがよいと思います。家族が同じブラウザでログインしており、夫が誤って妻側のアカウントで大金の寄付をしてしまった事例などもありました。
- ログインしたままだった、別のアカウントにログインしてしまった、のようにパターンはいくつかあり得ます。
- なかなか理解されない部分ではありますが重要な事象です。
- 繰り返しになりますが、2A と 2C は効果が明らかに違います。2B は最近 Microsoft が Authenticator を入力型に変えて、明らかにそこに対して耐性を持たせるよう意識するようになっています。縦の項目は見直した方がいいと思いますが、相当いいものになると私は思います。そうすると次は、2A と 3 を分けている意味は何なのだろうという話になってきます。実際、フィッシング耐性を確保するための実装で、そのクレデンシャルに含まれる内容によっては、耐タンパ性の必然性はほとんどないと思います。私の所属先でも早い段階でパートナー企業に対してその目的ではセキュアエレメントは不要ですと言いました。Restricted Operating Environments なんていう言い方をしますが、そこは HW で守るけどそこを操作するソフトウェアはユーザースペースで動いていたりするのですが、それで充分だったりもします。そうすると多くのケースはレベル 3 じゃなくていいということになります。そこをどう説明するのが良いのですかね。
- この表で 2A と 3 の違いになる脅威が書かれていないことが問題だと思います。元々耐タンパ性がカバーしようとしていたのは物理デバイスを盗んでチップを電子顕微鏡で分析して・・・といった、そういう脅威のはずです。
- クレデンシャルの中に基本 4 情報が入っているマイナンバーカードのような仕組みであれば当然耐タンパ性のあるデバイスに入れないといけない話になりますし、そのクレデンシャルが

ランダムな文字列で、それだけ見ても何の意味も持たないものであれば耐タンパ性の必然性はほとんどないと思います。レベル 3 と 2A を区別するための脅威をきちんと明確に書いておいた方が良いと思います。

- ISO/IEC 29115 だと、クレデンシャルの複製などが脅威に入っていて区別がつきます。逆に HW オンリーだと書かなくてもそっちでカバーされる。もう一つ言うならば、クレデンシャルの貸し借りも書いておくと、レベル 3 のところでそれに対応しないといけなくなったら、おそらくリアルタイムの生体認証が要求されることになって 3 と 2A の区別がつくようになると思います。
- 昔ながらの表現であればフェイルセーフかフールプルーフかっていう話になるかなと思っていて、悪意なくミスしてしまうケースと悪意があるケースそれでいいのではないかという気がします。
- クレデンシャルの複製と貸し借りと誤ったログインをこの脅威に追加して、SIM スワップは削除、セッションハイジャックは必須にするとレベル 2 は無理なので推奨とするのが良いと思います。ちなみに ISO/IEC 29115 だと、セッションハイジャックと man-in-the-middle は分けて書かれています。man-in-the-middle は認証の瞬間、セッションハイジャックは認証が終わった後の話です。
- 脅威に対して何をどうしたら防げるのかと併せて書かないと、読者が付いてこられないのではないか、と感じました。
    - 事務局：おっしゃるとおりと考えておりまして、身元確認と同様に、当人認証についても現在世の中に広まっている手法だとこれが該当しますというのを参考情報として掲載を予定しています。
- オペレーションガイダンスがないとおそらく使えませんね。レベルの分け方は先ほどのように整理すると良いと思います。
    - 事務局：レベルの細分化と脅威の見直しについては、いただいたご意見をもとに再度検討させていただきたいと思います。
- 素人目線で見たとき、「耐タンパ性がある HW トークン」と言い切ってもらった方が、読み手には伝わりやすくて良いのかなと感じる部分もあります。あくまで補足の話としてこのレベルであればこれは必須、これは推奨、と書くのが良いのか、読んでも意味が分からないかもしれないが「とりあえず守ってくれ」と書くのか、どっちの方がいいのかは判断が分かれるところだと思いました。
- おっしゃっているのはもっともですし、そういう意味で 2A～2C は何ですかと確認させていただきました。NIST SP 800 63-4 には synced passkey の話が入ってくるはずなのですが、この表では 2A に相当するはずです。クレデンシャルがデバイスの外に出ることも含めてフィッシング耐性があることは認められますが、明らかに 3 とは違います。やり方がきちんと書いてあればやりやすいと思います。
- 宣言するものが近い将来出てくる可能性は大いにあると思うので、それだったら分かりやすいと思います。落してしまっても大丈夫ですと一定のセキュリティ水準で宣言しているのが分かりやすいので、2A と 3 のグレーゾーンがあるのは分かるので時代と共に 3 側に寄ってくるという考えで良いのではと思います。
- 技術の進歩で変わってきますが、レベルに対して何年の段階では実装例としてこういうものがありますよ、というのが整理されていれば良いのだと思います。

改定ポイント⑤「リスク評価プロセスを全面的に見直し」、改定ポイント⑥「リスク評価と手法選定のための参考資料やツール群の拡充」について

事務局より、資料 1 に基づき改定ポイント⑤及び改定ポイント⑥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）

- 今までは政府等が運用する CSP を規制する前提で議論してきたと思います。外部 IdP が政府の基準を満たすということを認定する場合、その外部 IdP の認証結果をそのまま受け入れるのか、あるいは一定の留保をつけるのかというところは少し考えどころで、例えば政府がトラストフレームワークの受け皿を作って運用するつもりがあるならば、外部 IdP の利用はテーラリングではなくて利用を希望するシステムにそのフレームワークに入ってもらうことだと思うので、そこまで考えているのか、少し疑問に思って説明を聞いていました。
  - 事務局：外部 CSP の認定制度やトラストフレームワークといったところまでは検討できておりません。また、そもそもこのガイドラインのスコープなのかという確認も必要と考えています。現段階では、将来的に予想される民間との連携のケースにも、できるだけ対応できるように想定しておきたい、というレベルで考えているところです。
- ここでいう外部 IdP とはどのような定義なのでしょうか。NIST SP 800-63-3 の記述は、同一の密結合のシステムの中にない CSP と RP の間のプロトコルはフェデレーションのレベルで支配されるという話なので、外部 IdP に限定しておらず政府内の IdP も含んでいます。その点を踏まえた上でこの資料において外部 IdP と表現されているのが何なのかということを定義してもらうのが良いと思います。
  - 事務局：例えば電子申請システムの担当者からみたとき、G ビズ ID やマイナポータルは政府内の別組織のシステムになりますので、そういう意味で外部 IdP という表現をしておりました。ご指摘のとおり、疎結合のために実装された同一組織内・同一システム内の IdP について考慮できていないと認識いたしました。
- フェデレーションの概念をテーラリングで入れるのはすごく違和感があるので、そうしようと考えた理由を解説していただけないでしょうか。
  - 事務局：政府機関で利用可能な IdP の選択肢は限られていますので、外部 IdP を利用することを先に決定してリスクアセスメントを行った場合、必要とするレベルを担保する外部 IdP が存在しないということが起こり得ると思います。であれば、保証レベルを先に判定し、条件を満たす政府の IdP があれば利用する、というフローの方が検討側にとって自然なものとなると考えました。
- 同じエンティティが外出しの CSP をシステム的に利用する場合というのをあまり考えていらっしゃらない気がします。例えば政府の同一の部署内で認証部分だけは独立したシステムになっていて、1 つの IdP と 1 つの RP しかない場合であっても、その間のプロトコルに問題があるとダメなので、当人認証保証レベル 3 を求めるものであれば認証連携レベルも 3 を採用しなさいというのが NIST SP 800-63 の精神だと思います。そう考えるとテーラリングの部分に入れるのは遅過ぎると思います。
- 以前にフェデレーションの話をしたとき、手段の話なのかプロトコルの話なのかという議論に

なったと思いますが、身元確認保証レベルや当人認証保証レベルを定義する中で外部の結果に対する依拠をどう判断するかという軸を入れておかないといけなくて、テーラリングのタイミングでは手遅れであるというのは私も同じ意見です。

- テーラリングプロセスがヒットするかはさておき、私は手法の選択でフェデレーション、IdP の話が出てくること自体はあまり違和感がなくて、リスクアセスメントから始めて必要なレベルを特定した上でフェデレーションができるかどうかを判断することになると思います。利用できる IdP が先に決まっていることはあると思いますが、自前で実装するかフェデレーションに頼るかというところがフラットに選択肢に挙がるということには違和感はなかったです。36 ページの表の上部の方については確かにそうだろうなと思っていて、トラストフレームワークに入るか入らないかという話や、IdP の自己を含めた評価などでケアしていく話なのかなと思っていました。
- 私も外部 IdP の利用検討はテーラリングではなくリスク評価のタイミングで行うべきではないかと思いました。
- 何を考えるかが決まると、どこで考えるべきかが決まると思います。要求する身元確認保証レベルや当人認証保証レベルが決まり、それを誰かに肩代わりしてもらえるかもしれないという考え方になっているのはよく分かります。それが、RP 自身は何もせずにプロセスも含めて IdP に 100%依拠するということであれば特に問題はないと思うのですが、元々RP 側で ID や PW を持っていてそれを紐づけるパターンや、認証のメソッドとしてではなく身分証明書を取り寄せるための手段として IdP を利用するパターンでは、フェデレーションのプロトコルはテクニカルに定まるものの用途でぶれることがあるので、検討を行うタイミングが前半か後半かということとは別に、フェデレーションを行うのであればフェデレーションを行う上でのリスク評価をきちんと実施すべきではないかと思います。
- 「リスクの特定」の部分についてコメントすると、リスク評価と影響度の評価につながりがあるのかという点が疑問です。想定されるリスクとしてなりすましやクレデンシャルの貸し借りなどが挙げられていますが、結果がどれも一緒になっているので、リスクを特定した結果がリスクの評価にどう影響するのかが分かりませんでした。そのリスクの発生確率を乗じるという考え方も入れる必要があると感じました。
    - 事務局:リスクの特定がリスクの影響度に必ずしも紐づかないというのは認識しております。3.2 のリスクの特定結果は、リスクの評価だけでなくテーラリングにおいて手法を選択する際にも利用することを想定しております。
- 結果が一緒になるので、貸し借りだったのか盗られたのかというのはリスクベースでの判断は難しいような気がします。
- 事象の引き金として区別するために分けて記載するのは問題ないと思うのですが、結果的に起きているリスクは同じものになると思います。
- 先の話で出た、当人認証保証レベルの評価項目を追加する件に関連する話だと思っています。
- もっと業務的な話で、保険証を貸し借りした結果なりすましで入院できるといった話がありますが、そういうリスクの分析は難易度がかなり高いものと考えています。区別することでリスクの種類を思い至ることはできるのですが、そこまで作り込ませるべきなのかは正直分かりません。元々これをやるのが行政官とそれを支援する事業者という想定であるため、なかな

か難しいかなと思います。

- フェデレーションに関しては私の所属先でも少し苦労しているところでして、過去の経験からは、外部とのフェデレーションを行う際には、相手方について正しく評価をすることが重要だということを学びました。例えば所属先のルールでは一度紐づけた電話番号は簡単には変更できない仕組みになっているのですが、パートナー企業では変更が可能であるといった具合に、かつての事前の検討では気が付かなかったような脅威が出てきまして、それをどう評価するかというのは本当に難しいと思います。強いて言えばテーラリングという言葉でその時その時に応じて、というのはニュアンスとして分からなくもないですが、リスク評価としてとても難しいところだと思います。ID 連携については相当丁寧なリスク分析が必要と思います。自分のところがあるレベルを保っていても相手側がダメであれば問題が発生する可能性があり、その対策としてはどうしたらよいか、そういったことはきちんと書いておく方がいいと思いました。
- このガイドラインが民間側から参照される場合を意識すると、検討負荷を下げるために他者に頼るフェデレーションという選択肢があるということを紹介することについて、もっと前の段階でこういう考え方もあるので念頭に置いて読んでくださいという書き方をする方が良いのではないかと感じました。
- RP が要求する保証レベルと IdP が提供する保証レベルに差異がある場合は特に注意が必要であるというのが、過去の学びだと考えています。IdP に 100%依拠するパターンは大丈夫だと思いますが、そうでない場合は高いレベルの認証結果を受け取るところまでは良いのですが、それを受け取った後どうするか、変更できないように縛るか、そうしないと抜け穴が出てくる、ということを考えないといけません。ライトな民間サービスの認証にマイナンバーカードを使います、というような場合に良からぬことが起きるかなと思いますので、フェデレーションのリスク分析は特別注意が必要です。別冊で語っても難しいとは思うのですが、そんな簡単なものじゃないということは伝える必要があると思います。
- 少なくとも中央省庁もそれぞれ分かれているので我々にも分からない事情などがあると思いますが、あまり乱立して入り組みがある状態というのは健全な状態を生み出さないのではないかという感じがします。
- 認証した結果を RP に正しく伝えられるかどうか、ということを当人認証保証レベルの評価要素として追加するのがよいと思っています。
- 認証連携保証レベルの本来の意味はそうですね。外部という言葉が引っかかったのはそれで、フレームワークを作ってその運用をどうやっているのかという話になるためクロス組織になると途端に難しくなります。モダンなシステムで RP と CSP が分かれていないシステムはほとんどなく、何らかの形で分かれていると思います。それが OpenID Connect だったりあるいは Kerberos だったりするだけの話で。使っているプロトコルが果たしてどのくらい信用できるのかという話がまず認証連携レベルの最初のステップだと思います。
- 外部 IdP の定義が何であるかというところはきちんと対応しないといけないと思っていて、36 ページの表で見ると②だけいきなり外部 IdP を選択せよと書いてあるように見えます。IdP は Identity Provider であって Identity Verification Method ではないので本人確認手法の選択のところで登場するのは違和感があります。

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。次回の第 5 回は令和 6 年 2 月 27 日（火）を予定しております。前回と今回でご意見をいただきましたガイドラインの改定方針の全体を取りまとめ、残検討事項を列挙したものをお持ちさせていただく予定です。また、一部追加で議論いただきたい論点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。次回もどうぞよろしく願いいたします。

（了）