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 3 回）
令和 6 年 12 月 5 日（木）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）
新崎卓	株式会社 Cedar 代表取締役
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）ガイドライン改定案の妥当性に関する論点協議

「1. はじめに」及び「2. 本人確認の枠組み」

事務局より、資料 2 P3～19 に基づき、ガイドライン改定案の目次「1. はじめに」及び「2. 本人確認の枠組み」に関する説明を行い、有識者による自由討議を行った。

（有識者意見）

- 1.5 章の公平性に関する書き方は、生体認証の対象物ではなく、例えば「何らかの事情で指紋が登録できない方がいらっしゃる」といったような事例を示し、そのような場合に（認証手法によっては）公平性が損なわれる懸念がある、といったような書き方でいかがでしょうか。
- また、このガイドラインでナショナルセキュリティまで言及する必要があるのかという点については、少し疑問もあります。身元確認保証レベル 3 は、そのようなシステムが該当する可能性もあるかもしれませんが、通常の行政手続を担う政府情報システムは該当しないことが多いのではないでしょうか。「自分たちのシステムは大事である」という考えから、システム担当

者は必要以上のセキュリティ基準を求めてしまう傾向があることもあり、ナショナルセキュリティの記載まではなくて良いと個人的には考えます。ただしセキュリティが業務目的であるという場合を考慮し、セキュリティの項目ではなく業務遂行の観点として、安全保障に関連した業務を遂行する場合はより高いレベルを検討する必要があるといった記載をする方が良いのではないでしょうか。

- ナショナルセキュリティを考慮したほうがいいのではないか、とコメントした意図は、例えば旅券発行手続において正規の旅券が不正に取得され、国の信頼が損なわれてビザ免除もされなくなってしまう、といったような事例を想定しておりました。
- 生体認証の事例以外を先に示した方が良いのではないか、といった事前のコメントにも関連しますが、従事している仕事によっては指紋が削れてしまって指紋認証が使用できない方もいらっしゃいます。そのような方のために、生体認証については他の手段も提供しておくことは大事だと思います。イメージしにくいということであれば、「指紋が削れて指紋認証が使用できない場合がある」といったような具体例がいくつもありますので、そのような具体例を示していくのが良いと思います。また、ナショナルセキュリティや肌の色といった点では、日本といえども様々な出自の多様性があるため、丁寧な検討が必要だと思います。表現をどうするかと言った点はありますが、多様性を忘れてはならないと思っています。
- 多様性に対する考慮は記載していく必要があるものの表現をどこまで気を付けなければならないのかについては、センシティブな問題だと思います。身体的特徴や障害に当たるような内容は書き方によっては誤解されてしまう懸念を持ちました。年齢の違いによる公平性の例をコメントしましたが、表現や言い回しについては考慮が必要だと思います。
- 例えば eKYC のうちカメラを用いて書類や容貌を撮影する手法による身元確認は、現実的に目の見えない方には利用できないあるいは利用しにくい手法なのではと考えています。また、生体認証に関するものだけでなく、年齢によるリテラシーやデバイス所持の割合等も例示し、デバイスを限定すると対象外となる人もがいるというようなことを示せると好ましいのではないかと思いました。
- 例示としては、軽微な病気や怪我など一過性の状況を取り上げることも検討できるのではないでしょうか。
- 参考ですが、標準化の世界では“Demographic bias”といった表現で、直接例を記すのではなく、人口統計学的なバイアスが発生する、といった言い回しが用いられることもあります。
- （事務局）続きまして、2 章に記載しております、連携モデル・非連携モデルのメリット・デメリットやモデルの名称に関してのコメント・ご意見をいただいてもよろしいでしょうか。
- 現在の記載案では、連携モデルと非連携モデルのメリット・デメリットが書かれていないのにもかかわらず、どちらかのモデルを選択しなければならない構成となっています。「連携モデルを優先して採用すべき」と記載することは問題ないと考えますが、2.2 の冒頭に明示的に記載してはどうでしょうか。また、別のパラグラフで「なぜ連携モデルを優先すべきなのか」といった理由をメリットやデメリットともに記載するべきではないかと思います。

- 非連携モデルと連携モデルを積極的に選択させることが必要なのか、という疑問もあります。非連携モデルを採用する場合、サービスを提供する組織が IdP もセットで構築する必要があるため、それぞれの行政サービスを提供する主体の負担が大きいように感じます。信頼できる IdP にフェデレーションして行政がサービスを提供できるようにすれば、全体としての負担は軽くなるのではないでしょうか。そうした内容を説明し、連携モデルを推奨することには意味があると思います。あくまでもモデルは選択をするものだということであればメリット・デメリットを記載する必要があると思いますが、そうではない場合、素直に連携モデルを推奨するといった旨を記載することでよいと思います。
- 連携モデルを採用することが前提であるという認識で読み進めていました。「非連携モデルを採用すべき場合」のようなものを書いておき、それに合致する場合のみ非連携モデルを採用し、そうでなければ連携モデルを採用するよう、誘導した方がシンプルなのではないでしょうか。
- 私の過去の経験上、あえて、非連携モデルにしたケースもあります。IdP が使用できなくなった場合でも継続して利用できなければならない可用性のシステムを構築したときは、特定のシステムだけをフェデレーションから外し、非連携モデルを採用しました。このようなケースが行政サービスの中にあるのであれば、非連携モデルを採用すべき基準になるのではないでしょうか。
- 国民から見えるような大規模なシステムは連携モデルを積極的に採用する方針でよいと思います。一方で、システム規模があまり大きくなく、利用者が数人に限られ連携モデルを構築する予算まで確保できないようなシステムも想定されますので、職員がどちらのモデルを採用すればよいか判断できる情報をメリット・デメリットとして記載するのが望ましいと考えます。
- 必ず IdP を作らなければならない、といったメッセージである必要はないと思います。必要な業務システムのまわりに、接続するに値する IdP が存在するか確認していただきたい、というような記載をすることが限界なのではないでしょうか。サービスレベルが異なるシステムも存在すると思います。IdP に接続することを目的化する書き方まではしなくても良いと思います。
- 連携モデルの前に記載してある IAL や AAL は、「フェデレーションモデルを適切に構築するための基礎技術」であるといったことも明示しておかないといけないと思いました。
- 非連携モデルは「レガシー型」や「一体型」と呼称することもよいのではないでしょうか。
- 「スタンドアロン型」や「モノリシック型」のような言葉はどうでしょうか。
- 「一体型」や「スタンドアロン型」とした場合には、機械翻訳では Non-Federated Model とは変換されませんが、意味は通じますよね。
- 翻訳で Non-Federated Model と変換されることに固執する必要はないと思います。他国との Mapping のために必要な用語は合わせていく必要がありますが、意味が通じるということに重きを置きたいです。
- Non-Federated Model をそのままカタカナにし、「ノンフェデレーテッドモデル」とするのはいかがでしょうか。

- 国民の理解が難しくなるため望ましくはないです。広く知れわたっており、国語辞典に乗っているようなカタカナ用語であれば使用できると思いますが、フェデレーションは難しいと思います。
- 私がかかわっている日本語化の業務では、原則漢字に翻訳し、どうしても該当する漢字がない場合にのみ、カタカナで記載して注釈をつけています。
- 正しく概念をかみ砕き、正しく翻訳できる用語説明をしたうえで、原則として漢字の言葉で表現することが望ましいと思います。対訳があることが、国内で概念を定着させていく上でも重要であると考えます。
- 参考ですが、機械翻訳サービスで Federated Model を翻訳すると「連邦型モデル」になります。
- 英語を良く使われている他の委員にお伺いしたいのですが、Federation と同じ意味で使われている別の用語はないのでしょうか。
- 昔はあったかもしれませんが、最近では Federation 以外の用語を使用することはあまりないと思います。
- 以前、OpenID 2.0 を翻訳する際に Federation を「認証連携」と訳したのは失敗だと思っています。「ID 連携」という言葉であれば、世の中である程度使用されており、その訳が適切かどうかを議論したいと考えました。
- 私の所属企業の中でも、Federation を示す際に「ID 連携」という言葉を使っています。ID 連携という用語はある程度、市民権を得ている用語なのではないかと思います。昨今はフェデレーションという言葉でも通じるようにはなっていますが、あくまで日本語の言葉を作るということであれば、ID 連携という用語は適切なのではないかと思います。
- 用語定義にて、ID 連携とはフェデレーションの技術（例えば OpenID や SAML）を使って実現するものである、と定義づけておけば、大きく解釈がずれてしまうような事も無いと考えます。
- Federation の訳語は ID 連携でいいと思います。しかし、ID という言葉を使った際に、Identity や Identifier など、色々な意味が混在してしまう点には留意が必要です。
- 参考ですが、以前に Non-Federation Model を「一枚岩型」、Federation Model を「分業型」として説明していたことがありました。「分業するため効率が良い」というように説明しやすかったです。
- ある論文では、Non-Federation Model を「Isolated Identity Model」と説明されていた例もありました。そのように世の中に存在する言葉を探すのも良いかもしれません。

<u>議題（2）ガイドライン改定案の妥当性に関する論点協議</u>

<u>「3.1. 身元確認」</u>

事務局より、資料 2 P20～30 に基づき「3.1. 身元確認」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）

- 「本人確認書類」という用語については、「本人確認」が「身元確認」と「当人認証」の構成要素に分解される説明がされた後、「身元確認」の章の中にまた「本人確認」書類という分解される前の言葉が出てくる、という不整合に違和感を覚えていました。また、Validation と Verification のどちらにも「検証」という用語をあてていることは課題だと感じています。
- 「認証」という言葉だけでは何を認証しているかわからりませんから、認証の対象を含めた言葉を使うべきだと日頃から申し上げています。NIST のガイドラインでは Verification を「肉体との紐づけ」という意味としてしまったため、署名の検証の意味で Verification が使えなくなってしまっています。
- 目次の順序については、いきなり脅威と対策を書くのではなく、先にプロセスの全体像を書くのはどうでしょうか。
- 現行のガイドラインで先に脅威と対策が書いてあったため、今回のガイドライン案でも脅威と対策を先に書いているのでしょうか。
- （事務局）現行のガイドラインでは、3 つのプロセスはガイドライン本編中に記載はなく、別冊に記載されています。今回、有識者会議を進めていく中で「脅威ベースでの対策基準の策定」が一つの大きなテーマでしたので、脅威をまず説明し、それに対抗するためのプロセスを説明しようと考えていました。
- 脅威から記載することには賛成です。ただ、いま事務局から説明された内容はガイドライン内にも明示したほうが良いのではないかと思います。また、3 つの各プロセス（Resolution、Validation、Verification）の関係性のサマリーも書いてあった方が望ましいと思います。
- （事務局）ご意見を受け、冒頭に概観図があるべきだと認識しました。ガイドラインには、他にも概観図を差し込むべき箇所があると思いますので、同様に見直しを実施したいと思います。
- 概観図を作成する際には、図中に脅威も記載することで読み手の理解が促されると思います。理解されることが重要だと思うので、記載の順番はどちらでも構わないと思います。
- 2.1.でも各構成要素の説明がされていますが、ガイドラインを読み進めているうちに、読み手は説明の内容を忘れてしまうこともありますので、3 章の各構成要素の箇所でも改めて目的や概要を記載しておくと、読み手の理解が進むと思います。
- 資料2の P27 に記されている最初のコメントの通りですが、身元確認でどのような目的のために何をする必要があるのかを示した方がよいと思います。また、本人確認全体の中で「身元確認」と呼ばれているのはどのプロセスなのかがわかるような図等があると、より理解が進むのではないかと思いました。
- リスク分析の方法として、「脅威」と「脆弱性」を挙げたうえで、それらに対する対策を検討することがありますが、今回のガイドラインをその手順を記載しても、必ずしも読み手にとって理解しやすいものにはならないと感じました。
- （事務局）ご指摘のとおりと考えており、現在の案では大まかな脅威のみを冒頭に記載しています。しかしながら、この方法ですと具体脅威を書ききれない部分もありますので、当人認証の同じ部分でコメントいただいた内容も踏まえ、改善を図りたいと考えます。

- 確認コードの送付を含め、郵送を使う場合の考慮事項については、今回の議論対象外となっている「身元確認に関する補足－郵送により身元確認を行う場合について」にまとめて記載する形でよいのではないかと思いました。
- 確認コードを使用した本人確認手法の手順は、世界ではある程度標準化されているのでしょうか。最近、私自身も検討したことがあったのですが、リスクやプロセスを丁寧に確認しないと、誤った使われ方をする可能性が高いと思いました。確認コードを送付することで認証する手法に関するナレッジが世の中にあるかについては、疑問があります。
- 一般の企業でも、確認コードを郵送で送っているという事例があります。
- それは恐らく、住所確認が目的ではあります。
- その点では、身元確認という言葉を使うとき、身元確認によって「何を確認したいのか」という観点が重要だと感じます。
- 確認コードの送付というのは、安易に番号を送ればいいということではない、ということを表記し、ミッションの確認とテーラリングが必要である、といった旨を記載する必要があるかと思います。
- 郵送の手段については、法律上の本人確認の効果の有無にも留意が必要です。例えば本人限定受取郵便は法令上に規定されていますが、そうではない民間のサービスは、行政手続における本人確認には使用できません。
- 法律上の規定はないかもしれないですが、ある民間企業で提供しているサービスは、郵便の本人限定受取郵便と同等であるとされていたりもします。本人限定受取郵便を使用できない場合に確認コードを使用する場合は、こうした点も考慮して相当工夫して使用しなければならず、そういった場合にテーラリングが重要となってきます。安易な書き方をすると確認が不十分な使い方をしてしまうので、慎重に記載する必要があると思いました。
- OpenID Connect for Identity Assurance を作成する際に、郵便に関する議論がありました。そこでは Secure Mail という抽象的な言葉を用いました。
- 外国であれば、普通郵便と法律文書を送ったりする Secure Mail とは別で記載をしていたりしますね。
- Secure Mail は日本の書留に近いものであり、トレーサビリティです。Secure Mail がどのような郵送方法を指すのかは国によって違う点は気をつけなければなりません。確認コードを送るだけの際は、属性情報としての住所に対する到達性確認を行っており、本人限定受取郵便は、身分証により Identity Verification を行うため、全く別の性質のものです。また、転送禁止を追加するべきか否か等含め、テーラリングをすることは極めて難しいと感じました。
- Mail という言葉は、電子メールと誤解されてしまう可能性にも留意が必要だと思いました。
- （事務局）現在の記載案では、いま議論いただいたような内容を盛り込めておりませんので、記載内容の拡充に加え、場合によっては確認コードの位置づけを変更することも検討したいと思います。
- 協議ポイント❷の「様々な要因によって強度に幅の生じる手法の解説について」は、記載自

体は必要だと考えますが、読者にとっては「ではどうすればいいのか」となってしまいます。明確な解がある訳ではありませんが、例えば NIST は「トレーニングの必要性」のようなことまでは書いています。このガイドラインでも画一的な記載は難しいとは思いますが、何らかの指針を書くところまでは踏み込んだ方が良いのではないかと思いコメントいたしました。

- いくらトレーニングを実施してもばらつきが出るというリスクがあるので、それが許容できないのであればデジタルな手法を利用したほうが良い、と記載することが望ましいのではないでしょうか。
- マイナンバーカードの真贋判定機のような例も出して、「様々な要因を排除するためのシステム化が大事である」ということを、ガイドライン内で明記することが望ましいと思います。
- まとめますと、踏み込んでトレーニングをしなければならないと書くのも意味がありますが、ばらつきが出てしまうリスクを許容できなければ、システム化をするべきだといったことも記載の必要があると思います。
- 「ばらつきが出てしまう」ということを、あらかじめ脅威として記載してしまうこともよいのではないでしょうか。
- マイナンバーカードには IC チップに券面情報や顔写真があり、厳格な本人確認が瞬時にできることは、誇りに思ってよいと思います。

議題(2)ガイドライン改定案の妥当性に関する論点協議

「3.2. 当人認証」

事務局より、資料 2 P31～51 に基づき「3.2. 当人認証」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）

- Authenticator を認証「情報」と訳すのは望ましくないと思います。データであると捉えられてしまう可能性があります。
- 「認証情報」だと「クレデンシャル」と捉えられて、Authenticator の持つ意味と異なる捉えられ方をされてしまう可能性もあります。
- 認証の三要素については、もはやこだわるべきではないという議論があるのは承知しています。新しい観点で認証要素を定義していくという動きもあります。そのうえで、今回、このガイドラインの読者を想定すると、いま認証の三要素を消すのはややアグレッシブすぎるのではないかと思いました。認証の三要素では、生体を使った認証があり、所持をすることが重要であり、所持をしていることが担保できればフィッシング攻撃に対してある程度有効な対策になりうる、ということがシンプルに説明できます。知識認証だけをいくら重ねてもフィッシングされてしまいます。早急に消さず、まだ使用していく方が良いと思います。
- 電子メールのワンタイムパスワードに関しては、電子メールをまだ大切に使用しているお客様もいらっしゃる現状を鑑みると、メールアドレスを所持と捉えている方もいらっしゃるのでは

ないかと思います。他方、問題なのは、攻撃者は、簡単に手に入れることができるメールアドレスやエイリアスを使用することです。その点から、メールアドレスが SMS と比較して所持の要素が希薄であるということは明確です。加えて、ワンタイムパスワードは所持ではなくフィッシングへの耐性がありません。メールアドレスを使用したワンタイムパスワードは、所持認証ではないとはっきり書く必要があると思います。

- 協議ポイント❹の「当人認証保証レベル 2A におけるフィッシング耐性要件について」は、NIST はまだドラフト段階でありますし、「必ず使用しなければならない」と強く主張する意図はございませんが、利用者に選択肢を与えるという点は積極的に進めていただきたいと考えています。昨今は攻撃も高度化しており、今までフィッシングで狙われていなかったところもフィッシングが狙われるようになってきていますので、フィッシングへの対策は強く進めていく方が望ましいのではないかと思っています。
- メールを使用したワンタイムパスワードを所持認証とみなさないとした場合、ブートストラップ問題をどうやって解決していくのかについて疑問があります。このガイドラインには Authenticator の登録プロセスの記載がないのですが、本来はそこに影響するのではないかと思っています。登録プロセスの記載をしたうえで、整合性が取れるかどうか検討が必要だと思います。
- 私の理解では、NIST における AAL2 の中で電子メールは物理的にバインドされていない、といったような記載は、あくまで AAL2 の中での意味づけだと認識しています。電子メールの所持性が希薄化しているため所有物とはみなさない、という記載は、少々アグレッシブではないかと思います。ただし、電子メールにアクセスする際の資格情報が結局は利用しようとしている知識要素と同じになってしまい、所有要素と知識要素が「互いに素」であるように運用すること・確認することは容易ではありません。リスクが違うということは事実なので、それが理解できるよう、レベル 2 プラスやレベル 2 マイナスといったような段階を表現できるのであれば、それぞれのリスクと合わせて記載することで許容できるのではないかと思います。
- 利用者が所有物としているメールアドレスを窃取して使う攻撃と、新しいメールアドレスを用意して攻撃を行う場合とは、区別して考える必要があります。SMS は電話番号のため契約をしないと入手できず発生しにくいがメールアドレスはそれに対して入手しやすいため、両方で考えることが大事であると考えます。
- 既存アカウントのテイクオーバーと、悪意を持った者によるアカウントの新規作成という 2 つのリスクシナリオがあることを、意図的かつ明示的に記載しなければ、読者は区別できないと思います。通常はアカウントのテイクオーバーのみを注目することが多いと思います。キャンペーンの応募等でよく使用されている、携帯電話アドレスを軸として複数アカウントの登録を防ぐといった方法はよくあると思います。他方、メールアドレスを利用したワンタイムパスワードは、悪意の有無はさておき、その人かどうかを確認するための手段として使用されることを想定しており、リスクはあるものの手段として記載しておくことでよいのではないでしょうか。
- そのリスクが受容できるかどうかは、ミッションによると思います。多くのシステムでマイナン

バーカードのような身元確認がしっかりとできるような本人確認書類が出てきた今、行政サービスの中で、そのようなリスクを受け入れられるような手続があるのか疑問に感じています。今回の改定のタイミングで区別をしていった方が、数年後の改定までの間の脅威に耐えることができるのではないでしょうか。

- アカウントの乗っ取りについては当人認証のプロセスで対策することには賛成ですが、悪意をもって複数のアカウントを新規に作成するという事象に対しては、身元確認のプロセスにおいて対策をすることで区別できるのではないでしょうか。
- 2.1.の身元確認の概要説明に、「手続やサービスを利用しようとする申請者に対し、申請者の属性情報を収集することで、申請者を一意に識別する」と記載があります。それに対し、フリーメールのようなものを利用し、複数のアカウントを作成できてしまうような状態は避けなければならないという記載は、必要になると考えます。
- 今の議論の中でも、「所持」という要素の中にたくさん意味が入っています。認証の三要素すべてを一括でなくしてしまうのではなく、所持の中でも Credential の複製可能性等といった細かい脅威をわけて取り扱う必要があると思います。Credential Management Phase の記載がないことは、NIST SP 800-63 の一つの特徴ですが、Credential Management Phase に関連する脅威と対策については「身元確認」の一部で扱うべき話題かと思います。
- NIST SP 800-63-4 2nd PD でいう Syncable Authenticator でも、所有の概念としてあるデバイスの中に情報を閉じ込めているということにこだわっていましたが、クラウドで同期されていても、クラウドが安全性を持っており、その所有者の中で共有されているのであれば、フィッシング耐性も確保でき、所持と同等であるとみなすことはできます。メールアドレスや SMS ワンタイムパスワードなどはあくまでも知識認証であり、所有物ではないというように理解したほうがシンプルではないかと思いました。
- メールアドレスの取得のコストが安すぎる、という点は、身元確認の Resolution のところに書くのはいかがでしょうか。「不十分な識別」の脅威に関するものだと思いますし、属性でしかないメアドで「識別」しようとするところに問題があるように思います。
- ガイドラインの読者を一般の行政官と想定したときに、このような細かい話を十分に理解してもらうことは難しいのではないかと思います。行政手続であれば、ある程度想定される手続きは限定されるのではないでしょうか。認証の三要素をこだわるのをやめるのと同時に手法も例示することで、リスクを低減できるのではないかと思いました。
- 例示を示した場合、テーラリングばかりとなってしまうことが想定されます。素人がテーラリングをやろうとすると、適切ではないテーラリングをしてしまうため、注意書き等をする必要があるのではないかと思います。
- 認証の三要素の中身が変わっていくことはあると思いますが、認証情報はそれぞれ独立しているように見えます。将来、軸の数が変わるかもしれませんが、現状では三要素を意識していただいたほうが良いのではないでしょうか。認証の三要素を意識しなくなった場合、二要素認証ではなく二段階認証のように一つだけで何とかしてしまおうとすることが考えられます。

行政手続も様々あるため、テーラリングは発生せざるを得ないのではないかと考えます。

- 昨年度の有識者会議において、実際に運用をするのは委託先の事業者であり、公務員はその監督を行うのであるといったような話を聞きました。
- Credential の発行の際のメールアドレスの確認は、当人認証ではなく、身元確認プロセスのうちの一つだと思います。身元確認の際に、どういう属性を集めなければならないかは、ミッションごとに異なってきます。まず、身元確認の際にどういった情報が必要になるかを決定するということが重要になると思います。
- メールアドレスにはグループアドレスがあり、1 エンティティに結び付いていない運用があるという点も課題になると思います。検出することが困難であり、ミッション遂行でそのリスクを許容できるかどうかを論点として記載しなければならないと思っています。
- 実務上では、電子メールを Activation Factor として使えないとすると、相当大きな問題が生じると思います。
- 実務的に、テーラリングのポイントを別冊で記載するなどしてはどうでしょうか。本編で全てを説明しきるのは無理があるように思えます。
- インシデントやテーラリングを組み合わせてリスクを記載し、実際にやる場合は気を付けるような注意を促す記載が良いと思います。
- アカウントリカバリーを弱くすると攻撃の起点になるため、気を付けなければならないと思います。一方、亡くなったときや自分で動作できないとき、意識を失っているとき等の場合、どうするべきかを行政サービスとしてどうするのかを検討しておく必要があると思います。本人以外が実施し、本人ではないことが明確に分かるようにしておくようにするといった対応が想定されます。
- NIST SP 800-63-4 2nd PD では、アカウントリカバリーとともに並置されて Authenticator の Binding も記載されていました。二要素となると、Post Enrollment Binding 等の整理も必要となると考えます。

<u>議題(2)ガイドライン改定案の妥当性に関する論点協議</u>

<u>「3.3. フェデレーション」</u>

事務局より、資料 2 P52～59 に基づき「3.3. フェデレーション」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）

- フェデレーションを一律の基準として記述することには賛成です。OpenID Connect や SAML を適切なプロファイルで活用すれば、適切な運用レベルになると思います。
- 私も、その意見に近いです。NIST の 3 つのレベルは結局のところ、CSRF が可能なレベル、CSRF が不可能なレベル、Holder-Binding がなされているレベルの 3 段階です。「CSRF が可能なレベル」は今更許容できるものではないため不要であると思います。Holder-Binding につ

いては（一般の手法では）実装不能なため、将来的に出てきたときに足せるようになっていればよいと思います。

- 無理やりレベルで分けする必要はないと思います。
- フェデレーションが侵入口になるケースは考えられるため、脅威を並べ、対策を記載しておくことに意味があると思います。
- フェデレーションを実際に運用する場合、スキルのある人員がトラストフレームワークを組んで対応することになると思いますので、あまり神経質にならなくてもよいのではないかと思います。
- 本当にスキルがあるのかというのは疑問に思います。SaaS も増えているため、見よう見まねで IdP を立てて繋ぐような場合もあり、多種多様です。

閉会

- （事務局）本日の会議は以上といたします。本日もお時間いただきありがとうございました。

（了）