【資料3】

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1回）
令和 5 年 10 月 31 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

（事務局）

- 昔からテクノロジーの進化によってビデオ会議のセットアップに必要な時間は短縮されていくのだろうと考えていましたが期待を裏切られてはや四半世紀が経ちます。古くて新しい問題なのだと感じています。会議のテーマである ID も同様に、マイナンバーカードの普及によって様々な問題が解決されるのだろうと簡単に考えていたこともありましたが、現在までに 9,000 万枚以上のカードが発行されている中で紐づけの問題や代理人の問題が顕在化している状況であり、ただクレデンシャルを発行すればよいというものではないのだと実感しています。このような問題は電子委任状の検討においても議論しているところですが、身元確認保証レベルや当人認証保証レベルの話も行政において 20 年近く検討を進め土台が整ってきた結果、利活用が増えていく中でエッジケースが発見され、諸外国においても多くの見直しの議論が必要となっている、非常に注目度の高い分野だと考えています。世の中で何が起こっているのか、どういったニーズが生まれてきているのか、テクノロジーとしてどのようなことが実現可能となっているのか、どこにギャップがあるのか、世界中の議論をしっかりとキャッチアップしつつ、我々自身が肌感・手触り感を持って検討を進めていかなければならないと感じています。引続きご指導のほどよろしくお願いします。
- 本日の会議の説明を行います。みなさま昨年に引続き会議にご参加いただきましてありがとうございます。今年度の会議では、資料及び議事録は Web 上にて公開させていただく予定です。また、今年度は全 5 回の開催を予定しています。現時点の計画として 2023 年内に 3 回

開催し論点の協議を行い、2024 年予定の 2 回の開催では当タスクフォースで用意した本人確認ガイドライン改定版のドラフトを基に議論を進めていただく予定です。2023 年内の 3 回の開催において協議予定の論点は資料 1 の開催要綱に掲載しています。今後のスケジュールといたしましては、今年度末までに本人確認ガイドライン改定版のドラフトを作成し、年度末に最終化される予定の NIST SP 800-63-4 の内容を次年度前半で取込み、みなさまと議論しながら改定版を最終化の上発行したいと考えています。

議題（2） ガイドライン改定に向けた論点協議

「論点 1. 身元確認保証レベルの見直し」について

事務局より、資料 2 に基づき論点 1-1～1-3 に対する現時点での方針を説明し、有識者による自由討議を行った。

（有識者意見）

- 事務局からの説明で身分証明書の盗難について話が出ましたが、NIST では身分証明書の貸し借りについても考慮しているのだと思います。国内においても身分証明書の貸し借りを考慮する場合に現在の方針のままでよいのか検討が必要と感じました。また、マイナンバーカードの初回発行や紛失時の再発行のプロセスのポリシーと、今回本人確認ガイドラインに定めようとしているポリシーとの関係性の整理がどうなっているのかが気になりました。再発行まで長い時間が必要な場合、その間に行政手続ができなくなると困ってしまうため、救済手段をどうするのかという点についてもガイドラインに記載されている必要があると感じます。NIST SP 800-63-4 でも、身分証明書がないことを理由に排除してはいけないといった趣旨の記載がありますので、その辺りの例外処理をどのように入れていくのか見解を伺いたいです。
- NIST IAL3 に揃えていくという大方針については問題ないと思います。ただ、現時点ですと NIST でいう Supervised Remote Identity Proofing というのが何を意味するのかということと、日本における ID エビデンスの相互運用性と米国における ID エビデンスの相互運用性は当然異なるものであるため、定義や相場観を煮詰めるところと並行してやっていく必要があると思っています。そうした理由から NIST IAL3 に揃えることを宣言したとしても本当にそれを実現できるのかという点については不透明であると考えており、議論を深めていかなければならないポイントだと思っています。
- 生体情報の比較の件については、Supervised Remote の場合に AAL2 か FAL2 でのデジタルアカウントで認証するというのも Verification の要件に含まれていたはずで、マイナンバーカードと PIN での認証は自身の登録済みのマイナンバーカードのアカウントにアクセスしたことを証明していることになるので NIST IAL3 に合致していると思います。ただ、先に出た話のようにマイナンバーカードの貸し借りが行われた際に PIN 情報も併せて共有されてしまうと、別人による認証も可能となってしまいます。生体情報の記録を必須化するという話もあることから、後から追跡を行う発見的統制は実現できるものの、予防的統制にはならないので、従来の行政の考え方と照らし合わせたときに許容できるのかというところは肌感として持っておくのが良いのだろうと思っています。
- そもそも身元確認保証レベルを 3 段階に固定して検討しないといけないのかという点につい

ては、議論の余地を残した方が良いのではないかと思います。弊社で作成した社内向けのデジタルアイデンティティガイドラインでは、NIST IAL の 3 段階を踏襲すべきか、という点について検討を重ねた結果、3 段階としました。運用は概ねうまくいっているものと思っていますが、厳格さを考慮したときに 3 段階のレベルに対してプラス・マイナスをつけた方が良いケースがあることを実感しています。本検討においては、身元確認保証レベル 3 を、一般の行政手続は該当しない非常に厳密なレベルとして定義する場合、実質的な保証レベルはレベル1と 2 の 2 段階となってしまいますので、例えば NIST IAL3 に相当する身元確認保証レベルを 3+のように追加で定義することも検討余地があるのではと思いました。

- 生体情報比較については、昨今民間では顔写真のない健康保険証などは身元確認書類として使用できなくなってきているという動向があります。身分証明書の貸し借りの問題も含めて、容貌の確認の必要性が理解されてきたと考えています。他方、マイナンバーカードの電子証明書と暗証番号による多要素認証によってリモートでの身元確認を行うことも現実的には有効だと考えており、実際に弊社のビジネスでも 2022 年 3 月から順次 JPKI を利用可能としたところ利用率が高まっていることを確認しています。ただ、やはり暗証番号を覚えていない方もいらっしゃいます。最近では、9 月より IC チップの存在と容貌確認での身元確認も開始しました。本人確認ガイドラインにおいて単に「生体情報比較を必須とはしない」としてしまうと「容貌の確認が必要ない」と捉えられてしまうと思いますので、貸し借りの話も含め、こうした考え方を積極的に推していく方向にはしない方がよいのではないかと思います。
- 登録コードの件についてはほかの意見もあまり出ていないので個別に議論する形でも良いと思いますが、個人的には意味はあると考えています。
- 論点 1-2 については、知識認証で検証された結果と容貌の確認を同列に扱うように見えてしまっているので、少し差はつけるべきではないかと思います。少なくとも Relying Party が何を利用して検証されたのかを確認できる状態を作っておくのが大事なのではないかと思いました。
- 生体認証について議論を進めると色々なハレーションが起きる可能性が高いため、どのように国民に知らしめていくかという点については慎重に進めていかなければならないだろうと感じています。もう一つは他人受入率（FAR）に関してですが、外国人の方で日本に住民票があってマイナンバーカードを持っている方を受け入れていこうとするとある程度許容率を上げていかないと難しくなってくるのではないかと思います。
- 将来的な海外との相互運用性などを考慮して NIST IAL3 に身元確認保証レベル 3 を合わせていくという点については賛成なのですが、2 年ほど前に DADC の場で民間の本人確認ガイドラインを検討した際、多くの手法がレベル 2 に集中してしまい細分化を行ったということがあったように、本来なら違うレベルのものが混ざってしまうのではないかという点について懸念しています。身元確認保証レベル 2 については知識認証が不可能な場合に生体認証を行うと読み取られてしまう可能性があるので、「公的個人認証または」のような記述にしてしまっても良いのではないかと思います。
- 別件として、現行の本人確認ガイドラインは「対面または遠隔」という記載がされていて、遠隔の中にオンラインの手続と郵送の手続が含まれていたと認識しているのですが、今回の資料には「リモート」や「デジタルエビデンス」という記載がされているので郵送の手続はベースラインから排除していくながれなのかをお聞きしたいと思いました。

- 私も身元確認保証レベル 2 の守備範囲が広くなることを懸念しています。改定後の本人確認ガイドラインを民間側で参照する場合、おそらく金融関連の手続の確認は全部レベル 2 になると思います。銀行口座の開設やクレジットカードの作成といったように様々な手続がレベル 2 に集中してしまう形になるので、本人確認ガイドラインが民間側でも参照されることを前提に置いた上で、民間側で参照する場合は身元確認保証レベルの細分化を適宜検討することを推奨するガイドを公開していただいた方が民間事業者としては受け取りやすいのではないかと感じました。
- 身元確認保証レベル 3 を厳格化することになると基本的に選択するレベルは 1 か 2 になり、リスク評価から必要な保証レベルを考えていくとなった場合に行政手続がレベル 2 の中に収まるのか、あるいはクライテリアが重要になるのでレベル 2 に振り分けることができるクライテリアを設定できるだろうかという点が気になっています。
- 身元確認保証レベルが実質的に 2 段階になってしまう可能性があるという点については問題だと思うのですが、日本は行政の集める情報が信頼のおけるものであり、かつレベル 2 も証明しやすいものとなっていたことから運用しやすいものであったと考えています。現時点であれば実質 2 段階でも問題ないようにも思われますが、将来的な日本の治安などを考慮すると少し柔軟に考えておかないといけないのかもしれません。現在政府機関でマイナンバーカードが職員認証に使用されていますが、身元確認保証レベル 3 はそれとは別の米国の PIV と同等のものを運用するという覚悟の問題だと思っているのですが認識は合っているでしょうか。
- 登録コードの話については、メールアドレスが使われるというのがレベル 1 とレベル 2 のギャップになるのではないかと思います。若い世代の方々は郵便や電話ではなくメールで登録コードを利用するのでこれはやはり差があるのではないかと思います。
- 日本では 2 段階でも良いのではないかという点については、外国人の方が大勢日本にいらっしゃるようになっており犯罪の手口が複雑化していることを考えると、性善説に立ちきれないところがあるなというのは感じています。利用者がどの国の出身であるかということによる差別は絶対にあってはならないものであり、公平性や厳格さをもって保証レベルを定義できると良いと考えます。
- メールアドレスについては、エイリアスや Gmail の問題を利用することで巧妙に攻撃を仕掛けてくるようなケースも発生しているので、メールアドレスの所持についても慎重に判断した方が良いのではないかと考えています。メールを受信できることと SMS を受信できることは区別されるべきとの指摘があり、実際そのように運用している事業者があることについても認識しています。
- 保証レベルについては、過去に保証レベルが 4 段階あった時代でもレベル 2 マイナスやレベル 1.5 が必要ではないかという議論がされていたこともあるので、今回さらに実質的ではあるが 2 段階にしてしまうと保証レベルに対する解像度はさらに落ちてしまうと思います。日本の現状に即してという話をすると、NIST SP 800-63-4 内でもテーラリングについての記載が多く確認できるので、それをどう考えるかという点も意識していく必要があるように思います。
- 生体認証を必須としなくても良いのではないかという点についてはこういう脅威に対応するからこうだ、というのを整理していただいた方が納得しやすいように思います。盗難ということで考えるとカバーされていますが貸借のことを考えるとカバーできていません。特殊詐欺も身分

証明書の貸し借りに該当する事例と考えています。

- 登録コードについては手段に対して信頼性のグラデーションが当然あるものなので区別が必要なのだろうというのは認識のとおりです。昨年度の会議ではなるべく下位のレベルを厚めに定義した方がよいのではないか、身元確認保証レベル 0 に対し高レベルの当人認証保証レベルを組み合わせることで対応することも一案なのではないか、とお話しさせていただきました。登録コードについては身元確認保証レベルの観点のみで妥当性を判断するのは難しいのではないかと思います。下位レベルでは差があまりなくなってくるのではないかと。レベル 2 に該当するケースが非常に多くなるのはそのとおりで、レベル 2 の中でも下位のものについては本人確認保証レベルのみで日本国内の行政手続を行う上での信頼性を担保できているものではなくなってきていると思いますので、レベル1を厚めに定義して当人認証保証レベルと組み合わせてリスクに対応する方向性に導くことができると良いのではないかと思います。
- 登録コードについては下位のレベルの対策基準のバリエーションを豊富にすることによってそれがどのようなユースケースに活用されコストカットなどに繋がるのかがあまり想像できませんでした。
- レベル 1 の登録コードについて事業者目線で考えてみると、身分証明書を撮影した画像をメールに添付する、あるいは Web サイトにアップロードするといったことだと想像しています。登録コードがレベル 1 に追加された場合、現在運用されているこれらの手順をレベル 1 に該当させるために改修が発生するのではないかと思いました。登録コードについては住所への通知が無難だと思いながらも今後登録コード以外の様々な通知をしていくことを考えたときには、例えば携帯電話番号などの情報を取り込んで連絡先としても利用していくのは有意義なのではないかと思いました。
- 大学での例を紹介すると、大学では二要素認証の導入が始まったところなのですが携帯電話番号の登録を行っているものの自己申告のみでベリファイしていないという実態があります。そうした場合、登録された携帯電話番号は登録コードとしては扱えないものとなってしまうのですが、意外と運用はうまくいっているので、携帯電話番号を登録コードとして扱うことは妥当性があると考えています。この話は当人認証保証レベルの話ではありますが、身元確認保証レベルにおいてもレベル 1 とレベル 2 で採用可能な登録コードは別のものにしておくのがよいのではというのが私の考えです。
- 身元確認保証レベル 1 を厚くするという話はそのとおりかなと思います。以前は NIST IAL1と NIST IAL2 だったものがくっついて NIST IAL0 が今回なくなっているので、NIST IAL1 は実態として裾野が広くなっているのがアメリカの動向としてあると理解しています。
- 登録コードについて、申請者と連絡がついてそれぞれの連絡手段ごとに、例えばメールであれば 24 時間、住所に対する郵送であれば一定のまとまった期間のように、有効期間の長さを変えてコントロールしようとしているコンセプトについては良いと思います。ただ、SMS を受信できることとメールを受信できることは Authentication の観点で異なることであるので、当人認証の手段として SMS を利用することは区別して考えると良いと思います。身元確認手段としてはバリエーションがあっても良いと思いますが、当人認証の手段としてはより深い考慮が必要だと感じています。
- 対策基準項目の各項目に対してそれぞれの保証レベルに求められる基準が記載されていま

すが、これらは実態としては想定されるリスクに対し対策基準として定義された確認方法を経ることによってリスクが低減され、結果としてこれくらいのことが達成できていれば NIST xAL はいくつである、というような検討がされた結果となるので、日本においてテーラリングするときは NIST が提示している対策基準項目に囚われすぎると正確性が低下し納得感が伴わない結果となるため、リスクが何であるかという観点で分解して考えるのが必要だと思います。現行ガイドラインの対策基準にも記載があったと思いますが、存在性、生存性、一意性といった観点も取り入れて、写真付きの身分証を使用した場合には生存性の査証に対してどうであるか、といったような明細に裏付けられた議論が必要になってくるのだろうと考えています。

- 登録コードに話が戻りますが、日本では特定郵便のような住所を確認するプラスアルファの仕組みがあり、住所に対して登録コードを郵送して提示したから身元確認保証レベル 1 であるという話とは別軸だと思うので、登録コードの提示に加えて訓練された配達員がチェックをすることで身元確認保証レベル 2 とする、といったような調整も考えられるのではないかと思いました。
- 論点設定を壊してしまう可能性があるのでその場合は指摘いただきたいのですが、本日身元確認保証レベル 3 を NIST IAL3 基準に合わせると求められる対策基準が高すぎて多くの手続がレベル 2 に集中してしまうことについて色々と議論がされ、またレベル 2 はオンラインでの身元確認時の生体情報比較の必要性の話が中心となっていました。行政における身元確認がどのようなシーンで発生するかを考えた場合に、NIST IAL3 レベルの確認が求められるのは極めて特殊・限定的なケースとのことでした。今後より多くの国民が求められるオンラインでの身元確認をするときに前提となっている現行マイナンバーカードや次期マイナンバーカードがどのように成り立っているかというと、現状役所に行って住民基本台帳を参照するレベルの身元確認が行われています。ここでどういうレベルの身元確認が行われているかが重要になってくるのではないかと以前より感じていました。もしマイナンバーカード発行時の身元確認を一定のレベルで確実に実施することになれば、マイナンバーカードを利用した本人確認の品質が高くなってくるので、本日対象となる論点には入っていませんが、行政機関における対面での本人確認がどうあるべきか、という点は重要だと思います。
- 対面確認でもなりすましの問題があって、店頭でも提出された身分証明書に対する真贋判定を行うことで効果が上がっている事例があることを認識しています。ただし、その真贋判定すらすり抜けるような方法を考えるような犯罪グループも存在することから単純ではないのですが、対面の身元確認をあるレベルに昇華させると、少なくともそれ以降の現行・次期マイナンバーカードあるいはスマートフォンに搭載したそれらの役割を果たせるものが非常に効果的にオンラインで役割を果たすと思いますので、身元確認保証レベルや当人認証保証レベルも大事なのですが、身元確認の根幹の部分、別のテクノロジーでいうとエンドポイントのような言い方をしますが、そこをしっかりと実施することがその後のトラストチェーンになると思いますので、本日の論点には含まれていませんでしたがとても重要なことであると考え発言しました。
- 事務局からの説明で、本人確認ガイドラインのタイトルの変更を検討しているということでしたが、現行の 2019 年に発行された本人確認ガイドラインは個人と法人両方の本人確認が対象として記載されていると認識しています。しかし少なくとも本日の議論の対象は個人に対する本人確認のみとなっています。今後どこかの場で法人に対する本人確認の議論がされる予

定なのでしょうか。それとも法人に対する本人確認は本人確認ガイドラインのスコープから外れる予定なのでしょうか。参考情報となりますが、Trusted Web の中に法人に対する身元確認のユースケース検討や実証実験を行っている事業者がありますので、そういったところと連携してうまく結果を利用されるのも有益なのではないかと思いました。

- NIST は SP 800-63-3 でガイドラインを徹底したことで行政サービスから住民を排除してしまったケースが発生してしまったことについて、決して起きてはならないことであったと強く反省しており、SP 800-63-4 の説明会などでは今後そうした事態が発生しないようにテーラリングするべきであると強調しています。残念ながらテーラリングは米国内でもなかなかうまくいっていないのですが。必要以上に対策基準を厳しくしてしまうとそれが金科玉条のようになって排除されてしまうということが起きかねません。これは海外ではよく発生していることであり、例えばウガンダでは、緊急に医療が必要とされる状態にもかかわらず国民 ID カードが未取得であったことを理由に医療を受けることができなかったという事例が報告されています。行政サービスというのは懐の広さが要求されるので、それをどのようにして文書の中に取り込んで人々が読めるようにするのかが重要なのだと思います。
- SP-800-63-3 から SP-800-63-4 に対する変化の中で私が特に印象的だったのは、かなり複雑な構成となっていたフローチャートがなくなったという点です。フローチャートがなくなったことによりそれぞれ自分たちで検討をしなければならなくなりました。ガイドラインにあまり細かく記載すると本当に必要なニーズに応えられないからという、そうしたコンセプトがあるのだと思います。
- 私はフローチャートがなくなったことについて方向性としては正しいと思っていて、リスク評価はフローチャートでやることではないと理解しています。フローチャートの存在に有難みを感じている方も、実際にフローチャートを利用する際に結局きちんとリスク評価をしなければならないということに気が付くはずです。リスク評価が正しく行えている場合はフローチャートに従うことで必要な保証レベルが決定されると思いますが、事業に対する影響度について何がそれぞれ重大・中・低に該当するのかという話になってくるので最終的にはそこに問題が棚上げされているのだと思います。
- 元々NIST SP 800-63 が政府職員向けであったということはその通りだと思っていて、その名残として一職員の PIV が盗難された場合のクレデンシャルの複製のようなリスクをすごく重みのあるものとしており、それが IAL3 となっています。想定しているシステムのリスクが、ある Authenticator が盗難された場合にその権限でアクセスが可能な様々な国民のデータに水平的に広がりがあるからというふうに私は認識しています。government-to-citizen のようなサービスになってくると、基本的には影響範囲は特定ユーザのスコープに閉じると考えており、この両者をきちんと想像しながら身元確認保証レベルを 3 に設定すべきサービスなのか、もしくはレベル 2 で問題ないサービスなのかというようにリスクをマッピングしてこのサービスはどの要求レベルにするのかというところに収束させていくと収まりが良いのではないかと考えています。共通認識を構築するために、身元確認保証レベル 3 が要求されるのが具体的にはどのようなシステムなのかということを一度きちんと考えてみることが重要なのではないかと思います。
- 私を含め複数の委員の方から繰り返し発言があったものとなりますが、手段を基準に検討を進めることも良いのですが、どの脅威に対応しているのかをきちんと示してあげられるガイド

ラインになると良いのかなと思います。様々なユースケースについてその脅威は考慮する必要がないというようなことはたくさんあると思いますし、柔軟な対応が可能となることで住民をサービスから排除することがなくなる、テーラリングが容易になる、などのメリットも多く存在するはずなので、是非検討いただきたいと思います。同様のことを NIST SP 800-63-4 にもコメントしていたりします。

- あとは、当初から例外処理をきちんと考える、これはぜひ入れていただきたいです。今回かなりマイナンバーカードセントリックになっていて、それはそれでいいと思いますが、マイナンバーカードを紛失した場合どのように対処するのか、そういった点を読み取りやすいように記載していただければと思います。
- 登録コードのところは認証強度が違うので郵送とその他の手段をしっかり区別しなければならないという点と、郵送の中でも特定郵便については一定の強度が保てるのではないかという話であったと理解していますので、補足させていただきます。
- 脅威ベースにすればそれがきちんと出てくるはずです。特定郵便を採用することで色々な脅威が消えているはずなので。
- すごく広がる話で N 対 N 対 N のような形になってまとめるのが大変そうな内容ではありますが、そのとおりだと思います。

<u>その他の議論：ガイドラインと保証レベルの意義について</u>

- 弊社では、社内向けのガイドラインができたことによって明らかにリスク対策のレベルが上がりました。身元確認保証レベルもそうですし、この後の論点になっている当人認証保証レベルの方はなおさらです。この会議のように有識者で集まると本質的にそこではないですよねと議論になりますが、実際に実装していく立場で考えると、やはり共通言語として使える保証レベルを設定しておいた方が対応を進めやすいです。SP 800-63-4 でフローチャートがなくなった一方、弊社内ではガイドラインのフローチャートをもう少し細かくしてほしいとの要望が上がりました。このようにガイドラインの整備・改定を行う際には、それを実際使う側の立場になって考えることが必要だと感じています。
- 大学においても同様のことが起きていて、脅威を列挙してそれを一つずつ潰していく、つまりは高度なレベルの知的対応をできる人がなかなかいないという問題があります。それでも一定のレベルは維持しないといけないので、ガイドラインで示してこれをやっておけば大丈夫という状態にして、少しずつオペレーションのレベルを上げるしかないと考えています。そういった意味では、技術的な選択肢が増えたのであまり意味がないことだとしても、現場で対応する人々にとっては考え方をガイドする意味はいまだに大きいと思います。生徒に色々とやってくださいと頼む側からするとそれはひしひしと感じることです。
- 説明においても評価においてもそのためのフレームワークがないと対応がし辛い部分があります。何かしらあった方が便利なのだろうとは思います。とはいえそこで閉じてしまってはいけないということも併せて伝える必要はあると思いますが。
- 民間であれば、例えばあるサービスで問題が起こった場合の損害額やビジネス影響等で基準を設け、それをなぞっていって高が一つでもあったら〇〇だ、というようなフレームワークが比較的作りやすいと思います。行政の場合だと置かれている立場も違うため難しいとは思い

ますが。

- リスクに関して、きちんとリスク評価を行った上で対応を進めていくべきだという意見にはもちろん賛成なのですが、現在の NIST SP 800-63-4 におけるリスクの定義はかなり大雑把なものになっていると感じています。ガイドラインをベースにして設計をしていく場合に、リスクについて人命に関わるものであるか、といったような基準で評価をしていくと、一か所に固まってしまうことが多いです。リスクベースで対応するのであれば行政手続におけるリスクというものをどこまで精緻に定義できるのかというところに懸かってくると思います。
- フローチャートの話でいうと、共通言語としてあった方がいいというのはある一方で、それに縛られすぎてしまうという意見があるのも事実だと思っていて、個人的な意見として SP 800-63-3 のフローチャートの一番よくなかったところは全部 Yes/No のバイナリにしてしまったところだと思っていて、先の話にもあった例外を作らないといけないという点を考慮したフローチャートがもし完成するとすれば有用なのではないかと思います。

「論点 2. 当人認証保証レベルの見直し」について

事務局より、資料 2 に基づき論点 2-1 に関する現時点での方針を説明し、有識者による自由討議を行った。

（有識者意見）

- フィッシング耐性については長年携わってきているので私から提案できることがあると思っています。弊社では、あるサービスサイトに対して、実際にフィッシング耐性のある認証に限定することによって、お客様からの「身に覚えがない取引がされている」というような問い合わせがなくなったという実績があります。きわめて自信を持てる結果となっていて、全体として被害額も減りました。サービスをご利用いただくために必要な認証にフィッシング耐性があるということは、国民が安心して生活を送るためにものすごく重要なことであると考えています。先ほど本人確認ガイドラインの身元確認保証レベル 3 を NIST IAL3 相当にするという話もありましたが、当人認証保証レベルの定義についても調整の余地があるのであれば、フィッシング耐性があるまたはそれに近い状態のもの、13 ページの表でいうとフィッシング耐性なしだがアウトバウンドのところまでで線を引いて、強く推奨することは実行上非常に意味のあることだと理解しています。
- 私はフィッシング耐性については必須とすることはなかなか難しいと思いつつ、レベル 2 で選択可能な認証方法に対して推奨する度合いの強弱は明らかにつけた方が良いと思っています。1 万人にメールを送ってそのうちの 1 人から 10 万円を受け取れれば経済合理性がはたらくタイプの攻撃と、1 人の政府職員の PIV カードのトークンを盗んで複製されるリスクとでは想定しているものの性質が全然違うので、今はオンラインで不特定多数の人々向けの攻撃方法がある以上重要度が高まっているのは相違ありません。基本的には資料にまとめていただいたとおりで問題ないと思います。
- 一方、フィッシング耐性のないワンタイムパスワード認証を例にとっても、そもそも多要素認証をやっている・やっていないことの間には大きな差があると認識しています。攻撃を受けた際の影響を更にゼロに近づけていく効果に差はあるものの、多要素認証を行うところまで持ち

上げる選択肢を狭めすぎると逆に使いにくくなる、あるいはやめてしまおうという方向に進んでしまうことを少し懸念しているので、選択肢としては残しておくのが良いと思います。

- 自治体のアドバイザリーも務めている中で、なかなかこの多要素認証なりフィッシング耐性を実現するためのできるだけ簡素な方法であっても、例えば当人認証保証レベル 2 に必須ですとなってくると自治体としては選びづらい、自治体職員は、住民と直接接しておりやはりユーザが見えているので作るのも受け入れてもらうのもハードルが上がってしまうな、となってしまう気がします。かといってはずすことは難しいと思うので、世の受容がどう進んでいくかを読まないといけないと思いました。
- 二段階認証は本当に簡単に突破されてしまうので、二段階認証とそうでないものとの線は大切にしていただけたらと思います。また資料内にパスワード＋SMS 認証コードというのはありますがメールでワンタイムパスワードを受け取るものが記載されていません。これは差がありますよね、良し悪しがありますけど、メニューとしてはどちらかというと両方準備しておくのがよいと思います。

<u>その他の議論：ガイドラインにおける脅威や手法の記載粒度について</u>

- 脅威は変化しますが、現時点で分かっている脅威を明示的に記載することは躊躇せず行うべきだと思います。推奨の度合いに変化を持たせる以上、推奨しにくいものと強く推奨するものとの理由づけがないと利用者には伝わらないと思います。採用すべきではないということが記載されているものについてはどういう脅威があって、それが時間の変化とともに発生確率が上がってきて一般的になってきたらもうそれは使えないと思ってください、と書いておくことでそのドキュメントの有効期限を文字面上は伸ばすことができるのではと思います。NIST も SMS を Restricted としてメッセージを伝えつつも選択肢として残しており、うまい方法だなと思いましたし、そう記載せざるを得なかったのだろうなと感じます。
- フィッシング対策協議会が発行しているフィッシング対策ガイドラインでは「利用者にメールを送る際の注意点」、「フィッシングが発生してしまった場合の対応」等、前後の対策を含めて示されています。レベル2でフィッシング耐性を必須にできないのであればこういったところを参考にすればよい、というところはヒントになると思いました。

<u>閉会・次回案内</u>

（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 11 月 16 日（木）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）