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1回）
令和 6 年 9 月 17 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）
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）

開会挨拶

（事務局）

- 有識者会議も 3 年目に入りました。有識者の皆様には毎年お力添えをいただきありがとうございます。NIST SP 800-63-4 2nd public draft が発出され、この有識者会議も今年度で最終年度となる予定です。
- ガイドラインの改定案ですが、まずは、ページ数をなるべく少なくしたいと考えています。本ガイドラインはページ数が多い必要はないと感じています。わかりやすい図表を用い、機械翻訳できるようなわかりやすい日本語で書きたいと考えています。シンプルな日本語で書くことで、翻訳しやすくし、様々な国の方に読んでいただけるようになります。また、目次より前の部分に、「保証レベルは高ければ高いほど良いわけではない」という旨を記載したいと考えています。目次以降を読む率は少ないため、最低限読んでほしい内容を記載したいと考えています。標準技術の採用についても、官民連携を視野に入れているため、行政機関固有の部分とそうではない箇所の記載を明確に区別できるような記載にしたいと考えています。Acknowledgement（謝辞）の項目を入れたいと考えています。今までのガイドラインではありませんでしたが、希望を取ったうえで、コメント出しなどで貢献いただいた方を記載したいです。

また、ページ数の削減のため、必要に応じて別冊の作成も検討しています。以上のような点に気を付けながら作成したいと考えます。

- 昨年度に引き続き、それぞれに深い見識をお持ちのメンバーでご参集いただきありがとうございます。本人確認についてはここ数年で FIDO やパスキーの登場など環境の急速な変化や、様々な攻撃があることは理解していましたが、世間からここまで注目が浴びるものになるとは考えていませんでした。SP 800-63-4 2nd public draft (2pd)は発表が予定より遅れましたが、63-4 をキャッチアップするとともに、これからの 5-10 年を見据えた議論をしたいと考えています。日本のルールを決めていくだけでなく、世界が悩んでいることに貢献していくような議論を期待しています。

議題(1)開催要綱説明

事務局より、資料 1 に基づき本有識者会議の開催要綱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

事務局より、資料 2 に基づき本日の論点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)

- 「❸ Identity Proofing Roles / Types」についてですが、Proofing Agent が、ID ドキュメントの真正性を判断するときに何をしなければならないか、また Agent に対しても訓練をする必要性が記載されています。おそらく、ガイドラインを使う方々に対して、どのような攻撃があったかをある程度例示をする必要があるのではないかと感じています。
- 実際に起こりうる、もしくは、過去に起こった攻撃方法等を例示するというイメージでしょうか。
- はい。機械的な真贋判定を実施するのであれば必要はないですが、IC チップの読み取りが普及していない中、手元で物理的な券面を見る場合に何を確認すればよいのかを例示するものがあると望ましいのではないでしょうか。海外では、ID ドキュメントの確認担当者に対して、どのような攻撃がありうるかを教育しているという話があります。
- ❺の AAL2 のフィッシング耐性については、事業者の立場からも、フィッシング攻撃については避けることができない議題であると感じています。一方で、金融機関等でも財務事情によっては改めて FIDO・パスキーをこれから導入することが難しい可能性もあるのではないかと感じています。要件として書き込むことは必要だと感じていますが、現実問題として、事業者はフィッシングに対して、どこまで対応するのが良いのかは、懸念として残っています。
- また、フィッシングを防ぐ策を導入すると、異なる箇所での攻撃が発生することが想定され

ます。特にアカウントリカバリにおいて、攻撃が発生するのではないかと懸念しています。

- NIST のセミナーにおいては、知り合い 3 人が保証した場合にアカウントリカバリができるという手法が明示されていましたが、Facebook は過去にその手法を廃止しました。それは、その手法を使用し、攻撃が発生したからだと推察しています。そうした点には留意が必要かと考えています。
- コードを友達 3 人に送り、それを使用しアカウントリカバリをするということであれば、その認証レベルに落ちてしまいます。アカウント登録とアカウントリカバリの間で認証レベルの整合性が取れていないことが問題だと感じています。
- 2pd で AAL ごとにアカウントリカバリの手法を記載が記載されていました。保証レベルごとにアカウントリカバリの方法を考えようというスタンスはとても良いと感じます。内容を参考にしつつ推奨する手法を記載することを検討してもよいと感じています。
- 「❹ IAL1 の刷新と IAL2 の見直し」についてですが、IAL について、IAL1 は Fair Evidence 1点で認証が可能だとされていますが、Fair Evidence に求められている要件が強化されており、必ずしも IAL1 でこれほどの情報を取る必要性はないのではないかと感じています。
- 私も同感です。initial public draft（ipd）では、以前申請を受けた人物と同一人物であれば、コア属性を含めて Verification する必要がない場合を、IAL0 としていました。本人確認ガイドラインでは、あえて追随せず、IAL0 を残しておいた方が良いのではないでしょうか。
- 2pd では IAL0 の言葉自体は削除されていますが、文章内に埋め込まれており、気が付かない可能性が高いのではないかと考えます。行政分野は IAL1 以上からのみ使われることが想定されますが、民間からも参照されることを考慮し、読み手にわかりやすい記載をしたほうが良いのではないでしょうか。
- 日本において使用される ID ドキュメントを念頭に置いて進める方が、日本の現状に合った分類が可能になるのではないでしょうか。
- 同感です。日本と違い、米国では本人確認に使用できない ID ドキュメントが多くなっています。そのため、IAL のレベル分けについては、米国に追従する必要がないと考えます。日本においては、マイナンバーカードを所持していない国民に対し、どのように本人確認を実施していくのかを検討することは適切なのではないかと考えます。
- IAL は今回の改定で、我が国に取り込みやすくなったのではないかと感じています。改定前は、IAL3 に求められる Evidence は、Superior Evidence 2 枚が必要であり、誰も実現できない状態でした。その状態を是正するために、Superior Evidence 1 枚に修正されました。それに応じて、IAL2 と IAL3 の差別化を行うために、IAL1・IAL2 がそれぞれ修正されたという経緯かと思っております。
- 2pd では Fair Evidence として写真付きの Evidence を or 条件として記載されていますが、日本においては、例えば住民票の写しが相当するかを議論していくイメージです。住民票は、物理対策はある程度あり、リファレンス番号もあり、顔写真は記載されていませんが、問い合わせをすればある程度の確認が可能です。このように、実際に使用できる ID ドキュ

メントを考えながら、検討していくとよいのではないでしょうか。

- Fair Evidence について、先週ワシントン D.C.で TSA と会話した際に確認したところ、難民に対し UNHCR が発行している証明書は、NIST の基準では IAL2 に該当するのではないかと聞きました。Equity の観点からネイティブアメリカンに対して発行している、Tribal Certificate を IAL2 とせざるを得なかったからとのことです。UNHCR が発行している証明書は Core Attribute の Verification ができていない状態なのではないかという矛盾が生じているように感じますが、これは米国の事情であり、今回は置いておきます。これらの整理が、日本においては、マイナンバーカードを所持していない国民に対し、どのように本人確認を実施していくのかの手掛かりになるのではないかと感じています。
- 想定すべきケースとして、例えば、運転免許証の返納後に顔写真付きの本人確認書類を何も持っていない状態の国民などが考えられます。
- 運転経歴証明書は、運転免許証返納時に受け取ることができますが、運転免許証と同等と考えられますか。
- 運転経歴証明書は、顔写真の記載はありますが、IC チップが搭載されていません。
- 健康保険証の資格確認書についても考慮が必要です。運転経歴証明書の IC チップについてはそのとおりです。
- 技術的な話だけをすれば、レーザーエングレービングで陰影をつけている IC カードの券面偽造はそれなりに難しいはずですが、そうでない IC カードでは、アセトンなどで券面の印刷を除去し、熱転写プリンタを使用して再印刷すれば、券面偽造は可能であるということを考慮に入れる必要があります。
- アカウントリカバリの件についてですが、災害発生時にどこまで確認すべきか、といった点については議論したことがあります。NIST には、そのあたりの記載はないのでしょうか。
- NIST には、アカウントリカバリの手段は記載されていますが、そのリスクについては記載されていません。
- 容貌の確認を厳密に実施することは、日本では心理的な障壁も大きいと感じます。機械がアラートを発するだけであれば、大きな問題は発生しませんが、本人確認書類の写真と顔をじっくり見比べて、本人かどうかを厳密に確認する作業を実施することは、依頼しにくいと感じます。
- 国のガイドラインとして、容貌の確認の際に「マスクを外すこと」等を記載すれば、現場の職員は容貌の確認を実施しやすくなるということはありますか。
- プライバシーや人権問題の考慮も必要ですが、事業者としては、ガイドラインに容貌を確認する旨の記載があれば、オペレーションがしやすくなります。
- リスク管理の考え方として、例えば「マスクを外す」などの正規のプロセスを経ていないアカウントについては、高リスクアカウントとして識別する必要があるのではないでしょうか。
- 疑わしき場合には、機械を通したり担当者とテレビ電話でつないだり、といったリスク対応のプロセスは、世の中に似たようなプロセスが色々あると思います。

- 2pd においては、Proofing Agent や Trusted Referee についても記載が多くありましたが、Applicant Reference の記載も多くありました。これらに関する例外対応も書かれていましたので、本人確認ガイドラインにも反映する必要があるのではないかと感じました。
- Applicant Reference は重要ですよね。特に災害対応の場合に必要になってくると感じています。
- 2pd では、Applicant Reference に関するロールが整理されたことは大きな変更点であると認識しています。ただし、今までの本人確認ガイドラインでは要求していないことですので、どのように本人確認ガイドラインへ反映させていくかを考えなければならないと思っております。また、それぞれのロールは、トレーニングも含めて用意しないと達成できないものであると考えています。
- Process Assistant については、あまり議論されていませんよね。
- ミッションデリバリーを実現するためには、Trusted Referee や Applicant Reference を定義しないと達成しえません。Applicant Reference が悪意のある者と結託した場合、何でもできてしまうので、どのようにガイドラインに落とし込むかは難易度が高いと考えます。
- 昔の話ですが、カナダでは Applicant Reference は公務員が担っていました。
- 学校がすべて公立の国家の場合は、先生が全員公務員になります。また、医療システムがすべて国立の国家の場合はかかりつけ医が公務員となるため、そうした国では実施しやすくなるのかもしれません。
- ドイツの場合は郵便局員が該当すると考えられます。Trusted Referee が事業者の場合はどのようにトレーニングするかが問題となると思いますが、なかなか実現のイメージができていません。
- 2pd では、業界の中でよく議論されているものから、議論が未成熟なものまでさまざま記載が追加・修正されている認識ですが、❷Risk Management の見直しや❸Identity Proofing Roles/Types はどの定義議論されてはいってきたものなのでしょうか。
- 少なくとも、❸Identity Proofing Roles/Types の Trusted Referee は ipd のころから記載がありました。今回の改定で一定の議論がなされ、記載がより洗練された印象です。
- ipd では、Trusted Referee は Proofing Agent の一種であり、同一の人物が担当してもよい、というような書き方でした。
- ipd では、Trusted Referee は Agent の役割の一つであると書かれていました。
- 2pd のように明確に Roles ごとに定義して記載することは、事業者としてはやることが明確になり、とても良いと考えます。
- 64-3 の際は、最後 FAQ に「議論の余地がある」と明記されており、IAL と AAL を区別して記載したことは、これから意義を見出していくという記載がありました。DS-500 をまとめていくにあたっても、ややチャレンジングだがこれから検討していくような内容を盛り込む意義もあるのではないでしょうか。
- 特にウォレットモデルに関しては、全く未熟な状態のものだと思います。

- その意味では、いつの時点でガイドラインの改定をするか、というスケジュールを前提として議論しないといけない認識です。民間での参照については問題ありませんが、行政官はガイドラインの内容を遵守しなければなりませんので、（チャレンジングな内容を盛り込むなら）その考慮が必要です。特に、ウォレットに関しては、デジタル庁では様々な議論が行われていることは認識していますが、世の中の実装がどうなのかという点も考慮が必要かと思います。
- 当初の見通しでは、63-4 の Final 版が早めに発出されると考えていましたが、見通しよりも大幅に遅れている状況となっています。NIST のスケジュールに依存しすぎず、ガイドラインの改定を進めていかなければならないと考えています。私たちが NIST のスケジュールに振り回されているように、この本人確認ガイドラインの改定スケジュールに影響を受ける人たちも多いと思います。また、例えば作成中のものを公開してプルリクエストを受け付けるとか、そういったことも検討すべきだと考えています。
- 本人確認ガイドラインの改定は今後もずっと必要になるため、いつ改定するのかだけでも方針を決めていくといいのではないでしょうか。
- その意味では、カード代替電磁的記録関連の法令改正等も控えていることも考慮すると、DS-500 を分冊化するなどしてモジュラー化し、SP 800-63-4 と関係なく早めに改定版を公開することも検討が必要だと考えています。
- デジタル庁として認識している課題を取り入れる方が、NIST から出てくるものを随時取り入れるかどうかを検討するよりも重要なのではないでしょうか。
- この短期間で 2pd の変更点を取りまとめていることには感心しましたが、ウォレットに関する内容が資料 3 ページ目の❶、❻、❼のように多く含まれている点には率直に少し驚きました。昨年度の議論では、ウォレットモデルは別枠として考えてもよいのでは、といった議論もあったはずですので、ここまで踏み込んで本人確認ガイドラインへの反映を検討する必要があるのか、という点については少し疑問があります。
- ❺の AAL2 のフィッシング耐性要件強化については、立場上バイアスがかかって聞こえるかもしれませんが、二段階認証でもフィッシング被害は防げず、多くの被害が発生しています。しかし昨年度もお伝えしましたとおり、FIDO を必須にした結果、被害の発生を抑えることができている例が複数あります。実装が難しいという話もありましたが、国民を被害から守るという観点からは、IAL2 でフィッシング耐性の選択肢を提供するという NIST の改定は英断だと思っており、本人確認ガイドラインでも参考にすべきだと考えています。その上で、アカウントリカバリについては、昨年度もよく議論できた内容を入れていく方が良いのではないかと感じています。
- ❻や❼のウォレットに関する要件については、議論があるのは承知していますが、別冊として扱ってもよいのではないでしょうか。
- 本人確認は、容貌の確認を大事にし、認証においてはフィッシング耐性の確保を伝えていくことが大切なのではないかと感じています。

- 仰るとおり、2pd の改定内容にはウォレットの内容が記載されていますが、「ウォレット」ではなく「クレデンシャル」の方が大事だと考えています。ウォレットの話を中心に反映すると、そこが曖昧になってしまうのではないでしょうか。本人確認ガイドラインでは、「スマホ搭載されたマイナンバーカード」をどう扱うのか、という点に集中してもよいのではないかと考えます。そういう意味では❶のウォレットモデルを定義すべきかという論点に関しては、私は必要ないのではと考えます。
- ウォレットからクレデンシャルや属性情報を取得する、というケースは当然想定されますが、それを「モデル」として無理に定義する必要はないのではないか、と思いました。それから❻ですが、これは米国特有の都合で、mDL を認証に使いたいという意図から記載されたものではないかと感じています。
- 2pd でウォレットモデルを入れてきた背景として、NIST IAM ロードマップを見ても、mDL を認証に使いたいという意図は見えました。
- 有識者の皆様のおっしゃるとおり、ウォレットについては本人確認ガイドラインの本編には無理に盛り込まず、別途ディスカッションペーパーのような形でまとめる方が良いと、皆様の議論を伺って感じました。その一方、法律で定められた「カード代替電磁的記録」による本人確認をガイドライン上でどのように扱うかについては、制度上の直近の課題です。
- カード代替電磁的記録については、iPhone でも Android でもどのみち JPKI を使うのですから、当面はその前提で考えてよいのではと思います。一方、もし仮に、カード代替電磁的記録単体での本人確認を将来認めるのであれば、ガイドラインとしての記載方針も当然検討が必要です。EUDIW や SP 800-63-4 におけるウォレットモデルとは関係なく、日本法におけるカード代替電磁的記録を本人確認ガイドライン上どう扱うか、という話は別格の議論になるかと思いました。
- 基本的には、ID ドキュメントに何が記載されているかという、Identity Evidence の話に集約されるのではないかと感じています。
- ID ドキュメントに何が記載されているか、どのように発行されたのか、という強度の話と、ID ドキュメントから取り出したデータをどのように受け渡すのか、という受け渡しの強度の話が本来 63C で書かれるべきことだと思うのですが、そこを押さえておけば、おそらく「ウォレット」そのものには言及しなくてもよくなるのではと考えます。
- 一般的なユーザーの感覚からしても、IdP（Issuer）からカードが出て、それを RP に見せるというモデルの方が直観的に理解しやすく、逆にウォレットモデルを理解するほうが、難易度が高いのではないかと感じます。
- 「クレデンシャル」という視点で理解したほうがユーザー目線ではわかりやすいかもしれないと認識しました。システムの仕様や実装としては難しいかもしれないですが、ガイドラインとしてはわかりやすいものになるのではないかと感じました。
- DS-500 は、「マイナンバーカード」という具体的なクレデンシャルを本文中で扱うことになると思いますので、スマホ搭載についても、それと同じようにガイドラインに埋め込まれるとよ

いのではないかと感じました。

- 具体的な手段ではなく、「電磁的記録を使用したもの」や「デバイスにバインドされたもの」と定義しておくことは大事ではないでしょうか。
- はい。具体的な実現手段を名指しせずとも、将来的に実装の可能性のあるものが含まれるような内容にできると理想だと思います。
- そのためには、例えば「Credential Duplication Attack に対応していること」のように、「この Threats に対応していること」といった形で要件を記載すべきだと思います。
- 手段という点については、次期マイナンバーカードにも考慮が必要であり、ガイドラインとしては具体手段についても解説や随時の更新が必要になってくると認識しています。そのため、Normative なドキュメントとしてガイドラインを出した後、Informative なドキュメントとして具体手段についての参考情報を出していかざるを得ないと考えています。冒頭、今年が最終年度であると申し上げましたが、分冊化した部分の議論は引き続き実施していかなければならないと認識しました。
- 理想を言えば、より大きなアイデンティティコミュニティの中で活発な議論を進め、コミュニティとして自走するタイミングを考えないといけないのではないかと感じています。
- 現行の本人確認ガイドラインで最も問い合わせがあったのは、リスク分析の部分でした。当時は SP 800-63-3 の Draft 段階のものを基に作成しており、それが原因となった問合せもありました。今回も同様のことにならないか心配しています。
- 現行ガイドラインのリスク分析の箇所については、専門的な方々が読めばわかりやすい記載になっていたのではないかと感じています。フローチャートではすべての事象を記載できず、事例集を別冊のような形で用意するほうが良いという話や、デジタル庁にリスク分析官を設置したほうが良いかどうかという話を昨年度の有識者会議において、検討しました。
- リスク分析官を置くというのは、デジタル庁に設置するのでしょうか、もしくは地方自治体に設置するのでしょうか。このガイドラインを社会実装するときに、何をどこまで用意してあげるのか、という点の議論を始めていただきたいと考えています。
- リスクマネジメントをしやすくなるという観点では、今回の改定にある Define the Online Service の部分は DS-500 にも反映を検討したいと考えています。
- 8 ページ目の変更点は、Step 1: Define the Online Service が追加され、Step 5: Continuously Evaluate & Improve で収集すべきメトリクスが新しく追加された、という部分ですね。
- メトリクスが明示されたことで、やらなければならないことがわかりやすくなったのではないかと感じています。
- Step 5: Continuously Evaluate & Improve については、米国の Risk Management Framework から考えると普通のことではありますが、日本において、この文化が根付くかどうかに懸念があります。一度決めてしまったら、それで Fix としてしまうのではないでしょうか。
- フローチャートがないと納得しない人も多いのだと思います。例えば、何も考えずにフロー

チャートを使用すると厳しい要件が出るが、詳しく分析すれば要件が調整される、というような方法は考えられるのかもしれません。

- 例えば NIST の SP800-60B には、各連邦政府の業務について、CIA（Confidentiality / Integrity / Availability）があらかじめ定義されています。実際に使われているかは不明ですが、非常に分かりやすいのではないかと感じています。しかし、実際にやってみようとしたところ非常に難しかったです。
- 同様の認識です。以前、業務リスク分析を実施した際に、グラフ構造で、すべての価値の流れとデータの流れを表現できると考えていましたが、結局理解しやすいかたちで表現するに至らず、最終的には具体的な業務で記載をしました。具体的に想像できる形で記載が必要だと考えています。
- 60B に記載されている表を見ると、moderate や high に分類されているものは少なく、ほとんどが low に分類されていることがわかります。一般に、担当者は自分の仕事のリスクを高く見積もる傾向にあります。
- それは、役所の文化の中でも起こりやすいと感じています。現場の担当者でない人間がリスク分析を実施することで、「何かあった時の責任がとれないので」という考え方で、過剰なセキュリティになりやすいと考えます。
- 「最も高いレベルのセキュリティを実装したほうが良い」と考える方が多いように感じます。一切何も起こらないようにすることを目的としてしまっており、中央でリスク分析をするということは、オーバーセキュリティになりやすいと考えます。
- 中央集権的にリスク分析を実施したほうが良い可能性もありますが、担当者が入れ替わった途端に厳しい基準となってしまい、結果的に誰も守らない基準となってしまう恐れがあります。
- ゼロから作るのでもなく、全て同じ基準とするのでもなく、いくつかパターンを用意し、マッピングをできるような形にするとよりよくなるのではないでしょうか。
- 例えば、IAL1 の業務とは何か、を具体的に考えるとよいのではないでしょうか。
- 元々税務署は IAL1 のような概念で業務を実施していました。誤りがあった場合は修正申告を実施すればよいという考えで、本人確認を実施していませんでした。これは、現場において、リスク分析をした結果だと考えています。
- 一度で完璧なリスク分析を実施するのではなく、時間をかけて適切なものにしていくという理解が必要なのではないかと感じています。弊社では、2021 年より、リスク分析を実施し始めましたが、当初はやや過剰な判断になってしまっていたところもありました。その結果、現場の運用が大変になり、徐々に調整されていったという経緯があります。
- 他の委員がおっしゃったように、データを取らないと継続的に改善できないと考えます。まずは、データを中心に改善を進めれば、改善するにあたって、だれも文句が言えないようになると考えます。ガイドラインのため、全ての認証システムのデータを取る必要はありませんが、典型的な認証の部分のデータを取得することはいかがでしょうか。

- 良いと思います。データに基づいたメンテナンスをしていくということは記載したいと思います。
- そのためにも Step 5: Continuously Evaluate & Improve で収集すべきメトリクスを記載しておくことは重要だと認識しました。継続的な改善を実現するためにデータ取得が必要だということを理解してもらわないといけないと考えています。この点は、民間でもあまりできていないのではないかと感じます。
- 非常に良い取り組みだと考えます。過去には、セキュリティを強化したことによってサービスが直感的に使いにくくなったといわれることもありました。データに基づく検討では数字を使って改善しているため、感覚的・属人的な評価ではなく、積極的に確認や議論ができるようになったのはとても良い状態であると感じています。
- 大変有意義な議論をありがとうございます。本会議も残り 5 分となりましたので、全体を通してコメントがございましたらご発言をよろしくお願いいたします。
- 個別論点❹の IAL1 の刷新と IAL2 の見直しに記載がある「住所へのコード送付」については、検証済みアドレスへの確認コード送付とのみ記載がありますが、日本では本人確認郵便など NIST にはない概念がある中で、ガイドラインには書ききらないほうが良いのかどうかといった議論が必要なのではないかと感じます。実際に実施できる事業者は数社しかないと思います。
- それができる事業者は、ある種の Trusted Referee になるのでしょうか。
- はい。最終的に確認コードと一緒に担当者が出向いていき、何らかの方法で Onsite の本人確認を行うことになると考えます。
- 日本においては、郵便が本人確認プロセスにおいて重要な役割を担っています。米国とは郵便の信頼性も到達性も異なります。例えば、日本においては引っ越しの際の転送が可能ですが、米国では可能ではありません。そのようなリスクに基づいて別個の検討が必要だと考えます。
- NIST に対しては住所の売買や住所貸しに対するリスクをどのように考えているかを質問したいと考えています。
- 郵便については、確認コードとしての扱い方のほかに、自治体が住民基本台帳に記載されている住所に送付し、署名・捺印して返送することや本人確認書類のコピーを同封して返送するような手法は当分残るのではないかと感じています。郵送を全件、本人限定受取郵便として送付してしまうとコストが上がってしまうため、どのように取り扱うかの検討が必要ではないかと感じています。
- あくまで、デジタルにバインドするためのフィジカルな手段として記載すればよいのではないかと思います。
- 郵送の取扱いに関しては昨年度の有識者会議でもご指摘いただき、中間とりまとめでも今後の検討事項として挙げさせていただきました。事務局内でも検討を進めておりますので、第 3 回・第 4 回の有識者会議にてガイドライン改定案とともに検討結果を提示できるように

準備中でございます。

閉会

（事務局）

- 以上で本会議を終了させていただきます。本日の議事録は、本日から 2 週間以内に各委員に送付予定ですので、ご確認をお願いいたします。本日は長い時間の議論、誠にありがとうございました。

（了）