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 4 回）
令和 7 年 1 月 16 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 Sr. 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
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
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） ガイドライン改定案に対するコメント、意見交換

「3.1 身元確認（Identity Proofing）」について

事務局より、資料 1 P5～32 に基づき、ガイドライン改定案の「3.1 身元確認（Identity Proofing）」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）

- P32 は、以前の会議で提示されたものよりも整理されてきたと感じます。協議ポイントの「❶ 身元確認における脅威の整理結果について」と「❷ 本人確認プロセスの概観図について」については、図が随所にあり、読者にとって直感的に分かりやすくなっていると感じました。
- 協議ポイントの「❹ 保証レベル 2B の位置づけ」ですが、「国民を詐欺から守る総合政策」においても IC チップの利用を指摘されているところであり、IC チップのない本人確認書類の真正性確認は極めて難しいと理解しております。本ガイドラインでも IC チップの必要性について積極的に触れていくことで実効性が高まると考えます。その点で、現在の案のレベル 2A と 2B の差は大きいと考えます。一意見ではありますが、いま保証レベル 2A としているものを「保証レベル 2」とし、保証レベル 2B は、あくまでも例外的な扱いとすることが望ましいと考えます。保証レベル 2B を保証レベル 1 に含めてしまうかどうかは議論の余地があると思いますが、本人確認書類に IC チップが入っていることをデフォルトにしていくべきだと思います。ただ、現状の案はレベル 2 の中で「容貌の確認」をするか否かの区別がない状態となってい

ます。盗用や売買等で不正にマイナンバーカードを入手し、本人ではない方が本人であるかのように取り扱われるケースがあります。そのため、保証レベル 2A を保証レベル 2 の基本としつつ、その中で分類するのであれば、容貌の確認をしているかいないかという分類が求められるのではないかと思います。

- 協議ポイント❸の「本人確認書類の非対面での券面検査」をレベル 1 とする方針、❺の「本人確認書類に対する対策基準の定め方」については、議論すべきではありますが、中心的ではなくやや補助的な議論となるのではないでしょうか。テーラリングの中で補足していく事項だと考えています。
- 私も現在保証レベル 2A としているものを「保証レベル 2」として扱い、保証レベル 2B は例外的な扱いとすることが望ましいと考えます。また、そもそも保証レベルを 1～4 ではなく 3/2A/2B/1 としていることについては、NIST が 3 段階のレベルであるということを知らない読み手からすると、よくわからないのではないかと思います。もし保証レベル 2B を残すのであれば、保証レベルを 1～4 とした方が望ましいのではないかと思います。
- これまでの意見におおむね賛成です。一点、「容貌の確認」を実施するか否かに関しては、いくつかの法令では公的個人認証での電子署名を実施する手法が定められていますが、そこでは容貌の確認までは求めないものもあります。他方、民間事業者と議論する中では、不正対策の背景から公的個人認証に容貌の確認を加えたいといった要望もあります。法令では公的個人認証で必要とされていない中、容貌の確認の追加を是とすべきかについては、ユーザーの負担の観点からも悩んでいます。
- 保証レベル 2B を例外的な扱いとすることに関して、より実効性の高いガイドラインにするためには、国で使える本人確認手法例を記載してある補助的なドキュメントを作成してもよいのではないでしょうか。使用できる本人確認書類の中には、療養手帳等、IC チップの含まれていない本人確認書類が入ってくると考えられ、それらの扱いをどうするかを示したほうが良いと考えます。
- P20 に関して意見を述べます。主な手法の中に「申請者自身が記入し、それに対して問い合わせをすることで検証する」といった旨が記載されていますが、現在の記載だけでは次の本人確認プロセスの検証につながらないのではないかと思います。Evidence と合わせて提示をしないと、本人確認書類の検証につながらないのではないかと思います。
- P8 の脅威の整理案のうち「❹ 本確認書類の複製」は、現状は物理的なものを前提に書かれている理解ですが、電子的な複製においては 1 ビット単位で複製する duplicate なのか、それとも単なる copy なのか、Digital Credential の将来的な利用も考慮して、区別して書き分けるべきだと思います。
- P9 からの対策基準のマッピングの表現方法に関しては、それぞれのレベルの違いが視覚的に分かりにくく感じます。前のレベルとの差分を違う色にするなど、より視認性が高い図の作成が望ましいと考えます。
- P9 の表現方法は好みの問題もありますが、組み合わせの表現に関する情報量が少ないと

感じます。この図の枠の中に入っているものであればどれを選んでもよく、最低限も枠内の最も弱いところまで許容できるということを表現するところまでと思います。保証レベル 2 や 3 を定義するのであれば、枠内の最も弱いところを選択した場合にも妥当かを一度確認する必要があると思います。

- 保証レベル 3 の図を見ると、「暗証番号による認証」と「容貌確認」を実施することに境界があることが分かりますが、保証レベル 2A では容貌確認を実施する場合、しない場合が同じように見えてしまいます。ガイドとしては容貌確認の有無を区別したうえで、テーラリングの際にその要否を判断できるようになる方が望ましいです。マイナンバーカードを利用する場合でも、暗証番号を利用する場合と容貌の確認をしている場合がありますのでそことの整合性を取る必要はあるかもしれないですが、それらに差があることは、今後を見据えて 明示しておくべきだと思います。
- 暗証番号については、例えば子どもの PIN を親が知っていることは、ミッションデリバリーの観点では問題ないと思います。しかし、それを脆弱性として利用される場合も出てきますので、どのような場合に暗証番号を確認していたとしても容貌確認をすべきかについては、この表だけでは表現できないと考えます。どのように表現すべきか悩ましいですが、リスクは同じ保証レベルの中でも手法ごとにグラデーションで異なってきますので、より厳しい方に合わせるのか、もしくは中間のようなものとするのかを考えたうえで、そのリスクへの対策を検討するのだろうと思います。また、厳しすぎるリスク対策はミッションデリバリーの観点を満たさない可能性がありますので、ある程度対策を緩める場合もあると思います。
- 対策基準案として示している表は、強度の「弱」から「強」までの大枠が視覚的に分かるようになっていることはとても良いと思いました。ただ、脅威の「❺ 本人確認書類の不正な発行」は左から右まで一つの塊となってしまっており、弱でも強でも同じ対策でよいかのように見えてしまう点は、改善する必要があると考えます。例えば、発行機関が政府機関である場合は、強寄りとするなど、同じ塊の中でもグラデーションをつける必要があると思います。また脅威のうち「❶ 重複登録」、「❷ 別人との誤紐づけ」、「❸ 本人確認書類の偽造・改ざん」、「❺ 本人確認書類の不正な発行」、「❻ 本人確認書類の盗用」については、「対策なし」の場合はレベル 1 にも満たないということを明記するべきだと考えます。
- P9 の「非対面での容貌確認」には「注：統制環境下のみ可」と記載されていますが、あくまでも対面での容貌確認が原則であるという観点から、対面での容貌確認における注意書きとして記載するのが良いのではないかと思いました。
- P11 の身元確認保証レベル 2B の「❶ 重複登録」と「❷ 別人との誤紐づけ」における対策手法に関しては、エビデンスとともに提示する前提であれば、手入力を許可してもよいのではないでしょうか。OCR での読み取りも 100%正しいわけではないので変わらないと感じました。
- 参考情報ではありますが、「❽ カメラ映像の偽造・改ざん」に関しては、国際的にも ISO/IEC JTC 1/SC 27 と ISO/IEC JTC 1/SC 37 の生体認証のジョイントワーキングチームを作りインジェクションアタックについての規格策定が始まっています。昨今はカメラ映像をすり替えて

動画を流す事例などが見受けられるようになってきているので、こういう脅威があるということは書いておくのが良いと思います。

- 「非対面での券面の検査」をレベル 1 とすることで犯収法のホ方式がレベル 1 に該当することになる件については、以前から懸念を持っていた事業者も多くおり、大きな問題は起きないのではないかと考えます。ただし、犯収法とガイドラインの差について事業者側がどのように受け取るかという懸念がありますので、犯収法における対応から踏み込んで、こういう場合はレベル1ではなくレベル 2 の手法を採用した方が良いという方向に誘導できるような指針を示せると望ましいのではないかと思います。
- 犯収法のホ方式がレベル 1 になることについては、昨今の情勢をみると致し方ないと認識しています。犯収法や携帯法でも見直しが進められる予定ですので、おおむね問題ないのではと考えます。
- 協議ポイント❺の「本人確認書類に対する対策基準の定め方」についてコメントします。利用価値の高いガイドラインとするためには、できるだけ具体的な例を記載することが望ましいと考えます。改定までの期間を考慮すると網羅的な例示は難しいかもしれませんが、補足的なドキュメントを作成することで例示を補えると良いと考えます。
- P29 の最後のコメントについてです。本人確認書類に対する要求事項は、レベル 3 は明確になってきていると思います。しかし、レベル 2 の手続として適切なものを定義した後、現場の運用が回らないため一部レベルを下げるテーラリングすることになるだろうと想定します。その際、どの程度リスクが増えたのか、補助的な書類によってどの程度そのリスクへの対策ができているかを検討する必要があるという旨を、ガイドライン中に記載しておいた方が良いのではないかと思います。手続上原則 IC チップを確認する必要があり、そうではない場合は例外として補助書類を求める、といったような運用は受け入れられると思います。また、NIST の「SUPERIOR」のような画一的な本人確認書類の分類は、日本の現状にそぐわないといった考えには賛同します。その点を考慮しても、補助書類に触れる記述が必要だと思います。また、世の中一般的に受入れられる補助書類はこれであるというものを提示しないと、個別判断は難しいのではないかと感じます。
- その点では、公共料金の領収書など生活の痕跡がないとできない決済の証跡は、SUPERIOR 相当には及ばないものの、比較的使用しやすい補助書類の一つであると考えます。
- 補助書類が具体的にどういった書類であるかも、別冊にて明記すると望ましいと思います。
- NIST は今回の改定において、有効期限の扱いも変わっています。有効期限が切れていてもデジタル的にはある程度は問題ないという考え方もあるため、業務によって幅を持たせてよいという指針が明記されているのが望ましいと思います。
- 使えるドキュメントを例外として羅列するよりも、例外が必要となるケース別に記載するほうが良いのではないでしょうか。例えば、自然災害でデジタル署名を検証する装置が使用できない場合に、どのような補助書類を使用すればよいかといったような記載があると、わかりや

すいのではないでしょうか。レベル 2A と 2B は IC チップを使用できるか否かの状況の違いでしかないため、そのような切り口で例外を記載する書き方もあるのではないかと思います。

- 災害時だからといって基準を単純に緩めるのではなく、どのような緩め方にすればよいのかの例をガイドラインに記載しておくのもよいと思います。
- このガイドラインにおいては、Trusted Referee には触れるのですか。
- Trusted Referee のような考え方をテーラリングの一環として盛り込むという方法は十分に考えられます。
- （事務局）機械が使えない状況という定義は難しいと思います。業務システムが動いていれば常にかざして読めて正確に処理できるかというと、そんなに簡単ではありません。そのため、テーラリングの例示はできるとは思いますが、画一的に、レベル 2B を使用してよいといったような基準の記載は難しいと思います。レベル 2B を選ぶ際には、そのリスクを適切に認識し、全体のプロセスのうちどこかでリスク受容できるように、リスク評価やテーラリングを実施するということしかできないと感じます。また、他人に迷惑をかけるなという観点はあるため、身分証の発行等、レベル 2B を利用するべきではないハイリスクのケースを記載するのもよいと思います。
- ブートストラップ問題の中で、SUPERIOR 相当の本人確認書類が減ってきているという話がありましたが、本当に減っているのかは疑問です。過去にはたくさん種類があったものの、所有者数が限定されているものが多かったのではないかと思います。

「4 本人確認手法の検討方法」について

事務局より、資料 1 P33～47 に基づき、ガイドライン改定案の目次「4 本人確認手法の検討方法」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）

- 身元確認保証レベルと当人認証保証レベルの組み合わせに関する記載が十分でないように感じます。例えば、身元確認の保証レベルが高くてもフィッシング耐性のない当人認証の手段しか提供していないとそこで簡単になりすましが発生します。当人認証保証レベルが高くフィッシング耐性が高い認証手法を使用していたとしても、身元確認保証レベルが低い場合には、全くの別人が高い当人認証レベルでその人らしく振る舞うと言うことが出てきます。そうした保証レベルの組み合わせについても大事であるため、より読者に伝わりやすいように明記するべきだと思います。
- ガイドライン改定案の表 4-4 は、誤解を招く恐れがあると思います。実際には、身元確認保証レベルと当人認証のレベルは同一になることが多いと思いますが、最終的なテーラリングの結果ずれることはあったとしても、初期のレベル判定時には保証レベルの決定を簡素化して同一としても良いのではないかと思います。
- ガイドラインはどこから読んでもわかりやすい設計にするべきです。3 章の「本人確認におけ

る脅威と対策」の中で、「身元確認」「当人認証」「フェデレーション」の章があり説明されているため頭から読み進めれば理解できる構造にはなっているものの、身元確認と本人確認を区別できている読者は非常に少ないこと、3 章を十分に読解していない読者が読んだ場合も想定して、4 章を記載できると望ましいです。

- 本人確認は「身元確認」と「当人認証」の 2 つの観点で考えなければならないこと、さらに、その組み合わせで検討しなければならないことは、各章で言及したほうが良いのではないでしょうか。
- いま身元確認と当人認証のどちらに言及しているのかがわかりやすいようにラベリングされていると、より良いのではないかと思います。
- 法令や行政文書はシンプルに作成しておき、実務では解説書を参照するような形が現場では多いと思います。このガイドラインも同様に、ガイドライン本編を長大なものにするのではなく、解説書で詳細を記載するようにする方が良いのではないでしょうか。
- 金融ビジネスでは犯収法に準拠した身元確認ならびにフィッシング耐性のある当人確認が実施されていますが、例えばコンテンツを購入するような場合には犯収法に従う必要がないため、当人認証レベルはフィッシング耐性があるもので同一なものの身元確認レベルが異なるケースも発生し得ます。そうした点にも留意が必要です。
- これまでの議論を聞いていると、アカデミアでの身元確認は、行政手続における身元確認と全く異なると感じます。一方、当人認証はテクニカルな部分であるため概ね一致する評価ができると感じます。そのため、トラストフレームワーク間の相互認証のために IAL を共通的なものにはできないが AAL だけ共通的なものにするような動きが出てきた際には、共通的なレベルとしての A/B/C が分解されていると望ましいのではないかと思いました。
- DS-500 ができた当初は、フィッシングが現在のように簡単にできる時代ではありませんでした。フィッシングされない認証を積極的に使用していただくことで、ある資格を持っている、あるいは、ある身元確認レベルを達成されているユーザーが日々サービスを利用する際にはそのユーザーであることが特定されつつ、資格確認という部分においては差がある状態を積極的に認めておくことは、様々な可能性を広げられるのではないかと思っています。
- 様々な方がガイドラインを利用することを想定すると、よりシンプルな方法でレベルの判定をしていくことが望ましいと考えます。それぞれの当人認証レベルと身元確認レベルの判定を行ったうえで、応用的に、最後に組み合わせた際に露見するリスクに目を向けられるようになると思います。

- <u>閉会</u>

  （事務局）本日も活発なご議論ありがとうございました。この分野は変化が大きい中、最新の知見に基づいてご助言をいただけるのは贅沢な場であると思っております。今回改定が実現すれば、デジタル庁が立ち上がってから初めての大規模改定となります。今後 5 年・10 年通用していくガイドラインの礎となる議論ができていると思いますので、引き続きよろしくお願い

いたします。

（了）