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 5 回）
令和 7 年 3 月 4 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 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
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） 令和 6 年度とりまとめ及び本人確認ガイドライン改定案に関する意見交換
「本人確認ガイドライン改定方針 令和 6 年度とりまとめ（案）」について
事務局より、資料 1 に基づき説明を行い、有識者による自由討議を行った。
（有識者意見）

- P26 に記載されている身元確認保証レベル 3 での申請者の検証方法で「本人確認書類の盗用に対し、容貌の確認又は暗証番号による検証を必須とする。」とありますが、「容貌の確認」と「暗証番号による検証」が「又は」によって並列の記載となっていることに違和感を覚えます。以前に議論した際に、容貌の確認の有無で結果が異なることが議論されました。容貌確認の有無によって身元確認の強度に明らかに差が出るため、レベル別の区分けをしないまでも、厳格な身元確認を実施したい場合には容貌の確認を推奨するなどを追記したほうが良いのではないかと思います。また、「本人確認書類の貸し借りへの対策は必須とはせず」といった記載をあえて書く必要はないのではないかと思います。今回改定するガイドラインを長く使用できるものにするためにも、貸し借りの問題はこれから重要な問題にもなってくると思います。この文を削除し、容貌確認の重要性を記載するのはいかがでしょうか。
- P17 の図表に「PASSWORD」という文字が記載されています。P33 に当人認証保証レベル 1 にパスワードの記載があることは理解できますが、パスワードだけではすでに十分ではない

ということを主張しているガイドラインにおいて、パスワードを大きく主張するような図表を挿入すべきではないと思います。認証を構成する要素のうち、知識情報はパスワードと呼ばれるものだけではないことから、図中から「PASSWORD」の文字を削除するのはいかがでしょうか。PIN やパスコードを入力する場合があるため、入力を示すアスタリスクは残しておくのがよいと思います。また、図中のアイコンの順番も揃っておらず、P17 では、パスワード・鍵のアイコン・顔のアイコンとなっています。例えば、人が中心になるだろうと考えられるため、まず生体認証を表す顔のアイコンを中心に置き、認証の三要素である所有の一つである鍵を表すアイコンを左に配置し、右に知識情報を表すアイコン配置する案が望ましいのではないかと思います。また、P33 の OTP のイラストには「1234」とありますが、アスタリスクに揃えても良いのではないでしょうか。

- P18 の図に、身元確認の方には「サービスの初回利用時等」、当人認証には「2 回目のサービス利用時等」とありますが、正確な説明ではないように思います。単純に「身元確認時」「当人認証時」とするか、削除してもよいのではないでしょうか。
- 確認ですが、P21 に記載されているウォレットモデルに関する補足は、ガイドライン本編や解説書には記載されない情報と理解してよいでしょうか。
- （事務局）ご認識のとおりです。
- 同じページに「今回のガイドライン改定案への盛り込みを見送る方針」とありますが、令和 6 年度とりまとめを公表するときには、「方針」を削除し、「今回のガイドライン改定案への盛り込みを見送る」と記載すべきではないでしょうか。
- （事務局）今回ご確認いただいている資料 1 は、「本人確認ガイドライン改定方針」として、ガイドライン本編の改定版よりも先に公表することを想定している資料です。そのため、「方針」という表現で記載しております。
- 「容貌の確認」と「暗証番号による検証」が並列の記載となっている図のまま公開されるのでしょうか。先ほどの提案には、別の委員からも賛同のリアクションを得られていたように感じています。これが合意された場合、別途とりまとめ資料として公開されるという認識であっていますか。デジタル庁から出された「とりまとめ資料」として名前が付く資料のため、重要な資料になると思っています。
- （事務局）本日の会議資料としては、いまご覧の状態のものが公開されます。その後、本日のご指摘を反映し「案」をとった資料が、正式版として公開される形となります。
- P26 に IC リーダにマイナンバーカードをかざしている図がありますが、マイナンバーカードのスマホ搭載なども考慮すると、スマートフォンをかざしている図にしても良いと思いました。
- 本ガイドラインは、犯収法や携帯法と総合的に影響しあうと思います。法令や施行規則ではなく本ガイドラインを読んでしまう人がいる可能性があることも考慮し、FAQ 等に犯収法等との関係性を記載しておく方が良いと思いました。
- NIST SP800-63-4 の動向にかかわらず、日本では IC チップを利用した厳格な身元確認が比較的利用しやすい環境が作られてきました。しかし、注意喚起だけではフィッシング詐欺を防

ぐことができないことなどから、身元確認保証レベル 3 がより重要になってきていると思います。そのため、より厳密な手続を行うためには、容貌の確認まで実施することが望ましいがわかるように記述されると良いと思います。

- 「容貌の確認又は暗証番号による検証」というように、「容貌の確認」と「暗証番号による検証」が並列の記載となっていることは、現状は暗証番号による検証をしているシステムも多くあるからだというように理解しました。現状は併記せざるを得ないかもしれませんが、容貌の確認が重要である旨の補記はしておいた方が望ましいと思います。
- 令和 6 年度とりまとめ資料において、当人認証については脅威耐性の表がありますが、身元確認にはありません。ガイドライン本編には身元確認の脅威も記載されていますので、とりまとめ資料にも脅威を載せるべきだと思います。
- 当人認証保証レベルの表には、フィッシング耐性（推奨）といった表記があります。身元確認において容貌の確認をすることについても、同様に推奨するというような記載を加えるのはいかがでしょうか。対面時において容貌確認のない暗証番号による検証は強固な検証であるといった誤解を解くようなきっかけになるのではないかと思います。
- P26 の暗証番号のアイコンにはアスタリスクが 4 桁しかなく、エントロピーが少なくてもよいような誤解を与える可能性があると思います。また、有効期限を記載してもよいのではないかと思います。
- P.20 において『本ガイドラインではフェデレーションを活用した「連携モデル」の採用を第一候補」としている関係上、以前の版のように「主要な改定のポイント ④ 脅威と対策の最新化、保証レベルの見直し 3.1 身元確認（Identity Proofing）」の一部の手続きにのみ「ID プロバイダからの情報取得」が書いてあるのは誤解を招くとして削除されたとのことですが、逆に「ID プロバイダからの情報取得」を使用してもよいということが読み取りにくくなっているのではないでしょうか。
- マイナンバーカードのデジタル認証アプリは、民間事業者が使用することも多いため、わかりやすい記載があったほうが望ましいと思います。
- P17 や P19 の図中から読み取ることができるのではないでしょうか。
- RP 側が情報を取得し、自らが身元確認をする状態が多いと思いますが、行政手続によっては、IdP 側で高いレベルで身元確認がされていることがわかりさえすればよいといった業務もあると思います。また、プライバシー面等を考慮し、そちらの方が望ましい場合もあると考えられます。
- （事務局）行政手続の多くは公的個人認証に依拠すると考えられ、公的個人認証で身元確認済みということがわかれば、基本四情報等が必要でない場合もあると思います。本編への記載は、あくまで一般的な場合を記載したいと考えておりますが、解説書等への反映を検討いたします。
- Data Minimization という考え方からは、情報の取得時だけでなく取り扱いも最小限にするといったことも検討したほうが良いと思います。

- Authenticator の訳語は「認証器」に統一されたと認識しておりますが、「認証情報」という用語がまだ残されています。
- （事務局）認証情報という言葉をすべて認証器に置き換えるべきかどうかは現在精査中です。NIST でいうところの Credential や Authenticator Output に相当する意味で使用している箇所もあるため、ガイドライン改定案の発表までには整理と修正を行う予定です。
- P27 の図の縦横は、他の保証レベルの記載と同様に、保証レベルを縦に記載したほうが良いのではないでしょうか。
- （事務局）修正を検討します。

「本人確認ガイドライン改定案（令和 6 年度とりまとめ時点案）」について

事務局より、資料 2 に基づき説明を行い、有識者による自由討議を行った。

（有識者意見）

- P1 において、「重要であるとご認識いただきたい。」といった記載をしていますが、「適切な手法を選択することが期待される。」といったやわらかい表現にしてはどうでしょうか。
- ガイドライン中で「定義する」という言葉がやや乱用されているように見受けられます。適切な表現になっているかを再度確認していただきたいです。
- 「パスキー」という用語が書いてあるものの、解説が記載されていません。P30 の「ウ」にあてはまる技術であり、「国民を詐欺から守る総合対策」の中でも期待されている技術であることから、簡単な説明を加えたほうが、より有益なガイドラインになるのではないかと思いました。
- 表 1-1「本人確認に係る用語の定義」の中で、「法人等」という用語が定義されていますが、個人事業主やフリーランスが除外される記述になっており、個人としての行政手続で収まるのかどうかといったことが懸念されます。
- 個人事業主やフリーランスは、法人番号を所持していないため、個人事業主やフリーランスが除外される記述となっている「法人等」の定義は正しいと思います。また、法人等と個人が同等の手続をすることもありますが、個人事業主は、個人として扱うことになると思います。
- 個人事業主の属性を定義することは難しく、個人という扱いでよいと思います。
- 表 1-1 の用語定義には、解説や例示が多く含まれています。定義の記載を分離して書いたほうが良いのではないでしょうか。
- P7「プライバシー」で記載しているのは、プライバシー原則の一部でしかありません。参考情報として JIS X 9250 等を記載することが望ましいと思います。
- 表 2-1 は表 1-1 と内容が重複していませんか。
- （事務局）用語定義を読まずに 2 章を読む読者を想定し、あえて重複して記載しております。
- P15 の「ア」の説明文などにも、対象となる母集団を定義することが重要だと記載するほうが望ましいと思います。
- 表 3-5 共通において、ISO/IEC 29115 などと同様に明文化された基準に基づく本人確認書類の発行を求めるべきではないでしょうか。フェデレーションで身元確認を実施するケースに

おいては、IdP 側で明文化されたプロセスを持っていないと、適切ではないと思います。また、明文化されていないと監査ができないことから必要な措置であると思います。

- 表 3-5 の「電子データの不正な取り出しや複製が困難な仕組み（耐タンパ性を有する IC チップや、それに類する技術的対策等）を備えていること」は、デジタル署名全体ではなく、鍵に関する記述のため、それがわかるように修正いただきたい。
- 表 3-9、これまでの検討会で整理してきた身元確認保証レベルと脅威耐性のマッピングの議論が、何かしらの方法で反映されていると望ましいのではないかと思います。
- 脅威耐性のマッピングの図を残すことは難しかったでしょうか。当人認証の主な脅威はフィッシングであることはわかりやすかったですが、身元確認の主な脅威がなりすましであることは分かりにくいと思います。SIM スワップや支払う意思がない者等になりすまされるといった具体例を記載し、それらを防ぐための対策を記述するほうがわかりやすいのではないでしょうか。
- 表 1-1「本人確認」の用語定義文も、定義は 1 行目に書かれているはずですが、2 行目以降にも定義文が続いているように読めます。また、表 1-1「保証レベル」の用語定義では、「本人確認の確からしさを段階的なレベルとして表現するカテゴリー」と定義されていますが、保証レベルは「カテゴリー」ではなく「レベル」と表現したほうが理解しやすいのではないでしょうか。また、その後に、「本ガイドラインでは「身元確認保証レベル」と「当人認証保証レベル」の 2 種類の保証レベルを定義する。」と記載するとあるにもかかわらず、それぞれの用語定義がないように見えます。
- 表 1-1「本人確認」において、「本ガイドラインでは、本人確認を「身元確認」、「当人認証」及び「フェデレーション」の 3 つの要素によって定義する。」と記載されています。しかし、「2.1. 本人確認の構成要素」においては、「本ガイドラインでは、本人確認を構成する要素として「身元確認」と「当人認証」を定義する。さらに、身元確認や当人認証を他者（信頼できる ID プロバイダ）に依拠して実現する要素として「フェデレーション」を定義する。」と書かれていますので、表現は合わせた方がよいかと思います。
- 他の図表等では「暗証番号」と記載しているところに、図 3-1 の中にだけ「PIN」という単語が使われております。
- 図中から「PIN」、「PASSWORD」といった文字は削除し、アスタリスクのみ図示したほうが良いのではないでしょうか。
- （事務局）本ガイドラインの読み手への伝わりやすさも考慮しつつ、修正を検討させていただきます。
- 用語定義において、知識認証が Authenticator Output なのか否かといったことを区別して用語を使い分けることは検討されたのでしょうか。
- （事務局）検討はいたしましたが、結果としてその概念が「保証レベル」の判定に影響を及ぼさないため、言葉の使い分けをしないこととしました。解説書で記載できればと考えています。
- 「PIN」、「暗証番号」、「OTP」の 3 つの表記が見受けられるため、これらも整理したほうが良

いと思います。ローカルで完結するパスコードとリモートにアウトプットされるパスワードの違いは明らかであるため、その違いは明示したほうが良いと思います。

- （事務局）今回のガイドラインでは、保証レベルや対策基準に関係のない要素は「解説書」へと記載する方針としています。
- 表 4-3 で、リスクの影響度は高位/中位/低位の三段階で評価するとされているが、「プライバシーの侵害」と「犯罪や攻撃への悪用」は高位のみとなっています。令和 6 年度とりまとめ案の資料では、これらは「侵害の度合いによらず「高位」にする」といった説明が記載されているため、本編にもそういった記載を加えたほうが良いと思います。
- 「パスワード」の記載ですが、文中ではカタカナ、アイコンでは英語の表記となっており、どちらかに揃えても良いのではと思いました。
- P48 に「代表者等」という言葉がありますが、ここだけで用いられている表現です。P49 に説明書きはありますが、少し気になります。
- P48 のみ、丸付きの数字が黒丸（❶、❷、❸）となっている点も気になりました。
- いま、「容貌の確認」は人間が目視で行うことを前提として書かれているように見えるのですが、今後は対面であっても機械的な照合が広がることも想定されます。機械的な照合が行われることも踏まえた記載を検討しても良いと思います。
- 機械ではなく目視での容貌の確認の際も、適切な訓練を受けた担当者が確認をすることを法令で求めている国もあります。そういった見方等を教育する場があってもよいのではないでしょうか。
- 目の前の申請者が写真とは別人のように思えても、身元確認の担当者が遠慮して指摘できない、といったような問題も発生し得ます。技術的な問題以外にも総合的に考える必要があると思います。
- 入場ゲートなどでは機械判定を導入することで、「機械が判定しているため入場できない」といった説明を従業員が説明しやすくなる、という話も聞いたことがあります。
- P22 等に記載のある「レベル 1」などの表現は、令和 6 年度とりまとめ資料と同様に「身元確認保証レベル 1」、「身元確認保証レベル 2」といった表記に変更したほうが良いと思います。
- P44 の「補完的対策の検討、保証レベルの見直し、例外措置の検討を行い、対象手続で採用する本人確認手法を決定する。」とありますが、検討した結果を明文化することも記載したほうが良いのではないでしょうか。

<u>閉会</u>

- （事務局）デジタル庁が発足してから、本人確認ガイドラインの改定は必ず必要となる事項でした。委員の皆様のご知見と、有識者会議での議論の積み重ねによって改定案のとりまとめまで至ることができ、誠に感謝しております。今後予定しているガイドライン解説書の作成や、各省協議の結果確認などでも、引き続きお力添えいただけますとありがたく思います。
- （事務局）今年度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）