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 5 回）
令和 6 年 2 月 27 日（火）18:00～20:20

（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<br>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<br>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<br>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<br>FIDO アライアンス執行評議会・ボードメンバー・FIDO Japan WG 座長<br>W3C, Inc.理事（ボードメンバー） |

（挨拶・事務局説明）

- それでは本人確認ガイドラインの改定に向けた有識者会議の第 5 回を始めさせていただきます。お忙しいところをご参集いただきましてありがとうございます。
- 本日議論いただきたい論点は大きく 2 点ございます。1 点目は前回までの議論を基に作成した「令和 5 年度中間とりまとめ（案）」のご確認を、2 点目は今回追加でお持ちしたフェデレーションに関する論点協議をお願いしたく考えています。

議題（1） 令和 5 年度中間とりまとめ（案）について

事務局より、資料 1 に基づき令和 5 年度中間とりまとめ（案）について現時点での検討結果を説明し、有識者による自由討議を行った。

（有識者意見）

改定ポイント①：ガイドラインの適用対象と名称を変更

改定ポイント②：ミッション遂行などの「基本的な考え方」を解説

事務局より、資料の修正点、これまでの議論内容をとりまとめた「今後の検討事項」等を説明し、有識者からの追加の意見等を確認した。

- この会議ではマイナンバーカード以外の本人確認書類についてあまり議論ができていないように思います。NIST の考え方では証明書ごとのエビデンス強度を明らかにした上でその組み合わせにより保証レベルを決定していますので、マイナンバーカードありきの議論になってしまわないよう注意して後続の議論ができれば良いと思っています。

改定ポイント③：本人確認の枠組みを定義・解説

事務局より、資料の再検討結果、これまでの議論内容をとりまとめた「今後の検討事項」等を説明し、有識者による自由討議を行った。

- モデルはうまくまとめられており、そのおかげで問題点にも気づきやすい内容になっていると感じます。まず、属性プロバイダを明示したほうが良いと思います。ウォレットモデルにおけるIdP はウォレットでして、この図中に「ID プロバイダ」と書かれている枠は IdP ではなく属性プロバイダと捉えるべきです。ウォレットモデルと認証連携モデルはよく似ており、属性プロバイダを明示することでその差も明確になると思います。
- 用語の使い方ですが、非認証連携モデルでも「RP」という言葉を使うのか？という点は気になりました。また、ウォレットモデルの Issuer、Holder、Verifier、Credential などの用語は NIST とは異なる意味で使われていますので、全体の整合性を考慮しつつ用語の名称を再検討いただくのが良いと感じました。
  - 事務局：仮に用語の定義があいまいな状態で NIST SP 800-63-4 が公開された場合、我々としてはどのような対応を取るべきでしょうか。
  - 有識者：NIST の定義があいまいだったとしても、他国に対して相互運用のための対応表を作成することに備え、きちんと定義しておく必要があると考えます。
- P22 に「Issuer と Verifier を分離できるモデル」と書かれていますが、「Verifier の情報を Issuer に渡さないことが可能なモデル」とする方が正確だと感じます。
- P18 の「身元確認」のところに「当人性」という言葉が使われていますが、当人認証における「当人」という言葉の意味が異なるので気を付けていただきたいです。
- ウォレットモデルは本人確認というよりは資格保持の確認に着目したものであり、属性情報のマッチングのみでは発行された証明書に対する妥当性確認が不十分であるため署名を付けて Verify する、ものです。ですので、今回の改定時に無理に入れる必要性は低いと考えています。
- 「認証連携」という用語は「今後の検討事項」に含めて先送るという話でしたが、この中間とりまとめの資料でも「ID 連携」という言葉に置き換えてしてしまっても良いと感じます。
- ウォレットモデルの図では Issuer の箱の中にも Verifier が書かれていますが、この Verifier が「当人認証」を行う意味ならば、Issuer の枠にも必要ではないかと思いました。また、Verifiable Presentation を渡して検証する意味での”Verify”は、単に資格情報を検証するという意味ですので、当人認証を行うという行為の”Verify”とは分離すべきではないか、と感じました。
- 資格情報を暗号学的に検証するという意味での Verify と、NIST において当人認証を行う際の Verify は別物ですので、それらが混同されて議論されないようにするためにも、他のモデルと無理に並べるべきでないと思います。ウォレットモデルが今後着目すべきモデルであることは間違いないので、認証連携モデルなどと並べず別途記載するという方法は検討されてもよいと思います。
- この資料でウォレットモデルに言及しているのは、デジタル庁で並行して検討を進めている DIW（Digital Identity Wallet）の影響を受けて追加したものなのか？とも読み手に受け取られるのではと感じたのですが、実際はどうなのでしょうか。
  - 事務局：今回の資料のウォレットモデルは、あくまで NIST SP 800-63-4 Second Public

Draft での追加予定に備えて整理を行ったものとなります。並行している DIW の取組みから影響を受けたものではありませんので、その点についてはきちんと説明が必要と認識しました。

- 用語を含めて、ほかの 2 つのモデルとは切り離した位置付けであることを明示した方が良いかもしれませんね。
- 24 ページの記載ですが、現時点で民間側から認証結果や属性情報を受け入れるユースケースが明確に存在しないのであれば、24 ページの記述を削除することでシンプルな話になると感じました。
- 私が関わった業務ではデータ入力ミスの発生率が一定数あることを実感していることもあり、民間が持つ属性情報の連携の可能性を強く感じています。そのため 24 ページの存在は喜ばしく感じました。
- 今までの議論を基に厳格な保証レベルが定義され、そこから発行される Issuer の Verifiable Credential があり、認証に必要なもののみの開示が実現することは大いに意味があるので、24 ページの存在自体は問題ないと思います。
- 24 ページ内の 2 点目のトラストフレームワークの記載ですが、政府外のみだけでなく政府内での連携でも必要な内容ですので、記載について再度検討いただくのが良いと思います。また、ウォレットモデルの図示する場合であっても、身分証を提供する者を明確に位置付けることができる、権威的源泉が複数あり得ることを示すことができる、などの理由から属性プロバイダの追加は効果的であると思います。
- 属性プロバイダとして一般化すると身元確認とは少し違った認可の話になるのではと思いましたので、分けて議論するのが良いと感じました。また、トラストフレームワークについては府省共通研究開発システム（e-Rad）を大学の ID で利用できるようにするといった、実現が期待されるユースケースが存在していますので、24 ページの赤枠部分は残していただきたいと思っています。
- 属性プロバイダの利用方法によって変わってくる話だと思います。今後のために入れておくのは良いと思いますが、全ての属性プロバイダにおいて同じレベルの身元確認がされるわけではなく、属性提供の前提として別の当人認証が必要な場合もあるため、記載を見直していただく必要はあるかと感じました。
- ウォレットモデルについては前回までの議論でも、NIST SP 800-63-4 Second Public Draft でどのような形で登場するかに注目することとなっていたと記憶しています。
  - 事務局：現在の案は、改定版公開までの今後の期間、公開後の見直し頻度、改定版ガイドラインの寿命などの観点で検討した結果、今回の改定版で入れておいた方が良い、という意見に基づく結果となっています。
- タイムスパンも考慮する必要がありますし、身元確認保証レベルについての解像度も上げる必要があると思っています。今後の集約等により現行ガイドラインのままでは保証レベルについて表現しきれなくなると思っています。属性単位での保証レベル、という話も考えなくてはならなくなり、粒度感についてあたりを付けた上で議論を進めないとまとまりきらない気がしています。
- Verifiable Credential についての議論は難しいですが、今後きっと役に立ちます。注目が高まっていく領域であるため扱うことについての意義は理解するのですが、少なくとも ID プロバイ

ダではなく属性プロバイダであるべきです。また Verify と Credential という言葉があちこちに出てくるので、一般の読者が文脈ごとの言葉の意味を正しく理解できるように配慮して検討を進めていくことが重要だと感じます。

- 「今後の検討事項」にある認証連携モデルと非認証連携モデルのハイブリッドモデルの検討についてですが、例えば一人につき一度の申請しか認められないようなユースケースにおいて、個人に対し複数 ID の利用をさせないために名寄せを行う必要があると思うのですが、解決するための技術の目途は立っているのでしょうか。
  - 事務局：具体的な対応策の検討には至っていないのが実際のところですが、その検知の可否は、どのような身元確認を行うかにもよると考えています。特に、マイナンバーを利用しない手続については検討が必要であるとの課題認識をいたしました。
- 本日の後半でフェデレーションについての議論があると思いますが、そこでテクニカルな話に留めて読者に検討を委ねるのか、実際のサービス連携をまたがってユーザーの一意性を担保するために必要なことまで記載するのか、そこ次第だと思って聞いておりました。
- 「技術的に確立しているか」という問いは、いま研究段階にある技術もあり、厳密には難しい面があると思っています。高い信頼性を持って誰もが使えるようなものはまだ存在しないように思いますが、世界中の技術者により研究が進められていることは確かです。
- 実現の可能性がないから記載すること自体が滑稽であるという話ではないと理解しました。
- 19 ページで政府の IdP と民間の IdP を積極的に分ける理由は本質的にはなく、単純にどのトラストフレームワークに属しているかというだけの違いだと思っています。
- 透明性や品質保証をガバナンスしていくためのトラストフレームワークを作るべきであるか、ということを課題として残すことは良いと思いますが、おっしゃるとおりだと思います。
- 本日は最終回だと認識していますが大丈夫でしょうか。
  - 事務局：本日いただいたコメントについて、現在の取りまとめ案の記載に大きく問題がある部分については年度内に修正を行いますが、追加の検討が必要なものについては今後の検討事項として来年度への申し送り事項とすることを想定しています。

<u>改定ポイント④：保証レベルと対策基準の一部を見直し ― 身元確認保証レベルの見直し</u>

- 29 ページの「生体情報の比較」が Biometric Authentication のことを指しているのであれば、その方法としてリモートでの容貌確認が記載されていることに違和感があります。Biometric Authentication でなく目視での容貌確認という意味であるならば、注釈部分の生体情報の記録（Biometric Collection）という部分が矛盾していると感じます。
  - 事務局：ここで意図しているのは後者の容貌確認のことでして、例えば身元確認した際の顔写真を保存しておくといった内容を想定しています。NIST の言葉と無理に紐づけず、意図どおりの記載となるように見直したいと思います。
- 32 ページの生体情報の偽装について、マスク着用による容貌の偽装は生体情報の偽装と異なるものであり、後者についてはうまくまとめられたドキュメントが存在しますので整理して紹介するのが良いと思います。
- 33 ページで身元確認保証レベル 3 に対し必要な本人確認書類の数について言及されていますが、例えば真贋判定機を利用する場合は1点、しない場合は 2 点、としているような例もあ

るようですので、今回のガイドラインでも詳細を書いておいた方が良いと思います。

- 30 ページの身元確認保証レベル 2 の詳細化の部分で、レベル 2B とレベル 2C のように認証強度と詳細レベルの関係が逆転しているように見受けられる部分があるので確認してもらえればと思います。また、物理的な検証の券面の写し（コピー）を収集するだけでは確認になりませんので記載を修正いただければと思います。
- 29 ページの表の Verification の部分で検証方法のグルーピング方針が当人認証保証レベルとずれがあるように感じられます。c）と d）を別グループとし知識・生体・所持の認証の 3 要素としておくと、今後新たな方法が登場した際にも対応が容易になると考えます。
- 組合せ数の少ない 4 桁の暗証番号は本人でなくてもマッチしてしまう可能性が比較的高いため、保証レベルを高める場合には容貌の確認を追加する、ということだと思います。
- 本人確認書類と申請者の紐づき確認において 2 要素で検証できれば信頼度は上がるといった考えが適用できそうですね。
- 以前も話に出ましたが、当人認証保証レベルを先に持ってくる方が良いのかもしれませんね。Validation はきちんと実施するが Verification は若干適当であるような事業者も見かけますので。
- 当人認証保証レベルについては「パスワードのみでは NG」、「2 段階認証も NG」など大分答えが見えてきていますが、身元確認保証レベルについては国によって本人確認書類も異なっていることもあって整理するのが難しく、その分重要性も増していると感じます。身元確認が前提となって当人認証に利用可能なクレデンシャルが発行できるわけなので、私は今の順で良いような気がします。
- Verification には Authentication の要素が多分に含まれているので、きれいに分けることは難しいのかなとも思います。
- NIST SP 800-63-4 では Verification という言葉が 2 つの意味で使用されているので注意が必要です。また、顔写真を保存するのは多重登録を防ぐための意味合いがあるのですが、現在の記載ではそれが読み取れないと思いました。
- 券面コピーの収集の必要性は私も理解しています。そして、保持期間、収集する目的、破棄の条件についても記載しておくことが重要だと考えます。
- 個人情報なので収集する場合は安全管理、アクセス管理、不要になった場合の破棄・保管期限は必ずセットで検討すべき事項だと思います。
- 30 ページの身元確認保証レベル 2 を 5 段階に細分化することについてですが、このように細分化されることは理解しつつも、実際の運用において機能するのか、ということが気になりました。また、32 ページの表の見方で迷ったところがあり、凡例の表記が正確性に欠けると思われる部分が確認できましたので、記載の見直しをお願いしたいです。
  - 事務局：ご指摘のとおり、凡例が正確でない点について修正させていただきます。
- Presentation Attack の定義については、事務局内で一度確認してください。
- NIST の Biometric Collection の記載ですが、顔認証、顔写真の比較、指紋の比較といったような手法が書かれており、入国審査で行うように顔の写真を撮ってパスポートの画像と比較する方法でも IAL3 を認めているようです。Presentation Attack に対する耐性や Liveness Check はリモートの場合は特にチェックせよとしていますが、それほど区別されていません。生体情報というと CSP の都合で Biometric のテンプレートを収集して記録する話から、単に

窓口に出頭した人の顔写真を保存しておくというものも含まれています。目的を書いておくことが重要だという話が先ほど出ていましたが、生体情報の収集を行う目的はアカウントリカバリーにおける IAL3 の身元確認を容易にすることなので、それはしっかりと書いておいた方が良いと思います。

- c)の「本人確認書類の認証機能(暗証番号等)による認証」というのは、現行のガイドラインに書かれていたものでしょうか。それとも今回新たに追加するものでしょうか。
  - 事務局:現行ガイドラインにはモデルとしての記載はなく、今回マイナンバーカードを意識して新たに追加したものとなります。
- マイナンバーカードを意識した記述だということは理解できるのですが、銀行のキャッシュカードの 4 桁の暗証番号とマイナンバーカードのような耐タンパ性のある領域をアクティベーションするための 4 桁の暗証番号とでは明確に意味が異なるので、その点を読者が読み取れるように記載する必要があると思いました。またマイナンバーカードを意識したということであれば e)と内容があまり変わらない気もしており違和感がありました。暗証番号の入力はあくまで、IC カードをアクティベーションしその IC カードの機能で電子署名なり券面画像なりをアプリ経由で取り出すためのものだと理解しているので、c)はそれ自体を手段としてしまうと勘違いされてしまいそうだなと感じました。
  - 事務局:ご認識のとおり実際には e)を実施するために暗証番号を入力しているのですが Verification と Validation に分離した際にどのように機能しているかを表現するために現在の記述としておりました。しかし懸念されているとおり誤解を生む可能性があると感じましたので再度検討させていただきたいと思います。
- 28 ページの身元確認保証レベル 1 について「郵送等での・・・」という記載があり、これは登録コードの利用を想定していると思われますが、本人限定受取郵便等を利用した身元確認も含まれると誤解を招く可能性がありますので、記載方法を変えていただいた方が良いと思います
- 基礎的な質問で恐縮ですが、32 ページの表が何を目的として書かれているものなのかを説明していただけますか。読者はこれを見て何を判断するのでしょうか。
  - 事務局:32 ページの表は、今まで検討してきた 29 ページ記載の内容に対して、保証レベル 1、2、3 の脅威耐性にどのような差があるのかという点を整理したものです。ガイドラインの読者がこの表を見て何かを判断するといった使用は想定しておりません。
- 保証レベル 3 の列にチェックのある a)と e)が揃った場合のみ保証レベル 3 を認めるという見方で合っているでしょうか。
  - 事務局:ご認識のとおりです。

<u>改定ポイント④:保証レベルと対策基準の一部を見直し ― 当人認証保証レベルの見直し</u>
<u>改定ポイント⑤:リスク評価プロセスを全面的に見直し</u>

事務局より、資料の修正点、これまでの議論内容をとりまとめた「今後の検討事項」等を説明し、有識者からの追加の意見等を確認した。

- 当人認証保証レベルの対策基準を ISO/IEC 29115 と比較してみたのですが、不足している脅威は 4 点でした。Credential Theft、Credential Sharing、Credential Duplication、Offline

Guessing の 4 点を追加いただくと、さらにきれいにまとまると思います。ISO/IEC とも平仄が取れますし、耐タンパ性のあるハードウェアが必要なのは Credential Duplication に対する耐性獲得のため、生体情報を利用した紐づけが求められるのは Credential Theft や Credential Sharing に対する耐性獲得のため、といった説明ができるようになります。

議題（2） 追加の論点協議

事務局より、資料 2 に基づき新たに追加した論点について説明し、有識者による自由討議を行った。

- 「Dynamic Registration は不要ではないか」との説明がありましたが、ウォレットモデルでは Client Attestation を利用した Dynamic Registration が必要になる場合があると思います。次に、Bound Authenticator については、Token Binding がなくなってしまった現在では PIV カード以外に実装手段があるのか、という点に留意すべきだと思います。また、Shared Signaling は Apple などが採用し米国でも注目されているので、改定版ガイドラインが長期的に利用されることを踏まえて入れておくのは良いかもしれません。ただし「必須」とするのはやりすぎで、「推奨」に留めるべきだと考えます。
- 技術的には NIST FAL2 の条件は NIST IAL3 の身元確認結果を NIST AAL3 を用いて流通することに耐えられることとなっており、そのこと自体は妥当と考えます。強いて言うのであれば Trust Agreement は結構重要な事項なので、身元確認保証レベルと当人認証保証レベルの組合せをきちんと検討すべきであると明記するのが良いと思います。Static について記述されていることが最低ラインであり、Dynamic について記述するための検討までは必要ないのではと個人的には考えます。
- Dynamic Trust Agreement と Dynamic Registration は全く別の話ですので、個別に検討が必要だと思います。
- NIST FAL では Assertion に個人情報が含まれる場合レベルに関係なく暗号化が必須となっています。SAML では E メールアドレスが識別子になっていることが珍しくありませんので、認証連携保証レベルの条件を満たすために暗号化が必須となった場合、影響がかなり大きくなります。採用可能な手段として何があるか、条件が追加されるとそこにどのような影響があるか、ということを考えておくことが必要だと思います。条件を緩く設定せよということではなく、影響が出る部分について明記し、実装者側に必要な対応を促していくことが重要だというお話です。
- Shared Signaling の必要性についてですが、今後予定されている RP との連携についてもう少しブレークダウンして、どのようなことが可能になるかを具体化してもらえれば、適切なコメントが可能になる可能性があると感じました。
- RP 側の立場としては Shared Signaling があると嬉しいなと思う一方で、個人としては今後連携が複雑化した場合に過去のシグナル送信の同意によって意図しない属性情報の更新が行われてしまうのではないかと少し気になりました。
  - 事務局：Shared Signaling は変更の通知が目的であり、属性情報の書き換えを行うためのものではないためその点は問題ないかと思います。
- Shared Signaling についてはガイドラインから実装を促すことよりも、実際の IdP のインターフ

ェース仕様書などで規定して、それを利用するRPが増えていくといった世界観の方が重要だと思っています。現在進行形の技術だということもあり、ガイドラインへ記載されることと実装時に採用されることにはあまり関連性がないのではないように思います。必要な仕様であれば、IdPの設計者がインターフェース仕様書への追加を検討するはずです。ただ、悪い影響を生むものでもないので、控えめに記載されている分には問題ないと思います。

- 民間の企業でも金融庁などの関係省庁から出されるガイドラインに従ってやっているビジネスはいくつもありますが、ある時までは問題ないアカウントに紐づいたものが制裁リストに入ったことについてSignalingがあれば適切なハンドリングができるといった応用がありそうな気はします。
- 事務局：冒頭説明のとおり、追加の論点については本日いただいたご意見を踏まえつつ、今後も検討を進めていきたいと思います。ありがとうございました。

<u>閉会・今後の予定の案内</u>

（事務局）

- 第一線でご活躍中のみなさまに大変濃い議論を展開いただき、事務局としても充実した一年となりました。NIST SP 800-63-4 Second Public Draftの公開など来年度もなかなか大変な状況が続くことになりますが、この分野は米国や欧州において国際的に検討を進めていこうという機運も高まっており、重要性が明らかに増していると思います。一方で欧州でのDIW検討の遅延やステークホルダーの増加により、今後より状況が流動的になるのではないかという危機感も持っています。来年度は論ずべきことと基準として落とし込むところの峻別を意識しつつ、国際的な貢献にも繋げられるよう意識的にアウトプットをしていきたいと思いますので、引続きご支援のほどよろしくお願いします。
- 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）