

本人確認実務の課題・事例・手法とそのガイドラインに関する有識者会議(第1回)

令和7年9月30日(火)18:00~20:00

(出席者)

狩野達也	株式会社メルカリ Foundation and Identity Principal Engineer
後藤聡	TOPPAN エッジ株式会社 データマネジメント統括本部 DX ビジネス本部 RCS 開発部 部長
崎村夏彦	NAT コンサルティング合同会社 代表社員
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) 開催要項説明

事務局より、資料1に基づき説明を行った。

議題(2) ガイドライン解説書の記載内容(案)に関する協議

「身元確認手法の具体例について」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)

- コラムというのは身元確認手法の具体例の間に挟んで掲載するのでしょうか。
  - (事務局)読みやすさを考慮して、関係する手法の近い位置に挟む形で掲載できればと考えています。
- ガイドライン本編ではフェデレーションを新しく追加するとのことでしたが、解説書において具体的な方法や留意事項などをまとめたりしないのでしょうか。
  - (事務局)本日の会議は身元確認と本人認証の議題としてお持ちしていますが、実際の解説書にはフェデレーションについても掲載予定です。
- 改定は比較的短期間で行うとのことですが、例えばどの程度のスパンで、こういった手続を行うか、その運用というのはガイドラインそのものに記載するのでしょうか。何かしらの手法

に脆弱性が発見されて、その手法を採用していた場合にどう扱わないといけなかが、わかるようになっていると良いと思います。

➤ (事務局)ガイドラインそのものに改定の運用を記載する予定はありませんでしたが、ご意見を受け検討したいと思います。

- いろいろな手法が記載されていますが、具体的に何をどう選べばいいのかが、Yes/No チャートではないが、要件から選択できるような形が取れると良いと感じます。
- 例えば外国籍の方の在留カードやパスポートなど申請者の検証を機能として持っているドキュメントがあるということを紹介しても良いのではと感じます。
- P12 の実物のマイナンバーカードの券面事項入力補助 AP のプライバシーに関して「特になし」となっていますが、スマホ搭載の方は選択的開示ができて良いと書いてあるので、物理の方は選択的開示ができないことが、プライバシー上の考慮事項ではないかと思います。
- P38 に「レベル 1 に満たない」と書かれているケースがありますが、使ってはいけないというように見えてしまいます。使っても良いが、申請者の検証を必ず行うという記載にしないといけないのではないのでしょうか。レベル 0 を使うケースは行政手続においては存在しないと考えて良いのでしょうか。
  - (事務局)行政手続という意味では、身元確認を行わない手続はほぼ無いと想定していますが、行政手続に限らない一般の行政サービスにおいては、レベル 0 を用いるケースもあり得ると想定しています。
- そういったケースは今回のガイドにどこまで含めるのでしょうか。匿名のケースがここに記載のものに該当するのであればそのように書いた方が良く、あくまでレベル 1 から 3 に押し込めることをゴールに書くのであれば、レベル 1 に満たない場合はどうするのか、書き方を変えた方が良いと感じます。
- P48 のスマートフォンのクレデンシャルについて、1 枚だけ発行されていることというよりは、「発行状態が正しく管理されていること」といった書き方が良いのではないのでしょうか。1 枚なのか、2 枚でも 3 枚でも、いつどこに誰が発行したかを発行者が把握している状態、という方が正確なのではないかと思います。例えば US の例でいうと、mDL を複数枚発行する場合は、複数枚をしっかりと管理せよとガイドに書かれています。厳密に 1 枚だけでならないかということではなく、本質的に言えば本人に対して発行されているということがわかっている状態のものであることが必要ということのはずです。
- eIDAS で eID をバッチ発行した場合は 1 枚なのか、という話になります。これからマルチデバイスが当たり前の世界になってくると、結局その人のキーだとわかっているものが複数デバイスの中にあって、そこにバインディングされていれば問題ないということになるように思います。もちろん、それによる貸し借りのリスクが増えることは認識しないといけません。
- 1 枚であるかどうかというのは、区別をして書く意味もあると思います。金融機関サービスで自然人が口座を 1 つしか持てないというのも、そうした意味だと思います。マイナンバーカードでもスマホ搭載するときに別のスマホに搭載しようとする、それまで搭載されていた方が

らは消去されます。管理することはもちろん大事ではありますが、1枚であるかどうかというのも、これからいろいろなシーンで大事になる場合があります。

- 郵送と住所への到達確認のところで、例で書かれている、本人確認書類を郵送してもらい、その住所へ確認コードを郵送するというケースは、実務ではあまり見られないかと思います。順番が逆になりますが、行政機関から申請書にキーのような番号や、住所・氏名等を印字したものを郵送し、それに対して申請者が追記、署名等したうえで、本人確認書類を添付して郵送してもらうことで、住所への到達確認を行う方法が良いのではと思いました。民間ではこの方法で、申請者のリストを持ち確認していくことが実務としてあります。
- DS-511 では、「本人確認」をどう定義していたでしょうか。申請者を一意に識別するとともに、その実在性を確認する、ということだけだと、例えば公的個人認証を使う場合はシリアルナンバーだけで十分なはずで属性情報はいらなはずです。本質的には、本人確認と言われているものは、その業務プロセスにおいて必要な属性を確立することだと思います。ここで言っているものが、何のための本人確認のガイドブックを書こうとしているのか、ということは、もう少し明らかにした方が良いのではと思います。
- 元となるクレデンシャルの、例えばアメリカだと mDL の発行プロセスですが、それがどれだけ信用できるのかという問題があります。電子署名された画像が入っていると言っても、例えばモーフィングアタックされている画像であったら、2 人の人が使えるということになってしまいます。本人確認書類の発行時のリスクについて、どこかに書かなくても良いのでしょうか。日本は公文書は真正に成立したものとみなす国であるので、正しいと言い切ってしまうというものもあるかもしれませんが、アメリカの金融機関などでは、州によって発行プロセスが違っているので、どのくらい信用できるのか、追加的な確認をしなければならないのでは、ということを考えています。mDL を発行しているところは責任を取ってくれないので、金融機関がそういうところまで考えています。
- 今年の 8 月に NIST から NISTIR 8584 という、政府機関等に対するガイドラインのようなものが出されています。発行のときにも本人確認のときにも、モーフィングのことを考えようというのが出てしまいました。今までは、あまり表に出ないような形で対策を取ろうとしていたところがありましたが、そういったものが出てきているということは、例えばコラムなどで実施担当者に対する訓練というところで、そういう攻撃方法があるということを経験しておいた方が良くないかもしれません。
- 発行時の対策というと、ライブキャプチャーか、あるいは信頼できるフォトブースで写真を撮るしかなくて、controlled environment になります。今すぐできるかというところもあるでしょうが、そういうことも考えていった方が良くないということ、ここに入れるのもありだと思います。
- 全幅の信頼は置けないということをおっしゃることは良いと思います。
  - (事務局) Verifier としてどのように意識すべきであるかということも扱いがあると思います。ディープフェイク等の話も含めて、いろいろなところでフェイスシャルイメージの成

形がかつてなく容易になっているということ、Verifier としてどう意識すべきか、それによってどのような攻撃が想定されるか、というところのモデリングまでは、この文書のスコープであり得るかと思えます。ただ、身分証がモーフィングアタックを受けているだろうと推定するのは難しいところもあります。

- ガイドラインを誰が読むのかという事には関連しますが、書類の発行者に関してちゃんと整理するのであれば、自治体を含めたいろいろなところが出す本人確認書類を整理したドキュメントを別途考えるという手もあるのではないのでしょうか。
- European Digital Identity Framework における、QEAA Provider の認定要件などは、それに類するものです。マイナンバーカードでは、例えば住所は変えていない人も普通にいます。
- 一意に識別するだけであれば識別子だけで良いはずで、そうではなくて住所を取るのであれば、正しい住所を取る必要がある業務がその裏にあるはずです。
  - (事務局)法的義務として行っているものもあれば、債権管理やリスク管理のために行っているものもあると認識しています。
- 例えば、この間の日経の一面では、金融機関が電力会社のリストと突き合わせるとありました。
- そうなると、正しい住所とは何か、という話になってしまうと思います。
- 逆に言うと、限界はちゃんと理解する必要があります。マイナンバーがなかったころの基本 4 情報における住所というのは識別子の一部であって、居所ではありませんでした。マイナンバーがある現在、ここで言っている住所というのは何なのか、ということを受け取る人間は考えて、それをどう使うのかということも、本当は考えなければならぬ、ということはコラムにぴったりなものだと思います。
- P33、34 の写真付き本人確認書類の対面確認の部分では、トレーニングをやることなどの話が書かれていますが、コストをかけて頑張っても、保証確認レベルは 2 となってしまいます。手間がかかる割に、という手法となりますし、身分証に関しての不正や改ざんが高度化しているという話も受けた中で言うと、この方法は積極的には採用せずに、前段の他の手法というのをできるだけ使ったほうが良い、ということをもそのまま書いてしまってもよいのではないのでしょうか。
- 対面確認に偽造検知のための機械を組み合わせる方法があるだろうと思っています。一方で、前に書かれている対面確認アプリの方がそれよりも良いという話が示されているのかと思います。民間事業者において、窓口に改ざん検知の機械を置いて確認するというのと、あるいは対面確認アプリをそれぞれの窓口の担当者の方が使うのでは、コンパチが効くといえますか、移行が進むのでしょうか。
- 移行が進むと思っています。スマートフォンで正当性が確認できるというのは、テクノロジーに非常に可能性を感じています。
- 本編が Normative であって、それに対する Informative なガイドラインということで、本編は行政手続のためとなっていますが、このガイドラインもあくまでもその範囲にするのでしょうか。

これが民間にも役に立つものであるとか、含んでいないと思いますが自然人のためだけじゃなく法人も含んでいるとか、こういったスコープについては、ガイドラインの冒頭に記載があって良いのではないかと思います。

- 法令・省令その他に照らし合わせて、ここに書かれていることがどういったニーズにミートするのかというのも書いた方が良いのではないのでしょうか。法令や省令との関係等をガイドラインの中に書いていただいたら、非常に使い勝手の良いガイドラインになるのではないかと思います。
- 関連して、利用者証明用電子証明書を使うシーンには可能性を感じつつ、利用者証明用電子証明書で申請を確認し、基本 4 情報を取るという組み合わせをすると、DS-511 におけるレベル 3 を満たすというのはわかっていますが、残念ながら法令・省令等では同等の本人確認と言えるという記述はない、という理解です。目的によっては使えますが、目的によっては満たせない、という状況があると、書いた方が良いのではないのでしょうか。
- 署名用電子証明書を使った本人確認は、実物のマイナンバーカードでも、iPhone のマイナンバーカードでも、来る Android のマイナンバーカードでも実印相当であると言われることがしばしばありますが、その目的は基本的には否認防止も含めた署名であるから、おいそれとやらせるものではない、ということが発言される先生方もいらっしゃいます。そうすると、このガイドラインの中で、この手法を積極的に推奨するレベル 3 であるというのか、実印を押させるのはやめましょうというのか、熟考するべきところではないかと思います。コラムなのかどうかは別として、そういったところも触れた方が良いと思います。
- 写真付き本人確認書類の対面確認の訓練の話は、実際に差が出得るので、レベル 3 にはできないと思います。そのため、訓練をするべきだということを積極的に言うよりは、限界があるということを明記した方が良いのではないかと思います。
- P7 の本人確認する検証手法として、「信頼できる情報源への照会」が入っています。これはあっても良いと思いますが、「QR コードなどにより」と実現方法が書かれてあり、それで本当に信頼できる情報になるのか、は疑問が残ります。
- P8 に「対面での容貌確認、非対面での容貌確認又は暗証番号による」とありますが、対面でも非対面でも容貌の確認か暗証番号か、どうかかっているのかわかりにくいのですが、両方にかかるはずなので、後ろの方との一貫性で言っても直された方が良いと思います。
- レベル 4 に相当する証明書でやたら署名させるものではないというのは、以前から言っています。プライバシーコンシダレーションなので、プライバシーの中に書いた方が良いです。プライバシーの部分で、特になしとしている部分が多いですが、必要のない情報を取ってしまうことは、確実にプライバシーに関するコンシダレーションになります。そうすると iPhone のマイナンバーカードの優位性というのも明らかになると思います。
- 公的個人認証法が挙げっていますが、電子署名法も挙げた方が良いと思います。署名行為に該当する可能性があり、その場合は署名の対象物が明らかにならなければいけないと言われていて、それは留意点であることは間違いありません。また、認証に電子署名を使うこと

をあまり推奨しているように誤認されないほうが良いと思います。

- 手法の掲載の順番や構成は工夫された方が良い気がします。掲載順番が推奨順に見えてしまいます。
- 実際には、1つの手法だけしか実装しないということはないはずで、複数の手法が候補として10個挙げられていますが、どれとどれを選ぼうか、要件はこうだから、というときに、一覧性があるってわかりやすい方が良いと思います。例えばレベル2という業務をしようと思っている場合に、レベル2に該当するものをフィルタリングするような見せ方をした方が良いと思います。
  - (事務局)実際のガイドラインでは順番や見せ方を再検討いたします。また、手法の選び方を解説するようなことを検討します。
- P11の券面事項補助入力補助APはマイナンバーを取得する前提で、かなり用途が限定されると思います。例えば利用者証明用電子証明書と組み合わせて使うパターンを切り出しても良いのではないかと思います。
- 1から9の手法はいずれも、顔写真付きの本人確認書類を持っている人が前提になっています。コラムで顔写真付き証明書を持っていない人の記載があっても良いのではないかと思います。
- 本人限定受取郵便の部分は、特定事項伝達型にのみ言及されているが、他にもパターンがあるはずで、詳細を知らない方もいらっしゃるでしょうし、法律上のものとそうでないものも名称的に混ざっているの、その点は解説していただけたらと思います。
- マイナンバーカードによる手法が中心になっていますが、免許証、在留カード、特別永住者証明書もICチップが載っていて、法令に照らしたときに使ってよいとされているものもあります。こういったICチップを使った手法というのが、犯収法の世界では撮影手法の代わりに使っていく手法の2つのうちの1つになっていますので、ここをどう表現するのかは考えても良いと思います。
- 免許証の中の顔写真はcontrolled environmentであるため、顔写真照合をする必要があるような、要するに貸し借りに対する耐性を求める時には有用なものだと思います。
- 行政手続に限定するにしても、何を受け入れるかというのを行政は決めないといけません。そうすると認定プロセスとかが走ってしまいますので、行政機関は確保しておいた方が良いのではないかと思います。認定とまではいなくても、日本版のmDLとかデジタル学生証とかが、もう少し地位が高くて良いのではないかと思います。特にモバイルの上で動く身分証については、考える価値があるかもしれないと思います。
- P48のところの記載から、スマートフォンに入っていくものの中で、オーソリティがしっかりしていれば、このガイドラインがそれを排除するものではないと考えています。
- 住民票は、昔は誰でも書き換えられて、書き換えられた住民票の住所の確認などは一切していませんでしたから、全て自己申告データに基づく証明書でした。
- NIST SP 800-63も本来は、Credential Issuingのための本人確認ですので、何のための本人

確認なのかということ意識した方が良いです。

- 貸し借りへの対応に必要な場合は追加の容貌確認を実施すると書かれていますが、読み手としては実際に使える容貌確認の方法は何なのか、ということと、その強度はどの程度なのか、ということが気になると思います。ガイドライン全体を通して理解すればわかる話なのですが、どこか一箇所に書いてあると良いかと思います。例えば対面の話で言うと、対面アプリで取得した情報とその容貌を比較するときと、マイナンバーカードを渡されてそこに記載されているものと容貌を比較するときは、強度が違います。非対面で言うと、ここに書いてある、非対面で使える容貌確認はレベル 1 の 9 番目だけだと思います。非対面の容貌確認をした方が良く書いてありますが、具体的にどのようにするのか、ということが気になりました。

#### 「本人認証手法の具体例について」について

事務局より、資料 3 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)

- パスキーの留意事項にアカウント回復方法に関する記載がありますが、アカウント回復方法が脆弱な手法であれば、他の認証方法を導入しても同じですので、パスキー部分に記載するのであれば、他の部分にも記載すべきかと思います。
- 同期パスキーを使っていた場合の考慮事項として、パスキープロバイダーに依存する点があります。パスキープロバイダーが乗っ取られた場合などに自分のサービスにも影響が及んだとき、どこまで責任を負えばいいのか、全部保証しないといけないのか、それともプラットフォーム側に持ってもらえるのか、ということらを考慮する必要がありますので考慮事項として挙げておくべきかと思います。また、クラウドサービスのアカウントが乗っ取られた場合のリスクがあるので、同期パスキーとデバイス固定パスキーのリスクや考慮事項は大きく違います。読む側が、使う側というよりも導入して運用する側の話であれば、同期パスキーとデバイス固定パスキーを解説書の中では区別した方が、むしろわかりやすいのではないかと思います。
- 身元確認の部分でもチャートがあった方が良く、順番を考慮した方が良く、という意見がありました。こちらでもレベル 3 の後にパスワード認証のレベル 1 があり、その後にレベル 2 となっています。何が推奨かそうでないかという意味合いで言っても、やや違和感がありますので、構成は工夫をされた方が良くのではないかと思います。
- ワンタイムパスワードとパスワードの違いとして、パスワードは誤ログインが発生しやすいという点があります。ワンタイムパスワードを加えることで、誤ログインは圧倒的に減ります。プライバシーの観点で非常に有用なので、そういう観点も含めて書いた方が良くのではないかと思います。
- 利用者証明の部分ですが、実物のマイナンバーカード、スマートフォンのマイナンバーカード

のマイナンバー利用者は、利用者の目線でいってもどうやって使うのか、というところがあるので、わかりやすく書いた方が良いと思います。

- パスキーに関して、最近話を聞くのは、パスキーを設定するシーンで適切な身元確認が行われていない、第三者が被害者のパスキーに当たるものを攻撃者のスマホに設定するという事例がありますので、それは留意事項として必ず書くべきだと思います。
- 同期パスキーとデバイス固定パスキーの書き分けについては、いずれもフィッシング耐性があり、どこまでディテールを記載するかは、このガイドラインの位置付けに合わせて適切に表現するのが良いと思います。
- 実物のマイナンバーカードでは、プライバシーに考慮事項がないとされているが、X.509 の証明書については Unlinkability がない、つまり Linkability があるので、そこは書くべきではないでしょうか。
- パスキーはシェアリングできるものだとことを理解して使えば良いが、ご存知ない方もいらっしゃるのでは、足しておいても良いと思います。
- パスワード認証の箇所、「暗号鍵は利用しない」と記載があるが、パスワードのことを、weak cryptographic key と呼ぶこともあるので、正確な記述なのかは確認した方が良いと思います。また、P26 も TOTP は明らかに暗号鍵(シード)を利用します。
- P14 のかざし利用は、利用者証明を行ったうえで、その後にかざす 2 回目の話と認識していますが、時間の概念を入れる必要がないでしょうか。短時間の間に連続で使うような場合は本当にダメなのでしょうか。セッション管理の問題かもしれませんが。
- P24 のパスワードについて、異なる混在文字を要求してはならないとか、定期的な変更を求めはいけないとかがありますが、これをやることによってセキュリティのレベルが上がるわけではないという理解です。他に挙げられている秘密の質問はダメですが、混在や定期的な変更はニュアンスを変えた方が良いと思います。
  - (事務局)実装してはならないものと、強要してはいけないものが混ざってしまっていました。秘密の質問はアタックサーフェスを増やしてしまうので禁止ですが、混在の方に関しては強要してはならないであって、使うことを咎めるものではありません。見直しを行います。
- 電子メールの認証コードの送付の件で、結局のところメールの自動転送とか共有をしたいという目的で電子メールの認証コードを使う、という必要があります。行政機関の現場では職員が1アカウントを持っていないというのが未だにあり、そういった人たちが、個人スマホを組織では使えないので転送しているような事例があります。そのレベル感を共有するといえますか、ルールの対応を見せた教育的な内容にしてもらいたいです。
  - (事務局)適切なメールの自動転送、アカウントの共有があるかもしれないということで承知しました。表現は改善します。
  - アンオーソライズな転送はいけないということです。代理人アカウントがないような場合に、秘書が代わりに見るような場合もあります。

- パスワードの定期的な変更を強要してはならないというのは、NIST SP 800-63 には確かに記載がありますが、共用アカウントの場合は例外だと思えます。ISO/IEC 27002 では、頻繁な変更を要求するのは良くないと書いてありますが、それは共用アカウントのようなものを考えて、メンバーが入れ替わるときにも変えないといけないですし、仮にメンバーが入れ替わった時に変え忘れていても、定期的な変更により最大限そこまで止まるということを書いてあります。
- P28 のワンタイムパスワード方式で、メールと SMS が並列に書かれていますが、SMS の方がレベルが一段高いように思えます。記載されているリスクはそのとおりですが、そこに差があるような見え方が良いと思えます。公式アカウント制度がある RCS も選択肢に入るかもしれません。
- P11 のところで、ユーザビリティの考慮事項として、身元確認は良いとしても、本人認証の都度マイナンバーカードを読み取るというのはユーザビリティがあまり高くないと思えます。
- P20 の複数の端末を共有するケースですが、パソコンを利用しているときにスマホに搭載したパスキーで、QR コードで読んで Bluetooth で接続するという認証方法があります。この場合はパソコンを家族で共有していても、その人が使っている瞬間、その人のスマホで認証できます。クロスデバイスユースケースと言いまして、CTAP というものを使いますが、パスキー以外のシーンでも有効に使えるのではないかと思います。これを利用すれば、マイナンバーカードのクレデンシャルはスマートフォン 1 台にしか搭載できませんが、パソコンで、スマートフォンに搭載したマイナンバーカードのクレデンシャルを用いて、本人確認ができる時代が来ると思えます。そういったことを考えたときに、「複数の利用者が端末を共有するケースでの利用は困難」という表現は、いろいろな可能性に蓋をしている気がしますので、書き方については検討してもらいたいです。
- 認証を実行するその瞬間の話が多かったですが、認証完了後のセッション管理に関する話として、侵害されたらセッションを切断するとか、そうした内容についてもガイドラインの中にあつた方が良いのではないかと思います。
- フィッシング耐性についてですが、チャネルバインディングと検証者名バインディングが書かれていますが、これを読んで理解できる人というのは少ないと正直思えます。どちらかという、フィッシング耐性がないものをリストアップした方がわかりやすいのではないかと思います。パスワード乱数リカバリーとかはもちろんですが、Push modification も E メールマジックリンクも利用者の注意に依存する方法です。OTP も書いてあるとおりでありますが、もっと細かく、送る文字の種類を番号じゃなくて文字にするとか、取りうる数が大きいとか、入力方法が違うからといって、フィッシング耐性があるとは言えないということを含めて、説明があっても良いと思えます。

## 閉会

- (事務局)おかげさまで、本日、DS-500 の改定版がデジタル社会推進会議幹事会を無事通

過しまして、長丁場でございましたが、デジタル庁としての新しいガイドラインができました。今回ご検討いただいているところは、まさにこれに魂を吹き込んでいくものになります。カード代替電磁的記録も含めて、そして世の中の証券不正の問題も含め、パスキーやフィッシング耐性に対する世間の関心も非常に高まっているところですので、ぜひこのガイドラインを機動的に出せればと考えておりますので、引き続きご協力のほどよろしく申し上げます。ありがとうございました。

(了)