

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2回)

令和7年11月26日(水)16:00~18:00

(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 セキュア DX 統括本部 デジタルソリューション本部 本部長 兼 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)ガイドライン解説書の記載内容(案)に関する協議

「本人確認ガイドライン解説書の目次(案)及び第4章の全体像」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)

- P12 のメトリクスに関して、本人認証の認証要素を登録する際の情報もあると良いと思います。パスキー等の場合、ユーザーの環境によって登録の成功/失敗が分かれるため、今後パスキーを推奨していくことを考えると、パスキー以外の認証方式も必要かどうかを判定する材料として、パスキー等の登録成功率や全体ユーザーのうち認証要素を持つ割合などのデータもあれば良いと思います。
- P8 の表はガイドライン本編の表をもとにしていると思いますが、ガイドライン本編の方ではリスク特定の考え方とされていて、顕在化した際の影響内容が記載されています。これをどう使うか、想像がしにくいと感じます。特定の考え方を見て具体的なリスクがあることを理解するといった利用法を想定しているのか、あるいは影響があるということから逆引きをする想定なのか、いずれでしょうか。
 - (事務局)逆引きではなく、こういった形でリスクの特定と評価をしてほしいという例示を意図しています。将来的には、実際の評価結果から事例の拡充をすることで、逆引きの

ように使えることも目指したいと考えています。

- そうなると、本編の書き方がわかりやすいのではないかと思います。
- (事務局)本編との記載粒度を含めて確認します。
- P8 のリスクケースにおいて、実在する人物になりすます場合と、実在しない人物になりすます場合の違いを、解説書を読む現場の方が区別できるのか、気になりました。
 - (事務局)表現を修正します。
- P8 において、リスクに応じた「適切な保証レベル」を選択するのが目的ですが、リスクの影響度が高い方に寄りがちになる傾向があるという課題が以前からあるところ、昨年度までの会議にて、ワークシートのようなものを用意するという話があったと思います。それは目次でいうところの、「別紙 2 参考資料」などに添付されるのでしょうか。
 - (事務局)ワークシートを作成する方針は変わっておりません。解説書の一部に位置付けるか、解説書の外部に位置付けるかは内部で検討中です。また、2 年ほど前の有識者会議で提示したワークシート案は、NIST SP 800 63-3 の判定フローをもとにした複雑なものでしたが、DS-511 の 4 章に沿ったワークシートは簡素なものとなる見込みです。
 - 具体的にどういった行政手続で、どのようなプロセスを経てこのレベルを選択した、という事例が共有されるような仕組みは考えているのでしょうか。
 - (事務局)ワークシートを作ることで、類似の検討状況をもとにフィードバックできるようにしたいとは考えておりますが、解説書内に記載することは考えておりません。
- P8 では低位から高位があり、実態上どれに当たるのかがどうしても問題になりますが、サンプル等があるのでしょうか。NIST SP 800-60 では、政府業務の high、moderate、low がありますが、それがいないため、ある程度判断が付くようにしてもらいたいです。
- 手続内容そのものを表現、可視化しないとリスクの特定が難しい場合もあると思います。国家サイバー統括室(NCO)の SBD マニュアルでも、前半のほぼ半分を業務のモデルの書き方が占めています。分量が多くなりすぎるとプロマネやエンタープライズアーキテクチャの範疇になるかもしれませんが、認証の観点から業務をどう整理するか、可視化の仕方なども記載してもらいたいです。
- P12 に示されているメトリクスの情報を収集できるようにしたいとは思いますが、評価できるところが現実的にどれだけあるかというと、専門的なことができないと正直作れないと思います。だからこそ、フェデレーションを使ってほしいとなると思うのですが、強調してもらいたいのは、人間のレビューだけにならないようにモニタリングしてフィードバックをするという点だと思います。
- P7 の「1)リスクの特定」と「2)リスクの影響度の評価」の部分が、実際に使う上で難しい部分だと思います。具体的なケースがある程度ないと、判別がつかないように思います。このマテリアルを誰が読むかという事を考えると、少し齟齬が出てきているのではないのでしょうか。実務手引的な文章でもあるので、ある程度事例ベースであったほうが良いという印象を受けました。

- P8に関して、このガイドラインや解説書を初めて読んだ人にはやや難しい内容と感じました。前のページの、プロセスとしてレベル判定から続く部分はわかりやすいですが、保証レベルを判定する行政官やシステムを設計する人が読んだ場合に、自分たちの出会う状況がどの保証レベルなのか、というのを理解したがるはずだと思います。「顕在化時の影響内容」では、一番下に「登録者のメールアドレスやパスワードが攻撃者に漏洩する」とあり、これはパスワードを使えば必ず当てはまります。実際のシステムの性質に応じてレベルを判断したいと思いますが、ここに記載されているのはシステムの特長そのもので、あまり判断材料になっていないように思います。総合的な影響度「低位」というのも、漏洩しても良いからレベル1で良いと言いたいのか、少しロジックがつかみにくいと感じます。提供しようとしているサービスは、レベル3なのかレベル2でもよいのか、というのは、一番関心を寄せる場所だと思いますので判定のヒントが欲しいです。この1ページに押し込めるのではなく、もう少し判断に役立つロジックと例の充足をした方が良いと思います。
- P12の記載内容はすごく奥が深く、何をもちて完了とするのか、失敗とするのか、にも差が出てくると思います。完了までの時間の定義がシステムによって異なっているといったこともあります。この会議で答えを出すのは難しいと思いますが、解説書はタイムリーに修正していくということですので、知見を蓄えていてもらいたいです。
- P3の内容はガイドライン解説書にも記載されるとのことですが、内部事務等を実施する職員向けの本人確認は別ガイドラインを整備予定ということも記載するのでしょうか。
 - (事務局)その点は解説書そのものに記載する予定はありません。
 - 対象外とあると、何を読めば良いのかわからないので、本ガイドラインが参考にはなるということは記載しても良いのではないかと思います。対象外とだけでは、別のものはあるのか、となってしまいます。
 - (事務局)その点、網羅できるように記載しようと思います。
- P12に関し、生体認証をシステム導入した際に、正しく利用できているのかという問題がありました。本論ではないですが、セキュリティ側ではなく運用側でモニターしながら、うまく利用できていない人を見つけ出す仕組みをやっているところもあるので、そこと併せて使えると良いなと思いました。

「身元確認手法の選定の考え方」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)

- 検討フローの「2)マイナンバーカード以外による手法の検討」まで決めてから「3)実装モデルと実現手段の検討」をする点が少し気になりました。というのも、3の実装モデルを選んだ時点で1と2の手法が定まってしまうので、3のタイミングが難しいと思います。2まで考えた後に3を考えるというのも良いとは思いますが、検討が無駄になってしまう可能性があります。

- (事務局)おっしゃるとおりの部分もあります。3 を先に書いてしまうと「選べるものを選ぶ」という判断となってしまうと考え、まずはあるべき手法を考えられるよう、今はこのような順序としています。
- マイナンバーカードを中心として、それが十分でない場合に他の手段を検討する点はとてもわかりやすく良いと思います。一方で、P19 にて、マイナンバーカード以外の手法は、保証レベルベースでどれを採用するか選択する、という書き方になっていますが、他の採用できる方法というのは、業務の提供チャンネルに依存するものだと思います。例えば、オンラインのみなのか、対面なのか、郵送もあるのか、などもととの業務があって、その上でできることをするので、オンラインサービスである場合に、対面の窓口も用意するというは無理があると思います。P20 にある図がわかりやすいので、保証レベル及び業務の提供チャンネルによってどれを選択するかを選ぶ、その手法で保証レベルが不足する場合に追加的対策を考えるとこのような書き方でも良いのではと思いました。関連して、P15 の検討結果の例の部分は、かなり強度の高い方法を例として挙げているように思いますが、マイナンバーカードの代替手法として、郵送や対面による代替手法を採用するという採用の例と、それぞれにおける身元保証レベルの具体的な例が混ざっているように思います。分量が多くなるかもしれませんが、2 パターンに分けて、提供チャンネルがオンラインの場合と、郵送・対面のチャンネルを持っている場合とで、2 つに分けて提示しても良いのではないかと思います。
- マイナンバーカードを使うかそれ以外か、よりも前に、この行政サービスではどのような身元確認が求められているのか、というコンセプトが一番大事だと思います。率直に言うと、この前段に何かあるべきではないか、ということです。例えば、犯罪収益移転防止法で実際に送金するようなサービス、携帯事業における本人確認など、それぞれ法令で身元確認かくあるべき、というのが定義されています。国民に行政としてサービスを提供するということであれば、それらと全く同じものはないとはいえあるかもしれないし、あるいはそれに準ずるものがあつたら、それに近い身元確認をまずやるべき、というのがあると思います。そのうえで、それを実現するためにマイナンバーカードが非常に有効ということだと思います。順番として、まずどういう性質の身元確認を求めべきか、というのが最初にあり、そのうえで手段としてマイナンバーカードを使った本人確認手法を、解説文書の中で積極的に推進していく、というのは良いことだと思いますし、それ以外の手法も「誰一人取り残されない」というコンセプトから記載して良いと思います。
- 実装モデルの中でマイナンバーカードを使うという点で考えるべきことがあります。JPKI が早い時期から注目されてスマホ搭載も先行しましたが、署名用電子証明書を使ったものは実印相当であるとおっしゃっている先生もいらっしゃいます。カード代替電磁的記録が実用化された現代、解説文書の中においては、カード代替電磁的記録を積極的に促していくのは1つの案としてあると思います。
- JPKI でもカード代替電磁的記録でも、スマホ電子証明書は国民の持つスマホに1つだけ登録できるようになっています。Androidを持っている人がiPhoneだとどうするのかという話もありま

す。PC で行政サービスを受けたいが、PC にはマイナンバーカードが載っていないものの、マイナンバーカードをスマホに搭載して、PC で本人確認ができるということはテクノロジーとしては揃ってきています。そういったことも解説文書に記載する必要があるということ、念頭に置いて書かれていくのが良いのではないかなと思います。

- (事務局)例えばマイナポータルでは、QRコードを使ったクロスデバイスでの認証ができるようになっていきます。それがどこまで汎用的に使えるのか、という問題はありますが、一定量カバーができると考えています。
- P15にて、券面事項入力補助 AP と記載がありますが、確か第 1 回の資料でも照合番号 A と B では申請者の検証ができないという記載があったと思いますので、それがないと誤解を招くと思いました。
 - いわゆる 4PIN を想定した使い方という意味で良かったでしょうか。
 - (事務局)おっしゃるとおりです。
 - マイナンバーを取得するユースケースはそれほどないのではと思っていますが、そうでもないのでしょうか。
 - (事務局)マイナンバーを取得するユースケースはあまりありませんが、取得するかどうかに依らず、券面事項入力補助 AP を利用することは可能だと認識しています。
 - 4桁の PIN だと、マイナンバーも入ってきてしまって、利用事務や関係事務に関わる方しか使えないのではと思っていました。
 - (事務局)民間の方が参考にされる場合も踏まえ、適切な記載を検討いたします。
- P18にて、先ほど実印相当という言葉もありましたが、1-b)のアクセシビリティ、ユーザビリティの面に関わる点で、利用者の方に実印を押しているというのを理解してもらうために、UX なり表示なりをガイドすることが必要だと思います。なぜマイナンバーカードを何度もかざす必要があるのか、パスワードや PIN を使い分け入力する必要があるのか等は今でもよく聞く話だと思います。ハンコと証明を 1 つのカードに押し込んでしまったことで混乱を起こしている点があるだろうと思います。また、今後スマホ搭載も入ってくるので、今、自分が何をやっているのか、というのをユーザー目線でわかるようなアクセシビリティ、ユーザビリティの注意書きみたいなものをガイドすべき、という事を記載するのが良いと思います。
- P19にて、やむを得ない場合で保証レベルを満たさない手法を採用する場合の記載がありますが、役所の窓口などの実務において、書類が足りていないが無理やり申請をする場合もあると認識しています。これはガイドライン的にはダメだと書くのが本筋だとは思いつつ、実際に行われている現状を考えると、書類が足りてない場合に後から不足分を取り戻すような手法を、推奨するわけではないけども明示しておくべきだと思います。
- 身元確認にどの属性が必要か、というのは常に考える必要があります。ここに挙がっているものだと、レベル 1 ですら全部の情報が入ってしまうのであまり望ましくないと思います。プライバシーの観点からも、選択的開示ができる手段を明示してあげる方が良いと思います。カード代替電磁的記録を使う場合はできますし、デジタル庁のデジタル認証アプリでもできます。

そういったものがあるということを、選択肢としてわかるように示すのは、ガイドラインとしては大事だと思います。

- P15 の保証レベル 3 のマイナンバーカードを保有していない人向けの代替手段として IC カードが記載されていますが、この条件を満たすものに何かがあるのか普通の人は思いつかないと思います。書いてあげた方が良いのではと思います。代替手段として認定・認証局が書いてあっても良いと思いました。
- マイナンバーカード以外による手法をなくせないのは、マイナンバーカードが即時発行できないこと、つまり、失効した時に最短でも 1 週間使えない期間が生じること、義務化されていないということが、理由でしょうか。
 - (事務局)おっしゃるとおり、新規発行や再発行を待てないような緊急性の高い手続を、代表的なケースとして想定しています。
- 代替手段を設けた場合、サービス主体側にコストが掛かるものがあります。例えば本人限定受取郵便(特定事項伝達型)は非常にコストがかかりますので、用意しづらかったり、用意する必要が本当にあるか悩んだりする点になります。また、代替手段の方が大抵セキュリティ的に緩い手法になりますので、易きに流れてしまう人が多いのではないかという懸念があります。代替手段があることで、マイナンバーカードを使ってほしいという方向から逆行してしまうのではないか、代替手段が選ばれ続けた結果、代替手段を外せなくなってしまうのではないか、という懸念です。代替手段があるということ、言わないほうが良いのかもしれない、フラットに代替手段の記載をしないほうが良いのではないかと思います。
 - マイナンバーカードを使う方向に誘導する方がシンプルで良いと思っていました。代替手段である、マイナンバーカードを使わない方法は、極端にユーザビリティが落ちているので、結果としてマイナンバーカードの使用を推奨しているという整理でも良いのではないのでしょうか。
 - 代替手段はユーザー側にコストが掛かるということであればバランスは良いと思いますが、サービス提供側にコストが掛かり、手法を選ぶユーザー側に負担がないとなると、少し難しいと感じます。
- マイナンバーカードを使うという方針は揺るがないと思っています。また、JPKI やカード代替電磁的記録以外に、マイナンバーカードを IC チップ付の身元確認書類として用いた eKYC もあり、マイナンバーカードの暗証番号を覚えていなくても使えるというメリットがあります。運転免許証を、IC チップをもった eKYC として利用する手法よりも利用率が高く、成功率も高いという数字が取れています。そういったマイナンバーカードの使い方みたいなものも、解説書に入れるのでしょうか。
 - (事務局)マイナンバーカードもいろいろな手法があるので、簡単に概要を紹介するものを別紙に付けようと考えております。おっしゃった外部サービスとしての eKYC は記載候補に挙がっていませんでしたが、検討いたします。
- P21 の IdP について、行政機関内の IdP であるということに記載しておきたいと思います。ま

た、デジタル認証アプリの他の選択肢として、G ビズ ID は法人向けのため記載できないとしても、例えば eMAFF 等はもう少し個人向けですので、例示なり解説なりがあっても良いのではと思いました。

- 最近では地域限定のアイデンティティを配るところもあります。地方公共団体、自治体が連携しているのですが、それらをきちんと押さえておかないと、本来信頼してはならない IdP を活用してしまうことになるので、今から手を打っておいた方が良いと思います。ガイドラインに対するコメントではなく、現状をどう抑えておくかという意味でのコメントです。

「本人認証手法の選定の考え方」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)

- 非常にストレートに記載されていて、良い意味で驚きました。「国民を詐欺から守るための総合対策」においても、DMARC と並んで、パスキーは国際標準化団体が定めた規格として、フィッシングに耐性のある認証方式であると記載されています。金融庁、日本証券業協会でも 10 月 15 日に、それぞれ監督指針、ガイドラインで、フィッシングに耐性がある認証方式を必須にする、デフォルト化すると策定されています。これに追従する形で、急速にパスキーの実装や提供開始が増えています。そういった状況を踏まえると、選択肢としてマイナンバーカードによる利用者証明、あるいはパスキー以外はなさそうに思いますので、解説文書としては、これくらい具体的に書いてもらえると、実務に携わる方々もわかりやすいと思います。金融庁、日本証券業協会でも、「パスキーを」と書かれているわけではなく、「フィッシングに耐性がある認証を」と記載されていて、例としてパスキー又は PKI ベースのもの、と書かれており、実質的にこの 2 つを指していると思いますので、整合が取れていると思います。
- 報道発表されていたと思いますが、OpenID ファウンデーション・ジャパンの皆さんが、金融庁の監督指針の一部改正に係るパブリックコメントに対するコメントを出されています。この中で、パスキーを登録するときの本人確認、身元確認が重要になると書かれています。2021 年に総務省がマイナンバーカードのスマホ搭載を進めているときにも伝えましたが、パスキーを設定するときの本人確認が非常に重要になります。パスキーを登録するときに二段階認証だけとなっていて、攻撃者が攻撃者の端末にパスキーを設定するという事例が報告され始めています。これは由々しき事態ですので、特に本件におけるレベル 3 において、フィッシングに耐性のある認証を使う場合は、その設定時の本人確認が大事である、ということを必ず書き添えてほしいです。
- 本人認証手法の項目に入れるべきか、別途議論だと思いましたが、目次を見た限り、アカウントのリカバリーに関する話がないように思います。ここに入れるしかないと思いますが、記載すべきだと思います。今、おっしゃった設定時の本人確認の内容にも繋がります。
 - バインディングやリカバリーは、CSP が果たすべき義務であって、この解説書では、行

政官が利用者に使用を許す認証の方法が記載されている認識です。どちらも言わないといけないのでしょうか、お二人のコメントは想定する読者が二重になっているように思います。解説書にどう入れ込むかはなかなか難しいと思いました。

- マイナンバーカードの利用者証明用電子証明書を使う代表的なものとして、デジタル認証アプリがあると思いますが、具体的な名前を書いたほうが読み手は迷わないと思います。
- CSP を選ぶ時に、CSP がちゃんと運用されているか、テストされているか、は重要です。デジタル認証アプリしか CSP を考えないのであれば良いのですが、そういった観点もどこかに示しておいた方が良くもしいかもしれません。実際に、過去に秘密鍵を晒してしまう CSP もありましたし、きちんとプロトコルに沿っていないということもあります。パスキーというとプロトコルも指しますが、利用者証明用電子証明書といった場合はプロトコルまでは必ずしも指していないと思います。本来はプロトコルもセキュアである必要がありますので、そこは記載が必要ではないでしょうか。
 - 行政官や設計者が、プロバイダが適切に行っていることを確認する手段というのはどういったものを考えられているのでしょうか。
 - プロトコル内の Attest や Certify を確認することになるので、トラストフレームワークを組むしかないと思います。
 - そういったものを活用するしかない、自分で個別に確認しにいかず Attestation できないので、トラストフレームワークを組むしかないということで、理解しました。
- リカバリーの話になりますが、よくあるパターンとして、通常使う認証要素はパスキーで、パスキーが使えない状況において、再度身元確認を行ってパスキーをリカバリーするということがあります。DS-511 でも代表的なアカウント回復手段の例に、身元確認の再実施と書かれていますので、それは含まれているものと思いますが、この解説書でどのレベルに当たるのかが読み切れなかったので明確にしてほしいと思います。P26 では、マイナンバーカード(利用者証明用電子証明書)と限定されているので、身元確認の再実施というよりも、本人認証としてのマイナンバーカードの利用が想定されていると思いました。身元確認を再実施することでアカウント回復をするのは、レベル 3 になるのかがわかりません。パスキーでもマイナンバーカードでもないの、別の手法になるのかもわかりませんでした。その点、ドキュメントの中で明確にしてもらいたいです。
 - (事務局)アカウントの回復に関して、本日いただいたご意見を受けて、解説書の中で拡充しようと思います。関係性や対応関係についても、明確になるように整理いたします。
- 身元確認の中に本人認証の話もあるし、リカバリーの例だとその逆もあります。この手の話をするときは、身元確認、本人認証が別々に記載されてしまいますが、実は相互に絡んでいるということの解説があっても良いのではと思いました。
 - NIST の文書でも同じと認識しています。
 - 身元確認、本人認証は、エンタープライズではこの順番が多いのですが、対市民サービスだとひっくり返した方がうまくいく場合もある、という話は以前からあります。要は、パ

スキーを先に登録させてから、IAL を引き上げるというもので、必ずしもこの順番ではないというのは言っても良いと思います。日本はマイナンバーカードがあるので、どちらでも良いかもしれませんが、アメリカのように電子的に統一的な認証手段がない場合は、身元確認をしてからクレデンシャルをどう渡すのかという問題がありますので、先にクレデンシャルを渡してから、そのアカウントの IAL を上げる、という方が、危険度が低いという話もあります。

- パスキーを意図せず登録されてしまった方がいた場合に、その方がどうやって被害に気付くのか、また、そのパスキーを払い出してしまった RP サイドに何ができるのか、という事を考えると、一定程度の確保が必要ではないかと個人的には思います。
 - 先ほど申し上げた、クレデンシャルファーストフローの場合も、クレデンシャル登録時点では何もできません。そのセッションで身元確認をすることしかできないです。
 - クレデンシャルを持っているときに、そのクレデンシャルが持っている権限がコントロールできるシステムにおいては有効ですが、そこまでやっているシステムは少ないと思います。解説書を通じてそういった部分も教育できれば良いかもしれませんので、そこまで踏み込めると良いと思います。
 - 継続的アクセス評価の観点で言うと、そのレベルを記録して、上げ下げを自由にできるようにシステムを作っておかないといけません。今後はそういった点も求められるようになると思います。
- 当人認証の前に身元確認をしないとイケないということは、一般の人にはわからないと思います。メタ化した脅威は整理されていると認識していますが、せっかく Informative の文書ですので、具体的な事例をいくつか書いていただくと理解がしやすいのではないかと、思うのでぜひ検討いただきたいです。
 - ローカルな身分証明書の話で、どこかの自治体が VC (Verifiable Credential) を作ってスマホにデバイスバインドして、Android のキーストアを利用したような場合、それらをふるいにかける仕組みがあるのでしょうか。
 - 同様の話はアメリカの mDL でもあります。アメリカの mDL を使って口座開設するとき、州によっては mDL が Real ID Act に沿わずに発行されているものもあり、なんらかのフラグがないと困るため、拡張をどうするかという議論がされています。
 - 実際の対面の手続の場合、行政が発行していないものでも本人確認ができてしまうものもありますので、そういう場合においては一定受け入れることもあると思います。とはいえ、ガイドライン本編の範疇になってしまいますので、本日のスコープ外とは思いますが。
 - (事務局) 歴史的には広く認めてきて、2000 年代初頭までは、社員証の方が住民基本台帳カードよりもはるかに信頼度が高かったように思います。ただ、9.11 以降は犯罪収益移転防止法や携帯電話不正利用防止法ではないですけども、リスク軽減策として求めているだけであれば、どの場合にリスクを取って良いかというリスクミティゲーションの話でしかないので、受け入れることは十分にあり得ます。インクルージョンのために良

いのか、というのは議論があっても良いのかと思います。

- DS-511 の際に議論が出ていましたが、マスクの問題などは解説書にも入ってくるのでしょうか。実態として出てくる問題かと思いますが、解説書に記載があると良いと思います。
 - (事務局)別紙の個別手法の解説としての記載を予定しております。
- DS-511 を紹介する機会がこれまでありましたが、全部読んでほしいというのはなかなか難しいので、Word 版だけではなくて説明用の PowerPoint での概要版を用意していただけると幸いです。

閉会

- (事務局)今年度は具体的なプラクティスの話で、DS-511 よりも実は大事かもしれないと思っております。というのも、実際に求められているのは Philosophy ではなく手引書である、というところがあります。加えて、来年には携帯電話不正利用防止法、再来年には犯罪収益移転防止法の改正が予定されており、いずれもオンラインと比べると対面も含めてチップの読取りもするようになるというのは、大きな変換点です。目視による本人確認を何十年もやっていたので、今やろうとしているチャレンジというのは、何十年ぶりの大きな転換になります。そのベースとなるドキュメントですので、しっかり議論いただきたいです。一方で、Informative 文書なので、完璧を目指すというよりはタイムリーな情報も載せて更新していけたら良いと考えております。引き続きご意見いただけたらと思いますので、よろしくお願いいたします。
- (事務局)最後に、事務的なご案内をして終わりたいと思います。本日の議事録も、これまでと同様に 2 週間以内に案を作成して皆様に共有させていただきますので、ご確認いただけたらと思います。皆様からのご確認を賜り次第、デジタル庁の Web サイトにて公開を予定しております。それでは、本日の有識者会議は以上とさせていただきます。ありがとうございました。

(了)