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 2 回）
令和 5 年 11 月 16 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 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	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 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 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） 開会・開催要綱説明

（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 2 回目を始めさせていただきます。みなさん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。本日は「リスク評価プロセスをどのように反映するか」、「リスク評価のためにデジタル庁でどういった支援ができるか」という 2 つの論点を用意しています。

議題（2） ガイドライン改定に向けた論点協議

論点 4-1. NIST で改定されたリスク評価プロセスをどのように反映すべきか

事務局より、資料 1 に基づき論点 4-1 に対する現時点での方針を説明し、有識者による自由討議を行った。

（有識者意見）

- 資料 1 の 7 ページの図は、テーラリングをして手法と脅威を細分化して、保証レベル 1 や 2 の細分化に反映していくというイメージでしょうか。手続の種類によって脅威がどのパターンなのかということは設計する時にあらかじめ確認しておき、結果、手法が決定されるということでしょうか。リスク評価を最初にざっくり行うわけですよね。
  - 事務局：ステップ 1 の検討プロセスの複雑化を防ぐためにも、保証レベルの細分化は避けたいと考えています。検討の手順はご認識のとおりでして、まずは例えば「生命に対する損害がどの程度想定されるのか」といったようなカテゴリ別の 3 段階のざっくりしたリスク評価を行いまして、その後に保証レベルに対応する手法の脅威耐性をみながら、採

用する手法選択を行うことを想定しています。

- 脅威への耐性から採用すべき手法を判定できるのであれば、ステップ 1 は不要なのではと疑問に思いました。
  - 事務局：タスクフォース内の検討でも同様の議論はあったのですが、保証レベル 1・2・3 というのはコミュニケーションの際の基準として有用であることや、ステップ 2 から始めると、どうしても「すべての脅威に対応できる一番上の手法（レベル 3 相当の手法）」を選ばれてしまうのではという懸念がありまして、保証レベル判定度の手法選択、という 2 段階のプロセスを考えております。
- ステップ 2 で手法を細分化するということですが、それは行政手続における RP が利用するものなのでしょうか。OIDC では Evidence を持ってこいという訳ですが、そういうことをお考えなのでしょうか。
  - 事務局：7 ページの図は、まずは RP が自ら身元確認や当人認証の機能を実装する場合のモデルを想定しています。が、フェデレーションを行う場合にも同じような考えが取り入れられると思っております。
- フェデレーションの場合は、行政手続側が利用する Authenticator を指定するという感じになるのでしょうか。この手法の例えば A・B・C は受けつけないとか、そういうふうになるのですかね。
  - 事務局：IdP が複数の認証手段を提供している場合には、それらの手法が当該手続で採用可能なものであるのか、といった観点からテーラリングを行い、必要な脅威耐性を有していない手法は受け入れないといった考え方になると考えています。
- 7 ページの図で、保証レベル 3 の場合には脅威 a、b、c、d への対応が必須、保証レベル 2 の場合には脅威 c、d への耐性は必須で脅威 b については必須もしくは推奨、のように保証レベルによって必要な脅威耐性を決めていくということでしょうか。
  - 事務局：対策基準の要求事項として脅威耐性を直接どんどん書いていく、ということは想定しておりません。NIST と同様の粒度で、「対面であること」といったような基準を想定しています。ただ、当人認証保証レベルについては NIST AAL と同じく、いくつか脅威耐性そのものが対策基準になることもあると思っております。
- 7 ページ目の図のステップ 1 では xAL のカテゴリごと、立体をイメージしていうなら 3 層のリスク評価があって、一方で右側で手法を選んでしまうとそれが縮退したように決まってしまうと思うのですが、その立体が平面にうまく乗るのかなという点を疑問に思いました。その例が先ほどのお話なのだろうと思うのですが、ここで結構脳内変換が必要そうですよね。
- リスクという塊のなかにどういう脅威があるかをまず確認し、その脅威として例えば脅威 a、b、c が存在するのであれば、対応する手法として手法 A や B を選ぶ、という流れならば、図の位置関係は逆にした方が良いかもしれませんね。
- ステップ 2 だけで良いのではというコメントがありましたが、実際の現場では脅威耐性の必要性の判断が難しい場合もありますし、「この場合はレベル 2 でいいですよね」といったコミュニケーションにも使えますので、ステップ 1 のレベル分けはガイダンスとしてはとても役に立つと思います。ただ、ステップ 1 にも 6 つのカテゴリがあって、そこを理解したうえで 3 段階のレベルを判定するとなると、意外とこのステップ 1 すらも難しいプロセスになるのでは。
- ガイドラインの読者が誰になるのかという観点も含めて考えると、例えば犯収法で定められた

手法にも実際はいろいろ差があるように、同じレベルに該当する手法でも脅威耐性には差がある訳ですから、本人確認のあり方を考えるという点では右側の脅威ベースのアプローチは役に立つと思います。一方で、いきなり右側に書かれているような脅威耐性の要否から理解・判断できる人は少ないですから、そういう方にとっては左側のレベル分けのアプローチが役に立つ。こうして左側のアプローチと右側のアプローチを目的に応じて分解できれば、とても良いドキュメントになるのではと思いました。

- システム開発をやっている企業の立場で申し上げると、基本的にサービス導入においては社内のステアリングコミッティのようなところでリスク判定を実施するプロセスになると思いますが、専門的なところはセキュリティコンサルタントやシステムを開発したベンダに判断を任せるケースも多いだろうと認識しています。企業だけでなく、行政手続や自治体などでも同様なのではと思います。となると、このガイドラインの参考資料のメインの読み手として誰を想定するのかという点が重要になってくるのだろうと思います。組織の中で内製的にやろうとするなら左側のアプローチ、専門家に見てくださいという話なら右側のアプローチからでも良いのではないでしょうか。
- 私も皆さんの仰っているとおりと思います。右側のアプローチでは非常に細かい内容が出てくると思いますが、例えば「フィッシング耐性」という言葉が出てきたとき、自分のビジネスにどんなインパクトがあるのか思いを巡らすのは正直難しいと思います。セキュリティコンサルティングに長く携わっていた立場としては運用が回るのかということが極めて重要だと思っておりまして、どれだけ綺麗に整理されていても運用が回らないものを作っては意味がないと思っております。よくやっていたのは、この図の左側のようなアプローチで、例えば「個人情報を扱っていますか」といったようなシンプルな問いでざっくりレベル分けできるように設計し、そこから解像度を上げていく作業というのは、リスク分析に対する見識がある専門家を巻き込むというものです。現場の人がまずは粗く判定して、それを自組織内の専門家に相談して更に細分化して、といったような段階的なフローを想定しないと、運用が回らないのではと思いましたので、その点ではこの資料は少々きれいに書かれすぎているかもと感じました。
- 昨年度の議論でも、リスク分析をデジタル庁が中央集権的にやるべきか、現場がやるべきかという議論があってなかなか答えが出なかったのですが、私の経験としては運用が回るかというところが課題になることが多かったものですから、この図のステップ 1 はもっとシンプルに、2 段階ぐらいであるべきなのではというイメージを持っています。その後に組織内の専門家と相談して必要ならば解像度を上げて、これはもっと上に挙げないといけないねとなったら中央集権的なところに上げて判断をする、といったような階層的な構造がプロセスにも反映され得るのではと感じています。
- 「テーラリング」という言葉が果たして通じるだろうか、という点も気になりました。ガイドラインの読み手が、この場面で一体何をして、何を達成すればよいのか、というところを明確にしなければならないのではと思います。今回の案ではテーラリングをしっかりやっていくということが骨子になっているかと思いますのでコメントしました。
    - 事務局：テーラリングという言葉は置き換えと解説が必要だと認識しています。また、ガイドラインの読み手が誰なのか、という点ですが、基本的には行政手続の担当職員でして、システム規模によっては支援事業者もそこに入ると想定しておりますので、少なくとも行政官だけで検討したときも想定した書きぶりにしないといけないと考えています。い

ま議論いただいた内容を踏まえると、ステップ 1 については行政手続を担当する行政官による検討を想定していましたが、ステップ 2 については専門家による検討が必要だと思いましたので、それぞれのステップで想定する読み手を変えて考える必要があると認識しました。また、ステップ 1 を分ける意義についても本日何度か議論いただきましたが、読み手の違いを考えてステップ 1 を読む人、1 と 2 の両方を読まなければならない人の 2 種類を読み手として捉える必要があるのだと考えました。

- 左側のアプローチは行政手続を企画する方向けで、法令に対する理解やシステムに対する一定の認識はありながら、セキュリティの細かいところについてはコンサルテーションを受ける必要があるレベルの方。右側のアプローチはセキュリティやその他の観点を正確に理解して判断できる方向け。そういった想定読者のイメージがどこかに書かれていると、ドキュメントが作り上げられる過程でも理解されやすくなると思います。
- ついつい我々は NIST SP 800-63 のことばかり読んでしまいますが、米国の行政官が読むのは OMB M-04-04 の方なのです。間違ったら人が死ぬかどうか、多大な損害を受けるかどうかとか、そういった観点でリスクレベルが規定されていて、行政官の仕事というのはそこまでだと思います。NIST SP 800-63 では、公平性やプライバシーの観点が入ってきますが、基本的にはこの行政サービスを提供できなかったら、あるいは間違った主体に提供してしまったらどうなるのか、というリスクの線引きをするところまでが左側の部分だと思います。そういう粒度でレベルが規定されたあとに、専門家が脅威に応じて細かい判断をしたり、プライバシーの話ならば組織側だけでは残存リスクを受け入れていいかの判断ができない場合がありますので、ステークホルダコンサルテーションが必要になったり、という流れになるのでは。
- 6 つのカテゴリでリスクを評価することについて複雑なのではという話もありましたが、私はこれくらいは必要なのではと思います。

（事務局説明）

- 当初の予定ですとこの後論点 4-1.の取りまとめに入る予定でしたが、いただいたご意見を踏まえますと先に論点 4-2.に直接進ませていただいて、その後全体でコメントをいただいた方が良いと思いましたので、論点 4-2.を説明させていただきます。

論点 4-2. 適切なリスク評価のためにどのような検討支援や統制が必要か

事務局より、資料 1 に基づき論点 4-2 に対する現時点での方針を説明し、有識者による自由討議を行った。

（有識者意見）

- レベル 3 に該当する行政手続って具体的に何なのでしょうか。それが分かっているなら、それだけ除外する方法で判断した方が早いのでは。
  - 事務局：行政手続のパターンを調べ上げて保証レベルを直接提示するという方法も案としては考えたのですが、このガイドラインが改定後にある程度の期間運用されることや、自治体や民間からも参照されるものであるということを考慮しまして、まずはガイドラインではあるべき論を書いて、各レベルに当てはまる行政手続の例などは Informative な情報としてまとめていこうという話をタスクフォースの中では検討しておりました。

- 実際のリスク影響度の記載を見てみると、13 ページの②③④あたりを 3 つのレベルから選ばせると上振れしそうだなと思いましたので、「該当するかしないか」という質問の仕方は上振れを防ぐ意味でも有効なのではと思いました。
- リスクを評価する立場に立ったとき、「完全に非該当」と言い切ることが難しいものもあるのでは。特にプライバシーに関わるところなどでは非該当と言い切れず、この聞き方だとレベル 3 と判定されるケースが割と出てくるのではと気になりました。「原則該当しないけど、こういうパターンでは該当するかもしれない」といったようなケースも想定した幅があってもいいのではと思いますし、そこを考えることが良いリスク評価につながるのではと考えます。
- 当社でもステアリングコミッティにかける際には“前捌きシート”のようなものを作成して提出するということをやっていますが、その目的はシート上で正確な判断をやってもらうというよりも、ステアリングコミッティとのコミュニケーションツールとしての側面の方が強いので、このワークシートもコミュニケーションツールとしての位置づけであるのかなと。
- PIA レポートもそういうものです。レポートを書くためにきちんと考えなければいけないし、レポートの項目が決まっていればコミュニケーションツールとして非常に使いやすくなると思います。
  - 事務局：ありがとうございます。今回のツールはコミュニケーションツールとしてもそうですが、このシートを「リスク評価結果を文書化したもの」として残すことで、継続的な改善にも繋げられればと考えています。
- 全然違う切り口かもしれないですが、文書化されたリスク評価結果というのは、行政文書として公開されるものに該当するのでしょうか。もしそうなら攻撃者にとってヒントになってしまいますので、取扱いには気を付けないといけないと思いました。
  - 事務局：情報公開請求時には、通常の情報システムの設計書と同じような扱いで、セキュリティ上の懸念がある部分については非公開の対応になると思っております。
- 参考ですが欧州では PIA レポートは「公開用 PIA レポート」を作って公開しなければならないことになっています。

（事務局説明）

- ここまでの議論を踏まえて一度整理しますと、論点 4-2.でご説明したようなワークシートなどを使って、ステップ 1 のリスク評価をなんとか行政官の方が検討しやすくできないかと考えております。とはいえ、その判定だけでは粒度が大きすぎますし、場合によってはレベル 3 と判定されたものでも公平性やプライバシーの観点からレベル 2 相当の手法と補足的な対策を組み合わせるべき、といったような検討をできるように、ステップ 2 のテーラリングのプロセスを専門家や支援事業者が関わりながら調整できるようなガイドラインにできると理想だと認識いたしました。
- 実際の検討事例をヒアリングしてみると、ユーザビリティの観点から現行ガイドラインで示されている手法例とは異なる手法を採用した手続きもありまして、そうした現場側でのテーラリングをうまくプロセスとして定義できるようにしたいと考えます。

（有識者意見）

- 身元確認の障害モードについては、テーラリングで検討すべきなのか、それともステップ 1 の

リスク評価にもともと含めるべきなのかという検討が必要だと思います。有名な事例として、ウガンダにおいて国民 ID を持っていなかった妊婦が医療の提供を拒否されてしまった、というような事例があり、こうしたケースでは身元確認ができないことが生死のリスクに関係してきます。セキュリティの観点ばかり考えてしまいがちですが、行政サービスが提供できなかった場合のリスクということも考えなければならず、こうした観点は 7 ページ目の左側のリスク評価に含めるべきだと思います。

- 前回会議でもお伝えしたように、保証レベル判定のフローチャートの問題は”If Then”はあるけど”Else”がないというところです。リスク評価においては「何ができなかった場合どうする」、「それ以外の例外ケースはどうする」ということまでステップ 1 のリスク評価で考えておくというのを盛り込んだうえで、3 段階の保証レベルに振り分けるとよいのではと思います。
- このリスク評価ワークシートの例では「該当する場合にリスクを記入」となっていますが、非該当とする場合でも、その判断根拠は記録として残しておくことが必要なのではないかと思います。
- 選択肢が「該当」「非該当」だと、エッジケースを捉えられてしまう懸念があるのでは。考え方としては、PCI DSS でいう代替コントロールのような考え方をもって、受容できないリスクが残存しているかどうか、といった聞き方の方が良いのではと思います。そうしておくと、例えばユーザビリティ等の観点で別の手法を採用したい場合などに、代替コントロールを講じることで残存リスクの受容判断ができるのではと。その判断結果をここに書かせることが重要だと思います。
- 文書化して残すということは非常に重要です。先ほど公開されるのかどうかという議論がありましたが、少なくとも行政機関の中では共有した方が良いと思います。
- 残存リスクとして受容判断した部分は、記録に残して公開しておくべきでしょう。行政の中では整理できている内容であっても、その意図をくみ取ることのできない民間の事業者が行政の証明書を別の用途に使ってしまう可能性があるので、そこを防ぐ役割もあるのではと思います。
- 共通言語として使うというのがワークシートの目的だと思っています。その観点では、該当/非該当の理由だけを書かせてしまうと情報量が落ちてしまうと思っており、具体的な障害モードを記入させるというのも重要だと思います。自分のサービスを提供できなかったとき、どのような望ましくないことが起きるのか、といったことを所管がちゃんと考えて、記録として残す形にすることも考えても良いのではと思います。最初は生みの苦しみがあって時間がかかるかもしれませんが、蓄積していったときに過去の判断を参照できるようになり、全体の効率化にもつながるのではと思います。
- 少しネガティブなことを申し上げますと、このリスク評価ワークシートをどう記入するかということについて、今までの議論を踏まえますとかなり高いスキルを要求することになるのではと思います。非常に重要なことなので、研修や知識の共有といったことは必要になってくると思います。一方で、この検討に特化した人材を各組織に作りかねないことにもなると思いますので、なるべくベースとなるリスク評価は誰もが実施でき、その上で専門家が詳細を判断できるような体制や仕組みをデジタル庁が作るべきなのでは、と思いながら話を聞いていました。
- 1 点確認させてください。資料の 13 ページのリスク評価ワークシートと、12 ページの障害モードとの関係性はどうなっているのですか。

- 事務局：おそらく行政手続によって考慮すべき障害モードが異なってくると思っていますので、「間違った人にサービスを提供してしまう」や「サービス自体を提供できない」といった主要な障害モードの例示をガイドラインに記載しまして、その手続で考慮すべき障害モードが生じた際のリスク影響度をワークシートで判定してもらうイメージでした。先ほどコメントいただいた件を踏まえますと、考慮しなければならない障害モードもこのワークシートの上部などに書き出させることが良いのではと考えております。

- 本来リスク分析のプロが検討する際は、守るべき資産が何で、アタックパスが何で、それらをリストアップして攻撃シナリオを考えて、このあたりで障害モードが出てきて、保証レベルやリスク受容の判断、残存リスクの整理、セキュリティゴール達成の確認などを行うことになると思います。が、それを全て求めても運用は回りませんから、行政手続の所管が当事者として高い精度で書き出せるものが障害モードなのかなと考えています。

（事務局説明）

- 終了予定時刻が近づいてまいりましたのでまとめに入らせていただきます。論点 4-2 についてはワークシートの部分も含め多くのご意見・ご助言をいただきありがとうございます。このワークシートが機能するように、いただいたコメントを盛り込んでいこうと考えます。
- 最後に、このワークシートによるアプローチの是非について改めてコメントいただきたいと思っています。今までの議論では概ね評価をいただけたのではないかという感触ですが、一方で NIST ではフローチャートが削除されているという点が事務局の懸念でして、このワークシートを利用するという方針で検討を進めてよいのかという点について、特にネガティブなご意見があればそこをコメントいただけますと幸いです。

（有識者意見）

- 私は良いと思います。1 回決めたら終わりではなくて、運用しながら得られたフィードバックを積極的に反映して運用を続けていくことを前提とすると、運用についての学びも得られます。
- 検討結果の文書化を求めるなら、いずれにせよ共通の記載項目や目次構成を決めなければいけません。今回のワークシートは、それをもう一段階細かくしたレベルだと思っています。たまたまその目次構成がワークシートという形を取っているだけなので、私も良いのではないかと思います。
- 私も良いと思います。ワークシートを利用することで初めてリスク分析に近いものができて、フローチャートに魂が吹き込まれるという形になるのだと思います。いきなりフローチャートにいくとよくわからない状態になってしまいますので、このワークシートによる整理が必要なのだと思います。
- 記録を残すという意味でもコミュニケーションするためのツールという意味でもこういったドキュメントは必要ですから、そのドキュメントの呼び方をどのようにするかというだけの違いなのではないかと思います。

（事務局説明）

- ありがとうございます。ステップ 1 のリスク評価の部分については、現在の方針で進めさせていただこうと思います。一方、ステップ 2 のテーラリングの部分については少し整理が必要か

なと思っておりますので、本日いただいたご意見を事務局内で検討し、第 3 回会議で方針案としてご説明できるように準備いたします。

閉会・次回案内

（事務局）

- 本日は途中からの参加になってしまいましたが、本当に熱心に議論いただいて、やはり本気で取り組んでいらっしゃるみなさまなので議論のレベルも非常に素晴らしいと感じましたし、どうやって魂を吹き込んでいくか、神は細部に宿るといいますか、こういう具体的な議論がやはり大事なのだろうと改めて思ったところです。ガイドラインを形にしていくためにも、もう 1 ステップ、2 ステップ必要だなと、ご指摘を伺いながら改めて思ったところではありますので、NIST SP 800-63-4 を輸入学問として持ってくるというだけではなくて、やはり我が国の中で具体的な脅威、あるいは様々な技術をどのように適応していくかというところで、自分たちで繰り返し考えていく、そして新しく発生する脅威に対して対応していきながら、その履歴をきちんと文書として残していく営みというのは本当に大事だと思いますので、こうした営みを通じて役所だけではなく民間も含めたセキュリティレベルの底上げに繋がるような形に持っていければと考えております。引続きご指導のほどよろしくお願いいたします。ありがとうございました。
- 本日の会議は以上となります。次回は 12 月 26 日（火）を予定しております。本日も誠にありがとうございました。

（了）