マイナンバーカードの機能のスマートフォン搭載等に関する検討会（第８回）
議事概要

１．日 時：令和３年 11 月 24 日（水）15 時 00 分～17 時 00 分

２．場 所：Web 会議による開催

３．出席者（敬称略）

（１）有識者

手塚座長、太田座長代理、小尾構成員、瀧構成員、野村構成員、宮内構成員、森山構成員

（２）自治体・関係団体

岡田情報政策課長（前橋市）、牧野マイナンバー推進担当課長・菊池係長・西海係長（神戸市）、荒井個人番号センター長・谷個人番号センター副センター長・橋本公的個人認証部長・林公的個人認証担当部長（地方公共団体情報システム機構）、佐々木ＭＶＮＯ委員会運営分科会主査（一般社団法人テレコムサービス協会）、江口業務部長・斎藤氏・馬場氏・静氏・地崎氏・山田氏・加藤氏・君島氏・上野氏（一般社団法人電気通信事業者協会）

（３）オブザーバー

エヌ・ティ・ティ・コミュニケーションズ株式会社、xID 株式会社、一般社団法人全国携帯電話販売代理店協会、一般財団法人日本情報経済社会推進協会、日本電気株式会社、株式会社日立製作所、フェリカネットワークス株式会社、一般社団法人リユースモバイル・ジャパン

（４）事務局

（デジタル庁）

楠統括官（デジタル社会共通機能グループ長）、

国民向けサービスグループ　上仮屋参事官、城戸企画官、向上参事官補佐、
長谷川参事官補佐、二茅参事官補佐

（総務省）

長谷川住民制度課長、田中マイナンバー制度支援室長、細川課長補佐

竹村総括審議官、辺見審議官、松井情報流通振興課長、平松情報流通高度化推進室長、小村課長補佐

４．配付資料

資料１　開催要綱

資料２　スマートフォンにおける公的個人認証サービスの利活用環境実現に向けた調査研究結果　中間成果報告

資料３　スマートフォン用電子証明書のユースケース

資料４　スマートフォン用電子証明書の保証レベル
資料５　デジタル ID 及びトラストに関する国際動向

５．議事経過

（１）開会

（２）議事（議題１）

議題１開催要綱の改正について、事務局から資料１に基づき説明。

（３）議事（議題２）

議題２技術検証の中間報告について､株式会社 NTT データから資料２に基づき説明。

（３）意見交換①

概要は「６．構成員等からの主な意見」のとおり。

（４）議事（議題３）

議題３スマートフォン用電子証明書のユースケース等に関する検討状況について、事務局から資料３～５に基づき説明。

（５）意見交換②

概要は「６．構成員等からの主な意見」のとおり。

（６）閉会

６．構成員等からの主な意見（要約）

【資料２について】

〇マイナポータル等のログインの際に生体認証に加えて、スマートフォンの画面ロック解除に用いられるパターンコードや PIN が使えるようにデザインされており、ユーザテストの結果に示されているような生体認証を好まない利用者も安心して安全に利用できる準備が進んでいると思う。そのような利用者には生体認証以外の方法を奨励できるよう進めていけばよい。

〇より多くの国民に利用いただけるよう引き続き UI/UX の改善に注力していく必要がある。

〇UI/UX は、サービス開発の初期段階ではすぐに正解が出ない。今後も分かりやすさを追求するための PDCA サイクルを回していく必要がある。

〇多くの部分において検討が進んでいるが、残っている大きな技術的課題としては、アプリ間連携とかざし利用の通信性能があると思う。アプリ間連携については、アプリケーションの分割・構成をどのように実現すれば安全であり、関係事業者からの様々な要望に応えられるかが課題。かざし利用の通信性能については、国内で出荷されているスマートフォンに対して、キャリアや端末メーカーは NFC Type-A/B のかざし利用の通信性能に関する自主的な要件を定めておらず、かざし利用の可否に係る基準が不明確であるという課題がある。早く要件を固め、サービス提供開始後に速やかに利用可能とすべく取り組む必要がある。

〇今般ユーザテストが実施されたことは良いことであり、今後の開発に指針を与え得る。英国の Government Digital Service（GDS）が 2016 年に導入した GOV.UK Verify では、

７割の利用者が手続を完結できるという目標を設定しているが、本サービスについても同様に、ユーザテストの検討をさらに一歩進め、特にマイナポータルのログインの際に利用意思のある低リテラシー・高齢者の方のうち何割が自力で最後まで手続できるかという目標を設定できないか。目標設定の前提として、リリース直後に７割の目標を置いても達成は難しいため、リリース後も継続的にシステムの改善が可能な契約形態となっていること、また、仮に７割を目標とした場合に残りの３割が手続を完結できるような支援体制が必要であることも念頭に置くべき。

〇かざし利用の通信性能について、単純にスマートフォンを IC カードリーダにかざして反応するか否かの検証だけでなく、モードの切替え等、スマートフォンが通信に反応する状態にするまでの UI/UX の検討も重要である。

〇ユースケースによってかざし利用の適用可否が異なるが、各ユースケースに対して利用者がスマートフォンでどのような操作が必要であるか、利用者向けの啓発を含め、一貫性のあるメッセージを考えていく必要がある。

【資料３について】

〇スマートフォンだけで完結する利用方法とコンビニ交付サービス等のスマートフォンを IC カードリーダにかざす利用方法では、UI が大きく異なる。例えば、コンビニ交付サービスで生体認証を利用する場合にはコンビニ側のシステムも改修が必要になると思う。具体的なユースケースを考える上では、システム側を含めて全体として検討すると分かりやすくなるのではないか。

〇マイナンバーカード用電子証明書の民間サービスにおける利用は、主に電子署名を用途とするものであり、認証器として使う例はほとんどない。スマートフォンでの利用を考える場合には、認証手段として利用してもらうことが非常に重要であり、そのようなユースケースをもう少し広く検討した方がよい。

〇電子認証と電子署名の分類をきちんと整理し、それぞれの用途で検討することは重要である。

〇コンビニ交付サービスや健康保険証の利用が伸びてくると思うが、その次にマイナポータルの活用、最終的にはスマートフォンでほぼ全てのサービスが提供され、皆がそれを使っていくという方向性のロードマップを描いてほしい。

【資料４について】

〇IAL 及び AAL に関する整理に異存はない。しかし、AAL とは基本的に当人認証のためのものであるため、利用者証明用電子証明書については本資料の整理でよいと思うが、署名用電子証明書を用いた電子署名に関しては必ずしも十分ではない。署名に関して、例えば、eIDAS 規則では電子署名生成装置（electronic signature creation device）が位置づけられており、その認定制度もある。電子署名は認証とは別の話である点を理解した上で、このような観点からも今後検討が必要ではないか。

〇日本の場合、eIDAS 規則の適格電子署名と高度電子署名のような電子署名のレベル分けが明確にされていない。スマートフォン用の JPKI で電子署名を実現する場合、適格電子署名に相当すると言えることが適当であると思うが、その方向性は明確にしておいた方がよい。

〇各手続に対しどのような保証レベルを求めるかについての解釈は幅があると思う。例えば、e-Tax の税申告や法人関係の手続は、実際にはレベル２相当の認証で相当のことを行うことができるのではないかと感じている。個人の一連の手続について必要な保証レベルについては、ガイドラインや規則の原典だけでなく、米国・欧州における実際の運用を含めた調査を行うとともに、それぞれのユースケースを基に判断していく必要があるのではないか。

〇スマートフォン用電子証明書の身元確認保証レベルが「レベル？」とされているが、マイナンバーカードを所持し、本人しか知り得ない知識（パスワード）を用いてマイナンバーカード用電子証明書による身元確認をした結果が派生していることに照らし合わせると、電子証明書をスマートフォンに搭載する際にも同じことをしていると言えるのであれば、レベル３の身元確認保証レベルが派生したと解釈してよいと思う。

〇電子証明書がスマートフォンに搭載されて使用頻度が増えていった際に、近親者によって本人しか知り得ないはずの知識が利用される可能性はあり、今後このような課題についても検討していく必要があるのではないか。本人しか知らないはずの知識よりも、生体認証の方がより安心して安全に使える可能性もあり、今後さらに議論していくべき。

〇犯罪収益移転防止法施行規則第６条第１号ワでマイナンバーカードの署名用電子証明書を利用した本人確認が認められている一方、同号ホでは容貌の画像等を送信する方法によっても本人確認が認められている。後者の方法と比べると、マイナンバーカードの機能をスマートフォンに搭載した場合の利用者証明用電子証明書及び署名用電子証明書を利用することは、はるかに論理的に安全な認証方式と言えると思う。スマートフォンへの搭載に当たっても、保証レベル３とする前提で、リスクを考慮しながら検討・議論できればよいのではないか。

〇スマートフォン用電子証明書を保証レベル３とするのは、レベル３のマイナンバーカードが存在し、そこから他が介在する余地なく同等レベルで派生するという考え方で初めて実現できることである。さらに、J-LIS の認証局として構築されているトラストアンカーに紐付いていることが重要である。

【資料５について】

〇NIST SP 800-63-3 が制定された 2017 年当時、FIDO 認証は UAF が少し利用されている程度であったが、SP 800-63-4 では FIDO 認証を含めたスマートフォンの生体認証の扱いや認証器に対する考え方が整理される可能性が高いのではないかと考えている。国際的な動向を注視していくだけでなく、日本からも積極的にコメントを提出する等の関与を考えてもよいのではないか。

〇最近の国際動向を見ると、モバイル運転免許証への対応を含めて、スマートフォンの OS に国際基準に沿った機能を埋め込み、標準機能としてサポートする動きが広がっている。このような国際動向にうまく同調することで、セキュアエレメントの機能を使いながら、費用を抑えて身分証明書のスマートフォン搭載を実現できる可能性が出てきたのではないか。GP-SE 方式の検討当初はスマートフォン関係各社のロードマップや国際標準が形になっておらず、十分に意識することは難しかったが、実際に電子証明書のスマートフォン搭載がサービスインする時間軸で見た時には、スマートフォンに身分証明書が搭載されることは当たり前になることが想定される中で社会的な評価を受けることになる点は意識しておく必要があるのではないか。

○現在の NIST SP 800-63-3 におけるレベル３は、耐タンパ性を有する IC チップの利用とされているが、SP 800-63-4 に向けた議論の中では、スマートフォンに搭載されている全ての IC チップがレベル３とは言えない場合の扱いについて議論がある。１つの方向性として、耐タンパ性を有する IC チップがない場合でも、フィッシング耐性を確保する認証手段としての所持と知識、あるいは所持と生体情報の組合せが評価されるようになっており、３段階のレベルに例えばレベル２プラス等を追加するような議論になっているという認識である。

○米国では住民票のようなものが整備されておらず、カードの運転免許証も州単位で発行されていた背景があり、モバイル運転免許証によってマイナンバーカードに相当する統一感のあるものを実現しようとしている。その意味では、国民の本人確認基盤の仕組みに関して我が国は先行しており、これから米国のように運転免許証をベースにしていく訳ではない。既存制度をきちんと捉え、認証局の有無といった X.509 とそれ以外のアーキテクチャの関係性も踏まえて、我が国としての対応を検討する必要がある。

○スマートフォンで利用する機能の中でも認証の利用が圧倒的に多いと思うが、マイナンバーカードの機能のスマートフォン搭載の検討が始まってから状況が変化している中で、GP-SE を前提としない認証サービスの案を検討してもよいのではないか。

○リモート署名が増加する中で、スマートフォンに電子証明書を格納しない形で電子署名をする方法は国際的にはどのように扱われるのか。極めて例外的であるのか又は主流になるのか。

○EU の場合、eIDAS 規則においてリモート署名を適格電子署名として認める形があるため、モバイル端末向けにリモート署名をベースに電子署名を実現している国があると認識している。一方、リモート署名方式の適格電子署名とするためには、署名用デバイスとして耐タンパハードウェアである HSM をサーバ側に用意する必要がある。EU 各国の人口は日本と比べると多くない。仮にリモート署名方式を日本で実現することを考えた場合、電子証明書をスマートフォンに格納する方式と比較してどちらがコストパフォーマンスがよいかは、よくよく議論する必要がある。

○リモート署名では秘密鍵自体をリモート署名事業者に預けるため、一般の判子でいう実印をこのような事業者に預けることに相当し、その点をどのように整理するのかという問題もある。リモート署名の場合、単なるシステムだけの問題ではなく、制度面の検討も必要になる。

○本検討会のスコープを外れるが、今後電子証明書のスマートフォン搭載の周辺環境をどのように整えるかという意味では、ユースケースに合わせた適切な技術方式を議論していく必要があるのではないか。海外の PKI と比較しても電子証明書の中に基本４情報を埋め込む形は特殊な実装になっていると思っており、電子証明書をシリアルナンバーで突合することが適切であるかも含め、利用方法の変化や技術動向を踏まえて今後の JPKI の運用自体を考えていくべき。

○Android Ready SE プログラムによって、低価格端末でも GP-SE の搭載が必須化される方向である。

以上