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２回）
議事概要

１．日 時：令和２年12月４日（金）10時00分～12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、楠構成員、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・大橋氏・斎藤氏・馬場氏・関本氏・中野氏・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、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、内閣官房情報通信技術（IT）総合戦略室、内閣官房番号制度推進室

（４）総務省（事務局）

三橋住民制度課長、渡邉参事官、池田企画官、隅田課長補佐、細川課長補佐

竹村総括審議官、辺見審議官、飯倉情報流通振興課長、飯嶋デジタル企業行動室長、清尾課長補佐

４．配付資料

資料１　開催要綱

資料２　第１回検討会における指摘事項

資料３　電子証明書のスマートフォン搭載に関する初期発行フロー（継続）

資料４　スマートフォン特有のライフサイクルへの対応（継続）

資料５　各業務におけるユーザ操作イメージの整理

資料６　中古端末における利用者情報の取扱い

資料７　スマートフォンへの生体認証の搭載・FIDO認証の適用を通じて得られた知見を基にしたご提案

参考資料１　QSCD（Smart Card）認証スキーム調査報告

参考資料２　電子証明書のスマートフォン搭載に関する初期発行フロー

参考資料３　スマートフォン特有のライフサイクルへの対応

５．議事経過

（１）開会

（２）議事（議題１から６まで）

議題１開催要綱の改正、議題２第１回検討会における指摘事項、議題３電子証明書のスマートフォン搭載に関する初期発行フロー（継続）、議題４スマートフォン特有のライフサイクルへの対応（継続）、議題５各業務におけるユーザ操作イメージの整理、議題６中古端末における利用者情報の取扱いについて、事務局から、それぞれ資料１～６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」を参照。

（４）議事（議題８）

議題８スマートフォンへの生体認証の搭載・FIDO 認証の適用について、森山構成員から、資料７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」を参照。

（６）閉会

６．構成員等からの主な意見（要約）

〇Android OS におけるセキュアエレメントは 2 つの方法によりアクセス可能であり、グローバルプラットフォーム・サポーテッド・セキュアエレメントとも呼ばれていることなどを踏まえ、「Android-SE」ではなくて、「GP-SE」といったより汎用的な呼称とするのが望ましい。

〇現在、マイナンバーカードだけで 4 種類の PIN が存在し、十分に理解できていない利用者が大半だと思われる。今回のスマートフォン用の仮 PIN も含めて、新たに利用者が意識する PIN がどれだけ出てくるのか、これらは別の値を設定しなければならないのか、同じ値でも構わないのか、呼称の区別も含めて利用者が十分に理解できるような整理が必要。

〇スマートフォン用の仮 PIN の必要性、PIN ロック解除フローについて整理が必要。

〇PIN の初期化について、今回のフローだと他人のスマートフォンの PIN を初期化できてしまう恐れがある。PIN を失念したら再発行で良いのではないか。

〇SEI-TSM はどういう事業者に対して、どのように認定するのか。例えば J-LIS が何らかの認定や監査を行うのか検討が必要。

〇競争性が発揮される形での調達が行われる必要があり、ベンダーロックインとならないように十分配慮してほしい。

○マイナンバーカードを取得していることが前提となっているが、スマートフォンだけで利用したいという要望が今後出てくると思われるので、将来的にはその方向についても検討する必要がある。

○CC 認証は全体としてコンポジット認証を取得することが好ましい。CC 認証に対する扱い方はインダストリーにより異なるため、どの部分をコンポジット認証とするのか検討が必要。

○失効された署名用電子証明書がオフラインで勝手に利用されないように、例えば J-LIS 側で証明書の有効性確認のうえ、アプリケーションに対して外部認証しないと署名できない仕組みについても検討してはどうか。

○エストニアの SIM 方式のモバイル ID やスマート ID は全てのスマート端末で利用可能となっている。政府が提供するサービスである場合、誰でも利用できるという点は非常に重要だと思われるので、なぜ日本はスマートフォンに限定され、利用できない端末があるのかということについて、諸外国と比較して説明できるようにしておくべき。

○生体認証の活用に関して、現在と同様に J-LIS が責任を持って運用するためには、J-LIS が生体認証のロジックや各スマートフォン端末の第三者評価の状況等を把握できる仕組みが必要。また、成りすましが発生した際に、端末メーカーの責任とすることや、生体情報の適切な管理まで利用者に要求することは難しいと思われ、責任分界をどうするのか議論が必要。さらに電子署名法第３条の固有性の要件を充足できるかが課題。

○日本の場合、EU のように保証レベルがあまり議論されていない。生体認証を使う場合には、例えば EU の保証レベルの中又は高なのか、署名の場合には、適格署名又は高度署名なのか等をまずは議論した上で生体認証の活用について時間をかけて議論すべき。

○生体認証における他人受入率（FAR）は 0.002% 以下とのことだが、本人拒否率（FRR）がどの程度か確認したい。

○高齢者がマイナンバーカードの電子証明書の有効期限切れで自治体窓口に来られた際、大半の方が PIN を失念している状況。利用者にとって使いやすいモデルを検討していく中で、今回提案のあった FIDO 認証含め様々な認証方式についても議論したい。

○FIDO 認証は、金融業界でも大幅に導入が進んでいる状況。既に 2 年程度運用されているが、FIDO 認証に起因した不正送金等は承知していない。従前のワンタイムパスワード等と比べて大幅にユーザビリティが改善され、アプリの利用者が増加している状況。

○スマートフォンに認証器を搭載する場合の技術要件等も含めて、諸外国の例も参考としながら、整理をしていくことが必要。

○マイナポータルをはじめ、政府のウェブサイトのユーザビリティを改善すべきと、総理等から強く求められているところであり、来年前半の早い時期に向けて整理が必要。

以上