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３回）
議事概要

１．日 時：令和２年 12 月 23 日（水）13 時 00 分～15 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）、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・小田氏・関本氏・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）

髙原自治行政局長、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　第２回検討会における指摘事項

資料２　中古端末の流通・紛失に係る事業者の対応

資料３　リユースモバイルガイドラインに基づく取組

資料４　旧端末に搭載した電子証明書及び秘密鍵の悪用防止策

資料５　第１次とりまとめ（案）
～電子証明書のスマートフォン搭載の実現に向けて～

資料６　公的個人認証法の改正による電子証明書のスマートフォンへの搭載（制度骨子案）

参考資料　PIN 初期化の概略フローの修正

５．議事経過

（１）開会

（２）議事（議題１及び２）

議題１中古端末の流通・紛失に係る事業者の対応について、事務局から、資料２に基づき説明し、一般社団法人リユースモバイル・ジャパンから、資料３に基づき説明。議題２旧端末に残る電子証明書・秘密鍵の悪用防止について、事務局から、資料４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４及び５）

議題４カード機能のスマートフォン搭載の検討に係る第１次取りまとめ、議題５公的個人認証法の改正概要について、事務局から、それぞれ資料５及び６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）

〇資料全体に渡って、電子証明書と表記されている場合は秘密鍵を含んでおらず、電子証明書等と表記されている場合は秘密鍵を含んでいるという理解でよいか。どこかで電子証明書等を定義したうえで、電子証明書等と表記すれば十分な箇所が見受けられる。

〇電子証明書は場合によっては他人にも見せるものであり、秘密鍵のような重大な秘密ではないことから、電子証明書と秘密鍵では相当に秘密の重大性が異なる。その辺りのメリハリがあってもよいのではないかと思うが、秘密鍵と同様に管理して、削除もするという形でもよい。

〇ネットワーク利用制限確認／SIM ロック解除等の大口対応窓口の設置、キャリアショップ店頭でのデータ消去対応については、現時点でキャリアが対応すべき理由には乏しいのではないか。また、MNO との間で中古端末の国内流通に向けた協議を加速することに期待する声が高まっているとの記載について、これは本検討会のスコープ外と思われ、別の場で議論されるべき事項と考える。

〇自社が販売した Android 端末については、店頭で GP-SE 内のデータを消去可能と思われるが、他社が関わったものなど全ての Android 端末の GP-SE 内のデータを消去できるわけではないのではないか。また、実際に店頭では GP-SE 内のデータを消去するのみであって、電子証明書が失効済であり適切に削除されていることの確認まではできないのではないか。さらに、端末の初期化では GP-SE 内のデータは消去できないのではないか。

〇Google 社が定める Android 互換性定義ドキュメント（Compatibility Definition Document（CDD））において、生体情報については、ファクトリーリセットしたときにリムーブすることが規定されている。一方で、GP-SE については、Android 端末の実装必

須要件ではないこともあり、GP-SE 内のデータ削除については規定がない。理想的には CDD の中で、GP-SE 内のデータについてもファクトリーリセットした際にはリムーブすると規定いただき、メーカーにそれを準拠していただくのがよいのではないか。もし国や地域によってはそれが必須要件となると困るという事情がある場合には、今回は日本国内のスマートフォン市場において、FeliCa 対応のための要件の中で削除することを規定するのが良いのではないか。

○今回の検討内容が実用化される時期において、既に GP-SE が搭載されたスマートフォンに対して、削除機能を後から具備できるか否かについて確認すべき。また、技術的に可能であっても、実際にビジネスの観点からメーカーが後から削除機能を具備するか否かは疑問が残るので、それでも利用を推進するのか、削除機能が具備されることを必須要件とするのか確認すべき。

○ガバナンスの効きづらいマーケットプレイスでの CtoC でのスマートフォン端末の売買に対しての懸念やその対策について確認したい。

○GP-SE の状態を端末リセット等で初期化できてしまうこととすると、セキュアエレメントそのもののセキュリティ、安全性の低下を招く可能性があるので十分注意しながら議論することが必要。

○セキュアエレメントのデータを消去するソフトウェアの内容、品質は重要であり、ソフトウェアそのものの認定の概念について検討すべき。

○エストニアのスマート ID 等を参考に GP-SE を必要としない方式の必要性も検討するとのことだが、こういったスマート ID 等は、リモート署名の仕組みを含んでいるように思われるため、リモート署名についても記載したほう良いのではないか。また、利用者証明用電子証明書が重要なデジタル ID であるという表現になっているが、一般的な表現なのか確認してほしい。

○前回議論になった仮 PIN について、スマートフォンで PIN が全く設定されていない状態で、最初に PIN を設定する際には TSM 側で仮 PIN を設定する必要があるということで理解した。

○一時保留時に簡単な本人確認を行うとのことだが、署名用電子証明書が搭載されているスマートフォンを紛失し、それを悪意の第三者が拾得した場合、基本 4 情報、マイナンバー以外ほぼ全ての情報を拾得した者も持っていることとなるが、それは本人確認になり得るのか。また、一時保留という措置自体の必要性を確認したい。

○移動端末設備用の電子証明書とカード用の電子証明書の扱いは同等なのかそれとも異なるのか確認したい。

○NIST SP 800-63-2 において議論されていた Level of Assurance（LOA）は、NIST SP 800-63-3 において Identity Assurance のレベル（IAL）、Authenticator Assurance のレベル（AAL）、Federation Assurance のレベル（FAL）の 3 つの体系に分解されている。カード用の電子証明書は対面での本人確認のため IAL3 であり、耐タンパ領域に格納されているため AAL3 である。

○移動端末設備用の電子証明書について、マイナンバーカードが基となって derived される環境を経て、プロセスが一定の IAL を保証できるならば、IAL3 と見なすことができ、鍵の生成においても、秘密鍵は一切外へ出さないため AAL3 であることが保証でき

ることから、対面での本人確認ではないもののカード用の電子証明書と同等と考えても良いのではないか。

〇EU でも同様にナショナル eID から発行された eID については最も高い保証レベルを認めており、カード用の電子証明書と同等とみなしても良いと考えるが、ライフサイクルが異なるため識別は必要。また識別と区別の 2 つの表現が混在しているが、識別という表現に統一すべき。

〇署名して申請することとなっているが、15 歳未満の方は署名用電子証明書を持っていないため、15 歳以上の方のみを対象にするということで良いのか。

〇国際標準の変化のスピードは早くなっており、スマートフォンのエコシステムにおけるデファクトスタンダードとなっている CDD は毎年更新されていることから、毎年確認をしていくことが重要。

〇生体認証について、利用者証明用電子証明書への導入を提案し、署名用電子証明書への導入については要継続検討と考えていたので、一旦このような整理で良いと思うが、将来に向けての可能性に蓋はしないほうが良い。

〇利用者証明用電子証明書におけるパスワードないし 4 桁の暗証番号、署名用電子証明書におけるパスワード 6 文字から 16 文字に対して PIN という表現が利用者にとって分かりやすいか否か検討が必要。

〇移動端末設備用の電子証明書とカード用の電子証明書の PIN は違うものであるべき又は本人の判断で同じものを設定して良いといった考え方はあるのか。PIN を失念する方が多数いる中、4 桁の方については、生体認証を利用できると道が開けるが、6 桁以上の方については、またさらに別の PIN を設定するとなると、利用しやすいものになるのか疑問であるため整理してほしい。

〇サービスモデルを展開する中で、例えば健康保険証の活用といった一定の利用者を確保できるものから、段階的に順次普及を図っていくという考え方も必要。今回のスマートフォン活用の取組は、最終的にはオンライン上で完結することを目指していると思われるので、ユースケースの将来像の中にあるコンビニ交付については、過渡期としては良いが、最終的には段階的に収束していく展開を考えるべき。

〇エストニアについて、デジタル ID の普及率が 99%ということが取り上げられるが、スマートフォン活用はあまり進んでいないのが実情で、35%程度しかオンラインでの手続には利用されていないという話も聞いている。また、我が国が目指しているものと仕組みに相当な差異があるところ、エストニアの 35%を超えるようなものを目指してほしい。

以上