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４回）
議事概要

１．日 時：令和３年１月29日（金）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、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）、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）、江口業務部長・大橋氏・斎藤氏・馬場氏・静氏、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、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　開催要綱

資料２　スマホならではの使いやすいUXの実現に向けて

資料３　エストニアの電子証明書等について

資料４　公的個人認証サービスと紐付けられた民間事業者が発行する電子証明書の利活用について

資料５　前橋市のマイナンバーカード利活用について

５．議事経過

（１）開会

（２）議事（議題１及び２）

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。議題２生体認証等の活用について、森山構成員から、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」を参照。

（４）議事（議題４及び５）

議題４エストニアの電子証明書等について、事務局から、資料３に基づき説明。議題５公的個人認証サービスと紐付けられた民間事業者が発行する電子証明書等の利活用について、xID 株式会社から、資料４に基づき説明し、前橋市から、資料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」を参照。

（６）閉会

６．構成員等からの主な意見（要約）

〇生体認証について、今回の電子証明書のスマートフォンへの搭載の場合にどのように活用するのか確認したい。基本的には、ローカル PIN やパスワードで署名鍵が暗号化されており、署名鍵を復号するための情報をスマートフォンに入れないと、電子署名ができないこととなる。GP-SE には、いわゆる署名鍵は平文で格納され、その利用の許可をするために PIN 等の確認をしているのか。

〇基本的な考え方として、ローカル PIN がスマートフォンから入力され、それを GP-SE に渡し、GP-SE において誤りがないか確認をした後に署名するという手続きとなる。このスマートフォンからの結果に関しては、API を呼び出しその結果として、スマートフォンのレベルで一致したか否かの結果が渡ることとなるが、結果の渡し方については議論の途上であると理解している。

〇GP-SE、マイナンバーカードともに、署名鍵は外から取り出したり、覗いたりすることが一切できないチップ内の領域に平文の形で安全に格納される。カードはその中に入っている鍵をどのような状態であれば使えるかという管理機能を有しており、例えば PIN の場合だと、アプリケーションに PIN が入力され、内部の安全な領域に格納されている PIN 情報と照合すると、署名鍵を演算できる状態にするという制御を行っている。

〇生体認証を活用する方向で検討することになっており、提案に示されている方法は有効かと思われる。一方で、スマホ版の JPKI は、カード版の JPKI と異なり Android 上のアプリケーションと、GP-SE 内のアプリケーションをセットで考えなければならず、特殊な実装になる。生体認証を実装するに当たって、それぞれのアプリケーション処理の J-LIS の責任分界について、今後検討が必要。

〇提案に示されている問題が万が一発生した場合には、生体認証の機能を停止しつつも JPKI の PIN 入力は使える状態にして利用を継続できる考え方は、責任分界の観点からも非常に有効と思われる。

〇Android の API において、生体認証で認証されたのか、PIN やパターンで認証されたのかは、アプリケーション開発者が知ることができるようになっている。Android の API

で使われたのか、ローカルPINで使われたのかを基盤として知りうる手段をあらかじめ設計、実装していくことが必要。

〇公的個人認証法第17条において、CRLやOCSPを受けられるものが限定されている。住民基本台帳カードのときは公的機関のみとなっており、マイナンバーカードになったときに少し緩和されたのが今の状況ではあるが、過剰な規制のように思う。誰でもCRLやOCSPを受けられても良いのではないか。

〇認証局の議論をしている中でID事業者という表現は誤解を招く恐れがある。認証業務を営む事業者、電子署名法では特定認証業務、さらには認定認証業務という表現となっており、ID事業者というのとはレイヤーが別であると認識している。

〇エストニアの事例のeID、Mobile-ID、Smart-IDは、全て共通のeIDが使えて、それをICカードで利用する、SIMに格納してスマートフォンで利用する、簡便なポータルにより利用するなど日本の考え方とは異なる。

〇日本の場合は電子署名法と公的個人認証法それぞれ別々にあり、基本的に対象は同じ認証局の世界であることから、まさに相互認証の概念になっていくと思われる。ID連携ということではなく、あくまでもX.509証明書、認証局の連携の話の中で議論をしていくべきであり、そこでどういった法律体系があるか整理をしていくことが必要。

〇民間IDといったときに、いわゆる民間署名検証者の議論と、電子署名法上の認証局の発行した証明書の議論と、それらと紐付いた形で別のデジタルIDのようなものがあるときに、類型化とそれぞれの位置付けを明確にしていくことが必要。

〇現状、JPKIの中でシリアル番号と証明書との紐付けを行っているが、シリアル番号は連番であり、これまでいくつ証明書が発行されたかほぼ見ることができ、少し番号を変えると他の方に当たる。シリアル番号はリスクが高いから保護しているという意識ではあるが、本来、アイデンティファイアとして使うのであれば、よりエントロピーが高いものを利用する方が望ましいが、歴史的経緯でシリアル番号による紐付けが広く行われている。民間でのユースケースが増えていく中で、本当にこの運用で良いのか。IDごとに区別して扱えるような仕組みがあることが望ましい。

〇日本の基準はNIST SP800-63-3やeIDASを踏まえながら検討されてきたものであるとは思うが、現状のeIDASと十分な相互運用性があるものとなっているかは疑問であり、eIDASと相互運用性のある基準にしていくことが必要。

〇エストニアの事例のSmart-IDでは、IDを入力して、デバイスに確認コードが表示され、それを入力することとなっており、Mobile-IDでは、SMSにいわゆるワンタイムパスコードが送信され、それを入力することとなっている。最近の偽サイトや偽ブラウザではこのような仕組みを使って入力文字を搾取することがよく行われており、一見２要素認証に見えるが実はそうなっておらず、今NISTで議論になっているという認識。これは知識だけの１要素２段階認証であり、フィッシングに対しては脆弱である。

〇電子証明書がスマートフォンに搭載されてより便利に利用できるようになることから、パスワードではなくて、FIDO認証を活用し、より広く多くの方々がメリットを享受できるよう、フィッシングに対する課題を解決できるような利用方法を検討すべき。

〇電子認証について、国が公共分野で民間IDを受け入れるとなると、その民間IDはどの保証レベルに該当するのかを、何らかの形で認定・審査する仕組みが必要になるが、現状のガイドラインとの整合等、もう少ししっかりした制度設計を行うことが必要。

〇EU の場合、eIDAS が法律のようなものとして定義されており、eID などの電子認証がどの保証レベルに該当するかレギュレーションとして規定されている。それぞれの国がそのレギュレーションに合致しているかを評価して公表するという手順を行い、他国の eID が自国で受けられるか審査する仕組みがある。日本においても、同様にいろいろな側面から評価するような制度をつくるべき。

〇リモート署名がクラウド型になり導入が容易となっているので、民間や行政手続きでの利用が進んでおり、日本でどの程度本格的に普及しているかを定量的に理解しておいたほうが良い。

〇経済産業省の電子署名法研究会において、リモート署名について検討されており、EU においても同時期に検討を行っていたため、そちらも踏まえながら、JT2A においてリモート署名のガイドラインを策定しているので、参考にしてほしい。

〇エストニアの事例の Mobile-ID が有料とのことだが、今回の電子証明書のスマートフォンへの搭載に関しては、スマートフォンの買換え期間が今５年に１回となっており、そのうち GP-SE 対応のスマートフォンでしか普及していかず、１人当たりのコストがどの程度か不明であるため、どこまでのコストを許容できるのか分析した方が良い。

〇サービスに応じた適切な認証方法について示されているが、今後サービスを提供していく中でそれぞれのサービスに応じてどの認証方法が良いのかというレベル分けも考えながら検証いただき、結果をフィードバックしてほしい。

以上