参考資料2

公的個人認証サービスによる本人確認に基づき民間事業者が発行した電子証明書等を行政分野で利活用するに当たっての課題の再抽出

令和３年７月28日

総務省　情報流通行政局　情報流通高度化推進室

オンライン識別手段の保証レベル①

指摘内容	回
日本として署名や認証についての安全性のレベルを定義をする必要があると思う。例えばEUであれば、認証レベル、eIDのレベルとして3段階のレベルを提供しており、米国ではSP 800-63でより細かく定義しているが、日本のeIDや電子署名についての安全性のレベルをどう考えるか明確にしておく必要がある。なぜなら、民間のIDとの連携という話があるが、どのような民間のIDを受け入れるか、明確な基準がなければならない。また、例えばマイナポータルへのログインについて、認証レベルが最も高い、EUでhighと言われている認証レベルのものを受け付けるのであれば、認証の鍵がソフトウェアで保護されているものは高いレベルとは基本的に認められないはずなので、それはマイナポータルへのログインには使えないよう制御をせざるを得ないと思う。その意味では、どのようなものが最も高い認証レベルに適合しているのか等を定めておく必要がある。そうしなければ、民間の方々も、何をサービスとして提供すれば受け入れてもらえる・もらえないのか判断できない可能性があるため、整理が必要と思う。 生体認証についても同じで、従来、例えばEUであれば、最も高いレベルのeIDについて生体認証を認めている国は基本的にはないと認識している。エストニア等では更新時に生体認証を取り入れる工夫をされている部分もあるが、実際の利用時において何かにプラスして生体認証を使ってログインするものを、最も高い認証レベルと認めている国は恐らくないと認識しているので、その辺りの整理もしていく必要があると思う。	1
マイナポータルとの関係では、マイナポータルだから最高レベルのセキュリティを（求める）ということではなく、申請書の提出、電子申請の話をしているのか、自己情報（取得）APIへのアクセスの話をしているのか、資格確認をしているのか、様々なユースケースがある中で、それぞれのリスクレベルを見て、そのリスクに応じたレベル感をルールに従って検討していくことが重要になってくると思う。	1
全体を通して、アプリケーションとの連携のところも含めて、大きな意味ではポリシーマッピングをどうするかという議論になると思う。様々なコンポーネントがあって、Identity Assurance、Authenticator Assurance、Federation Assuranceという3つの大きな概念があって、これはNIST SP 800-63-3に書かれている考え方である。eIDAS規則ではクオリファイド証明書とアドバンスト証明書の考え方があり、幾つか切り口はある。このようなところを整理して、我が国としてどうあるべきかを検討するということが非常に重要だと感じている。	1
認証強度について、事務局から返答があったように、IT室の「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」において3段階のレベルになっているが、これに対してマイナンバーカードに紐づいた民間IDがどれに相当するのかあまり整理されていないので、それが今回はっきりしたらよいと思う。ユースケースについては様々な方から指摘があったが、ガイドラインを見ていると、レベル3と一番高いもので行政で想定されているのは、税確定申告や在外邦人のインターネット投票のような年に1回するかどうかのもので、マイナンバーカードのJPKIでいうと、署名用電子証明書を使うということになっている。マイナンバーカードでいうと利用者証明用電子証明書、あるいは基準でいうと対面あるいは郵送オンラインの身元確認等、複数の当人認証でできることで想定しているのが、今般のコロナでもあった給付金の話など、ほとんどの電子申請等はレベル2で可能なので、ユースケースと突き合わせて、何をしたいのか整理した方がよいと思う。	1
日本の場合、EUのように保証レベルが議論されていない。生体認証を使う場合には、例えばEUで言う認証レベルの中又は高なのか、署名の場合に、適格署名なのか高度署名なのか等をまず議論した上で、電子認証、電子署名に対して、生体認証をどう使うのかについてもう少し時間をかけて議論した方がよいと感じている。	2

オンライン識別手段の保証レベル②

指摘内容	回
（生体認証の利用は）世界でやっていないということではなく、御紹介があったように、台湾、韓国、エストニアでも類似のものが使われている状況であり、欧州のeIDASにおいてどのような整理が行われているかというようなところもある話なので、例えば署名用（に対して生体認証を利用する）ということは中々ハードルが高く、例えばリモート署名との組合せ等の議論にもなってくると思うが、スマートフォンの中に認証器として入れる場合の技術要件等も含めて、諸外国における整理も参考としながら、来年（令和3年）前半に整理をしていく必要があると思う。	2
ICカード、マイナンバー（カード）が基になって、derivedの場合、このような環境を経て、プロセスが一定のIALを保証できるのであればIAL3と見てもよいということになってきている。今回の方式を見たときには、（スマホ用証明書の保証レベルはカード用証明書の保証レベルと）同等としてもよいのではないかと判断している。具体的には、鍵の生成時に秘密鍵は一切外へ出さないためAAL3が保証でき、対面ではないがプロセスがきちんと閉じていることから考えると、これは同等と考えてよいのではないかと思う。	3
先程NISTの話があったが、EUでも同様に派生クレデンシャル、ナショナルeIDから発行されたeIDについては最も高いレベルの用途と認めているので、恐らく今回のもの（スマホ用証明書）についてもマイナンバーカードと同等とみなしてもよいと思う。	3
NIST SP 800-63は63-4のレビューの段階にある。その意味では、NISTのこれに取り組んでいる方々も、様々なところから意見を聴いて改訂に向けて動いているところであると思う。こういった状況をよく捉えていくことが非常に大事であって、2017年に策定された63-3が全てではない。	3
NIST 800-63-3については、社内にこの考え方を啓蒙して、身元確認と当人認証のレベルを高める、そして他のサービス事業者との連携についてもこの考え方でやろうと話している。これは非常に大事な取組と思っている。国内においては経産省の検討会（※）において本人確認＝身元確認＋当人認証という定義をガイドライン（※）の中で書いていた。この中では、身元確認をレベル3で実施して、当人認証のレベルも3であれば、本人確認をレベル3でできる旨が書かれていたと記憶している。	3
【保証レベルの考え方が存在しない】（電子署名法には）当人認証の考え方が存在しないにもかかわらず、（取得のハードルは高いものの）認定認証さえ取得すればすべての行政手続きが可能となってしまっており、制度と現実が乖離してしまっている。認定認証業務の身元確認の手法についても、公的個人認証以外の対面ではない本人確認手法が認められており、IAL2とIAL3の区別がつけられていない。	4
電子署名法に基づく認証業務に係る電子署名は、犯罪収益移転防止法律における特定取引時の本人確認や、携帯電話不正利用防止法の契約時の本人確認等に利用することができる。この例のように、電子署名法に基づく電子署名の効力が、公的個人認証法に基づく電子署名と同等に位置づけられるよう、法令の整備をお願いしたい。	4

※それぞれ「オンラインサービスにおける身元確認に関する研究会」及び「オンラインサービスにおける身元確認手法の整理に関する検討報告書」

オンライン識別手段の保証レベル③

指摘内容	回
公的個人認証で遠隔による本人確認を行って発行された電子証明書はIAL3になり得るのかについては、内閣官房が2019年に出したNISTをベースにしたガイドライン（※）があるが、スマホ搭載JPKIはIAL3のマイナンバーカードの電子証明書により本人確認されているとみなしてもよいのではないかという御指摘があった。スマホ搭載JPKIがIAL3になるとすれば、同様の本人確認を行って認定認証局が証明書を発行する場合にもIAL3になるのかが1つの論点だと思う。その参考として、エストニアのSmart-IDは非対面のeIDによる本人確認で、LoAの最高位を取得している。その上でリモート署名のレベルをどう捉えるかが課題と思う。秘密鍵を利用した端末とサーバーとに分割して保管している場合にIAL3とみなすことができるのか。エストニアの場合には秘密鍵を利用者端末とサーバーに分割して、LoA highを取得しているが、本来、リモート署名よりローカル署名の方が秘密鍵の漏えいに関しては本人の意思に反して署名がされてしまうリスクが高いと考えている。最後に、リモート署名にはソウルコントロールの課題はあるが、例えばSmart-IDのように秘密鍵を端末とサーバーに分割して管理することで、ローカル署名のソウルコントロールとリモート署名の秘密鍵安全性という双方の長所を持ち合わせるという大きな特徴を生かすことができるのではないかと考えている。	4
民間IDと言った時に、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、それらと紐づいた形で別のデジタルIDのようなものがある時に、これらの類型化とそれぞれの位置づけは明確にしていく必要があると思う。	4
資料4のp.17にIALとAALの話があるが、IDを拠り所にして別のIDを振っていく時のIALやAALの考え方等、AALについてはどちらかというとリモート署名を使ったときの考え方は、元々日本の基準はSP 800-63-3やeIDAS規則を見ながら検討されてきたものだとは思うが、これを見る限り、必ずしも現状のeIDAS規則との間で十分にインターオペラビリティがある仕様となっているのか分からないので、検討を深めていく中で、日本の基準が独自のものになっているのであれば、インターオペラビリティを持てる基準にしていく必要があるのではないかと思う。	4
事務局からTEEがGP-SEと同じぐらい安全という話があったが言い過ぎだと思う。SEとTEEの安全性のレベルは違うというのが一般的な考え方だと思うので、少し注意していただきたい。	5
TEEとSEのセキュリティレベルについては、欧州を含めて国際的にどのようなレベル付けがされているのか、そして現状はマイナンバーカードで4PINを入れる局面はそこまで機微ではないものが相当ある中で、どこまでこのやり方でできるのか、議論できるとよい。	5
NIST SP 800-63-4の検討については、米国の考え方が大分見えていると思う。あくまで私見だが、米国と欧州の大きな違いは、日本と欧州の近いところも含めて言うと、米国ではカードを民間適用ではスキップするという感じ。政府ではPIVがあるが、民間との関係ではICカードを公的機関から発行してそれに基づく考え方はなく、FIDO認証を利用して本人認証、アイデンティティマネジメントをする動きに見えている。その先は、例えばクラウド上で様々な処理をさせるような概念か。また、従来のID、パスワードとの親和性が高く、公開鍵方式ではあるがX.509を使わない世界でのやり方であり、その点ではこれからSP 800-63-4やISO/IEC 23220の動きを見なければならないのも事実だと思う。一方、我が国とEUは、政策的にICカードを国民全員に配るという方向で、そのカードには署名が入っている。米国の場合は、署名は全然違う概念で動いているように見えている。ただ、FIDOなどを使って本人認証ができれば、その延長上でリモート署名なども考えられるので、必要な場合にはその方向性で米国は動く気もする。	6

※「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（平成31年2月25日CIO連絡会議決定）

電子署名（電子認証局の信頼性確保）：技術動向を踏まえた電子署名法の見直し

指摘内容	回
民間事業者が発行する電子証明書というのは、認定認証業務による発行を想定していると考えてよいか。そうだとした時に、現在様々なところで（利用が）進んでいる秘密鍵を預けるタイプのリモート署名で認定認証業務の電子証明書を使う場合は検討するのか。そうだとすれば、電子署名法施行規則の変更が必要になる可能性があるが、これを見込んでいるのか。	1
電子証明書の法的根拠となる電子署名法は、20年前に制定されたまま現状抜本的な改正がなされていないため、昨今の技術に制度が追いついてないことから、実際の認定認証業務には以下のとおりの多くの課題がある。（下記4項目に続く）	4
【コスト面での課題】パブリッククラウド等の利用は想定されておらず、厳格な入退室管理がなされた設備室が求められる上、証明書の発行や管理以外では遠隔操作が認められない等、自社でデータセンターを運営することが事実上必須となり非常に高コスト。監査費用だけでも年間400～600万円程度が継続的に発生する。帳簿の作成や保管等の業務手順の要件も非常に多く、煩雑。紙を前提としての帳簿保管も一部見られるため、そのような部分を棚卸していく必要があると思う。高い運用コストは証明書の価格に反映されてしまっており、現状1通1万円～程度となっており一般個人には全く普及していない。認定基準が厳しいこともあり、2016年を最後に新たな認定取得事業者はでていない。	4
【リモート署名が想定されていない】サーバー側で利用者秘密鍵を生成した場合は、「それを利用者に安全に渡した後、速やかに破棄」することが規定されており、一般的な利用者秘密鍵を事業者側で生成・保管する形式のリモート署名は事実上不可能。	4
【オンラインによる自動的な本人確認手法が想定されていない】公的個人認証は認定認証業務の本人確認手法として規定されているものの、人的な業務にて本人確認を行うことが前提とされている。例えば申込書の受領者氏名や本人確認の諾否を決定した者の氏名等を帳票として随時記録すること等が求められている。	4
【利用者秘密鍵の取扱いに規定が全く無い】電子署名法には、本人確認から秘密鍵の発行・管理業務は基準が詳細に規定されているものの、利用者署名鍵の保管方法や当人認証についての規定は存在しないため、安全面に課題のある鍵管理方法であったとしても認定の取得は理論上可能となってしまっている。	4
リモート署名が民間で急速に普及しており、自治体でも検討が始まっていて、リモート署名でできる手続が増えていくことは定量的に理解をしておいた方がよい。電子署名は民間や行政で使える手続があるから普及するので、リモート署名が日本でどのぐらい本格的に普及していくのかは、レポート等が昨年末から多く出ているので理解しておいた方がよいと思う。特に行政と話をしていると、リモート署名でクラウド型になっていると導入が非常に簡単であり、それで民間だけでなく自治体も検討していると思う。	4
約4年前にJT2Aでリモート署名について検討している。そこでは、電子署名法自体を書き換える必要があるのかないのかという議論までは至っていないが、その一歩手前のところでリモート署名ガイドラインを作成している。当然、EUもリモート署名の検討をちょうど同じ頃行っていたのも参考にしたり、向こうとも一部議論をしたりして、レベル感を持たせているので参考にしていただきたい。 また、クラウド型になると、エンドユーザーに証明書や秘密鍵を渡さないことで非常にコストが下がる。電子認証でクラウドに入り、その延長上で自分の鍵を署名に使うことになるが、その厳格性についてはHSM等の技術基準も含めてEUも規則や標準化でまとめており、日本でもそれを併せてガイドラインの形にしているので、それが1つの叩き台になるのではないか。	4

電子署名（電子認証局の信頼性確保）：認証局の相互認証

指摘内容	回
資料4のp.12に民間デジタルID事業者とあるが、この議論は認証局の議論をしているように見えるので、ID事業者というと誤解を招く気がする。電子署名法では、認証業務を営む事業者があり、特定認証業務、認定認証業務があるので、IDの事業者とはレイヤーが別だと思う。そのため、IDと証明書の議論というのは別だということを明確にしていく必要があると思う。その上で、エストニアの例でeID、Mobile-ID、Smart-IDが出てくるが、IDの考え方が日本と違っていると思う。同じeIDをサブジェクトネームに入れる形になっているので、IDが共通に使えて、それをICカードの形で使う場合、SIMに入れてスマートフォンの形で使う場合、より簡便なポータルを利用する場合がある。日本の場合は、マイナンバーでIDを統一して民間でも使えるのかというとそうではない。ここはあくまでもX.509の証明書、認証局の連携の議論をしていくべきという気がする。日本の場合は電子署名法と公的個人認証法が別々にあるが、対象は基本的に同じ認証局の世界で考えていて、今その連携ということが出てきたので、まさに相互認証の概念になっていくと思う。ですから、それはIDの連携ではなく、X.509（証明書）の連携の議論の下で、どのような法律体系があって、それは公的個人認証法であり電子署名法があるという整理をしていく必要がある。	4
公的個人認証系の話と、電子署名法に基づく民間の認定認証事業者などの認証局、そこから発行される証明書、その両方が国内で流通していく中で、それぞれの証明書側で署名した場合に、それがお互いに渡ったときにどうなるのかについて整理していく必要が出てきたと思う。昔からそれはあったが、エンドユーザーが使う環境で実際に見えてきたところで、今後整理していく必要があるということが、xIDから発表されていると思う。	4
（IALやAALのインターオペラビリティについては）実は別のスロットで、トラストサービス、eIDAS規則の中でもeシールについて、基本的にはEU側との相互認証の議論になっており、検討しなければならないことは事実だと思う。	4
公的個人認証証明書で本人確認を行う認証局は、認定認証局の4号の届出と特定認証局の5号認定の2つがある。電子申請での利用はブリッジ認証局と相互認証を行う必要があって、現状では認定認証局、4号認定に限られる。5号認定を受けた特定認証局であっても、その認定基準には署名法と同等な技術・設備・運用の要件が示されているので、電子申請での利用の可否を検討するべきと思う。また、5号認定を受けた特定認証局も含め、ブリッジに接続する等の相互認証の方法を検討するべきではないか。 公的個人認証証明書で本人確認を行う民間の電子証明書の利用は、オンラインでの本人確認が可能なため、今後はリモート署名サービスやベースレジストリと連携した属性情報の付加によって、電子申請あるいは電子契約など様々な官民のアプリで、ワンストップでクラウド上での電子署名の利用が容易になると考えられる。 今後、認定認証局あるいは5号認定を受けた特定認証局は、対面と同等な本人確認あるいは技術・設備・運用要件が示されているので、EUの適格証明書と技術的同等性が確保されていると考えられる。従って、今後国際相互承認を入れた相互認証の方法を検討すべきではないか。	5
トラステッドリスト等の将来性ついて検討するのは是非やるべきと思う。電子署名法による認定と公的個人認証法の5号認定の基準は非常に近いが、実は認定の運用の厳格さが違うなどにより5号認定でやっている人がいることを理解した。この2つの制度が同様の基準で同様のことをしているのに併存するのはおかしいので、将来的にはこの2つをまとめていく方向で進めるべきではないか。	5
そもそも公的個人認証法の5号認定と電子署名法の認定は、本来同じ制度の下、同じの基準の下であるべきと思う。施行規則レベルでは本当に同じで、違うのは欠格事業者の部分くらいしかないので、包括的な認証制度の検討は今後行うべきだと思う。	5

電子認証（法制度の整備）①

指摘内容	回
xIDの説明では電子署名法について秘密鍵の格納を維持できていかないとか、保証レベルの考え方が明確でないなどの意見があったが、皆さんの意見を伺っていると、電子署名と電子認証の切り分けとか、それぞれ何が必要かを明確に分けられていない部分がまだあると思う。電子認証について、いわゆるeIDと言われている部分に相当するが、ガイドラインはあるが制度がないことが今後問題になってくると思う。特に、国が公共分野で民間が提供するIDを受け入れることになると、その民間が提供するIDはどの保証レベルに該当するのか何らかの形で認定・審査する仕組みが必要になると思うが、その拠り所が現状ではガイドラインに合っているかどうかになってしまっているのを、もう少し制度として作る必要があると思う。先程からEUの話は出ているが、EUの場合には、eIDAS規則がそもそもEUの中の法律のように定義されているし、さらに電子認証がどのレベルに該当するかについて規則が出されている。各国がその規則に合致しているか、自分たちがeIDとしているものが規則に合致しているかを評価をして公表するという手順を行って、他国のeIDが自国で受けられるか審査する仕組みがあるので、日本においても同様に様々な側面から評価を行う制度を作るべきであると思う。	4
電子認証と電子署名は分けて議論しなければならない。特にFIDO認証は電子認証を中心に見ていて、電子署名は一切ない。FIDOとの比較で言うと、X.509（証明書）を使う世界か使わない世界かという違いが電子認証に現れていることがポイントだと思う。FIDOも公開鍵方式を使っている点では技術的に原理は同じであるが、FIDOでは公開鍵をFIDO認証サーバーに登録するところを、一旦認証局から公開鍵を認証してもらったものを登録することによっても、同じ構造を作ることができる。 国際的にも、EU側が日本と同様にX.509の世界でeIDAS規則等を実現してきている。それに対してFIDOをeIDAS規則に適合するようにする考え方でも提案が出てきていて、（FIDOを）X.509化するという流れも一方ではある。我が国においても、X.509の世界とFIDOが今後混在してくると思うので、ここで議論するかはさておき、見ていく必要がある。	5
利用者証明用電子証明書の法的位置づけや普通のFIDO認証との違いは、署名用（電子証明書）と比べるとあまり整理されていないような気もするので、本来マイナンバーカードの立ち上がりのタイミングで議論されてきたことではあるとは思うが、どこかで整理、再確認しておく必要があると思う。	6
欧州の動きは参考にしていく必要があるし、日本の署名用電子証明書、利用者証明用電子証明書をどこにマッピングしていくのか等インターオペラビリティを考えていく必要はあると思う。一方で、欧州は体系を作るのは得意だが、本当にそれで利活用が進んでいるのか等を含めうまくいっているのかもフォローしていく必要があると思う。 また、マイナンバーカードに特化した論点では、冒頭の前半の議論でもあった利用者証明用電子証明書の位置づけが、トラストにおける意思の証明でないことは明らかだが、果たして発行元証明であるのか、存在証明であるのかを明らかにすることが非常に重要だと思う。 現状の署名用電子証明書のユースケースというのが、結局、基本4情報が取れるものなので、実質的に身元確認のため利用されてしまっているのが実態で、そのような使われ方をすることによって、逆に、それが本当に意思の証明であるかが揺らいでしまう。本来、利用者証明（用電子証明書）というのは、利用者を証明できるはずであるが、そこから基本4情報が引けないことによって、結果として存在証明にしかなっていない面もあると思う。署名用電子証明書が意思の証明として機能するように、また利用者証明用電子証明書が単なる存在証明ではなく、発行元の証明になるための仕組みを作っていく必要があるのではないかと思う。	6

電子認証（法制度の整備）②

指摘内容	回
確かに署名用・利用者証明用電子証明書の論点は非常に重要で、特に民間側では、電子署名法には利用者証明用電子証明書に相当するものは全く定義されておらず、署名用のみである。だから電子署名法という名前で呼ばれている。その点では、公的個人認証法では利用者証明用電子証明書についても入っているということで、包括的なトラスト（基盤）を見た時には電子認証という世界を定義し考えていくというお題が出てきていると思う。今後、トラストに関するWTでは、包括的な立て付けの中で電子認証をどのような位置づけにするのかが議論の対象となり、検討していく必要があるだろうと考えている。 その意味では、我が国の中で全体ということなので、民間の方では電子署名、タイムスタンプ、この先出てくるeシールと呼ばれているもの等々が対象であるが、既存の公的個人認証法や商業登記に基づく電子認証制度なども概念としては同じ領域である。今後責任分界点も含めた様々な視点で、これらを我が国としてどう体系化をしていくかは非常に重要な1つの論点でもある。特にEU、UNCITRAL等では、これらを包括的な視点から捉えているので、我が国としてその方向性を今後デジタル庁等で検討していく内容になると思っている。	6