参考資料1

民間事業者が利用者の本人確認のために公的個人認証サービスを利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

⓪検討の進め方・範囲

指摘内容	回
今日（第1回）の検討というよりは、全体の検討の方向性で1つ申し上げたい。検討事項(2)「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、もう一度課題を確認して、その課題に関してどんなタイムラインで実行していくのかをもう少し明らかにした方がよいと思う。具体的には、プラットフォーム事業者は5年前からあるが、残念ながらあまり活用されていない。そこには、カードが普及していないということ以外の理由があり、システムの話でも法の話でもない、運用の話というのがあって、来年には実現できてしまうものもあると思う。例えば、プラットフォーム事業者はパブリッククラウドの活用というのは認められておらず（※）、数千万円をかけてサーバーを構築しなければならないことがあるが、これは実は運用の話で、プラットフォーム事業者の先の実際に公的個人認証を使う民間事業者のコストになっている。また、シリアル番号の管理も運用の話だと思う。この2つ以外にも運用面の課題を洗い出して、それに関していつまでに何をやるのかというのを検討してもらいたい。資料2のp.7を見ると令和4年まで何も変わらないように見える。	1
この検討会の検討の範囲について、これまでマイナンバーカードをスマートフォン搭載にかかわらず民間企業で特に利用されてこなかった背景としては、事業者がこういったマイナンバーカードの機能を実装したサービスを開発すること自体が手間が多く、例えば、それは大臣認定を取ったり、あるいは大臣認定を取っている事業者と連携することも面倒だったりということがあったと思う。今回の検討会において、スマホ搭載に関しては、エンドユーザーの利便性について追求する議論を行うと思うが、事業者がマイナンバーカードの機能のスマホ搭載されたものを活用して、どういった形で、その事業者が検討するサービスに実装できるのか、そこの利便性がどう高まっていくのか、それは行政サービス・民間サービス双方なのかについて、今後の検討会で議論できればと思う。	1

※認証業務及びこれに附帯する業務の実施に関する技術的基準（平成15年総務省告示第706号）を改正し、設備室への入出場管理、災害の防止等のために必要な措置の記載を改めることで、パブリッククラウドの活用が既に可能となっている。（令和3年総務省告示第45号（令和3年2月15日施行））

①JPKIの利用コスト（PF事業者のシステム利用料、失効情報提供手数料）

指摘内容	回
JPKIの利用に関しては、シリアルの管理等も含めて検討が必要であるが、最も民間がJPKIを利用しにくいという部分は恐らく費用の問題があると認識している。現在では、CRLでもOCSPでも、1回当たり、署名（用電子証明書）の場合は20円、利用者証明（用電子証明書）の場合、2円の費用がかかる。海外の例では、例えばOCSPについては、リアルタイムで問合せを行うことになるため課金している国がほとんどであるが、CRLについては無料で開放している例も結構ある。もちろんOCSPとCRLの利用にはタイムラグがあるので、どのような場面はOCSPを利用しなければならないというのはあると思うが、費用面の考え方も検討が必要であると思う。	1
マイナンバーカードの応用を検討したことがあるが、実感としては、2円、20円というのはあまり高くない。これが実際にプラットフォーム事業者を介して使おうとすると、数百円ぐらいかかってしまうケースがあるのが実情。費用の話は、単なるJ-LISの問題だけではなく、マイナンバーカードを利用するエコシステム全体で考えていく必要があると思う。	1
パブリッククラウドの利用が認められていない（※）ので、サーバー構築、データセンターの運営等に多大なコストがかかる。	4
元々J-LISの失効情報確認の利用料金というのは20円、2円であるが、実際にはそこのコストというのが、乗合いで下がる想定だったが下がっていないこと、数百円以上かかるということが課題になっていると思う。	4
現状はOCSPだけでなくてCRLも課金されているが、実際諸外国においてはCRLは無料で開放しているケースも多いということで、こういったところが具体的に課題になってきていると感じる。	4
まえばしIDでは、サービス利用に基づく個人情報管理の許諾を電子署名で行うために、まえばしIDとマイナンバーカードの紐づけを行う構想。具体的には、マイナンバーカードに搭載される2つの電子証明書に記載されるシリアル番号を取得し、当該シリアル番号とまえばしIDのひもづけを行うことを想定。この際に、個人情報管理の許諾を電子署名で行う場合は、署名検証者等の情報提供手数料の無償化や、個人情報管理の許諾管理にマイナンバーを利用可能とするなどの規制緩和が必要と考えている。	4

※前ページ参照。

②民間事業者の提供するサービスの利用者識別情報との紐づけ

指摘内容	回
民間サービスにおいて、今、不正アクセスを防止する手段としては民間IDにSMS受信可能な携帯電話番号を予め紐付けて、利用者を一意に特定する手法が多く使われている。ただ、この方法は加入者が携帯電話を解約して一定期間経過すると、また同じ電話番号が他の方に再利用される問題が指摘されている。既に提供されているマイナンバーカード制度対応の本人確認サービスよりも軽量で利用者を一意に特定できるサービスができると不正アクセスを防止する手段として大変よいと思う。つまり、その方であるということから本人を特定できるよりは匿名性を持つ、仮名という言い方が恐らく正しいと思うが、NIST SP 800-63-3で表現されているpseudonymous identityとして利用できるものがあると大変便利に使えると思う。	2
エストニアの場合にサブジェクトネームに何を入れているかという話もあった。どこまで議論をしていいのか悩ましいが、現状JPKIの中でシリアル番号とマイナンバーとの紐付けが行われている。これはかねがね気持ち悪いと思っており、シリアル番号は連番であるため、これまで何枚の証明書が発行されたかをほぼ見ることができ、番号を変えると他人に当たる。なぜシリアル番号を保護しているかというと、基本的にそれだけリスクが高いからという意識ではあるが、本来、識別子として使うのであれば、よりエントロピーが高くて、当てずっぽうに番号を入れ替えても当たらないようなものを利用したほうが望ましい。歴史的経緯で他に使える識別子がなかったので、証明書シリアル番号による紐付けが広く行われているが、民間でのユースケースも増えていく中で、本当にこれがよいのかというのは、この検討会で議論すべきか、マイナンバーカード自体の使用の議論も今後あるように聞いているが、そういったところで議論すべきかを含めて、今の運用が本当にベストかについては悩むところがある。	4
シリアル番号との関係というのは、シリアル番号そのものが外に出ていった時に様々な予測ができる。エントロピーが足りないとか、他の事業者から見ると問題だということで、IDごとに、これをペアワイズというと誤解される可能性があるが、区別して扱えるような仕組みがあればなおよいだろうという話をしている。ぜひこういった点については、非常に可能性のある議論だと思うので、今後、議論の土俵に乗せていただけたらと思う。	4
サービス提供者がシリアル番号を利用することになるため、総務省の認定を受けるか、認定事業者からの届出を受けるというようなプロセスは必要かと思う。さらに、ここにいわゆるlinkability、IDとシリアル番号の組があるため、万一にもIDとシリアル番号の組が漏えいしてしまった場合などに様々な波及リスクがある。前回の議論の中でもシリアル番号の使い勝手の悪さについては議論があったと思う。NIST SP 800-63-3でもいわゆるpairwise pseudonymous identity、サービス提供者ごとに限定できるような仮名性を確保したIDの必要性が触れられているので、これをシリアル番号に代えて利用できればより一層利活用しやすいアカウントリカバリーの基盤になると思う。	5

③署名用電子証明書で署名した文書の保管

指摘内容	回
本検討会の対象でないことを十分理解した上でコメントであるが、JPKIの失効情報、CRLやOCSPをより自由に流通させるべきだと思っている。そうでなければ、いわゆる長期署名などの長期保存に関する様々な情報のアーカイブに当たって非常に不便があると言われている。そうすると、公的な申請だけでは（JPKIの）利用が進まないというおそれがあるのではないか、要するにマイナンバーカードの普及も進まないのではないかと思っている。その意味で、民間事業者が発行する電子証明書の利活用に関して考えていくことは非常に重要なものだと思うが、民間事業者の証明書を発行・利用するためだけにマイナンバーカードの取得やJPKI（証明書）をスマホにインストールするということが本当に行われるのかどうかについては若干不安を感じている。	1
電子契約書への電子署名というのは、証明書の有効期限の終了後であっても、それを検証する必要が出てくる。そのためには、CRLとOCSPを電子署名や電子証明書と併せて保存したり、あるいは相手方に提供したりする必要がある。現在の公的個人認証法ではCRLやOCSPのやり取りはできないので、考えていかなければならない。	1
マイナンバーカードで署名するということが定着しない背景には、署名を行うとシリアル番号が文書データに残ってしまって、これをプラットフォーム事業者しか保管できないということがある。押印された紙の文書であれば、自分のところの金庫に入れておけばよいが、マイナンバーカードで署名した瞬間に、自分たちの持ち物なのに自分たちの金庫に置いておくこともできない。実際にシリアル番号のプライバシーに対するインパクトの問題があってこのようになっていると思うが、今のルールのままでは民間の利用が広がっていかないのではないかと心配している。	1
現状、電子証明書、シリアルナンバー、CRL、OCSPの各情報は、データセンターを持たないみなし署名検証事業者では一切の保存・管理が禁じられている。例えば電子契約にマイナンバーカードを使いたいと言っても、証明書が含まれている電子文書を保管するということが、みなし署名検証事業者は当然にできないため、かなりユーザビリティが悪くなっている現状がある。また、署名を付した文書データを利用者ですら保管が現状できず、失効情報確認が前提になるが、非常に使いにくい状態となっている。本来、電子署名に関しては、将来にわたり検証する必要が生ずるので、検証者に証明書やOCSP、CRLを流通・提供できないと民間利用が広がらないのではないかというのは、非常に同意するところである。	4
認定認証業務の要件として、本人確認実施時の証跡を帳簿として残すことが求められているが、（中略）PF事業者以外が公的個人認証の結果としての電子証明書やOCSPレスポンスを保管することができない（理論的には保管は可能であるが、実際に行おうとすると帳票までもPF事業者データセンター内で10年以上管理する必要があり、非常に高コストとなり非現実的）。	4
資料4のp.11のJPKIの課題は全く同感で是非解決していくべきものであるが、論点として、公的個人認証法第17条ではCRLやOCSPを受ける者を限定している。元々、住基カードの時から公的機関しかできないとなっていて、これがマイナンバーカードになった時に少し緩和されたが、なぜこれを限定しなければならないのか、政府の見解を改めて教えてほしい。マイナンバーカードの電子証明書があまりにも便利になると、現在の認定認証業務に対する民業圧迫になるのではないかという話を聞いたことがあるが、それが原因なのか、ほかに原因があるのか。それを考えなければ、この課題をどう解決すべきかについて話が進まない。	4
シリアル番号のデータベース化（の禁止）は今の法律にもあり、それは一般に検証者以外にもかかる制約だと理解しているが、CRLやOCSPを取得できる者を限っているのはどのような理由か。そのようなことをしないで、誰でもCRLやOCSPを取れてもよいのではないか。CRLでもOCSPでも（シリアル番号は）1個ずつしか入っていないので、そのような制限は過剰な規制のような気がする。（この後、シリアル番号のリストを作れないようにしたいということがポイントと承知。）	4
資料4のp.14の認定認証業務の課題には民間署名検証者の話も入っていると思うが、マイナWGでも議論があったように（※）、利用環境の改善をしっかりと考えていく必要があると思う。	4

※次ページ参照。

（参考）マイナンバー制度及び国と地方のデジタル基盤抜本改善WGにおける議論

デジタル・ガバメント実行計画（令和2年12月25日閣議決定）
「マイナンバー制度及び国と地方のデジタル基盤の抜本的な改善に向けて（国・地方デジタル化指針）」（抄）

III　33の課題を解決するための取組方針
3. マイナンバーカードの機能強化
3.2 カード機能（公的個人認証サービス）の抜本的改善（スマートフォンへの搭載、クラウド利用、レベルに応じた認証、民間IDとの紐付け等）
③認証の保証レベルに応じた認証サービスの推進
【現状】
マイナンバーカードは、公的個人認証サービスのほか、ICチップの空き領域にアプリケーションを搭載することで、認証手段として活用することが可能であり、国及び地方の行政機関等はもちろん、民間企業も認証の保証レベルに応じて方法を選択し、活用することが可能である。また、公的個人認証サービスに、民間IDを紐づけて、登録が確かな民間IDとして活用することも可能である。
【取組方針】
（イ）利用要件・利用手続等の改善
民間事業者の要望をよく聴き、民間事業者の視点に立ち、利用要件・利用手続等の継続的な改善を実施する。なお、この一環として、2020年度（令和２年度）中に、署名等確認に用いる設備に係る基準を見直し、クラウド利用を認める（※）。また、JPKI証明書を使って署名が行われた文書の保管についても、JPKIの民間利用を妨げることがないよう検討し、必要な措置を講ずる。

※p.1を参照。

④基本4情報の取扱い／⑤利用者証明用電子証明書の活用

指摘内容（④）	回
署名用電子証明書に含まれる個人情報の再検討ということで、現状は名前、生年月日、性別、住所の基本4情報が入っているが、事業者からすると取り扱いにくい。また住所が入っていることで、住民票の異動を伴う引越しによって、証明書のライフサイクルも短くなる（転出すると証明書が失効してしまう仕組みであるため）。やはりマイナンバーカード、マイナンバーに対する国民の不安というのは一定程度あると感じている。そういった中では、基本4情報までが含まれている証明書をスマホに搭載するというところに対して懸念点がある方も一定数いるのではないかと思う。今回J-LISの方でも令和4年に失効情報確認した後に最新の基本4情報を提供するAPIも提供していただけるということなので、証明書にそもそも本当に基本4情報は必要なのか、例えばスマホ搭載JPKIに関しては、証明書に含める情報に関して見直しを行う等も検討してもよいのではないか。例えばエストニア（のeIDカード）の場合には、eIDと名前の情報のみという形であるので、住所等を含めないことで、よりライフサイクルが長くなるということもあるのではないか。	4

指摘内容（⑤）	回
FIDO認証の登録をする時にJPKIを使うことができれば、署名用電子証明書を利用することで、基本4情報を含む証明書により厳格な本人確認が、1回当たりの費用は高いかもしれないができる。あるいは利用者証明用電子証明書を使って、基本4情報が変更になっても証明書は有効で、基本4情報が含まれている証明書に基づくものではないが、その方であるという一意性を表現することはできて、その符号としてシリアル番号も利用でき、1回当たりの費用は安価である。かつスマホでは生体認証も今後使えるようになる方向ということで、便利に使えるであろう。	5