参考資料2

# 第4回検討会における民間事業者が発行する電子証明書等の利活用に向けた課題に関する指摘事項

令和3年3月3日

総務省　情報流通行政局　デジタル企業行動室

# 民間事業者が発行する電子証明書等の利活用に向けた課題に関する指摘事項（第４回検討会①）



## ◆課題整理の方向性

① IDと証明書の議論は別ということを明確にしていく必要がある。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、基本的に対象は同じ認証局の世界で考えていて、その連携は相互認証の概念。これはID連携ということではなく、PKIのX.509の連携がどうかという議論の元で、どういう法律体系となっているかを整理すべき。

② 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、電子証明法上の認証局の発行した証明書の議論と、それらとひもづいた形で、また別のデジタルＩＤ的があるときに、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。

## ◆民間発行の電子証明書自体の課題

① 認定認証業務は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。

② 当人認証の考え方が存在しないにもかかわらず、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。

③ リモート署名や鍵分割の本人確認保証レベルをどのように評価するか。

④ リモート署名が民間で急速に普及し、自治体も導入が容易なクラウド型を検討していて今後対応サービスが増えていくことを理解しておくべき。

⑤ 電子署名法では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。

⑥ 電子署名法では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おり、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。

⑦ 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。

## ◆民間証明書をJPKIに紐付ける際のJPKI側の課題

① 署名用電子証明書には基本4情報の全てが記録されており、事業者にとっては取扱いにくい。また、住民票の異動を伴う引越しによってライフサイクルも短くなるため、含まれる個人情報を再検討すべき。

② 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。実際に行おうとすると非常に高コストとなり非現実的。

③ OCSPやCRLを誰でも取得できて良いのではないか。【→「ID」の課題①が根本にあり】

# 民間事業者が発行する電子証明書等の利活用に向けた課題に関する指摘事項（第４回検討会②）



## ◆民間証明書の受入れに当たる課題（保証レベルと対応手続）

① 身元確認（IAL）については、主務大臣による認定認証によって法的な認定を得ることができるが、当人認証（AAL）や署名プロセスについてはそもそも法的に認定する制度がない。認定認証のスコープに含めていくのか別の制度を整備していくのか。

② 「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」においても、公的個人認証や署名プロセスについてはあまり考慮されておらず、さらなる整理と議論が必要。公的法のみならず電子署名法も抜本的な見直しが必要なのではないか。

③ 民間取引における本人確認についても、改正犯罪収益移転防止法、携帯電話不正利用防止法、等が保証レベルに基づいた整理となっておらず、一貫性がない。

④ 「電子署名法」に基づく認証業務に係る電子署名は、犯罪による収益の移転防止に関する法律における特定取引時の本人確認や、携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律の契約時の本人確認等に利用することができます。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ます。

⑤ IDを拠り所にして別のIDを振っていくということにおけるIALの考え方、またAALの考え方等、AALはどちらかというとリモート署名を使ったときのAAL等の考え方について、日本の保証レベルの基準が独自のものになっているのであれば、NISTやeIDASとのインターオペラビリティが持てる基準にしていく必要がある。

⑥ 電子認証について、いわゆるここでいうeID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る。電子認証について、民間が提供するIDを公共分野で受け入れるとなると、そのIDがどういう保証レベルに該当するのかを、 EUのように様々な側面から審査・認定する仕組みが必要。

## ◆JPKIにおける「ID」の課題

① 電子証明書と紐付くシリアル番号をidentifierとして使うのであれば、よりエントロピーが高く、当てずっぽうに番号を入れ替えても他の証明書に当たらないようなものを利用したほうが望ましい。

② JPKIよりも軽量で利用者を一意に特定できるサービスを実現できないか。現状の本人確認サービスでの提供機能に加えて、利用者証明のみ実施しただけで、NISTのSP 800-63-3におけるpseudonymous identityにあたる値を提供。証明書のシリアル番号は5年、カードのシリアル番号は10年で変わってしまうので、利用者を一意に特定できる環境で、サービス提供者毎に「仮名加工」して廉価に提供できる環境ができると、デジタル化の推進を活性化できる。【第2回の再掲】

## ◆その他

① マイナンバーカードの普及が進む今、開発者にとって使いやすい周辺環境の整備、例えば認定タイムスタンプ事業者などの他のトラストサービスとの連携、署名フォーマットAPIの提供など、市場原理を理解しながらビジネスエコシステムの構築を進めていく必要がある。

② 単一のeIDを用いてあらゆるサービスで認証・署名ができる利便性は単一障害点ともなる可能性があり、国民の生活基盤となっているeIDでの認証や署名にダウンタイムがあればその経済的損失は計り知れない。官民連携によりJPKIにおける単一障害点をカバーすべき。

③ 役所に行かなくても、証明書が有効期限内であれば、オンラインで更新可能とすべき。