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

誰一人取り残さないデジタル社会実現のための、トラストサービス領域での
官民共創・連携を民間デジタルID活用により推進するための課題

xID株式会社
2021年1月29日

本資料の内容

海外における民間デジタルID(民間電子証明書)と公的身分証(公的電子証明書)の関係性や役割

- 欧州におけるモバイル派生IDのサービス分布
- モバイル派生IDの概要(エストニア・ベルギー事例比較)
- eIDカードとSmartIDで可能なこと比較整理
- 時代ニーズと課題解決を考えたeIDエコシステム(エストニア参考)
- 公的電子証明書(eID)と民間電子証明書(SmartID)の補完関係

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

- 「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」とは？
- 現状の公的個人認証サービスとその課題
- 民間デジタルID事業者が発行する電子証明書の信頼性を担保する方法とその課題
- 公的個人認証に紐付けられた認定認証業務とは？
- 認定認証業務の課題
- 本人確認保証レベルとは？
- リスク評価と必要な保証レベル
- 本人確認保証レベルによる分類
- 本人確認保証レベルにおける論点
- トラストアンカー（JPKI）とトラストサービスの役割
- 誰一人取り残さないデジタル社会の実現のために

現行のスキームに関する課題等

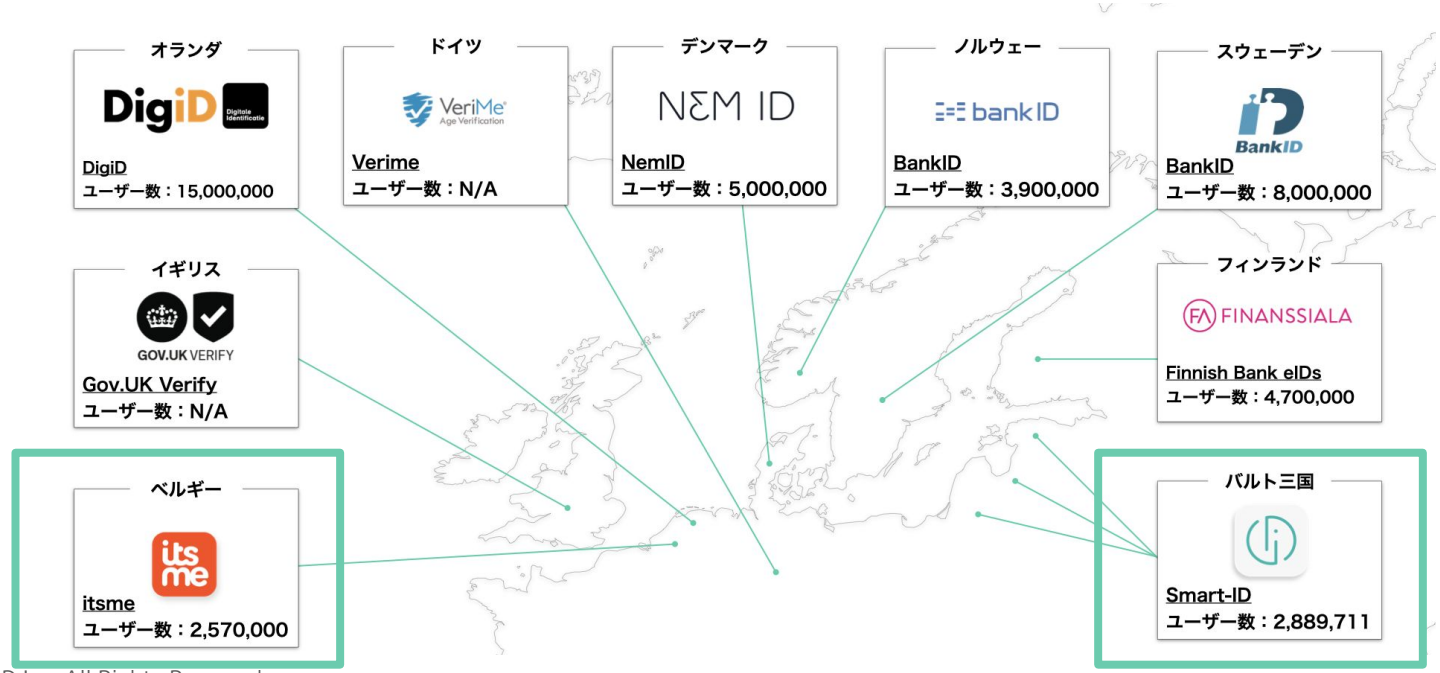
- トラストアンカーを提供する政府にご検討いただきたいこと
- トラストサービスを提供する民間事業者として推進していくこと

海外における民間デジタルID(民間電子証明書)と公的身分証(公的電子証明書※)の関係性や役割

※公的電子証明書：政府機関が発行する電子証明書

欧州におけるモバイル派生IDのサービス分布

欧州では、**政府発行のeIDカードや国民IDをトラストアンカーとした民間企業の提供するモバイル派生デジタルIDサービス**が多く見られる。その中でも、**政府発行eIDカードのICチップ内に記録された公的な電子証明書を活用した本人確認により、**モバイル派生デジタルIDサービスを提供する**民間企業も電子証明書を発行**している代表例としては、**エストニア**で提供されている**SmartID**、**ベルギー**提供されている**itsme**がある。



モバイル派生IDの概要(エストニア・ベルギー事例比較)

	SmartID (エストニア)	itsme (ベルギー)
提供開始年	2016年	2017年
運営主体	SK ID Solutions	Belgian Mobile ID
本人確認の手法	**eIDカードに格納された電子証明書による本人確認(電子署名)**	**eIDカードに格納された電子証明書による本人確認(電子署名)**
プライマリ認証	2種類のPIN(認証用:4桁/署名用:5桁)	1種類のPIN(5桁)
生体認証サポート(セカンダリ)	なし	**あり - 認証、電子署名双方に利用可能**
電子署名(eIDAS準拠)	**リモートQSCD**	**リモートQSCD**
鍵生成と管理	利用者端末上 **(ただし、秘密鍵を分割管理しており、リモート署名方式に分類)**	事業者側環境 リモート署名方式(秘密鍵の保管も全て事業者側)
サポートOS	**iOS/Android**	**iOS/Android/Huawei**
利用可能なサービス	**130以上のサービスで利用可能** (行政/保険/ヘルスケア/金融/教育/通信/その他各種民間サービス)	**150以上のサービスで利用可能** (税務/金融機関/医療/保険/各種民間企業/行政サービス/教育)
利用者数 (2020年12月30日現在)	**2,893,963人(国内41.5%の利用者)** ※利用者人数はラトビア・リトアニアを含む	**2,631,206人(国内23%の利用者)**
署名アルゴリズム/鍵長	**RSA/4096bits**	**RSA/2048bits**
eIDAS LoA	**HIGH**	**HIGH**

出典：https://www.ria.ee/sites/default/files/smart-id_tagatistaseme_kirjeldus_abiv.pdf
出典：https://brand.belgianmobileid.be/d/YShKZtiEUmGM

eIDカードとSmartIDで可能なこと比較整理

エストニア政府発行のeIDカード(公的電子証明書)と、民間企業発行のSmartIDを例として、できることの違いを比較する。
SmartIDは2018年8月に、eIDAS準拠のリモートQSCDとして認められてからオンライン投票を除く行政手続きにおいても認証、電子署名双方の手段として導入されている。オンライン投票については現行法で政府発行の公的電子証明書に限定される記載があり、昨年の国会で議論されたがまだ法改正には至っていない。

	eIDカード (政府発行の公的電子証明書)		SmartID (民間企業発行のeIDAS準拠QSCDの電子証明書)	
利用目的	認証	電子署名	認証	電子署名
電子契約(電子署名)	N/A	官-民、民-民の契約で利用可能	N/A	官-民(一部制限あり)、民-民の契約で利用可能
電子処方箋の受取	✔	✔	✔	✔
医療ポータル(電子カルテ)へのアクセス	✔	✔	✔	✔
オンライン投票	✔	✔	非対応	非対応
e-tax	✔	✔	✔	非対応
国民ポータルへのアクセス	✔	✔	✔	手続きごとに異なる
オンライン法人登記	✔	✔	✔	✔
車両登録手続き	✔	✔	✔	✔
オンラインバンキング	✔	✔	✔	✔

時代ニーズと課題解決を考えたeIDエコシステム(エストニア参考)

2010年以降、スマートフォンの普及によりデジタルサービスの利用方法はスマホにシフト。2011年にはモバイルSIMに証明書が搭載されたMobileIDが登場したが、2019年末時点での国内利用率は17%に留まる。その後、2016年後半にSmartIDが登場。2020年末時点で国民の40%以上が利用している。

	eIDカード (ICカード) 国民の99%が保有	MobileID (モバイルSIM) 国民の17%が利用	SmartID (iOS/Android対応) 国民の41.5%が利用
課題など	・ICカードの接触不良などのトラブル ・スマホ、タブレット非対応 など	・携帯ショップでの店頭手続必須 ・渡航時SIM入れ替え、ローミング利用必須 ・音声回線の契約必須、通信回線のみ不可 など	・一部の行政サービスでは利用不可 ・スマホ、タブレット非対応 など
解決・改善点	N/A	**・国内通信3キャリアと連携しSIMを活用 ・SIMカードに証明書と秘密鍵を搭載 ・公的電子証明書なので、全ての手続きで利用可能**	**・iOS/Androidアプリダウンロードで利用可 ・SIM不要、通信回線のみでも利用可 ・スマホ、タブレットの両方に対応 ・リモート署名形式**

出典：https://www.id.ee/en/

公的電子証明書(eID)と民間電子証明書(SmartID)の補完関係

国民が広くeIDの利便性を享受するためには、あらゆるデジタルサービスでeIDが日常的に活用できることが必要不可欠である。エストニアでは行政サービスのみならず、金融・医療・教育などのサービスにおいてもeIDが認証基盤として利用されている。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。
eIDをトラストアンカーとした、民間の個人認証基盤を活用することで、一意な国民IDの利便性と同時に単一障害点の課題も克服することが可能となっており、国民にとっても利用シーンに応じて最適な認証方法を選択できるようになった。

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

「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」とは？

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

マイナンバーカードの署名用電子証明書による公的個人認証を行い身元確認を行った者に対して、民間の認証局が発行した電子証明書

本議論の対象

上述の電子証明書を活用するための利用者(個人)向けアプリケーション = **民間デジタルID**

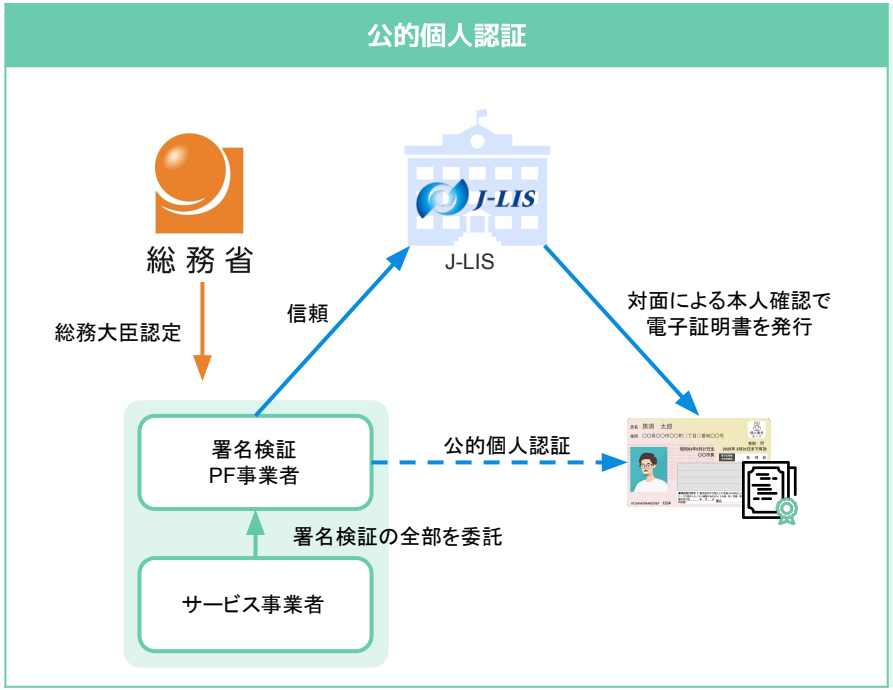
民間デジタルIDが利用者に提供できること

- 各種法令に準拠したオンライン本人確認 (Verification)
- 複数要素による安全な当人認証 (Authentication)
- 法令に準拠した電子署名 (Digital Signature)

そしてこれらのソリューションを活用することで利用者に、利便性、信頼性、安全性の高い、ペーパレスなユーザー体験を提供したいサービス事業者が、簡単にこれらを実装し、電子証明書というトラストサービスを使えることを可能にするものです。

現状の公的個人認証サービスとその課題

- 公的個人認証サービスを民間事業者が利用し、マイナンバーカードの各種電子証明書の署名検証を行う場合、総務大臣による認定が必要
- 認定取得には設備要件などの高いハードルがあるが、既に認定を取得したプラットフォーム事業者（PF事業者）に署名検証業務の全部を委託する場合、PF事業者を通じてより簡便な手続きで認定を取得することができる（みなし認定事業者）



コスト面の課題

- パブリッククラウドの利用が認められず、サーバー構築、データセンター運営等に多大なコストがかかる。
- 元々J-LISの失効情報確認の利用料金は1件あたり20円～2円であるが、PF事業者を介すると1件数百円以上かかるのが実情。
- 現状OCSPだけでなく、CRLも課金されているが、諸外国においてはCRLは無料開放しているケースも多い。

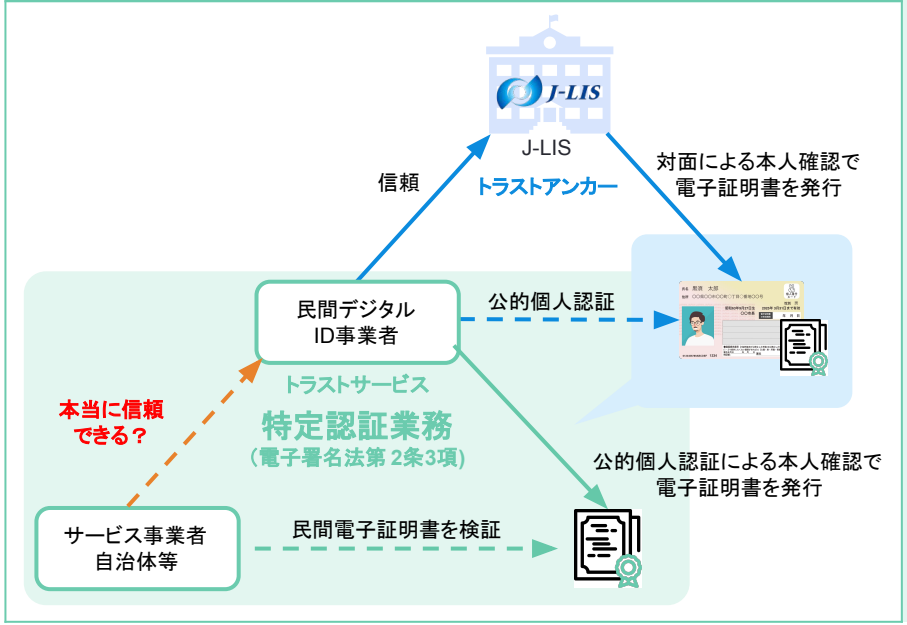
電子証明書関連データ保管の課題

- 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。
- 署名を付した文書データは利用者ですら保管できず、非常に使いにくい。
- 本来電子署名は将来に渡り検証する必要が生ずるが、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。

民間デジタルID事業者が発行する電子証明書の信頼性を担保する方法とその課題

「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」とは、公的個人認証サービスで身元確認を行い発行された電子証明書のことであり、電子署名法における特定認証業務に相当するが、それだけではその信頼性は公的個人認証の信頼性と同等に取扱うにはいくつかの課題がある。現状の解決法として最も確実なものは、指定調査機関(JIPDEC)よる監査を受け主務大臣による認定を受けることである。

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



民間事業者が発行する電子証明書が、本当に公的個人認証によって正しく本人確認を行った上で発行されたのかどうかを担保するには、以下の方法が想定される。

①委託契約により担保

- 一般的な事業者間の契約で認証業務の真正性を担保する方法
- 民間デジタルID事業者側の善管注意義務や企業コンプライアンスに頼らざるを得ず、第三者による評価が不透明で信頼性に課題あり。

②民間の認証局監査により担保

- JCANトラステッドサービスや、WebTrust等、各種の認証局監査機関による監査と認定を取得する。
- 第三者の監査により認証業務の真正性が一定担保されるが法的な効力はなく、現行法上は上記①と同列と扱われてしまう。

③主務大臣による認定を受ける（後述）

- 主務大臣又は指定調査機関（JIPDEC）による監査を受け、電子署名法で規定している設備や業務方法の基準に適合しているとして認定を取得することができる。
- 各種行政手続きに使うことができる。

公的個人認証に紐付けられた認定認証業務とは？

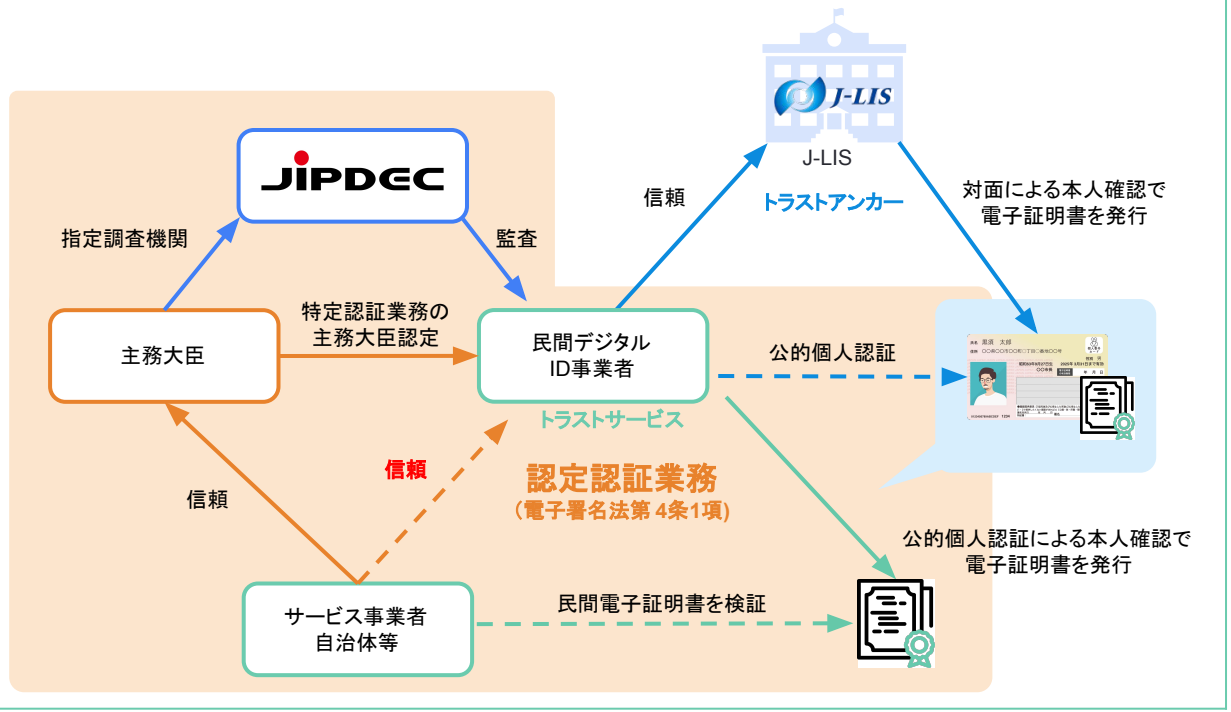
特定認証業務は、主務大臣又は指定調査機関(JIPDEC)による監査の元、電子署名法で規定している設備や業務方法の基準に適合していることが認められると、認定を取得することができる（認定認証業務）。

公的個人認証は、認定認証業務における本人確認の手法として認められており、認定を取得することで、公的個人認証と結びついた電子証明書であることが監査により担保される。

また、主務省令で定める行政手続き等においては、下記３つの電子証明書が限定列挙されており、認定を取得することでマイナンバーカードと同様に各種行政手続きで利活用することが可能になる。

・マイナンバーカードの署名用電子証明書
・認定認証業務による電子証明書
・商業登記電子証明書

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（主務大臣認定）



認定認証業務の課題

しかしながら、電子証明書の法的根拠となる電子署名法は約２０年前に制定されたまま抜本的な改正がなされておらず、昨今の技術に制度が追いついていないことから、実際の認定認証業務は以下の通り多くの課題を抱えている。

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。
- 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。

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。

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。

公的個人認証で本人確認を行った場合、帳票保管ができない

- 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、前述のとおり公的個人認証法側の課題として、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）

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。

保証レベルの考え方が存在しない

- 上記のとおり、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。

本人確認保証レベルとは？

我が国においては、NIST SP 800-63-3 Digital Identity Guidelines（米国国立標準技術研究所）を参考に、内閣官房情報通信技術(IT)総合戦略室が「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」を公表している。同ガイドラインによると、身元確認レベル(IAL)、当人認証レベル(AAL)のそれぞれの評価軸で本人確認手法を評価することで本人確認保証レベルを規定している。

保証レベル	身元確認レベル（IAL）		当人認証レベル（AAL）	
	登録	**発行・管理**	**トークン**	**署名プロセス**
	登録する氏名・住所・生年月日等が正しいことを確認すること	トークンを登録者へ確実に発行すること	認証の3要素（知識・所持・生体）のいずれかの照合すること	電子署名の方法など
レベル３ （身元が対面で確認され、信用度が非常に高い）	・ 写真付き身分証明書の**対面での確認** ・ 公的な台帳との照合 ・ 重複登録ではないことの確認	対面、もしくは本人限定受取郵便により発行	耐タンパ性をもつハードウェアを含む複数の認証要素による認証	電子政府推奨暗号リストに記載の電子署名（証明書の用途は電子署名限定）
レベル２ （身元が遠隔又は対面で確認され、信用度が相当程度ある）	・ 公的な台帳との照合、もしくは公的証明書の添付 ・ 電子署名もしくは署名捺印	対面／郵送／PW郵送＋ダウンロード／電子署名＋ダウンロード／電話番号検証＋ダウンロード	複数の認証要素による認証	電子政府推奨暗号リストに記載の電子署名
レベル１ （信用度は自己表明相当でほとんどなし）	・ 電子メールの到達確認	電子メール、もしくは登録時にダウンロード	単要素による認証	
備考	各レベルごとに該当項目の全てを満たすことが必要	失効や更新等の基準については割愛	SMS等を用いた二段階認証は、一般的に多要素認証とは認められていない	電子署名は必須ではないが、電子署名を用いない場合は各種脅威に対するセキュリティ対策が必須

※それぞれの評価軸について異なるレベルで評価された場合は、最も低いレベルが本人確認の保証レベルとなる。
（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を参照し弊社にて作成）

リスク評価と必要な保証レベル

利便性および金銭面における低位なリスク以外で、なんらかのリスクが評価される場合においては、基本的にレベル２以上の保証レベルが求められている。

リスク分類	リスク評価と保証レベル			
	影響なし	低	中	高
①利用者に不便、苦痛を与える、又は機関等が信頼を失う	Lv1	Lv1	Lv2	Lv3
②利用者に金銭的被害を与える、機関等に賠償責任が生じるなど、 財務上の影響を与える	Lv1	Lv1	Lv2	Lv3
③機関等の活動計画や公共の利益に対して影響を与える	Lv1	Lv2	Lv2	Lv3
④利用者の個人情報等の機微な情報が漏えいする	Lv1	Lv2	Lv2	Lv3
⑤利用者の身の安全に影響を与える	Lv1	Lv2	Lv3	Lv3
⑥法律に違反する	Lv1	Lv2	Lv2	Lv3

「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」（内閣官房 情報通信技術(IT)総合戦略室 2019年3月）を参考に弊社作成

本人確認保証レベルによる分類

デジタルID	登録（身元確認手法）	電子証明書の発行	トークン	本人確認保証レベル
マイナンバーカード	公的身分証による対面での身元確認 IAL3	対面もしくは本人限定受取郵便により ICカードを発行 IAL3	・マイナンバーカード（耐タンパーHW） ・PIN AAL3	**レベル３**
スマホ搭載JPKI	MNCによる公的個人認証 IAL3?	利用者端末へダウンロード IAL3?	・GP-SE（耐タンパーHW） ・PIN （生体認証は検討中） AAL3	レベル？
xID	MNCによる公的個人認証 IAL3?	サーバー上で保管 IAL3?	・鍵分割（利用者端末＆サーバー） ・PIN or 生体認証 AAL3?	レベル？
Smart-ID (参考:エストニアでの民間発行デジタルID)	eIDカードによる認証 IAL3?	サーバー上で保管 IAL3?	・鍵分割（利用者端末＆サーバー） ・PIN (生体認証は非対応) AAL3?	Remote QSCD 取得済 **eIDAS LoA:High**

論点① MNCの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になりうるのか？

論点② リモート署名のレベルをどう捉えるか？

本人確認保証レベルにおける論点

論点① 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になりうるのか？

- 「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」によると、IAL3は対面による本人確認が必要。
- 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がされているため、IAL3とみなしてもよいのではないか？
- スマホ搭載JPKIがIAL3だとすれば、同様の本人確認を行っている民間デジタルIDは、IAL3となるのか？
- エストニアのSmart-IDは、非対面でのeIDによる本人確認によりeIDAS LoAにおける最高位（High）を取得している。

論点② リモート署名のレベルをどう捉えるか？

- 秘密鍵を利用者端末とサーバーとに分割して保管している場合はAAL3とみなすことができるのか？
- エストニアのSmart-IDは秘密鍵を利用者端末とサーバーとに分割することで、eIDAS LoAにおける最高位（High）を取得している。
- 本来、リモート署名よりローカル署名のほうが、秘密鍵の漏洩により本人の意思に反して署名が生成されてしまうリスクが高い。
- ローカル署名は秘密鍵管理の責任や煩雑さが利用者側に寄っているため、端末の買い替えや破棄について配慮が必要。
- 一方で、リモート署名にはソロコントロールの課題がある。秘密鍵を端末とサーバーに分割して管理することで、ローカル署名のソロコントロールと、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ているのが、鍵分割の大きな特長。

その他の論点

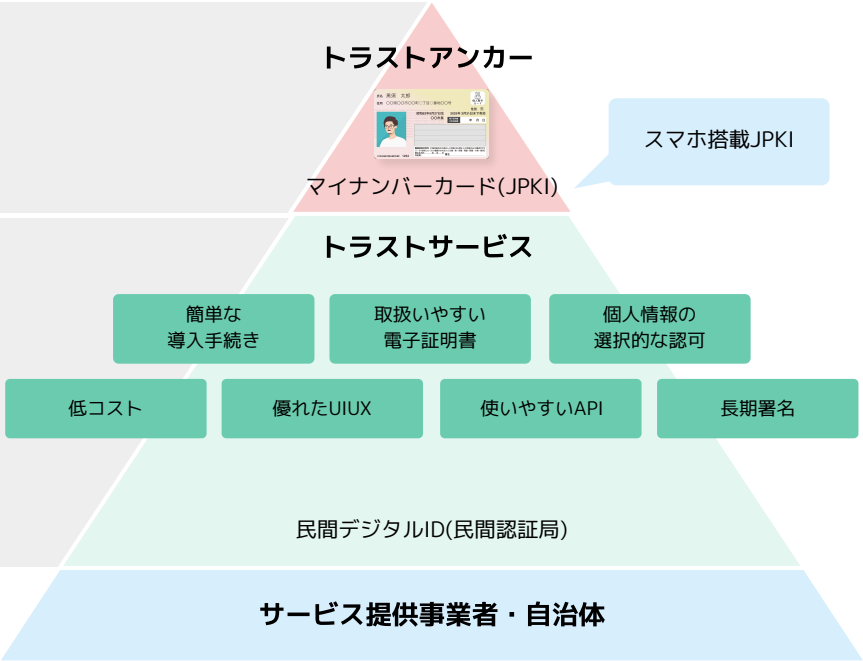
- 身元確認(IAL)については、（課題はあるものの）主務大臣による認定認証によって法的な認定を得ることができるが、当人認証(AAL)や署名プロセスについてはそもそも法的に認定する制度がない。
  →認定認証のスコープ内に含めてゆくのか、別の制度を整備してゆくのか？
- 「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」においても、公的個人認証や署名プロセスについてはあまり考慮されておらず、さらなる整理と議論が必要なのではないか。
  →公的個人認証法のみならず、電子署名法も抜本的な見直しが必要なのではないか？
- 民間取引における本人確認についても、改正犯罪収益移転防止法、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。

トラストアンカー(JPKI)とトラストサービスの役割

デジタルIDと言っても、そこに求められているニーズは多岐にわたっている。国民に広く一般に電子証明書の利活用を推進するためには、**スマートフォンに搭載することがゴールではなく、サービス事業者の現実的なニーズに対して柔軟なソリューションを提供することが不可欠である。**
デジタルIDには、信頼性を提供するという「トラストアンカー」としての役割だけでなく、それを活用するための「トラストサービス」としての役割が求められる。

トラストアンカーには極めて高い信頼性が求められる。

「トラストサービス」には、サービス事業者や、その先の利用者に対してきめ細かなサービスを提供することが求められる。
革新性の高いサービスで新たな市場を切り開き、多様なニーズに対して柔軟に選択肢を提供するのは公的機関が得意とする分野ではなく、むしろ様々な民間プレーヤーの活躍が期待される分野である。

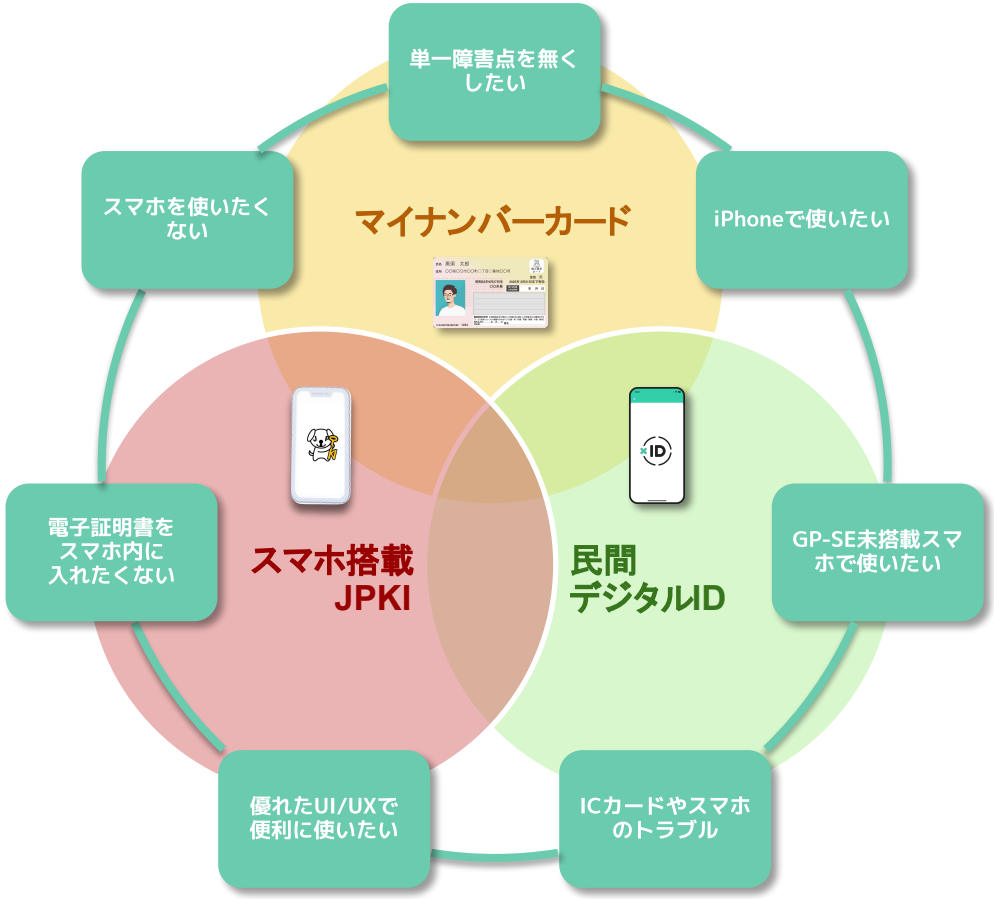


誰一人取り残さないデジタル社会の実現のために

デジタルIDを行政手続きや民間サービスの基本インフラとして整備してゆくにあたり、一つのIDで社会の様々なニーズをカバーするのは困難である。

また、すべてのサービスが唯一のデジタルIDに依拠していると、そこが単一障害点となり障害発生時の影響が極大化する懸念がある。

諸外国では官民がそれぞれ異なるデジタルIDを運営することで国民に複数の選択肢を提供するだけでなく、様々な民間サービスと連携することで新産業の創出が進められている。



現行のスキームに関する課題

トラストアンカーを提供する政府にご検討いただきたいこと

サービス事業者・開発者にとって使いやすいトラストサービスの実現のための官民連携
→ 利便性の高い民間サービスが増えなければ、行政サービスだけでは日常的な”便利”を享受できない。
JPKIがスマホ搭載されただけでは、国民にとって利便性向上とは言えない。

証明書のOTA更新
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る。
→今回のスマホ搭載JPKI検討で、カード用JPKIでオンライン身元確認し証明書発行が実現すれば、実現性が高まる。

署名用電子証明書に含まれる個人情報の再検討
現在基本4情報の全てが記録されている。
→事業者からすると取扱いにくい。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)

トラストサービスを提供する民間事業者として推進していくこと

開発者にとって使いやすいAPIの提供や技術支援、ビジネスエコシステムの構築

利便性の高い民間サービスを増やすことは、本来民間企業の役割である。しかし、マイナンバーカードを活用した利便性の高いサービスを民間企業が真剣に考えてきたとは決して言える状況ではない。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と考えています。

官民連携によりJPKIにおける単一障害点をカバー

欧州においても、政府発行のIDのみならず、民間事業者によるデジタルIDが広く用いられている実例があり、国民に選択肢を提供することや単一障害点の回避という両面で民間デジタルIDが重要な役割を果たしている。我が国においても、今後はマイナポータルやeTaxに限らず、保険証や運転免許証などの行政手続きにマイナンバーカードの利活用が広がる中で、xIDも民間デジタルID事業者としてこれらの手続きに連携できるよう、実証や検証を重ねてゆきたい。