資料2

第1回検討会における指摘事項

令和2年12月4日

総務省　情報流通行政局　デジタル企業行動室

頂いた指摘事項への対応について

「カード機能のスマホへの搭載」に関する指摘事項【p.2】

- システム構成と初期発行フロー
- スマホ特有のライフサイクルへの対応
- 生体認証の活用
- マイナンバーカードの他の機能

次期通常国会における法案提出に向けて、
年内に優先的に検討

「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」に関する指摘事項【p.3】

- 検討の進め方
- 保証レベルと利活用可能な範囲
- 現行スキームに関する課題
- その他

左記の検討状況を踏まえつつ、
主として年明け以降に検討

「カード機能のスマホへの搭載」に関する指摘事項

◆システム構成と初期発行フロー

① マイナンバーカードとスマホでは所有者・チップの管理者が異なることを踏まえ、スマホに搭載する電子証明書とマイナンバーカードの電子証明書は区別して扱うべき。
② トラブルを防止するため、署名用電子証明書は推定効を有する重要な電子証明書であることを広く周知すべき。
③ 「FeliCa-SE」は、正確には「FeliCaアプレットを搭載可能なGlobalPlatform準拠のSE」であり、従来のFeliCaチップと誤解されないよう呼称を工夫すべき。
④ SEI-TSMはフェリカネットワークスが担当することが想定されているが、同社しか提供できないと誤解されないよう、他社も参入できる余地があることを明確にすべき。
⑤ メーカーブランドで売られているSIMフリーのスマホについて「FeliCa-SEチップ」はどの程度搭載されているのか。
⑥ キャリア端末と異なり、SIMフリー端末においては、国際的に広く採用されていない規格のチップは国内市場においても搭載が広がりにくいと考えている。キャリア端末についても、国際標準に準拠しないものをガラパゴス的に国内でのみ販売される端末に搭載する努力をキャリアが続けなければ供給が止まってしまうことになり、サービスとして継続可能か懸念。将来に対して不確定要素になり得ることは可能な限り排除した検討を進めていくべき。
⑦ 「FeliCa-SEチップ」を搭載したスマホ端末はEUのeIDAS規則の適格電子署名生成装置（QSCD）に該当するか確認したい。
⑧ カードをかざすというUXが今後も本命なのか、リモート署名のようにクラウド上に秘密鍵を暗号化した状態で置き、スマホ側でそれを解く鍵を持つという手法も検討される可能性はあるのかを確認したい。
⑨ iPhoneへの対応がされるのかどうかは、民間事業者がコストをかけてサービスを開発するか判断する上で重要なポイント。

◆スマホ特有のライフサイクルへの対応

① 多くのユーザーはスマホを最初に設定したときのことを機種変更の時には覚えていない。また、モバイルFeliCaサービスやメッセージングアプリの機種変更時に、旧端末で必要な操作を行わなかったため機種変更がうまくできないというケースも多い。より多くの方に広く便利に使ってもらうためには、ユーザーが必ず旧端末を操作して失効させる形ではなく、何か適切な手続をすれば失効できるようにする等、セキュリティを確保した上でユーザー利便性を実現する必要がある。
② 既存の交通系ICカードやクレジットカード等の場合、機種変更の際に手続が煩雑なものが多い。スマホに搭載した電子証明書については、機種変更の際にセキュリティを担保しつつ簡略化されたフローを検討し、デファクトスタンダードになるような手法を目指してほしい。
③ 紛失した場合にはスマホを持っていない状況になるので、マイナンバーカードで必要な手続をできるようにすべき。他方、端末譲渡時の失効手続についてマイナンバーカードの読み取りを必要とすると面倒なため必要な手続が行われない可能性があることから、スマホに搭載した電子証明書だけを利用して失効できるようにすべき。また、機種変更の際の新端末での電子証明書発行時だけでなく、初期発行の場合にも、二重発行が行われないよう未発行又は失効済みであることを確認するプロセスが必要。
④ スマホに搭載した電子証明書を利用する際には、マイナンバーカードと同じ使い勝手を再現するのではなく、例えばOSのAPIと密接に連携して、マイナポータルアプリとブラウザの間を行ったり来たりしなくてすむようにする等、スマホならではの使い勝手の良いUXを実現していく必要がある。
⑤ 情報リテラシーの低い高齢者の方に対しては、機種変更時の手続が難しいUXとなる場合、サービス提供者においては、例えば確定申告期には機種変更しないようにといった誘導をすることが必要になってしまう。民間のリソースも活用して可能な限りユーザーテストを実施し、ちゃんとユーザーに理解されるUXを担保してほしい。

◆生体認証の活用

① 生体認証をスマホで広く利用できる環境となっており、マイナンバーカードの機能をスマホに搭載して国民に便利に安心して使っていただく上で、FIDOアライアンスの取組を生かすことができると考えている。
② EUでは最も高いレベルのeIDについて生体認証を使ったログインを認めている例はないと認識。どのようなレベルであれば生体認証を活用可能か整理すべき。
③ 最も高いプライバシー情報である生体情報を安全に守りながら生体認証を活用する方式としてFIDO認証が広く導入されてきており、EUの決済サービス指令（PSD2）でも有力な方法とされている。生体認証の安全性については今後の検討会において議論したい。

◆マイナンバーカードの他の機能

① マイナンバーカードの券面事項入力補助機能や健康保険証利用など様々な資格確認を実現していく上で必要な機能についてもスマホに搭載していくことが重要。

「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」に関する指摘事項

◆検討の進め方

① 公的個人認証サービスと紐付けられた民間IDの利活用に関する課題を確認し、その課題に対してどんなタイムラインで実行していくのか明らかにすべき。
② スマホの耐タンパ性が確保されたチップに電子証明書を搭載するのが一番の本命とは思うが、特定のチップを搭載したスマホだけを行政サービスの対象とするということは厳しいと思う。それ以外の機種にどのように対応していくか、例えばリモート署名とFIDOの組合せなど民間ID対応していくのか、国としてやるべきことがあるのか議論すべき。
③ 民間IDについて、当人認証についてはFIDO認証の利用が進んできているが、その際に課題となるのはIDに紐付いた本人の身元確認の部分であり、マイナンバーカードの公的個人認証サービスを活用した本人確認が今後役に立つと期待。
④ 民間IDの利活用のうち取り組みやすいものからサービスを展開するなど、サービスモデルの戦略も並行して検討すべき。
⑤ 公的個人認証サービスの民間利用が広がらない背景として、例えば総務大臣認定を受けることやプラットフォーム事業者と連携することの手間等が一因にある。民間企業の観点も考慮して、マイナンバーカードの機能をスマホに搭載することでどのような行政・民間サービスのユースケースにおいて便利になるのかを議論すべき。

◆保証レベルと利活用可能な範囲

① NIST SP 800-63-3に規定されている保証レベル（IAL、AAL、FAL）の考え方、eIDAS規則に規定されているeIDや適格電子署名・先進電子署名、適格電子署名生成装置の考え方等を踏まえ、ポリシーマッピングとして目指すべき方向性を整理すべき。
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、マインバーカードの公的個人認証サービスと紐付いた民間IDがどの保証レベルに該当するか整理するとともに、例えば、保証レベル3が必要なものは確定申告や在外邦人のインターネット投票など頻度の低いものに限り、ほとんどの電子申請は保証レベル2で対応可能とするなど、保証レベルとユースケースとを突き合わせて実現したいことを整理すべき。
③ EUのeIDのレベル分けやNIST SP 800-63-3等を参考に、我が国のeIDや電子署名の安全性のレベルを定義し、どのようなレベルの民間IDであれば受け入れられるのかを明確にすべき。例えばマイナポータルへのログインには最高レベルの認証が必要であれば、秘密鍵がソフトウェアで保護されているものは使えないといった制御が必要となる。
④ マイナポータルについても、マイナポータルであれば最高の保証レベルが必要ということではなく、それが電子申請か、自己情報取得APIへのアクセスか、資格確認なのか、ユースケースに応じてそれぞれのリスクレベルを判断し、そのリスクに応じた保証レベルをルールに従って検討していくことが必要。

◆現行スキームに関する課題

① （総務大臣の認定を受けて公的個人認証サービスを利用する）プラットフォーム事業者はパブリッククラウドの利用が認められていないためサーバ構築等に多大なコストを要しており、それがプラットフォーム事業者を活用して実際に公的個人認証サービスを利用する民間事業者のコストに跳ね返ってきている。
② 署名用電子証明書で署名した場合、署名用電子証明書のシリアルナンバーが文書データに残るが、シリアルナンバーはプラットフォーム事業者以外は管理が認められていないため、署名を付した利用者自身が文書データを保管できないという使いにくい状況にあり、今のルールのままでは民間での利用が広がっていかないと懸念。
③ 電子契約書への電子署名は電子証明書の有効期限終了後も検証する必要が生ずる。そのためには、証明書失効情報確認に用いるCRLやOCSPを電子署名や電子証明書と併せて保存したり、契約相手方に提供したりする必要があるが、現行の公的個人認証法では不可能。CRLやOCSPを自由に流通させられるようにしないと、公的個人認証サービスの民間利用が広がらず、マイナンバーカードの普及やスマホへの搭載も進まないのではないか。
④ 民間がJPKIを利用しにくい要因として費用の問題がある。CRL、OCSPとも署名の場合は1回20円、利用者証明は1回2円の費用が掛かるが、諸外国においてはOCSPは課金しているがCRLは無料開放しているところも多い。費用面の考え方について検討が必要。
⑤ 元々20円、2円のところ、プラットフォーム事業者を介して利用する場合、1件当たり数百円もの費用が掛かるのが実情であり、J-LISのみならず公的個人認証サービスのエコシステム全体の問題として考えていく必要がある。
⑥ リモート署名で認定認証業務の電子証明書を使うことを認めるためには電子署名法施行規則の改正が必要。

◆その他

① ISO/IEC 18013-5に準拠したモバイル運転免許証など、国際的な相互運用性が求められる身分証のデジタル化をどのように考えていくか。

指摘事項に対する考え方

「カード機能のスマホへの搭載」に関する指摘事項
に対する考え方

「システム構成と初期発行フロー」に関する指摘事項に対する考え方

#	指摘事項	考え方
①	マイナンバーカードとスマホでは所有者・チップの管理者が異なることを踏まえ、スマホに搭載する電子証明書とマイナンバーカードの電子証明書は区別して扱うべき。	スマホに搭載する電子証明書とマイナンバーカードの電子証明書は法制度上区別して規定するとともに、運用管理上も固有のシリアル番号等により識別可能とする考え。
②	トラブルを防止するため、署名用電子証明書は推定効を有する重要な電子証明書であることを広く周知すべき。	広く周知するとともに、JPKIアプリを起動した際にユーザに注意喚起する等、適切な周知及び注意喚起の方法を引き続き検討してまいりたい。
③	「FeliCa-SE」は、正確には「FeliCaアプレットを搭載可能なGlobalPlatform準拠のSE」であり、従来のFeliCaチップと誤解されないよう呼称を工夫すべき。	ご指摘を踏まえ、「Android-SE（GlobalPlatform準拠）」に改める。 なお、対象となるチップは、GP準拠であって、かつ、JPKIとして必要な機能、性能、セキュリティ、互換性等が確保されたものであり、具体的要件について技術的条件として規定する考え。
④	SEI-TSMはフェリカネットワークスが担当することが想定されているが、同社しか提供できないと誤解されないよう他社も参入できる余地がある旨明確にすべき。	SEI-TSMに求められる具体的要件について明らかにする等により、新規参入の可能性について明確化を図る考え。
⑤	メーカーブランドで売られているSIMフリーのスマホについて「FeliCa-SEチップ」はどの程度搭載されているのか。	2020年度下期発売のSIMフリーのAndroid端末のうち、GPに準拠したFeliCa対応端末の割合は機種ベースで約半数と見込まれる。 なお、FeliCa対応端末のうちGP準拠の割合は、2019年度下期の約22%から約90%へと拡大しており、今後更に普及が進むと見込まれている。
⑥	キャリア端末とは異なり、SIMフリー端末においては、国際的に広く採用されていない規格のチップは国内市場においても搭載が広がりにくいと考えている。キャリア端末についても、国際標準に準拠しないものをガラパゴス的に国内でのみ販売される端末に搭載する努力をキャリアが続けなければ供給が止まってしまうことになり、サービスとして継続可能か懸念。将来に対して不確定要素になり得ることは可能な限り排除した検討を進めていくべき。	SIMカード、サブSIM、eSIM、TEE等、これまで様々な格納媒体の活用可能性を検討してきたが、現時点で可能性があるのはAndroid-SE（GP準拠）のみ。上記の通り、キャリア端末のみならずSIMフリー端末についてもAndroid-SE（GP準拠）の普及が見込まれている。 なお、非搭載端末への対応の観点からも、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検討する考え。
⑦	「FeliCa-SEチップ」を搭載したスマホ端末はEUのeIDAS規則の適格電子署名生成装置（QSCD）に該当するか確認したい。	Android-SE（GP準拠）は、OS・HWとも、QSCDが参照するProtection Profile (PP)と同一のPPに準拠したCC認証等を取得しており、QSCDに該当し得るチップと考えられる。【参考資料1】
⑧	カードをかざすというUXが今後も本命なのか、リモート署名のようにクラウド上に秘密鍵を暗号化した状態で置き、スマホ側でそれを解く鍵を持つという手法も検討される可能性はあるのかを確認したい。	公的個人認証機能をスマホに搭載することによりカードをかざす手間を不要にする考え。カードと同等の保証レベルを実現すべく、耐タンパ性を有するSEに秘密鍵を搭載することを検討。リモート署名は民間IDの活用において検討。
⑨	iPhoneへの対応がされるのかどうかは、民間事業者がコストをかけてサービスを開発するか判断する上で重要なポイント。	iPhoneへの搭載の実現に向けて引き続き働きかけを行ってまいりたい。

「スマホ特有のライフサイクルへの対応」に関する指摘事項への考え方

#	指摘事項	考え方
①	多くのユーザーはスマホを最初に設定したときのことを機種変更の時には覚えていない。また、モバイルFeliCaサービスやメッセージングアプリの機種変更時に、旧端末で必要な操作を行わなかったため機種変更がうまくできないというケースも多い。より多くの方に広く便利に使ってもらうためには、ユーザーが必ず旧端末を操作して失効させる形ではなく、何か適切な手続をすれば失効できるようにする等、セキュリティを確保した上でユーザー利便性を実現する必要がある。	機種変更においては、ユーザーは新端末において所定の手続を行うのみで（旧端末での手続を必要とせず）対応可能とすべくフローを見直し（本日の議事(5)において説明）。 他方、旧端末に搭載されている秘密鍵や電子証明書が悪用されないよう、適切に削除されることが望まれることから、 ・新端末での手続により電子証明書が失効された場合には、旧端末が起動した際にSE内の秘密鍵や電子証明書を削除するプロセスを設定 ・旧端末での操作により、電子証明書を失効させるとともに、SE内の秘密鍵や電子証明書を削除可能 ・旧端末の初期化により、SE内の秘密鍵や電子証明書を削除可能 とする等の措置を講じるとともに、利用者に対して適切に失効手続や削除を行うことを勧奨する方法について検討する考え。
②	既存の交通系ICカードやクレジットカード等の場合、機種変更の際に手続が煩雑なものが多い。スマホに搭載した電子証明書については、機種変更の際にセキュリティを担保しつつ簡略化されたフローを検討し、デファクトスタンダードになるような手法を目指してほしい。	
③	紛失した場合にはスマホを持っていない状況になるので、マイナンバーカードで必要な手続をできるようにすべき。他方、端末譲渡時の失効手続についてマイナンバーカードの読み取りを必要とすると面倒なため必要な手続が行われない可能性があることから、スマホに搭載した電子証明書だけを利用して失効できるようにすべき。また、機種変更の際の新端末での電子証明書発行時だけでなく、初期発行の場合にも、二重発行が行われないよう未発行又は失効済みであることを確認するプロセスが必要。	ご指摘のとおり、 ・スマホ紛失時にはマイナンバーカードの署名用電子証明書を用いて必要な手続をオンラインで実現可能とする ・端末譲渡時や機種変更の際の失効手続については、スマホに署名用電子証明書も搭載する場合にはスマホのみで実現可能とする ・初期発行時にも未発行又は失効済みであることを確認するプロセスを設定する考え。
④	スマホに搭載した電子証明書を利用する際には、マイナンバーカードと同じ使い勝手を再現するのではなく、例えばOSのAPIと密接に連携して、マイナポータルアプリとブラウザの間を行ったり来たりしなくてすむようにする等、スマホならではの使い勝手の良いUXを実現していく必要がある。	JPKIアプリからAndroid-SE（GP準拠）へのアクセスは、Android Open Mobile APIを利用する考え。ご指摘を踏まえ、実証等を通じて使い勝手の良いUXの実現に取り組んでまいりたい。
⑤	情報リテラシーの低い高齢者の方に対しては、機種変更時の手続が難しいUXとなる場合、サービス提供者においては、例えば確定申告期には機種変更しないようにといった誘導をすることが必要になってしまう。民間のリソースも活用して可能な限りユーザーテストを実施し、ちゃんとユーザーに理解されるUXを担保してほしい。	ご指摘を踏まえ、使い勝手の良いUXの実現に向けて、実証等において民間のご協力をいただき、ユーザーテストの実施を検討してまいりたい。

「生体認証の活用」等に関する指摘事項に対する考え方

＜生体認証の活用＞

#	質問	対応案
①	生体認証をスマホで広く利用できる環境となっており、マイナンバーカードの機能をスマホに搭載して国民に便利に安心して使っていただく上で、FIDOアライアンスの取組を生かすことができると考えている。	本日の議事(8)において、利用者の利便性向上の観点から、安全性を確保しつつ生体認証を活用する方向性についてご議論いただきたい。
②	EUでは最も高いレベルのeIDについて生体認証を使ったログインを認めている例はないと認識。どのようなレベルであれば生体認証を活用可能か整理すべき。	
③	最も高いプライバシー情報である生体情報を安全に守りながら生体認証を活用する方式としてFIDO認証が広く導入されてきており、EUの決済サービス指令（PSD2）でも有力な方法とされている。生体認証の安全性については今後の検討会において議論したい。	

＜マイナンバーカードの他の機能＞

#	質問	対応案
①	マイナンバーカードの券面事項入力補助機能や健康保険証利用など様々な資格確認を実現していく上で必要な機能についてもスマホに搭載していくことが重要。	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における議論の方向性も踏まえ、今後検討。