資料4

スマートフォン用電子証明書の保証レベル

令和３年11月24日

総務省　情報流通行政局　情報流通高度化推進室

マイナンバーカード用・スマートフォン用電子証明書の本人確認保証レベル

○ マイナンバーカードの機能のスマートフォン搭載による利便性向上を最大化するためには、マイナンバーカード用電子証明書で利用可能な行政手続の全てをスマートフォン用電子証明書でも利用出来ることが必要。
○ これを実現するためには、身元確認・当人認証に係る保証レベルがマイナンバーカードと同等であることが必須。

■身元確認・当人認証保証レベル（IAL・AAL）の定義

表 2-1 身元確認保証レベル

身元確認保証レベル	レベルの定義
レベル１（IAL1）	身元識別情報が確認される必要がなく、身元確認の信用度がほとんどない。身元識別情報は、自己表明若しくは自己表明相当である。
レベル２（IAL2）	身元識別情報が遠隔又は対面で確認され、身元確認の信用度が相当程度ある。
レベル３（IAL3）	身元識別情報が特定された担当者の対面で確認され、身元確認の信用度が非常に高い。

出典）「デジタルアイデンティティガイドライン（SP800-63-3）」より作成

表 2-2 当人認証保証レベル

当人認証保証レベル	レベルの定義
レベル１（AAL1）	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、単要素若しくは複数要素を使うことにより、当人認証の信用度がある程度ある。
レベル２（AAL2）	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、複数要素を使うことにより、当人認証の信用度が相当程度ある。
レベル３（AAL3）	認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、耐タンパ性を有するハードウェアを含む複数要素を使うことにより、当人認証の信用度が非常に高い。

出典）「デジタルアイデンティティガイドライン（SP800-63-3）」より作成

※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）より抜粋

■マイナンバーカード用電子証明書とスマートフォン用電子証明書の保証レベルの比較

保証レベル	マイナンバーカード用電子証明書	スマートフォン用電子証明書
IAL（身元確認） レベル３の要件 【対面での身元確認】	レベル３ ○自治体窓口等での対面による交付等	レベル？ ○対面交付されたMNCによる電子署名に基づき発行
AAL（当人認証） レベル３の要件 【耐タンパ性が確保されたハードウェアを含む複数の認証要素による認証】	レベル３ ○所持（耐タンパ性を有するマイナンバーカードのICチップ） ○知識（パスワード）	レベル３ ○所持（スマホに搭載された耐タンパ性を有するGP-SE） ○知識（パスワード）or 生体（指紋・顔）

○マイナンバーカードを用いたスマートフォン内ローカル環境（GP-SE内のアプレット）での鍵ペア生成。
○公開鍵をJPKI側に登録し、電子証明書を発行。
⇒一連のスキームにおいて、マイナンバーカード交付時の本人確認の強度が引き継がれており、特にスマホとJPKIとの間に第三者が関与する余地がない。

○耐タンパ性を保証するため、マイナンバーカードと同様にCC認証の取得が必須。
⇒CC認証取得を前提とすれば、耐タンパ性ハードウェアを含む複数要素による認証はクリアし、レベル３となるか。

■スマートフォン用電子証明書の保証レベルの考え方

○マイナンバーカード交付時の本人確認の強度が引き継がれていること
☞前提として、マイナンバーカード用電子証明書のパスワードは利用者本人の適切な管理のもとで第三者が知り得ることがない。
スマートフォン用電子証明書は、対面による厳格な身元確認の上で交付されるマイナンバーカードを用いてのみ発行され、下記の通り発行プロセスにおいて第三者の関与の余地がないことからも、**マイナンバーカード交付時の本人確認の強度が引き継がれている。**

○スマートフォンとJPKIシステムとの間に第三者が関与する余地がないこと
☞スマートフォン用電子証明書発行時等における端末内のGP-SEとTSMとの間の通信はGlobalPlatformによって定められたセキュアチャネルプロトコル（SCP03）を採用し、通信経路途中においてデータのスキミングによる解読や改ざんなどを困難とするほか、TSMとJPKIシステムとの間は専用線により高セキュリティな秘匿通信を行う。
システムの運用上も、SEI-TSM運用者・SP-TSM運用者・JPKIシステム運用者のみが介在し、**第三者の関与は排除されている。**

○CC認証の取得
☞GP-SEプラットフォーム（HW+OS）に加え、搭載アプレットも含めてCC認証（EAL4+, AVA_VAN.5）を取得することで、**マイナンバーカードと同等の耐タンパ性**が保証される。

（参考）eIDAS規則における派生クレデンシャルの保証レベルの考え方

eIDAS規則では、欧州委員会に通知された電子識別スキームに基づいて発行された電子識別手段の保証レベルについて「low」、「substantial」、「high」のいずれかを指定する必要がある旨規定している。（※eIDAS規則 (EU) No 910/2014 第8条及びCommission Implementing Regulation (EU) 2015/1502 Annex参照）

マイナンバーカード用電子証明書は、「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」や「NIST SP 800-63-3」に照らして保証レベルをIAL3/AAL3と整理できるものであるが、eIDAS規則に沿って整理する場合にも、下表のように最高レベルの「high」を適用可能と解釈することができる。

【eIDAS規則の保証レベルの要件（一例）】

保証レベル	身元確認及び検証（IALに相当）※1	当人認証（AALに相当）※2
Low	身元証明用のエビデンスを所有しているが、エビデンスの真正性・有効性の確認の必要がなく、信頼できる情報源により申請者本人と主張された身元が同一人物であると想定することができる。	最低でも1つの認証要素を利用。
Substantial	身元証明用のエビデンスによって身元確認が行われており、当該エビデンスは真正性が確認されているか、信頼できる情報源によって有効性及び実際の人物との関連性が確認されている。また、紛失・盗難・一時停止・失効・期限切れ等のリスクを考慮して、本人の身元と主張された身元が異なるリスクを最小化する手段が講じられている。	最低でも異なる2つの認証要素（少なくとも1つは知識又は生体）を利用。
High	Substantialの要件に加え、 写真又は生体認証のエビデンスを所有しており、当該エビデンスは信頼できる情報源に基づいて有効性が確認されている。また、1つ以上の身体的特徴を信頼できる情報源と比較することで身元確認が行われる。（対面発行の要件記述なし）	Substantialの要件に加え、 暗号鍵の耐タンパハードウェアへの格納等により複製や改ざんに対する高い攻撃耐性を持ち、かつ、強力な認証によって保護されている。

Commission Implementing Regulation (EU) 2015/1502 Annex 参照
※1：2.1.2. Identity proofing and verification (natural person) 、※2：2.2.1. Electronic identification means characteristics and design

■派生クレデンシャルの保証レベルについて

Commission Implementing Regulation(EU) 2015/1502 Annex※3及びそのガイダンスでは、身元確認及び検証に関する保証レベル（IALに相当）が「high」の電子識別手段に基づいて発行される電子識別手段（派生クレデンシャル）については身元証明や検証プロセスを繰り返す必要なく同等の保証レベルが維持されるとされていることを踏まえると、**マイナンバーカード用電子証明書から派生したスマートフォン用電子証明書は、身元確認の保証レベルにおいてマイナンバーカード用と同等レベル（High）と整理できると考えられる**。

※3 Commission Implementing Regulation **(EU) 2015/1502 Annex 2.1.2. Identity proofing and verification (natural person) Assurance Level HIGH 参照**

(c)Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.

仮訳

(c)電子識別手段が、**保証レベルが「high」の有効な通知済み電子識別手段に基づいて発行されている場合、本人識別データの変更によるリスクを考慮すると、身元証明及び検証プロセスを繰り返す必要はない。**根拠となる電子識別手段が通知されていない場合は、規則（EC）No 765/2008のArticle 2(13)に記載されている適合性評価機関又は同等の機関によって保証レベル「high」であることが確認されなければならず、通知済み電子識別手段の前回の発行手続の結果が有効であることを示すための措置が取られる。