マイナンバーカードの機能の
スマートフォン搭載等について

令和3年11月9日

デジタル庁

「カード機能のスマホへの搭載」の基本方針

基 本 方 針

1．スマホひとつで、様々な手続やサービスが利用可能

2．オンラインで簡単にスマホに搭載

3．スマホならではの使いやすいUX

4．安全・安心に利用できる高いセキュリティ

5．グローバルスタンダードに対応

１．スマホひとつで、様々な手続やサービスが利用可能

基本方針１

- 高いセキュリティでなりすましや改ざんを防ぎ、オンラインによる高度な本人確認を可能とするマイナンバーカードの機能（公的個人認証サービス）をスマホに搭載することにより、毎回カードをかざすことなく、スマホのみで手続等を行うことを可能とし、利用者の利便性向上を図る。
- その際、マイナポータルの機能拡充や各種国家資格等のデジタル化など、マイナンバーカードの利用シーン拡大に向けた取組や民間における利用ニーズにも対応できるようにする。

具体的方針

- マイナンバーカードの公的個人認証サービスの2種類の電子証明書（署名用電子証明書、利用者証明用電子証明書）のいずれもスマホに搭載可能とし、マイナポータルへのログイン等における本人認証のみならず、様々なオンライン申請等もスマホから簡単にできるようにする。
- オンラインによる利用に加え、コンビニ交付など、NFCを利用したカードリーダーでの読み取りの可否について検証を進める。
- 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ID）の利活用の促進に向けた検討を進め、その課題と対応を整理する。
- マイナンバーカードの持つ他の機能（券面入力補助機能等）についても、今後関係する国際標準規格との相互運用性の確保など様々な課題を整理した上で、スマホへの搭載方法について検討する。

ユースケースの将来像 ※検討中のものを含む

【想定ユースケース】

オンライン利用

生体認証を使って
便利で安心

カードを毎回
読み取らないから
簡単・スマート

マイナポータル

- 自己情報の確認
  - ・お薬・健診情報
  - ・母子健康手帳　等
- オンライン行政手続
  - ・子育て支援
  - ・年末調整・確定申告　等

民間サービス

- ・銀行、証券口座開設
- ・住宅ローン契約
- ・携帯電話申込　等

資格確認

- ・ハローワーク受付
- ・障害者割引適用　等

※健康保険証としての
利用についても検討

カードリーダーの
読取にも対応

カードリーダー読み取り

資格確認

- ・コンビニ交付
- ・公共施設利用　等

2．オンラインで簡単にスマホに搭載

基本方針２

- マイナンバーカードの公的個人認証サービスの電子証明書の発行（再発行）を受けるには、現在は自治体の窓口に赴いて手続を行う必要があるが、スマホに搭載する電子証明書については、マイナンバーカードを保有していることを前提として、窓口に赴くことなく、オンラインで簡単に発行を受けることができるようにする。
- カードと異なり、スマホに搭載する場合には、機種変更や譲渡（転売）といったスマホ特有のライフサイクルにも配慮することが必要。機種変更等の際にも、オンラインで簡単かつ安全に新たなスマホに搭載できるようにする。

具体的方針

- マイナンバーカードをスマホで読み取り、カード用署名用電子証明書に基づく署名を用いてスマホから申請を行うことにより、オンラインでスマホ用電子証明書の発行を受けられるようにする（自治体の窓口で対面による本人確認を行い交付されたマイナンバーカードを保有していることが前提）。スマホ用電子証明書は1人につき各種1枚ずつ発行できるものとする。
- スマホが紛失・故障等した場合にも、新しいスマホに速やかに新たなスマホ用電子証明書を搭載できるように、新規発行と同様、カード用署名用電子証明書を用いてオンラインで再発行を受けられるようにする。
- 機種変更に際しては、本人からの失効申請を原則とした上で、旧端末での操作を必須とせず、新端末の操作のみでも必要な手続を完了できるようにし、既存の同種のアプリと比べても簡単なUXを実現する。
- スマホ用電子証明書を失効させる場合には、カードを要さず、スマホのみで必要な手続ができるようにする。
- スマホ用電子証明書のPIN/パスワードの設定もオンラインでできるようにする。

３．スマホならではの使いやすいUX

基本方針３

- カードではなく、スマホに搭載することの強みを最大限に活かす。これまで積み上げられてきたスマホのエコシステム、既に実装されている機能を最大限活用して、利用者の声を聴きつつ、使いやすくわかりやすいUXを実現する。
- マイナンバーカードの電子証明書の利用に際してPIN/パスワードの入力が利用者の負担となっている状況を踏まえ、十分なセキュリティを確保しつつ、スマホの生体認証を活用したPIN/パスワードに依存しない認証の仕組みの導入を検討する。

具体的方針

- 実証段階において民間の協力を得てユーザテストを実施するなど、利用者の声を聴きつつ、多くの画面遷移や複雑な操作を伴わない、利用者にとってわかりやすい操作フローを実現する。
- スマホのOSに実装されているAPIを活用して、正当なアプリのみがアクセス可能とするとともに、アプリ間の画面遷移がないストレスフリーなUXの実現を目指す。
- 利用者にとってスマホに搭載されている生体認証装置の利用が一般的になっている状況を踏まえ、公的個人認証サービスに求められるセキュリティの確保を第一としつつ、生体認証を活用する方策について検討を進める。その際、現在の生体認証の認証レベルも考慮し、利用者証明機能への適用を検討することとし、スマホにおけるオンライン認証で生体認証を使うアプローチとして普及してきた「FIDO認証」の考え方や仕組みも参考に、生体認証機能に求められる要求条件や第三者評価の在り方、認証レベルの考え方、万一の問題等発生時に備えた責任分界点、利用者への十分な案内などの課題について整理・検討し、高いセキュリティを確保しながら使い勝手の良いUXの実現を目指す。

４．安全・安心に利用できる高いセキュリティ

基本方針４

- スマホに搭載する電子証明書についても、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り、また、利用者証明用電子証明書はマイナポータルへのログイン等を可能とする重要な電子証明書であることから、マイナンバーカードの電子証明書と同様、高いセキュリティ水準を確保することが不可欠。
- また、機種変更や譲渡の際に、旧端末のチップ内に電子証明書や秘密鍵が残存したまま第三者に移転すると悪用されてしまう懸念があることから、旧端末の電子証明書や秘密鍵を適切に失効・削除できるようにする。

具体的方針

- 自治体の窓口で厳格な本人確認を行った上で交付されるマイナンバーカードを保有している者を対象として、カード用署名用電子証明書による本人確認に基づきスマホ用電子証明書を発行。
  カード用電子証明書とは識別可能な形で発行されるスマホ用電子証明書は、カード用電子証明書に紐付けて管理され、カード用電子証明書の失効に連動してスマホ用電子証明書も失効する。
- スマホ用電子証明書に紐付く秘密鍵は、スマホ端末内の耐タンパ性を有する安全なチップ（GP-SE）内で生成し、外部に一切出ること無く、チップ内のアプレットに安全に格納する。サーバとスマホ端末内のチップとの通信は、国際標準に準拠したセキュアチャネルプロトコル（SCP03）により安全性を確保する。
- スマホ紛失時等に電子証明書や秘密鍵が旧端末内に残存したまま第三者に移転して悪用されることを防ぐため、以下の方策について技術面や運用面に係る検討を行う。
  - スマホ紛失時等に備え、コールセンターにおいて一時保留を受け付ける
  - 役所に赴くことなくスマホひとつで失効申請を行うことができることとし、機種変更に際し、新端末から旧端末の電子証明書の失効申請をあわせて実施する
  - 失効を受けてリモートで旧端末内の電子証明書や秘密鍵を削除する
  - 適切に削除されない場合も想定し、端末初期化により電子証明書や秘密鍵を削除する
  - 窓口における確認や周知等に関し、携帯キャリアや中古端末取扱事業者と連携する
  - 失効済みの署名用電子証明書に紐付く秘密鍵による電子署名を防止するための技術的措置について検討する

5．グローバルスタンダードに対応

基本方針５

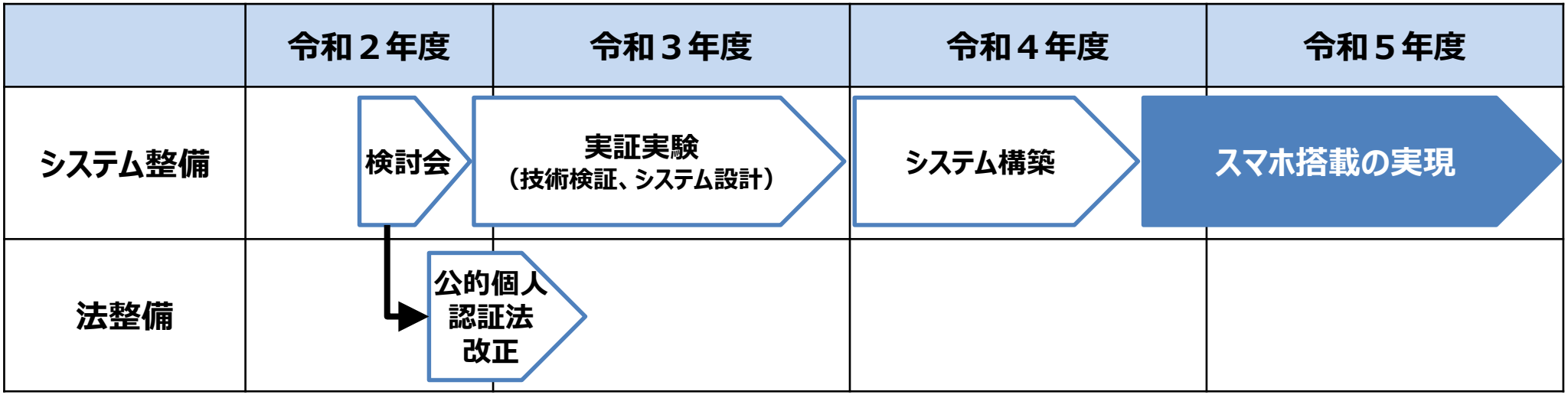
- スマホへの搭載の実現にあたり、国際的にサポートされていないガラパゴスな方式を採用した場合には、結果的に対応可能なスマホの機種が限定され、広く普及が進まないおそれがある。そのため、具体的な実現方式の検討にあたっては、グローバルスタンダードへの対応を図るとともに、現実的な普及可能性を十分考慮する。
- さらに、デジタルIDや電子署名に係る国際的な動向を踏まえ、利用者の利便性向上の観点から不断に見直しを行っていく必要がある。

具体的方針

- 米国NISTのデジタルアイデンティティガイドライン（SP 800-63-3）等における身元確認、当人認証のレベルを参照しつつ、公的個人認証サービスとして十分な信頼性を確保する。
- 国際標準であるGlobalPlatformに準拠した汎用チップであり、今後キャリア端末・SIMフリー端末とを問わず広く搭載が進むことが見込まれる「GP-SE」を電子証明書や秘密鍵の格納媒体として利用する。
- 格納媒体に係る技術的要件については、国際標準であるISO/IEC 15408（CC認証）、欧州eIDAS規則の適格電子署名生成装置（QSCD）に係る基準、米国FIPS 140-2等との整合性を確保する。
- スマートフォンのグローバルなエコシステムにおけるデファクトスタンダード（Android互換性定義ドキュメント（CDD）など）との親和性確保についても十分留意する。
- デジタルID等に係る国際的動向や「GP-SE」の搭載状況、公的個人認証と紐付いた民間IDの普及状況等を踏まえて、リモート署名やエストニアのスマートID等を参考に、「GP-SE」を必要としない方式の必要性も検討する。

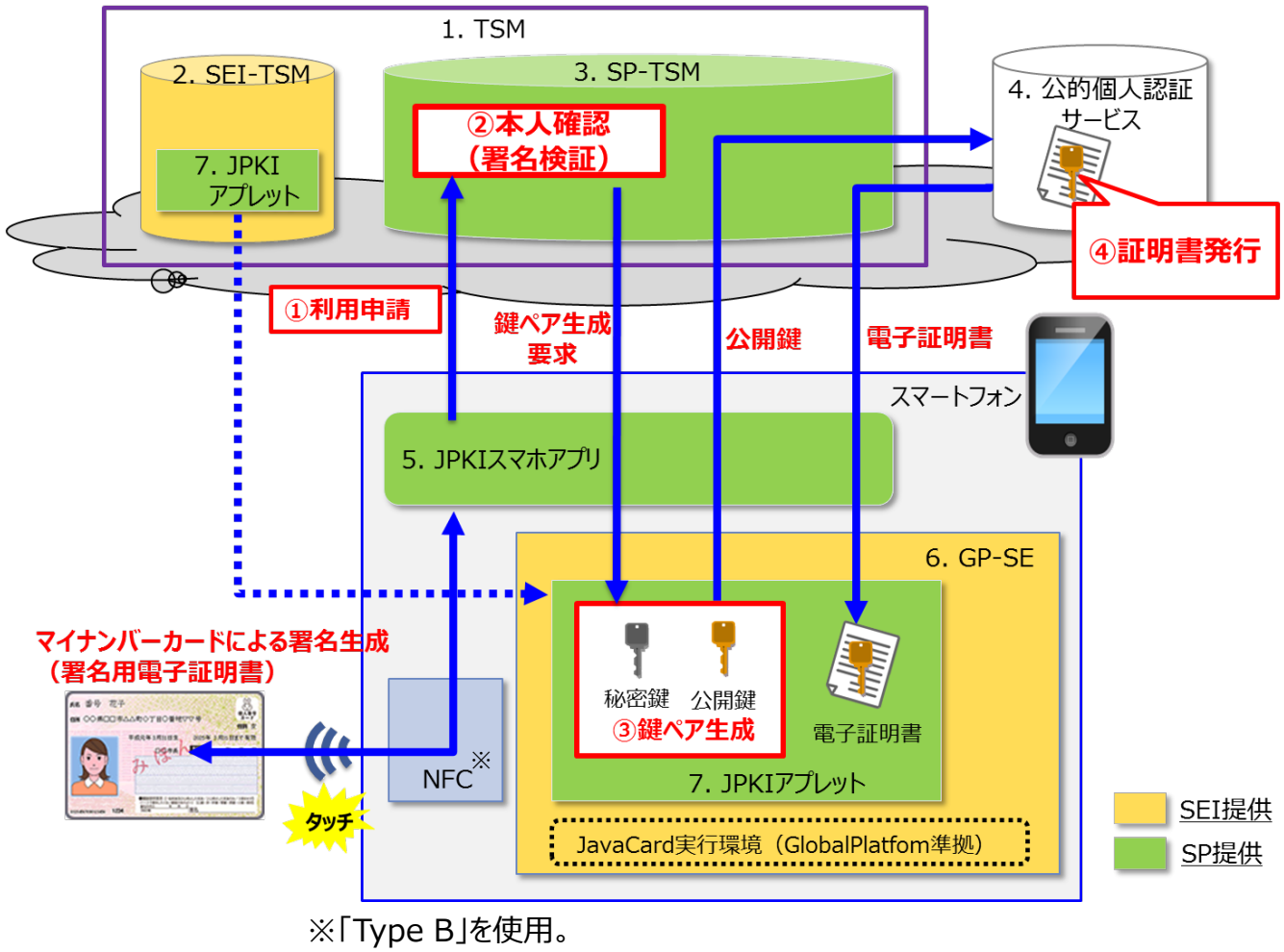
実現に向けたスケジュール

- **令和４年度内にAndroid端末への搭載を目指す。**
- 必要な制度整備を行うため、**次期通常国会に公的個人認証法改正案を提出。**
- **iPhoneについても早期実現を目指す。**



スマホに電子証明書を搭載するためのシステム構成

スマホに電子証明書を搭載するためのシステム構成およびその用語解説



※「Type B」を使用。

（補足）上図ではJPKIスマホアプリは利用者によってGoogle Playからダウンロードされた状態を想定。

サーバ側

1. TSM: Trusted Service Manager
   - SEI-TSMとSP-TSMで構成される。スマートフォン上のSecure Element（SE）へのデータ配信をセキュアに実施する。

2. SEI-TSM
   - SEの発行者（SEI: Secure Element Issuer）が運営するTSM。
   - サービス提供者（SP: Service Provider）のアプレットを預かり、SEにアプレットを格納する役割を担う。

3. SP-TSM
   - SPが運営するTSM。
   - ユーザの利用申請を受け付け、SEのパーソナライズを行う役割を担う。

4. 公的個人認証サービス
   - J-LISが運営する認証サービス。

スマートフォン側

5. JPKIスマホアプリ
   - 利用申請やサービス利用時に使用するAndroidアプリ。
   - Google Playからダウンロードする。利用申請時やサービス利用時に使用する。

6. GP-SE
   - Androidスマートフォンに搭載されるSE。
   - GlobalPlatform仕様に準拠し、Javaアプレットをダウンロードできる。

7. JPKIアプレット
   - JPKI機能を実装するJavaアプレット。