資料3

第２次とりまとめ（案）
～デジタル社会の新たな基盤の構築に向けて～

令和4年3月28日

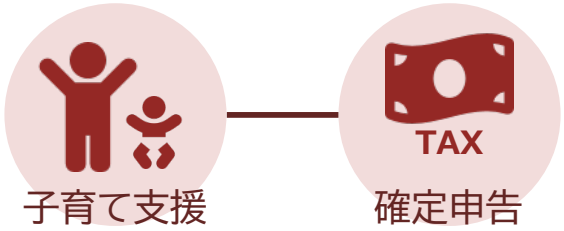
「マイナンバーカード機能のスマートフォン搭載」によって目指す姿

- 公的個人認証サービスの電子証明書の機能をスマートフォンに搭載することによって、スマートフォンひとつで、いつでもどこでもオンライン行政手続等を行うことができる環境の構築を目指す。
- また、スマートフォン搭載による利便性の向上等を通じて公的個人認証サービスのユースケースの拡大を促進し、安心・安全な本人確認等の手段として日常の様々なシーンで同サービスが利用される社会の実現を目指す。

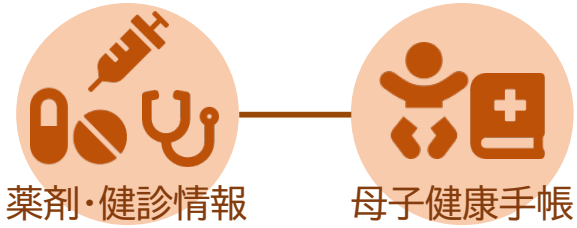
（現在）
マイナンバーカード用電子証明書の利用には、毎回カードの読み取りが必要

スマートフォンひとつで、いつでもどこでも、様々な手続・サービスが利用可能に

生体認証等の活用によって
スマートフォンならではの利便性を実現

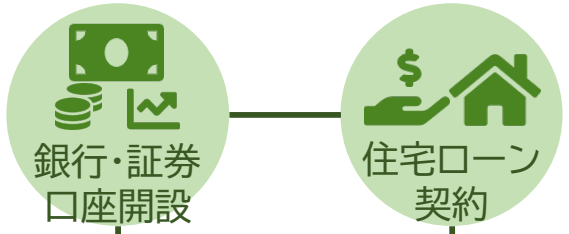


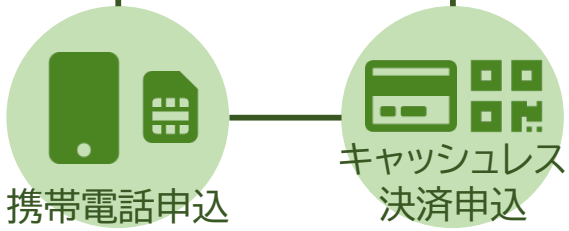
オンライン行政手続



自己情報取得（マイナポータル）

資格確認





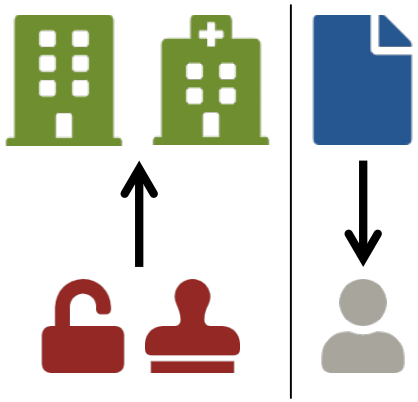
各種民間サービス

「マイナンバーカード機能のスマートフォン搭載」の全体像

- 様々なステークホルダーとの協力体制を構築の上、ライフサイクルを通して、安心・安全かつ簡単に幅広いユースケースで利用できるサービスを実現する。
- 令和4年度中にAndroidスマートフォンへの搭載実現を目指すとともに、iPhoneについても早期実現を目指す。

1. 利用開始

- 簡単なアプリ操作によって、オンラインで電子証明書をスマートフォンに発行

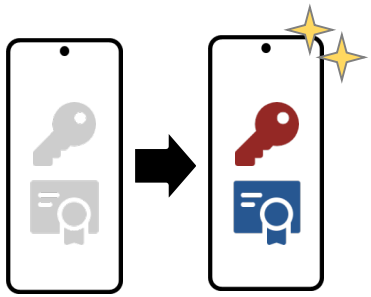


2. 利用

- マイナンバーカードと同様に幅広いユースケースで利用可能
- スマートフォンならではの使いやすいUXを実現

3. 安心・安全

- 安心・安全を確保するための重層的セキュリティ対策
- 紛失・盗難時等の安全性を確保するための技術面・運用面の対応



4. 機種変更・失効

- 簡単なアプリ操作で機種変更・失効時の手続を完結
- 今後発売されるスマートフォンでも継続的に対応

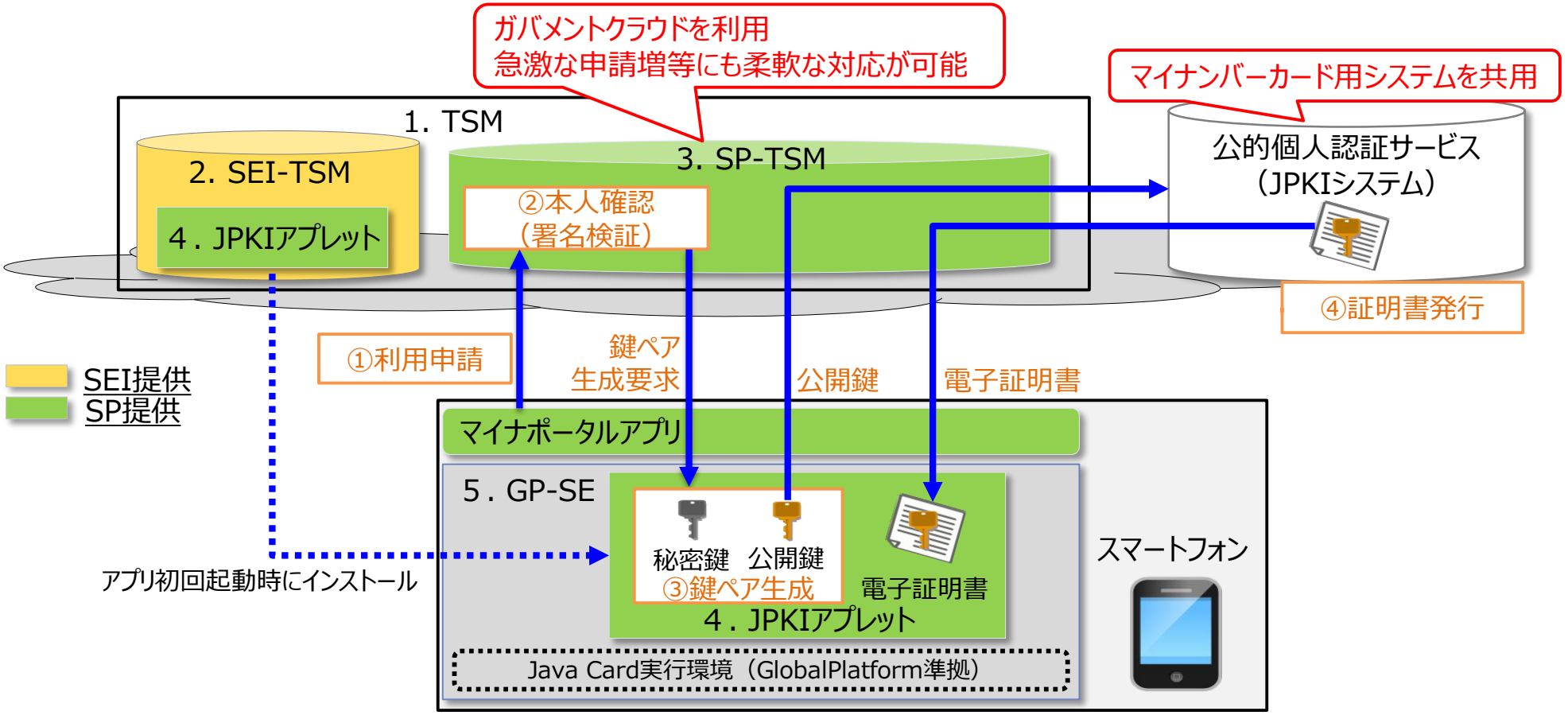
J-LIS、**スマートフォン製造事業者**、**OS事業者**、**携帯電話事業者**、**中古端末取扱事業者**等との協力を通じて安定的なサービス提供を図る。

※対応端末は順次公表予定

スマートフォン搭載を実現するためのシステム構成

■ クラウドサービスや既存システムの活用等によって構築・運用コストの低減を図る。引き続き、運用コストや柔軟な拡張性等も考慮して設計・構築を進める。

スマートフォン用電子証明書（仮称、以下同じ）発行時の流れ



1. TSM（Trusted Service Manager）：SEI-TSMとSP-TSMで構成。スマートフォン内のSecure Element（SE）へのデータ配信をセキュアに実施する。
2. SEI-TSM：Secure Element（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。
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。
4. JPKIアプレット：スマートフォン用電子証明書・秘密鍵をGP-SEに格納するためのJavaアプレット。
5. GP-SE：GlobalPlatform仕様に準拠し、Javaアプレットをダウンロードできる Secure Element（ICチップ）。2021年度上半期に発売されたスマートフォンでは、一部海外メーカー製のSIMフリー端末等を除いてGP-SEを搭載。

「マイナンバーカード機能のスマートフォン搭載」に関する基本方針

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

- マイナンバーカードと同様の幅広いユースケースに対応
- マイナンバーカードをかざすことなくスマートフォンのみで利用可能とすることによって利便性を向上
- NFCを利用したカードリーダーでの読み取り（かざし利用）への対応も検討

2. オンラインで簡単にスマホに搭載

- マイナンバーカードを利用して、スマートフォンからオンラインで申請・発行
- 夜間・早朝の申請も可能
- 機種変更時も簡単に手続

3. スマホならではの使いやすいUX

- 電子証明書利用時のパスワード入力に代えて生体認証を活用
- ユーザテスト等を通じて、利用者に分かりやすい操作フローを実現、リリース後も継続的に改善
- マイナポータルアプリとの一体化による利便性向上

4. 安全・安心に利用できる高いセキュリティ

- スマートフォン内の安全なICチップの活用等、重層的なセキュリティ対策を講ずることによって安全・安心を確保
- 関係事業者とも協力の下、万が一の悪用リスクを排除するための対策を実施

5. グローバルスタンダードに対応

- スマートフォンに関する国内外の技術動向との親和性を確保し、持続的かつ安定的なサービス提供を実現
- 諸外国の基準も踏まえつつ、十分な信頼性を確保できる仕組みを実現

スマートフォン用電子証明書の主なユースケース

■ マイナンバーカードと同等のセキュリティを確保できる仕組みでスマートフォン搭載を実現することによって、マイナンバーカードの電子証明書を使って利用できる手続・サービスをスマートフォン1つで完結できるようになる。

主なユースケース	概要	スマートフォン対応予定時期	備考
マイナポータル	毎回マイナンバーカードをかざす必要がなく、生体認証等によって簡単にログインすることができ、いつでもどこでも、マイナポータルのサービスを利用できるようになる。	令和４年度末	マイナポータルでは、 • 子育て関係等の行政サービスの検索・電子申請 • 自己情報の確認・提供（税・年金・薬剤情報・特定検診情報等） • 確定申告の簡便化 等の様々なサービスを利用可能。
各種行政手続のオンライン申請	スマートフォン用電子証明書を使用した電子署名等によって、いつでもどこでも、各種行政手続のオンライン申請が可能になる。	令和４年度末	
コンビニ交付サービス	スマートフォンを携行していれば、全国のコンビニ等において、住民票の写しや印鑑登録証明等の証明書の取得が可能になる。	令和４年度末以降順次	一部のコンビニに設置されているマルチコピー機や一部のスマートフォンで対応が必要になる可能性有。調整中。
健康保険証	健康保険証やマイナンバーカードを携行することなく、医療機関の受診等が可能になる。	検討中	厚生労働省において、オンライン資格確認システムの改修等の対応を予定。
各種民間サービスのオンライン手続等	スマートフォン用電子証明書を使用した電子署名等によって、いつでもどこでも、証券口座の開設や住宅ローン契約等のオンライン手続が可能になる。	令和４年度末以降順次	民間事業者141社が公的個人認証サービスを活用（令和4年3月25日時点）。 民間事業者においてスマートフォン対応のためのシステム改修等が必要。遅くとも令和4年9月にはAPIを公開予定。

マイナポータルにおける利用イメージ

これまで

マイナポータルへのログイン時には毎回マイナンバーカードの読み取りが必要

スマートフォン用電子証明書を利用

マイナンバーカードを読み取る必要がなく、生体認証等を使って簡単にログインが可能

→通勤中でも、外出先でも、いつでもどこでもサービスを利用可能

マイナポータルで利用できる主なサービス	
行政手続の検索・電子申請	自治体の各種手続の検索及び電子申請が可能。対象手続拡大中。 【例】保育施設利用申込み、給付金申請、児童手当申請
自己情報の確認・提供	行政機関等が保有する自分の情報を確認したり、第三者に提供することが可能。 【例】税・所得情報（金融機関や自治体における手続等に利用） 予防接種履歴・薬剤情報（民間の健康管理アプリ・お薬手帳アプリ等と連携が可能）
お知らせ	行政機関等から情報配信を受けることが可能。 【例】税金の納付依頼、児童手当の手続等の利用者の状況に応じた行政手続の案内

これまで（役所窓口）

書類作成、役所訪問・提出 → 本人確認・申請完了

スマートフォン用電子証明書を利用（電子申請）

マイナポータルで手続を検索・申込内容を入力 → 電子証明書を使って電子署名・電子申請

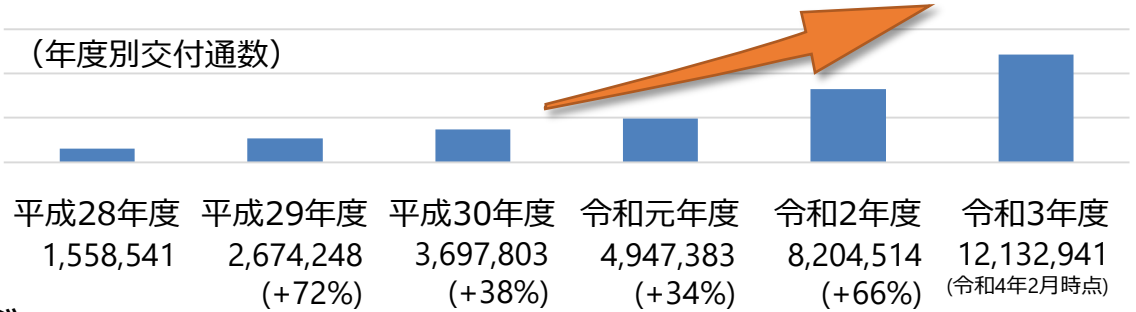
- 入力支援機能を使って、氏名・住所や過去の申請情報等を簡単に入力
- 役所窓口に出向くことなく、いつでもどこでも、スマートフォンひとつで手続可能

コンビニ交付サービスにおける利用イメージ

- コンビニ交付サービスは年々利用が大きく増加している国民に身近なユースケースの1つであり、スマートフォン用電子証明書でも対応することが必要。
- 関係事業者との協力の下、NFC（Type-B）を利用したスマートフォン・ICリーダライタ間の通信性能の評価等、スマートフォン対応の実現に向けて必要な調整を進める。

コンビニ交付サービスの利用状況

参加団体数：928（令和4年2月末時点）
キオスク端末設置拠点数：56,285（令和3年9月末時点）



スマートフォン用電子証明書による利用イメージ

操作開始	スマートフォンをかざす	本人確認・証明書種別	証明書の印刷
	 NFC Type-B		
コンビニ等に設置されたキオスク端末を操作して、証明書交付サービスを選択 →全国のコンビニ等で早朝・夜間・土日祝日も利用可能	キオスク端末のICカード読み取り部分にスマートフォンをかざす →マイナンバーカードを携行する必要がない	キオスク端末でスマートフォン用電子証明書のパスワードを入力 証明書の種類・印刷部数等を選択し、料金を支払う	マルチコピー機で選択した証明書が印刷される

※現時点におけるイメージであり、今後変更となる可能性がある。

健康保険証としての利用イメージ

健康保険証を利用した流れ

健康保険証提示 → 健康保険証確認 → 情報登録（初回来院時） → 受付完了

スマートフォン用電子証明書を活用した流れ

QRコード読み取り

医療機関等に掲示された専用QRコードを患者のスマートフォンで読み取り

→健康保険証やマイナンバーカードを持ち歩く必要がなくなる

本人確認（生体認証）

スマートフォン内の電子証明書、生体認証機能を使って、本人確認（パスワード等も利用可能）

同意事項確認

スマートフォン上で薬剤情報や特定健診等情報の提供に関する同意事項を確認

→より良い医療を受けられる環境

受付完了

健康保険証の資格情報を自動でシステムに登録

→医療機関等職員の作業負担軽減

→資格過誤によるレセプト返戻がなくなり、再確認業務の発生が少なくなる

※現時点におけるイメージであり、今後変更となる可能性がある。

民間サービスにおける利用イメージ

金融機関の口座開設の流れ（窓口･eKYC）

金融機関訪問
申込書記入

本人確認

金融機関
における処理

利用開始

金融機関HP等
申込内容入力

eKYC
（顔･身分証明書の撮影）

スマートフォン用電子証明書を活用した流れ

金融機関HP等 申込内容入力

金融機関のHP等から口座開設の申込みを開始、申込内容を入力

本人確認

スマートフォン内の電子証明書を使って本人確認（マイナポータルアプリと連携）

→身分証明書等の撮影不要、いつでもどこでも手続可能

金融機関における処理

金融機関において申請内容確認、事務処理

→真贋確認が不要、手続期間が短縮

利用開始

利用者が処理結果を確認、利用開始

※現時点におけるイメージであり、今後変更となる可能性がある。

※遅くとも令和4年9月には民間サービス等との連携に必要なAPI情報を公開予定。また、民間サービスにおける更なる利用拡大を促進する観点から、海外事例（シンガポール等）も参考としつつ、開発者目線の利便性向上にも取り組む。

公的個人認証サービスと紐付けられた民間IDの利活用促進

■ 電子証明書の機能を搭載できないスマートフォンからでも各種オンライン手続を行えるよう配慮する必要がある。この観点から、公的個人認証サービスと紐付けられた民間ID※（以下単に「民間ID」という。）の利活用を進めることが重要。

※ 「公的個人認証サービスと紐付けられた民間ID」とは、マイナンバーカードの署名用電子証明書による確実な本人確認に基づき利用者に対して発行されるオンライン識別手段全般を指し、電子認証局によって発行される電子証明書を想定。ただし、電子署名法に基づく認定認証業務において発行される電子証明書については、既に行政手続での利用が可能であるため、検討の対象からは除く。

本検討会では、公的個人認証サービスの独自性に基づく観点から、民間IDの利便性向上策について検討。

【利便性向上策】

- 民間IDのトラストアンカーとなった公的個人認証サービスの署名用電子証明書について、その**失効の有無を確認**

→公的個人認証サービスの署名用電子証明書は住所異動等の事由により失効するため、その有効性を確認することにより、民間ID発行時の基本４情報（氏名・生年月日・性別・住所）が最新のものかどうか確認可能である。

→基本４情報が最新でないことが判明した場合、アプリ等の通知により民間IDの再発行を促すことで、民間IDと紐付いた基本４情報の最新化を促すことも可能となる。

- 令和３年の公的個人認証法改正により可能となった、本人同意に基づく署名検証者への**基本４情報の提供の仕組みを活用**

→事前の本人同意を前提として、民間IDのトラストアンカーとなった公的個人認証サービスの署名用電子証明書が失効した場合であっても、民間IDの発行事業者がJ-LISから最新の基本４情報の提供を受け、当該基本４情報を基に民間IDを再発行することで、民間IDを本人確認に利用する事業者が本人から最新の基本４情報の提供を受けられるようになることも考えられる。

今後は、民間事業者向けのガイドラインや各種説明会等において、上記の方策とともに民間IDの活用場面を紹介することにより、その利活用の促進と一層の利便性向上を図ることが重要

スマートフォン用電子証明書の利用手続

新規発行

自治体窓口に赴くことなく、いつでもどこでもマイナポータルアプリから簡単に発行申請が可能。

マイナンバーカード用電子証明書

開庁時間に
役所窓口を訪問

スマートフォン用電子証明書

オンラインで手続が完結

夜間・早朝も
発行申請を受付

発行申請手続のイメージ

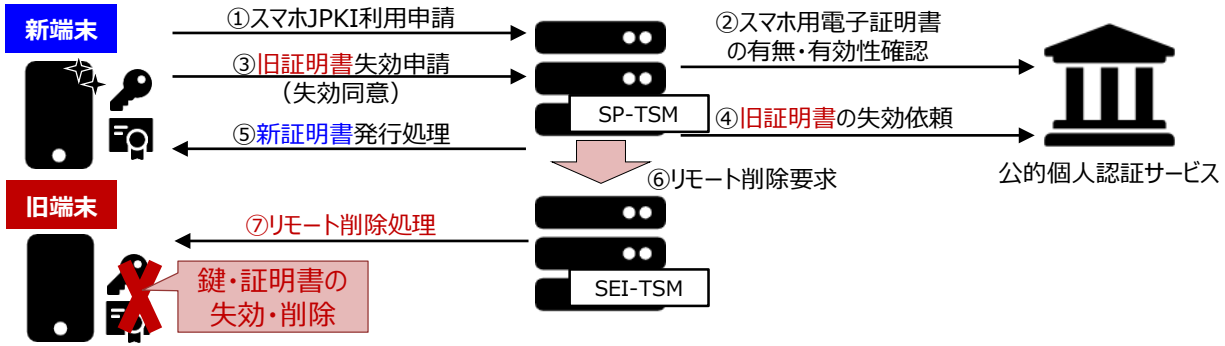
マイナポータル
アプリから申請

マイナンバーカードによる
電子署名・申請

スマートフォン用電子証明書
のパスワード設定

機種変更

新端末での電子証明書の発行申請と同時に、シームレスに旧端末の電子証明書の失効・削除手続を行うことが可能。



その他の手続

失効手続やパスワード設定等の手続は、マイナンバーカードを必要とせず、スマートフォンのみで完結。

サポート体制

J-LISコールセンターの拡充等によって、申請方法・利用方法等に関する相談へのサポート体制を構築。
デジタル活用支援推進事業等の政府の取組との連携、関係事業者への協力の呼びかけについても検討。

生体認証等の活用

- Androidスマートフォンに設定される画面ロック（※）は、生体認証その他の一定の水準を満たす簡易で安全な認証によって解除することができ、これらの認証機能は、金融分野等の高いセキュリティが求められるアプリやウェブサイトへのログインにも広く活用されている。
  ※Android互換性定義ドキュメント（CDD）に規定されている「Secure Lock Screen」
- 現在普及している生体認証装置の性能や画面ロック解除機能の安全性向上等の状況も踏まえつつ、簡単な認証やパスワード忘れの防止等による利便性の向上を図る観点から、利用者証明用電子証明書を利用するためのパスワードについて、同等のセキュリティを確保することができると考えられる画面ロック解除機能（生体認証等）によって代替することを可能とする。
- 実装に当たっては、技術検証の結果を踏まえて、BiometricPrompt APIを用いた安全かつ簡便な方法によって生体認証等の登録を行う仕組みを採用する。

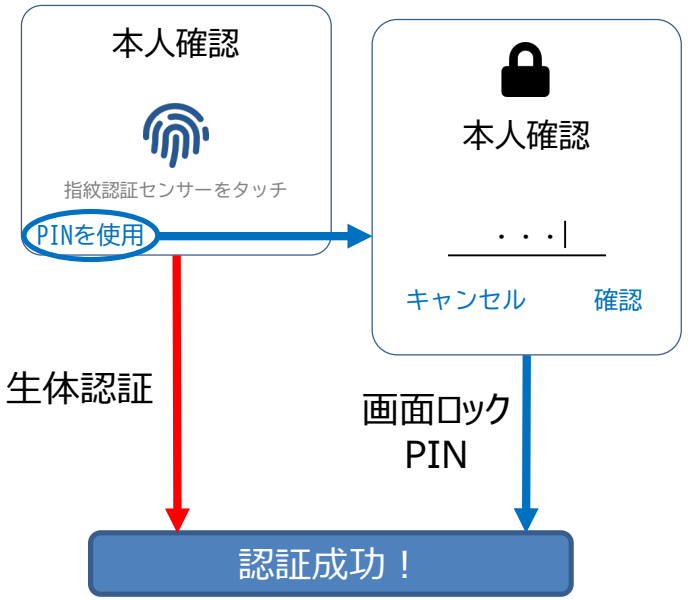
スマートフォン用電子証明書で利用可能な認証手段

	GP-SEに設定されたパスワード	Androidスマートフォンの画面ロック解除機能
署名用電子証明書	○ （6～16桁の英大文字・数字の組合せ）	×
利用者証明用電子証明書	○ （4桁の数字）	○ （※）

※利用者証明用電子証明書のパスワードを代替可能な画面ロック解除機能は、Android CDDに沿って、以下の要件を満たすものとする。

	要件
プライマリ認証	画面ロック解除用のPIN・パターン・パスワード
セカンダリ認証	Class 3（Android 10以前：強）の生体認証 • FAR（他人受入率）：0.002%（5万人に1人）以下 • SAR（スプーフィング攻撃への耐性）：7%以下 • IAR（なりすまし攻撃への耐性）：7%以下 • 少なくとも72時間に一度はプライマリ認証が求められる

認証操作フロー（イメージ）



利用者にとって分かりやすい操作フローの実現

- 実証段階において、発行申請等の基本機能の操作フローに関するユーザテストを実施し、設計時に課題点を改善。

ユーザテストを通じて確認された主な課題

- スマートフォンでマイナンバーカードを読み取る方法が分からない（カメラでマイナンバーカードを読み取るものと誤認 等）
- 生体認証の設定時にOSの設定画面へ遷移することで混乱が生じた
- アプリのどこに機種変更手続のメニューがあるのか分からない

改善点

- マイナンバーカード読み取り方法を簡単に理解できるアニメーションの活用
- 分かりやすく、混乱の生じない導線設計を検討

- 引き続き、システム構築と並行して、具体的なユースケース（行政手続・健康保険証利用・口座開設等）を想定したユーザテスト（アクセシビリティの検証を含む）を実施。
- ユーザ評価等について一定の目標を設定の上、サービスの提供開始後においても、 Firebase等の解析機能を活用しつつ、継続的に操作フロー等を改善。
- また、電子署名を使用する際に、利用者がその重要性を認識しやすいUI設計を検討。

マイナポータルアプリとの一体化

- 利用者にとっていくつものアプリをダウンロードしなければならない状況は負担感が大きいため、スマートフォン用電子証明書を発行・利用する機能のみを提供する独立アプリとして開発するのではなく、既存のJPKI関連アプリと一体化することが望ましい。
- 既存アプリのうち、総合的な行政サービスの窓口であるマイナポータルアプリと一体化することによって、スマートフォン用電子証明書を使って、いつでもどこでも、1つのアプリでシームレスに様々な手続・サービスを完結できるようになる等、大幅な利用者の利便性向上が期待されるため、スマートフォン用電子証明書の機能を同アプリに追加することとする。
- 既存アプリとの一体化によって、別個のアプリとして運用する場合と比べた運用・保守業務の効率化を図る。
- また、複数の機能が1つのアプリに統合されることによって、将来的な拡張可能性や柔軟性が損なわれることのないよう、システムの設計・構築に当たって、
  - 共通機能と個別機能を整理の上で機能毎にソースコードのクラス分けを行い、疎結合する
  - アプリ規模に応じて項目数が増える回帰テストを自動化する
  - バックエンドから各機能の利用制限を操作し、縮退運用を可能とする

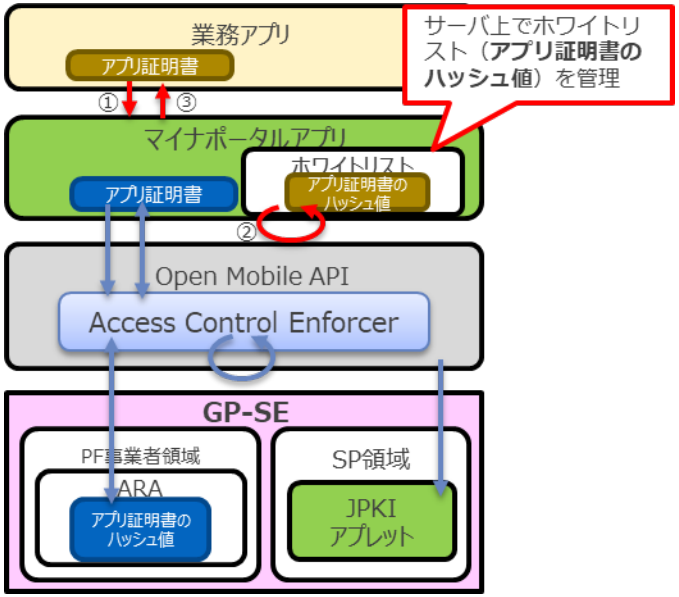
  等の対応を検討する。

他サービスのアプリ・ブラウザとの連携

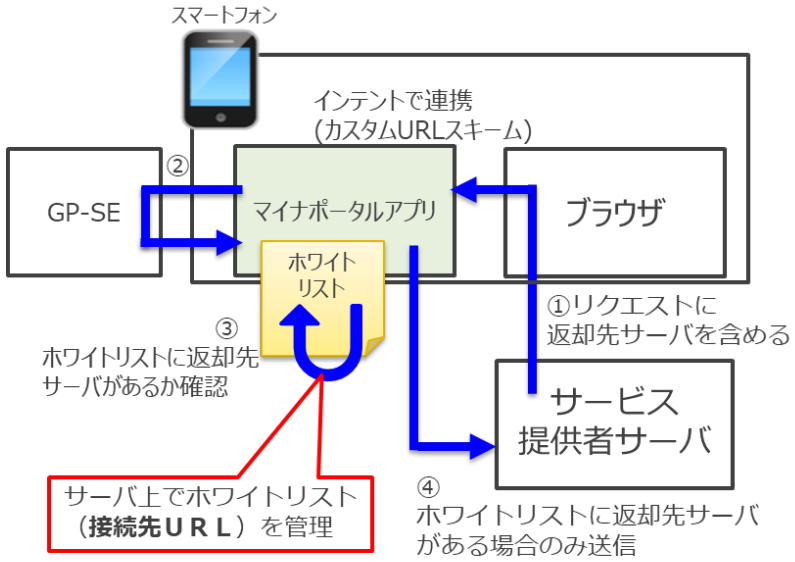
- 何ら対策を講じない場合、常時、アプリ経由又はブラウザからインターネット越しに、スマートフォン用電子証明書及び秘密鍵の格納領域（GP-SE）へアクセスし得ることとなるため、他サービスのアプリ・ブラウザとの連携に当たっては、
  - マイナポータルアプリを介してのみGP-SEにアクセス可能とする
  - 一定水準のセキュリティ対策が講じられたプラットフォーム事業者（署名検証者）・サービスプロバイダ事業者（みなし署名検証者）のアプリ・ブラウザにアクセスを限定し、ホワイトリストで管理する

  等の重層的な対策を講ずる。
- 具体的な要件等について引き続き検討の上、「公的個人認証サービス利用のための民間事業者向けガイドライン」等に反映する。また、今後のリスクの顕在化の状況等を踏まえつつ、必要に応じて、更なる重層的対策の要否について検討する。
- 電子証明書の利用時にマイナポータルアプリに遷移することによって利用者に混乱等が生ずることのないよう、適切なUI設計を図る。

ネイティブアプリの場合



ブラウザの場合



- セキュリティ対策を1つのアプリに集中して行うことが可能
- 利用者が行う生体認証の登録・変更設定はマイナポータルアプリのみとなるため利便性に優れ、GP-SEの容量も圧迫しない
  （複数アプリからGP-SEにアクセスする場合、アプリ毎に設定が必要）

安全・安心のための重層的なセキュリティ対策

厳格な本人確認に基づく発行

- 役所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用電子証明書による本人確認に基づいて発行。
- マイナンバーカード用電子証明書が失効した場合には、スマートフォン用電子証明書も連動失効。

高セキュリティな秘匿通信

- GP-SEとサーバ（TSM）との間の通信には、国際標準に準拠したセキュアチャネルプロトコル（SCP03）を採用。通信経路途中におけるデータのスキミングによる解読や改ざん等を防止。
- TSMとJPKIシステムとの間は専用線によって高セキュリティな通信を確保。

格納媒体等の安全性

- 耐タンパ性※を有する安全なチップ（GP-SE）内で秘密鍵を生成し、GP-SE内のアプレットに安全に格納。

※ICチップ内の情報が不正に読み出されたり、解析されようとした場合、自動的に内容が消去される等の対抗措置が講じられる性質

- マイナンバーカードと同様に第三者機関によるセキュリティ評価・認証を取得することで、安全性を担保。（GP-SEとアプレットを一体としてCC認証・EAL4+のコンポジット認証を取得）
- GP-SE内の電子証明書へのアクセスをマイナポータルアプリに限定し、厳格なアクセス制御を実施。
- スマートフォンの紛失時等に、もしGP-SE内に電子証明書や秘密鍵が残存していたとしても、外から読み出すことはできない等、安全性が確保されていることを確認。

脆弱性対策

- 特定のハードウェア・ソフトウェアに重大な脆弱性が確認された場合に備え、即時的に利用制限を行うための独自サーバを構築。
- 脆弱性情報の収集体制や利用制限要否の判断基準等の運用の在り方について引き続き検討。

不正な端末の検知

- SafetyNet Attestation APIを用いてroot化・カスタムROM等によって正規の状態にない端末を検知することで、不正利用を防止。
- また、不正利用対策として利用されるAPI等の今後の動向にも追従。

更なるセキュリティ対策の検討

- 技術検証において実施したセキュリティ脅威分析の結果等を踏まえて、更なる対策を検討。

※上記のようなセキュリティ対策等を行うに当たって利用者の同意が必要となる場合があることも踏まえて、本サービスの利用規約を整理。

スマートフォン用電子証明書に係る技術的基準の要件

- マイナンバーカード用電子証明書に係る電子署名、電子利用者証明、電子証明書等に係る技術的な基準については、「認証業務及びこれに附帯する業務の実施に関する技術的基準」（平成15年総務省告示第706号）において規定されている。
- 現行の告示には、鍵の一意性や電子証明書の規格等について定められているところ、スマートフォン用電子証明書に係る基準について、同告示において規定する必要がある。
- 想定される具体的な規定内容案は以下のとおり。

【規定内容案】

- スマートフォンのICチップ内に、スマートフォン用電子証明書に係る専用の領域が確保されること。
- 当該領域がICチップの他の領域から独立していること。
- ICチップは偽造を目的とした不正行為に対する耐タンパ性を有すること。
- スマートフォン用電子証明書に係る専用の領域を含め、ICチップ（※アプレットを含む）がCC認証を取得していること。
- ICチップ内で生成されるスマートフォン用電子証明書に係る鍵ペアについて、マイナンバーカード用電子証明書に係る鍵ペアとも重複しないよう、一意性が担保されていること。
- スマートフォンとTSMとの間の通信は、主務大臣が適当と認める暗号化通信により行うこと。
- ICチップに記録された情報を保護するために、アクセス権限の制御を行うこと。

等

悪用防止対策

■ 仮にGP-SE内に電子証明書や秘密鍵が残存していたとしても、外から読み出すことはできない等、安全性が確保されているものの、万が一の悪用リスクを排除するために重層的な対策を講ずる。

リモート削除機能の実装

- 技術検証を通じて実現可能性が確認された「リモート削除」機能を実装。
- 機種変更時の手続やマイナンバーカード用電子証明書の失効時（スマートフォン用電子証明書も連動失効）に活用し、電子証明書等を適切に削除。

※別途検討した端末初期化による電子証明書等の削除については、技術面の困難さや相応の実装コストを要することが判明。
他の対策によって基本的に安全性が担保されていることを踏まえると、実装は不要と判断。

メール通知の実装

- 電子証明書を利用するための認証が行われた場合に利用者にメール通知する機能（任意設定）を実装。
- 日頃から利用停止時には適切な失効・削除手続を行う必要があることを注意喚起するとともに、万が一不正利用が発生した場合にも利用者が認知できる等の効果。

関係事業者との連携

- スマートフォン用電子証明書の利用が確認できた方に対して、
  - ✓ スマートフォンの買取り・下取り・修理等の受付時に、電子証明書の適切な失効・削除手続を促す
  - ✓ 通信サービスの一時中断を受け付ける際にJ-LISコールセンターに連絡すべき旨を案内する

  等の協力を携帯事業者・中古端末取扱事業者等に呼びかけ。
- 今後、関係事業者の協力を得て具体的な対応フローの検証を行い、ガイドライン等を整備予定。

持続的かつ安定的なサービス提供の実現

- 将来にわたって幅広い種類のスマートフォンで本サービスを利用できるよう、既存のエコシステムとの関係も考慮の上、国際標準であるGlobalPlatform仕様に準拠し、モバイル決済サービス等の重要な基盤として国内で広く普及しているGP-SEを電子証明書や秘密鍵の格納媒体として活用する。
- 新規のAndroid端末を出荷するために準拠することが求められる互換性定義ドキュメント（CDD）等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との親和性を確保し、スマートフォン用電子証明書を利用するための独自要件を最小化する。
- 持続的かつ安定的なサービス提供を実現するためには、今後の技術動向の変化に適確に対応していくことが重要であることも踏まえて、関係事業者との協力体制の構築を図る。
- CC認証の有効期限や古いバージョンのOSに関する取扱いについては引き続き検討する。

主な関係事業者との協力体制のイメージ

スマートフォンのエコシステム（製造・製品アップデート段階）

- OS提供事業者
- GP-SE製造事業者
- 携帯事業者
- スマートフォン製造事業者

- 幅広い対応端末の確保（CC認証の対応を含む）
- NFC（Type-B）を利用した通信性能の評価
- CDD改訂・OSアップデート対応
- 脆弱性対応　等

デジタル庁
総務省
J-LIS
運用事業者

コンビニ交付用マルチコピー機のエコシステム

- コンビニ交付サービス提供事業者
- マルチコピー機製造事業者
- カードリーダー製造事業者

- コンビニ交付サービスの実現に向けた技術的検討　等

スマートフォンのエコシステム（市場流通段階）

- 携帯事業者
- 販売代理店／中古端末取扱事業者

- 買取り・下取り・修理等の対応
- サービスの周知広報　等

スマートフォン用電子証明書の本人確認保証レベル等

- スマートフォン用電子証明書は、マイナンバーカード用電子証明書と同等の本人確認保証レベル（IAL3・AAL3）を確保することによって、高い保証レベルが求められる手続・サービスを含め、幅広いユースケースに対応可能。
- また、「スマートフォン用電子証明書に係る電子署名」と「マイナンバーカード用電子証明書に係る電子署名」は、ともにeIDAS規則における適格電子署名の主な要件（高度電子署名・適格電子証明書・適格電子署名生成装置）を満たしているものと考えられる。

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	**レベル３相当** ○対面交付されたマイナンバーカード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相当** ○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）又は 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のローカル環境（GP-SE内のアプレット）での鍵ペア生成

○高セキュリティな秘匿通信の環境下で公開鍵をJPKI側に登録して電子証明書を発行

→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

○マイナンバーカードのICチップとGP-SE（アプレットを含む）はいずれもCC認証を取得し、耐タンパ性を保証

米国NISTデジタルアイデンティティガイドライン（SP 800-63-3）参照

（参考）スマートフォン用電子証明書及びカード用電子証明書に係る電子署名

対象	スマートフォン用署名用電子証明書及び マイナンバーカード用署名用電子証明書に係る電子署名
電子署名	【スマートフォン用署名用電子証明書及びカード用署名用電子証明書に基づく電子署名】 ➢ 電子証明書に記載された基本４情報に基づいて署名者に一意に紐付いており、署名者の識別が可能 ➢ 署名者のみが知るパスワードの入力により、署名者のICチップ内に格納された秘密鍵を用いて生成される ➢ PKIのアーキテクチャに基づき、文書の改ざん検出が可能
電子証明書	【スマートフォン用署名用電子証明書及びカード用署名用電子証明書】 ➢ 住民基本台帳に基づく氏名・通称を含む署名者の基本４情報 ➢ 公開鍵情報 ➢ 電子証明書の有効期間（開始日時・終了日時） ➢ 一意のシリアル番号 ➢ 発行者（J-LIS）の電子署名 ➢ J-LISホームページ上でCA証明書の情報を公開 ➢ 証明書失効リスト（CRL）配布点に関する情報を公開（実際のURLは署名検証者に個別提供）
電子署名生成装置	【スマートフォン（GP-SE・アプリ）及びマイナンバーカード（ICチップ・アプリ）】 ➢ 秘密鍵はICチップの耐タンパ領域に格納されるため、機密性が保証されている ➢ 秘密鍵はICチップの耐タンパ領域に一定の管理下で記録され、同じ鍵は再度生成されない ➢ 秘密鍵の派生は認められていない。PKIのアーキテクチャに基づき、文書の改ざんから確実に保護される ➢ 本人のみが知るパスワードによってのみ署名することができ、他者による使用から確実に保護される ➢ 署名対象データが改変されることはなく、署名前に署名対象データの提示を妨げることはない ➢ ICチップ内の署名用鍵の生成・管理は利用者自身のみが行う（ローカル署名）

eIDAS規則における適格電子署名の主な要件

【高度電子署名】

- 署名者に一意に紐付いており、署名者の識別が可能
- 高いレベルの固有性を持つ電子署名生成データを用いて生成
- 署名後の改ざん検出が可能な方法で署名されたデータに紐付いている

【適格電子証明書】

- 署名者の氏名又は仮名（仮名を使用する場合はその旨を表示）
- 電子署名作成データに対応する電子署名検証データ
- 電子証明書の有効期間の開始日及び終了日の詳細
- 電子証明書の識別コード（適格トラストサービスプロバイダー内で一意）
- 電子証明書の発行者である適格トラストサービスプロバイダーの高度電子署名
- 適格トラストサービスプロバイダーの高度電子署名に対応する電子証明書が無料で入手できる場所
- 適格電子証明書の有効性の状態を問い合わせるために使用できるサービスの場所

【適格電子署名生成装置】

- 電子署名生成に使用される電子署名生成データの機密性が合理的に保証される
- 電子署名生成に使用される電子署名生成データが一度しか生成されない
- 電子署名生成に使用される電子署名生成データが合理的な保証の下で派生することなく、電子署名が現在利用可能な技術を用いた偽造から確実に保護される
- 電子署名生成に使用される電子署名作成データが、正当な署名者によって他者による使用から確実に保護される
- 署名対象データを改変したり、署名前に署名対象データを署名者に対して提示することを妨げたりしてはならない
- 署名者に代わって電子署名作成データを生成又は管理することは、適格トラストサービスプロバイダーのみが可能

デジタルID及びトラストに関する国際動向

- デジタルIDやトラストに関する議論が、標準化・制度整備等の観点から国際的に行われ、関連技術の普及も進められている状況にあり、今後もこのような取組が継続する見通し。議論の中心は身分証明機能のモバイル端末への搭載であり、電子証明書の機能の搭載そのものではないが、これらの動向とも乖離することのないよう引き続き注視するとともに、将来の状況に応じて見直しを行っていく必要がある。
- 国際的に見てもSEを利用するユースケースについて幅広く議論されている状況。また、GP-SEとeSIMを1つのチップに統合した製品が各チップベンダーから発売されており、当該製品のAndroidスマートフォンへの搭載は今後も拡大する見込み。

分野	項目	概要
国際標準	ISO/IEC 18013-5	モバイル端末に格納されるモバイル運転免許証（mDL）を実装するためのインターフェース仕様を規定しており、mDL発行元以外の者（他国の運転免許証発行機関、民間サービスでの運転免許証による身元確認者等）がmDLの検証を可能とすることを目的としている。2021年9月公開。
	ISO/IEC 23220シリーズ	各国の政府や民間等の発行機関が発行するモバイル身分証明書（モバイルeID）の相互運用を可能にすることを目的とした規定群。2022年中の規格発行を目指して議論が進められており、モバイルeIDシステムの全体アーキテクチャについて規定するPart 1の国際規格原案（DIS）が既に発行されている。格納媒体として、GP-SEを含む埋め込み型SEへの格納も想定されている。
技術	Android Ready SE	2021年3月、Google社はAndroidにおけるデジタルキー、mDL、電子マネー等のユースケースの採用を拡大するため、Androidにおいて耐タンパハードウェアに基づくセキュリティを実現する「Android Ready SE」の普及に取り組む枠組み「Android Ready SE Alliance」を設立し、SEベンダー等と協力してオープンソースのアプレットの開発に取り組んでいる旨発表。同アライアンスにはGP-SE製造ベンダーも参画。
制度	NIST SP 800-63-4	SP 800-63-3の改定作業が進められており、2022年中にドラフト版が公開される見込み。モバイル端末を用いた身元確認等に関する改定が想定される。
	eIDAS規則の改正提案	2021年6月、欧州委員会は「European Digital Identity Wallet」の導入を中心としたeIDAS規則の改正提案を発表。2022年10月までの技術アーキテクチャ等の文書群の公表を目標とする。同Walletは身元情報・資格情報・属性情報の保存や提供、認証、クオリファイド電子署名等の機能を持ち、保証レベルhighの電子識別スキームに基づいて発行される。利用者は同Walletに関して完全なデータコントロール権を持ち、関連するパーソナルデータは他のデータから物理的・論理的に隔離されることが求められている。