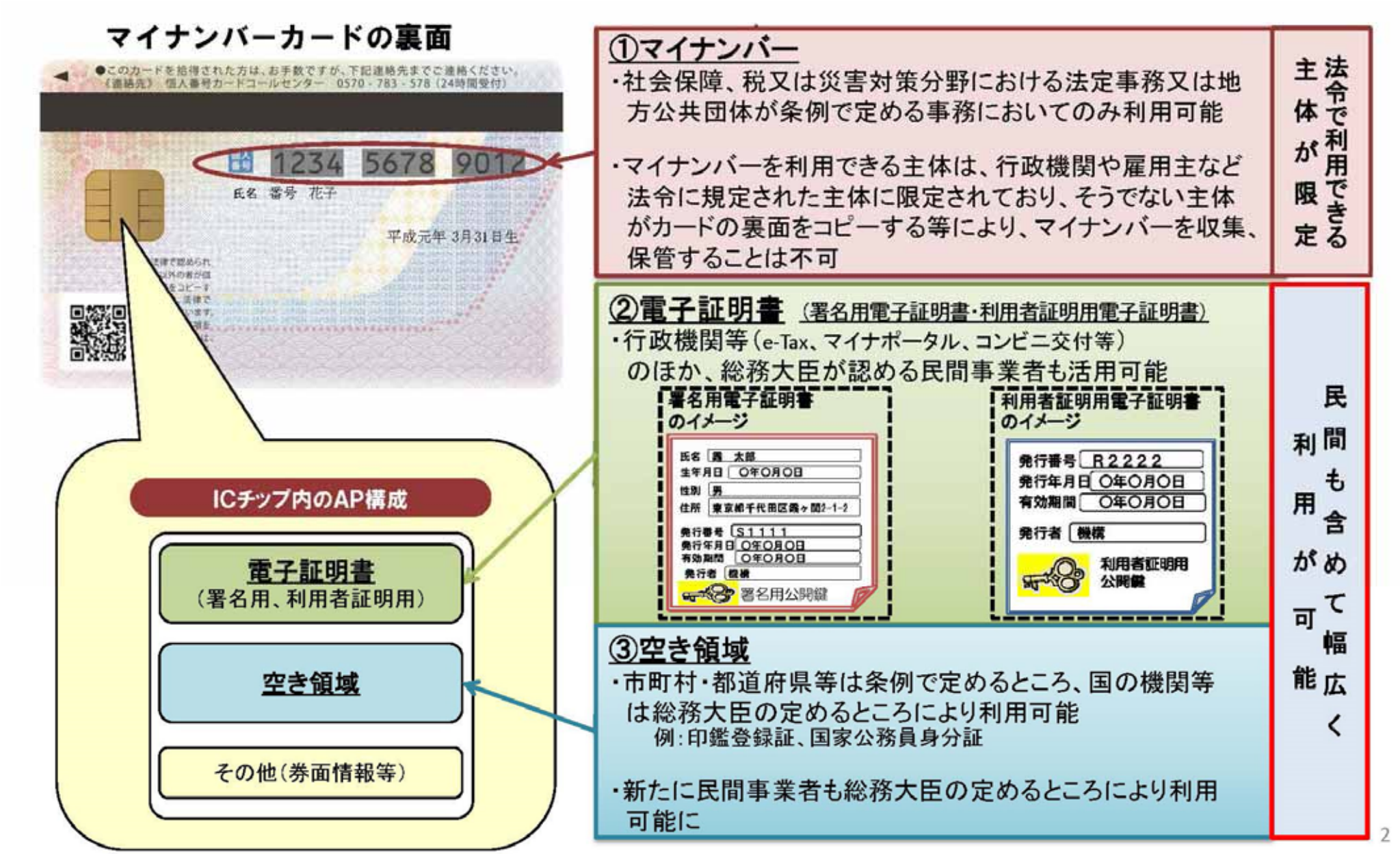
DIPCのめざす社会/
本当に安心安全な社会を実現するために

DIPC理事
情報セキュリティ大学院大学 客員教授
辻　秀典

2022年4月21日

マイナンバーカードの中身



引用元: https://www.soumu.go.jp/main_sosiki/kenkyu/mynumber_smartphone/index.html

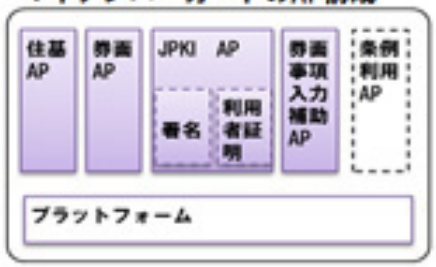
マイナンバーカードの中身

マイナンバーカードのアプリの概要

マイナンバーカードの表面（案）

マイナンバーカードの裏面（案）

マイナンバーカードのAP構成



AP	個人番号取得、本人確認における役割	アクセスコントロール
券面AP	（目的） ・対面における券面記載情報の改ざん検知 ・対面における本人確認の証跡として画像情報の利用 （記録する情報） ・表面情報：4情報＋顔写真の画像 ・裏面情報：個人番号の画像	・個人番号を利用できる者 表と裏の券面情報 ：照合番号A（個人番号12桁） ・個人番号を利用できない者 表の券面情報のみ ：照合番号B（14桁：生年月日6桁＋有効期限西暦部分4桁＋セキュリティコード4桁）
JPKI-AP	（署名用） ・電子申請に利用	暗証番号（6～16桁の英数字）
	（利用者証明用）【新規】 ・マイナポータル等のログインに利用	暗証番号（4桁の数字）
券面事項入力補助AP【新規】	・個人番号や4情報を確認（対面・非対面）し、テキストデータとして利用することが可能 【記録・利用する情報】 ①個人番号及び4情報 並びにその電子署名データ ②個人番号 及びその電子署名データ ③4情報 及びその電子署名データ 注）①、②については、番号法に基づく事務でのみ利用可能。	①については、暗証番号（4桁の数字） ②については、照合番号A（個人番号12桁） ※これにより、券面目視により個人番号を手入力するようなケースで正誤チェックが可能となる。 ③については、照合番号B（14桁：生年月日6桁＋有効期限西暦部分4桁＋セキュリティコード4桁）
住基AP	・住民票コードを記録 ・住基ネットの事務のために住民票コードをテキストデータとして利用可能	暗証番号（4桁の数字）

※「暗証番号（4桁の数字）」については、統一の設定も可能。
ただし、生年月日やセキュリティコード等と同一は不適当。

引用元: https://www.soumu.go.jp/kojinbango_card/03.html#merit

マイナンバーカードの安全性

マイナンバーカードの安全性

なりすましはできない

✓ 顔写真入りのため、
対面での悪用は困難。

万全のセキュリティ対策

- 紛失・盗難の場合は、24時間365日体制で停止可能
- アプリ毎に暗証番号を設定し、一定回数間違うと機能ロック
- 不正に情報を読み出そうとすると、ICチップが壊れる仕組

大切な個人情報は入っていない

✓ ICチップ部分には、
税や年金などの
個人情報は記録されない。

マイナンバーを見られても個人情報は盗まれない

✓ マイナンバーを利用するには、
顔写真付き身分証明書等での
本人確認があるため、悪用は困難。

オンラインの利用には マイナンバーは使われない

2

引用元: https://www.cao.go.jp/bangouseido/pdf/topic_card_anzen.pdf

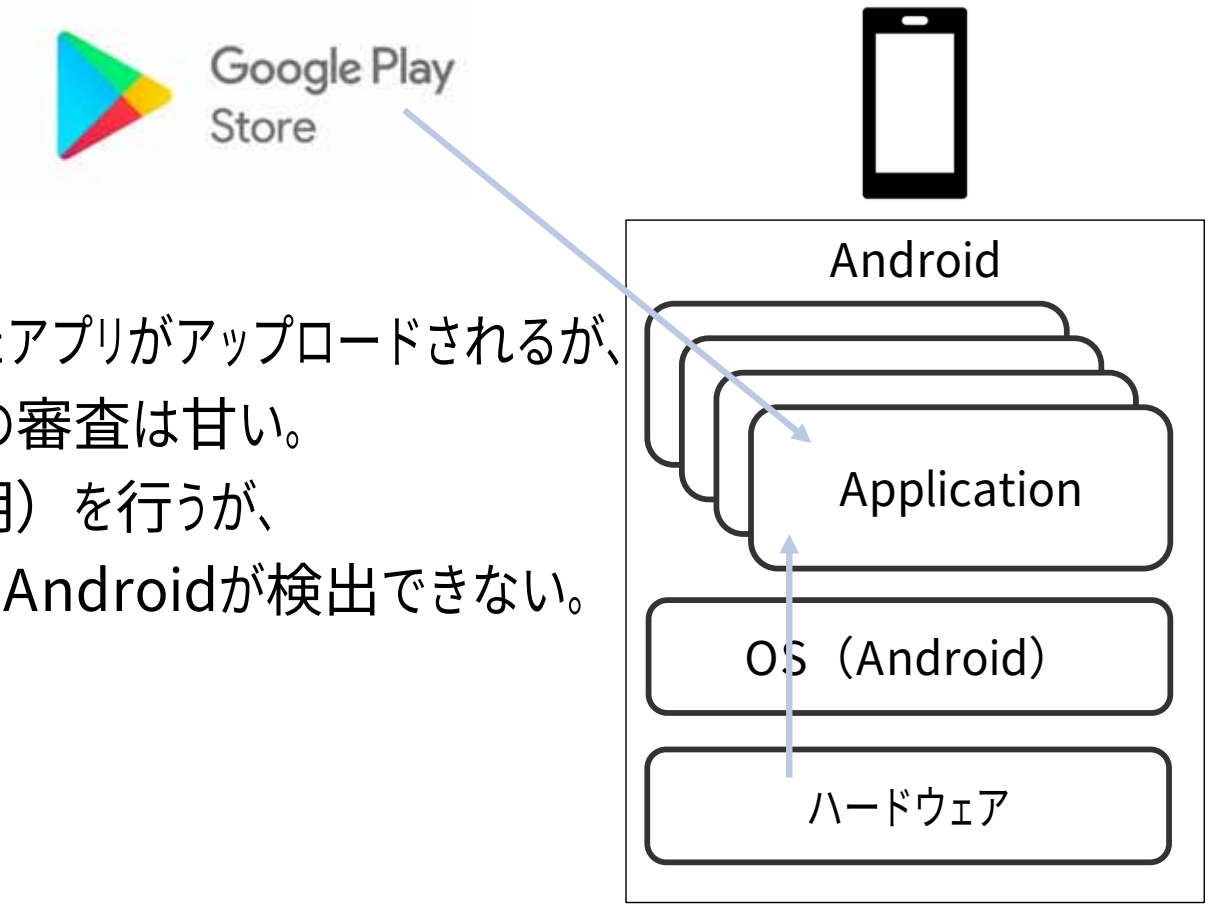
ICカード

ICカードは、単体の閉じたコンピュータ。目的の機能だけが書き込まれ、実行（処理）されているので、外部から改ざんできないが、自由に書き換えができない。サービスの数だけ必要。
インターネット通信もできず専用の近接通信に限られる。

<u>→セキュリティの大原則、安全性と利便性は相反する。</u>

Androidアプリの危険性

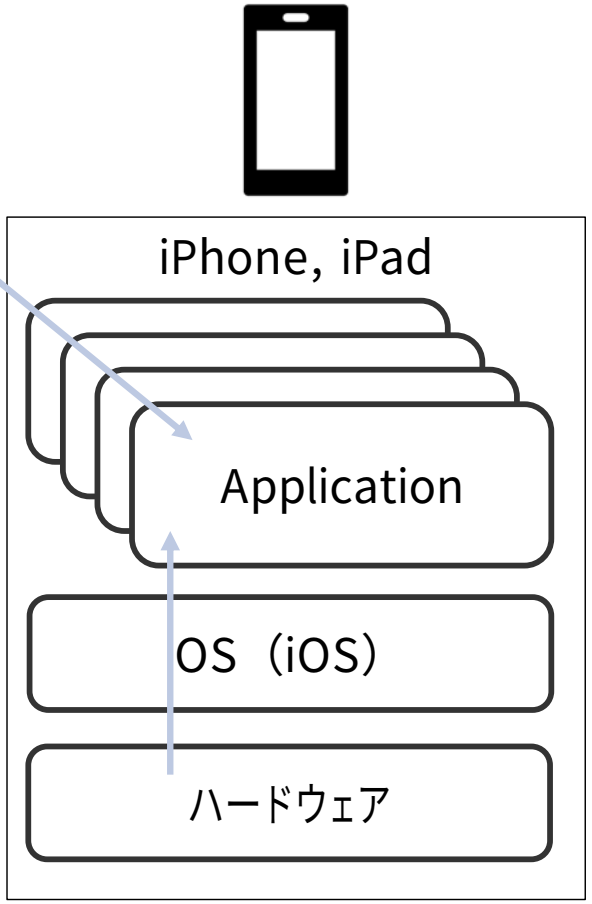
Andoridはアプリの安全性を担保するしくみがあるが、抜け穴がある。
＝悪さをするアプリが付け入るスキがある。



ストアにはGoogleが審査したアプリがアップロードされるが、
規定の審査だけで、安全性の審査は甘い。
アプリに署名（作成者の証明）を行うが、
それを差し替えることが可能。Androidが検出できない。

iOS（Apple）アプリの危険性

iOSはアプリの安全性を担保するしくみがある。
＝が、その仕組みはAppleにコントロールされ手が出ない。

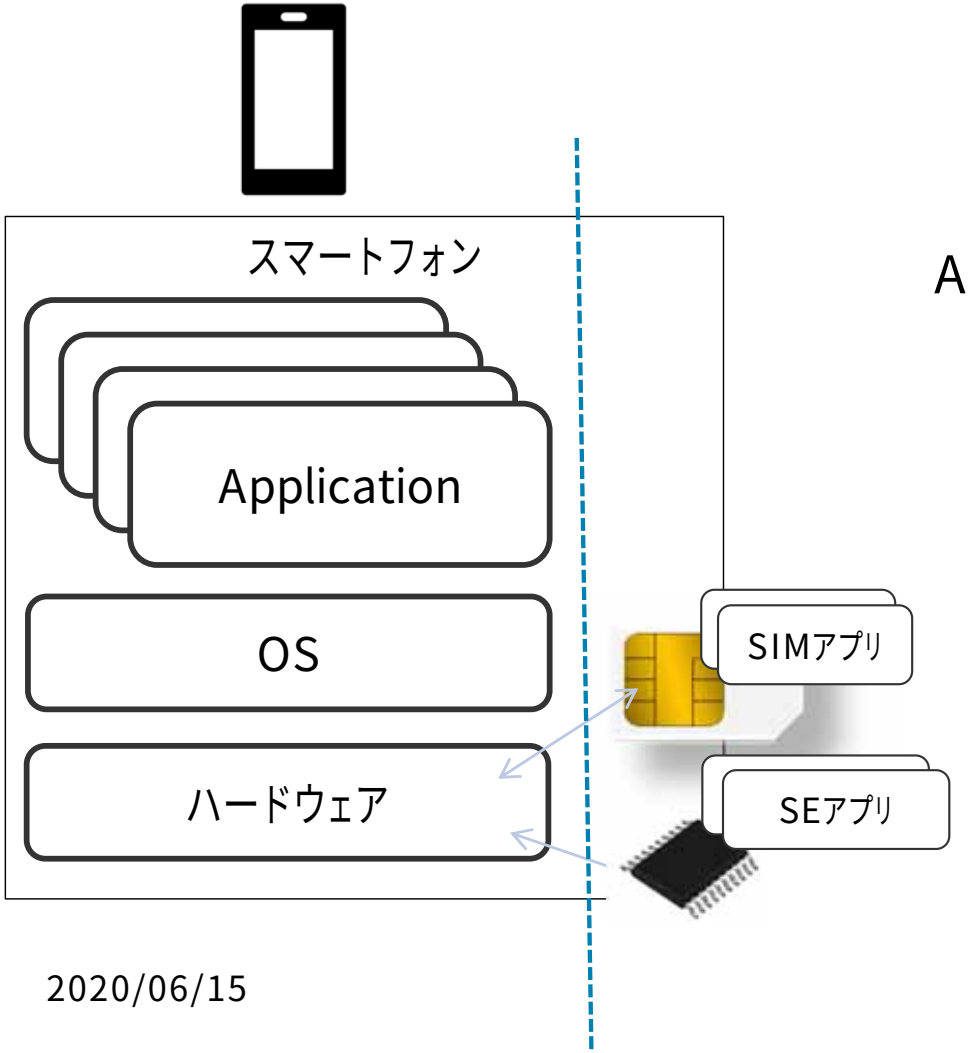


ストアにはAppleが審査したアプリがアップロードされるが、規定の審査とAndroidより厳しい安全性の審査がある。
アプリに署名はAppleが発行し、第三者が差し替えることができない仕組みがiOS上にある。

一方で、安全性のコントロールをAppleが行っているため、サービス提供者がコントロールできない。

スマホを安全にするしくみがある

スマートフォンの中には、別世界のICカードが入っている



SIMだけなく、セキュアエレメント（SE）も
新しいスマートフォンに入っている

SIMとSEは同じ筐体に入っているが、
Android/iOSとは切り離された別世界。
お互い実行されるアプリは干渉できない
（通信でやりとりはできる）

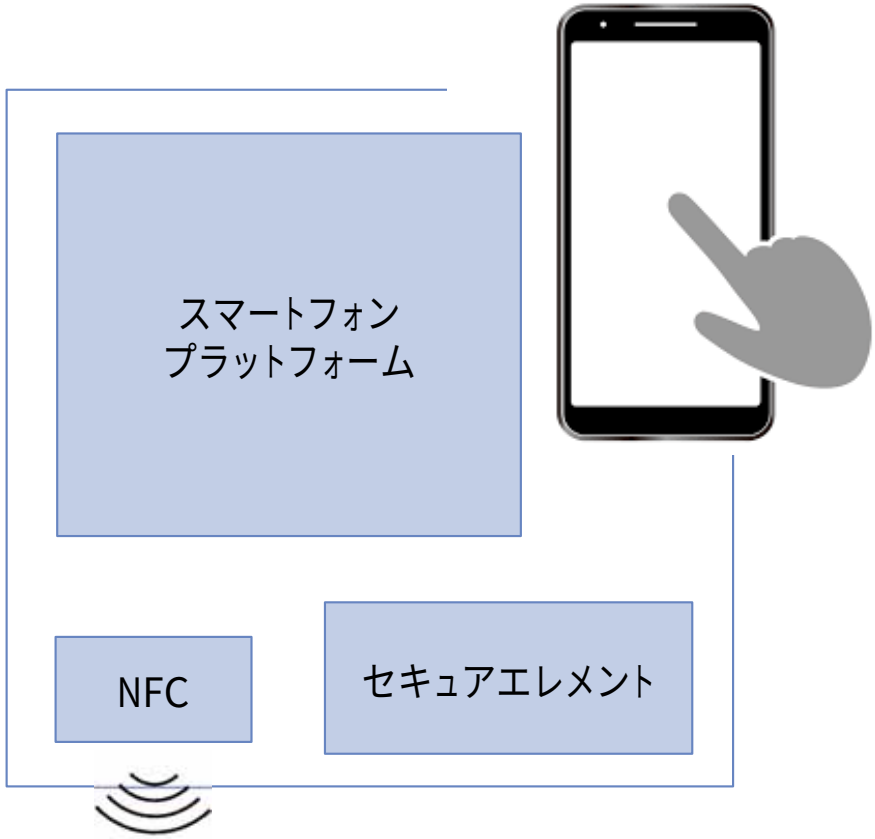
2020/06/15

セキュアエレメントとは

セキュアエレメント（Secure Element）は、耐タンパー性を持ち、アプリケーションや暗号データを安全に保管、処理することができる、セキュアICチップです。ICカードの業界標準であるGlobal Platformの認証や、EMVCo、Common Criteriaのセキュリティ認証などを取得しています。

Androidスマートフォンの一部のモデルや、iPhoneなどにセキュアレメントは搭載されています。

セキュアエレメントと合わせてスマートフォンに組み込まれるNFCコントローラは、NFC（Near FieldCommunication）のプロトコルをサポートし、外部の読み取り装置との通信を行い、読み取り装置からのデータをセキュアエレメントにルーティングすることで、セキュアエレメントと読み取り装置の間でのNFCによる通信処理をサポートします。



参考：
・GlobalPlatform：“Introduction to Secure Elements、”May 2018 https://globalplatform.wpengine.com/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf
・Google社 Android開発者向けサイト https://developers.google.com/android/security/android-ready-se
・Apple社 Appleプラットフォームのセキュリティ サイト
https://support.apple.com/ja-jp/guide/security/sec2561eb018/web

スマホ搭載のセキュリティコンセプト

マイナンバーカードと同等の安全性を保ちつつ、スマホならではの機能を積極的に活用

- マイナンバーの機能のうち、公的個人認証の機能をスマホで実現
  - マイナンバーカードとは別に、スマホ用の新たな電子証明書を発行する(次ページ図参照)

    ※そもそも公的個人認証サービスでは個人番号は使われない
  - 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）に基づく安全性を実現

- スマホに搭載されている機能の活用による公的個人認証サービス利便性の向上
  - 今後広く搭載が進むことが見込まれる耐タンパ性を有するモバイル端末向けセキュアエレメントを活用
    - 国際標準であるISO/IEC 15408、欧州eIDAS規則に基づく、CC認証獲得を検討する。

  - スマホの認証機能の活用による利便性向上
  - スマホの紛失、盗難を想定したセキュリティ対策の実施

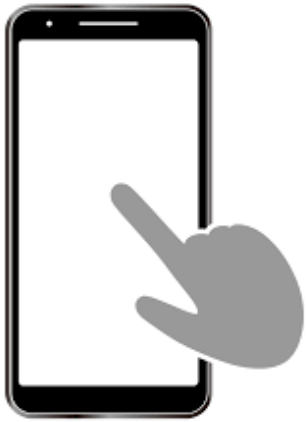
カードとスマホの電子証明書の関係

公的個人認証で利用するのは、
マイナンバーカードのICチップ内にある二つの証明書

- 利用者証明用電子証明書（本人確認用）
- 署名用電子証明書（電子署名用）

証明書を利用する際にはPINが必要
（利用者証明用と署名用は異なる）

マイナンバーカードはIAL3（SP 800-63A）レベルで
発行されているもの



<u>マイナンバーカードがなければスマホ用証明書は発行できない</u>
スマホ用電子証明書は、マイナンバーカードを
スマホにタッチすることで新規に発行される

- 利用者証明用電子証明書（スマホ用）
- 署名用電子証明書（スマホ用）

証明書を利用する際にはPINが必要（カードと別のスマホ用のもの）
（これも利用者証明用と署名用は異なる）

２つの電子証明書

引用元: https://www.soumu.go.jp/main_sosiki/kenkyu/mynumber_smartphone/index.html

マイナンバーカードに格納される公的個人認証サービスについて

公開鍵暗号方式

公的個人認証サービスが採用する暗号方式。秘密鍵と公開鍵はペアとなっており、片方の鍵で暗号化されたものは、もう一方の鍵でしか復号できない性質をもつ。

署名用電子証明書

（性質）
インターネットで電子文書を送信する際などに、署名用電子証明書を用いて、文書が改ざんされていないかどうか等を確認することができる仕組み

（利用局面）
e-Taxの確定申告等、文書を伴う電子申請等に利用される。

（利用されるデータの概要）

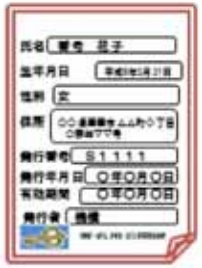
※電子署名法（平成12年法律第102号）の「電子署名」に該当し、同法第3条による「真正な成立の推定」の対象になり得る。

署名用秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ



※基本4情報を記録

利用者証明用電子証明書

（性質）
インターネットを閲覧する際などに、利用者証明用電子証明書（基本4情報の記載なし）を用いて、利用者本人であることのみを証明する仕組み

（利用局面）
マイナポータルのログイン等、本人であることの認証手段として利用される。

（利用されるデータの概要）

利用者証明用秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ

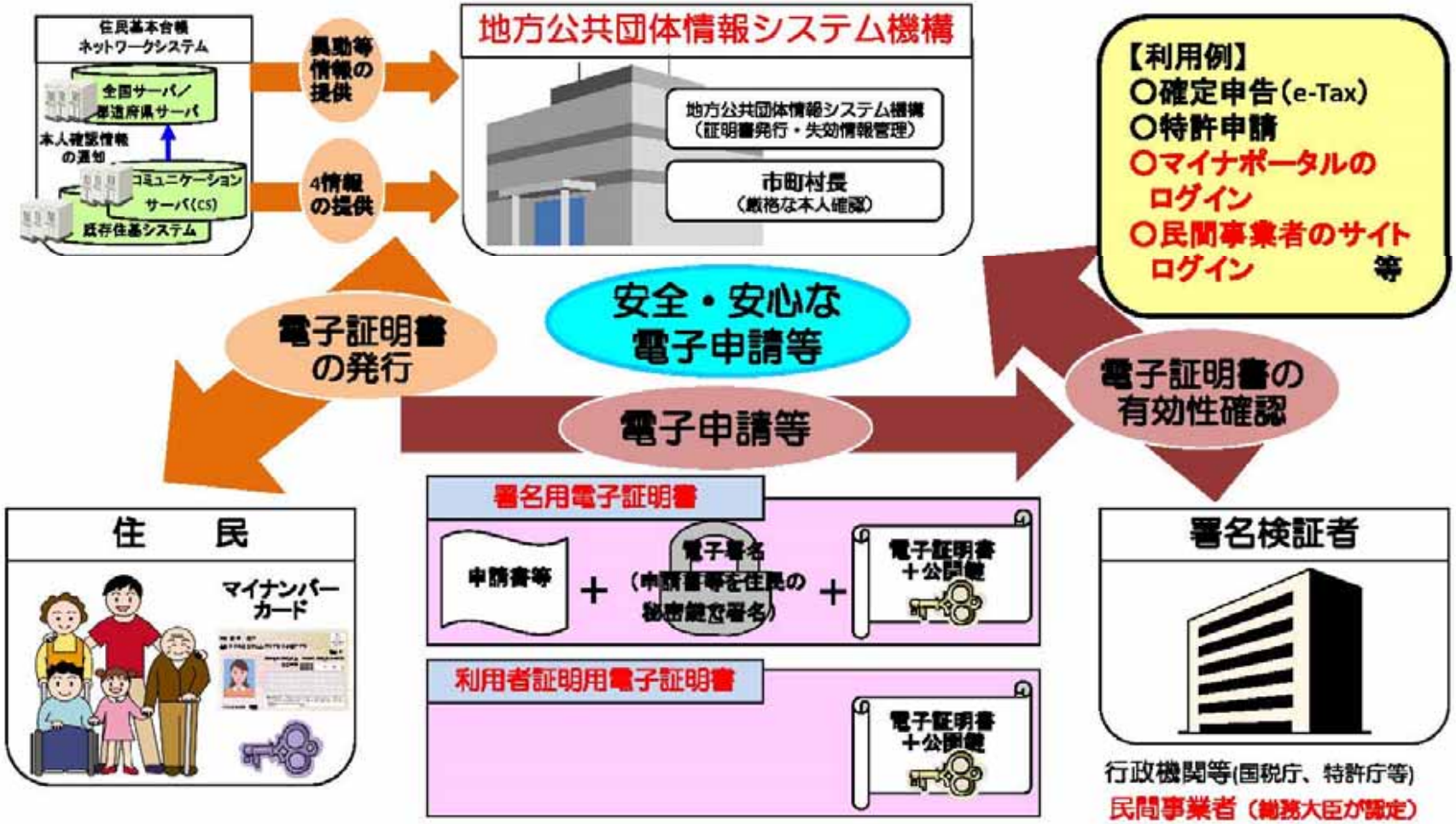
※基本4情報の記録なし

JPKIについて

引用元: https://www.soumu.go.jp/main_sosiki/kenkyu/mynumber_smartphone/index.html

公的個人認証サービスについて

○ オンラインでの行政手続等における本人確認のための公的サービス。
○ 成りすまし・改ざんを防ぎ、送信否認を担保するため、高いセキュリティを確保。



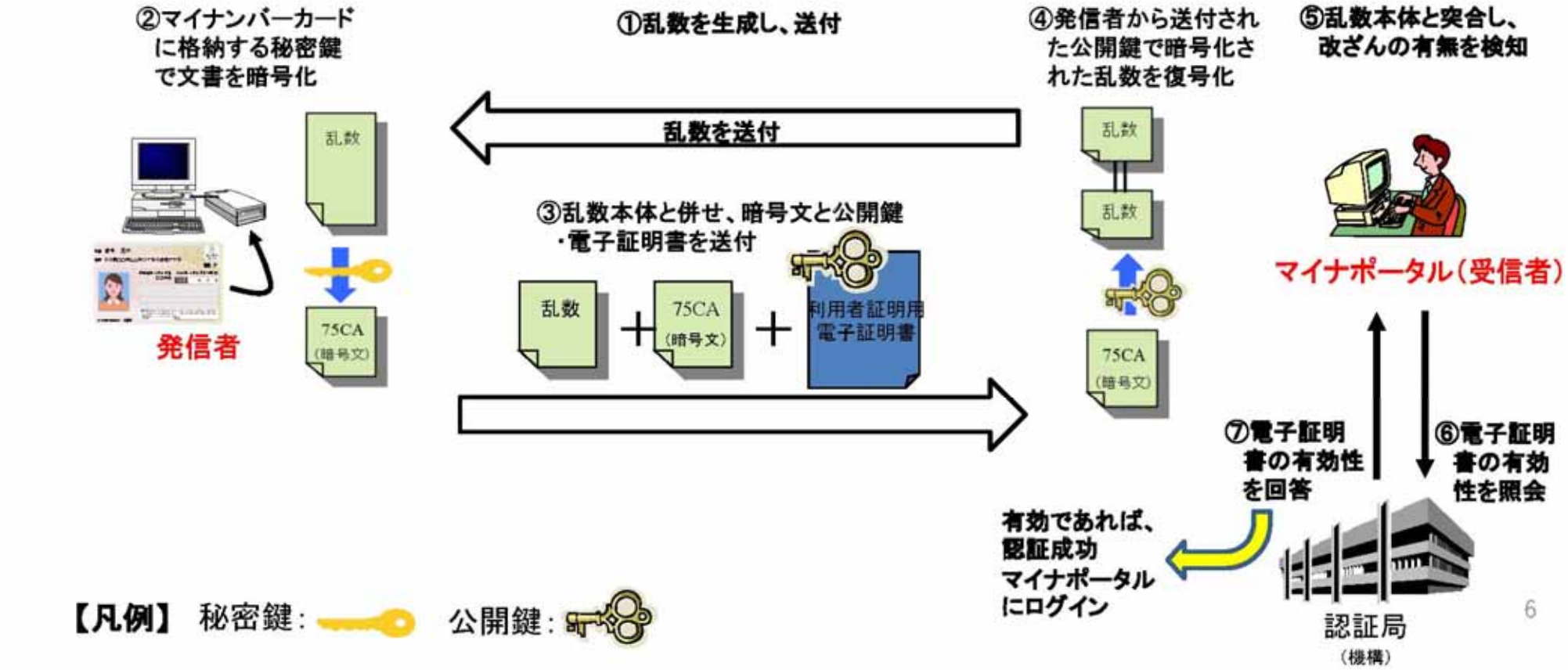
２つの電子証明書

引用元: https://www.soumu.go.jp/main_sosiki/kenkyu/mynumber_smartphone/index.html

公的個人認証サービスの仕組み（利用者証明用電子証明書）

（1）受信者から乱数を送付
（2）発信者がマイナンバーカードに格納されている秘密鍵を用いて文書を暗号化し、その秘密鍵とペアとなっている公開鍵とともに元の乱数、暗号化した乱数を送付。
（3）受信者は発信者から送付を受けた公開鍵を用いて暗号化した乱数を復号し、乱数本体と突合し、改ざんの有無を検知。
（4）受信者は送付を受けた利用者証明証電子証明書の有効性を確認。

【マイナポータルにおける例】



２つの電子証明書

引用元: https://www.soumu.go.jp/main_sosiki/kenkyu/mynumber_smartphone/index.html

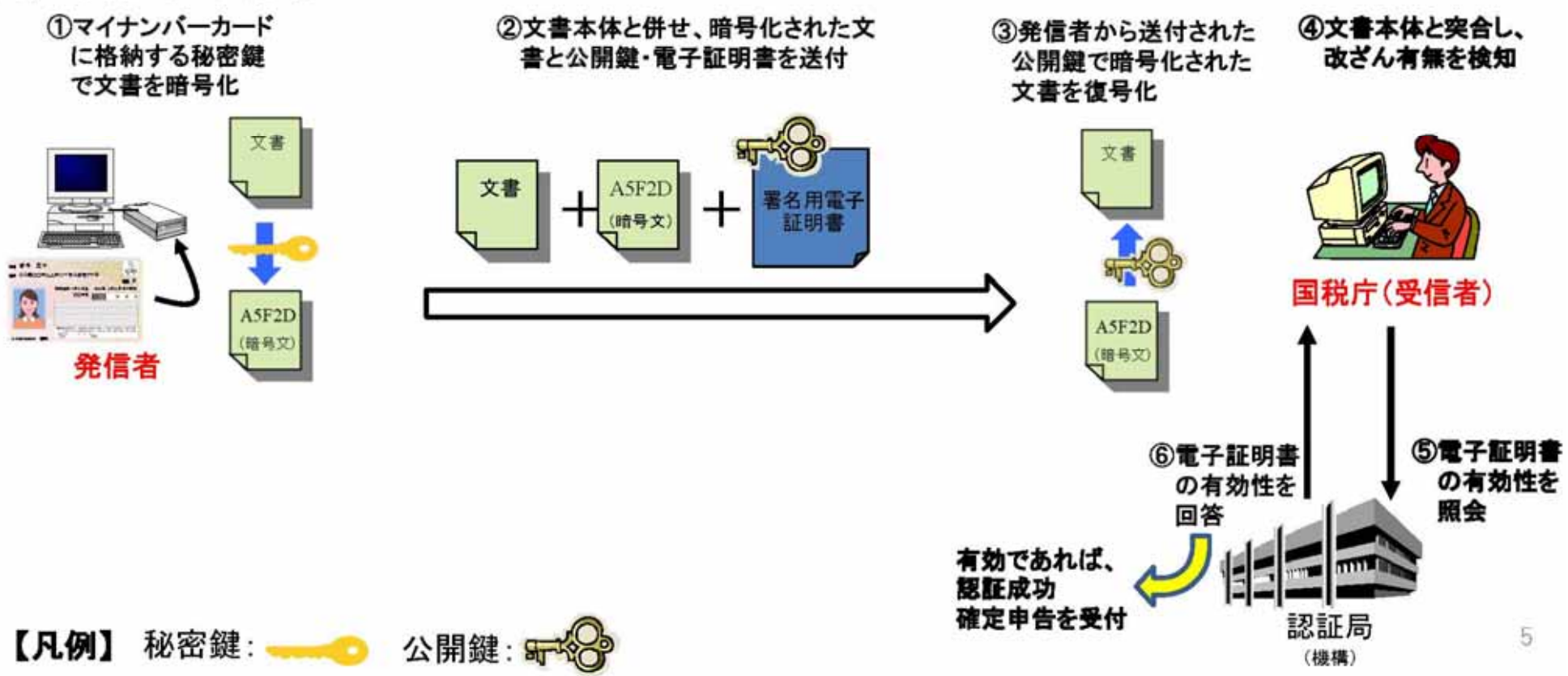
公的個人認証サービスの仕組み（署名用電子証明書）

（1）発信者がマイナンバーカードに格納されている秘密鍵を用いて文書を暗号化し、その秘密鍵とペアとなっている公開鍵とともに元の文書、暗号化した文書を送付。

（2）受信者は発信者から送付を受けた公開鍵を用いて暗号化した文書を復号し、文書本体と突合し、改ざんの有無を検知。

（3）受信者は送付を受けた署名用電子証明書の有効性を確認。

【確定申告における例】



２つの電子証明書

引用元: 第二次とりまとめ
https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000332.html

基本方針４ 安全・安心に利用できる高いセキュリティ

16

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。

２つの電子証明書

引用元: 第二次とりまとめ
https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000332.html

基本方針３ スマホならではの使いやすいUX

12

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。

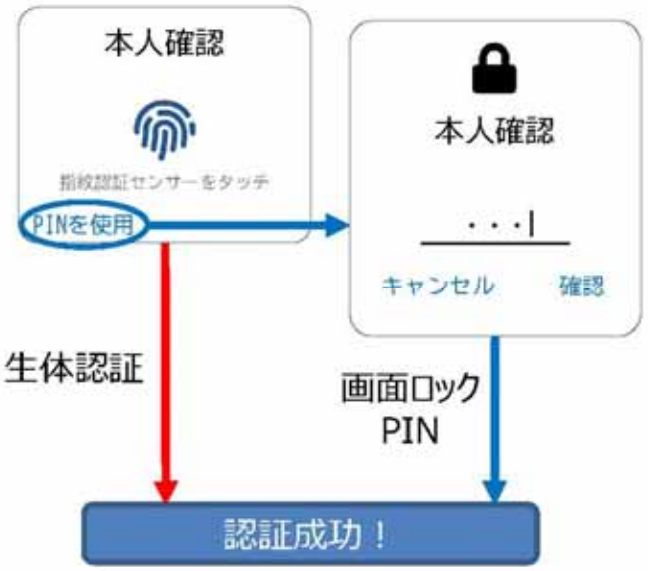
スマートフォン用電子証明書で利用可能な認証手段

	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）



２つの電子証明書

引用元: 第二次とりまとめ
https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000332.html

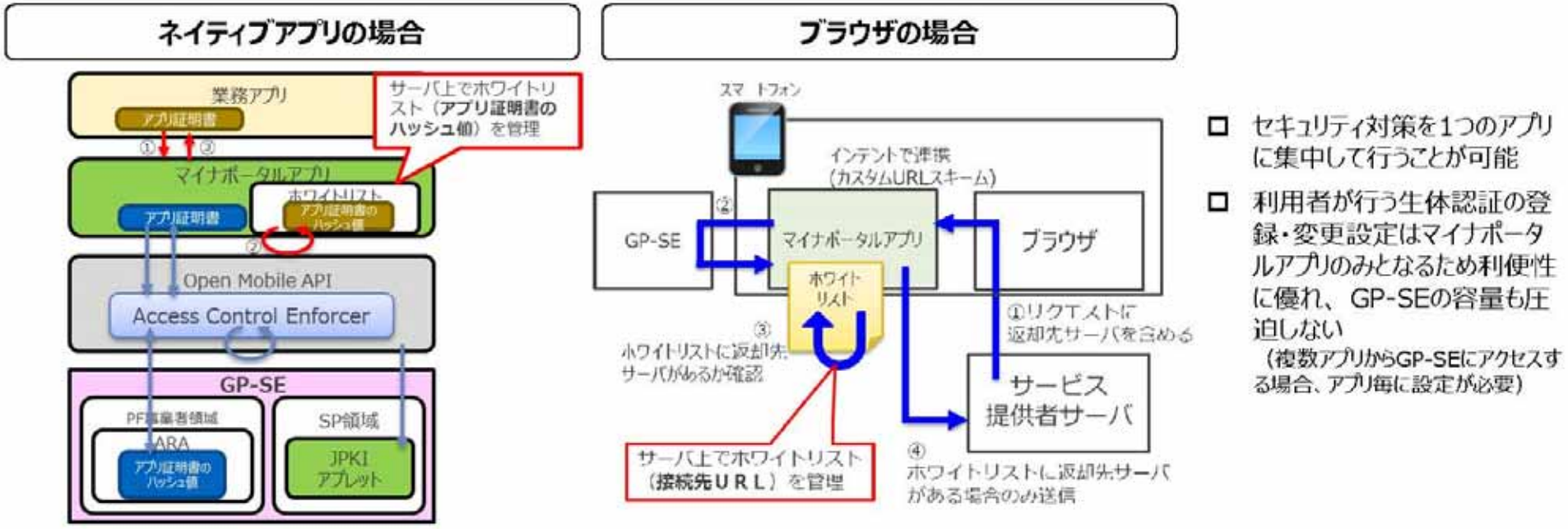
基本方針３ スマホならではの使いやすいUX

15

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。



スマホ搭載、構成

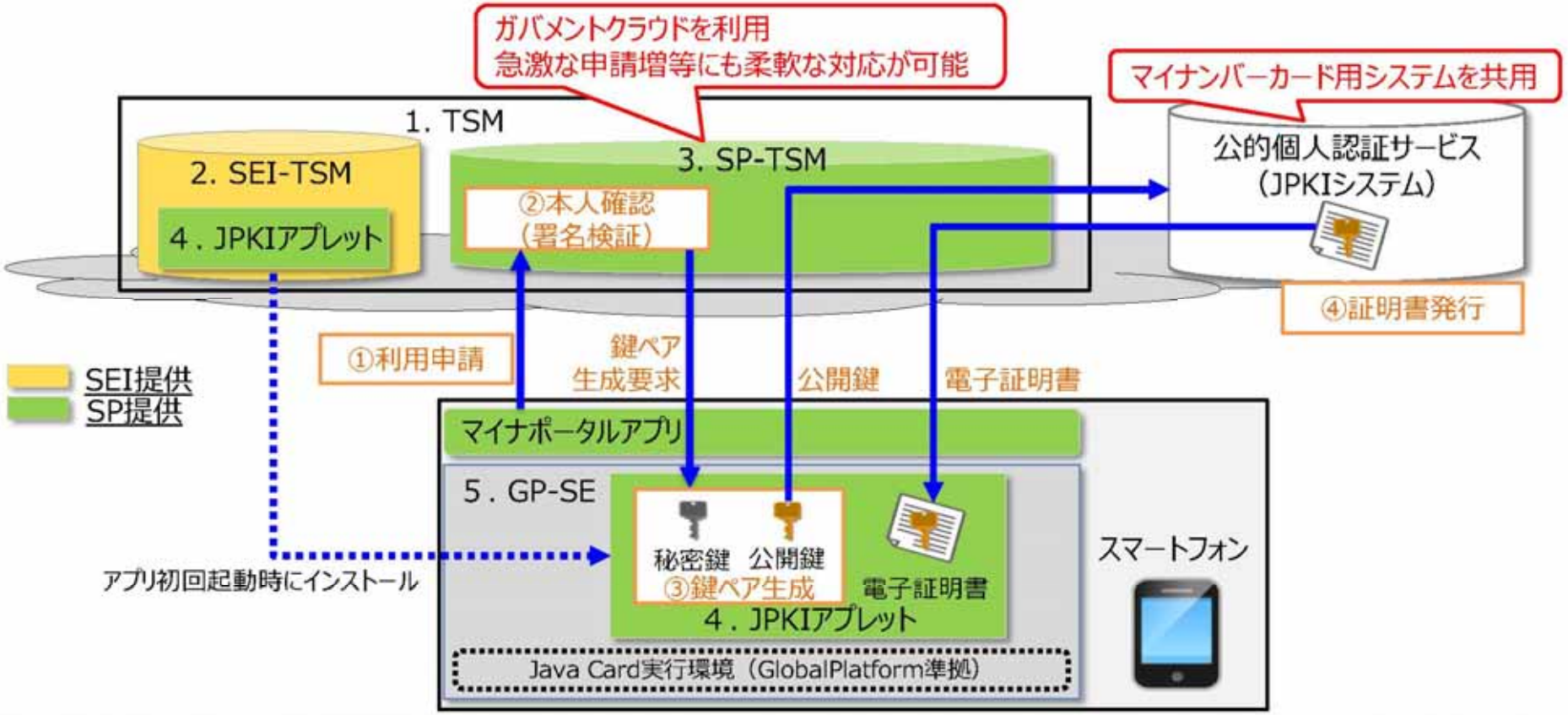
引用元: 第二次とりまとめ
https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000332.html

スマートフォン搭載を実現するためのシステム構成

3

■ 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。