別紙

第１次とりまとめ
～電子証明書のスマートフォン搭載の実現に向けて～

令和2年12月25日

「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

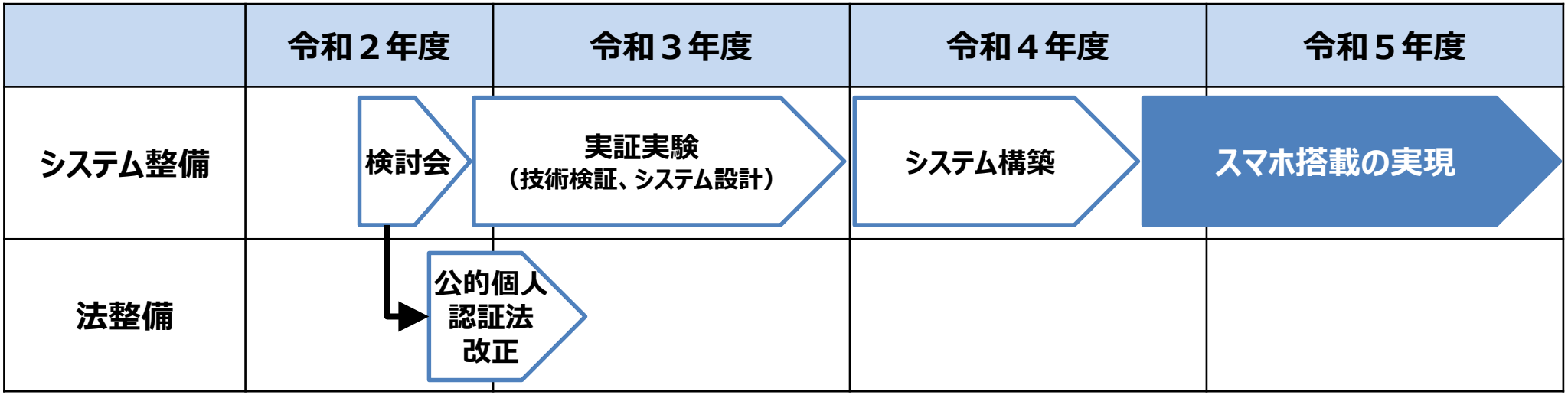
- スマホへの搭載の実現にあたり、国際的にサポートされていないガラパゴスな方式を採用した場合には、結果的に対応可能なスマホの機種が限定され、広く普及が進まないおそれがある。そのため、具体的な実現方式の検討にあたっては、グローバルスタンダードへの対応を図るとともに、現実的な普及可能性を十分考慮する。
- さらに、デジタルIDや電子署名に係る国際的な動向を踏まえ、利用者の利便性向上の観点から不断に見直しを行っていく必要がある。

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

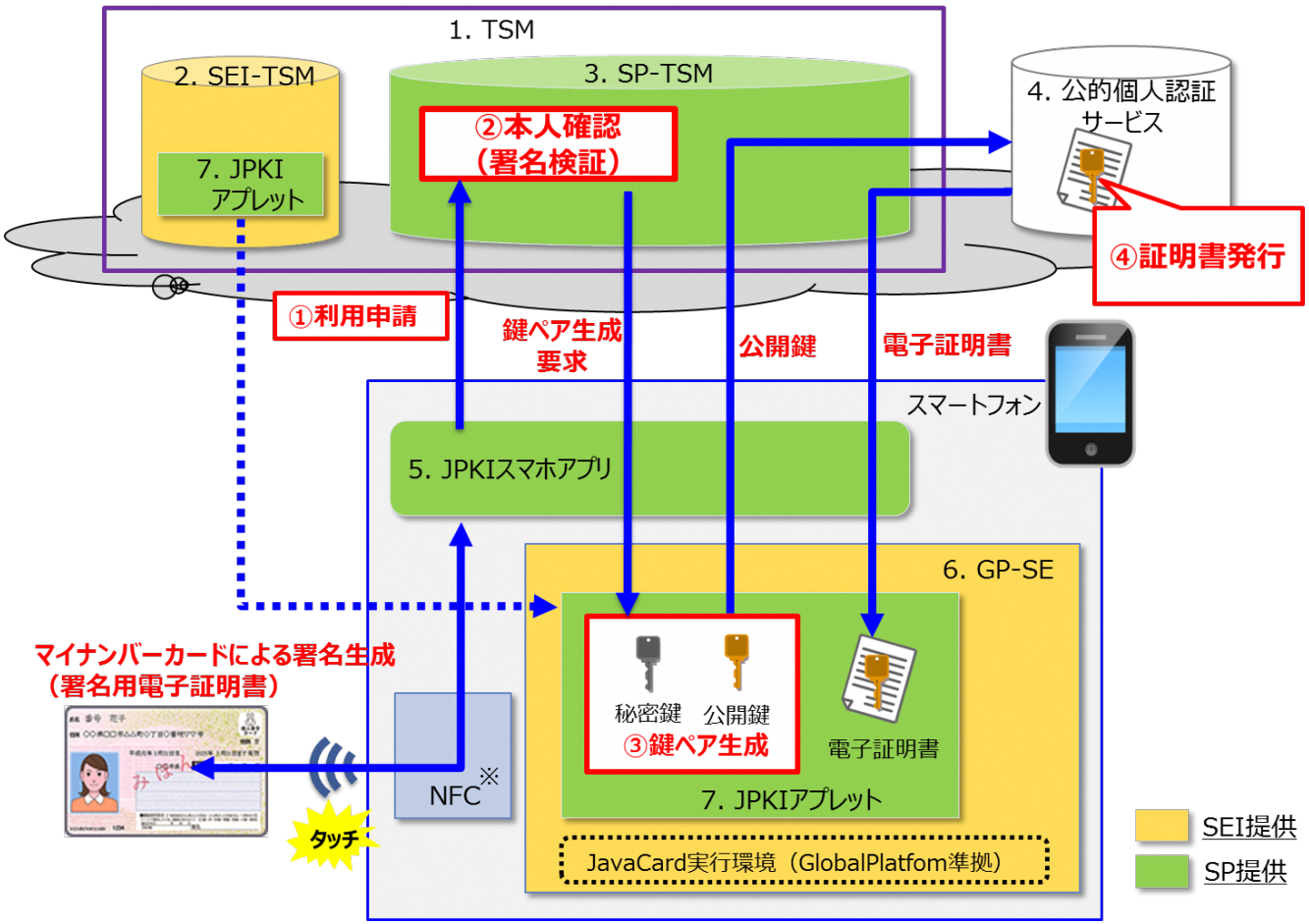
- **令和４年度内にAndroid端末への搭載を目指す。**
- 必要な制度整備を行うため、**次期通常国会に公的個人認証法改正案を提出。**
- **iPhoneについても早期実現を目指す。**



参考資料

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。

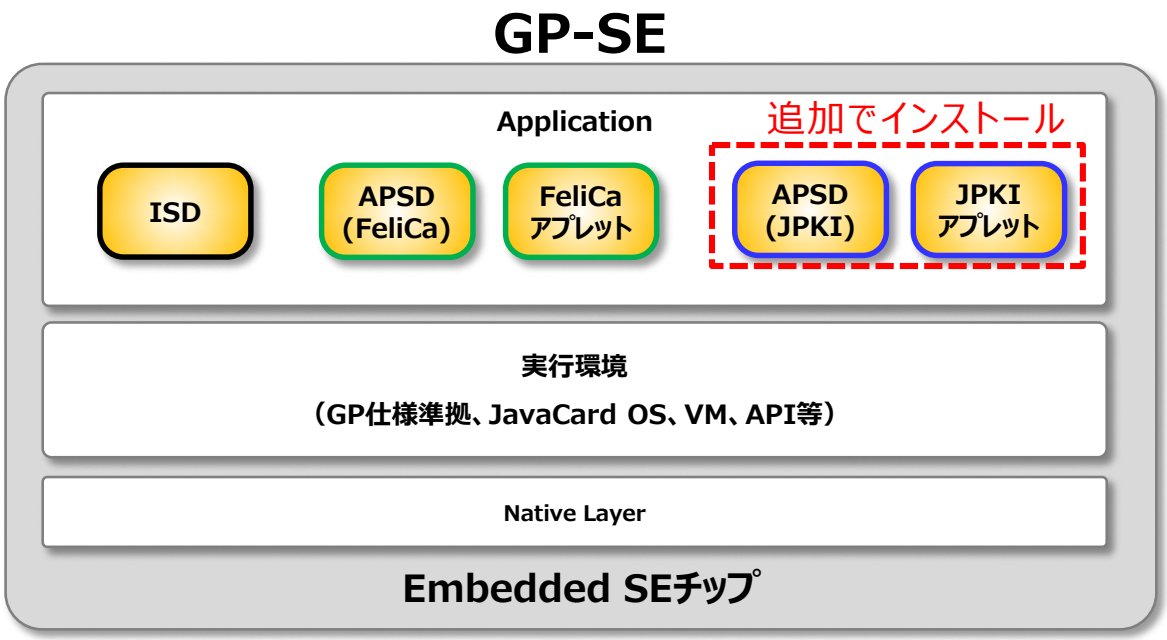
GP-SEの概要

【GP-SEとは】

GP-SEとは、スマートフォン等の本体基板に埋め込まれたSecure Element（SE）であり、GlobalPlatform（GP）仕様に対応したJavaCard実行環境をプラットフォームとして有し、サービス提供者が開発したJavaアプレットをインストールして動作させることが可能なICチップである。GP-SEのチップ概要とソフトウェア構成図を以下に示す。JPKI機能を実装するJavaアプレットをインストールすれば、マイナポータルへのログイン認証、住民票等のコンビニ交付がスマートフォンで利用できるようになる。

【普及状況】

GP-SEは、フェリカネットワークス社によって開発され、2019年春モデルよりGP-SEを搭載したスマートフォンが販売開始された。2020年4月には国内の新規発売されたAndroidスマートフォンの約30%がGP-SE搭載スマートフォンとなっており、今後も普及拡大が進む見込みである。現状ではFeliCa機能を実装するFeliCaアプレットがプリインストールされた状態で出荷され、Suica、iD、QUICPay等の決済サービスで利用されている。

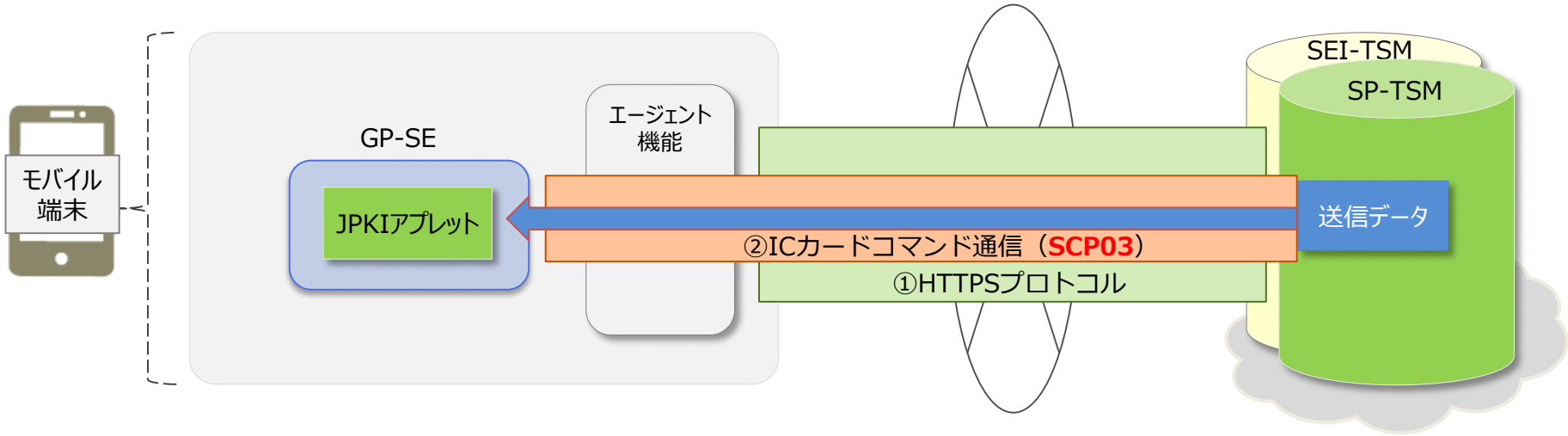


- **ISD: Issuer Security Domain**
  発行者用のSecurity Domain（SD）。主に発行者関連のコンテンツ管理を行う。新たにAPSDを作成したい場合、ISDから承認を受け作成しなければならない。
- **APSD: Application Provider Security Domain**
  SEに独自のアプリケーション（左図のFeliCaアプレットやJPKIアプレット）をインストールするときに必要なSD。
- **JPKIアプレット**
  JPKI機能を実装するアプレット。スマホ用電子証明書・秘密鍵を格納する。
- **FeliCaアプレット**
  FeliCaのファイルシステム、コマンド処理、暗号処理等を行うアプレット。

GP-SEのセキュリティ機能①

（1）セキュアチャネルプロトコル

GP-SEとTSMとの間は、セキュアチャネルプロトコル（SCP03）によってデータ通信が実施される。SCP03は、GlobalPlatformによって定めれた暗号通信プロトコルであり、GP-SEとTSMの2者間での鍵共有と暗号化されたデータを送受信するため、経路途中のデータがスキミングされたとしても解読、改ざんが極めて困難。



（2）GP-SEの暗号機能

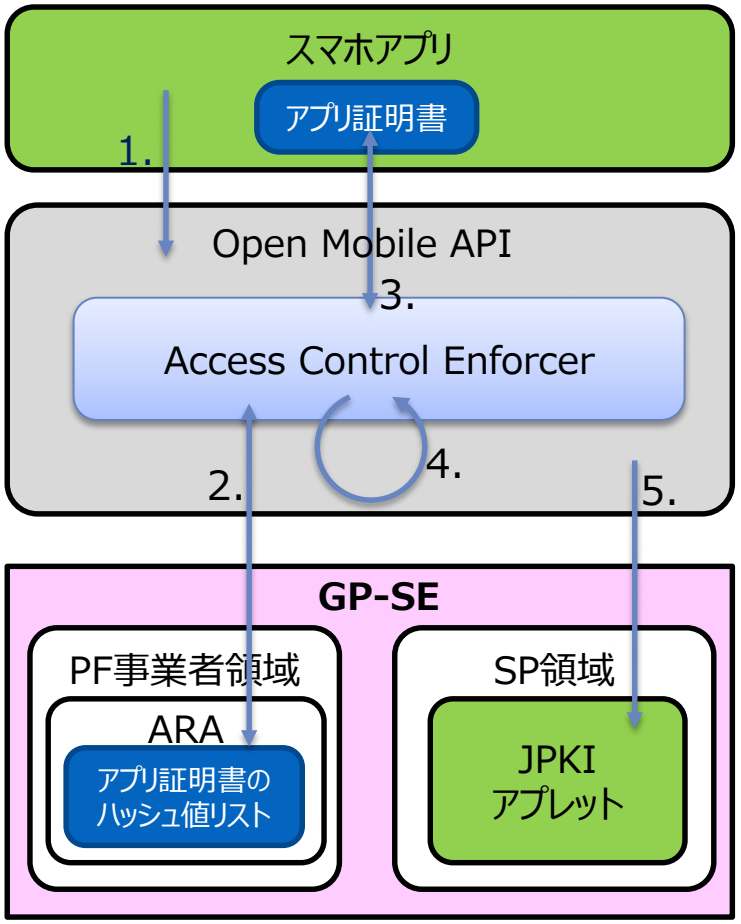
GP-SEは、公的個人認証サービスで要求される以下の暗号アルゴリズムに対応している。また、RSA2048bitの鍵ペア生成も可能となっている。

No.	暗号アルゴリズム	サポート状況	備考
1	RSA2048bit	○	署名はRSASSA-PKCS#1_v1.5に対応
2	AES128bit	○	SCP03の暗号化プロトコル
3	乱数生成	○	SCPで使用

GP-SEのセキュリティ機能②

（3）スマホアプリからのアクセスに関するセキュリティ機能

GP-SE内に格納されたアプレット（JPKIアプレット）は、下図の仕組みによりアクセス元アプリケーションの認証を行なうことで、正当なAndroidアプリケーション（スマホアプリ）のみがアクセス可能となっている。この仕組みにより、第三者がGP-SEにアクセス可能なスマホアプリを作ることは極めて困難である。



【参考】GlobalPlatform, Secure Element Access Control v1.0

■アプレットにアクセスできるアプリケーションリストの登録方法

1. SPは、JPKIアプレットにアクセスできるアプリケーションのホワイトリスト（Androidアプリケーションの証明書ハッシュ値リスト）を作成し、SEI-TSMに登録しておく。
2. SEI-TSMがJPKIアプレットをGP-SEに格納する際に、上記のリストをARA（Access Rule Application）に格納する。

■認証手順（番号は左図に対応）

1. スマホアプリがOpen Mobile APIにアクセスする。
   Open Mobile API： GP仕様に準拠したGP-SE内のセキュアな領域にアクセスするために提供されているAndroid用API
2. Open Mobile API内部のACE（Access Control Enforcer）がPF事業者領域内のARA（Access Rule Application）から、アクセスルールを取得する。
3. ACEは、アクセス元のAndroidアプリケーションに付与されている公開鍵証明書のハッシュ値を算出する。
4. ACEは、手順2と手順3で取得したハッシュ値を比較する。一致した場合は、正しいアプリケーションからのアクセスであると判断する。
5. 手順4で一致した場合は、手順1で要求されたOpen Mobile API処理が実行される。

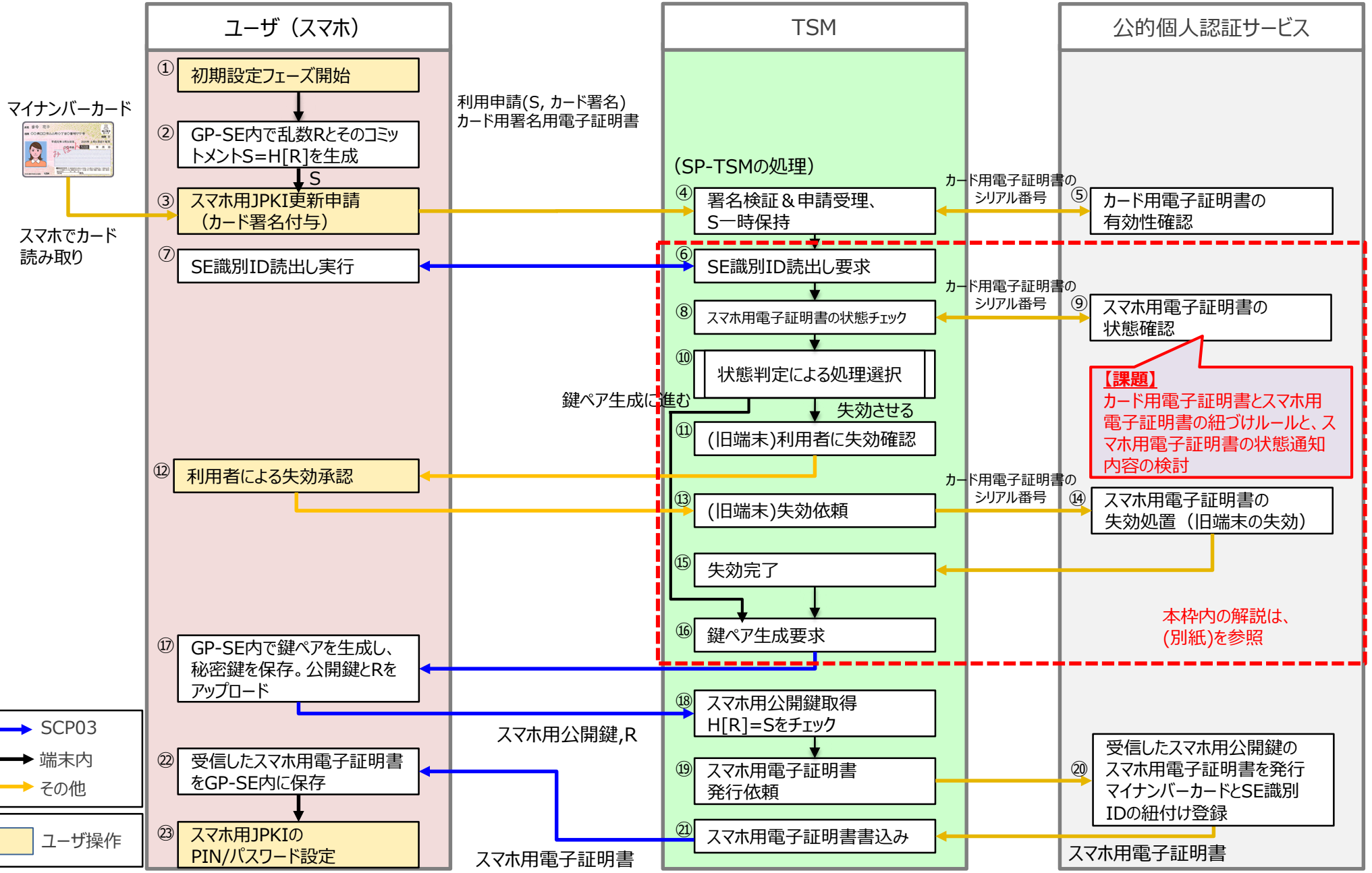
GP-SEのセキュリティ評価

GP-SEでは、プラットフォーム（HW＋OS）としてCC認証又はEMV認定を取得したICチップが採用されている。マイナンバーカードとGP-SEのセキュリティ評価に関する比較表を以下に示す。

項目	マイナンバーカードのセキュリティ評価（CC認証）	GP-SEプラットフォームのセキュリティ評価	
		CC認証（HW＋OS）	EMV認定（HW+OS）
セキュリティ要件	ISO/IEC 15408に基づいて作成されたプロテクションプロファイル（公開） EAL4+（AVA_VAN.5）	ISO/IEC 15408に基づいて作成されたプロテクションプロファイル（公開） EAL4+（AVA_VAN.5）	EMVCoが定めるSecurity Guideline（非公開） EAL4+（AVA_VAN.5）
評価の範囲	製品の評価及びその開発プロセスを含んだ評価	製品の評価及びその開発プロセスを含んだ評価	
脆弱性評価	JIWG文書（※1）で示される攻撃への対抗	JIWG文書（※1）で示される攻撃への対抗	
有効期間	認証取得国による	認証取得国による	1年（再評価後1年、最長6年）
評価機関	認証機関が認定した評価機関	認証機関が認定した評価機関	EMVCoが認定した評価機関
認証機関	認証制度に基づく認証機関（公的機関）	認証制度に基づく認証機関（公的機関）	EMVCo

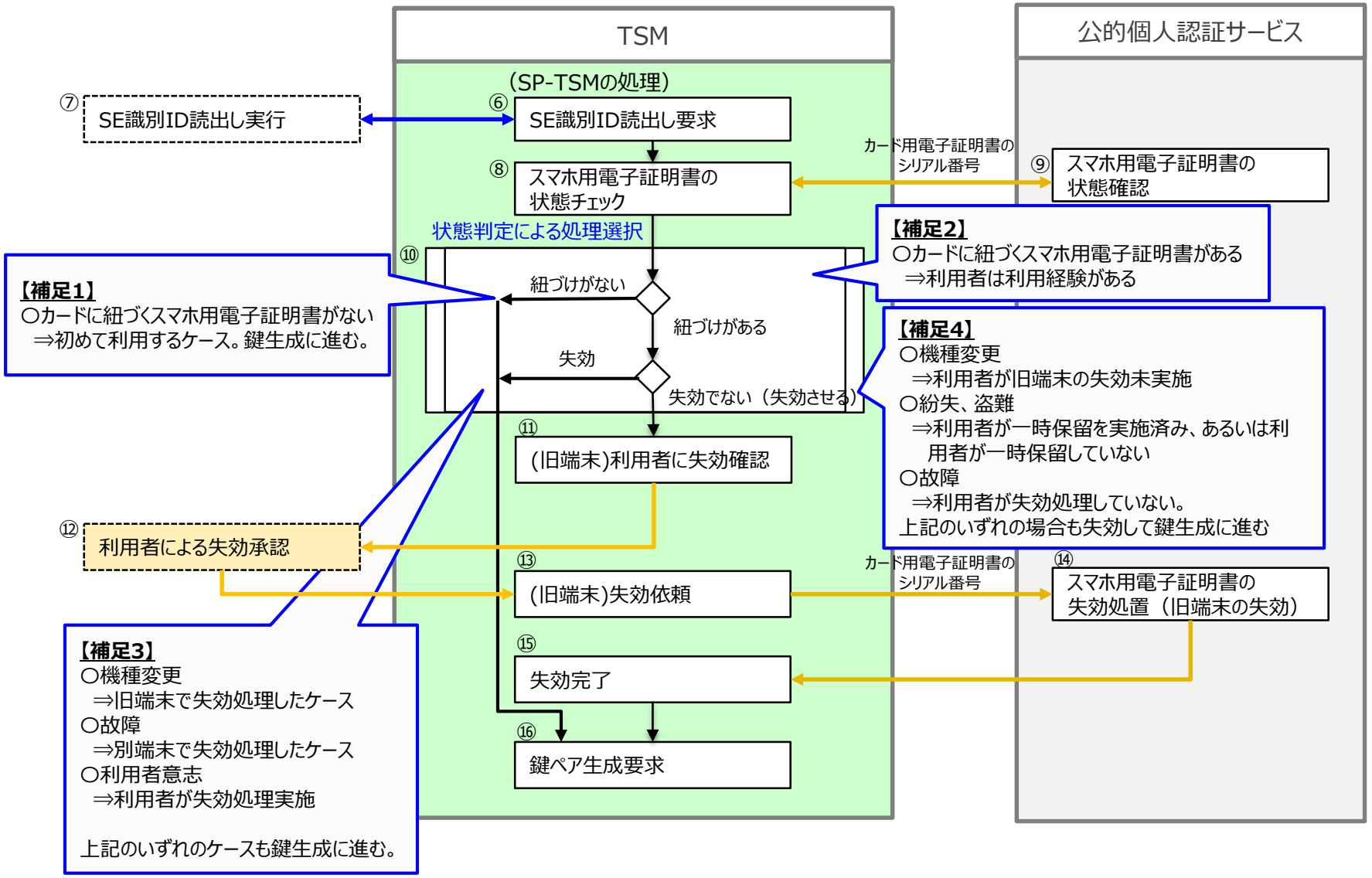
GP-SEのCC認証、EMV認定では、脆弱性分析においてはマイナンバーカードと同様に最高レベルであるAVA_VAN.5を達成している。GP-SEはマイナンバーカードと同等レベルの耐タンパ性を有するものと評価できる。

スマホ用電子証明書の発行フロー①



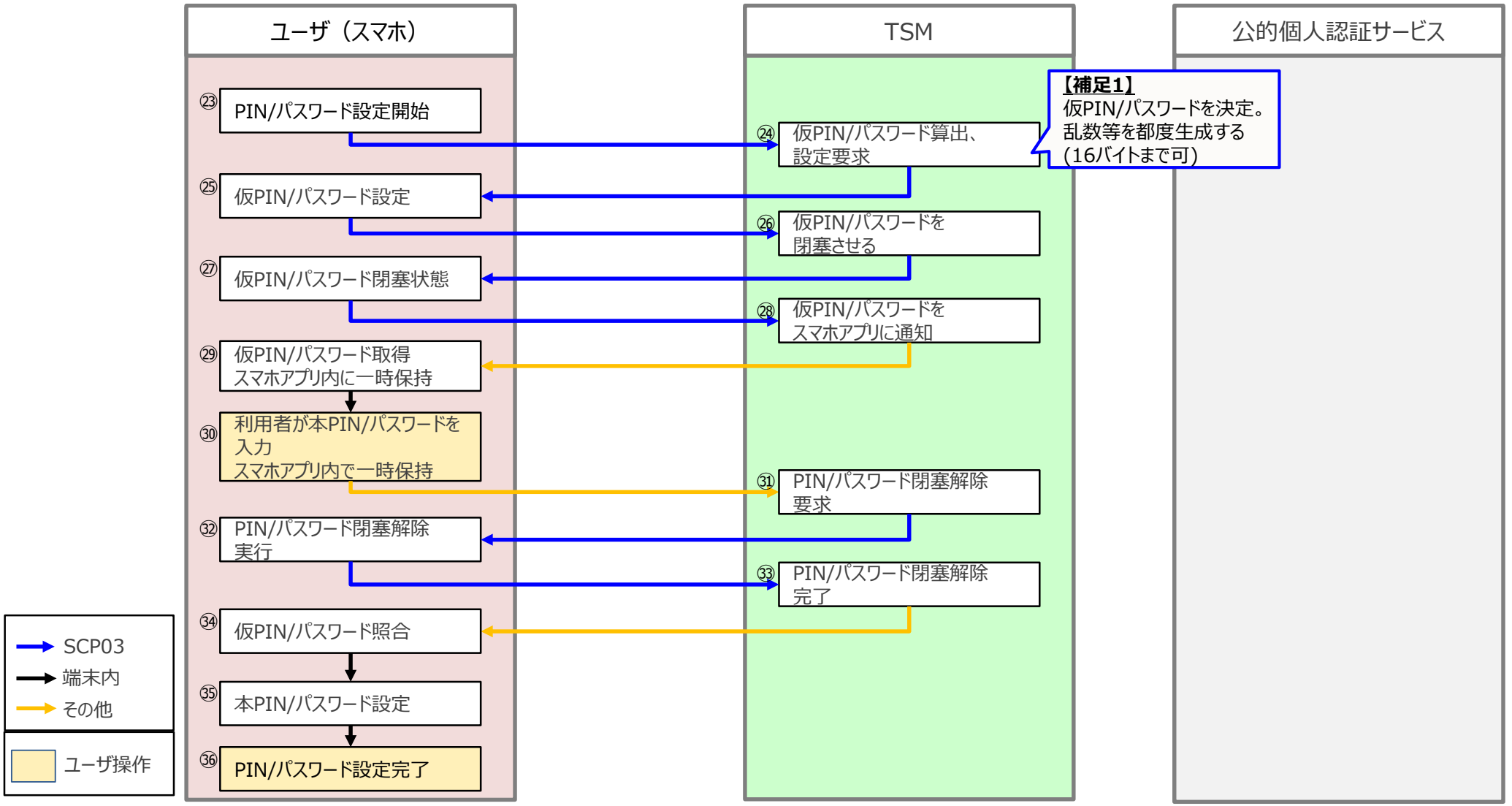
スマホ用電子証明書の発行フロー②（別紙）

前ページの赤枠部分に係るスマートフォン特有のライフサイクルとの関係



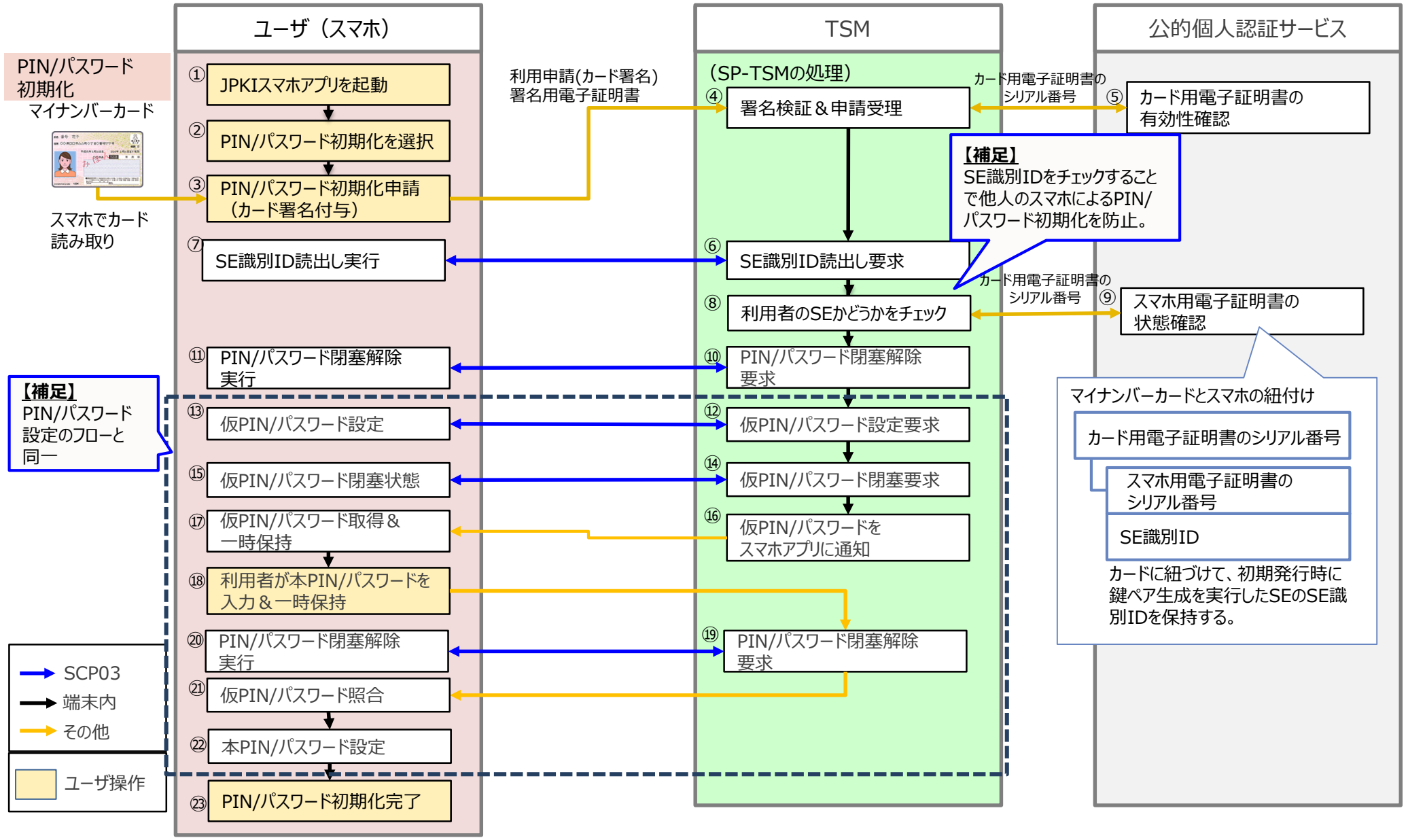
PIN/パスワードの初期設定フロー

・スマホ用電子証明書の発行フロー㉓から開始。発行フローの続きとして一連のセッションで実行（カード署名が有効のセッション）。
・仮PIN/パスワードはシステム内で使用するが、利用者は仮PIN/パスワードの存在を意識することはない。



PIN/パスワードの初期化フロー

カードの署名検証（本人確認）によってPIN/パスワード初期化が実行できるものとする（オンラインで実施可能）。

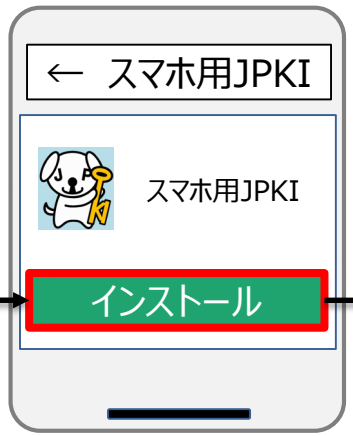


各業務におけるユーザ操作イメージ①

フェーズ１　アプリ準備

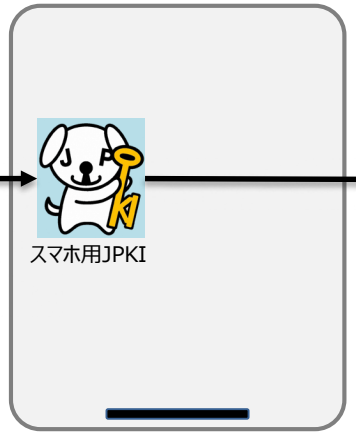
①アプリを検索

②アプリをインストール



フェーズ２　アプレット準備

③アプリを初回起動



JPKIアプレット
存在チェック

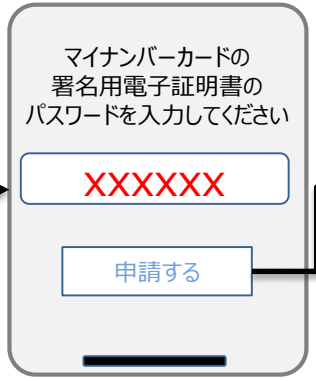
【補足】
中古端末を使用した
場合等で残留している
アプレット等を削除。

④アプレット準備完了
初期設定へ

フェーズ３　初期設定

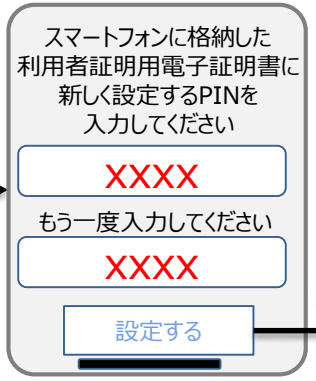
①発行手続を開始

②カード用署名用電子証明書のパスワードを入力

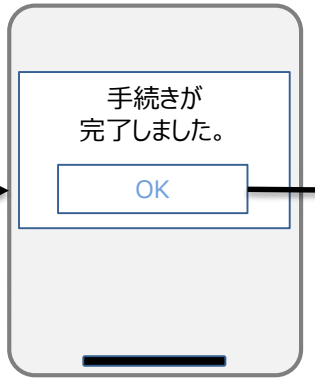


③マイナンバーカードをかざして電子署名を付与

④スマホ用電子証明書のPIN/パスワードを設定



⑤初期設定フェーズ完了



⑥利用フェーズ開始

各業務におけるユーザ操作イメージ②

フェーズ４　サービス利用・証明書管理

①メニューを選択

マイナポータル
ログイン

電子証明書管理

**②スマホ用
利用者証明用電子証明書の
PINを入力してログイン**

スマートフォンに格納した
利用者証明用電子証明書の
PINを入力してください

XXXX

ログイン

**③マイナポータル
ログイン完了**

マイナポータル

健康保険証利用の申込

利用を申し込む

・
・
・

②手続を選択

更新・再発行

失効

一時保留解除

PIN/PW初期化

PIN/PW変更

**③カード用
署名用電子証明書の
パスワードを入力**

マイナンバーカードの
署名用電子証明書の
パスワードを入力してください

XXXXXX

変更する

**④マイナンバーカードを
かざして電子署名を付与**

マイナンバーカードを
NFC読取位置に
密着させてください

**⑤スマホ用電子証明書の
PIN/パスワードを入力**

スマートフォンに格納した
利用者証明用電子証明書に
新しく設定するPINを
入力してください

XXXX

もう一度入力してください

XXXX

設定する

⑥手続完了

手続きが
完了しました。

OK

⑦メニューに戻る

マイナポータル
ログイン

電子証明書管理

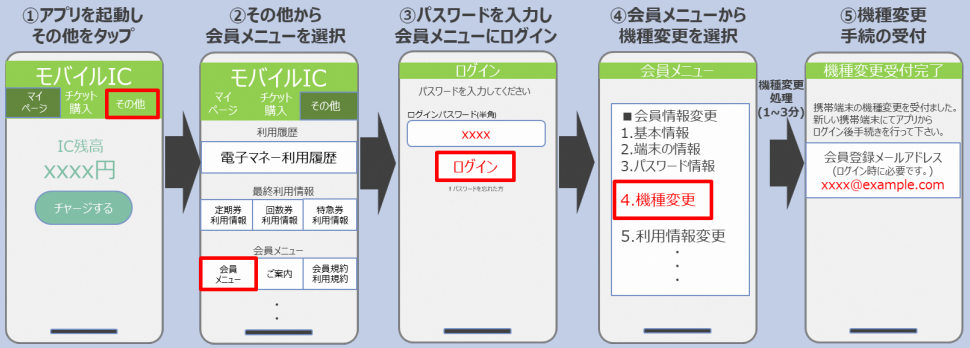
※手続の一例として
更新・再発行の場合を明示

機種変更時における交通系ICカードアプリとの比較

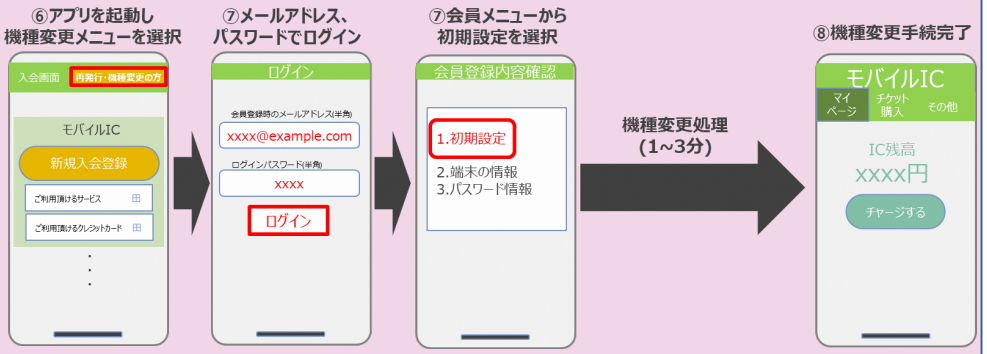
交通系IC

スマホ用JPKI

旧端末



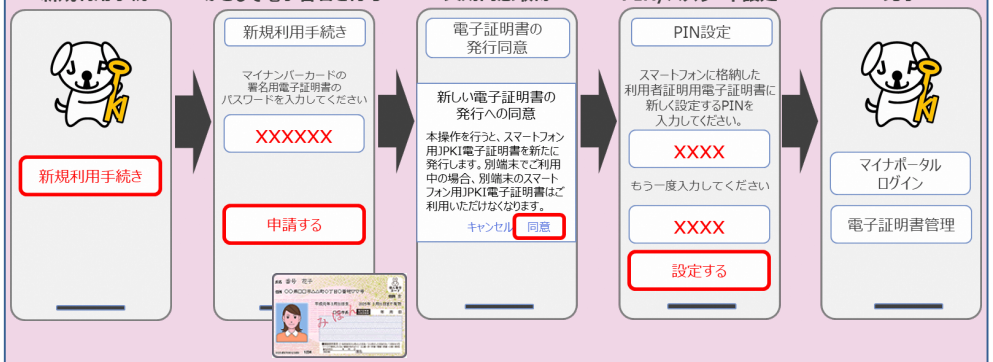
新端末



機種変更後もスマホ用JPKIを利用するために、
旧端末での操作は不要。

新端末での新規利用手続において、
旧端末の電子証明書の失効手続もあわせて実施。

※旧端末に残る電子証明書や秘密鍵が悪用されないよう、
旧端末での操作により削除できる手段を別に用意



旧端末に搭載した電子証明書及び秘密鍵の悪用防止

・機種変更や譲渡・紛失等により、スマホ（旧端末）に搭載した電子証明書の利用を以後停止する場合、
①旧端末に搭載した電子証明書を失効させることが必要（※法律上は利用者に失効申請義務を課すことを想定）。
②また、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、
これらの電子証明書や秘密鍵が適切に削除されることが望まれる。

カードの場合と同様に罰則の伴わない「義務」とする想定のため、実際には申請しない利用者も想定される

新端末に電子証明書を搭載する場合

機種変更の場合や、譲渡・紛失等に伴い新たな端末を購入した場合等において、利用者が新端末でもスマホ用電子証明書を搭載・利用する場合

失効手続

削除措置

旧端末に搭載した電子証明書の利用を以後停止

新端末での新規利用手続において、旧端末の電子証明書の失効手続をあわせて実施 **【対策１－１】**

旧端末の電子証明書の失効を受けて、リモートで旧端末の電子証明書や秘密鍵を削除 **【対策１－２】**

【課題２】
失効は完了。
スマホが通信できない場合等削除されないケースが存在

旧端末での手続を勧奨

法律上は利用者に失効申請義務（想定）

【旧端末で手続を行う場合】

旧端末から（任意の）失効申請を実施 **【対策２－１】**

旧端末の失効申請を受けて、旧端末内の電子証明書や秘密鍵を削除 **【対策２－２】**

失効、削除とも完了

新端末に電子証明書を搭載しない場合

新端末ではスマホ用電子証明書の利用を行わないと判断した場合や、スマホの利用自体を取り止めた場合

紛失の場合等旧端末が手元にない、あるいは旧端末が手元にあっても実際には申請しない利用者を想定

PIN/パスワードで保護されている

【旧端末で手続を行わない場合】

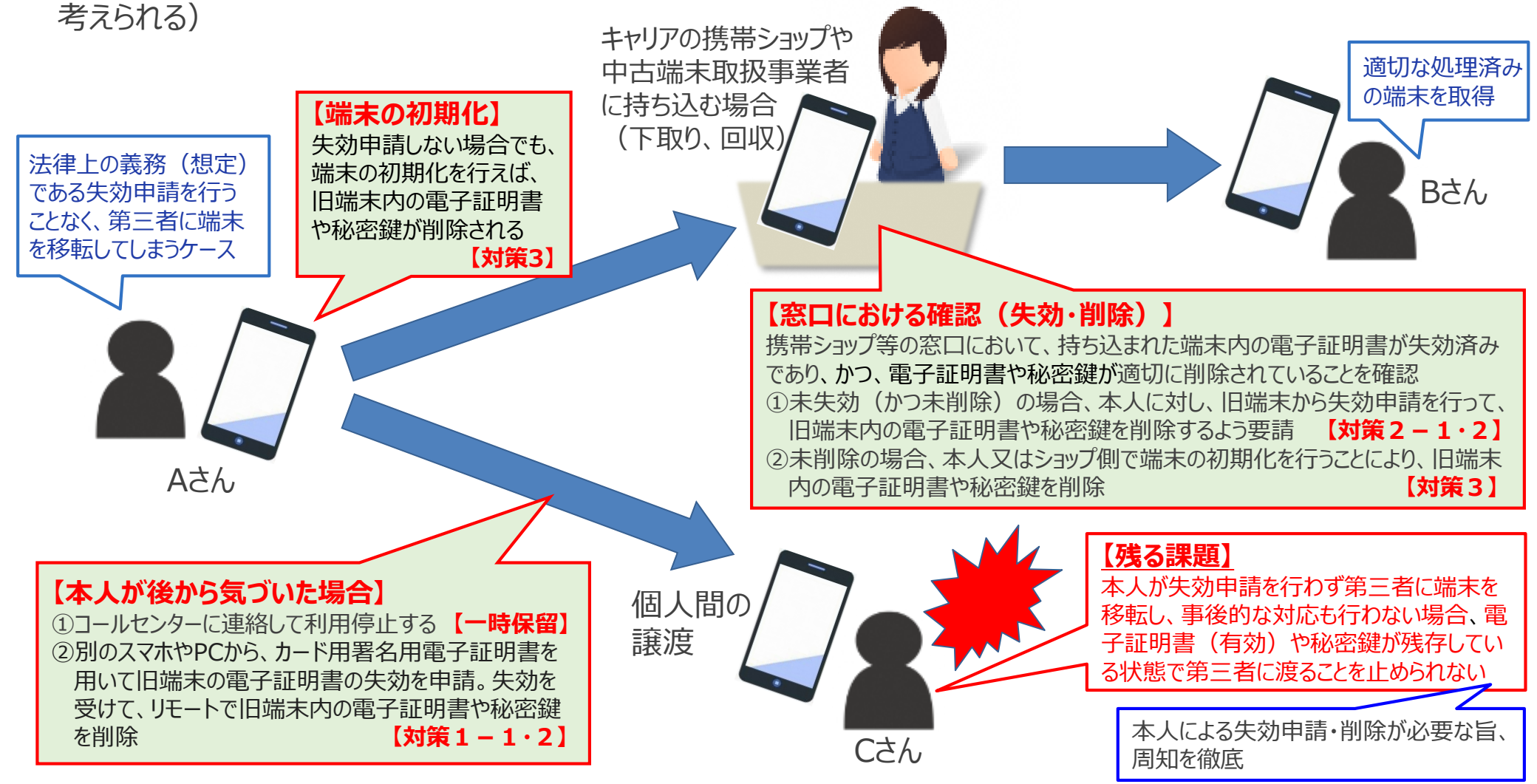
（旧端末の電子証明書は失効していない状態）

（旧端末の電子証明書や秘密鍵は削除されていない状態）

【課題１】
端末内に未失効の電子証明書が残存する状態で第三者に移転するリスク

端末内に未失効の電子証明書が残存する場合（課題１）の対策案

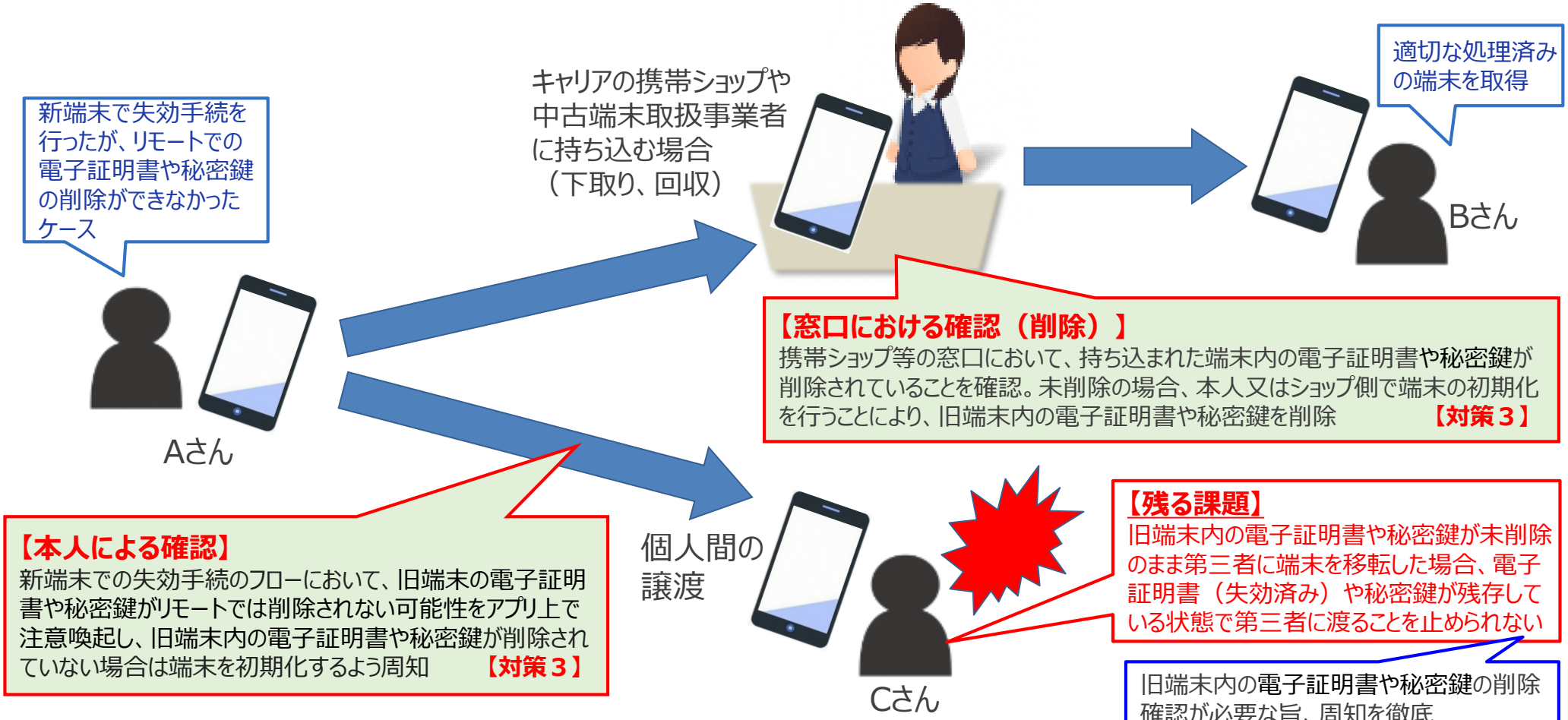
スマホ用電子証明書の利用を停止する場合、法律上、利用者に失効申請を行う義務を課す想定だが、現実的には失効申請を行わないことも想定される。その場合、未失効の電子証明書が端末内に残存した状態で第三者に移転することから、悪用されるリスクをできる限り排除するため、以下の措置を検討。
（注：カード紛失の場合と同様、スマホ用電子証明書もPIN/パスワードで保護されており、悪用されるリスクは低いと考えられる）



端末内の電子証明書や秘密鍵が未削除である場合（課題２）の対策案

新端末での新規利用手続において、旧端末内の電子証明書を失効させ、**リモートで**旧端末内の電子証明書や秘密鍵を削除しようとする場合に、旧端末がネットワーク通信できない場合やプッシュ通知の受信拒否設定をしている場合等、**削除できないケースが存在**。

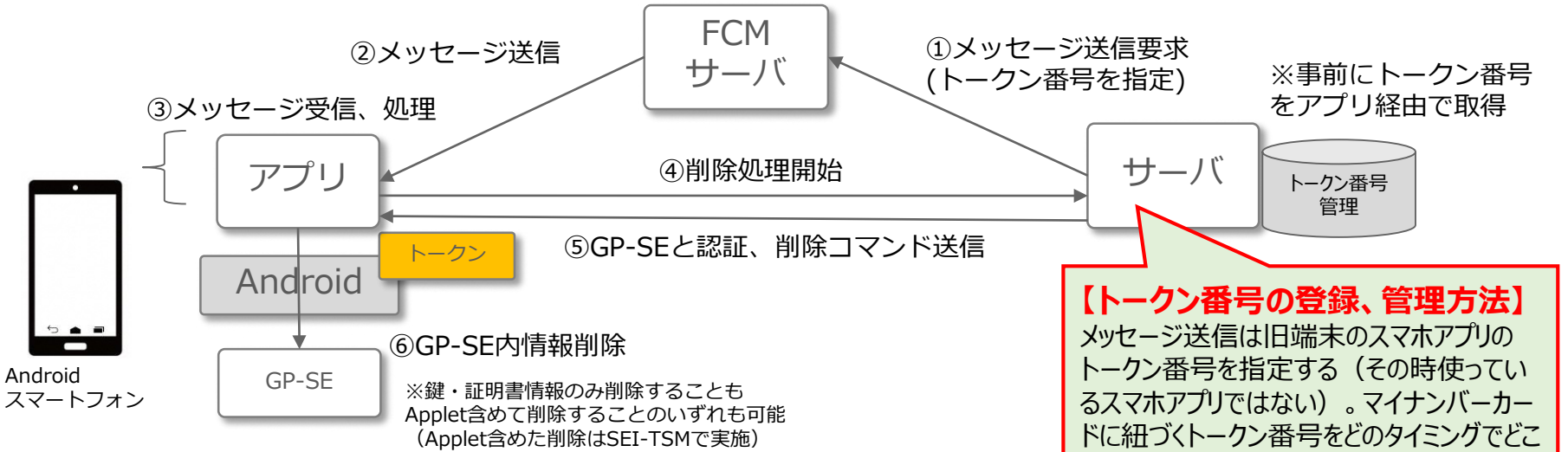
⇒電子証明書自体は失効しており利用できないが、旧端末内に電子証明書や秘密鍵が残存した状態で第三者に移転することにより悪用されるリスク※をできる限り排除するため、以下の措置を検討



※署名用電子証明書に記録されている基本4情報が読み出されたり、失効済みの署名用電子証明書に紐付く秘密鍵により電子署名が行われたりすることが挙げられる。後者については、電子署名を防止するための技術的措置について別途検討する。

リモートでのGP-SE内の情報削除

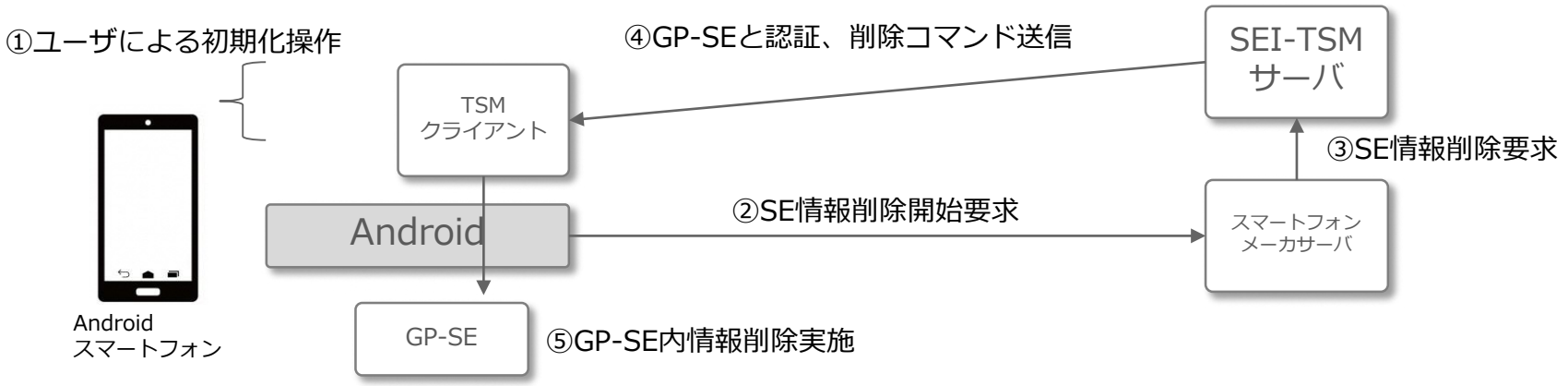
- **サーバから要求を開始して、GP-SEにアクセスし、GP-SE内の情報を削除することが技術的に可能。**
- **Google社が提供するFCM（Firebase Cloud Messaging）という、サーバからスマートフォン上のアプリにメッセージを送信するサービスを利用する。**
- **スマートフォン1台毎に“トークン“と呼ばれるユニークな番号がFCMの仕組みで発番され、サーバはトークン番号をキーにメッセージを送信する。**
- **ユーザのアプリ操作なしに、サーバとアプリの通信で処理を行うことが可能。**
- **リモートでの処理が必ず成功することを保証するサービスではないため、削除ができないケースがあり得る。**
  - スマートフォンがネットワーク通信できない場合はメッセージ送信が失敗する。
  - アプリの削除や端末の初期化が行われた場合や、あるいはその他の理由、トークンが削除されたり無効になった場合もメッセージ送信が失敗する。
  - その他の理由で、FCMサーバからのメッセージ送信は失敗するケースがあり得る。



【トークン番号の登録、管理方法】
メッセージ送信は旧端末のスマホアプリのトークン番号を指定する（その時使っているスマホアプリではない）。マイナンバーカードに紐づくトークン番号をどのタイミングでどこに（TSM、JPKI側）登録し、管理するか詳細化が必要。

端末初期化によるGP-SE内の情報削除

- **ユーザによるスマートフォンの初期化時に、GP-SE内の情報を削除（クリア）することが技術的に可能。**
  ただし、実現に当たっては、Android OSの提供者であるGoogle社やスマートフォンメーカ各社の協力を得る必要がある。
- **初期化操作時にスマートフォンからサーバに対して、GP-SE内情報の削除を要求する。**



fido ALLIANCE MEMBER

docomo

1. スマートフォン搭載における生体認証の利活用について

ドコモにおける世界初の虹彩認証搭載スマートフォンを含む生体認証対応Androidスマートフォンの FIDO対応（2015年5月）を基点とし、業界の連携で、スマートフォンにおける生体認証の搭載と利用が一般的となりました。これを実現しているしくみ等を勘案し、FeliCa-SEを搭載するスマートフォンでは、利用者証明用電子証明書の利用シーンからスマートフォンに搭載している生体認証を活用することを提案します。

署名用パスワード 半角文字
6文字から16文字まで、かつ、
数字とアルファベット の混在

市場のスマートフォンに搭載の
生体認証装置で証明書の
所持者であることを検証可能か、
要継続検討

利用者証明用パスワード
（暗証番号）4桁の数字

市場のスマートフォンに搭載の
生体認証装置で証明書の
所持者であることを検証可能

第2回　マイナンバーカードの機能のスマートフォン搭載等に関する検討会
資料7「スマートフォンへの生体認証の搭載・FIDO認証の適用を通じて得られた知見を基にしたご提案」（森山構成員）

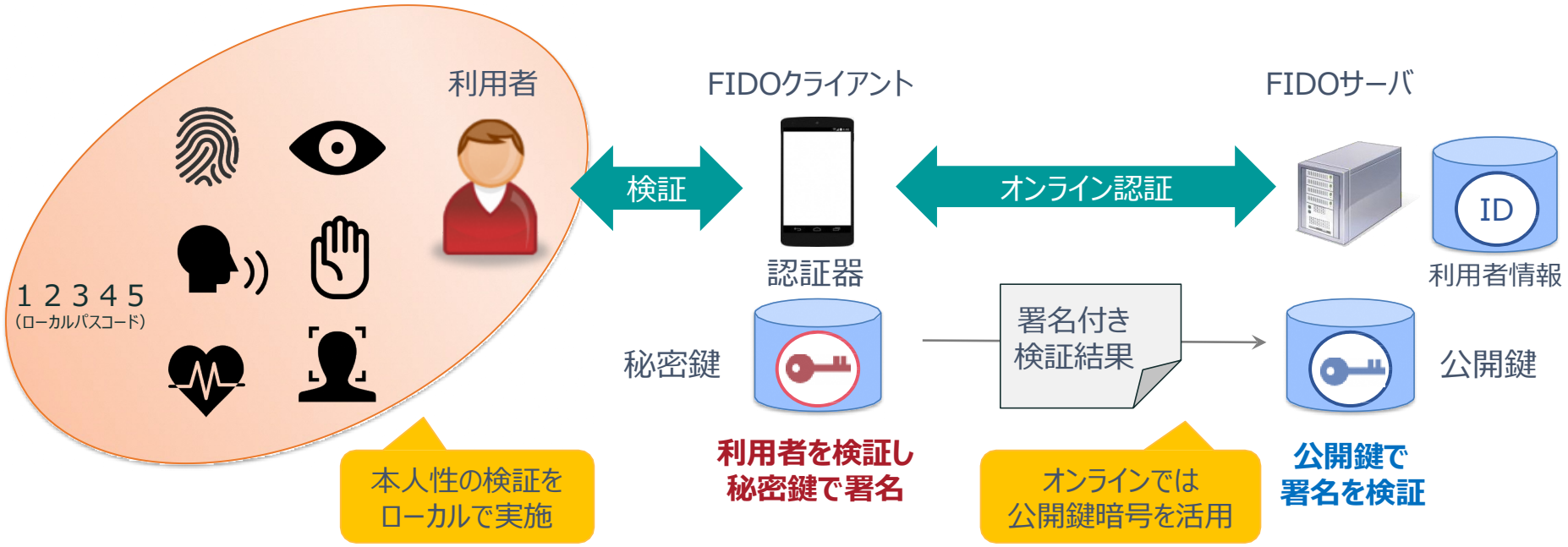
FIDO認証の概要

- FIDO ALLIANCE, INC. (A NONPROFIT MUTUAL BENEFIT CORPORATION) -

FIDO（ファイド）アライアンス

2012年に設立、現在約250社で構成。米国カリフォルニア州法に基づくグローバルな非営利団体（相互利益法人）
パスワードと認証にまつわる課題解決のため、「FIDO認証モデル」に基づく技術仕様の策定、技術仕様を導入展開するためのプログラム運営、各標準化団体との協業などを通じたさらなる導入展開を推進。

FIDO認証モデル（端末とサーバで秘密を共有しない）



利用者が「認証器」（Authenticator）に適切な秘密鍵を保有することを検証することによって認証を実現しており、認証器の簡単な操作だけで（動的な）多要素認証