

スマホ用電子証明書等の悪用防止及び 利用に関する周知等に関する方向性と課題

令和3年5月17日

総務省 情報流通行政局 デジタル企業行動室

方向性

- スマホに搭載した電子証明書※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が課されるが、現実的には適切に失効申請が行われないことも想定され、スマホに搭載された電子証明書や秘密鍵が残存した状態で売買、譲渡、紛失等した場合に、当該電子証明書等が他人に悪用されるリスクが生じる。

※ スマホ用署名用電子証明書には基本4情報（氏名、性別、住所、生年月日）が記載される。

- こうした事態を極力避けるため、本検討会でのこれまでの議論や第一次とりまとめでも示されたように、

① 今後行う技術実証の中で、技術的な見地からの検討※を行うことに加え、

※ 例：旧端末に残存している電子証明書等を新端末から失効・削除することを可能とする方策の検討、未失効の電子証明書等が削除された場合の電子証明書の失効管理の方法についての検討 等

② 運用上の検討を重層的に行うことが必要。

- 特に、悪用防止に関して②の運用上の検討を行うにあたっては、利用者が適切に失効申請等を行えるよう、スマホ用電子証明書の失効情報等を管理することとなるJ-LISの役割を明確にするとともに、利用者が実際にスマホを売買、譲渡、紛失等する際に接することとなる携帯キャリア等（MNO及びキャリアショップ運営代理店、MVNO、中古端末取扱事業者）やC to Cプラットフォーム事業者等の関係事業者に対しても、スマホ用電子証明書等の悪用防止に向けた協力を求めることが肝要。

- また、スマホ用電子証明書等の悪用防止に向けて上記の関係事業者と連携して行う取組については、電子証明書のスマホ搭載が混乱無く円滑に実現されるよう、社会実装までに、必要なマニュアルの整備や利用者対応フローの検証を行うことが望ましい。

方向性

- 利用者の混乱を避けるため、スマホ用電子証明書に関する問い合わせ対応については現行のJ-LISコールセンターで行うこととし、J-LISコールセンターでは、スマホ用電子証明書の一時保留対応だけでなく、アプリのダウンロードの仕方や使用方法等、スマホ用電子証明書についての問い合わせ対応も行うこととする。
- 電子証明書を搭載したスマホ紛失時の対応については、カードと同様、J-LISコールセンターへ連絡を受けることにより完了する手続とする。
- 国においては、紛失時のJ-LISコールセンターへの連絡の必要性やその具体的方法について、広く周知していく。

課題

- スマホ用電子証明書利用者等からの問合せ対応を円滑に実施するため、必要に応じてJ-LISコールセンターの体制整備が必要。また、対応マニュアルの整備が必要。
- スマホ用電子証明書の一時保留解除の考え方について整理が必要※。

※ カードの場合、一時保留を行った場合には、利用者証明用電子証明書については後日自治体窓口で解除が可能であるが、署名用電子証明書については後日自治体窓口で失効申請及び再発行手続が必要となる。他方、スマホ用電子証明書においては、利用者証明用電子証明書、署名用電子証明書を問わず、利用者において新端末からスマホ用電子証明書の再発行手続がとれることから、必ずしもカード同様の手続をとる必要はなく、スマホ用利用者証明用電子証明書、スマホ用署名用電子証明書の両方について、一時保留解除ではなく、再発行手続を行うこととすることも考えられる。

方向性

- スマホ利用者とのタッチポイントとなる携帯キャリア等において、端末の下取り・回収等の際に、利用者に対し、スマホ用電子証明書等の失効・削除について適切に案内するよう協力を求める。また、C to Cプラットフォームを介した端末取引が行われる場合にも、利用規約等において利用者に対し注意喚起されるよう協力を求める。
- 上記措置を講じたとしても、電子証明書等が残った端末が下取り・回収されてしまう可能性がゼロではないことから、そのような場合には、携帯キャリア等において電子証明書等を削除するよう協力を求める。
- 携帯キャリア等において、利用者から端末紛失の連絡を受けた際に、J-LISコールセンターへ連絡すべきであることを案内するよう協力を求める。

課題

- 利用者に対してスマホ用電子証明書等の失効・削除を案内することによる、窓口対応のコスト増に留意が必要。
【コストに留意した取組等（例）】
〔 ・ スマホ用電子証明書対応端末の情報を明示することにより、利用者への案内を効率的に行えるようにする
・ 事業者において必要な対応が確実にとれるよう、政府において、最低限必要となる対応マニュアルを策定する 等 〕
- 電子証明書等の残存した端末が下取り・回収される事態を極力避けるため、電子証明書等の失効・削除が行われたことを簡便に確認できる仕組み（アプリ上で証明書等の状態を表示する等）の検討が必要。
- 万が一電子証明書等が残存した端末が下取り・回収された場合に備え、GP-SE内のデータを簡便に消去できる仕組み（端末初期化によるGP-SE内データ削除等）の検討が必要。
- 極力漏れの無い対応を実施するためには、携帯キャリア等やC to Cプラットフォーム事業者のみならず、端末保証サービスを提供する事業者や仲介事業者等、端末を取り扱う可能性のある幅広い事業者に対する協力要請が必要。
- 端末紛失時にWeb上でネットワークの一時中断を受け付ける場合に、J-LISコールセンターに連絡すべきことを案内する方法について検討が必要。

方向性

- マイナンバーカードの機能（電子証明書）のスマホ搭載は、その実現によりスマホのみで安全に行政手続等を行うことが可能となり、マイナンバーカードの利便性を抜本的に向上させるものであることから、**これまでマイナンバーカードを取得してこなかった方も含め、多くの方々にその利便性や安全性、利用方法等について広く周知していく必要がある。**
- そのためには、現在マイナンバー制度の広報として政府が活用している政府広報やHP、WEB動画等による周知のみならず、**直接スマホ利用者とのタッチポイントとなっている携帯キャリア等や、マイナンバーカード関連業務により日々住民と接している地方自治体とも連携して幅広く周知を進めていくことが望ましい。**
- その際、関心を持たない未利用者に向けた単純な制度周知にとどまるのではなく、関心を持っている者や利用を開始した者の疑問解消にも資する情報提供が可能となるよう検討していくことが必要。また、誰一人取り残さないデジタル社会の実現に資するよう、**デジタル活用に不安のある高齢者等に対しても丁寧な説明や周知を行うことが重要。**
- また、こうした説明や周知のために想定される**利用者対応フロー等についても、必要に応じて、悪用防止に関して関係事業者と連携して行われる取組とあわせて、社会実装前に検証を行うことが望ましい。**

方向性

- スマホ用電子証明書に関する手続については、法令上、自治体の事務が規定されていないが、実際には住民から自治体に対する問い合わせが発生することが想定されることから、自治体窓口において適切に対応がなされるよう、国から助言等を行う。
- 住民へ効果的な周知を行うため、マイナンバーカード関連の周知にあわせて、スマホ用電子証明書についても周知が行われることが望ましい。

課題

- 住民からの問合せに対応する際の負担を考慮し、国として自治体向けの対応マニュアルを作るとともに、通知等を通じ、スマホ用電子証明書に関する周知や住民対応について、自治体に向けた助言等を行う必要がある。

【窓口での問合せ対応（例）】

- ・ 問合せに対してJ-LISコールセンターを案内
- ・ 窓口において、スマホ用電子証明書に関するパンフレット等を設置・配布

【マイナンバーカード関連の周知にあわせた取組（例）】

- ・ 自治体HPにおいて、スマホ用電子証明書関連HPのリンク掲載

- 今般の郵便局事務取扱法の一部改正によって、郵便局においてもマイナンバーカード用電子証明書の発行・更新等の事務を行うことが可能となることから、郵便局でもスマホ用電子証明書に関する周知について、自治体同様の対応ができるか今後検討が必要。

方向性

- 効果的な周知を行うため、スマホ利用者とのタッチポイントとなる携帯キャリア等において、利用者から問合せを受けた際や、スマホ用電子証明書対応端末での新規契約、機種変更を取り扱う際等に、利用者に対し、スマホ用電子証明書に関する説明や周知が行われるよう協力を求める。
- 必ずしもスマホ利用者が窓口で新規契約等を行うとは限らないことも踏まえ、携帯キャリア等の端末カタログやHPにおいて、スマホ用電子証明書対応端末の明示や、スマホ用電子証明書関連HPのリンク掲載等、利用者に対して十分な情報提供が行われるよう協力を求める。
- また、誰一人取り残さないデジタル社会の実現に資するよう、デジタル活用に不安のある高齢者等に対しても、スマホ用電子証明書に関する説明が丁寧に行われるよう協力を求める。

課題

- 利用者に対してスマホ用電子証明書に関する説明や周知を行うことによる、窓口対応のコスト増に留意が必要。
【コストに留意した取組等（例）】
 - ・問合せに対してJ-LISコールセンターを案内
 - ・キャリアショップ等において、スマホ用電子証明書に関するパンフレット等を設置・配布
 - ・要望があった場合に有償でスマホ用電子証明書搭載等についての端末操作をサポート
 - ・事業者において、正しい説明や周知が行えるよう、政府において、最低限必要となる対応マニュアルを策定する 等
- スマホ用電子証明書対応端末を端末カタログやHP上で掲載するためには、対応端末情報について、事前に事業者・J-LIS間で連携している必要がある。
- 令和4年度以降のデジタル活用支援事業と連携するなど、デジタル活用に不安のある高齢者等に対して説明を行う方策について検討が必要。

(参考) 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

【旧端末で手続を行う場合】

法律上は利用者に失効申請義務（想定）

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

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

【旧端末で手続を行わない場合】

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

（旧端末の電子証明書は失効していない状態）

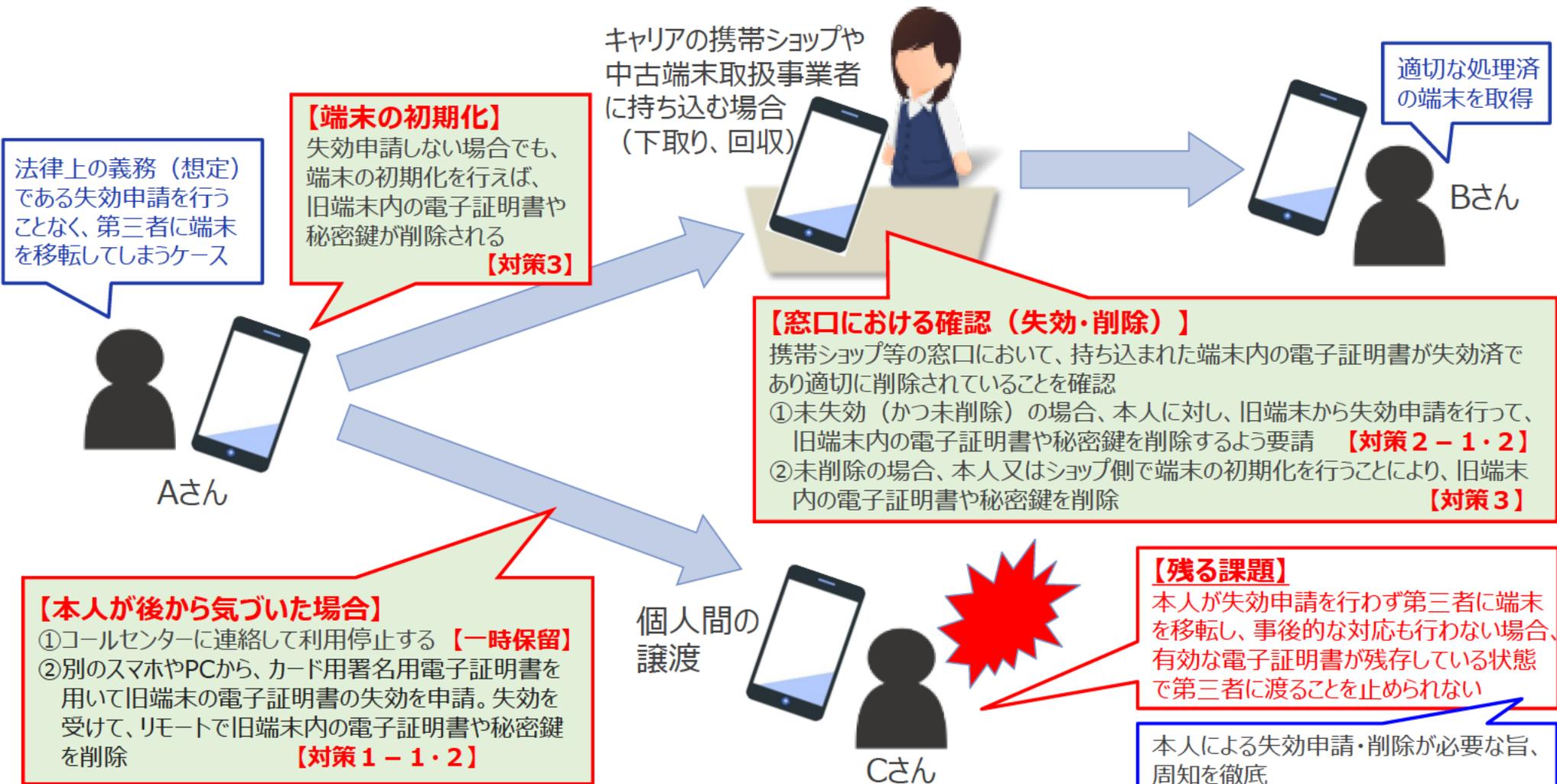
（旧端末の電子証明書や秘密鍵は削除されていない状態）

PINで保護されている

【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

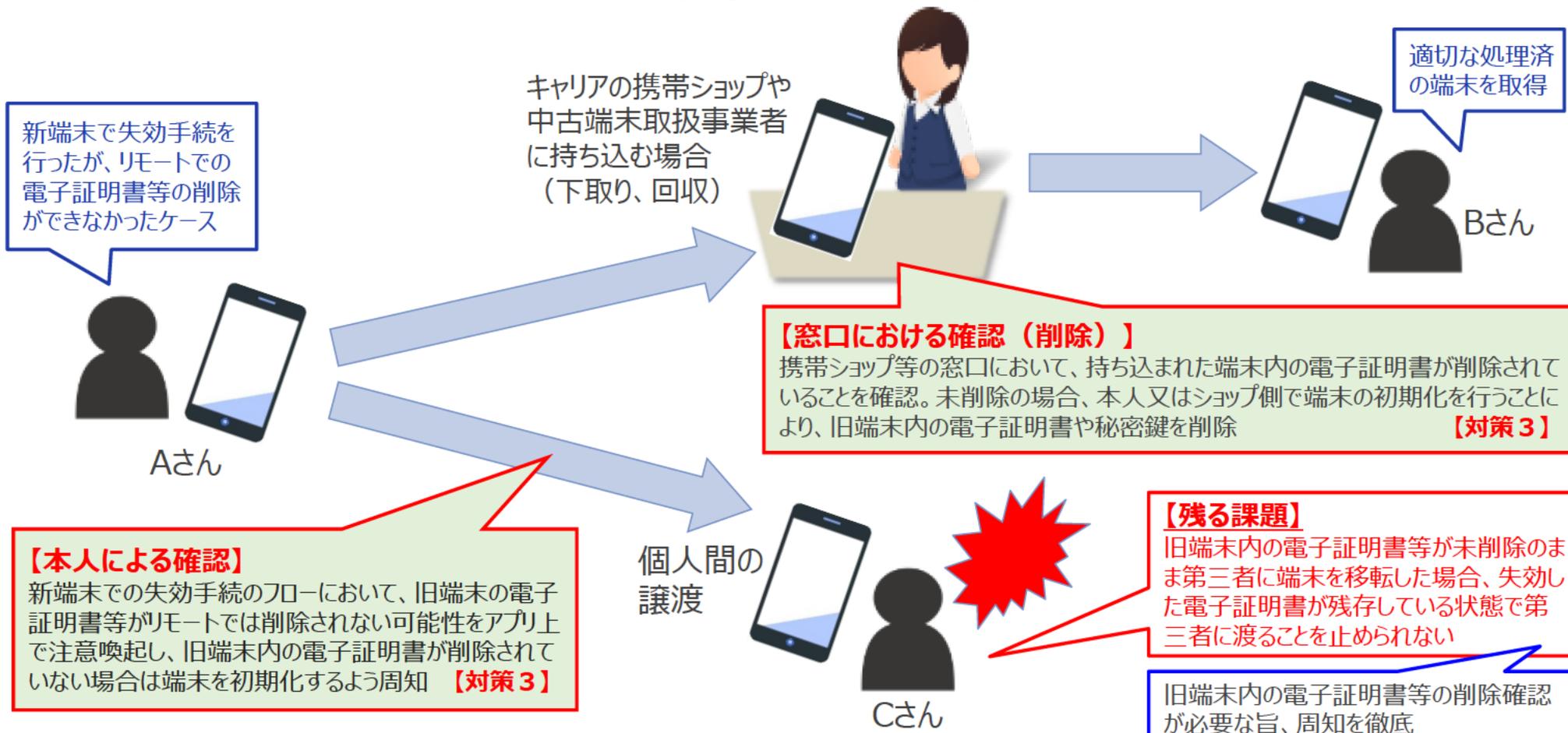
スマホ用電子証明書の利用を停止する場合、法律上、利用者に失効申請を行う義務を課す想定だが、現実的には失効申請を行わないことも想定される。その場合、未失効の電子証明書が端末内に残存した状態で第三者に移転することから、悪用されるリスクをできる限り排除するため、以下の措置を検討。

(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)



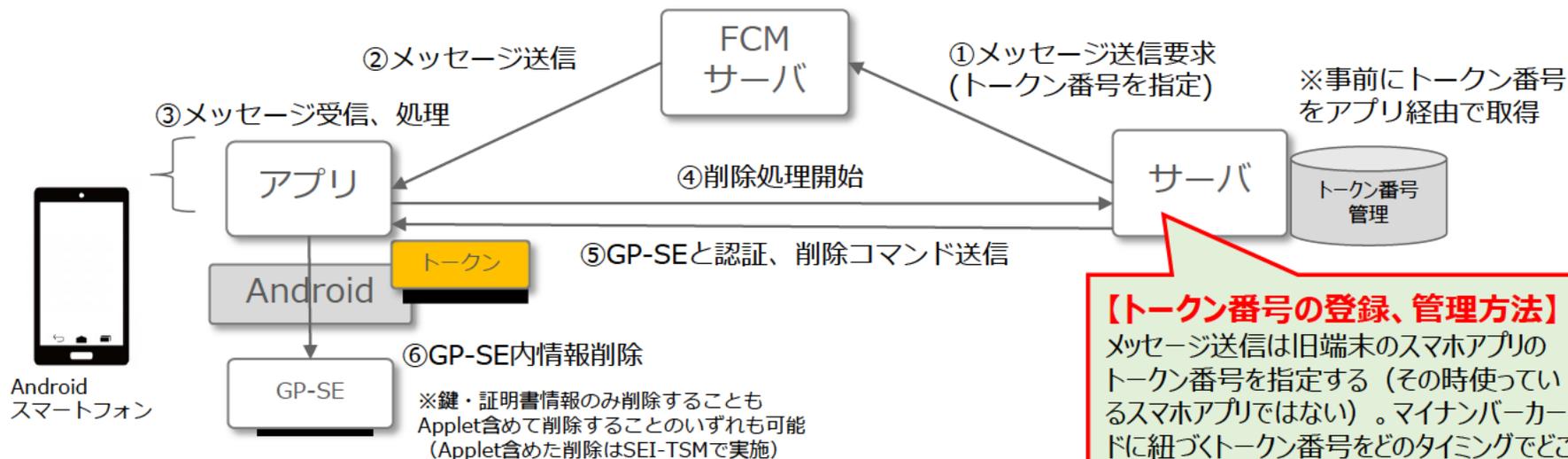
新端末での新規利用手順において、旧端末内の電子証明書を失効させ、**リモート**で旧端末内の電子証明書や秘密鍵を削除しようとする場合に、旧端末がネットワーク通信できない場合やプッシュ通知の受信拒否設定をしている場合等、**削除できないケースが存在**。

⇒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。

- 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。

- 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ー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。



- **デジタル社会形成基本法案、デジタル庁設置法案、デジタル社会の形成を図るための関係法律の整備に関する法律案、公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律案及び預貯金者の意思に基づく個人番号の利用による預貯金口座の管理等に関する法律案に対する附帯決議 (衆・内閣委 2021年4月2日)**

政府は、デジタル改革関連5法の施行に当たっては、次の事項に留意し、その運用等について遺漏なきを期すべきである。また、政府は、地方公共団体における運用等についても次の事項の趣旨にのっとり行われるよう、必要な助言を行うこと。

一～三 (略)

四 デジタル社会の形成を図るための関係法律の整備に関する法律の施行に関し、以下の事項について配慮すること。

1～11 (略)

12 **移動端末設備用電子証明書が記録されている移動端末設備の譲渡又は紛失等によって、電子証明書及び署名利用者符号等が悪用されることのないよう、国は、これらを迅速かつ確実に失効・削除する仕組みを整備するとともに、移動端末設備の買取り等を行う関係事業者に対して電子証明書が失効済であること並びに電子証明書及び署名利用者符号等が復元不可能な形で削除済であることを確認するよう要請するなど、万全の措置を講ずること。**

13～14 (略)

五・六 (略)

- **デジタル社会形成基本法案、デジタル庁設置法案、デジタル社会の形成を図るための関係法律の整備に関する法律案、公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律案及び預貯金者の意思に基づく個人番号の利用による預貯金口座の管理等に関する法律案に対する附帯決議 (参・内閣委 2021年5月11日)**

政府は、デジタル改革関連五法の施行に当たり、次の諸点について適切な措置を講ずるべきである。また、政府は、地方公共団体における運用等についても次の諸点の趣旨にのっとり行われるよう、必要な助言を行うこと。

一～三 (略)

四 デジタル社会の形成を図るための関係法律の整備に関する法律の施行に関し、以下の事項について配慮すること。

1～11 (略)

- 12 **移動端末設備用電子証明書が記録されている移動端末設備の譲渡又は紛失等によって、電子証明書及び署名利用者符号等が悪用されることのないよう、国は、これらを迅速かつ確実に失効・削除する仕組みを整備するとともに、移動端末設備の買取り等を行う関係事業者に対して電子証明書が失効済であること並びに電子証明書及び署名利用者符号等が復元不可能な形で削除済であることを確認するよう要請するなど、万全の措置を講ずること。**

13～15 (略)

五・六 (略)