資料4

旧端末に搭載した電子証明書及び秘密鍵の悪用防止策

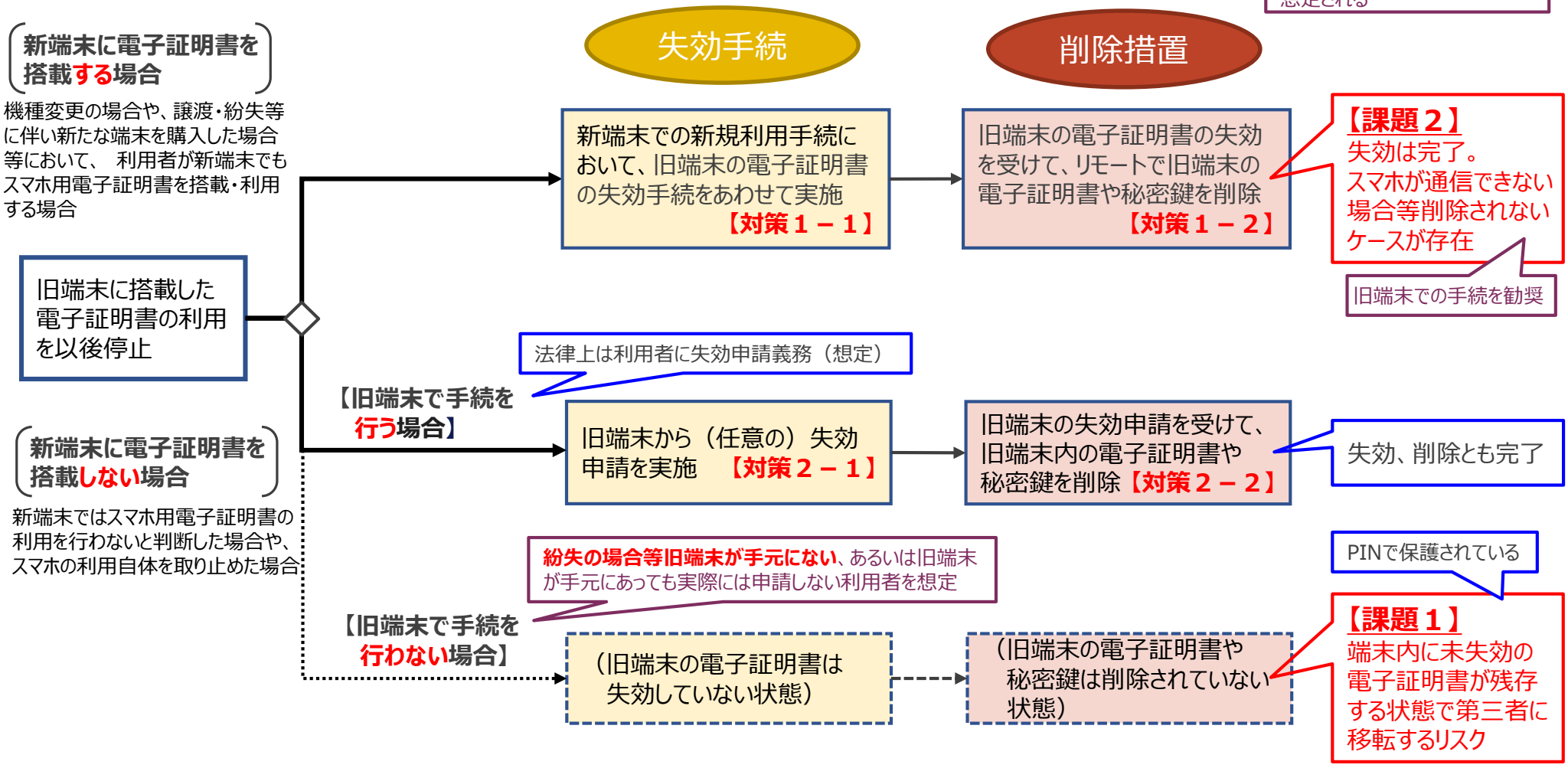
令和2年12月23日

総務省　情報流通行政局　デジタル企業行動室

旧端末に搭載した電子証明書及び秘密鍵の悪用防止

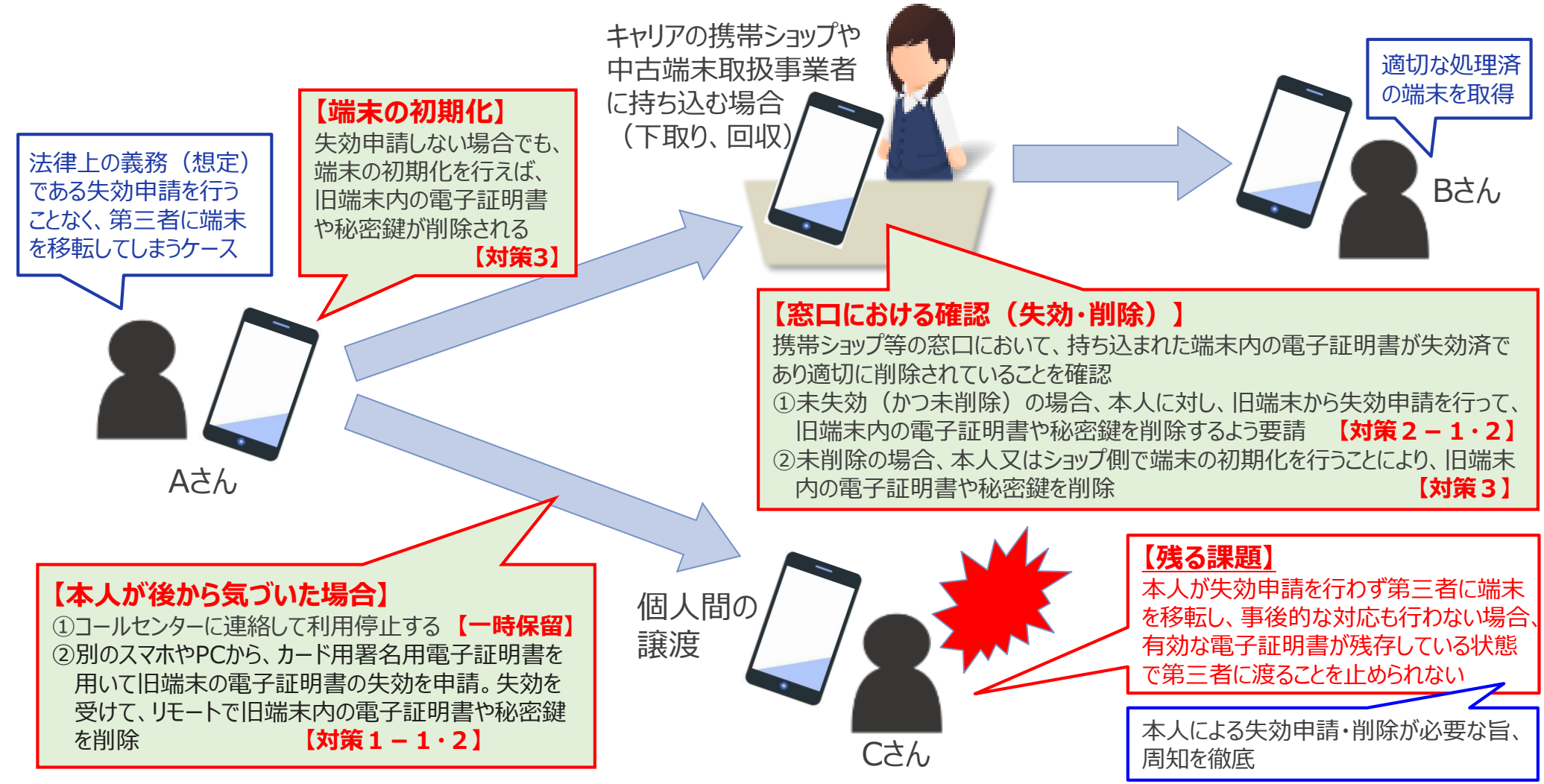
・機種変更や譲渡・紛失等により、スマホ（旧端末）に搭載した電子証明書の利用を以後停止する場合、
①旧端末に搭載した電子証明書を失効させることが必要（※法律上は利用者に失効申請義務を課すことを想定）。
②また、電子証明書や秘密鍵が旧端末内に残存したまま第三者に移転して悪用されることを防ぐため、
これらの電子証明書や秘密鍵が適切に削除されることが望まれる。

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



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

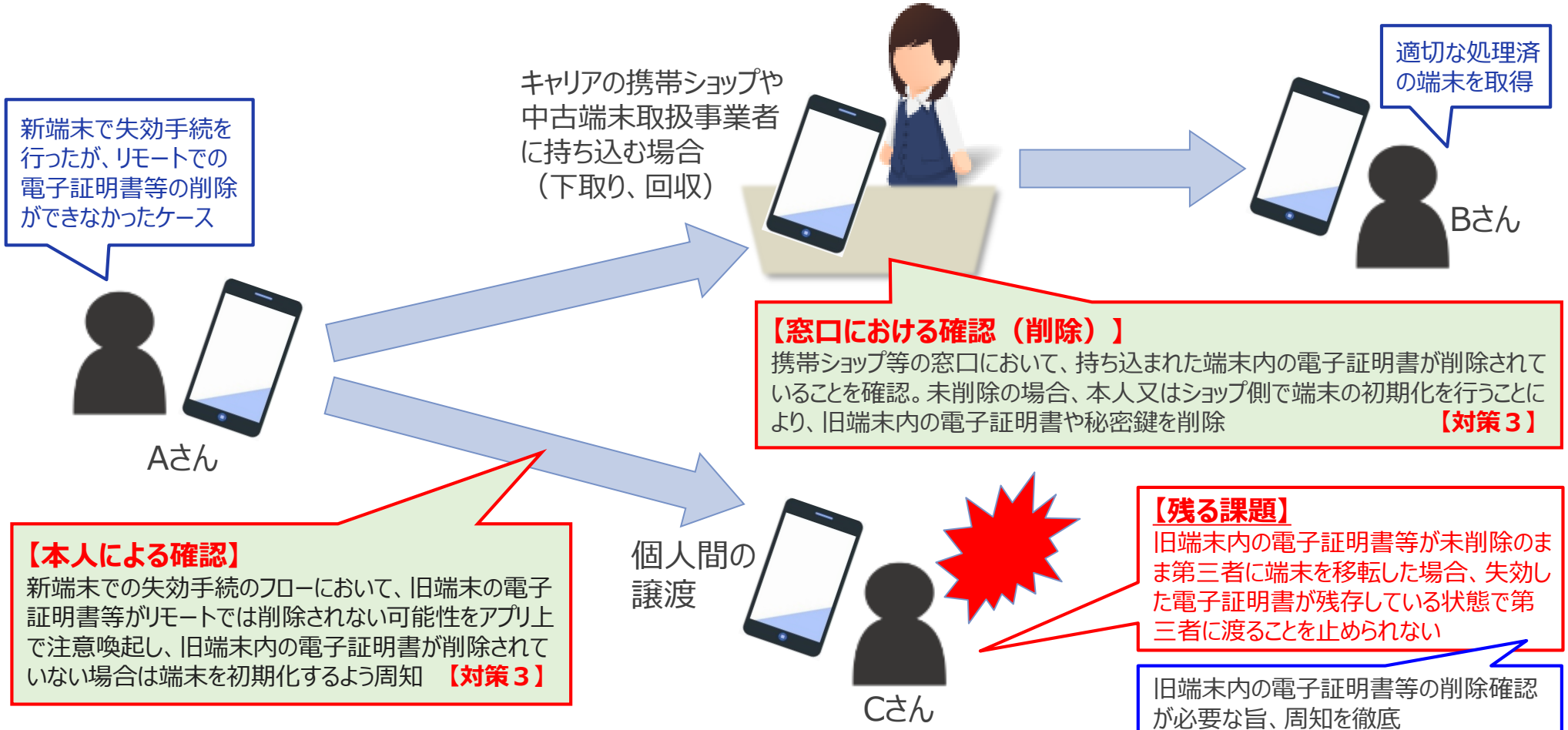
スマホ用電子証明書の利用を停止する場合、法律上、利用者に失効申請を行う義務を課す想定だが、現実的には失効申請を行わないことも想定される。その場合、未失効の電子証明書が端末内に残存した状態で第三者に移転することから、悪用されるリスクをできる限り排除するため、以下の措置を検討。
（注：カード紛失の場合と同様、スマホ用電子証明書もPINで保護されており、悪用されるリスクは低いと考えられる）



端末内の電子証明書等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**。

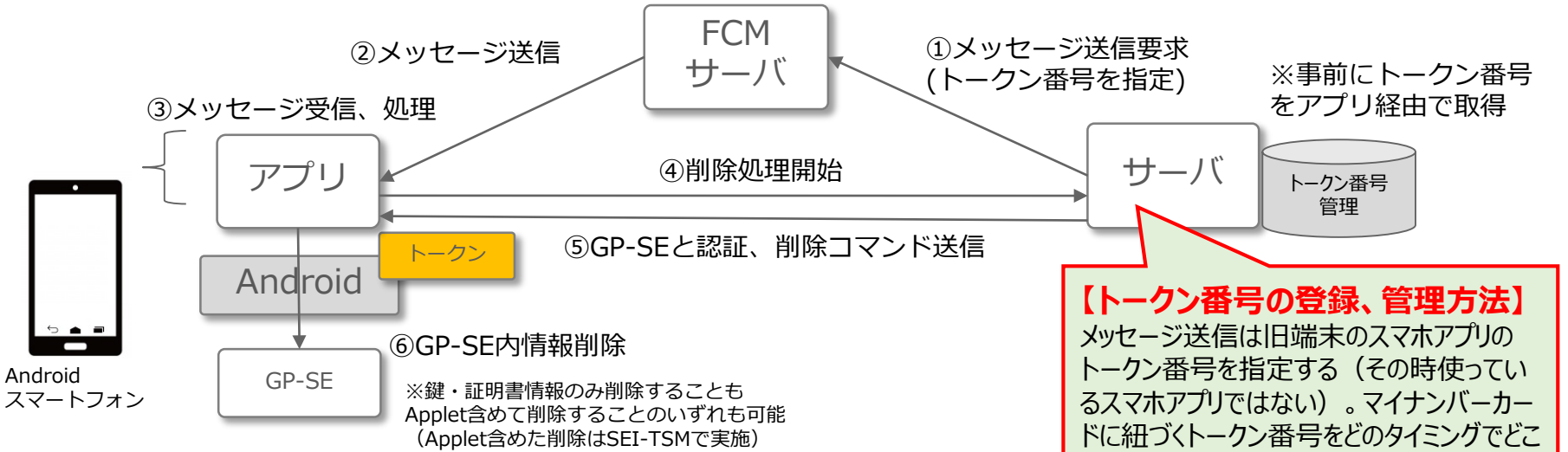
⇒電子証明書自体は失効しており利用できないが、旧端末内に電子証明書や秘密鍵が残存した状態で第三者に移転することにより悪用されるリスク※をできる限り排除するため、以下の措置を検討



※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。**