資料3－2

スマートフォンへの利用者認証機能のダウンロードにおける検証課題について

平成28年2月16日

NTT DATA

1．技術的な検討課題について

「技術的な検討課題」について詳細化を検討した。検討結果を以下に示す。

ＳＩＭカードへの利用者認証機能の格納における実現に向けた課題		課題の詳細化
（１）電子証明書及び秘密鍵のSIMカードへダウンロード		
	ア．SIMカードの電子証明書等の格納媒体としての要件（セキュリティの確保）	① 現在のSIMカードに実装されているセキュリティ機能、ライフサイクル機能等の詳細を把握する必要がある。
		② 個人番号カードに関する要件、ユースケースから出される要件、民間モバイルNFCサービス事例を参考に、SIMカードに求められる機能要件、セキュリティ要件を明らかにする必要がある。
		③ ①②に基づき実現方式を検討する。必要に応じて、JPKI-アプレットでの機能拡張や、SP-TSM等で補完することも検討の上、SIMカードに求められる要件を決定する。
	イ．SIMカードへの電子証明書等の安全なダウンロードの方法（ネットワーク経由又は窓口における格納）	④ ネットワークを経由しての電子証明書等のダウンロードについて、キャリア各社が提供するモバイルNFCサービスに基づいた方法を検討する。必要に応じて、SP独自のセキュリティ対策の追加も検討する（別紙1参照）
		⑤ 窓口のリーダライタ経由での電子証明書等のダウンロードについて、J-LISから窓口端末への電子証明書等の安全な配送方法、窓口端末からSIMカードへの安全な書込み方法を検討する。
	ウ．多様なスマートフォン/SIMカード上で動作するJPKI-UIアプリ/JPKI-アプレットの効率的な品質確保手段(追加)	⑥ スマートフォンのOSのバージョンや製造メーカ、キャリアに極力依存しないJPKI-UIアプリの構成、開発方法を検討する必要がある。試験を効率化するため、認定基準を設けることなども必要。
		⑦ SIMカードのバージョンやメーカ、キャリアに極力依存しないJPKI-アプレットの構成、開発方法を検討する必要がある。マルチベンダ対応の共通アプレット等、開発の効率化が可能か検討する。
	エ. SIMカードへの利用者証明機能の格納において新たに開発すべきシステム（追加）	⑧ スマートフォン上で動作するUIアプリ、SIMカード上で動作するJPKI-アプレット、JPKI-アプレットに電子証明書等を書き込むSP-TSMなどが新たに必要。
（２）既存システムへの影響		
	ア.JLISのJPKIシステムの改修（スマートフォンにダウンロードされた電子証明書の発行・管理機能（個人番号カードの電子証明書との紐付け、有効期限等ライフサイクル管理(発行、失効、一時停止)))	⑨SP-TSMとJPKIシステムの最適な機能分担とそのインタフェースについての検討 ⑩申請データ（4情報含む）による個人番号カードの発行有無の確認（後述のパターン1の場合）

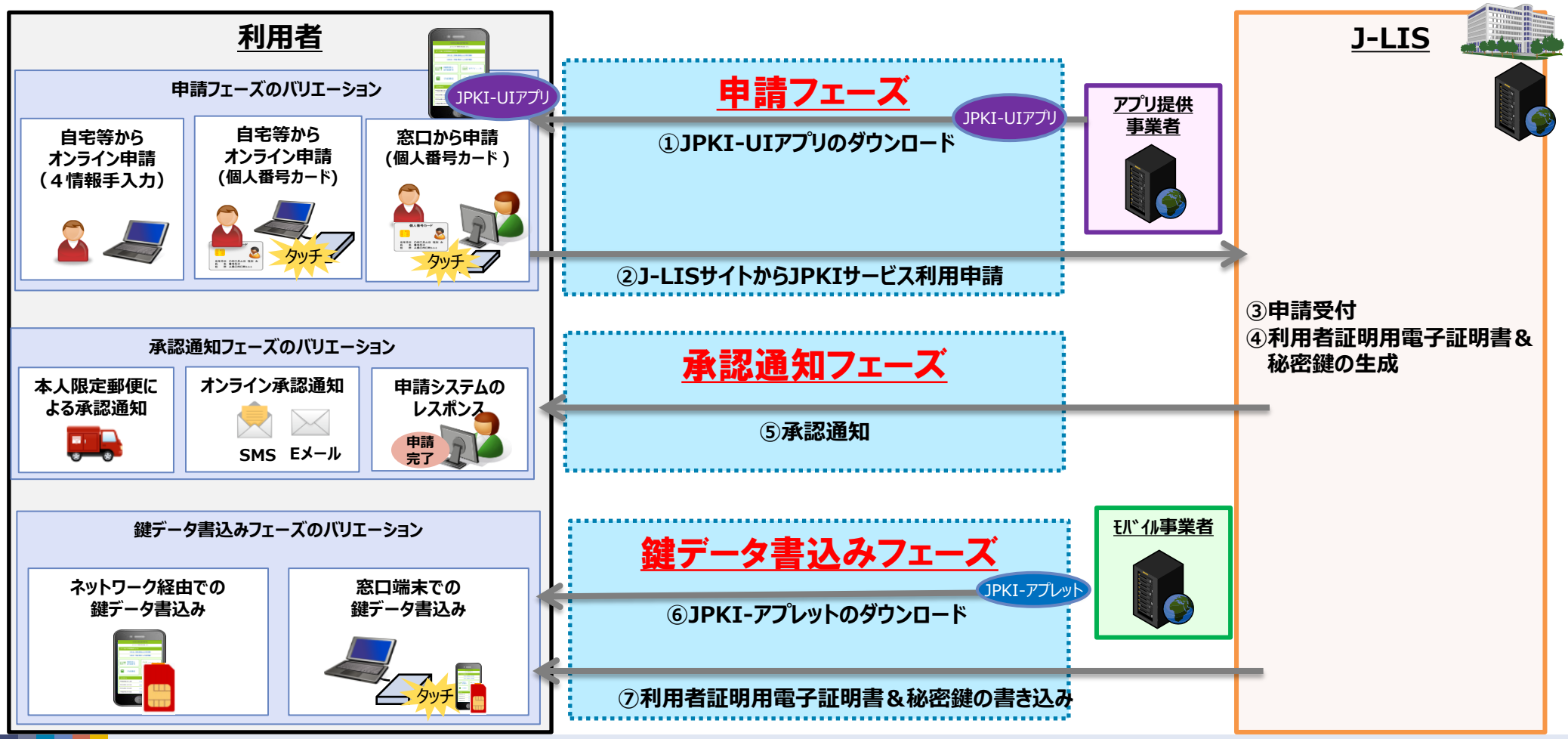
2．制度面・運用面での課題について

制度面・運用面での課題おいて、初回申請フローを検討することで、特に、「運用面の課題」について、課題の詳細化を図った。

ＳＩＭカードへの利用者認証機能の格納における実現に向けた課題
【制度面の課題】
(1) 利用者証明用電子証明書の二重発行の禁止（公的個人認証法第25条）
(2) 利用者証明用電子証明書の発行の手順（公的個人認証法第22条）
【運用面の課題】
(1) 申請者の本人認証の方法（署名用電子証明書による署名検証、対面、本人限定受取郵便等）
(2) 申請者とSIMカードとの紐付け・連携方法
(3) SIMカードの領域使用に関する責任分界点(モバイル事業者,JLIS,自治体,利用者）、費用負担の在り方
(4) 通信事業者間、端末間移動した際におけるサービスの利用継続性の確保
(5) 自らSIMカードを発行していないMVNOにおけるサービス提供の在り方
(6) 消費者対応の在り方（操作方法、対応端末等に関する問い合わせ等）
(7) ユースケースの整理

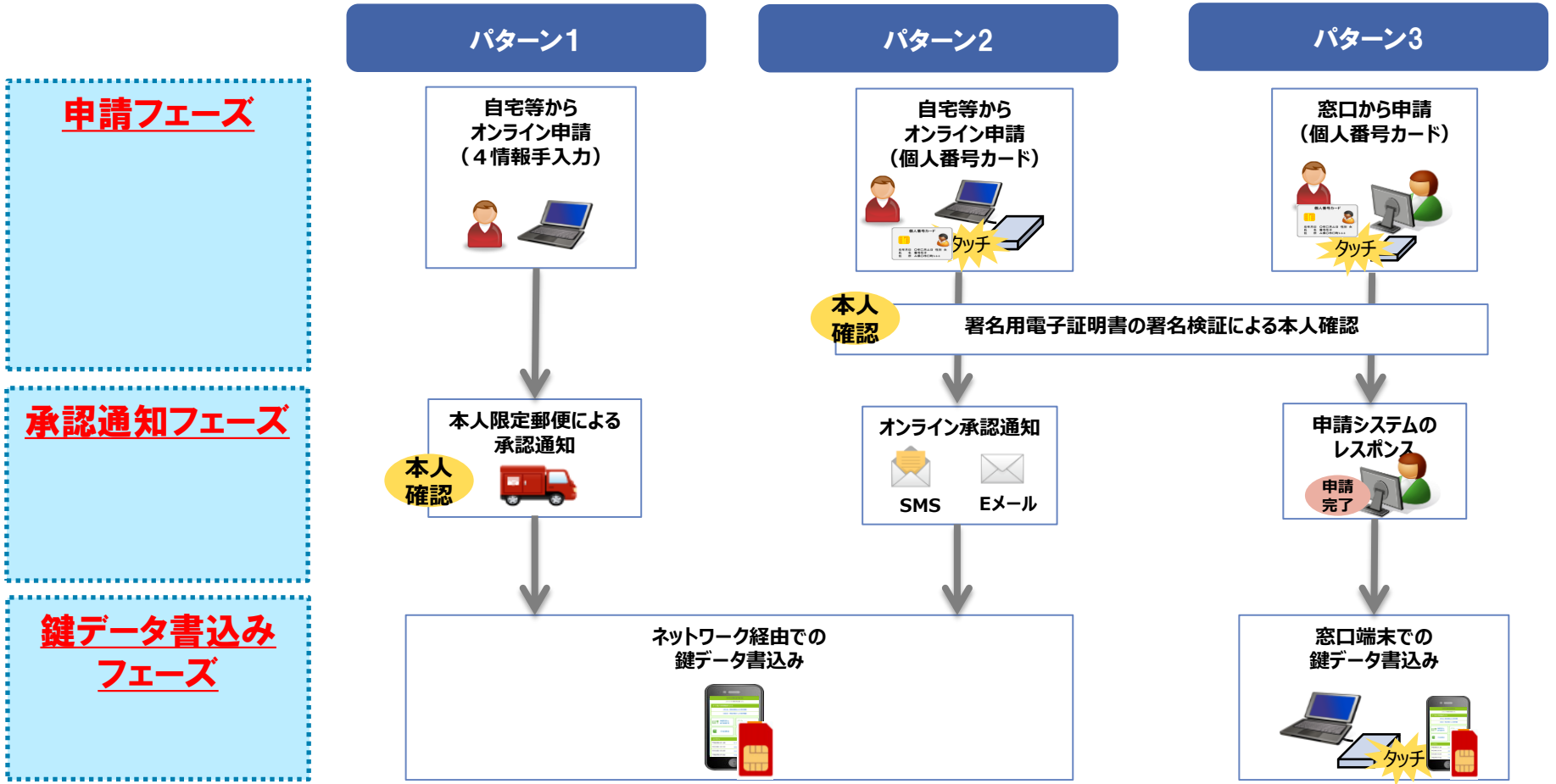
3．SIMカードへの利用者証明機能格納のフェーズ分け

・SIMカードへの利用者証明機能ダウンロードの実施方法は、「申請フェーズ」、「(J-LISからの)承認通知フェーズ」、「鍵データ書込みフェーズ」の大きく３つのフェーズに分けることができる。
・各フェーズでの目的は以下の通り。
　– 申請フェーズ：利用者がサービス提供者へ利用者証明書を使う為の申請を行うフェーズ。
　– 承認通知フェーズ：サービス提供者が利用者証明書発行準備ができたことを利用者に通知する(アクセスコードの送付を含む)。
　– 鍵データ書込みフェーズ：利用者の携帯電話へサービス提供者に指定される手段で鍵データ書込みを行う。



４．利用書証明機能ダウンロードの実現パターンについて

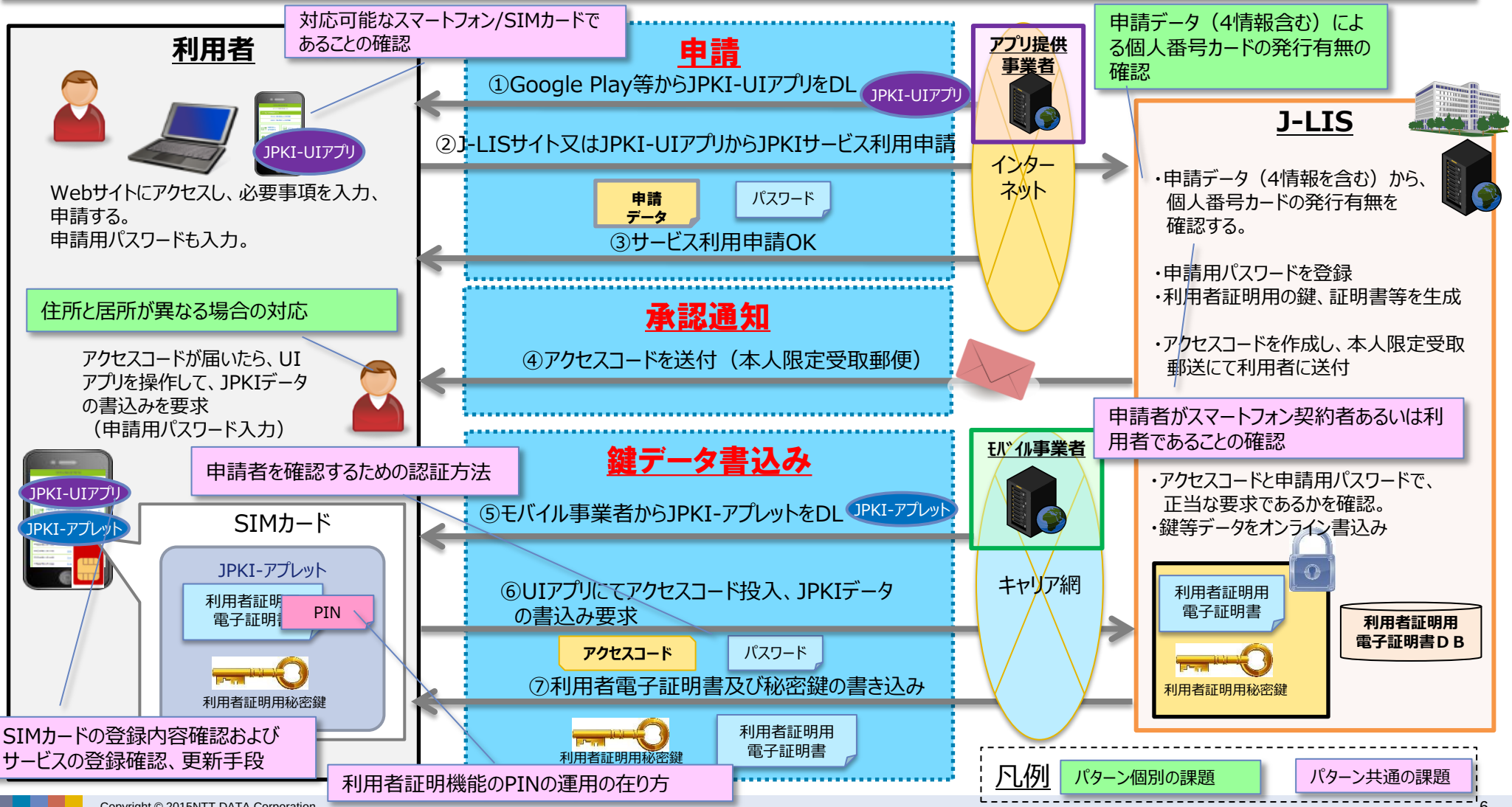
利用者証明機能ダウンロードの方法は前述の３フェーズ毎にバリエーションがあるが、概ね以下の３つに分類することができる。
－パターン1：民間で実績のある申請フローを踏襲し、本人限定郵便による本人確認、ネットワーク経由での鍵データ書込みを行う。
－パターン2：個人番号カードの電子署名機能を活用したオンライン申請、ネットワーク経由での鍵データ書込みを行う。
－パターン3：市町村窓口等の端末から申請し、市町村窓口等の端末から鍵データ書込みを行う。



次頁以降では、実現パターン毎に課題の洗い出しを行うこととする。

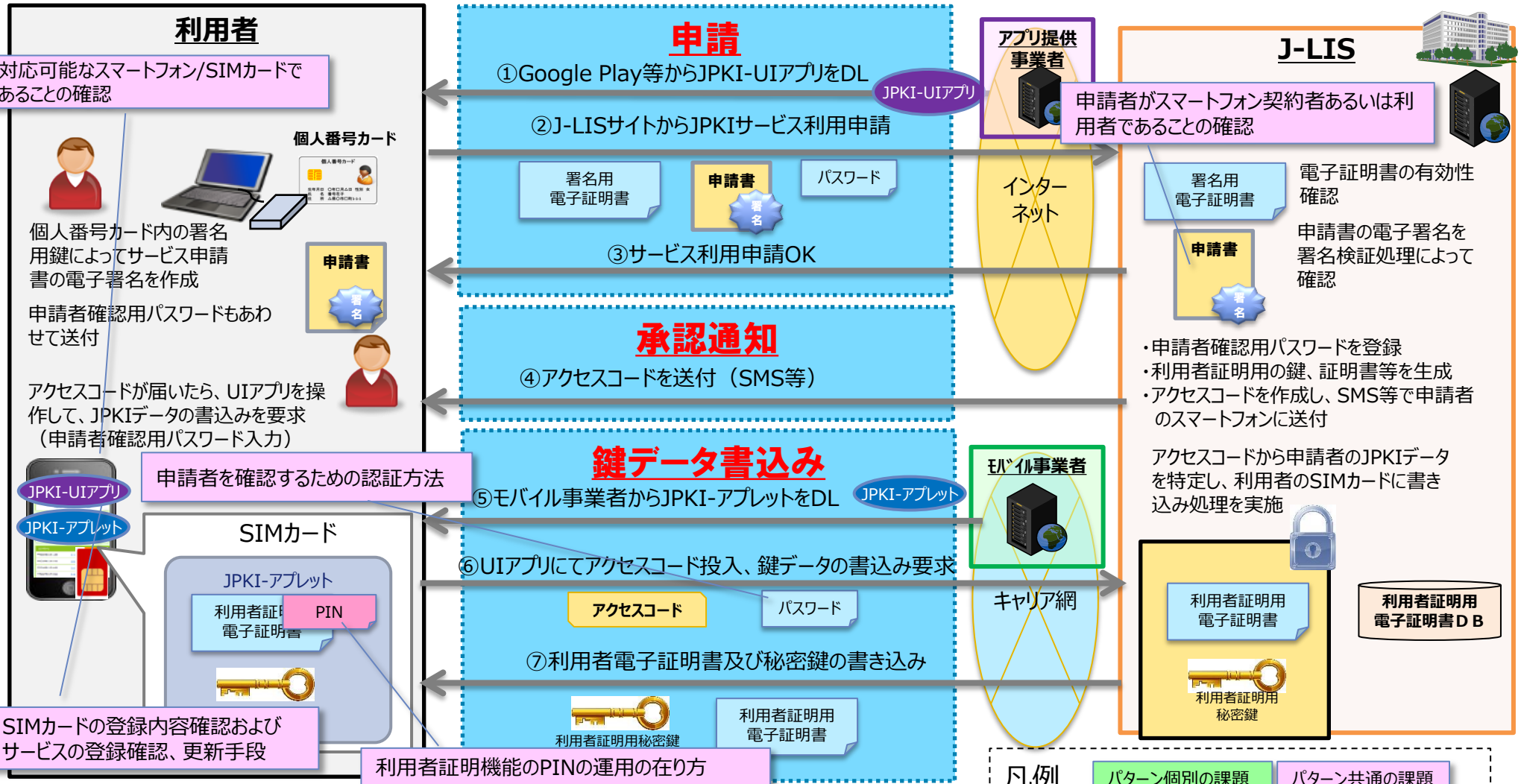
5．パターン1の課題の洗い出し
～本人限定受取郵便による本人確認と鍵データのオンライン書込み

民間のNFCクレジットサービスを踏襲した申請フロー例である。
本人確認に本人限定受取郵便を利用し、電子証明書等をネットワーク経由でダウンロードする方法である。



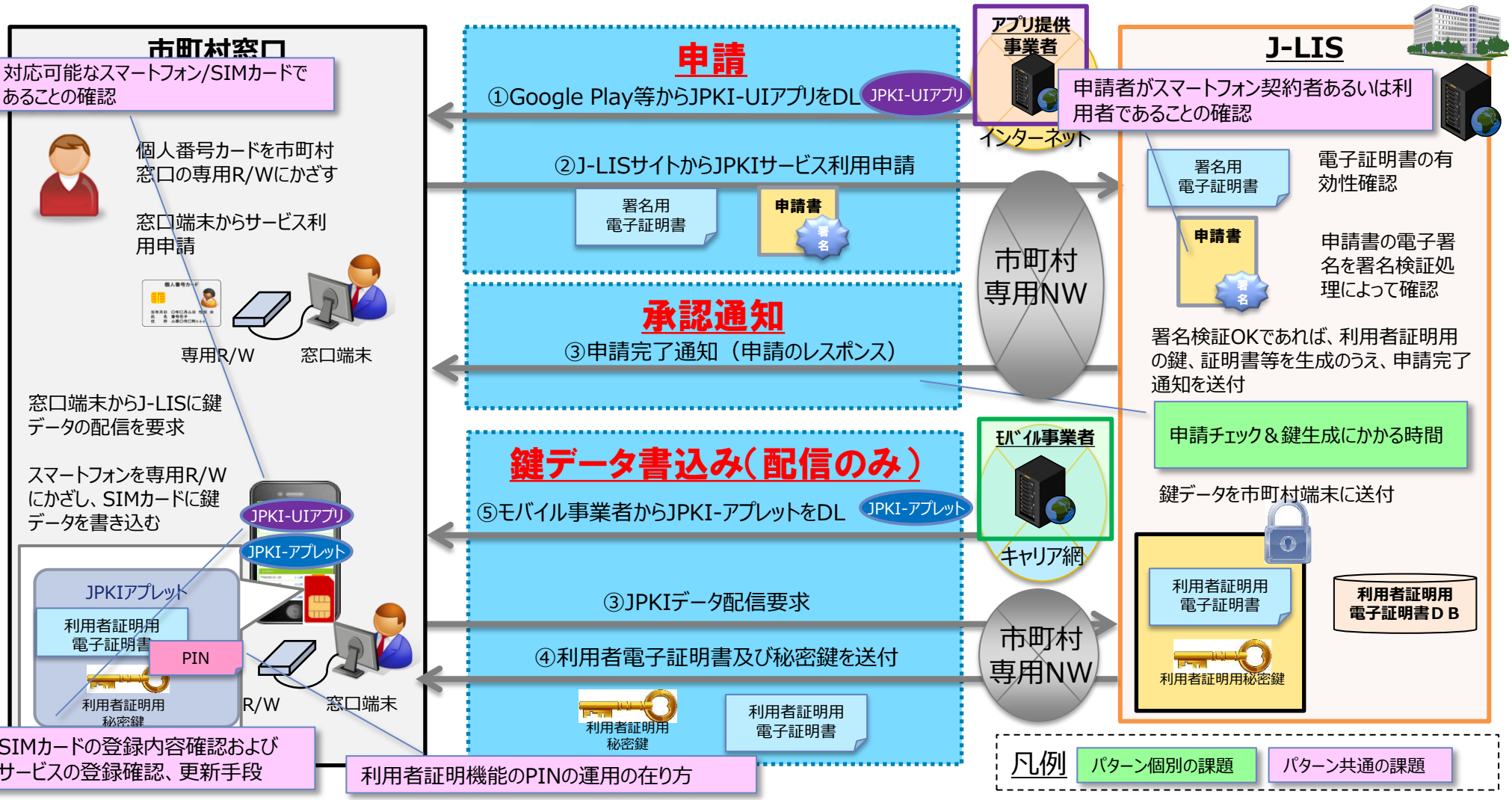
6．パターン2の課題の洗い出し
～自宅PC等による署名検証による本人確認と鍵データのオンライン書込み

個人番号カードによるオンライン本人確認機能、モバイルの通信機能を最大限生かした申請フロー例。
本人確認に署名用電子証明書による署名検証を行い、電子証明書等をネットワーク経由でダウンロードする方法である。



7．パターン3の課題の洗い出し
～窓口端末における署名検証による本人確認と鍵データのRW書込み

市町村窓口で電子証明書等をSIMカードに書き込む場合の申請フローである。
本人確認に署名用電子証明書による署名検証を行い、電子証明書等を専用RW経由で書き込む方法である。



8．運用面での課題（1/2）

利用者がサービス利用を申請し、SIMカードへの鍵データ書込みに至るまでの処理における課題を以下に示す。

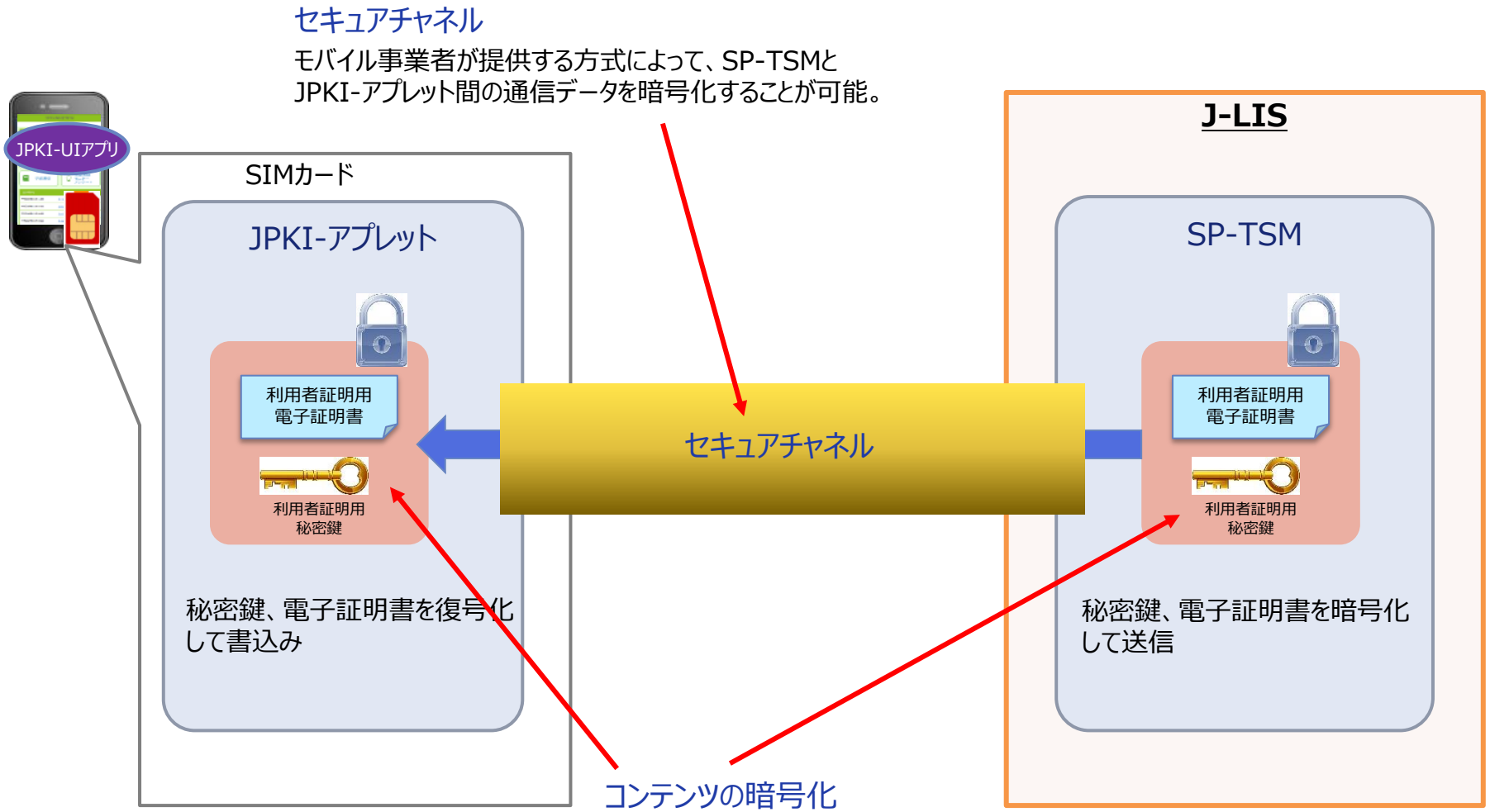
項番	フェーズ	課題	課題詳細	パターン		
				1	2	3
①	共通	対応可能なスマートフォン/SIMカードであることの確認	・スマートフォンの機種、SIMカードの種類によって利用者証明機能のダウンロードができない場合もある。 ・UIアプリでチェックするのが最も確実だが、ダウンロードする手間が掛かる。機種変更時は分からない。利用者の負担の少ない確認方法を検討する必要がある。	○	○	○
②	共通	利用者証明機能のPINの運用の在り方	・個人番号カードの場合と同様としたとき、PINの失念・ロックした際の市町村窓口で再設定等の処理が必要となり利用者の利便性を損なう。 ・オンラインPINとする、あるいは、PINロック解除等をオンラインで可能とする等の検討が必要である。	○	○	○
③	共通	SIMカードの登録内容確認およびサービスの登録確認、更新手段	・SIMカード内に格納された電子証明書の有効期限等の確認や、本サービスに登録した利用者情報の確認、更新を想定すべきではないか。	○	○	○
④	申請	申請データ（4情報含む）による個人番号カードの発行有無の確認	・J-LISにおいて申請データ（4情報を含む）から個人番号カードの保有者であり、JPKIサービスの利用者であるを確認する必要がある。 ・申請者の入力データに誤入力等、運用面で手間がかかる可能性がある。	○		
⑤	申請	申請者がスマートフォン契約者あるいは利用者であることの確認	・申請者がスマートフォンの契約者あるいは利用者であることを確認すべきか否か。	○	○	○
⑥	承認通知	住所と居所が異なる場合の対応	・本人限定受取郵便による本人確認を行う場合、住所と居所が異なる場合の対処方法を検討しておく必要がある。	○		
⑦	承認通知	申請チェック及び鍵生成時間	・申請者を窓口で待たせることになるため、ある程度の時間内で処理できる必要がある。			○
⑧	鍵データ書込み	申請者を確認するための認証方法	・クレジット事例と同様の方式として、アクセスコードの特定をパスワードによって確保する手段が考えられるが、パスワードによる確認で十分か。	○	○	

9．運用面での課題まとめ（2/2）

ＳＩＭカードへの利用者認証機能の格納における実現に向けた課題	課題の詳細化
【制度面の課題】	
(1) 利用者証明用電子証明書の二重発行の禁止（公的個人認証法第25条）	ー
(2) 利用者証明用電子証明書の発行の手順（公的個人認証法第22条）	ー
【運用面の課題】	
(1) 申請者の本人認証の方法（署名用電子証明書による署名検証、対面、本人限定受取郵便等）	④申請データ（4情報含む）による個人番号カードの発行有無の確認 ⑥住所と居所が異なる場合の対応 ⑦申請チェック及び鍵生成にかかる時間 ⑧申請者を確認するための認証方法
(2) 申請者とSIMカードとの紐付け・連携方法	⑤申請者が携帯電話契約者あるいは利用者であることを確認
(3) SIMカードの領域使用に関する責任分界点(モバイル事業者,JLIS,自治体,利用者）、費用負担の在り方	ー
(4) 通信事業者間、端末間移動した際におけるサービスの利用継続性の確保	ー
(5) 自らSIMカードを発行していないMVNOにおけるサービス提供の在り方	ー
(6) 消費者対応の在り方（操作方法、対応端末等に関する問い合わせ等）	①対応可能なスマートフォン/SIMカードであることの確認 ②利用者証明機能のPINの運用の在り方 ③SIMカードの登録内容確認およびサービスの登録確認、更新手段
(7) ユースケースの整理	利用形態として、カード代わりに利用する方法、スマートフォンに搭載されたUIアプリ等を経由してSIMカードにアクセスする方法の2通りがある（別紙3参照）。

【別紙1】鍵データ書込みにおけるセキュリティ確保手段について

・SP-TSMとJPKI-アプレット間は、モバイル事業者が提供する方式により、通信データの暗号化を行うことが可能。
・更に、秘密鍵、電子証明書の配信におけるセキュリティ対策は強化するため、SP独自の方式によって秘密鍵、電子証明書の暗号化を実施することも可能。



【別紙2】各種ライフサイクルの関する検討

SIMカードによる利用者証明機能の実現においては、ダウンロードに関する処理だけでなく、以下のような関連する機器、ソフトウェアモジュール、電子証明書等におけるそれぞれのライフサイクルにおける処理方式を検討する必要がある。

項番	対象	ライフサイクル	備考
1	スマートフォン	・新規購入前、購入、機種変更、廃棄、譲渡 ・紛失・破損・故障 ・SIMロック解除後	
2	SIMカード	・新規、有効期限切れ、バージョンアップ、廃棄、譲渡 ・紛失・破損 ・SIMロック解除後	
3	UIアプリ	・インストール、利用、ロック、削除、バージョンアップ	
4	アプレット	・インストール、利用、ロック、削除、バージョンアップ	
5	利用者証明用 電子証明書	・交付、失効、一時停止、利用	
6	利用者証明用 PIN	・設定、利用、ロック、ロック解除 ※利用者証明用秘密鍵による署名生成機能を有効にするためのPIN	補足参照

（補足）
利用者証明用のPINでは、一定回数PIN認証を失敗するとロックする仕様となることが想定される。個人番号カードと同様の運用とする場合、ロック解除は市町村窓口端末で行う。利用者の利便性は考慮すると、市町村窓口に出向くのは不便であり、SIMカードでの利用者認証機能では遠隔でのロック解除の実現を検討したい。

【別紙3】スマートフォンでの利用者証明機能の利用形態

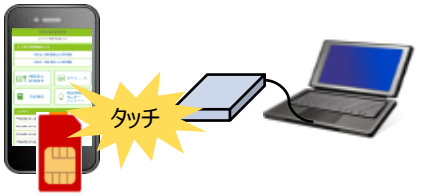
- スマートフォンでの利用者証明機能の利用形態として、以下２つのパターンが想定される。
  - カード代わりに使用：スマートフォンをリーダライタにタッチして利用者証明機能を利用する
  - UIアプリ等を経由してSIMカードにアクセス：スマートフォンアプリ等からのネットワーク経由でサービス提供者のサイトにアクセス。ログイン時等に利用者証明機能を利用する

カード代わりに使用

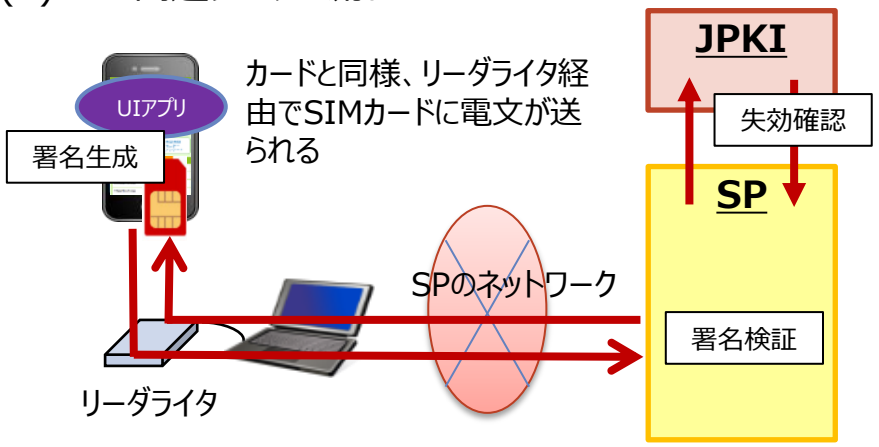
(1)利用形態

スマートフォンをリーダライタにタッチ

例）
- クレジット決済
- 健康保険証の資格確認



(2)JPKI関連データの流れ



UIアプリ等を経由してSIMカードにアクセス

(1)利用形態

スマートフォンに搭載されたUIアプリ等を操作してサービスを利用

例）
- ネットバンキングへのログイン
- お薬手帳、母子健康情報閲覧

(2)JPKI関連データの流れ

SIMカードへの電文は、モバイルネットワークを介して、UIアプリ、ブラウザを経由で送られる。