

属性認証検討SWG及びスマートフォンへの利用者証明機能 ダウンロード検討SWGの検討状況について

平成28年4月21日

項目	実証内容	ステークホルダー	当面の目標
⑤-2電子調達・電子私書箱 における公的個人認証 サービスの活用 (SWG検討課題)	<ul style="list-style-type: none"> 政府の調達システム及び電子私書箱における属性認証（法人や個人が作成する書類について、権限確認（作成権限のある者が作成））を受取機関から確認できる仕組みの検証 	<ul style="list-style-type: none"> 国 日本郵便 民間認証事業者 	<ul style="list-style-type: none"> 公的個人認証サービスを活用した法人間取引における権限の認証等の実現に向けた制度整備について検討を進め、可能な限り早期に国会に法案を提出する。
⑥利用者証明機能のスマートフォンへのダウンロード (SWG検討課題)	<ul style="list-style-type: none"> 利用者証明機能のスマートフォンへのダウンロードの実現方法及び課題解決策の検討（制度運用面・技術面） 	<ul style="list-style-type: none"> 国 モバイル事業者 地方公共団体情報システム機構 	<ul style="list-style-type: none"> 2016年度以降、利用者証明機能のスマートフォンへのオンラインによるダウンロードの実現に向けた検証を実施する。 実証結果を踏まえ、所要の制度整備、システム整備等を実施する。

属性認証検討サブワーキンググループからの 報告

制度整備の方向性(案)

1. 概要

1. 2015年の成長戦略に記載された「電子調達」「電子私書箱」等に係る目標を達成するため、所要の制度整備を行う。
2. 具体的には、法人の代表者から委任を受けた者が、(自己の個人番号カードを用いて)対面・書面なく電子的に、契約書や証明書の作成・提出等を行うことを可能とする制度を整備する。

2. 背景

1. 特に法人間で行われる電子的な取引や手続において、「安全」「安心」な情報の送受を可能とするためには、当該書面の作成者について、以下の点が書面の「受け手」に証明されることが必要。
 - ① 書面の作成者の本人性
 - ② 作成者が所属する法人の実在性
 - ③ 法人の代表者から当該作成者が委任された権限の存在(いわゆる「属性認証」)。
2. ①については「電子署名法」や「公的個人認証法」に基づき、「認定認証事業者」や「JLIS」が証明する制度、②については「商業登記法」に基づき「登記所」が証明する制度が措置済。③の「法人の代表者から委任された権限」を証明する制度が現在存在しない。

3. 方向性

法人の役員又は使用人が電子署名を行った電磁的記録の提供を受けた者に対し、当該法人の代表者が当該役員又は使用人に与えている権限の範囲を証明する業務の認定制度を設けるとともに、認定を受けた者が行う業務の円滑な実施のため、所要の措置を設ける。

法人の代表者から委任を受けた者が、(自己のマイナンバーカードを用いて)対面・書面なく電子的に、契約書や証明書の作成・提出等を行うことを可能とするため、法人の代表者から与えられている権限の範囲を表示する電磁的記録を「電子委任状」と定義し、主務大臣による電子委任状の普及に関する指針の策定、委託を受けて電子委任状を「保管」し、必要に応じ第三者に「送信」する業務の認定制度の創設等の措置を講ずる。

(1) 電子委任状等の定義

「電子委任状」とは、法人の代表者から与えられている権限の範囲を表示する電磁的記録をいう。

「電子委任状取扱業務」とは、委託を受けて電子委任状を保管し、必要に応じ第三者に送信する業務をいう。

(2) 電子委任状の普及に関する指針

主務大臣は、電子委任状の普及に関する指針を定めるものとする。

(3) 電子委任状取扱業務の認定

電子委任状取扱業務を営み、又は営もうとする者は、当該電子委任状取扱業務が(2)の指針に適合するものであることの認定を受けることができることとする。

(4) その他

上記のほか、電子委任状の普及のための所要の措置を定める。

1. 「認定を受けた事業者である旨」の表示

⇒ 認定を受けていない者が同様の表示を行うことを禁止(表示独占)

2. 以下の各観点における、認定事業者の法的位置付けを検討

○ 電気通信事業

○ 公的個人認証法上の署名等検証者

○ 国・地方公共団体の調達手続における位置付け

1. 電子委任状取扱事業者の認定要件

- ① 法人代表者性の確認方法
- ② 業務用設備の要件
- ③ その他業務の実施方法

⇒②・③については、経済産業省における検討結果を踏まえ、リモート署名を用いる場合の要件についても検討

2. 電子委任状取扱業務を利用する企業、電子委任状取扱事業者、電子委任状を受領する企業の3者間での責任分界の考え方

3. 電子委任状の失効管理、長期保存等のあり方

※必ずしも以上全ての事項を法律で定めるものではなく、政省令やガイドライン等で整理していく事項もあり得る。

属性認証検討SWG 構成員

(敬称略、五十音順)

愛場 豊和	日本電気株式会社 公共システム開発本部 シニアマネージャー
新井 聡	株式会社エヌ・ティ・ティネオメイト ITビジネス本部 プラットフォームサービス推進部 電子認証サービス担当 主査
小木曾 稔	一般社団法人新経済連盟 事務局員
小田嶋 昭浩	株式会社帝国データバンク 業務推進部 ネットサービス課
小尾 高史	東京工業大学 科学技術創成研究院 准教授
柴垣 圭吾	一般社団法人 日本ケーブルテレビ連盟 企画部 部長
下江 達二	富士通株式会社 ミドルウェア事業本部 サービスマネジメント・ミドルウェア事業部第二開発部 シニアエキスパート
砂押 宏行	日本放送協会 営業局 専任局長
竹内 英二	一般財団法人 日本情報経済社会推進協会 電子署名・認証センター センター長
主査 手塚 悟	慶應義塾大学大学院政策・メディア研究科 特任教授
長尾 慎一郎	新日本有限責任監査法人 アドバイザリー事業部 シニアパートナー
中村 克巳	ジャパンネット株式会社 技術部長
中村 信次	株式会社日立製作所 公共システム事業部 公共戦略企画部 部長
西山 晃	セコムトラストシステムズ株式会社 プロフェッショナルサポート2部担当部長
宮内 宏	五番町法律事務所 弁護士
宮脇 勝哉	日本電子認証株式会社 総合管理部 システム管理室 副室長
山田 伸治	日本郵便株式会社 トータル生活サポート事業部 部付部長
【関係省庁】	
信朝 裕行	内閣官房 情報通信技術(IT)総合戦略室 IT利活用戦略推進官
大峯 隆	法務省 民事局 商事課 法務専門官
希代 浩正	経済産業省 商務情報政策局 情報セキュリティ政策室 室長補佐

スマートフォンへの利用者証明機能ダウンロード 検討SWGからの報告

スマートフォンのSIMカードへの公的個人認証サービス（JPKI）の利用者証明機能のセキュアなダウンロードを実現するための技術的課題等について検証するとともに、当該利用者証明機能を活用したユースケースの実現に向けた推進方策について検討。

（１）SIMカード及びスマートフォンの要件の検討

- ①対象とするSIMカードの範囲、機能要件の整理
- ②対象とするスマートフォンの範囲、機能要件についての整理

（２）JPKIアプレット及びJPKI-UIアプリの要件の検討

- ①SIMカードにJPKIの利用者証明用秘密鍵及び利用者証明用電子証明書をダウンロードするのに必要なアプレット、JPKI-UIアプリを開発し、機能要件についての整理

（３）SIMカードへの安全なダウンロード方法の検討

- ①モバイル通信事業者が提供するモバイルNFCサービスプラットフォームを活用し、JPKI-アプレット及びJPKI-利用者証明用秘密鍵等を申請者のSIMカードにダウンロードするシステム（SP-TSM）の開発（別紙1）
- ②セキュアなダウンロード方法の検証（別紙2、3）
- ③MVNOのサービスで提供されるSIMカード及びSIMロックフリー端末・SIMロック解除端末でサービス提供するための対応方法の検討

（４）既存のJPKIシステムの改修に関する検討

- ①SP-TSMとJPKIシステムとの最適な機能分担、インタフェースの検討
- ②マイナンバーカードの利用者証明用電子証明書とスマートフォンにダウンロードされた利用者証明用電子証明書との紐付け、管理機能の検討

（５）運用面での課題の洗い出し

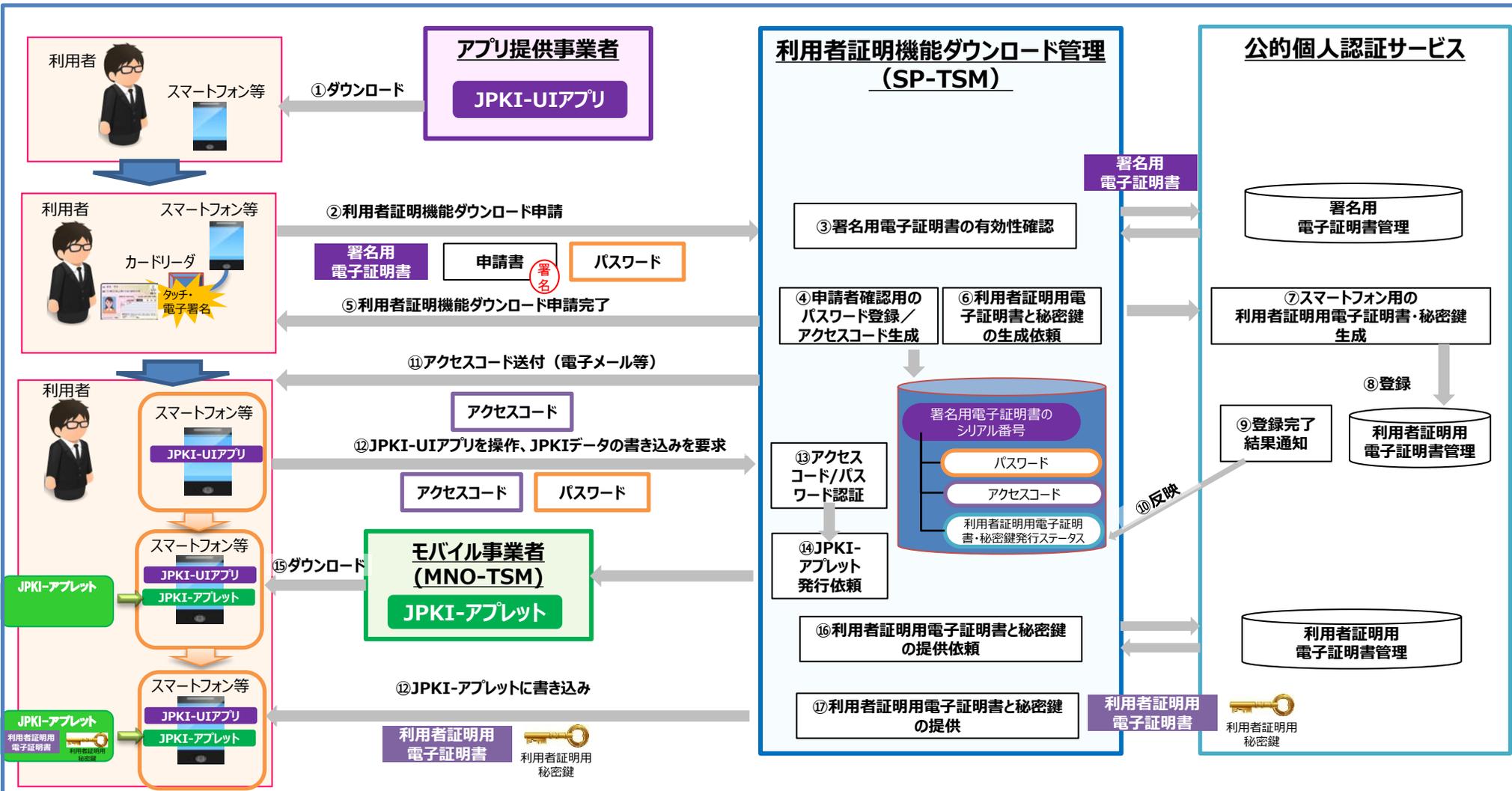
- ①マイナンバーカードを使ったオンライン申請及びオンラインダウンロードを実現する際の課題の抽出、解決策の検討

（６）ユースケースの検討

- ①スマートフォンでの利用形態にあわせて、ユーザニーズの高いユースケースを設定し、実現に向けた課題を抽出し、実現するための推進方策を検討（別紙4）。

【実現イメージの概要】

利用者はマイナンバーカードの公的個人認証サービスを使って、利用者証明機能の発行申請を行い、利用者証明用電子証明書・秘密鍵をスマートフォン内のSIMカードにオンラインによるダウンロードを実現。



- 国においては、28年度からオンラインでJPKIの利用者証明機能をセキュアにダウンロードする方法、必要なSIMカードや端末、JPKIアプリ等の機能要件、運用面の課題を検証し、必要な制度整備を行う。
- J-LISにおいては、実証事業に協力し、実証事業の成果を踏まえてシステムの有り様について検討。
- モバイル事業者（MNO及びMVNO）においては、MNO-TSMやモバイルネットワークを最大限有効に活用できるよう、実証事業に協力。また、MVNO利用者へのJPKIの利用者証明機能の提供に向けた実現方法について、MNOとMVNOが連携して検討。
- 実証事業の成果は、本SWGにおいて共有、解決策について検討。

概要	2016年度 (平成28年度)	2017年度 (平成29年度)	2018年度 (平成30年度)	2019年度 (平成31年度)
国	技術面からの課題検証	運用面からの課題検証	法案提出・運用ルール等整備	
J-LIS	連携 実証実験 実現に向けた課題の抽出、実現方法、課題解決策の検討		JPKIシステム改修 SP-TSM、JPKIアプリ等の商用開発	テスト運用・本番開始
モバイル事業者 (MNO/MVNO)	実証検証への協力 MVNO利用者への提供に向け、連携して検討		運用ルールを整備するとともに必要に応じてシステム改修	サービス開始
アプリサービス提供者		モバイルサービス提供者によるサービス具体化		サービス開始

1. 検討にあたっての前提条件

- (1) SIMカードへのダウンロード申請は、マイナンバーカード交付済みである利用者であることを前提に検討する。
- (2) SIMカードへのダウンロード申請は、マイナンバーカードの公的個人認証サービスを使った本人確認、電子署名を使って行うものを第一の方法として考え、実現に向けた課題解決策について整理する。
- (3) JPKIアプレット、利用者証明用秘密鍵、利用者証明用電子証明書のダウンロードはオンラインでの実現を前提に検討を行う。
- (4) JPKIアプレットのSIMカードへのダウンロードは、既存のMNO-TSM装置を前提とし、利用者証明用秘密鍵、利用者証明用電子証明書のダウンロードにあたっては、モバイル通信事業者が提供しているモバイルNFCサービスプラットフォームを活用し、必要なシステムを構築する。実現方法の検討にあたっては、セキュリティに配慮しつつ、既存の仕組みを最大限活用できるよう考慮する。
- (5) 検討に当たっては、MVNOのサービス利用者や、SIMロックフリー端末・SIMロック解除端末の利用者も考慮する。
- (6) ユースケースの検討にあたっては、スマートフォンの特徴をいかしたユースケースであること、利用者の裾野が広いことなど利用ニーズが高いものを選定し、検証する。

2. 検証項目

(1) SIMカード及びスマートフォンの要件の検討

- 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を踏まえ、民間モバイルNFCサービス（クレジット）を参考に、対象とするSIMカードの対象範囲、JPKIの利用者証明用秘密鍵及び利用者証明用電子証明書をダウンロードするための必要な機能要件※について整理を行い、実現方法を検討すること（MVNOの提供するSIMカードを含む）。

※ 機能要件の例：

暗号アルゴリズム、メモリ容量、アプレット、パーソナライズデータのセキュアダウンロードするためのSIMの機能、SIM間の利用者証明機能の移転やSIMの廃棄・失効等に関する要件、PINなし認証 等

2. 検証項目(続き)

- ② JPKIの利用者証明用秘密鍵等のダウンロードを可能とするスマートフォン（例：NFC対応スマートフォンであること（Android）等）、機能要件について整理を行うこと（SIMロックフリー端末・SIMロック解除端末を含む）。

※機能要件の例

- ・ダウンロード時の書き込みI/F(携帯電話網、Wi-Fi)
- ・NFC対応スマートフォンとしての要件
- ・MNO-TSMとの通信機能、SIMの読み書き機能(キャリア間の仕様差分への対応、MVNOへの対応)

(2) JPKI-アプレット及びJPKI-UIアプリの要件の検討

- ① SIMカードにJPKIの利用者証明用秘密鍵等をダウンロードするのに必要なJPKIアプレットを開発し、JPKIアプレットの機能要件の整理を行うこと。その際、マルチベンダ対応の共通アプレット等効率的な開発・品質確保の方法やSIM毎にカスタマイズの要否についても検討すること（速度等の機能要件への対応等）。
- ② SIMカードにJPKIの利用者証明用秘密鍵等をダウンロードするのに必要なJPKI-UIアプリを開発すること。その際、スマートフォンのOSのバージョンや製造メーカー、キャリアに極力依存しないJPKI-UIアプリの構成、開発・品質確保の方法を検討すること。

(3) SIMカードへの安全なダウンロード方法の検討

- ① 利用者の利便性とセキュリティを確保した、パソコン、スマートフォン等からの利用者証明機能のオンラインによる申請方法を検証すること。その際、JPKI-アプレットを当該申請者が指定する端末にのみダウンロードする仕組みを検証すること。
- ② モバイル通信事業者が提供するモバイルNFCサービスプラットフォームを活用し、JPKI-アプレット及び利用者証明用秘密鍵等を申請者のSIMカードにダウンロードするシステム（SP-TSM）を開発すること。

2. 検証項目（続き）

（3）SIMカードへの安全なダウンロード方法の検証（続き）

- ③ 既存のモバイルNFCサービスプラットフォームの実現方法を踏まえ、SIMカードへのJPKIアプレットのダウンロード時におけるダウンロードに必要な鍵の格納場所及びセキュアなダウンロード方法を検証すること。必要に応じて、SP独自のセキュリティ対策を検討すること。【別紙1，別紙2】
- ④ JPKIの利用者証明機能を格納するSIMの登録・管理方法について検討を行うこと。（オンライン申請を前提とし、SP-TSM側でのSIMの識別情報の利用の可否等）
- ⑤ 例えば、以下のような時、モバイル事業者間におけるSIMの仕様差分への対応方法について整理すること。
 - ア JPKIアプレットをSIMカードにダウンロード時
 - イ パーソナライズ（利用者証明用秘密鍵等のSIMへのダウンロード）時 等
- ⑥ MVNOのSIMカード及びSIMフリー端末・SIMロック解除端末等への対応方法について検討すること。

（4）既存JPKIシステムの改修に関する検証

- ① SP-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
- ② マイナンバーカードの署名用電子証明書及び利用者証明用電子証明書とスマートフォンにダウンロードされた利用者証明用電子証明書との紐付け機能、マイナンバーカードあるいはスマートフォンの更新・紛失時におけるスマートフォンに格納された利用者証明用電子証明書の取扱等）を整理すること。

（5）JPKIの利用者証明機能のダウンロードを実現するにあたっての運用面の検討

- ① マイナンバーカードを使ったオンライン申請を検討の前提とした場合における、署名用電子証明書による署名検証による本人確認を行う上での課題の洗い出し、解決策を検討すること。

2. 検証項目(続き)

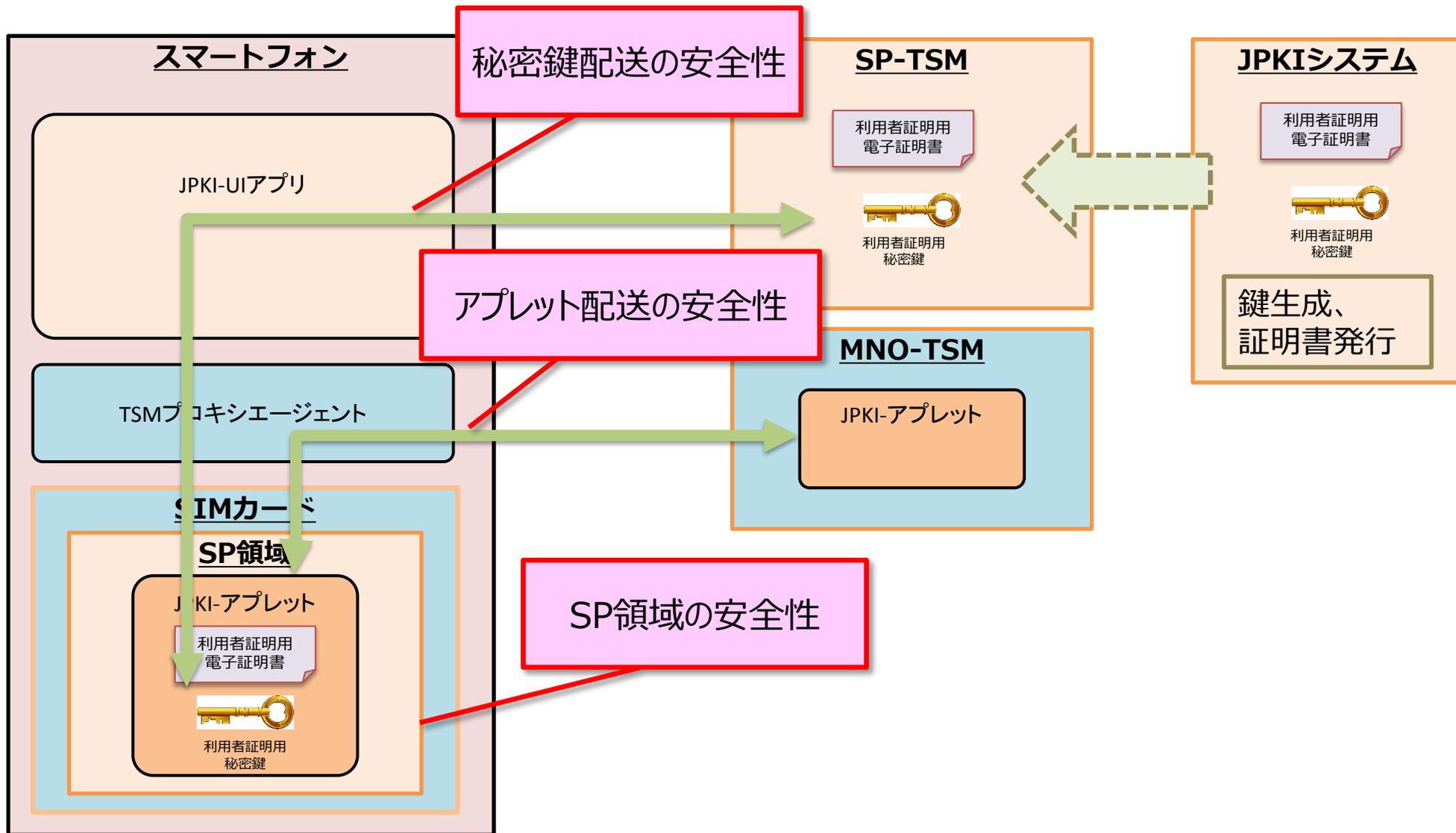
(5) JPKIの利用者証明機能ダウンロードを実現するにあたっての運用面の検討(続き)

- ② マイナンバーカードを使ったオンライン申請による場合、JPKIの利用者証明機能をダウンロードするSIMカードの識別方法、申請者が当該携帯電話の契約者あるいは利用者であることを確認の要否等を検討すること。
- ③ PINを失念・ロックした際の再設定方法（マイナンバーカードの場合、市町村窓口端末において対応）
- ④ SIMカードに格納された電子証明書の有効期限等の確認方法
- ⑤ JPKIの利用者証明機能ダウンロードに当たっての関係者の役割分担、責任分解点を整理すること。
- 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）について検討すること。
- ⑦ SIMカード間の利用者証明機能の移転方法について整理すること（MNO-MVNO間含む）。
- ⑧ 技術的課題を検討する中で マイナンバーカードを使ったオンライン申請・ オンラインダウンロードを実現する際の運用面での課題の整理し、対応方法について整理すること。

3. ユースケースの検討

(6) ユースケースの検討

- ① 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通りがあることを前提としてユースケースを設定し、実現に向けた課題の抽出、解決策を検証すること。
- ② ①で検討したユースケースの実現に向けた推進方策について検討すること。

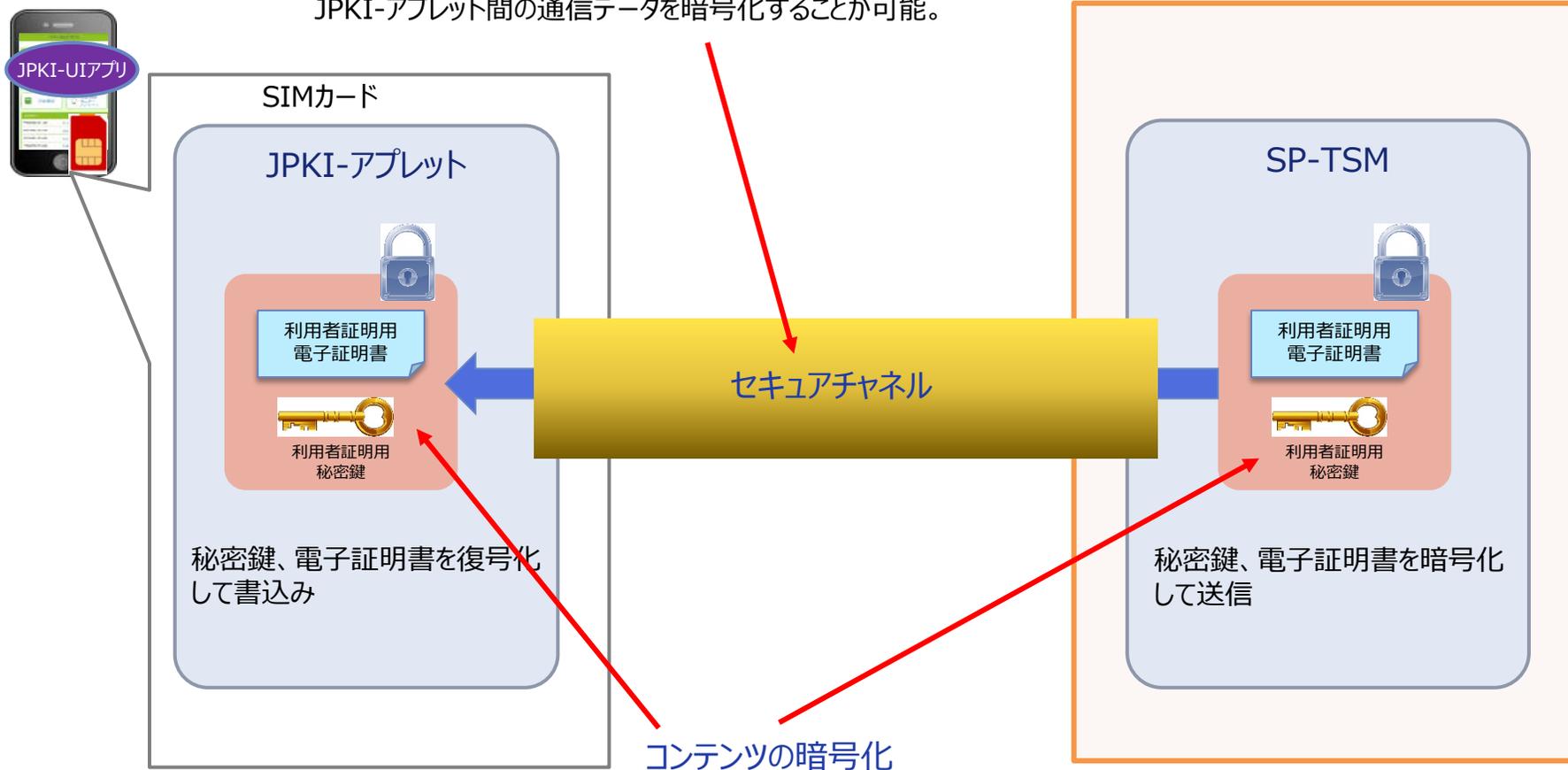


【別紙3】鍵及び電子証明書の書込みにおけるセキュリティ確保について

- SP-TSMとJPKI-アプレット間には、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。

セキュアチャネル

モバイル事業者が提供する方式によって、SP-TSMとJPKI-アプレット間の通信データを暗号化することが可能。



コンテンツの暗号化

SP独自の方式により、秘密鍵、電子証明書等を暗号化し、セキュリティレベルを高めることが可能。

- 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

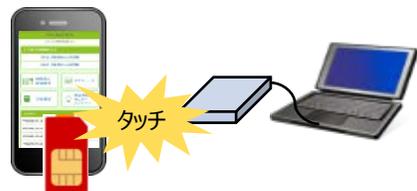
カード代わりに使用

(1)利用形態

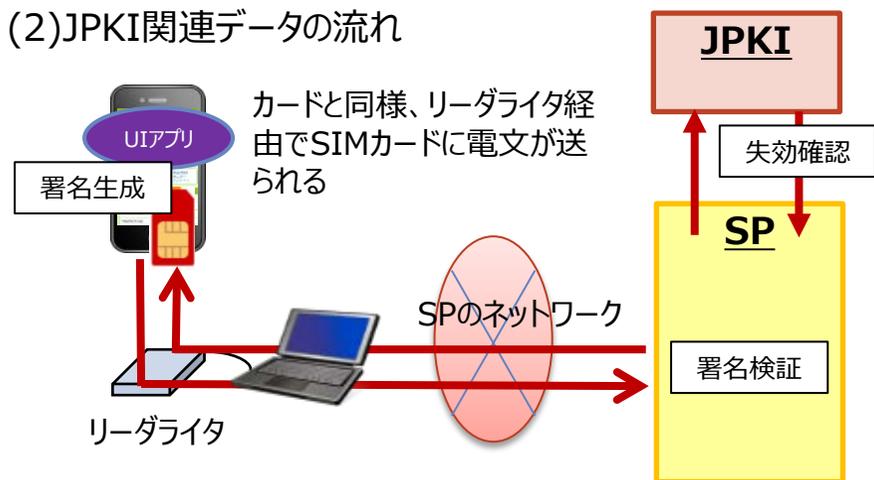
スマートフォンをリーダライタにタッチ

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アプリ等を利用してサービスを利用

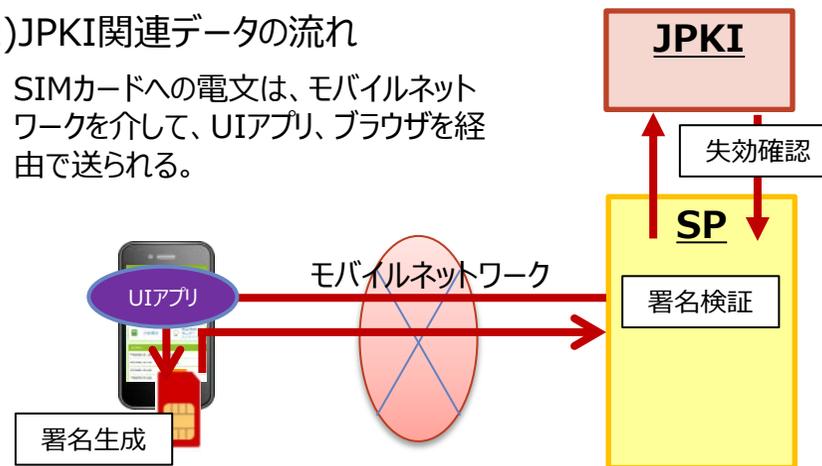
例)

- 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、ブラウザを経由して送られる。



スマートフォンへの利用者証明機能ダウンロード検討SWG 構成員

(敬称略、五十音順)

【有識者】

小尾 高史 国立大学法人東京工業大学 科学技術創成研究院 准教授
主査 手塚 悟 慶應義塾大学大学院 政策・メディア研究科 特任教授

【自治体】

新井 剛 前橋市 政策部情報政策課長
白戸 謙一 三鷹市 企画部情報推進課番号制度担当課長

【通信事業者】

金山 由美子 KDDI株式会社 商品・CS統括本部 サービス企画本部
パーソナルサービス企画部 部長
ソフトバンク株式会社 プロダクト&マーケティング統括
サービスプラットフォーム戦略開発本部 プラットフォーム企画統括
部 アプリケーション部 部長
橋井 崇
田村 穂積 株式会社NTTドコモ 執行役員 スマートライフ推進部長
庭野 栄一 日本電信電話株式会社 研究企画部門 担当部長

【業界団体等】

川関 雅文 一般社団法人テレコムサービス協会 MVNO委員会運営分科会
主査
斉藤 隆志 一般社団法人電波産業会 研究開発本部移動通信グループ
主任研究員
林 徹 地方公共団体情報システム機構
個人番号センター 公的個人認証部 次長

【ベンダ】

木村 充洋 富士通株式会社 ネットワークサービス事業本部
FENICS事業部 モバイルサービス部長
高橋 尚 エヌ・ティ・ティ・コミュニケーションズ株式会社
第三営業本部 営業推進部門 担当部長
蔦田 剛士 ジェムアルト株式会社 モバイルコム事業本部兼
M2M事業本部兼OEM&CE事業本部 本部長
野田 茂門 日本電気株式会社公共システム開発本部
シニアマネージャー
松田 純一 株式会社日立製作所 公共システム事業部
公共システム推進第一部 担当部長
宮野 哲紀 大日本印刷株式会社 情報イノベーション事業部
C&Iセンター ソリューションエンジニアリング本部
シニアエキスパート
村上 貴夫 株式会社エヌ・ティ・ティ・データ 第一公共事業本部
e-コミュニティ事業部 第二ビジネス統括部 統括部長

【ユーザ企業】

阿部 展久 株式会社みずほフィナンシャルグループ
インキュベーションPT PT長
吉本 和彦 フィデアホールディングス株式会社 顧問

経済財政運営と改革の基本方針2015(平成27年6月30日閣議決定)

第2章 経済の好循環の拡大と中長期の発展に向けた重点課題 1 我が国の潜在力の強化と未来社会を見据えた改革 (IT・ロボットによる産業構造の改革)

「世界最高水準のIT利活用社会」の実現に向け、「世界最先端IT国家創造宣言」に基づく施策を着実に進める。(略) **個人番号カード、電子私書箱等を活用したワンストップサービスや政府調達全工程の電子化等を通じ、公共サービスの改革を進める。(略)**

日本再興戦略 改訂2015 (平成27年6月30日閣議決定)

一. 日本産業再興プラン5. 世界最高水準のIT社会の実現

(3) 新たに講ずべき具体的施策 ii) 安全・安心を前提としたマイナンバー制度の活用

② 個人番号カードの普及・利活用の促進

(略) 2017年度以降の**個人番号カードのキャッシュカードやデビットカード、クレジットカードとしての利用**やATM等からのマイナポータルへのアクセスの実現に向けて、個人情報保護や金融犯罪の防止等が十分確保されることを前提に、民間事業者と検討を進める。加えて、**個人番号カードの公的個人認証機能について、2017年中のスマートフォンでの読み取り申請の実現や、2019年中の利用者証明機能のスマートフォンへのダウンロードを実現すべく、必要な技術開発及び関係者との協議を進める。**(略) また、個人番号カードにより提供されるサービスの多様化を図るために、**個人番号カードを利用した、住民票、印鑑登録証明書、戸籍謄本等のコンビニ交付について、来年度中に実施団体の人口の合計が6千万人を超えることを目指す。**さらに、**住民票を有しない在留邦人への個人番号カードの交付や、海外転出後の公的個人認証機能の継続利用等のサービスの2019年度中の開始を目指し、検討を進める。**

④ マイナポータルを活用したワンストップサービスの提供

個人番号カードの公的個人認証機能を活用し、官民で連携した仕組みを設け、電子私書箱機能を活用した官民の証明書類の提出や引越・死亡等に係るワンストップサービスや、テレビ・スマートフォン等を活用した電子的な行政手続等への多様なアクセスを、2017年1月のマイナポータルの運用開始に合わせて順次実現する。

⑤ 個人番号カード及び法人番号を活用した官民の政府調達事務の効率化

法人の代表者から委任を受けた者が、対面・書面なく電子申請・電子契約等を行うことを可能とする制度的措置及びシステム構築に向けた検討を行い、個人番号カード及び法人番号を用いて、政府調達に関する入札参加資格審査から契約までの一貫した電子化を2017年度から順次開始する。また、入札資格情報や調達情報の国・地方公共団体間での共有や、調達情報の取得を容易にすることで、民間事業者による参入を促進すべく、2017年度から順次地方公共団体での上記システムの利用を可能とする。