NTT DATA
Global IT Innovator

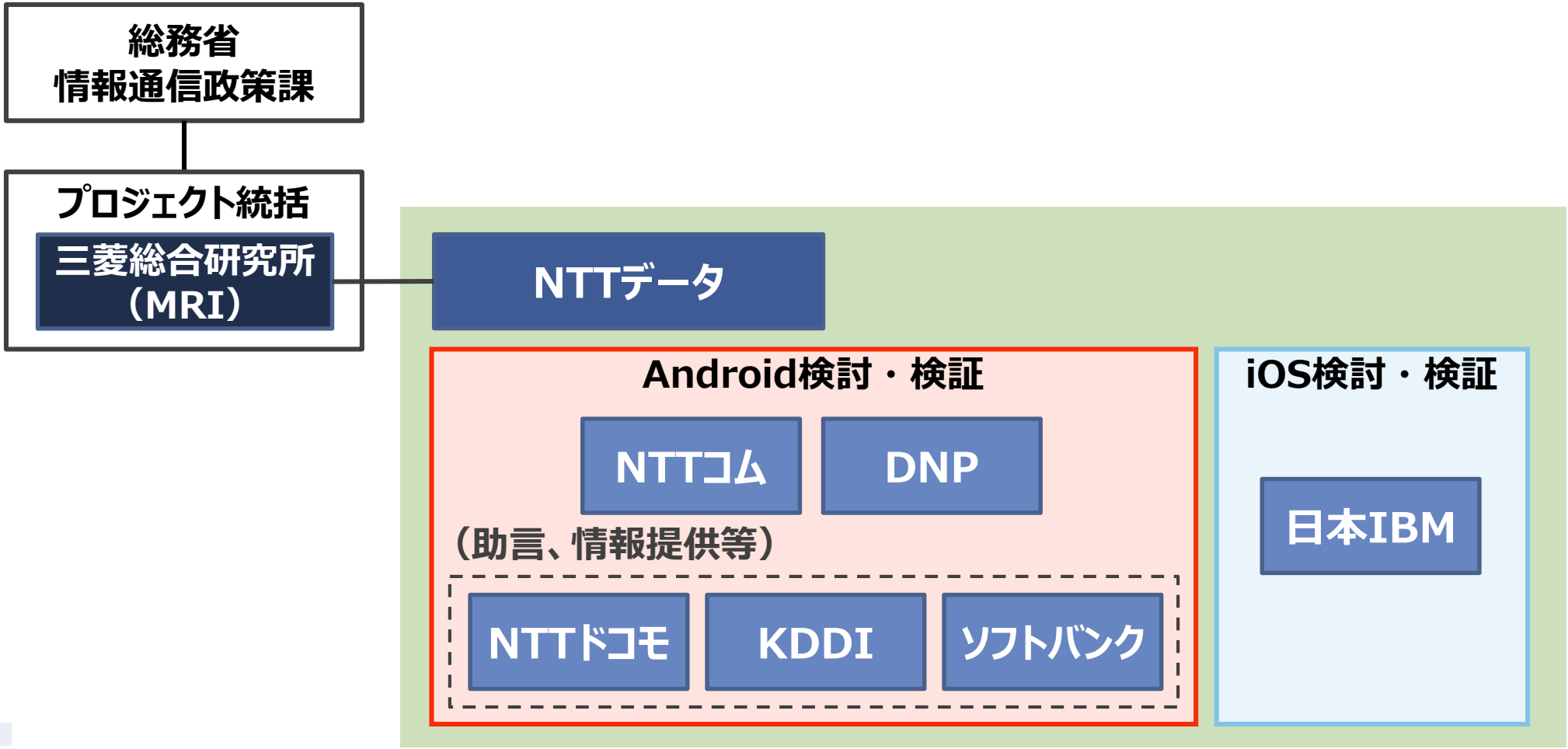
資料７－３

スマートフォンのSIM カード等へ利用者証明機能を搭載するための課題への対応方策の検討

平成29年11月28日

1. 実施体制について

本実証事業の実施体制は以下の通りです。



NTT DATA

2. 平成29年度実証事業の背景と基本的考え方

対面での本人確認を反映した検討及び検証を行うこととしています。

H28年度実証結果

利用者証明機能ダウンロードの検証
モバイル回線等を使ったオンライン発行

【システム検証】

・実証システムを構築
・Android、iOS双方の実現性を確認

【安全性対策検討】

・有識者を交えた評価会を実施
・技術面、運用面での安全性対策を検討し、課題を提起

対面での確実な本人確認の実施

H28年度実証では以下の検討が十分ではなかった。
①市町村窓口における対面での本人確認
②市町村窓口に設置された統合端末から発行
③SIM入替えのリスク及び対策検討

H29年度実証（調査研究及び検証）

昨年度の実証結果を活かしつつ、窓口発行方式についての課題を検討。
・市町村窓口における申請、発行フローの検討及び検証
・SIM差し替え等、体系的なリスクの整理、検討
・窓口ICカードRWとスマートフォンのNFC通信実態調査

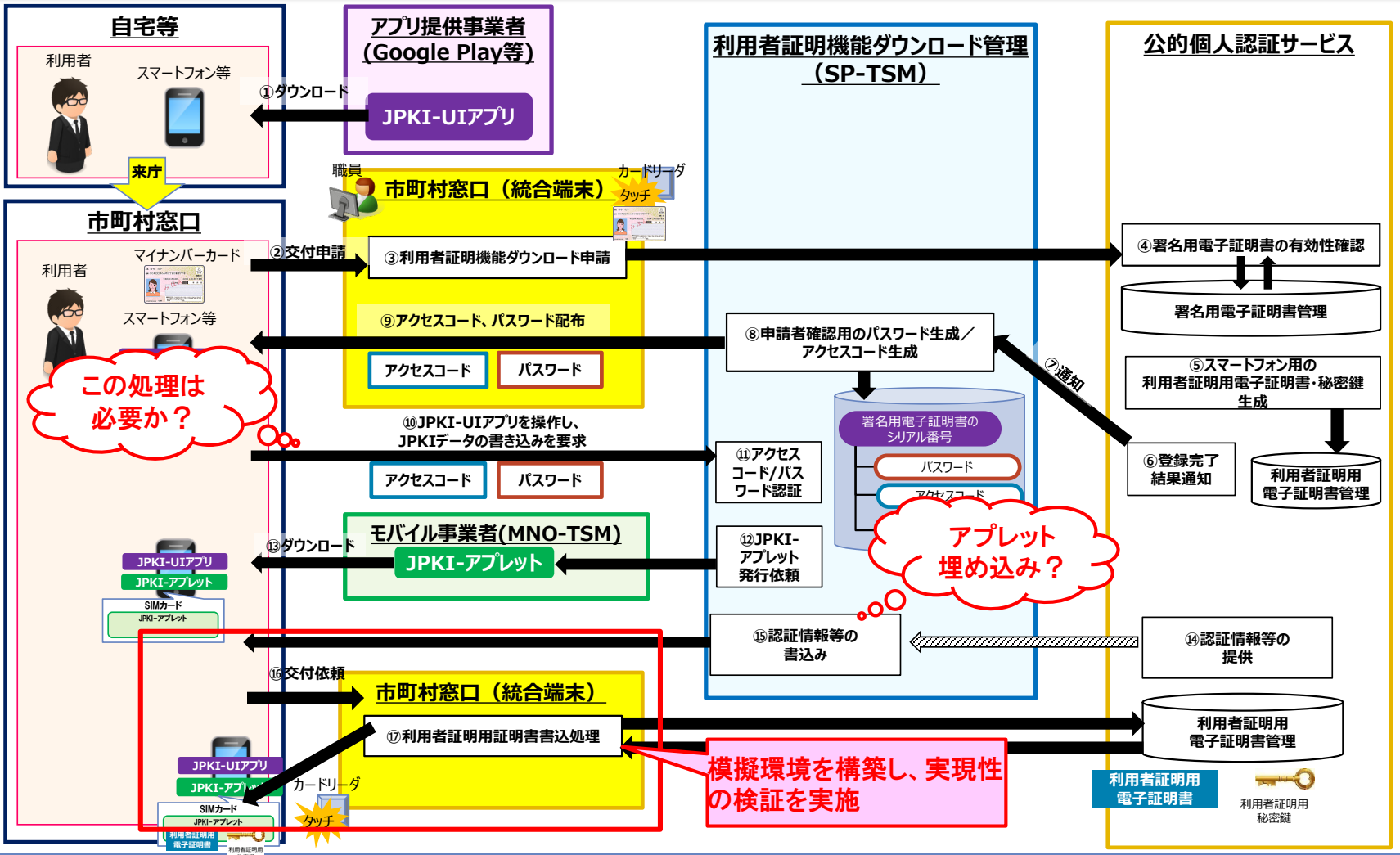
3. スマートフォンのSIM カード等へ利用者証明機能を搭載するための課題への対応方策の検討

- 具体的な検討項目は以下の通りです。
- H28年度実証と同様に、Android端末・iOS端末での実現方法について、有識者との評価会を実施します。

実施項目		Android	iOS	説明
課題①	市町村窓口における申請から電子証明書のSIMカード等への格納に関する安全性対策の検討及び検証	○	○	電子証明書等の記録媒体：Android搭載スマートフォンはSIMカード、iOS搭載スマートフォンはKeychain領域
課題②	市町村窓口におけるPINの初期化、変更に関する検討及び検証	○	○	
課題③	SIMカード（電子証明書を格納済み）を本人以外のスマートフォンに差し替えて利用されることを防止する対策の検討	○	ー	iOS搭載スマートフォンでは電子証明書等の記録媒体（Keychain領域）が端末と一体であり、着脱不可のため対象外
課題④	電子証明書の発行時及び利用時の脅威とその対策についての検討	○	○	
課題⑤	市町村窓口での各種申請を基本とする電子証明書のライフサイクル（失効、更新、再発行等）の検討	○	○	
課題⑥	業務アプリからSIMカード等へのアクセス方法の検討	○	○	
課題⑦	市町村窓口のICカードRWとスマートフォンの通信確認	○	ー	iOS搭載スマートフォンは、ICカードRWからの電子証明書等の読取りは不可のため対象外
課題⑧	現行制度への影響調査	○	○	

4. (1)Android：課題①及び②窓口端末を想定した処理フロー

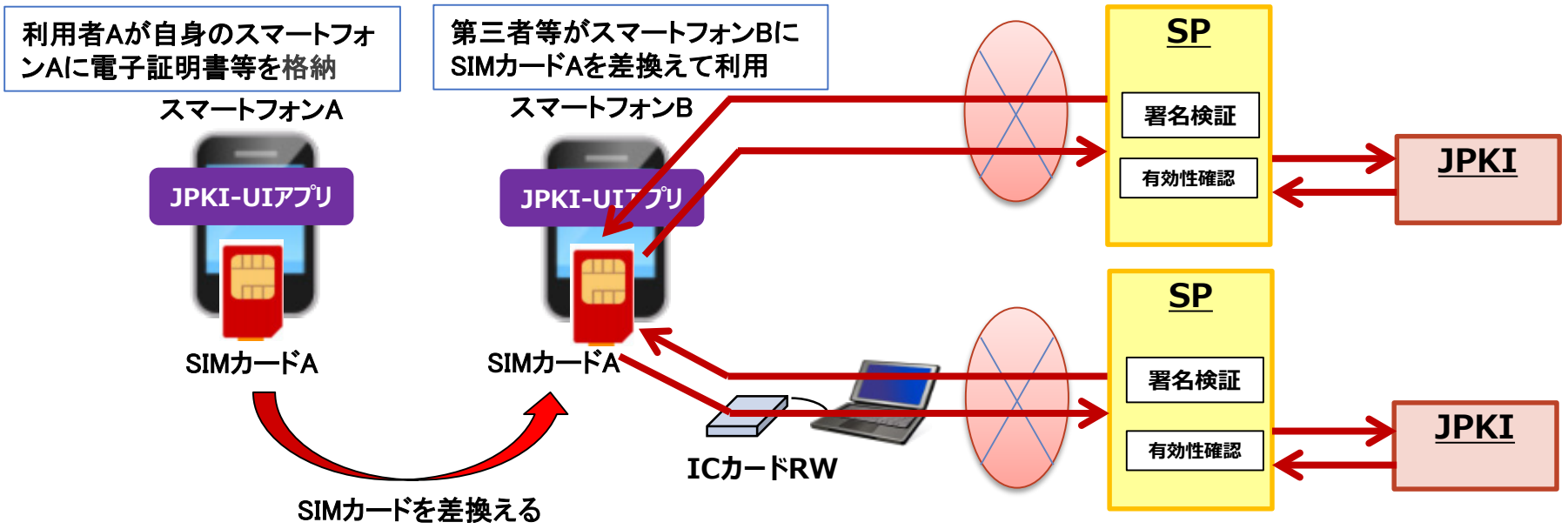
市町村窓口端末を想定した処理フローを検討します。現時点で想定される全体フロー(Androidの場合)を以下に示します。PINの初期化、変更等を含めた処理フローを検討します。



4. (2)Android：課題③SIMカード差し替えリスクと対策

課題検討項目		検討項目	備考
課題③	SIMカード（電子証明書を格納済み）を本人以外のスマートフォンに差し替えて利用されることを防止する対策の検討	JPKI-UIアプリ経由でSIMカードにアクセスする利用形態における防止策を検討	
		ICカードRW経由でSIMカードにアクセスする利用形態における防止策を検討	Android搭載スマートフォンでは電源OFF状態でもかざして利用が可能である点を考慮
		モバイル事業者が提供するリモートロックサービス（※1）による防止策を検討	

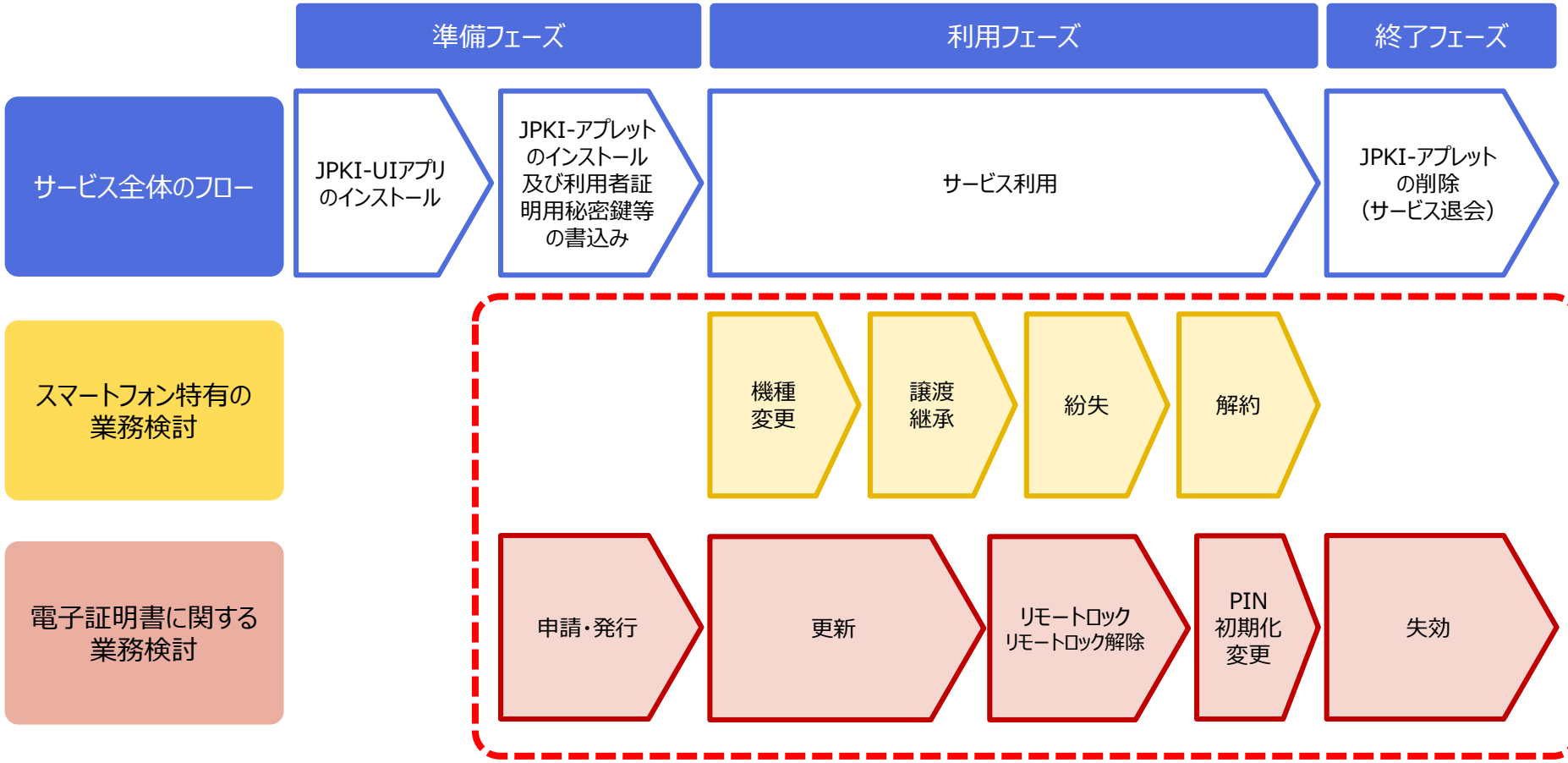
※1：利用者の申請によってスマートフォン及びSIMカードの機能を一時停止状態にするサービス



（補足）課題④では電子証明書の発行時、利用時の脅威と対策を体系的に整理する。

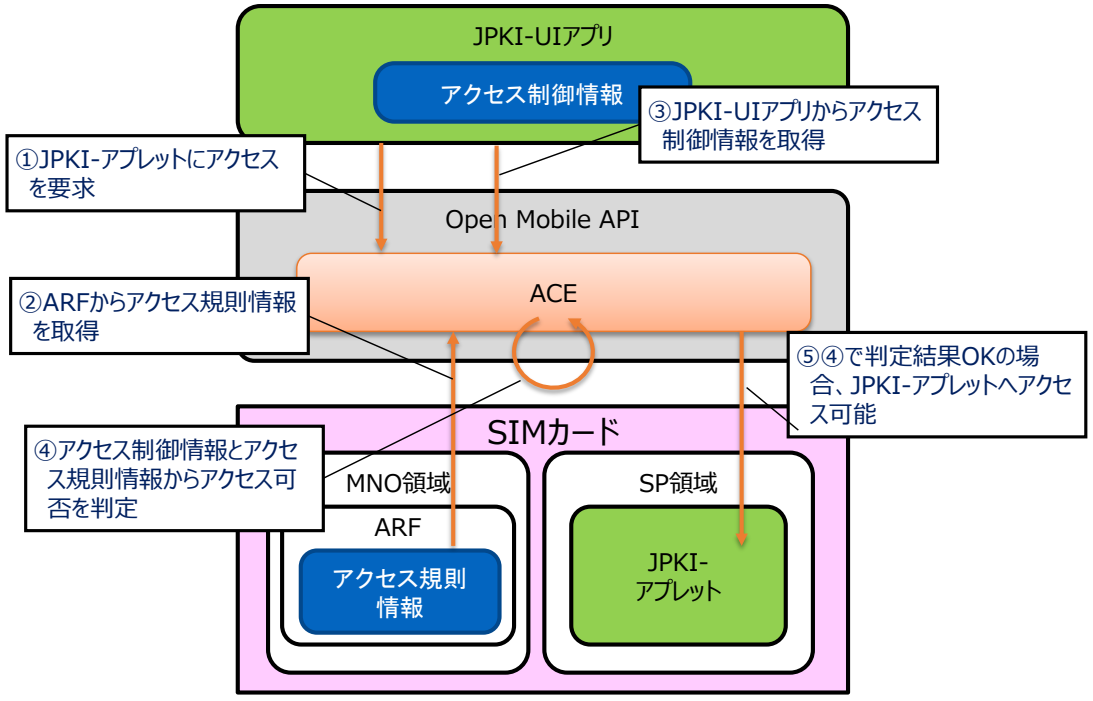
6. Android／iOS共通：課題⑤電子証明書ライフサイクルの検討

・市町村窓口での申請を基本として、電子証明書のライフサイクル業務（更新、失効等）を検討します。
・スマートフォン特有の業務（機種変更、紛失、解約等）も併せて検討します。



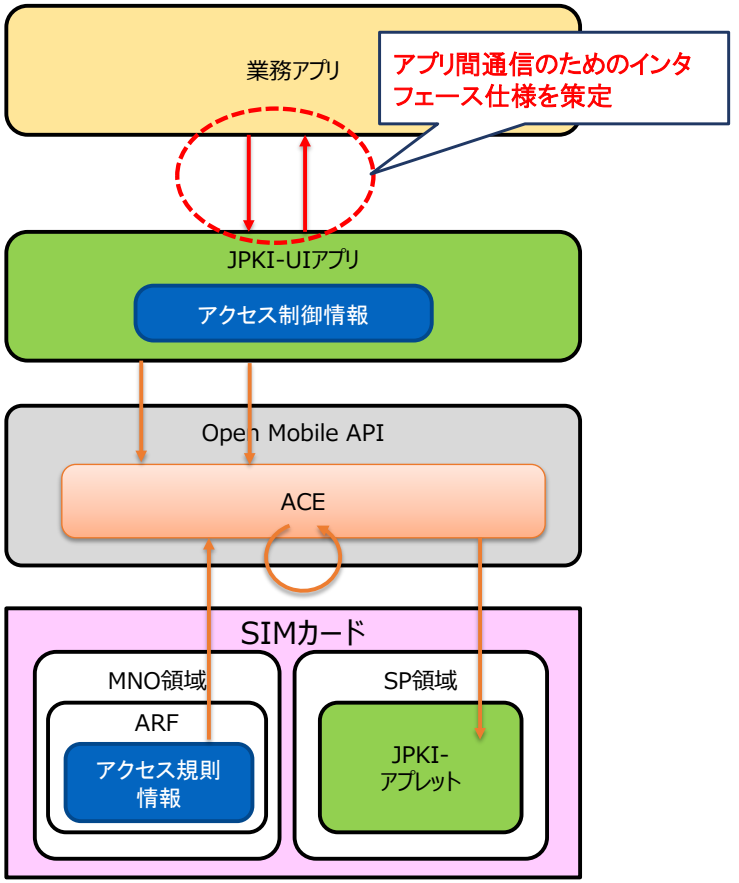
4. (3)Android：課題⑥業務アプリからSIMカードへのアクセス方法

・Androidスマートフォンでは、JPKI-アプレットへのアクセスはACEと呼ばれる方式でアクセス制御が行われます。
・本検討ではJPKI-UIアプリとSIMカードによって行われるアクセス制御を活用して、業務アプリからJPKI-UIアプリ経由でJPKI-アプレットにアクセスする方法を検討します。



ACE：Access Control Enforcer
ARF：Access Rule File

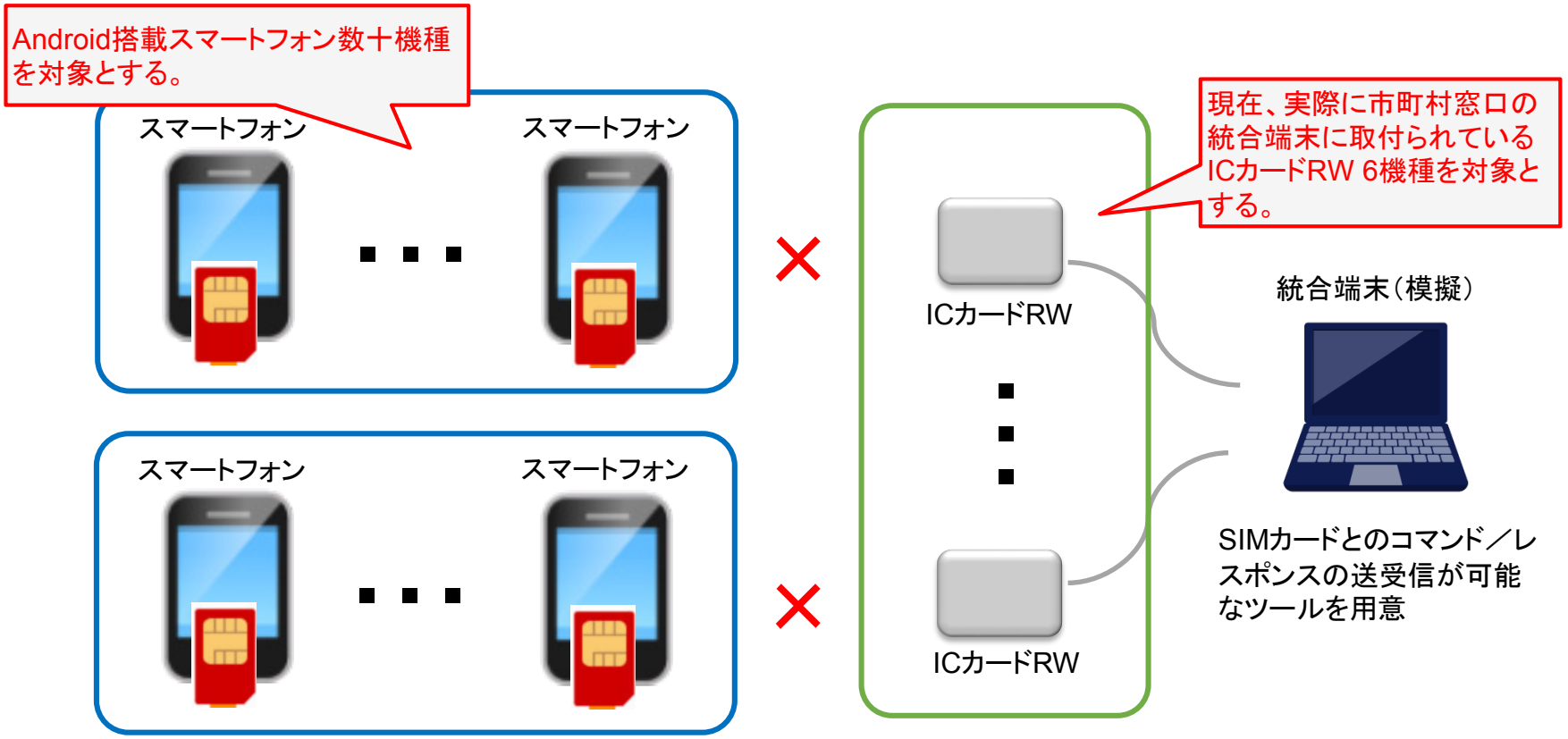
図①　アプレットへのアクセス制御の仕組み



図②　業務アプリからJPKI-アプレットへのアクセス方式

4. (4)Android：課題⑦ICカードRWとスマートフォンの通信確認

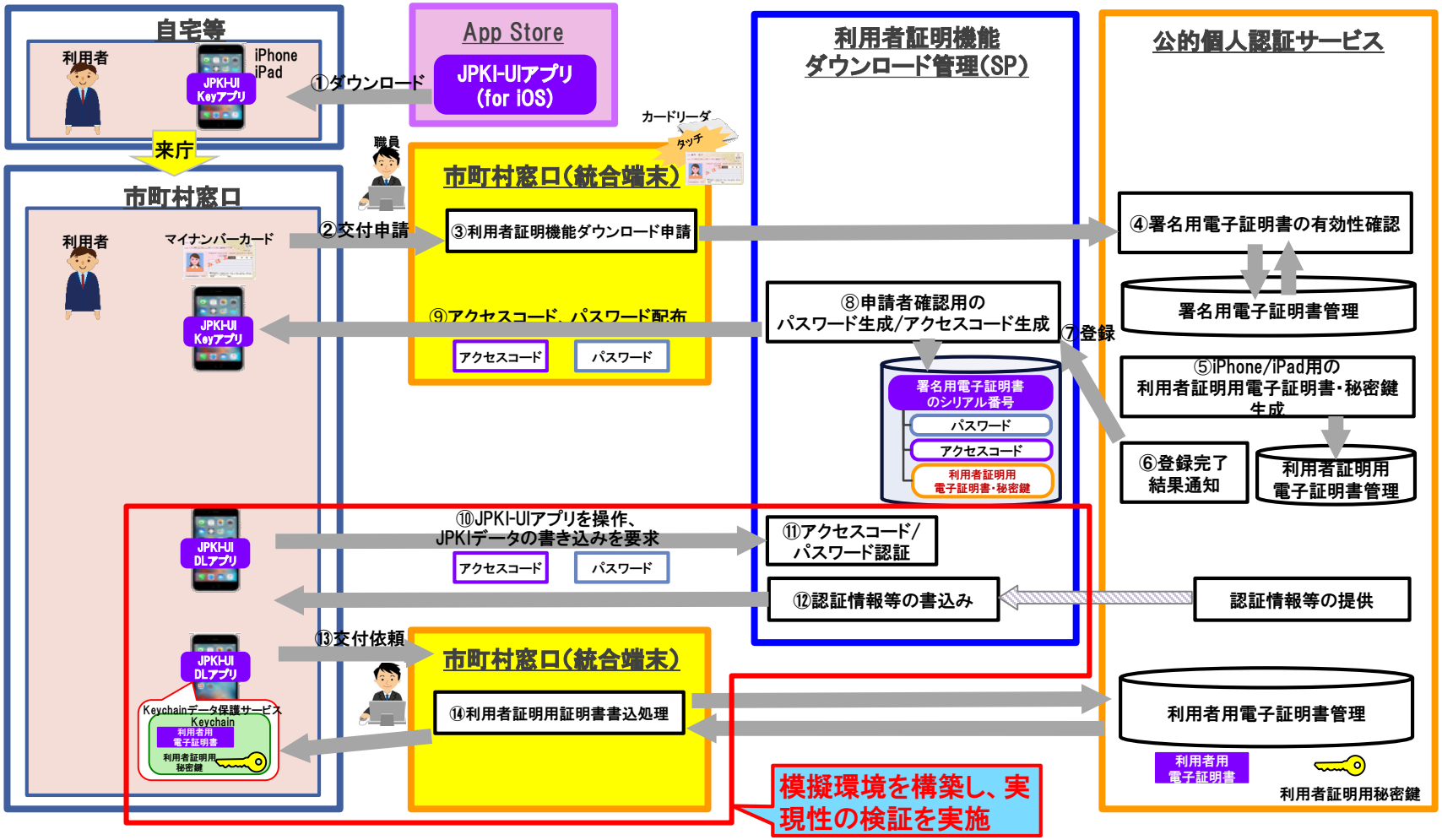
・現在、NFC機能を搭載したAndroidスマートフォンは150機種以上存在すると言われています。
・これらの機種が窓口のICカードRWでどの程度通信可能なのかわかっていません。
・今後のスマートフォン対象機種の選定基準策定に向けて、実態調査を行い、基準策定のための提言を行います。



NTT DATA

5. (1)iOS：課題①及び②窓口端末を想定した処理フロー

市町村窓口端末を想定した処理フローを検討します。現時点で想定される全体フロー(iOSの場合)を以下に示します。PINの初期化、変更等を含めた処理フローを検討します。

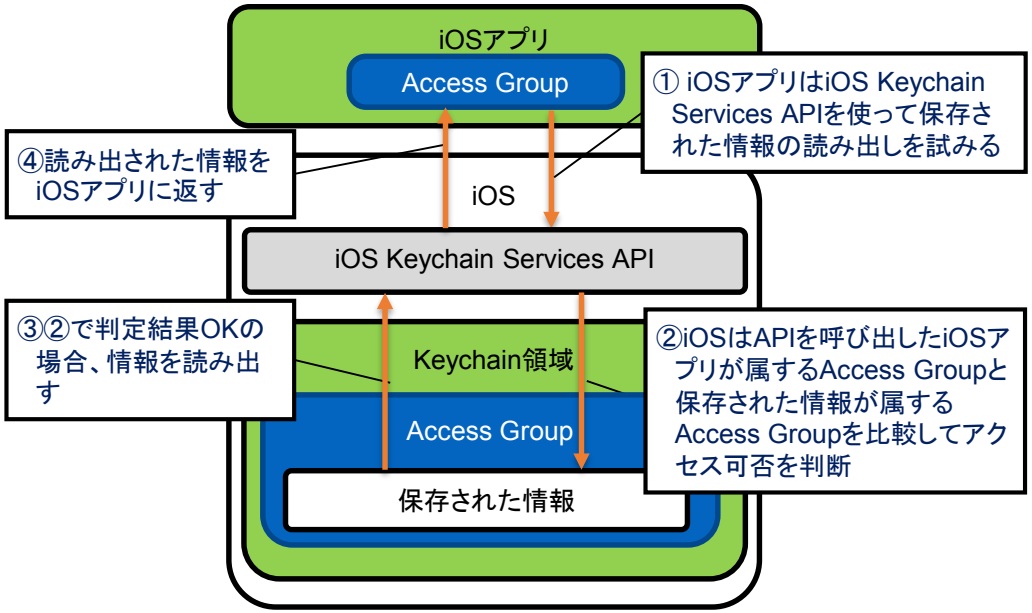


NTT DATA

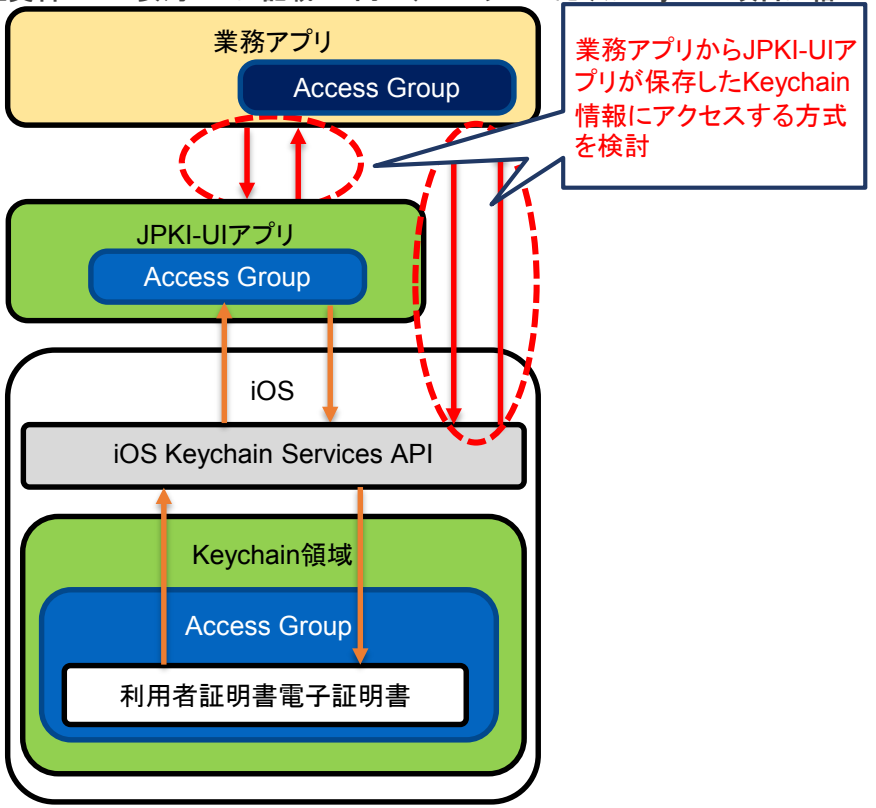
5. (2)iOS：課題⑥業務アプリからKeychain領域へのアクセス

・iOSのKeychain領域にアクセスする場合、図②においてJPKI-UIアプリと業務アプリが同一のグループに属する必要があります。そのグループをAccess Groupと呼び、iOSアプリ毎に固有の値で区別されます。JPKI-UIアプリと同一のAccess Groupとしてアクセスできるのは、JPKI-UIアプリと同一のApple社の開発者プログラム契約の元でコード署名されたアプリに限られます。(※)
・Androidと同様のアプリ間通信ではKeychain領域のアクセスは実現できない可能性があり、他の方式を含めて検討します。

(※)スマートフォンへの利用者証明機能ダウンロード検討サブワーキンググループ(第6回)の補足資料B B-3 安対-03 に記載の「同一デベロッパーだけがKeychain項目に格納した情報を共用利用することを保証する」仕組みの詳細になります。



図① Keychain領域へのアクセス制御の仕組み



図② 業務アプリからKeychain領域へのアクセス方式

7. 評価会等の開催

評価会等の開催

市町村窓口における電子証明書のSIMカード等への格納及び運用面における安全性対策の検討及び検証にあたり、有識者が参加する評価会および検討会をAndroid／iOS搭載スマートフォンそれぞれについて開催する。検討体制は以下の通り。

評価会

〔Android搭載スマートフォン評価会〕	〔iOS搭載スマートフォン評価会〕
[評価者]有識者、J-LIS [説明者]提案関係社(NTTデータ･NTTコム･DNP) [オブザーバ]総務省、モバイル通信事業者（NTTドコモ、KDDI、ソフトバンク）	[評価者]有識者、J-LIS [説明者]提案関係社（NTTデータ･日本IBM） [オブザーバ]総務省
〔Android／iOS搭載スマートフォン評価会共通〕【実施内容】 ・各課題に関する協議（第1～3回）・技術検証に向けた協議（第1回）	

検討会

〔Android搭載スマートフォン検討会〕	〔iOS搭載スマートフォン検討会〕
[実施者]提案関係社(NTTデータ･NTTコム･DNP) [オブザーバ]モバイル通信事業者（NTTドコモ、KDDI、ソフトバンク）	[実施者]提案関係社（NTTデータ･日本IBM）
〔Android／iOS搭載スマートフォン検討会共通〕【実施内容】 ・各課題に関する協議（評価会向け報告に関する検討）	

Android／iOS搭載スマートフォン評価会の開催スケジュール（案）は以下の通り。

#	議題	開催時期
第1回	・課題①～④に関する協議、課題①②の技術検証に向けた協議（Android／iOS）	2017年12月下旬 目途
第2回	・課題⑤～⑥に関する協議（Android／iOS） ・第1回の指摘事項の検討結果（Android／iOS）	2018年2月上旬 目途
第3回	・課題⑤～⑥に関する協議（Android／iOS） ・第2回の指摘事項の検討結果（Android／iOS）	2018年3月上旬 目途

8. 実証実施スケジュール

検討会及び評価会は以下のスケジュールで開催を予定しています。

#	項目	１０月	１１月	１２月	１月	２月	３月
1	検討会			▲第1回		▲第2回	▲第3回
2	評価会			▲第1回		▲第2回	▲第3回
3	Android課題①～④検討		課題の解決方法の検討		残課題の検討		
4	Android課題①、②、⑦検証		検証準備		検証環境構築	検証	
5	Android課題⑤～⑧検討			課題の解決方法の検討		残課題の検討	
6	iOS課題①②④検討		課題の解決方法の検討		残課題の検討		
7	iOS課題①、②検証		検証準備		検証環境構築	検証	
8	iOS課題⑤⑥⑧検討			課題の解決方法の検討		残課題の検討	

NTT DATA