

ARIBにおける検討状況

2015年11月9日

東京工科大学
手塚 悟

携帯電話を利用した公的個人認証サービスの利活用

- 方式1

 - 携帯電話がICカードR/Wの役割を担い、PCと連動する方式

- 方式2

 - 携帯電話がICカードR/WとPCの役割を担う方式

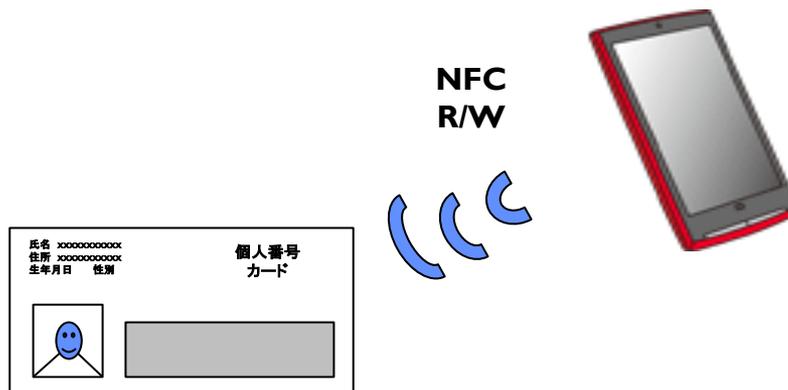
- 方式3

 - 携帯電話に電子証明書等を格納し活用する方式

R/W:Reader/Writer

NFC搭載スマートフォンのR/Wの検討

- 方式1、方式2の検討
- NFC搭載スマートフォンのICカードR/W機能を利用して、今後発行が予定される個人番号カードを読み取ることができることを目指し、番号制度とモバイルコマース分野の連携に寄与する。
- 個人番号カードの読み取りが可能なNFC搭載スマートフォンの認定の在り方を検討する。
- 上記目的を達成することにより、より大きな経済波及効果の期待できる市場を展望し、新しいビジネスマーケット創出に寄与する。

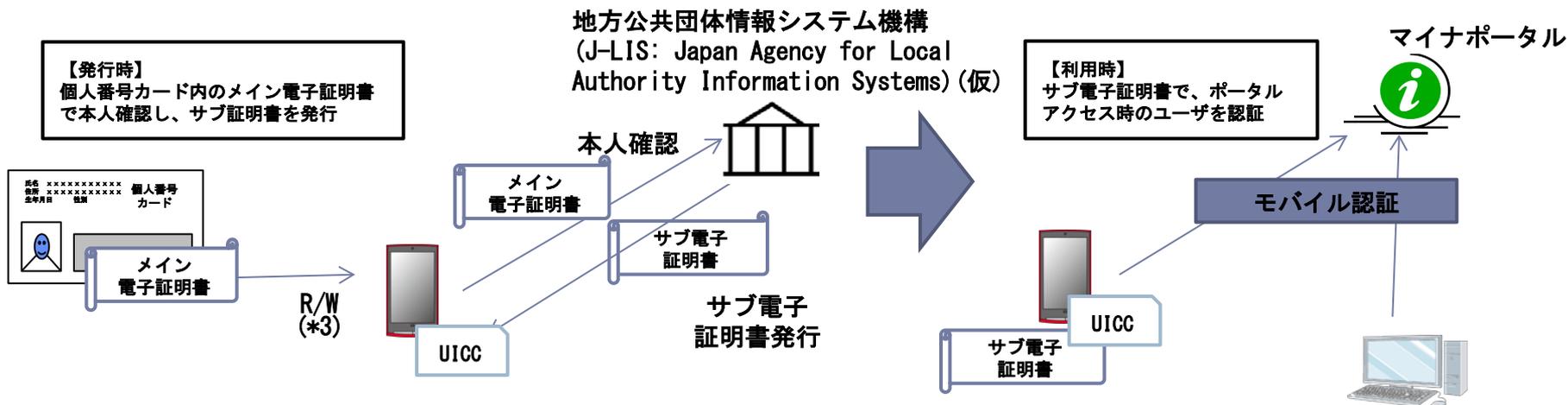


NFC: Near Field Communication
R/W: Reader/Writer

UICCへのJPKIサブ電子証明書搭載の検討

● 方式3：R/Wと連携したJPKI のUICC搭載方式について

- 目的
 - JPKI対応方式として、第一段階のR/W方式から、次ステップのUICC搭載方式への移行促進。
- 前提(*2)
 - UICCに対しサブ電子証明書を発行する。（←デバイス多様化に対応した新しい電子証明書）
 - 従来の電子証明書（メイン電子証明書と呼ぶ）は発行済みとし、その認証に基づきサブ電子証明書は発行される。
 - 現行制度にとらわれない。
- 検討内容
 - サブ電子証明書発行のための前提、構成、運用・制度上の課題整理（有効期限、制度変更部分など）
 - マイナポータルアクセス時のモバイル認証方式（PC等との連携など）

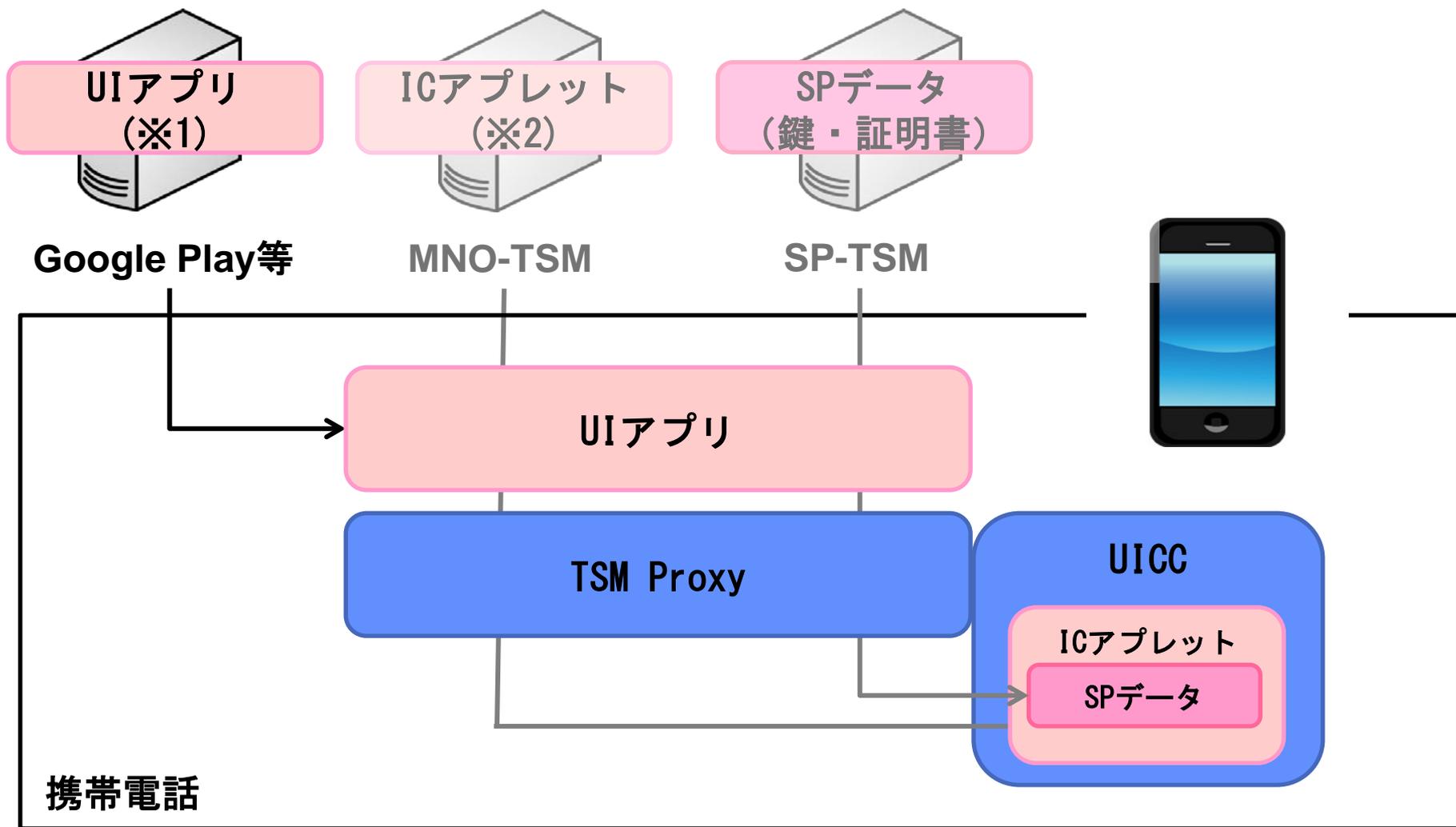


- (*1) UICC： Universal Integrated Circuit Card、電話番号を特定するための固有のID番号が記録されたICカードである。
- (*2) UICCに対するメイン電子証明書のリモート発行、及び、その際の本人確認方法については、別途検討する。
- (*3) スマートフォンR/Wにより、サービス条件を満たす安定的なカード読み取り自体が技術的、法的に可能である場合に限る。

公的個人認証における携帯電話を利用した電子証明書の発行は、鍵・証明書のダウンロードを行う前に携帯電話にアプリをインストールする必要があるため、以下の3つのフローに分かれる。

- (1) 電子証明書発行アプリ(UIアプリ)をダウンロードする。
- (2) ICアプレットをダウンロードする。
- (3) 公的個人認証の鍵・証明書をダウンロードする。

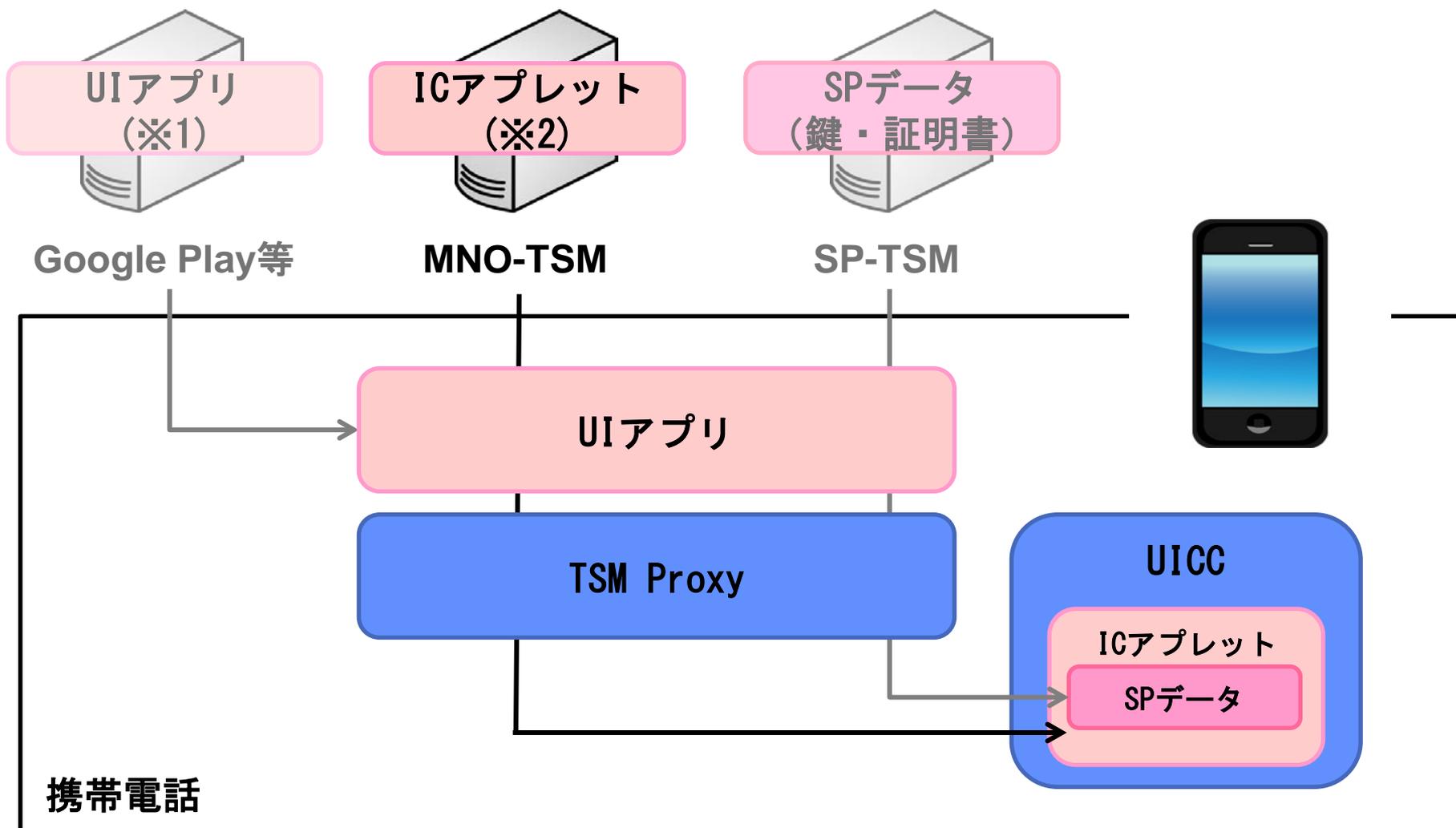
(1) 電子証明書発行アプリ (UIアプリ) のダウンロード



※1: 公的個人認証利用者クライアントソフト (Android版)

※2: 個人番号カードにおける公的個人認証APIに相当。

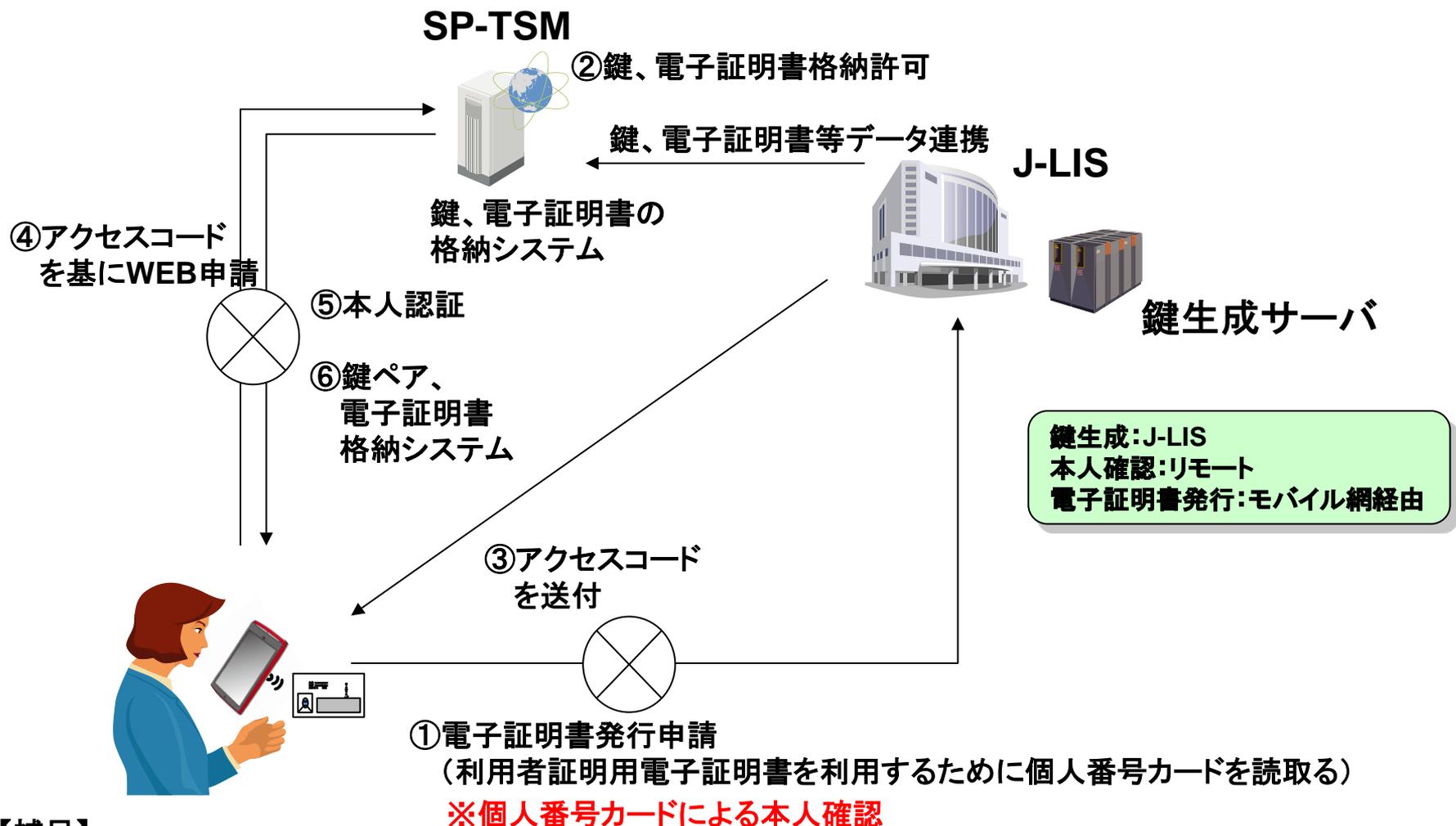
(2) ICアプレットのダウンロード



※1: 公的個人認証利用者クライアントソフト(Android版)

※2: 個人番号カードにおける公的個人認証APに相当。

(3) JPKIの鍵・電子証明書の格納



【補足】

- ・ネットワーク網はモバイル網を前提とする。Wi-Fi網の検討は別途とする。
- ・鍵ペア、電子証明書をダウンロードするネットワークセキュリティはモバイル網のセキュリティレベルを以て可とする。