公的個人認証サービスの新たな利用シーンへの展開

東京工業大学　科学技術創成研究院
未来産業技術研究所　兼
社会情報流通基盤研究センター

小尾高史

ASIST
Assist in improving the information quality

TOKYO TECH
Pursuing Excellence
TOKYO INSTITUTE OF TECHNOLOGY

マイナンバーカード

搭載カードアプリ	主な利用方法など
券面ＡＰ	対面利用時の券面改ざん検知、本人確認の証跡管理 画像取得には券面記載情報によるアクセスコントロール
ＪＰＫＩ	電子署名　　パスワード：6から16ケタの英数字 電子利用者証明　　ＰＩＮ　　：4ケタの数字
番号ＡＰ	個人番号、4情報に電子署名をしたものを記録 個人番号の読出しにはＰＩＮの入力が必要
住基ＡＰ	住民票コードを記録 ＰＩＮの入力が必要

公的個人認証サービス

- **公的個人認証サービス**
  （JPKI：Japan Public Key Infrastructure）
  - 2004年1月29日より提供開始（開始時は電子署名のみ）
  - インターネットを通じて安全・確実な行政手続き等を行うために、他人によるなりすまし申請や電子データが通信途中で改ざんされていないことを確認するために必要な機能を提供
  - 個人番号制度の導入（整備法）により、2016年1月より「電子利用者証明（いわゆる電子認証）」の仕組みを導入
  - 総務大臣が認定した民間事業者も証明書の有効性確認を実施可能（２０１６年２月現在民間３団体を認定済み）
  - 電子署名用証明書には基本４情報が記載（情報の変更があると失効）されるが、電子利用者用証明書には個人情報の記載はなし（証明書のシリアル番号で管理）
  - 電子利用者証明については、PINの入力を求めない利用が可能

JPKI利用拡大の検討状況

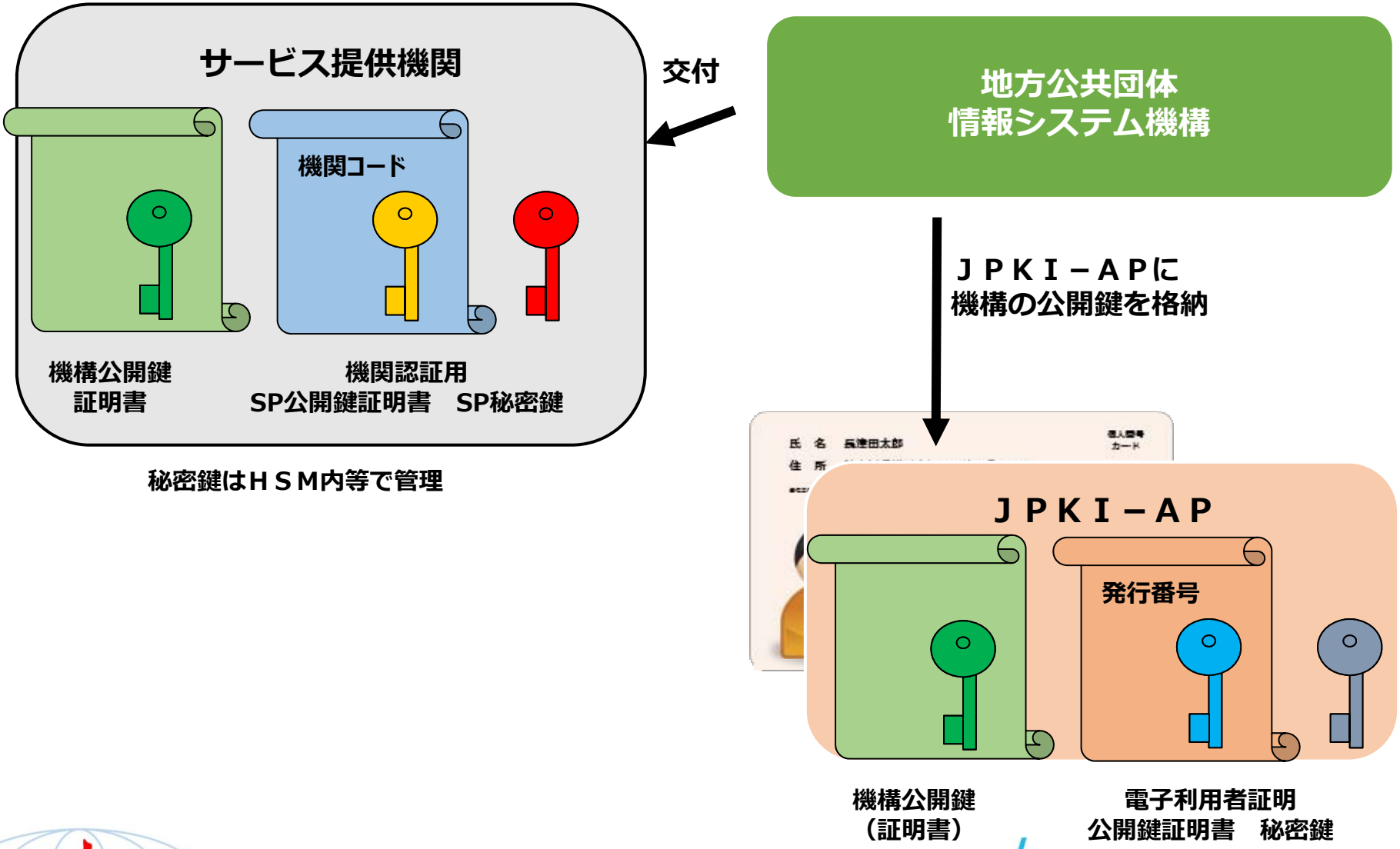
- **イベント入場、保険資格確認などへの適用を検討**
  - PINを求めない利用者証明機能利用時に用いる機関認証用秘密鍵の端末搭載の検討

  → 機関認証に基づく利用者認証機能の利用シーン拡大
- **電子委任状取扱業務の制度整備を検討**
  - 法人間等の取引等において権限等の委任関係を電子的に確認するための仕組みを検討
- **UIMへのJPKI電子利用者証明機能搭載の検討**
  - ２枚目の利用者証明用PKCの発行
  - 将来的には電子署名用証明書の２枚目発行も
  - ２枚目以降の証明書の記載事項の変更も想定

ASIST
Assist in improving the information quality

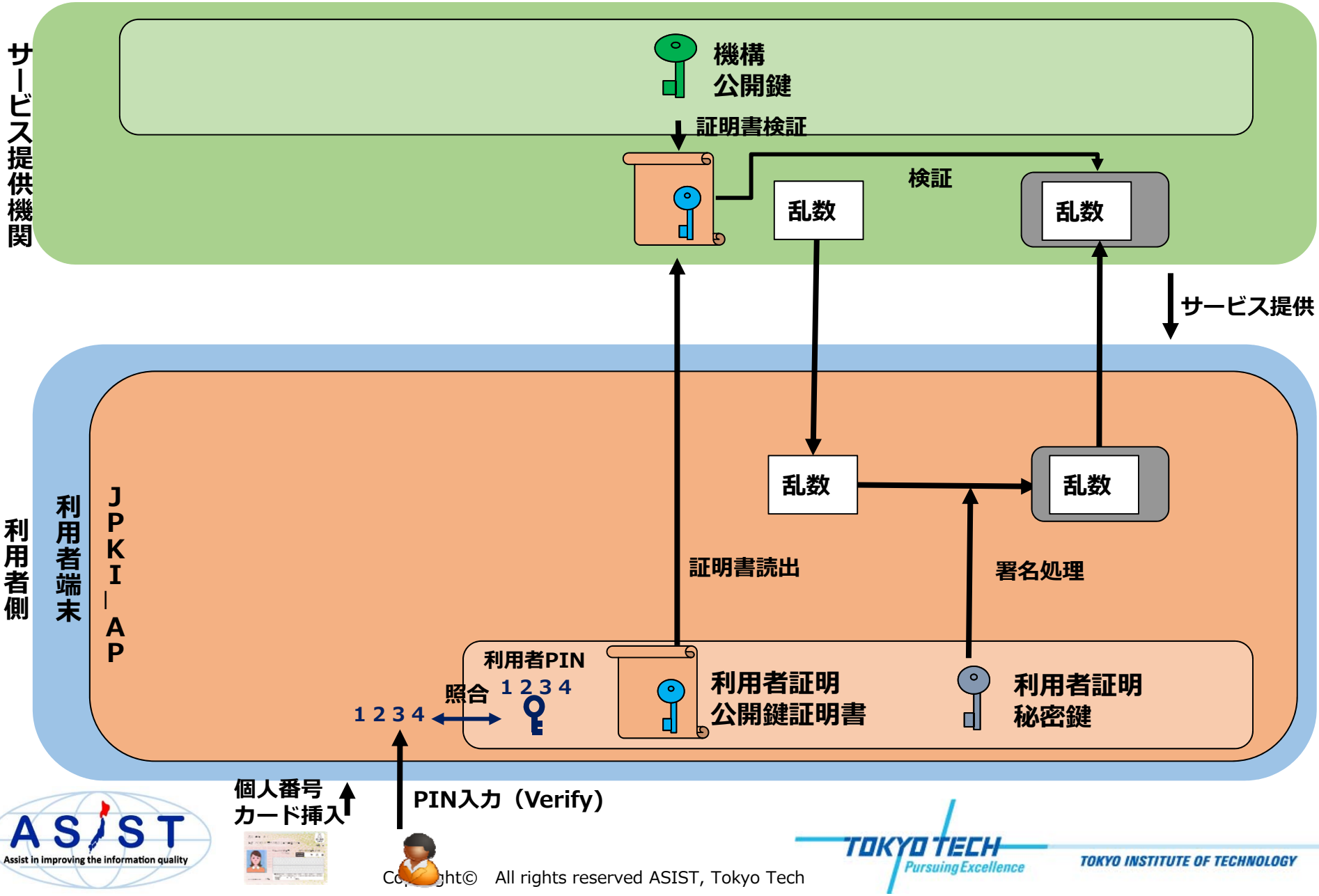
TOKYO TECH Pursuing Excellence
TOKYO INSTITUTE OF TECHNOLOGY

機関認証利用の登録

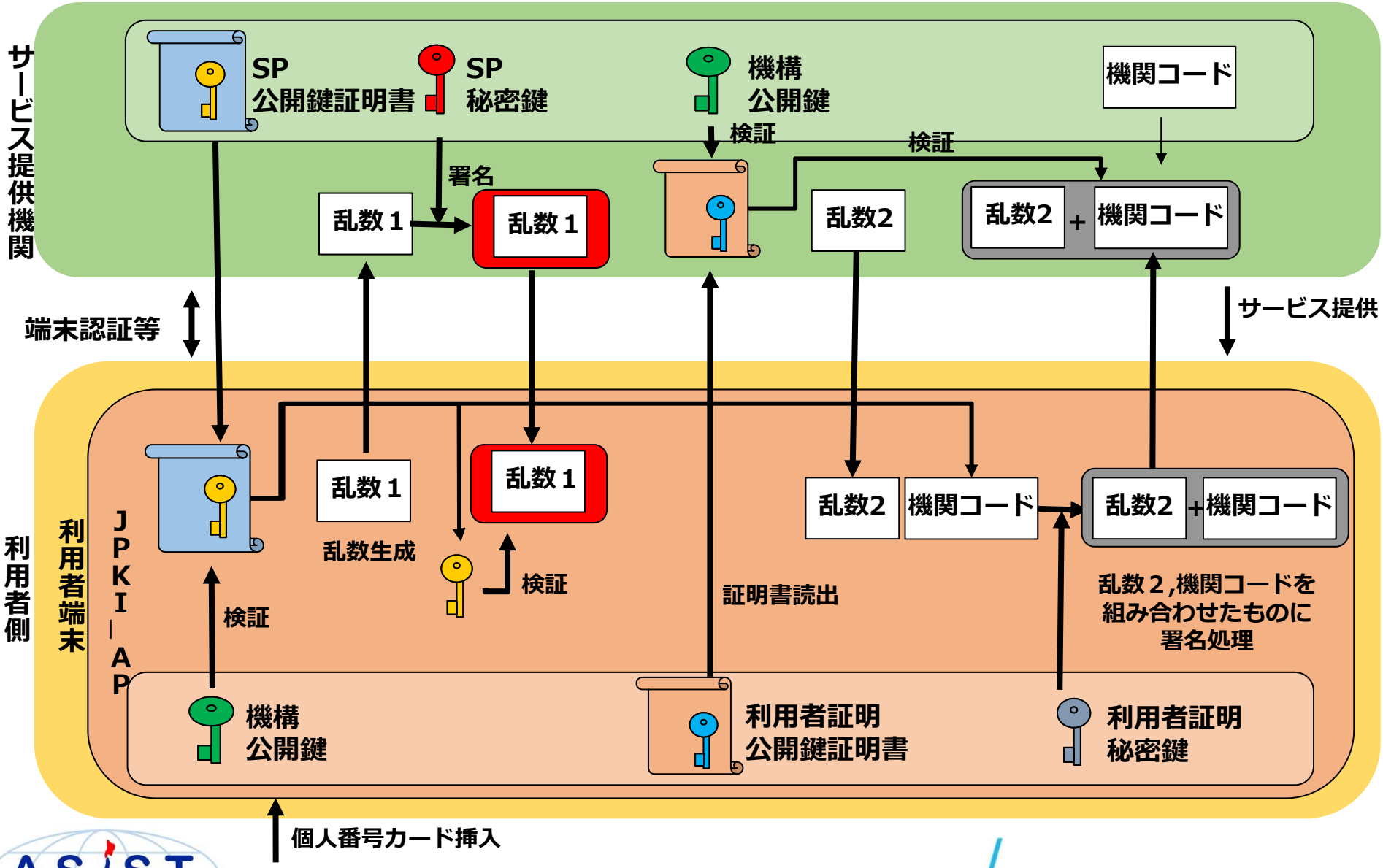


秘密鍵はＨＳＭ内等で管理

PIN入力による利用者証明機能の利用



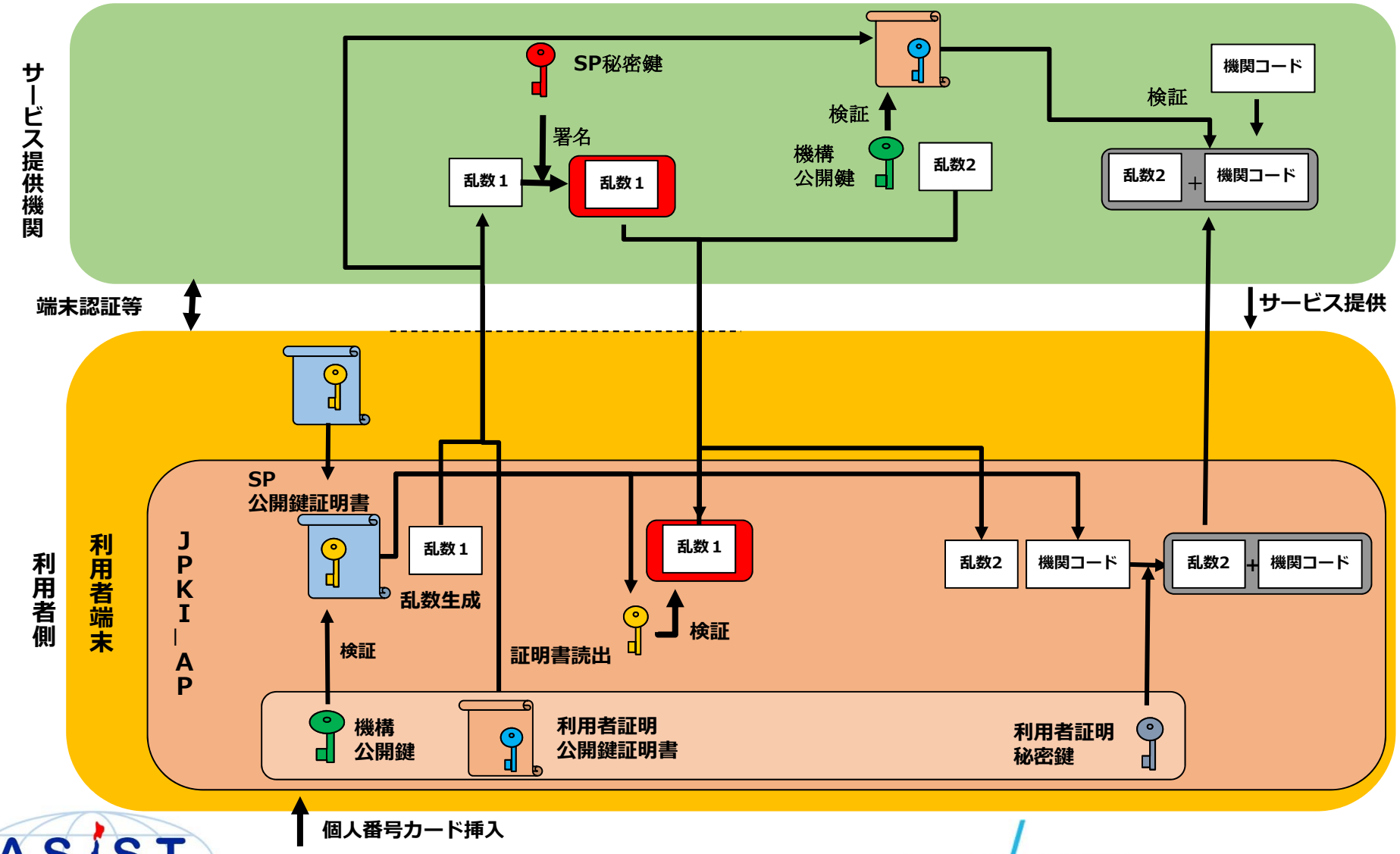
機関認証による利用者証明機能の利用



処理時間短縮の検討

- **認証シーケンスの見直し**
  - サービス提供機関側での処理を並列化
- **機関認証処理自体の処理時間短縮**
  - 機関認証鍵等を利用者側の端末に格納
  - 機関認証処理をローカルに実施
- **具体的な事例は福田先生の発表で**

認証シーケンスの見直し



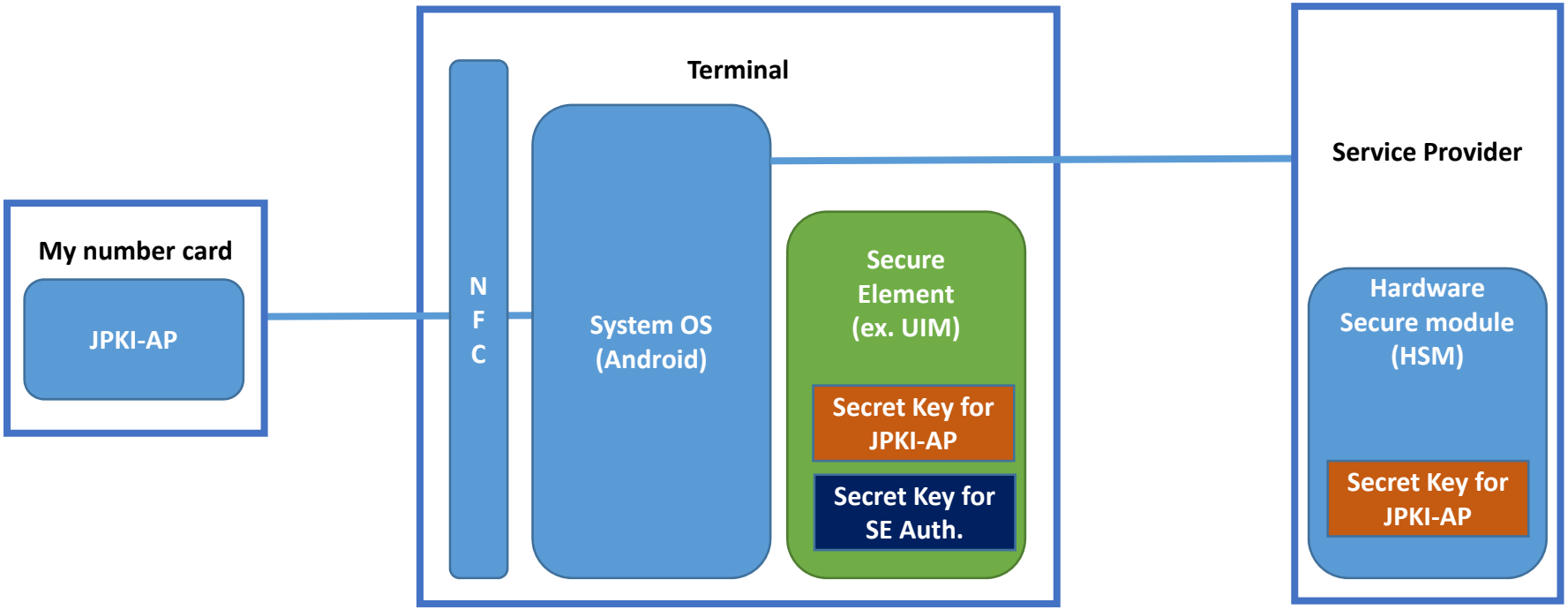
利用者端末を用いた機関認証

- **サービス提供機関による端末への機関認証鍵格納**
  - サービス提供機関は、J-LISより発行された機関認証用公開鍵証明書及びそれに対応する秘密鍵を端末に格納、その管理責任を負うと想定
- **端末盗難時等の盗難端末での機関認証機能の利用停止**
  - 端末盗難時等には、サービス提供機関が直接的に端末を利用停止状態にさせる
- **端末利用組織の端末管理責任の明確化**
  - 端末利用組織は、サービス提供者より貸し出された端末の管理責任を負うと想定

現時点で想定される安全対策

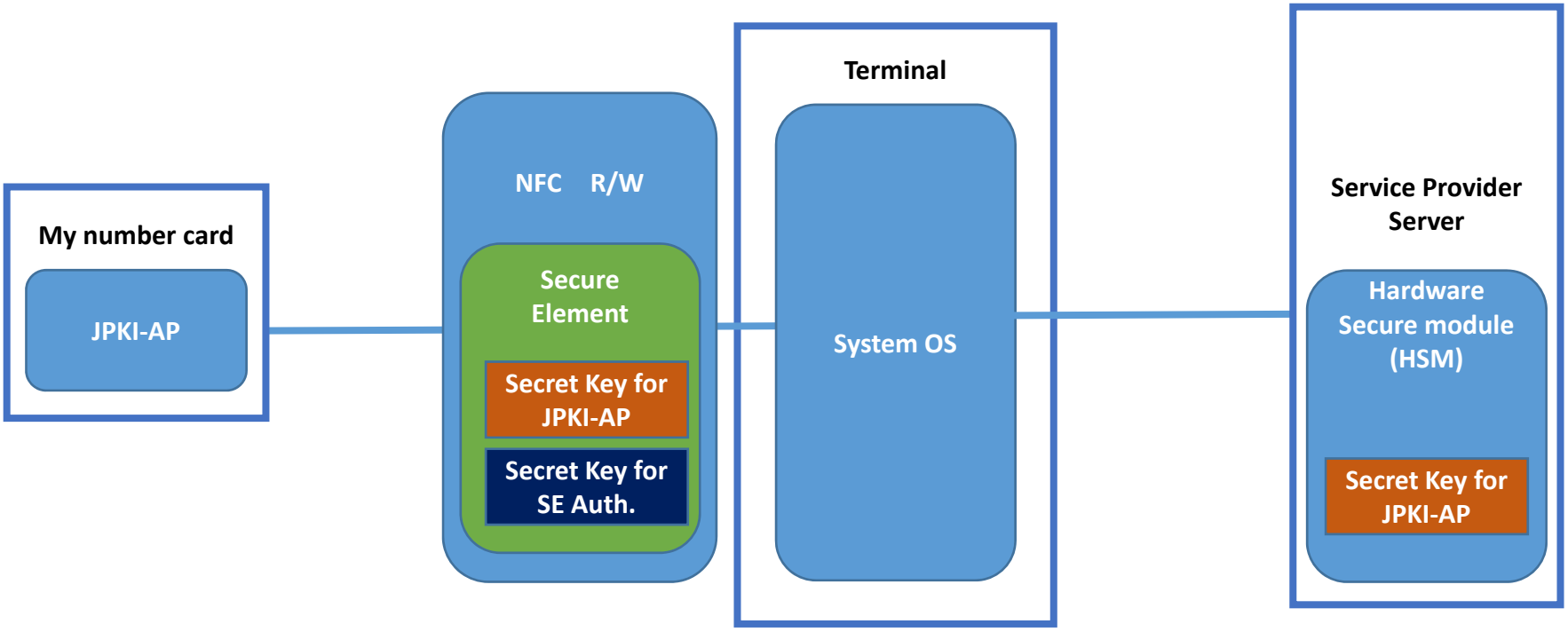
- **機関認証用秘密鍵の安全な管理**
  - Secure Elementの利用
  - 機関認証用秘密鍵利用開始時に、機器認証により端末等の確認を行うとともに、サービス提供機関の認証を行うことで機関認証用秘密鍵の利用を可能とする
- **サービス提供機関による機関認証利用時の端末の確認**
- **サービス提供機関と端末での安全な通信路の確保**
  - TLS、IP-sec、専用線などの利用
- **端末利用開始時の端末登録組織（者）認証（オフライン時）**
  - 端末利用者のJPKI等の利用を想定
- **無人端末等ではカード所有者の明示的な同意の下での利用**
  - 機関認証JPKI利用時には、カード所有者に“OK”ボタンを押させるなど、機関認証JPKIの利用を意識させるユーザインターフェースを用意

端末の構成(端末にSEを搭載）

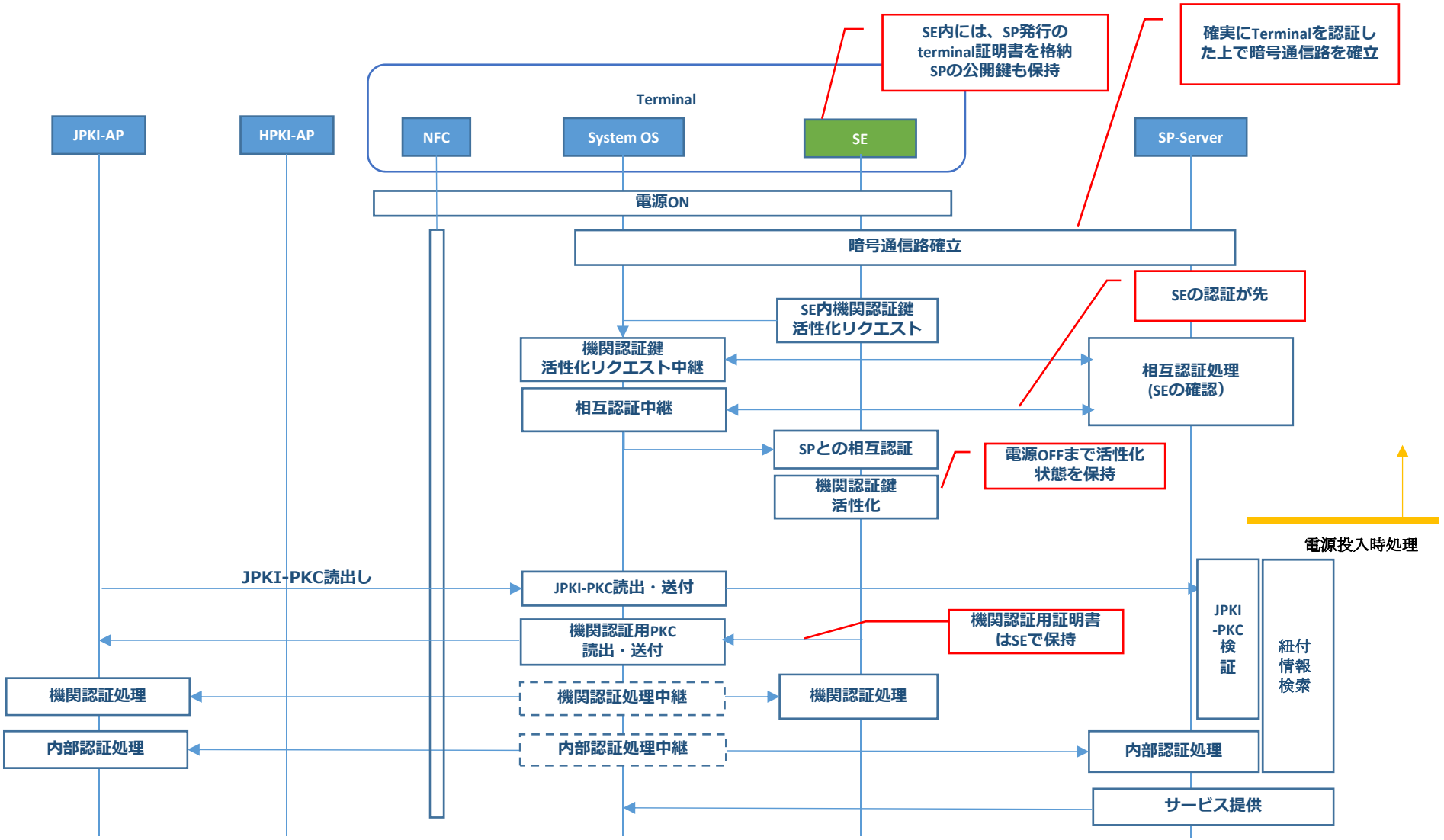


Secure Elementの代わりに
Trusted Execution Environmentの利用も想定

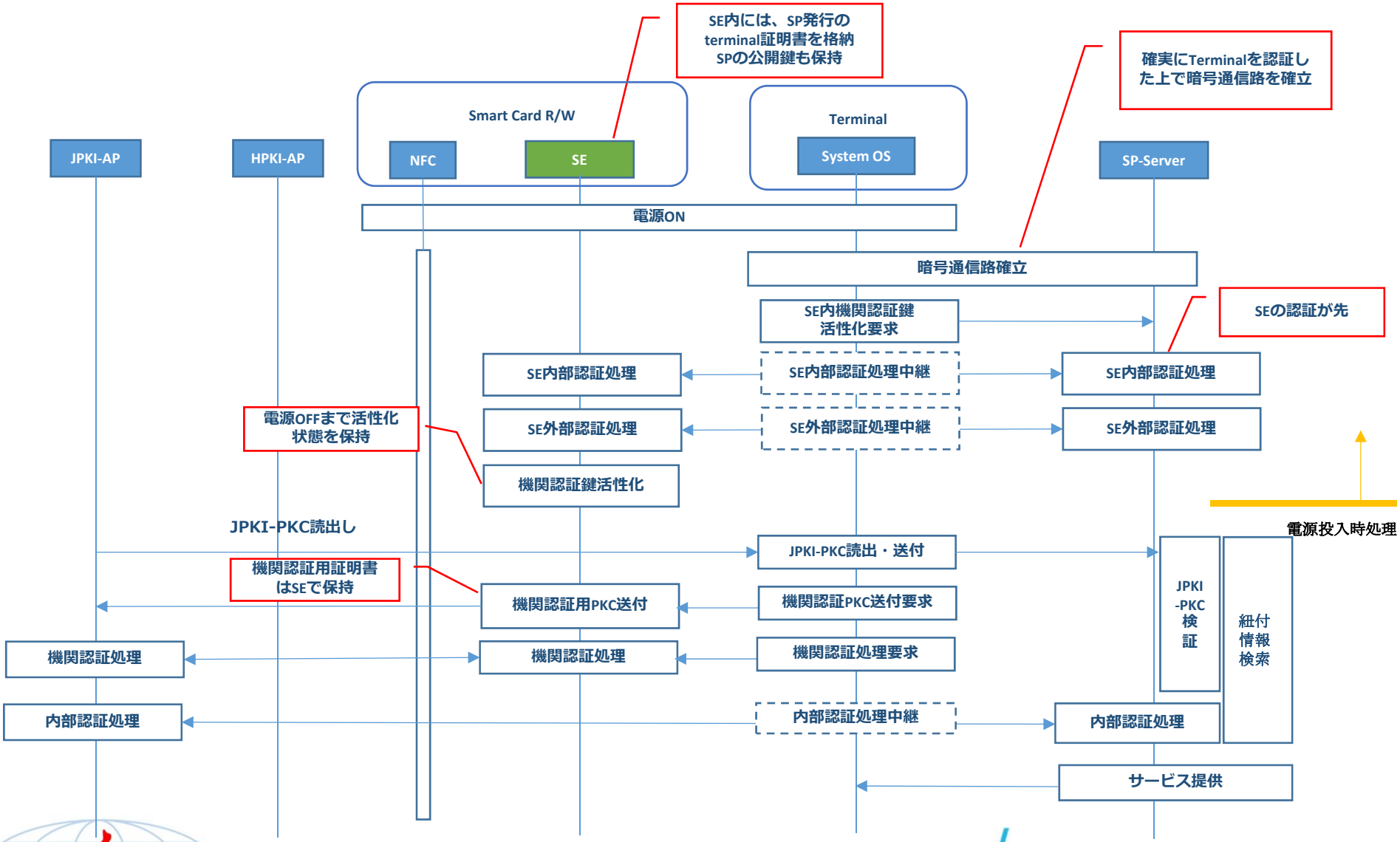
端末の構成(専用R/WにSE搭載)



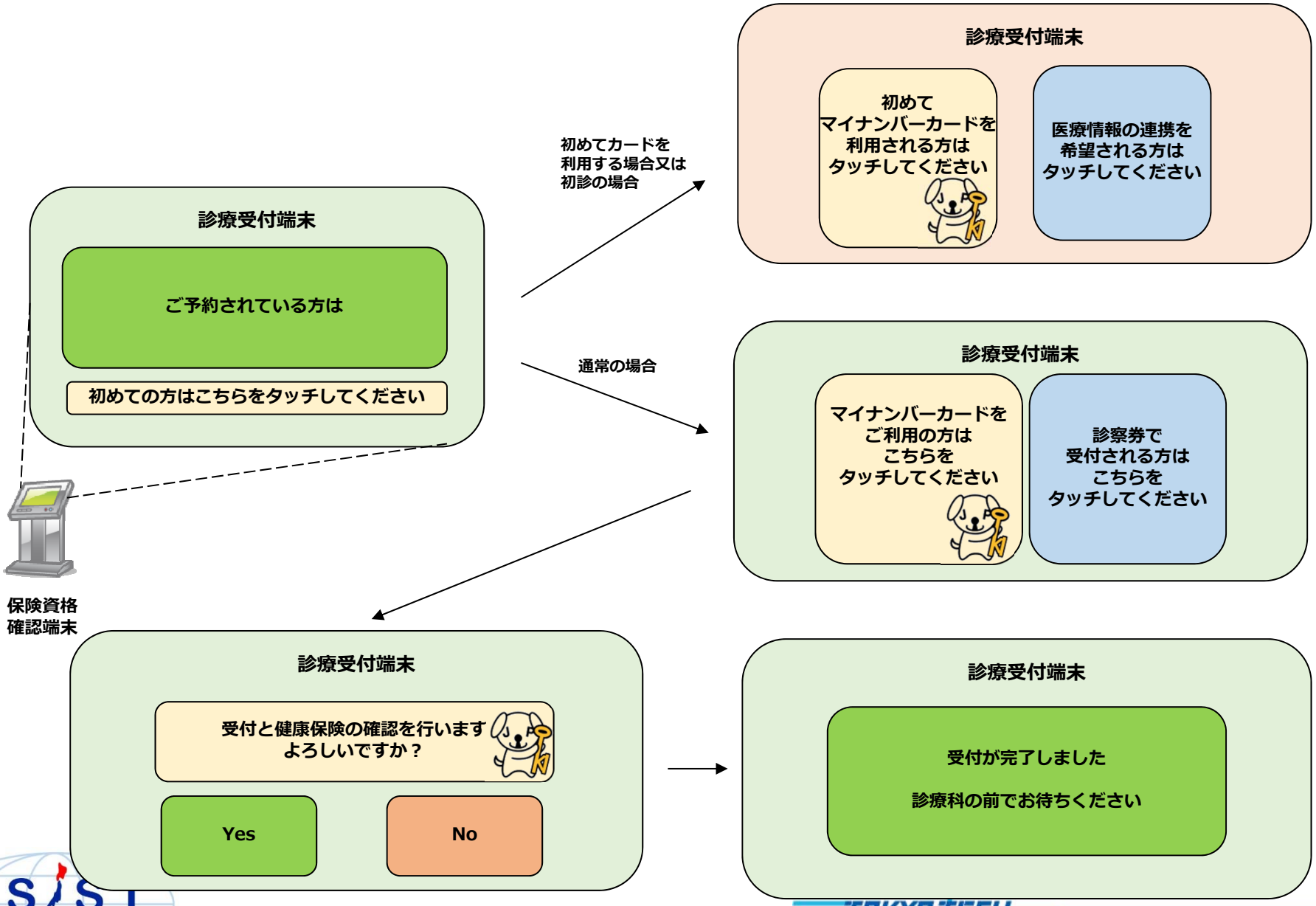
想定処理フロー（端末にSE搭載）



想定処理フロー（R/WにSE搭載）



医療機関での受付イメージ



機関認証を利用した医療機関個別IDの利用

マイナンバーカードのみで再診受付を実現

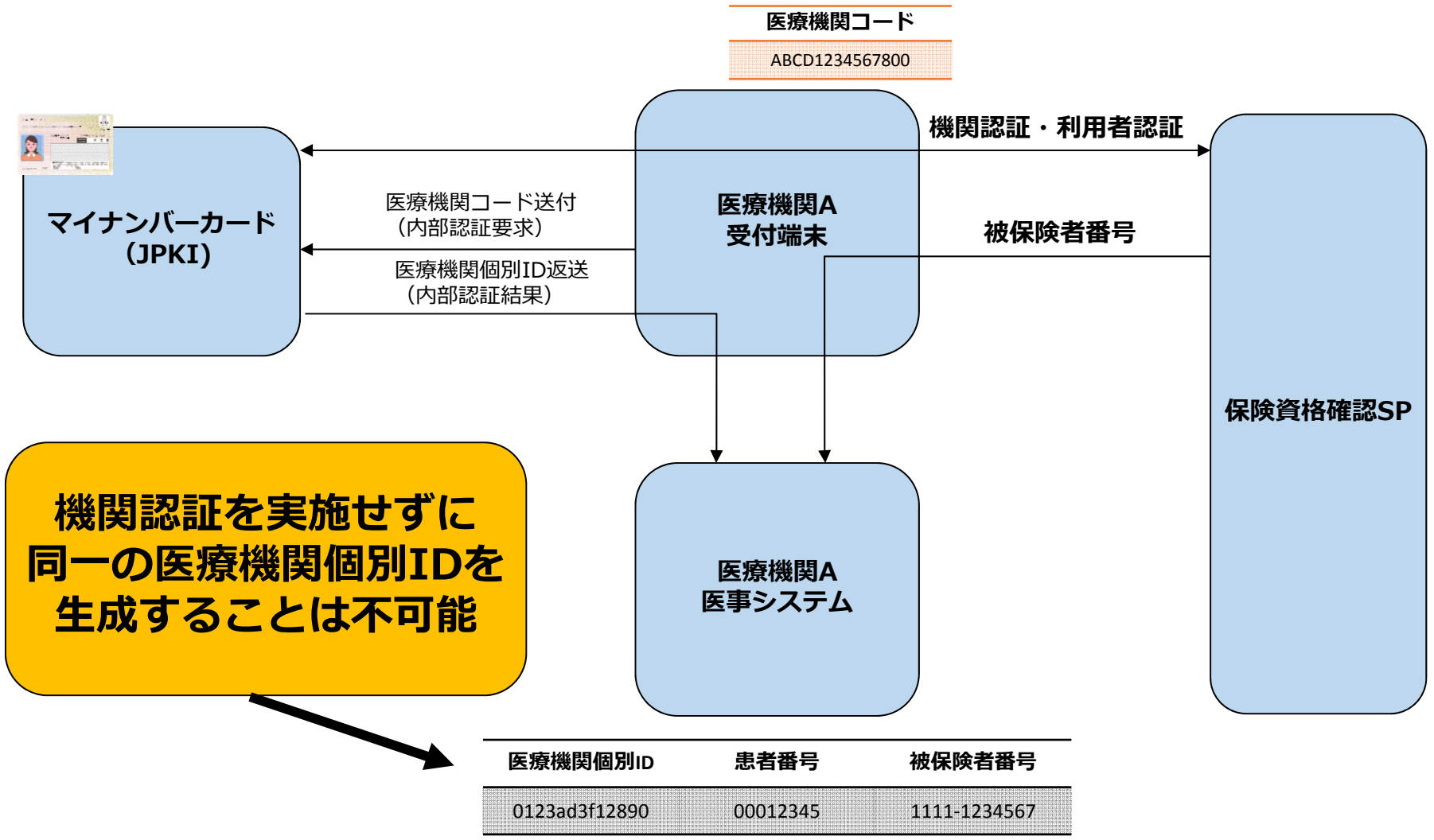
- **シリアル番号の取得管理を医療機関は行えない**
  - 公的個人認証法第六十三条
    - …利用者証明検証者以外の者は、何人も、業として、…利用者証明用電子証明書の発行の番号の記録されたデータベースであって、当該データベースに記録された情報が他に提供されることが予定されているものを構成してはならない。
- **利用者証明書のcommonName(CN)の利用**
  - マイキーIDとして利用が検討されているもの
    - マイキーPFでは、サービスID照会の利用を想定
    - 他分野と同じIDを利用することへの懸念

機関認証による利用者証明機能を用いた
医療機関個別IDの生成

ASIST
Assist in improving the information quality

TOKYO TECH Pursuing Excellence
TOKYO INSTITUTE OF TECHNOLOGY

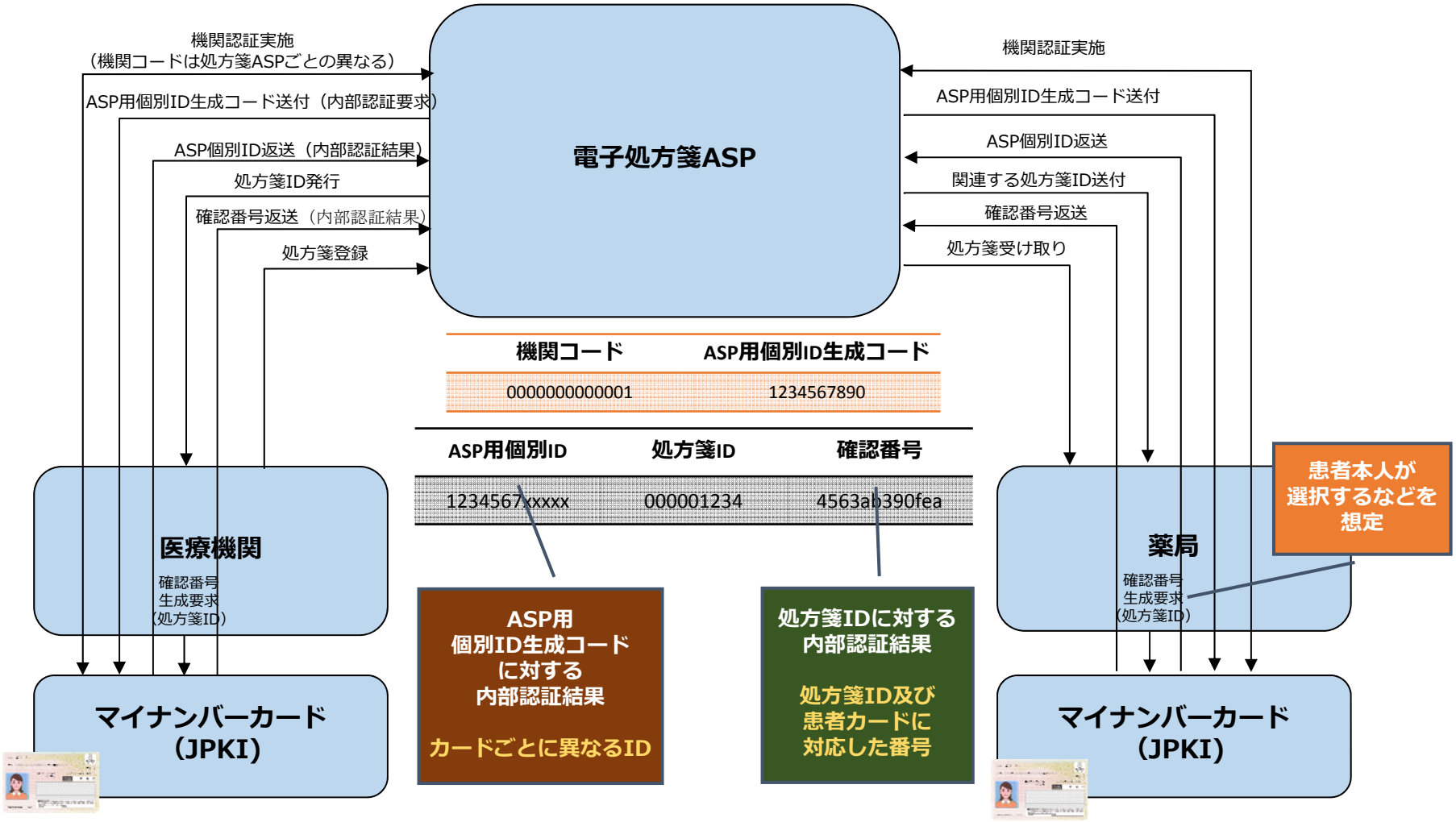
医療機関窓口での利用



医療機関個別IDの特徴

- **保険資格確認等と組み合わせて利用することで個別ID生成に利用者証明機能を利用**
- **保険資格確認が行える組織以外は発行不可**
  - 機関認証機能との組み合わせでのみ実現
  - 生成には保険資格確認機関の機関コードが必要
- **医療機関毎に異なる医療機関個別IDを生成可能**
- **シリアルと異なり医療機関で保存可能と想定**

電子処方箋運用への適用



電子処方箋適用例の特徴

- **電子処方箋ASP**
  - 患者管理が不要
  - ASP個別IDは、ASPごとに異なるように生成可能
  - 機関認証の利用は必要だが、保険資格確認SPとの連携や機関認証を実装した端末の利用も可能
  - 利用者証明書の検証、利用者証明機能の利用はオプション
- **課題**
  - 薬局での処方箋ASPの所在の確認方法
    - PHRシステムとの連携による対応などを今後検討
  - 複数処方箋発行時の対応
  - JPKI更新時、カード紛失時などへの対応

機関認証と利用者証明の組み合わせ

- 医療情報の参照など、様々なサービスでの医療機関でのJPKIの利用が検討されている。
  例えば、未成年やお年寄りなどが医療機関にかかる場合には、患者本人がマイナンバーカードを利用せず、保護者等が本人に代わりカードを提示することも想定される。

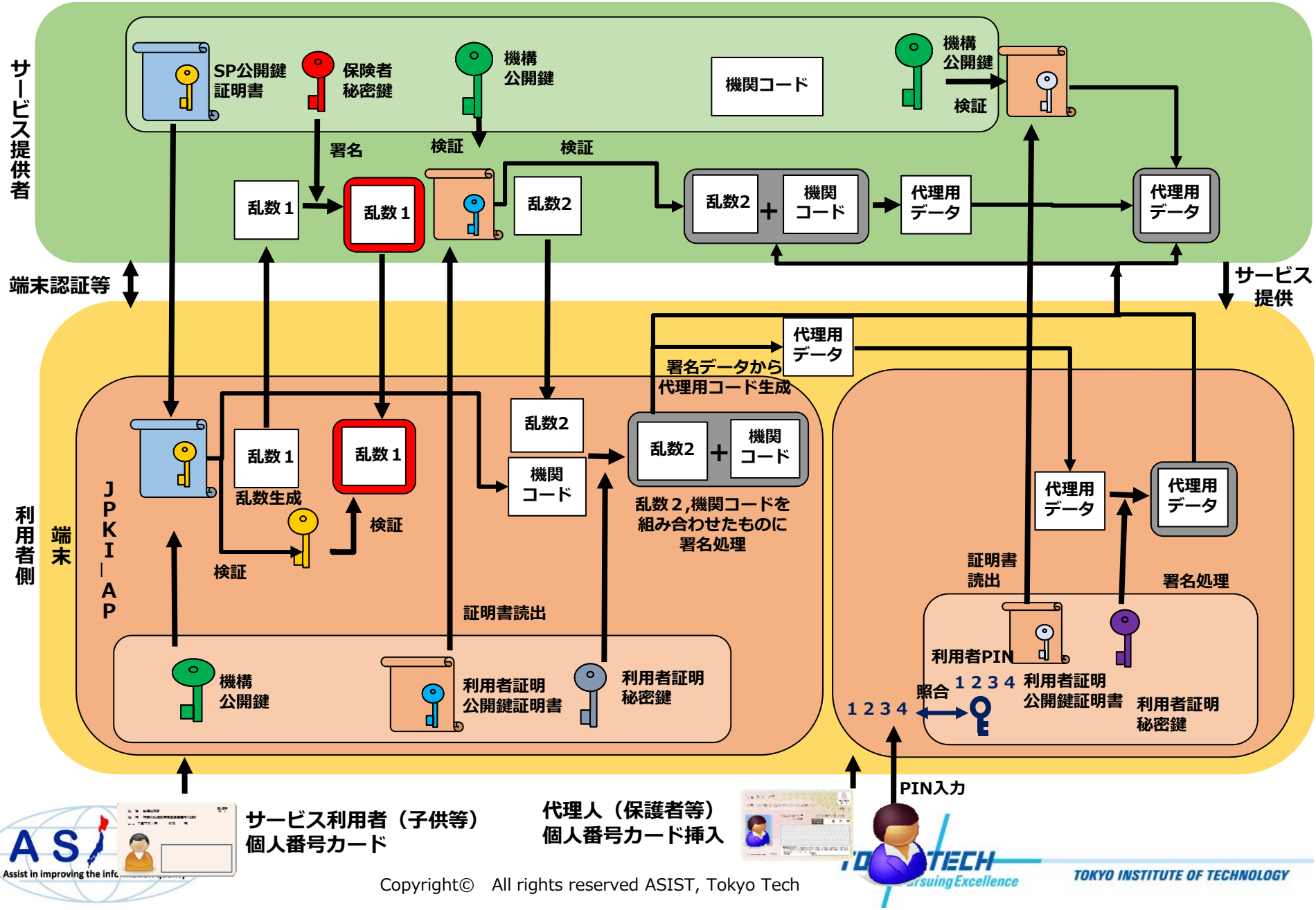
- サービス提供側が、誰が代理でカードを利用しているかを把握するとともに、事後的に誰が代理で利用したかの証跡を保持できる仕組みが必要

外部機関認証に基づく利用者証明と
代理人による利用者証明の利用を
組み合わせることで代理利用者の確認とその証跡を保存

ASIST
Assist in improving the information quality

TOKYO TECH Pursuing Excellence
TOKYO INSTITUTE OF TECHNOLOGY

代理人による医療サービス利用



おわりに

- JPKIの利用者認証機能の利用拡大は、マイナンバーカード普及のカギ
- 機関認証に基づく利用者認証機能は、いわゆるPIN無しの利用者認証としての利用だけでなく、様々な応用が考えられる
- より使い勝手のあるカードへ

Thank you

A part of this work was supported by Health Labour Sciences Research Grant, Research on Region Medical H26-Iryo-Shitei-034.