公的個人認証サービスによる
電子利用者証明の民間利用拡大に向けて

第８回　社会情報流通基盤研究センター・シンポジウム

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

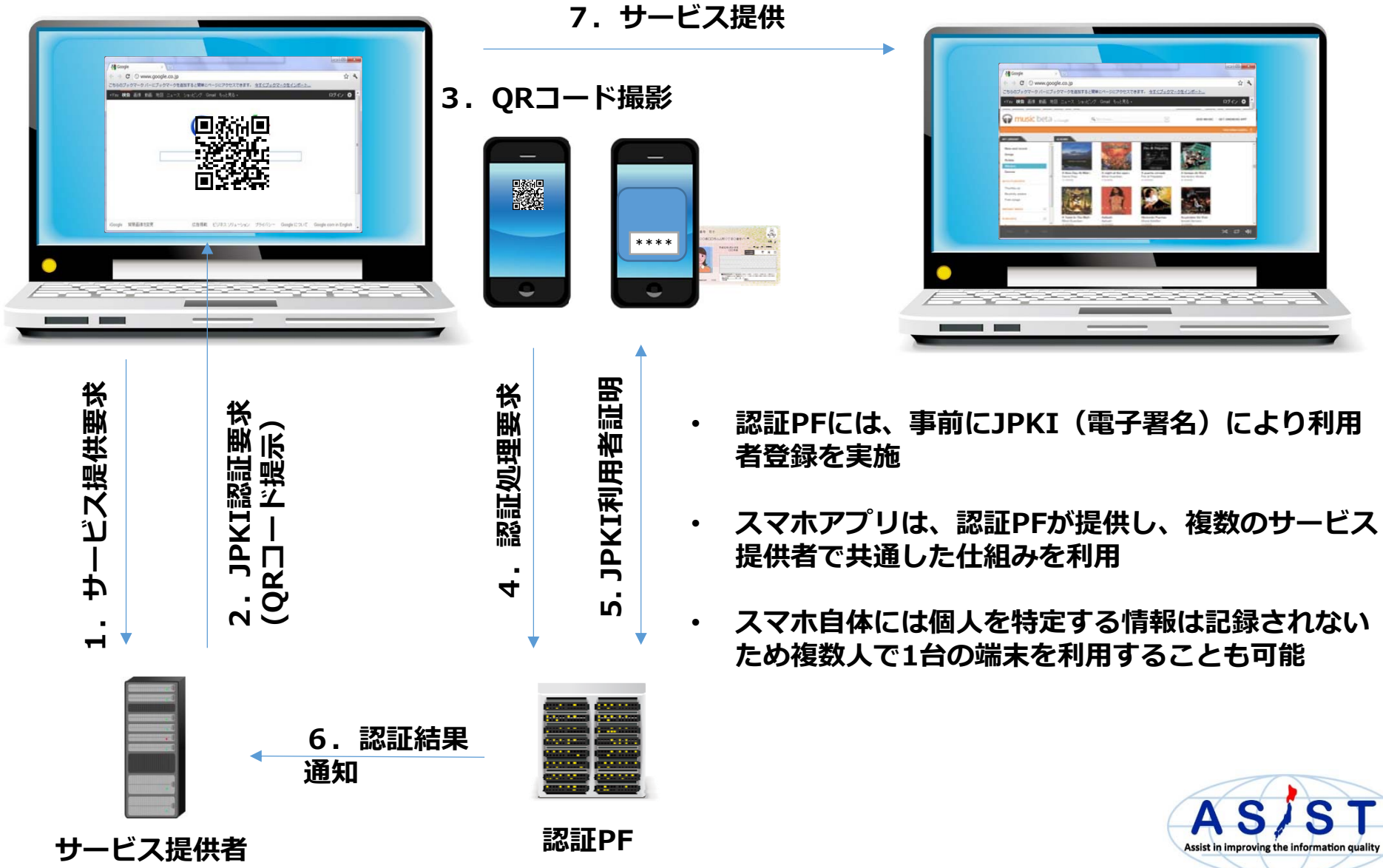
研究の内容

- 現在の公的個人認証サービスには、電子署名機能だけでなく、電子利用者証明（電子認証 ）の機能が追加されている
- 電子利用者証明機能は、公共分野での利用にとどまらず、多くの民間事業者が利用することを想定
- 公的個人認証サービス、特に電子利用者証明機能の民間利用で必要となる、個人情報を管理・運用する仕組みのあり方を検討

認証PF事業者のサービス機能強化

- より簡単にJPKIによる利用者証明を利用可能とするための仕組みの提供
- ユーザーのプライバシ確保に配慮しつつサービス提供者が利用者の確認を行える仕組みの提供

スマホと連携した利用者認証



- 認証PFには、事前にJPKI（電子署名）により利用者登録を実施
- スマホアプリは、認証PFが提供し、複数のサービス提供者で共通した仕組みを利用
- スマホ自体には個人を特定する情報は記録されないため複数人で1台の端末を利用することも可能

オンラインバンキングでのログイン

オンラインバンキングサービス利用開始時
JPKIによるユーザ認証

スマートフォン側での操作

プライバシー侵害に関する懸念

- **PKIを利用した認証時には、サービス提供側に対して、電子証明書の提示が必要なため、広く民間で利用されると**
  - 証明書内に記載された情報をマッチングキーとして、ある利用者がどのようなサービスを利用したかを一定期間把握できる可能性
  - 様々な組織に個人情報が蓄積され、情報漏えいが発生した場合、プライバシーを侵害される危険性

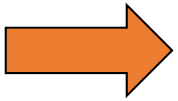
現在の対策

- **利用者証明用証明書内に、基本４情報（氏名・生年月日・性別・住所）などの個人の特定が可能な情報を記載しない**
- **署名検証者及び利用者証明検証者に対し、電子証明書（公開鍵、発行番号）や失効情報の目的外利用、第3者提供の制限を設ける**

- **証明書ポリシー（公的個人認証サービス利用者証明用認証局運用規程）により用途を以下に限定**
  - 行政機関等及び裁判所で行うオンライン申請･届出等の手続に係る電子利用者証明
  - 民間企業による電子商取引に係る電子利用者証明

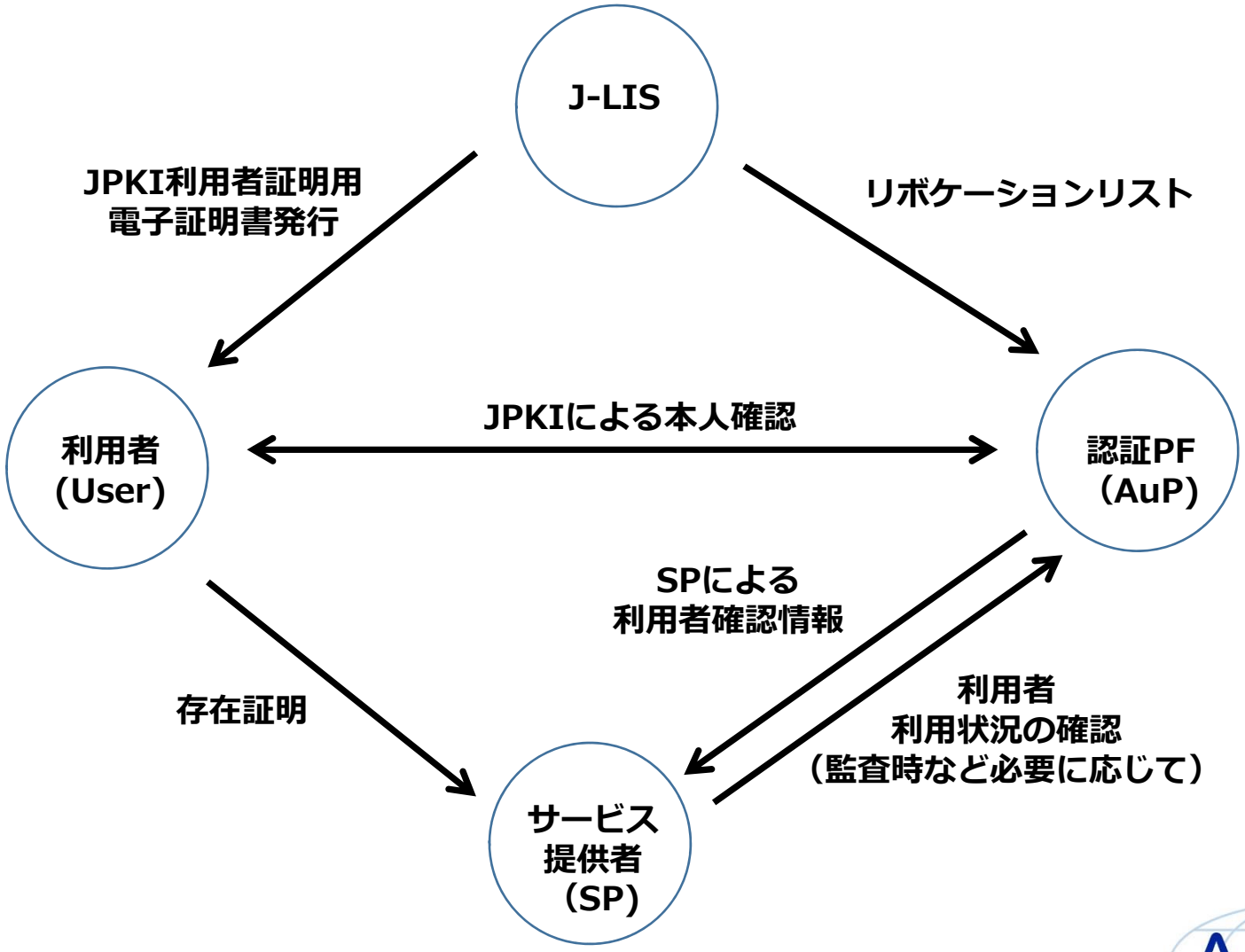
昨年度の検討

- **機関認証による利用者証明機能を用いたカード識別IDの生成**
  - 定数に対して署名させることで、固定のカード識別IDを取得し、サービス利用者はカード所有者の識別に利用
  - カードIDの生成は、PKCS#1 v1.5でのみ実現可能
- **デジタル署名の方式が、PKCS-PSS　(Probabilistic Signature Scheme)やECDSAに移行する際には利用できない**
  - デジタル署名時にカード内で生成された乱数が利用されるため



電子利用者証明用証明書シリアルを利用できないか

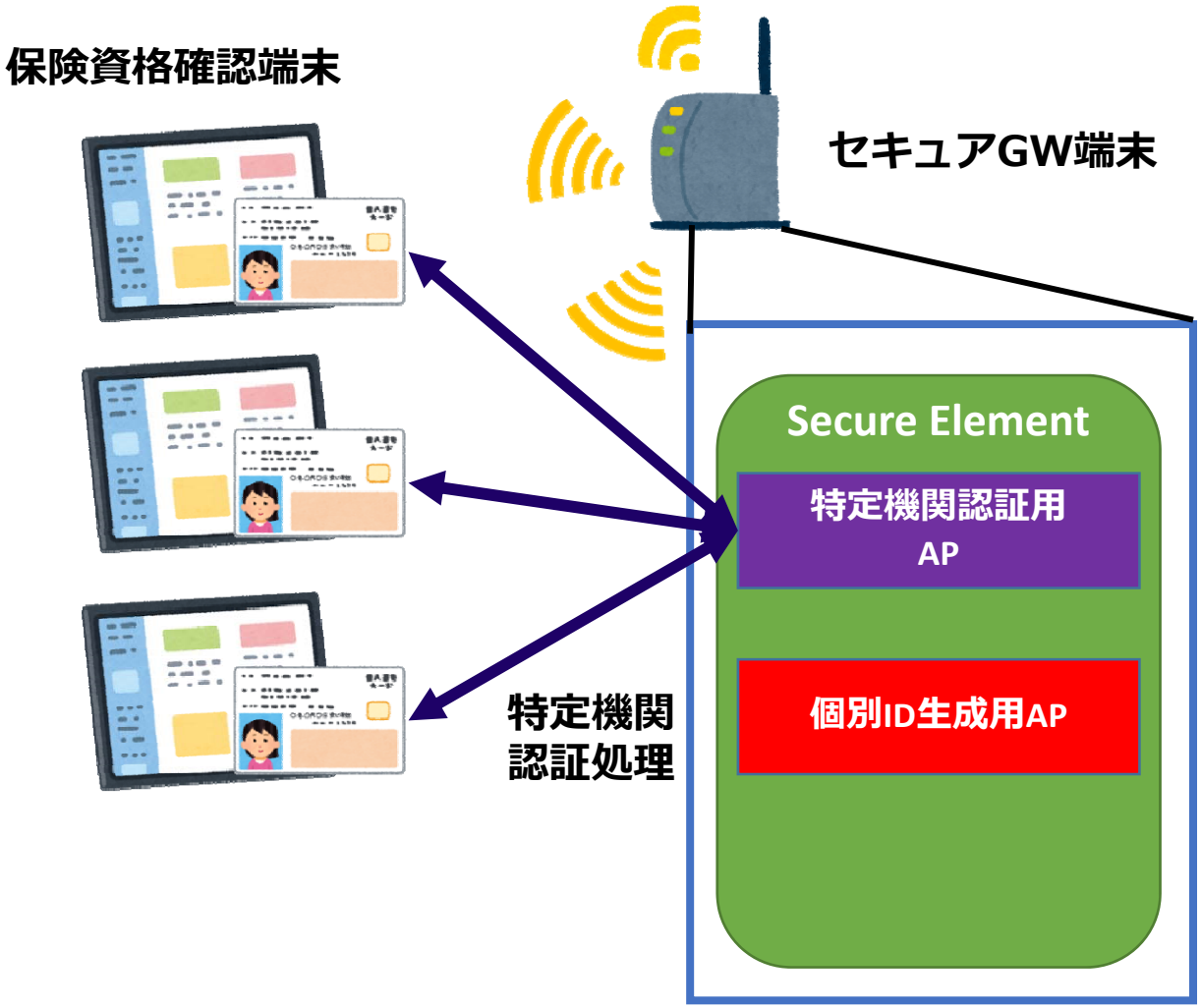
想定するプレーヤ


J-LIS
JPKI利用者証明用
電子証明書発行
リポケーションリスト
利用者
(User)
JPKIによる本人確認
認証PF
(AuP)
SPによる
利用者確認情報
存在証明
利用者
利用状況の確認
（監査時など必要に応じて）
サービス
提供者
(SP)

サービス提供者による利用者確認

1. サービス提供者（SP)は証明書シリアル等の管理が不要であること
2. 認証PFは各SP内でのみ利用者を特定可能な利用者情報を提供すること（利用者のマッチングにつながる可能性があるため）
3. ２の利用者情報を用いて、SPはJ-LISが配布する失効リストに基づく失効確認が可能であること
4. 通常利用時は、SPからAPへ利用者情報の提供は行わないこと（認証PFにユーザーのサービス利用状況を把握されることを防ぐため）
5. 上記を実現するために必要な処理は、現在のICカードでも実装可能な剰余演算及びハッシュ値生成とすること

GW端末等に搭載されるSE等を利用



配布資料には、詳細は記載していません

まとめ

- 公的個人認証サービスの民間利用拡大を念頭に、認証PFが用意すべき機能を具体的に検討

- 今後は、制度や暗号理論の標準化提案状況、端末へ搭載されるセキュアエレメントなどの機能の状況等を踏まえ、更なる検討を進めていく予定

Tokyo Tech

Thank you