ブロックチェーンにおける本人性確認の方法に関する考察

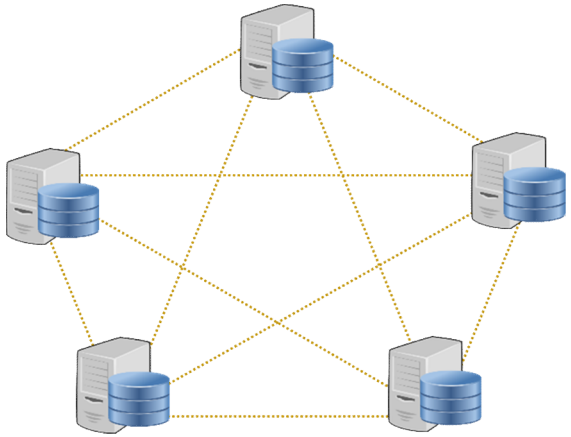
東京工業大学　科学技術創成研究院
社会情報流通基盤研究センター
永田　和之

発表内容

1. 本考察の目的
2. ブロックチェーンの概要
3. 公的個人認証サービス（JPKI）の概要
4. ブロックチェーンにおける本人性確認
5. まとめと課題

1．本考察の目的

ブロックチェーン



公的個人認証サービス

愛称
「マイキーくん」

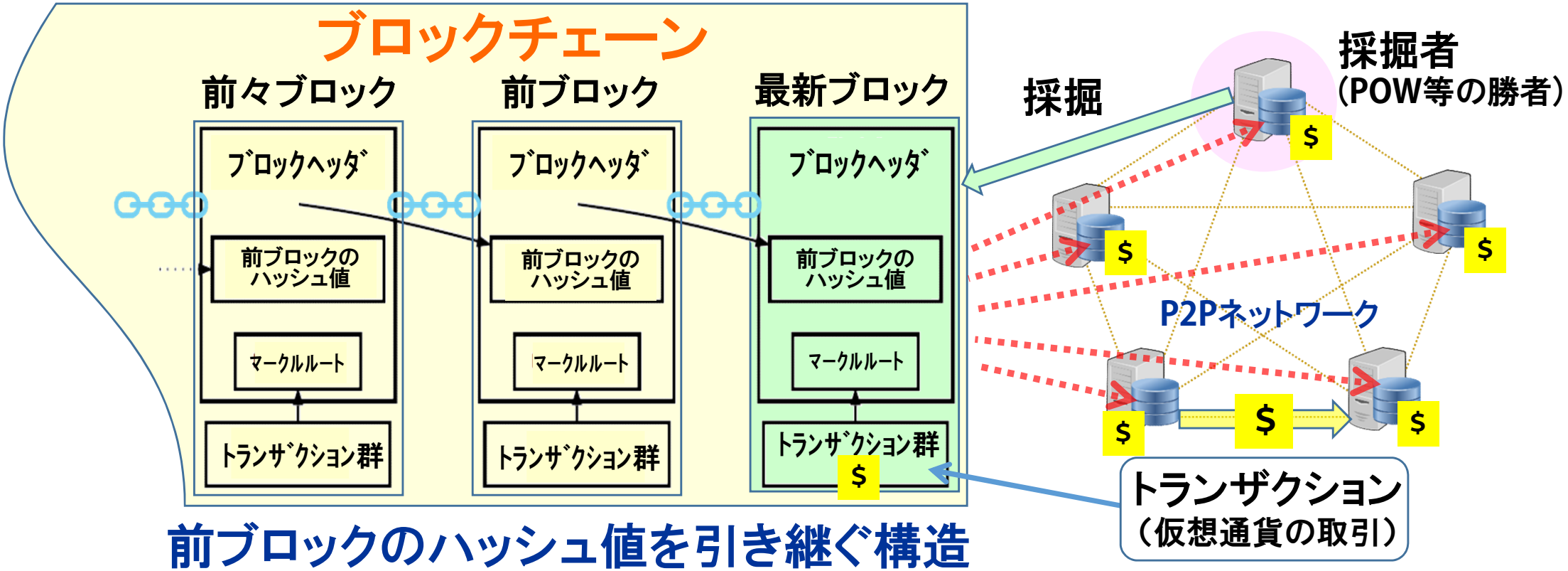
⇨ ブロックチェーンにおける本人性確認

⇩

新たなサービスの創出への寄与

2. ブロックチェーンの概要

- “Bitcoin: A Peer-to-Peer Electric Cash System” by Satoshi Nakamoto, 2008



前ブロックのハッシュ値を引き継ぐ構造

改ざんが困難な電子分散台帳としての特徴

2. ブロックチェーンの概要

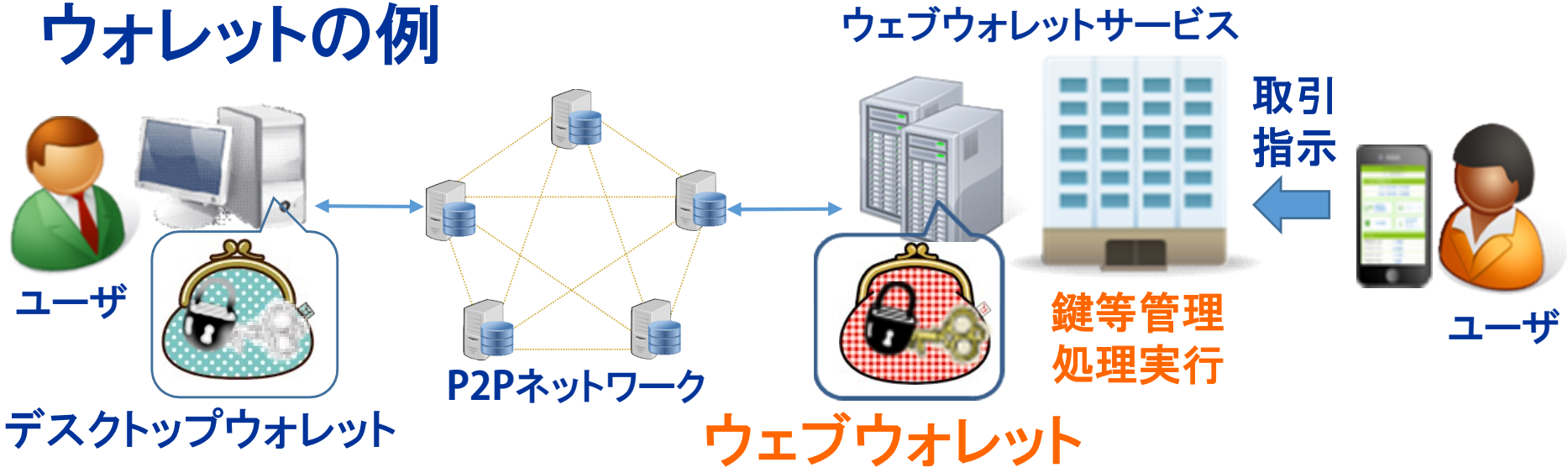
➢ Bitcoinのトランザクション

■ プライバシ保護のため、通常、トランザクション毎に

秘密鍵 → 公開鍵 → アドレス を生成 ⇒ 仮名での処理

※暗号方式：ECDSA

■ ウォレットの例

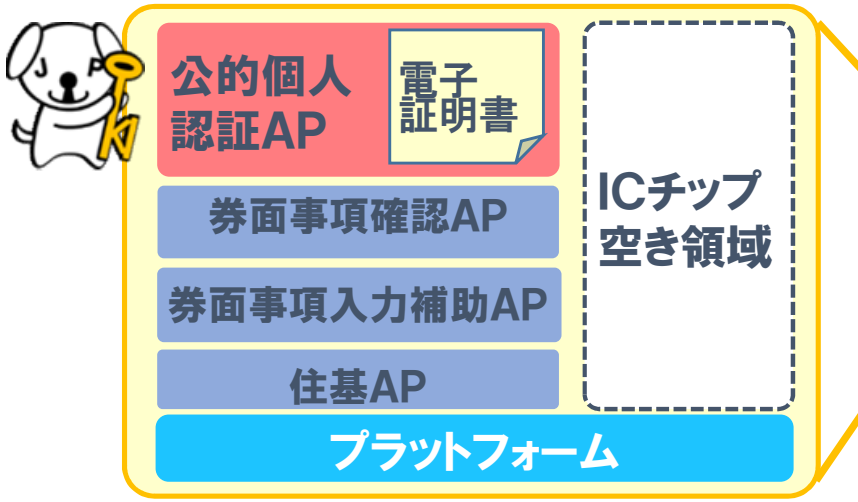


■ データ記録が可能（標準仕様で 最大80バイト）

※「OP_RETURN」スクリプトの利用

3. 公的個人認証サービス（JPKI）の概要

個人番号カード（マイナンバーカード）のイメージ

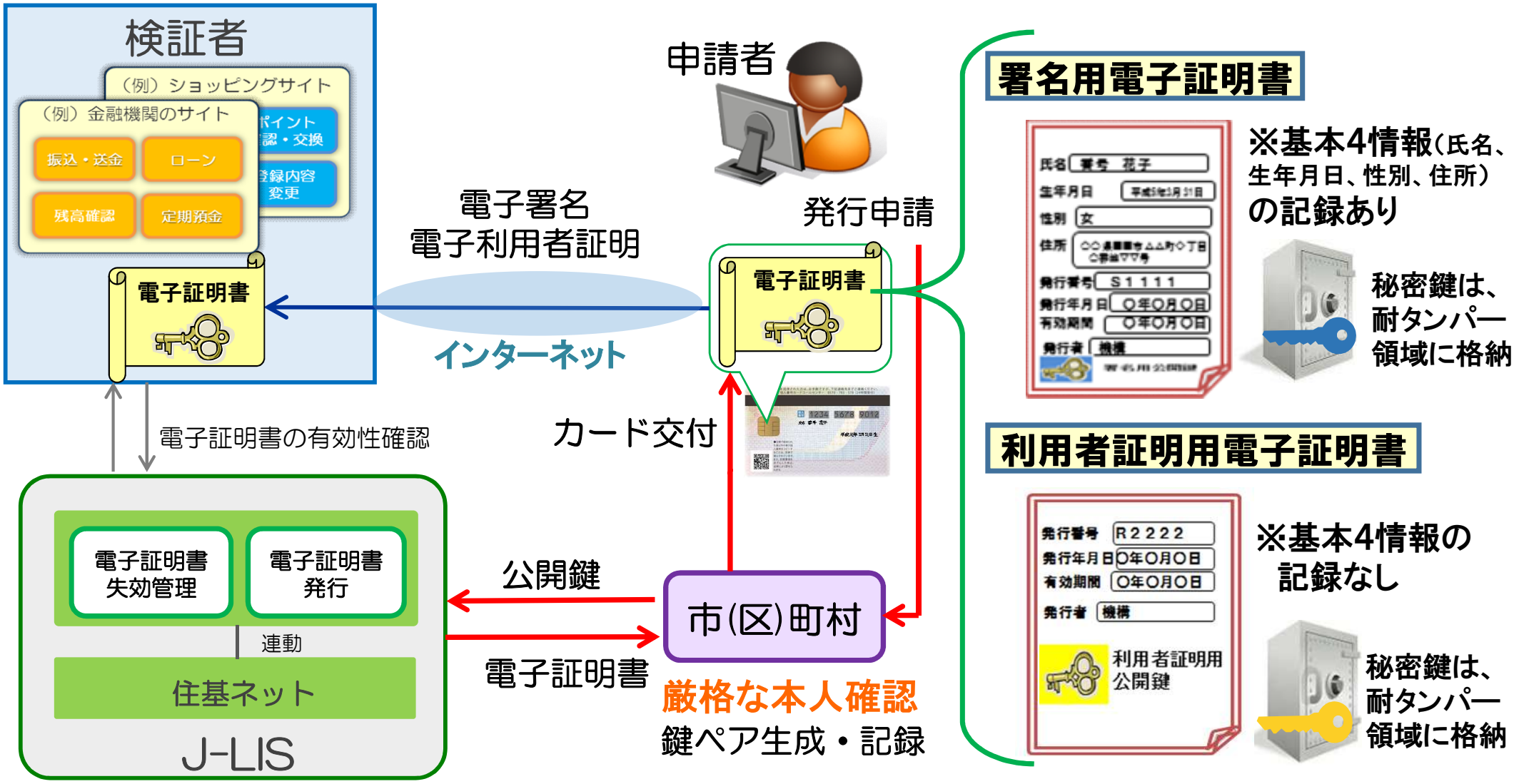


	マイナンバーカードのJPKI	（参考）住民基本台帳カードのJPKI
根拠法令	電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律	電子署名に係る地方公共団体の認証業務に関する法律
提供主体	地方公共団体情報システム機構（J-LIS）	都道府県
機能	・電子署名 ・電子利用者証明（電子認証機能）	・電子署名
検証者	・行政機関等 ・総務大臣が認める民間事業者	・行政機関等

図出典：「マイナンバーカードの概要及び公的個人認証サービスを活用したオンライン取引等の可能性について」
総務省自治行政局住民制度課（平成28年11月）に基づき作成

3. 公的個人認証サービス(JPKI)の概要

顧客データと**電子証明書の発行番号**を**紐付けて管理・利用**可能

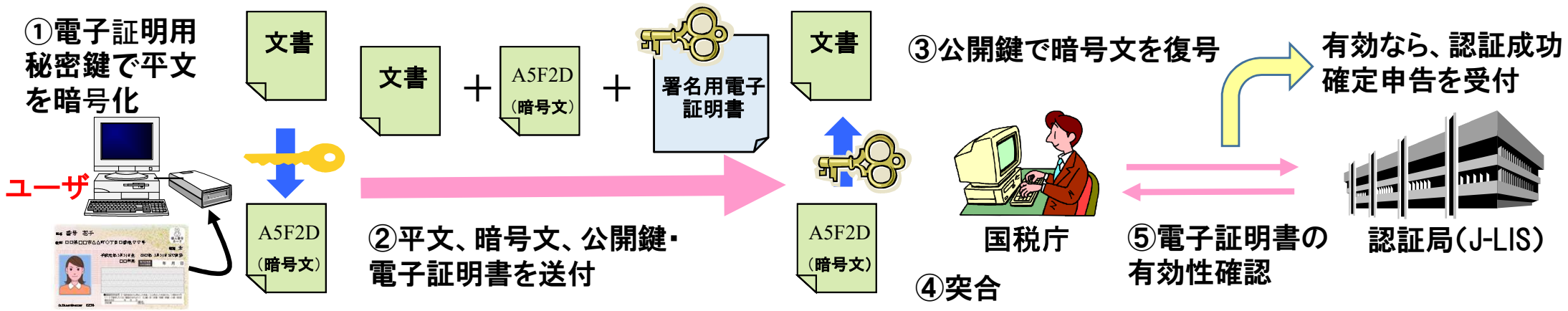


出典:「マイナンバーカードの概要及び公的個人認証サービスを活用したオンライン取引等の可能性について」
総務省自治行政局住民制度課(平成28年11月)に基づき作成

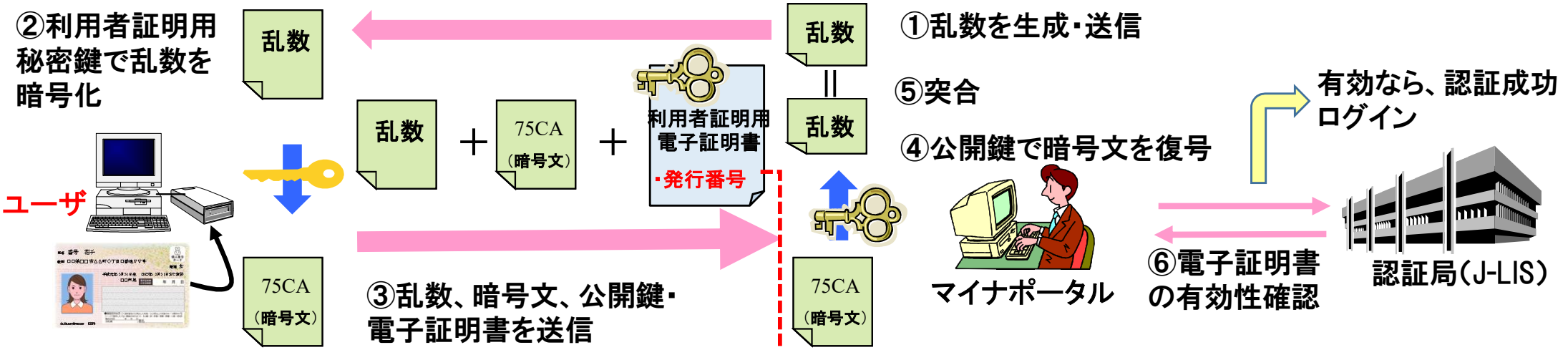
3. 公的個人認証サービス(JPKI)の概要

【凡例】 秘密鍵: 公開鍵: ※ 下図は主な処理に限りそのイメージを記載

1 電子署名 （例） e-Tax(国税電子申告・納税システム)による確定申告(イメージ)

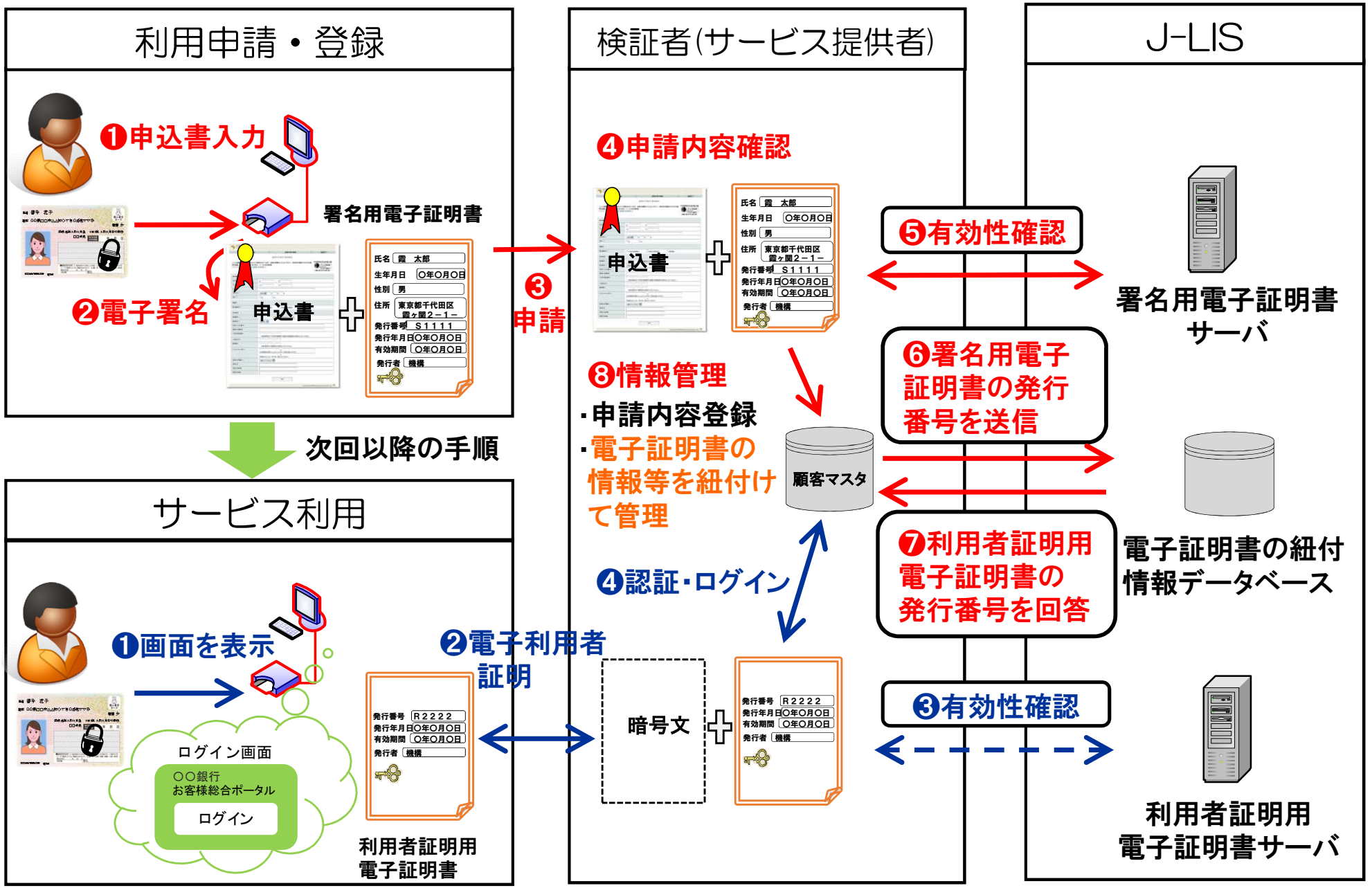


2 電子利用者証明 （例） マイナポータルへのログイン(イメージ)



出典:「マイナンバーカードの概要及び公的個人認証サービスを活用したオンライン取引等の可能性について」総務省自治行政局住民制度課（平成28年11月）に基づき作成

3. 公的個人認証サービス(JPKI)の概要



出典:「マイナンバーカードの概要及び公的個人認証サービスを活用したオンライン取引等の可能性について」総務省自治行政局住民制度課(平成28年11月)に基づき作成

4. ブロックチェーンにおける本人性確認

- 本考察の前提
  - 検討システムとして Bitcoin を対象
  - 本人性確認の方法として JPKI を利用
  - システムの基本的な仕様・運用の変更不要な方法を検討

  - ブロックチェーンのトランザクション実行者の本人性を確認する方法を検討

4. ブロックチェーンにおける本人性確認

- 他者を介在させない方法

  ⇨ トランザクション実行者がアドレス等とその証跡を生成

  - トランザクション毎に生成されるアドレス等の本人性確認が困難
  - JPKIの電子署名のデータサイズ（約256バイト）と署名検証の問題

⇩

本検討の対象外

4. ブロックチェーンにおける本人性確認

➢ 他者を介在させる方法

前提

- ユーザは、**ウェブウォレット**によりトランザクションを実行
  → アドレス等生成の証跡確保が可能
- ウェブウォレットサービス提供者は **JPKIの検証者**

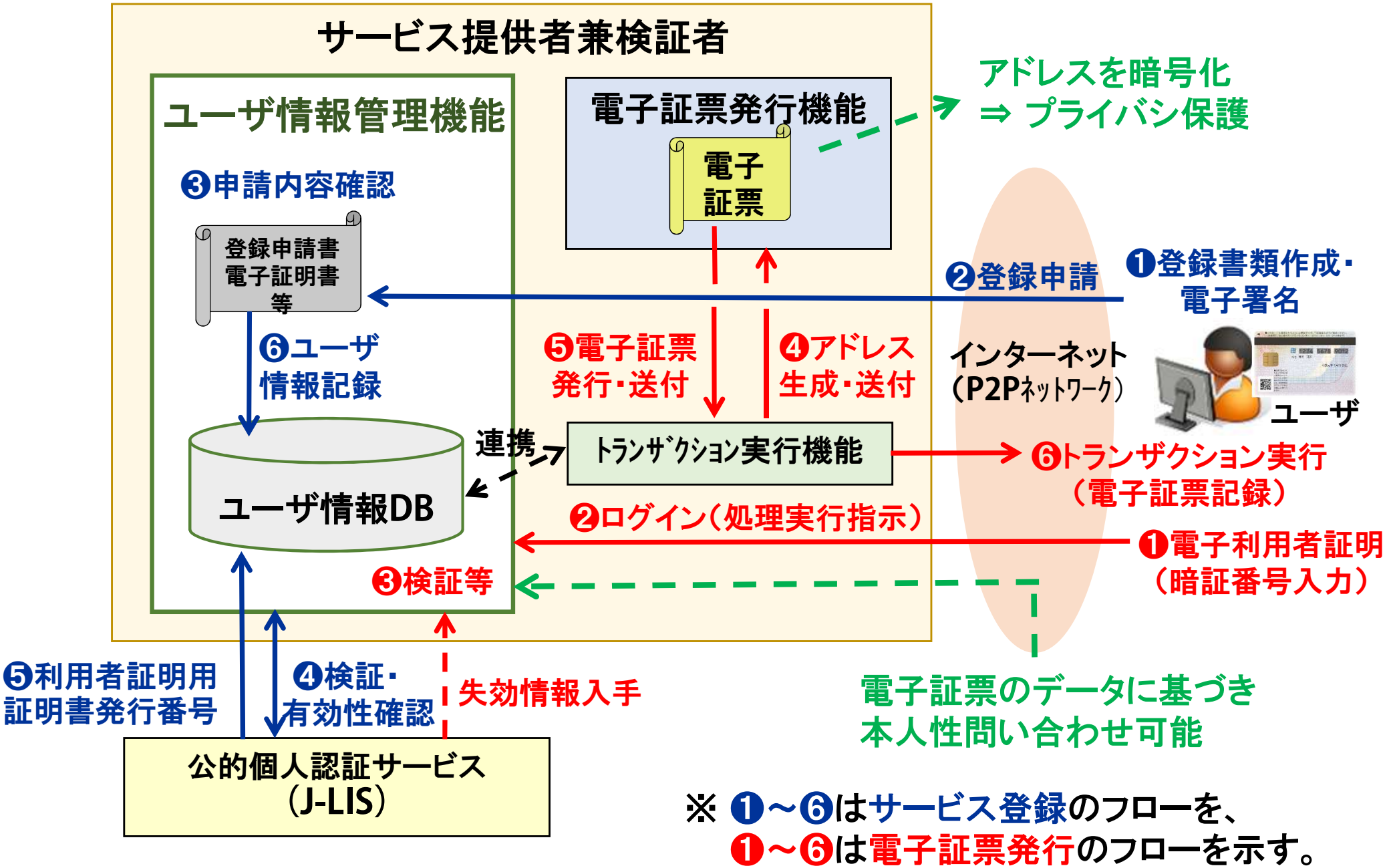
方法

- **JPKIの電子署名**（申請）・**電子利用者証明**（ログイン）を利用
- ユーザの指示により、サービス提供者が**電子証票**を発行・記録

✓ 発行者識別符号
✓ アドレスの暗号化・ハッシュ値
等から構成（数十バイト以下）

本人性を示す
電子的情報

4. ブロックチェーンにおける本人性確認



※ ❶～❻はサービス登録のフローを、
❶～❻は電子証票発行のフローを示す。

5. まとめと課題

➢ まとめ

JPKIを利用して、トランザクション実行者の本人性を示す**電子証票**を**ブロックチェーン上に記録**する際の基本的な考え方と処理手順等を例示

⇒ **実名**に基づく処理が可能

➢ 課題

- 想定するユースケース毎に実環境での検証等を通じた**処理手順等の精緻化**や**セキュリティ面の安検討**等
- 電子証票発行サービス提供者に対する信頼性確保に向けた**制度面の検討**

ご清聴ありがとうございました。