さまざまな決済スキームとそのセキュリティ
～デジタルウォレット～

筑波大学
面 和成

2025年3月6日

様々なデジタルウォレット

- 暗号資産ウォレット
  - BitcoinやEthereumなどの暗号資産取引に使用する秘密鍵を管理するためのウォレット
  - ホットウォレット，コールドウォレット，スマートコントラクトウォレット
- デジタルIDウォレット
  - 個人情報や電子証明書を管理し，オンライン認証に利用するウォレット
  - 政府が発行する電子IDを管理するウォレット（eIDウォレット）が有名
    - European Digital Identity Wallet (EUDIW) (EU)
    - マイナンバーカード（日本）
- 決済ウォレット
  - スマホ決済に使用するウォレット
  - クレジットカード，デビットカード，交通系ICカードなどを安全に保存できる
    - Google Wallet，Apple Wallet

暗号資産ウォレット

- ホットウォレット（オンラインウォレット）
  - インターネットに接続された状態で運用されるウォレット
  - リアルタイムで取引が可能
  - ブラウザ拡張機能やモバイルアプリで利用可能
    - MetaMaskなど

METAMASK

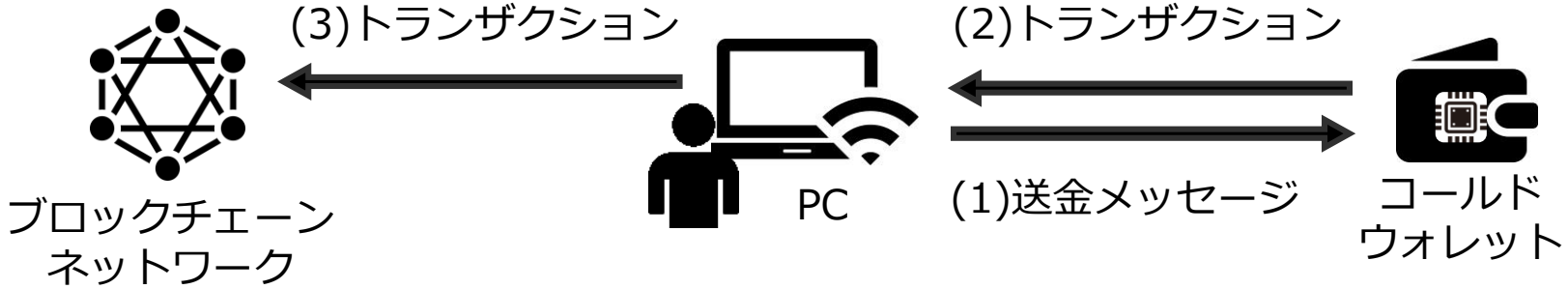
- コールドウォレット（オフラインウォレット）
  - インターネットへの接続を前提としない状態で秘密鍵を保管するウォレット
    - ハードウェアウォレット，ペーパーウォレットなど
  - 外部からのハッキングを受けにくく，セキュリティが非常に高い.

Ledger Nano S

Bitcoin ペーパーウォレット

コールドウォレットの「安全神話」に潜むリスク

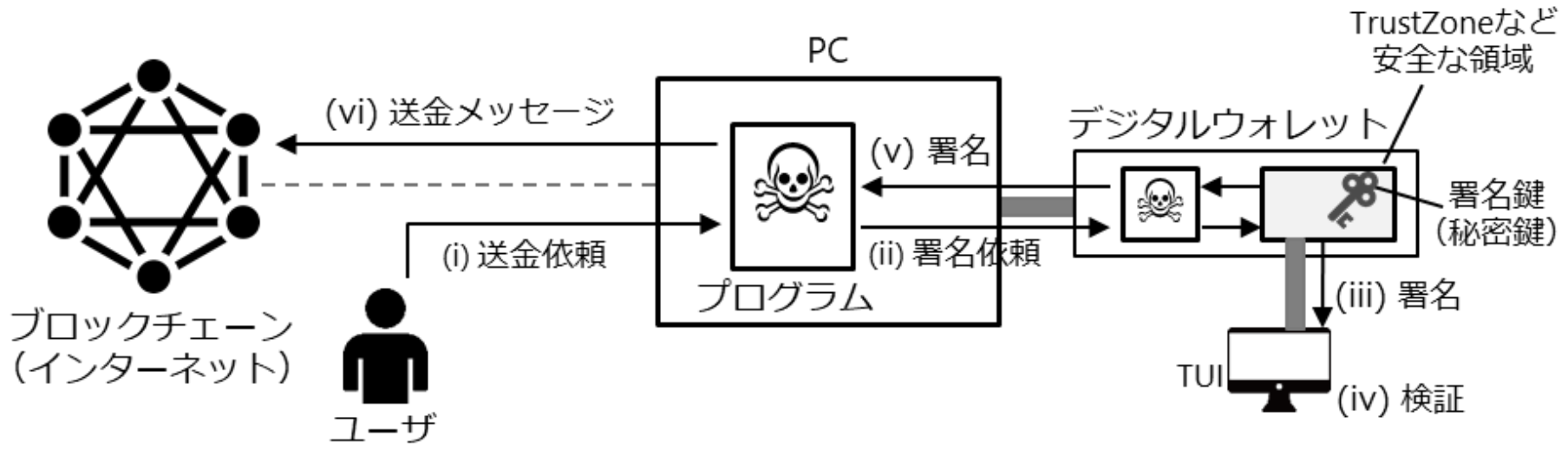
- 秘密鍵の紛失・破損のリスク
- ウォレットの物理的盗難
- 実はウォームウォレットと同じリスクをもつ
  - マルウェア感染による秘密鍵の漏洩（Man-in-the-Mobile攻撃）
  - 送金依頼メッセージの改ざん
  - 送信時のビューマンエラー



ウォームウォレット：
- 一時的にオンライン接続することで取引できるが，通常はオフライン保管.
- コールドウォレットではないが，ホットウォレットより安全とされる.

安全なウォレットシステムの例 [KO24]

- 送金依頼メッセージがPC内のプログラムで改ざんされたら，いくらデジタルウォレットが安全でも意味がない.
- TrustZoneとTrusted UIを用いることによって，マルウェア感染による秘密鍵の漏洩や送金依頼メッセージの改ざんに耐性を持つ.



[KO24] 小林紘也，面和成，「不正なトランザクションの発行を防ぐコールドウォレットシステムの提案」，コンピュータセキュリティ研究会，2024-CSEC-107(28)，pp.1-7，2024年12月.

マイナンバーカードを用いたウォレット

- デジタルIDウォレットの一つ
- マイナンバーカードが2026年を目処にRSA署名からECDSA署名に移行する
- ECDSAベースのマイナンバーカードでは，安全性を考慮しなければ，暗号資産ウォレットとして使用することは可能
  - マイナンバーカードの検証鍵（公開鍵）からウォレットアドレスを生成すればOK
    - Bitcoin：公開鍵をSHA-256とRIPEMD-160に通して出力されたハッシュ値から生成
    - Ethereum：公開鍵をKeccak-256に通して出力されたハッシュ値から生成
- マイナンバーカードに紐づく署名鍵（秘密鍵）と検証鍵（公開鍵）はユーザ毎に固定
  - トランザクションの署名からプライバシーの問題が生じる可能性がある.