高度なサイバー攻撃に耐性を持つデジタルウォレットシステムに関する研究

研究代表者　面　和成　　筑波大学　システム情報系　教授

1　はじめに

近年，ブロックチェーン技術を基盤とする暗号資産は，新たな価値交換手段として急速に普及している [25]．このような環境において，資産の安全性を担保するためには，秘密鍵の適切な管理と，トランザクションの真正性の確保が極めて重要となる．一般に，暗号資産の管理手法としては，常時ネットワークに接続されたホットウォレットと，オフライン環境で秘密鍵を保持するコールドウォレットが存在し，後者は高い安全性を有することから広く推奨されている [1][2]．

しかしながら，コールドウォレットであっても完全に安全とは言えない．実際の送金処理においては，トランザクションの生成やブロードキャストのために，PC やスマートフォンなどのオンラインデバイスと連携する必要がある．このとき，オンラインデバイスがマルウェアに感染している場合，ユーザが意図したトランザクション内容が改ざんされる危険性がある．特に，送金先アドレスの改ざんは重大な脅威であり，一度承認されたトランザクションは取り消すことができないため，被害は不可逆的である．

このような攻撃は，Man-in-the-Mobile（MitMo）攻撃 [19] と呼ばれ，モバイル端末内部に侵入したマルウェアがトランザクションデータを改ざんすることで実現される．例えば，ユーザが正しい送信先アドレスを入力しても，署名直前に攻撃者のアドレスへと置換されるケースが報告されている．さらに，アドレスは長い英数字列であるため，ユーザが目視で正当性を確認することは困難であり，ヒューマンエラーに依存した従来の対策には限界がある．

この問題に対し，これまで様々な研究が提案されてきた．TrustZone などの Trusted Execution Environment(TEE)を用いて秘密鍵管理や署名処理を保護する手法[13][14]，QR コードを用いたオフライン連携による攻撃面の縮小 [24]，さらには Ethereum Name Service（ENS）[23]を用いたアドレス解決の信頼性向上手法などが検討されている．しかしながら，これらの研究はそれぞれ異なる側面に焦点を当てており，トランザクション内容の真正性確認，ユーザ認証，および送金先アドレスの正当性保証を統合的に実現する枠組みは十分に確立されていない．

公益財団法人電気通信普及財団
研究調査助成報告書　第41号　2026年度

従来のコールドウォレットにおいては，「表示された情報が正しい」という前提に依存している点も問題である．オンラインデバイスやリッチ OS が侵害されている場合，ユーザに提示される情報自体が信頼できない可能性がある．このような状況では，単に秘密鍵を安全に管理するだけでは不十分であり，「ユーザが確認する情報の信頼性」を保証する仕組みが不可欠となる．

以上の背景を踏まえ，本研究では，既存のコールドウォレットにおける課題を統合的に解決する新たなアーキテクチャの構築を目的とする．具体的には，TEE(TrustZone)による安全な署名生成と Trusted UI による情報提示の信頼性確保，eID カードを用いた強固なユーザ認証，および ENS と電子署名を組み合わせた送金先アドレスの正当性検証を導入することで，オンラインデバイスが信頼できない環境においても安全なトランザクション実行を実現する．

本稿では，これら複数の研究を統合・発展させた新たな 2 つの提案方式を示し，それぞれの有効性と実用性について議論する．これにより，暗号資産取引における MitMo 攻撃やアドレス改ざん攻撃に対して包括的な防御を提供し，ユーザが意図したトランザクションのみを確実に実行できる環境の実現を目指す．

2 準備

本章では，本研究で提案するコールドウォレットシステムの理解に必要となる基礎技術について説明する．具体的には，暗号資産とコールドウォレットの基本概念，電子身分証明（eID)，Trusted Execution Environment（TEE)，および送金先アドレス解決技術について述べる．

2.1 暗号資産とコールドウォレット

暗号資産は，ブロックチェーン技術に基づく分散型デジタル通貨であり，Bitcoin や Ethereum に代表されるように，中央管理者を持たずに取引が成立する仕組みを有する．トランザクションの正当性は，送信者が保持する秘密鍵による電子署名によって保証される [3]．また，ブロックチェーンに記録された取引は高い耐改ざん性を有する一方で，一度承認されたトランザクションは取り消すことができないという不可逆性を持つ．

秘密鍵の管理手法としては，オンライン環境で管理するホットウォレットと，オフライン環境で管理するコールドウォレットが存在する．コールドウォレットはネットワークから隔離されているため，高い安全性を提供するが，実際の送金時にはオンラインデバイスとの連携が必要となる．この連携過程において，トランザクションデータが改ざんされるリスクが存在する．さらに，ハードウェアウォレットの安全性に関する形式的解析も提案されており，秘密鍵の隔離やトランザクション検証の重要性が指摘さ

れている．

2.2 eIDカードと電子署名

eIDカードは，政府などが発行する電子的な身分証明書であり，ICチップ内に公開鍵基盤（PKI）に基づく電子証明書を格納している．ユーザは暗証番号（PIN）を用いて認証を行い，秘密鍵を用いた電子署名を生成することができる [4]．この電子署名により，データの真正性および完全性が保証される [5]．

本研究では，このeIDカードを用いてユーザ認証を行い，コールドウォレットにおける署名生成処理の正当性を担保する．特に，チャレンジレスポンス方式を用いることで，リプレイ攻撃などへの耐性を確保する．

2.3 TEEとTrustZone

Trusted Execution Environment（TEE）は，メインのオペレーティングシステムから分離された安全な実行環境であり，機密情報の保護やセキュアな処理の実行を目的としている．ARM TrustZoneは，TEEを実現する代表的なハードウェア技術であり，システムを「セキュアワールド」と「ノーマルワールド」に分割することで，セキュリティクリティカルな処理を安全な領域で実行することを可能にする [6][7][8][9]．

この構造により，仮にノーマルワールドで動作するOSやアプリケーションがマルウェアに感染した場合でも，セキュアワールド内の秘密鍵や署名処理は保護される．本研究では，この特性を活用し，秘密鍵管理およびトランザクション署名生成をTEE内で実行する．

さらに，TEEの拡張機能としてTrusted UIがある [10]．これは，TEEがディスプレイや入力デバイスを直接制御することで，ユーザに提示される情報の信頼性を保証する仕組みである．これにより，マルウェアによる画面改ざんや入力の盗聴を防ぐことができる．

2.4 ENSによるアドレス解決

Ethereum Name Service（ENS）は，人間が理解しやすいドメイン名とブロックチェーンアドレスを対応付ける仕組みであり，スマートコントラクトとして実装されている．ENSはレジストリとリゾルバから構成され，ドメイン名に対応するアドレス情報を分散型台帳上で管理する．

ENSの利点は，中央集権的なDNSと異なり，ブロックチェーンの特性により高い耐改ざん性を持つ点である．しかし，ENSを利用する場合でも，オンラインデバイスを経由する過程でアドレス情報が改ざんされる可能性がある．そのため，本研究ではENSによるアドレス解決に加え，電子署名を組み合わせることで，取得したアドレスの正当

性を暗号学的に検証する仕組みを導入する.

2.5 脅威モデルの前提

本研究では，オンラインデバイスは信頼できないものと仮定し，マルウェア感染による Man-in-the-Mobile（MitMo）攻撃を主要な脅威として想定する．この攻撃では，トランザクションデータや送金先アドレスが改ざんされる可能性がある．さらに，Android マルウェアの分析も報告されている [11][12].

したがって，本研究では，(1)秘密鍵の安全な管理，(2)ユーザ認証の強化，(3)ユーザが確認する情報の信頼性確保，(4)送金先アドレスの正当性検証，の 4 点を満たすシステム設計を目標とする．これにより，ユーザが意図したトランザクションのみを安全に実行可能とする.

3 既存研究

本章では，本研究の位置付けを明確にするために，コールドウォレットおよび暗号資産取引の安全性向上に関する既存研究を整理する.

3.1 TEE を用いたウォレットの研究

TEE を活用したウォレットの研究として，Miraje ら [13] は TrustZone を用いた Bitcoin ウォレットを提案し，秘密鍵の漏洩防止に有効であることを示した．この研究では，セキュアワールドにおいて鍵管理および署名処理を行うことで，辞書攻撃やサイドチャネル攻撃に対する耐性を強化している．しかしながら，当該手法はホットウォレットとして設計されており，全ブロックデータを保持する必要があるため，リソース制約のあるデバイスには適さないという課題がある.

これに対し，Dai ら [14] は TrustZone を用いた軽量ウォレットを提案し，ブロックヘッダのみを用いた検証により，データ量を削減した．この手法は組み込み機器でも動作可能である点で実用性が高いが，トランザクション検証のためにオンライン環境への依存が残るため，オンラインデバイスが信頼できない場合には改ざんリスクが残存する.

さらに，TEE の安全性を拡張する技術として Trusted UI が提案されている．Trusted UI は，TEE がディスプレイや入力装置を直接制御することで，ユーザが確認する情報の真正性を保証する仕組みである．しかし，既存研究においては，Trusted UI をトランザクション検証に体系的に適用した例は限定的である.

3.2 コールドウォレットの構成と連携手法

コールドウォレットの運用に関する研究として，Khan ら [15] は 2 台の Android 端

末を用い，QR コードを介してトランザクションデータをやり取りする手法を提案している．この方式では，秘密鍵を保持するデバイスをオフラインに保つことで，鍵漏洩リスクを低減している．QR コード自体の技術的背景についても広く研究されている．

しかし，この手法は主に秘密鍵の保護に焦点を当てており，トランザクション内容そのものの正当性検証については十分に考慮されていない．特に，オンラインデバイス上で生成されるトランザクションデータが改ざんされた場合，その検知が困難であるという問題がある．

大塚ら［16］は SIM カードと TEE を組み合わせた認証方式を検討しており，高いセキュリティを実現可能であることを示している．しかし，TEE による画面出力機能の普及率の低さなど，実用面での課題が指摘されている．

3.3 アドレス改ざん攻撃とその対策

暗号資産における代表的な攻撃の一つが送金先アドレスの改ざんである．Ivanov ら［22］は，クリップボードを介してアドレスを書き換える EthClipper 攻撃を報告しており，視覚的に類似したアドレスを生成することでユーザの目視確認を欺く手法を示している．さらに，近年ではアドレスポイズニング攻撃のように，ユーザの誤認を誘発する新たな攻撃も報告されている．

Garba ら［21］は Web 上で公開されているアドレスの多くが非セキュアな通信路で提供されていることを指摘し，MitMo 攻撃による改ざんリスクを明らかにしている．これらの研究は，アドレス取得段階および入力段階の双方において改ざんの危険性が存在することを示している．また，MitMo 対策技術として SIM ベースの研究も存在する．

従来の対策としては，コールドウォレットの画面に表示されたアドレスをユーザが目視で確認する方法が一般的である［17][20]．しかし，長大な英数字列の比較は人間にとって困難であり，ヒューマンエラーを完全に排除することはできない．このため，ユーザの注意に依存しない自動的な検証機構の必要性が指摘されている．

3.4 アドレス認証および信頼性保証

アドレスの正当性を保証するための研究として，Ateniese ら［18］は認証局を用いた「Certified Bitcoins」を提案している．この手法では，アドレス生成時に認証局が関与することで，送金先の身元を保証することが可能である．

しかしながら，この方式は新規アドレスの生成を前提としており，既存のアドレスには適用できないという制約がある．また，ネットワーク全体のプロトコル変更が必要となるため，実用的な導入の障壁が高い．

一方，近年では ENS を用いて人間可読なドメイン名とアドレスを対応付ける手法が普及している．ENS はブロックチェーン上で管理されるため耐改ざん性が高いが，オン

ラインデバイスを経由する過程で応答が改ざんされる可能性がある．そのため，ENS 単体では完全な安全性を保証することはできない．

3.5 既存研究の課題と本研究の位置付け

以上の既存研究を整理すると，秘密鍵の保護，ユーザ認証，トランザクション検証，アドレス正当性保証といった要素技術は個別に提案されているものの，これらを統合的に扱った研究は限られている．特に，オンラインデバイスが完全に信頼できないという前提のもとで，ユーザが確認する情報の信頼性まで含めて保証する枠組みは不十分である．

本研究は，これらの課題を解決するために，TEE（TrustZone）による安全な署名生成，Trusted UI による情報提示の信頼性確保，eID カードによる強固な認証，および ENS と電子署名を組み合わせたアドレス検証を導入した新たなコールドウォレットアーキテクチャを提案する．これにより，従来研究の限界であった MitMo 攻撃およびアドレス改ざん攻撃に対して包括的な防御を実現する点に特徴がある．

また，近年では暗号資産ウォレット全体のセキュリティを体系的に整理した研究も存在する．例えば，SoK 研究ではウォレット設計における攻撃面や防御手法が包括的に分析されており，本研究の位置付けを理解する上で重要である．

4　提案方式 1（概要）

本章では，既存研究で提案されてきた TEE および Trusted UI を活用したコールドウォレット技術を基盤とし，eID カードによる強固なユーザ認証を統合した提案方式 1 について述べる．本方式は，特にトランザクション内容の真正性検証とユーザ意図の保証に重点を置き，Man-in-the-Mobile（MitMo）攻撃に対する耐性を強化することを目的とする．

4.1 設計方針

従来のコールドウォレットでは，秘密鍵の安全な保管は実現されているものの，トランザクションの生成や表示がオンラインデバイスに依存しているため，ユーザが確認する情報の信頼性が保証されていないという問題があった．また，TEE を用いた既存研究においても，署名処理の安全性は確保されているが，ユーザが確認する情報が改ざんされていないことを保証する仕組みは限定的である．

本方式では，「秘密鍵の安全性」だけでなく，「ユーザが確認する情報の信頼性」および「ユーザ本人による操作であることの保証」を同時に満たすことを設計目標とする．そのために，(1)TEE による安全な処理実行，(2)Trusted UI による表示の信頼性確保，(3)eID カードによる強固なユーザ認証，の三要素を統合する．

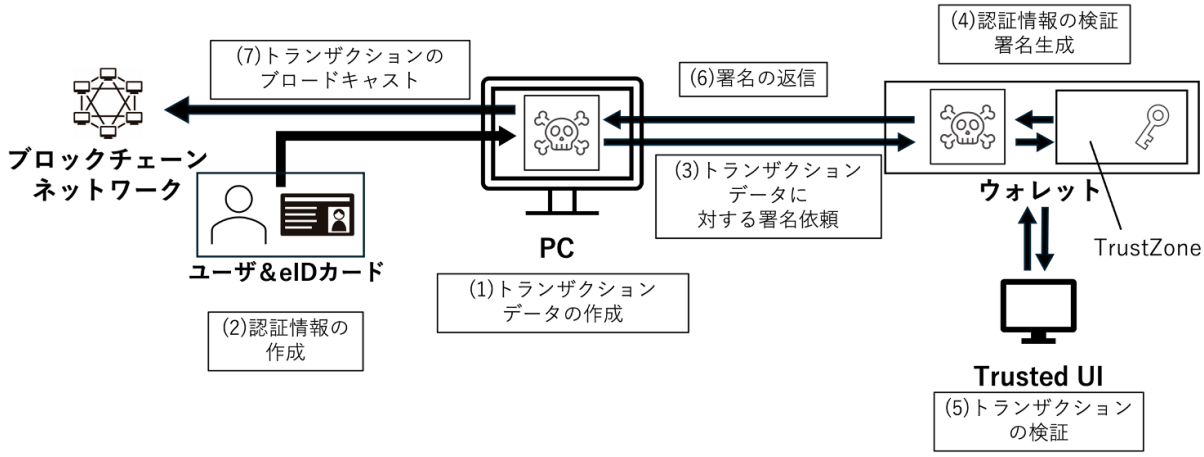

図 1　提案方式 1 の全体図

4.2 システム構成

提案方式 1 は，図 1 に示すとおり，主に以下の 4 つの構成要素から成る．

- オンラインデバイス（PC／スマートフォン）
  トランザクションデータの作成およびブロックチェーンネットワークへの送信を担う．本研究では，このデバイスはマルウェアに感染している可能性があるため，信頼できない要素として扱う．
- コールドウォレット（TEE 搭載デバイス）
  秘密鍵を TrustZone 内に保持し，署名生成および認証処理を実行する．すべてのセキュリティクリティカルな処理はセキュアワールド内で実行される．
- eID カード
  ユーザの本人性を証明するために用いる．電子証明書および秘密鍵を保持し，チャレンジレスポンス型の認証を実現する．
- Trusted UI
  TEE が直接制御する表示・入力インターフェースであり，ユーザに提示される情報の真正性を保証する．

4.3 プロトコルの流れ

提案方式 1 における送金処理は，以下の手順で実行される．

(1)．オンラインデバイス上でトランザクションデータを作成する．
(2)．eID カードはユーザの認証情報を作成する．
(3)．作成したトランザクション及び認証情報をコールドウォレットに送信する．
(4)．コールドウォレットは認証情報を検証し，検証が成功したら TrustZone 内の秘

密鍵を用いてトランザクションに対して署名を生成する.

(5). 認証成功後，トランザクションの内容を Trusted UI 上に表示する．ユーザは表示内容を確認し，承認操作を行う.

(6). 署名済みトランザクションをオンラインデバイスに返送する.

(7). オンラインデバイスがトランザクションをブロックチェーンネットワークへ送信する.

このプロセスにおいて重要なのは，トランザクション内容の最終確認および署名生成がすべて TEE 内で行われる点である．これにより，オンラインデバイス上での改ざんがあっても，ユーザが確認した内容と異なるトランザクションが署名されることはない.

4.4 セキュリティ分析

本方式は，MitMo 攻撃に対して以下の点で耐性を有する．まず，トランザクションの改ざん攻撃に対しては，Trusted UI 上でユーザが最終確認を行うため，オンラインデバイス上での改ざんは検知可能である．従来のようにリッチ OS が表示する情報に依存する場合と異なり，TEE が直接制御する表示は信頼できる.

次に，不正な署名生成要求に対しては，eID カードによる認証が必須であるため，攻撃者が任意のトランザクションに対して署名を生成させることは困難である．チャレンジレスポンス方式を用いることで，リプレイ攻撃も防止される.

さらに，画面のなりすまし攻撃に対しても，Trusted UI による表示により，ユーザが確認する情報の真正性が保証される．これにより，「正しい内容が表示されているように見せかける」攻撃を防ぐことができる.

4.5 限界と課題

本方式にはいくつかの課題も存在する．まず，送金先アドレスそのものの正当性については，本方式単体では保証されない．すなわち，ユーザが入力したアドレスが正しいものであるかどうかは別途検証が必要である.

また，Trusted UI を利用可能なデバイスの普及状況や，eID カードの利用環境に依存する点も実用上の課題である．さらに，ユーザによる確認操作が必要であるため，完全な自動化は困難である.

5　提案方式 2（概要）

本章では，提案方式 1 で残された課題，すなわち送金先アドレスの正当性保証の問題を解決するための提案方式 2 について述べる.本方式は,Ethereum Name Service(ENS)

と電子署名を組み合わせることで，オンラインデバイスが信頼できない環境においても，正しい送金先アドレスの取得と検証を可能にすることを目的とする．

5.1 設計方針

従来のコールドウォレットでは，送金先アドレスの正当性確認はユーザの目視に依存しており，ヒューマンエラーの影響を排除できないという問題があった．また，クリップボード改ざんや類似アドレス攻撃 [9] などにより，ユーザが意図しないアドレスへ送金してしまうリスクが指摘されている．

さらに，ENS のような仕組みを用いることでアドレスの可読性は向上するものの，オンラインデバイスを経由する通信経路において応答が改ざんされる可能性があるため，単体では十分な安全性を保証できない．ENS に関する仕様および設計については，標準仕様として提案されている．また，ENS のセキュリティ特性に関する分析も行われている．

本方式では，「オンラインデバイスを完全に信頼しない」という前提のもとで，(1)ENS によるアドレス解決，(2)サーバによる電子署名付与，(3)コールドウォレット側での署名検証，を組み合わせることで，アドレスの正当性を暗号学的に保証する．

5.2 システム構成

提案方式 2 は，図 2 に示すとおり，以下の構成要素から成る．

- コールドウォレット
  オフライン環境で動作し，秘密鍵の管理およびトランザクション署名を行う．信頼できる要素として扱う．
- オンラインデバイス
  コールドウォレットと外部サーバとの通信を中継する．マルウェア感染を前提とし，信頼できない要素とする．
- アドレス管理サーバ
  ENS を参照してアドレス解決を行い，その結果に電子署名を付与する．本研究では信頼できる要素と仮定する．
- ENS (Ethereum Name Service)
  ドメイン名とブロックチェーンアドレスの対応付けを行う分散型システムであり，高い耐改ざん性を有する．

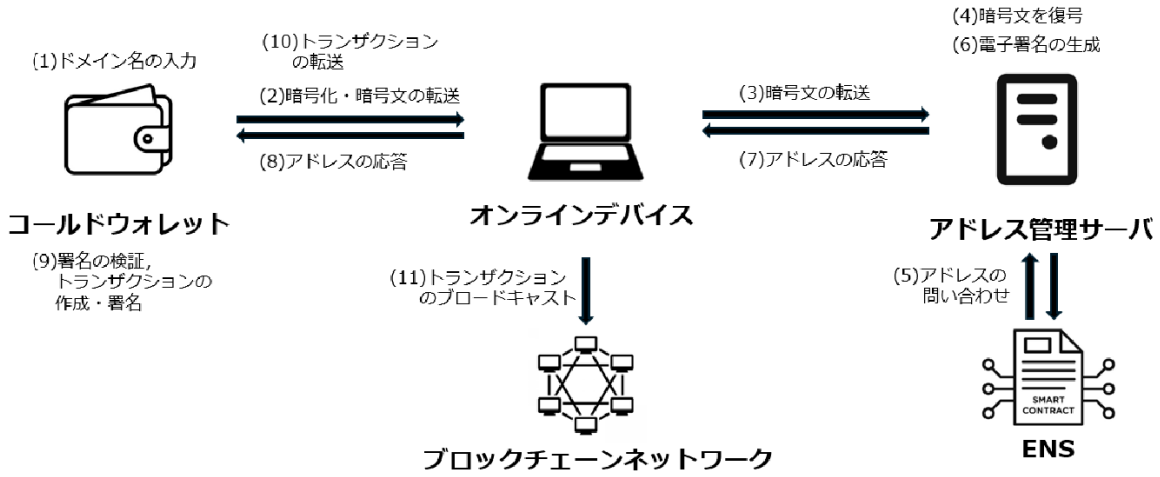

図 2　提案方式 2 の全体図

5.3 プロトコルの流れ

提案方式 2 の送金処理は以下の手順で行われる．

(1)．　ユーザはコールドウォレットに送金先の ENS ドメイン名を入力する．
(2)．　ドメイン名とチャレンジをサーバの公開鍵で暗号化し，オンラインデバイスへ送信する．
(3)．　オンラインデバイスは暗号文をそのままサーバへ転送する．
(4)．　サーバは暗号文を復号し，ドメイン名とチャレンジを取り出す．
(5)．　ENS を用いてアドレス解決を行う．
(6)．　解決したアドレスとチャレンジに対して電子署名を生成する．
(7)．　アドレスと署名をオンラインデバイスへ送信する．
(8)．　オンラインデバイスはデータをそのままコールドウォレットへ転送する．
(9)．　コールドウォレットは署名を検証して正当性を確認するとともに，トランザクションを作成し署名する．
(10)．署名済みトランザクションをオンラインデバイスに送信する．
(11)．署名済みトランザクションをブロックチェーンネットワークへブロードキャストする．

このプロトコルにより，オンラインデバイスが攻撃者に制御されている場合でも，アドレス情報の改ざんを検知することが可能となる．

5.4 セキュリティ分析

本方式は，以下の攻撃に対して耐性を有する．まず，アドレス改ざん攻撃に対して

は，サーバが生成した電子署名をコールドウォレット側で検証するため，改ざんされたアドレスは検出される．オンラインデバイスは署名を生成できないため，正当な応答を偽装することは困難である．

次に，リプレイ攻撃に対しては，チャレンジを導入することで防御している．トランザクションごとに異なるランダム値を用いることで，過去の応答の再利用は無効となる．

また，サーバなりすまし攻撃に対しても，事前に登録された公開鍵を用いた署名検証により，正当なサーバからの応答であることを確認できる．さらに，ENS 自体はブロックチェーン上で管理されているため，そのデータの改ざんは極めて困難である．これにより，アドレス解決の基盤となる情報の信頼性も担保される．

5.6 限界と今後の課題

本方式においては，アドレス管理サーバを信頼できる存在として仮定している点が制約となる．サーバが侵害された場合，誤ったアドレスに対して正当な署名が付与される可能性がある [26]．この問題に対しては，分散型サーバ構成や複数署名の導入などが今後の課題として考えられる．

また，通信遅延やシステムの複雑化に伴うユーザビリティの低下も考慮する必要がある．これらの課題を踏まえ，実運用を見据えた最適化が求められる．

6 まとめ

本研究では，暗号資産取引におけるコールドウォレットの安全性向上を目的として，二つの提案方式を示した．従来のコールドウォレットは秘密鍵の保護に重点が置かれていたが，オンラインデバイスを経由する過程でのトランザクション改ざんや送金先アドレスの不正変更といった問題に対しては十分な対策が講じられていなかった．特に，Man-in-the-Mobile（MitMo）攻撃により，ユーザが意図しないトランザクションが生成されるリスクが指摘されている．

提案方式 1 では，TEE（TrustZone）および Trusted UI を活用することで，ユーザが確認するトランザクション内容の真正性を保証し，さらに eID カードによる認証を組み合わせることで，不正な署名生成を防止した．これにより，オンラインデバイスが侵害されている場合でも，ユーザの意図に基づいたトランザクションのみが実行されることを実現した．

提案方式 2 では，ENS と電子署名を組み合わせたアドレス検証手法を導入し，送金先アドレスの正当性を暗号学的に保証した．従来の目視確認に依存した方法とは異なり，ヒューマンエラーの影響を排除し，オンラインデバイスを信頼しない前提でも安全なアドレス取得を可能とした．

今後の課題としては，アドレス管理サーバへの信頼依存の低減や，分散化による耐障害性の向上が挙げられる．また，ユーザビリティの観点から，操作負担を軽減しつつ高い安全性を維持する設計についても検討が必要である．これらの課題に取り組むことで，より実用的かつ安全な暗号資産取引基盤の実現が期待される．

【参考文献】

[1] Suratkar, S., Shirole, M. and Bhirud, S.: Cryptocurrency Wallet: A Review, 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), pp. 1–7 (2020).

[2] Zaghloul, E., Li, T., Mutka, M. W. and Ren, J.: Bitcoin and Blockchain: Security and Privacy, IEEE Internet of Things Journal, Vol. 7, No. 10, pp. 10288–10313 (2020).

[3] Nakamoto, S. and Bitcoin, A.: A peer-to-peer electronic cash system, Bitcoin.–URL: https://bitcoin.org/bitcoin. pdf, Vol. 4, No. 2, pp. 1–15 (2008).

[4] Shehu, A.-s., Pinto, A. and Correia, M. E.: On the inter-operability of European national identity cards, Ambient Intel ligence–Software and Applications–, 9th International Symposium on Ambient Intel ligence, Springer, pp. 338–348 (2019).

[5] 総務省：マイナンバー制度とマイナンバーカード｜マイナンバーカード，https://www.soumu.go.jp/kojinbango_card/03.html (2021)

[6] Pinto, S. and Santos, N.: Demystifying Arm TrustZone: A Comprehensive Survey, ACM Comput. Surv., Vol. 51, No. 6, pp. 1–36 (2019).

[7] Ngabonziza, B., Martin, D., Bailey, A., Cho, H. and Martin, S.: TrustZone Explained: Architectural Features and Use Cases, 2016 IEEE 2nd International Conference on Col laboration and Internet Computing (CIC), IEEE, pp. 445–451 (2016).

[8] Alves, T. and Felton, D.: Trustzone: Integrated hardware and software security, ARM white paper, Vol. 3, No. 4, pp. 18–24 (2004).

[9] ARM: ARM Security Technology. Building a Secure System using TrustZone Technology, ARM white paper (2009).

[10] Global Platform: Trusted User Interface API (2013).

[11] Cekerevac, Z., Cekerevac, P., Prigoda, L. and Al-Naima, F.: SECURITY RISKS FROM THE MODERN MAN-IN-THE-MIDDLE ATTACKS, MEST Journal, Vol. 13, pp. 34–51 (2025).

[12] Zhou, Y. and Jiang, X.: Dissecting android malware: Characterization and evolution, 2012 IEEE symposium on security and privacy, IEEE, pp. 95–109 (2012).

[13] Gentilal, M., Martins, P. and Sousa, L.: TrustZone-backed bitcoin wallet, Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems, Association for Computing Machinery, p. 25–28 (2017).
[14] Dai, W., Deng, J., Wang, Q., Cui, C., Zou, D. and Jin, H.: SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone, IEEE Access, Vol. 6, pp. 40638–40648 (2018).
[15] Khan, A. G., Zahid, A. H., Hussain, M. and Riaz, U.: Security Of Cryptocurrency Using Hardware Wallet And QR Code, 2019 International Conference on Innovative Computing (ICIC), pp. 1–10 (2019).
[16] 大塚玲, 佐藤裕之, 櫻木正一郎, 落合三男, 横田勇一, 藤澤将吾, 本間靖朗, 小関松子: SIM-Sign: 実用的な Android 端末向け MitMo 対策技術, コンピュータセキュリティシンポジウム 2016 論文集, Vol. 2016, No. 2, pp. 996-1003 (2016).
bitco
[17] M. Arapinis, A. Gkaniatsou, D. Karakostas, and A. Kiayias. A formal treatment of hardware wallets. In I. Goldberg and T. Moore, editors, Financial Cryptography and Data Security, pages 426–445, Cham, 2019. Springer International Publishing.
[18] G. Ateniese, A. Faonio, B. Magri, and B. de Medeiros. Certified bitcoins. In I. Boureanu, P. Owesarski, and S. Vaudenay, editors, Applied Cryptography and Network Security, pages 80–96, Cham, 2014. Springer International Publishing.
[19] Z. ˇCekerevac, P. Cekerevac, L. Prigoda, and F. Al-Naima. Security risks from the modern man-in-the-middle attacks. MEST J., 13(1):34–51, Jan. 2025.
[20] Y. Erinle, Y. Kethepalli, Y. Feng, and J. Xu. SoK: Design, vulnerabilities, and security measures of cryptocurrency wallets. Comput. Netw., 273(111691):111691, Dec. 2025.
[21] A. Garba, Z. Guan, A. Li, and Z. Chen. Analysis of man-in-the-middle of attack on bitcoin address. In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, pages 388–395. SCITEPRESS – Science and Technology Publications, 2018.
[22] N. Ivanov and Q. Yan. Ethclipper: A clipboard meddling attack on hardware wallets with address verification evasion. In 2021 IEEE Conference on Communications and Network Security (CNS), pages 191–199, 2021.
[23] N. Johnson. Erc-137: Ethereum domain name service - specification. Ethereum Improvement Proposals, https://eips.ethereum.org/EIPS/eip-137, April 2016. accessed: 2025-11-22.

[24] S. Tiwari. An introduction to qr code technology. In 2016 International Conference on Information Technology (ICIT), pages 39–44, 2016.
[25] C. S. Wright. Bitcoin: A peer-to-peer electronic cash system. SSRN Electronic Journal, 2008.
[26] P. Xia, H. Wang, Z. Yu, X. Liu, X. Luo, and G. Xu. Ethereum name service: the good, the bad, and the ugly, 2021.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
A Secure Cold Wallet System Against Unauthorized Transaction Issuance	International Conference on Intelligent Information Technology (ICIIT 2026)	2026 年 3 月
コールドウォレット向けアドレス改ざん防止手法	暗号と情報セキュリティシンポジウム (SCIS 2026)	2026 年 1 月
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	コンピュータセキュリティシンポジウム (CSS 2025)	2025 年 10 月