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

小林 紘也[1,a)]　面 和成[1,b)]

概要：我々はこれまで SCIS2024 において TrustZone を用いた安全に送金可能なコールドウォレットシステムの提案を行い，第 107 回 CSEC において MitMo 攻撃対策として Trusted UI を用いた信頼できる情報検証手法について議論してきた．しかし，SCIS2024 では TrustZone での実装評価が残されており，第 107 回 CSEC ではマイナンバーカード認証が未実装という課題が残されていた．本研究は，これらの過去研究の集大成として，TrustZone と Trusted UI を統合した完全なコールドウォレットシステムを提案・実装・評価する．本システムは，トランザクションの内容に署名を付けて TrustZone から直接的に画面表示を行い，Trusted UI のもとで信頼できる情報の確認を実現することで，マルウェアの有無に関係なく，ユーザが意図したトランザクションを発行することを可能にする．さらに，従来未実装であったマイナンバーカードによる eID 認証機能を組み込み，TrustZone の実装を Raspberry Pi を用いて行い，提案コールドウォレットにおけるトランザクションの署名生成処理時間の計測評価を行った．

キーワード：コールドウォレット，TrustZone，eID カード，Man-in-the-Mobile 攻撃，暗号資産

A Secure Cold Wallet System Against Unauthorized Transaction Issuance

Hiroya Kobayashi[1,a)]　Kazumasa Omote[1,b)]

Abstract: We have previously proposed a secure cold wallet system using TrustZone for safe fund transfers at SCIS2024, and discussed reliable information verification methods using Trusted UI as a countermeasure against MitMo attacks at the 107th CSEC. However, implementation evaluation with TrustZone remained incomplete in SCIS2024, and My Number card authentication was not implemented in the 107th CSEC, leaving these issues unresolved. This study serves as a culmination of our previous research, proposing, implementing, and evaluating a complete cold wallet system that integrates TrustZone and Trusted UI. Our system attaches signatures to transaction contents and displays them directly from TrustZone, enabling reliable information verification under Trusted UI, thus allowing users to issue their intended transactions regardless of the presence of malware. Furthermore, we incorporated the previously unimplemented eID authentication function using My Number cards, implemented TrustZone on Raspberry Pi, and conducted measurement evaluations of transaction signature generation processing time in the proposed cold wallet system.

Keywords: Cold wallet, TrustZone, eID card, Man-in-the-Mobile attack, Cryptocurrency

1. はじめに

暗号資産の普及に伴い，多くのユーザが暗号資産を保管・管理するためにウォレットを利用している．その一つであるコールドウォレットは，オフラインで秘密鍵を保持

[1] 筑波大学, 〒 305-8573 茨城県つくば市天王台 1-1-1, University of Tsukuba,, 1-1-1 Tennodai, Tsukuba, Ibaraki 305-8573 Japan
[a)] s2420532@u.tsukuba.ac.jp
[b)] omote@risk.tsukuba.ac.jp

し，ユーザの資産をセキュアに管理することができる．一般的に，オンラインで暗号資産の保管や取引などを行うホットウォレットに比べて，より安全であると考えられている [1][2].

一般的なコールドウォレットは，オフラインで秘密鍵を管理するために物理的なデバイス（ハードウェアウォレット）を使用することが多いが，取引の際はインターネットに接続された PC 等のデバイスを用いる．しかし，インターネットに接続されたデバイスにマルウェアが感染してしまうと，マルウェアが生成した不正なトランザクションに署名がなされてしまい，資産を奪われるというリスクが考えられる．

我々は，SCIS2024 において暗号資産取引における不正なトランザクション発行を防ぐコールドウォレットシステム [3] を提案し，TrustZone を用いた秘密鍵の生成・管理手法を示した．その後，第 107 回 CSEC では，SCIS2024 の提案を改良し，リッチ OS が出力する情報は信頼できないという課題を解決したシステム [4] を提案した．第 107 回 CSEC では，TrustZone とマイナンバーカードを連携させることで，ユーザ認証後にセキュアにトランザクションの署名生成を行い，さらに，TrustZone から画面表示を行う Trusted UI のもとでユーザがトランザクションの内容を確認及び検証を行うことで，マルウェアの有無に関係なく，ユーザが意図したトランザクションを発行することを可能にする手法を示した．

本稿では，これまでの研究成果をもとに，提案手法のさらなる改良と詳細な実装評価を行う．特に，第 107 回 CSEC では課題として残されていたマイナンバーカード認証の実装を完了し，TrustZone を活用したコールドウォレットシステムの処理性能の評価と実環境での動作検証を実施する．提案手法を用いることで，マルウェアによるトランザクションの改ざんを防ぎ，安全に送金を行うことができる．

以下では，背景と関連研究を紹介し，脅威モデルを概説した後，提案手法の詳細，実装および評価結果を示す．最後に，本研究の意義を議論し，今後の研究課題について述べる．

2. 準備

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を用いた電子的な貨幣であり，トランザクション（取引データ）は秘密鍵を持つユーザのみが発行できる [5]．コールドウォレットは秘密鍵をオフライン環境で保管するウォレットであり，オンラインのホットウォレットと比較して高い安全性を提供する．本研究では，このコールドウォレットにおける秘密鍵管理の安全性向上を目的とする．

2.2 eID カード

eID カードは政府が発行する電子身分証明書であり，IC チップに記録された PKI 電子署名機能を備える [6]．ユーザ認証および署名用の電子証明書を含み，暗証番号と PIN による認証が必要である．証明書の秘密鍵を用いた電子署名により，文書の真正性と整合性を維持できる [7].

2.3 TEE と TrustZone

TEE（Trusted Execution Environment）は，メインプロセッサ内に存在する安全な領域であり，メインのオペレーティングシステム（REE：Rich Execution Environment）から分離されている．ARM TrustZone は，ARM ベースのプロセッサにおける TEE の基盤となるハードウェアセキュリティ拡張である．TrustZone は，システムのハードウェアおよびソフトウェア資源を「セキュアワールド」と「ノーマルワールド」に分割する．

一般的な OS（Linux，Android など）やアプリケーションはノーマルワールドで動作し，鍵管理などのセキュリティ関連処理はセキュアワールドで実行される．ノーマルワールドで動作する OS がマルウェアに感染していたとしても，セキュアワールドで動作するアプリケーションの機密性や整合性，およびセキュアワールドの処理には影響を与えない [8], [9], [10], [11].

TrustZone は，CPU 内に安全な実行環境を構築する能力を持ち，高いセキュリティが求められる金融取引や機密データ処理などのアプリケーションにとって重要である．セキュリティクリティカルな処理をメイン OS から分離することで，メイン OS が侵害されても安全な処理が維持される．この環境の分離は，機密情報の整合性と機密性を維持するために不可欠である．

2.3.1 Trusted UI

Trusted UI [12] は，TEE が直接ディスプレイや入力デバイスを制御することで，マルウェアによる画面改ざんや入力盗聴を防ぐ仕組みである．本研究では，この機能を用いてトランザクション内容の安全な検証を実現する．

2.4 Man-in-the-Mobile（MitMo）

Man-in-the-Mobile（MitMo）攻撃は，Man-in-the-Middle（MitM）攻撃の一種である．これらの攻撃は，DNS スプーフィング，セッションハイジャック，悪意のあるアプリなどの技術に分類され，近年ではモバイルプラットフォームへの移行が進んでいる [13].

インターネットに接続されたデバイスがマルウェアに感染すると，Man-in-the-Mobile（MitMo）攻撃が可能となる．例えば，多くのユーザが利用する Android OS では，任意のアプリケーションが実行可能であり，マルウェアの 80%以上が有名アプリを偽装したリパッケージ攻撃によってデバイスに侵入している [14].

このような攻撃によって導入されたマルウェアは，ルート権限を取得し，ユーザが作成したトランザクションデータを改ざんしたり，TrustZone に不正な署名生成を要求したりする可能性がある．

3. 関連研究

本節では，ハードウェアウォレットに関連するいくつかの研究を紹介し，それらとの違いについて説明する．

3.1 TrustZone を用いた研究

Miraje らの研究 [15] では，TrustZone を用いた Bitcoin ウォレットの実装が行われた．この研究では，TrustZone による実行領域の分離により，秘密鍵の漏洩を防止できることが示された．また，辞書攻撃やサイドチャネル攻撃など，さまざまな攻撃に対して高い耐性を持つウォレットの実装が可能であることも示された．しかし，この手法はホットウォレットとして機能し，すべてのブロックデータを保持する必要があるため，スマートフォンやタブレット，組み込み機器などの広く利用されているハードウェアデバイスには適していない．

Dai らの研究 [16] では，TrustZone を用いたウォレットを提案し，Raspberry Pi 3 Model B を用いて実装・評価を行った．この研究では，TrustZone によって分離された安全な環境で署名や検証などのウォレット処理を行うことで，安全な送金が可能であることが示された．さらに，Miraje らの研究 [15] で課題となっていた全ブロックデータの保持問題を解決し，全ブロックデータの約 1/1000 のデータ量でウォレットを実装できることを示した．

このウォレットは，トランザクションの検証時にブロックチェーンネットワーク上のフルノードからブロックヘッダーのみを要求し，それを用いてトランザクションを検証する．この際，ブロックチェーンネットワークに接続するためにオンライン環境が必要となる．そのため，Dai らの研究 [16] で使用されたデバイスがマルウェアに感染している場合，信頼できない情報を用いてトランザクションの検証が行われ，ユーザが意図しないトランザクションを発行する可能性がある．

Khan らの研究 [17] では，Android アプリとしてホットウォレットとコールドウォレットの 2 種類を開発し，QR コードの読み取りによるアプリ間の連携を実装した．この研究では，QR コードによる署名生成とユーザ認証を行うことで，より安全なトランザクションを実現している．

コールドウォレットアプリはオフラインで動作し，ホットウォレットアプリはオンラインで動作する．しかし，Android デバイスがマルウェアに感染した場合，ホットウォレットが危険にさらされ，QR コードの読み取りによる秘密鍵の取得処理がマルウェアに監視され，秘密鍵が漏洩する可能性がある．

大塚らの研究 [18] では，Android 端末を用いた送金取引において，不正送金を防ぐための SIM カードを用いた対策技術について複数の構成法を検討し，最も安全な取引認証の構成として TEE+SIM を紹介している．しかし，Android 端末における TEE からの画面出力に対応しているスクリーンの普及率の低さから，実用的ではないとしている．

3.2 関連研究のまとめと本研究との違い

3.1 節で紹介した関連研究では，それぞれの手法によりユーザ認証やトランザクション署名生成を安全に行うことが可能である．しかし，MitMo 攻撃に対する十分な耐性は備えていない．

本研究では，関連研究で課題となっていた MitMo 攻撃に対して十分な耐性を持つコールドウォレットを提案する．具体的には，eID カードによる厳格な認証，TrustZone による安全なトランザクション署名生成，TEE を介した画面表示によるトランザクションの検証を行うことで，マルウェアによるトランザクション改ざんを防止し，安全な送金を実現する．

4. 脅威モデル

本研究では，ユーザのデバイス（PC またはスマートフォン）から開始される暗号資産トランザクションの整合性を脅かす脅威に焦点を当てる．主な脅威は，Man-in-the-Mobile（MitMo）攻撃である．

コールドウォレットの文脈では，一般的なシナリオとして，ホストコンピュータ上のマルウェアが，ユーザが承認した後にトランザクションの詳細（送金先アドレスや金額など）を改ざんし，署名前に不正な内容に変更するというものがある．この脆弱性は，商用ハードウェアウォレットにおいても確認されており [19]，PC 上では正しいアドレスが表示されているにもかかわらず，ウォレットには不正なアドレスが送られ，署名されてしまう可能性がある．

ハードウェアウォレットを使用する際の脅威モデルでは，MitMo 攻撃に関連する以下の脅威が考慮される：

- **マルウェアによるトランザクション改ざん：** ハードウェアウォレットに接続された PC がマルウェアに感染している場合，ユーザが生成したトランザクションデータがマルウェアによって改ざんされる可能性がある．これにより，ユーザが意図しないトランザクションを承認してしまう危険性がある．
- **不正な署名生成要求：** PC がマルウェアに感染している場合，マルウェアが TrustZone に対して新たなトランザクションの署名を不正に要求する可能性がある．このような不正な要求により，攻撃者のアドレスに資産が送金される有効なトランザクションが生成される可能性がある．

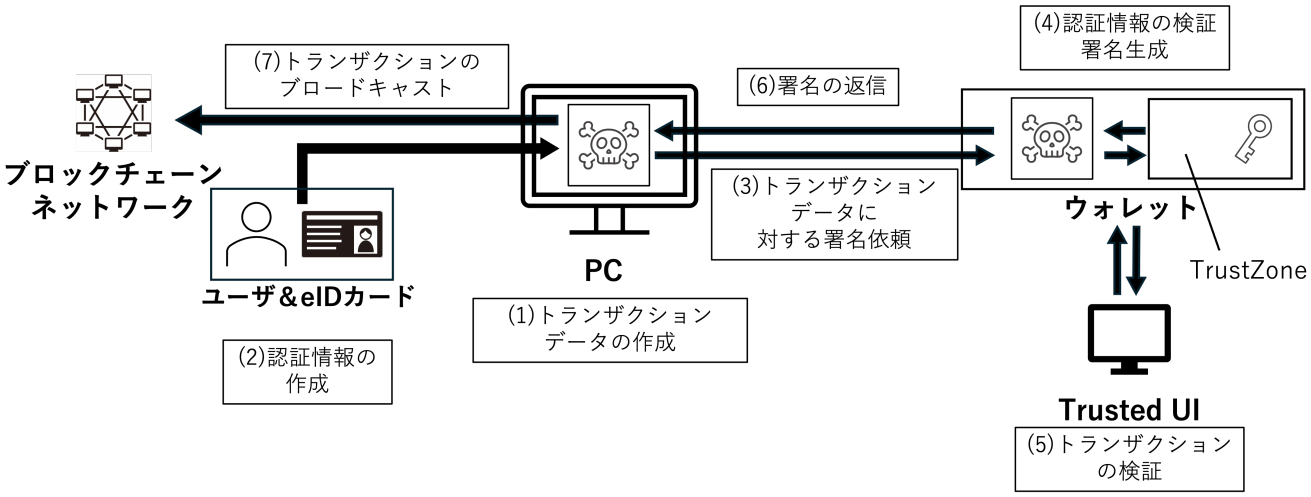

図 1　提案手法の概要

- **不正な画面表示：** 攻撃者が正規のトランザクションと不正なトランザクションをウォレットに送信し，画面には正規のトランザクションを表示しながら，ネットワークには不正なトランザクションを送信する可能性がある．このような欺瞞により，ユーザは正しいトランザクションを承認したと誤認し，不正なトランザクションを承認してしまう．

これらの脅威は，ユーザが意図しないトランザクションを発行する結果を招き，資産の盗難につながる可能性がある．ハードウェアウォレットに接続された PC 上のマルウェアの存在は，トランザクションデータの改ざん，署名の不正生成，欺瞞的な画面表示など，重大なリスクをもたらす．これらの脅威に対処することは，暗号資産トランザクションの安全性と整合性を確保する上で極めて重要である．

5. 提案手法

5.1 概要

暗号資産取引における不正なトランザクションの発行を防ぎ，安全に送金を行うことができるコールドウォレットシステムを提案する．提案手法の全体図を図 1 に示す．まず，(1)PC でトランザクションデータを作成し，(2)eID カードで TrustZone からのチャレンジに対して，レスポンスとなる認証情報を作成する．その後，(3) 認証情報と共にウォレットに対してトランザクションデータに対する署名生成の依頼をし，(4) ウォレットの TrustZone 内で認証情報を検証し，認証が成功した後にトランザクションデータに対する署名を生成する．その後，(5) 署名済みトランザクションを検証する．(6) 検証が問題なければ，署名済みトランザクションを PC に返信し，(7) トランザクションをブロックチェーンネットワークに対してブロードキャストし，送金取引を完了させる．

5.2 構成要素

- PC：インターネットに接続され，ブロックチェーンネットワークにアクセスできる．USB を通じてウォレットと接続し，カードリーダを通じて eID カードと接続する．トランザクションを作成し，ウォレットに対してその署名生成の依頼を行う．ウォレットからトランザクションの署名が返ってきたら，その検証を行い，整合性を確認する．また，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できる．
- ウォレット：ハードウェアウォレットとして機能し，秘密鍵を TrustZone 内に保管する．秘密鍵の生成や eID カードによる認証の検証，トランザクションの署名を生成するなどの処理を全て TrustZone 内で実行する．
- eID カード：ウォレットを所有するユーザが本人であることを証明するために用いる．ウォレットの TrustZone からのチャレンジに対して，eID カードを用いて署名（レスポンス）を返し，それを TrustZone で検証することで安全性の高いユーザ認証を行う．
- Trusted UI：TrustZone から画面を出力するためのデバイスで，ユーザがトランザクションの内容を確認及び検証を行うために用いる．例として，ディスプレイが挙げられる．

5.3 記法

本論文では，表 1 に示す記法を用いる．

5.4 送金の流れ

提案手法の流れを図 2 に示す．

5.4.1 pk_m の登録とウォレットの生成

トランザクションに対する署名を行う際に，eID カードを用いた認証を行うため，予め pk_m を TrustZone に登録しておく．また，ハードウェアウォレット内で sk_w，pk_w，

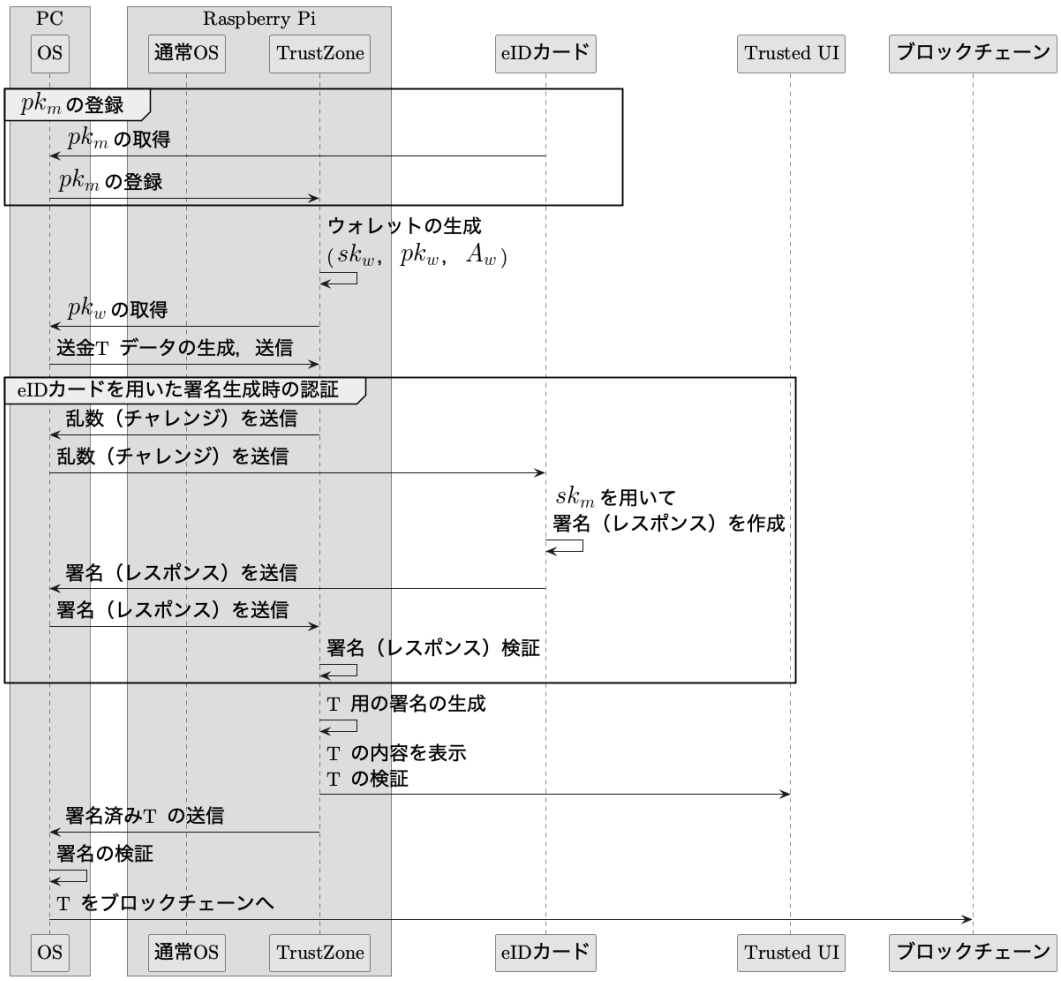

図 2 提案手法の流れ

表 1 表記法

記号	定義
pk_m	eID カードの公開鍵
sk_m	eID カードの秘密鍵
pk_w	ウォレットの公開鍵
sk_w	ウォレットの秘密鍵
A_w	ウォレットのアドレス
Tx	トランザクション

A_w を生成し，pk_w と A_w を PC に送信して利用可能な状態にする．pk_w はトランザクションの検証の際に，A_w はトランザクションの作成の際に使用する．

5.4.2 トランザクションデータの作成・送信

PC にて，署名されていない生のトランザクションデータを作成する．このトランザクションデータには，以下の情報が含まれている．

- from：送金元のアドレス
- to：送金先のアドレス
- amount：送金額
- gasPrice：ガス代
- gas：ガスの上限値
- nonce：ナンス

この内の from，to，amount をユーザが指定し，gasPrice，gas は固定値として設定する．また，ナンスは A_w から算出する．トランザクションデータを作成した後，ウォレットに対してトランザクションデータを送信する．

5.4.3 eID カードを用いた署名生成時の認証

ウォレットがトランザクションデータを受け取った後，トランザクションデータに対する署名の生成処理に入る．安全な署名を行うために，eID カードを用いた認証を行う．ウォレットは eID カードに対するチャレンジを生成し，eID カードはそのチャレンジに対して署名を行い，その署名をレスポンスとしてウォレットに返す．その際 IC カードリーダを PC に接続する関係上，PC を介してチャレンジとレスポンスのやり取りを行う．ウォレットは eID カードから受け取ったレスポンスを検証し，問題がなければトランザクションデータに署名を行う．

5.4.4 トランザクションの検証

トランザクションの検証は二種類ある．一つは，トランザクションデータがユーザの意図したものになっているかどうかの検証である．これは TrustZone を介した Trusted UI による安全な検証を行う．もう一つは pk_w を用いたト

ランザクションの署名の検証である．両方の検証が成功した場合，ユーザが内容を確認して問題なければトランザクションをブロックチェーンネットワークに対してブロードキャストし，送金取引を完了させる．

6. 実装評価

提案手法の実現可能性を示すために，図 1 に示したシステムを Raspberry Pi 3 Model B+，JavaCard，およびマイナンバーカードを用いて実装した．この実装は，提案手法の汎用性と実用性を多角的に示すことを目的としている．

汎用 JavaCard を用いた実装は，特定の国の制度に依存せず，標準的なスマートカード技術プラットフォーム上で広く応用可能であることを示す．一方，マイナンバーカードを用いた実装は，日本国内で最も広く利用されているスマートカードであり，追加のハードウェアを必要とせず多くのユーザが利用可能であることから，社会インフラとしての高い実用性を示す．

この実装では，トランザクションの署名・検証だけでなく，eID カードによるユーザ認証も含まれており，提案システムの全体的な有効性を評価可能である．

6.1 環境

実験環境を図 3 に示す．PC には MacBook Pro を使用し，コールドウォレットは Raspberry Pi 3 Model B+で実装した．Raspberry Pi と PC は USB で接続され，通信はオフライン環境で行った．

ブロックチェーンには Ethereum のテストネット「Sepolia」を使用した．コールドウォレットの機能は Python で実装し，送金先アドレスは Ethereum ソフトウェアウォレット「Metamask」で作成した．

eID カードによるユーザ認証では，コールドウォレットシステムにおける高度なセキュリティ要件と通信の安定性を考慮し，ISO/IEC 7816 準拠の接触型 IC カードリーダを主に使用した．評価では，システムの汎用性を示すため JavaCard とマイナンバーカードの両方で実装を行い，さらに比較検証のためマイナンバーカードでは非接触型インターフェースでも評価を実施した．

- **JavaCard ベースの eID 実装：** JavaCard 3.0.5 スマートカードを使用．コールドウォレットにおける高度なセキュリティ要件を満たすため，データ送受信の安定性が確保された接触型インターフェースを選択し，ISO/IEC 7816 準拠の接触型 IC カードリーダを用いて通信を行った．
- **マイナンバーカード実装：** 日本のマイナンバーカードを用いて認証を実装．主な評価では ISO/IEC 7816 準拠の接触型 IC カードリーダを使用し，比較のために非接触型リーダも使用した．

図 3 実験環境

6.2 検証フロー

6.2.1 ウォレット生成

Raspberry Pi 上で sk_w，pk_w，A_w を生成し，pk_w と A_w を PC に送信する．sk_w はウォレットの TrustZone 内に保存され，オンライン環境とは直接接続されていない．

6.2.2 トランザクション作成

PC 上で未署名の生トランザクションデータを作成する．5.4.2 節で述べたように，送信者アドレス，受信者アドレス，送金額を指定してトランザクションデータを作成する．ここでは，受信者アドレスに Metamask で作成したアドレスを使用し，送金額は 0.1 SepoliaETH とした．

6.2.3 eID カードによる認証

トランザクション署名前にユーザ認証を行うため，eID カードを用いたチャレンジ・レスポンス方式を実装した．ウォレットは TrustZone 内でチャレンジを生成し，PC を経由して IC カードリーダを通じて eID カードに送信する．JavaCard ベースの eID とマイナンバーカードはそれぞれチャレンジに署名し，レスポンスを返した．ウォレットは事前登録された公開鍵 pk_m を用いてレスポンスを検証し，成功すれば署名処理に進む．

6.2.4 トランザクション署名生成

PC で作成されたトランザクションデータは Raspberry Pi に送信され，ECDSA 署名が生成される．トランザクション内容の検証は，TrustZone を介した画面表示によって行われる．

6.2.5 トランザクション署名検証

署名済みトランザクションは，pk_w を用いて ECDSA 署名の検証が行われる．問題がなければ，トランザクションはブロックチェーンネットワークに送信される．

6.3 実行時間の測定

トランザクション署名生成，検証，および eID カードによる認証に要した時間を 10 回測定し，平均時間を算出した．Python の `time` モジュールを用いて測定を行った．

認証では，チャレンジが eID カードに送信されてからレスポンスが返され，ウォレットで検証されるまでの時間を測定した．これは，各インターフェースを通じた APDU 通信とカード上での署名処理を含む．

結果は表 2 および表 3 に示す．

表 2 署名生成・検証に要した時間

	署名生成	署名検証
通常 OS	10.23 ms	20.54 ms
TrustZone	32.63 ms	55.34 ms

表 3 eID カード認証に要した時間

カードとインターフェース	時間
JavaCard（接触型）	921.84 ms
マイナンバーカード（接触型）	1129.95 ms
マイナンバーカード（非接触型）	401.72 ms

TrustZone や eID カードの使用によって追加のオーバーヘッドはあるものの，測定された時間は実用上十分に高速である．TrustZone での署名生成は 32.63 ms，検証は 55.34 ms であった．認証時間は，JavaCard（接触型）が 921.84ms，マイナンバーカード（接触型）が 1129.95ms，マイナンバーカード（非接触型）が 401.72ms であった．

7. 考察

7.1 マルウェアによるトランザクション改ざん

PC がマルウェアに感染している場合，トランザクションデータが改ざんされる可能性がある．ユーザがウォレットに送信したトランザクションデータが，マルウェアによって変更され，不正なデータに署名される可能性がある．このような事態を防ぐためには，トランザクションデータがユーザの意図と一致しているかを検証する必要がある．

提案手法では，トランザクションのブロードキャスト前に内容を確認することで，ウォレットが不正なデータに署名していたとしても，送金を防ぐことが可能である．この検証処理は，マルウェアによる改ざんを防ぐ上で重要である．ただし，これはユーザが Trusted UI を通じてトランザクション内容を確認することを前提としている．ユーザが確認を怠った場合，不正なトランザクションが発行されるリスクが残るため，課題が残る．

7.2 不正な署名生成

トランザクションに署名する際，適切なユーザ認証が行われない場合，不正なトランザクションが発行される可能性がある．マルウェアがウォレットにアクセスできる場合，ユーザの意図に反する新たなトランザクションデータを作成し，ウォレットに送信することが可能となる．このような状況では，攻撃者が任意のトランザクションを発行できてしまうため，ユーザ認証は不可欠である．

提案手法では，eID カードによる厳格な認証を行うことで，不正な署名要求を防止している．eID カードは強力な認証手段を提供し，正当なユーザのみがトランザクションを承認できるようにする．仮に eID カードが紛失し，悪意のある第三者が署名を試みた場合でも，PIN の入力が求められ，3 回（認証）または 5 回（署名）間違えるとカードがロックされる．このロック機構により，カードが盗まれても不正利用を防ぐことができる．

7.3 不正な画面表示

攻撃者が正規のトランザクションと不正なトランザクションをウォレットに送信し，画面には正規のトランザクションを表示しながら，ネットワークには不正なトランザクションを送信する可能性がある．このような欺瞞により，ユーザは正しいトランザクションを承認したと誤認し，不正なトランザクションを承認してしまう．

提案手法では，Trusted UI を用いて TEE 経由でトランザクションを検証することで，不正な画面表示によるトランザクション送信を防止している．Trusted UI は，ユーザに表示される情報が正確であり，マルウェアによって改ざんされていないことを保証する．この安全な表示機構は，ユーザの信頼を維持し，トランザクション処理の整合性を確保する上で重要である．

7.4 マイナンバーカードと JavaCard の比較

本研究では，汎用 JavaCard とマイナンバーカードの両方を用いてシステムを実装・評価した．両カードについて接触型インターフェースで認証時間を測定し，マイナンバーカードについては非接触型インターフェースでも比較を行った．

表 3 に示す性能評価から，以下の 3 点が明らかとなった．

1 つ目は，接触型インターフェースを用いた場合，JavaCard は 921.84ms，マイナンバーカードは 1129.95ms であった．この差は，IC チップのハードウェア性能によるものである可能性が高い．高性能な JavaCard は暗号処理専用のコプロセッサを搭載している場合があり，処理が高速化される．一方，マイナンバーカードは公共インフラとしての供給安定性やコストを重視しているため，商用カードとは異なる仕様である可能性がある．

2 つ目は，マイナンバーカードにおいて，非接触型インターフェース（401.72ms）が接触型（1129.95ms）よりも大幅に高速であった．この差は，通信プロトコル（非接触：ISO/IEC 14443，接触：ISO/IEC 7816 T=0/T=1）やカードリーダ・カード OS の処理効率に起因する．インターフェースの選択が性能に大きく影響することが示された．

3 つ目は，最も遅いケースでも 1 秒強であり，ウォレットシステムにおけるユーザ認証としては十分に実用的な範囲であることが確認された．これにより，以下の 2 つの運用モードが可能であることが示された：

- **マイナンバーカードを用いたモード：** 多くのユーザが既に保有している公的 ID カードを活用でき，追加のハードウェアが不要であり，接触・非接触の両インターフェースに対応可能．
- **高性能 JavaCard を用いたモード：** マイナンバーカー

ドよりも若干高速な認証が可能である．なお，JavaCard では接触型インターフェースのみを使用した．これは，コールドウォレットシステムにおける高度なセキュリティ要件と通信の安定性を重視し，より確実な認証環境を提供するためである．

このように，本システムは多様な認証メディアとインターフェースに対応しており，ユーザ環境やハードウェアの可用性に応じて柔軟に運用可能である．この柔軟性は，MitMo 攻撃に対するセキュリティを幅広い環境で確保する上で大きな利点となる．

8. 結論

本研究では，暗号資産取引における不正なトランザクション発行を防止する新たなコールドウォレットシステムを提案・実装・評価した．Raspberry Pi を用いてハードウェアウォレットを実装し，トランザクションデータおよび署名の検証を通じて，マルウェアによる不正なトランザクション発行を防ぎ，安全な送金が可能であることを示した．

さらに，トランザクション署名生成，検証，および eID カードによるユーザ認証に要する時間を測定し，本システムが実用的な性能を有していることを確認した．

今後の課題としては，ユーザがトランザクション内容を確認しない場合への対策が挙げられる．

謝辞 本研究は、公益財団法人電気通信普及財団の研究調査助成および JSPS 科研費 JP23K24844 の助成を受けたものである。

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] 小林紘也，面和成：安全に送金可能なコールドウォレットの構築に向けて，*Symposium on Cryptography and Information Security (SCIS2024)*, 3B4-2, 長崎県長崎市 (2024).

[4] 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, pp. 1–7 (2024).

[5] 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).

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

[7] 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).

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

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

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

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

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

[13] 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).

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

[15] 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).

[16] 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).

[17] 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).

[18] 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).

[19] Chainalysis Team: Collaboration in the Wake of Record-Breaking Bybit Theft: Following the $1.5 Billion Trail (2025).