SNS プラットフォームにおける暗号資産詐欺の実態調査

伊藤 大貴[1,a)]　渡邉 卓弥[1]　高田 雄太[1]　熊谷 裕志[1]　神薗 雅紀[1]

概要：暗号資産のエアドロップでは，保有者を増やすための紹介リンク共有や認知度を上げるためのハッシュタグ付き投稿が参加条件として設定されることが多く，SNS プラットフォームが重要な役割を担っている．暗号資産を狙った詐欺でも同様に，攻撃者はエアドロップを騙る投稿や返信を通じて詐欺サイトの URL を拡散している．本研究では，SNS 上のエアドロップを騙る詐欺の実態を調査する．具体的には，X 上で観測されたエアドロップ関連投稿 455,842 件を収集し，アカウント，投稿内容，タイムライン，スマートコントラクト（SC）アドレスの観点から特徴と傾向を分析する．その結果，既存アカウントを用いた詐欺投稿や，短命なインフラを用いた詐欺サイトの構築により，現行の対策が回避されていることを示す．加えて，本調査結果から複数の詐欺サイトにおいて同一の SC アドレスが利用されていることを示す．この特徴を踏まえて，SC アドレスを用いることによる詐欺サイトの検知率向上や，新たな詐欺サイトの収集可能性ついて議論する．

キーワード：暗号資産詐欺, SNS, ブロックチェーン, フィッシング

Investigating Cryptocurrency Scams on Social Networking Platforms

Daiki Ito[1,a)]　Takuya Watanabe[1]　Yuta Takata[1]　Hiroshi Kumagai[1]　Masaki Kamizono[1]

Abstract: In cryptocurrency airdrops, participation often requires actions such as sharing referral links to increase the number of holders or posting with specific hashtags to enhance visibility, making social networking platforms play a crucial role. Similarly, in cryptocurrency-related scams, attackers disseminate fraudulent website URLs through posts and replies that impersonate airdrop campaigns. This study investigates the realities of scams on social networking services that impersonate cryptocurrency airdrops. Specifically, we collected 455,842 airdrop-related posts observed on X and analyzed their characteristics and trends from the perspectives of accounts, post content, timelines, and smart contract (SC) addresses. The results reveal that scammers evade existing countermeasures by exploiting pre-existing accounts for fraudulent posts and by constructing scam websites using short-lived infrastructure. Furthermore, our analysis shows that identical SC addresses are used across multiple scam websites. Based on this finding, we discuss the potential for improving scam site detection rates and enabling the discovery of new scam sites through the use of SC addresses.

Keywords: Cryptocurrency Scam, SNS, Blockchain, Phishing

1. はじめに

ブロックチェーン技術の進展に伴い，暗号資産を中核とする分散型エコシステムが急速に拡大している．暗号資産による資金調達手法，分散型金融（DeFi），NFT をはじめとする新たな応用は，個人投資家から開発者・企業に至るまで広範な関与を生み出しており，経済的・社会的に注目を集めている．一方で，このような暗号資産市場の急速な発展の背後では，資産の盗難や詐欺といった問題も深刻化しており，ユーザを脅かす重大なリスクとして顕在化している．例えば，「ウォレットドレイナー」と呼ばれる暗号資産窃取ツールを悪用した攻撃では，2024 年に総額約 4 億 9,400 万ドルに上る被害が報告されている [1]．過去の調査

[1] デロイト トーマツ サイバー合同会社,
Deloitte Tohmatsu Cyber LLC
[a)] ito.daiki@tohmatsu.co.jp

研究では，高利回りを謳う投資詐欺や偽造された ERC-20 トークンの販売等により，総額 19 億ドルを超える暗号資産が窃取されていたことが明らかとなっている [2].

これらの暗号資産詐欺の特徴として, SNS プラットフォームを介したソーシャルエンジニアリングが挙げられる．攻撃者は，SNS 投稿や広告を通じて詐欺情報を広範囲に拡散し，ユーザの不注意や知識不足につけ込むことで，被害の拡大を図っている．特に X（旧 Twitter）は，暗号資産関連の情報流通において中心的な役割を果たしており，エアドロップやトークン配布キャンペーンなどの広告情報は，同プラットフォーム上で頻繁に拡散されている．エアドロップでは，公式アカウントのフォロー，特定投稿のリツイート，ハッシュタグを付した投稿，あるいは紹介リンクの共有などが参加要件や追加報酬条件として設定される場合があり，その結果，X 上ではエアドロップ関連情報が大量に投稿・共有されている．攻撃者はこの特性を悪用し，正規のキャンペーンに便乗する形で類似の投稿や返信，引用リツイートなどを通じて詐欺的なリンクやアドレスを流布している．このような情報の即時性と拡散力により，X は暗号資産詐欺における効果的な攻撃チャネルとなっている．

本研究は，暗号資産詐欺の手口の一つであるエアドロップを騙る詐欺に着目し，その実態を多面的に明らかにすることを目的とする．具体的には，X 上で観測されたエアドロップ関連投稿 455,842 件を収集し，アカウント，投稿内容，タイムライン，およびスマートコントラクト (SC) アドレスの 4 つの観点から，エアドロップを騙る詐欺の特徴や傾向を分析した．加えて，当該詐欺の流れを「投稿拡散」「誘引」「ウォレット接続・送金」の 3 フェーズに整理し，それぞれにおける既存対策の実効性と限界を評価した．本研究の貢献を以下に示す．

- アカウントの調査の結果，詐欺投稿に用いられたアカウントの 57.5% は 2025 年以前に作成されたものであったが，そのうち 72.8% は凍結されておらず，SNS プラットフォームによる対策を回避していることを明らかにした．
- タイムラインの調査の結果，攻撃者がホスティング業者によるテイクダウンやブロックリストベースの対策を回避するために短期的なインフラ運用を行っていることを明らかにした．具体的には，詐欺投稿の 91.9% がドメイン名の登録から 5 日以内に投稿されていることを確認した．
- SC アドレスの調査の結果，複数の詐欺サイトが RPC（Remote Procedure Call）を介して同一の SC アドレスを参照し，SC の関数を使用する挙動を確認した．
- ブロックリストによる既存対策の限界を評価するとともに，本研究の調査結果を踏まえて，SC アドレスからドメイン名を特定するためのデータ収集方法や，それらデータの活用を想定した詐欺サイトの新たな検出手法の検討と検証を実施した．

2. 関連研究

暗号資産を標的とした詐欺行為の解明および検知を目的とする研究は複数報告されている．集めた資金を持ち逃げするラグプル詐欺を継続的に実行するアドレスの行動パターンの分析手法 [3] や、機械学習を用いて検出する手法 [4] が報告されている．また，証明書透明性ログから取得できる新規発行ドメインを用いて，暗号資産の投資詐欺サイトをリアルタイムに検知する手法も提案されている [5].

SNS を介した暗号資産詐欺に着目した研究も増加している．Liu らは，SNS 上で展開されるギブアウェイ詐欺に注目し，被害者を詐欺に誘導するプロセスおよび被害額を分析している [6]．さらに，Kimber らは，複数の SNS 投稿と Ethereum 上のトランザクションデータを分析し，フィッシング詐欺のライフサイクルを明らかにしている [2].

上述の研究は，詐欺のプロセス解明，被害実態の把握，および検知技術の開発に重点を置いているが，一連の詐欺プロセスにおける対策は十分に議論されていない．本研究では，エアドロップを騙る詐欺の実態を多面的に明らかにするとともに，詐欺のプロセスを 3 フェーズに整理し，各フェーズにおける対策の現状と有効性について分析した．

3. 調査方法

本研究では，X 上のエアドロップを装った詐欺に着目し，その実態と対策の現状を調査する．本調査は投稿の収集，分類，分析の 3 段階で構成される．投稿の収集では，X 上のエアドロップ関連投稿を取得するための検索条件を策定し，それに基づいて投稿を収集する．投稿の分類では，収集した投稿を Benign，Malicious，Suspicious の 3 種類に分類する．投稿の分析では，Malicious に分類された投稿を対象に特徴や傾向を分析する．加えて，投稿に含まれる URL に実際にアクセスし，一連の詐欺プロセスにおける対策の有無とその有効性を調査する．

3.1 投稿の収集

エアドロップを装った詐欺の傾向を分析するために，X が提供する API を用いて，エアドロップに関連する投稿を収集した．X API には取得件数に上限があり，すべての関連投稿を収集することは困難であるため，関連性の高い投稿を取得するための検索条件を，暗号資産ユーザの SNS 上での慣習や利用実態に基づいて，以下のように構築した．

3.1.1 キャッシュタグの検索

X では，`$BTC` や `$ETH` のように，ティッカーシンボルの先頭にドル記号（$）を付したキャッシュタグ (CT) によって，特定の CT を含む投稿を検索できる機能が提供されている [7]．本研究では，ユーザの関心を集めやすいプロジェクトのティッカーシンボルは，詐欺投稿においても

悪用されやすいと仮定し，以下の 3 つの観点から検索条件に含める CT を選定した．

時価総額上位のプロジェクトティッカーシンボル．一般ユーザに広く認知されているプロジェクトは，その知名度の高さゆえに関心を集めやすく，詐欺投稿の対象としても悪用されやすいと考えた．そのため，暗号資産の単価や時価総額，取引量等の情報を提供するプラットフォームである CoinMarketCap [8] に基づき，時価総額上位の暗号資産プロジェクトを特定した．本研究では，同サービスにおける「時価総額」ランキングから上位 5 銘柄のティッカーシンボルを取得した．

時価総額上位のミームコインティッカーシンボル．ミームコインは，SNS 上での話題性によって価格が急騰落する特徴を持ち，ユーザの関心を集めやすく，詐欺投稿にも狙われやすいと考えた．本研究では，CoinMarketCap の「Memes」カテゴリに基づき，ミームコインに分類される時価総額上位 5 銘柄のティッカーシンボルを取得した．

エアドロップ開催中のプロジェクトティッカーシンボル．エアドロップが開催されているプロジェクトは，正規のキャンペーンを装った詐欺投稿の対象として特に悪用されやすいと考えた．本研究では，エアドロップの開催情報を集約するプラットフォームである CryptoRank [9] を利用し，開催日が新しい順に 5 件のプロジェクトを抽出した．

3.1.2 その他の検索条件

エアドロップとは無関係な投稿を除外し，より詐欺に関連性の高い投稿を取得するために，CT に加えて以下の条件を検索対象として設定した．

キーワード．エアドロップに関連する投稿を効果的に抽出するため，「airdrop」または「claim」の文字列を本文に含む投稿を対象とした．特に「claim」は，ユーザがエアドロップによって配布された報酬を受け取る操作を指す用語として広く使用されており，詐欺投稿においても頻出すると考えた．

URL リンクの有無．攻撃者はユーザを詐欺サイトへ誘導する手段として，投稿本文に URL リンクを含めるため，本文中に URL を含む投稿のみを検索対象とした．

リツイートの除外．同一内容の拡散に該当するリツイート投稿を除外することで，より多様な投稿を優先的に収集できるよう条件を設定した．

3.1.3 収集データ

X API を用いて収集できるデータには，投稿に紐づく情報とアカウントに紐づく情報が含まれる．以下にそれぞれの情報に含まれる項目を示す．

投稿に紐づく情報．投稿に紐づく情報には，投稿日時，投稿の本文，投稿主アカウントの識別子，キャッシュタグ，ハッシュタグ，投稿に含まれる URL，リツイート数，リプライ数，いいね数，インプレッション数等が含まれる．

アカウントに紐づく情報．アカウントの識別子，アカウント名，アカウント作成日，フォロワー数，フォロー数，ツイート数等が含まれる．

3.2 投稿の分類

前節で収集した投稿を，投稿内に含まれる URL の属性に基づき，*Malicious*（悪性），*Benign*（良性），*Suspicious*（疑わしい） の三種類に分類した．

Malicious 判定には，Metamask が公開するブロックリスト [10] を用いた．このリストには，Web3 ユーザを標的とした悪性ドメイン名が登録されている．投稿中に含まれる URL のドメイン名が当該リストに含まれる場合，その投稿を Malicious と分類した．さらに，悪性サイトは寿命が短く，投稿収集時点で既に削除・無効化されている可能性がある．この点を考慮し，投稿に含まれる URL のドメインが名前解決不能（NXDOMAIN）であった場合や HTTP エラーが発生した場合も，Malicious と判定した．

Benign 判定には，Metamask が公開する正規ドメイン名のリストに加えて，2025 年 3 月 26 日に取得した Tranco リスト [11] の Top 1K および 3.1.1 項で選定したプロジェクトの公式ウェブサイトの URL に，ドメイン名が含まれる場合に Benign と判定した．Tranco リストは，Cisco Umbrella や Majestic など複数のランキングソースを統合して作成される再現可能なドメイン名ランキングである．なお，悪性ウェブサイトの中には，短縮 URL やホスティングサービスを利用するものも存在するため，Tranco Top 1K ドメインのうち，これらのドメイン名に該当するものは Suspicious に分類した．最後に Malicious, Benign のいずれにも分類されない投稿は，Suspicious と分類した．

3.3 分析

3.3.1 詐欺の分析

エアドロップを装った詐欺の実態を明らかにするため，収集・分類した投稿を以下の 4 つの観点から分析する．

アカウント．Malicious 投稿を行ったアカウントに着目し，その作成時期や影響力（インプレッション数）との関係を分析する．この分析により，攻撃者がどのようなアカウントを用いて詐欺投稿を拡散しているか，また，影響力の大きなアカウントに共通する特徴を明らかにする．

キャッシュタグ．投稿に含まれる CT の数や種類に着目し，それらが投稿の拡散やターゲットユーザ層に与える影響を分析する．特に，詐欺投稿における CT の出現傾向，CT の使用パターンを分析することで，攻撃者によるターゲティングの有無や意図を明らかにする．

タイムライン．詐欺サイトのドメイン名登録日，投稿時期，対象プロジェクトにおけるエアドロップ開始時期との関係を分析する．この分析により，攻撃者による一連の詐欺プロセスを時系列の観点で整理し，傾向や特徴を明らかにする．

表 1　検索条件に含めるティッカーシンボルの調査結果

時価総額	ミームコイン	エアドロップ開催中
ETH	DOGE	RIZ
BTC	SHIB	KAITO
XRP	PEPE	SHELL
USDT	TRUMP	IP
BNB	BONK	JUP

SC アドレス．Malicious 投稿に含まれるリンク先ウェブサイトにおいて，RPC による SC の関数呼び出しを検知し，SC アドレスを抽出する．この分析により，詐欺サイト URL と SC アドレスとの対応関係を明らかにする．

3.3.2　対策の分析

SNS を起点としたエアドロップを騙る詐欺は，投稿の拡散，詐欺サイトへの誘引，ウォレットの接続・送金という 3 段階のフェーズを経て実行される．そこで本分析では，収集・分類した投稿およびアクセス先ウェブサイトの調査結果を基に，各フェーズにおける対策の有無および有効性を検証する．

投稿拡散フェーズでは，詐欺投稿の拡散防止やアカウント凍結等，SNS プラットフォームによる対策を調査する．誘引フェーズでは，詐欺投稿に含まれる URL アクセス時の，詐欺サイトへの到達を防ぐ機構や警告表示の有無等，ブラウザおよびウォレットアプリによる対策を調査する．接続・送金フェーズでは，詐欺サイトにおけるウォレット接続・送金時の警告表示やリスク検知の有無等，ウォレットアプリによる対策を調査する．なお，本調査では，ブラウザは Google Chrome を利用し，ウォレットアプリはブラウザの拡張機能である Metamask を有効にして調査した．

4.　調査結果

4.1　投稿の収集結果

2025 年 2 月に 3.1.1 項に示した方法で，ティッカーシンボルを選定した結果を表 1 に示す．「時価総額」列に，時価総額上位 5 銘柄のティッカーシンボルを示す．これらには ETH や BTC など，取引量が非常に多く，ユーザの関心も高い主要銘柄が含まれる．「ミームコイン」列に，ミームコインの時価総額上位 5 銘柄のティッカーシンボルを示す．ミームコインは投機性や話題性を背景に注目を集める傾向が強く，特に 2025 年 2 月時点では，トランプ大統領の再選報道を契機に DOGE や TRUMP などの銘柄が急騰し，関心を集めていた．「エアドロップ開催中」列には，2025 年 2 月時点でエアドロップキャンペーンを実施していたプロジェクトのうち，開始時期が新しい順に選定した 5 件のティッカーシンボルを示している．このうち，Jupiter（JUP）を除く 4 件のプロジェクトは，いずれも 2025 年 2 月にエアドロップを開始していた．

これら 15 件のティッカーシンボルに，3.1.2 節の条件を加え，X 上でエアドロップ関連投稿を収集するための検索クエリを構築した．なお，X API の制限の都合により，収集対象の期間を 2025 年 2 月 10 日から同年 2 月 24 日までとした．図 1 の構築した検索クエリを用いて，455,842 件の投稿を収集し，これらの投稿から 172,489 件のユニークな URL を収集した．

図 1　検索クエリ

```
($RIZ OR $KAITO OR $JUP OR $SHELL OR $IP OR $ETH OR
$BTC OR $XRP OR $USDT OR $BNB OR $DOGE OR $SHIB OR
$PEPE OR $TRUMP OR $BONK)
(airdrop OR claim) has:links -is:retweet
since:2025-02-10 until:2025-02-24
```

表 2　URL および投稿の分類結果

分類	URL	投稿
Benign	167,216 (96.9%)	441,870 (96.9%)
Malicious	2,616 (1.6%)	3,959 (0.9%)
Suspicious	2,657 (1.5%)	10,013 (2.2%)
合計	172,489	455,842

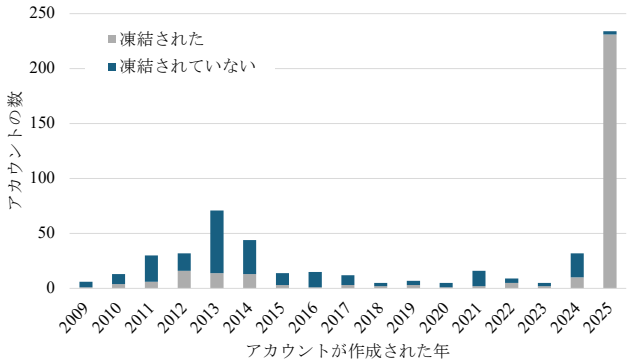

図 2　アカウント作成年別のアカウント数

4.2　投稿の分類結果

収集した URL および投稿に対して，3.2 節の分類手法を適用した結果を表 2 に示す．なお，1 件の投稿に複数の URL が含まれる場合には，当該投稿に含まれる URL の中で最も危険性の高いカテゴリに従って投稿を分類した．その結果，Benign に分類された URL は 167,216 件であり，収集した URL の 95% 以上は正規ウェブサイトの URL であった．一方，96 件の URL には既知の悪性なドメイン名が使用されており，2,520 件の URL は名前解決できない等の理由によりアクセスに失敗したため，計 2,616 件の URL を Malicious と判定した．それ以外の Suspicious URL は 2,657 件であった．

URL の分類結果に基づく Malicious 投稿は 3,959 件（0.9%）であり，少数ではあるものの，エアドロップ関連の投稿の中にも一定数の悪性な投稿が存在することが確認された．以降の分析は，これらの Malicious 投稿を対象とした．

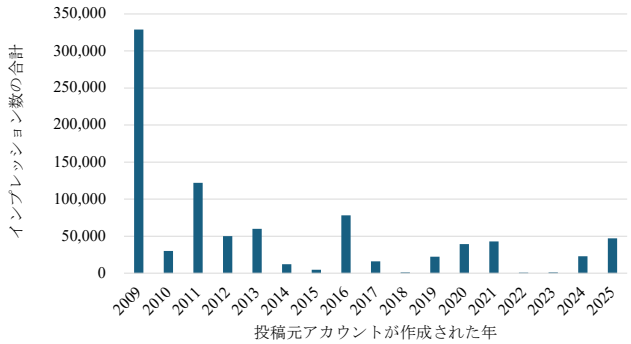

図 3 アカウント作成年別のインプレッション数の合計

4.3 投稿の分析結果

4.3.1 アカウントに基づく分析結果

投稿アカウントを分析した結果，計 550 件が Malicious 投稿を行っていた．それらアカウントの数を，アカウント作成年ごとに調査した結果を図 2 に示す．調査の結果，550 件のうち 231 件（42.5%）は 2025 年に作成されたアカウントであった．これは，攻撃者が詐欺投稿専用にアカウントを新規作成していると考えられる．残る 319 件（57.5%）は 2025 年以前に作成されたものであり，なかには 10 年以上前（2015 年以前）に作成されたアカウントが 50 件以上確認された．以上の結果から，攻撃者は新規および既存の両アカウントを用いて詐欺投稿を拡散していることが明らかとなった．新規アカウントは安価に量産できる一方でサービス事業者によってアカウント停止されやすく，古いアカウントは作成にコストがかかるものの停止されにくいと考えられる．

次に，アカウントの運用年数と Malicious 投稿の影響力の相関を分析した．図 3 に，Malicious 投稿のインプレッション数を，投稿アカウントの作成年ごとに集計した結果を示す．図 3 より，2009 年作成のアカウントによる詐欺投稿のインプレッション数が最も多く，32 万回を超えていた．一方，2025 年作成のアカウントによるそれは約 4 万 7 千回に留まっており，2009 年のアカウントに比べて少なかった．これは，古いアカウントが信頼性やフォロワー基盤を有している場合が多く，その結果として投稿がより多くのユーザーに届きやすいためと考えられる．

4.3.2 キャッシュタグに基づく分析結果

各投稿に含まれる CT の数に着目し，投稿の分類ごとに集計した結果を表 3 に示す．Benign 投稿のうち，95.3% 以上は CT を 1 つだけ含む投稿 (以降，単一 CT 投稿と呼ぶ) であり，複数の CT を含む投稿 (以降，複数 CT 投稿と呼ぶ) は 4.7% にとどまった．一方で，Malicious 投稿では 15.4%（610 件），Suspicious 投稿では 30% 以上 が複数 CT 投稿であった．特に 10 件以上の CT を含む投稿については，Benign では 1.1%, Suspicious では 2.1% に対し，Malicious では 7.6% であり，Malicious 投稿は多数の CT を含む投稿の割合が高かった．これは Malicious 投稿において，より多くの CT を含めることで広範なユーザに拡散しようとしていると考えられる．

表 3 キャッシュタグに基づく分析結果

CT の数	Benign	Malicious	Suspicious
なし	19 (0.0%)	0 (0.0%)	13 (0.1%)
単一	421,213 (95.3%)	3,349 (84.6%)	6,985 (69.8%)
複数	20,638 (4.7%)	610 (15.4%)	3,015 (30.1%)
合計	441,870	3,959	10,013

表 4 Malicious な単一 CT 投稿における頻出 CT Top 5

		投稿数		
#	CT	単一 CT	複数 CT	合計
1	`$SHELL`	2,265	1	2,266
2	`$RIZ`	559	22	581
3	`$KAITO`	249	23	272
4	`$IP`	164	77	241
5	`$TRUMP`	44	189	233

表 5 複数の CT を含む Malicious 投稿の頻出 CT Top 5

		投稿数		
#	CT	単一 CT	複数 CT	合計
1	`$XRP`	42	222	264
2	`$ETH`	5	216	221
3	`$BTC`	1	207	208
4	`$TRUMP`	44	189	233
5	`$SOL`	0	186	186

表 6 投稿に含まれる CT の数に対するインプレッション数の統計

CT の数	合計値	平均値	最大値	最小値	中央値
単一	577,562	172	20,837	0	0
複数	301,181	494	27,268	0	172

次に，Malicious 投稿における CT の傾向を分析した．表 4 に Malicious な単一 CT 投稿における頻出 CT Top5 を示す．単一 CT 投稿に多かった CT はいずれも，2025 年 2 月にエアドロップを開始した新興プロジェクトのティッカーシンボルであった．これらのプロジェクトは当該時期に一時的に注目を集めていたため，その関心に便乗して Malicious 投稿が拡散されたと考えられる．

表 5 に Malicious 複数 CT 投稿における頻出 CT Top5 を示す．複数 CT 投稿では，`$XRP`，`$ETH`，`$BTC`，`$SOL` など，時価総額上位の主要な暗号資産プロジェクトのティッカーシンボルが多く含まれる傾向がみられた．これは，著名な CT の組み合わせによって，より広範なユーザへの拡散を狙ったと推察される．

表 6 に，投稿に含まれる CT 数に対するインプレッション数の合計値，平均値，最大値，最小値，中央値を示す．単一 CT 投稿のインプレッション合計値は複数 CT 投稿を上回り，全体としてより大きな影響を及ぼしている．しかし，中央値が 0 であることから，多くの単一 CT 投稿は実際にはユーザに届いていないといえる．これは，単一 CT 投稿

表 7　各 CT を含む Malicious 投稿の日別投稿数の分布

投稿日	$SHELL	$RIZ	$KAITO	$IP	$TRUMP	$XRP	$ETH	$BTC	$SOL
2025/2/10	1	0	0	0	19	36	19	14	19
2025/2/11	1	0	0	0	14	81	14	53	14
2025/2/12	14	1	0	0	29	36	29	24	29
2025/2/13	**132**	0	0	58	16	13	16	2	16
2025/2/14	22	1	0	**2,192**	38	8	38	8	38
2025/2/15	3	0	0	0	47	5	47	1	47
2025/2/16	5	1	0	12	25	0	25	4	25
2025/2/17	9	0	0	0	5	4	5	4	5
2025/2/18	9	5	0	0	10	8	10	9	10
2025/2/19	12	6	0	0	5	6	5	12	5
2025/2/20	17	**135**	32	0	9	2	9	12	9
2025/2/21	6	85	**383**	1	7	7	7	10	7
2025/2/22	5	25	131	3	3	1	3	12	3
2025/2/23	3	6	27	0	6	1	6	6	6
2025/2/24	2	7	8	0	0	0	0	15	0

が特定の暗号資産プロジェクトに関心を持つ限定的なユーザを標的としているためだと考えられる．一方，複数 CT 投稿は平均値・中央値ともに単一 CT 投稿を上回る結果となった．これは，複数 CT 投稿が特定のプロジェクトに依存せず，より広範なユーザ層に拡散できるため，少数の投稿であっても効率的にユーザに届くことを示している．

4.3.3　タイムラインに基づく分析結果

表 4，表 5 に示す各 CT を含む Malicious 投稿について，日別の投稿数を表 7 に示す．複数 CT 投稿に多かった CT は，一定数の投稿が継続的に発生する傾向にある一方で，単一 CT 投稿に多かった `$SHELL`，`$RIZ`，`$KAITO`，`$IP` は，特定の日に投稿が集中する傾向が見て取れる．投稿が集中した CT のプロジェクトはエアドロップ開催のタイミングが影響しており，いずれもエアドロップ実施直後に Malicious 投稿が急増していた．この結果から，攻撃者はエアドロップの注目が集まるタイミングを狙って，詐欺投稿の拡散を図っていると考えられる．

次に，Malicious 投稿に含まれていた URL のドメイン名を分析した．Malicious なドメイン名（eTLD+1）は 208 件であり，その登録日を調査した結果，168 件（80.8%）が 2025 年に登録されたものであった．さらに，ドメイン登録日とそれを含む投稿の投稿日との日数差を調査したところ，684 件がドメイン登録当日に，3,639 件が登録から 5 日以内に投稿されていた．これらの結果より，攻撃者はドメイン登録から投稿拡散までを迅速に完了させることで，ホスティング事業者等によるテイクダウンやブロックリストベースによるセキュリティ対策を回避しようとしていると考えられる．

4.3.4　SC アドレスに基づく分析結果

Malicious URL のうち，既知の悪性ドメイン名が使用されていた 96 件に対して，ウェブブラウザを用いてアクセス調査を実施した．その結果，49 件（51.0%）は正常にアクセスでき，残りの 47 件（49.0%）は HTTP エラーの発生または DNS 名前解決の失敗によりアクセスできなかった．アクセスに成功した 49 件のウェブサイトを調査した結果，17 件（34.7%）において，アクセス直後に SC の関数を呼び出す RPC リクエストが確認され，そこから計 3 件の SC アドレスを抽出できた．いずれの SC も BNB チェーン上にデプロイされたものであり，17 件すべてのウェブサイトが共通してこれら 3 件の SC アドレスを参照していた．これらアドレスを調査した結果，いずれも Inferno Drainer [12] と呼ばれるウォレットドレイナーで確認されているものと一致したことから，17 件のウェブサイトはウォレットドレイナーを使用して作成された詐欺サイトであると考えられる．

4.4　現行の対策の分析結果

4.4.1　投稿拡散フェーズ

投稿拡散フェーズでは，主に SNS プラットフォーマーによるポリシー違反投稿の削除，およびユーザからの通報を契機としたアカウント凍結措置等の対策がある [13]．本調査においても，Malicious 投稿をした一部のアカウントがすでに凍結されていることを確認した．図 2 は，Malicious 投稿をしたアカウントのうち，凍結されたものとされていないものの件数をアカウント作成年別に示している．図 2 から明らかなように，2025 年に作成されたアカウントの大多数 98.7% が凍結されていた．この結果は，詐欺投稿を目的として新規作成されたアカウントに対しては，アカウント凍結措置が一定の抑止力として機能している可能性を示唆している．

一方で，2025 年以前に作成されたアカウントの 72.8% は凍結されておらず，過去に作成されたアカウントの場合には，当該対策が十分に機能しないことが懸念される．実際に，図 3 に示すように，2009 年や 2011 年に作成された

アカウントによる投稿は高いインプレッション数を記録しており，これらのアカウントは凍結を免れている可能性が高い．

4.4.2 誘引フェーズ

誘引フェーズでは，ユーザがアクセスする詐欺サイト URL に対して，ブラウザや拡張機能によるリストベースのブロックや警告表示等の対策がある．本調査では，96 件の URL が既存のブロックリストに登録されており，ブラウザ拡張機能である Metamask を有効にした状態でアクセスした結果，警告画面が表示され，アクセスが遮断されることを確認した．

一方，半数ほどの URL はエラーによりアクセスできなかったため，詐欺サイトがすでに運用終了した，すなわち使い捨てられた可能性が高いことを示唆している．さらに，4.3.3 項に記載したとおり，詐欺に使用された多くのドメイン名は，登録から数日以内に悪用されていることが判明しているため，短命な攻撃インフラとして運用されている傾向がある．このような特徴は，ブロックリストが有効に機能するまでの時間的ギャップを狙って詐欺を実行している可能性を示唆している．この結果から，現行のリストベースの対策は一定の効果を有するものの，リアルタイム性の限界と短命なインフラの運用により，防御が後手に回る可能性が高いといえる．

4.4.3 ウォレット接続・送金フェーズ

接続・送金フェーズでは，ユーザによる接続先ウェブサイトの正当性確認や用途に応じたウォレットアドレスの切り替え等の対策がある [14], [15]．これらの対策は，ウォレット接続時の被害リスクを一定程度軽減する上で有効ではあるが，いずれもユーザのリテラシーやセキュリティ意識に強く依存している．また，追加の確認作業や操作を利用者に強いるため，利便性や操作性を損ない，結果としてユーザ体験の悪化を招く可能性がある．

本フェーズにおいては，詐欺サイトの誘導に従ってウォレットを接続した際に，警告表示やリスク検知といったセキュリティ機構が存在するかを調査した．その結果，ウォレットによる警告表示やリスク検知は確認されなかった．つまり，現行のウォレットアプリでは接続時の防御機構は十分に備わっておらず，ユーザが自らリスクを判断しない限り，詐欺サイトへの接続を防ぐことは困難であることが明らかとなった．

5. 議論

5.1 新たなデータ収集の検討

本節では，暗号資産詐欺に関係する投稿やウェブサイトを効率的に収集するための手法について議論する．

5.1.1 効率的な投稿データの収集

本調査では，エアドロップ関連の投稿を収集するために検索クエリに CT を活用した．検索クエリに CT を含めない場合，同期間に収集される投稿数は 4,439,389 件に上るのに対し，CT を含めた図 1 のクエリでは 455,842 件であった．すなわち，CT を用いることで収集対象を約 90% 削減し，効率的に関連投稿を抽出できる．さらに，分析の結果，Malicious な単一 CT 投稿はエアドロップ開催中のプロジェクト CT を含み，エアドロップ開催と連動して突発的に投稿される傾向がある一方で，複数 CT 投稿は著名なプロジェクト CT を含み，継続的に投稿される傾向があることを確認した．この傾向から，収集対象とするプロジェクトに応じて収集期間を適切に設計することで，限られたリソースでも効率的かつ目的に沿ったデータ収集が可能であると考えられる．

しかし，SNS 上の投稿を起点とした詐欺サイトの収集分析には依然として課題が残る．まず，SNS 上で収集できる詐欺サイトの範囲は検索クエリに依存するため，一部を見逃す可能性がある．次に，SNS 上に投稿されない詐欺サイトは本手法で収集できないため，我々の調査方法では網羅性に欠ける．以上の課題を踏まえ，より包括的かつ効率的なデータ収集を実現するためには，2 章の関連研究で記載した手法を補完的に活用する必要があると考える．

5.1.2 ウェブサイトと SC アドレスの関係データの収集

4.3.4 項において，複数の詐欺サイトが同一の SC アドレスを参照していたことを確認したが，Passive DNS を用いて悪性 IP アドレスから複数の悪性ドメイン名候補を特定できるように，URL/ドメイン名と SC アドレスを関連付ける仕組みがあれば，詐欺サイトに悪用されている特定の SC アドレスに紐づく URL/ドメイン名を効率的に特定できる可能性がある．このような仕組みを実現する方法として，RPC ノードプロバイダやエンドユーザにおけるデータ収集が考えられる．前者は，ブロックチェーンとの通信過程で得られるメタデータを活用する方式であり，後者はユーザ端末におけるアクセス情報を利用する方式である．

RPC ノードプロバイダによるデータ収集と提供. RPC ノードプロバイダは，ブロックチェーンとの通信を仲介する RPC ノードを多数のサービスに対して提供している．したがって，RPC ノードプロバイダは，HTTP リファラ等，各 RPC リクエストの送信元情報を通じて，ウェブサイトと SC アドレス間の対応関係を特定できると考えられる．ただし，プロバイダによるデータ保持や共有体制に加え，プライバシー保護や利用規約，各種ポリシーの整備等が不可欠である．

ユーザによるデータ収集と共有. 各エンドユーザは，ブラウザ拡張等を通じてが自身のブラウジング環境で発生した RPC リクエストをローカルで収集し，匿名化した上で共有する．このような分散型コンテキストに沿った手法により，サービス提供者に依存せずにデータ収集基盤を形成することができる．一方で，ユーザ側に負担が発生することや，共有データの匿名化・セキュリティ確保といった課題

も存在する．

5.2 新たな検知手法の検討

本節では，前節におけるウェブサイトと SC アドレスの関係データを収集できた場合に，収集データを活用して未知の悪性サイトを検知可能か検証する．本検証では，Malicious サイトで確認した 3 件の SC アドレスの中に，表 2 の Suspicious ウェブサイトから 4.3.4 項の手法で抽出した SC アドレスが含まれるか調査した．調査の結果，5 件の Suspicious サイトにおいて，Malicious サイトと同一の SC アドレスを参照していることを確認した．目視でそれらのウェブコンテンツを確認したところ，これらはいずれも KAITO のエアドロップを装った詐欺サイトであった．

以上の結果から，SC アドレスとウェブサイトの関係性に着目することにより，従来のブロックリストベースの対策で見逃されていた詐欺サイトを検出できることが明らかとなった．特に，ウォレットドレイナーを用いた詐欺キャンペーンでは，同一の SC が複数の詐欺サイトで繰り返し流用される事例 [12] が確認されているため，本手法はそのような攻撃パターンに対して有効だと考えられる．前節で述べたデータ収集方法，および本節で述べた検知手法の大規模データによる評価は，今後の課題とする．

5.3 制限事項および研究倫理

本調査では，X API の制約により，検索条件を限定的かつ厳格に設定した．したがって，本研究で確認された詐欺サイトの傾向や特徴は，検索条件でヒットした詐欺サイトのみに依存しており，すべての事例を網羅的に反映しているわけではない．投稿の分類も，単一のブロックリストのみに依存しているため，Malicious 判定の網羅性に欠ける．また，投稿収集から URL アクセスまでの間隔は数日に留まるもののリアルタイムではなかったため，すでにアクセスできない URL が多数存在し，それらについては調査できていない．さらに，4.4.2 項および 4.4.3 項では，MetaMask を用いた評価結果のみを示しており．異なるウォレットアプリによる詐欺挙動の差異や対策状況は評価できていない．

なお，4.4.2 項および 4.4.3 項の MetaMask を用いた評価では，実際に詐欺サイトにアクセスし，ウォレット接続する操作を実行した．この時，本調査で用いたウォレットには残高を保持させず，攻撃者に資金が送金されることがないよう配慮した．

6. まとめ

本研究では，SNS 上に蔓延するエアドロップを騙る暗号資産詐欺の特徴および傾向を明らかにすることを目的に調査を実施した．具体的には，SNS プラットフォーム X 上のエアドロップ関連投稿 455,842 件を収集，収集した投稿に含まれる URL の分類し，アカウント，キャッシュタグ，タイムライン，SC アドレスの 4 つの観点から多面的な分析を行った．さらに，詐欺の流れを「投稿拡散」「誘引」「ウォレット接続・送金」の 3 フェーズに整理し，各フェーズにおける既存対策の実効性と限界を評価した．

加えて，本調査を通じて確認した「詐欺サイトにおける SC アドレスの再利用」という特徴に着目し，既存のブロックリストでは検知できなかった詐欺サイトの特定および検知の可能性について議論した．これらの結果は，暗号資産領域における詐欺対策の高度化に向けて，新たな検知手法の方向性を示すものであり，今後の実践的な対策技術の開発に向けた基盤として活用されることが期待される．

参考文献

[1] Bleeping Computer LLC, “Cryptocurrency wallet drainers stole $494 million in 2024.” https://www.bleepingcomputer.com/news/security/\\cryptocurrency-wallet-drainers-stole-494-million-in-2024/.

[2] J. Kimber *et al.*, “An end to end analysis of crypto scams on ethereum,” *ACM Transactions on Internet Technology*, 2025.

[3] P. D. Huynh *et al.*, “Serial scammers and attack of the clones: How scammers coordinate multiple rug pulls on decentralized exchanges,” in *The ACM Web Conference*, 2025.

[4] A. Kalacheva *et al.*, “Detecting rug pulls in decentralized exchanges: The rise of meme coins,” *Blockchain: Research and Applications*, p. 100336, 2025.

[5] M. M. Others, “The Poorest Man in Babylon: A Longitudinal Study of Cryptocurrency Investment Scams,” in *The ACM Web Conference*, 2025.

[6] E. Liu *et al.*, “Give and take: An end-to-end investigation of giveaway scam conversion rates,” in *ACM Internet Measurement Conference*, pp. 704–712, 2024.

[7] X. https://help.x.com/ja/resources/glossary.

[8] CoinMarketCap. https://coinmarketcap.com/.

[9] CryptoRank. https://cryptorank.io/.

[10] Metamask. https://github.com/MetaMask/eth-phishing-detect.

[11] V. Le Pochat *et al.*, “Tranco: A research-oriented top sites ranking hardened against manipulation,” in *NDSS*, 2019.

[12] Check Point Software Technologies LTD, “Inferno Drainer Reloaded: Deep Dive into the Return of the Most Sophisticated Crypto Drainer.” https://research.checkpoint.com/2025/inferno-drainer-reloaded-deep-dive-into-the-return-of-the-most-sophisticated-crypto-drainer/.

[13] X. https://help.x.com/ja/managing-your-account/suspended-x-accounts.

[14] Group-IB. https://www.group-ib.com/resources/knowledge-hub/crypto-wallet-drainers/.

[15] Kaspersky. https://blog.kaspersky.co.jp/what-is-a-crypto-wallet-drainer/35783/.