一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report

ウォレット接続後の権限要求に注目した Web3 フィッシングサイトの動的検知手法

青砥　陸† 　インミンパパ†† 　吉岡　克成†††,††

† 横浜国立大学大学院環境情報学府
†† 横浜国立大学先端科学高等研究院
††† 横浜国立大学環境情報研究院
E-mail: †aoto-riku-hx@ynu.jp, ††{yinminn-papa-jp,yoshioka}@ynu.ac.jp

あらまし　Web3 はブロックチェーン技術に基づく分散型エコシステムであり，その中で仮想通貨や NFT（非代替性トークン）などのデジタル資産が急速に普及している．一方，これらを標的としたフィッシングサイトによる被害も増加している．現行の対策として，代表的なウォレットツールの 1 つである MetaMask では，ブロックリストに基づく警告機能を提供している．しかし，このブロックリストは有志による手動での更新に依存しており，フィッシングサイトがリストに追加されるまでにはタイムラグが存在する．そのため，短期間でフィッシングサイトのドメインが変更されると，現行の対策は回避される可能性がある．本研究では，ウォレット接続後の過剰な権限要求を検出することにより，フィッシングサイトを即座に特定する新たな手法を提案する．具体的には，ブラウザ自動化ツール Selenium を使用して，デジタル資産の取引が可能な Web3 ウェブサイトにアクセスし，ウォレット接続を自動的に行った後，サイトの挙動を分析してフィッシングサイトかを判定する．この方法により，Web3 フィッシングサイトをより効率的に検出し，従来の対策におけるタイムラグを解消することが期待される．
キーワード　Web3，フィッシング，動的検知，NFT，仮想通貨

Detection of Web3 Phishing Sites Focused on Permission Requests After Wallet Connection

Riku AOTO†, Yin Minn Pa Pa††, and Katsunari YOSHIOKA†††,††

† Graduate School of Environment and Information Sciences, Yokohama National University
†† Institute of Advanced Sciences, Yokohama National University
††† Faculty of Environment and Information Sciences, Yokohama National University
E-mail: †aoto-riku-hx@ynu.jp, ††{yinminn-papa-jp,yoshioka}@ynu.ac.jp

Abstract　Web3 is a decentralized ecosystem based on blockchain technology, where digital assets such as cryptocurrencies and NFTs (non-fungible tokens) are rapidly gaining popularity. However, the victims of phishing attacks targeting these assets are also on the rise. As a current countermeasure, MetaMask, one of the leading wallet tools, alerts users when they access a web-3 phishing site identified on a blocklist. This blocklist, however, relies on manual updates by volunteers, resulting in a time lag before phishing sites are added to the list. Consequently, if a phishing site rapidly changes its domain, such countermeasure is ineffective. In this study, we propose a new method to immediately identify phishing sites by detecting excessive permission requests after wallet connection. Specifically, by using the browser automation tool Selenium, we access Web3 websites that enable digital asset transactions, automatically connect the wallet, and then analyze the site's behavior to determine if it is a phishing site. This approach is expected to detect Web3 phishing sites more efficiently and eliminate the time lag inherent in traditional countermeasures.
Key words　Web3, Phishing, Dynamic Detection, Cryptocurrency, NFT

1. はじめに

近年，ブロックチェーン技術に基づく分散型エコシステムである Web3 の発展に伴い，仮想通貨や NFT（非代替性トークン）などのデジタル資産が注目を集めている．これらの資産の価値と流通量は年々増加しており，例えばビットコインの価格は 10 年間で数十万倍にも上昇している [1]．しかし，デジタル資産の普及とともに，これらを狙ったフィッシングサイトの数も増加しており，2023 年 4 月から 2024 年 3 月の 12 カ月間では，約 25 億ドルの資産が盗まれたことが報告されている [2] [3].

Web3 フィッシングサイトとは, 仮想通貨や NFT などの Web3 関連サービスを装って，ユーザーから個人情報や秘密鍵，仮想通貨を騙し取ることを目的とした詐欺サイトである [4].

既存の対策として，ドメインブロックリストに基づく方法がある．Web3 サイトを利用する際，ユーザーはブラウザ拡張機能としてウォレットツールをインストールする必要がある．代表的なウォレットの 1 つである MetaMask [5] は，フィッシングサイトのドメインブロックリストを搭載しており，ユーザーがブロックリストに登録されているサイトにアクセスすると警告が表示される [6]. しかし，このブロックリストは有志によって手動で更新されているため，フィッシングサイトが発見されてからリストに追加されるまでにタイムラグが生じ，その間に被害が発生する可能性がある．さらに，攻撃者がサイトのドメインを頻繁に変更した場合，ブロックリストによる対策は回避されてしまうと考えられる．

本研究では，フィッシングサイトに特有の挙動であるウォレット接続後の過剰な権限要求を検出することにより，フィッシングサイトを即座に特定する新たな手法を提案する．この手法をブラウザ自動化ツールにより実装することで，サイトを自動的かつ動的に検査し，フィッシングサイトをより迅速に発見することを目指す．本手法では，ウォレットの接続導線を持ち，ウォレット接続後に追加の権限要求を行うタイプの Web3 フィッシングサイトを対象とする．一方，ウォレット接続を行わずに秘密鍵の入力を要求するタイプなど，異なる手口を用いるフィッシングサイトについては，本手法の対象外とする．

本研究では，MetaMask が提供するフィッシングサイトのブロックリストを用いて評価用の正解データを用意し，提案手法によるフィッシングサイトの判定精度を評価した．2024 年 5 月 17 日に作成した合計 100 個の正解データに対して，2024 年 5 月 17 日から 2024 年 5 月 24 日の間で評価を行い，Accuracy(正解率) は 0.800, Precision（適合率）は 1.000, Recall（再現率）は 0.375, F1（F 値）は 0.545 となった．

提案システムにおけるフィッシングサイトの見逃しの原因は，主に次の 2 つが考えられる．1 つ目は，システムが対応していないパターンのサイトである．Web3 サイトでは，「Connect Wallet」や「MINT」,「Check Eligibility」などのボタンが用意されており，ユーザーはサイトにアクセス後，このボタンをクリックしてウォレットを接続する．しかし，ボタンのラベルはサイトによって多種多様であり，システムがあらかじめ想定していたラベルの文字列以外を使用しているケースが存在した．その場合，自動化ブラウザがボタンを見つけられず，ウォレットの接続ができないため，検出に失敗するというケースがあった．今後は，システムで想定していなかった新たなボタンラベルが見つかった際には，それを手動で抽出し，システムに追加していくことで，検出可能なパターンを拡充していきたいと考えている．

2 つ目の原因は，サイト側で自動化ブラウザ経由のアクセスを妨害するような実装が施されているケースである．フィッシングサイトの作成者は，資産を持つユーザーを欺くことが目的であり，自動化ブラウザなどでアクセスされてフィッシングサイトの実装を調査されることを避けたいと考えられる．実際に，Cloudflare が提供するボット検知ツールである Cloudflare Turnstile [7] を導入しているフィッシングサイトや，自動化ブラウザでアクセスした際にボタンが無効化され，ウォレットの接続ができなくなっているサイトも存在した．このように，攻撃者側も防衛策を講じているケースが一定数見受けられた．しかし現状，大半のフィッシングサイトは原始的な手法でユーザーの資産を窃取しようとしている．そのため，自動化ブラウザなどの検出に対して適切な工夫を行うことで，本研究の自動手法により高い精度でフィッシングサイトを検出できると考えられる．

次に，ドメイン検索 API である WhoisXML API [8] を用いて 2024 年 5 月 10 日から 2024 年 5 月 13 日の期間で実世界の Web3 ドメインを収集し，提案システムによるフィッシングサイトの検出実験を行った．WhoisXML API は，指定した条件にマッチするドメインの情報を提供する API サービスである．実験では，この API を用いて，Web3 に関連する 4 つのキーワード「nft」「blockchain」「crypto」「airdrop」を指定し，それぞれの条件ごとに 50 個のドメインを検索した．その結果，合計 200 個のドメインを収集した．ただし，検索結果として得られたドメインの中には，ウォレットの接続導線が含まれていないものや，すでにドメインが変更されていてアクセスできないものが存在した．そのため，検索結果を手動で全てフィルタリングし，サイトにアクセス可能であり，なおかつウォレット接続の導線が含まれている 100 個のサイトを最終的に選定し，実験対象とした．

実験の結果，100 個の Web3 ドメインのうち，17 個がフィッシングサイトとして判定された．検出された 17 個のフィッシングサイトには，正規の NFT マーケットサイトを模倣したサイトや，仮想通貨や NFT，DeFi トークンを無料で配布する Airdrop キャンペーンを装ったサイト，仮想通貨取引所を偽装したサイトなどが含まれていた．キーワードごとの内訳を見ると，ドメイン名に「nft」を含むサイトのうち 5.8%,「blockchain」を含むサイトのうち 12.0%,「crypto」を含むサイトのうち 8.0% がフィッシングサイトとして判定された．一方,「airdrop」を含むサイトでは，実に 30.0% がフィッシングサイトであった．この結果は，攻撃者が Airdrop をテーマにしたフィッシングサイトを他のテーマに比べて好んで作成していることを示唆している．さらに，全体の 17.0% がフィッシングサイトと判定

されたことから，Web3 のエコシステムは攻撃者にとって魅力的な標的となっていることが推察される．

今後は，本システムを用いて発見したフィッシングサイトのリストを MetaMask のブロックリストなどに提供し，Web3 コミュニティ全体のセキュリティ向上に貢献することを目指す．

2. 準　　備

2.1 Web3 とウォレットについて

Web3 は，ブロックチェーン技術に基づく分散型エコシステムであり，中央集権的な管理者を介さずに，ユーザー同士が直接やりとりを行うことができる．この新しいエコシステムにおいて，仮想通貨や NFT（非代替性トークン）などのデジタル資産が重要な役割を果たしている．

ユーザーが Web3 サービスを利用する際，自身のデジタル資産を管理するためのツールとしてウォレットが必要となる．ウォレットは，仮想通貨や NFT を保管・送受信するためのデジタルな財布であり，ユーザーの秘密鍵を安全に管理する．Web3 サイトを利用する際，ユーザーは自身のウォレットをサイトに接続することで，サイト上でデジタル資産を使用することができる．

2.2 Web3 フィッシングサイトとは

Web3 フィッシングサイトとは，仮想通貨や NFT などの Web3 関連サービスを装って，ユーザーから個人情報や秘密鍵，仮想通貨を騙し取ることを目的とした詐欺サイトである．これらのサイトは，正規の Web3 サービスの見た目を巧妙に模倣し，ユーザーに安全な環境下にいるという錯覚を与えることで，ウォレットの接続や機密情報の入力を促す．フィッシングサイトを運営する攻撃者は，ユーザーに対して送金要求の承認を求めたり，秘密鍵の入力を要求したりすることで，ユーザーの資産を不正に取得しようと試みる．[9].

Web3 エコシステムの急速な成長とデジタル資産への投資熱の高まりに伴い，Web3 フィッシングサイトは特に重大な問題となっている．仮想通貨や NFT の価格上昇は，攻撃者にとって魅力的なターゲットとなり，彼らはより巧妙で検出困難な手法を日々開発している．フィッシングサイトによる被害は，金銭的な損失だけでなく，ユーザーの信頼を損ない，Web3 コミュニティ全体の安全性に対する疑念を引き起こしうる．

2.3 フィッシングサイトと正規サイトの共通の挙動

Web3 サイト，特に仮想通貨や NFT に関連するサイトを利用する際，ユーザーは自身のウォレットをサイトに接続する必要がある．このウォレット接続は，ユーザーがサイトを利用するための前提条件であり，正規サイトであれフィッシングサイトであれ，以下の共通のプロセスを踏む．

1) 接続ボタンのクリック：ユーザーはサイト上に表示された「Connect Wallet」や「Mint」などのボタンをクリックする．このボタンは，サイトがウォレット接続をサポートしていることを示し，ユーザーが自身のウォレットをサイトに連携させるための入口となる．

2) 使用しているウォレットの選択：ボタンをクリックした後，サポートされているウォレットのリストが表示される．ユーザーはこの中から使用しているウォレットを選択する．

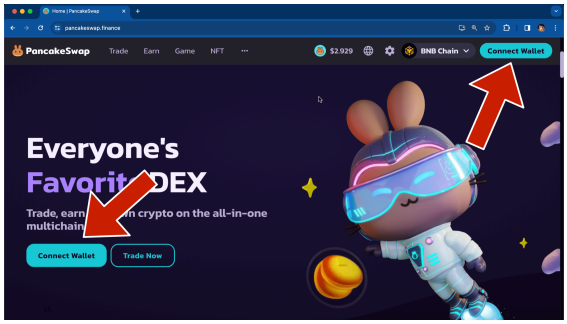

図 1: 接続ボタンのクリック

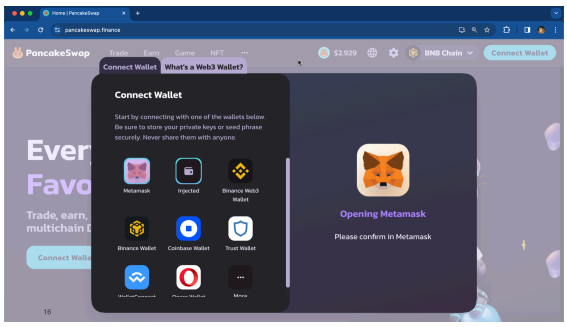

図 2: 使用しているウォレットの選択

3) ウォレットの接続の承認：ウォレットを選択した後，ウォレットアプリケーション（例：MetaMask）が自動的に起動し，ユーザーはサイトとの接続を承認する．この承認により，サイトはユーザーのウォレットアドレスへのアクセス権を得る．

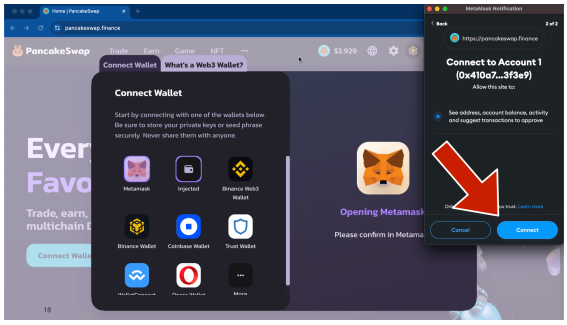

図 3: ウォレットの接続の承認

ウォレット接続の段階までは，フィッシングサイトも正規サイトも同様のユーザー体験を提供する．しかし，ウォレット接続後に両者の挙動に顕著な違いが現れる．この違いはフィッシングサイトの検出において重要な手がかりとなり，次のセクションで詳細に説明する．

2.4 フィッシングサイト特有の挙動：追加の権限要求

フィッシングサイトがウォレット接続後に示す最も識別可能な特徴の 1 つは，ウォレット接続後に発生する追加の権限要求である．要求される権限には，ユーザーのウォレットから仮想通貨を不正に送金するための権限や，ユーザーに気づかれずに資産を移動するための署名要求などがあり，悪意のある操

作を実行するために用いられる．正規サイトでは，ウォレット接続後にこれらの追加権限が必要とされることはほとんどなく，フィッシングサイトに特有の挙動として認識される．

図 4 はフィッシングサイトの一例である．ウォレットに $40 の残高がある状態でアクセスを行ったところ，このサイトではウォレット接続後に $18.71 の送金が要求され，送金のために必要な手数料であるガス代 $12.74 と合わせて合計 $31.44 を攻撃者のアカウントに送金する権限を要求する挙動が観測された．

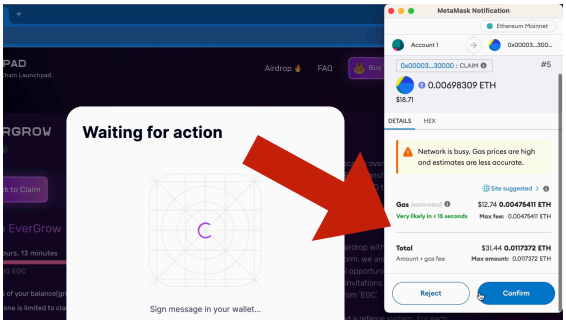

図 4: サイトが追加で要求してくる権限の例

2.5 関 連 研 究

本節では，Web3 フィッシングの検出に関連する先行研究を概観し，本論文で提案する手法との関連性と差異について議論する．

Yuan et al. [10] は，Ethereum ブロックチェーン上でのフィッシング詐欺の検出手法を提案している．著者らは，Ethereum のトランザクション記録を用いた 3 段階の検出フレームワークを提案し，node2vec を用いてフィッシングアカウントの特徴を抽出し，One-class SVM で分類している．提案手法の有効性を 2 つの実際の Ethereum ネットワークデータで検証し，高い検出精度を達成している．

Chen et al. [11] は，イーサリアムにおけるフィッシング詐欺の検出に向けて，トランザクションデータに基づく新しいアプローチを提案している．著者らは，グラフベースのカスケード特徴抽出手法と LightGBM ベースの Dual-sampling Ensemble アルゴリズムを用いて識別モデルを構築し，その有効性を複数の実験で示している．

Roy et al. [9] は，Twitter におけるフィッシングを目的とした NFT プロモーションの実態を明らかにしている．著者らは，439 のプロモーションサービスが 823 の NFT プロジェクトを宣伝し，そのうち 36 %以上が詐欺的なプロジェクトであることを突き止めた．また，プロモーションに関与するアカウントの大部分がボットであり，実在のユーザーを誘導していることも示している．さらに，既存のフィッシング対策の問題点を指摘し，機械学習を用いた新たな詐欺的 NFT プロジェクト検出ツールを開発・公開している．

He et al. [12] は，Ethereum におけるトランザクションベースのフィッシング（TxPhish）を体系的に調査し，大規模な TxPhish 検出システム TxPhishScope を構築している．TxPhishScope は，疑わしいウェブサイトを動的に巡回し，トランザクションをシミュレーションすることで TxPhish を検出する．8 ヶ月以上の運用で 26,333 の TxPhish ウェブサイトと 3,486 のフィッシングアカウントを検出し，報告された TxPhish サイトの 78.9% を最初に発見したことを示している．また，TxPhish サイトの寿命，コスト，更新頻度の観点から包括的な測定を行っている．

これらの先行研究は，様々なアプローチで Web3 フィッシング検出に取り組んでいる．本論文では，ブラウザ自動化を用いて，ウォレット接続後の動的な挙動を直接検証するアプローチを採用している点で，従来研究とは一線を画している．また，Web3 に特化したフィッシングの特徴であるウォレット接続後の権限要求に着目している点でも，新規性がある．本論文は，これらの先行研究の知見を踏まえつつ，Web3 時代のセキュリティ研究の新たな方向性を示すものである．

3. 提 案 手 法

本研究では，Web3 フィッシングサイトを自動的に検出するために，ブラウザ自動化ツールを用いてサイトの挙動を分析する手法を提案する．提案手法の流れは以下の 3 つのプロセスから構成される．

（1） **サイト訪問プロセス**：収集したドメインに対して，Selenium を使用して自動的にアクセスし，ウォレット接続のための導線となるボタンの存在を確認する

（2） **ウォレット接続プロセス**：サイト上のウォレット接続ボタンをクリックし，MetaMask などのウォレットアプリを介してサイトにウォレットを接続する．

（3） **挙動分析プロセス**：ウォレット接続後のサイトの挙動を分析し，追加の権限要求の有無を確認することで，フィッシングサイトであるかどうかを判定する．

3.1 サイト訪問プロセス

サイト訪問プロセスでは，検査対象のドメインに対して，Selenium を用いて自動的にアクセスを行う．その際，サイト上にウォレット接続のためのボタンが存在するかどうかを確認する．これらのボタンには通常，「Connect Wallet」や「Mint」など，ウォレット接続や NFT の購入に関連するキーワードが記載されている．システムで探索対象とするボタンのキーワードを決定するため，MetaMask のフィッシングサイトブロックリスト [13] に登録されているサイトを実際に訪問し，そこで使用されていたボタンのキーワードの中から 20 個を選定し，システムでの探索対象とした．本手法で探索対象としたキーワードを，Listing1 に示す．これらのキーワードを含むボタンがサイト上に見つからない場合は，ウォレット接続の導線がないとみなし，そのドメインを検査対象から除外する．一方，ボタンが見つかったサイトについては，次のプロセスで実際にウォレットの接続を試行する．

3.2 ウォレット接続プロセス

提案手法のウォレット接続プロセスでは，ブラウザ拡張機能型のウォレットアプリをサイトに接続する必要がある．本研究

Listing 1: キーワードリスト

```
Connect, CONNECT, Connect Wallet, CONNECT WALLET, Connect
your wallet, Access Wallet, Mint, MINT, Claim, CLAIM,
Claim Now, Claim now, Vote Now, Vote now, Check
Eligibility, Claim Airdrop, Claim airdrop, Check
allocation, Get Started, Get started
```

では，多くの Web3 サービスで使用されており，フィッシングサイトのウォレット接続導線でも上位に表示されることが多い MetaMask を使用するウォレットとして選定した．MetaMask は，Web3 エコシステムにおける代表的なウォレットの 1 つであり，これを採用することで，提案システムのカバー率を高めることができると考えられる．

ウォレット接続の手順としては，まず，サイト訪問プロセスで特定したウォレット接続ボタンをクリックする．次に，MetaMask を選択し，接続を承認することでサイトへのウォレット接続が完了する．ただし，自動化ツールである Selenium にはウォレットを直接操作する機能が提供されていないため，MetaMask の拡張機能のインストールやセットアップ，ウォレットの操作を行うためのプログラムを独自に実装した．

また，実際のユーザー環境に近い条件で検証を行うため，MetaMask には事前に約 10 ドル相当のイーサリアムを入金している．イーサリアムは，ビットコインと並んで広く普及している仮想通貨であり，多くの Web3 サービスで使用されている．一部のサイトでは，ウォレット接続後に残高がチェックされ，残高が一定の閾値を下回る場合にエラーが発生することがある．この問題を回避するためにも，一定の残高を持つウォレットを用意することは重要である．エラーを発生させる閾値はサイトによって異なり，中には 100 ドル以上の残高を要求するサイトも存在する可能性がある．しかし，本研究では，万が一の資産流出のリスクを考慮し，入金額を 10 ドルに設定している．

3.3 挙動分析プロセス

挙動分析プロセスでは，ウォレット接続後のサイトの挙動を分析し，フィッシングサイトであるかどうかを判定する．具体的には，ウォレット接続完了後に 10 秒間待機し，その間に追加の権限要求が発生するかどうかを確認する．追加の権限要求には，第三者への仮想通貨の送金要求や署名要求などが含まれる．これらの権限要求がサイト接続後にユーザーの明示的な操作なしに発生した場合，そのサイトはフィッシングサイトであると判定する．一方，追加の権限要求が観測されない場合は，正規のサイトであると判断する．ここで，ウォレット接続後の待機時間を 10 秒と設定した理由について説明する．多くのフィッシングサイトでは，ウォレット接続直後ではなく，数秒のラグの後に権限要求のポップアップが表示される傾向が観察された．実際に，MetaMask のフィッシングサイトブロックリストに登録されているサイトを調査したところ，大半のサイトでは 10 秒以内に追加の権限要求が発生していた．一方で，中には数十秒を要するサイトも存在した．待機時間の閾値を大きくすれば，より多くのフィッシングサイトを検出できる可能性があるが，一サイトあたりの検査時間が増大してしまう．したがって，検知率と効率性のバランスを考え，10 秒という値を採用している．

以上の 3 つのプロセスを経ることで, 提案手法は Web3 フィッシングサイトを自動的に検出することが可能となる．

4. 実　　験

4.1 評　　価

本研究で提案する Web3 フィッシングサイトの動的検知手法の有効性を検証するために，以下のような評価方法を採用した．評価の主な目的は，提案手法の性能を次の 2 つの観点から測定することである．評価には，2024 年 5 月 17 日に収集したドメインのデータセットを使用し，2024 年 5 月 17 日から 2024 年 5 月 24 日の間で実験を行った．

（1） フィッシングサイトの検知率：提案手法がフィッシングサイトをどの程度正確に識別できるかを測定する．

（2） 誤検知率：提案手法が正常な Web3 サイトを誤ってフィッシングサイトと判断する割合を測定する．

4.1.1 評価用データセットの作成方法

評価に使用したデータセットは 2 種類で構成される．第 1 のデータセットは，MetaMask が公開しているドメインブロックリストから収集した 300 個のフィッシングサイトのドメインである．このデータセットに含まれるドメインは，有志によってフィッシングサイトとして報告されたものであり，提案手法のフィッシングサイト検知率の測定に使用する．第 2 のデータセットは，MetaMask が公開しているドメインのホワイトリストから収集した 100 個の正規サイトのドメインである．このデータセットに含まれるドメインは，有志によって正規サイトとして認められたものであり，誤検知率の測定に使用する．

本システムはウォレットを接続する導線があり，かつウォレット接続後に権限を要求してくるタイプのフィッシングサイトの検知をターゲットにしているため，ウォレット接続の導線がないドメインや秘密鍵の入力を要求するタイプのドメインは正解データから除外した．正解データの選定条件は，ウォレットの接続導線があり，ウォレット接続後に権限を要求するというものである．第 1 のデータセット 300 個のドメインから，この条件に基づいて手作業で 97 個のドメインを検査した結果，47 個のドメインが除外され，最終的に 50 個の正解データを用意した．

除外された 47 個のドメインのうち，19 個のサイトでは，ウォレット接続後にエラーが発生した．具体的には，「Connect Wallet」などのボタンをクリックして，MetaMask を選択し，接続のローディングが表示された後，「Not eligible」など，サイトを使用する権利がないという表示がされた．エラーの文章はサイトによって異なり，「セキュリティ上の理由から，このウォレットは使用できない」という内容の文章が表示されるサ

イトも存在した．この明確な理由は表示されていなかったが，一つの原因としてはウォレットの残高が低すぎることが考えられる．フィッシングサイトの攻撃者は，高額な資産を保有するユーザーを標的とし，可能な限り多くの資産を窃取しようとする傾向があると推察される．一方で，今回テストに使用したウォレットは 10 ドルしか残高が入っておらず，フィッシングサイトの中には，接続時に残高をチェックして，その残高が特定の閾値以下の場合にエラーにさせるものが存在すると考えられる．このようにして，手動でのウォレットの接続時にエラーになるものも正解データからは除外した．実際にエラーになった時の画面を図 5 に示す．一方，残りの 28 個のサイトが除外された主な理由は，そもそもウォレットの接続導線が存在しなかったためである．MetaMask のフィッシングサイトブロックリストには，仮想通貨に関連するブログサイトなども含まれていたが，これらのサイトにはウォレットを接続するためのボタンなどの導線が含まれていなかった．このような理由で，残りの 28 個のサイトも正解データから除外された．

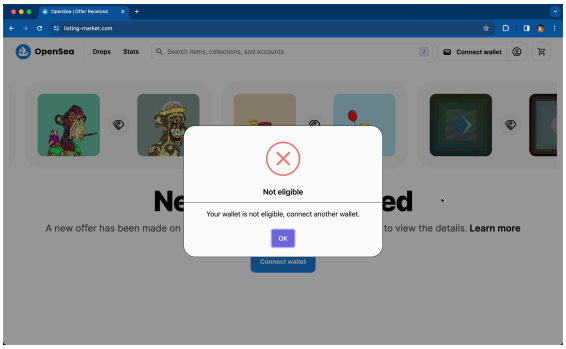

図 5: ウォレット接続時のエラー画面の例

4.1.2 評価結果

提案手法での検知結果を表 1 に示す．正解値が True で予測値が True の値を TP，正解値が True で予測値が False の値を FN，正解値が False で予測値が True の値を FP，正解値が False で予測値が False の値を TN とする．そのとき，$Accuracy = \frac{TP+TN}{TP+FP+FN+TN}$，$Presision = \frac{TP}{TP+FP}$，$Recall = \frac{TP}{TP+FN}$，$F1 = \frac{2(Precision \cdot Recall)}{Precision+Recall}$ として，小数点第 4 位は切り捨てる．その結果，Accuracy（正解率）は 0.800, Precision（適合率）は 1.000, Recall（再現率）は 0.375, F1（F 値）は 0.545 となった．

表 1: 評価実験の結果

		予測値	
		True	False
正解値	True	30	20
	False	0	50

提案システムにおけるフィッシングサイトの検出漏れは 20 個あり，その主な原因は次の 4 つが挙げられる．

a） 自動化ブラウザの検知 (9 個)

失敗したサイトの中には，自動化ブラウザ（Selenium）でアクセスした際と通常アクセスした場合で挙動が変化するものが存在した．具体的には，Selenium でアクセスした際には，ウォレット接続をするためのボタンのクリックが無効化され，クリックしても反応しないようになっていた．これは，サイト側がリクエストのユーザーエージェントをチェックし，自動化ブラウザからのアクセスを検知して妨害するために，ボタンを無効化していたと考えられる．

b） ボット検知システムの導入 (7 個)

フィッシングサイトの中には，Cloudflare Turnstile を導入しているものがあり，7 個のサイトでこれを採用していたために検知できなかった．Cloudflare Turnstile は CAPTCHA のようにボットのアクセスを検知するものであり，Selenium でアクセスした場合には突破できず，検査そのものができなかった．

c） 権限要求の遅延によるタイムアウト (2 個)

タイムアウトとは，サイトでウォレット接続が完了してから権限要求のポップアップが表示されるまでの時間が長すぎて，検査がタイムアウトしたことを指す．提案手法の章で述べたように，今回のシステムではウォレット接続後に 10 秒間待機し，その間に権限要求があるかをチェックしている．2 つのサイトでは，ウォレット接続完了からポップアップ表示までに 10 秒以上かかり，検知できなかった．

d） 未対応のボタンラベル (2 個)

未対応のボタンラベルとは，サイトのウォレット接続ボタンに書かれているラベル（文字列）が，システムがカバーしていなかったケースである．今回のシステムでは，”Connect Wallet”や”MINT”などの特定のキーワードを探してウォレット接続を行う仕組みだが，対応していないラベルを使用しているサイトがあり，ウォレット接続の試行ができずに失敗した．

誤検知率の評価結果としては，MetaMask のホワイトリストに登録されている 50 個のドメインのうち，フィッシングサイトと誤判定されたドメインは存在しなかった．これは，少なくともこの限られたサンプル内では，提案手法が誤検知を引き起こさなかったことを示している．しかし，試験したドメインの数が少ないため，より多くのドメインに対してテストを行うと誤検知が発生する可能性は存在する．

以上の手順により，提案手法のフィッシングサイト検知率と誤検知率を客観的に検証した．

4.2 実世界のドメインでの実験

MetaMask のリストを用いた正解データによる評価に加え，実世界のドメインに対しても本システムで検査を行い，フィッシングサイトの検出割合を調査する実験を行った．

4.2.1 実験データの作成方法

ドメインの収集には，WhoisXML API を用いた．WhoisXML API は，指定した条件にマッチするドメインの情報を提供する API サービスである．本実験では，この API を用いて 2024 年 5 月 10 日から 2024 年 5 月 13 日の期間で検査対象となる Web3 ドメインを収集した．API では，ドメイン名に含まれるキーワードを指定して，その条件にマッチするドメインを検索することができる．検索時には，Web3 に関連する 4 つのキーワード「nft」「blockchain」「crypto」「airdrop」を選定し，それぞれの

条件ごとに 50 個のドメインを検索した．その結果，合計 200 個のドメインを収集した．

ただし，検索結果として得られたドメインの中には，ウォレットの接続導線が含まれていないものや，すでにドメインが変更されていてアクセスできないものが存在した．そのため，検索結果を手動で全てフィルタリングし，サイトにアクセス可能であり，なおかつウォレット接続の導線が含まれている 100 個のサイトを最終的に選定し，実験対象とした．

フィルタリングの結果，選定された 100 個のドメイン名の中に含まれるキーワードの分布は，表 2 の通りとなった．選定されたドメイン名のキーワード分布が均等でない理由は，各キーワードによって，API の検索結果に含まれるウォレット接続の導線があるサイトの割合が異なるためである．例えば，「nft」というキーワードで検索した場合，検索結果の 50 個のドメインのうち，ウォレット接続の導線があるサイトは 17 個しかなく，25 個に到達しなかった．一方で，「airdrop」というキーワードでは，ウォレット接続の導線があるサイトが多く含まれていたため，33 個のドメインが選定された．このように，キーワードによってウォレット接続の導線があるサイトの割合が異なるため，各キーワードのドメイン数が均等になっていない．

表 2: 各キーワードごとのドメイン数とフィッシングサイトの検知結果

	nft	blockchain	crypto	airdrop	合計
ドメイン数	17	25	25	33	100
フィッシングサイト数	1	3	2	11	17
フィッシングサイトの割合	5.8%	12.0%	8.0%	30.0%	17.0%

4.2.2 実 験 結 果

実験の結果，100 個のドメインのうち，17 個が本システムによってフィッシングサイトとして検出された．キーワードごとの内訳を見ると，ドメイン名に「nft」を含む 17 個のサイトのうち 1 個（5.8%），「blockchain」を含む 25 個のサイトのうち 3 個（12.0%），「crypto」を含む 25 個のサイトのうち 2 個（8.0%）がフィッシングサイトとして判定された．一方，「airdrop」を含む 33 個のサイトでは，11 個（30.0%）がフィッシングサイトであった．この結果は，全体の平均であるフィッシングサイトの割合 17% と比較して，「airdrop」に関連するサイトで特に高い割合でフィッシングサイトが存在することを示している．つまり，攻撃者はフィッシングサイトを作成する際に，Airdrop をテーマにしたサイトを他のテーマのサイトに比べて好んで選択していると考えられる．

検出されたフィッシングサイトには，正規の NFT マーケットサイトを模倣したサイトや，仮想通貨や NFT，DeFi トークンを無料で配布する Airdrop キャンペーンを装ったサイト，仮想通貨取引所を偽装したサイトなどが含まれていた．これらのサイトは全て，ウォレット接続後に仮想通貨の送金権限を要求する挙動を示しており，その挙動の検知によってフィッシングサイトと判定された．

実験の結果，100 個のドメインのうち 17 個がフィッシングサイトとして判定されたことは，Web3 エコシステムにおけるセキュリティの課題を浮き彫りにしている．この 17% という数字は，Web2 の世界では考えられない高い割合である．Web2 のサイトでは，フィッシングサイトの割合はごくわずかであり，ほとんどのユーザーが安心してサイトを利用できる環境が整っている．一方，Web3 はまだ発展途上の段階にあり，フィッシングサイトに対する対策が十分に確立されていないと考えられる．また，Web3 の特性上，ユーザーが誤った操作を行ってしまうと，ワンクリックで膨大な量の資金が盗まれてしまう可能性がある．これらの要因が相まって，Web3 のエコシステムは攻撃者にとって魅力的な標的となっていると推察される．

5. 考　　察

本研究で提案する Web3 フィッシングサイトの動的検知手法の評価結果を踏まえ，検出率の向上と誤検知率の低減に向けた課題と展望について考察する．

5.1 検出率の向上に向けた課題

提案手法の Accuracy（正解率）は 0.800 であり，改善の余地が残されている．この検出率の向上に向けた主な課題として，以下の 2 点が挙げられる．

5.1.1 多様なフィッシング手法への対応

提案手法は，ウォレットの接続後に追加の権限を要求するタイプのフィッシングサイトの検出に特化している．しかし，フィッシングサイトは多様な手法を用いてユーザーの機密情報や資産を詐取しようと試みる．例えば，ウォレットの接続に失敗したように偽装し，ユーザーに機密情報の入力を促す手口などがある．提案手法はこのような手法への対応が不十分であり，検出率の向上のためには，より幅広いフィッシング手法に対応できるよう，検知アルゴリズムを拡張する必要がある．

5.1.2 フィッシングサイトの検出回避戦術への対策

フィッシングサイトは，検出を回避するために様々な戦術を採用している．例えば，ウォレットの残高をチェックし，一定の閾値以下である場合にエラーを表示してその後の操作を拒否するケースや，自動化されたブラウザを検知してボタンのクリックを無効化するケースなどが観測された．これらの戦術に対応するためには，提案手法をさらに洗練させ，フィッシングサイトが用いる可能性がある様々な検出回避手法に対応できるような仕組みを追加する必要がある．例えば，ユーザーエージェントの変更によって実際のユーザーからのアクセスに偽装したり，使用するウォレットに一定額以上の仮想通貨を実際に入金しておくなどの方法が考えられる．

5.2 誤検知率の評価と低減

提案手法の誤検知率を評価するために，MetaMask のホワイトリストに掲載されている正規サイトを用いてテストを行った．時間的制約から 50 個のドメインに対するテストのみを実施したが，この限定的なテストでは誤検知は発生しなかった．ただし，テスト対象となったドメインの数が限られているため，将来的にはより広範なドメインに対してテストを行うこ

とで，誤検知の可能性をさらに評価する必要がある．

誤検知は正規サイト運営者に深刻な問題を引き起こす可能性があるため，検出システムの継続的な改善と精度の向上が求められる．具体的には，正規サイトの挙動を詳細に分析し，フィッシングサイトとの違いを明確化することで，誤検知を最小限に抑えるための判定基準を確立することが重要である．

5.3 オンデマンド型検査システムへの発展

現在の提案手法では，API 経由で入手したドメインに対してフィッシングサイトの検査を行っている．しかし，将来的に Web3 のドメインが急増した場合，事前に入手したドメインのみを調査するアプローチには限界が生じる可能性がある．

この課題に対応するため，検知部分を切り出し，ユーザーのデバイスにインストールする拡張機能として提供するオンデマンド型の検査システムへと発展させることが考えられる．ユーザーがアクセスしたサイトに対して，リアルタイムで検査を行い，その結果を収集してブロックリストを動的に更新する仕組みである．これにより，Web3 エコシステムの拡大に合わせて，柔軟にフィッシングサイト検出を行うことが可能になるだろう．

以上のように，提案手法の発展を通じて，より包括的かつ効果的なフィッシングサイト対策の実現に貢献できると考えられる．

6. 結　　論

6.1 本研究の成果と意義

本研究では，Web3 フィッシングサイトを早期に検出するための新たな手法を提案した．提案手法は，ブラウザ自動化ツールを用いてサイトの挙動を動的に分析し，ウォレット接続後の過剰な権限要求を検出することで，フィッシングサイトを特定する．評価実験の結果，提案手法の Accuracy（正解率）は 0.800 となった．また，誤ってフィッシングサイトとして判定される誤検知は発生しなかった．これは，提案手法が Web3 エコシステムのセキュリティ向上に寄与する可能性を示唆している．

一方で，現状の提案手法の検出率には改善の余地があることも明らかになった．この原因として，フィッシングサイトが採用する多様な検出回避戦術への対応が不十分であることが挙げられる．例えば，自動化されたブラウザへの対策を講じるサイトの存在が検出を困難にしている．

本研究の意義は，Web3 フィッシングの問題に対して新たな視点と解決策を提供した点にある．提案手法は，従来のブロックリストベースの対策では対応が難しかった未知のフィッシングサイトに対しても有効であり，被害の減少に貢献することが期待される．一方で，検出率の向上とフィッシングサイトの巧妙化への対応は，今後の研究における重要な課題であることも明らかになった．

6.2 Web3 エコシステムの安全性向上に向けて

本研究で提案した手法は，Web3 フィッシングの問題に対する 1 つの解決策であるが，Web3 エコシステム全体のセキュリティを確保するためには，多角的なアプローチが必要である．Web2 の世界でもユーザーはフィッシングサイトに十分注意する必要があるが，非中央集権型であり，すべてが自己責任となる Web3 の世界では，より一層の注意が求められる．

Web3 では，ユーザーが要求された権限をきちんと読まずに，適当にボタンをクリックしてしまえば，その瞬間に自分が持っている資産がすべて盗まれてしまうといったリスクが存在する．たとえ自動検知システムでフィッシングサイトを見つけることができたとしても，最終的にはユーザー自身が十分な注意を払わなければ，被害を防ぐことは難しい．

そのため，技術的な対策の開発と並行して，ユーザー教育の強化や Web3 コミュニティ内での情報共有の促進など，人的・社会的な側面からのアプローチも欠かせない．ユーザーが Web3 の特性を理解し，自身の資産を守るための知識を身につけることが重要である．

今後の研究では，提案手法の改善を通じてフィッシングサイト検出の精度を高めるとともに，Web3 フィッシングに関する新たな知見の獲得を目指すことが重要である．フィッシングサイトの巧妙化に対応し，Web3 の健全な発展を支えることが，この研究領域の究極的な目標といえる．本研究がその一助となり，Web3 の可能性を最大限に引き出すための基盤となることを期待したい．

謝辞：本研究の一部は JSPS 科研費 22H03588 の助成を受けて行われた．

文　　献

[1] “Bitcoin’s Price History”. https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp.

[2] J. Wu, K. Lin, D. Lin, Z. Zheng, H. Huang, and Z. Zheng, “Financial crimes in web3-empowered metaverse: Taxonomy, countermeasures, and opportunities,” IEEE Open Journal of the Computer Society, vol.4, pp.37–49, 2023.

[3] “Web3 Scams & Security Incidents Report: March 2024”. https://blockfence.io/security/web3-security-incidents-report-march-2024-blockfence/.

[4] “Anatomy of a Web3 Scam”. https://forta.org/blog/anatomy-of-a-web3-scam/.

[5] “MetaMask”. https://metamask.io/.

[6] “”Deceptive site ahead” when trying to connect to a site”. https://support.metamask.io/hc/en-us/articles/4428045875483.

[7] “Cloudflare Turnstile, a free CAPTCHA replacement — Cloudflare”. https://www.cloudflare.com/products/turnstile/.

[8] “WhoisXML API”. https://www.whoisxmlapi.com/.

[9] S.S. Roy, D. Das, P. Bose, C. Kruegel, G. Vigna, and S. Nilizadeh, “Unveiling the risks of nft promotion scams,” 2023.

[10] Q. Yuan, B. Huang, J. Zhang, J. Wu, H. Zhang, and X. Zhang, “Detecting phishing scams on ethereum based on transaction records,” 2020 IEEE International Symposium on Circuits and Systems (ISCAS)IEEE, pp.1–5 2020.

[11] W. Chen, X. Guo, Z. Chen, Z. Zheng, and Y. Lu, “Phishing scam detection on ethereum: towards financial security for blockchain ecosystem,” Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20) Special Track on AI in FinTech, pp.4506–4512, 2020.

[12] B. He, Y. Chen, Z. Chen, X. Hu, Y. Hu, L. Wu, R. Chang, H. Wang, and Y. Zhou, “TxPhishScope: Towards detecting and understanding transaction-based phishing on Ethereum,” Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, pp.1–15, 2023.

[13] “eth-phishing-detect”. https://github.com/MetaMask/eth-phishing-detect.