表示画面情報を用いたテクニカルサポート詐欺サイトの軽量識別手法

堺 啓介[1,5]　竹重 耕介[2,5]　嶋村 誠[3]　松ヶ谷 新吾[3,4]　渡邊 泰司[4]　橋本 正樹[5,a)]

概要：本研究は，テクニカルサポート詐欺（TSS）の Web サイトを識別するために特に有効と考えられる表示画面情報を特徴量として，簡易かつ軽量な識別モデルを構築して実際の TSS 対策に活用可能な現実的な Web サイト識別技術の構築に寄与するとともに，識別した TSS サイトのドメイン，IP アドレス，SSL 証明書，ソース情報を合わせて収集，分析することにより TSS の犯罪手法を明らかとして安全・安心なインターネット社会の構築に寄与するものである．urlscan からデータを収集，学習，識別を行った結果 1,078 件の Web サイトデータに基づいて表示画面の画像分類を行い，誤判定なしに TSS サイトと非 TSS サイトを識別することが可能であることを確認した．識別した情報を分析したところ，TSS サイトにおいては Windows OS を標的とする TSS サイトが多く観察され，また Windows を提供する Microsoft 社のクラウド環境を利用した詐欺サイトが多いことが明らかとなった．

キーワード：テクニカルサポート詐欺，TSS，機械学習，urlScan

Lightweight Detection of Technical Support Scam Websites through Screenshot Analysis

Keisuke Sakai[1,5]　Kosuke Takeshige[2,5]　Makoto Shimamura[3]　Shingo Matsugaya[3,4]
Taiji Watanabe[4]　Masaki Hashimoto[5,a)]

Abstract: This research aims to contribute to the construction of a practical website identification technology that can be used for actual Technical Support Scam (TSS) countermeasures by constructing a simple and lightweight identification model using display screen information, which is considered to be particularly effective for identifying TSS websites, as a feature. It also aims to clarify the criminal methods of TSS by collecting and analyzing the domains, IP addresses, SSL certificates, and source information of identified TSS sites, thereby contributing to the construction of a safe and secure Internet society. As a result of collecting, learning, and identifying data from urlscan, it was confirmed that it was possible to classify display screen images based on 1,078 website data items and to distinguish TSS sites from non-TSS sites without false positives. Analysis of the identified information revealed that many TSS sites were observed targeting Windows OS, and that there was a significantly large number of scam sites using the Azure cloud environment.

Keywords: Technical Support Scam, TSS, Machine Learning, urlScan

1. はじめに

近年，インターネット利用者を狙った新たな詐欺手法として，テクニカルサポート詐欺（Technical Support Scam,

[1] 神奈川県警察本部 サイバーセキュリティ対策本部
Cyber Security Control Task Force, Kanagawa Prefectural Police Headquarters
[2] 千葉県警察本部 生活安全部 サイバー犯罪対策課
Cybercrime Division, Community Safety Department, Chiba Prefectural Police Headquarters
[3] トレンドマイクロ株式会社 Trend Micro, Inc.
[4] 日本サイバー犯罪対策センター
Japan Cybercrime Control Center
[5] 香川大学 創造工学部 電子・情報工学領域
Faculty of Engineering and Design, Kagawa University
[a)] hashimoto.masaki@kagawa-u.ac.jp

図 1　収集した代表的な警告画面例

Fig. 1　Representative warning screen examples collected.

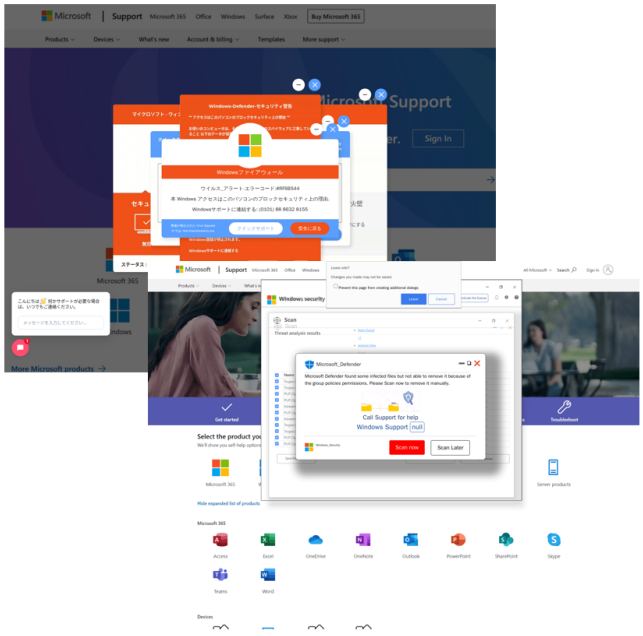
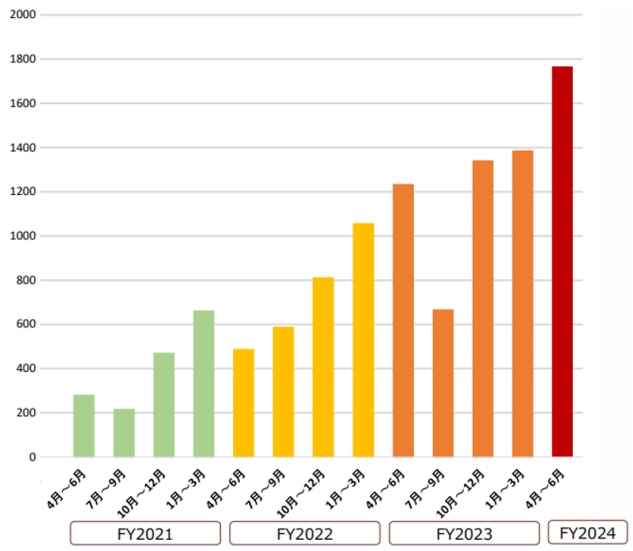


図 2　サポート詐欺の相談件数推移

Fig. 2　Trends in the number of support fraud inquiries.



以下 TSS）による被害が世界的に急増している．TSS は，偽のセキュリティ警告画面を通じて被害者を騙す多段階の攻撃手法である [1]．攻撃者は，突然表示される警告音付きの偽エラー画面（**図 1**）に Windows や Microsoft のロゴを配置し，正規のシステム警告と誤認させる．画面には緊急性を演出するメッセージと共にサポート窓口の電話番号が表示され，被害者が連絡すると詐欺師が遠隔操作ソフトのインストールを指示し，最終的に偽のサポート契約や料金支払いを要求する手法が用いられている．

TSS は世界中で観測されており，INTERNET CRIME COMPLAINT CENTER の報告では 3 番目に被害額が大きい犯罪として報告されている [2]．また，TSS は日本が最大の標的であり，リスク率は増加しているとも報告されており [3]，サポート詐欺相談件数も増加傾向にあると報告されている [4]（**図 2**）．

このような背景の元，情報処理推進機構（IPA）ではテクニカルサポート詐欺による被害状況を監視しており，攻撃手法の解説ページ [5] やサポート詐欺サイトの体験ページ [6] で詐欺ページからの離脱方法を公開する等の対策を進めているが，相談件数は今後も同水準で続くと予想している [4]．また，警察庁ではパソコンのウイルス除去をサポートするなどの名目で電子マネー等をだまし取る「サポート名目」は，認知件数 1,524 件，被害額は 10.0 億円 [7] と報告しているなか，JC3，警察庁，マイクロソフト，LAC が協力してインドで TSS の犯行グループを検挙する [8] といった産官学連携の取り組みが進められている．

本研究では，TSS サイトが被害者に正規のエラー画面と誤認させる必要があるという特性に着目し，表示画面情報を用いた軽量かつ実用的な識別手法の構築を目指す．従来の多特徴量を組み合わせた複雑なアプローチではなく，簡易な画像処理と機械学習により，リアルタイムでの大規模監視システムに適用可能な手法を提案する．

2.　関連研究

2.1　フィッシング・詐欺サイト検出の一般的手法

Web ベースの詐欺やフィッシング攻撃の検出に関する研究は長年にわたって行われており，様々なアプローチが提案されている．従来の手法は主に URL 特徴量，HTML コンテンツ解析，ネットワーク特徴量の 3 つのカテゴリに分類される．

URL 特徴量ベースの手法では，ドメイン名の長さ，サブドメインの数，特殊文字の使用頻度，既知の正規ドメインとの類似度などを特徴量として悪性サイトを検出する研究が報告されている．Xiang ら [9] は，HTML の DOM，検索エンジン，第三者サービスを活用した 8 つの新規特徴量を提案し，92%の真陽性率と 0.4%の偽陽性率を達成した包括的な特徴ベースアプローチ「CANTINA+」を提案している．これらの手法は軽量で高速な判定が可能である一方，攻撃者がドメイン名を巧妙に偽装した場合の検出精度に課題がある．

HTML コンテンツ解析による手法では，Web ページのソースコード内のリンク数，外部リソースへの参照，JavaScript の使用パターン，フォーム要素の特徴などを分析することで詐欺サイトを識別する．しかし，近年の詐欺サイトではコードの難読化やクローキング技術が用いられることが多く，静的解析による検出の限界が指摘されている．

Safi ら [10] による最新の包括的調査では，フィッシング検出技術の体系的なレビューが行われ，URL ベース，コンテンツベース，視覚的類似性，機械学習アプローチの研

究動向が分析されている．この調査により，TSS 検出手法開発に直接適用可能な研究ギャップが特定されている．

2.2 画像ベースの Web サイト分類手法

近年，Web サイトのスクリーンショット画像を用いた分類・検出手法が注目されている．この手法は，攻撃者がソースコードを難読化しても，エンドユーザーに表示される視覚的情報は改変できないという特性を活用している．

Abdelnabi ら [11] は，トリプレット CNN ベースの類似性フレームワーク「VisualPhishNet」を提案し，新しい視覚的外観を持つページにも汎化可能な Web サイトプロファイルの学習を実現した．この研究では，出版時点で最大の視覚的フィッシングデータセット「VisualPhish」も構築されており，視覚的特徴とコンテンツベース手法を橋渡しするアプローチを示している．

Lin ら [12] は，フィッシングサンプルでの訓練を必要としないロゴ認識とブランド変種マッチングに対処するハイブリッド深層学習アプローチ「Phishpedia」を提案した．この手法は 30 日間の展開で 1,704 の新しい実際のフィッシング Web サイトを発見し，スクリーンショット分析を通じた不正なテクニカルサポート Web サイトの識別に有効性を実証している．

Liu ら [13] は，CNN 分類を用いたセキュリティインジケータエリア（SIA）スクリーンショット分析を提案し，実世界の Web 環境をよりよく反映する不均衡データセットでの優れた性能を実証した．これは，正規サイトが詐欺サイトを大幅に上回る TSS 検出に直接適用可能である．

また，Yang ら [14] は深層畳み込みニューラルネットワークとランダムフォレストアンサンブル学習を組み合わせたフィッシング Web サイト検出手法を提案し，Li ら [15] は大規模言語モデルとマルチモーダル知識グラフを組み合わせた「KnowPhish」により，参照ベースのフィッシング検出の強化を実現している．

初期の視覚的類似性研究では，Wenyin ら [16] が Web ページスクリーンショット間の視覚的類似性評価に Earth Mover's Distance を用いる基礎的手法を確立し，89%の真陽性率と 0.71%の偽陽性率を達成している．

2.3 クラウド環境を悪用したサイバー攻撃

クラウドサービスの普及に伴い，これらの環境を悪用したサイバー攻撃が急速に増加している．特に，Amazon Web Services（AWS），Microsoft Azure, Google Cloud Platform（GCP）などの主要クラウドプロバイダが提供する無料枠やトライアルアカウントが攻撃者によって悪用される事例が多数報告されている．

Ho ら [17] は，1 億 1300 万通の電子メールを分析し，攻撃者が侵害された正規インフラストラクチャをフィッシングに活用する手法を明らかにした．この研究は，評判の良いクラウドプラットフォームでホストされる TSS サイトと類似した暗黙的信頼悪用パターンを実証しており，優秀論文賞を受賞している．

Liao ら [18] は，クラウド Web ホスティングサービス上のロングテール SEO スパムを特徴付ける初の包括的研究を実施し，主要クラウドサービス上で 318,470 のドアウェイページを特定した．この研究により，TSS 配布に関連する大規模悪意のあるキャンペーンを可能にするクラウドインフラストラクチャの悪用方法が明らかになっている．

Vasek ら [19] は，Web ホスティングプロバイダとの悪用データ共有の影響を測定し，正規のクラウドサービスを悪用した攻撃に対するエンドユーザー側での検出・防御技術開発の重要性を示している．

さらに，Gao ら [20] はコンテナクラウドの新たなセキュリティ脅威を明らかにし，Alqadhi ら [21] は無料コンテンツ Web のホスティングインフラストラクチャの統計分析により，クラウドプロバイダ全体での TSS Web サイト配布に不可欠な悪意のあるコンテンツのクラウドホスティングにおけるヘビーテール分布を実証している．

2.4 テクニカルサポート詐欺に特化した研究

TSS に特化した研究では，詐欺師が運営する数百の電話番号とドメインを自動検出するシステムを構築し，詐欺師と実際に連絡を取り合うことで TSS の実態解明を進めるとともに，ドメイン名と電話番号のブラックリストの網羅性が不十分であることが報告されている [22]．実際に詐欺師と連絡をとった研究例は他にもあり，実際にリモート接続でマシンを操作させた際にどのような行動を取るかの調査 [23] や X(旧 Twitter）上でテクニカルサポートリクエストのキーワードを含む独自の自動ツイートを投稿して詐欺師を誘い込むシステムを構築し，9,000 人以上の詐欺師の手口や送金先についての調査 [24] などが報告されている．

TSS の最大のターゲットである日本に着目した研究でも実際に詐欺師との通信を分析し，被害者を騙すために用いる手口や戦略を明らかにするとともに，日本を狙ったテクニカルサポート詐欺の攻撃者の拠点が特定の国に偏っていることや日本人被害者向けにカスタマイズされた攻撃マニュアルを用いて組織的な攻撃活動が行われていることが明らかになっている [25]．

TSS の判定に関する研究では，悪意のあるサイトと TSS サイトを各々約 8,000 サイトを収集し，42 の特徴を定義することで 100%に近い精度で AI（機械学習）が TSS サイトを判定するとともに，コードベースの特徴（リンク数、コメント、キーワード）が他の特徴よりも重要である [26] 等と報告する研究例や，SNS 上の TSS 詐欺師グループに潜入し，インドを拠点とする TSS グループが利用する TSS サイト情報を収集し，検索結果順位，バックリンク，ドメイン情報等のパラメータから AI（機械学習）で TSS サイ

トを高精度で判定した研究例 [27]，TSS の詐欺師に電話した内容を元に LLM で判定する研究例 [28] などが報告されている．

更に近年では URL や HTML のテキスト情報だけでなく，ウェブサイトのスクリーンショット画像からも情報を抽出して LLMs(GPT-4V) に判定することで偽ショッピング（英語，ドイツ語，日本語），テクニカルサポート詐欺（英語），仮想通貨詐欺（英語），投資詐欺（英語）の 4 種別・3 言語の詐欺サイトの高精度な判定を行い，識別根拠と共に出力する研究例 [29][30] が報告されている．

2.5 本研究の貢献

前述の関連研究により，Web ベースの詐欺サイト検出において多様なアプローチが提案されているが，それぞれに課題が存在する．一般的なフィッシング検出手法では，CANTINA+[9] のように 8 つの特徴量を組み合わせる包括的アプローチや，複数のデータソース（HTML DOM，検索エンジン，第三者サービス）を必要とする手法が主流である．画像ベースの手法においても，VisualPhishNet[11] のトリプレット CNN フレームワークや Phishpedia[12] のハイブリッド深層学習アプローチなど，高い検出精度を実現する一方で，複雑なモデル構築と大規模な計算資源を必要とする傾向にある．

また，近年の LLM ベースの手法 [29][30] では，GPT-4V 等の高性能モデルにより高精度な判定が実現されているが，課金要素が存在するため継続的な運用において経済的負担が課題となる．クラウド環境悪用に関する研究 [17][18] では攻撃者の手法解明に重点が置かれているものの，実用的な検出システムの提案は限定的である．

TSS 特化研究においても，Chen ら [26] の 42 特徴量を用いた手法や Liu ら [27] の多パラメータ解析など，高精度を追求する一方で複雑性が増大している．これらの手法は研究レベルでの有効性は実証されているが，実社会での継続的運用や大規模展開において，計算コストや実装の複雑さが障壁となる可能性がある．

本研究では，TSS サイトが被害者に正規のエラー画面と誤認させる必要があるという本質的特性に着目し，**表示画面情報が特に TSS 識別において決定的に有効である**という仮説に基づく．従来研究から判明している有効な特徴量のうち，視覚的情報に焦点を絞ることで，以下の独自性を有するアプローチを提案する：

(1) **極限的な軽量化**: グレースケール化，128 × 128px リサイズ，1 次元平坦化という極めてシンプルな前処理により，従来の複雑な画像解析手法と比較して大幅な計算コスト削減を実現する．

(2) **単一特徴量による高精度判定**: 複数特徴量の組み合わせに依存せず，表示画面のみで判定を行うことで，システムの簡素化と高速化を両立する．

(3) **実装可能性の重視**: 課金要素やクラウド API 依存を排除し，オープンソースライブラリのみで構築可能な現実的ソリューションを目指す．

(4) **TSS 特化最適化**: 一般的なフィッシングサイトではなく，Microsoft Azure を悪用した TSS サイトの特性に特化した検出手法を構築する．

(5) **産官学連携への適用性**: 実際の法執行機関や民間企業での運用を想定し，継続的監視システムとして実装可能な軽量性と信頼性を確保する．

本手法により，従来の高精度だが複雑な手法と，実用性を重視した軽量な手法との間のギャップを埋め，**リアルタイムでの大規模 TSS 検出システム**の実現を目指す．機械学習による特徴量抽出の知見を活用しつつも，最終的にはルールベースでの応用も視野に入れた段階的アプローチにより，より安全な Web 利用環境の実現に貢献することを目的とする．

3. データ収集と分類

3.1 データ収集

TSS サイトのデータを収集するにあたり，検索クエリ「country:”JP”」で 1 週間ほど手動でデータを確認した結果から TSS サイトを観測できたドメインについて着目し，以下のクエリで令和 7 年 3 月 30 日から同年 5 月 27 日までの間で定期観測を行い，ドメイン，IP アドレス，SSL 証明書，表示画面，ソース情報を 1,078 件収集した．

- windows.net AND date:>now-3d AND country:”JP”
- amazonaws.com AND date:>now-3d AND country:”JP”
- netlify.app AND date:>now-3d AND country:”JP”
- pages.dev AND date:>now-3d AND country:”JP”
- amplifyapp.com AND date:>now-3d AND country:”JP”

具体的には urlscan.io API v1[31] でクエリ条件に該当する uuid, url, domain, apexDomain, ip tlsIssuer tlsValidDays, country, asn, asnname, country，server, ip, title, url, tlsValidDays, screenshot を確認し（**図 3**），表示画面は screenshot の URL，ウェブサイトのソースは uuid から確認できる対象ページから HTTP transactions ページの情報を収集した．

3.2 データ分類

データ収集を行う前段階で URLScan から手動で収集した，非 TSS サイト 364 件と TSS サイト 151 件の画像を

- グレースケール化
- 128*128px にリサイズ
- 1 次元に平坦化

し，画像分類の機械学習モデル構築で使われる PyCaret という AutoML で判定用モデルを構築した。（**表 1**）．

表 1　PyCaret の実行結果
Table 1　Result of PyCaret

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT(Sec)
RandomForestClassifier	0.9832	0.9970	0.9809	0.9627	0.9714	0.9595	0.9599	1.661
AdaBoostClassifier	0.9832	0.9934	0.9718	0.9718	0.9705	0.9588	0.9600	6.208
ExtraTreesClassifier	0.9832	0.9961	0.9809	0.9627	0.9714	0.9595	0.9599	1.620
ExtremeGradientBoosting	0.9804	0.9958	0.9718	0.9618	0.9662	0.9524	0.9530	7.443
LightGradientBoostingMachine	0.9776	0.9973	0.9718	0.9527	0.9614	0.9457	0.9465	9.545
QuadraticDiscriminantAnalysis	0.9692	0.9797	0.9318	0.9598	0.9451	0.9237	0.9244	2.506
DecisionTreeClassifier	0.9554	0.9573	0.9618	0.8966	0.9271	0.8951	0.8972	1.945
LogisticRegression	0.9525	0.9812	0.9900	0.8720	0.9252	0.8909	0.8967	4.268
KneighborsClassifier	0.9415	0.9834	0.9345	0.8821	0.9027	0.8613	0.8668	1.593
LinearDiscriminantAnalysis	0.9220	0.9540	0.9818	0.8108	0.8838	0.8272	0.8400	2.635
NaiveBayes	0.9137	0.8589	0.7245	0.9778	0.8274	0.7721	0.7912	1.631
SVM-LinearKernel	0.8971	0.9691	0.7600	0.8782	0.7851	0.7250	0.7460	1.605
RidgeClassifier	0.8358	0.8387	0.9609	0.6539	0.7757	0.6545	0.6877	1.593
DummyClassifier	0.7075	0.5000	0.0000	0.0000	0.0000	0.0000	0.0000	2.133
CatBoostClassifier	0.0972	0.0992	0.1000	0.0909	0.0952	0.0933	0.0935	71.966

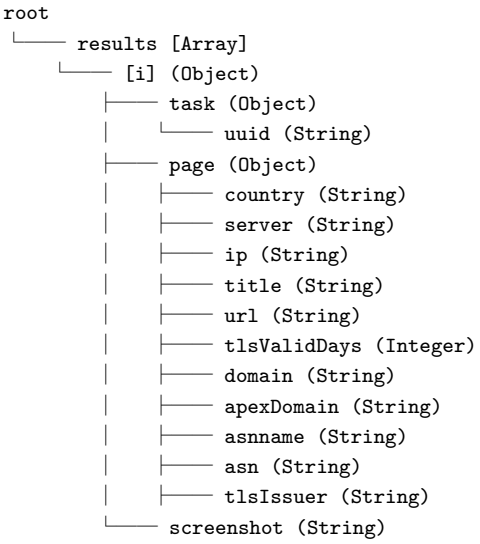


図 3　urlscan API v1 で取得したデータ（JSON）
Fig. 3　Data obtained by urlscan API v1 (JSON).

表 2　機械学習モデルの性能指標
Table 2　Performance of the machine learning models.

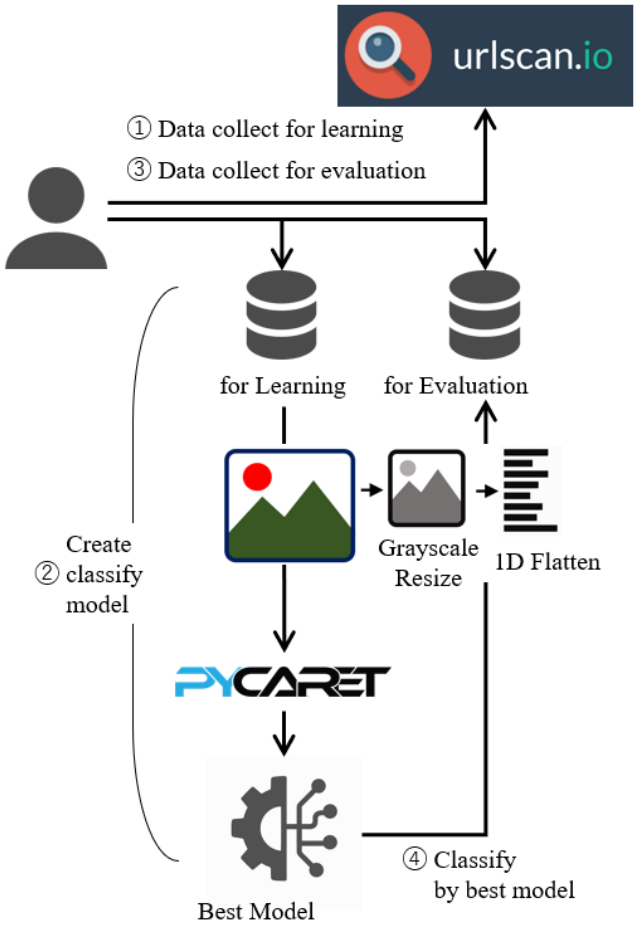
ACC	AUC	Recall	Prec.	F1	Kappa	MCC
0.983	0.997	0.981	0.963	0.971	0.960	0.960

構築した判定モデルから PyCaret の精度と学習時間のスコアを考慮した結果，RandomForestClassifier を選択し (**表 2**)，TSS 判定プログラムから収集したデータを判定した．本研究で行った評価フローを**図 4** に示す．

4.　データ分析

収集した 1,078 件のウェブサイトデータについて表示画面に基づいて分類を行ったところ，TSS サイト 155 件と非 TSS サイト 923 件に分類され，結果を目視で判定したところ誤判定は 1 件もなく，収集したデータの範囲においては誤判定は発生せず，100%の判定精度が確認できた．また，

図 4　本研究の評価フロー
Fig. 4　Evaluation flow of this research.

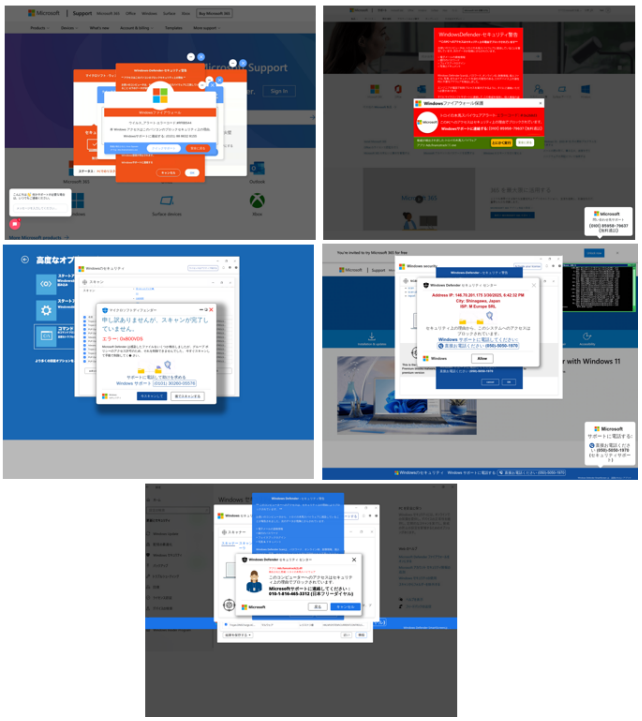


判定した TSS サイトは 154 件が WindowsOS を模倣したサイトで 1 件が MacOS を模倣したウェブサイトであることを目視で確認した．

MacOS を対象した TSS サイト (**図 5**) では JavaScript で「if (lang == ”fr”) 」等の分岐でドイツ語, ギリシャ語, スペイン語, フランス語, イタリア語, 日本語, オランダ語,

図 5　MacOS を対象とした TSS サイトの画面例
Fig. 5　Example of a TSS site for MacOS.

図 6　WindowsOS を対象とした TSS サイトの画面例
Fig. 6　Example of a TSS site for WindowsOS.



ポーランド語, ポルトガル語, ロシア語, スウェーデン語, トルコ語の 12 か国語に対応されており，同様の多言語に対応しているサイトは他に確認できなかった．また WindosOS を対象とした TSS サイトはエラーメッセージ部分の色調と背景部分の表示内容で区分したところ，5 パターンの TSS サイトが確認できた (**図 6**).

Apex domain は TSS サイトは全て windows.net であったが，非 TSS サイトでは windows.net, amazon.com, pages.dev, weebly.com 等の 703 種類を確認した．

urlscan の APIv1 で確認したサーバ情報において，TSS サイトは Windows-Azure-Web が 92 件，Windows-Azure-Blob が 63 件の 2 種類であったが，非 TSS サイトは AmazonS3, Apache, Github.com, Google Frontend, Nginx 等の 54 種類を確認し，asnname において TSS サイトは全て MICROSOFT-CORP-MSN-AS-BLOCK US であったが，非 TSS サイトは CLOUDFLARENET US, AMAZON-02 US, MICROSOFT-CORP-MSN-AS-BLOCK US, AKAMAI-ASN1 Akamai International B.V. NL, IIJ Internet Initiative Japan Inc. JP 等の 59 種類を確認した (**表 3**).

5.　考察

5.1　TSS の手口に関する推論

本研究で収集した TSS サイトの環境は，すべて Microsoft Azure のクラウド環境であった．これは，

- Microsoft Azure の無料枠 [32][33] 等を活用することで，インフラの費用をかけずに TSS サイトを構築できるため
- Microsoft のサービスを悪用することで，Microsoft 社の警告画面と誤認される可能性を高める（ドメイン情報や SSL 証明書情報から TSS サイトか判定できなくする）ため

といったことが要因と推測される．

また，URLScan で登録されたデータに基づき，実際に収集したデータを確認しようとしたが，いずれの項目についてもデータを得ることができなかった．これは，犯罪に使用される環境が使い捨てであることに加えて，サーバを必要なときにだけ起動させることができるクラウドの利便性が悪用されている可能性が示唆される．

5.2　本手法の限界

本研究では，使用したデータソースが URLScan に限られており，またデータ収集に用いたクエリも，事前調査に基づき収集された TSS サイトに限られている．このため調査対象となる TSS サイトに偏りがある可能性が否定できないが，現時点で可能な範囲で収集を行ったものである．

また，本研究で収集した Web サイトの判定では誤判定なく 100%の精度で判定に成功したが，TSS サイトの表示画面のパターン数が少ないことから高精度な判定となった可能性がありパターンが増えた場合には識別精度が低下する可能性がある．これに対しては，今後の課題として，TSS サイトへ誘導する手法を把握し，様々な表示画面パターンにおいても高精度な判定ができるか検証する必要性がある．

6.　おわりに

6.1　まとめ

本研究では，表示画面情報を特徴量とした軽量な TSS 識別手法を提案し，1,078 件の Web サイトデータに対して 100%の識別精度を達成した．

従来研究と比較して，本手法は以下の優位性を実証した：

表 3　収集データの分類
Table 3　Classification of collected data

site	Apexdomain	ASN name	Server information
TSS site	windows.net	MICROSOFT-CORP-MSN-AS-BLOCK, US	Windows-Azure-Web Windows-Azure-Blob
not TSS site	703 types	59 types	54 types

(1) **極限的な軽量化**：CANTINA+[9] の 8 特徴量や Chen ら [26] の 42 特徴量と比較し，単一の画像特徴量のみで高精度を実現
(2) **実装可能性**：LLM ベースの手法 [29] と異なり，課金要素なしでの継続運用が可能
(3) **TSS 特化最適化**：Microsoft Azure 悪用という実際の攻撃パターンに対応した実践的アプローチ

さらに，収集した TSS サイトの分析により，犯罪者が Microsoft Azure の無料枠とブランド信頼性を組み合わせて悪用する手口を明らかにした．

6.2　今後の課題

本研究で構築した手法は，収集したデータの範囲において高い識別精度を示したが，より包括的な TSS 対策の実現に向けて複数の課題が残されている．

まず，TSS サイトへの誘導手法の調査が重要である．ドメインパーキングと広告が悪用されているという報告はあるものの，現時点で体系的な研究が少なく，今後の調査が必要である．最近の TSS 誘導では Web 広告（Google 広告）を通じた事例が報告されており [34]，YouTube 広告などの動画広告は Google アカウントさえあれば出稿が可能である．広告掲載による費用が発生する条件 [35] が動画広告が 30 秒以上または最後まで再生された場合，自動再生された動画が 10 秒以上視聴された場合，広告がクリックされた場合等と限定的であることから，攻撃者にとって犯罪のビジネスモデルとして成立する範囲の費用となっており，TSS などの詐欺サイトへと効率的に誘導できる構造が形成されていると考えられる．Ho ら [17] が示したラテラルフィッシングのような手法と同様に，広告プラットフォームを悪用した TSS 誘導の実態について，より包括的かつ系統的な調査が課題である．

次に，技術的な課題として，収集されたソース情報については，難読化やクローキングといった手法により分析が阻害されており，技術的障害に対処する手法の研究も課題である．これは，従来の HTML コンテンツ解析による手法の限界を示しており，本研究で提案した表示画面情報に基づく手法の有効性を裏付けている．しかし，攻撃者が視覚的偽装技術を高度化させた場合への対応として，Abdelnabi ら [11] のような複数の視覚的特徴を組み合わせたアプローチとの統合も検討が必要である．

さらに，データ収集体制の強化も重要な課題である．URLScan などの既存サービスに依存することなく，よりリアルな被害データの収集体制を強化する必要があり，信頼性の高い生データを収集・分析することで，現実に即した情報を収集して詐欺行為の早期検出や対処精度の向上を図りたい．Liao ら [18] が示したクラウド悪用パターンを踏まえた予防的検出システムの構築や，Thomas ら [19] が提案するホスティングプロバイダとの情報共有体制の確立も，実用的な TSS 対策システム実現に向けて重要である．

最後に，産官学連携による社会実装において，リアルタイム監視システムの構築，法執行機関との情報共有体制，クラウドプロバイダとの連携体制の確立が求められる．本研究で明らかになった Microsoft Azure 悪用の実態を踏まえ，クラウドプロバイダ側での予防的対策と，エンドユーザー側での検出・防御技術の両輪による包括的な TSS 対策の実現を目指したい．

参考文献

[1] トレンドマイクロ株式会社. 偽のセキュリティ警告画面や警告音を出すサポート詐欺の手口と対処方法. https://helpcenter.trendmicro.com/ja-jp/article/tmka-12006.
[2] INTERNET CRIME COMPLAINT CENTER. Internet crime report 2024. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
[3] Gen Digital Inc. Gen q4/2024 threat report. https://www.gendigital.com/blog/insights/reports/threat-report-q4-2024.
[4] 独立行政法人情報処理推進機構. Ipa「サポート詐欺レポート」2024. https://www.ipa.go.jp/security/anshin/measures/f55m8k00000047km-att/supportscam_report2024.pdf.
[5] 独立行政法人情報処理推進機構. パソコンに偽のウイルス感染警告を表示させるサポート詐欺に注意-「今すぐ○○に電話してください」は偽物、絶対に電話をしないで！-. https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20241119.html.
[6] 独立行政法人情報処理推進機構. 偽セキュリティ警告（サポート詐欺）画面の閉じ方体験サイト. https://www.ipa.go.jp/security/anshin/measures/fakealert.html.
[7] 警察庁組織犯罪対策部. 令和６年における特殊詐欺及びＳＮＳ型投資・ロマンス詐欺の認知・検挙状況等について（確定値版）. https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2024.pdf.
[8] 日本サイバー犯罪対策センター. テクニカルサポート詐欺に対する jc3、株式会社ラック、マイクロソフト及び法執行機関の取. https://www.jc3.or.jp/news/2025/20250530-621.html.
[9] Guang Xiang, Jason Hong, Carolyn Penstein Rose, and Lorrie Cranor. Cantina+: A feature-rich machine

learning framework for detecting phishing web sites. *ACM Transactions on Information and System Security (TISSEC)*, Vol. 14, No. 2, pp. 1–28, 2011.

[10] Asadullah Safi and Satwinder Singh. A systematic literature review on phishing website detection techniques. *Journal of King Saud University-Computer and Information Sciences*, Vol. 35, No. 2, pp. 590–611, 2023.

[11] Sahar Abdelnabi, Katharina Krombholz, and Mario Fritz. Visualphishnet: Zero-day phishing website detection by visual similarity. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1681–1698, 2020.

[12] Yun Lin, Ruofan Liu, Dinil Mon Divakaran, Jun Yang Ng, Qing Zhou Chan, Yiwen Lu, Yuxuan Si, Fan Zhang, and Jin Song Dong. Phishpedia: A hybrid deep learning based approach to visually identify phishing webpages. In *30th USENIX Security Symposium (USENIX Security 21)*, pp. 3793–3810, 2021.

[13] Dong-Jie Liu and Jong-Hyouk Lee. A cnn-based sia screenshot method to visually identify phishing websites. *Journal of Network and Systems Management*, Vol. 32, No. 1, pp. 1–24, 2024.

[14] Wenqiang Yang, Weidong Zuo, and Bin Cui. Phishing website detection based on deep convolutional neural network and random forest ensemble learning. *Sensors*, Vol. 21, No. 24, p. 8281, 2021.

[15] Yuexin Li, et al. Knowphish: Large language models meet multimodal knowledge graphs for enhancing reference-based phishing detection. In *33rd USENIX Security Symposium (USENIX Security 24)*, 2024.

[16] Liu Wenyin, Guanglin Huang, Liu Xiaoyue, Zhang Min, and Xiaotie Deng. Detection of phishing web pages based on visual similarity. *Special interest tracks and posters of the 15th international conference on World Wide Web*, pp. 1060–1061, 2005.

[17] Grant Ho, Asaf Cidon, Lior Gavish, Marco Schweighauser, Vern Paxson, Stefan Savage, Geoffrey M Voelker, and David Wagner. Detecting and characterizing lateral phishing at scale. In *28th USENIX Security Symposium (USENIX Security 19)*, pp. 1273–1290, 2019.

[18] Xiaojing Liao, Chang Liu, Damon McCoy, Elaine Shi, Shuang Hao, and Raheem Beyah. Characterizing long-tail seo spam on cloud web hosting services. In *Proceedings of the 25th international conference on world wide web*, pp. 321–332, 2016.

[19] Marie Vasek, Matthew Weeden, and Tyler Moore. Measuring the impact of sharing abuse data with web hosting providers. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pp. 71–80, 2016.

[20] Xing Gao, Zhongshu Gu, Mehmet Kayaalp, Dimitrios Pendarakis, and Haining Wang. Containerleaks: Emerging security threats of information leakages in container clouds. In *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 237–248. IEEE, 2017.

[21] Mohammed Alqadhi, Motasem Alkinoon, Jeman Lin, Ahmed Abdulal, and David Mohaisen. Entangled clouds: Measuring the hosting infrastructure of the free contents web. In *Proceedings of the 2023 on Cloud Computing Security Workshop*, pp. 81–92, 2023.

[22] Najmeh Miramirkhani, Oleksii Starov, and Nick Nikiforakis. Dial one for scam: A large-scale analysis of technical support scams. In *Proceedings 2017 Network and Distributed System Security Symposium*. Internet Society, 2017.

[23] Sampsa Rauti and Ville Leppänen. “you have a potential hacker’s infection”: A study on technical support scams. *2017 IEEE International Conference on Computer and Information Technology (CIT)*, pp. 197–203, 2017.

[24] Bhupendra Acharya, Muhammad Saad, Antonio Emanuele Cinà, Lea Schönherr, Hoang Dai Nguyen, Adam Oest, Phani Vadrevu, and Thorsten Holz. Conning the crypto conman: End-to-end analysis of cryptocurrency-based technical support scams. In *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 17–35. IEEE, 2024.

[25] Ayumu Yamada, Hiroyuki Ito, Kosuke Kajimoto, Tetsuya Kageyama, Taichi Aoki, and Takahiro Kasama. Threat of technical support scams in japan. *2024 IEEE Conference on Dependable and Secure Computing (DSC)*, pp. 115–122, 2024.

[26] Ai@tss- intelligent technical support scam detection system. *Journal of Information Security and Applications*, Vol. 61, p. 102921, 2021.

[27] Jienan Liu, Pooja Pun, Phani Vadrevu, and Roberto Perdisci. Understanding, measuring, and detecting modern technical support scams. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, pp. 18–38, 2023.

[28] Poh Yi Jie Nicholas and Pai Chet Ng. Scamdetector: Leveraging fine-tuned language models for improved fraudulent call detection. In *TENCON 2024-2024 IEEE Region 10 Conference (TENCON)*, pp. 422–425. IEEE, 2024.

[29] 中野, 小出, 千葉駿, 大紀. 大規模言語モデルを用いた自律型詐欺サイト分析システム. コンピュータセキュリティシンポジウム 2024 論文集, pp. 1056–1063, 2024.

[30] Hiroki Nakano, Takashi Koide, and Daiki Chiba. Scamferret: Detecting scam websites autonomously with large language models. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 3–25. Springer, 2025.

[31] urlscan GmbH. urlscan.io api v1. https://urlscan.io/docs/api/.

[32] Microsoft Corporation. Create your azure free account today. https://azure-int.microsoft.com/en-us/free/.

[33] Microsoft Corporation. Static web apps の価格. https://azure.microsoft.com/ja-jp/pricing/details/app-service/static/.

[34] トレンドマイクロ株式会社. サポート詐欺の被害が拡大中–偽のセキュリティ警告にご注意ください. https://news.trendmicro.com/ja-jp/article-supportscam-overview/.

[35] Google LLC. Google 広告ヘルプ 動画広告フォーマットの概要. https://support.google.com/google-ads/answer/2375464.