Computer Security Symposium 2021
26 - 29 October 2021

安物に悪者が出る: 構築コストに基づく悪性ウェブサイト検知手法

伊藤 大貴[1,a)]　高田 雄太[1]　神薗 雅紀[1]

概要：悪性ウェブサイトは検知や対策から逃れるため，使い捨ての運用が行われることが多い．そのため，悪性ウェブサイトでは無料のドメイン名や証明書が使用される等ウェブサイトの構築にかけるコストが低くなると考えられる．そこで本稿では，ウェブサイトの構築コストに着目し，構築コストが低いウェブサイトを識別する手法を提案する．具体的には，対象サイトをドメイン名や DNS リソースレコード，証明書，インフラの 4 つの観点で分析し，機械学習によりその構築コストの高さを識別する．提案手法の評価には，従業員規模の異なる様々な企業のコーポレートサイトを使用するとともに，フィッシング，マルウェアホスト，フェイクニュースの三種類の悪性ウェブサイトを使用する．評価の結果，攻撃の種類やコンテンツに依存せず，8 割以上の精度で悪性ウェブサイトの構築コストを低いと識別できた．識別結果の分析により，攻撃の種類によって識別における特徴量の重要度が異なり，さらにその違いは各攻撃の特性に関連していることを示す．

キーワード：使い捨てウェブサイト，機械学習，フィッシング，マルウェア，フェイクニュース

Detection Method of Malicious Websites based on Building Cost

Daiki Ito[1,a)]　Yuta Takata[1]　Masaki Kamizono[1]

Abstract: Malicious websites tend to be disposable to evade our detection and analysis. Therefore, these websites utilize free domain names and certificates, and the building cost of websites is kept low. In this paper, we focus on the building cost and propose a method for classifying websites built with low cost. More precisely, our method analyzes target websites from the four perspectives of domain names, DNS resource records, certificates, and infrastructures, and classifies their cost using a machine learning. In our evaluation, we use various corporate websites of different employee scale and three types of malicious website: phishing, malware hosting, and fake news. Our evaluation shows the proposed method could classify the cost of over 80% malicious websites is low regardless of the attack types. We found that importance of features in classification differs depending on the type of attack, and we show the differences are related to each attack characteristic.

Keywords: Disposable Website, Machine Learning, Phishing, Malware, Fake News

1. はじめに

サイバー攻撃におけるウェブサイトは，重要な役割を果たしている．ウェブサイトを利用する攻撃の一つにフィッシング攻撃がある．フィッシングサイトは，正規のウェブサイトとほぼ同一のコンテンツや証明書を利用することによって，視覚的な信頼をユーザに抱かせ，認証情報やクレジットカード番号など個人情報の入力に誘導し窃取する．また，サイバー攻撃に用いられるマルウェアを保存するストレージとして，ウェブサイトが使用されることも多い．例えば，マルウェアホストサイトから異なるマルウェアをダウンロードし，ユーザ端末にインストールさせるドロッパーがある．これら典型的なサイバー攻撃のほか，近年で

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

はプロパガンダを目的としたフェイクニュースの拡散にもウェブサイトが利用されている．偽の情報やデマを配信するニュースサイトや情報サイトの記事が，SNS などを通じて拡散され，社会に多大な影響を与えている．

このような悪性ウェブサイトは，検知や対策から逃れるため使い捨ての運用が行われることが多い．そのため，攻撃者は安価または無料のサービスを利用して悪性ウェブサイトを構築する傾向にある．一方，企業組織が運用する正規のウェブサイトは，ユーザからの信頼獲得やセキュリティの向上，安定的な稼働のため，コストをかけてウェブサイトを構築している．すなわち，悪性ウェブサイトと正規ウェブサイトの間には，その構築コストに差があると考えられる．

そこで本稿では，ウェブサイトの構築コストに着目し，構築コストが低いウェブサイトを識別する手法を提案する．具体的には，対象サイトの FQDN をドメイン名や DNS リソースレコード，証明書，インフラの 4 つの観点で分析し，機械学習によりその構築コストの高さを識別する．既存手法の多くはウェブサイトのコンテンツや URL に含まれる悪性ウェブサイト特有の特徴を採用しているが，ウェブサイトの構築コストを特徴量とした手法は我々の知るところではまだ存在しない．提案手法の評価には，構築コストの低い正規ウェブサイトの存在も考慮し，従業員規模の異なる様々な企業のコーポレートサイトを使用するとともに，フィッシング，マルウェアホスト，フェイクニュースの三種類の悪性ウェブサイトを使用する．本稿の貢献は以下のとおりである．

- FQDN を構築コストの観点で分析し，対象ウェブサイトの構築コストの高低を識別する手法を提案する．
- 提案手法が攻撃の種類やコンテンツに依存せず，8 割以上の精度で悪性ウェブサイトを識別できることを示す．
- 識別結果を分析し，攻撃の種類によって識別における特徴量の重要度が異なり、さらにその違いは各攻撃の特性に関連があることを示す．具体的には，フィッシングサイトは正規サイトを装いユーザを騙すための証明書コストの特徴量が重要であり，マルウェアホストサイトは共用サーバに関連するインフラコストの特徴量が重要であることを示す．また，フェイクニュースサイトは多くのユーザにニュースを拡散する特性上，可用性に関連する特徴量が重要であることを示す．

2. 関連研究

機械学習を用いて，フィッシングサイトと正規サイトを識別する手法がいくつか提案されている [1], [2], [3]．これらの手法は，ウェブサイトのコンテンツや URL などに含まれる特徴を機械学習に用いている．そのほか，ブラックリストに掲載された悪性 URL のうち，攻撃者によって侵害された正規のドメイン名と悪意を持って登録されたドメイン名を識別する手法も提案されている [4], [5]．これらの研究は，フィッシングサイトだけでなくマルウェアホストサイトも対象としており，コンテンツや証明書，サードパーティのデータなど，様々な特徴を識別に採用している．上述の研究はいずれも，悪性サイトに特有な特徴に基づいてそれらを識別する手法であり，ウェブサイトの構築コストの高さを識別する我々の手法とは異なる．証明書のコストを特徴量として採用している既存手法も存在するものの [4]，ウェブサイトの構築コストを特徴量とする方法を検討したり，それを悪性サイトの識別に応用したりする研究は我々の知るところではまだ存在しない．

フェイクニュースを検知する手法は，手動による識別と機械学習を用いた識別が提案されている．手動による識別の研究は，PolitiFact[6] や Gossip Cop[7] などがあり，これら研究プロジェクトのウェブサイトには専門家によるファクトチェックの結果が公開されている．フェイクニュースの識別手法として，ニュース記事のテキストに基づくアプローチ [8] や，フェイクニュースを伝搬させるユーザやニュース記事を掲載するメディアなどのコンテキストに基づくアプローチ [9] が提案されている．しかしながらいずれの研究も，ウェブサイトの構築コストには着目しておらず，我々の研究が初の試みとなる．

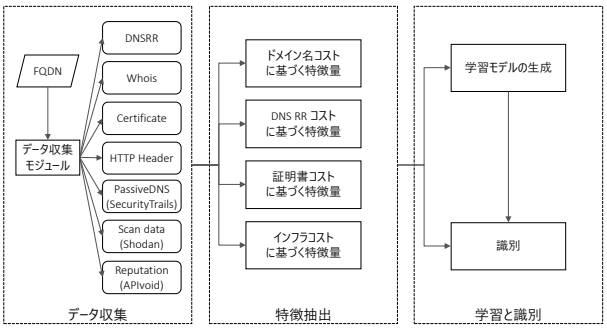

図 1 提案手法のプロセス

3. 提案手法

提案手法は，図 1 に示すデータ収集，特徴抽出，学習と識別の三つのフェーズで構成される．

3.1 データ収集

データ収集フェーズでは，対象ウェブサイトの FQDN に関連するデータ，およびその IP アドレスに関連するデータを収集する．

FQDN に関連するデータ．対象 FQDN の DNS リソースレコード，Whois 情報，証明書情報，HTTP レスポンスヘッダ，レピュテーションに関する情報を収集する．DNS リソースレコードは，A，CNAME，NS，MX，AAAA，SOA，TXT，DMARC，RRSIG の 9 種類のレコードを対

象に収集する．レピュテーションに関する情報の収集には，APIVoid [10] や McAfee 社が公開する TLD (Top Level Domain) ランキング情報 [11] を使用する．APIVoid より提供されるデータには，複数のドメイン名ブラックリストの検知結果のほか，ドメイン名の Alexa ランクや無料登録サービスの利用有無に関する情報も含まれる．McAfee 社が公開するランキングには，106 件の TLD におけるリスクを評価した結果が掲載されている．

IP アドレス に関連するデータ．対象 IP アドレスの Passive DNS のデータ，スキャンデータ，レピュテーションに関する情報を収集する．Passive DNS のデータ収集には，SecurityTrails [12] を使用する．SecurityTrails は，10 億を超える Passive DNS のデータを提供している．スキャンデータの収集には，Shodan [13] のデータを使用する．Shodan は，月に一度 IPv4 アドレス空間全体をスキャンし， その結果を提供している．Shodan より提供されるデータには，開放ポート，および稼働サービスの情報のほか，既知脆弱性の有無に関する情報も含まれる．レピュテーションに関する情報の収集には，FQDN と同様，APIVoid を使用する．APIVoid より提供されるデータには，複数の IP アドレスブラックリストの検知結果のほか，IP アドレスのカテゴリ (ホスティングサービスや VPN など) に関する情報も含まれる．

3.2 特徴抽出

特徴抽出フェーズでは，収集したデータをコストの観点で分析し，特徴量を算出する．分析は，ドメイン名，DNS リソースレコード，証明書，インフラの 4 つの観点で行う．

3.2.1 ドメイン名

ドメイン名の分析では，対象 FQDN のドメイン名[*1] を対象に以下 5 つの項目について分析する．

悪用されやすい TLD．対象ドメイン名の TLD が悪用されやすい TLD か調査する．各ブラックリストプロジェクトが公開するリスト [14], [15], および McAfee 社の TLD ランキング情報のうち，TLD のリスク比率が 3.0% 以上に該当する TLD を悪用されやすい TLD とする．悪用されやすい TLD は，攻撃に頻繁に利用される傾向にあることを意味しており，該当する TLD のドメイン名は比較的容易に取得可能であるといえる．つまり，取得の際の金銭的コストや手続き等にかかる手間が少ないと考えられる．

安全な TLD．TLD ランキング情報を用いて対象ドメイン名の TLD が安全な TLD かどうかを調査する．このとき，TLD のリスク比率が 1.0% 未満に該当する TLD を安全な TLD とする．安全な TLD は，攻撃に利用されることが少ないことを意味しており，取得の際の金銭的コストや手続き等にかかる手間が大きいと考えられる．

ドメイン名の運用年数．Whois 情報に含まれる登録日をもとにドメイン名の運用年数を算出し，運用年数が 10 年以上かどうかを調査する．ドメイン名の運用年数が長いほど，更新料などによる金銭的コストがより多く発生していると考えられる．Whois 情報が取得できない場合は，平均値を採用する．本稿では，コーポレートサイト，フィッシングサイト，マルウェアホストサイト，フェイクニュースサイトの 4 種類のウェブサイトを利用しており，その種類ごとに平均値を算出した．

Alexa ランク．対象ドメイン名が Alexa ランク上位 250,000 位以内に該当するかどうかを調査する．Alexa ランクが上位のドメイン名はアクセス数が多いことを意味する．そのため，当該ドメイン名を利用するウェブサイトは，可用性を高めるためのコストがかけられていると推測できる．

無料のドメイン名．APIVoid を用いて対象ドメイン名が無料で取得されたドメイン名に該当するかどうかを調査する．対象ドメイン名が無料で取得された場合，金銭的コストが低いことを意味する．

3.2.2 DNS リソースレコード

対象 FQDN またはそのドメイン名の DNS リソースレコードの設定状況を分析する．A, AAAA, CNAME, RRSIG レコードの分析は FQDN を対象とし，NS, MX, SPF, DMARC, SOA レコードの分析はドメイン名を対象とする．

A レコード．A レコードを分析し，IP アドレスが複数設定されているかを分析する．A レコードに複数の IP アドレスを設定することで，DNS ラウンドロビンによりサーバの負荷を分散することができる．この場合，ウェブサイトに対して複数のサーバが割り当てられていると考えられるため，設定されている IP アドレスが一つの場合に比べてコストが高いといえる．

NS レコード．3 件以上の NS レコードが設定されているかを分析する．NS レコードは，可用性を高めるため，複数設定されることが一般的である [16]．NS レコードのレコード数が多いほど，対象ドメイン名に対してより多くのネームサーバが割り当てられていると考えられるため，その数が多いほどコストが高いといえる．

その他のレコード．A および NS レコード以外の DNS リソースレコードの設定有無を分析する．設定されている DNS リソースレコードが多いほど，設定の更新等にかかる手間が増えるため，作業コストが高いといえる．例えば，MX レコードが設定されている場合，対応するメールサーバの運用も必要となる．CNAME レコードは，CDN などの外部サービスを利用する際に設定されることが多いが，そのようなサービスを利用していることが金銭面や運用面でコストがかかっていることを意味している．

[*1] ここでは，effective TLD (eTLD) +1 をドメイン名とする．

表 1　無料/格安証明書の Issuer のコモンネーム一覧

No.	Issuer CN
1	R3
2	Let's Encrypt Authority X3
3	cPanel Inc. Certification Authority
4	Encryption Everywhere DV TLS CA - G1
5	ZeroSSL RSA Domain Secure Site CA
6	Amazon
7	Go Daddy Secure Certificate Authority - G2
8	GTS CA 1D2
9	GTS CA 1O1
10	Microsoft IT TLS CA 1
11	Cloudflare Inc ECC CA-3
12	CloudFlare Inc ECC CA-2
13	COMODO RSA Domain Validation SecureServer CA
14	COMODO ECC Domain Validation SecureServer CA 2
15	RapidSSL RSA CA 2018
16	RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1
17	RapidSSL TLS RSA CA G1

3.2.3　証明書

証明書の分析では，以下 6 つの項目について分析する．

証明書の種類．証明書の種類が EV，OV，DV のいずれかに該当するかを分析する．一般的に EV，OV 証明書は，発行する際に厳密な審査行われ，価格も高い．一方，DV 証明書は比較的容易かつ安価に発行することができる．証明書の種類は，証明書のサブジェクトの項目に Business Category が含まれる場合は EV，証明書のサブジェクトの項目に 組織名が含まれるか場合は OV，EV と OV のいずれにも該当しない場合は DV と判定する．

証明書の検証エラー．証明書の検証エラーの発生有無を分析する．証明書の検証エラーが発生している場合，適切な管理や運用がされていないと考えられるため，運用コストが低いといえる．例えば，自己証明書や失効した証明書などの無効な証明書を利用している場合に，検証エラーが発生する．

無料/格安証明書の利用．発行者のコモンネーム（CN）の情報をもとに証明書が無料/格安かどうかを分析する．証明書を発行する認証局の中には，Let's Encrypt など，無料で証明書を発行する認証局が存在する [17], [18]．表 1 に無料/格安証明書と判定した発行者の CN 一覧を示す．

サブジェクト代替名の設定数．証明書のサブジェクト代替名に設定されている FQDN の数が 10 以上かどうかを分析する．多数の FQDN で証明書が使い回されている場合，FQDN 当たりの証明書コストは低くなる．

ワイルドカード証明書の利用．ワイルドカード証明書に該当するかを分析する．提案手法では，証明書のコモンネームやサブジェクト代替名に "∗" を含む FQDN が設定されている場合に，当該証明書をワイルドカード証明書と判定する．なお一部のサービスは，ワイルドカード証明書を無料で提供している [19], [20], [21].

証明書の有効期間．証明書の有効期間が 90 日以内かどうかを分析する．Let's Encrypt などの一部の無料証明書は有効期間が 90 日である [18], [19].

3.2.4　インフラ

インフラの分析では，以下 5 つの項目について分析する．

インフラ種別．IP アドレスのインフラ種別が，CDN，クラウド，ホスティングのいずれかに該当するかを分析する．提案手法では，既存研究 [22] の手法に則り，CDN やクラウドサービスが公開するドメイン名や IP アドレスの範囲情報に基づきその使用を判定した．また，ホスティングの判定には，APIVoid のデータに含まれる IP アドレスのカテゴリ情報を使用した．

Passive DNS．Passive DNS データを用いて，IP アドレスに設定されたドメイン名の数が 100 件以上であるかどうかを調査する．IP アドレスに対して多数のドメイン名が設定してある場合，当該 IP アドレスが比較的安価に利用できる共用サーバに割り当てられている可能性がある．

開放ポート数．スキャンデータを用いて，IP アドレスの開放ポート数が 10 以上であるかどうかを調査する．多数のポートが開放されている場合，当該 IP アドレス上ではウェブサーバやメールサーバ，DNS サーバ等の複数のサービスが稼働しているため，様々な用途に用いられる兼用サーバであると考えられる．この場合，ウェブサーバとしてのみ利用される IP アドレスと比較して，サービスあたりのインフラにかけるコストが低いと考えることができる．

脆弱性．スキャンデータを用いて，応答バナーから特定できる既知脆弱性を含むソフトウェアの利用有無を調査する．既知脆弱性を含むインフラが使用されている場合，定期的なソフトウェアのアップデートが実施されていないため，運用コストが低いと考えられる．

HTTP セキュリティヘッダ．対象の FQDN に対して HTTP リクエストを送信し，OWASP Secure Headers Project[23] に掲載されている HTTP セキュリティヘッダが設定されているか調査する．具体的には，`Content-Security-Policy`, `Strict-Transport-Security`, `X-Content-Type-Options`, `X-Frame-Options` 等の非推奨に該当しない 11 件のヘッダを分析する．これらのヘッダが設定されている場合，対象ウェブサーバはセキュアな運用がされているため，運用コストが高いと考えられる．

3.3　学習と識別

学習と識別フェーズでは，まず FQDN の構築コストの高さをラベル付けした学習用データセットを用いて，機械学習により識別モデルを構築する．機械学習のアルゴリズムには，ランダムフォレストを用いる．次に，構築したモデルを用いて，テスト用データセットに含まれる FQDN

の構築コストを識別する．

4. 評価

本評価では正規と悪性サイトの構築コストの差に着目し，ウェブサイトの構築コストの高さを識別できる提案手法を悪性サイトの識別に応用する．他の既存手法と異なり，提案手法は悪性サイト特有の特徴を使用していないため，攻撃種類の異なる様々な悪性サイトに適用できると考えられる．そこで本評価では，フィッシングサイト，マルウェアホストサイト，およびフェイクニュースサイトの三種類のデータを用いて，提案手法の識別性能を評価する．

4.1 データセット

フィッシング，マルウェアホスト，フェイクニュースの三種類の悪性サイトの FQDN を収集する．フィッシングサイトの FQDN 収集には，PhishTank [24] を利用した．PhishTank は，ユーザによって報告されたフィッシングサイトの疑いがある URL の情報を提供している．マルウェアホストサイトの FQDN 収集には，URLhaus [25] を利用した．URLhaus は，世界中のセキュリティアナリストや研究者の報告に基づくマルウェア配布に利用されている URL リストを提供している．フェイクニュースサイトの FQDN 収集には，FakeNewsNet データセット [26] を利用した．FakeNewNet データセットには，ファクトチェックサイトである Politifact および Gossip Cop によってフェイクと判定されたニュース記事の URL や，当該記事の URL を共有するツイートなどが含まれている．一方，正規ウェブサイトのデータセットには，D&B Hoovers [27] に登録されているコーポレートサイトの FQDN を利用した．D&B Hoovers は，企業の基本情報や財務情報などを提供するビジネスツールであり，1 億 8,000 万件を超える企業の情報を提供している．

2021 年 7 月に各データセットを取得した結果，フィッシングサイトは 2,380 件，マルウェアホストサイトは 1,857 件，フェイクニュースは 971 件，コーポレートサイトは 1,500 件の FQDN を収集できた．なお，コーポレートサイトについては，企業規模によってウェブサイトの構築にかけられるコストに差が出ると予想される．そこで本評価では，企業規模の差が結果にどのような影響をもたらすか評価するため，従業員数を基準[*2]とし，企業の従業員数ごとに均等に FQDN を収集した．

収集した FQDN の中には，ウェブサイトが稼働していないものが含まれる可能性がある．特に悪性サイトは，短命かつ使い捨てな運用が行われることが多いため，既にドメインパーキングにより管理されているドメイン名や HTTP コンテンツが空のウェブサイトが多く含まれる可能性がある．そこで本評価では，収集した FQDN のうち，以下の条件に当てはまるものは無効な FQDN と判定し，分析の対象外とした．

- HTTP body のサイズが 10 バイト未満である
- ドメインパーキングを利用している
- A レコードが設定されていない
- プライベート IP アドレスが設定されている
- IP アドレスに 100,000 件以上のドメイン名が設定されている
- HTTP ステータスコード 200 OK 以外を応答する
- 5 秒のタイムアウト等の理由によりアクセスに失敗する

最終的な分析対象 FQDN の選定結果を表 2 に示す．また，従業員数別のコーポレートサイトの分析対象 FQDN 選定結果内訳を表 3 に示す．表 2 より，フェイクニュースサイトは，ほかの悪性サイトと比較して無効な FQDN の数が少ないことが分かる．この理由は，FakeNewsNet はブラックリストではなく，SNS (Twitter や Facebook など) やニュースサイト (CNN や The New York Times) などの一般的なウェブサイトの URL も含んでいるからである．コーポレートサイトは，収集した FQDN のうち約 3 割が無効な FQDN と判定された．表 3 より，無効な FQDN の数は従業員規模が小さい企業で多いことが分かる．この結果から，規模が小さい企業より，規模が大きい企業ほどドメイン名の変更やウェブサイトの閉鎖などが少なく，安定してウェブサイトが稼働する傾向にあることが伺える．

表 2 分析対象の選定結果

データセット	収集 FQDN	無効な FQDN	分析対象
PhishTank	2,380	1,151	**1,229**
URLhaus	1,857	633	**1,224**
FakeNewsNet	971	203	**768**
D&B Hoovers	1,500	411	**1,089**

表 3 従業員数別の分析対象コーポレートサイトの FQDN 選定結果

従業員数	収集 FQDN	無効な FQDN	分析対象
100K 以上	300	46	254
10K 以上 100K 未満	300	61	239
1K 以上 10K 未満	300	76	224
100 以上 1K 未満	300	115	185
10 以上 100 未満	300	113	187
合計	1,500	411	1,089

4.2 モデルの構築

収集したデータセットから学習用データとテスト用データを作成し，機械学習を用いて識別モデルを構築する．まず，データセットに含まれる各 FQDN に対して 3.2 節に記載した特徴量をそれぞれ算出する．各悪性サイトとコーポレートサイトを組み合わせた 3 つのデータセットを作成し，それぞれ 7 対 3 の比率で学習用とテスト用データに分割した．なお，本評価では提案手法を悪性識別に応用して

[*2] 中小企業基本法では，資本金または従業員数で中小企業が定義されている (すなわち，企業規模が定義されている) [28].

表 4　ハイパーパラメータの探索結果

カテゴリ	決定木の数	特徴量の数
フィッシング	100	3
マルウェアホスト	180	3
フェイクニュース	80	2

表 5　識別結果

カテゴリ	Accuracy	Precision	Recall	F1-score
フィッシング	0.91	0.91	0.92	0.92
マルウェアホスト	0.87	0.87	0.90	0.88
フェイクニュース	0.80	0.80	0.71	0.75

いるため，構築コストの高さではなく悪性かどうかでラベル付けを行っている．次に，学習用データと機械学習を用いて，悪性サイトごとに合計 3 つの識別モデルを構築する．ランダムフォレストのハイパーパラメータである決定木の数と特徴量の数は，10 分割交差検証とグリッドサーチを用いてそれぞれ最適な値を求めた．なお，決定木の数は 10 から 500 までを 10 ずつ増加させ，特徴量の数は 1 から 39 を 1 ずつ増加させながら最適値を探索した．その探索結果を表 4 に示す．表 4 のとおり，サイトカテゴリによって異なる最適値となったため，以降の評価では各カテゴリの最適値をそれぞれの識別モデルに使用する．

4.3　モデルによる識別精度

前節で構築したモデルを用いて，三種類の悪性サイトの識別した結果を表 5 に示す．なお，評価指標は Accuracy, Precision, Recall, F1-score を採用した．表 5 の結果より，提案手法は攻撃の種類に関わらず 8 割以上の精度で悪性サイトを識別できることが分かる．フィッシングおよびマルウェアホストサイトは, 90%前後の精度で識別できたことから，これらと正規ウェブサイトとの間における構築コストの差は大きいと言える．一方，フェイクニュースサイトは，Accuracy，Precision の値は 80%であるものの， Recall, F1-score の値は 80% を下回る結果となり，他と比較すると精度は低かった．これは前述のとおり，FakeNewsNet データセットには悪性サイトだけでなく，一般的な SNS やニュースサイトも含まれていることが影響していると考えられる．

4.4　識別に有効な特徴量

三種類の悪性サイトの各モデルにおいて，識別に寄与した特徴量上位 10 件を表 6 に示す．

4.4.1　フィッシングサイト識別に有効な特徴量

表 6 から最も重要な特量量がドメインの登録年数であることが分かる．67% のコーポレートサイトが登録日から 10 年以上経過しているドメイン名を利用していたが，フィッシングサイトでは 約 11% しかなく，フィッシングサイトはコーポレートサイトに比べて短命のものが多いことが分かる．二番目に重要な特徴量は，CNAME レコードの設定有無であった．54%のコーポレートサイトが CNAME レコードを設定していたが，フィッシングサイトでは，11% しか設定していなかった．CNAME レコードの設定が必要な CDN 等の外部サービスが存在するが，比較的アクセス数が多いコーポレートサイトでは，そのような外部サービスの利用が多いと考えられる．

そのほかには，証明書の有効期間や無料/格安証明書の利用など，証明書コストに関連する特徴量が上位 10 件に含まれていた．フィッシングサイトでは，正規サイトを装いユーザを騙す必要性があることから，証明書の利用が多いと考えられる．実際に 80%以上のサイトが証明書を導入していた．一方で，攻撃者はウェブサイトの構築にコストをかけないため，証明書コストに関連する特徴が重要な特徴として表れたと考えられる．

4.4.2　マルウェアホストサイト識別に有効な特徴量

表 6 より，本識別においても，フィッシングサイトと同様にドメインの登録年数や CNAME の設定有無が重要な特徴量であることが分かる．登録日から 10 年以上経過しているドメイン名を使用したマルウェアホストサイトは 18%しかなく，フィッシングサイトと同様，短命かつ使い捨てで利用される傾向にあることがわかる．また，8%のマルウェアホストサイトでしか CNAME レコードは設定されておらず，CDN 等の外部サービスもほとんど利用されていないと考えられる．

マルウェアホストサイトにおける証明書に関連する特徴量の重要度は，フィッシングサイトと比較して低かった．前節で述べたとおり，フィッシングサイトはユーザを視覚的に騙す観点から，証明書の導入 (ブラウザ上にセキュアな接続を意味する鍵マークを表示すること) は重要である．一方で，マルウェアホストサイトは，必ずしもブラウザでウェブサイトにアクセスする必要はなく，ドロッパーなどのマルウェアがアクセスし，異なるマルウェアをダウンロードすることでも攻撃が成立する．したがって，マルウェアホストサイトの攻撃特性が関係して，証明書利用の重要性が低くなったと考えられる．

4.4.3　フェイクニュースサイト識別に有効な特徴量

表 6 から最も重要な特徴量は，ワイルドカード証明書であることが分かる．ワイルドカード証明書の利用は企業サイトで 22%，フェイクニュースサイトで 58%であり，フェイクニュースサイトでは半数以上がワイルドカード証明書を利用していた．これらの証明書を分析した結果，フェイクニュースサイトの多くが，Cloudflare や Croudfront などの CDN で提供される証明書を利用していたことが理由であることが分かった．これらのサービスでは無料でワイルドカード証明書を利用することができ，証明書へのコストを抑えていることが伺える．二番目に重要な特徴量は Alexa ランクであった．Alexa ランク Top 250K 以上のドメイン名はコーポレートサイトで 26%, フェイクニュース

表 6　識別に有効な特徴量トップ 10

順位	フィッシング	マルウェアホスト	フェイクニュース
1	ドメイン名の運用年数	ドメイン名の運用年数	ワイルドカード証明書の利用
2	CNAME レコード	CNAME レコード	Alexa ランク
3	MX レコード	開放ポート数	A レコード
4	証明書の有効期間	Passive DNS	CDN
5	開放ポート数	DMARC レコード	CNAME レコード
6	無料/格安証明書の利用	ホスティング	NS レコード
7	Passive DNS	NS レコード	無料/格安証明書
8	SPF レコード	X-Content-Type-Options	ドメイン名の運用年数
9	無料のドメイン名	X-Frame-Options	HTTP Strict Transport Security
10	DMARC レコード	証明書の有効期間	AAAA レコード

サイトで 63%であった．Alexa ランクはユーザのアクセス数に基づくランキングであるため，ユーザの注目を集めフェイクニュースを拡散する攻撃の特性上，コーポレートサイトよりも高くなったと考えられる．

そのほかの重要な特徴量は，A レコードの設定数や CDN の利用など，可用性向上に関連するものであった．実際に，複数の IP アドレスを設定したり，CDN を利用するウェブサイトはコーポレートサイトよりも多く，これらについてもフェイクニュースの攻撃の特性が関連していると考えられる．

5.　議論

5.1　悪性ウェブサイト見逃しの分析

悪性ウェブサイトのうち，正規ウェブサイトとして見逃した FQDN はフィッシングサイトが 29 件，マルウェアホストサイトが 37 件，フェイクニュースが 68 件であった．目視で確認した結果，これらの FQDN のうち，フィッシングサイトで 17 件，マルウェアホストサイトでは 25 件が正規ウェブサイトの FQDN であり，攻撃者によって侵害されていた．また，フェイクニュースサイトでは 36 件が運用年数 10 年以上のドメイン名を利用するニュースサイトであった．提案手法は構築コストを識別する手法であり，URL ではなく FQDN の粒度で対象を分析する．したがって，上記のように正規ウェブサイトが侵害された場合や正規のニュースサイトがフェイクニュースを発信した場合は，ウェブサイトの構築コストは高くなる傾向にあるため，正規ウェブサイトとして判定されたと考えられる．ウェブサイトの特定ページにおける URL は悪性であるが，FQDN は悪性ではないといった解釈となる．

5.2　正規ウェブサイト誤検知の分析

コーポレートサイトのうち，33 件がフィッシングサイト，50 件がマルウェアサイト，41 件がフェイクニュースと誤検知された．誤検知されたコーポレートサイトの従業員数別の内訳を図 2 に示す．従業員規模の小さい企業のウェブサイトの方が，フィッシングおよびマルウェアホストサイトとしてより多く誤検知されていることがわかる．

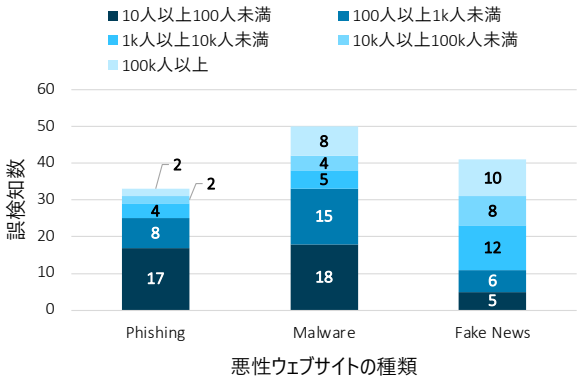

図 2　誤検知されたコーポレートサイト FQDN の従業員数別の内訳

このことから，提案手法は企業規模に関わらず一定の識別精度は出るものの，ウェブサイト構築への投資が後回しになっているであろう中小企業のコーポレートサイトに対しては，多少の誤検知が発生すると考えられる．また逆に，フェイクニュースサイト識別の観点では，企業規模が大きい企業のウェブサイトの方が多く誤検知されている．これら誤検知を分析した結果，フェイクニュースサイト識別で重要であった CDN および証明書に関連する特徴量が共通して一部の大企業のコーポレートサイトにも現れたことが原因であることがわかった．両ウェブサイトとも負荷分散のための CDN ならびに付随する無料証明書を活用している特徴が確認された．

5.3　悪性ウェブサイト検知のロバスト性

提案手法は，ウェブサイトの構築コストに関連する特徴に基づき，その高さを識別する．攻撃者が提案手法による検知を回避するためには，一般的なコーポレートサイトと同程度以上のコストをかけてウェブサイトを構築する必要がある．一方で，従来通りブラックリストによる検知等によりウェブサイトがテイクダウンされる可能性を踏まえると，攻撃者はコストを抑えた使い捨てのウェブサイトを運用せざるを得ない状況になると考える．すなわち，提案手法による検知の回避は，攻撃者の行動特性上，困難であると考えられる．

一方で，5.1 節で述べたとおり，侵害された正規ウェブサイトや踏み台に悪用された正規ウェブサイトは誤検知する可能性がある．これは，提案手法は URL ではなく FQDN の粒度でウェブサイトを分析しており，URL ごとに変化するコンテンツを分析していないからである．一方で，コンテンツは攻撃者によって容易に変更できるため，提案手法ではこれらの特徴量を用いなかった．上記のような誤検知を低減するためには，コンテンツを分析する既存研究 [4] の併用や誤検知や見逃しのさらなる分析を通じて，識別精度を向上させる必要がある．

5.4 ユースケース

本稿では，提案手法を悪性ウェブサイトの検知に応用したが，その他の用途にも応用可能であると考える．例えば，対象ウェブサイトの企業組織による保有状況の確認や，対象ウェブサイトのセキュリティ評価等の用途に応用できると考えられる．これら応用の評価は今後の課題とする．

5.5 制限事項

FQDN の収集に PhishTank，URLhaus，FakeNewsNet，D&B Hoovers より提供されるデータを利用したが，これらのデータの中には，データ収集を実施した時点ですでにウェブサイトが稼働していない無効な FQDN が含まれる．4.1 節に記載した条件に該当する FQDN を無効な FQDN として除外したが，目視による確認は行っていないため，すべての無効な FQDN を除外できたとは限らない．また逆に，除外した FQDN の中にはウェブサイトが稼働している FQDN も含まれていた可能性がある．さらに，使用した悪性ウェブサイトのデータセットの中には，侵害された企業組織のウェブサイトやニュースサイトの FQDN が含まれていた．本研究では，これら正規 FQDN を悪性として学習させたため，構築コストの識別精度に影響していると考えられる．事前にデータセットを精査することによる，より高い精度の識別モデルの構築やその評価は今後の課題とする．

6. まとめ

本稿では，ウェブサイトの構築コストをドメイン名，DNS リソースレコード，証明書，インフラの 4 つの観点で分析し，その高さを識別する手法を提案した．フィッシング，マルウェアホスト，フェイクニュースの三種類の悪性ウェブサイトおよび企業のコーポレートサイトに提案手法を適用した結果，80%以上の精度で悪性サイトを識別でき，提案手法を悪性サイト識別に応用できることを示した．さらに，攻撃の種類によって識別における特徴量の重要度が異なり，その違いは各攻撃の特性が関連していることがわかった．

参考文献

[1] A. K. Jain *et al.*, “Towards detection of phishing websites on client-side using machine learning based approach,” *Telecommunication Systems*.

[2] K. Tian *et al.*, “Needle in a haystack: Tracking down elite phishing domains in the wild,” in *ACM SIGCOMM IMC*, 2018.

[3] I. Corona *et al.*, “DeltaPhish: Detecting Phishing Webpages in Compromised Websites,” in *ESORICS*, 2017.

[4] S. Maroofi *et al.*, “COMAR: Classification of Compromised versus Maliciously Registered Domains,” in *IEEE Euro S&P*, 2020.

[5] R. D. Silva *et al.*, “Compromised or attacker-owned: A large scale classification and study of hosting domains of malicious urls,” in *USENIX Security Symposium*, 2021.

[6] “PolitiFact.” `https://www.politifact.com/`.

[7] “Gossip cop.” `https://www.gossipcop.com/`.

[8] M. Potthast *et al.*, “A stylometric inquiry into hyperpartisan and fake news,” in *Annual Meeting of the ACL*, 2018.

[9] V.-H. Nguyen *et al.*, “Fang: Leveraging social context for fake news detection using graph representation,” in *CIKM*, 2020.

[10] “APIvoid.” `https://www.apivoid.com/`.

[11] “危険な Web サイトの世界分布 2010.” `https://promos.mcafee.com/ja-JP/PDF/MTMW_Report.pdf`.

[12] “SecurityTrails.” `https://securitytrails.com/`.

[13] “Shodan.” `https://www.shodan.io/`.

[14] “The World’s Most Abused TLDs.” `https://www.spamhaus.org/statistics/tlds/`.

[15] “SURBL.” `http://www.surbl.org/tld`.

[16] “DNS NS レコード.” `https://www.cloudflare.com/ja-jp/learning/dns/dns-records/dns-ns-record/`.

[17] “Let’s Encrypt.” `https://letsencrypt.org/ja/about/`.

[18] “ZeroSSL.” `https://zerossl.com/pricing/`.

[19] “Let’s Encrypt FAQ.” `https://letsencrypt.org/docs/faq/`.

[20] “ACM 証明書の特徴.” `https://docs.aws.amazon.com/ja_jp/acm/latest/userguide/acm-certificate.html`.

[21] “Introducing Universal SSL.” `https://blog.cloudflare.com/introducing-universal-ssl/`.

[22] D. Chiba *et al.*, “DomainChroma: Building actionable threat intelligence from malicious domain names,” *Computers and Security*, 2018.

[23] “OWASP Secure Headers Project.” `https://owasp.org/www-project-secure-headers/#permissions-policy`.

[24] “PhishTank.” `https://phishtank.com/`.

[25] “URLhaus.” `https://urlhaus.abuse.ch/`.

[26] “FakeNewNet.” `https://github.com/KaiDMML/FakeNewsNet`.

[27] “D&B Hoovers.” `https://www.dnb.com/products/marketing-sales/dnb-hoovers.html`.

[28] “中小企業基本法.” `https://www.chusho.meti.go.jp/koukai/hourei/kihonhou/`.