情報処理学会論文誌 Vol.62 No.9 1536–1548 (Sep. 2021)

悪性Webサイトの探索によるモバイル向けブラックリスト構築手法の提案と実証実験データを用いた分析

石原 聖[1] 佐藤 将也[1,†1] 山内 利宏[2]

受付日 2020年11月30日, 採録日 2021年6月7日

概要：モバイル端末を対象とした攻撃手法の１つとして，リダイレクトにより利用者の意図しない Web サイトへ誘導する攻撃がある．我々が調査した限りでは，このような攻撃に着目してブラックリストを構築する研究はない．本論文では，この攻撃への対策として，悪性 Web サイトを探索し，モバイル向けのブラックリストを構築する手法を提案する．提案手法は，クローラを用いて Web 空間から収集した HTML ファイルについて，既知の悪性 Web サイトから抽出したキーワードを用いて悪性である可能性が高い HTML ファイルを検索することで，利用者の意図しない Web サイトへ誘導する攻撃で利用される悪性 Web サイトを発見する．評価では，スマートフォンを対象にしたユーザ参加型の Web 媒介型攻撃観測システムにより収集された実証実験データを用いて，提案手法により構築したブラックリストによる検知実験を実施した．この結果，構築したブラックリストは，利用者の意図しない Web サイトへ誘導する攻撃で用いられる悪性 Web サイトを少ない誤検知数で検知でき，構築したブラックリストを悪性 Web サイトの探索に利用することで，実証実験データから新たな悪性 Web サイトを発見できることを示した．さらに，発見した悪性 Web サイトから利用者の意図しない Web サイトへ誘導する攻撃を分析した結果について述べる．

キーワード：悪性 Web サイト，ブラックリスト，Web 媒介型攻撃，Android

Proposal of Method of Generating a Blacklist for Mobile Devices by Searching Malicious Websites and Analysis Using Demonstration Experiment Data

Takashi Ishihara[1] Masaya Sato[1,†1] Toshihiro Yamauchi[2]

Received: November 30, 2020, Accepted: June 7, 2021

Abstract: One of the methods to attack mobile devices is redirecting a user to unwanted websites. To the best of our knowledge, there is no method to generate a blacklist that focuses on such attacks. Therefore, we propose a method to generate a blacklist for mobile devices by searching malicious websites. To detect new malicious websites, this method collects HTML files from the webspace using a crawler and searches for HTML files highly likely to be malicious using keywords extracted from known malicious websites. In the evaluation, we performed detection experiments with the blacklist generated by the proposed method using the demonstration experiment data. The evaluation results showed that the generated blacklist detects malicious websites used in attacks of redirecting a user to unwanted websites with few false positives. In addition, new malicious websites were discovered using the generated blacklist; furthermore, we describe an analysis of attacks of redirecting a user to unwanted websites.

Keywords: malicious websites, blacklist, web-based attack, Android

[1] 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University, Okayama 700–8530, Japan
[2] 岡山大学学術研究院自然科学学域
Graduate School of Natural Science and Technology, Okayama University, Okayama 700–8530, Japan
[†1] 現在，岡山県立大学情報工学部
Presently with Faculty of Computer Science and Systems Engineering, Okayama Prefectural University

1. はじめに

スマートフォンやタブレットなどのモバイル端末が世界中で普及している．2020 年 1 月に公表された調査結果では，世界中のモバイル端末の利用者数は 2019 年から約 1 億 2,000 万人増加し，世界人口の 67%に達したと報告されている [1]．また，2020 年には世界中の Web トラフィックの約 51%がモバイル端末から発生している [2]．モバイル端末の利用者数の増加にともない，モバイル端末がサイバー攻撃の標的にされることが多くなっている [3]．

モバイル端末における攻撃として，利用者の意図しない Web サイトへ誘導する攻撃が存在する．この攻撃では，利用者が誘導元の Web サイト（以降，遷移元 Web サイト）へアクセスした際，自動的もしくは画面のタップなどの操作を契機として Web サイトの遷移が発生する．遷移の発生後，リダイレクトにより複数の Web サイト（以降，経由 Web サイト）を経由した後に，目的の Web サイト（以降，遷移先 Web サイト）へ誘導する [4]．モバイル端末は PC とは異なり，Drive-by Download 攻撃のように利用者の許可なく自動的にソフトウェアをインストールできない．このため，遷移先 Web サイトで利用者を欺くことで個人情報の奪取や広告収入の獲得などを行う．遷移先 Web サイトには，不審なアプリをインストールさせることが目的の Web サイト，個人情報の開示を促す Web サイト，および金銭の獲得を目的とした出会い系 Web サイトやゲーム Web サイトなどが確認されている [5]．

このように，利用者の意図しない Web サイトへ誘導する攻撃の流れや利用される Web サイトの種類について分析はされているものの，攻撃の実態については十分に分析されていない．また，利用者の意図しない Web サイトへ誘導する攻撃で利用される悪性 Web サイト（遷移元 Web サイト，経由 Web サイト，遷移先 Web サイト）について先行研究が少なく，データセットとして公開されている件数は少ない [6]．また，我々が調査した限りでは，このような攻撃に着目してブラックリストを構築する研究はない．

本論文では，利用者の意図しない Web サイトへ誘導する攻撃への対策として，悪性 Web サイトを探索し，モバイル向けのブラックリストを構築する手法を提案する．提案手法は，Web 空間から収集した HTML ファイルについて，既知の悪性 Web サイトから抽出した悪性である可能性が高い FQDN とファイル名（以降，キーワードと呼ぶ）を用いて，悪性である可能性が高い HTML ファイルを検索する．また，悪性である可能性が高い HTML ファイルに対応する URL について悪性判定を行い，悪性と判定された URL をブラックリストに登録する．さらに，悪性な URL に対応する HTML ファイルと悪性な URL への Web アクセス履歴からキーワードを抽出し，ブラックリストに登録する．提案手法で構築するブラックリストは，悪性な URL，およびキーワードとして抽出した FQDN とファイル名の列から構成される．

評価では，Twitter から収集した URL を用いて，探索による悪性 Web サイトの発見数の評価とブラックリストの構築を実施する．また，スマートフォンを対象にしたユーザ参加型の Web 媒介型攻撃観測システム [7] により収集された実証実験データを用いて，提案手法により構築したブラックリストの有効性を示す．さらに，ブラックリストによる検知結果をもとに利用者の意図しない Web サイトへ誘導する攻撃の分析を行い，攻撃の傾向を明らかにする．

本研究の主な貢献は，以下のとおりである．

(1) 悪性 Web サイトを探索し，ブラックリストを構築する手法を提案した．本手法で構築したブラックリストを用いることで，モバイル端末を対象として利用者の意図しない Web サイトへ誘導する攻撃で用いられる悪性 Web サイトを少ない誤検知数で検知できる．
(2) Twitter で配布される URL，WarpDrive で収集したモバイル端末の実証実験データの Web アクセス履歴を用いて，ブラックリストを適用することで，未知の悪性 Web サイトを検知できることを示した．また，実証実験データは，悪性 Web サイトに誘導される一連のリダイレクトに関わる URL リストが取得できているため，途中の 1 つの悪性 Web サイトを検知できれば，その前後のアクセスに存在する悪性 Web サイトも検出できることを示した．
(3) 利用者の意図しない Web サイトへ誘導する攻撃で使われる悪性 Web サイトと悪性 Web サイトにアクセスしたユーザについて分析を行った．悪性 Web サイトの分析では，攻撃者は悪性 Web サイトへの誘導方法を短期間で変更できることを示した．ユーザの分析では，少なくないユーザが毎月悪性 Web サイトによる危険にさらされていることを明らかにした．

本論文の構成を以下に示す．まず 2 章で利用者の意図しない Web サイトへ誘導する攻撃およびブラックリスト構築手法の概要について示す．3 章で提案手法の実現方式，4 章で提案手法の評価のために行った実験とその結果を報告する．5 章でブラックリストにより検出した悪性 Web サイトを用いて，利用者の意図しない Web サイトへ誘導する攻撃について分析をした結果を報告する．6 章で関連研究について述べ，最後に 7 章で本研究をまとめる．

2. モバイル向けブラックリスト構築手法

2.1 利用者の意図しない Web サイトへ誘導する攻撃

図 1 に利用者の意図しない Web サイトへの遷移の流れを示す．遷移元 Web サイトは Cookie の保持や取得の有無により挙動が異なるという特徴や，遷移元 Web サイトからのリダイレクト先や遷移元 Web サイトからのリダイレクト数は毎回同じであるとは限らないという特徴がある [4]．

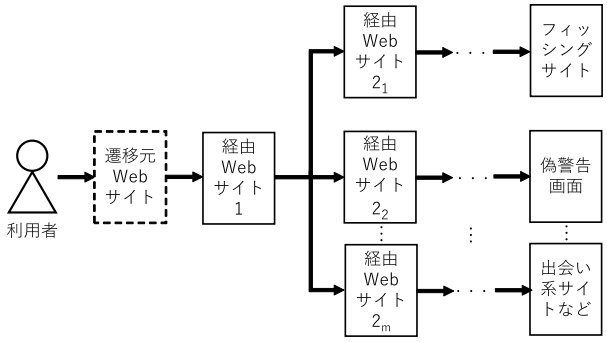

図 1 利用者の意図しない Web サイトへの遷移の流れ
Fig. 1 Flow of the transition to unwanted website.

このように，利用者の意図しない Web サイトへ誘導する攻撃では，遷移元 Web サイト，経由 Web サイト，および遷移先 Web サイトといった複数の悪性 Web サイトが利用される．ここで，ブラックリストに登録されている URL やキーワードを URL 内に含まず検知できない悪性 Web サイトを未知の悪性 Web サイトとする．また，遷移先 Web サイトに誘導する手口として，不正な広告を利用した手口が多いという報告がある [8]．利用者を遷移先 Web サイトに誘導する不正な広告として，自動リダイレクトと呼ばれる広告があり，これによる被害はモバイル端末で顕著である [9]．

2.2 研究目的

2.1 節で述べたように，悪性 Web サイトに誘導する攻撃が多く，脅威となっているものの，利用者の意図しない Web サイトへ誘導する攻撃で利用される Web サイトに着目したブラックリストは，我々が調べた限りない．たとえば，Google Safe Browsing（GSB）が検知する Web サイトは，フィッシングやマルウェアといった利用者のプライバシやセキュリティを脅かすもの [10] である．

そこで，本研究では，スマートフォン OS として広く利用されている Android を対象として，利用者の意図しない Web サイトへ誘導する攻撃を検知するブラックリスト構築手法を提案する．

2.3 基本方式

利用者の意図しない Web サイトへ誘導する攻撃では，複数の Web サイトを経由し，また共通の経由 Web サイトが利用されることが多いことが示されている [11]．このため，悪性 Web サイトへの誘導において，途中の 1 つの Web サイトでも悪性 Web サイトと検知できれば，攻撃を検知できる．このため，対策として，URL や FQDN のブラックリストの利用が有効である．本研究におけるブラックリストの使い方として，アクセス先の URL が，ブラックリストに登録されている URL やキーワードと 1 つでも部分一致する場合，警告を表示することを想定している．

悪性 Web サイトは，新たに構築され続けているため，攻撃の検知に有用なブラックリストを構築し維持するには，新たな悪性 Web サイトを早期にブラックリストに追加する必要がある．そこで，SNS で悪性 Web サイトに誘導する URL が拡散されていることに着目し，悪性 Web サイトを探索し，発見した悪性 Web サイトからブラックリストを構築する手法を提案する．提案手法は，データ収集部，検証部，および抽出部の 3 つに分類される．

Web 空間には 16 億を超える Web サイトが存在すると 2018 年の調査で報告されている [12]．悪性 Web サイトを探索するためには，広大な Web 空間における大規模なデータに対応する必要がある．そこで，データ収集部ではクローラを用いて，未知の URL と未知の URL に対応する Web コンテンツとして HTML ファイルを収集する．

収集した大量の Web コンテンツすべてを検証し，悪性 Web サイトを発見することは困難である．このため，収集した Web コンテンツから悪意のある可能性のある Web コンテンツを抽出し，抽出した Web コンテンツを検証，および分析する．これにより，効率的に悪性 Web サイトを発見できる．そこで，検証部では，既知の悪性 Web サイトから抽出したキーワードのリスト（以降，キーワードリスト）を用いて HTML ファイルを検索し，悪性である可能性が高い URL（以降，悪性見込 URL）を抽出する．また，悪性見込 URL の悪性判定を行う．

抽出部では，悪性な URL に対応する HTML ファイルと悪性な URL への Web アクセス履歴からキーワードを抽出し，キーワードリストの拡張とブラックリストの構築を行う．Web アクセス履歴の取得には，Google Chrome を利用して Web サイトへアクセスした際のアクセス先 URL などを収集するアプリを用いる．

提案手法では，キーワードを抽出するごとに，キーワードリストを拡張する．また，拡張したキーワードリストを用いて，過去に保存した HTML ファイルに対して検索を行う．これにより，拡張前のキーワードリストでは見逃した悪性 Web サイトを新たに発見できる可能性がある．

なお，提案するブラックリスト構築手法は，悪性 Web サイトに含まれる可能性が高い URL とキーワードをブラックリストに登録するものである．このため，1 度悪性と判定した Web サイトが，利用者の意図しない Web サイトへ誘導する攻撃で利用されない良性な Web サイトに変化したり，1 度良性と判定した Web サイトが悪性 Web サイトに変化したりしても，ブラックリストの内容は更新されず，誤検知や見逃しが発生する．ブラックリストを運用する際の URL とキーワードの登録と取り消し処理の実現については，残された課題とする．

2.4 提案手法の処理流れ

提案手法におけるブラックリスト構築の処理流れを図 2

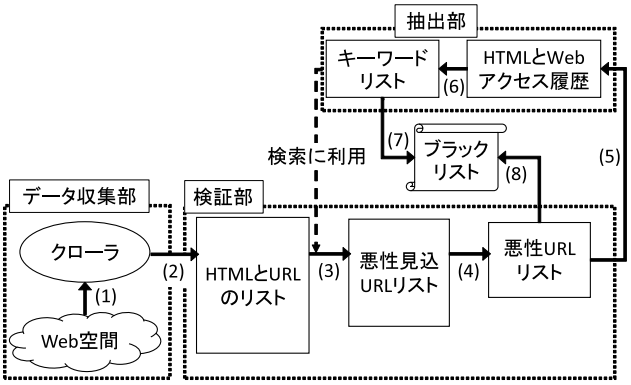

図 2 提案手法の処理流れ
Fig. 2 Flow of the proposed method.

に示し，以下で説明する．

(1) クローラを用いて Web 空間から Web コンテンツとして HTML ファイルを収集．
(2) 収集した HTML ファイルとクロール先 URL を保存．
(3) キーワードリストを用いて HTML ファイルを検索し，ファイル内にキーワードを含む場合，HTML ファイルに対応する URL を悪性見込 URL リストに追加．
(4) 悪性見込 URL リストに追加された URL が悪性 Web サイトであれば，悪性 URL リストに URL を追加．
(5) 悪性 Web サイトにアクセスした際の Web アクセス履歴を収集．
(6) 検証部における検索に用いるキーワードを抽出し，キーワードリストを拡張．
(7) 抽出したキーワードをブラックリストに登録．
(8) 悪性 URL リストの URL をブラックリストに登録．

次に，(5) と (6) で行うキーワードの抽出処理について述べる．(5) の処理で取得した Web アクセス履歴には，遷移元 Web サイトから遷移先 Web サイトまでのリダイレクトにおいてアクセスされた URL のリストが含まれる．(6) の処理では，(5) の処理で取得した URL リストから，経由 Web サイトと遷移先 Web サイトの FQDN を抽出する．また，遷移元 Web サイトで読み込まれているファイルについて，window.location.href などにより経由 Web サイトへ遷移させるコードが含まれているか否か確認し，含まれる場合，遷移に関連したファイルと見なす．この遷移に関連したと判断したファイル名と当該ファイルを提供する Web サイトの FQDN をキーワードとして抽出する．

2.5 ブラックリスト構築の考え方

提案手法は，探索により発見した遷移元 Web サイトの URL，および**表 1** に示す悪性 Web サイトから抽出したキーワードをブラックリストに登録する．遷移元 Web サイトには，利用者を遷移先 Web サイトまで遷移させる起点となるファイル（例：example.js）が存在する場合がある．また，既知の悪性 Web サイトについて，類似するドメインには共通の悪性 Web コンテンツが配置される可能性が高いという特徴がある [13]．利用者を遷移先 Web サイトまで遷移させる起点となるファイルのファイル名を抽出することで，ファイル名のみで複数の悪性 Web サイトを検知できる可能性がある．このため，遷移元 Web サイトの HTML ファイルから遷移の起点となるファイル名とこのファイルを提供する FQDN をキーワードとして抽出する．

また，経由 Web サイトの URL は，指定された URL とランダムに作成された文字列から作成される場合がある [4]．さらに，遷移先 Web サイトの URL は，利用者の端末情報を含む場合がある．このように URL が変化するため，URL 形式では悪性 Web サイトへのアクセスを検知できない可能性がある．このため，経由 Web サイトと遷移先 Web サイトの URL から FQDN をキーワードとして抽出する．

表 1 悪性 Web サイトから抽出するキーワード
Table 1 Keywords to extract.

対象	抽出するキーワード
遷移元 Web サイトの HTML ファイル	遷移の起点となるファイル名
	遷移の起点となるファイルを提供する FQDN
経由 Web サイトの URL	FQDN
遷移先 Web サイトの URL	FQDN

3. 実現方式

3.1 実現における課題

提案手法を実現するために，以下の実現課題に対処する必要がある．

（**課題 1**）クロールする URL の選定

データ収集部では，クローラを用いて未知の URL に対応する Web コンテンツを収集する．しかし，Web 空間には膨大な数の Web サイトが存在し，悪性 Web サイトはその URL を短期間で変更する．このため，Web 空間を手当たり次第にクロールする方法では，悪性 Web サイトの出現に即応できない．そこで，Web 空間から悪性 Web サイトを効率的に発見するために，クロールする URL を選定する必要がある．

（**課題 2**）悪性 Web サイトの検出

提案手法は，探索により発見した悪性 Web サイトをもとにブラックリストを構築する．このため，収集した Web サイトの中から悪性 Web サイトを検出する必要がある．

3.2 課題への対処

3.2.1 クロールする URL の選定

クロールする URL として，Twitter の Streaming API [14] の statuses/filter を利用して URL を収集する．これは，攻撃者が Twitter に悪性 Web サイトの URL を投稿するという手口があり，2010 年には 1 カ月間で 200 万件の悪性 Web

サイトのURLが投稿されているためである[15]．Twitter上からURLを収集することで，Web空間を手当たり次第にクロールする方法よりも効率的に悪性Webサイトを発見できると考える．また，TwitterのStreaming APIは，一定量間引かれて提供されるTweetをほぼリアルタイムで取得することができるため，攻撃者により投稿された未知の悪性WebサイトのURLをタイムリーに発見できる可能性がある．

3.2.2 悪性Webサイトの検出

2.2節で述べたように，利用者の意図しないWebサイトへ誘導する攻撃に着目したブラックリストは，我々が調べた限りないため，セキュリティ対策ソフトウェアの検知結果に頼ったとしても，正しく判定できる保証はない．

そこで，本研究では悪性Webサイトに手動でアクセスし，利用者の意図しない遷移により利用者の意図しないWebサイトへ誘導されるか否かを確認することで，悪性Webサイトの検出を行う．悪性Webサイトへの遷移は，1章で述べたように自動的もしくは画面のタップなどの操作を契機として発生する．ここで，正規のリンクをクリックすることによる遷移と，利用者の意図しない遷移を区別する必要がある．自動的もしくは画面のタップなどの操作を契機として利用者の意図しない遷移が発生した場合，遷移元Webサイトとする．ここで，自動的とは，Webページを表示後，ユーザの操作なしに，他のWebページに遷移する場合である．現在のところ，HTMLファイルの検査のみで，自動的またはタップなどの操作で悪性Webサイトに誘導するのか判別できないため，手間がかかるものの手動でアクセスする．本手法では悪性見込URLリストだけをチェックするため，手動チェックするWebサイト数は多くない．

4. 評価

4.1 評価項目

提案手法の有効性を明らかにするために，以下の評価を行った．

（**評価1**）探索による悪性Webサイトの発見数

提案手法により，Twitterから収集したURLから悪性Webサイトをどの程度発見できるかを示す．

（**評価2**）悪性Webサイトの検知実験

提案手法により構築したブラックリストが利用者の意図しないWebサイトへ誘導する攻撃で利用される悪性Webサイトを検知できるか否か，実証実験データを用いて評価した．

（**評価3**）ブラックリストを用いた悪性Webサイトの探索

提案手法により構築したブラックリストを用いて，実証実験データを対象に未知の悪性Webサイトを発見できるか否か評価した．

表2 探索による悪性Webサイトの発見数
Table 2 Number of malicious websites detected by the search.

提案手法の実施期間	2019年7月23日～2020年7月16日
クロールしたURL数	307,681件
発見した遷移元Webサイト数 （ユニークなFQDN数）	371件 （120件）
抽出したキーワード	ファイル名：5個 FQDN：143個
ブラックリストの内容	URL：371件 ファイル名：5個 FQDN：143個

4.2 探索による悪性Webサイトの発見数

4.2.1 評価内容

2019年7月23日から2020年7月16日の間で提案手法により，悪性Webサイトをどの程度発見できるのかを評価した．なお，初期のキーワードリストには，独自に発見した悪性Webサイトから抽出したキーワードを設定した．ここでキーワードリストの内容は，ファイル名のinvoke.jsが1個，invoke.jsを提供するFQDNが1個，経由Webサイトの FQDNが3個，および遷移先WebサイトのFQDNが1個であった．

4.2.2 評価結果と考察

評価結果を**表2**に示す．2019年7月23日から2020年7月16日の間にTwitterから収集したURL 307,681件をクロールした．また，これらのURLから発見した遷移元Webサイト数は371件（約1.2%）であった．このうち，ユニークなFQDNを持つ遷移元Webサイト数は120件であった．

さらに，遷移元Webサイトがどの程度，継続して悪性Webサイトへの遷移を発生させるのかを把握するため，2020年11月12日時点で，悪性Webサイトへの遷移を発生させるか否か実験を行った．この結果，ユニークなFQDNを持つ120件の遷移元Webサイトのうち，半数以上の69件のユニークなFQDNを持つ遷移元Webサイトで利用者の意図しない遷移が発生することを確認した．たとえば，2019年7月23日に収集した遷移元Webサイトには，2020年11月12日時点で利用者の意図しない遷移が発生するWebサイトがあった．このことから，長いもので1年以上の間，利用者を意図しないWebサイトへ誘導する攻撃を続けていることが分かった．

また，発見した遷移元WebサイトのHTMLファイルと利用者の意図しない遷移により遷移先Webサイトに到達するまでのWebアクセス履歴から，148個のキーワードを抽出した．抽出したキーワードのうち，ファイル名は5個であり，FQDNは143個であった．371件の遷移元WebサイトのURL，キーワードとして抽出した5個のファイル名と143個のFQDNからブラックリストを構築した．

4.3 悪性 Web サイトの検知実験

4.3.1 評価内容

提案手法は，ファイル名と FQDN を用いてブラックリストを構築するため，URL 形式のブラックリストに比べて誤検知が多くなる懸念がある．利便性を考えた場合，悪性 Web サイトの見逃しが少ないことよりも良性 Web サイトの誤検知が少ないことが重要である．このため，前節の実験で作成したブラックリストの有効性を評価するために，True Positive（TP）と False Positive（FP）について評価した．

4.3.2 WarpDrive 実証実験データセット

Web に関する攻撃について，実証実験を行う Web 媒介型攻撃対策技術の実用化に向けた研究開発（WarpDrive）[16] がある．WarpDrive では，Android を対象にしたユーザ参加型の Web 媒介型攻撃観測システムを提案している[*1][7]．Android を対象とした実証実験においてユーザから収集するデータには，Web アクセス履歴，アプリ表示履歴，インストールアプリ一覧，SMS のメッセージに含まれる URL，IP アドレス，および端末情報などがある．また，Web アクセス履歴として，Web ブラウザの種類，日付，URL などがある．

評価には，**表 3** に示す 2020 年 8 月 1 日から 2020 年 10 月 31 日の期間における 700 人のユニークなユーザによる 3,183,850 件の Web アクセス履歴を用いた．Twitter から集めた URL との違いとして，実証実験に参加しているユーザのアクセス URL を用いる点と，Twitter から収集した URL は遷移元 Web サイトの URL しか含まれないが，実証実験データの URL は遷移元 Web サイト，経由 Web サイト，および遷移先 Web サイトが含まれることが異なる．さらに，遷移元 Web サイトから遷移先 Web サイトまでの URL のうち，1 つの悪性の FQDN や URL を検知できれば，その前後のアクセス履歴の URL を確認することで，他の悪性 Web サイトを検知できる可能性がある点も異なる．

4.3.3 評価方法と評価環境

悪性 Web サイトの検知実験は以下の手順で行った．

(1) 実証実験データに含まれる URL に対して，4.2.2 項で作成したブラックリストと照合する．
(2) ブラックリストにより検知した URL（以降，検知 URL）に手動でアクセスし，悪性 Web サイトであるか否かを確認する．ここでは，利用者の意図しない遷移が発生した場合，アクセスした検知 URL を悪性 Web サイトと判断する．
(3) 検知 URL で利用者の意図しない遷移が発生しない場合，検知 URL は遷移先 Web サイトである可能性がある．実証実験データからはユーザごとに Web サイト遷移の履歴を確認できる．そこで，検知 URL にアクセスする前にユーザがアクセスした URL にアクセスし，利用者の意図しない遷移が発生するか否かを確認する．利用者の意図しない遷移が発生した場合，遷移先 Web サイトと検知 URL の FQDN が同じであれば，検知 URL を悪性 Web サイトと判断する．

[*1] タチコマ・セキュリティ・エージェント・モバイル（https://warpdrive-project.jp/mobile-app/）

表 3 実証実験データの内容
Table 3 Content of the demonstration experiment data.

収集期間	2020 年 8 月 1 日～2020 年 10 月 31 日
Web アクセス履歴があるユーザ数	700 人
URL 数	3,183,850 件

表 4 評価環境
Table 4 Environment for evaluation.

OS	Android 9.0
CPU	Snapdragon 845, 2.8 GHz
メモリ	4 GB
Google Chrome	86.0.4240.114
通信環境	Y!mobile（SoftBank）
端末	Pixel 3 XL

2.1 節で示したように，遷移元 Web サイトは Cookie の保持や取得の有無により挙動が異なるという特徴や，遷移元 Web サイトからのリダイレクト先や遷移元 Web サイトからのリダイレクト数は毎回同じであるとは限らないという特徴がある．そこで，検知 URL へのアクセスは，Cookie を削除して行った．また，検知 URL，および検知 URL にアクセスする前にユーザがアクセスした URL について，同一の URL へ最大 5 回までアクセスし，1 回でも悪性 Web サイトへの誘導が発生した時点で，アクセスした URL を悪性と判断した．また，5 回アクセスし，悪性 Web サイトへの誘導が発生しなかった場合，アクセスした URL を良性と判断した．同じ FQDN を持つ検知 URL が複数ある場合，1 件の検知 URL が悪性 Web サイトであれば，同様に悪性 Web サイトと判断した．評価に用いる環境を**表 4** に示す．

4.3.4 評価結果

評価結果を**表 5** に示す．検知結果について，TP は 1,285 件であり，FP は 114 件である．2 種類以上のキーワードにより重複して検知した URL が TP の中に 67 件含まれるため，重複を排除した TP は 1,218 件である．FP の中には，2 種類以上のキーワードにより重複して検知した URL は存在しなかった．検知 URL に含まれるキーワードは，ファイル名が 2 種類であり，FQDN が 28 種類であった．また，28 種類の FQDN のうち，TP が 1 件以上ある FQDN は 24 種類であった．ここで，キーワード 1（FQDN：経由 Web サイト）とキーワード 3（FQDN：経由 Web サイト）では同じホスト名が利用されていた．しかし，これ以外には，悪性 Web サイトの FQDN に類似性はみられなかった．TP

表 5 ブラックリストによる検知結果
Table 5 Detection results by the blacklist.

検知 URL に含まれるキーワード	TP	FP
キーワード 1（FQDN：経由 Web サイト）	520	3
キーワード 2（ファイル名：afu.php）	210	2
キーワード 3（FQDN：経由 Web サイト）	135	0
キーワード 4（FQDN：遷移先 Web サイト）	97	1
キーワード 5（FQDN：遷移先 Web サイト）	85	85
キーワード 6（FQDN：遷移先 Web サイト）	33	0
キーワード 7（FQDN：経由 Web サイト）	24	0
キーワード 8（FQDN：経由 Web サイト）	22	0
キーワード 9（FQDN：経由 Web サイト）	22	0
キーワード 10（FQDN：経由 Web サイト）	18	0
キーワード 11（FQDN：経由 Web サイト）	18	0
キーワード 12（FQDN：経由 Web サイト）	17	0
キーワード 13（FQDN：経由 Web サイト）	16	0
キーワード 14（FQDN：経由 Web サイト）	14	0
キーワード 15（ファイル名：streaming.php）	10	0
キーワード 16（FQDN：遷移先 Web サイト）	8	0
キーワード 17（FQDN：経由 Web サイト）	7	0
キーワード 18（FQDN：経由 Web サイト）	7	0
キーワード 19（FQDN：経由 Web サイト）	5	0
キーワード 20（FQDN：経由 Web サイト）	3	0
キーワード 21（FQDN：遷移先 Web サイト）	3	0
キーワード 22（FQDN：遷移先 Web サイト）	3	0
キーワード 23（FQDN：経由 Web サイト）	3	0
キーワード 24（FQDN：経由 Web サイト）	2	0
キーワード 25（FQDN：経由 Web サイト）	2	12
キーワード 26（FQDN：経由 Web サイト）	1	0
キーワード 27（FQDN：遷移先 Web サイト）	0	5
キーワード 28（FQDN：経由 Web サイト）	0	4
キーワード 29（FQDN：経由 Web サイト）	0	1
キーワード 30（FQDN：遷移先 Web サイト）	0	1
合計	1,285	114
合計（重複排除後）	1,218	114

が 1 件以上ある 24 種類の FQDN のうち，経由 Web サイトのキーワードは 18 種類であり，遷移先 Web サイトのキーワードは 6 種類であった．利用者の意図しない Web サイトへ誘導する攻撃は，複数の経由 Web サイトを経由した後に遷移先 Web サイトに誘導するため，利用する経由 Web サイトの数が多い．このため，遷移先 Web サイトに比べて検知した経由 Web サイトの種類が多くなったと考えられる．なお，ブラックリストに登録されている遷移元 Web サイトの URL により検知した URL は存在しなかった．

実証実験データの Web アクセス履歴に含まれる GSB による検知結果から，表 5 に示すブラックリストで正しく検知した 1,218 件の URL のうち，GSB が検知した URL の数は 3 件であることが分かった．提案手法は利用者の意図しない Web サイトへ誘導する攻撃を対象にブラックリストを構築しているため，この観点では GSB より，多くの悪性 Web サイトを検知できていることが分かる．

4.3.5 考察

表 5 より，キーワード 1（FQDN：経由 Web サイト）により 520 件の悪性 Web サイトを検知したことが分かる．キーワード 1（FQDN：経由 Web サイト）により検知した悪性 Web サイトは経由 Web サイトであった．また，この経由 Web サイトにアクセスする前にユーザがアクセスした Web サイトを確認したところ，ユニークな FQDN を持つ 28 件の遷移元 Web サイトを新たに発見した．このことから，複数の遷移元 Web サイトから，同じ経由 Web サイトへ遷移していることが分かる．

このように遷移元 Web サイトが異なる場合でも，提案手法により構築したブラックリストは経由 Web サイトへのアクセスを検知でき，未知の遷移元 Web サイトから生じた連続リダイレクトを検知できる．さらに，Twitter から収集した悪性 Web サイトをもとに構築したブラックリストを探索に用いることで，実証実験データから新たに悪性 Web サイトを発見できることが分かる．このように異なるデータセットにおける悪性 Web サイトの探索にもブラックリストは有効に働くことが分かる．また，新たに発見した悪性 Web サイトをもとにブラックリストを拡張することができる．

表 5 より，キーワード 2（ファイル名：afu.php）により 210 件の悪性 Web サイトを検知したことが分かる．検知 URL のうち，キーワード 2（ファイル名：afu.php）というファイルを提供する FQDN は 28 種類あり，複数の悪性 Web サイトで共通のファイル名が利用されていることが分かる．このように悪性 Web サイトにおいて，ファイル名は共通の名前を使うことが多いため，検知において有効に働いたと考える．

4.3.6 FP の事例

FP と判断した検知 URL について以下で説明する．

(1) ユーザの端末にインストールされているセキュリティアプリによる検知結果を通知する Web サイトの URL を検知した事例

この事例は，キーワード 1（FQDN：経由 Web サイト）で 3 件，キーワード 5（FQDN：遷移先 Web サイト）で 85 件あった．これは，キーワード 1（FQDN：経由 Web サイト）やキーワード 5（FQDN：遷移先 Web サイト）を FQDN に持つ URL を URL パラメータに含んでいたためである．このように，悪性な FQDN を持つ URL がパラメータとして利用される場合，検知結果を通知する Web サイトへのアクセスを検知してしまう．この問題には，セキュリティアプリによる検知結果を通知する Web サイトをホワイトリストに登録し，検知対象から除外することで対処できる．

(2) 利用者の意図しない遷移の発生を確認できなかった事例

利用者の意図しない遷移の発生を確認できず，遷移

先 Web サイトとしての利用も確認できなかったため，検知 URL を FP と判断した事例がある．この事例は，キーワード 2（ファイル名：afu.php）で 2 件，キーワード 4（FQDN：遷移先 Web サイト）で 1 件，キーワード 25（FQDN：経由 Web サイト）で 12 件，キーワード 27（FQDN：遷移先 Web サイト）で 5 件，キーワード 28（FQDN：経由 Web サイト）で 4 件，キーワード 29（FQDN：経由 Web サイト）で 1 件，キーワード 30（FQDN：遷移先 Web サイト）で 1 件あった．

ただし，遷移先 Web サイトの URL では，utm_source パラメータがキーワード 25（FQDN：経由 Web サイト）となっている事例があった．utm_source パラメータは，トラフィックを誘導した広告主，サイト，出版物，その他を識別する [18]．このことから，キーワード 25（FQDN：経由 Web サイト）を FQDN に持つ URL は，経由 Web サイトとして利用されている可能性が高いと推察する．

検知結果のうち正しく悪性と検知できた Web サイトの割合を示す適合率（= TP/(TP+FP)）は，約 91.4%である．なお，実証実験データに含まれる悪性 Web サイトの総数を明らかにするためには，実証実験データに含まれるすべての URL にアクセスして悪性 Web サイトか否かを判断する必要があるため，工数が大きく，悪性 Web サイトの総数を明らかにできていない．このため，実証実験データに含まれる悪性 Web サイトのうち，ブラックリストにより検知できた悪性 Web サイトの割合を示す再現率（= TP/(TP+FN)）は算出できていない．検知結果について，FP は 114 件（約 8.6%）ある．しかし，セキュリティアプリによる検知結果を通知する Web サイトをホワイトリストに登録することで 88 件の誤検知を防ぐことができる．また，キーワード 25（FQDN：経由 Web サイト）を FQDN に持つ 12 件の URL は悪性 Web サイトである可能性が高い．このことを考慮すると，提案手法により構築したブラックリストの FP は 14 件（約 1.1%）であり，誤検知が少なく利便性を損なわないブラックリストを構築できているといえる．

本研究では，構築したブラックリストは，ユーザの端末にインストールするモバイル向けアプリで使用し，悪性 Web サイトへのアクセス時に警告を表示することを想定している．このため，ユーザが Web ブラウジングをしている際に，ユーザの端末上でのみ警告が表示される．遷移先 Web サイトに誘導され，不審なアプリのインストールや個人情報の奪取などの危険にさらされるリスクを考えると，約 8.6%の誤検知は許容できると考えられる．なお，セキュリティーオペレーションセンタなど膨大な数のログが集まる環境において，本研究で構築したブラックリストを使用した場合，誤検知の数も多くなると推察できる．このため，本研究で構築するブラックリストの使用環境としては，膨大な数のログが集まる環境ではなく，ユーザ端末を想定している．

表 6 ブラックリストを用いた悪性 Web サイトの探索結果
Table 6 Result of the search using the blacklist.

悪性 Web サイトの種類	ユニークな FQDN を持つ新たな悪性 Web サイトの発見数
遷移元 Web サイト	70 件
経由 Web サイト	264 件
遷移先 Web サイト	7 件
合計	341 件

4.4 ブラックリストを用いた悪性 Web サイトの探索

4.4.1 評価内容

4.3.5 項で示したように，提案手法で構築したブラックリストは悪性 Web サイトの検知だけでなく，悪性 Web サイトの探索に利用できる．そこで，構築したブラックリストを用いた悪性 Web サイトの探索を行い，実証実験データから新たな悪性 Web サイトをどの程度発見できるかを評価した．

連続してリダイレクトの発生する回数は，悪性 Web サイトで 3 回以上の事例が多く，特に，4 回の事例が多い [19]．そこで，ブラックリストに登録されている URL とキーワードのうち 1 つでも部分一致した URL の前後 4 つの URL を実証実験データから抽出し，抽出した URL について利用者の意図しない遷移が発生するか否かを確認した．また，検証時に誘導された遷移先 Web サイトの FQDN を実証実験データから検索し，一致した FQDN を遷移先 Web サイトとした．

4.4.2 評価結果と考察

評価結果を**表 6** に示す．ブラックリストを用いた探索により，発見したユニークな FQDN を持つ悪性 Web サイト数は 341 件であった．利用者の意図しない Web サイトへ誘導する攻撃では，悪性 Web サイトへのアクセスが連続して発生する．ここで，未知の悪性 Web サイトが誘導に利用されていても，経由 Web サイトや遷移先 Web サイトなど誘導時に利用されるどれか 1 つの Web サイトを検知することで，利用者の意図しない Web サイトへ誘導する攻撃を検知できる．また，利用者の意図しない Web サイトへ誘導する攻撃を検知することで，検知した攻撃の一連のリダイレクトに関わる URL を手動でアクセスして確認することにより，誘導時に利用された未知の悪性 Web サイトを検知できる可能性がある．このため，実証実験データを用いることで，1 つの悪性 Web サイトを検知できれば，攻撃で利用された悪性 Web サイトを Web アクセス履歴から効率良く発見できる．

経由 Web サイトにおいて，異なる複数のホスト名を持つドメインを利用する Web サイトがあったため，経由 Web

サイトの発見数は多い．このドメインは，検知 URL のキーワード 1（FQDN：経由 Web サイト）のドメインと，キーワード 3（FQDN：経由 Web サイト）のドメインである．検知 URL のキーワード 3（FQDN：経由 Web サイト）のドメインでは，1 から 99 の数字による 99 種類のホスト名と sdfjjd という文字列のホスト名の合計 100 種類のホスト名を利用していた．また，キーワード 1（FQDN：経由 Web サイト）においても同様の傾向があり，数字によるホスト名と sdfjjd という文字列のホスト名の合計 81 種類のホスト名を利用していた．

5. 利用者の意図しない Web サイトへ誘導する攻撃の分析

5.1 概要

利用者の意図しない Web サイトへ誘導する攻撃の流れや利用される Web サイトの種類について分析はされているものの，攻撃の実態については十分に分析されていない．攻撃で利用される悪性 Web サイトや悪性 Web サイトにアクセスしたユーザに着目して分析を行うことで，利用者の意図しない Web サイトへ誘導する攻撃の傾向を明らかにでき，悪性 Web サイトへの対策に有用な情報が得られる可能性がある．また，本分析により，ユーザの端末でブラックリストが使用されていた場合に，どの程度の悪性 Web サイトを検知できたかを推定することができる．さらに，ユーザに着目した分析を行うことで，悪性 Web サイトへアクセスするユーザの割合などを評価することができる．

そこで，4.3 節でブラックリストの FQDN により検知した悪性 Web サイト 24 件と 4.4 節で発見したユニークな FQDN を持つ悪性 Web サイト 341 件の合計 365 件の悪性 Web サイトをもとに，利用者の意図しない Web サイトへ誘導する攻撃の分析を行う．この 365 件のユニークな FQDN を持つ悪性 Web サイトのうち，遷移元 Web サイトの数は 70 件，経由 Web サイトの数は 282 件，および遷移先 Web サイトの数は 13 件である．

5.2 悪性 Web サイトの分析

表 7 に，月ごとおよび 3 カ月間でアクセスされたユニークな FQDN を持つ悪性 Web サイト数を示す．どの月においても，3 カ月間にアクセスされた悪性 Web サイトのうち，半分以上の悪性 Web サイトへのアクセスが発生しており，毎月多くの悪性 Web サイトが攻撃に利用されていることが分かる．3 カ月間に毎月アクセスされた Web サイトが存在し，遷移元 Web サイトで 16 件，経由 Web サイトで 50 件，および遷移先 Web サイトで 8 件あった．一方，1 つの月の間にだけアクセスされた Web サイトは，遷移元 Web サイトで 39 件，経由 Web サイトで 128 件，および遷移先 Web サイトで 1 件あった．

遷移元 Web サイト，経由 Web サイト，および遷移先 Web サイトへのアクセス数の合計は 18,057 件であった．遷移元 Web サイト，経由 Web サイト，および遷移先 Web サイトごとに，3 カ月間の 1 カ月あたりの平均アクセス数とその累積相対度数を表すグラフを**図 3** に示す．

経由 Web サイトではアクセス数が 10 回未満の Web サイト数が 96.8%であるのに対し，遷移元 Web サイトではアクセス数が 10 回未満の Web サイト数は 68.6%，遷移先 Web サイトではアクセス数が 10 回未満の Web サイト数は 69.2%であり，アクセス数が多い Web サイトの数が多い．遷移元 Web サイトにおいて特にアクセス数が多かった Web サイトでは，漫画 Web サイトで平均 3,208 回，ア

表 7 アクセスされたユニークな FQDN を持つ悪性 Web サイト数
Table 7 Number of malicious websites with unique FQDNs accessed.

	8 月	9 月	10 月	8 月～10 月
遷移元 Web サイト	43	35	39	70
経由 Web サイト	156	146	183	282
遷移先 Web サイト	10	11	12	13
合計	209	192	234	365

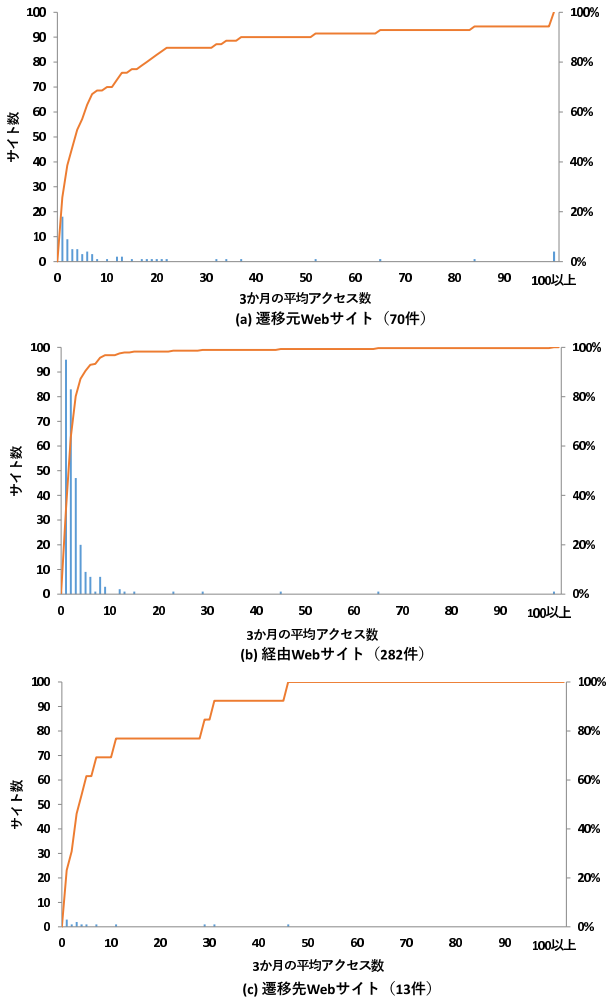

図 3 悪性 Web サイトへの平均アクセス数とその累積相対度数
Fig. 3 Average number of access to malicious websites and cumulative relative frequency.

表 8 悪性 Web サイトの 2020 年の月ごとのドメイン取得数
Table 8 Monthly number of domain acquisitions of malicious websites in 2020.

	1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	合計
遷移元 Web サイト	2	2	3	1	1	1	0	1	1	1	13
経由 Web サイト	8	0	5	2	3	3	9	12	17	8	67
遷移先 Web サイト	0	1	0	1	0	0	1	1	0	1	5

表 9 Web アクセス履歴があるユーザ数と悪性 Web サイトへアクセスしたユーザ数
Table 9 Number of active users and users who accessed the malicious website.

	8 月	9 月	10 月	8 月～10 月
Web アクセス履歴有	553	555	541	700
遷移元 Web サイト	38	40	34	74
経由 Web サイト	40	36	38	84
遷移先 Web サイト	30	34	36	70
上記いずれかの Web サイト	57	56	56	113

ニメ動画 Web サイトで平均 546 回，およびアダルト Web サイトで平均 457 回のアクセスがあった．遷移先 Web サイトでは，平均 45 回アクセスされた Web サイトとして，ギャンブル Web サイトがあった．

悪性 Web サイトは短期的にドメインを変えることで，ブラックリストによる対策を困難にする場合がある．そこで，悪性 Web サイトについて，ドメイン取得日を調査した．ここで，365 個の FQDN のうちユニークなドメイン数は，遷移元 Web サイトが 65 個，経由 Web サイトが 100 個，および遷移先 Web サイトが 12 個であった．2020 年に取得されたドメインについて，月ごとの取得数を**表 8** に示す．

表 8 より，毎月新たに悪性 Web サイトのドメインが取得されていることが分かる．特に，経由 Web サイトは 100 個中 67 個のドメインが 2020 年に取得されており，新たな悪性 Web サイトを攻撃に利用する傾向があることが分かる．また，ドメイン取得日が 8 月から 10 月の悪性 Web サイトのうち，ドメイン取得日の翌日にユーザによりアクセスされたドメインが 6 個あった．この 6 個は経由 Web サイトのドメインであり，攻撃者が悪性 Web サイトへの誘導方法を短期間で変更できることが分かる．

5.3 ユーザの分析

表 9 に，Web アクセス履歴があるユーザ数と悪性 Web サイトにアクセスしたユーザ数を月ごとに示す．8 月から 10 月の 3 カ月間において，悪性 Web サイトへアクセスしたユーザ数は 113 人であった．実証実験データに含まれる 700 人のユーザのうち 16.1%が少なくとも 1 回は悪性 Web サイトへ誘導され，アクセスしていることが分かる．また，毎月少なくとも 10.1%のユーザが遷移元 Web サイト，経由 Web サイト，および遷移先 Web サイトのいずれかの悪性 Web サイトへアクセスしていることが分かる．このように，悪性 Web サイトによる危険にさらされているユーザが毎月存在する．

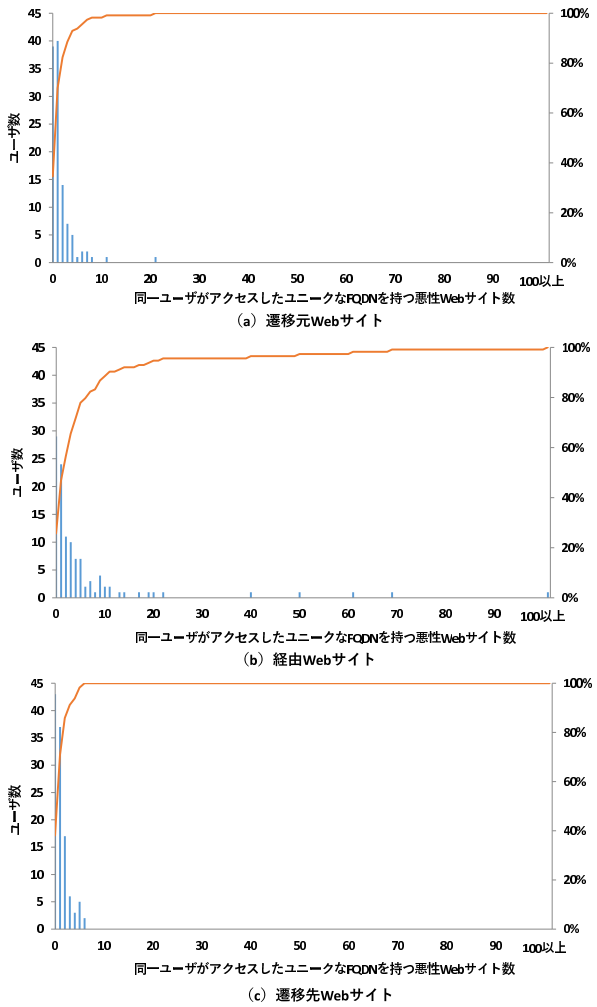

図 4 同一ユーザがアクセスしたユニーク FQDN を持つ悪性 Web サイト数とその累積相対度数
Fig. 4 Number of malicious websites with unique FQDN accessed by a unique user and cumulative relative frequency.

ユーザの中には，毎月 1,000 回以上遷移元 Web サイトにアクセスしたユーザ，毎月 50 回以上経由 Web サイトにアクセスしたユーザ，毎月 13 回以上遷移先 Web サイトにアクセスしたユーザが存在しており，ユーザは危険にさらされていることを意識できていない可能性がある．

同一ユーザがアクセスしたユニークな FQDN を持つ悪性 Web サイト数とその累積相対度数を表すグラフを**図 4**

に示す．悪性 Web サイトにアクセスした 113 人のユーザのうち，69.9%のユーザがアクセスしたユニークな FQDN を持つ遷移元 Web サイト数は 1 件以下であり，70.8%のユーザがアクセスしたユニークな FQDN を持つ経由 Web サイトは 1 件以下である．一方で，経由 Web サイトでは，46.9%のユーザがアクセスしたユニークな FQDN を持つ経由 Web サイト数は 1 件以下であり，遷移元 Web サイトと遷移先 Web サイトに比べ，経由 Web サイトは 1 人のユーザが複数種類の経由 Web サイトへアクセスすることが多いことが分かる．

10 月の実証実験データの中には，1 種類の遷移元 Web サイトにしかアクセスしていないにもかかわらず，106 種類の経由 Web サイトへアクセスしているユーザが 1 人存在した．このことから，遷移元 Web サイトだけではなく，経由 Web サイトや遷移先 Web サイトへのアクセスを検知できる対策が重要といえる．

6. 関連研究

6.1 利用者の意図しない遷移を防止する研究

利用者の意図しないタップを誘発する Web サイトへの対策として，2 段階タップ方式を用いて誤遷移を防止する手法 [20] がある．文献 [20] の手法では，タップされたリンク要素をユーザに伝え，意図しないリンク要素をタップしていた場合，ユーザはもう 1 度タップを行うことで操作をキャンセルする．しかし，文献 [20] の手法では，利用者の意図しない遷移が自動的に発生する場合には遷移を防止できない．一方で，提案手法は利用者の意図しない遷移が自動的に発生する場合においても，URL にキーワードが含まれていれば悪性 Web サイトへのアクセスを防止できる．

6.2 ブラックリスト構築に着目した研究

ブラックリストの構築に着目した研究として，文献 [21], [22] がある．文献 [21] では，Web 空間から新しい悪意のある URL を収集し，自動でブラックリストを構築する AutoBLG を提案している．AutoBLG は，複数のプレフィルタを利用して解析対象の URL 数を減らすことで，ブラックリストの構築を高速に行うことができる．上記の論文は，Web サイトを介した攻撃として Drive-by Download 攻撃に着目している．一方で，提案手法では，Web サイトを介した攻撃として利用者の意図しない Web サイトへ誘導する攻撃に着目している．文献 [22] では，オープンソースインテリジェンスを用いて効率的に悪意のある候補 URL を収集し，その情報に基づいて精度の高いブラックリストを構築する手法を提案している．文献 [22] の手法は，候補 URL からダウンロードしたファイルをアンチウイルスソフトウェアにより，悪性判定する．また，悪性であったファイルのダウンロード元 URL をブラックリストとして利用する．一方，提案手法は，Twitter から収集した遷移元 Web サイトの URL だけでなく，利用者の意図しない Web サイトへ誘導する攻撃で利用されるファイル名，および経由 Web サイトと遷移先 Web サイトの FQDN をブラックリストとして利用する．これにより，遷移元 Web サイトだけでなく経由 Web サイトや遷移先 Web サイトへのアクセスを検知できる．

6.3 モバイル端末で悪性 Web サイトを検知する研究

モバイル端末において悪性 Web サイトを検知することを目的とした研究として，文献 [23], [24], [25] がある．文献 [23] は，デスクトップ Web サイトとモバイル Web サイトの特徴が異なることに基づいた機械学習による検知手法を提案している．文献 [24] は，モバイル端末の利用者が悪意のあるコンテンツにさらされるか否か，機械学習を用いて事前に予測するシステムを提案している．文献 [23], [24] は，教師あり機械学習を利用しているため，学習に用いるラベル付きの教師データが事前に必要になる．しかし，このようなデータの作成はコストが高いという問題がある [21]．一方で，提案手法は，悪性 Web サイトから抽出した比較的少量のキーワードを用いることで，モバイル端末において悪性 Web サイトを検知できる．文献 [25] では，光学式文字認識（OCR）技術を用いて，モバイル端末のスクリーンショットからテキストを抽出し，悪性 Web サイトの検知に利用する手法を提案している．文献 [25] の手法では，スクリーンショットの取得や OCR によるテキストの抽出などにより悪性 Web サイトを検知するまでに約 3.3 秒かかる．このため，短い間隔で複数の遷移が発生する利用者の意図しない Web サイトへ誘導する攻撃への適用は難しいと推察する．一方で，ブラックリストは悪性 Web サイトを検知するまでに単純な照合だけですむため，高速である．

6.4 URL やドメイン名の特徴により悪性 Web サイトを検知する研究

URL に含まれる語彙的特徴を用いて悪性な Web サイトを検知することを目的とした研究として，文献 [26], [27], [28], [29] がある．文献 [26] では，ブラックリストに登録された URL の共通の語彙的特性を調査し，トップレベルドメインの置き換え，ディレクトリ構造の類似性，クエリ文字列の置換などにより，新たな悪性な URL を構築している．ディレクトリ構造の類似性に着目した手法では，共通のディレクトリ構造を持つ 2 つの URL には，同様のファイルが存在する可能性が高いという考え方に基づき，URL 間でファイル名を交換することで新しい URL を構築し，ブラックリストに追加する．一方で，提案手法は，類似する悪性 Web サイトには同様のファイルが存在する可能性が高いという考え方に基づき，ファイル名をブラックリストに登録する．これにより，悪性 Web サイトでよく用いられる既知のファイル名を検知の対象にして

いる．

文献 [27] は，ドメイン名の語彙的特徴を利用した 2 段階の検知メカニズムを提案している．第 1 段階では，既知の悪意のある URL のブラックリストを用いて，文字列が似ているドメインを検出する．第 2 段階では，ドメインの語彙的特徴を表す評価値を N-gram モデルに基づいて計算し，その評価値に基づいて悪性ドメインか良性ドメインかを判定する．文献 [28] は，URL の特徴のみを用いて，機械学習によりフィッシング Web サイトを検知するシステムを提案している．URL の長さ，ハイフンの数，ドットの数，数字の数，URL に IP アドレスが含まれるか否か，および類似度の 6 種類の特徴を利用することで，95.80%の認識率を達成している．また，文献 [29] は，教師あり機械学習により URL を悪性と良性に自動的に分類する手法を提案している．文献 [29] の手法は，URL の語彙的特徴とホストに関する特徴を用いることで，高精度な分類が可能であることを示している．文献 [27], [28], [29] のように悪性な URL の語彙的特徴を利用した検知手法では，悪性な URL を一般化でき，未知の悪性な Web サイトを検知できる．一方で，提案手法で構築するブラックリストは，ブラックリストに登録されている URL，FQDN，およびファイル名を URL 内に含まない未知の悪性 Web サイトを検知できない．そこで，ブラックリストに含まれる URL，FQDN，およびファイル名について，語彙的特徴を利用した検知手法に適用することで，利用者の意図しない Web サイトへ誘導する攻撃で利用される未知の悪性 Web サイトを検知できる可能性がある．

7. おわりに

利用者の意図しない Web サイトへ誘導する攻撃への対策を目的とし，悪性 Web サイトを探索し，モバイル向けのブラックリストを構築する手法を提案した．提案手法は，クローラを用いて Web 空間から収集した HTML ファイルについて，既知の悪性 Web サイトから抽出したキーワードを用いて悪性である可能性が高い HTML ファイルを検索することで，悪性である可能性が高い URL を発見する．また，悪性である可能性が高い URL へ手動でアクセスし，利用者の意図しない Web サイトへ誘導する攻撃で利用される悪性 Web サイトを検出する．

Twitter から収集した URL を用いて，探索による悪性 Web サイトの発見数の評価を実施した結果から，遷移元 Web サイト 371 件を発見した．また，実証実験データを利用した悪性 Web サイトの検知実験を実施した結果から，提案手法により構築したブラックリストは，利用者の意図しない Web サイトへ誘導する攻撃で用いられる悪性 Web サイトを少ない誤検知数で検知できることを示した．さらに，提案手法により構築したブラックリストを用いて，実証実験データから遷移元 Web サイト 70 件，経由 Web サイト 264 件，および遷移先 Web サイト 7 件を新たに発見できることを示した．最後に，利用者の意図しない Web サイトへ誘導する攻撃の分析により，毎月少なくないユーザが悪性 Web サイトによる危険にさらされており，悪性 Web サイトへの誘導に対する対策が重要であることを示した．

残された課題として，ブラックリスト運用時のブラックリストへの URL とキーワードの登録処理と取り消し処理の実現がある．

謝辞 本研究成果は，国立研究開発法人情報通信研究機構（NICT）の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」により得られたものです．評価にご協力いただいた岡山大学大学院自然科学研究科の横山綾氏，大賀美耶氏に深く感謝申し上げます．

参考文献

[1] DataReportal: Digital 2020: Global Digital Overview, available from ⟨https://datareportal.com/reports/digital-2020-global-digital-overview⟩ (accessed 2020-08-07).
[2] Clement, J.: Mobile percentage of website traffic 2020 | Statista, Statista, available from ⟨https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/⟩ (accessed 2020-08-07).
[3] McAfee: Mobile Threat Report, available from ⟨https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf⟩ (accessed 2020-08-07).
[4] Imamura, Y., Orito, R., Chaikaew, K., Manardo, C., Leelaprute, P., Sato, M. and Yamauchi, T.: Threat Analysis of Fake Virus Alerts Using WebView Monitor, *Proc. 7th International Symposium on Computing and Networking* (*CANDAR 2019*), pp.28–36 (2019).
[5] 利穂虹希，折戸凜太郎，佐藤将也，山内利宏：Android を対象とした利用者の意図しない Web サイトの分類，コンピュータセキュリティシンポジウム 2019（CSS2019）論文集，pp.1011–1016 (2019).
[6] 折戸凜太郎，佐藤将也，山内利宏：Android 向けセキュリティアプリにおける悪性 Web サイト検知率の調査，第 18 回情報科学技術フォーラム（FIT2019）講演論文集，Vol. 第 4 分冊，pp.181–182 (2019).
[7] 山田 明ほか：スマートフォンにおける Web 媒介型サイバー攻撃の観測機構：設計と実装，2020 年暗号と情報セキュリティシンポジウム（SCIS2020）論文集，電子媒体 (2020).
[8] 岡本勝之：2016 年個人の三大脅威：転換点を迎えた「モバイルを狙う脅威」，トレンドマイクロセキュリティブログ，入手先 ⟨https://blog.trendmicro.co.jp/archives/14307⟩（参照 2020-08-15）.
[9] GeoEdge: AUTO-REDIRECTS, available from ⟨https://site.geoedge.com/downloads/documents/Auto_Redirects.pdf⟩ (accessed 2020-08-15).
[10] Google: Google Safe Browsing – Google Transparency Report, available from ⟨https://transparencyreport.google.com/safe-browsing/overview⟩ (accessed 2020-08-18).
[11] 市岡秀一，川島千明，佐藤将也，山内利宏：Android における悪性 Web サイトアクセスの可視化手法の提案とページ遷移分析，コンピュータセキュリティシンポジウム 2020（CSS2020）論文集，pp.551–558 (2020).

[12] Internet Live Stats: Total number of Websites, available from ⟨https://www.internetlivestats.com/total-number-of-websites/⟩ (accessed 2019-08-08).
[13] Invernizzi, L., Comparetti, P.M., Benvenuti, S., et al.: Evilseed: A Guided Approach to Finding Malicious Web Pages, *Proc. 2012 IEEE Symposium on Security and Privacy*, pp.428–442 (2012).
[14] Twitter: statuses/filter|Docs|Twitter Developer, available from ⟨https://dev.twitter.com/streaming/overview⟩ (accessed 2019-06-25).
[15] Grier, C., Thomas, K., Paxson, V. and Zhang, M.: @spam: the underground on 140 characters or less, *Proc. 17th ACM Conference on Computer and Communications Security* (*CCS'10*), pp.27–37 (2010).
[16] WarpDrive, available from ⟨https://warpdrive-project.jp/index.html⟩ (accessed 2020-08-07).
[17] WarpDrive：利用規約 | タチコマ・セキュリティ・エージェント・モバイル，入手先 ⟨https://warpdrive-project.jp/mobile-app/terms/⟩（参照 2020-08-07）.
[18] Google：カスタム URL でキャンペーン データを収集する — アナリティクス ヘルプ，入手先 ⟨https://support.google.com/analytics/answer/1033863⟩（参照 2020-11-09）.
[19] 折戸凜太郎，石原 聖，佐藤将也，梅本 俊，中嶋 淳，山内利宏：Android における URL バーの切り替わり間隔に着目した利用者の意図しない Web サイトへの遷移の検知手法の評価，2020 年暗号と情報セキュリティシンポジウム（SCIS2020）論文集，電子媒体 (2020).
[20] 向山浩平，藤田真浩，白井丈晴，西垣正勝：Slyware 対策：意図しないタップを誘発する Web サイトの脅威とその対策に関する研究，情報処理学会論文誌，Vol.59, No.12, pp.2166–2179 (2018).
[21] Sun, B., Akiyama, M., Yagi, T. and Hatada, M.: Automating URL Blacklist Generation with Similarity Search Approach, *IEICE Trans. Information and Systems*, Vol.99, No.4, pp.873–882 (2016).
[22] Tanaka, Y. and Kashima, S.: SeedsMiner: Accurate URL Blacklist-Generation Based on Efficient OSINT Seed Collection, *Proc. IEEE/WIC/ACM International Conference on Web Intelligence* (*WI'19*), pp.250–255 (2019).
[23] Amrutkar, C., Kim, S.Y. and Traynor, P.: Detecting Mobile Malicious WebPages in Real Time, *IEEE Trans. Mobile Computing*, Vol.16, No.8, pp.2184–2197 (2017).
[24] Sharif, M., Urakawa, J., Christin, N., Kubota, A. and Yamada, A.: Predicting Impending Exposure to Malicious Content from User Behavior, *Proc. 2018 ACM SIGSAC Conference on Computer and Communications Security* (*CCS'18*), pp.1487–1501 (2018).
[25] Wu, L., Du, X. and Wu, J.: Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms, *IEEE Trans. Vehicular Technology*, Vol.65, No.8, pp.6678–6691 (2016).
[26] Pawan, P. et al.: PhishNet: Predictive Blacklisting to Detect Phishing Attacks, *Proc. 29th IEEE International Conference on Computer Communications* (*INFOCOM'10*), pp.346–350 (2010).
[27] Zhao, H., Chang, Z., Wang,W. and Zeng, X.: Malicious Domain Names Detection Algorithm Based on Lexical Analysis and Feature Quantification, *IEEE Access*, Vol.7, pp.128990–128999 (2019).
[28] Zouina, M. and Outtaj, B.: A novel lightweight URL phishing detection system using SVM and similarity index, *Human-centric Computing and Information Sciences*, Vol.7, No.17, pp.1–13 (2017).
[29] Ma, J., Saul, K.L, Savage, S. and Voelker, M.G.: Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs, *Proc. 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (*KDD'09*), pp.1245–1254 (2009).

石原 聖

2019 年岡山大学工学部情報系学科卒業．2021 年同大学大学院自然科学研究科博士前期課程修了．コンピュータセキュリティに興味を持つ．

佐藤 将也 （正会員）

2010 年岡山大学工学情報工学科卒業．2012 年同大学大学院自然科学研究科博士前期課程修了．2014 年同大学院同研究科博士後期課程修了．2013 年日本学術振興会特別研究員（DC2）．2014 年岡山大学大学院自然科学研究科助教．2021 年岡山県立大学情報工学部准教授．博士（工学）．コンピュータセキュリティ，仮想化技術に興味を持つ．2012 年度情報処理学会論文賞受賞．電子情報通信学会，ACM 各会員．

山内 利宏 （正会員）

1998 年九州大学工学部情報工学科卒業．2000 年同大学大学院システム情報科学研究科修士課程修了．2002 年同大学院システム情報科学府博士後期課程修了．2001 年日本学術振興会特別研究員（DC2）．2002 年九州大学大学院システム情報科学研究院助手．2005 年岡山大学大学院自然科学研究科助教授．2007 年同准教授．2021 年同大学学術研究院自然科学学域教授．博士（工学）．オペレーティングシステム，コンピュータセキュリティに興味を持つ．2010 年度 JIP Outstanding Paper Award，2012 年度情報処理学会論文賞等受賞．電子情報通信学会，ACM，USENIX，IEEE 各会員．本会シニア会員．