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実証実験データによる評価

石原 聖[1]　佐藤 将也[1]　山内 利宏[1]

概要：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への対策として，我々は悪性 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 空間から収集した大量の 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，利用者を意図しない Web サイトへ誘導する悪性 Web サイトを発見する．また，発見した悪性 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．本稿では，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データに含まれる URL に対して，提案手法により構築したブラックリストとの照合を実施し，悪性 Web サイトへのアクセスの検知結果について述べる．また，Web 媒介型攻撃観測システムにより収集されたデータに含まれる Google Safe Browsing による検知結果と比較し，提案手法により構築したブラックリストの有効性を述べる．

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

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

Takashi Ishihara[1]　Masaya Sato[1]　Toshihiro Yamauchi[1]

Abstract: As a countermeasure against the attack that redirecting a user to unwanted websites, we proposed a method to generate blacklists for mobile devices by searching malicious websites. The method collects many HTML files from the web space using a crawler. Additionally, searching for HTML files that are highly likely to be malicious using keywords extracted from the known malicious websites to discover the new malicious websites. Then, the blacklist is generated using keywords extracted from discovered malicious websites. In this paper, we describe the results of detection of access to malicious websites by checking URLs in the data collected by a demonstration experiment against the blacklist generated by the proposed method. Besides, we describe the effectiveness of the blacklist generated by the proposed method by comparing it with the detection results of Google Safe Browsing in the data collected by the demonstration experiment.

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 2000 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伴い，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．また，リダイレ

[1] 岡山大学 大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University

クトにより複数の Web サイト（以降，経由サイト）を経由した後に目的の Web サイト（以降，遷移先サイト）へ誘導する．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は，遷移元サイト，経由サイト，および遷移先サイトといった複数の悪性 Web サイトを利用する．また，遷移元サイトからのリダイレクト先やリダイレクト数は，毎回同じであるとは限らないという特徴が報告されている [4]．遷移先サイトには，不審なアプリをインストールさせることが目的のサイト，機密情報の開示を促すサイト，および金銭の獲得を目的とした出会い系サイトやゲームサイトなどが確認されている [5], [6]．

このような攻撃への対策として，URL やドメイン名のブラックリストを利用する方法がある．しかし，悪性 Web サイトの IP アドレスやドメイン名が短期間のうちに変更され，ブラックリストによる対策を困難にする場合がある [7]．また，利用者の意図しない Web サイトへ誘導する攻撃について，セキュリティアプリによる遷移先サイトの検知率は十分ではない [8]．このため，利用者の意図しない Web サイトへ誘導する攻撃へ対策する必要がある．また，悪性 Web サイトの特徴を機械学習により検知する対策 [9], [10] があるものの，遷移先サイトについて，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 [8]．このため，教師データが事前に必要な機械学習を用いた対策は難しい．

そこで，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，我々は悪性 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 [11]．提案手法は，クローラを用いて Web 空間から収集した大量の 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 Web サイトを発見する．また，発見した悪性 Web サイトと悪性 Web サイトの通信データから抽出したキーワードをブラックリストに登録する．

本稿では，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 [12] 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を評価した結果を報告する．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と提案手法により構築したブラックリストとの照合を実施し，悪性 Web サイトへのアクセスの検知結果について述べる．また，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に含まれる Google Safe Browsing（GSB）による検知結果と比較し，提案手法により構築したブラックリストの有効性を述べる．

表 1 悪性 Web サイトから抽出するキーワード

対象	抽出するキーワード
遷移元サイトの 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
経由サイトの URL	FQDN
遷移先サイトの URL	FQDN

2. 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 [11]

2.1 考え方

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，URL や FQDN のブラックリストの利用が有効であると推察する．URL や FQDN のブラックリストを利用することによって，遷移元サイトへのアクセスを未然に検知するだけでなく，リダイレクトによる経由サイトや遷移先サイトへのアクセスを検知する効果が期待できる．

提案手法は，探索により発見した遷移元サイトの 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．遷移元サイトには，利用者を遷移先サイトまで遷移させる起点となるファイル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，文献 [4] より，経由サイトの 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．さらに，遷移先サイトの 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，経由サイトと遷移先サイトの URL から FQDN をキーワードとして抽出する．

2.2 基本方式

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．データ収集部では，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．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）を発見する．また，悪性見込 URL の悪性判定を行う．抽出部では，悪性と判定

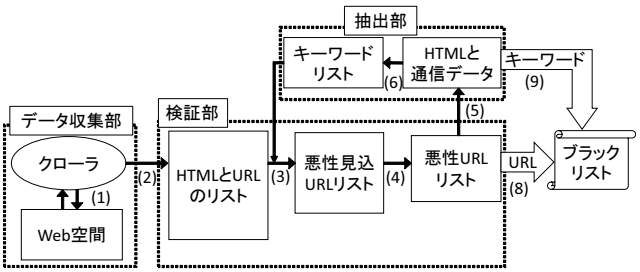

図 1 提案手法の処理流れ

された Web サイトの通信データを分析し，キーワードリストの拡張とブラックリストの構築に用いるキーワードを抽出する．

提案手法におけるブラックリスト構築の処理流れを**図 1** 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) クロール先の URL と HTML ファイルを保存
(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) 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て，悪性 Web サイトにアクセスした際の通信データを取得
(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) 拡張したキーワードリストを用いて，悪性見込 URL が見つからなくなるまで (3)〜(6) を繰り返し
(8) 悪性 URL リストの URL をブラックリストに登録
(9) 抽出したキーワードをブラックリストに登録

なお，本手法ではクロールする URL を Twitter の Streaming API の statuses/filter を利用して収集する．これは，攻撃者が Twitter や Facebook などの SNS に悪性 Web サイトの URL を投稿するという手口があるためである [14]．また，本手法では 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遷移先サイトへ誘導されるか否かを確認することで，Web サイトの悪性判定を行う．手動でのアクセスは手間がかかるものの，本手法では悪性見込 URL リストだけをチェックするため，チェックする Web サイト数は多くない．

3. WarpDrive 実証実験データセットを用いた評価

3.1 WarpDrive 実証実験データセット

3.1.1 WarpDrive

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）[15] がある．近年 Web 媒介型攻撃がスマートフォンに拡大していることから，WarpDrive 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を提案している [12], [16]．このシステムは，ユーザのスマートフォンにインストールするセンサアプリとデータを収集して分析するデータ収集・分析サーバから構成される．ユーザがスマートフォンにおいて Web ブラウザや他のアプリを操作すると，Web ブラウザの履歴やアプリの表示履歴がセンサアプリによってデータ収集・分析サーバへと送信される．なお，このシステムは，アプリの実装における制限が比較的少ない Android を対象にしている．

3.1.2 実証実験データセット

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．詳細は WarpDrive スマホ向け実証実験の参加規約 [17] に記載されている．

評価に用いたデータは，2020 年 7 月 1 日から 2020 年 7 月 31 日の期間に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のセンサアプリからデータ収集・分析サーバに送信された実証実験データである．このデータには最大で 2020 年 5 月 28 日まで前のユーザの Web アクセス履歴から 2020 年 7 月 31 日までのユーザの Web アクセス履歴が含まれている．また，このデータには，1,015,690 件の URL が含まれている．

3.2 ブラックリストの構築

実際のブラックリストの利用を想定し，実証実験データの Web アクセス履歴に含まれる日付よりも前に構築したブラックリストを評価に用いる．本評価に用いる実証実験データには，2020 年 5 月 28 日の Web アクセス履歴が含まれる．このため，2020 年 5 月 28 日より前の 2020 年 3 月 4 日に構築したブラックリストを評価に利用する．

2019 年 7 月 23 日から 2020 年 3 月 4 日の間で 2.2 節の提案手法の (1)〜(9) まで手順を行い，ブラックリストを構築した．**表 2** に，提案手法の実施結果を示す．2019 年 7 月 23 日から 2020 年 3 月 4 日の間でクロールした URL は 165,729 件であった．また，165,729 件の URL のうち，発見した遷移元サイト数は 242 件であり，ユニークな FQDN をもつ遷移元サイト数は 73 件であった．発見した遷移元サイトにアクセスした際の通信データから，118 個のキーワードを抽出し，ブラックリストに登録した．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 113 個であった．

表 2　提案手法の実施結果

提案手法の実施期間	2019 年 7 月 23 日～2020 年 3 月 4 日
クロールした URL 数	165,729 件
発見した遷移元サイト数 （ユニークな FQDN 数）	242 件 （73 件）
ブラックリストの内容	ファイル名：5 個 FQDN：113 個

表 3　検知 URL へのアクセス環境

OS	Android 7.1.2
CPU	Snapdragon 617, 1.5 GHz
メモリ	2 GB
Google Chrome	84.0.4147.105
通信環境	Y!mobile (Softbank)
端末	Kyocera DuraForce Pro KC-S702

3.3　評価の目的と方法

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，真陽性と偽陽性の数について評価を行う．ここで，真陽性は悪性 Web サイトを悪性と正しく判断したもの，偽陽性は良性 Web サイトを悪性と誤って判断してしまったものと定義する．

2020 年 7 月 1 日から 2020 年 7 月 31 日の期間にデータ収集・分析サーバへ送信された実証実験データに含まれる URL に対して，3.2 節のブラックリストのキーワードと照合する．また，照合により検知した 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．具体的には，検知 URL にアクセスし，遷移先サイトへの遷移が発生した場合，悪性 Web サイトと判断する．また，検知 URL が遷移先サイトである場合がある．実証実験データからはユーザごとにサイト遷移の履歴を確認できるため，検知 URL にアクセスする前にユーザがアクセスした Web サイトにアクセスし，遷移先サイトへ遷移が発生するか否かを確認する．遷移先サイトへの遷移が発生した場合，遷移先サイトと検知 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．なお，同じ FQDN をもつ検知 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 サイトと判断する．検知 URL へのアクセスは，**表 3** に示す Android 端末を用いて実施した．

実証実験データには，Web アクセス履歴の各 URL ごとに，GSB による検知結果が含まれる．また，GSB による検知結果は脅威のタイプが含まれる．そこで，GSB とブラックリストによる検知結果を比較し，提案手法の有効性を評価する．

表 4　ブラックリストによる検知結果

検知 URL に 含まれるキーワード	真陽性数 (重複排除後)	偽陽性数 (重複排除後)
キーワード 1（ファイル名）	62	0
キーワード 2（FQDN）	48	0
キーワード 3（FQDN）	28	3
キーワード 4（FQDN）	25	0
キーワード 5（FQDN）	9	9
キーワード 6（FQDN）	7	0
キーワード 7（FQDN）	6	0
キーワード 8（FQDN）	5	0
キーワード 9（FQDN）	5	0
キーワード 10（FQDN）	3	0
キーワード 11（FQDN）	2	0
キーワード 12（FQDN）	2	0
キーワード 13（FQDN）	2	0
キーワード 14（FQDN）	2	0
キーワード 15（FQDN）	2	0
キーワード 16（FQDN）	2	0
キーワード 17（ファイル名）	1	0
キーワード 18（FQDN）	1	0
キーワード 19（FQDN）	1	0
キーワード 20（FQDN）	1	0
キーワード 21（FQDN）	1	0
キーワード 22（FQDN）	1	0
キーワード 23（FQDN）	1	0
合計	217（196）	12（12）

3.4　評価結果と考察

3.4.1　キーワードの分析

表 4 に実証実験データに含まれる URL に対してブラックリストのキーワードとの照合を実施した際の検知結果を示す．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 21 種類である．検知結果について，真陽性数は 217 件であり，偽陽性数は 12 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 が真陽性数の中に 21 件含まれるため，重複を排除した真陽性数は 196 件である．なお，偽陽性数の中には，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．

表 4 より，キーワード 1（ファイル名）により 62 件の悪性 Web サイトを検知したことがわかる．検知 URL のうち，キーワード 1（ファイル名）というファイルを提供する FQDN は 14 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わかる．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．

また，表 4 より，キーワード 2（FQDN）により 48 件の悪性 Web サイトを検知したことがわかる．キーワード 2（FQDN）により検知した悪性 Web サイトは遷移先サイトであった．また，この遷移先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 をもつ 10 件の遷移元サイトを発見した．このことから，複数の遷移元サイトから，同じ遷移先サイトへ遷移していることがわかる．このように遷移元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遷移先サイトへのアクセスを検知できる．

23 種類のキーワードにより検知した URL のうち，18 種類のキーワードにより検知した URL は遷移先サイトにリダイレクトする Web サイトであった．また，5 種類のキーワードにより検知した URL は遷移先サイトであった．遷移先サイトには，カジノサイトが 2 種類，偽の警告を表示しクリーナアプリのインストールを促すサイトが 2 種類，および投資用の口座開設を促すサイトが 1 種類存在した．このような遷移先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 [18]．また，モバイル端末の利用者を遷移先サイトにリダイレクトさせ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る [19], [20]．提案手法により構築したブラックリストを利用することで，不正な広告などによる利用者の意図しないリダイレクトで誘導される悪性 Web サイトを検知できる．

3.4.2 偽陽性の事例

偽陽性と判断した 12 件の URL について以下で説明する．

(1) キーワード 3（FQDN）による 3 件の事例
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 が検知されていた．これは，キーワード 3（FQDN）を FQDN にもつ URL をクエリ文字列に含んでいたためである．このように，悪性な FQDN をもつ 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．なお，クエリ文字列に含まれていたキーワード 3（FQDN）を FQDN にもつ URL は，セキュリティアプリによる検知結果のクエリ文字列に “&Type=不正プログラム配信&Rating=危険” が含まれていることから，悪性である可能性が高い．

(2) キーワード 5（FQDN）による 9 件の事例
キーワード 5（FQDN）を FQDN にもつ URL にアクセスした際，真っ白な画面が表示され，遷移は発生しなかった．また，キーワード 5（FQDN）を FQDN にもつ URL への遷移元サイトと推察される Web サイトでは遷移が発生したものの，キーワード 5（FQDN）を FQDN にもつ URL への遷移は発生しなかった．このため，偽陽性とみなした．ただし，遷移先サイトであるキーワード 2（FQDN）を FQDN にもつ URL では，キーワード 5（FQDN）をリファラに持つ事例があった．このことから，キーワード 5（FQDN）を FQDN にもつ URL は，経由サイトとして利用されている可能性がある．

表 5 GSB による検知結果

GSB が検知した悪性 Web サイト	検知数 (GSB)	検知数 (ブラックリスト)	GSB による脅威タイプ情報
FQDN A	23	4	MALWARE
FQDN B	5	0	MALWARE
FQDN C	1	0	SOCIAL ENGINEERING
FQDN D	1	0	SOCIAL ENGINEERING
FQDN E	1	0	SOCIAL ENGINEERING
FQDN F	1	0	SOCIAL ENGINEERING
FQDN G	1	0	UNWANTED SOFTWARE
FQDN H	1	0	MALWARE
FQDN I	1	0	MALWARE
FQDN J	1	0	MALWARE
FQDN K	1	0	MALWARE
FQDN L	1	0	MALWARE
FQDN M	1	0	MALWARE
FQDN N	1	0	MALWARE
FQDN O	1	0	MALWARE
合計	41	4	

検知結果について，偽陽性と判断した URL は 12 件あるものの，これらの URL は上述のように悪性である可能性が高い．このことから，提案手法により構築したブラックリストは誤検知が少なく，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考える．

3.5 Google Safe Browsing による検知結果との比較

表 5 に GSB による悪性 Web サイトの検知結果を示す．Web アクセス履歴のうち，GSB による検知数は 41 件であった．表 4 に示すブラックリストによる検知結果と比べ，GSB により検知できる Web サイト数は多くない．これは，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 [21] であるからだと考える．リダイレクトで誘導される悪性 Web サイトには，他の Web サイトへの誘導が目的の経由サイトや広告収入を目的とした遷移先サイトなどがあり，これらは利用者のプライバシやセキュリティを脅かさない．このため，これらの悪性 Web サイトは GSB では悪性と判断されない可能性が高い．一方で，提案手法により構築したブラックリストは，リダイレクトで誘導される利用者のプライバシやセキュリティを脅かさない経由サイトや遷移先サイトを検知できる．これにより，利用者が遷移先サイトに誘導されることにより受ける被害を防止できる．また，広告収入などによる攻撃者の利益の増加を抑制できる．

提案手法により構築したブラックリストは，GSB による検知 URL のうち FQDN A の URL を 4 件検知した．また，

FQDN A の 4 件の URL は表 4 に示すキーワード 1（ファイル名）により検知した．悪性 Web サイトでは共通のファイル名が使われることが多い．このことから，FQDN がブラックリストに登録されていない場合でも，提案手法により構築したブラックリストを用いることで，ファイル名による検知が可能であることがわかる．

提案手法により構築したブラックリストでは検知できない URL がある．FQDN A の URL のうちブラックリストで検知できなかった 19 件は，URL にキーワード 1（ファイル名）を利用していなかった．FQDN H〜O は，同じドメインを用いており，このドメインはフィッシングサイトへ誘導するショートメッセージ (SMS) での利用が報告されている [22]．このことから，FQDN H〜O の URL にアクセスしたユーザは，SMS から誘導されたと推察する．提案手法により構築するブラックリストは，Twitter から収集した URL をもとに構築したため，SMS から誘導される悪性 Web サイトを検知できなかったと考える．一方で，GSB はこれらの悪性 Web サイトを検知できる．

以上より，提案手法により構築したブラックリストと GSB を併用することで，利用者の意図しないリダイレクトにより誘導された Web サイトと利用者のプライバシやセキュリティを脅かす Web サイトの双方を検知できることがわかる．

4. 研究倫理

実証実験では，取得データは個人情報を含まないパーソナルデータとして取り扱われる．パーソナルデータは，個人情報削除フィルタを適用して取得されており，取得データは合理的に可能な範囲で，ほかの情報と容易に照合できない [17]．

本稿で行った評価では，同じ FQDN をもつ検知 URL が複数ある場合，1 件の検知した URL が悪性であれば，同じ FQDN をもつ URL すべてを悪性とみなすことで，Web アクセスの回数を減らしている．これにより，アクセス先へのサーバへの負荷を低減できる．

本稿で扱った利用者の意図しない Web サイトへ誘導する攻撃は，iPhone などの iOS 端末でも確認されており [26]，Android 端末固有の攻撃ではない．ユーザ参加型の Web 媒介型攻撃観測システムは Android を対象としてデータを収集する．このため，本稿では検知 URL について，Android 端末を用いて遷移先サイトへの遷移が発生するか否かを確認した．しかし，iOS 端末を用いて遷移先サイトへの遷移が発生するか否かを確認した場合でも，同様の結果が得られる可能性がある．

5. 関連研究

悪性 Web サイトへの対策として，ブラックリストに着目した研究がある．文献 [7] では，Web 空間から新しい悪意のある URL を自動的に収集し，自動でブラックリストを生成する AutoBLG を提案している．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 [23] は，主要な Web ブラウザで利用されているブラックリストへの悪性 Web サイトの登録やその速さついて，クローキング技術が与える影響を測定している．文献 [24] は，3 つの主要なブラックリストについて，ブラックリストに含まれる URL の数や期間，ブラックリスト間の URL の重複と検知時間などを分析している．文献 [23], [24] はブラックリストの有効性について述べているものの，利用者の意図しない Web サイトへ誘導する攻撃への対策については検討されていない．

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がいくつか存在する．文献 [9] 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 [10] 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どうかを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 [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 [9], [10] 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問題がある [7]．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] 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. おわりに

本稿では，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について，WarpDrive 実証実験データを用いて行った評価結果について述べた．評価には，2019 年 7 月 23 日から 2020 年 3 月 4 日の間に悪性 Web サイトを探索し，発見した遷移元サイトから抽出した 118 個のキーワードを用いて構築したブラックリストを用いた．また，2020 年 7 月 1 日から 2020 年 7 月 31 日における実証実験データに含まれる URL に対してブラックリストのキーワードとの照合を行い，悪性 Web サイトの検知を実施した．

検知結果から，提案手法により構築したブラックリストは，少ない誤検知数でリダイレクトにより誘導される悪性 Web サイトを検知できることを示した．さらに，実証実験データに含まれる GSB による検知結果とブラックリストによる検知結果の比較を実施した．ブラックリストによる検知結果と比べ，GSB により検知できる Web サイト数は多くない．これは，GSB が検知する Web サイトは利用者のプライバシやセキュリティを脅かすものであるからだと考える．一方で，提案手法により構築したブラックリストは，他の Web サイトへの誘導が目的の経由サイトや広告収入を目的とした遷移先サイトなど利用者のプライバシやセキュリティを脅かさない Web サイトを検知できることを示した．

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．

参考文献

[1] DataReportal: Digital 2020: Global Digital Overview (online), available from ⟨https://datareportal.com/reports/digital-2020-global-digital-overview⟩ (accessed 2020-08-07).

[2] Clement, J: Percentage of mobile device website traffic worldwide from 1st quarter 2015 to 2nd quarter 2020 (online), 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 (online), 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., Yamauchi, T.: Threat Analysis of Fake Virus Alerts Using WebView Monitor, *Proc. The Seventh International Symposium on Computing and Networking (CANDAR)*, pp.28–36 (2019).

[5] Doevan, J.: Android virus. Versions provided. The list of infected apps for 2020 (online), 2-spyware, available from ⟨https://www.2-spyware.com/remove-android-virus.html⟩ (accessed 2020-08-07).

[6] 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）．

[7] Bo, S., Akiyama, M., Takeshi, T. and Hatada, M.: Automating URL Blacklist Generation with Similarity Search Approach, *IEICE Transactions on Information and Systems*, vol.99, no.4, pp.873–882 (2016).

[8] 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)．

[9] Amrutkar, C., Kim, Y. S. and Traynor, P.: Detecting Mobile Malicious WebPages in Real Time, *IEEE Transactions on Mobile Computing*, vol.16, no.8, pp.2184–2197 (2017).

[10] 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)*, pp.1487–1501 (2018).

[11] 石原聖，折戸凜太郎，佐藤将也，山内利宏：モバイル向け悪性 Web サイトの探索によるブラックリスト構築手法，コンピュータセキュリティシンポジウム 2019（CSS2019）論文集，pp.1017–1024（2019）．

[12] 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）．

[13] Invernizzi, L., Comparetti, P. M.: Evilseed: A Guided Approach to Finding Malicious Web Pages, *Proc. 2012 IEEE Symposium on Security and Privacy*, pp.428–442 (2012).

[14] Calyptix Security: Social Media Threats: Facebook Malware, Twitter Phishing, and More (online), available from ⟨https://www.calyptix.com/top-threats/social-media-threats-facebook-malware-twitter-phishing/⟩ (accessed 2020-08-07).

[15] WarpDrive，入手先 ⟨https://warpdrive-project.jp/index.html⟩ (参照 2020-08-07).

[16] WarpDrive：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/index.html⟩ (参照 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] 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 (オンライン)，入手先 ⟨https://blog.trendmicro.co.jp/archives/14307⟩ (参照 2020-08-15).

[19] GeoEdge: AUTO-REDIRECTS (online), available from ⟨https://site.geoedge.com/downloads/documents/Auto_Redirects.pdf⟩ (accessed 2020-08-15).

[20] GeoEdge: GeoEdge Researchers Uncover Malicious Auto-Redirect Ads in Programmatic VPAID Video inserted in Sandboxed iFrames (online), available from ⟨https://www.globenewswire.com/news-release/2019/09/20/1918541/0/en/GeoEdge-Researchers-Uncover-Malicious-Auto-Redirect-Ads-in-Programmatic-VPAID-Video-inserted-in-Sandboxed-iFrames.html⟩ (accessed 2020-08-15).

[21] Google Safe Browsing - Google Transparency Report，入手先 ⟨https://transparencyreport.google.com/safe-browsing/overview⟩ (参照 2020-08-18).

[22] フィッシング対策協議会：宅配便の不在通知を装うフィッシング (2020/07/09)，入手先 ⟨https://www.antiphishing.jp/news/alert/fuzaiSMS_20200709.html⟩ (参照 2020-08-18).

[23] Oest, A., Safaei, Y., Doupe, A., Ahn, G., Wardman, B. and Tyers, K.: PhishFarm: A Scalable Framework for Measuring the Effectiveness of Evasion Techniques Against Browser Phishing Blacklists *Proc. 40th IEEE Symposium on Security and Privacy*, pp.764–781 (2019).

[24] Bell, S. and Komisarczuk, P.: An Analysis of Phishing Blacklists: Google Safe Browsing, OpenPhish, and PhishTank, *Proc. 2020 Australasian Computer Science Week (ASCW)*, pp.1–3 (2020).

[25] Wu, L., Du, X. and Wu, J.: Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms, *IEEE Transactions on Vehicular Technology*, vol.65,

pp.6678–6691 (2016).
[26] IPA 独立行政法人 情報処理推進機構：安心相談窓口だより，入手先 ⟨https://www.ipa.go.jp/security/anshin/mgdayori20190918.html⟩ (参照 2020-08-09).