Computer Security Symposium 2020
26 - 29 October 2020

プロアクティブなユーザ保護に向けた Webアクセスパスの分析とドメインリスク評価手法の提案

高橋 健志[1,a)]　Christopher Kruegel[2]　Giovanni Vigna[2]　吉岡 克成[3]　井上 大介[1]

概要：Web アクセスにはマルウェア感染やソーシャルエンジニアリング攻撃などの脅威が存在する．Web ユーザを保護すべく各種の技術が実装されてきているが，悪性 URL に到達するユーザは依然存在する．そこで我々は，ユーザが悪性 URL にどのように到達するのかを理解すべく，ブラウザ拡張を用意して web アクセス記録を収集し，そこから悪性 URL にユーザが到達するまでの経路 (悪性 URL 到達経路) を抽出する方式を提案する．そして，すべての悪性 URL 到達経路を抽出・分析することにより，悪性 URL 到達経路の最初のアクセス (エントリーポイント) に占めるブックマークアクセスの割合が高いことを示す．同時にブックマークされたサイトのドメインのリスクレベルを算出し，悪性 URL に到達する可能性の高いブックマークエントリーが存在することを示す．また，エントリーポイントに限らず悪性 URL 到達経路上にある全 URL のドメインのリスクレベルを評価し，悪性 URL に到達する可能性の高いドメインを特定する方式を提案する．評価実験では，本方式がブラックリストに掲載されていない危険なドメインを特定し，ユーザが悪性 URL に到達するリスクを低減できることを示す．

Proactive User Protection based on Web Access Path Analysis and Domain Risk Evaluation

Takeshi Takahashi[1,a)]　Christopher Kruegel[2]　Giovanni Vigna[2]　Katsunari Yoshioka[3]
Daisuke Inoue[1]

Abstract: Web access exposes users to diverse types of attacks, including malware infections and social engineering attacks. To protect web users, various techniques have been implemented; however, some users continue to access malicious URLs. In this paper, we collect web access records of users from their using our browser extension and analyze them to understand how users reach such URLs. We then propose a scheme to extract an entire web access path to a malicious URL from the access records. By analyzing all the web access paths, we reveal that bookmark access is a major entry point to such paths. We also show that some bookmark entries often lead to malicious URLs. In addition, we propose a domain risk evaluation scheme that analyzes the risk level of all domains on the web access paths. We demonstrate the effectiveness of the scheme by identifying hazardous domains that are not included in blacklists.

1. はじめに

インターネットは必要不可欠な社会基盤となっており，多くの人々が日常生活の中で web にアクセスする．しかしながら，web ユーザはマルウェア感染やソーシャルエンジニアリング攻撃など，様々な種類の攻撃をうけるリスクを抱えている．悪性 URL へのアクセスを回避すべく，各種のブラックリストなどが活用されてきているものの，それでも悪性 URL に到達するユーザが存在する．そこで本稿では，ユーザ単位での web アクセス活動を分析すべく，ユーザ側にてデータを収集し，ユーザが悪性 URL に到達する経路を分析し，ユーザ保護のための対策技術を提案する．

まず最初に，我々の用意したブラウザ拡張を通じ，18 ヶ月間で平均 1590 人/月のユーザから合計 6,547,557,703 件

[1] 情報通信研究機構, National Institute of Information and Communications Technology
[2] University of California, Santa Barbara
[3] 横浜国立大学, Yokohama National University
[a)] takeshi_takahashi@nict.go.jp

のアクセス記録をユーザ側で収集する．ユーザ側でのデータ収集により，ユーザ ID やブラウザタブ ID，ナビゲーション情報など，ネットワークトラフィックからは得られない情報にアクセス可能になるため，ユーザの振る舞いをより精緻に分析可能となる．

そして，収集したアクセス記録から悪性 URL への web アクセスパス，すなわち悪性 URL 到達経路を抽出する手法を提案する．提案方式は，悪性 URL 到達経路を再構築するために，その最初のアクセス，すなわちエントリーポイントに到達するまで繰り返し一つ前のアクセスを追跡する．本方式はユーザとブラウザタブを識別することにより，アクセス記録の分析対象領域を絞り込む点に特徴があり，悪性 URL 到達経路を効率的に再構築する．

次に，抽出されたアクセスパス情報に基づき，我々は悪性 URL 到達経路のエントリーポイントを分析する．そして，アクセス数ベースで悪性 URL 到達経路の最大のエントリーポイントがブックマークアクセスであり，かつその割合はすべての経路上より悪性 URL 到達経路にて顕著に増大することを示す．さらに，悪性 URL に到達する確率を示すパラメータを定義し，ブックマークされた URL のリスクレベルを分析する．そして悪性 URL に確実に到達するブックマークエントリーが存在することを示し，ブックマークエントリーのレビューを実施することにより悪性 URL に到達するリスクを低減できる可能性を示す．

また，悪性 URL に到達する可能性の高いドメインを特定するドメインリスク評価手法を提案する．非悪性ドメインの中には，悪性 URL にしばしばユーザが到達するものも存在しており，そのようなドメインを特定すべく，本手法は悪性 URL 到達経路上に現れるすべてのドメインのリスクレベルを評価する．これらのドメイン自体は悪性コンテンツをホストしていなくとも，その先のアクセスで悪性 URL に到達するため，提案手法はこれらのドメインでトラフィックを遮断する，もしくは警告を発することにより，ユーザが悪性 URL に到達するのを阻止可能にする．評価実験では，ブラックリストに登録されていない危険なドメインを 820 個特定し，その有効性を示す．

2. ユーザ側でのデータ収集

我々は Chrome ブラウザ用の拡張 [1] を用意し，Web アクセス記録をユーザ側にて収集した．本拡張はセンサとして動作し，各ユーザの web アクセス活動を記録し，定期的にその記録をサーバに送信する．本拡張およびその配布ページは日本語にて提供されている．本節では，ユーザの獲得方法，収集データ，研究倫理，アクセスログの補完，そして生成した分析用データセットについて説明する．

ユーザの獲得方法　我々のブラウザー拡張をインストールし，かつ継続して利用してくれるユーザを確保すべく，我々は人々が自らこのブラウザ拡張に興味を持って頂けるよう工夫した．具体的には，タチコマと呼ばれる攻殻機動隊のキャラクターを導入した [2]．我々のブラウザ拡張を利用するとタチコマに会えるため，攻殻機動隊が好きな人々は好んで我々のブラウザ拡張を利用してくれることを狙った．

収集データ　一件のアクセス記録は次の計 11 個のデータにて構成される．(1) HTTP リクエストの **URL**，(2) そのリクエスト発行時刻を示す **timestamp**，(3) **referer**，(4) ブラウザタブを識別する**タブ ID**(その一意性は同一セッションの中でのみ保証)，(5) ブラウザタブに示される URL(**タブ URL**)，(6) メインフレームや画像，フォント，スクリプトなどを識別する**リソース種別**，(7) ブックマークアクセス，再読込，URL タイピングなどを識別する**ページ遷移種別**，(8) **ユーザ ID**，(9) 現在のタブの生成元タブの ID(**ソースタブ ID**) (例えば target=”_blank”や window.open() などにより，新しいウィンドウが生成された際にソースタブ ID を記録)，(10) URL の **Google Safe Browsing (GSB) [3] 評価結果**，(11) **Alexa Traffic Rank** の順位 (トップ 1,000 まで評価)[4]．尚，リソース種別およびページ遷移種別については，Google Chrome APIs[5] である webRequest および history にて定義された値をそのまま取得している．また，GSB 評価結果及び Alexa Traffic Rank については，一日一回，当日に収集したすべての URL を集約して GSB および Alexa Top Site にて評価を実施して取得している．

研究倫理　本研究の実施にあたり，我々のログの利用方法が倫理的に問題がなく，ユーザのプライバシに配慮していることを研究倫理委員会に確認している[*1]．ブラウザ拡張の利用規約では収集するデータ項目の一覧を明示し，それらを悪性 URL へのアクセスを検知・阻止する分析に利用することを明記し，ユーザは本利用規約に合意した後でのみ本拡張を取得可能となっている [1]．また，収集データの利用には制約を課し，プライバシに配慮している．具体的には，個人を特定可能な情報は保存せずに削除し，各ユーザ固有の値であるユーザ ID を個人を特定する情報とリンクせず，生 URL の外部共有を禁止[*2]し，さらに，各ユーザのログ削除要求にも対応している．同時に，アクセス制御などを含む各種のセキュリティ対策も講じている．

アクセスログの補完　通常，一つのページにアクセスすると，メインフレーム，イメージ，スクリプトなど，複数のコンテンツがリクエストされるが，我々のデータ収集では存在すべきメインフレームのログが欠落することがある．その原因として次の 3 つが考えられる．第一に，データ収集モジュールの実装が不完全である．センサがリクエ

[*1] 正確には，外部の有識者から構成される第三者委員会，および情報通信研究機構内部に設置されているパーソナルデータ取扱研究開発業務審議委員会にて審議．

[*2] そのため，生 URL のアップロードを求める VirusTotal[6] ではなく，それが不要な GSB を利用して URL の悪性を判定．

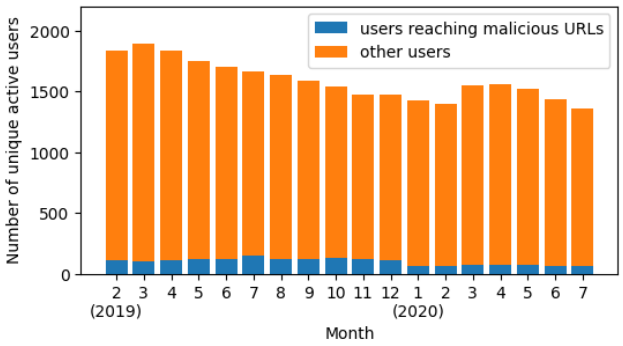

図 1　月別のユニークなアクティブユーザ数の推移

ストに対するレスポンスを受取る前に，ユーザが別のページに遷移すると，当該アクセスに関する情報の一部もしくはすべてが記録されないケースが発生する．第二に，ユーザはデータ収集を避けるよう設定可能である．本センサは，ユーザが事前に指定した URL およびドメインへのアクセスは記録しない．また，ユーザがシークレットモードで web アクセスした場合や，センサ自体を無効化して web アクセスをされた場合にもログは記録されない．第三に，Chrome ブラウザは，処理負荷が高くなると，想定された通りのデータを出力しない．我々の分析ではメインフレームの存在が重要であるため，メインフレームのログが欠落している際には，URL フィールドにはタブ URL の値を，タイムスタンプには同一タブ URL が記録されている複数リクエストのうち最初のものの値をセットすることにより，ログから欠落しているメインフレームの記録を補完する．

データセット　2019 年 2 月 1 日から 2020 年 7 月 31 日までに収集した 6,547,557,703 件のアクセス記録を本論文ではデータセットとして用いる．そのうち 92,603 件は悪性 URL へのアクセス記録である．図 1 は月毎のアクティブユーザ (一度でも web ブラウジング活動が記録されたユーザ) 数を示す．平均で 1,590 人/月のアクティブユーザが存在し，そのうち 99 人/月は悪性 URL にアクセスしている．本稿のすべての実験は本データセットを用いて実施する．

3.　悪性 URL 到達経路の再構築

本節では悪性 URL 到達経路を再構築する手法を提案する．提案方式は，悪性 URL 到達経路のエントリーポイントに到達するまで繰り返し一つ前のアクセスを追跡する．

3.1　一つ前のアクセスの追跡

図 2 に我々の追跡手法の概要を示す．ページ遷移種別が”reload”である場合には，現在のページが再読込されたページと判断し，**再読込追跡**を実施する．再読込追跡では，現在のアクセス記録と同一のタブ URL および URL を持つ直近のアクセス記録を探す．その際には，まずは同一タブ内のアクセス記録を調査し，該当がない場合に限りその

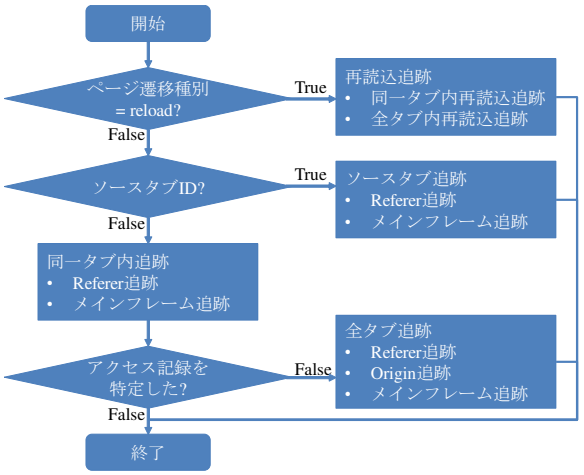

図 2　一つ前のアクセスを追跡するプロセスフロー

他のタブのアクセス記録を調査する．

ソースタブ ID が指定されている場合には，現在のアクセスが指定されたタブから生成されたと判断し，そのタブ内のアクセス記録を追跡する**ソースタブ追跡**を実施する．referer 情報が入手可能な際には，現在のアクセスから直前のメインフレームアクセスまでの間のアクセス記録のうち，URL が referer と一致するものを一つ前のアクセス記録として選択する (referer 追跡) が，referer 情報が提供されない，もしくは適切な記録が発見できない場合には，直前のメインフレームへのアクセス記録を一つ前のアクセス記録として選択する (メインフレーム追跡)．

上記以外のケースでは，同一タブ内にて一つ前のアクセス記録を追跡する**同一タブ内追跡**を実施する．ソースタブ追跡手法同様，referer 追跡とメインフレーム追跡技術を用いて記録を分析し，現在のタブ上のユーザの過去のアクセス記録から一つ前のアクセス記録を特定する．

もし適切な記録が発見できない際には，当該ユーザのすべての記録内を追跡する**全タブ追跡**を実施する．ソースタブ追跡と同一タブ内追跡同様，referer 情報が存在する場合にはまず referer 追跡を実施する．referer が origin 情報のみ保持しているケースでは，全タブ追跡では origin が一致する URL を持つ直前のメインフレームのアクセス記録を一つ前のアクセスとして決定する (origin 追跡)．尚，ソースタブ追跡及び同一タブ内追跡ではメインフレーム追跡により一つ前のアクセスの特定が高精度で実現できるため，origin 追跡は実施されない点に留意されたい．もし以上の処理で適切なエントリーが発見できない際には，全タブ追跡はメインフレーム追跡を実施可能である．但し，本手法は信頼性の高い追跡ができるとは限らないため，本論文では以降の分析にて本追跡は実施しない．

通常の web アクセスログを分析する限りにおいては，提案方式は単一ユーザの単一タブに属するログのみを追跡するケースが大半となるため，効率的に悪性 URL 到達経路の再構築が可能となる．

3.2 アクセスパスのエントリーポイント特定

第 3.1 節に記載したプロセスは，悪性 URL 到達経路へのエントリーポイントを特定するまで繰り返し実行される．ここで，我々はエントリーポイントを一つ前のアクセスと非連続なアクセスと定義しており，下記のものが存在する．

ブックマークアクセス ページ遷移種別が”auto_bookmark”であった際には，ユーザは現在のページにブックマークを選択して来訪したと判断する．

セッションの再構築 最近閉じたブラウザタブを復元するなどして，セッションの再構築が可能である．ページ遷移種別が”reload”であり，かつ同一のタブにて一定期間アクセスがなければ，セッションが再構築されたと判断する．

web 検索 サイト内検索は含まない．URL が主要検索エンジンのトップページと一致する，もしくはページ遷移種別が”form_submit”かつ URL が主要検索エンジンの検索結果ページである場合に，web 検索が実施されたと判断する．

オムニバーアクセス Chrome ブラウザのオムニバーは Google 検索ボックスとアドレスバーの機能を併せ持つ．ページ遷移種別が”generated”の際には，オムニバーを利用したアクセスであると判断する．

アドレス直接入力 ユーザは連続するブラウジング活動の一環として，アドレスバーにある現在の URL を編集して，トップページなどの別のページへ移動するケースが存在する．そのため，ページ推移種別が”typed”であるもののうち，直前のページと現在のページのドメインが異なる場合のみ，エントリーポイントとして判断する．

スタートページアクセス ページ遷移種別が”start_page”の際には，そのページがブラウザの起動により，プログラム引数もしくはデフォルト設定により開かれたと判断する．尚，外部アプリ上でリンクをクリックした際にも，OS 上にて Chrome がそのリンクの URL を引数として起動されるため，ページ遷移種別は”start_page”となる．

参考まで，表 1 に提案方式により再構成した悪性 URL 到達経路を例示する．

4. エントリーポイントの分析

本節では悪性 URL 到達経路のエントリーポイントを分析する．

4.1 エントリーポイント種別の順位評価

表 2 に 18 ヶ月間の悪性 URL 到達経路のエントリーポイント別アクセス数を測定した結果を示す．参考のため，非悪性 URL 到達経路を含むすべての経路におけるエントリーポイント別アクセス数も同表に示す．エントリーポイントの割合が最大のものはブックマークアクセスであり，その次が web 検索であった．セッションの再構築は第 3 位，オムニバーアクセスは第 4 位，第 5 位がアドレス入力であった．スタートページアクセスも悪性 URL 到達経路へのエントリーポイントとして発見されたが，その数は他のエントリーポイント種別と比較して小さい．上記の他，幾つかのエントリーポイントはリンクアクセスというラベルが付与されている．これらは，アクセス記録のページ遷移タイプが「リンク」であるものの，分析したログ内に適切な一つ前のアクセスが見つからず，そのアクセス記録が非連続になっているケースである．そのようなアクセスが発見できない理由として，(1) 本稿の分析は月単位で実施しているため，毎月の最初のアクセスより前のアクセスは追跡されないこと，(2) 第 2 節にて説明したログ収集の不完全性が挙げられる．このアクセス数での最上位に位置するブックマークアクセスについては第 4.2 節にて詳述する．

表 3 に，同期間の悪性 URL 到達経路のエントリーポイント別ユーザ数を測定した結果を示す．表 2 同様，非悪性 URL 到達経路を含むすべての経路におけるエントリーポイント別ユーザ数も同表に示す．表 2 とは異なり，表 3 では検索エンジン，ブックマークアクセス，オムニバーアクセス，セッション再構築，アドレス入力，スタートページアクセスの順にてユーザ数が多い結果となっている．このことから，一部のユーザがブックマークアクセスにより多数の悪性 URL に到達していることが分かる．また，検索エンジンにより悪性 URL に到達するケースはユーザ数ベースでは第一位であり，ブックマークアクセスよりも幅広いユーザが検索エンジンにより悪性 URL 到達経路に入っていることが分かる．ここで，検索エンジンから悪性 URL に至る特徴的なパターンが観測されたため，紹介する．ユーザは一般の検索エンジンにクエリーを投げることにより悪性 URL 到達経路に入っていくが，検索エンジンにクエリーを投げる前にそのクエリーとして記載するキーワードを web から取得するケースがしばしば観測された．例えば，正当なショッピングサイトにてポルノビデオの商品コードを見つけ出し，その商品コードを用いて web を検索し，ユーザは非合法的なサイトに到達し，悪性 URL へと導かれていく．このような特定のキーワードを用いた検索により，悪性 URL に到達するケースが相当数存在することは関連研究 [7] に報告されており，我々の発見を裏付けている．悪性 URL に到達する検索については関連研究 [7] に報告があるため，本稿では上述のブックマークアクセスに焦点を当て，分析を深化する．

上記議論の時系列変化の有無を確認すべく，図 3 および図 4 に，悪性 URL 到達経路のエントリーポイント別アクセス数の割合，およびユーザ数の割合を月単位の推移で示す．尚，図 4 の凡例は図 3 と同一であり，可読性向上のために省略した．2019 年 7 月は，アドレス入力により悪性 URL 到達経路に入っていく件数が特異に大きくなっている．しかしながら，ユーザ数別でみた図 4 では，同月の数

表 1　悪性 URL 到達経路抽出事例

時刻 (JST)	タブ ID	URL(抜粋)	ソースタブ ID	ページ遷移種別	リソース種別	追跡手法
15:26:57	182	http://javtorrent.re/category/		auto_bookmark	メインフレーム	同一タブ内追跡
15:27:14	182	http://javtorrent.re/?s=080819		form_submit	メインフレーム	同一タブ内追跡
15:27:26	182	http://javtorrent.re/uncensore		link	メインフレーム	同一タブ内追跡
15:28:28	182	http://javtorrent.re/?s=HEYZO-		form_submit	メインフレーム	同一タブ内追跡
		(omitted 18 access records)				
15:31:50	182	http://javtorrent.re/uncensore		link	メインフレーム	ソースタブ追跡
15:32:08	403	https://www.google.com/search?	182	link	メインフレーム	同一タブ内追跡
15:32:35	403	https://7mmtv.tv/zh/uncensored		link	メインフレーム	同一タブ内追跡
15:33:26	403	https://www.google.com/search?		link	メインフレーム	同一タブ内追跡
15:33:37	403	http://javhuge.com/Momoki%20		—	補完フレーム	同一タブ内追跡
15:33:37	403	http://javhuge.com/zb_users/th		—	スタイルシート	—

表 2　エントリーポイント別アクセス数

種別	悪性 URL 到達経路上	すべての経路上
ブックマークアクセス	4,062 (50.6%)	1,966,881 (38.1%)
検索エンジン	1,168 (14.5%)	840,709 (16.3%)
セッション再構築	985 (12.3%)	934,307 (18.1%)
オムニバーアクセス	789 (9.8%)	835,206 (16.2%)
アドレス入力	699 (8.7%)	131,794 (2.6%)
スタートページアクセス	237 (3.0%)	448,912 (8.7%)
リンクアクセス	94 (1.2%)	—
計	8,034 (100%)	5,157,809 (100%)

表 3　エントリーポイント別の月平均ユーザ数

種別	悪性 URL 到達経路上	すべての経路上
ブックマークアクセス	36 (26.2%)	1,039 (20.1%)
検索エンジン	41 (29.6%)	957 (18.5%)
セッション再構築	17 (12.5%)	973 (18.8%)
オムニバーアクセス	25 (18.3%)	802 (15.5%)
アドレス入力	7 (5.3%)	586 (11.4%)
スタートページアクセス	7 (4.8%)	807 (15.6%)
リンクアクセス	5 (3.3%)	—
計	139 (100%)	5,163 (100%)

値が特異なものにはなっていないことが確認できる．このことから，ごく少人数のユーザが悪性 URL に至る URL をアドレスバーに入力していていたと考えられる．総じて，月毎の若干のばらつきは存在するものの，大まかな傾向は時系列変化は特になく一定であると考えられる．

4.2　ブックマーク URL の分析

ブックマークされた URL のドメインのうち，悪性 URL に到達するリスクレベルが高いものを抽出する．ここで，悪性 URL に到達するリスクレベルを下式にて定義し，そのリスクレベルにより評価する．

$$R(domain) = \frac{NbrAccess_{malurl}(domain)}{NbrAccess_{all}(domain)} \quad (1)$$

ここで，$R(domain)$ は当該ドメインのリスクレベルを，$NbrAccess_{malurl}(domain)$ は当該ドメインのアクセス後に悪性 URL に到達する回数を，$NbrAccess_{all}(domain)$ は当該ドメインへのアクセス総数を指す．尚，悪性 URL が当

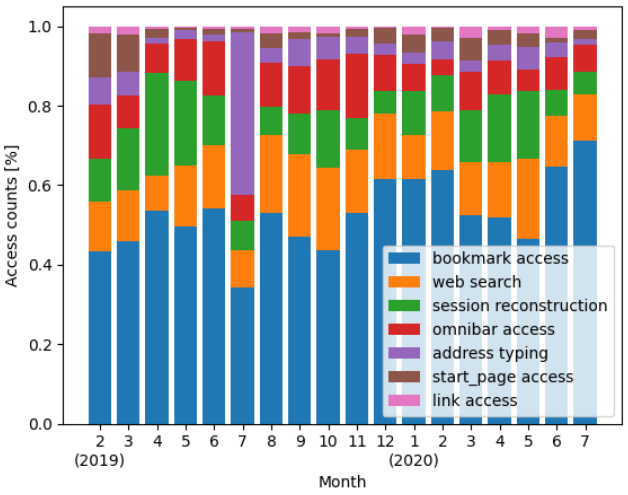

図 3　悪性 URL 到達経路のエントリーポイント別アクセス数の割合

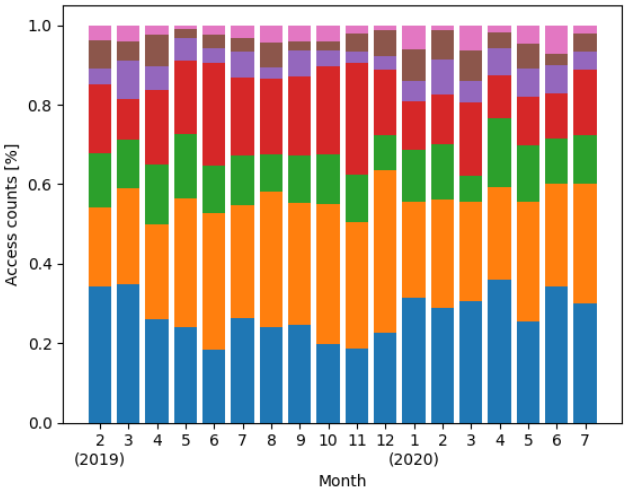

図 4　悪性 URL 到達経路のエントリーポイント別ユーザ数の割合

該ドメインの次のホップに存在するのか複数先のホップに存在するかは問わない．

ブックマークされた URL のドメインのうち，リスクレベルが 100%であったものは 30 個存在した．表 4 にアクセス数ベースでの上位 10 位を示す．悪性 URL に到達する回数のみに着目すると，本表には記載されないサイトが存在する．それらには `yahoo.co.jp` や `youtube.com`，`google.co.jp`

表 4　高リスクなブックマークドメイン上位 10 位

ドメイン名	ブックマークアクセス数	リスクレベル
bejav.net	126	100.00
javmost.com	42	100.00
theyoump3.com	9	100.00
xdytt.com	8	100.00
91mjw.com	6	100.00
incestflix.com	6	100.00
gofucker.com	5	100.00
javbraze.com	5	100.00
anipo.tv	3	100.00
avdvd.tv	2	100.00

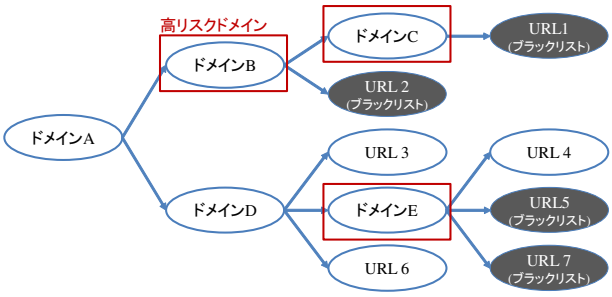

図 5　ドメインリスク評価手法のコンセプト

など，著名なドメインが含まれるが，これらのドメインのリスクレベルは低値となる．例えば google.co.jp ドメインのブックマーク URL アクセスから悪性 URL に 135 回到達しているものの，総アクセス数が 103,459 回であり，リスクレベルは 0.13%程度となるため，同表には含まれない．

上述の通りブックマークアクセスは悪性 URL 到達経路への主要なエントリーポイントとなっているため，ブックマークをレビューすることにより，悪性 URL へのアクセス数の低下を期待できる．また，ユーザが危険な URL をブックマーク登録するのを阻止する，もしくはブックマークされた危険な URL へのアクセスをブロックすることは容易ではないが，危険なブックマークへアクセスする際に警告を掲示するだけでも状況改善に資すると考えている．

5. ドメインリスク評価手法

悪性 URL はブラックリストに含まれるが，悪性 URL へと続く URL の中にはブラックリストに含まれないものが存在する．悪性 URL へと到達する可能性の高いドメインのことを，本稿では高リスクドメインと呼ぶ．我々はそのようなドメインを特定し，ブラックリストに登録する，もしくは警告を発する等の対策を講じることにより，悪性 URL へのアクセスを抑制する．図 5 にドメインリスク評価手法のコンセプトを示す．提案方式は，各ドメインから悪性 URL に到達する確率を算出し，その確率が閾値より高ければ当該ドメインを高リスクドメインとして特定する．本図では，異なる 7 つの URL に到達する複数のアクセスパスから構築されているアクセスパスツリーが描かれており，その URL のうちの 4 つはブラックリストに登録されている．ドメイン B および C を通じたアクセスはすべてブラックリスト登録されている URL に到達するため，これらのドメインは高リスクドメインとみなされる．ドメイン E を通じたアクセスは，ブラックリスト登録された URL とそうでない URL の両方に到達するが，本ドメインは閾値以上の確率で悪性 URL に到達するため，高リスクドメインとみなされる．他のドメインではその確率が閾値を超えないため，高リスクドメインとはみなされない．これらの高リスクドメインはブラックリストには掲載されていないものの，後述の通りブラックリスト登録候補であると考えられる．これらの高リスクドメインをブロックする，もしくはユーザに警告を発することにより，悪性 URL にユーザがアクセスするリスクを最小化する．

表 5　最大リスクレベルが 50%超の高リスクドメイン上位 10 位 (ブラックリスト掲載ドメインは除外)

ドメイン名	アクセス数		最大リスクレベル
	悪性 URL 到達経路	全経路	
avgle.com	33,049	96,647	53.57
olmsoneenh.info	10,851	41,336	63.5
smv.to	2,493	6,663	77.5
xbooks.to	1,134	11,139	66.66
codeday.me	990	1,105	100.00
ero-advertising.com	637	3,154	55.35
anitube.biz	300	1,271	74.62
aphookkensidah.pro	274	1,046	100.00
adextrem.com	172	228	85.71
threepro.co.jp	154	271	56.82

表 6　最大リスクレベルが 100%の低信頼度メイン上位 10 位 (ブラックリスト掲載ドメインは除外)

ドメイン名	アクセス数	
	悪性 URL 到達経路	全経路
codeday.me	990	1,105
aphookkensidah.pro	274	1,046
eimusics.com	58	101
xsnvshen.com	53	135
javbraze.com	41	44
livetotal.tv	35	122
jqaaa.com	35	91
collectionanalyser.com	32	65
romulation.net	28	33
vidia.tv	27	33

5.1 高リスクドメインの特定

提案方式を用い，我々は悪性 URL 到達経路上のすべてのドメインのリスクレベルを評価する．表 5 および表 6 に，18 ヶ月の間で s 最大リスクレベルが 50%を超えるドメインおよび 100%であるドメインをそれぞれ示す．既にブラックリストに指定されているドメインは除外している．最大

表 7　悪性 URL 到達経路上のドメイン数

リスクレベル	各ドメインの GSB 登録状況			
	完全登録	一部登録	未登録	総計
100%	1,121	34	820	1,975
[80%-100%)	21	7	54	82
[60%-80%)	11	16	130	157
計	1,153	57	1,004	2,214

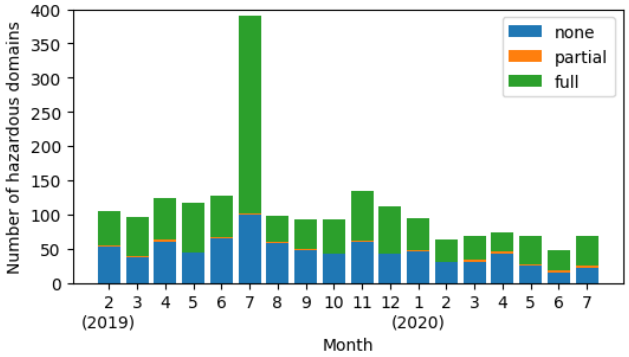

図 6　リスクレベルが 100%のドメイン数の推移

リスクレベル列は 18 ヶ月間の月々のドメインのリスクレベルの最大値を示しており，月数列はそのドメインが悪性 URL 到達経路上に現れた月数を示している．このように，ブラックリストに登録されていないものの，ブラックリストに必ず到達する，もしくは到達する確率の高いドメインが存在していることが分かる．

表 7 に，リスクレベル別に，悪性 URL 到達経路上のドメインの数の内訳を示す．ユーザを保護すべく，もしドメインのリスクレベルが一定の閾値を超えた際には，そのドメイン上にてトラフィックを遮断する，もしくは警告を発することが可能となる．その閾値を 80%とすると，GSB により既に指定されている 1,183 個のドメインに加え，874 個のドメインが高リスクドメインとして特定される．図 6 に，リスクレベルが 100%のドメイン数の月毎の推移を示す．第 4.1 節にて議論した通り，2019 年 7 月のみ例外的な数値を示しているものの，それ以外の月においては大きな傾向変化はなく，安定して提案方式がブラックリスト非掲載の高リスクドメインを特定できていることが分かる．

5.2　ブロックされた URL 群

高リスクドメインへのアクセスを禁止することにより，それに続く URL へのアクセスが不能となる．高リスクドメイン判定に用いる閾値を 80%とした際に，到達不能となった URL 群は下記のいづれかの種別に該当する．

(1) **GSB 掲載済み URL:** これらの URL は GSB を用いてアクセスをブロック可能であるが，提案方式ではその URL に至る経路上にある高リスクドメインにてアクセスがブロックされた．尚，本稿では GSB を用いて高リスクドメインを特定したが，その他のブラックリストの利用も可能である．

(2) **他ブラックリスト掲載済 URL:** これらの URL は GSB には登録されていなかったが，他のブラックリストに登録されていたものである．ここでは，我々は URL 文字列のシグネチャに基づき悪性 URL を特定する商用のブラックリストを利用した．しかしながら，そのような URL の数は少ない．これは，おそらくブラックリストごとに何を悪性と判定するかのポリシーが異なるためと考えている．実際，その商用ブラックリストと比較して，GSB ではソーシャルエンジニアリング型の URL をより多く悪性判定するのに対し，マルウェア関連型の URL をより少なく悪性判定する．

(3) **ブラックリスト掲載済 URL と同一ドメインにあるブラックリスト未掲載 URL:** GSB は悪性 URL の登録に時間を要することがあり，幾つかの悪性 URL はアクセスのあった時点では未登録であることがある．これらの URL，もしくはそのドメインは GSB 登録に今後登録される，もしくは登録されるべきものである．

(4) **到達不能 URL:** これらの URL は論文執筆現在において既に到達不能である．悪性 URL はしばしば一定期間後に削除されることが多く，これらの URL が悪性 URL であった可能性は小さくない．

(5) **違法または有害なコンテンツを含む URL:** これらの URL は上記のいずれに該当しないものの，グローバルベースで Alexa Top 1,000 サイト [4] には観測期間中に一度も含まれておらず，ポルノ，漫画や本のスキャン，音楽やビデオファイルを扱っている．GSB および上述のブラックリストにはこれらの URL が登録されていないが，悪性判定は各ブラックリストのポリシーに依存しており，ブラックリスト非掲載 URL が合法サイトであるとは限らない．これらのページは大半のユーザの日常生活には不要のものであり，これらのページに到達不能になることの影響は限定的である．

到達不能になった URL は上記の通り，悪性であるか，到達不能，違法，もしくは有害であるため，これらをブロックすることにより，ユーザの正当な活動を阻害することなく，ユーザの保護を高めることができる．

6.　考察

本章では我々のデータ収集・分析アプローチの利点，そしてデータセットの制約について議論する．

ユーザ側でのデータ収集の利点　我々の手法には，ユーザ側でのデータ収集に起因した 2 つの強みが存在する．第一の強みに，「効率的な分析」が挙げられる．本データに含まれるユーザ ID 及びブラウザタブ ID を用いることで，分析対象とするデータを絞り込むことができる．その結果，分析の複雑度および曖昧さは最小化され，より精度の高い分

析が可能となる．結果として，その分析に必要なコストと時間は最小化される．第二の強みに，「ネットワーク上では収集できない情報の取得」が挙げられる．ユーザのナビゲーション情報など，ネットワーク上でデータ収集をした際には取得できないデータを取得することができ，それらは詳細な分析に有用である．実際，我々のセンサーはインストールされているブラウザ拡張のリストやプロセス情報など，第 2 章に記載していないデータも収集可能である．

データセットの制約　我々のデータセットには幾つかの制約が存在する．第一に，我々はタチコマが好きな人にブラウザ拡張を配布していること，および本ブラウザ拡張もその配布ページも日本語であることから，ユーザ層に偏りが存在する．第二に，データセット内のユーザ数，特に悪性 URL に到達するユーザ数が少なく，ユーザの詳細な分類などの研究を実施するのは困難である．第三に，悪性 URL のラベル付け手法を検討する必要がある．今回，我々は GSB を利用してラベル付けを実施しているが，これが常に最適とは限らず，別のブラックリストも利用可能である．将来研究ではこれらのデータセットの制約を考慮されたい．

7. 関連研究

悪性 URL 検知に関する研究は多数報告されている．SpiderWeb [8] は HTTP リダイレクションのチェーンを構築し，それが悪性サイトに通じるか否かを識別する．WebWitness [9] は各種のマルウェアダウンロード攻撃の被害に遭うユーザのアクセスパスを分析し，そのパスがソーシャルエンジニアリングかドライブバイのどちらに至るかを識別する．同様の研究で，ソーシャルエンジニアリング攻撃の URL に焦点をあてたもの [10]，および悪性のエクスプロイトキットを特定することに焦点を当てたもの [11] も報告されている．その他，アクセス先 Web ページ内の JavaScript を分析する技術 [12] や URL の文字列自体に悪性サイトの特徴があると考えて URL を分析を実施する技術 [13]，シグネチャを自動生成する技術 [14] など，本領域では各種の検討結果が報告されている．

これらの関連研究とは異なり，我々はユーザ側にてデータを収集することにより，各ユーザ・ブラウザタブを識別した分析を実現している．本研究の初期検討結果は [15] にて発表済みであり，本稿はその内容を精査し，分析を一部深化したものである．具体的には，データセットの収集期間を 18 ヶ月に拡大し，すべての分析を再実施して内容を検証した．また，エントリーポイント分析において，ユーザ数ベースの分析結果を追加している．より幅広い従来研究については [15] を参考にされたい．

8. 結論

ユーザ側での web アクセス記録の収集は，ユーザ ID，ブラウザタブ ID，ユーザナビゲーション情報など，ネットワークトラフィックから収集しえない情報にアクセス可能になる．これらを活用することにより，本稿では効率的に悪性 URL 到達経路を再構築した．そして，その悪性 URL 到達経路を分析することにより，悪性 URL 到達経路の最大のエントリーポイントがブックマークアクセスであることを示し，ブックマークを定期的に評価・整理することにより悪性 URL に到達するリスクを低減できる可能性を示した．さらには，ドメインリスク評価手法を提案し，ブラックリストに掲載されていないものの高確率で悪性 URL へと到達するドメインを特定した．このように，ユーザ側でのデータ収集は，効率的かつ詳細に web アクセスの分析を実現する．本研究が，よりよいセキュリティをユーザに提供するための技術の発展の一助となれば幸いである．

謝辞　本研究の実施にあたりご協力頂いた WarpDrive プロジェクト [1] のメンバの皆様に深く感謝する．

参考文献

[1] Warpdrive. `https://warpdrive-project.jp/`. Accessed: June 1, 2020.
[2] Ghost in the shell. `http://www.production-ig.com/contents/works_sp/16_/index.html`. Accessed: June 1, 2020.
[3] Google safe browsing. `https://safebrowsing.google.com/`. Accessed: June 1, 2020.
[4] Alexa top sites. `https://www.alexa.com/topsites`. Accessed: June 1, 2020.
[5] Chrome: developer. `https://developer.chrome.com/home`. Accessed: June 1, 2020.
[6] Virustotal. `https://www.virustotal.com/`. Accessed: June 1, 2020.
[7] 源平祐太, 中川雄太, 高田一樹, et al. 悪性 web サイトに到達しやすい危険検索単語の検知. In *CSS*, 2019.
[8] G. Stringhini, C. Kruegel, and G. Vigna. Shady paths: Leveraging surfing crowds to detect malicious web pages. In *ACM CCS*, 2013.
[9] Nelms T, Perdisci R, Antonakakis M, et al. Webwitness: Investigating, categorizing, and mitigating malware download paths. In *USENIX Security*, 2015.
[10] Nelms T, Perdisci R, Antonakakis M, et al. Towards measuring and mitigating social engineering software download attacks. In *USENIX Security*, 2016.
[11] Taylor T, Hu X, Wang T, et al. Detecting malicious exploit kits using tree-based similarity searches. In *ACM CODASPY*, 2016.
[12] Fang Y, Huang C, Liu L, et al. Research on malicious javascript detection technology based on lstm. *IEEE Access*, 6, 2018.
[13] Ma J, Saul LK, Savage S, et al. Learning to detect malicious urls. *ACM Trans. Intell. Syst. Technol.*, 2, 2011.
[14] Zhang J, Seifert C, Stokes JW, et al. Arrow: Generating signatures to detect drive-by downloads. In *WWW*, 2011.
[15] Takahashi T, Kruegel C, Vigna G, et al. Tracing and analyzing web access paths based on user-side data colletion: How do users reach malicious urls? In *RAID*, 2020.