Vol.2020-DPS-182 No.40
Vol.2020-CSEC-88 No.40
2020/3/13

# リダイレクトの追跡による悪性 Web ページアクセス事例分析

嶌田一郎[1] 太田敏史[1] 白石訓裕[2] 中嶋淳[2] 田中翔真[3] 山田明[3] 高橋健志[4]

**概要**：Web サイトの閲覧を媒介としてマルウェアに感染させる Web 媒介型攻撃が深刻な問題となっている．Web 媒介型攻撃は，悪性 Web サイトの一部削除に対応するためやブラックリスト登録から逃れるために，複数の Web サイトを自動的に遷移させるリダイレクトを用いた構造をもつことが知られている．本稿では，Web ブラウザ拡張によって，リダイレクトに関する情報を効率的に収集する方式および複数のユーザから収集したリダイレクト情報を横断的に分析することによって構造分析する方式を提案する．提案方式は，Google Chrome の chrome Extension API を用いることによって，Web リクエストおよび関連するブラウジング情報を取得する．さらに，複数の Web ブラウザにおいて収集したブラウジング情報を全文検索エンジン ElasticSearch によって分析する．Web ブラウザ拡張を一般ユーザに配布した実験を 2018 年 6 月から行っており， 2020 年 1 月現在において約 9,000 名のユーザを集めた．さらに，収集データを分析したところ，「年間ビジターアンケート」「Microsoft を騙った偽警告サイト」「Apple を騙った偽警告サイト」という 3 つの攻撃事例を発見した．そこで，これらの事例について提案方式のリダイレクト追跡による構造分析の結果を示す．

**キーワード**：Web 媒介型攻撃，ドライブバイダウンロード，ソーシャルエンジニアリング, Web アクセスログ

# A Case Study of Malicious Web Page Access by Tracking Redirection Chains

ICHIRO SHIMADA[†1] TOSHIFUMI OOTA[†1] KUNIHIRO SHIRAISHI[†2]
JUN NAKAJIMA[†2] SHOMA TANAKA[†3] AKIRA YAMADA[†3]
TAKESHI TAKAHASHI[†4]

***Abstract***: Web-based cyber attacks, which infect computers with malware when users browse malicious websites, have become a serious problem due to the growing use of redirection, in which multiple Web sites are automatically visited in order to cope with partial deletion of malicious Web sites and to avoid blacklist registration. We present a method for efficiently collecting information on redirects caused by a Web browser extension and a method for analyzing the structure of redirects collected from multiple users. The collection method obtains Web requests and related Web browser histories for multiple users by using the chrome Extension API of Google Chrome while the analysis method analyzes the histories by using the ElasticSearch full-text search engine. An experiment in which the extension was distributed to general users was carried out in June 2018, and information for about 9,000 users was collected as of January 2020. Analysis of the collected data revealed three types of phishing scams: "annual visitor questionnaire," "Microsoft Security Warning," "Apple Security Warning." This paper presents the results of structural analysis of the redirection chains tracking by the proposed method for these identified scams.

***Keywords***: Web-based cyber attacks, Drive-by Download, Social Engineering, Web access log

## 1. はじめに

Web サイトの閲覧を媒介としてマルウェアに感染させる Web 媒介型攻撃が深刻な問題となっている．Web 媒介型攻撃は，悪性 Web サイトの一部削除に対応するためやブラックリスト登録から逃れるために，複数の Web サイトを自動的に遷移させるリダイレクトを用いた構造をもつことが知られている． 攻撃は，複数のページをリダイレクトしながら遷移し悪性サイトへ誘導するため，Web 上の攻撃ページにどのように到達し，マルウェアをダウンロードさせるか観測し，ページ遷移のコンテキストを把握することが，攻撃への防御策を検討する上では重要である．本稿では，Web ブラウザ拡張によって，リダイレクトに関する情報を効率的に収集する方式および複数のユーザから収集したリダイレクト情報を横断的に分析することによって構造分析する方式を提案する．

以下，2 章では，関連研究について述べ，3 章では，分析に使用するデータセットについて述べる．4 章では，収集したログを分析する方法について述べる．そして，5 章では，分析結果として，全文検索エンジン ElasticSearch による悪性 Web ページアクセス事例，及び悪性 Web サイトアクセス時のページ遷移追跡事例について述べ,6 章でまとめを述べる．なお本稿では，Web ページ閲覧を「Web ページアクセス」，Web ページアクセスにより収集したデータを

1 株式会社 構造計画研究所
KOZO KEIKAKU ENGINEERING Inc.
2 株式会社 セキュアブレイン
SecureBrain Corporation
3 株式会社 KDDI 総合研究所
KDDI Research, Inc.
4 国立研究開発法人 情報通信研究機構
National Institute of Information and Communications Technology

Vol.2020-DPS-182 No.40
Vol.2020-CSEC-88 No.40
2020/3/13

「ブラウジング情報」,ブラウジング情報から抽出した Web ページアクセスでの履歴に関する情報を「Web アクセス履歴」と定義し使用する.

## 2. 関連研究

Drive-by Download（DBD）攻撃の防御を開発・改良する目的でマルウェアのダウンロード経路を研究した文献として[1]がある．[1]では，DBD 攻撃対策として WebWitness と名付けられたインシデント調査システムを提案している．WebWitness では，Web 上のマルウェアのダウンロード経路をユーザのブラウジング情報から自動的にトレースバックしラベル付けしている．ラベルは，現在の攻撃傾向をよりよく把握し，より効果的な防御策を開発するために活用している．ブラウジング情報からマルウェアのダウンロードトレースバックを行うのに，ブラウジング情報から経路を再構築する必要があり，トレースバックの方法として，ログ上の Referer フィールドと Location フィールドを利用して Web アクセス間をリンクさせる方法がある．しかし，この方法では，ユーザが使用しているブラウザ，JavaScript，プラグインソフトウェアの特定のバージョンなどに依存して Referer フィールド，Location フィールドが抑制され，Web アクセス間のリンクが正しく再構築できない場合があるという課題がある．このため[1]では，”referrer indicator” を導入して Web アクセス間のリンク関係の重み付けをして，複数の経路から重要な経路を選択することで自動的にトレースバックする手法を提案している．”referrer indicator” の概略は以下の通りである．

- Location:リンク元の Location が，リンク先の URL と一致する場合.
- Referer:リンク元の URL が，リンク先の Referer と一致する場合.
- Domain-in-URL:リンク元のドメイン名が，リンク先の URL に組み込まれている場合.
- URL-in-Content:リンク元のレスポンスコンテンツに，リンク先の URL が含まれている場合.
- Same-Domain:リンク元とリンク先が同じドメイン名で，リンク間の時間間隔が短い場合.
- Common Expoitable Content:リンク元に.jar，.swf，.pdf など Exploit に利用され易いコンテンツが使用され，リンク先との時間間隔が短い場合.
- Ad-to-Ad:リンク間に連続した広告の要求関係があり，リンク間の時間間隔が短い場合.

上記の特徴を利用して，大規模な学術ネットワークからダウンロード経路情報を収集し，ブラウジング情報からリンクを再構築し，既存のブラックリスト手法と比較して DBD 攻撃での感染率を 6 倍低減している.

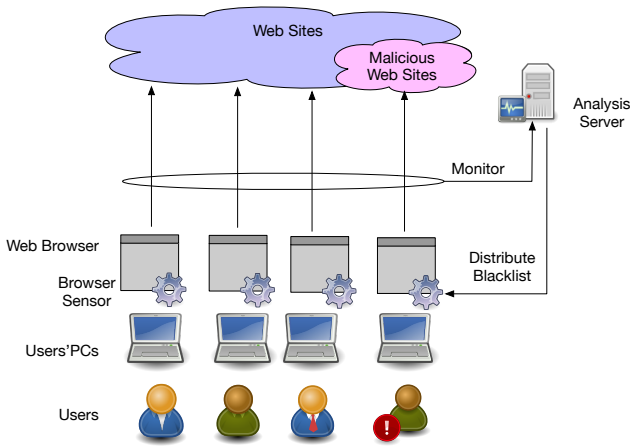



図 1　実証実験のシステム構成

本稿では，文献[2-3]の対策研究の枠組みの中で，Web アクセス履歴の追跡を[1]とは別の手法を用いて行った．[2]は，ユーザ参加による Web 媒介型攻撃対策(WarpDrive:Web-based Attack Response with Practical and Deployable Research InitiatiVE)の研究開発であり，一般ユーザの参加によって観測環境を構築する点が特徴となっている．システムはブラウザセンサと分析基盤からなっており，センサで収集されたブラウジング情報を分析基盤に集め，ユーザ端末で発生している攻撃の実態把握を実現している．Web ブラウザ拡張（ブラウザセンサ）を一般ユーザに配布した実証実験を 2018 年 6 月から開始して，約 3 ヶ月間で 5,000 人のユーザが利用し，毎日約 15 億件のブラウジング情報が収集されている．2020 年 1 月現在において約 9,000 名のユーザを集めている．[2]のデータセットを用いた研究として[4-5]がある. [4]は, Web サイトを構成するコンテンツの種類, 総数, サイズなどのリソース統計情報のみを用いたフィッシングサイト検知手法を提案している．また[5]は，スマートフォンを対象とした Web 媒介型サイバー攻撃の観測機構の設計と実装についての提案を行っている. 本稿では, 悪性 Web ページへのリダイレクトの追跡による構造分析を行う.

## 3. データセット

本稿で利用したデータセットは，2 章で述べたユーザ参加型実証実験 WarpDrive の実証実験ログである．以下，WarpDrive のシステム概要，データ収集処理概要，データセットの特徴について述べる.

### 3.1 システム概要

図 1 に，WarpDrive のシステム構成を示す．本システムは，ユーザへ配布したブラウザセンサによりユーザのブラウジング情報を収集し，分析システムを用いて分析するための分析基盤である．分析システムに集められたブラウジング情報をもとに，悪性サイトへのアクセス分析を行い，分析結果は被害の未然防止に活用する.

Vol.2020-DPS-182 No.40
Vol.2020-CSEC-88 No.40
2020/3/13

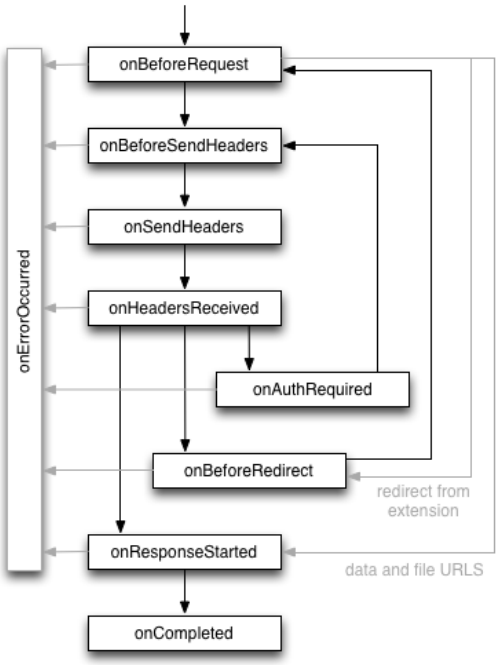



図 2　Web ページアクセス時の発生イベント

### 3.2 データ収集処理概要

WarpDrive で開発したブラウザセンサでは，ブラウジング情報の収集を，chrome Extension API[6]を利用して行っている（ページ遷移は chrome.webNavigation API[7]，URL アクセスは chrome.webRequest API[8]を利用）．ブラウジング情報の収集は，各 API のイベントリスナーにイベント取得登録を行い，ブラウザがページを表示する度に発生するイベントから得られるデータを収集する．発生イベントの概要を図 2 に示す[8]．図 2 のイベントはユーザのブラウジング開始により，次のタイミングで発生する．

- onBeforeRequest:リクエストが発生する直前に発生．
- onBeforeSendHeaders:ブラウザ内で初期リクエストヘッダが準備された時に発生．
- onSendHeaders:リクエストヘッダの最終バージョンの確定時に発生．
- onHeadersReceived: HTTP（S）レスポンスヘッダ受信時に発生．
- onAuthRequired:レスポンスヘッダに認証を要求するヘッダが存在する場合，onHeadersReceived イベントに続き発生．
- onBeforeRedirect:ブラウザによるサーバリダイレクト実行時に発生．
- onResponseStarted:レスポンスボディの最初のバイトが受信された時に発生．
- onCompleted:リクエストが正常に処理された時に発生．
- onErrorOccurred:リクエストを正常に処理できなかった時に発生．

### 3.3 データセットの特徴

収集するデータは，ブラウザがページを表示する際に得られるページに関連する情報（フレームとコンテンツの URL，URL のリソースタイプ，コンテンツの種類，Web ページアクセスを関連付けるキー情報，ページ遷移の理由を示すページ遷移タイプ，ページ遷移修飾子，リダイレクト先 URL，リダイレクトの種別），URL で要求した際のリクエストヘッダ，レスポンスヘッダ，レスポンス IP ステータスコード，リクエスト処理を開始した時間，リクエスト処理を完了した時間，表示に関わるブラウザ情報などである．付録 A に主な記録内容を示す．

本データセットは Web アクセス履歴の分析において以下の特徴を有する．

(1) **Referer ヘッダに依らないページ遷移の把握が可能**

ブラウジング情報のタイムスタンプは，ブラウザがページにアクセスした際に設定するものであり，type が "main_frame"(DOM の構成元となるページ[a])のブラウジング情報を時系列でソートするだけでページ遷移を示すデータとして利用可能となる．

(2) **Location ヘッダと 3XX ステータスコードに依らないサーバリダイレクト発生の識別**

redirect_url が設定されたブラウジング情報により，サーバリダイレクトの発生とリダイレクト先の URL が識別できる．また，type が"main_frame"または"sub_frame"の場合は，最終リダイレクト先にリダイレクト種別(サーバリダイレクト，クライアントリダイレクト)も設定されている．

(3) **ブラウジングに関係する全 URL の収集**

ブラウジングに関係する URL を取得する方法として chrome Extension API の history API を利用する方法があるが，この方法ではブラウザが最終的にレンダリングに使用したページの URL しか取得できず，結果として type が”main_frame”または”sub_frame”以外の場合の URL が収集できない．このため本システムでは，ブラウジングに関係する全 URL を収集する手法を用いることで，history API では収集できなかったリダイレクト元 URL やページを構成するコンテンツの URL の収集を可能とした．

## 4. 分析方法

本章では，Web アクセス履歴の分析方法として，全文検索エンジン ElasticSearch[9]を用いる方法と，データ収集システムに保管されるブラウジング情報を直接参照する方法について述べる．

a) Web ページアクセス時，HTML データはブラウザにより DOM(Document Object Model)として解釈される．ブラウザは，DOM 内の URL にアクセスしてコンテンツデータを取得し，DOM とコンテンツをブラウザ画面上にレンダリングして表示する．

Vol.2020-DPS-182 No.40
Vol.2020-CSEC-88 No.40
2020/3/13

### 4.1 全文検索エンジン ElasticSearch による分析方法

Web 媒介型攻撃対策の研究開発[2]では，ユーザ環境から収集したブラウジング情報を全文検索エンジン ElasticSearch による分析の仕組みを構築している．全文検索エンジン ElasticSearch を用いることで，付録 A に示すデータ項目を指定した絞り込み検索が可能であり，検索結果を簡単に参照することができる．本稿において，全文検索エンジン ElasticSearch を用いて「年間ビジターアンケート」によるソーシャルエンジニアリング（SE:Social Engineering）攻撃の事例分析を行った．分析結果は 5 章で述べる．

### 4.2 ページ遷移の追跡による分析方法

収集したブラウジング情報からページ遷移を追跡する方法について述べる．遷移先が新しいページへ遷移した場合は，分岐先の最初の履歴情報に，分岐元の履歴の tabid, frameid が記録される．本手法では，Referer，Location の情報は用いず，ページ遷移の追跡を以下のルールで行う．

(1) type が”main_frame”の履歴情報

(2) tabid が同一のログ(同じタブ上でのページ遷移)

(3) (1)(2)のデータの時系列順ソート

ページ遷移は，transition_type で判断する．付録 B.1 にユーザナビゲーション時のページ遷移とデータ設定内容の例を示す．ユーザナビゲーション時のユーザ操作内容が，transition_type，及び transition_qualifiers に設定される．

更に，本稿では，ページ遷移時に発生するリダイレクトを，クライアントリダイレクトとサーバリダイレクトとに区別した．クライアントリダイレクトは，meta tag refresh, 及び JavaScript での location 書き換えによるページ遷移であり, 一方, サーバリダイレクトは, Web サーバからの 3XX 応答で発生するリダイレクションである．各リダイレクトは，transition_qualifiers に，それぞれ“client_redirect”，及び”server_redirect”を設定して識別する．付録 B に，サーバリダイレクト，クライアントリダイレクト，ポップアップによるページ遷移の例を示す.

**(1) サーバリダイレクト**

サーバリダイレクトによるページ遷移時は，accessid の設定値にページ遷移元と遷移先で同じ値が設定される. また，最終リダイレクト先にのみ transition_type，transition_qualifiers に値が設定され，ページ遷移元の redirect_url にリダイレクト先 url が設定される（付録 B.2）.

**(2) クライアントリダイレクト**

クライアントリダイレクトによるページ遷移時は, accessid にページ遷移元と遷移先で違う値に設定される．また，リダイレクトの各段の transition_type，transition_qualifiers に値が設定され，meta tag refresh の場合，及び JavaScript での location 書き換えの場合ともに transition_type に”link”の値が設定される（付録 B.3）.

表 1　検索期間，シグネチャ，検出件数

| | |
|---|---|
| 検索期間 | 2019/8/16～2020/2/11 |
| 検索日数 | 180 日間 |
| シグネチャ 1 | bKMuT7EMVXU5Z6UvvSHONGlfu |
| 検知件数(シグネチャ 1) | 121 件 |
| シグネチャ 2 | QPF8euu28II5lw7O2iHhCugVqK5RzfdNsTpLaMM91qY1 |
| 検知件数(シグネチャ 2) | 97 件 |

**(3) ポップアップ**

ポップアップによるページ遷移の場合，ページ遷移先（分岐先）の source_frameid，source_tabid にページ遷移元（分岐元）の frameid, tabid と同じ値が設定される（付録 B.4）.

上記のページ遷移時のデータ設定内容をもとに行った悪性 Web ページアクセスの追跡，及び分析結果について 5 章で述べる.

## 5. 悪性 Web ページアクセス事例分析

### 5.1 全文検索エンジン ElasticSearch による分析結果

「年間ビジターアンケート」は，景品と引き換えにアンケートに個人情報を記入させ収集することを目的とした SE 攻撃である．経験則による発見手法であるが URL 上の特定のシグネチャを発見し，全文検索エンジン ElasticSearch によりマッチングさせて取得した結果，効率よく攻撃が検出できることが分かった．検索期間，シグネチャ, 検出件数を表 1 に, 取得データ事例を付録.C に示す. 調査の結果，2019/11/27 以降はシグネチャ 2 で検知されており，シグネチャ 1 では検知されていないことから，シグネチャを変更して攻撃を継続していることが分かった.

### 5.2 ページ遷移の追跡による分析結果

ブラウジング情報は，WarpDrive 参加ユーザのユーザ環境から収集した膨大なデータから構成されている．このため，悪性 Web ページアクセス事例の分析を行うためには，まず, ブラウジング情報全体から悪性 Web ページへのアクセスを抽出する必要がある．抽出は以下の手順で行った.

(1) ブラウジング情報からドメイン名を抽出する.

(2) 抽出したドメイン名の良性/悪性判定を行い，悪性と判定されたドメイン名を持つ Web サイトを悪性 Web サイトとして分類する.

(3) 悪性 Web ページアクセス時のページ遷移追跡は，ユーザ毎，tabid 毎に type が”main_frame”の Web アクセス履歴を時系列で抽出する 4.2 節で記載した手法を用いる.

(4) 追跡結果からリダイレクトの特徴などの悪性 Web ページアクセスの分析を行う.

なお，ドメイン名の良性，悪性の判定には，複数のアンチウイルス製品を使用してファイルや Web サイトの悪性判定を行う Web サイト VirusTotal[10]を用いた.

表 2　分析対象期間，ユーザ数，対象レコード数

| 対象期間 | 2019/2/3～2019/2/6 |
|---|---|
| 対象日数 | 4 日間 |
| 2/3 アクティブユーザ数 | 807 |
| 2/4 アクティブユーザ数 | 929 |
| 2/5 アクティブユーザ数 | 922 |
| 2/6 アクティブユーザ数 | 902 |
| ログレコード数(4 日間) | 316,870 |

表 3　悪性判定エンジン数とドメイン名

| ドメイン名 | 悪性判定エンジン数/判定エンジン総数 |
|---|---|
| www.microsoft.com-repair-windows.live | 7/72 |
| www.microsoft.com-repair-windows-system.live | 6/70 |
| www.apple.com-repair-os.live | 5/71 |
| www.apple.com-cleaning-os.live | 5/72 |
| 24pccheck.goodsafecontentnew.icu | 5/66 |

### 5.3 分析対象データと悪性ドメイン名

分析対象期間，日毎のアクティブユーザ数，及び抽出した type が”main_frame”のログレコード数を表 2 に，対象期間のデータから抽出した悪性判定エンジン数が多かった主なドメイン名を表 3 に示す．

判定の結果，悪性判定エンジン数が多かったのは www.microsoft.com-repair-windows.live（Microsoft を騙った偽警告サイト）や www.apple.com-repair-os.live（Apple を騙った偽警告サイト）などの Repair ウィルスサイトによる SE 攻撃であった．本稿では，Repair ウィルスサイトに着目し Web ページ遷移の追跡を行う．

### 5.4 ページ遷移の追跡

Repair ウィルスサイトは，電子メールアドレスなど個人情報を要求するフィッシング詐欺であり，Win32/FakeSysdef のマルウェアの亜種とされている[11]．表 4 に www.microsoft.com-repair-windows.live サイトへ到達するまでのページ遷移追跡結果を示す．表 4 の事例は，特定のユーザの時系列 Web ページアクセスについて，tabid が”155”，type が”main_frame”のデータを時系列でソートして追跡している．国コードはレスポンス IP から判定した国コードである．更に，Apple を騙る Repair ウィルス www.apple.com-repair-os.live の追跡事例を表 5 に示す．表 5 の事例は，特定のユーザの時系列 Web ページアクセスについて，tabid が”1837”，type が”main_frame”のデータを時系列でソートして追跡している．

### 5.5 ページ遷移の分析

5.4 節の事例は，サーバリダイレクトによるページ遷移であり，複数のホスト，複数の国を経由して Repair ウィルスサイトへ到達する特徴があった．更に，www.microsoft.com-repair-windows.live のアクセスは，5.4 節で示したアクセス事例以外にも複数存在した．このため，調査期間のブラウジング情報を対象に，www.microsoft.com-repair-windows.live サイトへの Web アクセス履歴を全て抽出し，抽出結果をグラフにより可視化して Web ページアクセスの特徴の分析を行った．分析結果を図 3 に示す．

ノードの大きさは，VirusTotal での悪性判定エンジン数を表している．ノードが最も大きい www.microsoft.com-repair-windows.live が 7 件，click.eclk.club が 4 件，tracking.marketing が 1 件の悪性判定エンジン数である．また，エッジの太さはページ遷移数を表している．エッジが最も太い tracking.marketing と www.microsoft.com-repair-windows.live 間がページ遷移数 10 である．ページ遷移の特徴として以

表 4　www.microsoft.com-repair-windows.live の追跡結果

| アクセス時刻 | アクセスドメイン名 | 国コード |
|---|---|---|
| 2019/2/4 12:28:37 | hantinlethemsed.info | US |
| 2019/2/4 12:28:38 | xml.adservme.com | US |
| 2019/2/4 12:28:39 | usd.silvanus-phe.com | US |
| 2019/2/4 12:28:39 | tracking.marketing | US |
| 2019/2/4 12:28:41 | www.microsoft.com-repair-windows.live | US |

表 5　www.apple.com-repair-windows.live の追跡結果

| アクセス時刻 | アクセスドメイン名 | 国コード |
|---|---|---|
| 2019/2/6 09:20:01 | hantinlethemsed.info | US |
| 2019/2/6 09:20:01 | xml.adoperatorx.com | US |
| 2019/2/6 09:20:02 | dsp.wtf | SG |
| 2019/2/6 09:20:03 | dsp.wtf | SG |
| 2019/2/6 09:20:03 | tracking.marketing | US |
| 2019/2/6 09:20:03 | www.apple.com-repair-os.live | US |

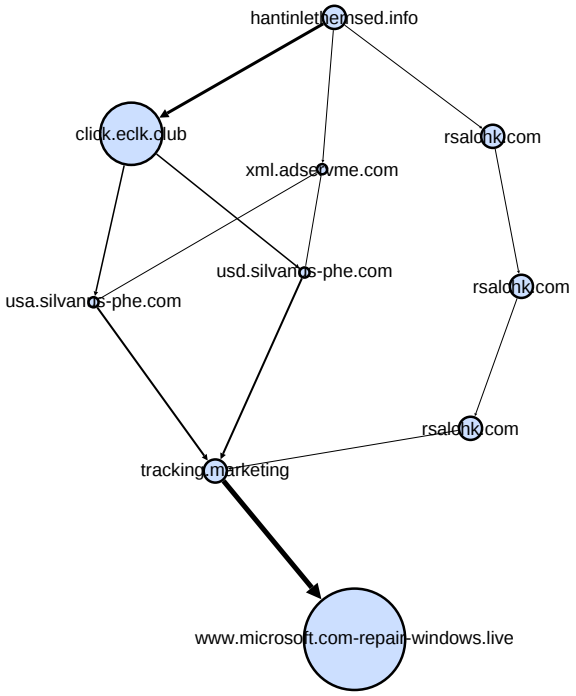



図 3　グラフ表現によるページ遷移の可視化例

下を確認した．

- 調査したページ遷移は，すべて hantinlethemsed.info を起点としている．
- www.microsoft.com-repair-windows.live へ到達するまでのページ遷移経路は複数あり，途中に 3-4 回のリダイレクトによるページ遷移を挟んで遷移する．
- www.microsoft.com-repair-windows.live へ到達する直前に必ず tracking.marketing を経由している．

## 6. おわりに

SE 攻撃の構造分析を行った結果，複数（3-4）回のサーバリダイレクトにより複数サイトを経由して目的のページへ到達している，主に国外のサーバを経由して目的のページに到達している，目的ページへ到達する前に必ず経由する特定のページが存在している，という特徴を確認することができた．

本稿において，リダイレクトによるページ遷移を構造的に分析・評価する分析基盤を構築することができた．今後は検知アルゴリズムの検討や，リダイレクトの最初の起点となったサイトへアクセスする際のユーザ操作に着目し，分析基盤を活用する．

**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．

## 参考文献

[1] Nelms, T., Perdisci, R., Antonakakis, M., Ahamad, M.. WebWitness: investigating, categorizing, and mitigating malware download paths. USENIX Security Symposium. 2015, p. 1025-1040.
[2] “Web 媒介型サイバー攻撃対策プロジェクト「WarpDrive」の実証実験開始について“. https://www.nict.go.jp/press/2018/06/01-1.html, (参照 2019-02-12).
[3] 山田明, 笠間貴弘, 井上大介. Web 媒介型攻撃対策「WarpDrive」の取組 ユーザ参加型による Web 攻撃対策の実現に向けて. NICT NEWS. 2018, Vol. 472, No.6, p. 10-11.
[4] 田中翔真, 松中隆志, 山田明, 窪田歩. Web サイトを構成するリソースの種類・サイズを用いたフィッシングサイト検知. 暗号と情報セキュリティシンポジウム(SCIS2020), 2020.
[5] 山田明, 佐野絢音, 窪田歩, 嶌田一郎, 中嶋淳, 吉岡克成, 瀬尾浩二郎, 満保雅浩, 佐藤将也, 松村礼央, 田辺瑠偉, 小澤誠一, 田中翔真, 梅本俊, 松田壮, 山内利宏, 澤谷雪子, 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. 暗号と情報セキュリティシンポジウム(SCIS2020), 2020.
[6] “Extension APIs”. https://developer.chrome.com/extensions/api_index, (参照 2019-02-12).
[7] “chrome.webNavigation”, https://developer.chrome.com/extensions/webNavigation, (参照 2019-02-14).
[8] “chrome.webRequest”, https://developer.chrome.com/extensions/webRequest, (参照 2019-02-14).
[9] “Elasticsearch | オフィシャルの分散型検索/分析エンジン”. https://www.elastic.co/jp/elasticsearch, (参照 2019-02-12).
[10] “VirusTotal: Virus Total”. https://www.virustotal.com/, (参照 2019-02-12).
[11] “Microsoft サポート: PC Repair ウィルスを駆除する方法”, https://support.microsoft.com/ja-jp/help/2617291/how-to-remove-the-pc-repair-virus, (参照 2019-02-12).

# 付録 A

## 付録 A.1 ブラウジング情報

| データ項目 | 取得タイミング | 説明 |
|---|---|---|
| tabid | chrome.webNavigation.onBeforeNavigate<br>chrome.webRequest.onBeforeRequest | ブラウザタブを識別する ID. |
| type | chrome.webRequest.onBeforeRequest | リソースの種別．詳細は付録 A.2 参照. |
| frameid | chrome.webNavigation.onBeforeNavigate<br>chrome.webRequest.onBeforeRequest | ページのフレームを識別する ID. |
| parentframeid | chrome.webNavigation.onBeforeNavigate<br>chrome.webRequest.onBeforeRequest | ページのフレームの親フレームを識別する ID. |
| accesseid | chrome.webNavigation.onBeforeNavigate<br>chrome.webRequest.onBeforeRequest | フレームを一意に識別する ID．フレーム毎に一意. |
| url | chrome.webNavigation.onBeforeNavigate<br>chrome.webRequest.onBeforeRequest | Web アクセスした URL. |
| reqid | chrome.webRequest.onBeforeRequest | Web ページアクセスを一意に識別する ID．Web リクエスト毎にユニーク. |
| request.timestamp | chrome.webRequest.onBeforeRequest | ブラウザがリクエスト処理を開始した時刻. |
| response.timestamp | chrome.webRequest.onBeforeRedirect<br>chrome.webRequest.onCompleted | ブラウザがリクエスト処理を終了した時刻. |
| response.ip | chrome.webRequest.onCompleted | アクセス先 IP アドレス. |
| transition_type | chrome.webNavigation.onCommitted | ページ遷移種別．詳細は付録 A.3 参照. |
| transition_qualifiers | chrome.webNavigation.onCommitted | ページ遷移に関連する追加情報．詳細は付録 A.4 参照. |
| process_id | chrome.webNavigation.onCommitted | フレームレンダリングを実行したプロセス ID（type が”main_frame”,”sub_frame”の場合に設定）. |
| redirect_url | chrome.webRequest.onBeforeRedirect | リダイレクト先の URL（サーバリダイレクトが発生した場合はリダイレクト元の履歴を設定）. |
| source_frameid | chrome.webNavigation.onCreatedNavigationTarget | 元フレーム ID（type が”main_frame”で新ウィンドウが生成された場合のみ）. |
| source_tabid | chrome.webNavigation.onCreatedNavigationTarget | 元タブ ID（type が”main_frame”で新ウィンドウが生成された場合のみ）. |

## 付録 A.2 データ項目 type の詳細

| 値 | 説明 |
|---|---|
| "main_frame" | タブにロードされたトップレベルのドキュメント. |
| "sub_frame" | <iframe>要素または<frame>要素にロードされたドキュメント. |
| "stylesheet" | ドキュメントの表現を記述するために読み込まれた CSS スタイルシート. |
| "script" | <script>要素によって実行される，またはワーカーで実行されるようにロードされるコード. |
| "image" | そのタイプをサポートするブラウザのイメージセットを除いて，イメージはイメージとしてレンダリングされるように読み込まれたリソース. |
| "font" | @ font-face CSS ルールのために読み込まれた Web フォント. |
| "object" | <object>要素または<embed>要素によってロードされるリソース. |
| "xmlhttprequest" | XMLHttpRequest オブジェクトまたは Fetch API によって送信されたリクエスト. |
| "ping" | ハイパーリンクが続いたときに，ハイパーリンクの ping 属性で指定された URL に送信されたリクエスト. |
| "csp_report" | ポリシーに違反する試みが検出されたときに，Content-Security-Policy ヘッダで指定された report-uri に送信された要求. |
| "media" | <video>要素または<audio>要素によって読み込まれるリソース. |
| "websocket" | WebSocket API を介してサーバへの接続を開始するリクエスト. |
| "other" | 他の利用可能な種類によってカバーされていないリソース. |

**付録 A.3 データ項目 transition_type の詳細**

| 値 | 説明 |
|---|---|
| "link" | ユーザは別のページのリンクをクリックした. |
| "typed" | ユーザが URL をアドレスバーに入力した．これは，ユーザがアドレスバーに入力を開始した後，提示された提案から URL を選択した場合にも使用される. |
| "auto_bookmark" | ユーザがブラウザ履歴内のブックマークまたはアイテムをクリックした. |
| "auto_subframe" | 親によって自動的にロードされるネストされた iframe. |
| "manual_subframe" | 明示的なユーザアクションとしてロードされたネストされた iframe. |
| "generated" | ユーザがアドレスバーに入力を開始した後，URL が含まれていない候補の項目をクリックした. |
| “start_page" | ページがコマンドラインで指定されたか，または開始ページ. |

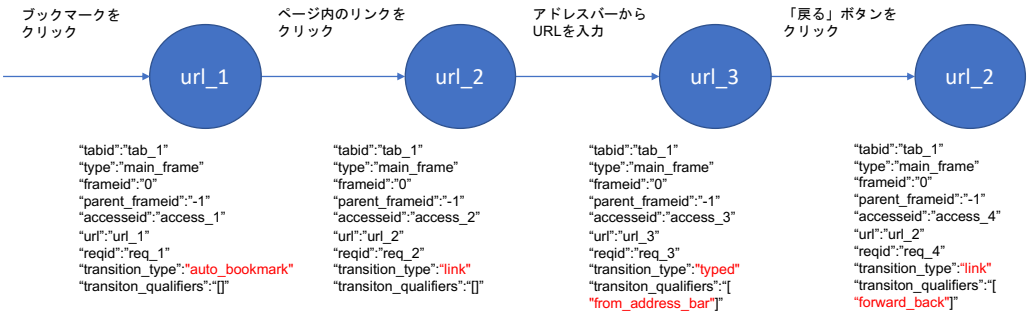
**付録 A.4 データ項目 transition_qualifiers の詳細**

| 値 | 説明 |
|---|---|
| "form_submit" | ユーザがフォームを送信した．フォームがスクリプトを使用してコンテンツを送信するなどの状況では，フォームを送信してもこの遷移タイプにはならない. |
| "reload" | ユーザは，リロードボタンを使用するか，アドレスバーの Enter キーを押してページをリロードした． これは，セッションの復元とクローズドタブの再オープンにも使用される. |
| "keyword" | URL は，ユーザが設定したキーワード検索を使用して生成された. |
| "keyword_generated" | キーワードに対して生成された訪問に対応. |
| "client_redirect" | ナビゲーション中にページ上の JavaScript またはメタリフレッシュタグに起因する 1 つまたは複数のリダイレクトが発生. |
| "server_redirect" | ナビゲーション中にサーバから送信された 3XX HTTP ステータスコードに起因する 1 つまたは複数のリダイレクトが発生. |
| "forward_back" | ユーザは，[進む]または[戻る]ボタンを使用してナビゲーションを開始. |
| "from_address_bar" | ユーザはアドレスバーからナビゲーションを開始. |

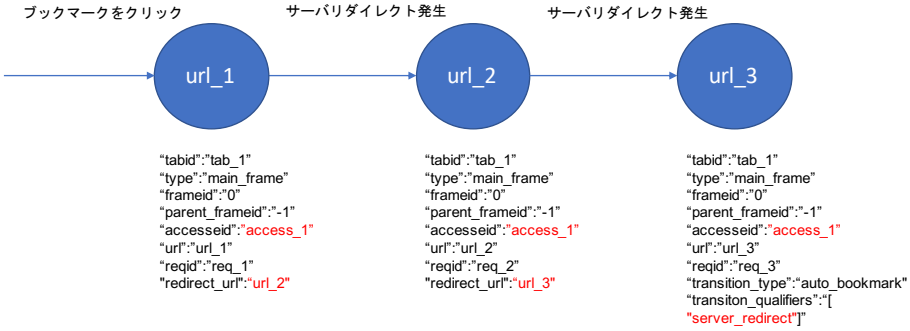
Vol.2020-DPS-182 No.40
Vol.2020-CSEC-88 No.40
2020/3/13

# 付録 B

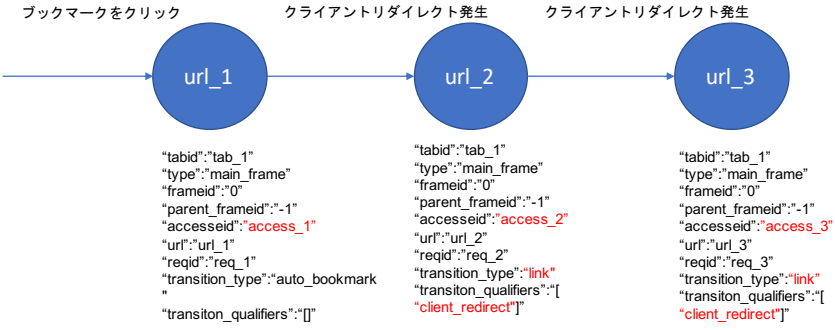
## 付録 B.1 ページ遷移例（ユーザナビゲーション）



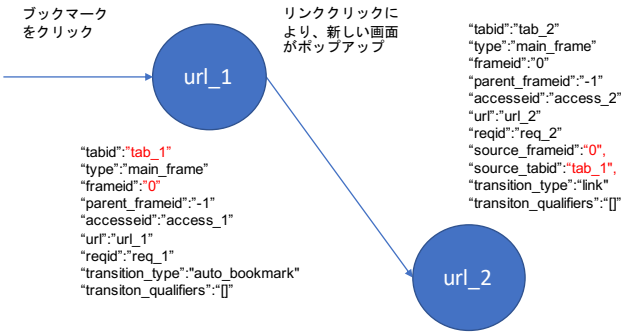

## 付録 B.2 ページ遷移例（サーバリダイレクト）




## 付録 B.3 ページ遷移例（クライアントリダイレクト）




## 付録 B.4 ページ遷移例（ポップアップ）



**付録 C 全文検索エンジン ElasticSearch による検知事例**

| request.timestamp | url | type | transition_qualifiers | transition_type |
|---|---|---|---|---|
| February 11th 2020 15:18:30.617 | http://reward4023.getprizes43.life/... | main_frame | client_redirect | link |
| February 9th 2020 23:17:58.263 | http://best2136.rowglsnil25.live/... | main_frame | client_redirect | link |
| February 9th 2020 23:17:56.572 | http://best2136.rowglsnil25.live/... | main_frame | client_redirect | link |
| February 5th 2020 14:11:26.314 | http://best5574.grownsnd54.live/... | main_frame | client_redirect | link |
| February 5th 2020 14:11:25.307 | http://best5574.grownsnd54.live/... | main_frame | client_redirect | link |
| February 5th 2020 14:11:07.706 | http://best5574.grownsnd54.live/... | main_frame | client_redirect | link |
| February 5th 2020 12:34:41.707 | http://play6697.grownsnd34.live/... | main_frame | client_redirect | link |
| February 5th 2020 12:34:39.362 | http://play6697.grownsnd34.live/... | main_frame | client_redirect | link |
| January 31st 2020 19:10:21.207 | http://mobile2711.bundleio36.live/... | main_frame | client_redirect | link |
| January 31st 2020 19:10:17.225 | http://mobile2711.bundleio36.live/... | main_frame | client_redirect | link |
| January 31st 2020 09:54:24.236 | http://app5212.bundleio80.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:22:13.055 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:22:11.872 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:22:08.794 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:22:06.904 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:21:55.602 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:21:54.403 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:21:49.418 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:21:48.225 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:21:44.918 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 18:21:42.624 | http://mobile3558.nonameprzs16.live/... | main_frame | client_redirect | link |
| January 26th 2020 17:16:57.445 | http://mobile6943.nonamerbon64.live/... | main_frame | client_redirect | link |
| January 26th 2020 17:16:56.287 | http://mobile6943.nonamerbon64.live/... | main_frame | client_redirect | link |
| January 26th 2020 17:16:52.639 | http://mobile6943.nonamerbon64.live/... | main_frame | client_redirect | link |
| January 26th 2020 17:16:50.431 | http://mobile6943.nonamerbon64.live/... | main_frame | client_redirect | link |
| January 21st 2020 08:33:24.324 | http://app6068.nonamecltf7.live/... | main_frame | client_redirect | link |
| January 21st 2020 08:33:18.901 | http://app6068.nonamecltf7.live/... | main_frame | client_redirect | link |
| January 18th 2020 11:42:46.215 | http://sweeps3929.nonamecltf25.live/... | main_frame | client_redirect | link |
| January 18th 2020 11:42:44.587 | http://sweeps3929.nonamecltf25.live/... | main_frame | client_redirect | link |
| January 16th 2020 22:40:21.247 | http://app7109.nonamenmnb27.live/... | main_frame | client_redirect | link |
| January 16th 2020 22:40:19.780 | http://app7109.nonamenmnb27.live/... | main_frame | client_redirect | link |
| January 16th 2020 15:23:51.313 | http://best9417.nonamedvlp2.live/... | main_frame | client_redirect | link |
| January 16th 2020 15:23:49.729 | http://best9417.nonamedvlp2.live/... | main_frame | client_redirect | link |
| January 16th 2020 15:14:51.885 | http://best8079.nonamebonu2.live/... | main_frame | | reload |
| January 16th 2020 15:08:29.658 | http://best8079.nonamebonu2.live/... | main_frame | client_redirect | link |
| January 16th 2020 15:08:28.141 | http://best8079.nonamebonu2.live/... | main_frame | client_redirect | link |
| January 16th 2020 00:47:31.741 | http://prize2810.nonamenmnb17.live/... | main_frame | client_redirect | link |
| January 16th 2020 00:47:29.752 | http://prize2810.nonamenmnb17.live/... | main_frame | client_redirect | link |
| January 16th 2020 00:47:20.487 | http://prize2810.nonamenmnb17.live/... | main_frame | client_redirect | link |
| January 8th 2020 14:14:56.238 | http://app5969.nonameriky34.live/... | main_frame | client_redirect | link |
| January 6th 2020 22:32:02.648 | http://best7492.nonametake61.live/... | main_frame | client_redirect | link |
| January 6th 2020 22:31:42.155 | http://best7492.nonametake61.live/... | main_frame | client_redirect | link |
| January 4th 2020 18:33:16.684 | http://reward0488.nonamelkes65.live/... | main_frame | client_redirect | link |