通信遷移とURLの属性情報を用いた悪性リダイレクト防止手法

佐藤 祐磨† 中村 嘉隆‡ 高橋 修‡

†公立はこだて未来大学大学院システム情報科学研究科
041-8655 北海道函館市亀田中野町 116 番地 2
g2115016@fun.ac.jp

‡公立はこだて未来大学システム情報科学部
041-8655 北海道函館市亀田中野町 116 番地 2
{y-nakamr, osamu}fun.ac.jp

あらまし Webの普及に伴い，Webを通じたサイバー攻撃が深刻化している．近年ではサイバー攻撃の一つであるドライブバイダウンロード攻撃による被害が増加している．我々は，先行研究として，階層が深いWebページのPageRankを取得し，PageRankが低い場合，攻撃とみなし，攻撃を防止するドライブバイダウンロード攻撃防止手法の提案をおこなった．しかし，深い階層の通信に着目しているため，階層が低いWebページの悪性判定が困難である問題がある．そこで本稿ではURLから得られる属性情報を利用することで，通信を網羅的に検査し，攻撃を防止する手法を提案する．

A method of preventing the malicious redirections of Web sites by transitions of HTTP communications and URL attribute information

Yuma Sato† Yoshitaka Nakamura‡ Osamu Takahashi‡

†Graduate School of Systems Information Science, Future University Hakodate
116-2 Kamedanakano-cho, Hakodate, Hokkaido, Japan 041-8655
g2115016@fun.ac.jp
‡School of Systems Information Science, Future University Hakodate
116-2 Kamedanakano-cho, Hakodate, Hokkaido, Japan 041-8655
{y-nakamr, osamu}@fun.ac.jp

Abstract Cyber attacks are increasing with the expansion of the Web. Drive-By Download attacks as cyber attacks inflict further damage on Web users. We proposed a method of preventing the malicious redirection of Web sites using transition of HTTP communications and PageRank status. However, this method has a problem that it cannot detect low layer Web pages. In order to solve this problem, in this paper, we propose improved method of preventing the malicious redirections of Web sites by transitions of HTTP communications and URL attribute information.

1 はじめに

近年，Web の普及に伴い，ドライブバイダウンロード攻撃が巧妙化している．ドライブバイダウンロード攻撃はWeb上を介して行われるサイバー攻撃であり，Web を利用するユーザの PC にマルウェアをダウンロードさせる攻撃である．IBM TOKYOSOC レポートでは 2014 年におい

て，ドライブバイダウンロード攻撃が 2296 件観測されている[1]. 2013 年から上半期・下半期の各期間で 800 件以上の感染が観測されている. 図 1 にドライブバイダウンロード攻撃の検知件数を示す.

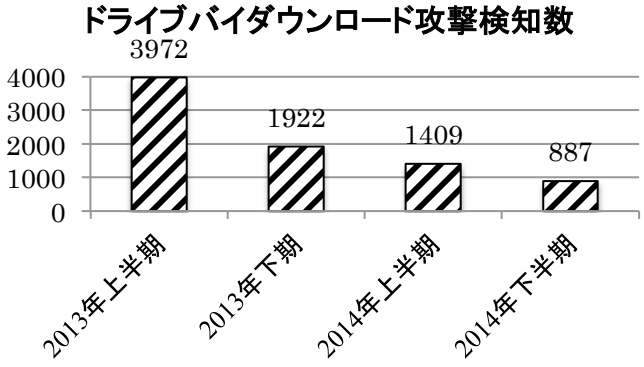

図 1 ドライブバイダウンロード攻撃検知数

ドライブバイダウンロード攻撃は，攻撃者が正規の Web サイトを改ざんして，その Web サイトを閲覧したユーザを攻撃サイトに誘導し，マルウェアに感染させる攻撃である. 一般にこの攻撃では，Web を利用するユーザの使用しているソフトウェアの脆弱性を突いてマルウェアがユーザ端末にダウンロードされる. マルウェアのダウンロードは，秘密裏で行われるため，攻撃中にユーザが気付くことは難しい. このようなドライブバイダウンロード攻撃には，スクリプトコードが利用される. ドライブバイダウンロード攻撃に利用されるスクリプトコードは，攻撃者によって難読化されていて，第三者である攻撃解析者が簡単に解析できないように細工してある. このようにドライブバイダウンロード攻撃は近年巧妙化する傾向にある.

ドライブバイダウンロード攻撃の対策として，難読化スクリプトコードの解析，悪性 URL の収集，HTTP 通信の情報解析など，様々な対策手法が提案されている. にもかかわらず，依然ドライブバイダウンロード攻撃による，マルウェアの感染が報告されている. そこで我々は，HTTP 通信遷移と PageRank を利用してドライブバイダウンロード攻撃において利用される悪性リダイレクトを防止することで，ドライブバイダウンロード攻撃の発生を阻止する手法を提案した[2]. ドライブバイダウンロード攻撃は Web サイトの改ざんによって引き起こされるため，Web サイトの改ざんを長期間検出できない場合，ドライブバイダウンロード攻撃の発見が遅れる場合が考えられる.

そこで本稿では，クライアントであるユーザが Web サイトにアクセスしたタイミングでドライブバイダウンロード攻撃の疑いのある Web ページを検出することで，ドライブバイダウンロード攻撃の防止を既存手法より高精度に行う手法の提案を行う.

2 攻撃手法と技術

2.1 ドライブバイダウンロード攻撃と攻撃フロー

ドライブバイダウンロード攻撃は，マルウェア感染攻撃の一種である. ユーザが Web サイトをアクセスした際，ユーザの意図に関わらず，ユーザに悪意あるソフトウェアをダウンロードさせる[3].

ドライブバイダウンロード攻撃の典型的なフローは図 2 のようになっている. 攻撃者は，正規 Web サイトの Web ページから攻撃者が用意する攻撃 Web サイトへのリダイレクトを目的として，正規 Web サイトのページを改ざんする. 改ざんされた Web ページにアクセスしたユーザは，攻撃者が改ざんによって仕掛けたリダイレクトにより，攻撃者が用意した攻撃サイトへ誘導される. 一般にドライブバイダウンロード攻撃におけるこのリダイレクトは複数存在することが多い. リダイレクトが複数ある理由は，攻撃者が攻撃検出を回避あるいは困難にするためと考えらえる. 攻撃サイトでは，ユーザの使用する OS，ブラウザ，ブラウザのアドオンの脆弱性を突く攻撃が行われ，ユーザの制御が攻撃者に奪われる. その後，ユーザはマルウェア配布サイトへ

誘導され，悪意あるソフトウェアをダウンロードさせられる．

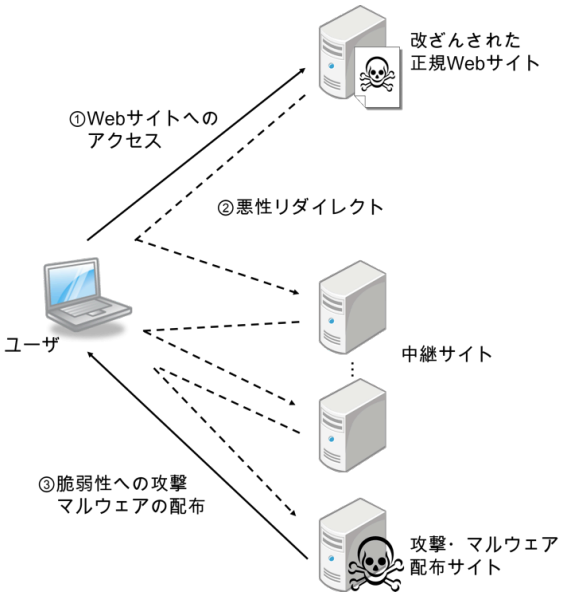

図 2 ドライブバイダウンロード攻撃のフロー

2.2 HTTP ヘッダ

ドライブバイダウンロード攻撃は Web を介してなされる．Web 上の HTTP 通信には HTTP メッセージが利用されており，クライアントからサーバへの要求である HTTP リクエストとサーバからクライアントへの応答である HTTP レスポンスの 2 つから成り立つ[4]．HTTP リクエストには，要求する Web ページ URI 情報も含まれる．HTTP レスポンスには，HTTP 通信の状態を示すステータスコードが含まれる．

HTTP リクエストのヘッダには，クライアントに関する情報が含まれる．HTTP レスポンスのヘッダには，サーバに関する情報，コンテンツの情報が含まれる．要求ヘッダのパラメータとして，要求先のホストを示す Host，HTTP リクエストの発生元を参照する Referer などが含まれる．応答ヘッダのパラメータとして，クライアントが取得するコンテンツの型を示す Content-Type，要求する Web ページの URL 以外の Web ページを提供するために利用される Location などが含まれる．Referer は HTTP リクエストの発生元の情報を含む．それにより Referer の情報から，クライアントの Web ページの遷移がわかる場合がある．ユーザの個人情報が Referer に含まれる場合などのユーザのプライバシーが守られない場合，RFC2068 では，Referer を HTTP ヘッダに付加させないことが推奨されている．

2.3 攻撃で利用される技術

2.3.1 フィンガープリンティング

近年のドライブバイダウンロード攻撃では，フィンガープリンティングが利用されている[5]．フィンガープリンティングとは，サーバである Web サイトが Web サイトにアクセスしたクライアント環境を識別する手法である．一般的に，ユーザの使用する環境に合わせたコンテンツを提供するために使用されるものであるが，ドライブバイダウンロード攻撃者は JavaScript を利用して，ユーザの使用するブラウザやプラグインの環境情報を取得し，その環境情報をもとにリダイレクト先 URL を変更する攻撃を行う．攻撃者は，このフィンガープリンティングによって，攻撃の成功率を向上させている．

2.3.2 難読化スクリプトコード

ドライブバイダウンロード攻撃では，図 3 の様な難読化されたスクリプトコードを利用するものがある．攻撃者は，スクリプトコード内の文字列の置き換えなど難読化を施し，攻撃解析をする第三者にスクリプトコードの挙動を簡単に解析できないようにしている．

```
a="%"+"zxmaaau"+"BzxmaaaD"+"BzxmaaaD"+"%"+"u"+"B"+"D
a88=(KAqaa.replace(/zxmaaa/g,"")); \r\n
ted]var KAqaa99="%"+"u"+"54"+"FF"+"%u"+"BE"+"A3%uB"+
a98=(KAqaa99.replace(/zxmaaa/g,"")); \r\n
```

図 3 難読化されたスクリプトコードの例

3　既存手法

我々は文献[2]において，ドライブバイダウンロード攻撃における悪性リダイレクトの防止手法を提案し，評価を行ってきた．

3.1　PageRank を用いた攻撃防止手法

既存手法は Web 階層と PageRank を用いてドライブバイダウンロード攻撃を検出し，悪性リダイレクトを防ぐ手法である．

3.1.1　Web 階層

Web 階層とは，任意の Web ページがリダイレクトによって読み込む Web ページの構造と定義する．

任意の Web ページの階層を 1 とする．その Web ページが読み込む Web ページの階層を 2 とする．Web ページの階層が 2 の読み込む Web ページの階層を 3 とする．3 層以上深い階層も同様に階層をカウントする．

Web 階層を木構造で表すと図 4 のようになる．階層 1 の Web ページを木構造の根とする．階層 1 の Web ページが読み込む階層 2 の Web ページは，根の子となる．

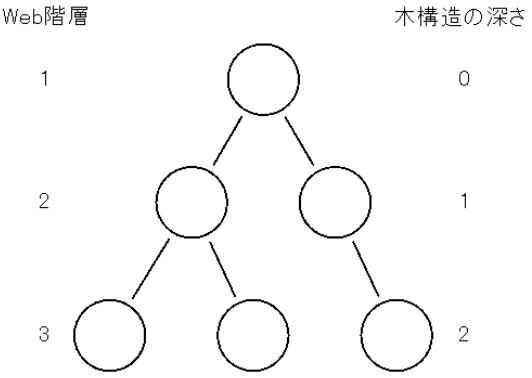

図 4　Web 階層

3.1.2　**PageRank**

PageRank は，ある論文の重要性は他の論文からの引用数によって評価されるという学術論文の考えを Web に適用したものである[6]．論文の重要度は，被引用数で決まり，PageRank は被リンク数が影響する．PageRank のアルゴリズムは，「任意の Web ページ A の PageRank は Web ページ A にリンクしている各ページの PageRank を，そのページからの外向きのリンク数で割った値の総和」として定義される．PageRank は Google から見た Web ページの重要度であり，0 から 10 の 11 段階でランク付けされる． PageRank の値が高ければ高いほど，Google から見た Web ページの重要度は高いとされる．Google は，自動化されたプログラムなどによって，リンクを作成するなど，不自然なリンクについてペナルティを与える場合もある．Google は，PageRank を上げるには，インターネットコミュニティで自然に人気を獲得すること，関連性の高い独自のコンテンツを作成することと述べている．本稿では，この PageRank を利用し，ユーザがアクセスする Web ページの信頼度のひとつの指標とする．

3.1.3　**既存手法のアルゴリズム**

HTTP 通信の Web 階層と PageRank を用いてドライブバイダウンロード攻撃による悪性リダイレクトを防止する．HTTP 通信の通信遷移を利用し，Web ページの Web 階層をカウントする．条件を満たす HTTP 通信の情報と，PageRank を利用し，通信が悪性リダイレクトかどうかを判別する．

ユーザのクリックまたは URL バーに入力した Web ページの階層を 1 とし，その Web ページが読み込む Web ページの階層を Referer，Location を利用して，Web 階層をカウントする．階層が 4 以上の通信に対して，リクエスト URL の完全修飾ドメイン名 FQDN の PageRank を取得する．PageRank が 0 または，存在しない場合は，悪性リダイレクトとみなし，通信を遮断する．また，HTTP ヘッダは書き換えが可能なので，Referer が存在しない場合もある．このときは，リクエスト URL に含まれる FQDN の PageRank を取得し，PageRank が 0 または存在しない場合は同様に悪性リダイレクトとみなす．さらに階層

が 2 以上で Content-Type が application/pdf の Web ページ，Web ブラウザが自動で読み込む Web ページが実行ファイルで，階層 1 の FQDN とリダイレクト先の FQDN が異なる場合リダイレクト先の FQDN の PageRank を取得し，悪性リダイレクトの判別を行う．文献[7]より悪性 Web サイトの生存期間は 1 日のものが多いとわかっている．生存期間が短い Web サイトに PageRank は存在しないため，Google に評価されてないを悪性 Web サイトと見なし，これらの Web サイトとの通信を遮断することで悪性リダイレクトを防ぐ手法である．

3.2 問題点

既存手法では，階層 2 以上の実行ファイル・PDF，階層 4 以上の Web ページ，及びつながりの不明な Web ページしか攻撃判別対象としていない．しかし，最近よく見られる攻撃パターンでは，階層 2 以上に画像ファイルのマルウェアが含まれている場合もあり，そのような場合，既存手法ではドライブバイダウンロード攻撃を防止することができないという問題点がある．

4 提案手法

4.1 提案手法のアルゴリズム

クライアントであるユーザが Web サイトにアクセスしたタイミングでドライブバイダウンロード攻撃の疑いのある Web ページを検出し，HTTP 通信の Web 階層とドメイン年齢と PageRank を用いてドライブバイダウンロード攻撃による悪性リダイレクトを防止する．提案手法は，既存手法を改善することにより，問題点を解決するドライブバイダウンロード攻撃を防ぐ手法である．HTTP 通信の通信遷移を利用し，Web ページの Web 階層をカウントする．条件を満たす HTTP 通信の情報と，PageRank を利用し，通信が悪性リダイレクトかどうかを判別する．

ユーザのクリックまたは URL バーに入力した Web ページの階層を 1 とし，その Web ページが読み込む Web ページの階層を Referer，Location を利用して，Web 階層をカウントする．以下に示すどれかに当てはまる場合，その Web ページの PageRank を取得する．

- ドメインの生存期間が 6 ヶ月以内
- Referer が存在しない
- 階層が 4 以上の通信
- 階層 2 以上で Content-Type が application/pdf の Web ページ
- Web ブラウザが自動で読み込む Web ページの Content-Type が application/octet-stream, application/x-download, application/x-msdownload, application/x-msdos-program かつ階層 1 の FQDN とリダイレクト先の FQDN が異なる場合

リクエスト URL の完全修飾ドメイン名 FQDN の PageRank を取得する．PageRank が 0 または，存在しない場合は，悪性リダイレクトとみなし，通信を遮断する．

ドメイン年齢とは，Web サイトのドメインが登録されてから現在までの期間である．ドメインの生存期間が 6 ヶ月以内という項目を既存手法に追加している．これは，既存手法の Web ページ判別対象範囲を広げるために追加した項目である．PageRank の取得条件に，ドメインの生存期間が 6 ヶ月以内としたのは，文献[8]はある特定の悪性サイトのドメイン生存期間が最長 6 ヶ月であるということを示している．既存手法では判別できない範囲 Web ページに対して，ドメイン情報を利用し，生存期間が短い Web ページを判別する．その Web ページが良性であるか悪性であるかの判別方法は，PageRank が 0 または存在しなければ悪性，それ以外であれば，良性とみなす．悪性であれば，通信を遮断する．このようにアクセスを防止することで，ドライブバイダウンロード攻撃で利用される悪性リダイレクトを防ぐ．

5　実験データと実験方法

5.1　実験データ

5.1.1　良性データ

Alexa Internet, Inc（以下 Alexa）は，Web サイトのアクセス数の調査や統計をとっており，世界・国別のカテゴリでそれぞれアクセス数が高い Web サイト上位 500 件のランキングを公表している[9]. また，Web コンテンツのカテゴリ別で，それぞれのアクセスが高い Web サイト最大上位 500 件を公表している.

本稿では，2015 年 4 月 16 日に取得したアクセスランキングに基づき，HTTP 通信を行う Web サイト 100 件を実験対象とする. 本実験では，これらのサイトの URL を巡回して発生する通信データを良性通信データ標本とする. 実験対象の Web サイト 100 件は，世界のアクセスランキングトップ 500 位以内にランクインしているが，必ずしも良性通信を行うとは限らない. しかし，本実験では，良性データの標本として取り扱う. また，HTTP 通信を行う Web サイト 100 件の URL をユーザのアクセスした URL として実験で使用する.

実際の良性通信データは，クローラで 100 件の URL が示す，Web サイトを巡回し，発生する通信データを tcpdump でパケットキャプチャしたることで取得したこの良性通信データは，PCAP 形式のファイルである.

5.1.2　悪性データ

NTT セキュアプラットフォーム研究所は，2010 年から Web クライアント型ハニーポットを使用し，ドライブバイダウンロード攻撃に関連するデータを収集している[10]. このデータは D3M（Drive-by Download Data by Marionete）データセットと呼ばれる. NTT セキュアプラットフォーム研究所は感染の検出・解析技術の研究を行う研究機関に D3M データセットを提供している. D3M データセットには，あるブラックリストを巡回して得られたドライブバイダウンロード攻撃の攻撃通信データ，巡回 URL，ドライブバイダウンロード攻撃によってクライアントにダウンロードされたマルウェアのハッシュ値，マルウェアをサンドボックス上で実行した際のマルウェアの通信データが含まれる.

本実験では，D3M データセットに含まれるあるブラックリストを巡回して得られたドライブバイダウンロード攻撃通信データと巡回 URL を使用する.

攻撃通信データは，ハニーポットの通信を tcpdump でパケットをキャプチャした PCAP 形式のファイルである. このファイルを悪性データとし，D3M2010 を除いたデータを本実験で使用する標本とする. また，巡回で利用された URL を実験で使用する.

5.2　標本のデータ抽出

標本である実験データには HTTP ヘッダ以外の雑音の通信が含まれる. 前処理として，実験データから HTTP リクエストと HTTP レスポンスのパケットを抽出し，抽出した各パケットからフレーム番号，HTTP リクエストフラグ，HTTP レスポンスフラグ，送信元ポート番号，送信先ポート番号，HTTP ヘッダの HOST, Referer, Location, Content-Type, リクエスト URI の 10 種類のパケット内の HTTP ヘッダ情報を抽出した. HTTP リクエストと HTTP レスポンスの対応は，送信元・先ポート番号を利用しリクエストとレスポンスの対応付ける処理を行った.

5.3　実験方法

実験は，標本である実験データからパケット・HTTP ヘッダ情報をテキストファイルに変換し，そのテキストファイルを使用する. 一般的にユーザは Web ブラウザでリンクをクリックする. または，URL バーに URL を入力し，Web サイトにアクセスする. この動作を再現するために，本実験では，実験データの取得の際，巡回した URL のテキストファイルを使用する. パケット・HTTP ヘッダ情報のテキストファイルと巡回した URL のテキストファイルの 2 種類のテキストファ

イルを読み込み，提案手法を適用し，実験を行う.

5.4 評価方法

本実験では，真陽性率，偽陰性率，真陰性率，偽陽性率，全体の攻撃検出率の 5 つの評価項目によって評価する.

悪性データはセッション単位で評価を行う. ここでのセッションとは，ユーザが任意の 1 件の Web ページにアクセスした際に行われる通信全てを示す. 本実験では，アクセス時間を考慮せず，ある Web サイトへの 1 回のアクセスを 1 セッションとする.

真陽性率は，攻撃が発生したセッションにリダイレクト先の攻撃を未然に防いだ場合の割合である. (1)の計算式で真陽性率を評価する.

真陽性率

$$= \frac{\textbf{\textit{マルウェアのダウンロードを未然に防いだ件数}}}{\textbf{\textit{悪性通信データに含まれるマルウェアの数}}} \quad (1)$$

偽陰性率は，攻撃が発生したセッションに対して，リダイレクト先の攻撃を防げなかった場合の割合である. (2)の計算式で偽陰性率を評価する.

偽陰性率

$$= \frac{\textbf{\textit{マルウェアをダウンロードした件数}}}{\textbf{\textit{悪性通信データに含まれるマルウェアの数}}} \quad (2)$$

良性データは Web ページごとに評価を行う. HTTP リクエストに対する HTTP レスポンスを一対とし，対ごとに評価を行う.

真陰性率は，良性 Web ページを良性 Web ページとみなした場合である. (3)の計算式で真陰性率を評価する.

真陰性率

$$= \frac{\textbf{\textit{良性Webページを良性とみなした件数}}}{\textbf{\textit{良性通信HTTPリクエスト・レスポンス組全数}}} \quad (3)$$

偽陽性率は，良性 Web ページを悪性リダイレクトとみなした場合である. (4)の計算式で偽陽性率を評価する

偽陽性率

$$= \frac{\textbf{\textit{良性Webページを悪性とみなした件数}}}{\textbf{\textit{良性通信HTTPリクエスト・レスポンス組全数}}} \quad (4)$$

また全体の攻撃検出率として，(5)の計算式を用いる.

全体の攻撃検出率

$$= \frac{\textbf{\textit{真陽性の件数}} + \textbf{\textit{真陰性の件数}}}{\textbf{\textit{真陽性}} + \textbf{\textit{偽陰性}} + \textbf{\textit{真陰性}} + \textbf{\textit{偽陽性の件数}}} \quad (5)$$

6 実験結果と考察

6.1 実験結果

本稿では，D3M2014 に含まれる，2011 年 2 月 14 日，2012 年 3 月 28 日，2014 年 4 月 11 日分取得されたデータに対する評価結果を示す. この 3 日分に関して，真陽性率は 100%，偽陰性率は 0%となった. つまり全ての悪性リダイレクトを防いだ.

6.2 考察

本稿で提案した手法は，真陽性率・偽陽性率については既存手法と同じ結果となったが，提案手法は既存手法よりも，攻撃判別対象範囲が広く，既存手法では判別できなかった Web ページを良性か悪性を判断することができると考えられる. さらに提案手法はマルウェアのダウンロードに至る前のリダイレクトを事前に防ぐことができる. これは，ドメイン生存期間を攻撃検出項目として利用することで，既存手法の問題点であった攻撃を判別できないという問題点を提案手法では解決できると考えられる. ドライブバイダウンロード攻撃のリダイレクトを防止する手法として既存手法より優れていると考えられる.

7　おわりに

本稿で提案する通信遷移とURLの属性情報を用いることで既存手法では良性か悪性かを判別できないものを判別することができるようになった. ドメイン生存期間が短い Web サイトの Web ページを PageRank で悪性かどうか判断することで，悪性 Web ページを既存手法よりも正確に悪性とみなすことができると考えられる. しかし，本手法では，既存手法よりも攻撃検査対象が広いため，良性を良性とみなす真陰性率が既存研究を下回ると考えられる.

今後の課題として，全ての D3M データセット，良性データに提案手法を適用し，提案手法を評価する必要がある. また，本提案手法は良性を良性みなす真陰性率が低くなることが考えられるので，真陰性率を向上する手法を考案，提案し，ドライブバイダウンロード攻撃の防止精度率向上を目指したい.

参考文献

[1] IBM, "Tokyo SOC 情報分析レポート", http://www-935.ibm.com/services/jp/ja/it-services/soc-report/

[2] 佐藤祐磨，中村嘉隆，高橋修，"通信遷移とPageRankを用いた悪性リダイレクト防止手法の評価"，情報処理学会研究報告，マルチメディア，分散，協調とモバイル(DICOMO2015) シンポジウム論文集，pp.927-933, 2015.

[3] IPA 独立行政法人 情報処理推進機構，"コンピュータウイルス・不正アクセスの届出状況[2010 年 11 月分]について", https://www.ipa.go.jp/security/txt/2010/12outline.html

[4] "RFC INDEX", http://www.rfc-editor.org/rfc-index.html

[5] C.Kolbitsch, B.Livshits, B.Zorn, C.Seifert, "Rozzle: De-cloaking Internet Malware", Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP'12), pp. 443-457, 2012.

[6] L.Page, S.Brin, R.Motwani, T. Winograd, "The pagerank citation ranking: Bringing order to the web", 1998

[7] 秋山満昭，八木 毅，針生剛男, "改ざんWebサイトのリダイレクトに基づく悪性Webサイトの生存期間測定"，情報処理学会研究報告, Vol. 2014-SPT-8, No.32, pp. 1-6, 2014.

[8] Christian Seifert, Vipul Delwadia, Peter Komisarczuk, David Stirling, Ian Welch, "Measurement Study on Malicious Web Servers in the .nz Domain", Proceedings of ACISP 2009, pp. 8-25, 2009.

[9] Alexa, "Actionable Analytics for the Web", http://www.alexa.com/

[10] 秋山満昭，神薗雅紀，松木隆宏，畑田光弘, "マルウェア対策のための研究用データセット～MWS Datasets 2014～"，情報処理学会研究報告, Vol. 2014-CSEC-66, No. 19, pp. 1-7, 2014.