Webページ内リンク情報の変化に基づくWeb改ざん検知の有効性検証

望月 翔太† 高田 哲司†

†電気通信大学
182-8585 東京都調布市 調布ケ丘 1 丁目 5-1
m-shouta@uec.ac.jp,zetaka@computer.org

あらまし 外見では改ざん判別が困難なWebページによる閲覧者を対象とした攻撃が行われている．これに対して我々は，Webページ内にあるリンクURLの時間変化に着目したWeb改ざん検知手法を提案した．しかし，提案手法の改ざん検知能力については未検証である．そこで本論文では，提案手法の有効性を検証すべく，Alexa Top 100を起点として収集したWebページを対象として評価実験を行った．その実験結果をふまえて，提案手法の有効性と今後の課題について議論する．

Validation of Web Alteration Detection using Link Change State in Web Page

Shouta Mochizuki† Tetsuji Takada†

†The University of Electro-Communications.
1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, JAPAN
m-shouta@uec.ac.jp, zetaka@computer.org

Abstract There are attacks targeted viewers by difficult Web page judgment of alteration. We have proposed a Web alteration detection method that focuses on the time change of the link URL in the Web page. However, it is untested for alteration detection capability of the proposed method. In this paper, in order to verify the effectiveness of the proposed method, we have an evaluation experiment targeted a Web page that collected the Alexa Top 100 as a starting point. Based on the experiment result, we discuss the effectiveness and future works of the proposed method.

1 はじめに

Web上で行われる攻撃の1つにDrive-by Download攻撃がある．この手法は，クライアント計算機に存在する脆弱性を突くWebサイト (攻撃サイト) を用意し，攻撃サイトへのリダイレクトを行うサイト (ランディングサイト) を訪れたユーザを攻撃する．ランディングサイトは，正規サイトの改ざんによって作成された場合が多い．

Drive-by Download攻撃への対策として，ブラックリスト (例 : Google Safe Browsing[2]) が挙げられる．これは，既知の悪性Webページのリストを用意し，ユーザがアクセスを試みるWebページがこのリスト内に存在するかをチェックする方法である．しかし，Webサイトは数多く存在し，かつ悪性サイトと判定するまでの間はブラックリストに反映されないため，ユーザが悪性Webページにアクセスしてもブラッ

クリストで防げない場合がある．

ブラックリストに基づくURL群を対象にclient honeypotを用いてDrive-by Download攻撃を検知する研究 [3, 6, 5] も行われている．あらかじめ，Drive-by Download攻撃に現れるリダイレクトなどの特徴を学習し，クローリングによって収集したサイトを分析することで未知のDrive-by Download攻撃を検出している．未知のDrive-by Download攻撃を検出した後，サーバ管理者へ報告または，ブラックリストへ反映させることで被害を抑えることが可能となる．

これらの対策は有用ではあるが，悪性サイトが開設されてから反映されるまでは時間がかかる．また，ユーザが訪れたWebページを毎回honeyclient等の検出システムで良性/悪性判定することは現実的でない．その結果，実害を被るのはユーザである．このような状況のため，ユーザ自身が日々のブラウジング環境でWebページの改ざんに気付けるような仕組みを考えていくべきであると考えた．前述したとおり，Drive-by Download攻撃等に使用される正規Webページの改ざんには，攻撃用のサーバにアクセスさせるためにiframeタグやscriptタグのようなリダイレクト可能なタグを挿入する．よって，正規WebページのDOMツリー内では，内部に記述されたURLの構成が変化していることが予想できる．そこで，我々は，このDOMツリー内に記載されるURLの構成の変化を特徴点ととらえ，視覚化することでユーザへWebページの異変を提示する手法を提案してきた．

本稿では，本手法がWeb改ざんをどの程度検知可能か検証した．Alexa[9] で公開されているWebページを起点として収集した12414のURLを対象に，Webページ上に記載されているURLリンクの時間変化を収集し，検証を行った．

2　関連研究

2.1　ランディングサイトの識別

ランディングサイトを識別する手法として，Stokesら [5] のWebCopがある．各サイトをリダイレクトやハイパーリンクに基づきグラフを作成し，既知のマルウェア配布サイトからランディングサイトへ逆にたどる手法(ボトムアップアプローチ)により，ランディングサイトを識別する．WebCopにより，約400,000の悪意のあるランディングサイト，350,000の未知のマルウェア配布サイトを識別した．しかし，WebCopはWebグラフを作成する必要があり，多くのWebページへアクセスする必要がある．また，多数のサイトを探索するため，実行時間がかかり，短命なマルウェア配布サイト，ランディングサイトを発見することが困難である．

2.2　Webサイトの時間変化に着目した悪性サイトの検出

Webサイトの時間変化に着目した手法として，Kevinら [7] のΔ-システムがある．Δ-システムはWebサイトの時間軸の異なる2つのバージョンを比較し，DOMツリー構造の差分に基づきクラスタリングを行うことで悪性サイトを識別する．JavaScriptによるDOMツリーの動的変化やJavaScriptコードの難読化により，異なるグループとして判定してしまう可能性があるため，どのようにデータを学習するかが課題となっている．

また松中ら [8] のFCDBDがある．FCDBDは，ユーザ参加型のDrive-by Download攻撃対策フレームワークである．アクセスしたWebページから1ホップ先のWebページが新規に追加されたWebページであり，かつ追加されたサイトの遷移元サイト，遷移先サイトの数の関係が多対一であった場合，ランディングサイトとして検出する．

3　提案システム

3.1　概要

本システムは，ユーザが評価対象Webページへ過去に訪れた際に取得したWebコンテンツと現在訪れているWebサイトのコンテンツを比較することでWeb改ざんの検知を行う．これは，ユーザは定期的に同じサイトを訪れる傾向があることを利用している．

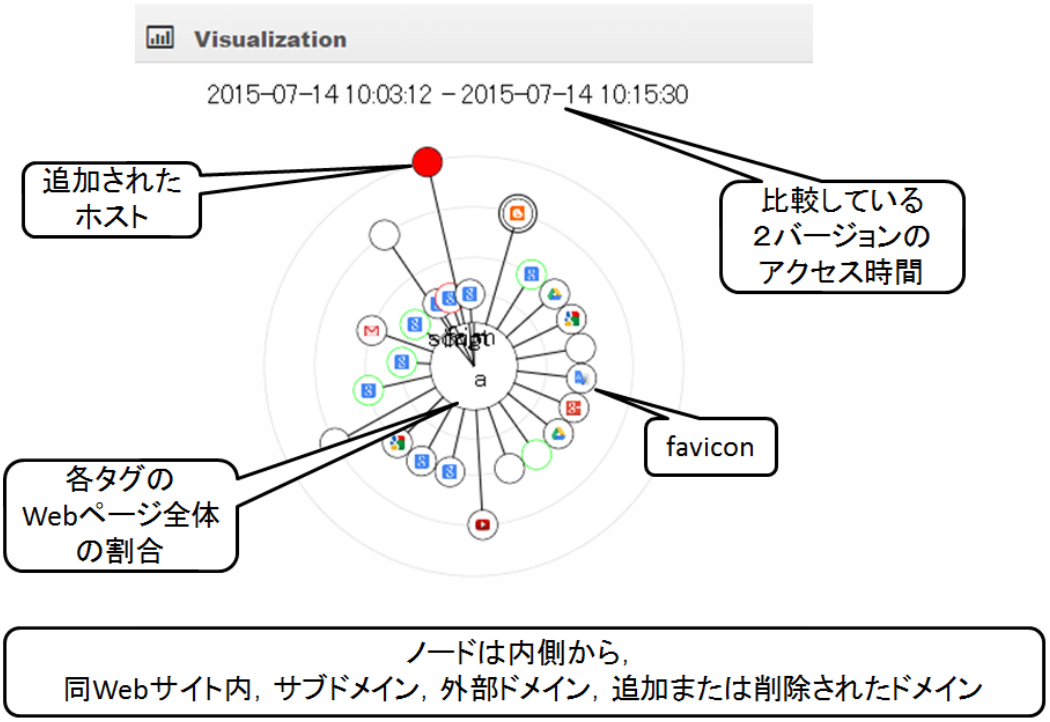

図 1: 視覚化例

本システムは，Google Chrome の拡張機能として実装されており，以下の仮説に基づき，ブラウザが構築した DOM ツリーからタグ情報とタグの属性値の URL を利用する．

- 正規 Web ページを閲覧しているユーザをマルウェア感染させるため，正規 Web ページから中継ページ，マルウェア配布ページへとリダイレクトさせる．
- リダイレクトには，script タグや iframe タグ等の URL が付加することができるタグが利用されている．

本システムはブラウザが構築した DOM ツリーからタグ情報とタグの属性値の URL を取得した後，取得先のページへ過去に訪れていないかデータベースをチェックする．もし訪れていた場合，過去に取得したデータと今回取得したデータをタグごとに比較し，データベースへと格納する．その後，比較結果を URL のホスト名，タグの種類，URL の変化に着目して視覚化を行う．URL は比較により，「消失 URL」，「現存 URL」，「出現 URL」の 3 種類に区別される．

3.2 視覚化

実際に視覚化した画面を図 1 に示す．

本視覚化手法では，中心の円は閲覧中の Web ページ内に記述される各タグの割合を示しており，各ノードは，閲覧中の Web ページに記述されている各タグごとのホストを示している．内側から，閲覧中のホスト，サブドメインが異なるホスト，外部ホスト，過去に閲覧した Web ページには記述されていなかったホストまたは過去には記述されていたが今回は記述されていないホスト順に表示される．つまり，円の外側に行けばいくほど閲覧中の Web ページとは異なる管理者が運営する Web ページが記述されている可能性があることを示している．

各ノードは，比較処理の結果が色で表現されている．ノードはタグとホスト名の組み合わせ

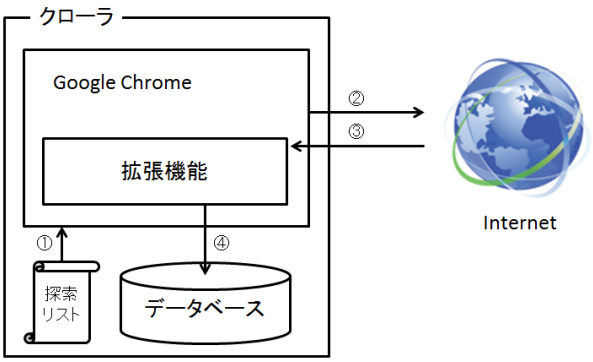

図 2: クローラ構成図

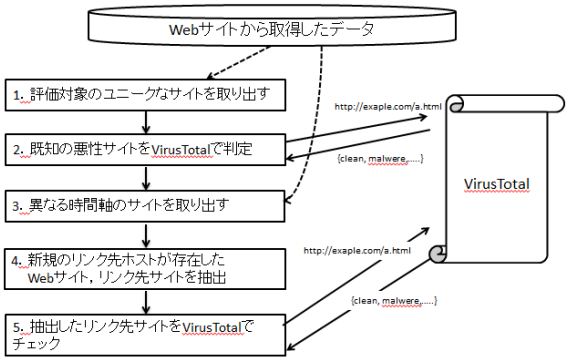

図 3: 実験手順

が一致するグループの単位で表しているため，ノードには複数の URL が属している．ノードに属する URL が消失 URL を含む場合に青色，出現 URL を含む場合に赤色で表現される．改ざんされた Web ページに追加される URL は，過去には記述されていなかったホストである可能性が高い．そのため，この特徴を持つホスト（ノードに属する URL がすべて出現 URL）の場合，危険色である赤でノードを塗りつぶすことにより，視覚化画面を閲覧するユーザが一目で理解できるように工夫した．

4 評価実験

4.1 実験方法

提案システムの Web 改ざん検知能力を検証するため，多くの Web コンテンツを収集し，検証実験を行った．実験方法の概要は以下の通りである．

1. 実験対象 Web ページの URL の取得
2. 提案システムによる Web ページの特徴情報取得
3. 提案システムによる改ざん検知評価
4. 手順 3 の検知結果を VirusTotal で照合

以降では上記手順について詳細を説明する．

手順 1：実験対象 Web ページの URL 取得

実験対象の Web ページとして Alexa[9] で公開されている Web ページランキングの Top 100 までの Web ページを起点とした．この 100Web ページの HTML を取得し，その HTML ファイル内に記載されている a タグの href 属性値，すなわちリンク先の URL を静的解析にて取得した．これにより Top 100 の URL100 個とあわせて合計 12414 URL を収集した．

手順 2：提案システムによる Web ページの特徴情報取得

実験対象 Web ページの特徴情報を提案システムを利用して取得する．実験対象 Web ページは手順 1 で取得した 12414 URLs でアクセスできる Web ページである．この特徴情報取得処理のため，図 2 に示すような提案手法による Web クローラシステムを実装した．これにより URL リスト内の URL へ提案システムによって次々とアクセスし当該 URL でアクセスできる Web ページから特徴情報を抽出する．この Web クローラの処理手順について説明する．手順 1 で得た URL リストがある．Web クローラは URL リストから URL を読み込み (①)，提案システムを組み込んだ Google Chrome Web ブラウザで Web ページへアクセスする．Web コンテンツが Web ブラウザに送られてくると，ブラウザは内部で Web コンテンツに基づき DOM ツリーを構成する．提案システムは，この DOM ツリーを入力情報とし，7 種のタグを対象として (タグ, URL) の対情報を収集する．現在，収集

対象になっているタグは a, img, script, iframe, frame, form, param の 7 種である．収集された対情報は収集時刻とともにデータベースに保存される (④)．

提案システムは，Web コンテンツ内に記載された URL 値の時間変化を利用している．よって同一 Web コンテンツの異なる収集時刻による特徴情報が必要となる．そこでこの手順 2 を時間間隔をあけて 2 度実施した．収集 1 回目と 2 回目の間の期間は最低 1 週間の間隔をあけている．

手順 3：提案システムによる改ざん検知評価

手順 2 により，各 URL によりアクセス可能な Web コンテンツの特徴情報を異なる収集時間で 2 version 分取得した．この収集した特徴データをもとに差分，すなわち Web 改ざんの疑いがあるかどうかを提案システムで評価する．入力値は 2 version 分の特徴情報で，出力値は差分あり or なしである．差分ありの場合は，提案システムの視覚化画面で赤又は青の塗りつぶしノードが出現することになる．また Web コンテンツの URL を VirusTotal で検証し，“clean site” と “not clean site” に分類する．clean 判定とは，VirusTotal で URL を入力値として検証を行い，その結果が clean site と unrated site だけであった場合と定義する．これ以外の判定結果になった場合は not clean site と定義する．これにより各 URL に対して (差分あり/なし) と (clean site/not clean site) の 2 属性情報が追加されたことになる．

手順 4：差分ありコンテンツの改ざん検証

手順 3 の評価により「差分あり」と判定された Web コンテンツについて，差分となった「追加された」または「削除された」URL を抽出する．この抽出された URL 群について VirusTotal で clean site か not clean site かを検証し，各 URL の Web コンテンツから抽出された URL 群のうち 1 つでも “not clean site” が存在した場合には「改ざん」と判定し，それ以外は「更新」と判定する．これにより，差分があった Web コンテンツが「改ざん」か「更新」かを判別する．

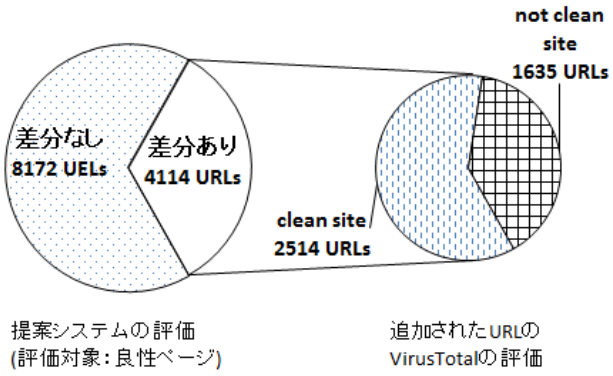

図 4: 追加評価

4.2 実験結果

手順 3 の結果を表 1 に示す．各 Web コンテンツについて (差分あり/なし) と (clean site/not clean site) に 2 属性情報が付与されている．それぞれの条件の URL をまとめたものである．これにより差分のある Web コンテンツは 4149 URLs(33.4%) となった．

次に差分のあった Web コンテンツについて，追加または削除された URL を VirusTotal で検証した結果，改ざんと判定されたのは 1635 URLs であり，更新と判定されたのは 2514 URLs である (図 4 参照)．これらは差分があるため提案システムでは改ざんとして検出されるが，clean site については改ざんではない可能性が高いため，本来は提案システムで「改ざん」として検出されないことが望ましい．つまり False positive 判定であると考える．この事例と対応策について考察で議論する．

5 考察

5.1 評価対象データの妥当性について

我々は評価用のデータとして Alexa Top 100 の Web ページから 1 階層たどった URL を対象とした．今回，提案システムが正規 Web ページの「改ざん」と「更新」を区別可能か検証することが目的の実験を行った．そのため，悪性 Web ページではなくかつ Web 改ざんがされていない Web ページを収集する必要があった．Alexa

表 1: 提案システムの評価

VirusTotal の結果	差分なし	割合	差分あり	割合	合計
clean site	8172 URLs	66.5%	4114 URLs	33.5%	12286 URLs
not clean site	93 URLs	72.7%	35 URLs	27.3%	128 URLs
合計	8265 URLs	66.6%	4149 URLs	33.4%	12414 URLs

表 2: 実験対象サイトの広告の割合

clean site	広告と思われるサイトが検出されたサイト	割合
4114 URLs	2241 URLs	54.5%

で公開されている Web ページを対象とした理由として，公開されている Web ページは人気のある Web ページであり，多数のユーザが訪れている Web ページであるため，多数の衆人環視（セキュリティ関係者含む）の状況があることから悪性の Web ページではなく，かつ Web 改ざんが発生しても即座に対応される Web ページ群であると考え，評価対象データとして利用した．また，1 階層たどった URL に関しては，Alexa Top 100 の Web ページにアクセスした人が訪れる可能性が高く，他の Web ページよりアクセス数が多いと考えられるため，同様に正規かつ Web 改ざんの起こっていない Web ページであると考えられるためである．

5.2 False positive について

提案システムは，視覚化画面で赤又は青の塗りつぶしノードが出現した場合,「改ざん」と判定する．False positive である,「更新」と判定された Web ページは実験手順 4 の結果（図 4）より，2514 URLs 存在した．提案システムが「更新」と思われる Web ページを誤判定してしまった原因として，以下の事例を確認した．

5.2.1 広告コンテンツによる False positive

False positve の原因として，広告の存在がある．広告はアクセス毎に URL が変更されるため，前回アクセス時の Web ページの差分を取得するのみでは新規ホストの出現として誤検知する可能性がある．広告による False positive の影響を調査するため，Adblock Plus[10] で使用されているフィルタを利用して検証した．検証結果を表 2 に示す．表 2 より，54.5%が広告による誤検知が存在していることが判明した．これは，False positive を引き起こす最大の原因となっていることが考えられる．しかし，広告を介した Drive-by Download 攻撃も観測されているため，単純に広告コンテンツを除外して改ざんを検知することは得策ではないと考えられる．Provos ら [3] によると，広告を利用した Drive-by Download 攻撃は，通常の広告のリダイレクト数と比較すると，リダイレクト数が Drive-by Download 攻撃の方が多くなるとの結果で出ている．そのため，広告と判明したリンク先について，リダイレクト数を調査し，評価指数（リダイレクト数が多いほど信頼性が低くなる）として追加して評価する方法が考えられる．

5.2.2 その他の理由による False positive

「改ざん」と判定した Web サイト中，広告の影響がなかったサイトを調査した結果，以下の特徴が判明した．

- 検索ページによる誤検知
- ブログ，ニュースサイトによる誤検知

以降では上記項目について詳細を説明する．

検索ページによる誤検知

検索ページはユーザからのリクエストに応じ，検索ワードに関連した結果を提示する．検索結果として出てくる順番は検索エンジンのランキングに応じて変更される．つまり，検索キーワードのランキングが変動した場合，前回検索時とは検索結果の Web ページの内容が変更されてしまう．この検索ワードのランキング変動によって，a タグのリンク先等が変更された結果,「差分あり」として提案システムが判定することで誤検知となってしまっている．検索ページによる誤検知を回避するため，ホワイトリストを作成し，検索ページは判定しないなどの対策が考えられる．

ブログ，ニュースサイトによる誤検知

ブログやニュースサイトは Web ページ管理者が情報発信を行うページであり，記事の更新などで日々Web ページのコンテンツが変更される．また，外部の Web ページを参照することも多い．そのため，a タグや img タグに属する URL が過去に Web ページ上ではリンクされることのないホスト先である可能性がある．結果として，提案システムが誤検知したと考えられる．

本システムで a，img タグを収集する理由として，SQL インジェクション等の攻撃によって href 属性や src 属性に JavaScript コードの埋め込みやリンク先を変更することで，アクセスしたユーザを別ページへと誘導するような改ざんを検知することが目的で収集している．上記 2 つの誤判定はどちらも a タグや img タグのリンクが起因している．このことより，a タグや img タグに対しては他のタグとは別のアプローチで評価する必要があると考えた．a タグのリンクの場合，ユーザにリンク先へ誘導するために，Web ページ上にリンク先の説明が記載されている可能性が高いことが容易に想像できる．そのため，a タグのリンクの場合のみ a タグ内のコンテンツの内容を加味して（例えば，a タグ内コンテンツの内容とアクセス先の title の内容の類似度判定）評価に重みづけすることで対応したいと考えている．

5.3 False negative について

提案システムは，収集時間の異なる Web ページの version 間に差分がない場合は「改ざん」ページとして判定しない．これは，正規 Web ページが Web 改ざんにより，悪性 Web ページへ誘導する現象をとらえるためである．しかし，この方式では検知できない Web 改ざんも存在する．False negative となりうる状況を以下に示す．

- Web ページ内の文字列の改ざん
- 正規 Web サーバ内へマルウェアの設置
- 短縮 URL を利用したリダイレクト

以降では上記項目について詳細を説明する．

Web ページ内の文字列の改ざん

正規 Web ページ内の文字列を書き換え，誹謗中傷等を書き込む Web 改ざんも存在する．我々は URL の変化を判断基準としているため，Web 改ざんとして検知することはない．このような Web 改ざんの場合，直接の被害が生じるのは Web ページの管理者である．また，我々は Web ページを閲覧するユーザが受ける被害を最小限にすることを最終目標としており，このような Web ページの改ざんは対象としていない．

正規 Web サイト内へマルウェアの設置

Web サーバ内に侵入を許してしまった場合．内部にマルウェアを設置される場合が考えられる．この場合，正規 Web ページには内部リンクが張られるため，外部の Web ページとのリンクを判断基準とする提案システムでは Web 改ざんを検知することができない．

短縮 URL を利用したリダイレクト

近年，短縮 URL を利用する機会が増えてきている．短縮 URL とは，主に文字数制限のある SNS 上で普及した URL で，通常の URL を短い文字列に変換したものである．短縮 URL に変換した場合，短縮 URL サービスのドメインへと変更されるため，悪性 Web ページへ誘導するための URL も短縮 URL サービスのドメ

インへと変換されてしまう．そのため，日常的に短縮URLを利用しているWebページでWeb改ざんが発生した場合に改ざんの傾向をとらえることが難しい．そこで，我々は短縮URLを発見した場合に元のURLへと戻す工程を加えることで対処する．

6 おわりに

Drive-by Download攻撃等，Web改ざんを起点とした攻撃手法が猛威を振るっている．これらの攻撃に対し，クライアント側は，Web管理者の自衛やブラックリストの反映待ちなど，受動的な対策しかすることができない．そこで，我々はユーザ自身で改ざんの兆候を検知するための手法を提案してきた．本稿では，Webページ内にあるリンクURLの時間変化に着目したWeb改ざん検知手法の能力を検証した．Alexa Top 100のWebページを起点に収集した14114 URLsを検証した結果,「更新」と判定されるべきWebページを2514 URLs誤検知した．今後，広告による新規ドメインの追加やaタグのリンク先の変更等に対し，誤検知率を軽減するための対策を行う．

参考文献

[1] 望月翔太，高田哲司．リンク情報の時間変化に着目したWeb改ざん検知支援システムの提案，情報処理学会研究報告　コンピュータセキュリティシンポジウム2014（CSS2014），2014．

[2] Google Safe Browsing API, https://developers.google.com/safe-browsing/, December 2014.

[3] N. Provos, P. Mavrommatis, M. A. Rajab and F. Monrose．All Your iFRAMEs Point to Us, Proc. of the 17th USENIX Security Symposium, pp. 115, 2008.

[4] Marco Cova, Christopher Kruegel, and Giovanni Vigna．Detection and analysis of drive-by-download attacks and malicious javascript code.， Proc．of the 19th International Conference on World Wide Web, WWW ’10, pages 281 ー 290, 2010．

[5] J. W. Stokes, R. Andersen, C. Seifert and K.Chellapilla．WebCop: Locating Neighborhoods of Malware on the Web, Proc. 3rd USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET 2010), 2010．

[6] J. Zhang, C. Seifert, J. W. Stokes and W. Lee．ARROW: GenerAting SignatuRes to Detect DRive-By DOWnloads, Proc. 20th International World Wide Web Conference(WWW2011), 2011

[7] Kevin Borgolte，Christopher Kruegel，Giovanni Vigna．Automatic Identification of Unknown Web-based Infection Campaigns，Proc. of the 2013 ACM SIGSAC conference on Computer & communications security，2013．

[8] 松中隆志，山田明，窪田歩．Drive-by Download攻撃対策フレームワーク実現に向けたリンク構造解析によるWebサイトの分析，情報処理学会研究報告　コンピュータセキュリティ（CSEC）2015-CSEC-68 Vol．2015，No．48，2015．

[9] Alexa: Actionable Analytics for the Web，入手先<http://www.alexa.com>(参照2015-07-01)．

[10] Adblock Plus，入手先<https://adblockplus.org/>（参照 2015-08-10）．

[11] VirusTotal，入手先<https://www.virustotal.com/>（参照2015-08-20）．

[12] IPA：【今月の呼びかけ】「 ウェブサイトを閲覧しただけでウイルスに感染させられる”ドライブ・バイ・ダウンロード”攻撃に注意しましょう！」，入手先<http://www.ipa.go.jp/files/000024628.pdf>（参照2015-08-20）．