情報処理学会論文誌 Vol.58 No.12 1833–1842 (Dec. 2017)

悪性コンテンツの隠蔽方法に着目したマルウェア感染への誘導用Webページ検知システムの提案

荻野 貴大[1,†1,a)] 高田 哲司[1]

受付日 2017年3月13日, 採録日 2017年9月5日

概要：Drive-by Download 攻撃など Web を通じたマルウェア感染の脅威が問題になっており，その対策が求められている．Web は pull 型の情報メディアであるため，マルウェアを流布するためには，Web 閲覧者をマルウェア流布のために構築した「仕掛け」に誘導する必要がある．本研究では，このために既存の Web ページを改ざんし，「仕掛け」に誘導するページを「誘導ページ」と定義し，その検出を可能にする研究を行った．誘導ページに関する Web 記事を対象に調査を行い，その結果から悪性コンテンツが隠蔽されるという特徴に着目した．この特徴を基に判定ルールを策定し，Web ブラウザ上で誘導ページを検出可能にするプロトタイプシステムを Firefox の拡張機能として実装した．実装したシステムを用いて誤検出率に関する検証を行った結果，False Positive については 5%を下回る結果を得た．また実際の運用可能性についても検証を行い，実用性についても見込みがあることを示した．

キーワード：Web セキュリティ，Drive-by Download 攻撃，Web ページ改ざん，隠蔽コンテンツ，悪性 Web ページ，マルウェア，検知システム

A Detection Scheme of a Compromised Web Page that Enables to Guide Viewers to a Malware Infection Trap Using Features of Hidden Schemes

Takahiro Ogino[1,†1,a)] Tetsuji Takada[1]

Received: March 13, 2017, Accepted: September 5, 2017

Abstract: Malware infection through a web browsing has been a threat for ICT users and effective countermeasures are required. Since web browsing is a pull type information media, an attacker need to guide target person to a trap that enables to infect malware to the victims. In this paper, we tried to implement a compromised web page detection system. The compromised web page is made by an attacker, and the page is generally injected codes in order to load a malicious content on an external server. At first, we extract the web page detection rule by investigating posted attack information. We, then, implement a web browser extension for Firefox to be able to determine whether or not a browsing page is compromised. Next, we conducted an experiment to derive false positive rate (FP rate) by crawling benign web pages. As a result of the experiment, we got under 5% of the FP rate in proposed scheme. We also conducted an evaluation of its practical operability by crawling a web page that is operated by WordPress, and it showed that the proposed scheme has a potential to detect compromised web page.

Keywords: Web security, Drive-by Download attack, Web page alteration, Hidden content, Malicious web page, Malware, Detection system

1. はじめに

Web を通じたマルウェア感染は，ICT ユーザにとって依然として大きな問題である．マルウェア流布に Web を悪用するうえで必要になるのは，攻撃対象者を攻撃用 Web

[1] 電気通信大学
The University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[†1] 現在，民間企業勤務
Presently with Private Company
[a)] takahiro.ogino@mail.uec.jp

© 2017 Information Processing Society of Japan

ページに「誘導する」ことである．Web は pull 型の情報システムであるため，攻撃者が攻撃対象者に直接マルウェアを送付することは困難である．かわりに，マルウェアを感染させるための「仕掛け（罠）」をインターネット上に事前に用意し，その仕掛けに攻撃対象者が “かかる” よう攻撃対象者を導く必要がある．以降は，Web を悪用した攻撃事例として著名な Drive-by Download 攻撃（以降，DbD 攻撃と略す）[18] を例に説明する．

DbD 攻撃では，まずはじめに攻撃者がマルウェアを感染させるための仕掛けをインターネット上に構築する．その後，もともと無害であった Web ページを改ざんし，ページ閲覧者を仕掛けページに誘導（転送）する．その結果，仕掛けページの閲覧者にマルウェアを感染させることが可能になる．この説明の中で「仕掛け（罠）」と称した仕組みは，Exploit Kit と呼ばれるツールを用いて構築される傾向があることが知られている．これゆえ，先行研究では Exploit Kit に由来する種々の特徴を用いた悪性 Web サイトの検知手法が提案されている．しかし，攻撃者が構築する仕掛けは，インターネット上のどこにでも自由に構築することが可能なため，先行研究による手法で検出され，その仕掛けサイトへのアクセスがブラックリストなどによって遮断されたとしても，新たに別の仕掛けサイトを構築し，そこへ誘導先を変更するだけで，マルウェア流布を継続することが可能となる．

そこで本研究では，攻撃対象者を「仕掛け（罠）」へ誘導するために構築される Web ページに追加されたコンテンツの「隠蔽方法」に着目し，その特徴を用いた検知手法の実現を試みた．また既存研究の欠点を補完するため，Web ブラウザから情報を収集し，クライアント計算機上で動作するシステムとして実装した．この誘導ページ検知手法が実現されれば，先行研究による「仕掛け（罠）」ページの検出と組み合わせ，Web プラットフォームを悪用した攻撃によるマルウェア感染の抑制に寄与する仕組みになりうると著者らは考える．つまり本研究では，既存の悪性 Web ページ検知システムの改良ではなく，それを補完しうる検知システムの提案を目的とする．

以降，本論文では，2 章で誘導ページの構築手法に関する調査について，調査方法と調査結果を述べる．3 章では，著者らが実装した誘導ページ検知システムについて，システムの詳細と誘導ページの判定ルールについて説明する．4 章では，実装したプロトタイプを用いた 2 つの検証実験について述べ，5 章で，提案手法の有用性や継続運用性について議論するとともに，検出精度の向上に向けた今後の課題について述べる．

2. 誘導ページ構築手法に関する調査

Web を悪用した攻撃では，攻撃対象者を仕掛けに誘導する必要があることについて前章で説明した．本研究では，このための Web ページを「誘導ページ」と呼び，以下のように定義する．

- 誘導ページは，攻撃者が既存の Web ページを改ざんすることで作成される．
- Web ページ改ざんにより，ページ閲覧者を攻撃するためのコンテンツが追加される．また追加されたコンテンツの存在を閲覧者に気づかれないよう細工する．

誘導ページ構築のために既存の Web ページを改ざんする理由は，そのページを閲覧するユーザを攻撃対象にするためである．攻撃者が，誘導ページをゼロから新たに構築しても，その Web ページを閲覧するユーザはほとんどいないため，攻撃は行われないことになる．時間経過とともにページ閲覧者は増える可能性はあるが，その数は限定的であり，既存の Web ページの閲覧者数には及ばないであろう．それゆえ，既存の Web ページ，特に閲覧者が多いと推測される Web ページや攻撃対象としたいユーザが閲覧する Web ページを狙って改ざんを試み，誘導ページを構築する．

また攻撃者は，誘導ページ構築のため，既存の Web ページに攻撃用コンテンツを追加する．また追加したコンテンツがあることを Web ページ閲覧者に気づかれにくくする「細工」を施すことが知られている．攻撃行為に気づかれなければ，その誘導ページを通じて長期間マルウェア流布を行うことが可能となり，結果としてより多くの感染成果を攻撃者にもたらすからである．

そこで本研究では，誘導ページの検出ルールを策定するため「既存の Web ページ」を「誘導ページ」に改ざんする際に Web ページに施される攻撃者の手法について調査を行った．本章では，その調査方法と調査結果について述べる．

2.1 調査方法

著者らは，Web サイト “Malware Traffic Analysis.net” [1]（以降，MTAnet と略す）の投稿記事を利用して，誘導サイト構築時の改ざん手法調査を行った．MTAnet とは，種々の攻撃事例に関する情報提供を行っている Web サイトであり，2016 年だけでも 347 件の事例データを公開している．また今回の調査を実施するのに必要となる情報を提供している記事が複数存在することが確認でき，国内外を問わず，他の先行研究 [2], [3], [4], [5], [6], [7] でも悪性データのデータセット提供元として利用されている情報源であることから信用できる情報源であると判断した．

調査対象としたデータは，上記 Web サイト内の “My Blog Posts” に掲載されている投稿記事のうち，2016 年下半期に該当する 2016 年 07 月 01 日から 2016 年 12 月 30 日の間に掲載された記事である．この期間に投稿された記事は全部で 229 件であった．ただし，本研究の調査目的に合致しない以下の内容に関する投稿記事は調査対象から除外

© 2017 Information Processing Society of Japan

表 1 利用されていた HTML 要素とその件数
Table 1 HTML tags in using compromised page and the number of blog posts.

	iframe	object & embed
件数	102 件（67.5%）	18 件（11.9%）

表 2 隠蔽方法とその割合
Table 2 Hiding schemes and its ratio.

	iframe	object & embed
微小化	30 件（19.9%）	18 件（11.9%）
領域外描画	72 件（47.7%）	0
透明化	0	18 件（11.9%）

した．その結果，調査対象となった記事件数は全部で 151 件となった．

- malspam（43 件）
  メールを悪用した攻撃手法のため除外
- data dump（25 件）
  Exploit Kit に関する総括的な内容であるため除外
- ISC diary（9 件）
  情報共有に関する報告内容であるため除外
- Android application（1 件）
  Android アプリに関する内容であるため除外

次に調査方法について述べる．調査方法は以下に説明する 2 段階で行った．

Step 1) 投稿記事の中に誘導ページに関する記述があるかを確認した．記述があった場合には，改ざんによって追加されたコンテンツの HTML 要素を特定し，そのタグ名を抽出した．なお記述がない場合は調査不能なため調査対象外とした．

Step 2) 誘導ページに関する記述があったデータに対し，改ざんによって追加されたコンテンツに対してどんな隠蔽方法が適用されているかについて調査し，分類を行った．

2.2 調査結果

調査結果について述べる．**表 1** は Step 1 の調査結果である．

この調査より `iframe`，`object`，`embed` の 3 種の HTML タグで誘導ページ構築に関する Web ページ改ざん事例の約 80%にあたることが明らかになった．また，それ以外の 31 件の投稿記事については，本調査に必要となる情報が記事から得られなかった．

次に Step 2 による調査結果を**表 2** に示す．表中の数字の単位は記事件数である．この調査により，改ざんにより追加されたコンテンツの隠蔽方法は，以下の 3 つの方法に集約できることが明らかになった．これらの多くは Cascading Style Sheets（以降 CSS と略す）による手法であった．

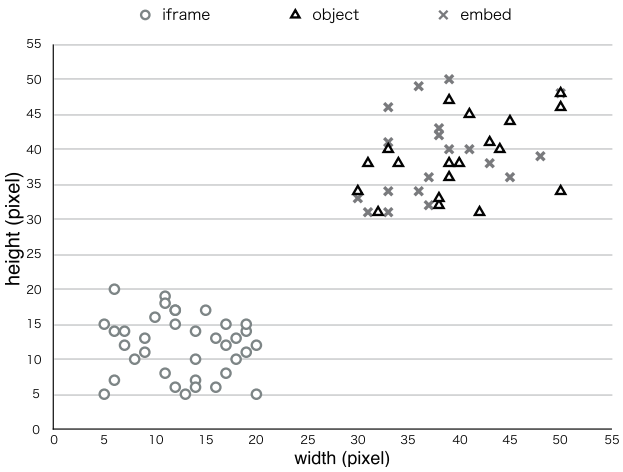

図 1 描画サイズの微小化における設定値の分布
Fig. 1 Distribution of width/height attribute values.

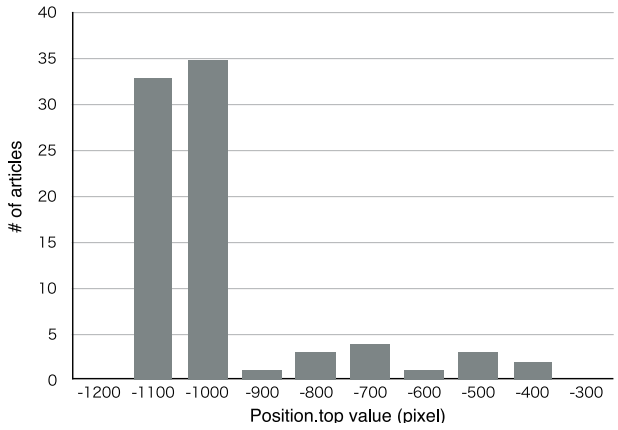

図 2 閲覧可能領域外への表示（Y 座標）の設定値分布
Fig. 2 Distribution of position.top values in rendering invisible area.

(1) 描画サイズの微小化（width，height 属性）
(2) 閲覧可能領域外への描画
（position.left，position.top 属性）
(3) 透明化（opacity 属性）

また上記 3 種の隠蔽方法に用いられた各属性値の調査結果を示す．**図 1** は，描画サイズの微小化による追加コンテンツの隠蔽における描画サイズの値を 2 次元プロット形式で示したものである．横軸が width 属性値を，縦軸が height 属性値の値を示しており，各事例で用いられていた描画サイズ値を $(X, Y) = (\text{width}, \text{height})$ と見立ててプロットした図である．なお今回プロットした微小サイズのデータは，width，height ともに「100 pixel 未満」という条件とした．

図 2 は閲覧可能領域外に描画する方法による追加コンテンツの隠蔽に関する調査結果のうち Y 座標の設定値分布をヒストグラムとして表したものである．調査で得られた Y 座標値を 100 pixel ごとに集計したものであるが，この結果から $-1{,}200 < \mathit{position.top} < -1{,}000$（pixel）の範囲に

© 2017 Information Processing Society of Japan

83 事例中 68 事例が該当していることが明らかになった．一方，X 軸座標で負値の設定をしていたケースは 4 件のみであり，値は (−449, −500, −500, −514) pixel であった．一般化するにはデータが少なすぎるが，400 から 500 pixel 前後の値が使われる傾向が見られた．

一方，opacity 属性を通じた透明化による追加コンテンツの隠蔽については該当するすべての事例が “opacity:0.0” によるものであった．

これらの結果から，3 種の HTML タグのそれぞれに適用される隠蔽方法には表 2 にも見られるように一定の関係性があり，またその際に設定される属性値にも一定の傾向があることが本調査から明らかになった．

本研究では，この調査結果に基づいて判定ルールを策定し，誘導ページを検出可能にする「誘導ページ検知システム」のプロトタイプシステムを実装した．次章では，このプロトタイプシステムと検出ルールについて述べる．

3. 誘導ページ検知システム

前章の調査を基に，誘導ページの検出を可能にする検知システムを実装した．本章では著者らが実装したプロトタイプシステムと，そのシステムで用いる判定ルールについて説明する．実装した検知システムは，「情報収集モジュール」と「検知モジュール」の 2 つの処理から構成される．以降の節では，個々のモジュールについて説明する．

3.1 情報収集モジュール

情報収集モジュールの役割は，誘導ページの検出に必要な情報を収集することである．ここで著者らは，本モジュールを Firefox の拡張機能として実装した．その理由は 2 つある．以下に説明する．

1 つめの理由は，Web ページ内の各要素に適用されている種々の属性情報を収集するためである．拡張機能は，Web ブラウザ内で構築される Document Object Model (DOM) Tree にアクセス可能となるため，Web ページ内の各要素についてタグ名や CSS 情報にアクセス可能になるからである．

もう 1 つの理由は，クライアント側，つまり Web ブラウザ内で動的に生成・変更される Web コンテンツも捕捉可能な点である．調査対象となる Web ページに関連するファイル群を取得し，静的解析を行う方法では，動的生成されるコンテンツの情報収集が困難な場合がある．これに対し，本処理は DOM tree を情報源とする．DOM tree は，Web ページに関する各種ファイルやスクリプトが解釈された結果であり，動的に生成される要素についても情報収集が可能となる．

本モジュールで収集する情報を**表 3** に示す．ただし，これらの情報を収集する要素タグは，`iframe`，`object`，`embed`，`a`，`img`，`html` の 6 種類に限定している．`iframe`，`object`，`embed` タグは，前章の調査から攻撃用コンテンツの埋め込みに利用される HTML タグであるため情報収集の対象としている．`html` タグは，閲覧可能領域を把握するためであり，残りの `a`，`img` タグは，良性コンテンツのリンク先情報として利用する．これら 2 種の要素タグにおけるリンク先は，多くの場合，悪性コンテンツではなく良性コンテンツであると推測される．この仮説のもと，誘導ページの検出を支援しうる情報として利用することを意図し，情報収集を行っている．

表 3 Web ページ内の各パーツに対する収集情報
Table 3 Detail of collected information from targeted HTML elements in a web page.

取得情報名	取得値の具体例
HTML タグの種類	img
URL 属性値	http://A.com
パーツのページ内 X 座標	30
パーツのページ内 Y 座標	60
width	200
height	100
opacity	1
visibility	visible
display	inline
URL のホスト部	A.com

なお情報収集対象の各要素が，その属性値として URL を持つ場合，URL 値を取得する．`img`，`iframe` タグにおける `src` 属性，`a` タグにおける `href` 属性などがこれに該当する．なお本モジュールにより取得した情報は，Firefox の profile ディレクトリ内にデータベースとして保存している．

3.2 検知モジュール

検知モジュールの役割は，情報収集モジュールにより収集された情報を入力とし，判定ルールを用いて現在閲覧中の Web ページが誘導ページか否かを判定することである．著者らは，本モジュールをクライアント計算機上で動作する Java プログラムとして実装した．

なお本研究では，比較考察のため以下の 2 つの判定ルールを策定した．

a) MTAnet ルール
MTAnet ルールとは，2 章で行った MTAnet の調査結果を可能な範囲で忠実に反映した判定ルールである．

b) 包括ルール
包括ルールとは，攻撃コンテンツの隠蔽に用いられる手法を総論的に含んだ判定ルールである．なおこの判定ルールは，MTAnet の判定ルールを完全に包含する内容となっている．

つまり，MTAnet ルールは精緻なルール，包括ルールは総論的なルールという対照的な 2 つの判定ルールを用意した

© 2017 Information Processing Society of Japan

表 4 判定ルール
Table 4 Detail of the two detection rules.

		描画サイズの微小化		閲覧可能領域外		透明化
		width	height	position.X	position.Y	opacity
MTAnet rule	iframe	5 ≦ w ≦ 20	5 ≦ h ≦ 20	ルールなし	-1300 ≦ Y < -400	ルールなし
	object	w ≦ 50	h ≦ 50	ルールなし	ルールなし	opacity = 0.0
	embed	w ≦ 50	h ≦ 50	ルールなし	ルールなし	opacity = 0.0
Comprehensive rule	iframe	w ≦ 50	h ≦ 50	X < 0	Y < 0	opacity < 0.5 OR visibility:hidden OR display:none
	object	w ≦ 50	h ≦ 50	X < 0	Y < 0	opacity < 0.5 OR visibility:hidden OR display:none
	embed	w ≦ 50	h ≦ 50	X < 0	Y < 0	opacity < 0.5 OR visibility:hidden OR display:none

ことになる．この両ルールで検知性能について比較評価を行った結果，同等程度の検出性能になった場合「悪性コンテンツの隠蔽方法を忠実に検出ルールに反映しなくても，同等レベルの検出が可能」という結論を導くことが可能となり，隠蔽方法の特徴を検出ルールに忠実に反映する必要はない，といえることになる．次節以降で，この 2 つのルールの詳細について説明する．

3.3 判定ルール

本研究における誘導ページの判定ルールとは，各属性値の値域の集合として定義されている．ここでいう属性値とは，攻撃者による改ざんによって誘導ページに追加された要素の「隠蔽」に用いられる値である．またこの値域は，要素タグの種別によって異なるものもあれば，要素タグを問わず共通のものもある．本節では，その詳細について隠蔽手法ごとに各判定ルールにおける値域を示す形で説明する．

3.3.1 描画サイズの微小化による隠蔽

2 章の調査結果より，`iframe` タグと `object`，`embed` タグで設定される描画サイズが異なることが明らかになった（図 1 参照）．この結果をふまえ，MTAnet ルールでは要素タグに応じた値域設定とした．また包括ルールでは，どの要素タグでも検知できるよう MTAnet ルールのうち値の大きい値を採用した．さらに包括ルールでは，隠蔽方法として知られている典型例（例：1 pixel × 1 pixel）についても検知できるよう，最小値の条件も変更した．

- **MTAnet ルール**
  `iframe` タグ：
  5 px ≤ width ≤ 20 px AND 5 px ≤ height ≤ 20 px
  `object`，`embed` タグ：
  width ≤ 50 px AND height ≤ 50 px
- **包括ルール**
  `iframe`，`object`，`embed` タグ：
  width ≤ 50 px OR height ≤ 50 px

3.3.2 描画領域外描画による隠蔽

調査結果より，本手法は `iframe` タグでのみ用いられる手法であることが明らかになった．また，`iframe` タグによるコンテンツの隠蔽に使われる値は，コンテンツを描画する位置を指示する Y 座標の属性値に負の値を設定し，その値域は最小値が −1,198 px，最大値が −423 px であった．設定値の分布は図 2 に示されたとおりである．これらの結果から，MTAnet ルールでは iframe タグについては若干の余裕を持たせた値域を設定し，object，embed タグについては判定ルール「なし」とした．

一方，包括ルールはこの値域を一般化し，基本的にパーツの座標値に負の値が設定されていれば，それは「隠蔽の意図あり」と見なすルールとした．また 3 種の要素タグによる場合分けも行わないこととした．

- **MTAnet ルール**
  `iframe` タグ：
  −1300 px ≤ Y < −400 px
  `object`，`embed` タグ：
  ルールなし
- **包括ルール**
  `iframe`，`object`，`embed` タグ：
  X < 0 px OR Y < 0 px

3.3.3 透明化による隠蔽

調査結果より，`object` および `embed` タグについては，CSS の opacity 属性を 0.0 に設定する事例が明らかになった．なお `iframe` タグについてはこの手法による隠蔽事例はなかったため判定ルールは「なし」とした．これらの内容を MTAnet ルールとした．

一方，包括ルールでは透明化の手法として opacity 属性以外にも知られている CSS の visibility と display 属性についても判定ルールに加えるとともに，opacity の値域も半透明に該当する 0.5 未満まで値域に幅を持たせたルールとした．

- **MTAnet ルール**
  `iframe` タグ：
  ルールなし
  `object`，`embed` タグ：
  opacity = 0.0
- **包括ルール**
  `iframe`，`object`，`embed` タグ：
  opacity < 0.5 OR “visibility:hidden” OR “display:none”

表 4 は，これらのルールを表にまとめたものである．見て分かるとおり，MTAnet ルールは HTML 要素タグごと

© 2017 Information Processing Society of Japan

に個別にルールを定義している一方で，包括ルールではHTML 要素タグにかかわらず隠蔽手法ごとに単一のルール定義となっている．

本モジュールにおける誘導ページの検出処理はシンプルである．閲覧中の Web ページから情報収集モジュールによって収集された情報の中に，これまでに説明した判定ルールに該当するデータが 1 つでも存在した場合，当該 Web ページを「誘導ページ」として検出する．

4. 検証実験

本研究では，提案する検知システムの有用性を明らかにする目的で 2 つの検証実験を行った．1 つは提案手法における False Positive rate（FP rate）を明らかにするための実験であり，もう 1 つは実運用の可能性を検証するための実験である．本章では両実験の実験内容と結果について述べる．

4.1 無害な Web ページによる誤検知検証

本研究では「無害と見なせる Web ページ」を対象に，提案手法による検出処理を行うことで FP rate に該当する誤検知率の検証を試みた．検証方法は以下のとおりである．

(1) Web ディレクトリ “DMOZ” [20] の URL リストから無作為に 3,000 URL を抽出．
(2) Python により実装した Web クローラにより Web サイトの存在を確認．
(3) プロトタイプシステムをインストールした Firefox を用意．
(4) Web ブラウザの操作自動化システムである Selenium [21] を用いて (1) で抽出した URL リストを巡回．
(5) 巡回の結果，得られた判定結果を収集情報とともにデータベースに保存．

(2) の検証段階で HTTP レスポンスが 200 以外であったサイトは検証対象から除外した．その結果，(4) の段階で検証対象のデータは 2,012 URLs になった．また (4) の結果，タイムアウトなどのエラーが発生し，意図する情報収集ができなかったサイトも以降のデータ集計対象から除外した．結果として，有効データ数は 1,962 URLs となった．

表 5 は，本実験における検証データの内容について示したものである．表内の各行の条件について説明する．「(a) 各要素タグを含む Web ページ数」とは，調査対象とした Web ページのうち各列に記載の 3 種の要素タグが含まれていた URL の数を示している．「(b) リンク属性値が URL 形式である Web ページ数」は，各列にある要素タグの属性値としてリンク情報が含まれており，かつその値が URL 形式で指定されていた Web ページの数を示している．一部の Web ページにはリンク先の属性値がなかったり，URL 形式以外の記述法で値が設定されていたりするものも存在した．これらの記載による設定値では，外部の Web サイトからコンテンツを取得する可能性が低いと見なし，URL 形式でリンク先情報が指定された Web ページのみを判定対象とした．最後に「(c) リンク先が外部サイトである Web ページ数」とは，URL 形式で指定されたリンク属性値内のホストが，閲覧中の Web ページのホストと異なる場合，つまり外部ホストへのリンクとなっている Web ページの数を示している．これら (a)，(b)，(c) の関係は包含関係として表すことができ，$(a) \supseteq (b) \supseteq (c)$ となる．結果として，調査データ全体の 41.5%（= 815/1,962）に該当する Web ページが提案手法で判定対象となる要素タグを含んでいた．なお表 5 の各行における数値は，排他的な関係にある値ではなく，部分的に重複している部分もある．1 つの Web ページに対象とする複数の要素タグが含まれている場合も存在するためである．したがって「判定対象数」列の各数値が表 5 の残りの 3 列の値の合計値と等しくないことは誤りではないことに注意されたい．「判定対象数」の数値は，今回の評価で判定対象となる「ユニークな Web ページ数」として記載した．なおこれは**表 6**，**表 7** も同様である．

表 5 検証データの詳細
Table 5 Detail of the crawled Web page data.

	iframe	object	embed	判定対象数
(a) 各要素タグを含む Web ページ数	697	141	124	815
(b) リンク属性値が URL 形式である Web ページ数	635	26	123	726
(c) リンク先が外部サイトである Web ページ数	604	23	27	620

検証実験の結果を表 6，表 7 に示す．表 6 は包括ルールによる検証結果を，表 7 は MTAnet ルールによる検証結果を表している．

包括ルールでは，`iframe` タグで 547 ページ，`object` タグで 105 ページ，`embed` タグで 34 ページが「誘導ページ」として誤検知となった．ただし，誘導ページに追加される悪性コンテンツは，外部サイトに存在するコンテンツを読み込むと想定されるため「リンク先が外部サイトである」というルールを加味して検出を行うと，誤検知数は 3 種の HTML タグで合計 484 ページとなった．したがって，包括ルールを用い，「リンク先が URL 形式」かつ「リンク先 URL のドメイン名が外部サイト」である場合の誤検知率は 24.7%（= 484/1,962）となる．

一方，MTAnet ルールにおける誤検出数は，`iframe` タグで 47 ページ，`object` タグで 27 ページ，`embed` タグで 16 ページとなった．また包括ルールと同様の条件で MTAnet ルールにおける誤検知率を計算すると，2.8%（= 54/1,962）となる．

© 2017 Information Processing Society of Japan

4.2 実環境における誘導ページの検出実験

本提案手法の有用性を検証するため，インターネット上で実際に稼働する Web ページを対象に，誘導ページの発見を目的としたクローリングを行った．実施内容は以下のとおりである．

- 実施期間：2017 年 2 月 22 日～2017 年 3 月 09 日
- 対象データ：外部協力者から提供を受けた WordPress が稼働する URL リストに掲載の Web サイト群を対象（URL 数：6,492）
- 判定ルール：MTAnet ルール

この実験の結果，2 つの Web ページを誘導ページとして検出した．発見された 2 つの Web ページの Top Level Domain は，どちらも ".ru" であった．発見した Web ページにおいて改ざんにより追加されたと疑われる部位の HTML コードを**図 3** に示す．

図 3 から分かるとおり，`iframe` タグにより外部サイトのコンテンツを読み込み，かつ当該コンテンツの描画位置が Y 座標で −1,000 px となっている．したがって，Web ページ閲覧者に気づかれないようにコンテンツを追加していることが明らかになっている．また `iframe` タグのリンク先を VirusTotal [22] で検証したところ，リンク先属性値のホストについて以下のような判定結果が得られた．

- Malicous site 2 件
- Malware site 4 件
- Suspicious site 2 件

この結果から，提案手法を用いてインターネット上の Web ページを巡回することで，誘導ページとして改ざんされている可能性の高い Web ページを発見可能なことを確認することができた．

表 6 誤検知検証結果：包括ルール
Table 6 Experimental result for false positive detection.

	iframe	object	embed	判定対象数
(a) 各要素タグを含む Web ページ数	547	105	34	629
(b) リンク属性値が URL 形式である Web ページ数	483	21	33	520
(c) リンク先が外部サイトである Web ページ数	469	19	10	484

表 7 誤検知検証結果：MTAnet ルール
Table 7 Experimental result for false positive detection.

	iframe	object	embed	判定対象数
(a) 各要素タグを含む Web ページ数	47	27	16	79
(b) リンク属性値が URL 形式である Web ページ数	45	7	16	63
(c) リンク先が外部サイトである Web ページ数	44	7	8	54

```
/></a><br />
<a href="http://www.example.com/">example.com</a>
<!--884c7b74e31d727d5814a0ed667c0255--><iframe src="http://example.org
/rotation/3wBsvX" width=300 height=25 style='position: absolute; left:
-1000px; top: -1000px; z-index:-1;'></iframe></p>
<div style="display: none">VN:F [1.7.5_995]</div>
<div class="ratingblock ">
<div class="ratingheader "></div>
```

図 3 誘導ページと判定された Web ページの HTML コード（一部）
Fig. 3 HTML code snippet in the detected web page.

5. 考察

本章では，提案した誘導ページ検知システムについて 4 点の議論を行う．

5.1 有用性について

本研究では，以下の 3 点を明らかにした．

(1) 判定ルールの策定
2016 年下半期の攻撃事例を基に誘導ページの判定ルールを策定した．これにより，MTAnet に投稿されている Web 攻撃事例のうち，およそ 8 割に該当する事例の誘導ページを検出可能とした．いいかえると，この数値は MTAnet で 2016 年下半期に報告された Web 攻撃事例に対する，提案手法の "True Positive rate"（TP rate）を表すといえる．

(2) 誤検知率
4 章における検証実験により，"FP rate" に該当する誤検知率を明らかにした．無害と推測される 1,962 の Web ページを対象に検証実験を行った結果，MTAnet ルールの場合，判定ルールどおりで 4.0%，判定ルールに加えて「リンク先が外部サイトである」という条件を付与した場合，2.8%という誤検知率になった（**表 8** 参照）．

(3) 実環境での検証
インターネット上で WordPress [23] が稼働する Web サイトを巡回し，誘導ページ化されたページの探索を行った．その結果，2 サイトで「誘導ページ化された疑いの強いページ」の発見に至った（4.2 節）．

これらの結果から，誘導ページの検知手法として一定の可能性を示すことができていると著者らは考えている．

一方，False Negative rate は上記 (1) での条件におけ

表 8 条件別誤検知率
Table 8 Wrong detection rates in each condition.

	包括ルール	MTAnet ルール
判定ルールのみの場合	32.1%（629）	4.0%（79）
判定ルール + リンク先が外部サイトの場合	24.7%（484）	2.8%（54）

© 2017 Information Processing Society of Japan

る TP rate の値を利用すれば約 20%となる．しかし，この TP rate の値は MTAnet の投稿記事を基に算出したものであり，一般的な評価によるものとはいいがたい．また False Negative の検証実験を行うためには「誘導ページ」のデータセットが MTAnet とは別に必要となるが，現時点では見つけられていない．これについては，検証実験に適するデータセットの探索から行う必要があり，今後の課題とする．

5.2 検出精度の向上に向けて

表 8 は，策定した両ルールにおける誤検知率について表 6 および表 7 の結果をまとめたものである．この結果から，以下の 2 つの事実を導くことができる．

- MTAnet ルールの方が誤検知率が低い．
- 「リンク先が外部サイト」という条件を判定ルールに追加すると，誤検知率が 20〜30%ほど改善される．

包括ルールは MTAnet ルールを基に一般化したルールであるため，誤検知率が高くなることは当然であるといえる．しかし，包括ルールにおける誤検知率がこれほど大きくなった原因は，一般化したルールの中に無害な Web ページで使われるルールを含んでしまったためである．現時点で明らかになっているのは透明化に関する “`display:none`” と “`visibility:hidden`” のルールであり，各 CSS 属性が設定されたタグは前者が 707 個，後者が 346 個見つかっている．

一方，判定ルールに追加した「外部サイトへのリンク」については，誤検知低減の効果がある一方で，これが誤検知の原因になる事例も見つかっている．以下の事例がそれに該当する．

- SNS コンテンツの埋め込み
- 個人認証連携
- アクセス解析のための要素埋め込み
- 広告コンテンツ

結果を見るかぎり，このようなコンテンツを提供するサイトの数は限定的である．このため判定ルールに「外部サイトへのリンク」を追加しつつ，誤検出を招くコンテンツプロバイダをホワイトリスト化することで誤検知を回避可能にできると考えている．なおこの際，ホワイトリストの不用意な追加にともない False Negative を増加させる懸念に対して「条件付きホワイトリスト」という手法を検討している．これは「この Web ページならば，このホストへのリンク先が存在することは正常である」というもので，リンク先ホストを無条件に信用するかわりに，リンク元とリンク先のペアでホワイトリスト化するものである．

また上記以外にも，以下の 2 種のサイト群をルールに加えることで誤検知率の低減が可能かについても検証を行う予定である．これは今後の課題である．

- `a`，`img` タグのリンク属性値に含まれるサイト
  検査対象の Web ページ内に存在する上記 2 種の HTML 要素のリンク属性値からホスト名を抽出し，各ホストの出現数を算出する．一定数以上の出現数があるサイトについては「無害なコンテンツへのリンク先」と見なせるものと考えている．これを無害コンテンツの提供元サイトとして判定に応用する．
- 閲覧ページと同一ドメインのサイト
  ドメイン名は同一だが，ホスト名だけが異なるサイトのことを意味する．たとえば，閲覧ページが `www.example.com` のとき，`img.example.com`，`db.example.com` などのサイトがこれに該当する．無害な Web ページでも，この種のリンクは多数存在するため，無害コンテンツの提供元として判定に応用する．

5.3 先行研究との比較議論

先行研究と本研究との比較議論を行う．Web 技術を悪用した攻撃で用いられる Exploit Kit に注目し，それに由来する特徴をとらえた攻撃検知が提案されている．例として，URL の特徴をとらえるもの [3], [8] やネットワーク通信の特徴をとらえるもの [2], [14] がある．これに対して著者らの提案する手法は，攻撃者によって作られる「誘導ページ」の特徴に基づいた検知手法であり，Exploit Kit に依存する検出手法ではない．

一方，攻撃を行う悪性 Web サイト検出として，攻撃に特徴的なコンテンツの特徴をとらえる攻撃検知手法もある．Web ページのリンク構造に着目した手法 [10], [11] や難読化 JavaScript に着目した手法 [9] などがこれに該当すると考える．これに対して提案手法は，攻撃に用いられるコンテンツには依存せず，「誘導ページ」の構築方法に着目した攻撃検知手法を提案している．なおコンテンツに依存せず，ネットワーク通信に用いたマルウェアの検知手法も提案されている（文献 [16], [17]）．しかし，これらはマルウェアの「感染検知」であり，攻撃検知ではない．

なお田村らの研究 [13] は，実際の改ざんページを調査し，そこから得られた特徴を用いて攻撃サイトを発見する手法として検索エンジンを用いる手法を提案している．本研究のアプローチと同じ研究であり，script タグについては width または height の属性値が 0 の場合など，隠蔽方法の一部も網羅している．しかし，提案されている検出ルールでは，本論文における 2 章の調査で明らかになった HTML 要素タグと隠蔽方法による悪性コンテンツの検出は困難である．

Wang らの研究 [19] も Landing page と呼ばれる攻撃用ページから改ざんによって追加された情報を特定し，そこから文字列ベースの特徴量を抽出して，類似した Landing page を検出する手法を提案している．しかし評価実験の結果は 60%を超えない検出率であり，単純比較はできないが，一般論として検出精度が高いとはいいがたい．

© 2017 Information Processing Society of Japan

これらの議論に対し，本研究の貢献は大きく 2 つあると考えている．

(1) クライアント計算機上で稼働する検知システムの実装
(2)「隠蔽方法」に着目した検出手法の提案とその評価

項目 (1) により，プロキシなど外部依存性なしに提案システムの利用が可能になる．また Web ブラウザ内で情報収集を行うため，ユーザが閲覧したすべてのページを検査可能となる．さらに検索エンジンや Web クローラによる対策では対応が困難なクローキングや標的型攻撃，Web メールの対応も可能である．また入力情報が DOM tree になるため，CSS 情報や難読化 JavaScript，動的生成の Web コンテンツも一部制限はあるものの検査可能となる．これは静的なファイルを入力とする検知手法にはない大きな利点となりうる．

項目 (2) は，攻撃方法や Web ページ改ざん方法に依存しない検出方法を提案し，その評価を行った点である．攻撃手法や Web ページの改ざん手法は多種多様であり，また今後も様々な方法が出現すると予想される．ただし，それらの行為は対象とする Web ページに悪性コンテンツを追加することであり，その発覚を防ぐために隠蔽することも知られている．この隠蔽方法に着目し，検出手法とする手法を提案し，その有用性について評価を通じて可能性を示した．

また我々の知る範囲において，Web 閲覧者を攻撃する際に作成される「誘導ページ」の特徴（要素タグと隠蔽に用いられる属性値の値域の組）を用いた攻撃検知の手法は他に見当たらず，提案手法には新規性があるものと考える．したがって，提案手法は先行研究で提案されている検知手法の改善ではなく，それらを補完する手法の提案であり，先行研究による検出手法と組み合わせることで，Web を悪用した攻撃の検知可能性を拡張するものである．

さらに本提案手法は Web ブラウザ内で動作するため，JavaScript による攻撃にも一部対応可能であり，特定の Exploit Kit にも依存しない検知手法である点もユニークな点であると考えている．一方，評価実験の規模やデータセット，継続運用性，および捕捉可能な攻撃手法の限界などの問題が残っている．これらについては次節で議論する．

5.4 今後の課題

今後の課題として 3 点議論する．1 つめは評価実験の追加実施についてである．残念ながら，本論文では無害と見なす Web ページを用いて FP rate に関する検証しか行えていない．またその検証規模も十分とはいえない．これについては，今後，あらためて検証を行う必要があると考えている．また 5.2 節で述べたホワイトリストや無害と思われるホスト群の適用による誤検出率の低減可能性についても同様である．

一方，False Negative に関する検証であるが，この実施については，1) 誘導ページのデータセットが得られない，2) 実装上，誘導ページが実際に稼働していないと検証できない，という 2 つの問題があるため検証に至っていない．これらについても今後の課題とし，データセットの探索から始める必要がある．

なお評価実験については，判定ルール策定における情報源の普遍性についても議論が残る．MTAnet に投稿された記事が実際に行われている攻撃事例をどれだけ網羅できているかは不明である．ただし，今回の調査では 151 件の記事しか調査しておらず，一般的に見て十分とはいいがたい．しかし，追加調査は攻撃情報が共有されないと行えないというジレンマをかかえており，著者らの能力だけでは対応に限界のある問題であるとも考えている．

2 つめの問題は，捕捉可能な攻撃手法の限界である．提案手法は DOM tree から情報を収集するため，JavaScript による動的な攻撃であっても，実行結果として DOM tree へ node が追加される形になるならば検出は可能である．ただし，情報収集のタイミングが onload イベント発生時となっているため，攻撃用スクリプトが遅延実行される場合，および onload イベント前にページ転送が行われる場合などは情報収集ができず，結果として検出不能になる．これらについても情報収集または別の方法による攻撃検知が可能かについて検討を進める必要がある．

最後の問題は，継続運用性についてである．提案手法はルールベースの検出手法であるため，攻撃者に判定ルールを知られると検出を回避されることになる．したがって新たに出現するであろう攻撃手法に追従するためには，攻撃情報の収集とルール策定・更新を継続する必要がある．また本論文では，判定ルールの策定を手動で実施したが，上記の理由からその自動化も進めていく必要がある．これらの問題を改善する手段として，攻撃手法の調査支援ツールや機械学習によるルール策定などが必要になると考えている．調査支援ツールについては，いくつかの先行研究が提案されているが [4], [15]，既存研究を参考にしつつ，上記課題に対応しうるシステムの開発を検討していく．

6. おわりに

Web を悪用したマルウェア流布が大きな脅威となっており，その対策が必要となっている．この状況において本研究ではマルウェア流布のために既存の Web ページを改ざんして構築される「誘導ページ」に着目し，それを検出可能にする検出システムを提案した．まずはじめに，判定ルール抽出のため Malware Traffic Analysis.net にて共有されている攻撃情報を調査し，その結果をもとに誘導ページの判定ルールを策定した．次に，Web ブラウザで閲覧中の Web ページを対象に誘導ページの検出を可能にするプロトタイプシステムを実装した．また無害といえる Web ページおよそ 2000URL を対象に誤検知率に関する検証を

© 2017 Information Processing Society of Japan

行い，その結果 False Positive の誤検知率は 5%以下という結果を得た．

Drive-by Download 攻撃をはじめとする Web 由来の攻撃検知手法は多数提案されているが，誘導ページに着目し，かつページ改ざん時に追加されるコンテンツの隠蔽手法を特徴として当該ページを検出する方法は今までにないユニークな方法であると考えている．しかし，判定ルールの策定に用いた情報源の普遍性や誤検知率の検証規模は十分とはいえず，今後の課題として追加の調査・検証を行う必要があると考えている．

参考文献

[1] MALWARE-TRAFFIC-ANALYASIS.NET (online), available from ⟨http://www.malware-traffic-analysis.net/⟩ (accessed 2017-02-19).

[2] 小林 峻，寺田成吾，瀬戸口武研，道根慶治，山下康一：Drive-by Download 攻撃検知手法の継続的評価と Exploit Kit に対する考察，コンピュータセキュリティシンポジウム 2016，pp.964–970 (2016).

[3] 佐藤祐磨，中村嘉隆，高橋 修：エクスプロイトキットで利用される文字列特徴を用いた悪性 URL 検出手法の提案，研究報告 コンピュータセキュリティ（CSEC），Vol.2016-CSEC-72, No.25 (2016).

[4] 青山佑平，吉井 章，大倉佳歩，尾崎幸也，坂東 翼，小林孝史：Drive-by Download 攻撃の解析支援アプリケーションの開発と評価，コンピュータセキュリティシンポジウム 2016，pp.819–825 (2016).

[5] 西尾祐哉，廣友雅徳，福田洋治，毛利公美，白石善明：悪性 Web サイトを分析するためのマルチ環境解析における通信ログ解析の効率化，コンピュータセキュリティシンポジウム 2016，pp.496–502 (2016).

[6] Ghafir, I. and Prenosil, V.: DNS traffic analysis for malicious domains detection, *Proc. Signal Processing and Integrated Networks* (*SPIN*) (2015).

[7] Taylor, T., Hu, X., Wang, T., Jang, J., Stoecklin, M.P., Monrose, F. and Sailer, R.: Detecting Malicious Exploit Kits using Tree-based Similarity Searches, *Proc. 6th ACM Conference on Data and Application Security and Privacy* (*CODASPY '16*), pp.255–266 (2016).

[8] 笠間貴弘，神薗雅紀，井上大介：Exploit Kit の特徴を用いた悪性 Web サイト検知手法の提案，コンピュータセキュリティシンポジウム 2013，pp.603–610 (2013).

[9] 西田雅太，星澤裕二，笠間貴弘，衛藤将史，井上大介，中尾康二：文字出現頻度をパラメータとした機械学習による悪質な難読化 JavaScript の検出，研究報告 コンピュータセキュリティ（CSEC），Vol.2014-CSEC-64, No.21 (2014).

[10] 伊藤大貴，永井達也，高野泰洋，神薗雅紀，毛利公美，白石善明，星澤裕二，森井昌克：リンク構造を用いた悪性 Web サイトの検知法，コンピュータセキュリティシンポジウム 2016，pp.1229–1233 (2016).

[11] 望月翔太，高田哲司：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，コンピュータセキュリティシンポジウム 2015，pp.504–511 (2015).

[12] 重本倫宏，磯部義明，仲小路博史：多種環境を用いた不正サイトの解析，コンピュータセキュリティシンポジウム 2016，pp.1223–1228 (2016).

[13] 田村佑輔，甲斐俊文，佐々木良一：ユーザ標的型 Web サイト改ざんに対する検索エンジンを用いた検知手法の提案，情報処理学会論文誌，Vol.51, No.1, pp.191–198 (2010).

[14] 酒井裕亮，佐々木良一：Drive By Download 攻撃に対する HTTP ヘッダ情報に基づく検知手法の提案，研究報告 コンピュータセキュリティ（CSEC），Vol.2013-CSEC-60, No.29 (2013).

[15] 尼子雄大，高田哲司：情報視覚化による Drive-by Download 攻撃対策の一検討，研究報告 コンピュータセキュリティ（CSEC），Vol.2014-CSEC-64, No.41 (2014).

[16] 畑田充弘，森 達哉：実行時の通信挙動を用いたマルウェアの分類と未知検体検出への応用，コンピュータセキュリティシンポジウム 2016，pp.647–654 (2016).

[17] Otsuki, Y., Ichino, M., Kimura, S., Hatada, M. and Yoshiura, H.: Evaluating payload features for malware infection detection, *Journal of Information Processing*, Vol.55, No.2 (2014).

[18] Provos, N., Mavrommatis, P., Rajab, M.A. and Monrose, F.: All Your iFRAMEs Point to Us, *Proc. 17th USENIX Security Symposium* (2008).

[19] Wang, G., Stokes, J.W., Herley, C. and Felstead, D.: Detecting malicious landing pages in Malware Distribution Networks, *Proc. 43rd Annual IEEE/IFIP Int'l Conf. on Dependable Systems and Networks* (*DSN 2013*) (2013).

[20] AOL Inc.: DMOZ - The Web Directory, available from ⟨https://www.dmoz.org/⟩ (accessed 2017-02-25).

[21] SeleniumHQ: Browser Automation, available from ⟨http://docs.seleniumhq.org/⟩ (accessed 2017-02-25).

[22] virustotal, available from ⟨https://www.virustotal.com/ja/⟩ (accessed 2017-02-25).

[23] WordPress.org 日本語，入手先 ⟨https://ja.wordpress.org/⟩（参照 2017-02-25）．

荻野 貴大 （学生会員）

2015 年電気通信大学情報理工学部卒業．2017 年電気通信大学大学院情報理工学研究科総合情報学専攻博士前期課程修了．在学中は Web セキュリティにかかる研究に従事．情報視覚化，個人認証，モバイルシステムにも関心がある．現在，民間企業勤務．

高田 哲司 （正会員）

2000 年電気通信大学大学院情報システム学研究科情報システム運用学専攻博士後期課程修了．博士（工学）．2003 年ソニーコンピュータサイエンス研究所研究員．2005 年独立行政法人産業技術総合研究所情報技術研究部門研究員．2010 年電気通信大学大学院情報理工学研究科准教授，現在に至る．個人認証，ユーザブルセキュリティ，情報視覚化に興味を持つ．IEEE/CS 会員．

© 2017 Information Processing Society of Japan