情報処理学会論文誌　Vol. 51　No. 1　191–198 (Jan. 2010)

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

田村佑輔[†1]　甲斐俊文[†2]　佐々木良一[†1]

近年，SQL インジェクションを用いて Web サイトに不正スクリプトを埋め込む改ざん攻撃が急増している．この攻撃は，サイトを閲覧したユーザにマルウェアを感染させることを目的としており，感染源が正規サイトであることから一般ユーザ側での対策が困難となっている．本研究では，実際の改ざんサイトや不正スクリプトの調査を通して，サイトタイトルやスクリプトの記述パターンを分析することで，未知不正スクリプトを自動的に検出可能な方法を発見した．この方法を用いて，改ざんサイトおよび不正スクリプトを検知するためのシステムを提案する．

Proposal of Detection Method Using Search Engine against Manipulation Attack Targeted at Common Users

Yusuke Tamura,[†1] Toshifumi Kai[†2] and Ryoichi Sasaki[†1]

Recently, the manipulation attack to website embedding malicious script using SQL injection vulnerability is increasing. Purpose of this attack is to infect users PC which browse the site with the malware. It is difficult for users to protect this attack because source of infection is website that gets high evaluation. We discovered automatic process of detect unknown malicious script, based on characteristics from an investigation. In this paper, we propose a method to detect in manipulation website and malicious script using the process.

†1 東京電機大学
Tokyo Denki University
†2 パナソニック電工株式会社
Panasonic Electric Works Co., Ltd.

1. はじめに

2000 年に発生した中央省庁の Web サイト改ざんに代表されるように，Web サイトへの改ざん攻撃は以前から行われていた．これらの改ざん攻撃は，サイトデザインを改ざんすることで，攻撃者自身の主張・メッセージを訴えることが目的であったといえる．しかし近年，Web サイトを閲覧した一般ユーザの PC にマルウェアを感染させることを目的として，サイトに不正なスクリプトを挿入する新たな Web サイト改ざん攻撃が増加している．2008 年 3 月には，日本をターゲットとした大規模な攻撃が行われ，多数の正規サイトが改ざんの被害に遭った．現在でも攻撃は継続しており，個人 HP や地方自治体などの多くのサイトが被害を受けている[1)]．

この改ざん攻撃に対し，サイト管理側での対策はもちろんのこと，標的となっている一般ユーザ側でも対策が求められている．しかし，「怪しいリンクをクリックしない」，「怪しいファイルをダウンロードしない」などの一般的なセキュリティノウハウだけでは，この攻撃を防ぐことはできない．

本研究では，実際の改ざんサイトおよび挿入された不正スクリプトを調査・分析し，そこから得られた特徴を用いて改ざんサイト・不正スクリプトを判別するための検知手法を提案する．なお本稿では，2 章でユーザ標的型改ざん攻撃について，3 章で既存の対策手法について，4 章で実施した調査について述べる．調査から得られた特徴を用いて，5 章で検知手法を提案し，6 章で考察を行い，最後に 7 章でまとめる．

2. ユーザ標的型 Web 改ざんについて

2.1 改ざん方法

ユーザ標的型 Web 改ざん攻撃における Web サイトの改ざんは，SQL インジェクションと呼ばれる手法を用いて行われている．

SQL インジェクションとは，正規サイト上でデータベースと連携して運用されている Web アプリケーションの脆弱性を突き，データベースを不正に操作することで，データベース内の情報の不正取得や改ざんなどを行う行為である．ユーザ標的型改ざん攻撃では，この手法を用いて JavaScript や iframe などのスクリプトを不正に Web サイト内に挿入している．また，攻撃プログラムやツールによって，一連の改ざん行為が自動化されているため，無差別かつ広範囲な攻撃となっている．

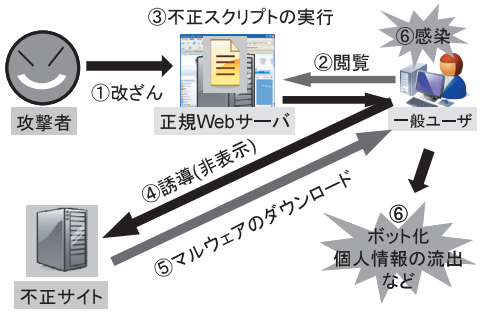

図 1　ユーザ標的型 Web 改ざんの流れ
Fig. 1　Process of manipulation attack targeted at common users.

```
<script src=http://誘導先 URL><script>
<iframe src=http://誘導先 URL><iframe>
```

図 2　挿入される不正スクリプトの例
Fig. 2　Example of malicious script.

2.2　攻撃の流れ

Web サイトの改ざんから一般ユーザにマルウェアが感染するまでの流れを**図 1** に示す．

まず，2.1 節で述べた手法で正規サイトが改ざんされる（図 1-①）．このとき挿入されるのは，**図 2** のようなスクリプトである．

一般ユーザが改ざんされた正規サイトを閲覧した場合（図 1-②），不正スクリプトが実行され（図 1-③），スクリプト中に記述された不正サイトの URL 先に誘導・接続される（図 1-④）．不正スクリプトには誘導先のサイトが表示されないよう細工がされているため，一般ユーザは不正サイトに接続されていることを認識できない．そして，不正サイトからマルウェアがダウンロードされ（図 1-⑤），一般ユーザの PC に脆弱性があれば感染してしまう（図 1-⑥）．このとき InternetExplorer，FlashPlayer など多種多様なアプリケーションの脆弱性が利用されるので，一部のアプリケーションのアップデートだけではこの攻撃に対処しきれない．

2.3　ユーザ側における対策の必要性

Web 改ざん攻撃が発生する根本的原因は，Web サイト側の脆弱性にあるといえ，Web サーバ管理者側で Web サイトの脆弱性をなくすことが有効な対策方法といえる．また，改ざんされた場合に備え，Web サーバの監視[2] を行うという対策も有効であるといえる．しかし，すべての Web サーバ管理者がこうした対策を行っているとは限らないため，ユーザ側でも対策をとる必要がある．Web における簡便なマルウェア対策として「怪しいページにアクセスしない」，「怪しいファイルをダウンロードしない」という人の手による対策方法があげられる．しかし，ユーザ標的型 Web 改ざん攻撃に対しては，下記のような理由からまったく効果がなくなってしまう．

- 改ざんされた正規ページを閲覧しただけで感染の恐れがある．
- 改ざんを直感的に認識できない．
- 不正サイトへの誘導が不可視である．

このようなことから，ユーザ側においては「機械的に改ざんサイトおよび不正サイトへのアクセスを防止する」という対策が必要となってくる．

3.　ユーザ側における既存対策手法

3.1　既存手法の概要

「機械的な改ざんサイトおよび不正サイトへのアクセス防止」という対策の具体的方法として，危険なサイトに対して事前に警告を出す Google のセーフブラウジング機能の活用や，不正サイトや不正スクリプトのブラックリストによるアクセス制限があげられる．セーフブラウジング機能は，Google の検索結果から危険と診断されたサイトにアクセスしようとした場合，警告を出すというものである．危険性の診断は，Google のクローラがサイトを巡回した際に行われていると考えられる[3]．

3.2　問　題　点

セーフブラウジング機能の警告は，Google のクローラが巡回した際にサイトの危険性を識別して出される．このことから，改ざんが行われてからクローラが巡回するまでの間は警告を出すことができないという問題点がある．ブラックリストによるアクセス制限は，この問題に対処することができるが，リストに掲載されていない未知の不正スクリプトに対しては対処できないという新たな問題がもちあがる．

そこで我々は，この「未知の不正スクリプト」に対処するための方法として，不正スクリプト共通の特徴を用いて判定を行うことを考えた．次章では，その特徴を抽出するために行った調査・分析について述べる．

表 1　実験環境
Table 1　Environment of experiment.

OS	Windows XP Professional
CPU	Intel® Pentium® M processor 1100MHz
メモリ	760MB
プログラム開発環境	Visual C# 2005 Express Edition
	Google AJAX Search API
検索エンジン	Google

4. 調　　査

4.1 調 査 概 要

本研究では，改ざんサイトを調査対象とした 1 次調査（2008 年 8 月〜9 月実施）と，不正スクリプトを調査対象とした 2 次調査（2008 年 11 月〜12 月実施）の 2 つを実施した．1 次，2 次ともに，検索エンジンを用いて行い，特定の検索キーワードによる検索結果から改ざんサイトや不正スクリプトを収集し，分析を行った．

調査作業は，**表 1** に示す環境下で自作のプログラムを用いて行った．実装時のステップ数は，1 次調査のプログラムが約 900 ステップ，2 次調査のプログラムが約 800 ステップである．検索エンジンとして Google を採用した理由は，他の Web 検索エンジンに比べて改ざんサイトの検索ヒット数が多かったためである．なお，“Google AJAX Search API” とは，Google の検索エンジンをプログラム上で使用するための API のことである．

4.2 1 次調査（改ざんサイト調査）

4.2.1 調査目的および方法

1 次調査の目的は，改ざんサイトおよび不正スクリプトにおいての共通の特徴を発見することである．

改ざんサイトの検索で用いる検索キーワードは，スクリプトの基本書式 “<script src=” に，Shadowserver Foundation で公開されている不正誘導先ドメインのブラックリスト[4] をつなぎ合わせたもので，“<script src=http://不正誘導先ドメイン” のような形になる．たとえば，ブラックリストに掲載された不正誘導先ドメインの 1 つが “abc.com” である場合，検索キーワードは “<script src=http://abc.com” となる．このような検索キーワードを用いてサイト検索を行い，検索結果から改ざんページを収集し，特徴の分析を行った（**図 3**）．

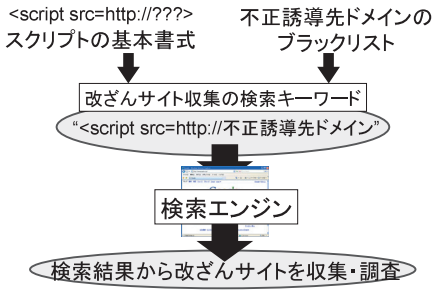

図 3　改ざんサイト情報収集方法
Fig. 3　Collection method of manipulated website information.

4.2.2 調 査 結 果

1 次調査では 20,439 件の改ざんページを収集することができた．また，サイト内容を確認したところ，個人 HP のほか，企業，公益法人，大学，さらには海外の政府関連組織までもが改ざん被害を受けていた．

4.2.3 1 次調査から得られた知見

調査結果を分析したところ，改ざんサイトおよび不正スクリプトについて以下の 2 つの特徴が得られた．

（特徴 A）タイトルの改ざん

「タイトルの改ざん」とは，<title> タグ内に不正スクリプトが挿入されるという特徴である．この特徴は，調査結果のうち 52%のページで確認できた．これは，自動的な攻撃を行ううえで，Web サイトに共通して存在する <title> タグが改ざんの標的になっているためではないかと考えられる．

（特徴 B）スクリプトの多重挿入

「スクリプトの多重挿入」とは，不正スクリプトが別の不正スクリプトによって上書きされている特徴のことである．多重挿入の例として 2 重にスクリプトが記載された “<<script〜”，“<scr<script〜” などがあげられ，スクリプトの途中から別のスクリプトが割り込むような形で上書きされている．このような特徴がある理由は，攻撃プログラムの無差別攻撃により，1 度改ざんされたサイトが再度攻撃を受け，同じような位置に不正スクリプトが挿入されるためであると考えられる．

今回の調査では，全体の 59%のサイトが特徴 A，B どちらかを有していたことが分かっ

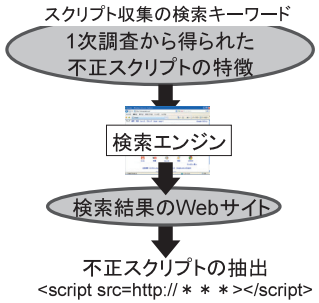

図 4　不正スクリプト収集方法
Fig. 4　Collection method of malicious script.

例 1：intitle:"<script src=http://*"

例 2："<s<script src=http://*"

図 5　検索キーワードの例
Fig. 5　Example of keywords for searching.

た．このことから，これらの特徴は，改ざん攻撃が攻撃プログラムによって自動的かつ無差別的に行われることにより，高い確率で生じる特徴であると考えられる．

4.3　2 次調査（不正スクリプト収集）

4.3.1　調査目的と方法

2 次調査の目的は，4.2.3 項で得られた特徴 A，B を用いて，3 章で述べたような「未知の不正スクリプト」が発見できるかを確かめることである．

2 次調査では，特徴 A，B を活用した検索キーワードによるサイト検索を行い，検索結果のサイトソースを分析することでスクリプトの抽出を行う（**図 4**）．

4.3.2　検索キーワード

「タイトルの改ざん」という特徴 A を有したサイトを検索するため，本調査では，ページタイトルのみを検索対象とする検索オプション “intitle:” を使用した（**図 5**-例 1）．また，「多重挿入」の特徴 B を有したサイトを検索するために，スクリプト重複の組合せすべてを検索キーワードとした（図 5-例 2）．なお，改ざんサイトの中にはスクリプトが多重になっていないものもあることから，特徴 B の検索キーワードは一部の改ざんサイトのみを対象としているといえる．ただ，多重挿入がない改ざんサイトも，特徴 A の検索キーワードを用いることで検索が可能であると考えられる．

表 2　2 次調査の結果
Table 2　Result of 2nd investigation.

既存ブラックリストとの比較	スクリプト(件)
掲載済	147
未掲載	96
合計	243

2 次調査では，1 次調査のように特定の URL を指定した検索は行わず，“http://〜” 以下の頭文字に ‘a’〜‘z’，‘0’〜‘9’ を設定して，“http://a*”，“http://b*”…“http://9*” などとする総当たり的な検索を行った．

4.3.3　調 査 結 果

2 次調査では 243 件のスクリプトを収集した（**表 2**）．

4.3.4　分　　析

調査実施時点の Shadowserver のブラックリスト[4] の掲載数は 432 件であり，2 次調査ではそのうち約 34%を発見した．なお，ブラックリストに掲載されていながら，調査で発見できなかったスクリプトの中には，すでに使用されていないものもあると考えられる．一方，ブラックリストに掲載されていないスクリプトについては，96 件発見した（表 2）．これらの未知スクリプトの信憑性を確かめるため，一部の未知スクリプトに対しスクリプト中に記載された URL 先への接続実験を行った．そして，接続先サイトからダウンロードされるファイルを，マルウェア解析サイト VirusTotal[5] に送りマルウェアの有無を判定した．その結果，任意に選択した 20 件の未知スクリプトのうち 5 件でマルウェアが確認された．確認されたマルウェアは 6 種類で，その内訳はトロイの木馬型が 4 つ，ダウンローダ型が 2 つであった．なお，マルウェアが確認された未知スクリプトの件数と，確認されたマルウェアの数が異なるのは，1 度に複数のマルウェアがダウンロードされたケースがあるためである．この結果から，4.2.3 項で示した特徴 A，B を用いることで，未知不正スクリプトは発見可能であると分かった．また，検索エンジンを利用したスクリプトの収集法によって，効率的に未知の不正スクリプトを見つけることが期待できると分かった．

1 次調査同様に，特徴についての分析を行ったところ，以下の 3 つの特徴を得ることができた．

（特徴 C）スクリプト名の偏り

スクリプト名とは，誘導先サイトに置かれた不正な Java スクリプト本体のファイル名のことである．「スクリプト名の偏り」とは，このスクリプト名に**図 6** に示すような偏りがあるという特徴である．なお，“単語 1 文字” とは “a.js”，“1.js” などのことを指す．このような特徴が得られた理由は，誘導先サイトも改ざん同様にツールで自動作成されており，スクリプト名の付け方に一定の決まりがあるためではないかと考えられる．

（特徴 D）トップレベルドメインの偏り

「トップレベルドメインの偏り」とは，不正誘導先 URL のトップレベルドメインが “.com”，“.cn”，“.ru” で 8 割以上を占めているという特徴である（**図 7**）．この特徴は，攻撃が組織的に行われているために見られるものではないかと考えられる．

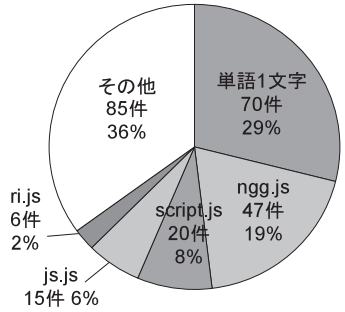

図 6　スクリプト名別の統計
Fig. 6　Statistics of script names.

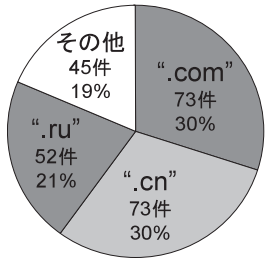

図 7　トップレベルドメインの統計
Fig. 7　Statistics of top level domain.

（特徴 E）スクリプト内の属性の設定・未設定

「スクリプト内の属性の設定・未設定」とは，特定の属性が設定もしくは未設定であるという特徴である．“type” や “language” といった属性は調査したすべての不正スクリプトで未設定だった．一方，“width”，“height” などは，スクリプトを非表示にするため，いずれかが ‘0’ に設定されていた．今回の攻撃では，誘導のための “src” 属性や非表示のための “width”，“height” 属性以外は必要ないため，省略しているのではないかと考えられる．

5. 提 案 手 法

提案手法は，4 章で得られた特徴を利用して，組織内ネットワークのプロキシにおいて改ざんサイトの判定・検知を行い，通信の遮断もしくは警告を行うシステムである．**図 8** にそのシステム図を示す．

改ざんサイト判定部（図 8-α）では，4.2.3 項の特徴 A，B および 4.3.4 項の特徴 C，E を用いて考案した「特徴分析による判定」と，既存の「ブラックリストによる判定」によって改ざんサイトの判定を行うこととした．**図 9** にその判定アルゴリズムを示す．

ブラックリストによる判定は図 9-(a) で行われ，特徴分析による判定は図 9-(b)〜(e) で行われる．特徴分析による判定の判定順位決定にあたり，正常なサイトにおいて改ざん特徴が出現する可能性を評価指標とした．そのため，特徴 B（図 9-b）は，正常なサイトに存在する可能性がきわめて低く，なおかつ 4.2.3 項で示したように，改ざん攻撃独特の特徴であることから最上位に配置し，この特徴単独で改ざんサイトと判定するようにした．また，特

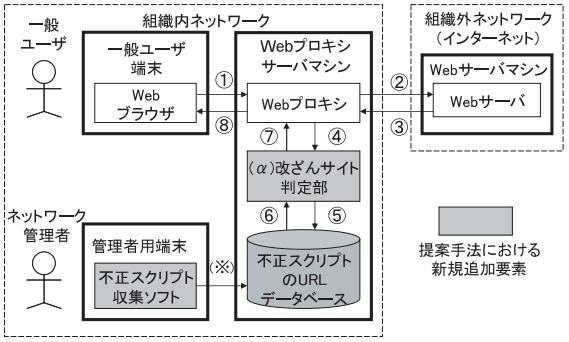

図 8　提案手法のシステム図
Fig. 8　System configuration for proposed method.

徴 A（図 9-c）は，4.2.3 項で示したように約半数の改ざんサイトで見られる特徴ではあるが，正常なサイトに存在しないとはいいきれないため，第 2 位に配置し，単独の判定では改ざんの疑いがあるという判定にとどめた．特徴 C，E（図 9-e，d）については，特徴単独では正常なサイトにも存在する可能性があるが，第 2 位の特徴 A と組み合わせることで改ざんサイトを判定できると考えられることから第 3 位，第 4 位に配置した．

次に提案手法全体の処理の流れを以下に示す．

- データベースのメンテナンス時
  1：定期的に管理者が不正スクリプト収集ソフトを動作させ，新しい不正スクリプトの URL を追加する（図 8-※部）．ここで用いる収集ソフトのアルゴリズムは，4.3 節の調査方法をベースとした検索エンジンによる収集アルゴリズムである．
- 一般ユーザによる Web アクセス時
  1：Web ブラウザからの Get 命令（または POST 命令）で，プロキシは対象 URL のソースファイルを取得する（図 8-①～③）．

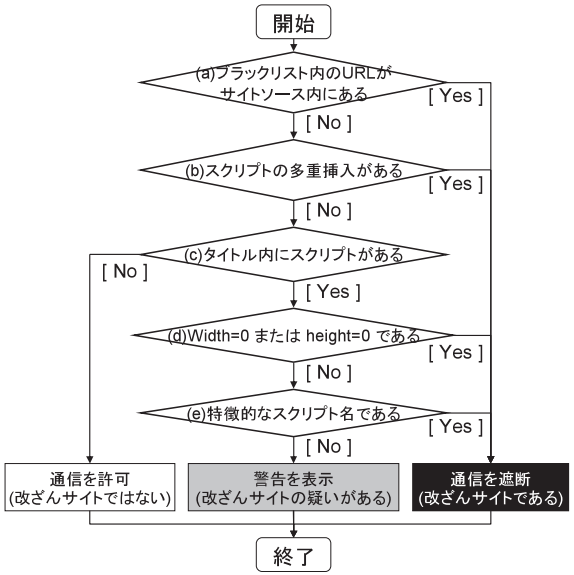

図 9　改ざんサイト判定アルゴリズム
Fig. 9　Algorithm of detection method.

2：取得したソースファイルについて，図 9 の判定アルゴリズムを用いて改ざんの有無をチェックする（図 8-④～⑦）．また，データベースに登録されていない不正スクリプトの URL を発見した場合は，データベースに追加する．
3：問題がなければブラウザで表示する（図 8-⑧）．改ざんが検知された場合は，通信を遮断，もしくは警告を表示する．

6. 考　　察

提案手法と既存手法を比較した場合の「ブラックリスト収集方法」と「検知手法」について，および「提案手法の判定アルゴリズムの誤判定」についての考察を下記で述べる．

6.1　ブラックリスト収集方法の比較

提案手法で用いている自動収集方式と従来手法の収集方式の比較を**表 3** に示す．

提案手法で用いている自動収集方式は，検索エンジンを用いて自動的かつ積極的に収集活動を行う方式である．そのため，報告をベースとした受身の従来手法に比べ，収集スピードが速く，収集可能範囲も広いといえる．実際，提案手法の収集方式によって，外部で公開された危険な誘導先ドメイン[6] を公開の 1 週間以上前に発見することができた．

6.2　検知手法の比較

ブラックリストによる判定の問題点であった未知の不正スクリプトに対しては，4.3.3 項の表 2 で示したように検知・収集が可能であることが分かった．

先の 3 章で述べた Google のセーフブラウジングについては，簡単な実験によって比較を行った．実験は，タイトル改ざんのキーワード（図 5-例 1）による検索結果から無作為に抽出した 40 件のサイトに対し，提案手法（図 9）とセーフブラウジングの判定を行い，改ざん検知の有無を調べるというものである．この実験から，**表 4** に示すような結果が得られた．

40 件中 20 件のサイトはすでに修復が行われており，いずれの判定でも改ざんを検知する

表 3　ブラックリスト収集方法の比較
Table 3　Comparison of collection methods against malicious script.

ブラックリストデータ収集方法	収集スピード	収集範囲	Web管理者の知識
提案手法の収集方式（能動的）	○	広い	不要
従来手法の収集方式（受動的）	×	狭い	要

表 4　セーフブラウジングとの比較実験結果
Table 4　Comparison result of proposed method and Safe Browsing method.

	改ざん未修復		改ざん修復済		合計（件）
	検知	非検知	検知	非検知	
特徴分析による判定（提案手法）	20	0	0	20	40
セーフブラウジング	15	5	0	20	40

ことはなかった．しかし，改ざんが修復されていないサイトについては，セーフブラウジングによる検知が 15 件だったのに対し，提案手法の特徴分析による判定では，5 件多い 20 件のサイトすべてを検知した．このうち，提案手法でのみ検知した 5 件のサイトについて，実際にサイトにアクセスして通信内容を分析した．その結果，すべてのサイトでスクリプトに記載されたアドレスと通信を行っていることが判明し，マルウェア感染の危険性があることが確認できた．検知結果に 5 件の差が出たことについては，2 つの理由が考えられる．1 つは，3.2 節で述べたように，Google のクローラが改ざん後 1 度も巡回しておらず，警告を出せなかったため．もう 1 つは，クローラが巡回していてもセーフブラウジングでは検知できず，提案手法では検知することができたサイトであったという理由である．いずれかについては，Google での採用方式が明らかになっていないので現状では判断できない．

6.3　改ざんサイト判定アルゴリズムの誤判定

図 9 の判定アルゴリズムには，現時点でも誤判定の可能性がある．図 9-(a)〜(e) それぞれの判定における誤判定について以下に示す．

- 図 9-(a)：ブラックリストが古く，掲載された URL がすでに使用されていない場合，False Positive となる．
- 図 9-(b)：<script> タグが 1 つだけ（重複せずに）埋め込まれている場合，False Negative となる．
- 図 9-(c)：タイトルにスクリプトがない場合，False Negative となる．
- 図 9-(d)：width が 1 以上，かつ height が 1 以上となる不正スクリプトの場合，False Negative となる．
- 図 9-(e)：特徴的なスクリプト名は変化しやすいため，False Positive，False Negative どちらにもなりうる．

なお，図 9-(b) において False Negative となり，かつ図 9-(c) において False Negative となった場合は，総合的に False Negative となりうる．

また，図 9 の判定アルゴリズムは普遍的なものではないため，今後の改ざん手法の変化によっては，改ざんが発見できない可能性も考えられ，監視を続け，つねにアルゴリズムの改善をしていく努力が必要である．

6.4　ま と め

6.1，6.2 節より，既存の対策手法では見つけられなかった不正スクリプトを，提案手法では発見することができた．このことから，提案手法を用いることで，従来に比べ多くの改ざんサイトが検知可能になると期待できる．また，上記 6.2 節の簡易実験においては，誤検知を確認することはなかったが，6.3 節で示したように完全にその可能性がないとはいえず，今後，さらに多くのデータに基づいて評価を行っていく必要がある．

7. おわりに

本稿では，改ざんサイトおよび不正スクリプトの調査・分析を通して，ユーザ標的型 Web 改ざん攻撃における特徴を発見し，そこから未知の不正スクリプトを自動的に検知可能な方法と，効果的な不正スクリプトの収集方法を考案した．そして，これらを用いて Web プロキシにおいて検知を行うシステムを対策手法として提案した．今後の課題は，iframe での改ざんに対する有効性の確認，誤検知率における実験評価，および提案手法の実装・評価を行うことである．

謝辞　本研究を進めるにあたり，貴重なご助言をいただいたコンピュータ疫学研究会の皆様に深く感謝いたします．

参 考 文 献

1) LAC：侵入傾向分析レポート，Vol.11, p.6（オンライン）(2008).
入手先 http://www.lac.co.jp/
2) 竹森敬祐，田中俊昭，中尾康二ほか：Web サーバリモート監視システムの実装および評価，情報処理学会論文誌，Vol.43, No.8, pp.2542–2551 (2002).
3) Google：Google セーフブラウジング診断ページ：www.google.com（オンライン）．
入手先 http://www.google.com/safebrowsing/diagnostic?site=http://www.google.com/&hl=ja（参照 2009-07-05）
4) Shadowserver Foundation: Shadowserver Foundation - Calendar - 2008-05-14（オンライン）．入手先 http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080514（参照 2009-01-22）
5) VirusTotal：VirusTotal — 無料オンラインウイルス/マルウェアスキャン（オンライン）．入手先 http://www.virustotal.com/jp/（参照 2009-07-05）

6) LAC：【緊急注意喚起】改ざんされた Web サイト閲覧による組織内へのボット潜入被害について（オンライン）．入手先 http://www.lac.co.jp/news/press20081222.html（参照 2009-01-22）

(平成 21 年 3 月 14 日受付)
(平成 21 年 10 月 2 日採録)

田村　佑輔

平成 17 年 4 月東京電機大学工学部第一部情報メディア学科入学．卒業研究でネットワークセキュリティに関する研究を実施．平成 21 年 3 月同学科卒業．同年 4 月セイコーエプソン株式会社入社．

甲斐　俊文（正会員）

平成 12 年九州工業大学情報工学部知能情報工学科卒業．平成 14 年九州工業大学大学院情報工学研究科博士前期課程修了．同年松下電工株式会社（現パナソニック電工株式会社）入社．トレースバック技術をはじめとするネットワークセキュリティ技術の研究開発に従事．

佐々木良一（フェロー）

昭和 46 年 3 月東京大学卒業．同年 4 月日立製作所入社．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．平成 13 年 4 月より東京電機大学工学部教授，平成 19 年 4 月より未来科学部教授．工学博士（東京大学）．平成 10 年電気学会著作賞，平成 14 年情報処理学会論文賞，平成 19 年総務大臣表彰，平成 20 年情報処理学会功績賞等を受賞．著書に，『IT リスクの考え方』岩波新書，2008 年等．情報処理学会コンピュータセキュリティ研究会顧問．日本セキュリティ・マネージメント学会会長，情報ネットワーク法学会理事長，日本ネットワークセキュリティ協会会長．