Computer Security Symposium 2016
11 - 13 October 2016

多種環境を用いた不正サイトの解析

重本 倫宏[†1]　磯部 義明[†1]　仲小路 博史[†1]

概要：近年，Web ブラウザや OS 等のソフトウェアの脆弱性を悪用し，マルウェアに感染させるドライブバイダウンロード攻撃による被害が多発している．このような問題に対応するためには，ドライブバイダウンロードに用いられる不正サイトの解析が重要となる．しかし，最近では接続してきた環境に応じて応答を変化させる不正サイトが存在し，適切な解析環境を用意しなければ不正サイトを解析できないという課題が存在する．そこで，本報告では，解析環境を変化させながら不正サイトへ接続し，このような不正サイトの解析に有効に動作する解析環境を考察する．さらに，実環境を用いた評価実験により，多種環境を用いた不正サイト解析の有効性を示す．

キーワード：不正サイト解析，マルウェア，動的解析

Analysis of Malicious Web Site using Various Environment

TOMOHIRO SHIGEMOTO[†1]　YOSHIAKI ISOBE[†1]　HIROFUMI NAKAKOOJI[†1]

Abstract: In recent years, incidents caused by Drive-by download attack which exploit vulnerability in OS or web browser have increased. So, it is important to analysis malicious web site used by Drive-by download attack in order to respond this problem. But there are some malicious web sites which change response depending on analysis environment. In this paper, we use various environment to analysis such malicious web sites. In addition, we also evaluate effectiveness of the proposed method by using the prototype system we have implemented.

Keywords: Malicious Web Site Analysis, Malware, Dynamic Analysis

1. はじめに

近年，民間企業や公的機関を狙ったサイバー攻撃が顕在化しており，個人のみならず，企業，国家の利益や安全を損なうリスクが高まっている．攻撃手法も巧妙化しており，標的型攻撃，特に APT（Advanced Persistent Threat）攻撃[1]は，秘密裏に，そして執拗に攻撃を続ける点で従来の脅威とは性質が異なる．また，2015 年 6 月には，日本年金機構において遠隔操作型マルウェアに感染した職員の端末から基礎年金番号を含む個人情報が約 125 万件漏えいし，大きな社会問題となった[2]．

日本年金機構への APT 攻撃では，マルウェアの感染にドライブバイダウンロード（Drive-by download）[3]という手法が利用された[4]．ドライブバイダウンロードとは，WEB ブラウザなどを介して，ユーザに気付かれないようにマルウェアをダウンロードさせる手法である．

ドライブバイダウンロードによる攻撃は，主に WEB ブラウザや，OS，その他のサードパーティ製のソフトウェアの脆弱性を突いて行われることが多い．このため，ある解析環境で不正サイトにアクセスしたとしても，攻撃者が狙っている脆弱性が存在しない解析環境ではマルウェア感染が起きず，不正サイトの解析を行えないといった課題が存在する．最近では，javascript を用いたブラウザフィンガープリントによってクライアント環境に応じた攻撃を仕掛ける不正サイトも確認されている[5]．

そこで本稿では，多種環境を用いた不正サイト解析システムを開発し，環境に応じて応答を変化させる不正サイトの解析を行う．さらに，実際の不正サイトを用いて，このような不正サイトの解析に有効に動作する解析環境を考察する．さらに，実環境を用いた評価実験により，多種環境を用いた不正サイト解析の有効性を示す．

2. 関連研究

2.1 マルチモーダルマルウェア解析システム

先行研究として，報告者らのグループでは，特定の解析環境でしか動作しないマルウェアの解析を目的とし，多種環境を用いてマルウェアを多角的に解析するマルチモーダルマルウェア解析システム（Multi-modal Malware Analysis System，以下 M3AS）の研究を進めている[6,7]．

報告者らが開発している M3AS の概要を図 1 に示す．M3AS では様々な OS やソフトウェアを組み合わせた複数の解析環境上でマルウェアを解析する．また，マルウェア解析のノウハウをスクリプト化することで，観測結果からマルウェアの挙動を自動抽出する技術を実装している．この技術によりマルウェアによるネットワーク接続などの不正行動を容易に解明することができ，被害の発生や拡大の防止に役立てることができるようになる．

†1 (株)日立製作所
Hitachi Ltd.

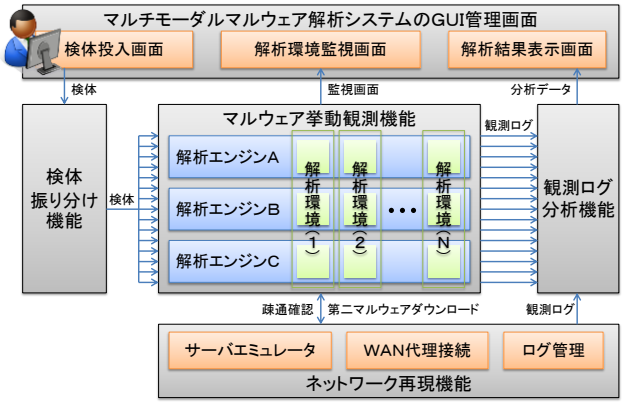

図 1　マルチモーダルマルウェア解析システムの概要

Figure 1　Multi-modal Malware Analysis System.

現行の M3AS は，マルウェア検体の解析を前提として解析環境を選定している．そこで報告者らは，M3AS を不正サイト解析に活用するため，不正サイト解析に有効な解析環境の考察を行う．

2.2 不正サイトの解析

不正サイトの解析を行う手段として，クライアントハニーポットに関する研究が存在する．クライアントハニーポットは，WEB ブラウザ，または，それを模擬したシステムにより不正サイトにアクセスすることで不正サイトを解析する技術である．実際のブラウザを用いたクライアントハニーポットを高対話型[8,9]と呼び，ブラウザをエミュレートして解析を行うクライアントハニーポットを低対話型[10,11]と呼ぶ．高対話型クライアントハニーポットの方が実際の環境を用いることで難読化処理を行うような攻撃に対しても攻撃の検知が可能であるが，網羅的な解析を行うためには，攻撃対象となる様々な解析環境を用意する必要があり，それだけ多くのサーバリソースが必要となる．

そこで，本研究では，高対話型クライアントハニーポットのサーバリソース削減を目的として，様々な解析環境を用いて不正サイトに接続し，効率的な（より少ないリソースで，より多くの不正サイトを解析する）解析環境の組み合わせを検討する．

3. 不正サイト解析システムの概要

ドライブバイダウンロードなどに用いられる不正サイトを解析する不正サイト解析システムは，攻撃者が攻撃に利用する脆弱性を備えた複数の解析環境を用いなければならない．このため，様々な OS やアプリケーションを備えた解析環境を構築し，不正サイトの解析に用いる．なお，不正サイト解析システムに実装する解析環境の構成については 4 章で検討する．不正サイト解析システムの概要を図 2 に示す．

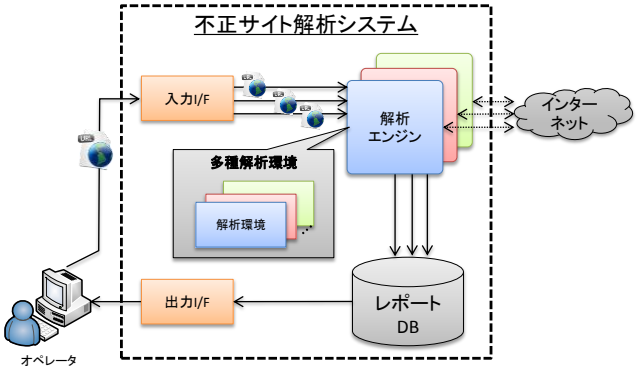

図 2　不正サイト解析システムの概要

Figure 2　Malicious Web site Analysis System.

不正サイト解析システムの具体的な処理の流れを説明する．

1. 解析者は, 不正サイト解析システムに解析対象の URL を投入する．
2. 不正サイト解析システムは，投入された URL を複数の動的解析エンジンに投入する．
3. 動的解析エンジンは，多種多様な解析環境において，WEB ブラウザを起動し，URL へ通信を行う．
4. 動的解析エンジンは，解析結果を解析結果 DB に格納する．
5. 不正サイト解析システムは，複数の解析結果を分析し，解析者へ分析結果を提供する．

以上のように，不正サイト解析システムは，複数の動的解析エンジン, 解析環境を用いて不正サイトの解析を行う．

4. 解析環境の検討

2 章で述べたように，高対話型クライアントハニーポットである不正サイト解析システムは，攻撃対象となる様々な解析環境を用意する必要があり，多くのサーバリソースが必要となる．本章では，この課題を解決するために，効率的な解析環境の組み合わせについて検討する．

4.1 検討方針

解析の成功率を上げるためには，攻撃を受けやすい解析環境を構築する必要がある．攻撃者は世の中で普及している OS やアプリケーションを攻撃対象として選ぶ可能性が高いため，世の中で普及している OS やアプリケーションを解析環境の候補とする．さらに，多くの脆弱性を持つ解析環境ほど攻撃が成功する可能性が高まる．つまり，多くの脆弱性を持つ解析環境を構築することで攻撃の成功率を向上させることが期待できるため，OS やアプリケーションが持つ脆弱性の数に着目し，解析環境候補の絞込みを行う．続いて，実際の不正サイトに接続して攻撃者が攻撃対象としている環境を調査し，解析環境候補の組み合わせに

ついて検討する．

4.2 普及率の調査

OS に関しては，企業で利用される OS の普及状況[12]を考慮し，Windows を対象に解析環境を候補とする．以下に解析環境候補の OS を示す．

・Windows XP（SP なし，SP1，SP2，SP3）
・Windows Vista（SP なし，SP1，SP2）
・Windows 7（SP なし，SP1）
・Windows 8（SP なし）
・Windows 8.1（SP なし）

WEB ブラウザに関しては，普及状況[13]を考慮し，IE, Firefox，chrome，Safari を対象に解析環境を候補とする．以下に解析環境候補の WEB ブラウザを示す．

・IE（ver.6～ver.11）
・Firefox（ver.0.1～ver.34）
・chrome（ver.0.1～ver.40）
・Safari（ver.1～ver.8）

4.3 脆弱性情報の調査

4.2 節で挙げた解析環境候補に対して，2012 年～2014 年に脆弱性情報データベース（NVD）[14]に公開された脆弱性情報 17,804 件の中から, CVSS[15]基本値の深刻度レベル High の脆弱性を調査した．

ここで，OS を例にとり，解析環境の優先順位の考え方について説明する．図 3 は，OS の脆弱性情報の集合を表した図である．まず，最も多くの脆弱性を持つ OS（図 3 中 OS A）を優先順位の 1 番目とする。次に OS の脆弱性の集合から優先順位 1 で選択された OS が持っている脆弱性の集合を除いた脆弱性集合のなかで，最も多くの脆弱性を持つ OS（図 3 中 OS B）を優先順位の 2 番目とする。以下同様に優先順位付けを行う。

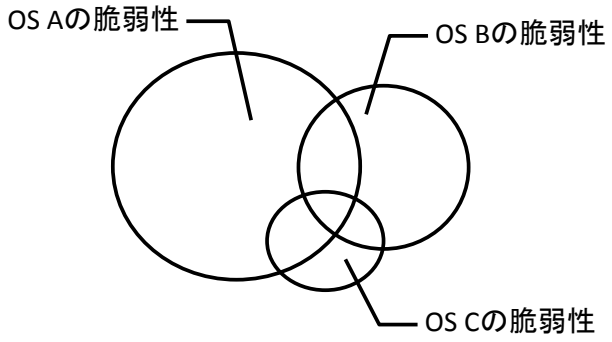

図 3　OS 選択の優先順位
Figure 3　OS Selection Rule.

上記の方法で算出した OS の優先順位を表 1 に，OS と同様にして算出した WEB ブラウザの優先順位を表 2 に示す。なお, WEB ブラウザの優先順位は 5 番までを表示した．ここで，表中の CVE カバー数は，これまでに選択された OS または WEB ブラウザが持つ脆弱性の数を表し，CVE カバー率は，OS または WEB ブラウザに存在する脆弱性の数に対する CVE カバー数の割合を表す。

表 1　OS の優先順位
Table 1　Priority of OS.

Priority	OS	Cover number of CVE	Cover ratio of CVE
1	Windows Vista (sp2,x64)	142	76.76%
2	Windows XP (sp3,x86)	167	90.27%
3	Windows 7 (sp1,x86)	179	96.76%
4	Windows Vista (sp2,x86)	184	99.46%
5	Windows Vista (-,x86)	185	100.00%

表 2　WEB ブラウザの優先順位
Table 2　Priority of WEB Brower.

Priority	WEB Brower	Cover number of CVE	Cover ratio of CVE
1	IE 9	260	18.58%
2	Firefox 4	515	36.81%
3	Safari 4	601	42.96%
4	chrome 25	635	45.39%
5	Firefox 19	728	52.04%

4.4 不正サイト応答の調査

続いて，実際の不正サイトに複数の環境で接続し，応答の有無から不正サイト解析システムに構築する解析環境を検討する．ここでは，2013 年 6 月から 2016 年 1 月の期間に収集した不正な接続先（2,439 件）に対して応答の有無を調査した．接続に用いたユーザエージェントの情報を表 3 に示す．なお，4.3 節の脆弱性調査結果及び，これまでのマルウェア解析の実績から不正サイト応答の調査に用いるユーザエージェントを選定した．

表 3　ユーザエージェント

Table 3　User Agent.

User Agent ID	OS	Brower	User-Agent
1	Windows XP (sp3,x86)	IE7	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0)
2	Windows XP (sp3,x86)	IE8	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
3	Windows XP (sp3,x86)	Firefox4	Mozilla/5.0 (Windows NT 5.1; rv:2.0) Gecko/20100101 Firefox/4.0
4	Windows XP (sp3,x86)	Safari4	Mozilla/5.0 (Windows; U; Windows NT 5.1; ja-JP) AppleWebKit/530.17 (KHTML, like Gecko) Version/4.0 Safari/530.17
5	Windows XP (sp3,x86)	Chrome25	Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.19 (KHTML, like Gecko) Chrome/25.0.1323.1 Safari/537.19
6	Windows Vista (sp2,x64)	IE7	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; WOW64; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.30729)
7	Windows Vista (sp2,x64)	IE8	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.30729)
8	Windows Vista (sp2,x64)	IE9	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; WOW64; Trident/5.0)
9	Windows Vista (sp2,x64)	Firefox4	Mozilla/5.0 (Windows NT 6.0; WOW64; rv:2.0) Gecko/20100101 Firefox/4.0
10	Windows Vista (sp2,x64)	Safari4	Mozilla/5.0 (Windows; U; Windows NT 6.0; ja-JP) AppleWebKit/530.17 (KHTML, like Gecko) Version/4.0 Safari/530.17
11	Windows Vista (sp2,x64)	Chrome25	Mozilla/5.0 (Windows NT 6.0; WOW64) AppleWebKit/537.19 (KHTML, like Gecko) Chrome/25.0.1323.1 Safari/537.19
12	Windows 7 (sp1,x86)	IE9	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)

2,439 件の不正サイトのうち，応答があった不正サイトは 318 件（応答率 13%（318 件/2,439 件））であった．表 4 に，ユーザエージェント毎に応答があった不正サイトの数を示す．

表 4　応答があった不正サイトの数

Table 4　Number of Response.

User Agent ID	Number of Responses
1	318
2	318
3	315
4	314
5	315
6	318
7	317
8	316
9	314
10	315
11	315
12	317

応答があった不正サイトのうち MD5 ハッシュ値が異なる不正サイトは 86 件（応答の変化率 27%（86 件/318 件））存在した．以下に，ユーザエージェントの違いにより応答サイズに顕著な差が見られた不正サイトを示す．

表 5　不正サイトの応答サイズ

Table 5　Number of Response.

User Agent ID	Case 644	Case 1054	Case 1120
1	2,684 Byte	322 Byte	36,839 Byte
2	2,684 Byte	322 Byte	36,839 Byte
3	0 Byte	0 Byte	0 Byte
4	0 Byte	0 Byte	0 Byte
5	0 Byte	0 Byte	0 Byte
6	2,684 Byte	322 Byte	36,839 Byte
7	2,684 Byte	322 Byte	36,839 Byte
8	2,684 Byte	322 Byte	0 Byte
9	0 Byte	0 Byte	0 Byte
10	0 Byte	0 Byte	0 Byte
11	0 Byte	0 Byte	0 Byte
12	2,684 Byte	322 Byte	0 Byte

Case 644 及び Case1054 は，IE（IE7, IE8, IE9）から，Case1120 は，IE7, IE8 からリクエストに対してのみコンテンツを応答していることが分かる．

以上の検討結果より得られた解析環境の優先順位を表 6 に示す．OS 選択の優先順位と同様，最も多くの応答があった解析環境を優先順位の 1 番目とし，次に不正サイトの集合から優先順位 1 で選択された解析環境で応答があった不正サイトの集合を除いた不正サイトの中で，最も多くの応答があった解析環境を優先順位の 2 番目とした．なお，応答数が同じ場合は，脆弱性の数が多い環境を優先して選択した．

表 6　解析環境の優先順位

Table 6　Priority of Sandbox.

Priority	OS	Brower
1	Windows XP (sp3,x86)	IE8
2	Windows Vista (sp2,x64)	IE9
3	Windows XP (sp3,x86)	Chrome25
4	Windows Vista (sp2,x64)	IE8
5	Windows Vista (sp2,x64)	Chrome25
6	Windows Vista (sp2,x64)	IE7
7	Windows 7 (sp1,x86)	IE9
8	Windows Vista (sp2,x64)	Firefox4

5. 評価実験

本章では，多種環境による不正サイト解析の有効性を評価するために実施した評価実験の結果について述べる．

5.1 評価目的

4 章で導出した解析環境を用いて実際の不正サイトに接続し，単一の解析環境ではどの程度不審な挙動を見逃しているかを評価する．具体的には不正サイトに接続した際に発生する不審なホストへのリダイレクト（以下，接続先ホスト）を観測し，解析環境の違いによる接続先ホストの違いを評価する．

5.2 評価方法

評価に用いた解析環境の構成を表 7 に示す．なお，評価には，4 章で導出した優先順位 1～3 の解析環境に加え，ブラウザの多様性を確保するために優先順位 8（Firefox4）の解析環境も用いた．

表 7　解析環境

Table 7　Specification of Sandbox.

Sandbox ID	OS	Brower
1	Windows XP (sp3,x86)	IE8
2	Windows Vista (sp2,x64)	IE9
3	Windows XP (sp3,x86)	Chrome25
4	Windows Vista (sp2,x64)	Firefox4

5.3 評価結果

実際の不正サイト 218 件に接続し，解析環境の違いによる振る舞いの違いを評価した．表 8 に，4 種類の解析環境において観測した接続先ホストの数及び，当該接続先のうち Virustotal[16]によって悪性ホストとして判断されたホストの数を示す．なお，悪性ホストの総数は 66 ホストであった．

表 8　不正サイトの数

Table 8　Number of Malicious Hosts.

Sandbox ID	Hosts (Total)	Hosts (Unique)	Malicious hosts (Total)	Malicious hosts (Unique)
1	1,643	456	228	58
2	1,066	321	208	55
3	1,875	464	229	49
4	2,945	714	213	55

表 8 より，観測された悪性ホストの数は解析環境ごとに異なり，Windows XP,IE8 の環境が最も多くの悪性ホストを観測できることが分かった．表 9 に，各解析環境で観測できた悪性ホストのカバー率を示す．

表 9　悪性ホストカバー率

Table 9　Cover Rate of Malicious Hosts.

Sandbox ID	Cover Rate
1	87.9%
2	83.3%
3	74.2%
4	83.3%

表 9 より，一つの解析環境で，平均 82.2%（最小 74.2%）の悪性ホストをカバーしていることがわかる．これより，一つの解析環境を用いた解析では，平均で 17.8%（最大 25.8%）の悪性ホストを見逃してしまう可能性があると言える．

図 4 に悪性ホストの包含関係を示す．ある特定の解析環境で観測された悪性ホストの数を円の大きさで示し，円が重複している部分は共通して観測された悪性ホストの数を表している．

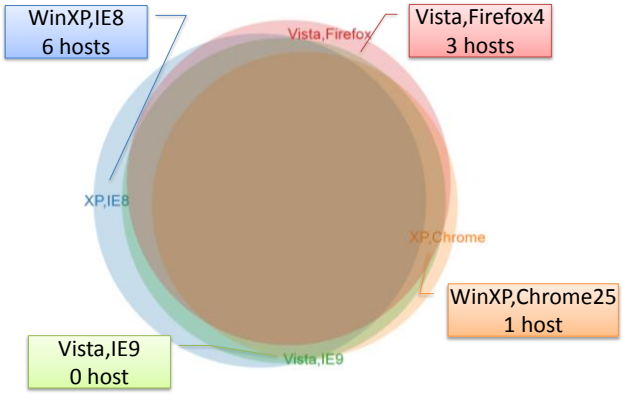

図 4　悪性ホストの包含関係

Figure 4　Inclusion Relation of Malicious Hosts.

図 4 より，Windows XP,IE8 でのみ観測された悪性ホストは 6 ホスト，Windows XP,Chrome でのみ観測された悪性ホストは 1 ホスト，Windows Vista,Firefox でのみ観測された悪性ホストは 3 ホストであることが分かった．また，4 つの解析環境で共通する悪性ホストの数は 42 ホストであったことから，36.4%（24 ホスト/66 ホスト）は環境によって振る舞いが変化する悪性ホストであると言える．

以上の評価結果より，多種環境で不正サイトを解析することで，単一解析環境だけでは見過ごす可能性のあった，

悪性ホストを明らかにできることがわかり，多種環境を用いた不正サイト解析の有効性が確認できた．

5.4 考察

(1) ブラウザの脆弱性を突く攻撃について

今回の評価で用いた不正サイトの中には，ブラウザの脆弱性を突いてマルウェアを実行するドライブバイダウンロード攻撃を観測することが出来なかった．Nappa らの調査によると，改ざんされたサイトの生存期間は短く，約 60%のサイトが 1 日以内に閉鎖されてしまう[17]．このため，ドライブバイダウンロード攻撃を観測するためには，不正サイトを入手と同時に解析することが望ましい．これに対しては，今後も不正サイトの解析を継続して行い，攻撃活動の実態を明らかにしていく．

(2) ユーザエージェントの相違による応答変化について

ここで，ユーザエージェントの違いによる応答の変化が見られた Case1054 に関して考察する．解析環境を用いて Case1054 の不審ホストに接続した際に Windows XP,IE8 の解析環境でのみに応答があり，その他の解析環境では応答がなかった．この結果より，Case1054 の不正サイトが備えている解析回避機能として，以下の 2 つが考えられる．

・サーバ側で環境を確認し，応答を変化させている
・同じ IP からの 2 回目の接続には応答しない

一つ目の解析回避機能は，多種環境で解析する本システムによって解析することができるが，二つ目の解析回避機能に関しては，本システムをそのまま適用するだけでは解析できない．これに対しては，一度目の通信で応答されたコンテンツをキャッシュし，別の解析環境で解析させることで，対応可能になると考える．

(3) 解析環境について

本報告で提案した不正サイト解析システムは，Windows 環境の解析環境のみを対象として構成している．しかし，個人保有の携帯端末を職場に持ち込みそれを業務に使用する BYOD の普及が進んでいることなどから，今後企業内で業務に活用される OS やブラウザの種類や組合せは変かしていくと考えられる．この問題に対しては，企業で業務に活用される OS 等のシェアを継続的に調査し，随時解析環境を更新していくことで対応する．

6. おわりに

本稿では，多種環境を用いた不正サイト解析システムを開発し，環境に応じて応答を変化させる不正サイトの解析を行った．さらに，このような不正サイトの解析に有効に動作する解析環境を考察した．また，実際の不正サイトを用いた評価実験により，不正サイトの中には解析環境の違いにより応答するコンテンツを変化させるものが存在し，単一の解析環境では平均 17.8%（最大 25.8%）の不正サイトを見逃していることを明らかにした．これより，多種環境で解析を行う不正サイト解析システムの有効性を確認した．今後は，不正サイトの解析を継続して行い，攻撃者の不正活動の実態を明らかにする．

参考文献

[1] “標的型攻撃/新しいタイプの攻撃の実態と対策”. http://www.ipa.go.jp/files/000024542.pdf, (参照 2016-07-28).
[2] “「日本年金機構の情報漏えい事件から得られる教訓」公開のお知らせ”. http://www.lac.co.jp/news/2015/06/09_news_01.html, (参照 2016-07-28).
[3] “ドライブバイダウンロード: 危険にさらされる Web”. http://www.viruslistjp.com/analysis/?pubid=204792056, (参照 2016-07-28).
[4] “APT「ブルーターマイト」:新たな手口で感染拡大”. https://blog.kaspersky.co.jp/blue-termite-apt-targeting-japan/8412/, (参照 2016-07-28).
[5] 高田雄太, 秋山満昭, 針生剛男, "ドライブバイダウンロード攻撃に使用される悪性な JavaScript の実態調査", 電子情報通信学会技術研究報告, vol. 113, no. 502, pp. 59-64, 2014.
[6] 仲小路博史, 重本倫宏, 鬼頭哲郎, 林直樹, 寺田真敏, 菊池浩明, “多種環境マルウェア動的解析システムの提案”, コンピュータセキュリティシンポジウム 2014 論文集, pp. 984-991, 2014.
[7] 林直樹, 重本倫宏, 鬼頭哲郎, 仲小路博史, “複数の解析環境から取得したマルウェアの振る舞い情報の非類似性尺度に関する検討”, コンピュータセキュリティシンポジウム 2014 論文集, pp. 992-999, 2014.
[8] Yi-Min Wang , Doug Beck, Xuxian Jiang, Chad Verbowski, Shuo Chen, Sam King, “Automated Web Patrol with Strider HoneyMonkeys: Finding Web Sites That Exploit Browser Vulnerabilities”, In Proceedings of Network and Distributed System Security Symposium (NDSS), pp. 35-49, February 2006.
[9] Mitsuaki AKIYAMA, Makoto IWAMURA, Yuhei KAWAKOYA, Kazufumi AOKI, Mitsutaka ITOH, “Design and Implementation of High Interaction Client Honeypot for Drive-by-Download Attacks”, IEICE TRANSACTIONS on Communications Vol.E93-B No.5 pp.1131-1139.
[10] “Capture-HPC”, https://projects.honeynet.org/capture-hpc, (参照 2016-07-28).
[11] “HTML Unit”, http://htmlunit.sourceforge.net/, (参照 2016-07-28).
[12] “企業 PC の OS シェア、Windows 7 が 74.4%に”, http://www.sbbit.jp/article/cont1/28758, (参照 2016-07-28).
[13] “Web ブラウザシェアランキング TOP10”, https://webrage.jp/mobile/data/pc_browser_share.html, (参照 2016-07-28).
[14] “National Vulnerability Database”, https://nvd.nist.gov/, (参照 2016-07-28).
[15] “NVD-CVSS”, https://nvd.nist.gov/cvss.cfm, (参照 2016-07-28).
[16] “VirusTotal”, https://www.virustotal.com/ja/, (参照 2016-07-28).
[17] A. Nappa, M. Z. Rafique, and J. Caballero, “Driving in the cloud: An analysis of drive-by download operations and abuse reporting”, In dimva, 2013.