挙動を変える悪性 Web サイトのマルチ環境解析

義則 隆之† 神薗 雅紀‡ 廣友 雅徳†† 毛利 公美‡‡ 白石 善明†

† 名古屋工業大学
466-8555 愛知県名古屋市昭和区御器所町
yoshinori.takayuki@nitzlab.com
zenmei@nitech.ac.jp

‡ 情報通信研究機構／セキュアブレイン
184-0015 東京都小金井市貫井北町 4-2-1／
102-0083 東京都千代田区麹町 2-6-7
麹町 RK ビル 4F
masaki_kamizono@securebrain.co.jp

†† 佐賀大学
840-8502 佐賀県佐賀市本庄町 1
hirotomo@cc.saga-u.ac.jp

‡‡ 岐阜大学
501-1193 岐阜県岐阜市柳戸 1-1
mmohri@gifu-u.ac.jp

あらまし Webブラウザやそのプラグインのソフトウェアの脆弱性を悪用し，マルウェアをダウンロードさせる悪性Webサイトによる受動的攻撃の被害は広がり続けている．その攻撃の対策をするためにはまず，悪性Webサイトへアクセスし，当該サイトのコンテンツやリダイレクト先の解析，さらにダウンロードされるファイルなどのデータの解析がなされる．しかしながら，悪性Webサイトには，アクセスする環境（OS，ブラウザ，プラグインなど）によって挙動を変えるものがあり，単一の環境での解析では捕捉されずにいた挙動があると考えられる．本稿では挙動を変える悪性Webサイトのマルチ環境解析を提案する．

Multi-Environment Analysis for Detecting Malicious Web Sites Changing Their Behavior

Takayuki Yoshinori† Masaki Kamizono‡ Masanori Hirotomo†† Masami Mohri‡‡ Yoshiaki Shiraishi†

† Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya, Aichi
466-8555, JAPAN
yoshinori.takayuki@nitzlab.com
zenmei@nitech.ac.jp

‡ NICT / Secure Brain, Corp.
4-2-1 Nukuikita-machi, Koganei, Tokyo
184-0015, JAPAN／
4F, Kouji-machi RK Bldg., Kouji-machi,
Chiyoda-ku, Tokyo 102-0083, JAPAN
masaki_kamizono@securebrain.co.jp

†† Saga University
1 Honjo-machi, Saga 840-8502, JAPAN
hirotomo@cc.saga-u.ac.jp

‡‡ Gifu University
1-1 Yanagido, Gifu 501-1193, JAPAN
mmohri@gifu-u.ac.jp

Abstract The damage of passive attack by malicious Web site exploiting vulnerabilities in Web browser and its plug-ins is widely spreading. The first step of countermeasures is to analyze the data downloaded from malicious Web site. However, some malicious web site changes the behavior by the client-side's execution environment. This paper proposes a multi-environment analysis to detect behavior changeable malicious Web site.

1 はじめに

マルウェアを用いた攻撃によって，個人情報をはじめとした情報資産が流出や消去されるなどといった被害が起きており，組織の情報資産は危険にさらされている．そうした組織はセキュリティコンサルタントに実施すべき対策の抽出や被害実態の調査を依頼することになる．そのようなセキュリティコンサルタントは，マルウェアによるリスクを分析する．

リスクの分析ではまず，リスク因子である「脅威」，「脆弱性」，「情報資産」の 3 因子を特定する[1]．「脅威」とは，情報システムや組織に損失や損害をもたらすセキュリティ事故の潜在的な原因のことであり，「ソフトウェアの故障」，「悪意のあるソフトウェア」，「盗聴」，「通信への侵入」などが含まれる．「脆弱性」とは，脅威発生を誘引する資産固有の弱点やセキュリティホールのことであり，「ソフトウェアの欠陥」，「仕様上の問題点」などが含まれる．「情報資産」とは，組織にとって価値をもつ情報のことであり，「顧客情報」，「技術情報」，「業務用ソフトウェア」などが含まれる．リスク因子が特定されると，それぞれの因子が組織に及ぼす影響を考慮して「脅威の大きさ」，「脆弱性の度合い」，「情報資産の価値」を評価する．リスク因子の特定と評価によって，あるリスクが組織にどれだけの影響を与えるかがわかれば，リスクへの対策に優先順位を付けることができる．

マルウェアによる攻撃の中にはソフトウェアの脆弱性を悪用する悪性 Web サイトを用いるものがある．利用されたソフトウェアの脆弱性やもたらされる被害などはセキュリティベンダの解析により明らかにされる．その過程で得られた情報は，アンチウイルスソフトウェアに代表されるセキュリティソフトウェアを開発することなどのために利用されており，「攻撃手法」，「悪用される CVE（Common Vulnerabilities and Exposures）」，「悪用されるアプリケーション」，「引き起こされる結果」，「関わりうるデータやファイル」が含まれる．これらの情報を，「攻撃手法」が「脅威」，「悪用される CVE」や「悪用されるアプリケーション」が「脆弱性」，「引き起こされる結果」や「関わりうるデータやファイル」が「情報資産」となるようにリスク因子に対応づけると，Web サイトの解析はリスクを分析する手段の一つとしてみなせる．

複数の脆弱性を持ち合わせている環境を標的として，実行する環境によって挙動を変える悪性 Web サイトがある．従来は解析されずにいた可能性のある Web サイトの挙動を把握できれば，悪性 Web サイトによるリスクの分析をより正確にできる．

本稿では，挙動を変える悪性 Web サイトを検知するためのマルチ環境解析を提案する．マルチ環境解析を行うことで，解析環境の不一致により従来は検知されない悪性 Web サイトの検知や見逃していたリスクを把握できるようになる．

2 悪性 Web サイトによる攻撃とその対策

インターネットを利用した攻撃の主流は，攻撃者が攻撃対象者に悪意のある情報を送信する能動的攻撃から，攻撃者が攻撃対象者の要求を受けて悪意のある情報を返信する受動的攻撃へと移り，受動的攻撃への対策の重要性が増している．悪性 Web サイトを用いた攻撃も受動的攻撃に含まれるものである．悪性 Web サイトを用いた攻撃の例を図 1 に示す．ここでは，入口サイト，中継サイト，攻撃サイト，マルウェア配付サイトを用いたものをそれぞれの役割にわけて説明する．

［**入口サイト**］ 攻撃の起点となるサイトである．アクセスすると，中継サイトへリダイレクトさせる．正規サイトを改ざんし，入口サイトとすることも多い．

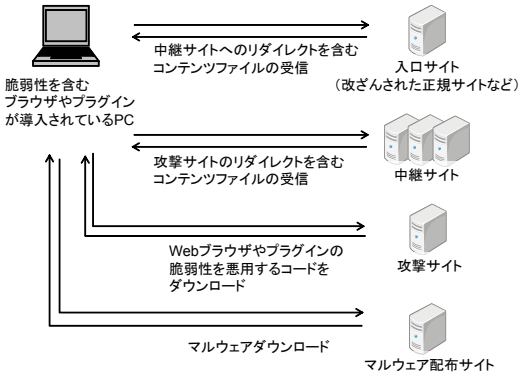

図 1　Drive-by Download 攻撃の概要

［**中継サイト**］　攻撃サイトへの中継を行うサイトである．複数の中継サイトを経由することもある．

［**攻撃サイト**］　クライアント PC の OS，Web ブラウザや，Web ブラウザ上で動作するプラグインの脆弱性を悪用し，マルウェア配付サイトからマルウェアをダウンロードするスクリプトを実行させる．

［**マルウェア配付サイト**］　攻撃サイトによって乗っ取られたクライアント PC のリクエストに応え，マルウェアを送信する．

上記のような，Web サイトへのアクセスによって脆弱性を悪用するスクリプトを実行させマルウェアをダウンロードさせる攻撃は，Drive-by Download（DBD）攻撃と呼ばれ，悪性 Web サイトを用いた攻撃の一般的な形態である．IBM[2]によると，2013 年上半期における DBD 攻撃の検知数は 3972 件であり，1 日平均で 10 件, 多い日には 80 件を超えている. また，マカフィー[3]によると 2013 年 1 月から 7 月までの月間ウイルス検知社数で上位 10 のウイルスの内，半数以上が DBD 攻撃を用いたものであり，特に 6 月は 8 件で過去最多であったと報じている．また，2013 年 3 月末までに集計された疑わしい URL の合計数は 6430 万件を超え，2013 年第 1 四半期に新たに検出された疑わしい URL は 260 万件存在し, そのうち 94%がマルウェアやエクスプロイト，セキュリティ侵害コードを含むものであるとされている[4].

文献[5]で示されている DBD 攻撃を防ぐことを困難にするテクニックのうちで，Web サイトに関わるものとして次のものがある．

1. 中継サイトがリバースプロキシになっており一つのドメインに対する IP アドレスが複数存在していることがある．これにより URL フィルタリングによるブロックが困難になる．

2. 中継サイトや攻撃サイトへリダイレクトさせるスクリプトに記述された接続先 URL に, 正常なドメインの文字列が多数含まれていることがある．これにより URL フィルタリングをすり抜ける．

3. 悪性 Web サイトより送信されるスクリプトが高度に難読化されていることがある．これにより侵入検知システム（IDS）をすり抜ける．

これらとその応用をするテクニックによって，防御の困難性はますます高まっている．Web サイトにアクセスして得られるデータを解析することで対策を検討することになるが，次のような挙動により本来確認したい悪性な挙動や期待した定性的なデータを得られないことがある[5].

A. 実行環境によって異なる挙動をする．例えば，正規サイトに改ざんが加えられた入口サイトにアクセスしたとき，通常のブラウザでは正規サイトが表示されるだけであるが，標的とするブラウザを使っている場合のみ，正規サイトの表示とともに中継サイトへのリダイレクトを起こさせる．これにより，標的とする以外の環境でアクセスした場合，悪性な挙動を検知できない．

B. 悪性 Web サイトへ接続するとき，同じ IP アドレスでは初回接続時のみ悪性な挙動を示す. 固定の IP アドレスでアクセスすると，2 回目以降のアクセスでは悪性な挙動を示さないため，すべての悪性な挙動を再現できない．また，悪性 Web サイトには時間によって挙動を変化させるものも存在する．

C. マルウェアをダウンロードさせるために複数の脆弱性が悪用される．これは解析の妨害を意図したものではないこともあるが，実際に悪用された脆弱性以外にどのような脆弱性を悪用しようとしていたかが把握できなくなるため，解析を困難にしている．

攻撃サイトには複数の脆弱性を狙う準備がされている．当該サイトにアクセスした際は，アクセス環境が有する脆弱性に該当したコードが実行され，その他の該当しない脆弱性に関わるコードは実行されない．このような挙動があるときに正確なデータを入手できなくなる大きな要因は，解析環境が単一の場合である．従来は解析されずにいた悪性 Web サイトについてより正確に挙動を把握するためには，複数の環境で解析しなければならない．

3 マルチ環境による Web サイト解析

3.1 マルチ環境解析システムの概要

2 章で述べたデータを入手困難にする挙動に対応するマルチ環境解析を提案する．複数の PC にそれぞれ異なる種類やバージョンのブラウザ，プラグインを導入し，Web サイトをクロールする度に IP アドレスを変更する機能を実装して，マルチ環境解析を実現する．以下に具体的な対応を示す．

A'. 悪性 Web サイトが標的としている Web ブラウザは，標的としている Web ブラウザでアクセスしなければ判明しない．そこで，標的にされやすい複数の Web ブラウザからアクセスして挙動を確認する．複数の Web ブラウザの中に標的となる Web ブラウザが存在すれば，悪性な挙動を確認できる．

B'. 一つの IP アドレスでアクセスできるのは一度までである．そこで，複数の IP アドレスを利用して複数回のアクセスを行う．クロールする度に IP アドレスを変更することで，複数回のアクセスが可能になり，単一の IP アドレスでは把握できなかった挙動を確認できる．

C'. プラグインのバージョンによって悪用する脆弱性を変える悪性 Web サイトがある．悪性 Web サイトが悪用する脆弱性を正確に把握するために，プラグインのバージョンが異なる複数の環境でアクセスする．標的のバージョンでアクセスできれば，単一環境では把握できなかった悪用される脆弱性

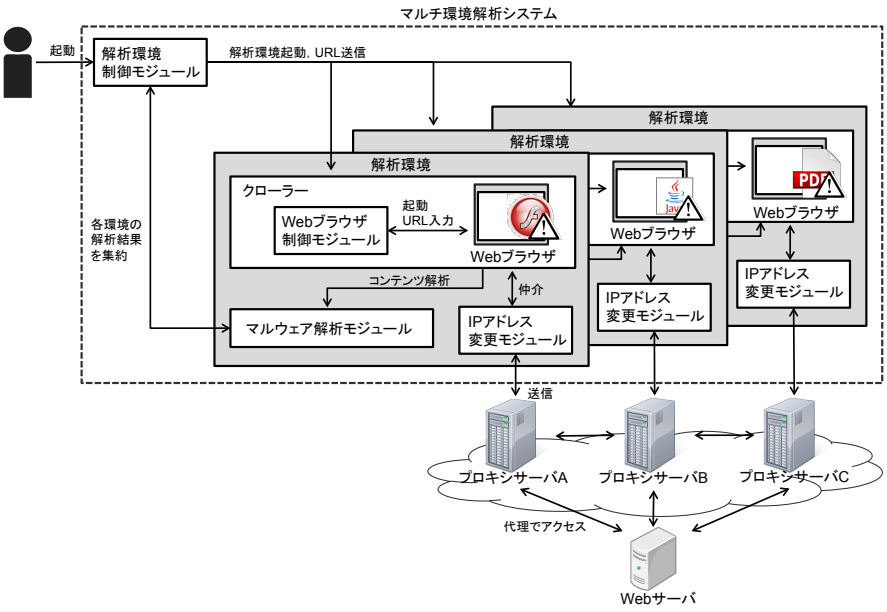

図 2 マルチ環境解析システムの構成

を確認できる．

3.2　マルチ環境解析システムの構成と機能

マルチ環境解析システムの構成を図 2 に示す．一つの解析環境は以下のモジュールで構成され，複数の解析環境を構築することでマルチ環境解析を行う．

［**クローラー**］ Web サイトに自動的にアクセスし，Web ページを構成するファイル（html, javascript，画像，pdf，flash など）を収集するプログラムである．Web ブラウザとその上で動作するプラグイン，また，Web ブラウザを制御するモジュールで構成される．

［**マルウェア解析モジュール**］ Web サイトからダウンロードしたコンテンツを解析する．例えば，シグネチャや URL とのパターンマッチングやヒューリスティック検知などの機能を導入する．

［**IP アドレス変更モジュール**］ 複数のプロキシサーバを利用し，Web サイトにアクセスするプロキシサーバを変更することで IP アドレスを変更する．

そして，複数の解析環境を制御する次のモジュールが存在する．

［**解析環境制御モジュール**］解析環境を制御する．解析環境の起動・終了，URL の入力，解析結果の出力，IP アドレス変更モジュールの ON／OFF の切り替えを行う．

マルチ環境解析システムによる解析の手順は次のようになる．ここでは，これまでに解析したことがない Web サイトを解析する場合を示している．

1. システムを起動すると，解析環境制御モジュールが複数の解析環境を起動する．
2. システムに URL を入力すると，解析環境制御モジュールがそれぞれの解析環境の Web ブラウザ制御モジュールに URL を送信する．
3. Web ブラウザ制御モジュールは Web ブラウザを起動し，入力された URL へアクセスさせる．
4. Web ブラウザのリクエストは IP アドレス変更モジュールが仲介し，プロキシサーバへと送信される．
5. プロキシサーバが代理で Web サイトにアクセスする．
6. Web サイトのレスポンスは，プロキシサーバ，IP アドレス変更モジュールを経由して Web ブラウザへと返される．
7. Web ブラウザが受信したコンテンツファイルを実行する．
8. コンテンツファイルの実行時に悪性な挙動が見られた場合，マルウェア解析モジュールが検知し，結果を解析環境制御モジュールに送信する．
9. 解析環境制御モジュールが複数の解析環境の解析結果を出力する．

この手順では，IP アドレス変更モジュールが ON になっている場合を示しているが，OFF になっている場合は Web ブラウザが直接 Web サイトにアクセスする．

4　評価

単一環境で解析した場合では検知できない可能性がある悪性 Web サイトをマルチ環境ならば検知できることを確かめる．ブラックリスト Malware Domain List[6]に掲載されている悪性 Web サイトに対して次の手順で実験を行った．

まず，表 1 に示す Web サイトを解析するための複数の環境を VMWare Workstation を利用して構築した．脆弱性を悪用されることの多い次のプラグインを導入した．

- PDF ビューワーAdobe Reader
- Flash の実行環境 Flash Player
- Java の実行環境 Java Runtime Environment（JRE）

マルウェア解析モジュールには ESET NOD32 アンチウイルス（NOD32）を利用した．

次に，Malware Domain List に 2013 年 4 月 17 日から 2013 年 7 月 16 日の期間に掲載された脆

表 1　評価用解析環境

仮想マシン	VMWare Workstation 9.0.2
OS	Windows 7 Professional （OS インストール時からアップデート未実施）
Web ブラウザ	Internet Explorer 10
プラグイン	解析環境 1：Adobe Reader XI 11.0.0 解析環境 2：Adobe Reader X 10.0 解析環境 3：Adobe Reader 9.2 解析環境 4：Adobe Flash Player 10.1 解析環境 5：JRE 7 解析環境 6：JRE 6 Update 16
アンチウイルスソフト	ESET NOD32 アンチウイルス （評価実験時点のウイルス定義データベースを適用する）

表 2　実験結果（2013 年 7 月 16 日）

アクセスした Web サイトの総数		116
表示された Web サイト	解析環境による挙動の変化を認められたもの	1
	解析環境による挙動の変化を認められなかったもの	14
表示されなかった Web サイト		101

弱性を悪用する 116 個の Web サイトの URL に，各環境の Web ブラウザでアクセスする．Web サイトの挙動や NOD32 がどのような警告を出すか確認する．

実験は 2013 年 7 月 16 日に実施した．実験結果を表 2 に示す．すべての環境で Malware Domain List に記載の悪性 Web サイトにアクセスしたところ，その中に，応答が 404 Not Found もしくは Web サイトを表示できないとの通知が表示されたものが 101 個あった．それらの Web サイトは現存していないか, URL に直接アクセスした場合は応答を返さないように設定されていると考えられる. 表示された Web サイトは 15 個であり，そのうち解析環境による挙動の変化を認められたものは 1 個（ドメイン名 : lulzstack.com），解析環境による挙動の変化を認められなかったものは 14 個あった．

lulzstack.com の挙動の変化は以下のようであった．

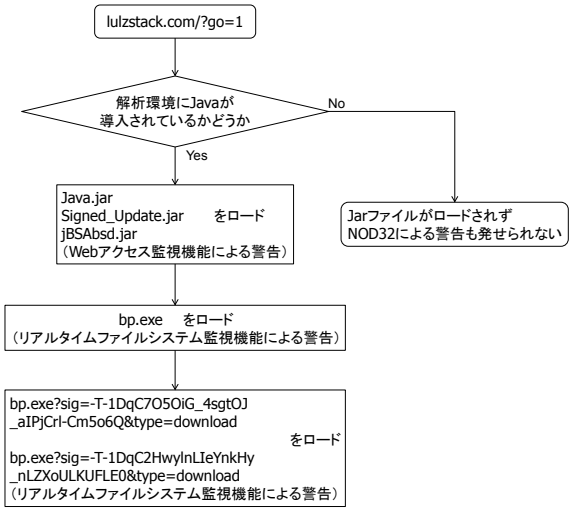

図 3　lulzstack.com の攻撃の概要

1. Adobe Reader，Adobe Flash Player を導入した解析環境 1～4 でアクセスすると，Web サイトが Java を使用しているとの通知が表示された．Web ページに組み込まれていた Java プログラムは動作せず，NOD32 はリアルタイムファイルシステム監視，Web アクセス監視共に警告を発さなかった．
2. Java のプラグインを導入した解析環境 5, 6 でアクセスすると，NOD32 が Web アクセス監視で Java.jar，Signed_Update.jar，jBSAbsd.jar に対し警告を発した．これらのファイルは NOD32 によって隔離されたため，これ以上の異常は発生しなかった．
3. 続いて，解析環境 5，6 で NOD32 の Web アクセス監視を無効にし，リアルタイムフ

ァイルシステム監視のみを有効にした状態で再度アクセスを試みた．すると，先述の Java ファイルに対する警告は表示されず，bp.exe がファイルシステム上に生成されたことを示す警告が表示された．また，temp ファイルの改変を行ったことを示す警告が表示された．

よって，lulzstack.com は環境によって挙動を変化させる悪性 Web サイトであると判断できる．lulzstack.com を解析した結果を図 3 に示す．lulzstack.com は Malware Domain List では Java を悪用していると紹介されており，解析環境 1～4 では検知できず，解析環境 5，6 ならば検知できることが確認できた．

マルチ環境解析を行ったことで, lulzstack.com は，JRE がインストールされている場合には悪性な挙動を示し，インストールされていない場合には悪性な挙動を示さないことがわかった．つまり，JRE がインストールされている単一の環境で lulzstack.com にアクセスした場合には，JRE がインストールされていない環境でどのような挙動を示すかわからない．もしも，JRE がインストールされていない場合には Adobe Reader の脆弱性を悪用するようになっていたとすると，lulzstack.com が Adobe Reader の脆弱性を悪用することだけでなく，その後どのようなマルウェアをダウンロード，実行させるかを知ることができないことになる．反対に，JRE がインストールされていない単一の環境で lulzstack.com にアクセスした場合には，lulzstack.com が悪性 Web サイトであることを検知できないことになる．

表 2 の挙動の変化が見られなかった 14 個について 2013 年 8 月 25 日に再度アクセスしたところ，次のような結果となった．

まず，14 個のうち 3 個は Web サイトが表示されなくなっていた．先に実施した 101 個のものと同様とみなされる．そして 6 個はリダイレクトも攻撃も行われなかった．これはブラックリストに登録されたことで無害なサイトに変更されたと考えられる．1 個はブラウザによって標的とするプラグインのバージョンを変えていることがわかり，表 1 の環境を変更してアクセスしたところ攻撃を検知できた．残りの 4 個は先に実施したときと同じで自動的に正規サイトにリダイレクトされたことから，特定のサイトからのアクセスに対してのみ攻撃が実行されるものと考えられる．

以上をまとめると次のようになる．2013 年 7 月 16 日と 8 月 25 日のそれぞれで 1 個ずつ攻撃検知できた結果から，3.1 節の A'と C'の対応が有効に機能したことを確認できた．

B'の対応は，近接したグローバル IP アドレスしか用意できなかったため十分に機能しなかったと考えられる．この対応が機能するようにシステムを構築できれば，両日で表示されなかった 101 個および 3 個のサイトで解析できるものがあったと予想される．B'の拡張となる特定サイトの IP アドレスの割り当てができれば, 14 個のうちの 4 個あった特定サイトへの攻撃を確認できると考えられる．これらの対応については今後検討していきたい．無害なサイトに変更されていた 6 個については, 悪性 Web サイトの出現を迅速に捉える文献[12]のような枠組みと連携することでサイト変更前の解析は可能であると考えられるが，ある時点での組織のリスクを分析するという観点からはそのような解析をする必要がないこともある．

5 おわりに

本稿では挙動を変える悪性 Web サイトを検知するためのマルチ環境解析を提案した．Web ブラウザやその上で動作するプラグインが異なり, また IP アドレスの変更が可能な複数の環境を構築して解析する．本研究は単一環境では検知できなかった悪性 Web サイトを検知することを目的としている．

悪性 Web サイトへの対策の必要性が高まっている中で，次のような関連技術がある．製品・サービスでは例えば次のものがある．aguse[7]は，ユーザの代わりに Web サイトにアクセスし，Web サイトのキャプチャ画像やダウンロードしたマルウェアをウイルス対策ソフ

トで解析した結果を提供する．gred[8]は，指定したWebサイトにアクセスし，取得したコンテンツを解析することで，Webサイトの改ざんを検知する．これらの製品・サービスは，複数の解析環境で解析した結果を表示しないことから，単一の環境で解析していると推測されるところが提案システムとは異なる．Origma+[9]は，指定した Web サイトを指定した環境でアクセスして解析する．ある環境が特定のWebサイトに対して脆弱であるかを確認するものであり，ある Web サイトにどのような脅威が潜んでいるかを調べるものではないという点で目的を異にしている．

研究開発で関連するものは例えば次のものがある．秋山ら[10]は，MARIONETTEと呼ばれる高対話型クライアント型ハニーポットを使い，従来の高対話型クライアント型ハニーポットより攻撃検知率を向上させ，検知する攻撃の種類を増やすメカニズムを提案している．MARIONETTE では，パターンファイルを利用した検知ではなく，脆弱性の監視，イベント検知，攻撃検知，スタックの異常検知，ヒープの異常検知を組み合わせることで検知率の向上を実現している．Liu ら[11]は，悪性 Web サイトよりダウンロードされたマルウェアを，メモリ上に展開されている System Service Dispatch Table（SSDT）の情報を改ざんすることで隠蔽する技術に対し，SSDT を監視することで検知率の向上を実現している．これらの成果は悪性 Web サイトによる攻撃の検知率を向上させるためのものである．このようなアプローチを提案システムと組み合わせることでさらなる検知率の向上が期待でき，従来は把握されていなかった可能性のある解析情報をより高精度に得られると考えられる．

マルチ環境を構築し Malware Domain List に記載の悪性Webサイトを解析したところ，2つの Web サイトで解析環境による挙動の変化が確認でき，悪性Webサイトであることが検知できた．あわせて，挙動の変化が確認できなかったものについても，条件が合えば検知ができるものと述べた．マルチ解析環境を利用して可能な限り悪性 Web サイトの潜在的な挙動を把握することで，守るべき組織の事前のリスク対策や，既に被害を受けていた際に見逃していたリスクを把握するのに有効であると考えられる．それらの具体的な活用方法について検討することが今後の課題としてあげられる．

参考文献

[1] ISMS：ISMS ユーザーズガイド-JIS Q 27001:2006(ISO/IEC 27001:2005)対応-（2008）．

[2] IBM：2013 年上半期 Tokyo SOC 情報分析レポート，（2013）．

[3] マカフィー：マンスリー ウイルスレポート，入手先<http://www.mcafee.com/japan/security/monthly/default.asp>（参照 2013-08-25）．

[4] マカフィー：McAfee 脅威レポート:2013 年第 1 四半期，（2013）．

[5] トレンドマイクロ：マルウェア解析の現場から-03 Gumblar 攻撃，入手先<http://blog.trendmicro.co.jp/archives/3340>（参照 2013-08-25）．

[6] Malware Domain List, available from <http://www.malwaredomainlist.com/> (accessed 2013-08-25).

[7] agusenet：aguse.，aguse.jp，入手先<http://www.aguse.jp/>（参照 2013-08-25）．

[8] セキュアブレイン：gred，入手先< http://check.gred.jp/>（参照 2013-08-25）．

[9] FFRI：Origma+ 製品概要，入手先<http://www.ffri.jp/products/origma/index.htm>（参照 2013-08-25）．

[10] Akiyama, M., Iwamura, M., Kawakoya, Y., Aoki, K. and Itoh, M.: 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, (2010).

[11] Liu, H., Zhang, D., Wei, G. and Zhong, J.: Detecting malicious rootkit web pages in high-interaction client honeypots, Information Theory and Information Security (ICITIS), 2010 IEEE International Conference, pp. 544-547, (2010).

[12] 笠間，井上，衛藤，中里，中尾：ドライブ・バイ・ダウンロード攻撃対策フレームワークの提案，コンピュータセキュリティシンポジウム 2011（CSS2011），pp.780-785，（2011）．