多種環境マルウェア動的解析システムの提案

仲小路 博史†‡　　重本 倫宏†　　鬼頭 哲郎†
林 直樹†　　寺田 真敏†　　菊池 浩明‡

†株式会社日立製作所
244-0817 神奈川県横浜市戸塚区吉田町 292 番地
‡明治大学
164-8525 東京都中野区中野 4-21-1

あらまし 近年，標的型攻撃に利用されるマルウェアが高度化し，既存の入口対策で検知できないまま組織内へ侵入を許してしまうケースが増えている。この場合，侵入したマルウェアの特性を解明し早急な被害拡大防止策を講じる必要がある。マルウェアの特性を解明する手法としてマルウェアを特殊な解析環境で実行して挙動を観測する動的解析手法が用いられている。一方，最近のマルウェアは実行環境を限定することで解析環境での解析を逃れるタイプも確認されている。本稿では，マルウェアを多種類の解析環境で実行させることで環境を選ぶマルウェアをも自動的に解析し，その挙動をレポートする多種環境マルウェア動的解析システム（M3AS）を提案する。

Proposal of Multimodal Malware Analysis System with Multiple Types of Sandboxes.

Hirofumi Nakakoji†‡　　Tomohiro Shigemoto†　　Tetsuro Kito†
Naoki Hayashi†　　Masato Terada†　　Hiroaki Kikuchi‡

†Hitachi, Ltd.
292, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa 244-0817, JAPAN

‡Meiji University
4-21-1, Nakano, Nakano-ku, Tokyo 164-8525, JAPAN

Abstract In recent years, the number of case where existing inbound measure have allowed incursions into the organization has increased. In a situation such as this, it is necessary to clarify the characteristics of the intruding malware so that countermeasures can be taken quickly to prevent the damage from expanding. A dynamic analysis method is used in order to clarify the malware's behavior. Recently, however, types of malware that avoid analysis in analytical environments by restricting execution environments have been growing more common. In response, we propose the multimodal malware analysis system. This system executes malware under a variety of different analytical environments, so that malware that only runs under a specific environment can still be automatically analyzed.

1　はじめに

近年，標的型攻撃に代表される高度なサイバー攻撃が企業や国家にとって大きな脅威となっている。企業の情報セキュリティに関する調査報告[1]によると，情報セキュリティに関わる事件・事故の原因のトップは依然としてクライアント PC のウイルス感染によるもので，さらにハニーポットで収集された新型マルウェアの傾向調査[2]によると，その 54%が既存のウイルス対策ソフトでは検知できないといわれている。マルウェアが組織の中に侵入してしまった場合，侵入したマルウェアの特性を解明し早急な被害拡大防止策を講じることが重要となる。本稿では，マルウェアを多種類の解析環境で実行させることで環境選択型マルウェアをも自動的に解析し，その挙動を解明する多種環境マルウェア動的解析システムを提案する。

2　マルウェア解析

例えば不審なメールに添付されたプログラム（検体）がマルウェアか否か，あるいはマルウェアとしてどのような機能を有するか，を解明する方法として，検体をリバースエンジニアリング等の技術によって解析する静的解析手法と，検体を特殊な解析環境で実行して，その振る舞いを観測する動的解析手法とがある[3][4]。静的解析手法は，検体の具備する機能の全てを詳細に解明できる利点があるが，プログラムや OS，ハードウェアの仕組み等に関する深い知識と，コードを一行ずつ読み解くための膨大なコストが必要となる。動的解析手法は，難読化（コード暗号化等）された検体でも容易に解析できるため，静的解析手法と比較して解析に要するコストが低い点，静的解析手法だけでは分からない挙動（例えば新たなマルウェアをインターネットからダウンロードして実行した後の挙動等）を確認できる点で有利である。一方で，観測中に顕現化しない機能はその挙動を把握できないという欠点もある。通常，検体を解析する際は検体の性質，解析の目的，解析者のスキルセットや経験則に応じて静的解析手法と動的解析手法とを補完的に組み合わせて実施する。

最近では，動的解析を支援する動的解析専用のソフトウェアが開発されており，OSS(Open Source Software)では Cuckoo Sandbox[5]が入手可能である。本ソフトウェアは仮想化されたサンドボックス上で検体を安全に実行して，ネットワーク通信や API コール等の観測結果を詳細に取得できる。このため解析を実務とする多くの専門家によって利用されており，MWS 2014 Datasets に含まれる FFRI Dataset 2014[6]も同ツールによって取得したデータが含まれる。

2.1　マルウェア動的解析の課題

これまでに述べたように我々守る側も技術やツールの進化により従来と比較して検体の解析が容易となってきた。しかし攻撃側の進化も著しく，作成したマルウェアが検知されたり解析されたりすることを回避するために，マルウェアが仮想環境やデバッグ環境，OS，インストールアプリケーション等のハードウェア／ソフトウェア構成を検知して，攻撃の対象であるか否かを判断して動作を変える環境選択型マルウェアの存在が確認されている[7]。また，攻撃者が用意したマルウェア配布サーバから第二のマルウェアをダウンロードさせることで攻撃を段階的に進めるダウンローダ型マルウェア[8]も確認されているほか，マルウェア配布サーバの中には，アクセス元の IP アドレスが攻撃対象の組織である場合のみマルウェアを配布し，それ以外の場合には正規のコンテンツを配布することで第三者によるマルウェア解析を回避するものまで確認されている[9]。

このような仕組みを持つマルウェアは，特定の環境しか用意されていない既存の動的解析ソフトウェアやサービスによる解析では，その挙動が明らかにできないケースが多い（課題 1）。また，攻撃を受けた組織が，外部の解析サービス（標的となる組織の IP アドレスを持たない組

織)に解析を委託した場合，前述したようにマルウェア配布サーバが正規のサーバとして解析者に対して振舞うため，やはりその挙動を明らかにできない(課題 2)。さらには PDF ファイル等の機密情報を含むファイルに寄生するマルウェアも確認されていることから「マルウェア＝機密情報」と位置付ける組織も存在する。このため，外部の解析サービスの利用を躊躇する組織も増えてきており，自組織内でマルウェアの特性を解明したいというニーズが高まってきている(課題 3)。

本稿で提案する多種環境マルウェア動的解析システムの目的は上記 3 つの課題を解決することにある。

3　多種環境マルウェア動的解析システム

多種環境マルウェア動的解析システム(Multi-modal Malware Analysis System, M3AS と略記)は，環境選択型マルウェアの解析成功率を向上させるため，複数種類の解析エンジン，複数種類の解析環境(サンドボックス)を用いて検体を解析する。本システムのアーキテクチャを図 1 に示す。

マルウェアと思しき検体を解析する解析者が本システムの検体投入画面を通して検体を投入(アップロード)すると，検体は検体振り分け機能によってマルウェア挙動観測機能に構成されている各サンドボックスに複製されて同時に投入される。サンドボックスでは，投入された検体を自動的に実行して挙動を観測し，結果を観測ログとして出力する。観測ログ分析機能は，マルウェア挙動観測機能から出力された大量の観測ログを収集し，各サンドボックスにおける検体の活動状況(例えばファイルアクセス，レジストリアクセス，ネットワークアクセス等)を統計的に分析したり，検体による生成ファイルや，ネットワーク接続先 URL を抽出したりする。これらの処理を同時並行かつ自動的に実施するため，解析時間の大幅な短縮や，解析作業の夜間バッチ化も期待できる。

以降では M3AS を構成する各機能について述べる。

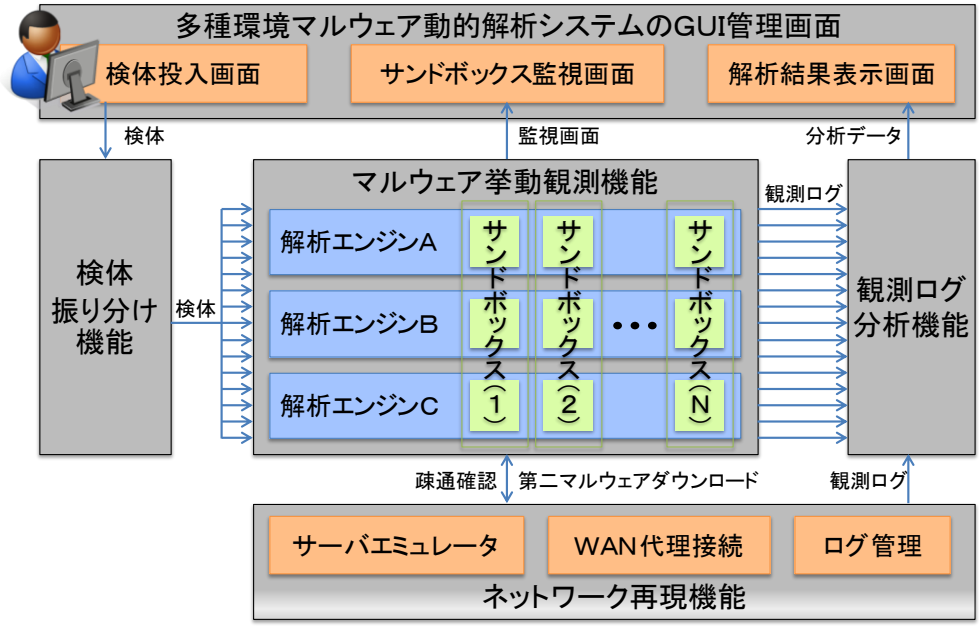

図 1　3 多種環境マルウェア動的解析システムの機能概要

3.1 マルウェア挙動観測機能

M3AS は，検体を数十種類のサンドボックスで解析することにより，環境選択型マルウェアの解析成功率の向上を実現する。サンドボックス群は解析エンジンやプラットフォーム，ソフトウェアの種類やバージョン等の異なる組合せにより構成される。サンドボックスが多いほど環境選択型マルウェアの解析成功率向上が期待できるが，使用できる物理マシンのリソースや，ソフトウェアライセンス等の制約により，全ての組合せを用意することは現実的でない。そのため M3AS のサンドボックスの構成要素を環境条件として表 1 に示す 5 項目に着目して整理する。

M3AS の「解析エンジン」は，前述した Cuckoo Sandbox を含む計 2 種類を採用している。解析エンジンは種類によってサポートする仮想マシンが異なっているため，解析エンジンの多種化は解析性能の多様化だけでなく，特定の仮想化ソフトウェアを検知するような機能を有するマルウェアの解析にも効果が期待できる。

「OS」や「アプリケーション」は種類やバージョン等のバリエーションが多く，組合せ爆発の原因となる。M3AS では，サンドボックスをマルウェアに感染させて可能な限り多くの挙動を解明することをコンセプトとしていることから，マルウェア開発者の視点に立ってマルウェアが感染および動作しやすい環境，つまり，攻撃の影響を受けやすい環境を優先的に選定する。そこで OS 構成は，マルウェアの感染が多く報告されている Windows XP 以降の主要 OS を Service Pack まで区別して設計した。また，アプリケーション構成は脆弱性が多いアプリケーション，即ち脆弱性情報の公開数の多いアプリケーションを優先的に選定した。脆弱性情報の公開数の調査には，JVN iPedia[10]の 2012 年 1 月 1 日から 2013 年 8 月 16 日までの情報を利用した。

なお，各サンドボックスは検体の実行完了，あるいは事前に設定した時間を経過すると自動的に環境を感染前へ復元する機能を備える。

3.2 ネットワーク再現機能

近年のマルウェアはネットワーク接続機能を有し，マルウェア配布サーバに接続して第二のマルウェアをダウンロードしたり，C&C サーバと接続して遠隔操作を受けたりすることが知られている。また，マルウェアの中には，実行直後にネットワークの疎通性を確認することにより，解析のために利用されることの多い閉塞ネットワーク環境で自身が実行されている否かを検知して動作を停止させる等，解析を阻害するタイプも確認されている。

表 1 サンドボックス環境の環境条件例

解析エンジン	プラットフォーム	アーキテクチャ	OS	アプリケーション
Threat Analyzer	・物理 PC ・仮想 PC （VMware ESXi）	・32bit(x86) ・64bit(x64)	・Windows XP ・Windows Vista ・Windows 7	・Microsoft Office ・Adobe Reader ・Internet Explorer ・Java ・Media Player ・一太郎
Cuckoo Sandbox	・仮想 PC （VMware Workstation）			

表 2 ネットワーク再現機能実装サービス

TCP	UDP
echo(7), http(80), discard(9), pop3(110), daytime(13), ident(113), quotd(17), chargen(19), https(443), ftp(21), smtps(465), smtp(25), time(37), ftps(990), dns(53), pop3s(995), irc(6667), finger(79)	echo(7), discard(9), quotd(17), ntp(123), chargen(19), syslog(514), time(37), dns(53), tftp(69)

（括弧内は利用ポート番号）

このため，M3AS はネットワーク再現機能を備え，サンドボックス内の検体からの各種サーバ向けリクエストに応答するサーバエミュレータ機能や，インターネットに代理接続してマルウェア配布サーバや C&C サーバと安全に通信する WAN 代理接続機能（開発中）を持つ。これにより，ダウンローダ型マルウェアが特定の Web サーバからファイルをダウンロードして実行するまでの挙動を高精度に再現，観測することができる。具体的には，インターネットサービスシミュレーションソフトウェア「INetSim」[11]を用いて表 2 に示す 21 のサービスのエミュレーションを行う。

3.3 観測ログ分析機能

観測ログ分析機能は，数十種類のサンドボックスで観測した大量のログからマルウェア特有の挙動を抽出する。抽出アルゴリズムの設計にあたっては，マルウェアの解析を実務としている専門家の高度で実績のあるマルウェア解析ノウハウ（暗黙知）に基づいて機能設計（形式知）を実施した。以下に機能の一部を説明する。

a. デバッガ検知の有無判定
　検体がデバッガによって解析されることを回避することを目的としてよく利用される，デバッガモード判定 API（isDebuggerPresent 等）の呼び出しを監視する。

b. プロセスインジェクションの有無判定
　検体が他のプロセスに不正なコードを挿入して，検体自身の実体を隠す際に呼ばれる API（WriteProcessMemory 等）の呼び出しを監視する。

c. 外部ネットワーク接続判定
　検体が第二のマルウェアのダウンロードや，C&C サーバとの通信を実行するために，外部ネットワークへの接続を行う通信内容を監視する。

上記判定対象の挙動は，マルウェアが不正活動を行う中で現れる場合が多い。このため，これらの挙動の有無を判定することはマルウェアか否かを推定するのに有益である。

3.4 解析結果表示機能

M3AS は，数十種類のサンドボックスでの検体の動作結果をサマリとして表示する機能と，個々のサンドボックスの解析結果を集約して一覧表示する機能とがある。

解析者はサマリ表示機能によって生成された画面を確認することにより，検体の接続先 URL や，作成ファイル，生成プロセス情報の他，16 種類のウイルス対策ソフトのパターンファイルと照合して得られた検知結果を確認することができる。検体がマルウェアであった場合に，ウイルス対策ソフトの検知対応状況や，従業員がそのマルウェアに感染してしまった際に発生する可能性のあるネットワークアクセスの接続先 URL，従業員端末に仕掛けられたトラップ（マルウェア関連ファイル）等を容易に把握することができる。これらの情報を用いてファイアウォールやプロキシ等で接続先 URL への通信を禁止したり，ウイルス対策ソフトのパターンファイルに駆除情報を追加したりすることによって，入口対策をすり抜けて従業員の端末で感染・発症した場合でも，内部対策や出口対策を活用した多層防御が可能となる。また，個々のサンドボックスの解析結果一覧表示機能によって生成された画面（図 2）を確認することにより，サンドボックス単位で検体の活動状況（ファイルアクセス，レジストリアクセス，プロセス操作，ネットワークアクセス）を視覚的に確認することができる。特にネットワークアクセスに関わる活動状況が顕著（赤色表示）だった場合には，ダウンローダ型マルウェア，あるいは C&C サーバと接続するマルウェアである可能性が高い。例えば，Adobe Reader のアプリケーション脆弱性を狙ったマルウェアであった場合，Adobe Reader のインストールされたサンドボックスが他のサンドボックスと比較してネットワークアクセスに関わる活動が顕著に表れる。このように，環境選択型マルウェアを動作させ，その挙動を明らかにするだけでなく，解析結果表示を確認することで，マルウェアが顕現する条件を明らかにすることもできる。

3.5　システム評価

独自に入手したマルウェア疑いの強い検体420種を用いて，M3ASの評価を行った。

（1）サンドボックス構成

本項では，評価に用いたM3ASのサンドボックスについて述べる。今回は表 1 に示す環境条件をさらに詳細化（OS，アプリケーションにバージョンやサービスパックのバリエーションを追加）した39項目の環境条件を用意した。今回はこの39項目の環境条件を組み合わせて46種類のサンドボックスを構築し評価する。

環境条件（例えば物理 PC）に着目し，n番目のサンドボックスの環境に環境条件が一致するか否かを$e_n = \{0(\text{不一致}), 1(\text{一致})\}$として表現した環境条件ベクトル$\mathbf{e}$を以下に定義する。

$$\mathbf{e}_{\text{物理PC}} = (e_1, \cdots, e_{46})$$

環境条件は39項目あることから，39のベクトル$\mathbf{e}$を得る。

（2）解析結果

検体の解析に要した時間，即ち46種類のサンドボックス全てで解析（検体の各サンドボックスへの複製，実行，観測，観測ログ取得，復元の処理）が完了するまでの時間は1検体あたり15 分程度であった。また，今回の解析によって，420 検体×46 種類の 19,320 ファイルの観測ログを取得した。

上記観測ログ中から，外部のサイトへネットワークアクセスした痕跡のあるマルウェアを顕現マルウェア，同じくネットワークアクセスした痕跡のあるサンドボックスを顕現サンドボックスと定義する。その結果，顕現マルウェア数は 291 検体（69.3%），顕現サンドボックス数は 8,335 サンドボックス（43.1%）であった。

ここで顕現状態（例えば検体ID=0123）に着目し，n番目のサンドボックスの環境で顕現したか否かを$m_n = \{0(\text{顕現}), 1(\text{非顕現})\}$として表現した顕現状態ベクトル$\mathbf{m}$を以下に定義する。

$$\mathbf{m}_{\mathbf{0123}} = (m_1, \cdots, m_{46})$$

（3）有効性評価

次に，環境選択型マルウェア（課題 1）に対するM3ASの有効性について評価する。

ここで説明を簡単にするため，ある検体（ID=0123）の解析結果を集計したデータを表 3 に例示して説明する。

図 2　解析結果表示機能（サンドボックス単位）

表 3　検体（ID=0123）におけるサンドボックス環境の解析結果集計例

顕現状態 $\mathbf{m}_{0123}$	物理PC $e_{\text{物理PC}}$	仮想PC $e_{\text{仮想PC}}$	XP e_{XP}	Vista e_{Vista}	Win7 e_{Win7}	Office 2007 $e_{Office2007}$	Office 2010 $e_{Office2010}$	Java 1.4 $e_{Java1.4}$	Java 5 e_{Java5}	一太郎 2013 $e_{一太郎2013}$	一太郎 ビューア $e_{一太郎ビューア}$	…	最大正相関 $\max(r_{0123})$
0	1	0	1	0	0	0	0	0	1	0	0	…	
1	1	0	0	1	0	0	0	0	1	0	0	…	
1	1	0	0	1	0	0	1	0	0	1	0	…	
相関係数 r_{0123}	–	–	**−1.0**	**1.0**	–	–	0.5	–	−0.5	0.5	–	…	**1.0**

各列は検体(ID=0123)における各サンドボックス(本例では 3 種類)の顕現状態ベクトル$\mathbf{m_{0123}}$と，そのサンドボックスの環境条件ベクトル$\mathbf{e}$(本例では 11 項目)を示している。$\mathbf{m_{0123}}$と，各環境条件ベクトル$\mathbf{e}$との相関性が高ければ環境依存度が高い，つまり環境選択型マルウェアの特徴を捉えているといえる。

上記環境選択型マルウェアの存在を M3AS の解析結果より抽出するために，$\mathbf{m_{0123}}$，各環境条件ベクトル$\mathbf{e}$との相関性をピアソン積率相関係数として求めた相関係数ベクトル$\mathbf{r_{0123}}$を表 3 の最下行に示す。本結果より，検体(ID=0123)は Vista 環境のサンドボックスで強い正相関(1.0)が，XP 環境で強い逆相関(−1.0)が確認できる。つまり，検体(ID=0123)は Vista で動作(顕現)し，XP 環境では動作しないことを示す。また相関係数ベクトル$\mathbf{r_{0123}}$の成分の最大値を検体(ID=0123)の最大正相関$\mathbf{max(r_{0123})}$として抽出する(表 3 右端)。

本評価方式を全 46 種類のサンドボックス，全 420 検体に適用する。これにより 46 次元の環境条件ベクトル$\mathbf{e}$を 39 項目分，また，検体毎に 46 次元の顕現状態ベクトル$\mathbf{m}$を 420 検体分，それぞれ得る。420 検体の各顕現状態ベクトル$\mathbf{m}$と環境条件ベクトル$\mathbf{e}$の相関係数から検体毎に最大正相関$\mathbf{max(r)}$を求めて，最大正相関が高い順に 5 検体分を抽出した結果を表 4 に示す。紙面の都合上，39 の環境条件のうち特徴のない項目は省略して表記している。

上記の結果，検体(ID＝1,2,5)の検体は物理 PC($\mathbf{e_{物理PC}}$)との相関係数が著しく高くなっていることから物理 PC 上では動作するものの仮想 PC 上では動作しない検体であることが推定できる。また，検体(ID＝3)は XP($\mathbf{e_{XP}}$)の相関係数が 0.82 となっていることから XP でのみ動作し，Vista や Windows7 では動作しない検体であることが推定できる。さらに，検体(ID＝4)の検体は一太郎 2013($\mathbf{e_{一太郎2013}}$)の相関係数が 0.81 と高い値を示していることから一太郎 2013 がインストールされている PC でのみ動作することが推定できる。実際に，検体(ID＝4)は日本を狙った標的型攻撃で利用されたマルウェア(PlugX[12]の一種)で，一太郎の脆弱性(CVE-2013-5990[13])を悪用したものであることが分かっている[14]。

以上の結果から，M3AS によって特定のソフトウェアがインストールされた環境でしか動作しない環境選択型マルウェアの解析に有効であることが示せた。

4 まとめ

本稿では，近年巧妙化が益々進むマルウェアに対抗するために，多種環境でマルウェアを同時並列的に解析する M3AS の提案を行い，実際のマルウェア 420 種を解析した。これにより，特定の環境でのみ動作(外部サーバへ接続)する環境選択型マルウェアの解析や，環境への依存性を定量的に示すことに成功し，課題 1 を解決した。

M3AS は，ネットワーク再現機能を備え，構成する全機能をハーフラックに構築している。このため，標的とされている組織や顧客先での解析が可能である。これにより外部に検体を提供することなく，また，攻撃対象のネットワーク環境で解析可能である。これにより課題 2，3 の解決が可能となる。

表 4 最大正相関の高い検体の相関係数

検体 ID	物理 PC $\mathbf{e_{物理PC}}$	仮想 PC $\mathbf{e_{仮想PC}}$	XP $\mathbf{e_{XP}}$	Vista $\mathbf{e_{Vista}}$	Win7 $\mathbf{e_{Win7}}$	Office 2007 $\mathbf{e_{Office2007}}$	Office 2010 $\mathbf{e_{Office2010}}$	Java 1.4 $\mathbf{e_{Java1.4}}$	Java 5 $\mathbf{e_{Java5}}$	一太郎 2013 $\mathbf{e_{一太郎2013}}$	一太郎ビューア $\mathbf{e_{一太郎ビューア}}$	最大正相関 max(r)
1	**0.92**	−0.92	−0.04	−0.26	0.07	0.04	0.03	0.00	0.05	0.31	0.21	0.92
2	**0.85**	−0.85	0.08	−0.25	−0.34	−0.03	−0.07	−0.01	−0.05	0.13	0.21	0.85
3	0.01	−0.01	**0.82**	−0.18	−0.22	0.01	0.01	0.12	−0.08	0.06	0.00	0.82
4	0.23	−0.23	0.18	−0.07	0.23	0.29	−0.11	0.36	−0.12	**0.81**	−0.07	0.81
5	**0.80**	−0.80	−0.09	−0.23	−0.01	−0.05	−0.25	−0.07	−0.16	0.18	0.26	0.80

M3AS を活用してマルウェアの環境条件を定量化することにより，顕現の容易性や環境選択型マルウェアの実行可能な環境条件を導出することができる。これらの情報は，例えば人手によるきめ細やかな解析のための解析環境構築の手掛かりにすることができる。

今後は，観測ログ分析機能の強化や，ネットワーク再現機能（WAN 代理接続機能）の開発および評価を行い，上記課題2,3の定量的な評価を行っていく。

謝辞 本稿で試作したシステムの評価にあたっては，総務省実証事業「サイバー攻撃解析・防御モデル実践演習の実証実験の請負」および北陸 StarBED 技術センターの協力を得て実施しています。関係者の方々に感謝いたします。

参考文献

[1] キーマンズネット：企業における情報セキュリティ対策状況，http://www.keyman.or.jp/at/30004867/

[2] NTT Innovation Institute： 2014 NTT Group Global Threat Intelligence Report，http://www.solutionary.com/research/threat-reports/annual-threat-report/ntt-solutionary-global-threat-intelligence-report-2014/

[3] 薗雅紀： マルウェア対策のための研究用データセット ～ MWS 2013 Datasets ～，情報処理学会シンポジウムシリーズ，Vol.2013，CSS2013(MWS2013)，(Oct. 2013)

[4] 新井 悠：アナライジング・マルウェア，オライリー・ジャパン，2010

[5] Claudio “nex” Guarnieri & Cuckoo Sandbox Developers：Automated Malware Analysis － Cuckoo Sandbox，http://www.cuckoosandbox.org/

[6] 株式会社 FFRI：FFRI Dataset 2014 のご紹介， http://www.iwsec.org/mws/2014/files/FFRI_Dataset_2014.pdf

[7] Rodrigo Rubira Branc：Scientific but Not Academical Overview of Malware Anti-Debugging，Anti-Disassembly and Anti-VM Technologies，Black Hat USA Conference 2012

[8] 松木隆宏：CCC DATAset 2009 によるマルウェア配布元の可視化， Vol2009，pp1-6，CSS2009（MWS2009），（Oct，2009）

[9] 株式会社ラック：日本における水飲み場型攻撃に関する注意喚起，http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html

[10] IPA ： 脆弱性対策情報データベース，http://jvndb.jvn.jp/

[11] Thomas Hungenberg & Matthias Eckert： INetSim Internet Services Simulation Suite，http://www.inetsim.org/index.html

[12] TREND MICRO：標的型攻撃に利用される「PlugX」を徹底解析，http://blog.trendmicro.co.jp/archives/6026

[13] Common Vulnerabilities and Exposures: CVE-2013-5990，http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5990

[14] naked security：From the Labs: New PlugX malware variant takes aim at Japan，http://nakedsecurity.sophos.com/2013/12/04/new-plugx-malware-variant-takes-aim-at-japan/