Vol.2015-CSEC-69 No.3
Vol.2015-IOT-29 No.3
2015/5/21

マルウェア解析向け通信制御システムの開発

重本倫宏[†1]　徳山喜一[†1]　下間直樹[†1]　林直樹[†1]　鬼頭哲郎[†1]　仲小路博史[†1]

近年，民間企業や，防衛関連企業，衆参両院を狙ったサイバー攻撃が顕在化しており，個人，企業，国家の利益や安全性を損なうリスクが高まっている．マルウェアの中には，悪性なプログラムが設置されたサイトからプログラムコードを取得・実行し，機能拡充を行うものが存在する．このため，攻撃の全貌を明らかにするためには，インターネットに接続させた状態でマルウェア解析を行う必要がある．しかし，マルウェアのインターネット通信をすべて許可すると，解析環境が外部に攻撃を行う可能性がある．本研究では，限定的にマルウェアの通信を許可しながら，マルウェア解析を行う通信制御システムを開発した．本稿では，開発した通信制御システムと，その評価結果について報告する．

Development of Malware Traffic Control System for Malware Analysis

TOMOHIRO SHIGEMOTO[†1]　KIICHI TOKUYAMA[†1]　NAOKI SHIMOTSUMA[†1]
NAOKI HAYASHI[†1]　TETSURO KITO[†1]　HIROFUMI NAKAKOJI[†1]

As the malware used in targeted attacks has grown more advanced in recent years, the number of cases where existing inbound measures have failed to detect attacks and allowed incursions into the organization has increased. It has been confirmed that “downloader” malware exists that downloads secondary malware from a malware distribution server prepared by the attacker, so that the attack can be carried out in stages. So, it is necessary to be connected to the Internet, and to analyze malware. But if all the malware connection is permitted, malware analysis environment may attack outside services. In this paper, we develop and evaluate Malware Traffic Control System which controls attack.

1. はじめに

近年，民間企業や，防衛関連企業，衆参両院を狙ったサイバー攻撃が顕在化しており，個人，企業，国家の利益や安全性を損なうリスクが高まっている．また，攻撃手法も益々巧妙化しており，標的型攻撃，特に APT（Advanced Persistent Threat）攻撃[1]は，秘密裏に，そして執拗に長期間攻撃を続ける点で従来の脅威とは性質が異なる．さらに近年では，新種のマルウェアの半数以上が既存のウイルス対策ソフトでは検知できないと報告されている[2]．このような状況下でマルウェアが組織の中に侵入してしまった場合には，侵入したマルウェアの特性を解明して被害拡大防止策を講じることが重要となる．

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が，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が増えている[3,4]．このような背景から，報告者らのグループでは，複数種類の動的解析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[5,6]．

報告者らが開発している M3AS の概要を図 1 に示す．

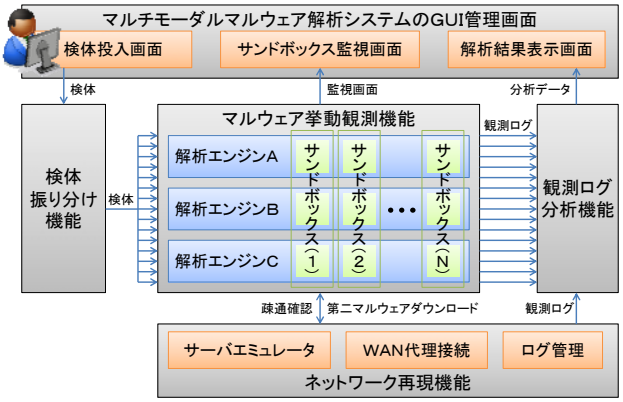

図 1　マルチモーダルマルウェア解析システムの概要

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．解析環境の構築にあたっては，公開された脆弱性情報や攻撃傾向に基づいてマルウェアが動作しやすい環境を選定している．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．

現行の M3AS 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」[7]を用いた解析を前提としている．しかし，マルウェアの中には，攻撃者が用意した

†1 (株)日立製作所
Hitachi Ltd.

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．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（以下, 水飲み場攻撃）まで確認されている[9,10]. このため，攻撃者による攻撃の全貌を明らかにするためには，インターネットに接続させた状態でマルウェア解析を行う必要がある．しかし，マルウェアのインターネット通信をすべて許可すると，解析環境が外部に攻撃を行う可能性がある．

そこで，報告者らは，限定的にマルウェアの通信を許可しながら，マルウェア解析を行うマルウェア通信制御システムの開発を行った．本報告では，開発したマルウェア通信制御システムと，マルウェア通信制御システムの評価結果について述べる．

2. 関連研究

インターネットに接続してマルウェア解析を行う解析システムとして， Botnet Watcher[11]が挙げられる．Botnet Watcher では，GateKeeper と呼ばれるモジュールが，解析環境とインターネットとの間の通信を仲介しており，C&C サーバとの通信や，HTTP によるファイルダウンロードの通信であると判断された場合に実インターネットと接続を行う．また，解析環境で観測されたマルウェアの通信の中から危険性が低いと判断された通信に関して，インターネット接続を許可して解析を行うマルウェア動的解析システムも提案されている[12].

しかし，未知のマルウェアを対象とする以上，完全に攻撃を検知・遮断することは困難である．また，前章で述べたような水飲み場攻撃を解析することが出来ない. そこで，本研究では，上記の課題を解決するための提案を行う．

3. マルウェア通信制御システムの提案

本章では，限定的にマルウェアの通信を許可しながら，マルウェア解析を行うマルウェア通信制御システムを提案する．まず，3.1 節では，マルウェア通信制御システムの要件を説明する．3.2 節では，前節で示された要件を満たす方式として提案手法を説明する．3.3 節では，提案システムの実装を説明する．

3.1 マルウェア通信制御システムの要件

報告者らは，マルウェア通信制御システムを提案するにあたり，マルウェアの通信制御に求められる要件を整理した．以下に要件を説明する．

【要件 1】外部への攻撃を抑制すること

マルウェアによる通信をすべて許可すると, 解析環境が攻撃（DoS 攻撃や，SPAM 発信等）に加担してしまう可能性がある．外部への攻撃が露呈すると，企業イメージが損なわれてしまったり，場合によっては訴訟を起こされたりする場合がある．このため，マルウェア通信制御システムには，外部への攻撃を抑制する機能を持たせることとする．

【要件 2】マルウェアダウンロード通信を許可すること

ダウンローダ型マルウェアが行う攻撃の全貌を把握するためには，マルウェア配布サーバからダウンロードしてくる第二のマルウェアを解析する必要がある．このため，マルウェア通信制御システムには，マルウェアのダウンロード通信を判別し，当該通信を許可する機能を持たせることとする．

【要件 3】水飲み場攻撃を解析すること

1 章で述べたように，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マルウェア解析を回避する水飲み場攻撃が確認されている．このようなマルウェアを解析するには，マルウェア解析システムを攻撃対象の組織内に設置する方法がある．しかし，すべての組織内にマルウェア解析システムを設置するのはコスト面から困難である．このため，マルウェア通信制御システムには，送信元の IP アドレスを制御し，攻撃対象の組織内ネットワークから通信する機能を持たせることとする．

【要件 4】多数の解析環境の通信を制御すること

報告らが研究している M3AS では，環境依存型のマルウェアを解析するために，多数の解析環境を用いてマルウェア解析を行う．このため，マルウェア通信制御システムには，多数の解析環境からのマルウェア通信を制御する機能を持たせることとする．

3.2 マルウェア通信制御システムの提案

本節では，3.1 節で整理した要件に基づきマルウェア通信制御システムを提案する．以下に，各要件に対する対応方針を述べる．

【要件 1】への対応として，通信抑制を行うモジュールを開発する．通信抑制モジュールでは，外部への攻撃を検知すると，トラフィックの遮断や，帯域制限を行う．

【要件 2】への対応として，ダウンローダ通信を判定するモジュールを開発する．

【要件 3】への対応として，IP アドレスを管理するモジュールを開発する．IP アドレス管理モジュールは，インターネットに接続する際の送信元 IP アドレスの管理を行う．

【要件 4】への対応として，キャッシュ管理を行うモジュールを開発する．キャッシュ管理モジュールでは，多数の解析環境から送信されるマルウェア通信の管理を行う．

提案するマルウェア通信制御システムを図 2 に示す．

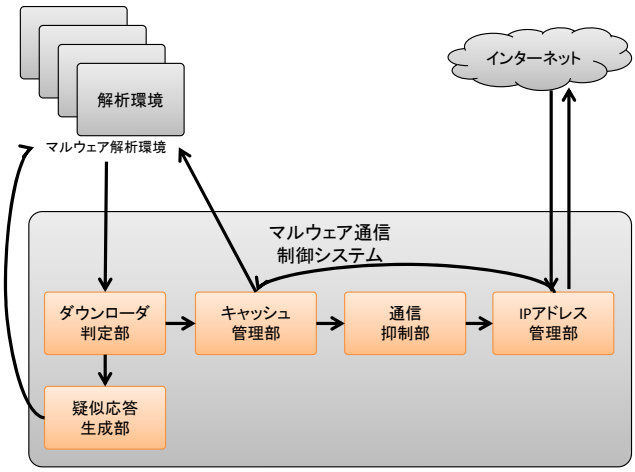

図 2　マルウェア通信制御システムの概要

マルウェア通信制御システムは，以下の 5 つのコンポーネントから構成される．

(1)　ダウンローダ判定部

ダウンローダ判定部では，マルウェアの通信がダウンローダによる通信か否かの判定を行う．ダウンロード通信でない場合は疑似応答生成部に通信を転送し，ダウンロード通信であればキャッシュ管理部に通信を転送する．なお，ダウンローダによる通信か否かは，疑似応答生成部が応答する実行ファイルによる通信を観測することで行う．

(2)　擬似応答生成部

疑似応答生成部では，ダウンロード要求に対して，マルウェア通信制御システムへ通信を行う実行ファイルを生成し，解析環境に送信する．

(3)　キャッシュ管理部

キャッシュ管理では，インターネットからダウンロードしたファイルをキャッシュする．キャッシュされているファイルに対するダウンロード要求はキャッシュ管理部が応答する．

(4)　通信抑制部

通信制御部では，外部への攻撃を検出した際に，ポリシに応じたトラフィック抑制を行う．なお，通信抑制部の構築には，IPS を用いる．

(5)　IP アドレス管理部

IP アドレス管理部では, IP アドレスを変更して通信を行う．水飲み場攻撃を解析するため，場合によっては IP アドレス管理部を解析対象の組織の中に配置する．

マルウェア解析の流れを図 3 に示す．

1.　ダウンローダ判定部は解析環境からファイルダウンロード要求を受信すると, 自身の持つ URL リストと比較を行い，URL リストに当該通信先が存在しない場合には，ダウンローダでないと判断し，当該 URL を URL リストに格納し，疑似応答生成部へ疑似応答生成要求を送信する．
2.　疑似応答生成部は，ダウンローダ判定部から疑似応答生成要求を受信すると，マルウェア通信制御装置へ通信を行う疑似プログラムを生成し，解析環境へ応答する．
3.　解析環境は，疑似応答生成部から応答された疑似プログラムを実行する．

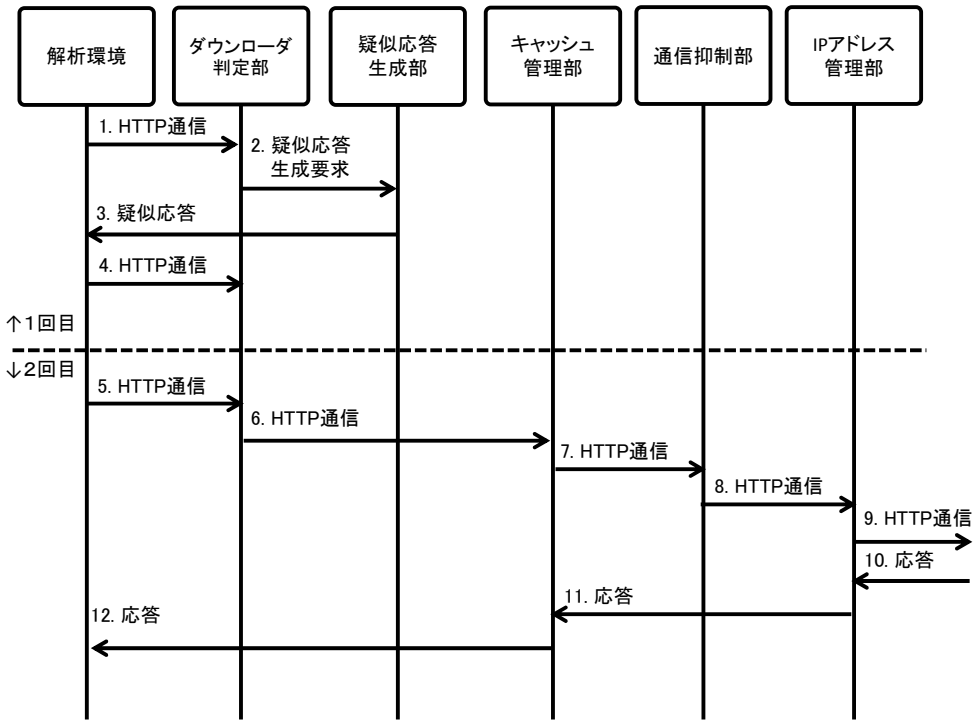

図 3　マルウェア解析の流れ

4. 解析環境で実行された,疑似プログラムからの HTTP 要求を受信したダウンローダ判定部は，当該通信をダウンロード要求と判定し，URL リストへ記録する．
5. ダウンロード判定部は，解析環境からファイルダウンロード要求を受信すると,自身の持つ URL リストと比較を行い,当該 URL がダウンロード要求として登録されている場合は，ダウンロード要求をキャッシュ管理部へ転送する．
6. キャッシュ管理部は，ダウンローダ判定部からダウンロード要求を受信すると，キャッシュ管理部にキャッシュされているかどうかの判定を行う．キャッシュされていない場合は，ダウンロード要求を通信抑制部へ転送する．
7. 通信抑制部は，キャッシュ管理部から受信したダウンロード要求に攻撃パケットが含まれていないか確認を行う．攻撃パケットが含まれていない場合は，ダウンロード要求を IP 管理部へ転送する．
8. IP アドレス管理部は，通信抑制部から受信したダウンロード要求に対し，IP アドレスの変更を行う．
9. IP アドレス管理部は，ダウンロード要求をインターネットへ送信する．
10. IP アドレス管理部は，インターネットから応答を受信すると，キャッシュ管理部へ応答を転送する．
11. キャッシュ管理部は，IP アドレス管理部から応答を受信すると，当該応答を自身の持つキャッシュデータに格納する．
12. キャッシュ管理部は，解析環境へ応答を送信する．

3.3 マルウェア通信制御システムの実装

本節では，マルウェア通信制御システムの実装について述べる．マルウェア通信制御システムの各機能と，それらの機能を具備するサーバの関係を図 4 に示す．

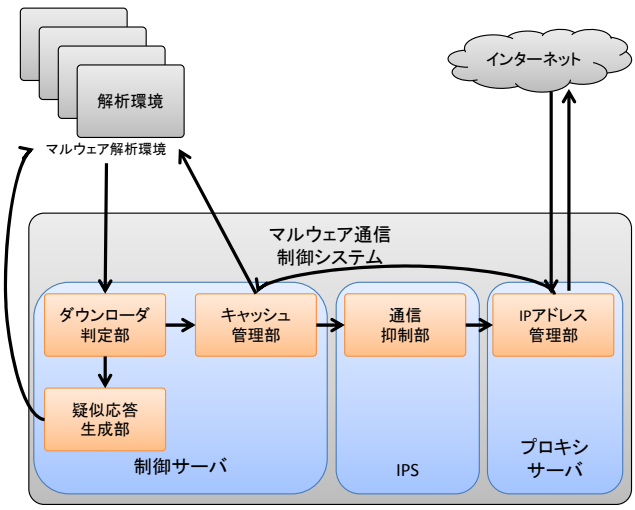

図 4 マルウェア通信制御システムの実装

マルウェア通信制御システムの機能のうち，通信抑制部は IPS（snort[13]）を用いて，IP アドレス管理部は，プロキシサーバ（squid[14]）を用いて構成する．以下では，実装した制御サーバについて述べる．

(1) ダウンローダ判定部の実装

ダウンローダの通信であるかどうかを判定するダウンローダ判定部は，HTTP 通信を制御するために，man-in-the-middle 型のプロキシサーバである mitmproxy[15]を用いて実装した．具体的には，解析環境からインターネット向けの通信を受信すると，URL リストデータにアクセス先の URL を記録する．また，解析環境からマルウェア通信制御システム向けの通信を受信すると,当該 URL のパス部分を URL リストデータと比較し，一致する URL が存在する場合に，ダウンローダの通信であると判定するようにした．

(2) 疑似応答生成部の実装

疑似応答生成部には，ダウンローダのダウンロード要求に対して,どの URL へのダウンロード要求かが判別可能な識別子を埋め込んだ実行ファイルを生成する機能を実装した．具体的には，マルウェア通信制御システムへ通信を行う，ベースプログラムを用意しておき，ダウンロード要求があるたびに，ベースプログラムの一部を動的に変更したファイルを，ダミーファイルとして応答する（図 5）．

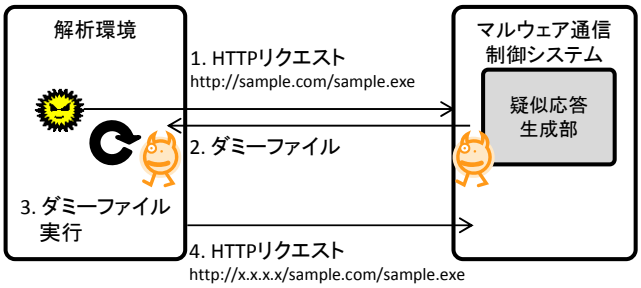

図 5 ダミーファイルの動的生成

解析環境上でダミーファイルが実行されると，マルウェア通信制御システムへ HTTP リクエストが送信される．これにより,どの URL へのアクセスがダウンローダによるダウンロード要求かが判別可能となる．

(3) キャッシュ管理部の実装

キャッシュ管理部は，ダウンローダ判定部と同様 mitmproxy を用いて実装した．具体的には，インターネットからの応答を URL ごとにキャッシュリストデータを用いて管理し,同じ URL に対して再度アクセスがあった場合には，キャッシュリストデータに格納されたデータを応答するようにした．

4. 評価実験

本章では，開発したマルウェア通信制御システムの評価結果について述べる．

4.1 評価目的

マルウェア通信制御システムは，外部への攻撃を抑制しながらマルウェアの解析を行うシステムである．マルウェア通信制御システムを以下の観点で評価する．

(1) マルウェア通信制御システムの性能について

マルウェア通信制御システムは，多数の解析環境を有する M3AS での利用を前提にしている．このため，複数の解析環境から発生する通信を制御する性能を有しているか評価する．

(2) マルウェア通信制御システムの有効性について

マルウェア検体の中にどの程度ダウンローダが存在するのか，また，マルウェア通信制御システムを用いることで，どの程度新たな脅威が明らかになるのか，マルウェア通信制御システムの有効性を評価する．

4.2 評価方法

(1) 性能評価について

負荷発生ツール（JMeter[16]）を用いて，同時接続数を変化させながら，マルウェア通信制御システムの応答時間を評価する．なお，評価に用いたマルウェア通信制御システム（制御サーバ）の性能を表 1 に示す．

表 1 制御サーバの性能

項目	性能
OS	Ubuntu 14.04
CPU	Intel Xeon CPU 3.0GHz
Memory	512MB

(2) 有効性評価について

2015 年 2 月に入手した検体（634 検体）を用いて，ダウンローダ検体数を評価する．

4.3 評価結果

(1) 性能評価結果

同時接続数を変化させながら計測した，平均応答時間を図 6 に，接続に失敗した割合（エラー率）を図 7 に示す．なお，平均応答時間の計測に当たり，最も負荷が高くなる疑似応答生成に要した平均応答時間を計測した．

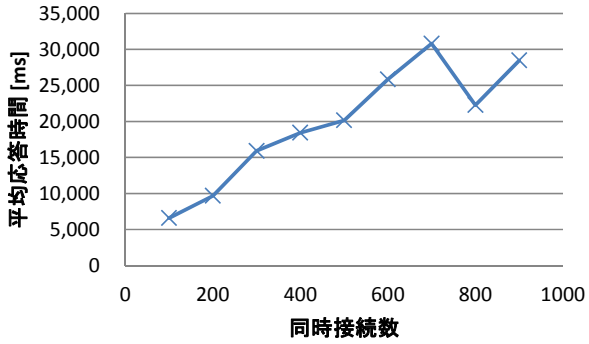

図 6 平均応答時間

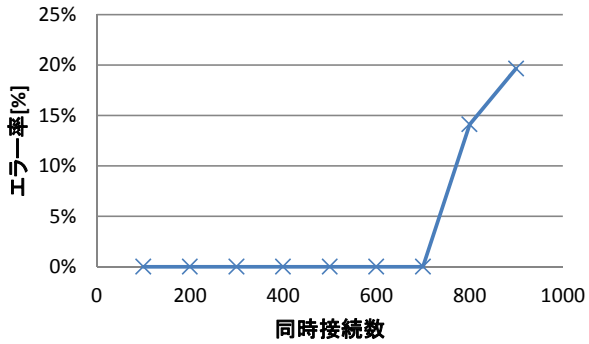

図 7 エラー率

図 7 より，同時接続数が 700 まではエラー率 0%で推移していることが分かる．これより，700 個の解析環境による同時接続に耐えられることが分かった．これは，M3AS（約 70 解析環境）の 10 倍程度の規模まで耐えられることを表す．

(2) 有効性評価結果

634 検体のマルウェアのうち，不審なホストへアクセスした検体数と，ダウンローダとして判定された検体数を表 2 に示す．なお，不審なホストとは，検体がアクセスしたホストのうち，microsoft.com 等の正規のホストへのアクセスを除いたものを表す．

表 2 マルウェア解析結果

項目	検体数	割合[%]
不審ホストへ通信した検体	545	86.0
ダウンローダと判定された検体	53	8.4

今回評価に用いたマルウェアのうち，86.0%の検体において不審なホストへのアクセスが見られ，8.4%の検体がダウンローダだと判定された．また，不審ホストとして，396 件の URL が観測され，そのうち，26 件がダウンローダによる通信先だと判定された．そこで，26 件のダウンローダの通信先に接続し，ダウンロードを行った結果を表 3 に示す．

表 3　ダウンロード結果

ダウンロードファイル	件数	割合[%]
実行ファイル	5	19.2
HTML	7	27.0
応答なし	14	53.8

26 件の接続先の内，5 件の接続先に関して，実行ファイルがダウンロードできた．応答がなかったものは，既にホスト自体にアクセスできず，HTML がダウンロードできたものは，ホストにはアクセスできたが，ファイルが削除されていたことを表す．なお，インターネットから得られた 5 件のファイルに対して動的解析を行ったところ，新たに，53 件の不審ホストへの接続が確認できた．

以上の結果より，マルウェア通信制御システムを用いることで，新たな不審ホストの情報を得ることができ有効性が確認できた．

4.4 考察

評価では，2 月に入手した検体に対して，インターネットからのファイルダウンロードを 3 月に実施した．時間経過により検体が削除される可能性が高まるため，19.2%しかダウンロードに成功しなかったと考えられる．検体を入手した時点で解析を行えば，マルウェアのダウンロード成功率は向上すると考える．

また，ダウンローダの中には，ダウンロードしたファイルのハッシュ値を，マルウェアの中にあらかじめ保持しているハッシュ値と比較し，ダウンロードの成否を確認するものが存在する[17]．このようなダウンローダは，疑似応答部で生成したダミーファイルを実行しないため，マルウェア通信制御システムではダウンローダとして判定されない．一回目の通信に関しては疑似応答生成部が応答を生成するが，当該 URL に対して再びダウンロード要求が発生した際に，ダウンローダと判定されていなくても通信を許可するようにすれば，この問題を解決できると考える．

5. おわりに

本稿では，攻撃者の攻撃活動全貌を明らかにするために，外部への攻撃を抑制しつつ，マルウェア解析を行うマルウェア通信制御手法を提案した．また，提案した手法を実装したプロトタイプシステムを開発した．さらに，プロトタイプシステムを用いた評価実験により 634 検体のマルウェアうち，8.4%（53 検体）がダウンローダであることを確認した．本提案手法は，侵入したマルウェアの特性解明に有効であると考える．

今後は，企業の IP アドレスを用いた評価を行い，水飲み場攻撃の解析を行う．

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請負」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) IPA: 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
2) Symantec: Antivirus software is dead, says security expert at Symantec, http://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec
3) Rodrigo Rubira Branc: Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti-VM Technologies, Black Hat USA Conference 2012.
4) Chen,X., Andersen,J., Mao,Z.M. et al.: Towards an Understanding of Anti-Virtualization and Anti-Debugging Behavior in Modern Malware, The 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp.177‐186(2008).
5) 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).
6) 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).
7) Thomas Hungenberg & Matthias Eckert: INetSim Internet Services Simulation Suite, http://www.inetsim.org/index.htm
8) 柏井祐樹, 森井昌克, 井上大介ほか: NONSTOP データを用いたマルウェアの時系列分析, コンピュータセキュリティシンポジウム 2013 論文集, pp848-853(2013).
9) Emurasoft: 今回のハッカーによる攻撃の詳細について, https://jp.emeditor.com/general/今回のハッカーによる攻撃の詳細について/
10) 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
11) 青木一史, 川古谷裕平, 岩村誠 , 伊藤光恭: 半透性仮想インターネットによるマルウェアの動的解析, コンピュータセキュリティシンポジウム 2009 (CSS2009) 論文集, pp 1-6(2009).
12) K. Yoshioka, T. Kasama, T. Matsumoto: Sandbox Analysis with Controlled Internet Connection for Observing Temporal Changes of Malware Behavior, The Fourth Joint Workshop on Information Security (JWIS 2009).
13) CISCO: Snort.org, https://www.snort.org/contact
14) squid-cache.org: Squid: Optimising Web Delivery, http://www.squid-cache.org/
15) Aldo Cortesi: mitmproxy, https://mitmproxy.org/
16) Apache Software Foundation: Apache JMeter, http:// http://jmeter.apache.org/
17) 本城信輔: PC のウイルスを根こそぎ削除する方法, 技術評論社(2011).