情報処理学会論文誌 Vol.57 No.9 2012–2020 (Sep. 2016)

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,a)] 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]

受付日 2015年12月3日, 採録日 2016年6月2日

概要：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，機能拡充を行うダウンローダ型マルウェアが存在する．このような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，マルウェアが行うインターネット通信をすべて許可すると，解析により，外部組織に被害が発生する可能性がある．本稿では，ダウンローダ型マルウェアが行うダウンロード通信を検知し，当該通信のみをインターネットに接続しながら，マルウェア解析を行う通信制御手法を提案する．また，実際のマルウェアを用いた評価実験により，提案手法の有効性を評価する．

キーワード：マルウェア解析，動的解析，通信制御

Development of Malware Traffic Control System for Malware Analysis

Tomohiro Shigemoto[1,a)] Kiichi Tokuyama[1] Naoki Shimotuma[1]
Naoki Hayashi[1] Tetsuro Kito[1] Hirofumi Nakakoji[1]

Received: December 3, 2015, Accepted: June 2, 2016

Abstract: 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.

Keywords: malware analysis, dynamic analysis, traffic control

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，国家それぞれ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る．マルウェアの動的解析にあたっては，マルウェア解析者が Sysinternals [3] 等のツールを使用して手作業で解析する方法や，解析を支援する動的解析サービス，動的解析ソフトウェアを利用する方法等がある．オンラインサービスでは Anubis [4] や，ThreatExpert [5] が，オフラインツールでは，Cuckoo Sandbox [6] や，Threat Analyzer [7]，Yarai Analyzer [8] が提供されている．また，報告者らの

[1] 株式会社日立製作所
Hitachi Ltd., Yokohama, Kanagawa 244–0817, Japan
[a)] tomohiro.shigemoto.jh@hitachi.com

グループでは，複数種類の解析環境を用いてマルウェアを多角的に動的解析する多種環境マルウェア動的解析システム（Multi-modal Malware Analysis System）[9], [10] の研究を進めている．

マルウェアの中には，攻撃者が用意したマルウェア配布サーバから第 2 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 [11] が存在する．また，マルウェア配布サーバの中には，攻撃の正体を隠ぺいするため，マルウェアがダウンロードできるのは，最初のアクセス 1 回のみで，同じ IP アドレスからアクセスすると，2 回目以降は正規サイトに誘導されるものも存在する [12]．さらに，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，クローキング）も確認されている [13], [14]．

このため，マルウェア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動的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（インターネット上のサーバ等）に攻撃を行い，被害が発生してしまう恐れがある．

そこで本稿では，ダウンローダ型マルウェアの通信（以下，MW ダウンロード通信）を検出し，当該 MW ダウンロード通信のみをインターネットに接続させることにより，マルウェアによる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システムを提案する．

まず，2 章では関連研究について述べ，3 章でマルウェア通信制御システムを提案する．4 章で提案手法の実装について説明し，5 章で実マルウェアを用いた評価実験を行う．そして最後に 6 章でまとめを述べる．

2. 関連研究

動的解析ツールを用いてマルウェアの解析を行う場合，インターネットから隔離した閉塞環境で解析を行う方法と，インターネットに接続した環境でマルウェア解析を行う方法が存在する．

閉塞環境での解析は，外部への攻撃を抑制することができ，ネットワークアクセスをともなわないマルウェアの解析には有効な方法である．しかし，近年の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し，隔離された環境では本来の挙動を示さないものも存在する．青木らも閉塞環境よりもインターネットに接続した環境の方がより多くの動的解析結果が得られると報告している [15]．そこで，ネットワーク環境をエミュレートすることで，マルウェアに対して疑似的なインターネット環境を提供する手法が提案されている [16]．しかし，疑似インターネット環境を利用した解析手法では，ダウンローダ型マルウェアのように，インターネットを介して第 2 のマルウェアをダウンロードするマルウェアの解析を行うことはできない．

一方，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 [15] があげられる．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インターネットと接続する．しかし，上記手法は，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を装った外部への攻撃を抑制することができない．また，Kreibich ら [17] は，通信フローごとに，ポリシに従って通信可否の制御を行う GQ honyform というシステムを提案している．しかし，Kreibich らの手法ではポリシの生成方法を言及しておらず，ポリシの決定は解析を行う管理者にゆだねられている．Yoshioka ら [18] は，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，順次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を提案している．しかし，Yoshioka らの手法は未知の脆弱性を突く外部への攻撃を抑制できない．

そこで，本稿では，MW ダウンロード通信を判定し，当該 MW ダウンロード通信のみをインターネットに接続させるマルウェア通信制御システムを提案する．提案手法の新規性は，ダウンローダ型マルウェアの挙動に着目して MW ダウンロード通信を判定するところにあり，従来技術では防げなかった外部への攻撃（HTTP ダウンロード通信を装った攻撃や，未知の脆弱性を突く攻撃）を抑制できることが提案手法の優位性である．提案手法と既存技術との比較を**表 1** にまとめる．

表 1 既存技術との比較
Table 1 Technical comparison with existing countermeasures.

	提案手法	青木ら[15]	Kreibich ら [17]	Yoshioka ら [18]
概要	MW ダウンロード通信のみを接続	C&C 通信や HTTP ダウンロード通信を接続	管理者の定めるポリシに従い接続	危険性が低いと判断された通信を接続
許可する通信の判定方法	MW ダウンロード通信の判定結果を利用	プロトコル識別結果を利用	管理者の定めるポリシを利用	統計検査，セッション検査，脆弱性検査の結果を利用
外部攻撃の少なさ	○（攻撃なし）	×（例：HTTP ダウンロードを装った攻撃）	-（管理者の定めるポリシに依存）	×（例：未知の脆弱性を突く攻撃）

3. マルウェア通信制御システムの提案

本章では，MW ダウンロード通信を検出し，当該 MW ダウンロード通信のみをインターネットに接続させるマルウェア通信制御システムを提案する．

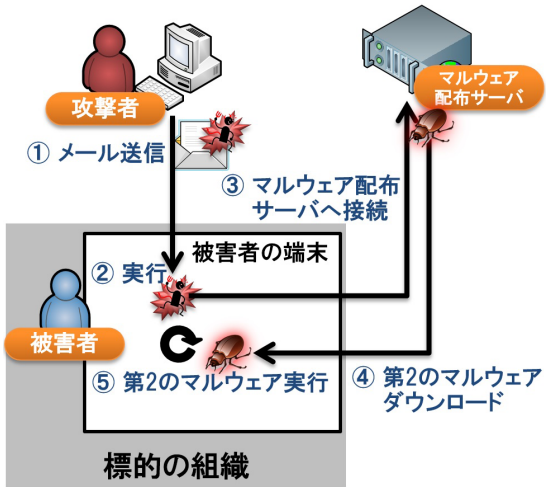

図 1 ダウンローダ型マルウェアを用いた攻撃の流れ
Fig. 1 Flow of attack using downloader.

3.1 MW ダウンロード通信判定手法

ダウンローダ型マルウェアとは，第 2 のマルウェアをダウンロードして実行するタイプのマルウェアであり，IPA の報告 [19] によると，2015 年第 4 四半期に最も多く検出された不正プログラムである．ダウンローダ型マルウェアは，多くの場合メールに添付して送られ，本命マルウェア（第 2 のマルウェア）に感染させるために利用される．

ダウンローダ型マルウェアを用いた攻撃の流れを図 **1** に示す．

ダウンローダ型マルウェアを用いた攻撃では，まず攻撃者がダウンローダ型マルウェアを添付したメールを被害者に送付する（図 1 中①）．被害者が誤って添付されたダウンローダ型マルウェアを実行（図 1 中②）してしまった場合，ダウンローダ型マルウェアは，攻撃者が用意したマルウェア配布サーバへ接続（図 1 中③）し，第 2 のマルウェアをダウンロード（図 1 中④）する．さらに，ダウンローダ型マルウェアは，ダウンロードしてきた第 2 のマルウェアを実行（図 1 中⑤）し，第 2 のマルウェアに感染させる．マルウェア配布サーバへの接続から，第 2 のマルウェアの実行（図 1 中③～⑤）は，ダウンローダ型マルウェアの働きによるものであり，被害者が気付かないうちに，第 2 のマルウェアに感染してしまう．

提案するマルウェア通信制御システムでは，ダウンローダ型マルウェアがマルウェア配布サーバから実行ファイル（第 2 のマルウェア）を取得し，実行する機能を備えている点（図 1 中③～⑤）[20] に着目し，この動きを利用して，MW ダウンロード通信の判定を行う．MW ダウンロード通信判定の流れを図 **2** に示す．

マルウェア通信制御システムが，解析環境からインターネット向けの HTTP 通信を受信すると，マルウェア通信制御システムに通信を行う疑似プログラムを生成し，解析環境に応答する．解析環境上でこの疑似プログラムが実行されると，マルウェア通信制御システムへ通信が行われるため，先ほどの HTTP 通信が MW ダウンロード通信であると判定できる．本判定手法により，解析環境に手を加えることなく，MW ダウンロード通信の判定が可能となる．

なお，1 章で述べたように，マルウェア配布サーバの中には，解析回避機能（クローキング等）を備えたものも存在する．このような解析回避機能への対応については，5.4 節で述べる．

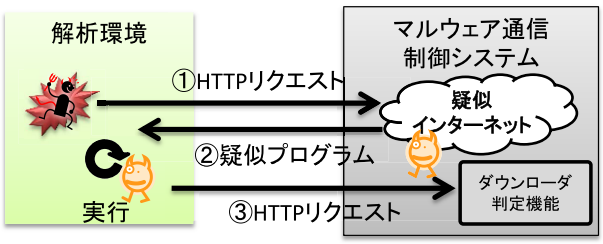

図 2 MW ダウンロード通信判定の流れ
Fig. 2 Flow of MW download connection determination.

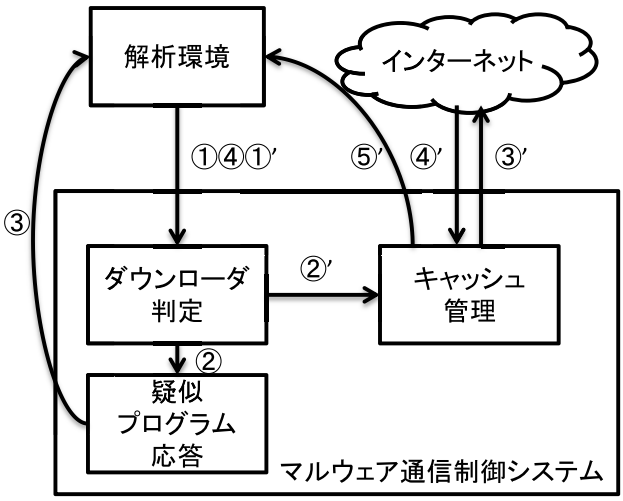

図 3 マルウェア通信制御システムの概要
Fig. 3 Overview of the malware traffic control system.

3.2 提案システムの概要

提案するマルウェア通信制御システムの概要を図 **3** に示す．

提案するマルウェア通信制御システムは，以下 3 つの機能から構成される．なお，これらの機能の詳細については，3.3 節で述べる．

(1) ダウンローダ判定
マルウェアの通信がダウンローダ型マルウェアによる MW ダウンロード通信か否かの判定を行う機能

(2) 疑似プログラム応答
MW ダウンロード通信の判定を行うために，疑似的なプログラムを生成し応答する機能

(3) キャッシュ管理
インターネットからダウンロードした第 2 のマルウェアをキャッシュする機能

マルウェア通信制御システムは，2つのフェーズを用いた解析により，マルウェアの通信を制御する．1つ目のフェーズ（図 3 中①～④）では，マルウェアが行う通信が MW ダウンロード通信か否かの判定を行い，2つ目のフェーズ（図 3 中①'～⑤'）では，インターネットから第 2 のマルウェアをダウンロードし，解析する．

まず，フェーズ 1 における解析の流れを説明する．ダウンローダ判定機能は解析環境から通信を受信（図 3 中①）すると，当該通信が MW ダウンロード通信か否かの判定を行う．MW ダウンロード通信でないと判定された場合には，疑似プログラム応答機能へ，疑似プログラム生成要求を送信（図 3 中②）する．疑似プログラム応答機能は，ダウンローダ判定機能から疑似プログラム生成要求を受信すると，マルウェア通信制御システムへ通信を行う疑似プログラムを生成し，解析環境へ応答（図 3 中③）する．解析環境は，疑似プログラム応答機能から応答された疑似プログラムを実行し，マルウェア通信制御システムへ通信（図 3 中④）を行う．マルウェア通信制御システムは，当該通信を観測することにより，先ほどの通信（図 3 中①）が MW ダウンロード通信であったことを検出する．

続いて，フェーズ 2 における解析の流れを説明する．ダウンロード判定機能は，解析環境から通信を受信（図 3 中①'）すると，当該通信が MW ダウンロード通信か否かの判定を行う．MW ダウンロード通信であると判定された場合には，通信をキャッシュ管理機能へ転送（図 3 中②'）する．キャッシュ管理機能は，ダウンローダ判定機能から MW ダウンロード通信を受信すると，当該通信に対する応答が，キャッシュ管理機能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，MW ダウンロード通信をインターネットへ送信（図 3 中③'）する．キャッシュ管理機能は，インターネットからの応答を受信（図 3 中④'）すると，当該応答を自身の持つキャッシュデータに格納し，解析環境へ応答（図 3 中⑤'）する．

以上のように，2つのフェーズに分けて解析を行うことにより，MW ダウンロード通信の検出と，当該 MW ダウンロード通信のみをインターネットに接続させるマルウェア通信制御システムを実現することが可能となる．

3.3 提案システムの詳細

続いて，提案システムを構成する 3 つの機能について，その詳細を説明する．

(1) ダウンローダ判定

ダウンローダ判定機能では，**表 2** に例示するダウンローダ判定リストを用いて，マルウェアの通信がダウンローダ型マルウェアによる MW ダウンロード通信か否かの判定を行う．ダウンローダ判定リストは，判定対象 URL と判定結果の組合せからなり，判定結果が 1 の場合は該当する判定対象 URL への通信が MW ダウンロード通信であると判定し，判定結果が 0 の場合は該当する判定対象 URL への通信が MW ダウンロード通信ではないと判定することを表す．具体的には，解析環境からインターネット向けの HTTP 通信を受信すると，ダウンローダ判定リストの判定対象 URL にアクセス先の URL が存在するか否かを検査し，ダウンローダ判定リストにアクセス先の URL が存在し，かつ，判定結果が 1（MW ダウンロード通信であると判定される）の場合には，キャッシュ管理部へ通信を転送する．ダウンローダ判定リストの判定対象 URL にアクセス先が存在しない，あるいは，アクセス先は存在するが判定結果が 0（MW ダウンロード通信ではないと判定される）の場合は，疑似プログラム応答機能へ疑似プログラム生成命令を送信する．なお，このとき，ダウンローダ判定リストの判定対象 URL にアクセス先が存在しない場合には，当該アクセス先をダウンローダ判定リストに登録し，判定結果に 0 を設定する．

また，疑似プログラム実行による通信を受信すると，当該 URL のパス部分をダウンローダ判定リストの判定対象 URL と比較する．一致する URL が存在する場合に，判定結果を 1 に設定し，以後，当該 URL への通信は MW ダウンロード通信として判定する．

表 2 の例では，「http://example.com/example.exe」への通信が MW ダウンロード通信として判定される．

(2) 疑似プログラム応答

疑似プログラム応答機能では，マルウェアが行う通信に対して，マルウェア通信制御システムへ通信を行う疑似プログラムを生成し，解析環境に応答する．具体的には，マルウェアが行う通信に対して，どの URL への通信かが判別可能な識別子を動的に埋め込んだ疑似プログラムを生成し，応答する（**図 4**）．

疑似プログラム応答機能は，マルウェアによるインター

表 2 ダウンローダ判定リストの例
Table 2 Example of the downloader determination list.

判定対象 URL	判定結果
http://example.com/example.exe	1
http://example.net/abc.exe	0

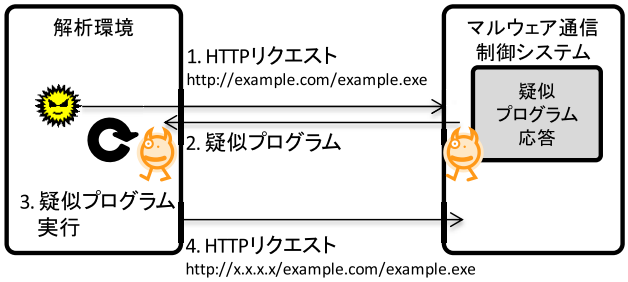

図 4 疑似プログラムの応答
Fig. 4 Response of the pseudo program.

```
        +0 +1 +2 +3 +4 +5 +6 +7 +8 +9 +A +B +C +D +E +F  0123456789ABCDEF
00AA60  39 3A 3B 3C 3D 3E 3F 40-41 42 43 44 45 46 47 48  9:;<=>?@ABCDEFGH
00AA70  49 4A 4B 4C 4D 4E 4F 50-51 52 53 54 55 56 57 58  IJKLMNOPQRSTUVWX
00AA80  59 5A 5B 5C 5D 5E 5F 60-61 62 63 64 65 66 67 68  YZ[¥]^_`abcdefgh
00AA90  69 6A 6B 6C 6D 6E 6F 70-71 72 73 74 75 76 77 78  ijklmnopqrstuvwx
00AAA0  79 7A 7B 7C 7D 7E 7F 00-68 74 74 70 3A 2F 2F 31  yz{|}~..http://1
00AAB0  2E 31 2E 31 2E 31 00 75-75 75 75 75 75 75 75 75  .1.1.1.uuuuuuuuu
00AAC0  75 75 75 75 75 75 75 75-75 75 75 75 75 75 75 75  uuuuuuuuuuuuuuuu
00AAD0  75 75 75 75 75 75 75 75-75 75 75 75 75 75 75 75  uuuuuuuuuuuuuuuu
00AAE0  75 75 75 75 75 75 75 75-75 75 75 75 75 75 75 75  uuuuuuuuuuuuuuuu
00AAF0  75 75 75 75 75 75 75 75-75 75 75 75 75 75 75 75  uuuuuuuuuuuuuuuu
00AB00  75 75 75 75 75 75 75 75-75 75 75 75 00 00 00 00  uuuuuuuuuuuu....
00AB10  65 78 61 6D 70 6C 65 2E-63 6F 6D 2F 65 78 61 6D  example.com/exam
00AB20  70 6C 65 2E 65 78 65 00-76 76 76 76 76 76 76 76  ple.exe.vvvvvvvv
00AB30  76 76 76 76 76 76 76 76-76 76 76 76 76 76 76 76  vvvvvvvvvvvvvvvv
```

図 5 疑似プログラムの生成

Fig. 5 Creation of the pseudo program.

表 3 キャッシュリストの例

Table 3 Example of the cache list.

通信先 URL	応答保存先
http://example.com/example.exe	/data/example.com/example.exe
http://example.net/abc.exe	-

ネット通信を受信すると，当該 URL と，マルウェア通信制御システムの IP アドレス（図 4 中 x.x.x.x）を含む新たな URL（図 4 中 http://x.x.x.x/example.com/example.exe）へアクセスする疑似プログラムを生成し，解析環境に応答する．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生成（**図 5**）し，応答する．

解析環境で実行されたマルウェアがダウンローダ型マルウェアであった場合，疑似プログラム応答機能で生成された疑似プログラムが解析環境上のダウンローダ型マルウェアによって実行され，マルウェア通信制御システムへの HTTP リクエストが送信される．当該 HTTP リクエストをマルウェア通信制御システムのダウンローダ判定機能で観測することにより，MW ダウンロード通信か否かの判定を行えるようになる．

(3) キャッシュ管理

1 章で述べたように，マルウェア配布サーバの中には，1 回目のアクセスに対してのみしか第 2 のマルウェアを配布しないものが存在する．これにより，複数の解析環境を用いて解析を行う多種環境マルウェア動的解析システムを用いる場合や，複数回解析を行いたい場合に，2 回目以降のアクセスに対してマルウェアがダウンロードされず，解析がうまく行われないという問題が発生する．

この問題を解決するため，1 回目のアクセスに対してインターネットからダウンロードした第 2 のマルウェアをキャッシュする，キャッシュ管理機能を用いる．解析環境から MW ダウンロード通信が発生した際に，当該通信先の応答ファイルがキャッシュされていれば，キャッシュ管理機能が応答する．具体的には，インターネットからの応答を URL ごとにファイルとして保存し，**表 3** に示すキャッシュリストを用いて管理する．

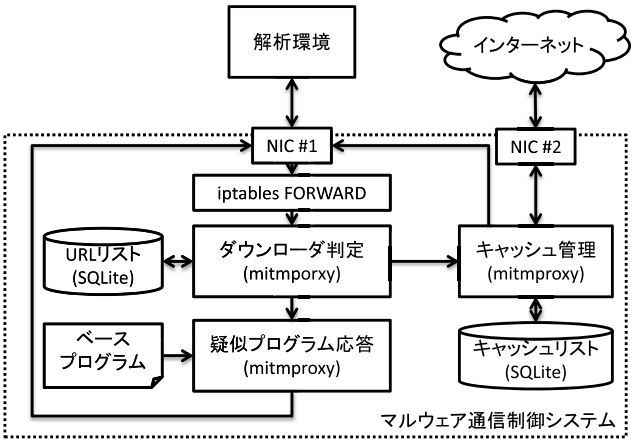

図 6 マルウェア通信制御システムの実装

Fig. 6 Implementation of the malware traffic control system.

4. マルウェア通信制御システムの実装

本章では，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，それらの実装に用いたソフトウェアの関係を**図 6** に示す．

マルウェア通信制御システムの機能のうち，ダウンローダ判定機能，疑似プログラム応答機能，キャッシュ管理機能は man-in-the-middle 型のプロキシサーバである mitmproxy [21] を用いて実装した．また，ダウンローダ判定リスト，キャッシュリストは，SQLite を用いて実装した．なお，ベースプログラムとして，Windows で実行可能な実行ファイルを用意した．

1 番目の NIC で受信した HTTP パケット（80 番向けポート）は，iptables の機能を用いて mitmproxy が監視しているポート（8080 番）に転送される．なお，mitmproxy からインターネットへの接続は，2 番目の NIC を用いて行われる．

5. 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．

5.1 評価目的

マルウェア通信制御システムは，マルウェアの MW ダウンロード通信を検知し，当該 MW ダウンロード通信のみをインターネットに接続するシステムである．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) 検知性能について

提案手法により，世の中に存在するダウンローダ型マルウェアの MW ダウンロード通信を検知できるかを評価する．

(2) 有効性について

ある組織に届いた検体を解析し，どの程度ダウンローダ型マルウェアが存在するのか，また，提案手法により，閉塞環境での解析や青木ら [15] の手法に基づく解析と比較

表 4 検知性能評価用マルウェア
Table 4 Evaluation malware for detection capability.

検知名	ハッシュ値（MD5）
Downloader	ee5f956efb93e2981b9ce9b75680c299
W97M.Downloader	cf9443e43b990077a3862aa4f9337fb2
JS.Downloader	20de9a1fc71d4654f980cee8e7ce84f2

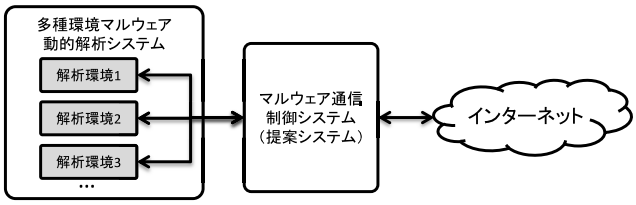

図 7 評価環境
Fig. 7 Evaluation environment.

し，どの程度新たな脅威が明らかになるのかを評価する．

5.2 評価方法

(1) 検知性能について

世の中に存在するダウンローダ型マルウェアを入手し，マルウェア通信制御システムによって当該マルウェアのMW ダウンロード通信を検知できるかを評価する．なお，Symantec 社のウイルス対策ソフトでダウンローダ型マルウェアと判定されたマルウェアを評価に用いた（**表 4**）．

(2) 有効性について

2015 年 2 月にある組織に届いたファイルの内，動的解析によって実行ファイルのドロップや，他のプロセスへのインジェクション等の不審な挙動（マルウェアと思われる挙動）を観測した検体（644 検体）を用いて，ダウンローダ型マルウェアの数を評価する．また，当該ダウンローダ型マルウェアが通信するマルウェア配布サイトに接続し，第 2 のマルウェアを取得できるかを評価する．

なお，評価では，我々のグループで開発している，多種環境マルウェア動的解析システムを利用してマルウェアの解析を行った．**図 7** に評価環境を示す．

多種環境マルウェア動的解析システムは，環境によって振舞いの異なるマルウェアを解析するために，様々な OS やアプリケーションを組み合わせた解析環境を約 70 種類備えている．マルウェアの解析を行う際には，これらの解析環境のすべてにマルウェアを配布し，実行する．

また，比較対象として，インターネットへの接続を行わない閉塞環境での解析と，青木ら [15] の手法に基づく解析も実施する．なお，閉塞環境での解析では，InetSim [22] を用いて，ネットワーク環境をエミュレートする．

5.3 評価結果

(1) 性能評価結果

評価用マルウェアに対して，MW ダウンロード通信として判定された通信先を**表 5** に示す．

表 5 検知性能評価結果
Table 5 Evaluation result of detection capability.

ハッシュ値（MD5）	通信先 URL
ee5f956efb93e2981b9ce9b75680c299	http://k[snip].com/putty3.exe
cf9443e43b990077a3862aa4f9337fb2	http://91.[snip]/upd2/install.exe
20de9a1fc71d4654f980cee8e7ce84f2	http://d[snip]/document.php?id=xxx

表 6 マルウェア検知結果
Table 6 Result of malware detection.

項目	VT 検知	VT 未検知	総計
不審ホストへの通信あり	309	236	545
不審ホストへの通信なし	68	31	99
総計	377	297	644

性能評価に用いたすべてのマルウェアにおいて，MW ダウンロード通信を検出することが確認できた．これより，本提案手法によって，MW ダウンロード通信の検出が確認できた．

(2) 有効性評価結果

評価用の 644 検体について，複数種類のウイルス対策ソフトを用いてファイルを検査するオンラインサービス（VirusTotal [23]）での検知結果および，多種環境マルウェア動的解析システムでの不審ホストへの通信有無判定結果を**表 6** に示す．なお，VirusTotal に関しては，複数種類のウイルス対策ソフトのうち 1 つでも検知したものを VT 検知検体とし，すべてのウイルス対策ソフトで検知していない，または，VirusTotal に検体が登録されていないものを VT 未検知検体とした．ここで，解析環境にインストールしたソフトウェアが自動アップデートで通信する可能性のあるホスト（microsoft.com，windows.com，java.sun.com，adobe.com）を正規のホストとし，正規以外のホストを不審ホストとした．

なお，本評価では，正規サイトが改ざんされていた場合，本来は危険なサイトと判断すべきところを，誤って正規サイトとして分類している可能性がある．このため，表 6 に示している不審ホストへの通信検出結果（236 件）は実際の値より少なくなる可能性があるが，提案手法によって世の中で知られていない検体（VT 未検知検体）を不審なホストへ通信した検体として検出できることが確認できた．

提案手法を用いた解析結果と，閉塞環境での解析結果の比較を**表 7** に示す．

提案手法を用いた解析結果と，青木ら [15] の手法に基づく解析結果の比較を**表 8** に示す．なお，青木らの手法に基づく解析においては，HTTP の GET メソッドを HTTP ファイルダウンロード通信と判定し，インターネットと接続させた．

評価の結果，多種環境マルウェア動的解析システムで不審ホストへの通信を観測した 545 検体のうち，58 検体がダウンローダ型マルウェアであることが，449 件の HTTP 通

表 7 閉塞環境での解析結果との比較
Table 7 Comparison of analysis result based on closed network.

項目	提案手法	閉塞環境
不審ホストへ通信した検体（ダウンローダ型マルウェア）	545 (58)	545 (-)
HTTP コネクション数	17,092	16,719
GET メソッド数	15,212	15,188
POST メソッド数	1,880	1,531
HTTP 通信先（マルウェア配布サイト）	449 (58)	396 (-)
インターネット接続数	58	-
実行ファイルダウンロード数	5	-

表 8 青木らの手法に基づく解析結果との比較
Table 8 Comparison of analysis result based on Aoki method.

項目	提案手法	青木ら[15]
インターネット接続数	58	15,212
実行ファイルダウンロード数	5	5

信先のうち，58 件がマルウェア配布サイトであることが判明した．

また，提案手法の方が閉塞環境での解析よりも，多くの HTTP 通信先を観測した．さらに，青木らの手法に基づく解析と比較し，インターネット接続数は少ないものの，実行ファイルダウンロード数は同じ 5 つとなり，実行ファイルのダウンロード効率は高いことが判明した．

なお，Snort を用いて提案手法のインターネット接続を監視したところ，外部への攻撃は発生しなかったことが確認できた．

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，ダウンローダ型マルウェアや，当該マルウェアが通信するマルウェア配布サイトが特定できることが確認できた．また，マルウェア配布サイトからマルウェアをダウンロードして解析することにより，今まで確認できなかった新たな不審ホストの情報を得ることも確認できた．

5.4 考察

(1) 外部への攻撃について

たとえば SQL インジェクション等は，HTTP の GET メソッドを利用した攻撃を行うため，提案手法では防ぐことができるが，青木らの手法に基づく解析では防ぐことができない．提案手法では，ダウンローダ型マルウェアが，第 2 のマルウェアを取得する挙動に着目し，当該 MW ダウンロード通信のみを許可している．このため，通信先は攻撃者の用意したマルウェア配布サイトに限られ，外部への攻撃は発生しない．

一方，MW ダウンロード通信のみをインターネットに接続する提案手法は，一部第 2 のマルウェアをダウンロードできないという問題が発生する．本課題については，考察 (2) で述べる．

(2) 第 2 のマルウェアダウンロードについて

評価実験では存在しなかったが，マルウェアの中には www.windowsupdate.com 等に接続し，疎通が確認できない場合は第 2 のマルウェアの取得を行わず，動作を停止するものも存在する [24]．このようなマルウェアに対して，青木ら [15] や Yoshioka ら [18] の手法では第 2 のマルウェアを取得できるが，提案手法では第 2 のマルウェアを取得することができない．

また，マルウェア配布サイトの中には，別のマルウェア配布サーバに通信をリダイレクトし，第 2 のマルウェアを配布するものも存在する．提案手法ではこのようなリダイレクトを行うマルウェア配布サイトに通信を行うダウンローダ型マルウェアも解析することができない．

さらに，マルウェアの中には，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も存在する [20]．このようなマルウェアは，疑似プログラム応答機能で生成した疑似プログラムを実行しないため，マルウェア通信制御システムではダウンローダ型マルウェアとして判定されず，第 2 のマルウェアを取得することができない．

以上述べたように，提案手法では一部ダウンロードが行われない検体が存在する可能性がある．しかし，インターネットへの接続を許可する通信を MW ダウンロード通信に限定することで，他の手法よりもインターネット接続の制限が厳しくなる提案手法は，外部サイトへの攻撃が発覚すると社会的信用が失墜してしまう大企業にとって，外部のサイトを攻撃しないという点で優れる．

(3) 提案手法と閉塞環境の差について

評価実験では，提案手法の方が閉塞環境での解析よりも，多くの HTTP コネクション数を観測した．これは，提案手法がインターネットから第 2 のマルウェアをダウンロードし，当該ダウンロードしたマルウェアを解析環境上で実行したためである．なお，HTTP の通信先に関して，GET メソッドの増加分よりも，POST メソッドの増加分が多いことが確認できた．これは，ダウンロードした第 2 のマルウェアがホスト上の情報を収集し，HTTP サーバ上にアップロードしようとしていたためである．

(4) インターネットからのダウンロードについて

評価実験で，インターネットに接続した通信は 58 件存在した．これら 58 件の通信先からのダウンロード結果を**表 9** に示す．

58 件の通信先のうち，5 件の通信先に関して実行ファイルがダウンロードできたが．HTML がダウンロードされたものが 36 件，応答がなかったものが 17 件存在した．これは，2 月に入手した検体に対して，マルウェア解析を 3 月に実施したため，時間経過により検体が削除され，ダウンロードに失敗したと考えられる．検体を入手した時点で解

表 9 ダウンロード結果
Table 9 Result of download.

ダウンロードファイル	件数
実行ファイル	5
HTML	36
応答なし	17

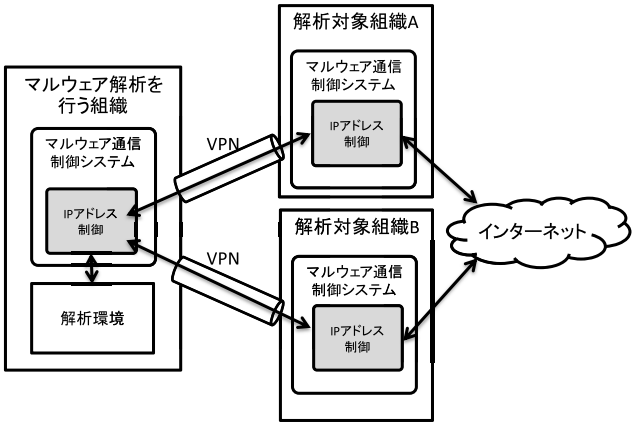

図 8 IP アドレス制御
Fig. 8 IP address control.

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．

(5) クローキングへの対応について

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クローキングという手法が存在する．このようなクローキングへ対応するには，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必要がある．しかし，解析対象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．このような攻撃を解析するために，マルウェア通信制御システムに，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，IP アドレス制御機能を持たせる．

図 8 に，IP アドレス制御の仕組みを示す．図 8 に示すように，マルウェア解析を行う組織と，解析対象のマルウェアを入手した組織が異なる場合に，これらの組織を VPN（Virtual Private Network）で接続し，マルウェアの MW ダウンロード通信を解析対象の組織からインターネットへ接続する．これにより，クローキングへも対応可能となる．

6. おわりに

本稿では，ダウンローダ型マルウェアの MW ダウンロード通信を検出し，当該 MW ダウンロード通信のみをインターネットに接続させることにより，マルウェアによる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，提案手法を実装したプロトタイプシステムを開発した．また，代表的なダウンローダ型マルウェアを用いた評価実験により，提案システムによってダウンローダ型マルウェアを検知できることを確認した．さらに，実検体を用いた評価実験により，644 検体のうち，58 検体がダウンローダ型マルウェアであること，また，解析を通じて外部への攻撃が発生しなかったことを確認した．以上の結果より，本提案手法によって，外部への攻撃を行うことなく，組織に侵入したマルウェアの特性を解明できることを明らかにした．

今後は，IP アドレス制御機能を実装し，クローキングへ対応できるか評価する．

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，入手先 ⟨http://www.ipa.go.jp/files/000024542.pdf⟩.
[2] Symantec: Antivirus software is dead, says security expert at Symantec, available from ⟨http://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec⟩.
[3] Microsoft: Windows Sysinternals, available from ⟨https://technet.microsoft.com/ja-jp/sysinternals/bb545021.aspx⟩.
[4] International Secure Systems Lab.: Anubis – Malware Analysis for Unknown Binaries, available from ⟨https://anubis.iseclab.org/⟩.
[5] ThreatExpert Ltd.: ThreatExpert, available from ⟨http://www.threatexpert.com/⟩.
[6] Cuckoo Foundation: Cuckoo Sandbox: Automated Malware Analysis, available from ⟨http://www.cuckoosandbox.org/⟩.
[7] ThreatTrack Security Inc.: Dynamic Malware Analysis Tools, Malware Sandbox, available from ⟨http://www.threattracksecurity.com/enterprise-security/malware-analysis-sandbox-tools.aspx⟩.
[8] FFRI：FFR yarai analyzer 製品概要，available from ⟨http://www.ffri.jp/products/yarai_analyzer/⟩.
[9] 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).
[10] 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).
[11] 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，pp.848–853 (2013).
[12] Hitachi Solutions：正規の Web サイトを改ざんしてウイルスを仕込む「Nine-Ball」攻撃に注意，入手先 ⟨http://securityblog.jp/news/757.html⟩.
[13] Emurasoft：今回のハッカーによる攻撃の詳細について，入手先 ⟨https://jp.emeditor.com/general/今回のハッカーによる攻撃の詳細について/⟩.

[14] Google: Trends in Circumventing Web-Malware Detection, available from ⟨http://static.googleusercontent.com/media/research.google.com/ja//archive/papers/rajab-2011a.pdf⟩.
[15] 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).
[16] Miwa, S., Miyachi, T., Eto, M., Yoshizumi, M. and Shinoda, Y.: Design and Implementation of an Isolated Sandbox with Mimetic Internet Used to Analyze Malwares, *Proc. DETER Community Workshop on Cyber Security Experimentation and Test* (2007).
[17] Kreibich, C., Weaver, N., Kanich, C., Cui, W. and Paxson, V.: GQ: Practical containment for measuring modern malware systems, *Proc. 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, pp.397–412 (2011).
[18] Yoshioka, K., Kasama, T. and Matsumoto, T.: Sandbox Analysis with Controlled Internet Connection for Observing Temporal Changes of Malware Behavior, *The 4th Joint Workshop on Information Security* (*JWIS 2009*) (2009).
[19] IPA：コンピュータウイルス・不正アクセスの届出状況および相談状況 [2015 年第 4 四半期 (10 月～12 月)]，入手先 ⟨https://www.ipa.go.jp/security/txt/2015/q4outline.html⟩.
[20] 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).
[21] Cortesi, A.: mitmproxy, available from ⟨https://mitmproxy.org/⟩.
[22] Hungenberg, T. and Echert, M.: INetSim Internet Services Simulation Suite, available from ⟨http://www.inetsim.org/index.html⟩.
[23] Google Inc.: VirusTotal, available from ⟨https://www.virustotal.com/ja/⟩.
[24] IPA：脆弱性を利用した新たなる脅威の分析による調査，入手先 ⟨https://www.ipa.go.jp/files/000017747.pdf⟩.

重本 倫宏 （正会員）

2006 年大阪大学大学院基礎工学研究科システム創成専攻修士課程修了．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）入所．現在はネットワークセキュリティ技術に関する研究開発に従事．

徳山 喜一

2014 年名古屋大学大学院多元数理科学研究科修士課程修了．同年（株）日立製作所システムイノベーションセンタに入所．現在はネットワークセキュリティ技術に関する研究開発に従事．

下間 直樹 （正会員）

2009 年群馬大学大学院工学研究科情報工学専攻修士課程修了．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）入所．現在はネットワークセキュリティ技術に関する研究開発に従事．

林 直樹 （正会員）

2007 年京都大学大学院情報学研究科数理工学専攻修士課程修了．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）に入所．次世代ネットワーク向け認証連携技術の研究開発に従事．現在はネットワークセキュリティ技術に関する研究開発に従事．

鬼頭 哲郎 （正会員）

2005 年東京大学大学院情報理工学系研究科電子情報学専攻修士課程修了．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）に入所．以来，ネットワークセキュリティ技術に関する研究開発に従事．

仲小路 博史 （正会員）

2001 年東京理科大学大学院理工学研究科情報科学専攻修士課程修了．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）入所．以来，サイバー攻撃対策技術の研究開発に従事．現在，日立製作所横浜研究所エンタープライズシステム研究部主任研究員．明治大学大学院先端数理科学研究科現象数理学専攻博士後期課程在籍．