情報処理学会論文誌 Vol. 51 No. 9 1600–1609 (Sep. 2010)

推薦論文

ボットネットの連携感染を判定する発見的手法について

桑原和也[†1] 菊池浩明[†1]
寺田真敏[†2] 藤原将志[†2]

本研究では，マルウェアのダウンロードやポートスキャンの振舞いを明らかにするために，94 台のおとりコンピュータ「ハニーポット」によって観測された攻撃通信路のデータセット CCC DATAset 2009 を解析する．本解析によって，複数の不正なサーバが連携して複数のマルウェアをある単一の PC に感染させる挙動が頻繁に観測された．このボットネットに特有の振舞いを連携感染と定義する．本論文では，この連携感染を検出する発見的手法とその精度について報告する．

Heuristics for Detecting Botnet Coordinated Attacks

Kazuya Kuwabara,[†1] Hiroaki Kikuchi,[†1]
Masato Terada[†2] and Masashi Fujiwara[†2]

This paper studies the analysis on the CCC DataSet 2009 consisting of connection data observed by 94 decoy computers, called “honeypot”, for clarifying behavior of downloads of the malware and the port-scans. Based on the analysis, it is found that several malicious servers often coordinate to attack a single target hosts by sending some kinds of malware. The behavior, particularly observed in botnet, is defined as a *coordinated attack*. The paper proposes heuristic techniques for detection of the coordinated attack and reports the accuracy of the proposed heuristics.

†1 東海大学大学院工学研究科
Graduate School of Engineering, Tokai University
†2 株式会社日立製作所
Hitachi Ltd.
本論文の内容は 2009 年 10 月のマルウェア対策研究人材育成ワークショップ 2009 にて報告され，コンピュータセキュリティシンポジウム 2009 プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

1. はじめに

近年，マルウェア（以下，MW）に感染した数 10〜数 100 万台の PC を従えたボットネットによる不正行為が深刻になっている．ボットネットは容易に検出されないように，複雑で高度な感染方式を用いる．まず感染に用いるマルウェアはポートスキャンやバックドア設置などの機能ごとに分割され，数多くの亜種が合成される．MW の配布も，数多くのダウンロードサーバ（以下，DL サーバ）に分散され[⋆1]，様々なプロトコルが用いられている．加えて感染の方式も複雑で，IRC[⋆2]などを介して動的にパターンが変更されたりする．この複雑な攻撃パターンを解析するために様々な研究が行われている．たとえば，水谷らは，ボットネットにおける状態遷移モデルを提案し，独自のファイル転送プロトコルの性質を報告している[2]．そのほかにも，中継ホストの活動期間やダウンロード関係の分布の解析[3]，マルウェアのライフサイクルに着目した攻撃解析手法[4]，通信プロトコルの種類と分類の研究[5]，攻撃と DNS のクエリの相関に注目した研究[7]，2 台のハニーポット間の連携を検出する研究[8] など多くの研究報告がされている．

MW の検出を困難にしている大きな原因は，複数の連携した DL サーバによる多種類の MW を用いた感染方式である．このボットネットに特有の感染方式を本論文では連携感染と呼ぶ．連携感染には様々な効果がある．まず，不正サーバが多いので，ボットネット全体の特定が難しい．加えて，感染させる MW を変えるだけで攻撃パターンの再構成が可能である．たとえば，本論文で後述する `WORM_SWTYMLAI.CD`（`WO3`） は，同時に感染する他の MW によってポートスキャンや DoS 攻撃のパターンが変わる[⋆3]．したがって，ボットネットからの攻撃を検出し，そのパターンを判別するためには，もはや単一の MW の解析だけでは不十分であり，MW に感染した PC と複数の DL サーバ間での通信などを総合的に解析する必要がある．

連携感染は，2008 年の松木らの論文[6] ですでにその存在が報告されている．松木らは，連携感染を定めるパラメータとして，1. 感染時間間隔，2. 攻撃元 IP アドレスの一致度，3. ソースポート番号の連続性，4. 検体名称，5. 検体ファイルサイズの 5 つを定義しているが，

⋆1 たとえば，竹森は，1 つの MW が平均 2 台，最大 69 台の DL サーバから配布されていたことを報告している[1]．
⋆2 Internet Relay Chat システム．ボットネットの命令を送信するチャネルとして多用されている．
⋆3 後述する表 7 に示すように，WO3 は 3 種の連携パターンのすべてに用いられていた．それゆえ，MW 名が分かっても，種類からその先に生じる不正行為はポートスキャン（s4），DoS，SMTP のどれであるか予測がつかなかった．この失敗が連携感染の重要性を認識することにつながった．

観測データ量の不足を理由に 1 の感染時間の間隔のみを時系列分析している．仮に十分な観測データが得られたとしても，5 つのパラメータの組合せは膨大で最適なパラメータを求めるのは困難であることが予測される．

そこで，本研究では，通信データから連携感染を検出する発見的手法を提案する．多くのパラメータの最適な組合せを求める代わりに，複数の検出ルールを組み合わせて，MW 名やソース IP アドレス，ポート番号，IRC 通信のメッセージなどの多くの情報を考慮した高精度の効率的な検出システムの実現を試みる．検出ルールを学習するデータとして，サイバークリーンセンター（以下，CCC）の 94 台のハニーポットで観測された通信データである CCC DATAset 2009 の攻撃通信データを用いる．キャプチャされた攻撃通信データの中から，複数の DL サーバの連携により感染と攻撃が行われているパターンが存在すると仮定し，そのタイミング，ポート，MW の種類，通信先などの様々な連携感染固有の特徴を明らかにする．本論文はこの特徴に基づいて，(1) 連携感染パターンに関するルール，(2) 感染の有無に関するルール，(3) ポートスキャンなどの他の攻撃に関するルールからなる発見的手法を提案する．さらに，特徴量の学習には用いなかった CCC DATAset 2009 の他の通信データを評価データと見なし，提案した発見的手法の精度を明らかにし，その有効性を検証する．

本研究と同様に，既知の通信パターンや不正ホストのアドレスリストを基にして感染を検出するシステムに，BotHunter[9]，BotSniffer[10] などのシステムがあげられる．BotHunter は MW に感染した PC の通信パターンを認識し，ボットの感染に用いられるトラフィックと MW に感染した PC の特定を試みる．BotSniffer は MW に感染した PC と C&C[⋆1] サーバのトラフィックの特徴を利用して疑わしい IRC 通信の検出をする．これらの既存システムは不正ホストを列挙することを目的としているのに対して，本研究は複数ホストによる連携感染パターンを検出するところに新規性がある．

本論文の構成は次に示すとおりである．まず，2 章で CCC DATAset の統計量と概要を示す．3 章では，連携感染，ポートスキャン，MW のダウンロードなどに関する特徴を報告する．これらの特徴に基づいて，4 章では連携感染を検出するためのアルゴリズムを 2 種類提案し，その精度を評価する．5 章で本研究を結論づける．

⋆1 C&C（Command and Control）サーバは感染した PC とボットネットの指令者を仲介する中継サーバである．これは指令者を見つかりにくくするためである．

2. 解析データ

2.1 攻撃通信データ内の MW とハッシュ値

研究用データセット CCC DATA set 2009 の攻撃通信データは，94 台のハニーポットで観測されたボットネットとの通信を tcpdump でパケットキャプチャした libpcap 形式のファイルである．文献 11) によると，ハニーポットは 1 台のホスト OS 上で動作する Windows 2000 と XP の 2 台のゲスト OS により構成されている．それぞれインターネット接続されており，パケットキャプチャはホスト OS 上で行われている．

ハニーポットは感染の有無にかかわらず定期的にリセットされて運用されている．この期間を次のように定める．

定義 1　1 台のハニーポットが起動して，（スケジュールに従って）リブートされるまでの観測期間を**スロット**という．

攻撃通信データ 2 日分はスロットについて 145 個に分割される[⋆2]．総 MW 数は 200 個あり，そのうちユニークハッシュ値は 24 種類，MW は**表 1** に示す 13 種類であった．ここ

表 1　2 日間で観測された全 MW のリスト
Table 1　List of MWs observed for two days.

MW 名	ラベル	UH 数	DL 数	スキャン数	プロトコル
PE_VIRUT.AV	PE1	8	91	18	TCP
PE_BOBAX.AK	PE2	1	4	4	TCP
PE_VIRUT.AT	PE3	1	1		TCP
BKDR_POEBOT.GN	BK1	1	30		TCP
BKDR_MYBOT.AH	BK2	1	1	6	UDP
BKDR_RBOT.ASA	BK3	4	5		UDP
TROJ_AGENT.ARWZ	TR1	1	6		TCP
TROJ_BUZUS.AGB	TR2	1	24		TCP
WORM_ALLAPLE.IK	WO1	1	1		TCP
WORM_POEBOT.AX	WO2	1	1		TCP
WORM_SWTYMLAI.CD	WO3	1	27		TCP
WORM_AUTORUN.CZU	WO4	1	3		TCP
WORM_IRCBOT.CHZ	WO5	1	1		TCP
UNKNOWN	UK	1	5		TCP

⋆2 CCC DATASet 攻撃通信データは，全スロットを単一のファイルに連結しているので，Windows XP が再起動するときに NTP サーバにアクセスする NTP パケットを利用して，スロットごとの通信データに分割して用いる．

表 2　単一の MW と攻撃パターンの関係
Table 2　Attack patterns for each single MW.

MW	スキャン（s4）	スキャン（r2）	DoS	SMTP	計
PE_VIRUT.AV	18	1	0	0	91
PE_BOBAX.AK	4	0	3	3	4
BKDR_POEBOT.GN	6	0	0	0	30
WORM_SWTYMLAI.CD	24	1	3	3	27
TROJ_BUZUS.AGB	24	1	0	0	24

表 3　識別に用いる特徴量一覧
Table 3　List of characteristics used to classify.

	特徴量	意味
統計量	$slot$	スロット ID$(0, \ldots, 145)$
	P_I, P_O	総入力（出力）パケット数 [pkt]
文字列の出現の有無	MZ	“MZ”
	PE	“PE”
	DOS	“!This program cannot be run in DOS mode.”
	win	“!Windows Program”
	N, J	“NICK” かつ “JOIN”
	$ip1$	“#las6 * ipscan s.s.s.s dcom2 -s”
	$ip2$	“#last * ipscan s.s.s.s dcom2 -s”
スキャン	ST	ポートスキャンの種類 $(s_2,\ s_3,\ s_4,\ r_3)$
	DL	感染の有無
	MW	マルウェア名

で，UH 数はユニークハッシュ数を，DL 数はダウンロード回数を示している．たとえば，PE_VIRUT.AV と識別される MW には，異なる 8 種類のハッシュ値があることを表している．プロトコルは MW を DL する際のトランスポート層の通信方式である．

MW が引き起こす攻撃パターンの頻度を**表 2** に示す．WORM_SWTYMLAI.CD のように，感染のたびに異なる攻撃をするものがあり，MW 名と攻撃の関係は一意ではない．しかし，後述する連携感染を考慮すれば，攻撃を一意に特定できる．

2.2　特徴量抽出

感染判定のために用いるスロットの特徴量を**表 3** に示す．特徴量には，ハニーポットの入出力パケット数 P_I，P_O，パケット中に含まれる文字列に関するもの，ポートスキャンに関するもの，ダウンロードした MW に関するものの 4 種類がある．文字列検索には，Network Grep [12] を用いる．ポートスキャンのタイプの s_4 は，スキャンあて先アドレスの第 4 オクテットが 1 ずつ増加する形式である．r_3 はランダムに第 3 オクテットまでを変化させる．入出力パケット数はハニーポットが送受信したパケット数である．ポートスキャンタイプの判定はハニーポットのパケットのあて先をすべて調査し，IP アドレスの変化によって明確に判定した．MW 名はその時点での最新パターンファイルを適用したウイルススキャナ（トレンドマイクロ社製）により判定されている [11]．判定できないものは UNKNOWN と表記される．MW の感染の有無は CCC DATAset2009 の攻撃元データとの参照により判定した．

3. 解析結果

3.1　概　　要

表 3 の特徴量について解析した結果の一部を**表 4** に示す．ここで，全スロットの総数を total，平均を ave の行に示す．「感染パターン」の列は，次節で詳細に述べる．

全 145 のスロットの中で MW をダウンロードしているスロットは 58 件であった．これらを詳細に解析した結果，**表 5** に示されるいくつかのルールを発見した．ルールは連携感染に関する Rule 1〜5，ポートスキャンに関する Rule 6〜8，MW に関する Rule 9〜10 がある．これらのルールの発見過程に用いた関連データを表 5 の第 3 列に示し，以後詳細に述べる．

3.2　連携感染に関する特徴

定義 2（連携感染）　単一のボットネットにより制御されている複数の DL サーバが連携して 1 つ以上の MW を単一ホストに多重に感染させる不正行為を**連携感染**と呼ぶ．

単一のハニーポットが複数の MW に感染しても，それが同一のボットネットによるものかどうかは厳密には分からない．しかし，連携感染は，通常スクリプトなどで機械的に引き起こされるので，感染間隔，MW の種類やポート番号に特定のパターンが生じやすい．利用される DL サーバ，ソース IP アドレスにも一定のパターンが生じる．そこで，多くのスロットを解析し，共通のパターンを抽出していく．

連携感染の基本パターンを**図 1** のタイムチャートに示す．脆弱性のあるホスト（ハニーポット）は感染すると S_1，S_2，S_3，の 3 種類の中継/DL サーバから，PE を時刻 t_0 で，TROJ，WORM の異なる MW を t_2 のタイミングでダウンロードする（Rule 1）．また，TROJ と WORM をダウンロードする直前に C&C サーバ S_0 との間で IRC のセッションを確立し，NICK [⋆1] と JOIN の命令を受ける（Rule 2）．時刻 t_4 で，指定されたあて先ネットワークにポートスキャンを試みる．ここで，最初の MW から次の MW をダウンロード

⋆1 NICK は C&C サーバと最初に通信を行う際のコマンドである．

表 4　スロットと各種特徴量（一部）
Table 4　Characteristic values for slot (snipped).

スロット	P_I	P_O	MZ	PE	DOS	N, J	$ip1$, $ip2$	$ST(s_4)$	感染	MW	感染パターン
0	276	17,774	9	13	3	1		1	1	$PE1$, $TR2$, $WO3$	1
1	61	352	0	4	0				0		
2	7,488	178,491	10	16	3	1	$ip2 \times 1$	1	1	$WO1$, $PE1$, $TR2$, $WO3$	1
3	350	240,148	12	10	4	1	$ip2 \times 1$	1	1	$PE1$, $TR2$, $WO3$, $PE1$	1
4	2	55	0	0	0				0		
5	5	59	0	0	0				0		
14	354	135,725	9	10	3	1	$ip1 \times 3$	1	1	$BK1$, $TR2$, $WO3$	2
55	822	179,581	21	16	7	1	$ip1 \times 2$	1	1	$BK1$, $WO3$, $TR2$, $BK1 \times 4$	2
46	379	791	0	0	0				1	$BK2$	
83	571	74,286	15	15	5	1		1	1	$PE1 \times 2$, $TR2$, $WO3$	1
139	450	96,211	13	18	3	1	$ip2 \times 1$	1	1	$PE2$, $WO4$, $WO3$	3
140	691	101,877	21	24	5	1	$ip2 \times 1$	1	1	$PE2$, $WO4$, $WO3$	3
total	44,452	3,038,276	691	966	219	60	33	28	58	200	
ave	306.57	20,953.63	4.77	6.66	1.51	0.41	0.23	0.19	0.4	1.38	

表 5　連携感染の特徴を表すルール一覧
Table 5　List of rules for feature of coordinated attacks.

NO.	ルール	関連（データ）
Rule 1	PE_VIRUT.AV をダウンロードしたならば WORM_SWTYMLAI.CD と TROJ_BUZUS.AGB を同時刻にダウンロードを開始する.	図 1
Rule 2	WORM_SWTYMLAI.CD と TROJ_BUZUS.AGB のダウンロード直前に JOIN がある.	図 1
Rule 3	WORM_SWTYMLAI.CD と TROJ_BUZUS.AGB の DL サーバはつねに一定.	表 6，8
Rule 4	PE_VIRUT.AV は 5 桁のポート番号使う.	表 6
Rule 5	WORM_SWTYMLAI.CD と TROJ_BUZUS.AGB はポート番号 80 番を使う	表 6
Rule 6	連携感染ならば，ポートスキャン先は PE_VIRUT.AV の DL サーバの第 1，2 オクテットと同じ.	表 9
Rule 7	IRC で “JOIN” を受信したならば約 5 秒後にポートスキャンを開始する.	図 3
Rule 8	連携感染したならば，1 秒間に 256 パケットのポートスキャンを連続して行う.	図 2
Rule 9	文字列 “MZ” かつ “PE” を含むならば TCP による感染である.	表 4
Rule 10	UDP で win という文字列があれば，TFTP のダウンロードである.	なし

する間隔と，IRC の JOIN からポートスキャンまでの間隔を各々，

$\Delta T_1 = t_2 - t_1$

$\Delta T_2 = t_4 - t_2$

と定義する.

連携感染する具体例を**表 6** に示す．PE_VIRUT.AV をダウンロードさせる DL サーバの IP アドレスはまちまちだが，WORM_SWTYMLAI.CD と TROJ_BUZUS.AGB の DL サーバの IP アドレスはすべてのスロットで同じであった（Rule 3）．どのスロットも，PE_VIRUT.AV は 5 桁のポート番号を用いている（Rule 4）．TROJ_BUZUS.AGB と WORM_SWTYMLAI.CD は 80 番である（Rule 5）.

MW をダウンロードしている 58 のスロットは**表 7** に示される 3 つの連携パターンに分

表 7　連携感染パターンとその統計量
Table 7　All patterns of coordinated attacks and statistics.

	パターン	スロット ID	スロット回数	ΔT_1 平均	標準偏差	イベント	ポート
連携 1	PE1 → TR2，WO3	0，2，3，16，29，30，50，60，63，69，70，71，83，94，100，130，132	17	127.24	158.75	$s4$	135
連携 2	BK1 → TR2，WO3	14，55，56，124，125，126	6	176.4	147.36	$s4$	135
連携 3	PE2 → WO4，WO3	139，140，141	3	253.25	176.25	$s4$，DOS，SMTP	135
4	WO1	2	1			$r3$	139，445

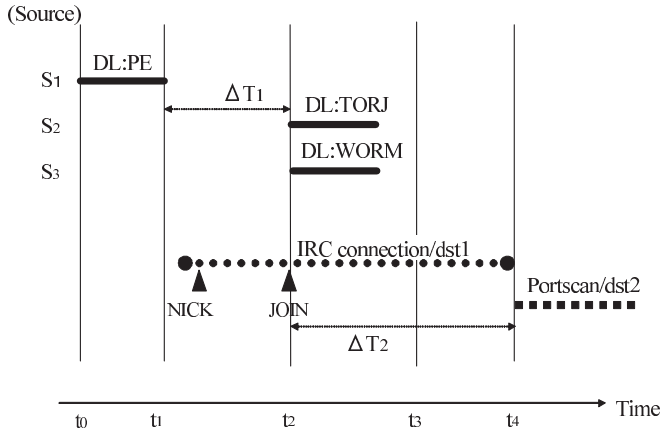

図 1　連携感染の通信路のタイムチャート
Fig. 1　Time-line chart of connection in typical coordinated attacks.

表 6　連携感染パターン 1 の通信路
Table 6　Connections of coordinated attack pattern #1.

スロット	時間	srcIP	dstPort	MW 名
0	0:02:11	124.86.A1.B1	47,556	PE_VIRUT.AV
0	0:03:48	67.215.C1.D1	80	TROJ_BUZUS.AGB
0	0:03:48	72.10.E1.F1	80	WORM_SWTYMLAI.CD
2	0:36:46	124.86.A2.B2	33,258	PE_VIRUT.AV
2	0:36:52	72.10.E1.F1	80	WORM_SWTYMLAI.CD
2	0:36:52	67.215.C1.D1	80	TROJ_BUZUS.AGB
3	0:46:56	124.86.A2.B2	33,258	PE_VIRUT.AV
3	0:48:52	67.215.C1.D1	80	TROJ_BUZUS.AGB
3	0:48:52	72.10.E1.F1	80	WORM_SWTYMLAI.CD
16	5:17:25	114.145.A3.B3	15,224	PE_VIRUT.AV
16	5:18:37	67.215.C1.D1	80	TROJ_BUZUS.AGB
16	5:18:38	72.10.E1.F1	80	WORM_SWTYMLAI.CD

表 8　MW ごとのユニーク DL サーバ
Table 8　Unique DL servers for each MW.

MW 名	ユニーク DL サーバ数
PE_VIRUT.AV	10
TROJ_BUZUS.AGB	1
WORM_SWTYMILAI.CD	1

類される．MW 名は表 1 をもとにしている．表 7 より，MW 感染が確認された 58 スロットの内 26 スロットが複数の DL サーバにわたる連携感染であることが分かる．なかでも，連携パターン 1 は，頻度が高く，ポートスキャンなどの攻撃もともなうので重要である．ダウンロードする MW の種類やポート番号には共通の特徴が見られるが，時差 ΔT_1 の分散は大きく，感染のたびに変化している．

MW と DL サーバの関係は 1 対 1 ではない．**表 8** に示されるように，連携感染の最初の PE_VIRUT.AV は，感染の度に異なる（10 台の）サーバからダウンロードされているのに対し，後半の TROJ，WORM のダウンロードは 1 台のサーバに集中していた．

3.3　ポートスキャンに関する特徴

表 9 は，連携感染してポートスキャンを引き起こしたスロットにおける，DL サーバ，ハニーポット（感染 PC），ポートスキャンあて先の IP アドレスを示している．3 つの IP アドレスの第 1，2 オクテットは，すべて等しく（Rule 6），ハニーポットとスキャンのあて先 IP アドレスの第 3，4 オクテットは等しい．なお，このあて先 IP アドレスは，1 ずつインクリメントされる．

図 2 は，連携感染 1 における入出力パケットの通信速度の変化を表している．上がハニーポットへの入力，下が出力を表している．スロット内の相対時刻で 600 [s] のときに連携感

表 9　DL サーバ，ハニーポット，スキャンの IP アドレス
Table 9　IP addresses of DL servers, honeypots and target networks.

slot	DL サーバ	ハニーポット	スキャンあて先
0	124.86.C1.D1	124.86.E1.F1	124.86.E1.F1 + 1
2	124.86.C2.D2	124.86.E2.F2	124.86.E2.F2 + 1
3	124.86.C2.D2	124.86.E2.F2	124.86.E2.F2 + 1
16	114.145.C3.D3	114.145.E3.F3	114.145.E3.F3 + 1
29	114.164.C4.D4	114.164.E4.F4	114.164.E4.F4 + 1
例	$A.B.C.D$	$A.B.E.F$	$A.B.E.F + 1$

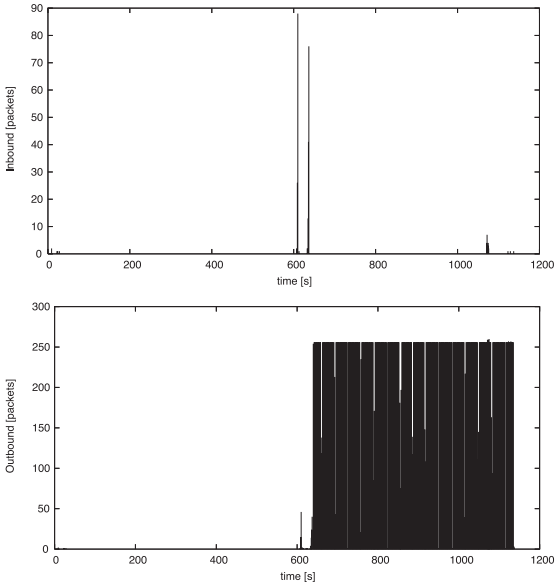

図 2　単位時間あたりの入出力パケット数の変化
Fig. 2　Number of inbound/outbound packets per second in time slot.

染が生じ，その直後にポートスキャンを外部に対して行っている．この送信は毎秒 256 パケットの一定の割合で行われる（Rule 8）．

ポートスキャンには，第 4 オクテットを 1 ずつ増加させる s_4 と第 3 オクテットをランダムに変える r_3 の 2 種類が観測された．コマンド “JOIN” が送られてからポートスキャンが起きるまでの時間差 ΔT_2 の分布を**図 3** に示す．X 軸は “JOIN”，Y 軸はポートスキャンの

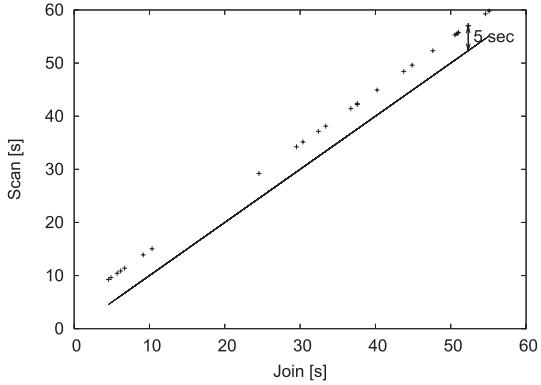

図 3　JOIN の送信時刻と Scan の開始時刻の差 ΔT_2 の分布
Fig. 3　Distribution of time difference between begining of measure “JOIN” and of port-scan ΔT_2.

通信開始時刻を表している（ただし，時間と分の値を略して，秒だけで表したグラフに重ねてプロットしている）．直線と観測時刻との間が時差 ΔT_2 である．観測された 26 回の s_4 のポートスキャンすべてで，JOIN に対しスキャン開始時間が正確に 5 秒遅延していることが分かる（Rule 7）．

3.4　MW のダウンロードに関する特徴

連携感染を行う際には，特徴的なメッセージが送信されている．表 4 に示されるように，“MZ” と “PE” の両方が送信されるときは感染をしている（Rule 9）．

3.5　UDP の感染に関する特徴

UDP を使った tftp での感染は 6 スロットあった．そのうち MW 名は 5 スロットが `BKDR_RBOT.ASA` で，残り 1 スロットは `BKDR_MYBOT.AH` であった（Rule 10）．

4.　感染判別の手法

4.1　一般感染の検出アルゴリズム

表 5 のルールに基づき，**図 4** に示す感染判定の決定木を提案する．ここでは連携感染と通常の感染の区別をせず，与えられたスロット内で（任意の）感染があることを自動判別する．決定木のノードは，表 3 で定義した識別の特徴量を示し，木の枝に示される式は識別の閾値を与えている．たとえば，木のルートは総入力パケット数 P_I が 85 パケット以上かどうかで分岐することを表している．“DOS” というノードは，exe ファイルがダウンロードさ

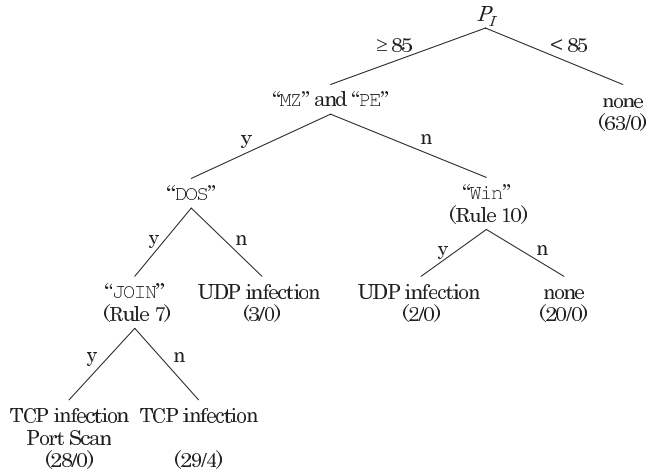

図 4　感染（連携感染を含む）を判定する決定木
Fig. 4　Decision tree classifying arbitrary infections (including coordinated attacks).

表 10　感染（連携感染を含む）を判定する決定木の精度
Table 10　Accuracy of decision tree to detect infection (including coordinated attack).

真値 \ 判定結果		感染あり	感染なし	total slot
学習	感染あり	58	0	58
データ	感染なし	0	87	87
評価	感染あり	6	0	6
データ	感染なし	0	14	14

れたときに文字列 "!This program cannot be run in DOS mode." が出現するか（Y）否か（N）で識別する．感染判定の決定木は 2009 年の攻撃通信データのみを使い作成した．このアルゴリズムの精度を**表 10** に示す．ルールを発見するための学習にはあるハニーポット（Windows XP）の攻撃通信データ，評価には別のハニーポット（Windows 2000）のデータを用いた．両データセットとも，誤検出は生じなかった．

代表的な決定木アルゴリズム C4.5 [13),14)] を適用して，抽出した感染を判別する決定木を**図 5** に示す．図 4 と同様，ノードは識別の特徴量を表す．葉の「1 (49/0)」は，その葉へ分類されるデータの数が 49 件あり，1（感染）という識別ラベルに対して誤識別が 0 であることを表している．図 4 と比較して，ノードの数が 4 つと少なく，最適化が試みられて

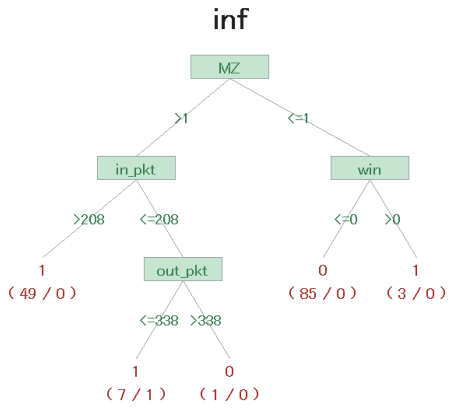

図 5　C4.5 による感染判定の決定木
Fig. 5　Decision tree to detect arbtrary infections generated by C4.5.

いるが，`Out_pkt < 338` に分類されている 7 スロット中，感染と誤判定（False Positive）されるスロットが 1 つ生じている．

4.2　連携感染パターンの発見的手法

単一の感染は，4.1 節の決定木で判別が容易だが，連携感染は例外的振舞いが多く，確定的なアルゴリズムでの検出が困難である．そこで，3 章で述べた連携感染に関する規則に基づき，各ルールを並列に評価した合計スコアによる発見的手法を提案する．

i 番目のスロットにおける Rule j の成立を $x_{ij} = 1$ と定める．スロット i のスコアは，$S_i = \sum_j^9 x_{ij}$ と定義する．このスコアが閾値以上かどうかで判定を行う．学習データにはあるハニーポットの 2 日間の全スロットデータを使用した．**表 11** は，学習データにおける各ルールの成立とスコアの一部である．この学習データでは，連携感染しているスロットの最小スコアが 3 であった．そこで，閾値を 3 と定める．このときのスコアの分布を**図 6** に示す．**表 12** の学習データにおいて，連携感染の誤検知が 2 スロット生じている．この内の 1 つはスロット 66 であり，表 7 で分類した 3 種類の連携感染のどのパターンでもなく，4 番目の新たな連携感染パターン（PE2 → WO4，WO3）に分類される[⋆1]．もう 1 つは CCC

⋆1 これは，手作業で表 7 を作成した際に列挙から漏れてしまっていたパターンであり，本来ならば，表 7 に加えるべきものである．したがって，提案方式の有効性を失わせるものではなく，むしろ，発見的手法が学習データの誤り検出に有効であったことを示している．

表 11　発見的手法のスコアと連携感染の有無の関係（一部）
Table 11　Relationship between Heuristics score and coordinated attacks (snipped).

スロット	Rule									スコア	
i	1	2	3	4	5	6	7	8	9	S_i	連携感染
0	1	1	1	1	1	1	1	1	1	9	1
1	0	0	0	0	0	0	0	0	0	0	0
2	1	1	1	1	1	1	1	1	1	9	1
3	1	1	1	1	1	1	1	1	1	9	1
14	0	1	1	0	1	0	1	1	1	6	1
15	0	0	0	0	0	0	0	0	1	1	0
139	0	0	0	0	0	0	1	1	1	3	1
total	17	24	24	17	24	17	28	28	56	170	28

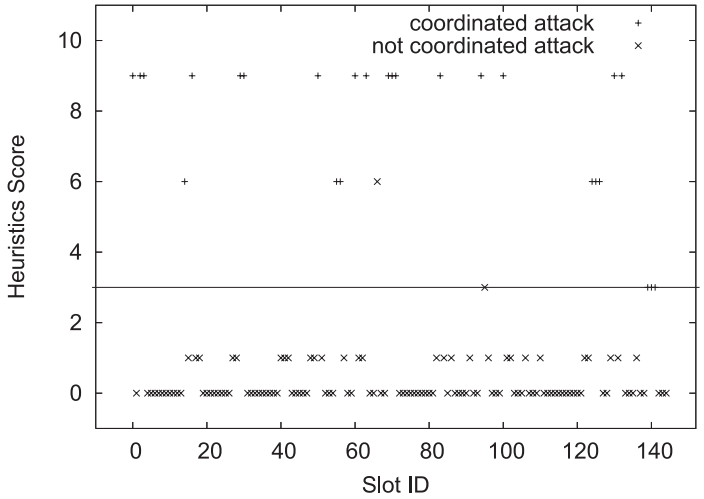

図 6　発見的手法のスコアの分布
Fig. 6　Distribution of heuristics scores.

DATAset 2009 攻撃元データの誤り[*1]から混入したものであった．この提案による精度を表 12 に示す．

145 スロットの中で感染している 58 パターンの出現頻度とその精度（ルールの成立割合）

⋆1 攻撃通信データには存在するが攻撃元データには記録のないスロットであった．

表 12　連携感染を判定する発見的手法の精度
Table 12　Accuracy of heuristics to detect coordinated attacks.

真値 \ 判定結果		連携感染と判定	連携感染でないと判定	FP	FN
学習	連携感染	26	0		
データ	連携感染でない	2	119	2/28	0/117
評価	連携感染	2	0		
データ	連携感染でない	1	7	1/3	0/7

表 13　Rule の出現頻度と成立割合
Table 13　Freaquency and ratio of satisfication for each rule.

ルール	出現頻度 [スロット]	成立割合 [スロット](%)
Rule 1	17/145	17/38 (45%)
Rule 2	17/145	17/27 (89%)
Rule 3	22/145	22/27 (81%)
Rule 4	17/145	17/17 (100%)
Rule 5	17/145	17/17 (100%)
Rule 6	17/145	17/17 (100%)
Rule 7	28/145	28/28 (100%)
Rule 8	28/145	26/28 (93%)
Rule 9	55/145	55/63 (87%)
Rule 10	6/145	6/6 (100%)

を**表 13** に示す．たとえば，Rule 1 は 145 スロット中 17 スロットが該当しており（頻度），その精度は `PE_VIRUT.AV` をダウンロードした全 38 スロット中，WORM と TROJ をダウンロードしたものが 17 スロットあることを示している．145 スロット中 58 の感染スロットの中で連携感染を行っているスロットは 26 あり，約半分が連携感染である．

5. 結　　論

本論文では，CCC DATAset 2009 攻撃通信データにおける，感染種類を判定する発見的手法を報告した．その中で UDP 感染，連携感染などのいくつかの有益な特徴を発見した．MW のダウンロード方式にもいくつかの種類があり，それらを識別するルール，アルゴリズム（決定木）と発見的手法を提案し，評価データによる検出精度を明らかにした．学習データに対して，2/28（7%）の誤検知（FP）があったが，未検知（FN）はなく，十分な精度が得られる手法である．

この研究では MW のダウンロードに対する，2.2 節で述べた文字列検索に重点をおいて

行ったが，文字列だけでは通常の通信を含めた場合の感染判定は難しい．今後は，検出ツールやDNSなどの他の特徴量も活用して新たな特徴を検出することにより，感染判定の精度を上げていきたいと考えている．

謝辞　マルウェアのダウンロードに関する技術について助言をいただいた日立製作所の仲小路博史氏，鬼頭哲郎氏，東海大学の大類将之氏，松尾俊治氏に感謝する．匿名の査読者に感謝する．

参　考　文　献

1) 竹森敬祐ほか：ボットネットおよびボットコードセットの耐性解析，マルウェア対策研究人材育成ワークショップ2008（MWS2008），pp.49–54 (2008).
2) 水谷正慶ほか：通信の状態遷移に着目したボット活動の調査，マルウェア対策研究人材育成ワークショップ2008（MWS2008），pp.25–30 (2008).
3) 石井宏樹，佐藤和哉，田端利宏：ダウンロードホストに着目したマルウェアの活動傾向分析，マルウェア対策研究人材育成ワークショップ2008（MWS2008），pp.97–102 (2008).
4) 小櫻文彦，津田　宏，鳥居　悟：ウイルスのライフサイクルに着目した攻撃挙動の見える化，マルウェア対策研究人材育成ワークショップ2008（MWS2008），pp.55–59 (2008).
5) 藤原将志，寺田真敏，安部哲哉，菊池浩明：マルウェアの感染動作に基づく分類に関する検討，情報処理学会，pp.177–182 (2008).
6) 松木隆宏ほか：時系列分析による連鎖感染の可視化と検体種別の推測，マルウェア対策研究人材育成ワークショップ2008（MWS2008），pp.37–42 (2008).
7) 東角芳樹，鳥居　悟：DNS通信の挙動からみたボット感染検知方式の検討，マルウェア対策研究人材育成ワークショップ2008（MWS2008），pp.13–18 (2008).
8) 仲小路博史ほか：パケット送受信における同調活動に着目したボット感染ノードへの指令および反応活動の可視化，マルウェア対策研究人材育成ワークショップ2008（MWS2008），pp.31–36 (2008).
9) Gu, G., Zhang, J. and Lee, W.: Botsniffer: Detecting botnet command and control channel, *Proc. Network and Distributed System Security Symposium* (*NDSS 2008*), Internet Society (Feb. 2008).
10) Gu, G., Porras, P., Yegneswaran, V., Fong, M. and Lee, W.: BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation, *Proc. 16th USENIX Security Symposium*, USENIX (2007).
11) 畑田充弘，中津留勇，寺田真敏，篠田陽一：マルウェア対策のための研究用データセットとワークショップを通じた研究成果の共有，マルウェア対策研究人材育成ワークショップ2009（MWS2009），pp.1–8 (2009).
12) Network Grep. http://ngrep.sourceforge.net/ (2009年10月参照)
13) Quinlan, J.R.: *C4.5 Progarams for Machine Learning*, Morgan Kaufmann, San Mateo, California.
14) 並木　翼，菊池浩明：ユーザビリティの高いGUIベースの決定木学習ツールID3Eの開発，情報処理学会第67回全国大会，Vol.w-8, No.3, pp.249–250 (2005).
15) tcpflow. http://www.circlemud.org/~jelson/software/tcpflow/ (2009年11月参照)
16) 畑田充弘ほか：複数観測データを用いたボットネットの活動分析に関する一考察，マルウェア対策研究人材育成ワークショップ2008（MWS2008），pp.87–92 (2008).
17) 阿部義徳，田中英彦：C&Cセッション分類によるボットネットの検出手法の一検討，FIT2007, L-033, pp.77–78 (2007).

(平成21年11月30日受付)
(平成22年 6 月 3 日採録)

推　薦　文

本研究は，ハニーポットにおける膨大な通信キャプチャデータから，効率的にマルウェアの感染を判定するものである．CCC DATAset 2009の攻撃通信データの各スロット解析して得られた特徴から，マルウェアの感染に関する発見的手法の規則を導き出し，感染判定のアルゴリズムを提案している．特に，複数のマルウェアが連携して1台のPCへの感染を試みる「連携感染」という挙動の存在を新たに報告するとともに，その検知手法を模索している点において，本研究の意義は高いと判断し，推薦するものである．

（コンピュータセキュリティシンポジウム2009プログラム委員長　西垣正勝）

付　　録

A.1　MW名判別の発見的手法

キャプチャデータから，tcpflow[15]などのツールを用いてMWをダウンロードすれば，アンチウイルスソフトにより検出が可能である．ただし，すべてのパケットから抽出できるのではなく，**表14**に示される割合で成立する．MWの特定はHTTP，UDPともファイル復元ができ，達成することができた．

表 14　MW 名の判定
Table 14　Identification of MW name.

ルール	ファイル復元	MW 名判定
TCP UDP	192/194 スロット 6/6 スロット	192/192 スロット 6/6 スロット
	ファイル復元数 /攻撃元データ	MW 判定数 /復元ファイル数

桑原　和也

2010 年東海大学情報理工学部情報メディア学科卒業．現在，同大学大学院修士課程在学中．2009 年 MWS 優秀学生論文発表賞受賞．ネットワークセキュリティに関する研究に従事．

菊池　浩明（正会員）

1988 年明治大学工学部電子通信工学科卒業．1990 年同大学大学院博士前期課程修了．1994 年同博士（工学）．1990 年富士通研究所勤務．1994 年東海大学工学部電気工学科助手．1995 年同専任講師．1999 年同助教授．2000 年同電子情報学部情報メディア学科助教授．2006 年同情報理工学部情報メディア学科教授．2008 年同情報通信学部通信ネットワーク工学科教授．1997〜1998 年カーネギーメロン大学計算機科学科訪問研究員．2009 年〜情報処理学会コンピュータセキュリティ研究会（CSEC）主査．WIDE プロジェクト暗号メールシステム FJPEM の開発，認証実用化実験協議会（ICAT），IPA 独創情報技術育成事業等に従事．暗号プロトコル，ネットワークセキュリティ，ファジィ論理，ソフトコンピューティング等に興味を持つ．1990 年日本ファジィ学会奨励賞，1993 年情報処理学会奨励賞，1996 年 SCIS 論文賞，2010 年情報処理学会 JIP Outstanding Paper Award．電子情報通信学会，日本知能情報ファジィ学会，IEEE，ACM 各会員．

寺田　真敏（正会員）

1986 年千葉大学大学院工学研究科写真工学専攻修士課程修了．同年（株）日立製作所入社．博士（工学）．現在，システム開発研究所にてネットワークセキュリティの研究に従事．2004 年から Hitachi Incident Response Team チーフコーディネーションデザイナ，2004 年 4 月から JPCERT コーディネーションセンター専門委員，2004 年 4 月から 2007 年まで中央大学研究開発機構客員研究員，2004 年 8 月から情報処理推進機構セキュリティセンター研究員 2008 年から中央大学大学院客員講師を兼務．

藤原　将志

（株）日立製作所 Hitachi Incident Response Team．製品・サービスの脆弱性対策ならびにインシデント対応に従事．