社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DPS－134 (31)
2008－CSEC－ 40 (31)
2008／3／7

マルウェアの感染動作に基づく分類に関する検討

藤原将志[†1] 寺田真敏[†1] 安部哲哉[†2] 菊池浩明[†3]

[†1)](株)日立製作所 Hitachi Incident Response Team (HIRT)
〒212-8567 神奈川県川崎市幸区鹿島田 890
[†2)]NTT 情報流通プラットフォーム研究所
〒180-8585 東京都武蔵野市緑町 3-9-11
[†3)]東海大学
〒259-1292 平塚市北金目 1117

概要：マルウェア対策研究が広がる中，マルウェアのネットワークを介した感染動作に関する調査報告は数少ない．本研究の目的は，ネットワークを介して感染活動を行うマルウェアを対象に，具体的な調査方法を示すこと，その方法に基づき調査した結果を示すことで，感染活動に関する調査活動を支援することにある．本稿では，Microsoft Windows の脆弱性を模擬してネットワークを介した侵害活動を誘い込み，マルウェア本体を捕獲する Nepenthes を用いて収集したデータを元に，感染動作に着目した調査結果について報告する．
キーワード：マルウェア，ボット，ハニーポット，ログ，感染動作

Study for the classification of malware by infection activities

Masashi Fujiwara[†1] Masato Terada[†1] Tetsuya Abe[†2] Hiroaki Kikuchi[†3]

[†1)] Hitachi Incident Response Team. Hitachi Ltd.
890 Kashimada, Saiwai-ku, Kawasaki, Kanagawa, 212-8567 Japan
[†2)] NTT Information Sharing Platform Laboratories NTT Corporation
3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan
[†3)] Course of Information Engineering, Graduate School of Engineering Tokai University
1117 Kitakaname, Hiratsuka, Kanagawa, 259-1292 Japan

Abstract:.. The requirements of investigation reports about activities such as infection behavior and trend are increasing. The purpose of this research is in the support of the investigation concerning the infection activity by showing a concrete examination method of the malware that does the infection activity through the network, and showing the result of the investigation based on the method. In this paper, we describe the investigation result of the infection activities based on the data collected by Nepenthes that collects the malware.
Key words: malware, bot, honey pot, log, infection

1 はじめに

インターネットの普及やツールの高機能化，利用拡大に伴い，ポートスキャン，ワーム，システム侵害ならびにサイトの運用を阻害する DoS 攻撃など，インターネット上での不正アクセス活動は活性化している．また，近年，ネットワーク型ワームによる大規模な感染被害は影を潜め，ボットのような活動が表面化しないマルウェアによる被害が深刻化している．マルウェア対策研究においては，マルウェアの感染検知，収集したマルウェアの動的／静的解析に着目した研究は多くみられるが，マルウェアのネットワークを介した感染動作に着目した調査報告の数は少ない．本研究の目的は，ネットワークを介して感染活動を行うマルウェアを対象に，具体的な調査方法を示すこと，その方法に基づき調査した結果を示すことで，感染活動に関する調査活動を支援することにある．

本稿では，Microsoft Windows の脆弱性を模擬してネットワークを介した侵害活動を誘い込み，マルウェア本体を捕獲する Nepenthes[1]を用いて収集したデータを元に，感染動作に着目した調査結果について報告する．

2 関連研究

本章では，2006 年以降報告されているマルウェア対策研究について，感染検知，動的／静的解析，広域観測の 3 つの視点から整理する．

商品名称等に関する表示
Microsoft，Windows は，米国 Microsoft Corporation.の米国およびその他の国における登録商標です．Kaspersky は，Kaspersky Labs International の商標または登録商標です．

2.1 マルウェアの感染検知

(1) トラフィック観測

主にボットに感染したホストを検出する研究が行われており，ボットネットの動作特徴を利用した手法として，ボットネットの制御サーバとボット群とのトラフィックに着目した手法が報告されている[2][3][4]．また，文献 5)では，より汎用的な手法として，無操作状態の正常なホストから送信されるトラフィックの正常通信プロファイルを元に，感染を検知する手法を報告している．

(2) イベント観測

マルウェアの活性化により，マルウェア自身が本来持っている機能が動作し始める．このような発症活動として，DDoS 攻撃，スパムメール発信，情報収集，フィッシングサイト開設などがある．文献 6) 7)では，発症活動に着目してボットに感染したホストを検出する手法を提案している．

(3) 自己防衛機能の逆用

マルウェアの自己防衛機能を逆用した検知ならびに対策技術の研究も行われている．文献 8)では，デバッガや仮想マシン環境の利用を検知すると停止するといった行為で，マルウェアの解析作業を妨げる装甲化機能を逆用することで，マルウェアの検知と活動抑止を提案している．文献 9)では，ウイルス対策ソフトやファイアウォールを無効化する機能を逆用することで，マルウェアの検知と活動抑止を提案している．

2.2 マルウェアの動的／静的解析

(1) 機能調査

文献 10)では，フィールド調査を通して，ボットの主要な機能の洗い出しを行っている．この報告によれば，主要な機能として，保守，制御，自己防衛，情報収集，感染，攻撃の 6 つの機能を挙げている．

(2) マルウェアの分類

文献 11)では，ネットワークアクセス情報に着目したマルウェアの特徴抽出を行っている．また，文献 12) 13)では，解析から抽出した特徴に基づき，発見されたマルウェアが新種であるか，あるいは既知のマルウェアの亜種や変種であるかを分類する手法を報告している．分類の応用として，判定した類似度からマルウェアの機能を推定する手法が報告されている[14].

(3) 挙動解析

マルウェアは，自己防衛機能，隠蔽機能などにより特定の条件下で動作する場合がある．文献 15)では，隔離された環境でマルウェアを実行し，その挙動を観察するマルウェア解析環境の調整を行うために，マルウェアの動作条件を抽出する手法を提案している．

また，ネットワークから切り離されたマルウェア解析環境における動的解析は本来の挙動，目的，発生する事象と一致しないことから，ハニーポットと仮想インターネット環境を組み合わせたシステムをインターネットに接続することによりボットネットの観測を行うシステムも提案されている[16].

2.3 広域観測

インターネットにおけるボットネットを観測する活動は，国内ならびに海外を含め，数多く実施されている[17]．ボットの解析やボットを駆除するために必要な情報を提供するサイバークリーンセンター[18]では，2006 年 12 月～2007 年 12 月までに収集した累積検体数は 5,965,100 件，同定した一意な検体数は累積で 143,577 件，未知検体数は累積で 8,014 件という活動実績を報告している．また，文献 19)では，Nepenthes と Snort[20]を使用した観測サイトを用意し，攻撃元に関する調査を行っている．

3 感染動作ログの収集環境

本章では，ネットワークを介した感染動作に着目した調査を行うにあたり構築したログ収集環境について述べる．

(1) システム構築の要件

感染動作ログ収集環境の構築要件は，次の通りである．

- 要件 1：マルウェアの検体収集が行えること．
- 要件 2：異なる組織間で収集したログならびに検体を相互に利用できること．

上記要件を満たすため，本研究では，Windows の脆弱性を模擬してネットワークを介した侵害活動を誘い込み，マルウェア本体を捕獲する Nepenthes を用いてログ収集環境を構築した(図 1)．また，マルウェア名の判定には，Kaspersky[21]を使用してスキャンし，ファイルの MD5 ハッシュ値とマルウェア名の対応表を生成した．

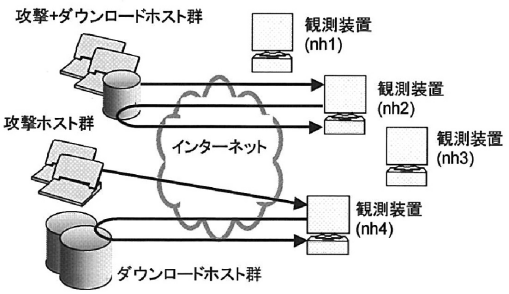

図 1：ログの収集環境

(2) 用語定義

Nepenthes では，攻撃ホスト群やマルウェア本体が格納されたダウンロードホスト群の IP アドレス等をログに残す．本稿では，攻撃ホスト群とダウンロードホスト群を，攻撃元とダウンロード元として次

のように定義する．

- 攻撃元

攻撃の基点となるマルウェアが，Nepenthes が稼動する観測装置に対して，脆弱性を攻撃するパケットを送信する(図 2の①)．このときの発信元ホストを「攻撃元」と定義する．

- ダウンロード元

図 2の①の攻撃が成功した場合，マルウェア本体をダウンロードするための動作(図 2の②)が発生する．このときの接続先ホストを「ダウンロード元」と定義する．図 2の場合，マルウェア本体をダウンロードするために，FTP プロトコルを使って，ダウンロード元 ftp.malware.com の 612 番ポートに接続することを意味する．

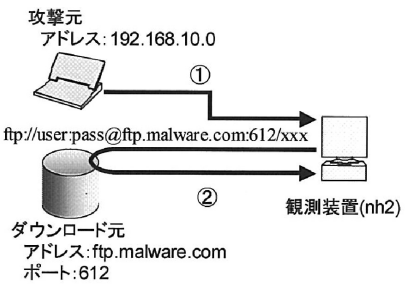

図 2：攻撃元とダウンロード元

表 1：観測装置の感染動作ログの概要

観測装置.	期間	攻撃件数	ダウンロード成功件数
nh1	2007 年 4 月 1 日～11 月 30 日	3,947	2,462 (62.4%)
nh2		61,500	29,792 (48.4%)
nh3		151,539	85,915 (56.7%)
nh4	2007 年 6 月 21 日～11 月 30 日	18,980	10,019 (52.8%)

注)観測装置 nh1 では，ダウンロード元から FTP によるダウンロードができない設定となっている．表 1では，FTP を除外した件数を表記した．FTP を除外しない場合には，攻撃件数 6,396 件，ダウンロード成功件数 2,462 (38.5%)件となる．

(3) 収集したログの概要

観測装置の収集した調査期間約 8 ヶ月のログに関する情報を表 1に示す．攻撃件数は「攻撃元」から発生したアクセス件数である．ダウンロード成功件数は「ダウンロード元」からマルウェア本体のダウンロードに成功した件数であり，平均成功率は約 54%となった．

4 感染動作に基づく分類

本章では，感染動作分類に利用できると思われるパラメタ毎に，その調査結果を示す．

4.1 感染動作を表現するためのパラメタ

(1) 攻撃元

攻撃元に着目することにより，IP アドレス空間上の論理的な地域性，国などの物理的な地域性を感染動作の分類に反映できる．図 3に IP アドレス空間上の攻撃元の分布を示す．縦軸は装置番号であり，横軸は攻撃元 IP アドレスの第 1 オクテットを示す．

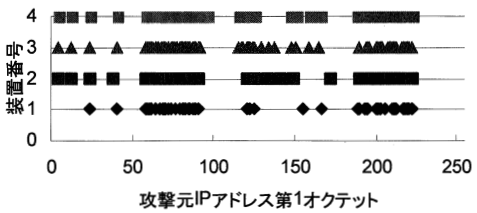

図 3：各装置で観測した攻撃元の分布

(2) ダウンロード元

ダウンロード元に着目することにより，IP アドレス空間上の論理的な地域性，国などの物理的な地域性を感染動作の分類に反映できる．図 4に IP アドレスで指定されたダウンロード元の分布を示す．縦軸は装置番号であり，横軸はダウンロード元 IP アドレスの第 1 オクテットを示す．

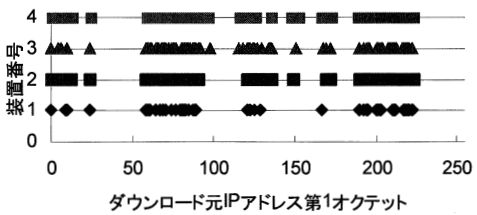

図 4：各装置で観測したダウンロード元の分布

(3) ダウンロード元へのアクセスプロトコル

ダウンロード元へのアクセスプロトコルに着目することにより，プロトコルの傾向を感染動作の分類に反映できる．Nepenthes には，マルウェア本体をダウンロードするプロトコルが複数実装されている．tftp, http, ftp に加えて，linkbot に実装されている link および blink と，Agobot に実装されている csend および creceive といったボット特有のプロトコルにも対応している[22]．ダウンロード元へのアクセスプロトコル比率をみると，link，ftp によるダウンロードが上位を占めていることがわかる(図 5)．

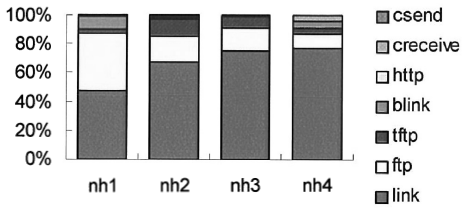

図 5：ダウンロード元へのアクセス
プロトコル比率

(4) アクセスプロトコルの成功率

アクセスプロトコルの成功率に着目することにより，アクセスプロトコルの可達性を感染動作の分類に反映できる．FTP についてはアクセスの利用では上位となっているが，ダウンロード成功率が低くなっている(図 6)．ログの収集環境の構成による影響調査については，今後の課題である．

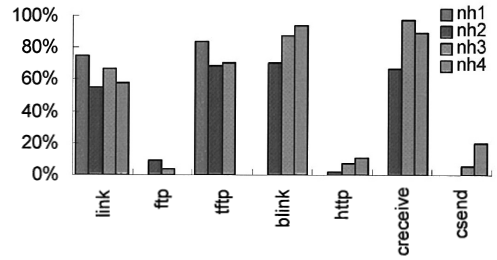

図 6：アクセスプロトコル毎の
ダウンロード成功率

(5) 攻撃元とダウンロード元の一致性

感染動作によっては，攻撃元とダウンロード元が必ずしも一致しない．図 7の上段は攻撃元からマルウェアをダウンロードする形態であり，下段は特定のサイトからマルウェアをダウンロードする形態である．このため，攻撃元とダウンロード元が同一であるか，否かは，感染動作の分類の指標として利用できる(図 8)．図 9は各装置で観測した攻撃元とダウンロード元の分布を示す．縦軸は IP アドレスの第 2 オクテットであり，横軸は IP アドレスの第 1 オクテットを示す．

図 4と図 9では，ホスト名で指定されているダウンロード元を除いてプロットしている．これは，時間の経過とともに，ホスト名に割当てられている IP アドレスが変わること，ホスト名に複数の IP アドレスを割当て可能なことを考慮したからである．また，図 8においては，ホスト名で指定されているダウンロード元は，攻撃元と不一致と仮定した．ホスト名の中で一番件数が多い urnst.dsaku72830.info では，延べ 1,965 件の攻撃において，攻撃元が 468 種類あることを考えると，この仮定は妥当であると推測できる．今後の課題として，攻撃発生時点でホスト名に割当てられている IP アドレスを記録し，検証を行う必要がある．

(6) マルウェアダウンロードに伴うアクセスプロトコル

マルウェア毎に，マルウェアがダウンロードされた際に使用されたプロトコルは，感染動作の分類の指標として利用できる(図 10).

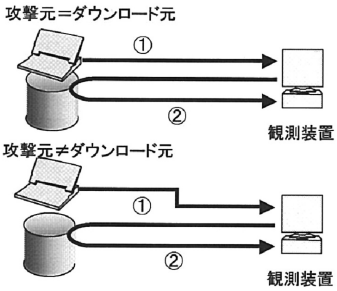

図 7：攻撃元とダウンロード元との関係

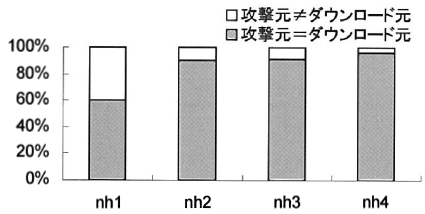

図 8：攻撃元とダウンロード元の一致性

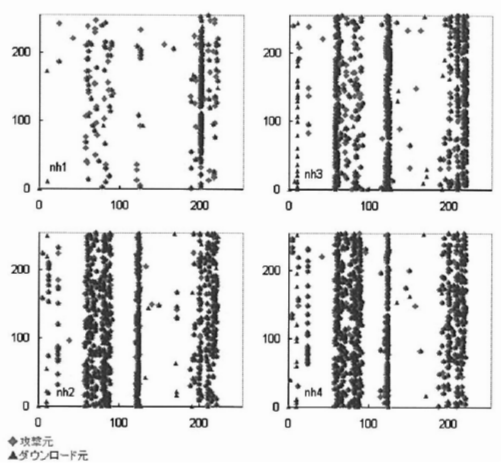

図 9：各装置で観測した攻撃元と
ダウンロード元の分布

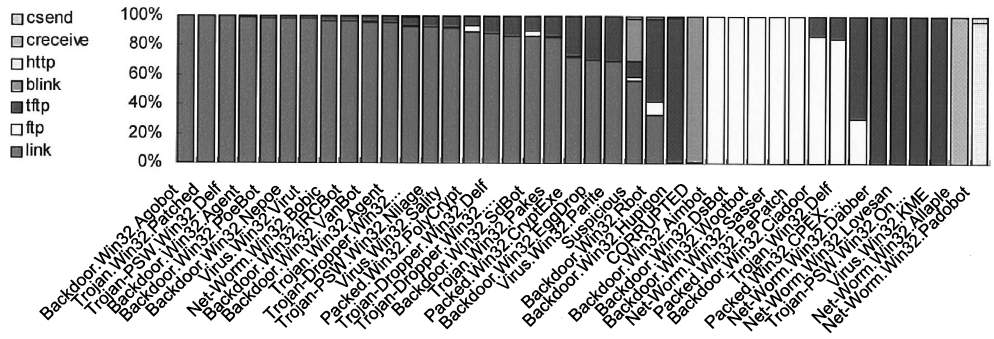

図 10：マルウェア毎のダウンロードに伴うアクセスプロトコル

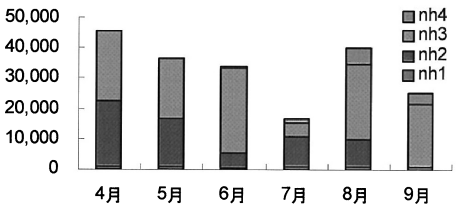

図 11：各装置の攻撃件数推移

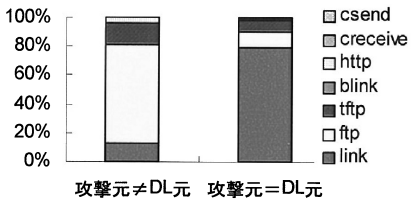

図 12：攻撃元とダウンロード元の一致性とアクセスプロトコル

4.2 考察

(1) 観測時間軸について

調査期間中の攻撃件数の推移を図 11に示す. 本調査では，感染動作の分類に観測時間軸を加味した調査を行うことができなかったが，攻撃元／ダウンロード元／アクセスプロトコルと観測時間軸との組み合わせも感染動作分類に利用できると考える.

(2) 攻撃元とダウンロード元の一致性について

攻撃元とダウンロード元が一致しない場合には，ftp, 一致する場合には link によるアクセスが多い(図 12). 一致しない場合には，色々な感染ホストからアクセスがあるという特性上，FTP/ HTTP/ TFTP などの待ち受け型の標準プロトコルが用いられていると考えられる.

また，今回の調査の結果，ダウンロード元へのアクセスがホスト名で指定されているレコードのうち，全ての装置に共通して存在するホスト名として，ssffttpp.jackill07.biz，urnst.dsaku72830.info, c0re.servehttp.com の 3 つを観測した．この中で，ssffttpp.jackill07.biz，urnst.dsaku72830.info については，次のような特徴が見られた.

- ホスト名と IP アドレスの対応(DNS の設定)が不定期ではあるが，変更されている.
  ダウンロードできるマルウェアのハッシュ値が不定期ではあるが，変更されている. urnst.dsaku72830.info からマルウェアを日次でダウンロードし，ハッシュ値を比較したところ，2007 年 11 月～12 月の 2 ヶ月間で 11 回更新されていた．このうち 10 回は同じタイミングで，ssffttpp.jackill07.biz でも同じハッシュ値のファイルがダウンロード可能であった.
- 2 つのドメインには，同じ IP アドレスが設定されており，異なるポート番号で，FTP サーバが稼動している.

また，上記 2 つのホスト名がダウンロード元になっているログは，nh1 で多く観測されており，IP アドレス空間上の論理的な地域性，国などの物理的な地域性に関連していると思われる.

(3) マルウェアのダウンロードについて

攻撃元とダウンロード元が一致しない感染活動を行うマルウェアを調査した結果，Backdoor.Win32.{Aimbot | PoeBot | Rbot | SdBot | VanBot}，Trojan.Win32.Agent の 6 種類に留まった. また，図 13に示す通り，装置毎にダウンロードするマルウェアの比率は異なっていることから，観測装置の IP アドレス空間上の論理的な地域性とダウンロードするマルウェアとの組み合わせも感染動作分類に利用できると考える.

5 おわりに

本稿では，マルウェア本体を捕獲する Nepenthes を用いて収集したデータを元に，攻撃元，ダウンロード元，アクセスプロトコルなど感染動作に着目した調査結果を報告した.

また，本調査を通して，異なる組織で保有している複数の観測装置を利用することで，次のような効果が得られた．

- 単一の観測点で発生している事象なのか，複数の観測点で発生している共通的な事象なのかを知ることができる．
- 特定のダウンロード元については，長期間に渡り，複数の装置で観測した．このようなダウンロード元の情報は運用面でのマルウェア対策に活用できる．

今後の課題は，本調査結果を元にマルウェアの感染活動の分類を行うと共に，ファイアウォールのログと組み合わせた観測，同様な観測装置を有する組織との協力による観測システム拡大などの検討が挙げられる[23].

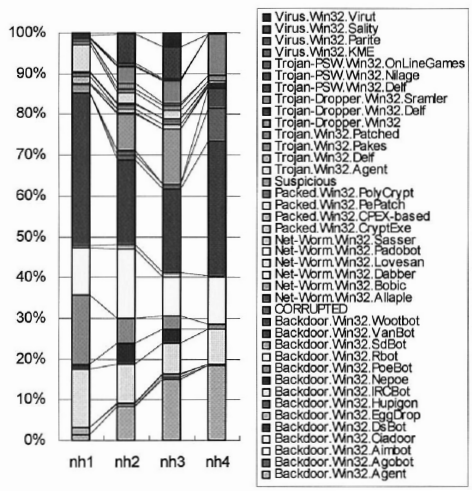

図 13：装置毎のマルウェアダウンロード比率

謝辞

本研究を進めるにあたって有益な助言と協力を頂いた東海大学の小堀智弘氏ならびに，NTT-CERT 関係者各位に深く感謝致します．

参考文献

1) Nepenthes: http://nepenthes.mwcollect.org/
2) 朝長秀誠 他：Botnet の命令サーバドメインネームを用いた Bot 感染検出方法，情報処理学会 CSEC 研究報告 No.129 p13-18 (2006 年 12 月)
3) 釘崎裕司 他：トラフィック解析に基づくボット検知手法, 情報処理学会 CSEC 研究報告 No.48 p57-62 (2007 年 5 月)
4) 阿部義徳 他：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 (2007 年 9 月)
5) 竹森敬祐 他：無操作ホストから発信されるパケットに注目したウィルス感染検知，情報処理学会 CSEC 研究報告 No.16 p141-146 (2007 年 3 月)
6) 高見知寛 他：セキュリティインシデントをトリガとしたボット検知方式：スパム発信に注目した異常検知，CSS2007 (2007 年 10 月)
7) 竹森敬祐 他：セキュリティインシデントをトリガとしたボット検知方式： 宛先 IP とドメインに注目した不正検知，CSS2007 (2007 年 10 月)
8) 松木隆宏 他：悪性プログラムの耐解析技術を逆用した活動抑制手法の提案，CSS2006 (2006 年 10 月)
9) 松木隆宏 他：セキュリティ無効化機能を逆用したマルウェア活動抑制手法の検討，CSS2007 (2007 年 10 月)
10) 高橋正和 他：フィールド調査によるボットネットの挙動解析，情報処理学会論文誌 Vol.47 No.8 p2512-2523 (2006 年 8 月)
11) 岡田隼人 他：BOT コードの静的解析によるネットワークアクセス情報抽出について，電子情報通信学会技術研究報告 Vol.107 No.347 p37-41 (2007 年 11 月)
12) 星澤裕二 他：マルウェアの亜種等の分類の自動化，情報処理学会 CSEC 研究報告 No.71 p271-278 (2007 年 7 月)
13) 岩本一樹 他：コンピュータウイルスのコード静的解析による特徴抽出と分類について，電子情報通信学会技術研究報告 Vol.107 No.397 p107-113 (2007 年 12 月)
14) 安本幸希 他：マルウェアコードの類似度判定による機能推定，電子情報通信学会技術研究報告 Vol.107 No.345 p31-36 (2007 年 11 月)
15) 星澤裕二 他：マルウェアの動作条件の抽出，情報処理学会 CSEC 研究報告 No.71,p265-269 (2007 年 7 月)
16) 須藤年章 他：仮想インターネットを用いたボットネット挙動解析システムの評価，CSS2006 (2006 年 10 月)
17) Shadowserver Foundation - Statistics: http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.Statistics
18) サイバークリーンセンター活動実績：https://www.ccc.go.jp/report/200712/0712monthly.html
19) 堀合啓一 他：定点観測によるボットネットの挙動観測とログ情報の視覚化，SCIS2007 (2007 年 1 月)
20) snort: http://www.snort.org/
21) Kaspersky: http://www.kaspersky.co.jp/
22) The Nepenthes Platform: http://www.atsystemgroup.org/system/files/nss07_wicherski_georg_the_nepenthes_platform_automated_botnet_detection_and_mitigation.pdf
23) IIJ : Malware Investigation Task Force - マルウェアの捕獲，解析，対策，http://www.iij.ad.jp/news/seminar/2007/techdays.html