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

仲小路 博史[†1]　川口 信隆[†1]　鬼頭 哲郎[†1]
小堀 智弘[†2]　菊池 浩明[†2]　寺田 真敏[†1]

†1) (株)日立製作所　システム開発研究所
〒212-8567 神奈川県川崎市幸区鹿島田 890
†2) 東海大学
〒259-1292 神奈川県平塚市北金目 1117

概要：近年，ボットの亜種の大量発生や，コードの難読化，通信の暗号化などによって，従来の IDS やウイルス対策ソフトなどの対策手法では防ぎきれない個体が増加傾向にある．特にネットワーク上での対策においては，暗号化通信による隠匿が大きな障壁となっており，パターンマッチングによらない検知手法の開発が課題となっている．本稿では，ボット感染ノードによる通信の「見える化」を試み，近年のボットの活動に現れる特有の事象を確認する．また，その事象を手掛かりにトラフィックからボットの活動と思しきパケットを抽出し，ボット感染ノードおよび司令サーバの推定を行う．
キーワード：ボット，同調活動，可視化，検知

Visualization of the commands and responses of botnets focused on the synchronization of packet transmission

Hirofumi Nakakoji[†1]　Nobutaka Kawaguchi[†1]　Tetsuro Kito[†1]
Tomohiro Kobori[†2]　Hiroaki Kikuchi[†2]　Masato Terada[†1]

†1) System Development Lab. Hitachi Ltd.
890 Kashimada, Saiwai-ku, Kawasaki, Kanagawa, 212-8567 Japan
†2) Tokai University.
1117 Kitakaname, Hiratsuka, Kanagawa, 259-1292 Japan

Abstract: In recent years, many bots has a large number of variants and uses code obfuscation and encryption channels to evade existing IDS and anti-virus software. In particular, encryption channels can prevent network-based approaches from analyzing packet contents, and therefore demand for the development of new detection methods that does not rely on pattern matching is increasing. In this research, we visualize the communication of bots and reveal the features of their activities. Then, we extract packets related to the bots activities from traffic based on the features, and identify the hosts infected by the bots and the command servers.
Keywords: Bot, synchronized activity, visualization, detection

1　はじめに

世界初のネットワークワーム（以降，単にワームと記す）とされる Morris ワーム[1]が 1988 年に発生したことを発端として，2001 年には Nimda[2]や CodeRed[3]などのインターネットに甚大な被害をもたらした高機能なワームが相次いで発生し，ネットワーク管理者や利用者は幾度となくそれらの脅威に対抗してきた．近年では，ワーム作成ツールの普及・高機能化に伴い，ツールさえ入手できれば誰でも容易に新種のワームを作成できてしまう状況となっている．ワーム作成の動機も，従来の自己顕示欲によるものから，個人情報の取得やスパムメールの送信などといった金銭目的によるものへと変わってきている．このような動機の変化か

ら，利用者に気づかれることなく長期間，端末に潜伏するような性質を有したボット型ワーム（以下，単にボットと記す）が蔓延するなど，脅威の実態の「見えない化」が進行している．

これらの脅威に対しては，利用者端末上でのウイルス対策ソフトの利用や，ネットワーク上での IDS などの利用が一般的に行われている．しかしながら，亜種の大量発生や，コードの難読化，通信の暗号化などによって，従来の対策手法では防ぎきれない個体が増加傾向にある[4]．特にネットワーク上での対策においては，暗号化通信による隠匿が大きな障壁となっており，ペイロードのパターンマッチングによる不正な通信の検知は益々困難になっている．

以上のような背景から，著者らは，ネットワーク管理者の分析活動を支援するために，文献[5]のようにワームに感染したノードが新たな感染先ノードを探索する際にネットワークへ送信するノード探索パケットの送信間隔の周期性に着目することにより，ノード探索特性を定量的に示してきた．また，ノード探索パケットの宛先 IP アドレスに含まれる 4 つのオクテットの値に着目してノード探索特性の可視化を行うことにより，それぞれのオクテットの値の走査範囲，均一性，周期性を確認する方式を提案した[6]．本稿では，CCC（Cyber Clean Center）[7]より提供された研究用データセット CCC DATAset 2008 の攻撃通信データ（以下，単に攻撃通信データ）を，上記可視化技術を用いて「見える化」し，近年のボットの活動に現れる特有の事象を確認する．また，そこで得られた知見をもとに攻撃通信データに含まれる全トラフィックデータからボットの活動と思しきトラフィックを抽出し，ボット感染ノードおよび司令サーバの同定を行う．

ISP やイントラネットなどのネットワーク管理者が，これらの知見をワームによるインシデント発生の発見に活用したり，IDS や FW のルール作成に活用したりすることで，より迅速で的確な対策の立案や，ボットによるトラフィックの制御が可能になると考える．

本稿の構成について述べる．2 章では，文献[6]で提案したワームによるノード探索活動の可視化手法を紹介し，攻撃通信データへの適用を試みる．3 章では，攻撃通信データがボット感染ノードによる通信であることに着目して 2 章で紹介した可視化手法の拡張し，可視化結果によって得られた知見を報告する．4 章では，可視化によって得られた知見に基づき，攻撃通信データからボット感染ノードへの司令サーバの同定を試みる．そして 5 章に考察としてまとめる．

2　パケット送信活動の可視化

ワームによる他ノードへの感染活動には，活動に関わるパケットの送信タイミング，感染先 IP アドレスの生成規則，感染先ポート番号とプロトコルの選択規則との 3 つの軸に特徴が現れることを文献[6]で述べた．本章では，感染先をボットのパケット送信先に置き換えて，これらパケット送信活動の特徴のうち，パケット送信先 IP アドレスの生成規則の可視化を行う．

2.1　可視化の手順

可視化にあたっての特徴は，次の通りである．

- パケットの送信活動を忠実に再現するために動画像を用いて表示する．
- パケットの送信先ノードの IP アドレスの規則性を正確に表現するために，IP アドレスを 4 つのオクテットに分解し，それぞれの値を可視化する．

本可視化では，パケット送信活動の概要を把握するために，ボット感染ノードがパケットを送信している様子を図 1 に示すように表現し，そこに見られる IP アドレス生成順序の規則性を把握する．まず，オクテットの値が巡回するような（0 の次の値が 255 に，あるいは 255 の次の値が 0 にジャンプするような）現象を連続的な変化として捉えられるようにするために，パケット送信先ノードの IP アドレスを構成している 4 つのオクテットを，円の中心から外周に向けて放射状に配置した 4 つのラインでそれぞれ表現し，各オクテットの値を，対応する各ラインの回転角に置き換えて表す．加えて各オクテットの値の推移をわかりやすく表現するために，一定時間の残像を表示することで，IP アドレスを構成する各オクテットの値の規則性を確認する．

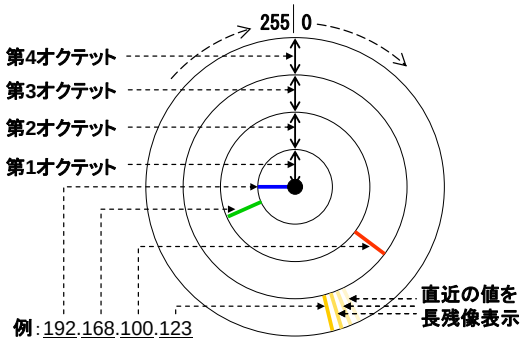

図 1 IP アドレス生成規則の可視化

2.2　データの準備

研究用データセット CCC DATAset 2008 には，CCC に設置されたハニーポットに関わる下記の 3 種類データが含まれている．

(1)　マルウェア検体[1]
(2)　攻撃通信データ
(3)　攻撃元データ

上記データのうち，可視化には，ハニーポットとのトラフィックが記録された (2) 攻撃通信データを利用する．

攻撃通信データには，ハニーポット 2 台分のトラフィックを tcpdump[8]を用いて 2 日分パケットキャプチャして得られた約 1,600 万パケットのデータが含まれている．以降では，それぞれのハニーポットをハニーポット 0 (H0)，ハニーポット 1 (H1) と呼ぶ．

ここでは，ハニーポットに感染したボットによる他ノードへのパケット送信状況 (1 台分) を可視化するために，可視化対象データとして，攻撃通信データに含まれるパケットの中から，以下の条件を満たすパケットを抽出した．

- 送信元 IP アドレスがハニーポット 0 の IP アドレスと一致
- UDP プロトコルもしくは TCP プロトコル

2.3　攻撃通信データの可視化

準備したデータ (以降，H0 データと記す) に含まれるパケット送信時間と，宛先 IP アドレスをもとに IP アドレス生成規則を可視化した様子を図 2 に示す．その結果，宛先 IP アドレスの第 1,2,3 オクテットが固定であること，第 4 オクテットは，時計回りにスイープ (値が順序正しく単調増加) していることが確認できる．この特性は MSBlaster[9]にも同様に見られ，近隣のノードを優先的に探索することで，パケットの到達性を向上させていると考える．

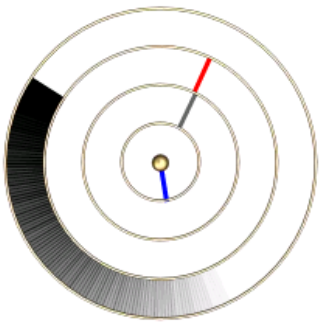

図 2 ハニーポット 0 によるパケット送信活動

[1] 検体のバイナリデータではなく，検体のバイナリハッシュ値データが提供される．

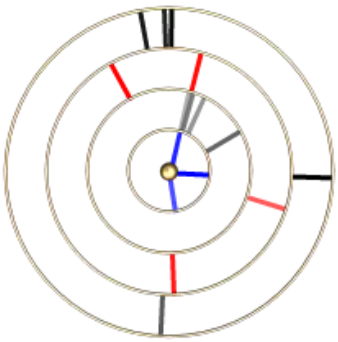

図 3 規則性の確認できない可視化例

実際には H0 データとは異なって，攻撃通信データには様々なパケットが含まれており，攻撃通信データに含まれるボットの活動を可視化にあたっては，以下の点に留意する必要がある．

(1)　複数台 (2 台) のハニーポットの存在
(2)　ボットの多重感染
(3)　インバウンドトラフィックの存在

攻撃通信データには 2 台のハニーポットに関わるトラフィックが含まれているため，これまでに提案してきた可視化手法では 2 台分の活動が重なり合って表示される場合がある．また，それぞれのハニーポットは，同時に複数のボットが感染している可能性があり，これらのボットによる活動も重なり合って表示される場合がある．さらに，ハニーポットによる活動 (アウトバウンドパケット) だけではなく，ハニーポットへの攻撃や指令 (インバウンドパケット) も含まれている．実際に，攻撃通信データを可視化した場合，図 2 に示したように特徴が明確に現れるパケット送信活動を確認できる時間帯もあったが，全く活動していない時間帯や，図 3 に示すように IP アドレスの生成規則に規則性が見られない時間帯も多く確認できた．

3　ボット通信の可視化手法の提案

2 章では，既存の可視化手法を用いて，ボットに感染したハニーポットのパケット送信活動の規則性を確認できた．一方，攻撃通信データに含まれる複数の事象の重なりによって，通信の把握に可視化が有効に働かない場合もあることを確認できた．本章では，攻撃通信データに含まれるボット通信の特性を把握するために，提案した可視化手法の拡張を行う．

3.1　可視化手法の拡張

2.3 節で挙げた攻撃通信データの可視化における課題を解決するために，以下に示す 3 つの拡張を行った．

(1)　2 台のハニーポットトラフィックの分離

(2)　宛先ポート番号の可視化
(3)　通信方向の可視化

攻撃通信データをハニーポット毎に分けて可視化することにより，同時刻における個々のハニーポットのパケット送受信活動の視認性を確保する．また，ボットの多重感染活動を少しでも見分けるために，宛先ポート番号を可視化の要素に組み込む．さらに，通信のインバウンドとアウトバウンドを見分けるために，パケットの向きも可視化の要素に組み込む．

可視化の手順を以下に示す．X 軸を 4 段階に分けて，各段階をパケットの送信元 IP アドレスのオクテット数に対応付け，Y 軸を各オクテットの値（0～255）に対応付ける．また，宛先ポート番号を色によって表現する．さらに，インバウンド（宛先 IP アドレスがハニーポットの IP アドレスと一致するパケット）と，アウトバウンド（送信元 IP アドレスがハニーポットの IP アドレスと一致するパケット）とをそれぞれ異なる領域（上段／下段）に描写する．

図 4 には，1 つのハニーポットに対するインバウンド（192.168.100.123 からハニーポットの 135/tcp に対する）パケットと，アウトバウンド（ハニーポットから 172.16.50.240 の 80/tcp に対する）パケットの例を示している．2.1 節で提案していた可視化手法と同様に，時系列変化をアニメーションさせることにより表現し，さらに各オクテットの値の推移を表現するために，一定時間の残像を表示させる．

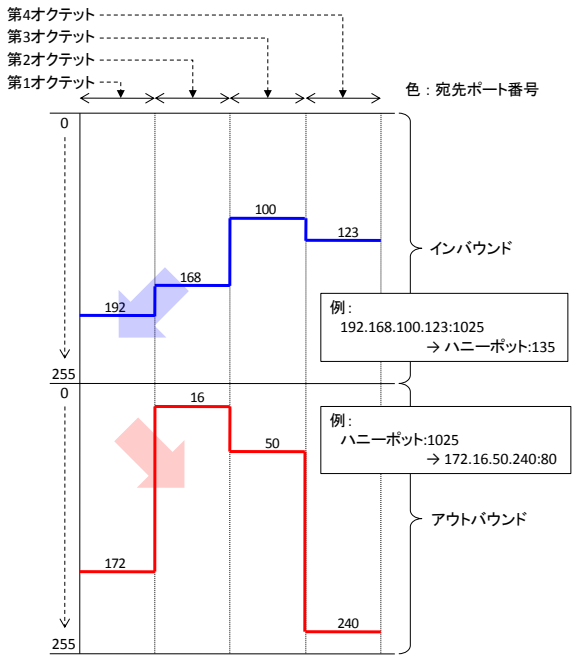

図 4 パケット送受信の可視化

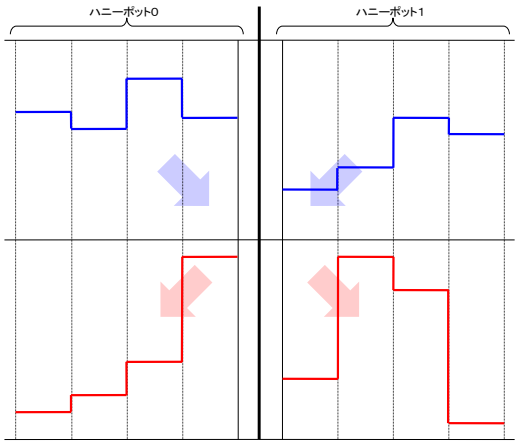

図 5 IP ハニーポット 2 台の同時可視化

次に，2 台のハニーポットのパケット送受信活動を同時に観察できるように，個々のハニーポットを並べて表示する（図 5）．左側がハニーポット 0，右側がハニーポット 1 の活動を可視化する領域である．なお，2 台のハニーポットの状態を比較しやすくするために，ハニーポット 0（左側）の描画領域を左右反転させて表示する．

3.2　攻撃通信データの可視化

本節では，3.1 節で提案した可視化手法を用いて，攻撃通信データの可視化を試みる．

攻撃通信データにおける 2008/04/28 17:20:10 付近の両ハニーポットによるパケット送受信活動の様子を図 6 に示す．

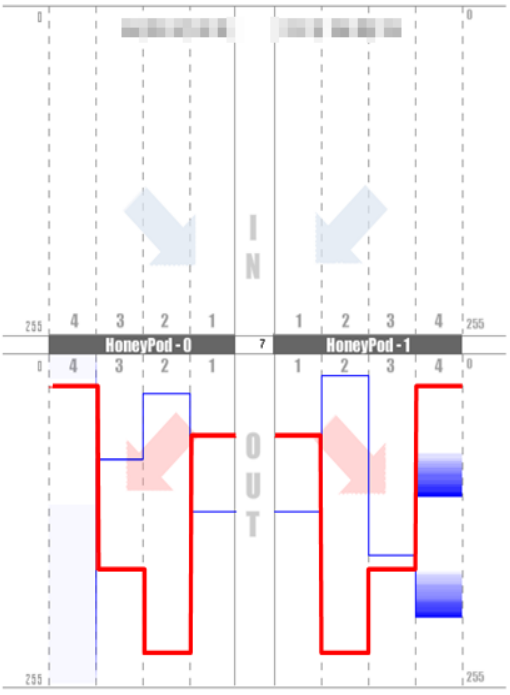

図 6 アウトバウンドの同調例

青色（原稿中では細線）で示されている線は宛先ポートとして 135/tcp を設定しているパケットを示し，赤色（原稿中では太線）で示されている線は宛先ポートとして 25/tcp を設定しているパケットを示している．この可視化結果では，25/tcp へのパケット送信を示す赤色（太）の線が左右対称になっていることから，両ハニーポットはほぼ同じ時刻に，同じメールサーバにパケットを送信していることが確認できる．同時に，それぞれのハニーポットは異なる IP アドレスを持つノードに対して 135/tcp を狙ったスキャン攻撃（青色／細）を仕掛けていることがわかる．

次に 2008/04/29 15:15:46 付近の両ハニーポットによるパケット送受信活動の様子を図 7 に示す．黒線（原稿中では太線）で示されるパケットが上下で同じ形状を構成していることから，インバウンドの送信元 IP アドレスとアウトバウンドの宛先 IP アドレスが同一であることが確認できる．さらに，左右対称であることから，両ハニーポットは同時刻に同じノードと通信していることがわかる．

2 台のハニーポットのパケット送受信活動は，多くの時間帯において異なる傾向を示したが，上記 2 つの例で示した他にも，両ハニーポットが同時刻に同じノードからパケットを受信したり，同じノードへパケットを送信したりする『同調活動』を確認することができた．

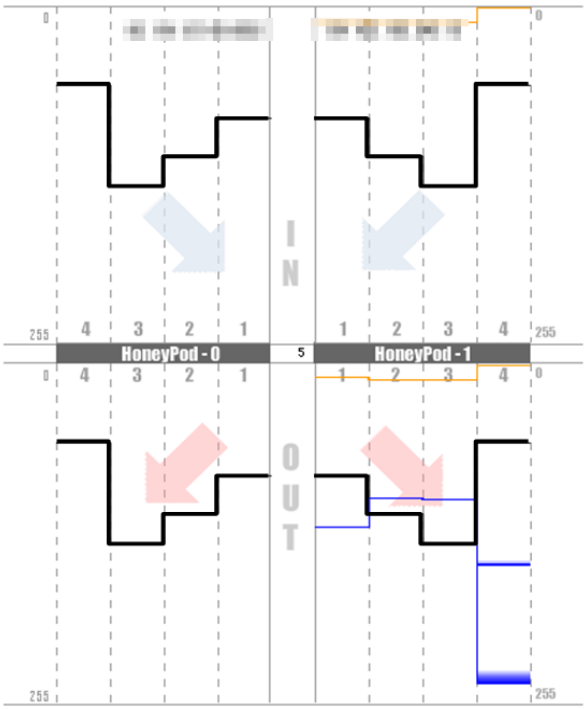

図 7 インバウンドの同調例

3.3 同時接続活動に基づく検知

前節では，攻撃通信データに 2 台のハニーポットによる同調活動パケットが含まれることを確認した．これは図 8 に示すようなボットの活動に表れる特徴に起因するものと考える．

一般的にボットに感染したノードは，C&C（Command and Control）サーバと呼ばれる司令塔の役割を担うノード（例えば IRC サーバ）に接続してハーダ（司令者）からの指令を待つ．C&C サーバは，同種のボットに感染した多数のノードが同時に接続している状態となる．次に，ハーダは，C&C サーバに対して指令文を送信する．指令文は直ちに同サーバに接続しているボット感染ノードに展開されることになる．図 7 に示した可視化画面上段に現れたインバウンドの左右対称の形状は，上記状況を捉えたものと考える．次に，指令文を受信したボット感染ノードは，上記指令文の内容に従い行動（反応）を起こす．例えば，ボット感染ノード自身のステータスを返したり（図 8-反応１），他のメールサーバに対してメールを送信したり（図 8-反応２），DDoS 攻撃や，感染拡大活動などを行う．可視化画面下段に現れたアウトバウンドの左右対称の形状は，上記状況を捉えたものと考える．

複数のハニーポットのトラフィックを監視し，ハニーポット群とは異なるノードへのパケット送信，あるいは他のノードからのパケット受信に同調活動を確認できた場合は，ボット感染ノードへの指令，あるいは同じ指令を受けたボット感染ノードからの反応に関わる何らかのパケットが流れていたと推測できる．この知見に基づき，攻撃通信データから同調活動の特徴を示すパケットを抽出した．抽出結果の一部を表 1 に示す（同調許容時間は前後 1 秒）．

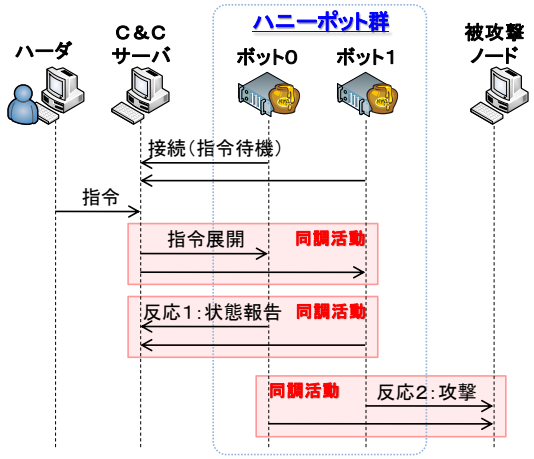

図 8 ボット通信の流れ

表 1 同時刻・同ノード接続一覧（許容 1 秒）

No.	日時	方向	IP アドレス	H0 のポート番号	H1 のポート番号
1	04/28 08:18:57	IN	aaa.215.15.145	80 > 3131 /tcp	80 > 1033 /tcp
2	04/28 09:33:17	OUT	bbb.233.167.25	3086 > 25 /tcp	3030 > 25/tcp
3	04/28 13:18:15	OUT	bbb.233.183.25	1159 > 25 /tcp	2269 > 25 /tcp
4	04/28 17:19:46	IN	ccc.130.197.204	2120 > 20663 /tcp	1942 > 6070 /tcp
5	04/28 17:19:48	OUT	bbb.233.167.25	1150 > 25 /tcp	2105 > 25 /tcp
6	04/28 17:35:42	IN	ddd.196.42.138	4777 > 20663 /tcp	4498 > 6070 /tcp

3.4 検証

前節の抽出結果を，攻撃通信データ（pcap データ）を用いて検証した．No.1 は，Web サーバ（aaa.215.15.145）との TCP コネクションの中で ACK のタイミングが一致していた事象を捉えたものであった．No.4,6 は，両ハニーポットが受信したパケットのペイロードに“CONNECT smtp2.google.com:25 HTTP/1.0”という共通の文字列が含まれていたことから，メール送信用 Proxy サーバとして両ハニーポットを悪用した活動を捉えたものであると考える．No.2,3,5 は，SMTP サーバ(bbb.233.167.25, bbb.233.183.25)への接続を捉えたもので，両サーバの通信ともに接続は成立していなかった．

検証を通じて，2 台のハニーポットが同じ目的を持つパケットを，同時刻に送受信していることを確認できた．また，表 1 に示した以外にも同調許容時間 1 秒で約 700 件，同 10 秒で約 5800 件と，多くの同調活動を確認することができた．この数値は，全体のパケット数の 1%にも満たないが，ハニーポットの台数を増やすことにより組み合わせの数も増やすことができるため，同調活動の検出数の向上が見込める．

4 まとめと今後の課題

本稿では，ワームによるノードの探索活動の可視化手法を拡張し，攻撃通信データに適用した．その結果，攻撃通信データに含まれる 2 台のハニーポットが，同時刻に同じノードと通信を行っている同調活動を複数確認することができた．これらは，2 台のハニーポット（ボット感染ノード）が同じ C&C サーバから発せられた指令パケットを受信した場合や，その指令によってハニーポットが自身のステータスの通知やメールの送信などの反応活動を行った場合に見られる現象であることがわかった．

同調活動に着目することにより，C&C サーバの特定や，ボット感染ノードの検出に活用できると考える．本手法は，通信先ノードおよび送受信タイミングに基づいて検知が可能である．つまり，C&C サーバとボット感染ノード間の通信が暗号化されていたとしても検知できる．

今後は，プロトタイプの実装および有効性の評価を行う．また，定期的な更新を行うソフトウェアアップデートツールなどの正常なプログラムの誤検知を防止するために，指令および反応パケットのディレイタイムの一致性にもとづいた検知手法を提案したい．

文　献

[1] ITpro，インターネット・ワームの原点「Morris Worm」の脅威，http://itpro.nikkeibp.co.jp/members/ITPro/SEC_CHECK/20010907/1/

[2] symantec，W32.Nimda.E@mm，http://www.symantec.com/region/jp/sarcj/data/w/w32.nimda.e@mm.html

[3] symantec，CodeRed Worm，http://www.symantec.com/region/jp/avcenter/venc/data/codered_worm.html

[4] Internet Watch，ボット対策を議論「もはや感染予防ソリューションでは対応不可能」，http://internet.watch.impress.co.jp/cda/event/2007/06/14/16051.html

[5] 仲小路博史，寺田真敏，周波数分析に基づくインシデント傾向検知手法に関する検討，Computer Security Symposium 2005, ISEC-193, SITE-192, pp.83--88 (2005)

[6] 仲小路博史，寺田真敏，洲崎誠一，ノード探索特性の可視化および定量化の提案，情報処理学会論文誌, Vol.48, No.9, pp.3163--3124 (2007)

[7] 総務省・経済産業省 連携プロジェクト Cyber Clean Center，https://www.ccc.go.jp/

[8] Manpage of TCPDUMP，http://www.linux.or.jp/JM/html/tcpdump/man1/tcpdump.1.html

[9] TRENDMICRO, WORM_MSBLAST.A，http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A

[10] 経済産業省：平成 18 年度ボット対策プロジェクト活動実績の公表について，http://www.meti.go.jp/press/20070425003/kouhyou-set.pdf