マルウェア感染時のトラヒック特徴に関する一考察

森 悠樹 †　　市野 将嗣 †　　畑田 充弘 ‡　　小松尚久 †

† 早稲田大学理工学術院
〒 169-8555 東京都新宿区大久保 3-4-1

{mori,ichino,komatsu}@kom.com.waseda.ac.jp
‡NTT コミュニケーションズ株式会社
〒 108-8118 東京都港区芝浦 3-4-1 グランパークタワー 17F

m.hatada@ntt.com

あらまし　近年，マルウェアによる被害が問題視されており, それらへの対策として感染の検知は不可欠なものである．そこでマルウェア感染時の異常なトラヒックデータを正常時のトラヒックデータと比較することで感染の検知を行うシステムを検討する．感染検知のためにトラヒックデータから特徴量を抽出し, それらに対して識別器を用いて判定を行う．本稿では,C&C サーバとの通信やマルウェアのダウンロード時の通信などを利用したマルウェア感染検知の識別器設計の方針を述べ，特徴量を整理し, 研究用データセット CCC DATASet 2009 の攻撃通信データを用いた特徴量に関する検討結果について述べる．

A study on features of malicious traffic

Yuki Mori†　　Masatsugu Ichino†　　Mitsuhiro Hatada‡　　Naohisa Komatsu†

†Faulty of Science and Engineering, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo, 169-8555, Japan

{mori,ichino,komatsu}@kom.com.waseda.ac.jp
‡NTT Communications Corporation
Gran Park Tower 17F, 3-4-1 Shibaura, Minato-ku, Tokyo, 108-8118 Japan

m.hatada@ntt.com

Abstract　Damage by malware attack has been viewed with suspicion recently. So detecting infected PCs is necessary for the attacks. Against this background, we have studied the infected PC detecting method by comparing malicious traffic with normal traffic, where features of malicious traffic are extracted and a classifier to detect malicious traffic is designed. In this paper, we propose an outline of the designing classifier using traffic between infected PCs and C&C server or traffic to download malwares. Simulation results are also described using CCC DATA Set 2009.

1　本研究の背景と目的

昨今のインターネットの普及により，マルウェアの脅威が広がっている．マルウェアとは悪意のあるソフトウェア (Malicious Software) の略称であり，その被害は個人情報の流出やパソコンの乗っ取りというように我々の生活を脅かす存在となっている．文献 [1] によると 2009 年度

上半期の日本国内での被害報告数は約 2 万 8 千件にものぼっており，活動が表面化しないボットネットによる被害の増加や Web からの感染が増加しているという現状で，早急に対策を講じる必要がある．

これまでの対策研究としては，文献 [2] で整理されているように，PC がマルウェアに感染しているかどうかを検知するためのマルウェアの感染検知，感染後の挙動の観測やコードの解析を行うマルウェアの検体解析，ハニーポットを用いたボットネット等の活動状況の観測を行う広域観測といった視点で研究が行われている．

ボットネットによる感染は気付きにくいという問題がある．感染検知は，感染の拡大を防ぐという意味で重要なことである．しかしながら，従来の感染検知では，既知のマルウェアのみしか検知することができない．新種のマルウェアを検知するために，マルウェア感染時のトラヒックデータの変化に着目し，パターン認識の技術に基づく識別器を用いたマルウェアの感染検知手法を用いることが考えられる．

そこで本研究では特にマルウェアの感染検知に着目して，識別器を設計する上で必要とされる特徴量の整理や有効性の評価といった基礎的検討の結果を報告する．

以下では，感染検知の従来手法，関連研究を紹介し，識別器を扱う上での注意点を述べる．また CCC DATASet 2009[3](以下 CCC2009) を用いた，マルウェア感染時のトラヒックデータの特徴及び識別器の利用可能な特徴量の調査結果を示す．

2 感染検知

2.1 感染検知の分類

文献 [2][4] を参考に感染検知の従来手法について簡単に整理する．

1. シグネチャベースによる検知

マルウェアごとにシグネチャデータを用意することで，パターンマッチングを行い検知する手法である．新たなマルウェアが現れるごとに分析をする必要があり，未知のものは検知できないといった課題がある．

2. ルールベースによる検知

脆弱性をつく攻撃に関してルールを設定することで，そういったパケットが到着した際に感染を検知する手法である．ゼロデイ攻撃のような，新たな脆弱性をついた攻撃には対応しきれないという課題がある．

3. トラヒックデータを用いた感染検知

ボットネットにおける C&C サーバと感染した PC 間の通信や感染後の DNS クエリの異常に着目することで検知を行う．

4. イベント観測

マルウェアの感染後の動作として現れる，DDoS 攻撃やスパムメール発信という発症活動に着目し感染したホストの検知を行う．

5. 自己防衛機能の逆用

デバッガや仮想マシン環境の利用といったマルウェアの装甲化機能を逆用することで検知を行う．

2.2 トラヒックデータを用いた感染検知の従来研究

トラヒックデータには時間的な変化があり，識別器に対して連続的な入力が仮定できる．この時間的な変化に着目することで，感染検知の性能が向上する可能性がある．例えばバイオメトリクスでは，発話時の唇動作個人認証において複数のアルゴリズムが提案されているが，時系列を使用しないアルゴリズムと使用するものを比較した際，後者のアルゴリズムのほうが高い精度での認証が可能であることが示されている [5]．そこでトラヒックデータから得られる特徴量の時系列データに着目する．

トラヒックデータを用いた感染検知の従来研究を紹介する．

文献 [4] では，ボットに感染した PC と C&C サーバとのセッションと Web 閲覧等とのパケットサイズの違いに着目している．またトラヒックデータよりパケットサイズ，送受信間隔によるヒストグラムを特徴量とし，SupportVectorMachine(SVM) を用いて C&C サーバのセッションを検知し，SVM が有効であることを示した．

文献 [6] では，文献 [4] と同様に C&C サーバとの通信の特徴として，パケットサイズと送受信間隔に着目し，C&C セッションにおける送信パケットが通常の IRC 通信と比較し応答時間が短く，Web 閲覧と比べて送受信パケットサイズの違いが顕著であることを確認している．加えてボットに使用される感染開始時からの通信プロトコルの遷移の仕方を特徴として提案している．

文献 [7] では，トラヒックデータからハニーポットの特徴的な挙動として攻撃を受けながらも感染しなかったケース，マルウェア本体のダウンロードにいたらなかったケース，攻撃から活動に至るまでの一通りの動作が行われたケース，複数の感染が確認されたケースが存在することを示している．また，DNS クエリに着目し，Windows2000 では IP アドレスを指定した正引きが行われ，WindowsXP ではリゾルバの逸脱を確認し，感染初期の活動の検知にこれらの特徴が利用できる可能性を示している．

2.3 感染検知のための識別器の設計方針

パターン認識とは入力されたパターン (指紋等の画像や) をいくつかのクラスごとに分類することができるとき，あるパターンを複数のクラスに対応させることである [8].

まず入力パターンに対し正規化やノイズ除去といった前処理後，特徴量を数値化して抽出する．抽出できた特徴をまとめて特徴ベクトルとし識別に用いる．いま d 個の特徴を用いるとき，特徴ベクトルは式 (1) で表される．

$$\vec{\mathbf{x}} = (x_1, x_2, \ldots, x_d)^t \qquad (1)$$

この特徴ベクトルによって構成される空間を特徴空間と呼ぶ．ある 1 つのパターンは特徴空間上の 1 点を示すこととなり，同一クラスに属するパターンは互いに類似しているためまとまったかたまりとして観測される．つまり特徴空間上に存在する複数のパターンを，クラスごとに分類できる識別境界の作成が識別器の設計ということになる．

未知の入力パターンを適切なクラスに分類することが目的であり，そのためにクラスごとのサンプルを用いて学習を行い，識別境界面を作成し，分類することとなる．手順を図 1 に示す．

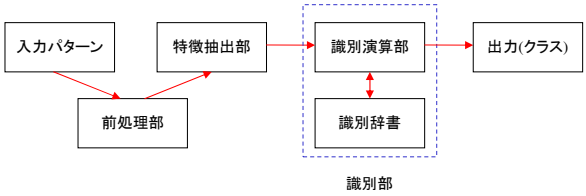

図 1: 認識系の流れ

本研究ではトラヒックデータを用いた感染検知という観点から，感染の有無を正常なトラヒックデータか否かという 2 つのクラスに対応させて考える．前処理部では，対象となる通信から特定のノードとの通信を切り出して特徴量を抽出しやすい形にする．次に，特徴抽出部でパケットサイズやパケット到着間隔といった特徴量を抽出し，あらかじめ学習をして作成した識別辞書との比較を行うことで，入力されたトラヒックデータが正常か異常かを決定する．

識別器の設計を行うにあたって重要である点は，各クラスの分布が分類できるような特徴量を用いることである．また識別アルゴリズムに関しても，特徴量の分布に適したものを利用する必要があるため，適切な識別器の選択，妥当性の評価をしなければならない．

しかしながらマルウェアの感染検知に関する従来研究では上記の評価が必ずしも十分なされていないというのが現状である．そこでパターン認識という観点からの基礎的検討が必要である．

検討するマルウェア感染検知手順の流れを図 2 に示す．

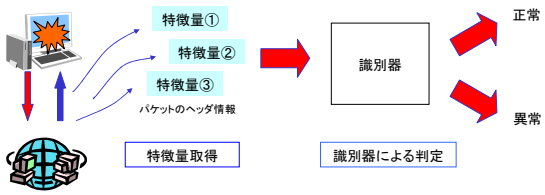

図 2: システムの概要

感染の有無を判別したい PC におけるトラヒッ

クデータを取り出し，前処理を行った後にヘッダ情報から複数の特徴量を取得する．これらの特徴量に関して識別器を用いて対象のトラヒックデータが正常か異常かの判定を行う．

識別器を作成する際には，あらかじめ実際の感染時のデータ，正常時のデータを用いて学習を行う．

3　特徴量の検討

識別器設計という観点から，マルウェアに感染していることを示す特徴量に関して検討を行う．

3.1　感染後のトラヒックデータ切り出し

今回調査の対象のデータベースとして CCC2009 の攻撃通信データを用いる．また正常時のデータとして，イントラネット内を流れるトラヒックデータを Wireshark[9] によってキャプチャしたものを使用する．

マルウェアに感染開始後のトラヒックデータの切り出しとして，まず，CCC2009 の攻撃元データから，マルウェア本体の取得時の時刻を得る．また，攻撃通信データに snort[10] を適用することで，アラート (攻撃の可能性のあるパケット) を得る．これらの 2 つの情報を比較しながら攻撃通信データを見ることで，攻撃の成功したパケットを特定し，マルウェア本体のダウンロード開始時を決定する．CCC2009 におけるハニーポットは周期的にクリーンな状態へリセットされるため，攻撃のパケットから OS がリセットされる直前までのトラヒックデータを感染状態の通信として調査の対象とした．

3.2　調査

マルウェアの感染後の挙動でトラヒックデータに影響を及ぼす可能性のあるものとして，

- リモートから脆弱性に対する攻撃を受ける
- 検体をダウンロードする
- インターネット接続を確認する
- 感染活動が成功したことを通知する
- 感染を拡大する
- C&C サーバに接続して指令を待つ
- 検体をアップデート
- DoS 攻撃をかける
- スパムメールを送信する

などがある．

今回は検体のダウンロード (検体のアップデートも含まれる)，感染の拡大 (ポートスキャン等) に着目し，感染時と正常時の各特徴量に関する時間的な変化を見ることで，特徴となる箇所を洗い出した．

またポートスキャン等に関するパケットが増えることで，パケットサイズごとのパケット数の割合に正常時と異常時の違いがあらわれる可能性がある．

3.3　検討結果

感染時および正常時トラヒックデータの時間的な変化を見て，1 秒間ごとに送受信されたパケットのサイズを合計した結果を図 3〜5 に示す．ここで，正常時のトラヒックデータに関しては，任意に選択した 1 ホストの通信を取り出した．

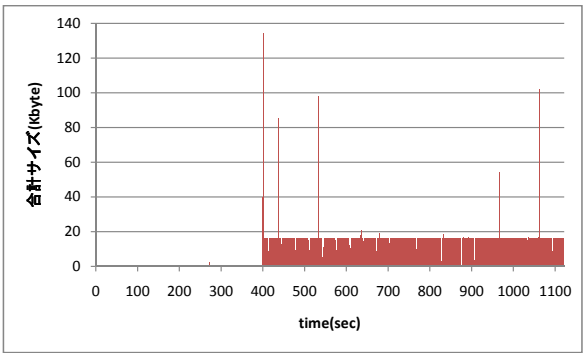

図 3: 感染時におけるポートスキャン実行時のトラヒックデータ時間推移

ポートスキャン実行時は連続して他のノードに対して SYN 要求を行っている．図 3 でもわか

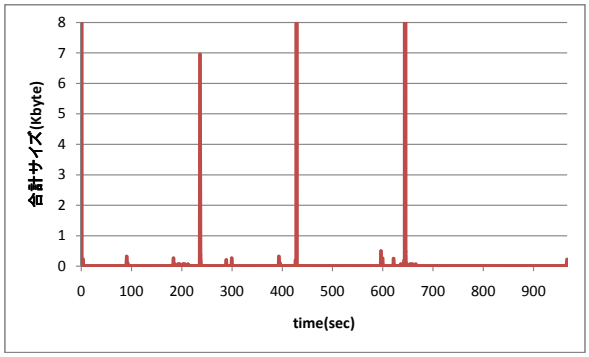

図 4: 感染時におけるポートスキャン非実行時のトラヒックデータ時間推移

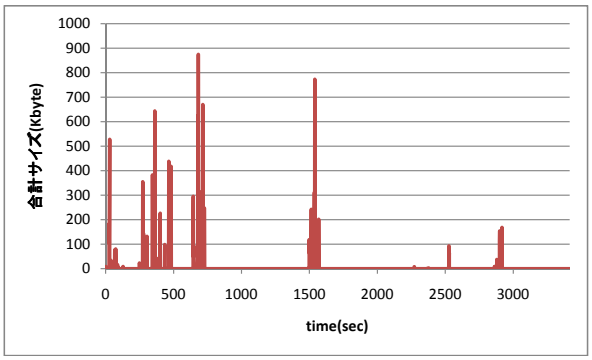

図 5: 正常時のトラヒックデータ時間推移

るように，一定サイズのパケットを送信し続けるため，方形波状でグラフに現れている．部分的に合計サイズの大きくなる箇所があるが，これはマルウェア本体のダウンロードが実行されている箇所である．図 4 ではポートスキャンが行われなかったため，特徴的なトラヒックは現れていない．前述と同様に，パルス状に現れるトラヒックはマルウェア本体のダウンロードとなっている．図 5 は Web 閲覧の様子を表しているが，パケットの送受信はもちろん一定とは言えない．またサイズに関しても他の 2 つと比べて大きいことがわかる．

これらより，ポートスキャンによる一定で継続した通信の存在がマルウェアの特徴として扱える可能性がある．一方でマルウェアのダウンロードについては特徴といえるべきものは確認できず，まだ検討の余地があるといえる．

次に，切り出したデータの総パケット数のうちパケットサイズごとにどれくらいの割合でパケットが存在するかを図 6〜8 に示す．

図 6〜8 は一例であるが，同条件の他のトラヒックデータについても調査したところ，各状態においてパケットの存在する割合が同じ傾向となっていた．図 6 では，ポートスキャンが原因でほぼ 100byte 以下のパケットとなっていることがわかり，図 8 では，1000byte を超えるパケットの割合が図 7 に比べて多くなっていることがわかる，これは Web からの受信時のパケットが多いことが原因と考えられる．今回は送受信の区別をせずにその総量について統計を取ったが，送信時と受信時を分けて見ることでまた新たな特徴が見られる可能性がある．

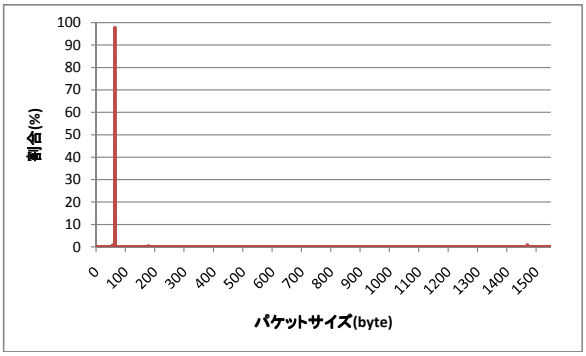

図 6: 感染時におけるポートスキャン実行時のパケットサイズごとの存在率

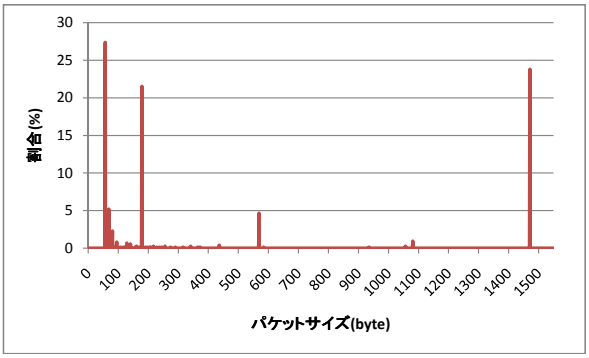

図 7: 感染時におけるポートスキャン非実行時のパケットサイズごとの存在率

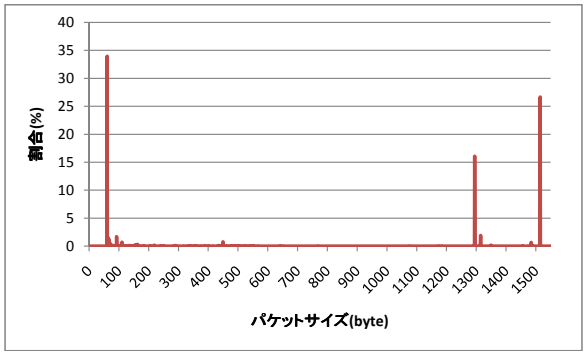

図 8: 正常時のパケットサイズごとの存在率

4 まとめ

本稿ではマルウェアの感染検知にトラヒックデータとパターン認識を用いた手法の必要性について述べた．またパターン認識の概要を述べるとともに，基礎的検討の必要性を示した．感染の有無によるトラヒックデータの特徴を示すことで違いを調査し，結果として感染検知にはポートスキャンの存在が有効であり，一定サイズの連続するパケットの送信が特徴であることを確認できた．

今後は上記の結果をふまえて，ポートスキャンの動作を特徴量としてどのように記述するかを検討するとともに，3.2 章で示したポートスキャン以外のマルウェアの感染後のふるまいに関してもトラヒックデータの調査を行い，検知に有効とされる特徴量を評価していく予定である．また，これらの特徴量の評価後は識別器の構築やそれによる精度評価を考えている．

マルウェア感染後のトラヒックデータの挙動を網羅することで，将来的に新種のマルウェアの検知を行えるような汎用性のある検知手法を検討していく．

参考文献

[1] インターネット脅威マンスリーレポート - 2009 年上半期・6 月度
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/article/20090706033829.html

[2] 藤原将志，寺田真敏，安部哲哉，菊池浩明，”マルウェアの感染方式に基づく分類に関する検討，”情報処理学会 CSEC 研究報告，No.21，p177-182，2008 年 3 月．

[3] 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，”MWS2009，2009 年 10 月．

[4] S.Kondo and N.Sato，”Botnet Traffic Detection Techniques by C&C Session Classification Using SVM，”IWSEC2007，Oct. 2007.

[5] 市野将嗣，坂野鋭，小松尚久，”核非線形相互部分空間法による話者認識，”信学論 (D-Ⅱ)，vol.J88-D-Ⅱ，no.8，pp.1331-1338，2005.

[6] 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，”FIT2007，2007 年 9 月．

[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，”MWS2008，2008 年 10 月．

[8] 石井健太郎，上田修功，前田英作，村瀬洋，“ わかりやすいパターン認識，” 1998.

[9] wireshark.org
http://www.wireshark.org/

[10] snort.org
http://www.snort.org