マルウェア感染検知のためのトラヒックデータにおけるペイロード情報の特徴量評価

大月 優輔† 市野 将嗣† 川元 研治†† 畑田 充弘††† 吉浦 裕†

†電気通信大学大学院情報理工学研究科
182-8585 東京都調布市調布ヶ丘 1-5-1
otsuki@uec.ac.jp, ichono@inf.uec.ac.jp,
yoshiura@hc.uec.ac.jp

††早稲田大学理工学術院基幹理工学研究科
169-8555 東京都新宿区大久保 3-4-1
kawamoto@kom.comm.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16F
m.hatada@ntt.com

あらまし 近年，トラヒックデータを用いたマルウェア感染検知において，複数の特徴量を用い、その組み合わせから正常時通信と感染時通信の識別をしている．しかし，個々の特徴量毎の有効性や，マルウェアの種類毎の有効性について明確に示されていない．そこで本研究では，ペイロードにおける感染検知において，感染時通信として CCCDATAset，D3M2012 を， 正常時通信として 2 種類のイントラネットのトラヒックデータを用い，マルウェアの種類としてワーム，トロイの木馬，ファイル感染型ウイルスを取り上げ，261 種類の特徴量に対して，4 つの量子化レベル数において各々TPR，TNR を求め，個々の有効な特徴量をマルウェアの種類毎に明らかにした．

Evaluating features of payload for malware detection

Yusuke Otsuki† Masatsugu Ichino† Kenji Kawamoto†† Mitsuhiro Hatada††† Hiroshi Yoshiura†

†Graduate School of Informatics and Engineering, The University of Electro-Communications
1-5-1 Chofugaoka, Chofu-si, Tokyo, 182-8585, JAPAN
otsuki@uec.ac.jp, ichono@inf.uec.ac.jp, yoshiura@hc.uec.ac.jp
††Graduate school of Fundamental Science and Engineering, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo, 169-8555, JAPAN
kawamoto@kom.comm.waseda.ac.jp
†††NTT Communications Corporation
Gran Park Tower 16F, 3-4-1 Shibahara, Minato-ku, Tokyo, 108-8118 Japan
m.hatada@ntt.com

Abstract We evaluated features used in related works based on traffic data since effectiveness of using these features in malware detection is not evaluated sufficiently. In the evaluation, CCCDATAset and D3M2012 are used as anomaly traffic data infected with malware, and traffic data captured in some Intranet are used as normal traffic data. We evaluated the features by comparing the distances between normal/anomaly codebooks made by vector quantization and input data. In this paper, we show and discuss the evaluation results of payload features in each type of malware.

1. はじめに

近年，仕事や生活等さまざまな場面でインターネットが必要不可欠な存在となっている．インターネットが普及し，便利さが増す反面，それらを悪用したマルウェアの活動による被害が拡大している．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，感染したPC のデータ破壊や個人情報の流出等，我々の日常生活を脅かす存在となっている．

2011 年前半に新しく出現したマルウェアの数は，120 万件で，2010 年の後半よりも 15.7%分増加している[1]．その上，近年のマルウェアは亜種が数多く存在し，複数のダウンロードサーバに分散して感染する等，複雑化・高度化が進んでいる．そのため，早急に対策を講じる必要がある．

これに対し，シグネチャ型，イベント監視型などの手法を用いてマルウェアの検知，駆除を行うマルウェア対策ソフトがセキュリティベンダによって開発されている[2]．しかしこれらの検知手法は，マルウェア毎に特徴を示すシグネチャを用意しなければならず，短期間で大量に出現する未知のマルウェアの検知に対応できない．そのため，未知のマルウェアに有効な感染検知，つまり感染してしまうことを前提として，感染後に早期に検知できるようにすることが必要とされている．

そこで近年，マルウェア感染検知の中でもトラヒックデータ検知に着目した手法が注目されている．なかでも，ヘッダ情報よりも情報量が多く，感染時通信と正常時通信を区別する情報が多く含まれていると考えられる，ペイロード情報を用いた検知手法が注目されている．

本研究ではまず，ペイロード情報に基づく感染検知を行う既存研究を分析した．その結果，検知手法の検討がメインで，どの特徴量が正常と感染を区別しやすいかという観点からの検討が十分に行われていないことがわかった．特徴量の有効性を明確にした上で複数の特徴量を適切に組み合わせることで，より高性能な識別ができる可能性がある．

そこで本研究では，マルウェア感染後のトラヒックデータを分析して，感染検知に有効な特徴量の有効性を明らかにした. その目的の方法として，感染時通信に，D3M2012，CCCDATAset2009，2010，2011[3] （以下 CCC2009，CCC2010，CCC2011）の攻撃通信データを，正常時通信に，2 カ所のあるイントラネットに流れる通信データを用いた． また，マルウェアは，種類毎で異なった通信（ワーム：インターネット接続確認等）を行うので，マルウェアの種類毎（ワーム，トロイの木馬，ファイル感染型ウイルス）に分類し，各々の特徴量の有効性を明らかにした．

以下，2.で既存研究においてよく用いられている特徴量を整理し，3.で 2.を踏まえた特徴量評価の目的を述べ，4.で実験方法と本稿において評価する特徴量について述べる．5.で特徴量毎に感染時通信と正常時通信の識別のしやすさを評価する実験を行った結果を示し，6.でマルウェアの種類毎で識別率の高い特徴量について考察する. また，時間的変化を用いた識別の有効性について述べる．

2. 特徴量評価

2.1. 既存研究の特徴量

本章では，既存のマルウェア感染検知やネットワーク異常検知に関する研究で用いられているペイロードの特徴量を整理する．

文献[4]，[5]，[6]等では，特徴量として文字列の出現頻度が使われている．桑原ら[6]は，ボットの攻撃通信データのペイロード情報から，マルウェアの挙動とそれに対応した特徴的な文字列（exe，NICK 等）があることを確認し，それらを特徴量として用いている

また，Wei Lu[7] らは，ボットが行う遠隔制御用通信のトラヒックデータに着目する手法を提案し，正常時通信とボットが行っている感染（異常）時通信パケットのペイロード情報に着目しペイロード内の ASCII 文字コードの出現頻度（バイト数）を特徴量としている．

また，山田ら[8]は，侵入検知システムにおける未知攻撃の課題に対する解決策として，決定木を用いたアノマリ検知を示し，HTTP リクエスト長，HTTP リクエストの総サイズを特徴量としている．

上記より，マルウェア検知用の特徴量として ASCII 文字コードの出現頻度，文字列の出現頻度，HTTP リクエスト長がよく用いられていることがわかる．しかし，いずれの研究においても，特徴量の有効性については評価されていない．

2.2. マルウェアの種類毎の特徴量評価

トレンドマイクロ社のセキュリティデータベース[9]等に示されているように，マルウェアの種類毎で特有の挙動がある．例として，ワームはソフトウェアに存在する脆弱性を利用し，ネットワーク上で感染活動を行う．トロイの木馬は特定のサイトにアクセスし，不正なファイルのダウンロードを要求し，感染した PC がさらなる脅威にさらされるなどの挙動がある．同種類のマルウェアの亜種で共通した挙動の傾向があることが確認できている[9]．このため，マルウェアの種類毎に有効な特徴量が異なる可能性がある．

そこで本研究では，マルウェアの種類毎での特徴量評価を行った．種類毎で有効な特徴量を評価し，有効な特徴量を組み合わせることで，効率的かつ早期の検知に繋がると考える．

3. 特徴量評価の目的

既存研究では，トラヒックデータを用いたマルウェア感染検知において，複数の特徴量を用い，その組み合わせから正常時通信と感染時通信の識別をしている．しかし，個々の特徴量の有効性について明らかではなく，マルウェアの種類毎にどのような特徴量が有効であるかも明らかではない．また，有効な特徴量を感染検知に用いない場合，識別率の低下が考えられる．

そこで本研究では，ペイロードを用いたマルウェア感染検知において，個々の特徴量の有効性をマルウェアの種類毎に明らかにする．マルウェアの種類として，ワーム，トロイの木馬，ファイル感染型ウイルスを定め，有効な特徴量をそれぞれ評価した．

4. 特徴量評価実験概要

4.1. タイムスロット

本研究では，トラヒックデータからの特徴抽出にタイムスロットを用いた．タイムスロットとは，トラヒックデータを特定の秒数で区切った範囲のことを示す．

時間的変化を伴う通信をタイムスロットで分割し，タイムスロットの時間的変化を追うことで，通信全体の時間的変化に着目した識別を行うことができる．また，トラヒックデータの特徴抽出の取得単位としてフローを用いる方法がある．しかしこの手法は，通信が終了するまで特徴量が取得できないため，早期検知に不適切である．一方タイムスロットを用いる方法は，タイムスロット幅を調整することで，早期に検知できる可能性がある．本実験では，タイムスロット幅は 1 秒とし，タイムスロット毎に特徴量を求めた．

4.2. ペイロードの特徴量

本研究では既存研究で多く用いられていた次に示す 261 種類の特徴量を評価対象とする．

- ASCII 文字コードの出現頻度 255 種類
- 特徴的な文字列の出現頻度：5 種類
  (GET，POST ，exe，whatismyip，checkip)
- HTTP リクエスト長

4.3. 評価方法

本研究での感染時通信と正常時通信の識別方法について説明する．

4.3.1. ベクトル量子化によるコードブック作成

ベクトル量子化を用いて，感染時通信のみを用いて学習を行った感染コードブックと，正常時通信のみを用いて学習を行った正常コードブックを予め作成する．今回は，各特徴量を個別に評価することが目的であるため，特徴量毎に 1 次元コードブックを作成した．ベクトル量子化のアルゴリズムには，LBG+Splitting アルゴリズム[10]を用い，レベル数は 2，4，8，16 の 4 種類とした．そして，予め感染時通信か正常時通信かのラベル付けされた各特徴量の 1 次元テストデータ（1 タイムスロット毎から抽出される特徴量）を与え，テストデータと感染，正常コードブックとの距離を計算し，感染(正常)コードブックとの距離の方が小さければ感染（正常）と識別している．

4.3.2. 実験データ

本研究では, 取得環境の違いを評価するために, 正常時通信として，異なる 2 カ所のイントラネットに流れる通信を用いた．これにより，取得環境の違いによる影響を受けにくい特徴量を評価できる．それぞれのデータを，正常コードブック作成のための学習データとテストデータ用に分割して

いる．

また，感染時通信に D3M2012，CCC2009, CCC2010, CCC2011 を用い，感染コードブック作成用の学習データとテストデータ用に分割した．さらにこれらのデータをマルウェアの種類毎でマルウェアの検体数が均等になるように分割した．CCC2009，CCC2010, CCC2011 の攻撃通信データにはマルウェアに感染するまでの通信が含まれている．そこで本研究では，文献[11]と同じ方法を用いて，攻撃通信からマルウェアに感染した後の通信のみを切り出し評価した．

本研究ではマルウェアの種類をワーム，トロイの木馬，ファイル感染型ウイルスとした．ファイル感染型ウイルスとは，拡張子 exe 等の実行型ファイルに感染するウイルスである．また，マルウェア検体名は CCCDATAset において，攻撃元通信データのログファイルに記載されている名称を用いた．D3M2012 においては，マルウェア検体のハッシュ値を用い，G-data 社，トレンドマイクロ社，Kaspersky 社のそれぞれが命名しているマルウェア検体の名称を用いた．表 1 に今回実験で使用した各データセットのマルウェアをまとめた．

表 1:各データセットのマルウェア

種類	CCCDATAset2011	CCCDATAset2010	CCCDATAset2009	D3M2012
ワーム	WORM_DOWNAD.AD	WORM_DOWNAD.AD WORM_MAINBOT.AH WORM_MAINBOT.FY WORM_PALEVO.SMD WORM_PALEVO.BL	WORM_SWTYMLAI.CD	
トロイの木馬			TROJ_BUZUS.AGB	TROJ_GEN.R47C7C2 Trojan.Generic.KD.578000 Trojan.Generic.KD.410743 Trojan-Dropper.Win32.Dapato.aoxn
ファイル感染型		PE_VIRUT.AV PE_VIRUT.XV	PE_BOBAX.AK	

5. 実験結果

マルウェア感染検知の要件は，感染と正常を正しく識別できる特徴量を用いることである．このため，感染・正常のみを正しく識別できる特徴量を併用することも有効である．感染検知に有効な特徴量について検討するため，TPR（感染データを感染と正しく分類した割合），TNR（正常データを正常と正しく分類した割合）が共に高い特徴量，TPR のみが高い特徴量，TNR のみが高い特徴量の観点から検討した．以下に評価実験の結果を示す．

5.1. TPR, TNR 共に高い特徴量

取得環境の影響を受けにくい特徴量を評価する観点から，2 種類の正常時通信を用い，安定的に検知するという観点から，4 つの量子化レベル数の TPR，TNR の平均値を特徴量 261 個に対してそれぞれ求めた．その結果の中から，イントラネット A における平均 TPR・TNR の値が高い上位 15 個と，それに対応するイントラネット B の TPR・TNR を表 2 に示す．表 2（赤字）より，ワームの ASCII 文字コード「i」とファイル感染型ウイルスの「HTTP リクエスト長」の TPR・TNR の値が，2 種類の正常時通信を用いた時の差異が少なく，安定して高い値を示すことがわかった．これらの特徴量を用いたときの詳細を表 3，表 4 に示す．これらの特徴量は，2 種類の正常時通信を用い，量子化レベル数と変化させても，TPR が 95%以上かつ TNR が 80%以上で安定的に検知できることがわかった．

表 2:イントラネット毎の平均 TPR・TNR

マルウェアの種類	特徴量	イントラネットAの平均TPR	イントラネットBの平均TPR	特徴量	イントラネットAの平均TNR	イントラネットBの平均TNR
ワーム	HTTPリクエスト長	100%	99%	ASCII文字コード「>」	89%	79%
	ASCII文字コード「i」	98%	98%	ASCII文字コード「I」	88%	78%
	ASCII文字コード「f」	98%	97%	ASCII文字コード「ETB」	88%	70%
	ASCII文字コード「C」	98%	92%	ASCII文字コード「J」	85%	83%
	ASCII文字コード「E」	97%	94%	ASCII文字コード「H」	84%	74%
	ASCII文字コード「e」	97%	91%	ASCII文字コード「#」	84%	78%
	ASCII文字コード「a」	96%	91%	ASCII文字コード「.」	84%	76%
	ASCII文字コード「0」	95%	97%	ASCII文字コード「B」	84%	74%
	ASCII文字コード「r」	95%	91%	ASCII文字コード「E」	84%	75%
	ASCII文字コード「OR」	95%	91%	ASCII文字コード「P」	84%	75%
	ASCII文字コード「/」	95%	92%	ASCII文字コード「R」	84%	74%
	ASCII文字コード「:」	95%	94%	ASCII文字コード「S」	84%	73%
	ASCII文字コード「c」	95%	93%	ASCII文字コード「i」	83%	83%
	ASCII文字コード「s」	95%	94%	ASCII文字コード「M」	83%	75%
	ASCII文字コード「m」	95%	91%	ASCII文字コード「N」	83%	77%
トロイの木馬	HTTPリクエスト長	100%	100%	ASCII文字コード「<」	85%	72%
	ASCII文字コード「NL*」	100%	100%	ASCII文字コード「US」	85%	76%
	ASCII文字コード「OR」	100%	100%	ASCII文字コード「>」	85%	41%
	ASCII文字コード「0」	100%	100%	ASCII文字コード「¥」	83%	73%
	ASCII文字コード「5」	100%	100%	ASCII文字コード「VT」	82%	56%
	ASCII文字コード「C」	100%	100%	ASCII文字コード「]」	82%	68%
	ASCII文字コード「d」	100%	100%	ASCII文字コード「HT」	81%	65%
	ASCII文字コード「e」	100%	100%	ASCII文字コード「SOH」	80%	56%
	ASCII文字コード「t」	100%	100%	ASCII文字コード「^」	80%	69%
	ASCII文字コード「x」	100%	100%	ASCII文字コード「'」	80%	67%
	ASCII文字コード「A」	100%	100%	ASCII文字コード「FS」	80%	63%
	ASCII文字コード「o」	100%	100%	ASCII文字コード「ESC」	79%	62%
	ASCII文字コード「r」	100%	100%	ASCII文字コード「ACK」	79%	63%
	ASCII文字コード「1」	100%	100%	ASCII文字コード「$」	79%	65%
	ASCII文字コード「2」	100%	100%	ASCII文字コード「EOT」	79%	60%
ファイル感染型ウイルス	HTTPリクエスト長	100%	100%	ASCII文字コード「DC2」	92%	68%
	ASCII文字コード「p」	99%	99%	ASCII文字コード「DC3」	90%	68%
	ASCII文字コード「B」	99%	75%	ASCII文字コード「ETB」	89%	62%
	ASCII文字コード「S」	98%	98%	ASCII文字コード「#」	89%	67%
	ASCII文字コード「e」	98%	98%	ASCII文字コード「S」	89%	69%
	ASCII文字コード「T」	98%	94%	ASCII文字コード「Y」	88%	76%
	ASCII文字コード「i」	98%	98%	ASCII文字コード「'」	87%	79%
	ASCII文字コード「o」	97%	98%	ASCII文字コード「M」	87%	79%
	ASCII文字コード「H」	96%	94%	ASCII文字コード「R」	86%	79%
	ASCII文字コード「X」	95%	74%	ASCII文字コード「US」	86%	69%
	ASCII文字コード「W」	95%	93%	ASCII文字コード「)」	85%	75%
	ASCII文字コード「r」	95%	94%	HTTPリクエスト長	82%	84%
	ASCII文字コード「G」	95%	78%	ASCII文字コード「(」	82%	78%
	ASCII文字コード「N」	95%	80%	ASCII文字コード「f」	82%	73%
	ASCII文字コード「q」	95%	94%	ASCII文字コード「j」	82%	75%

表 3:ワームの ASCII 文字コード「i」の TPR・TNR

	TPR				TNR			
量子化レベル数	2	4	8	16	2	4	8	16
イントラネットA	98%	99%	98%	98%	83%	80%	86%	83%
イントラネットB	97%	98%	98%	97%	83%	80%	80%	82%

表 4:ファイル感染型ウイルスの「HTTP リクエスト長」の TPR・TNR

	TPR				TNR			
量子化レベル数	2	4	8	16	2	4	8	16
イントラネットA	100%	100%	100%	100%	82%	80%	81%	81%
イントラネットB	100%	100%	100%	94%	88%	86%	88%	86%

5.2. TPR のみ高い特徴量

表 2（青字）から TPR のみ高い特徴量として，ワームでは HTTP リクエスト長, ASCII 文字コード「0」，「f」，トロイの木馬では，HTTP リクエスト長, ASCII 文字コード「NL*」，「CR」，「0」，「5」，「A」，「C」，「M」，「d」，「e」，「r」，「t」，「x」，ファイル感染型ウイルスでは ASCII 文字コード「S」，「e」，「i」，「o」，「p」が確認できた．これらは 2 種類の正常時通信を用いても，TPR が 95%以上で安定的に検知できることがわかった．

5.3. TNR のみ高い特徴量

表 2（緑字）から TNR のみ高い特徴量として，ワームでは ASCII 文字コード「J」が確認できた．これらは 2 種類の正常時通信を用いても, TNR が 80%以上で安定的に検知できることがわかった．

6. 考察

5 章で有効だと判断した特徴量について，正常時通信と感染時通信の重なり具合を視覚的に確認するため，出現頻度に着目して考察した．また，マルウェア種類毎の共通した挙動を挙げ，それらの挙動について説明し，マルウェアの種類毎に有効な特徴量の考察した．

6.1. TPR・TNR が共に高い特徴量について

5 章で求められた特徴量に対してヒストグラムを作成した．これらは縦軸を感染時通信（正常時通信）全体のスロット数の割合[%]，横軸を出現頻度としている．5 章で有効だと判断した特徴量の中から例として，ファイル感染型ウイルスの感染時通信とイントラネット A の正常時通信を用いた HTTP リクエスト長のヒストグラムを図 1，図 2 に示す．これらは量子化レベル数を 2 としたときの結果であり，図 1 は HTTP リクエスト長が 200 まで，図 2 は HTTP リクエスト長が 10,000 までを示している．また，図 1 から感染時データの出現頻度が 100 以下であることが確認できる．それに対し，正常時データの多くが 100 以上であることが確認できる．

正常時通信（ユーザの通信）は様々であり，HTTP リクエスト長にばらつきが存在する．感染時データは，HTTP リクエスト長が短いものが多く，感染時コードブックに分類される．これにより，TPR の値が高くなったが，正常時通信の中にも HTTP リクエスト長が短くなるものもあるため，TNR の値は低くなったと考えられる．

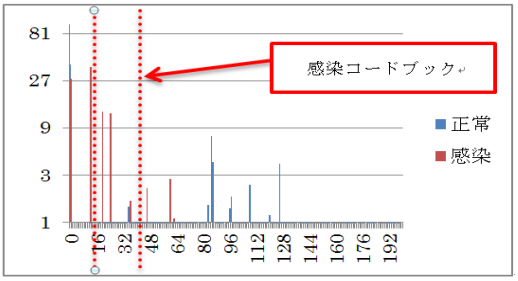

図 1：HTTP リクエスト長のスロット数の割合が 1%以上のヒストグラム
（縦軸：スロット数の割合[%]，横軸：リクエスト長）

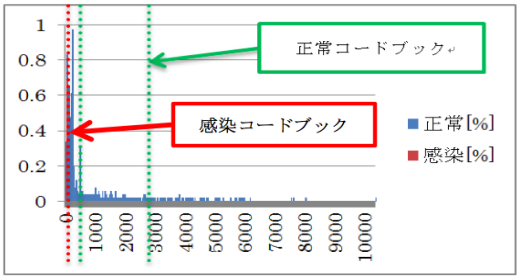

図 2：HTTP リクエスト長のスロット数の割合が 1%以下のヒストグラム
（縦軸：スロット数の割合[%]，横軸：リクエスト長）

ワームの ASCII 文字コード「i」のヒストグラムは図 3，図 4 のようになった．これらの図は縦軸を感染時通信（正常時通信）全体のスロットの割合[%]，横軸を出現頻度[回]としている．また，正常時通信は，上記と同様にイントラネット A の正常時通信を用いている．

ASCII 文字コード「i」の場合も，正常時通信に比べて感染時通信の出現頻度が少ない割合であることが確認でき, 感染コードブックが小さい値で，正常コードブックは比較的大きい値で作成された．これは正常時通信の場合，感染時通信のペイロードの情報よりも多くの情報量が含まれているため，ASCII 文字の出現頻度が多くなるためだと考えられる．また，ASCII 文字コード「i」が有効だと判断された理由として, User-Agent に含まれる情報（Mozilla，Windows 等）や HTTP GET に含まれる情報（image，login 等）が感染時通信に比べて正常時通信で多く出現しているためである．

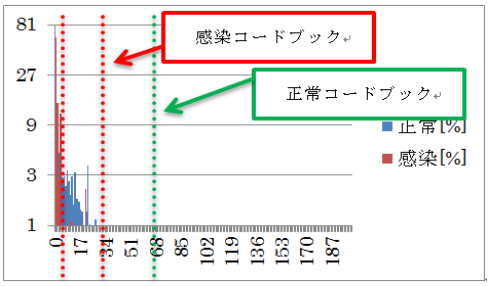

図 3：ASCII 文字コード「i」のスロット数の割合が 1%以上のヒストグラム

（縦軸：スロット数の割合[%]，横軸：出現頻度[回]）

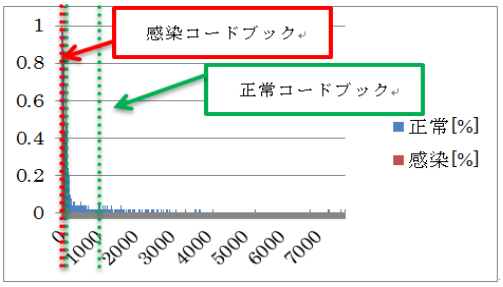

図 4：ASCII 文字コード「i」のスロット数の割合が 1%以下のヒストグラム

（縦軸：スロット数の割合[%]，横軸：出現頻度[回]）

正常の分布と感染の分布の重なり具合に着目すると，主に出現頻度が低いところで正常の分布と感染の分布に重なりがあることが確認できる．

しかし，重なっている部分は正常時通信のごく一部であり（正常時通信全体の 5%未満），正常時通信と感染時通信を分離できるため，5.1 節，5.2 節で評価した特徴量が有効であることが考えられる．また，TNR に関しても，ユーザの通信内容によって出現頻度が異なるが，正常時通信で出現頻度が高いところで分布し，感染時通信の重なっている部分が比較的少ない（正常時通信全体の 20%未満）く，正常時通信と感染時通信を分離できるため，5.1 節，5.3 節で評価した特徴量が有効であることが考えられる．また，イントラネット B の正常時通信を用いた場合でも，同様の結果が得られたことを確認できた．

上記の結果から，正常時通信と感染時通信に違いが見られることが確認でき， HTTP リクエスト長，ASCII 文字コード「i」を用いることで，感染と正常を区別できたと考えられる．

6.2. マルウェア種類毎に有効な特徴量

マルウェア種類毎に有効な特徴量について，ワーム，トロイの木馬，ファイル感染型ウイルスに分類されるマルウェアそれぞれにおいて共通した挙動（ペイロード情報）を挙げ，それらの挙動を説明し，有効な特徴量について考察した．

- **ワーム**

インターネット接続確認

ワームが感染活動を行い，PC を感染させた後に，その PC がインターネットに接続されているかを確認する．その際ワームは、特定のドメインにインターネット接続確認を行う．特定のドメインとは，「www.whatismyipaddress.com」や「checkip.dyndns.org」のような IP アドレスを表示するサイトである．

攻撃通信を行うためのマルウェアのダウンロード

起点となるワームに感染後，各サーバーから他のマルウェアを HTTP GET によりダウンロードする．このコマンドは，「GET /vss.exe HTTP/1.0」や「GET /fdc1.data HTTP/1.0」のようなものである．感染後に行う通信は，HTTP リクエスト長が概ね 100 以下と短くなる．それに対して，正常時通信は概ね 100 以上の通信を行っているものがほとんど（スロット数の割合が 95%以上）である．

よって，ドメイン等に含まれる ASCII 文字コードが正常時通信と比べて出現頻度が低いことや，HTTP リクエスト長が感染時通信で短くなることから，表 2 で示した特徴量はマルウェア感染検知に有効であると判断できる．

- **トロイの木馬**

攻撃通信を行うためのマルウェアのダウンロード

起点となるマルウェアをダウンロード後，各サーバーから他のマルウェアを HTTP GET によりダウンロードする．例としては，「GET /vot.exe HTTP/1.0」や「GET /15Psv3zJ/4ah6NuS.exe HTTP/1.0」のような HTTP GET によるダウンロードを行う．HTTP GET による通信だけを行っているものが多く，ペイロードの情報量が少ない．そのため，正常時通信と比較すると、改行（¥r¥n）の数が少ない傾向がある．また感染後に行う通信は，HTTP リクエスト長が概ね 30 以下と短くなる．それに対し，正常時通信は概ね 100 以上であるものが大半（スロット数の割合が 95%以上）である．

よって HTTP GET 等に含まれる ASCII 文字コードが正常時通信と比べて出現頻度が低いことや，

HTTP リクエスト長が感染時通信で短くなることから，表 2 に示した特徴量はマルウェア感染検知に有効であると判断できる．

- **ファイル感染型ウイルス**

IRC 通信による C&C サーバーに接続（IRC 接続）

ファイル感染型ウイルスは感染活動を行うための準備として，IRC 通信を行い C&C サーバーに接続する．IRC 接続を行った後，攻撃通信を行うためのマルウェアのダウンロードや標的に対して妨害攻撃を行う等の活動が行われる．今回用いた検体では，攻撃通信を行うためのマルウェアのダウンロードを行っていた．IRC 通信を行う際の通信内容は特定の文字列（IRC ドメイン:*norks.org* 001 *tjrrxaek*:等）が同程度の数が繰り返し多く出現する．それらの文字列に含まれる文字は，感染時通信において同程度の数が繰り返し多く出現する．

攻撃通信を行うためのマルウェアのダウンロード

起点となるマルウェアをダウンロード後，マルウェアは各サーバーから他のマルウェアを HTTP GET によりダウンロードする．例としては，「GET /jiri.data HTTP/1.0」や「GET 44.data HTTP/1.0」などのような HTTP GET によるダウンロードを行う．ファイル感染型ウイルスが感染後に行う通信は，HTTP リクエスト長が 10～80 であるのに対し，正常時通信は概ね 100 以上であるものが大半（スロット数の割合が 95%以上）である．

よって，IRC 通信に含まれる ASCII 文字コードが正常時通信と比べて出現頻度が**同程度の数で繰り返し多い**ことや，HTTP リクエスト長が感染時通信で短くなることから，表 2 で示した特徴量はマルウェア感染検知に有効であると判断できる．

以上マルウェア 3 種の考察から，今回用いたデータセットの場合，HTTP 通信を用いたマルウェアの感染活動は，インターネットの接続確認や攻撃通信を行うためのマルウェアのダウンロードを行っている．また，攻撃通信を行うためのマルウェアのダウンロードを行う際に，IRC 通信を行うものや外部サーバーから直接ダウンロードを行うもの等，マルウェアの種類毎で異なる挙動が確認できた．さらに，感染活動を行うときのマルウェアの種類毎でマルウェアのダウンロードを行う時等のペイロード情報の文字列が異なるため，マルウェアの種類毎で有効だと判断された特徴量が異なったと考えられる．

6.3. 時間的変化を用いた識別の有効性

トラヒックデータは時間的な変化を伴うため，時間的変化を考慮した識別の有効性を考察する．

例として，ファイル感染型ウイルスの ASCII 文字コード「o」と正常時通信の比較を図 5，図 6 に示す．これらの図では，縦軸を出現頻度，横軸をスロットとした．出現頻度は 1 スロット毎の 1 パケットの出現頻度である．

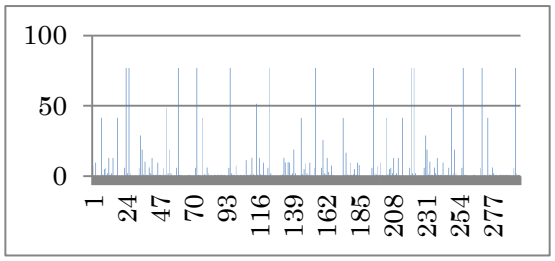

図 5：ファイル感染型ウイルスの ASCII 文字コード「o」の出現頻度の時間的変化
（縦軸：出現頻度[回]，横軸：スロット番号）

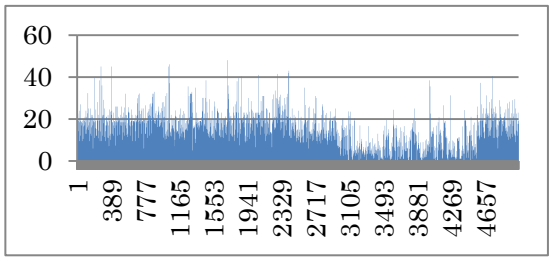

図 6：正常時通信の ASCII 文字コード「o」の出現頻度の時間的変化
（縦軸：出現頻度[回]，横軸：スロット番号）

ファイル感染型ウイルスの出現頻度（図 5）の時間的変化は，正常時通信（図 6）に比べて大きい．また，ファイル感染型ウイルスの出現頻度が高くなっているスロットは，ファイル感染型ウイルスが IRC 通信を行っており，そのペイロード情報に特定の文字列（IRC ドメイン:*norks.org* 001 *tjrrxaek*:など）が連続的に多く出現し，その文字列に含まれる ASCII 文字コードが多く出現するためである．この特徴は，本実験では，ワームやトロイの木馬に出現せず，ファイル感染型ウイルス特有の特徴であった．

時間的な変化を考慮した識別を行うに当たり，今回の実験より以下のような特徴を考慮することが有効であると考える．

i. ワーム
・ 出現頻度の増減を確認する
→増減が小さい場合，感染している可能性有
ii. トロイの木馬
・ 出現頻度が周期的に一定値を示しているかを確認する
→一定の場合，感染している可能性有
・ 出現頻度の増減を確認する
→増減幅が小さい場合，感染している可能性有
iii. ファイル感染型ウイルス
・ 出現頻度の増減を確認する
→増減が大きく，増加したときの出現頻度が一定の場合，感染している可能性有

7. まとめ

本稿では，D3M2012，CCC2009，2010，2011と2種類の正常時通信を用い，マルウェアの種類毎（ワーム，トロイの木馬，ファイル感染型ウイルス）における，感染検知の識別に有効な特徴量を評価した．その結果，マルウェアの種類毎で，特定のASCII文字コードとHTTPリクエスト長が，2つの正常時通信を用い，量子化レベル数を変化させても，TPR・TNRが高く，安定的に検知できることがわかった．具体的には，TPRのみが高い特徴量としてワームで3種類，トロイの木馬で15種類，ファイル感染型ウイルスで5種類を示し，TNRが高い特徴量としてワームで1種類を示した．その中でも，TPR・TNRが共に高い特徴量として，ワームではASCII文字コード「i」とファイル感染型ウイルスではHTTPリクエスト長が特に安定的に検知できることがわかった．

また，ワームでは「インターネット接続確認等」，トロイの木馬では「攻撃通信を行うためのマルウェアのダウンロード等」，ファイル感染型ウイルスでは「IRC接続等」の感染活動行うことが確認でき，挙動と有効な特徴量の間の関連性を明らかにした．さらに，時間的変化においても，正常時通信とマルウェアの種類毎の感染時通信を比較したとき，マルウェアの種類毎の感染時通信で，正常時通信の特徴には表れない時間的な特徴が表れた．

よって，これらの種類毎に有効な特徴量として使用できる可能性があるものとして示した特徴量を適切に組み合わせることで，マルウェア感染検知の検知率の向上につながることが考えられる．

今後は，今回評価できなかった特徴量に対して，マルウェア感染検知に有効であるかを調査し，特徴量を組み合わせたマルウェア感染検知について検討していく．さらに，今回の実験で定義したマルウェアの種類は，ベンダーが定義した種類名を使用したが，マルウェアの挙動（インターネット接続確認やIRC接続等）をクラスタリングし，クラスタごとに有効な特徴量の評価も検討していく．

参考文献

[1] Gdataマルウェアレポート 2011年上半期 http://www.gdata.co.jp/files/GdDataH1MalRep.pdf

[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] MWS2012 実行委員会，研究用データセット MWS 2012 Datasetsについて，http://www.iwsec.org/mws/2012/about.html#datasets

[4] 与那原亨　大谷尚通　馬場達也　稲田勉，“トラフィック解析によるスパイウェア検知の一考察，”電子情報通信学会技術研究報告，Vol.2005, No.70, 2005-CSEC-30, pp.23-29

[5] Marius Kloft et.al，“Automatic feature selection for anomaly detection，” Conference on Computer and Communications Security 2008

[6] 桑原和也，菊池浩明，寺田真敏，藤原将志，“パケットキャプチャから感染種類を判定する発見的手法について，”マルウェア対策研究人材育成ワークショップ2009(MWS2009)，2009年

[7] Wei Lu et.al.，“Automatic Discovery of Botnet Communities on Large-Scale Communication Networks,” the 4th International Symposium on Information, Computer, and Communications Security, 2009

[8] 山田明，三宅優，田中俊昭，竹森敬祐，“学習データを自動生成する未知攻撃検知システム，”情報処理学会論文誌，Vol.46，No.8，pp.1947-1958，2005

[9] トレンドマイクロ　セキュリティデータベース，http://jp.trendmicro.com/jp/home/index.html

[10] Linde Y, Buzo A. and Gray R，“An Algorithm for Vector Quantization，” IEEE Trans，Commun，Vol.28 No,1 pp84-95,1980

[11] 川元研治，市田達也，市野将嗣，畑田充弘，小松尚久，“マルウェア感染検知のための経年変化を考慮した特徴量評価に関する一考察，”マルウェア対策研究人材育成ワークショップ2011(MWS2011)，2011年