Vol.2018-IOT-40 No.33
2018/3/6

パケットのヘッダ情報に基づく不審な通信挙動の検知

鍛治 一祐[1,a)]　青木 茂樹[1,b)]　宮本 貴朗[1]

概要：近年，サイバー攻撃が著しく増加している．企業や団体ではサイバー攻撃による組織内ネットワークへのマルウェアの侵入を防ぐ対策として，侵入検知システムやファイアウォールを設置している．しかし，最近特に観測される標的型攻撃は，組織内のネットワークに侵入するために，入念な調査を行い侵入可能な方法を探しだし，通常の通信に紛れて侵入する．そのため，マルウェアの侵入を防ぐための対策だけでは十分ではない．そこで，マルウェア感染後の活動を検知する対策の重要性が高まっている．本研究では，パケットのヘッダ情報に基づいて，ホストの通常の通信を学習し，学習した通信とマルウェアが行う通信との差異に注目することで，不審な通信を検知する手法を提案する．MWS データセットを対象に実験を実施し，提案手法の有効性を確認した．

キーワード：標的型攻撃，多層防御，MWS データセット

Behavior-Based Malware Detection Using Packet Header

Kazumasa Kaji[1,a)]　Shigeki Aoki[1,b)]　Takao Miyamoto[1]

Abstract: In recent years, cyber-attacks are increasing. Organizations succeeded in preventing cyber-attacks by taking security measures such as firewalls and intrusion detection systems. However, recently, targeted attacks are increasing among cyber-attacks. The attacks investigate Intranet of the organization. Since the attacks are mixed with ordinary traffic, it is difficult to prevent with conventional security measures. In this paper, we focus on difference in traffic before and after a certain PC is attacked. After an attacker intrudes, malware connections are added to normal connections. Therefore, we detect suspicious traffic behavior. In order to verify the effectiveness of the proposed method, we performed an experiment using normal traffic data and BOS Dataset 2015 in MWS Dataset 2017. As results of experiments, we were able to detect targeted attacks.

Keywords: Targeted Attack, Multi-protection, MWS Dataset

1. はじめに

近年，多種多様なサイバー攻撃が存在しており，年々，攻撃手法が巧妙化している．従来のサイバー攻撃は，不特定多数のホストの中から，サイバー攻撃に対する対策が不十分なホストを自動的に探索して攻撃を行っていた．そのため，組織や団体はファイアウォールや侵入検知システムを設置し，ホストではウィルス対策ソフトを稼働させることで，組織内ネットワークやホストへの侵入を試みる通信やネットワーク内の不審な通信を検出してきた．しかし，近年観測されている標的型攻撃は，従来のサイバー攻撃とは異なり，これまでの対策では攻撃を防ぐことが難しいと言われている．

標的型攻撃は，情報の搾取を目的に組織内のネットワークに侵入する攻撃である．従来のサイバー攻撃とは違い，攻撃目標を選定するまでに入念な調査活動を行い計画を立案する．調査活動において，攻撃目標とする組織が行うセキュリティ対策，またその脆弱性を調査して，攻撃を実行する．

ウィルス対策ソフトや侵入検知システムはパターンマッ

[1] 大阪府立大学大学院人間社会システム科学研究科
Graduate School of Humanities and Sustainable System Sciences, Osaka Prifecture University
[a)] swa01078@edu.osakafu-u.ac.jp
[b)] aoki@kis.osakafu-u.ac.jp

チングによりサイバー攻撃の侵入を防いでいる．そのため，すでにパターンファイルに記録された特徴をもつ攻撃に対しては高い確率で検出することができるが，新たな攻撃に対してはパターンファイルにその特徴が記録されていないため検出することができない．標的型攻撃を目論む攻撃者は，組織が設置しているウィルス対策ソフトや侵入検知システムを調査し，パターンファイルにない攻撃方法を計画する．そのため，パターンマッチング手法では標的型攻撃を防ぐことは難しい．

現在では，監視対象の異なるセキュリティ対策を何重にも組み合わせることで，侵入や情報漏洩の可能性を下げる多層防御技術が重要になってきている [1]．多層防御技術は，侵入対策，拡大対策，漏洩対策の 3 段階に分けて考えられることが多い．侵入対策では，ファイアーウォールや侵入検知システムを用いて，ネットワークの外部と内部の境界を監視して不正なアクセスを遮断している．拡大対策では，振る舞い検知型のソフトウェアにより，ネットワーク内における不審な通信を監視している．また，各ホストにおけるパスワードの強化やパッチの監視なども拡大対策に含まれる．漏洩対策では，ファイアーウォールや侵入検知システムによる監視に加えて，アクセスログや送信ログの取得・監視などを行うことによって，機密情報が外部に送信されることを防ぐ役割を担っている．

本研究では，拡大対策・漏洩対策としての運用を想定する，組織内のホストにおいて不審な通信を検知する手法を提案する．本稿では，2 節で関連研究について述べ，3 節で提案手法について説明する．4 節で実験と考察について述べ，5 節でまとめる．

2. 関連研究

文献 [2] では標的型攻撃の攻撃段階について述べられている．標的型攻撃には 7 つの攻撃段階が存在する．攻撃段階の概要を表 1 に示す．(1) 計画立案では，得られる情報や情報窃取できる可能性などを考慮して攻撃目標の選定を行う．(2) 攻撃準備では，攻撃目標の組織におけるネットワーク環境の脆弱性を見つけ出し，組織の対策環境に合わせた攻撃方法の準備を行う．また，C&C(Command and Control) サーバと呼ばれるサーバを用意する．C&C サーバとは，攻撃者がマルウェア感染ホストへ指示を行うためのサーバである．(3) 初期潜入で準備した攻撃を仕掛け，組織内のホストをマルウェアに感染させる．(4) 基盤構築では，マルウェア感染ホストを利用し，ネットワーク内の環境を調査する．ポートスキャンやホストスキャンを実行してサービスポートや IP の探索を行う．探索行為では，特定のポートに絞ったり，スキャンの実行時間間隔を開けるなど，不正操作と気づかれないような工夫がなされている．(5) 内部侵入・調査では，ネットワーク内のホストを次々と乗っ取り，サーバへのアクセス権限を持つホストを探し出す．(6) 目的遂行では，機密情報を外部に送信する．また，重要なシステムを破壊することで，業務を妨害する．(7) 再侵入では，バックドアから再び侵入を図る．この 7 つの手順に基づいて標的型攻撃が行われる．

表 1 標的型攻撃の攻撃段階

1	計画立案	攻撃目標選定 関連調査	組織外ネットワーク
2	攻撃準備	標的型メール ウェブサイト改ざん C&C サーバの準備	
3	初期潜入	標的型メールの送付	組織内ネットワーク
4	基盤構築	バックドア開設 ホスト情報入手 ホスト情報入手	
5	内部侵入・調査	他のホスト情報入手 サーバ侵入 管理者情報窃取	
6	目的遂行	情報窃取 システム破壊	
7	再侵入	バックドアを通じ再侵入	

文献 [3] では，標的型攻撃による遠隔操作の特徴について述べられている．これまでは，「攻撃側発呼型」の遠隔操作ツールが観測されていたが，組織が実施するセキュリティ対策に合わせて「攻撃側着呼型」の遠隔操作ツールへと変化している．2000 年前後に観測された「攻撃側発呼型」は，C&C サーバから組織内のホストに通信確立した後，C&C サーバから遠隔操作を指示する．それに対し 2010 年以降に観測される「攻撃側着呼型」は，組織内のホストから C&C サーバにコネクション確立した後，C&C サーバから遠隔操作を指示する．通信確立の方向が反転した要因の一つに，組織内ネットワークとイントラネットとの境界にファイアウォールが設置されたり，PC にパーソナルファイアウォールが導入されたことなどが挙げられる．この「攻撃側着呼型」は，C&C サーバとの通信を図る際，一般的に使用される頻度の高い 53/tcp，80/tcp，443/tcp のポート，プロトコルには HTTP や HTTPS を用いて通信することが多い．これは，通常の通信に紛れて不正操作による通信と検知されるのを免れるためだと考えられる．また，暗号化した通信によって情報の送受信を行うため，ペイロードの中の情報から判断するような異常検知手法では検知が難しい．

次に，拡大対策・漏洩対策に関する研究について述べる．文献 [4] では，ネットワークログの解析によって，マルウェア感染ホストを検知する手法を提案している．HTTP Proxy サーバのログを用いた既存手法に Firewall ログを加えることで，HTTP 以外の通信でもマルウェアの挙動を追跡することに成功している．しかし，ネットワークログを

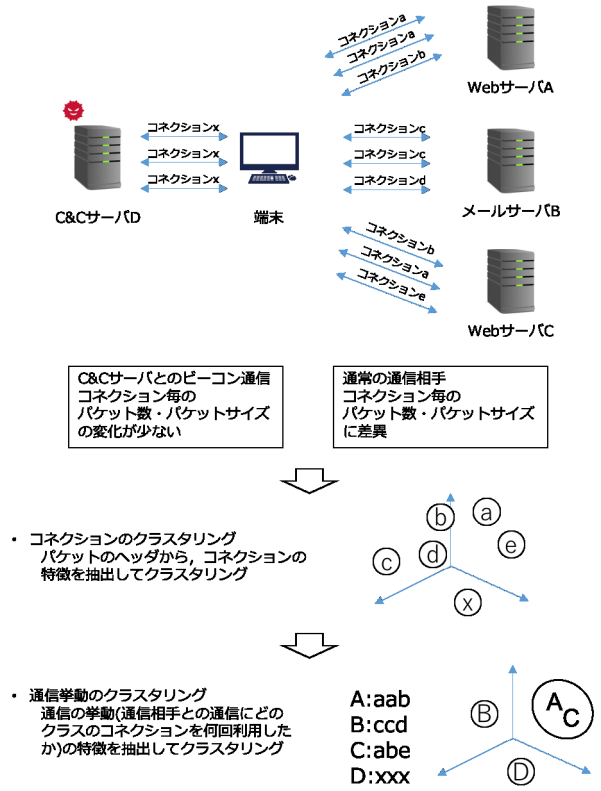

図 1　手法の概要

観測する手法では内部ホスト同士の通信を監視できないため，マルウェアによる内部調査を検知することはできない．文献 [5] ではマルウェア感染ホストが行う通信と正常な通信の違いに着目し，パケットのヘッダ情報から不正アクセスを検知している．文献 [6] では，トラフィックデータからセッション毎に特徴を抽出してクラスタリングし，各ホストの通信のクラスタ遷移を比較することで未知の攻撃を検知している．

本研究でも文献 [5],[6] と同様に正常な通信とマルウェアの通信の差異に注目し，標的型攻撃の手順 (3) 以降における不審な通信を検知する手法を提案する．本手法では，コネクションの特徴に注目したコネクションのクラスタリングと，通信相手がどのクラスのコネクションを何回使ったかを示す通信挙動に注目した，通信相手のクラスタリングに基づいて，マルウェアが C&C サーバ等と行う不審な通信を検知する．また，標的型攻撃による通信を観測したトラフィックデータを用いた検知実験を行い，提案手法の有効性を確認する．

3. 提案手法

本手法では，Web やメール等の通常の通信と C&C サーバ等との標的型攻撃における通信との TCP コネクションの特徴に基づき，標的型攻撃の通信を検出する．図 1 に手法の概要を示す．Web やメールなどの通常の通信においてはコネクション毎に，パケット数やパケットサイズなどの特徴が異なると考えられる．Web サーバとの通信であれば，同一サーバとのコネクションであっても，閲覧するページによってページのサイズ等が異なり．メールサーバであれば，送受信するメールのサイズによってコネクションに含まれるパケット数やパケットサイズ等が異なる．一方，C&C サーバとのビーコン通信の場合，情報を決まった書式で送信すると考えられるため，コネクションごとのパケット数やパケットサイズ等の変化が少ないと考えられる．

そこでまず，あるホストの通常のトラフィックデータから全ての通信相手に対するコネクションを抽出する．抽出したコネクションからパケット数やパケットサイズなどの特徴を抽出し，コネクションをクラスタリングする．次に，通信相手がどのクラスのコネクションを何回使用しているかを調べ，通信相手の通信挙動を示す特徴ベクトルとし，通信相手をクラスタリングする．以上の処理により通常通信を学習する．その後，新たな通信が観測された時，新たなトラフィックデータから，同様の手順でコネクションの特徴抽出を行い，コネクションのクラスタリング結果を用いて，新たに観測されたコネクションが異常であるかを検知する．また，新たなトラフィックデータの通信相手でも通信挙動を抽出し，抽出した通信挙動が学習時の挙動と類似しない場合に，不審な通信挙動として検知する．

3.1 学習処理

3.1.1 コネクションと特徴量の抽出

まず，監視ホストで日常的に行われる通信を tcpdump[7] で取得する．次に取得したトラフィックデータから送信元 IP アドレス，宛先 IP アドレス，送信元ポート，宛先ポートの組み合わせを抽出する．抽出した IP アドレスの組とポートの組からコネクション単位でパケットを抽出する．抽出した 4 つの情報では送信元から宛先へのパケットしか抽出できないため，送信元 IP アドレス，宛先 IP アドレスを入れ替えたパケットを合わせて抽出する．そして，抽出した双方向のパケットをパケット到着時間の情報を基にソートすることでコネクションを抽出する．

抽出したコネクションから表 2 に示す 36 種類の特徴量を抽出する．また後述する，通信相手の特徴抽出のために，特徴量を抽出する際に通信相手の IP アドレスを記録しておく．

3.1.2 コネクションのクラスタリング

抽出した特徴量をクラスタリングすることで，コネクションの特徴を学習する．まず，抽出した 36 種類の特徴量は高次元であるため，次元削減手法の一つである主成分分析を用いて次元を圧縮する．ここでは累積寄与率 85%以上となる最小の次元数を用いる．

次に次元削減を行なった特徴量を Mean-Shift 法を用いてクラスタリングする．Mean-Shift 法は事前にクラス数

表 2　特徴量の一覧

上りパケットサイズ平均	下りパケットサイズ平均
上りパケットサイズ最大	下りパケットサイズ最大
上りパケットサイズ最小	下りパケットサイズ最小
上りパケットサイズ合計	下りパケットサイズ合計
上りパケット数	下りパケット数
上りパケットサイズ分散	下りパケットサイズ分散
上り TTL 値平均	下り TTL 値平均
上り TTL 値分散	下り TTL 値分散
上り URG パケット数	下り URG パケット数
上り ACK パケット数	下り ACK パケット数
上り PSH パケット数	下り PSH パケット数
上り RST パケット数	下り RST パケット数
上り SYN パケット数	下り SYN パケット数
上り FIN パケット数	下り FIN パケット数
上り PSH&ACK パケット数	下り PSH&ACK パケット数
上り RST&ACK パケット数	下り RST&ACK パケット数
上り SYN&ACK パケット数	下り SYN&ACK パケット数
上り FIN&ACK パケット数	下り FIN&ACK パケット数
通信相手の IP アドレス	

を決定する必要がないため，本研究のように取得するトラフィックデータによってクラス数が変動する場合に適していると考えられる．クラスタリングすることで，コネクションの特徴が分類される．

3.1.3　通信挙動の抽出とクラスタリング

コネクションのクラスタリング結果から通信相手の特徴 (通信挙動) を抽出する．通信挙動に注目することで，コネクション単位では特徴が表れない攻撃の検知を目標としている．

まず，通信相手が，3.1.2 節でクラスタリングした結果中のどのクラスに分類されたコネクションで何回通信していたかを調べて，通信挙動の特徴ベクトルとする．次に特徴ベクトルを 3.1.2 節と同様に Mean-Shift 法でクラスタリングする．但し，通信挙動の学習では，コネクション数自体に特徴が表れているため，次元の圧縮は行わない．

3.2　異常検知

新たな通信が観測された時，まず，新たなトラフィックデータに対して 3.1.1 節のコネクションの分割，特徴量の抽出，そして，次元削減を行う．その後，新たなトラフィックデータから得られたコネクションの特徴を，コネクションをクラスタリングした空間に投影する．そして，各クラスの重心と投影した特徴量との距離を求め，最も距離が近いクラスを選択する．最も近いクラスの重心との距離 f_c がしきい値未満の場合には，そのクラスに属すると判断し，通常の通信で行われるコネクションであると判断する．しきい値以上の場合には通常の通信のクラスには含まれないとし，不審なコネクションと判断する．ここでしきい値は，クラス内の最も離れた特徴量との距離と設定している．

次に，通信相手の通信挙動の特徴ベクトルを学習時と同様に抽出する．ここで，通信挙動の中に不審なコネクションが含まれる場合，不審なコネクションは除いて特徴ベクトルを抽出する．抽出した特徴ベクトルを，通信挙動を学習した空間に投影し，各クラスの重心との距離を調べ，最も近いクラスを選択する．そして，最も近いクラスの重心との距離 f_b がしきい値未満であれば，学習した通信挙動と類似する挙動であると判断し，しきい値以上であれば不審な通信挙動であると判断する．しきい値は，クラス内の最も距離の離れた特徴ベクトルとの距離を基に決定している．

表 3　取得したトラフィックデータ

	コネクション数
Mail	160
PostgreSQL	40
Skype	150
TeamViewer	800
AppStore(Update)	150
Safari	1000
合計	2300

4.　実験

4.1　実験条件

実験に使用する通常のトラフィックデータは Mac mini(Late 2012)，macOS バージョン 10.12.6 を用いて取得した．まず，通常使用するアプリケーションの例として 6 つのアプリケーション (Mail，PostgreSQL，Skype，TeamViewer，AppStore，Safari) を稼働させ，トラフィックデータを取得した．各アプリケーションの稼働時に抽出したコネクション数を表 3 に示す．表 3 に示すトラフィックデータをアプリケーション毎に 2 分割し，それぞれを学習用とテスト用データとして用いる．ここで取得したトラフィックデータには使用したアプリケーションとは別のバックグラウンドで実行されているプロセスの通信も混入している．次に標的型攻撃の通信を含む例として，MWS Dataset 2017 の一つである，組織内ネットワークへの侵害活動を想定した動的活動観測のデータセット BOS Dataset 2015[9] を用いた．ここでは，2015 年 1 月 24 日の pcap データを使用した．BOS Dataset は組織内ネットワークを模擬した環境を構築し，攻撃者によるサイバー攻撃活動を観測したものである．使用した pcap データに含まれる通信内容の例と各 IP アドレスから抽出したコネクション数を表 4 に示す．表 4 に示す通信内容は文献 [3] を参照している．

学習処理において，Mean-Shift 法の初期値である半径を，コネクションの特徴を用いたクラスタリングでは 2.5，通信挙動の特徴を用いたクラスタリングでは 0.25 と設定した．また，通信挙動の異常検知のしきい値は，クラス内の最も距離の離れた特徴ベクトルとの距離の 4 倍の値を用いた．

4.2　実験結果と考察

4.1 節の実験データに対して，本手法の有効性を確認する

表 4　BOS Dataset

IP アドレス	通信内容	コネクション数
外部サーバ A	C&C サーバ 情報の送受信	546
ホスト A	DNS,SMB2,NTP 等のプロトコルを使用した 内部ホストとの通信	110
ホスト B	内部ホストとの通信 セッション未接続に終わるコネクション多数	97
ホスト C	HTTP プロトコルを使用した 内部ホストとの通信	24
ホスト D	NTP プロトコルを使用した通信	2
ホスト E	SMB プロトコルを使用した通信	1
ホスト F	SMB プロトコルを使用した通信	4
外部サーバ B	セッション未接続に終わるコネクション	1

全コネクション数	785

表 5　通常通信 コネクションの特徴の学習結果

アプリケーション	クラス
Mail	2,5,7∼11,13∼15
PostgreSQL	17,18
Skype	19,20,22
TeamViewer	23,24,25
AppStore(update)	27,28
Safari	29∼35
Mail, PostgreSQL Skype, TeamViewer AppStore, Safari	1,3
Mail, PostgreSQL Skype, TeamViewer Safari	12
Mail, Skype TeamViewer, Safari	4
PostgreSQL, Skype AppStore	16
Skype, AppStore Safari	21
AppStore, Safari	26

全クラス数	35

実験を行った．まず，通常通信の学習用データからコネクションを抽出してクラスタリングし，コネクションのクラスタリング結果を評価する．次に，通常通信の学習用データから通信挙動をクラスタリングし，通信相手のクラスタリング結果を評価する．その後，通常通信のテスト用データを利用して，コネクションの異常検出実験と通信挙動の異常検知実験を行い，正常と識別したコネクションや通信挙動がどのようなものであったかを評価し，更に異常を検知したコネクションや通信挙動を評価する．最後に，BOS Dataset 2015 を利用して，マルウェアによる C&C サーバとのビーコン通信や，内部ネットワーク間の調査を行う通信を検出できることを確認する．

通常通信の学習用データを用いて，コネクションの特徴に注目したクラスタリング実験の結果を表 5 に示す．コネクションをクラスタリングした結果，35 のクラスに分類された．分類されたクラスには，各アプリケーションを稼働した時刻のコネクションのみを含むクラスとアプリケーションを稼働した際に共通して見られるコネクションを含むクラスがあった．それぞれのアプリケーションを稼働した時刻のコネクションのみを含むクラスは，Mail は 10 個，PostgeSQL は 2 個，Skype 3 個など，同一のアプリケーションを稼働させている場合でも，幾つかのクラスに分割して学習されていた．また，複数のアプリケーションを稼働した時刻のコネクションを含むクラスは，7 個作成された．

表 6　通常通信 通信挙動の特徴を用いた学習結果

クラス	IP 数	クラス	IP 数
1	1	25	1
2	1	26	1
3	1	27	2
4	1	28	2
5	1	29	1
6	1	30	1
7	1	31	12
8	96	32	1
9	1	33	1
10	1	34	1
11	1	35	1
12	1	36	3
13	1	37	1
14	21	38	4
15	1	39	2
16	1	40	2
17	5	41	2
18	8	42	1
19	1	43	1
20	6	44	1
21	1	45	1
22	1	46	1
23	1	47	1
24	1	48	1

全 IP アドレス数	200

通常通信の通信挙動のクラスタリング実験を行なった．結果を表 6 に示す．通常通信の通信挙動は 48 のクラスに分類された．複数の通信相手が分類されているクラスは 48 のうち 13 クラスであった．Mail を使用した際の通信相手はクラス 5，7，9，10，PostgreSQL を用いた際の通信相手はクラス 13，TeamViewer を用いた際の通信相手はクラス 24 に分類された．クラス 8 に分類された通信相手のいくつかについて，通信内容を確認すると Apple のサーバと通信していた．この通信は AppStore(update) の通信を取得した時とは別の通信であり，バックグラウンドで実行されているプロセスの通信と考えられる．またクラス 8 に分類された通信挙動に共通した特徴として，コネクションの回数が他の通信挙動と比べ少なかった．

通常通信のテストデータに対して，コネクションの特徴に注目した異常検知実験を行なった結果を表 7 に示す．各アプリケーションのコネクションは PostgreSQL を除いて 82.5%以上が学習したクラスに分類された．PostgreSQL

表 7 通常通信 コネクションの特徴を用いた異常検知結果

アプリケーション	学習したクラスと同じクラスに分類されたコネクション数	学習したクラスとは別のクラスに分類されたコネクション数	異常と判断されたコネクション数
Mail	66 / 80 (82.5%)	5 / 80 (6.3%)	9 / 80 (11.2%)
PostgreSQL	14 / 20 (70%)	1 / 20 (5%)	5 / 20 (25%)
Skype	70 / 75 (93.3%)	0 / 75 (0%)	5 / 75 (6.7%)
TeamViewer	378 / 400 (94.5%)	20 / 400 (5%)	2 / 400 (0.5%)
AppStore(update)	68 / 75 (90.7%)	0 / 75 (0%)	7 / 75 (9.3%)
Safari	465 / 500 (93%)	0 / 500 (0%)	35 / 500 (7%)

表 8 通常通信の通信挙動の特徴を用いた異常検知結果

クラス	8	14	18	20	27	31	36	38	40	41	異常
IP アドレス数	125	17	6	20	2	7	29	6	1	4	24

表 9 通常通信の通信挙動の特徴例

通常の通信相手	クラス	1	2∼20	21	22∼35
	コネクション数	3	0	5	0

不審な通信相手 A	クラス	1	23∼35
	コネクション数	30	0

不審な通信相手 B	クラス	1∼20	21	22∼35
	コネクション数	0	27	0

表 10 BOS Dataset コネクションの特徴を用いた異常検知結果

IP アドレス	異常と判断されたコネクション
外部サーバ A	213 / 546
ホスト A	61 / 110
ホスト B	0 / 97
ホスト C	0 / 24
ホスト D	0 / 2
ホスト E	0 / 1
ホスト F	3 / 4
外部サーバ B	0 / 1

表 11 BOS Dataset 通信挙動の特徴を用いた異常検知結果

IP アドレス	異常検知結果
外部サーバ A	異常
ホスト A	異常
ホスト B	異常
ホスト C	異常
ホスト D	通常
ホスト E	通常
ホスト F	通常
外部サーバ B	通常

表 12 BOS Dataset 通信挙動の特徴の例

外部サーバ A	クラス	1	2∼3	4	5	6	7∼35
(不審な通信)	コネクション数	325	0	4	0	4	0

ホスト B	クラス	1∼22	23	24∼35
(不審な通信)	コネクション数	0	97	0

ホスト E	クラス	1	2∼35
(通常の通信)	コネクション数	1	0

が他のアプリケーションより異常と判断される割合が高かったのは学習したコネクションの数が少ないためである考えられる．異常と判断されたコネクションについて Wireshark を用いて通信内容を確認した．これらのコネクションはそれぞれのアプリケーションを使用した時のコネクションであり，バックグラウンドプロセスの通信のコネクションではなかった．なお，通信内容を確認しても明確な異常は発見できなかった．本手法により異常と検出されたのは，学習用データのデータ量が少なかったため，学習用データから抽出した特徴とテストデータから抽出した特徴に差異が表われたためであると考えられる．

通常通信のテストデータを用いた通信挙動の特徴に注目した異常検知実験の結果を表 8 に示す．テストデータでは，241 の通信相手と通信しており，そのうち 24 の IP アドレスが不審な通信相手と判断された．通常の通信相手と不審な通信相手の通信挙動の特徴例を表 9 に示す．表中の通常の通信相手に注目すると，使用しているコネクションは 2 種類で，コネクション数も少ないことが確認できる．それに対し，不審な通信相手は，特定のクラスに分類されたコネクションを多数使用している場合や，コネクション数が少ないが，様々なコネクションを使用していることを確認できた．

BOS Dataset 2015 に含まれる 1 月 24 日のコネクションの特徴を用いた異常検知実験の結果を表 10 に示す．外部サーバ A，ホスト A，ホスト F との通信には不審なコネクションがあると判断された．これらの不審であると判断されたコネクションの内容を確認すると，外部サーバ A，ホスト A の通信には TCP Retransmission のパケットが多数含まれていた．これより，FIN と ACK のフラグ数の差異から不審な通信と判断されたと考えられる．ホスト F とのコネクションでは，PSH と ACK のフラグ数が多いコネクションが不審なコネクションと判断された．内部調査を行なっていると思われるホスト B，ホスト C とのコネクションは検知できなかった．ホスト B とのコネクションは TeamViewer を使用した際の通信と同じクラスに含まれた．ホスト C とのコネクションは，HTTP プロトコルを使用したコネクションで正常にセッションを接続して終了しているため，通常のコネクションと判断された．以上より，C&C サーバである外部サーバ A とのビーコン通信，ホスト A との内部調査の通信に関しては検知できた．しかし，ホスト B，ホスト C の内部調査は検知できなかった．

BOS Dataset 2015 の通信挙動の特徴を用いた異常検知

実験を行なった．結果を表 11 に示す．コネクションの特徴を用いた異常検知結果と比較すると，外部サーバ A，ホスト A に加え，ホスト B，ホスト C との通信が異常，ホスト F との通信が通常と判断された．異常と判断された 4 つの通信相手は通信時のコネクション数が多く，通信挙動に特徴が表れたと考えられる．それに対し，通常の通信相手と判断されたホスト D，ホスト E，ホスト F，外部サーバ B に関しては，通信時のコネクションの数がごく少数であり，通信挙動に特徴が表れなかったと考えられる．通常の通信相手と異常な通信相手の通信挙動の特徴を表 12 に示す．外部サーバ A はクラス 1 に 325 のコネクション，ホスト B はクラス 23 に 97 のコネクションが分類されたことが確認できる．これに対し，ホスト E はコネクション数が少なく，クラス 1 にコネクションが 1 つ分類されたのみであった．今回のデータセットでは，C&C サーバとの通信や内部調査を行う通信はコネクション数が多く，コネクションの特徴が似た通信を行うため，異常だと判断されたと考えられる．しかし，使用するコネクション数が少ない通信相手の場合，通常の通信挙動との差異が表れにくく，ホスト D やホスト E，ホスト F，外部サーバ B の 4 つの通信相手は通常の通信と判断されたと考えられる．通信挙動の特徴を用いた異常検知では，コネクションの特徴を用いた異常検知では検知できなかったホスト B，ホスト C の内部調査を検知することができた．

以上より C&C サーバとの通信，組織内ネットワークの内部調査を検知できることを確認できた．今回使用した通信挙動の特徴量は，通常の通信相手と比較して使用するコネクション数が多い C&C サーバとの通信や内部調査を行う通信を不審な通信として検知できることを確認できた．しかし，使用するコネクションの少ない通信相手に対しては検知できない可能性がある．今後の課題として，C&C サーバとの通信や内部調査を行う通信を早期に発見するために新たな特徴を追加することなどが挙げられる．

5. おわりに

本稿では，パケットのヘッダから特徴を抽出し，通信挙動を学習してサイバー攻撃による不審な通信を検知する手法を提案した．標的型攻撃によるマルウェアの動的観測データを用いた実験では，C&C サーバとの通信，組織内ネットワークにおける内部調査を検知できた．しかし，通信挙動を特徴とする場合，使用するコネクション数が少ない通信相手に関しては異常を検知できない可能性がある．今後の課題として，使用するコネクションが少数でも異常検知できるよう，新たな特徴量の追加などが挙げられる．

参考文献

[1] McAfee Blog:なぜ多層防御なのか？リスクを最小限にする最強のセキュリティ対策，入手先 ⟨http://blogs.mcafee.jp/defense-in-depth-multilayer-protection⟩(2017.12.18).
[2] IPA 情報処理推進機構:攻撃者に狙われる設計・運用上の弱点についてのレポート，入手先 ⟨https://www.ipa.go.jp/files/000037456.pdf⟩(2017.11.28).
[3] 寺田真敏，堀健太郎，成島佳孝，吉野龍平，萩原健太:研究用データセット「動的活動観測 2015」，コンピュータセキュリティシンポジウム 2015 論文集，Vol.2015，No.3，pp.1387-1393(2015)
[4] 神谷和憲，青木一史，中田健介，佐藤 徹，倉上 弘，谷川真樹:Firewall ログを用いたマルウェア感染端末の検知手法，第 77 回全国大会講演論文集，Vol.2015，No.1，pp.433-434(2015)
[5] 蒋 丹，面 和成:初期段階における Remote Access Trojan の検知手法，コンピュータセキュリティシンポジウム 2014 論文集，Vol.2014，No.2，pp.719-726(2014)
[6] 蒋 丹，面 和成:通信のクラスタ間遷移に基づくサイバー攻撃検知手法，コンピュータセキュリティシンポジウム 2015 論文集，Vol.2015，No.3，pp.1066-1072(2015)
[7] tcpdump, 入手先 ⟨http://www.tcpdump.org⟩(2017.12.14).
[8] Wireshark, 入手先 ⟨https://www.wireshark.org⟩(2017.12.14).
[9] 神薗雅紀，秋山満昭，笠間貴弘，村上純一，畑田充弘，寺田真敏:マルウェア対策のための研究用データセット ~MWS Datasets 2015~，研究報告コンピュータセキュリティ，Vol.2015-CSEC-70，No.6，pp.1-8(2015)