論　文

エントロピーを特徴として用いた初期潜入段階におけるRATの通信検知*

石井　将大[†a)]　宇野　真純　猪俣　敦夫[††,†††]　新井イスマイル[††]
藤川　和利[††]

A RAT Detection Method by Using Packet Entropy on Early Intrusion Stage*

Masahiro ISHII[†a)], Masumi UNO, Atsuo INOMATA[††,†††], Ismail ARAI[††], and Kazutoshi FUJIKAWA[††]

あらまし　標的型攻撃の検知においては，初期侵入段階から端末制御段階までにRemote Access Trojan/Tool (RAT) の通信を検知することが有用とされている．本研究では初期侵入段階から端末制御段階までの間にRATの通信を検知することを目的とする．そのために，RATの通信検知に関する先行研究において用いられたパケット数やサイズといった特徴に加え，RATが通信を確立した際のC&Cサーバとの通信のパケットから，エントロピーを定義し，新たに特徴として加えた機械学習による検知手法を提案した．本研究で定義するエントロピーは，現状のRATと正常なアプリケーションの通信におけるパケットの偏りを表すものである．提案手法に対してk–分割交差検証を行い，RATと正常なアプリケーションの通信の分類実験を行った結果，ランダムフォレストによる検知において96.4%の高い精度と0.7%の低い誤検知率（偽陽性）が得られ，検知モデルの他の評価指標においても，提案手法が優れていることが分かった．

キーワード　RAT，侵入検知，ネットワークセキュリティ，機械学習

1. まえがき

標的型攻撃によって情報漏洩等の被害が深刻化し，社会問題となっている．標的型攻撃は特定の組織や機関を狙った攻撃の総称であり，以下の複数の段階を踏み，長期に渡って実施される [1].

（1）　事前準備：標的の情報収集．不正プログラムの準備，

（2）　初期侵入：標的型メール送信，不正プログラムの実行，

（3）　端末制御：C&Cサーバ間通信の確立，感染環境の確認，

（4）　情報探索：内部活動ツール送出，LAN内情の探索，

（5）　情報集約：有益な情報の収集，

（6）　データ送出：収集情報の入手．

初期侵入段階において，Remote Access Trojan/Tool (RAT) と呼ばれる遠隔操作を可能にするツールが用いられる．RATとはマルウェアの一種であり，標的型攻撃の検知では，侵入されることを前提と考え，初期侵入から端末制御段階の侵入時活動までにRATの通信を検知することが有用とされている [2]．攻撃者の行動が開始される前に攻撃の存在を知ることにより，被害を未然に防ぐことができる可能性が高くなる．

本研究では，ある特定の通信プロトコルを用いる等の制約された環境に依存しない，初期の侵入段階におけるRAT通信の検知を目的とする．寺田ら [3] の動的活動観測報告によると，RATが被害者端末に侵入し実行されてから攻撃者が遠隔操作を開始するまでの時間は最短で7分，最長で38時間であった．この期間内に得られる情報のみを用いて，環境や特定の動作

† 東京工業大学学術国際情報センター，東京都
Global Scientific Information and Computing Center, Tokyo Institute of Technology, Tokyo, 152–8550 Japan
†† 奈良先端科学技術大学院大学総合情報基盤センター，生駒市
Information Initiative Center, Nara Institute of Science and Technology, Ikoma-shi, 630–0192 Japan
††† 東京電機大学，東京都
Tokyo Denki University, Tokyo, 120–8551 Japan
a) E-mail: mishii@gsic.titech.ac.jp
* 本論文はインターネットアーキテクチャ研究専門委員会推薦論文である．
DOI:10.14923/transcomj.2017JBT0001

に依存せず，RAT の通信の検知が可能な手法を提案する．

Jiang ら [4] は，RAT が通信を開始した短期間における通信内容を解析し，機械学習によって RAT と正常アプリケーションの通信を分類する手法を提案している．先行研究で用いられている特徴は，TCP 通信の外向き，あるいは内向きのパケット数やパケットサイズ等である．ただし，通信の観測期間はかなり短く，また，特徴の数は少ないため，RAT に対して，通信の特徴が似ている正常アプリケーションが存在し，誤検知や見逃しが起こる．

本研究では，RAT と正常アプリケーションの通信の特徴の差をより明確にするために，パケットの送信間隔の偏りを表すエントロピーを定義し，それを新たな特徴として加えて機械学習を行い，その検知モデルの評価を行う．更に，RAT 検知に有用なエントロピーを定義するために，先行研究と比較して長期間（初期の侵入段階における RAT 通信を検知する目的は達成できる数十秒間）アプリケーションの通信を観測する．

先行研究 [4] と同様の検知システムにおいて評価実験を行った結果，検知精度 (ACC) や，誤検知率 (FPR)，見逃し率 (FNR) 等，その他検知モデルを評価するあらゆる指標において，我々の提案手法が優れていることが分かった．具体的には，ランダムフォレストにより 96.4%の ACC と 0.7%の FPR が達成され，先行研究の手法に対するそれぞれの評価値は 95.8%, 0.7%であった．また，FNR は決定木による 20.0%が最良で，先行研究の 33.3%と比較して，より低い FNR を達成している．

本論文の構成は以下のとおりである．**2.** では既存のネットワークベースなマルウェアの検知手法を述べた上で，RAT の早期検知に適した手法を検討する．**3.** において，RAT と正常なアプリケーションの通信の特徴とその違いに注目し，本研究で通信の新たな特徴として用いるエントロピーの定義を与える．**4.** では，機械学習アルゴリズムを用いた，RAT 通信の早期検知を行う提案手法の詳細を述べる．**5.** において，提案手法の評価実験結果，及びそれに対する考察を示し，**6.** で本研究のまとめと今後の課題について述べる．

2. ネットワークベースのマルウェア検知に関する研究

マルウェアの検知方式は，主としてホストベースとネットワークベースに分けられる．

ホストベースの検知手法では，主にホスト上で取得されるプロセス情報を用いて検知を行う．具体例としてバイナリ解析や API コールの監視，マルウェアの動的解析が挙げられる．ホストベースの検知手法の利点は，システムの挙動の解析が可能であり，検知に利用可能な情報が多いことである．しかし一方で，難読化されたマルウェアの解析などに多くのリソースを要すること，各ホストにインストールが必要であることや，検知のために得られる情報が OS 等のプラットホームに強く依存するため，プラットホームの知識が必要であること，検知に用いる情報を解析し，収集するために時間を要するといった欠点が存在する．具体的には，シグネチャマッチングによる検知は，シグネチャの生成に時間を要することが問題として挙げられている．セキュリティベンダーの McAfee 社の 2016 年第 4 半期 (Q4) 脅威レポート [5] によると，マルウェアは増加の傾向にあり，2016 年の第 3 四半期 (Q3) の時点で，そのサンプル数は 6 億を超えている．

マルウェアの動的解析の関連研究としては [6], [7] 等が挙げられるが，本研究のターゲットである，RAT が完全に端末制御段階に入る前の早期検知に対するシナリオにおいては各手法の適用が難しい．

また，RAT の早期検知を目的としたホストベース検知手法が [8], [9] によって提案されている．これらの研究においては，採取するそれぞれ通信の観測時間は比較的短いが，機械学習に用いる標本データである通信の特徴ベクトルの抽出，またその分類に掛かる処理性能の評価結果が示されておらず，ネットワークのトラヒック量が比較的大きい場合にリアルタイムに検知が行えるかは明らかではない．

一方，ネットワークベースの検知手法では RAT と正常なアプリケーションの通信特徴の違いに着眼し，ネットワークから得られるパケット等の通信の情報を用いて検知を行う．具体例として，ネットワーク監視や通信パケット解析，ネットワークのシグネチャマッチング解析や通信シーケンスのパターンマッチング解析などが挙げられる．ネットワークベースの検知手法の利点は，リアルタイム性に優れ，早期の段階で検知が可能であることが挙げられる．欠点は，ネットワークから得られる大量の情報から分類・検知を行うため，新規のサンプルの検出に非効率的であることや，収集できる特徴の種類がホストベースの検知手法に比較して少ないことが挙げられる．

本研究に関連するネットワークベースの検知手法に

ついて，次節で詳しく説明する．

2.1 ネットワークベース検知手法

ネットワークベースの検知手法として通信シーケンスのパターンマッチング解析や HTTP ヘッダ解析などのパケット解析が挙げられる．具体的な既存手法について以下に詳細を述べる．

2.1.1 通信シーケンスのパターンマッチング解析

通信シーケンスのパターンマッチング解析では，実際にマルウェアにシステムの侵入を許した際にどのような通信シーケンスを行うかを正常な通信シーケンスと比較し，特徴を明確にして検知に用いる．この手法は，解析に用いる通信シーケンスのパターンが誤検知を発生させないように，正常な通信とマルウェアの通信の明確な定義が必要である．また，ネットワークに接続された端末ごとに通信シーケンスを監視する必要がある．

山田ら [10] の研究では，SMB の操作終了と RAT の out-bound 通信を結びつけ，特徴として検知に用いている．この手法では，攻撃の通信の特徴として，特定のプロトコル（SMB）が利用されることを前提としている．そのため，プロトコルの特徴に強く依存しているため，異なるタイプのプロトコルを用いた通信が用いられた場合に検知するのは困難である．また，検知に RAT 通信と内部攻撃通信の相関を用いているが，二つの通信の間にダミーの操作や通信が行われると，相関が取れず検知ができない．

2.1.2 通信パケット解析

通信パケット解析とは，マルウェアが C&C サーバと通信を行う際に得られた通信パケットを解析し，検知に用いる手法である．通信パケットからマルウェアの通信の特徴を抽出し，通常の通信との差によってそれぞれの通信を判別する．

山内ら [11] は，通信パケットから得られる in-/out-bound 通信のそれぞれのパケット数の合計とデータサイズの合計，セッション時間，アクセス回数，アクセス時間間隔を特徴とし，マルウェアの C&C トラヒックの抽出を行い，その実験結果に対して評価を行っている．この手法は HTTP 通信を行う場合のみに有効であり．他のプロトコルを用いたマルウェアの通信に対応ができない．更に，C&C サーバよりマルウェアが命令を受け取った際のパケットを分類に用いるため，検知ができた段階で既に攻撃者に情報が漏洩している可能性がある．

Li ら [12] の研究では，RAT の検知のための MANTO というシステムを作成している．MANTO は学習フェーズと検知フェーズから成る．MANTO は特徴ベクトルの要素として in-bound 通信と out-bound 通信のバイト数の比率を用いているが，P2P 通信を行う RAT が HTTP や HTTPS 通信を行う RAT よりもその比率が異なるために検知出来ず，それが全体の検知率を下げている．

Jiang ら [4] は，検知に用いる情報の取得期間として新たに**初期段階** (*early stage*) の定義を行い，正常なアプリケーションと RAT の通信の特徴を明確にし，検知を行っている．初期段階とは感染端末から TCP コネクションの SYN パケットが送信されてから，パケットの送受信を観測した際，初めてパケットの間隔がしきい値を超えるまでの期間のことをいう．[4] ではその間隔として 1 秒が最適であると報告されている．しかし，用いる特徴は初期段階内で観測されたパケットの情報のみであるため，判断材料の情報が少なく，検知できるものに限界があり誤検知を生む可能性が非常に高い．検知に用いられる特徴が RAT のパケット数に強く依存しており，初期段階内の通信パケット数の少ない Skype や Dropbox などの正常なアプリケーションと RAT が判別できない問題がある．この手法で用いられた特徴だけでは，正常なアプリケーションと RAT の通信パケットの差は少なく，互いを明確に判別するための特徴としては不十分である．

Wu ら [13] は，攻撃者によって遠隔操作が行われる，情報探索・集約，データ送出段階における通信パケットを検知する手法を提案しており，0.6%の非常に低い誤検知率を達成している．また，頻出系列マイニングにより，RAT が行う keep-alive 通信を除外し，人為的な操作による通信パターンを検知することに成功している．

2.2 RAT 通信の早期検知システムの必要要件

先述したとおり，RAT の通信検知は初期侵入から端末制御段階に行うことが有用である．RAT による被害を考慮した早期検知のために，以下の 3 点の要件が必要とされる．

- 初期侵入から端末制御段階までの間に特徴の収集が可能であること，
- 特定の環境やプロトコルに依存せず亜種にも対応できること，
- 検知システムにリアルタイム性があること．

リアルタイム性に関しては，ネットワークベースの検知手法が優れているため，RAT の通信検知にはネッ

トワークベースの検知手法が適していると考えられる．

2.1 で述べた先行研究のうち，唯一の要件を満たす手法は Jiang らの手法 [4] のみである．しかし，先に述べたように Jiang らが用いた特徴だけでは，分類が難しい RAT の通信データがある．実際に我々が採取した RAT の一種である Adwind の通信データの特徴は，初期段階であってもパケット数が比較的多い．本研究ではそのような RAT の通信も検知できることを示す．

3. アプリケーションの通信の偏りを表すエントロピーの定義

本研究は，Jiang ら [4] の研究において，**2.1** で述べた特徴に加えて，エントロピーを新たな特徴として利用し，より多くの RAT に対して検知実験・評価を行う．本節では，本研究で定義するエントロピーの意味を，RAT の通信の特徴を正常アプリケーションとの対比を行うことで説明する．

3.1 RAT の通信の特徴

RAT と正常なアプリケーションの通信の特徴とその違いについて述べる．図 1，2 はそれぞれ RAT の一種である Adwind と，正常なアプリケーションである Skype の通信パケットの入出力グラフである．横軸がパケットキャプチャを行った継続時間，縦軸が 1 秒間に送信されたパケット数である．双方のグラフを比較した場合，初期のパケット数は Adwind は 241，Skype は 561 と非常に多い．図 2 において，14 秒経ったあたりから Skype の通信パケットは一定量のパケットが連続して送受信されている．それに対し，Adwind の通信パケットはキャプチャ開始直後に多くのパケットの送受信が行われた後は，次のパケットが送受信されるまでに広い間隔があり，入出力パケット数に大きな偏りがある．

寺田ら [3] の報告によると，RAT が被害者端末に侵入し，実行されてから攻撃者が遠隔操作を開始するまでの時間は最短で 7 分，最長で 38 時間とある．Adwind におけるこの偏りは，攻撃者が RAT の操作を行わないためだと推定される．また，RAT が実行された後に攻撃者が操作を開始されるまで keep-alive 通信を行うものも多くあるが，keep-alive 通信が始まるまでの時間がある程度長い場合，全体的なパケット数の偏りが生じる．攻撃者が RAT を操作する段階に入ると，その操作は人為的なもので複雑であり，偏りは小さくなる傾向がある．

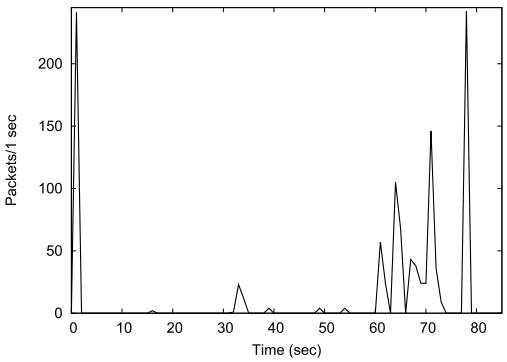

図 1　Adwind のパケット入出力グラフ
Fig. 1　Number of input and output Adwind packets.

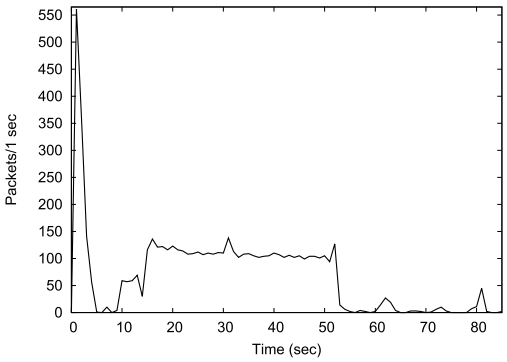

図 2　Skype のパケット入出力グラフ
Fig. 2　Number of input and output Skype packets.

このような RAT の通信特徴に対し，正常なアプリケーションにおいては，通信開始直後からユーザによる操作が始まり，パケット数の偏りは比較的小さく，エントロピーが大きくなる傾向がある．

3.2 本研究におけるエントロピーの定義

前節で RAT の通信の特徴として，パケットの送受信間隔，その量に偏りがあることを指摘した．本節と次節では，エントロピーを用いた，その偏りの特徴の数値化について説明する．

エントロピーの計算には以下の式で表される，シャノンによるエントロピーを用いる．

$$H(X) = -\sum_i p_i \log p_i. \tag{1}$$

本研究においては，RAT による通信の out-bound パケットの送信間隔，パケット数の偏りをエントロピーを用いて表す．Out-bound パケットのみ注目する理由は，RAT に感染した後に，攻撃者がその RAT を操作するまでに行われる通信においては，RAT から

外向きに送信されるパケットが，逆の内向きのパケットより意味があり，多く観測されるためである．すなわち，上の考察から，p_i を以下のように定義する．

$$p_i = \frac{T_i}{S}, \tag{2}$$

ただし，

S: s 秒間の通信における out-bound パケットの総数，

T_i: s 秒間の通信を t 秒間隔で分割した i 番目の区間における out-bound パケット数

である．

実際には，各 TCP セッションに対し，S は 3 ウェイハンドシェイクの SYN パケットを送信してから s 秒間に得られた out-bound パケット数として定義され，そのセッションの特徴ベクトルを生成する際のエントロピー計算で用いる．定義より，s, t の値の設定により，各区間で観測される out-bound パケット数の割合 p_i と，それによるエントロピーの値は変化する．パラメータ s, t を適切に設定することにより，例えば偏りが大きい場合は，out-bound 通信の偏りが p_i によって表されることから，式 (1) によるエントロピーが小さくなり，RAT と正常アプリケーションに対する out-bound 通信の偏りの差を本研究で定義するエントロピーによって区別できる．

3.3 エントロピーによるパケット送信間隔の偏りの数値化

本節では，**3.2** で述べた，エントロピーを適切に定義するためのパラメータ s, t を事前実験により決定する．具体的には，通信の out-bound パケットの偏りを，本研究で定義するエントロピーを用いて数値化した場合，RAT と正常なアプリケーションの特徴の差を最も効果的に捉えられるような s と t をそれぞれ求める．

3.3.1 通信の観測時間 s に関して

エントロピーの算出に用いる s の適切な値を求める．s 秒間に観測される out-bound パケット数 S に関して，s の値の変化がエントロピーにどのような変化を与えるか実験を行った．以下，区間幅 t は 0.05 秒で固定し，s の値を変化させたときのエントロピーの値の変化を示す．実験において，アプリケーションとして RAT は Adwind, DarkComet, 正常なものは Dropbox（アプリケーション），TeamViewer, Skype, Firefox を利用した．

表 1 は s を変化させたとき，各アプリケーションの通信におけるエントロピーの値を示したものである．また，図 3 はそのエントロピーの変化をグラフに表したものである．s を小さくしたとき，感染端末に潜入した RAT に関して，攻撃者の C&C サーバへ 3 ウェイハンドシェイクの SYN パケット送信した後，攻撃者とのネットワーク確立までの通信パケット数が少ないものは，偏りが大きくエントロピーの値が極端に小さくなる傾向がある．これは keep-alive 通信による定期的な通信のパケットが，エントロピーの計算に含まれず，データに偏りが顕著に現れた結果だと推測される．逆に，s が大きくなった場合 RAT と正常なアプリケーションの値の差が少なくなっている．これは s を長く取るほど keep-alive 通信が影響を与え，out-bound 通信のパケット数の偏りを小さくしているからである．

s が 10 秒未満といった小さな値を取るとき，図 1 の Adwind RAT のように，コネクション開始時の通信により入出力パケット数が大きい場合は，正常アプリケーションのエントロピーに対して差が拡がらないことが想定される．更に，上で述べた keep-alive 通信の影響も考慮し，本実験は $10 \leq s \leq 40$ の範囲で行った．また，次節において，区間幅 t に対するエントロピーの変化について考察を与えているが，本実験にお

表 1 観測時間 s に対するエントロピーの比較
Table 1 Entropy defined by the multiple values of parameter s.

s (sec)	10	20	30	40
Adwind	2.65	2.79	2.79	3.21
DarkComet	0.06	0.22	3.51	3.62
Dropbox	4.50	4.78	4.81	5.52
TeamViewer	3.62	3.80	4.15	4.02
Skype	6.68	7.78	8.58	9.17
Firefox	4.39	4.67	5.36	4.90

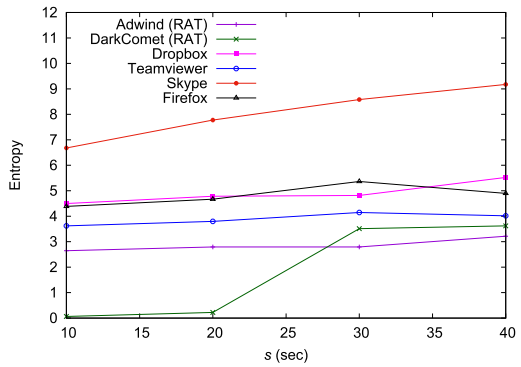

図 3 観測時間 s に対するエントロピーの変化
Fig. 3 Relation between entropy and parameter s.

表 2　区間幅 t に対するエントロピーの比較
Table 2　Entropy defined by the multiple values of parameter t.

t (sec)	0.01	0.02	0.04	0.06	0.08	0.1
Adwind	2.79	2.47	1.55	1.68	1.32	0.65
DarkComet	3.51	2.72	1.64	1.03	0.81	0.68
Dropbox	4.81	4.61	4.23	4.11	3.89	3.87
TeamViewer	4.19	4.23	3.99	3.79	3.70	3.63
Skype	8.58	8.44	8.14	7.80	7.50	7.23
Firefox	5.36	4.65	4.48	4.24	4.18	4.20

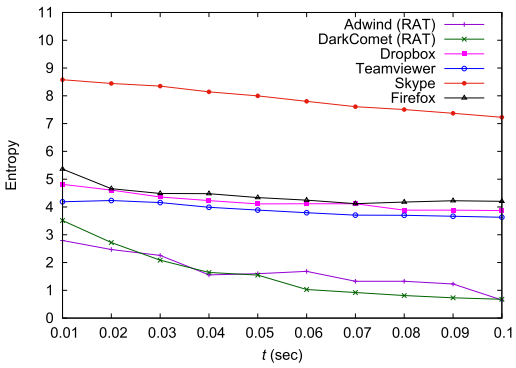

図 4　区間幅 t に対するエントロピーの変化
Fig. 4　Relation between entropy and parameter t.

いてはその他の t に対しても上記のエントロピーの性質が確認できたため，$t = 0.05$ の評価結果を示した．

3.3.2　通信観測時間の分割区間幅 t に関して

通信の観測時間 s を分割する際の区間幅 t の適切な値を求める．以下に，$s = 30$ 秒に対する t を変化させた際の，エントロピーについてその値と変化を示す．使用した RAT, 正常アプリケーションは **3.3.1** で述べたものと同じである．

表 2 は $s = 30$ 秒のとき，区間幅 t を変化させたときのエントロピーの比較表である．区間幅 t の増加に伴い，全体的にエントロピーが小さくなる傾向が確認できる．また，図 4 はその値の変化をグラフで表している．t が増加した場合，エントロピーの値は減少していくが，RAT は正常なアプリケーションよりも値が低くエントロピーの減少率が高いことが分かる．

これは，本手法では i 番目の区間に存在するパケット数が 0 となる場合，エントロピーの計算において $p_i = 0$ となることから，区間幅 t を極端に狭めると，大きな偏りを分割してしまい，通信間隔がほぼ等間隔とみなされるためである．したがって，keep-alive 通信までのインターバルタイムがエントロピーの計算結果に与える影響も少なくなり，偏りを上手く表せない結果となる．実際に，$t = 0.01$ といった分割幅が過剰に小さい場合は，上記の性質が現れることを確認した．また，RAT の通信データに対し，$t > 0.1$ の範囲では正常なアプリケーションのエントロピーは低下し続け，本実験で扱った Adwind, DarkComet といった RAT のある TCP セッションに対するエントロピーは，その小さな値が増加してしまい，エントロピーの差が低下してしまう現象も見られた．以上の理由から，本実験は $0.01 \leq t \leq 0.1$ の範囲で行った．

3.3.3　エントロピーの定義のための適切なパラメータ s, t の設定

先述したとおり，s を増加させたとき，RAT と正常なアプリケーションの通信から得られたエントロピーの値の差は少なくなっている．特に，RAT の一種である DarkComet は 20 秒を過ぎたあたりから急速に値が上昇している．これは keep-alive 通信が行われ，結果として，偏りが正常なアプリケーションのものと区別がし難く，そのエントロピーが近い値になる．したがって，s は keep-alive 通信が行われるまでとしなければ，検知に適したエントロピーを定義できない．また，本研究は初期潜入から端末制御段階までの検知を目的としているため，s は長期間であってはいけない．図 3 より，s の値は，通常のアプリケーションによる通信のエントロピーと RAT による通信のエントロピーとの差が最も開く，keep-alive 通信が行われる前の $s = 20$ 秒が適していると考えられる．

また，分割区間幅 t について，図 4 より t の増加に伴い，RAT と正常なアプリケーションの通信から得られたエントロピーの差は大きくなっている．一方で分割区間幅が 0.1 秒より少なかった場合にそれぞれのエントロピーの値の差は少なくなっている．これは分割区間幅が小さく，適切に偏りを捉えられず，上手く正常なアプリケーションの通信の偏りと区別がつかなくなるからである．したがって，適した t の値は偏りを分割しない $t = 0.1$ 秒が適していると考えられる．

4.　エントロピーを用いた RAT の通信検知手法

本節では RAT の通信検知のための提案手法を述べる．

4.1　機械学習を用いた RAT の通信の早期検知 [4]

提案手法は初期侵入段階から端末制御段階までの間に，RAT の通信を検知することを目標としている．したがって，検知のための時間に制限があり，リアルタ

イム検知が可能な実装が求められる．

Jiang ら [4] は，各 TCP 通信において**初期段階** (*early stage*) を定義し，その範囲で観測されたパケットに対して，機械学習で用いる特徴ベクトルを算出し，通信の分類を行った．より具体的には，それぞれのアプリケーションの通信は**セッション**ごとに分割され，それぞれのセッションに対し特徴ベクトルが定まる．ここで，セッションは TCP コネクションの意味しており，初期段階とは，3 ウェイハンドシェイクの SYN パケットが送信されてから，各パケットの通信間隔が設定されたしきい値を超えるまで [4] (Definition 1) と定義されている．Jiang ら [4] の検知システムは以下の三つの要素から構成される．

（1） 特徴抽出フェーズ，
（2） ラーニングフェーズ，
（3） 検知フェーズ．

特徴抽出フェーズでは，TCP コネクションごとのパケットを入力とし，必要な特徴を抽出して特徴ベクトルを生成する．

ラーニングフェーズにおいて，特徴抽出フェーズで得られる既知の通信データの特徴ベクトルを入力とし，それぞれ RAT の通信と通常のアプリケーションの通信をラベリングし，そのデータを学習させる．ラーニングフェーズにおける出力は検知モデル（分類器）である．

検知フェーズにおける入力は，ラーニングフェーズで得られた検知モデルと，通信が正常なものか RAT のものか判別したい未知の特徴ベクトルである．判別したいパケットデータを特徴抽出フェーズに入力し，ラベルが付けられていない未知の特徴ベクトルを生成する．検知フェーズにおいて，その未知の特徴ベクトルに対し，検知モデルを用いて正常な通信か RAT による通信かを予測させる．

4.2 提案手法の概要

提案手法における RAT 検知の流れは，**4.1** で述べた Jiang ら [4] のフレームワークに従う．機械学習で用いる特徴ベクトルは表 3 に示した 8 種類の特徴を抽出して定義される．

表 3 において，初めの 7 種の特徴は Jiang ら [4] で用いられているものであり，Entropy が本研究で新たに追加した特徴となる．

先行研究 [4] と比較して，特徴抽出フェーズにおいてエントロピーを算出するための計算時間が必要だが，特に計算コストの高いラーニングフェーズは独立しており，実際の通信の分類を行う前に実行しておけば良いため，特徴の抽出と，検知フェーズの計算性能が検知システムのリアルタイム性に影響を与える．

表 3 特徴の種類
Table 3 Network features.

特徴	説明
PacketNumber	パケット数
OutByte	out-bound データサイズ
OutPacketNumber	out-bound パケット数
InByte	in-bound データサイズ
InPacketNumber	in-bound パケット数
O/I PacketNumber	out-/in-bound パケット数の比
OutByte/OutPacNum	out-/in-bound データサイズの比
Entropy	エントロピー

4.3 検知フレームワークの実装

本節では，提案手法の具体的な実装方法について説明する．実装は Python 2.7.13 を用いて行い，パケットの処理には Python ライブラリの dpkt [14] を用いた．また，機械学習の各モデルの生成や，評価指標の算出には scikit-learn [15] を利用した．

4.3.1 特徴抽出フェーズ

特徴は表 3 に示したとおりであり，本フェーズにおいて各セッション（TCP コネクション）に対する各特徴量を計算していく．計算過程は [4] (Fig. 2) に準ずる．本研究では，**3.3.3** で述べたとおり，エントロピーの定義から $s = 20$ 秒をセッションの観測時間としている．したがって，セッションの観測を始め，20 秒経つまでに随時 PacketNumber, OutByte, OutPacketNumber, InByte, InPacketNumber の値を更新していく．そして，観測を始めて 20 秒経った後に O/I PacketNumber, OutByte/OutPacNum, Entropy を計算して，そのセッションに対応する特徴ベクトルを出力する．

4.3.2 ラーニングフェーズ

本フェーズでは，特徴抽出フェーズで得られた既知のセッションの特徴ベクトルに，それぞれ RAT による通信か通常なアプリケーションの通信かをラベリングし，教師あり学習を用いて各アルゴリズムによる検知モデルを生成する．

既知の特徴ベクトルに対して，対応するセッションが RAT のものならば ‘1’ を，通常のアプリケーションのものならば ‘0’ をラベリングしていく．それらのラベル付けされたデータに対し，表 4 に示す教師あり学習の各アルゴリズムによる検知モデルを生成する．

4.3.3 検知フェーズ

本フェーズでは，ラーニングフェーズで得られた検

表 4　本研究で使用した機械学習の分類アルゴリズム
Table 4　Classifiers for experiment.

検知モデルの名称	説明
SVM	サポートベクターマシン
NB	ナイーブベイズ分類器
KNN	k-近傍法
DT	決定木
RF	ランダムフォレスト

知モデルと特徴抽出フェーズで得られた未知の特徴ベクトルを入力とし，未知の特徴ベクトルが RAT の通信によるものであるか，正常なアプリケーションの通信によるものかの予測を行う．出力はその特徴ベクトルに対するラベル ‘0’ あるいは ‘1’ である．出力結果が ‘1’ であった場合，入力の特徴ベクトルは RAT による通信によるもの，‘0’ であった場合は正常なアプリケーションの通信によるものであると分類される．

5.　実験結果と評価

本章では，**4.** で述べた提案手法の検知システムを実装し，各検知モデルの評価を行い，Jiang ら [4] の手法による結果と比較を行う．

評価実験に用いた RAT と正常アプリケーションの種類，特徴ベクトルの個数をそれぞれ表 5, 6 に示す．

正常なアプリケーションについては Jiang ら [4] が用いたものを利用する．ただし，RAT に関しては，十分な長さの通信データ等，本提案手法で必要なデータとして，[4] (Table 3) に挙げられている全ての検体のデータを手に入れることができなかった．したがって，先行研究とは異なる種類の RAT と，そのデータを用いて実験を行った．しかし，提案手法とともに，Jiang ら [4] の手法でも評価を行っているため，今回用いたデータに関しては，各手法の検知モデルの評価とその比較結果が得られている．

利用した RAT について，Bandook, Gh0st Rat, Turkojan, Poison Ivy 等は観測時期が 2000 年代と古いものであるが，先行研究との比較のため用いている．また，Adwind, DarkComet, Imminent Monitor, LuminosityLink 等は比較的観測時期の新しい，広範囲に影響を及ぼしている RAT であり，[4] では利用されていないものである．

検知モデルの評価のために，先行研究と同様にして k–分割交差検証を行った．標本データ（特徴ベクトル）に対し，k–分割交差検証は以下の 3 ステップを行う．

（1）　標本データを k 個のグループに分割する．

表 5　評価実験に用いた RAT と特徴ベクトルの個数
Table 5　Number of feature vectors of each RAT.

RAT	特徴ベクトル
Adwind	1
Babylon Rat	1
Bandook	1
Blackshades	1
Crimson	1
DarkComet	1
Gh0st Rat	1
Imminent Monitor	1
jRat	1
LuminosityLink	1
NanoCore	1
njRAT	1
Turkojan	1
Poison Ivy	1
Xtreme	1
	計 15 種 15 個

表 6　評価実験に用いた正常アプリケーションと特徴ベクトルの個数
Table 6　Number of feature vectors of each normal application.

正常アプリケーション	特徴ベクトル
BitComet (P2P software)	1
BitTorrent (P2P software)	5
Chrome (web browser)	23
Dropbox (cloud service)	6
Firefox (web browser)	20
Skype (instant messenger)	33
Teamviewer (P2P software)	6
TorBrowser (web browser)	12
PPTV (P2P software)	38
Yahoo! Messenger (instant messenger)	6
	計 10 種 150 個

（2）　分割したうちの一つのグループのデータをテスト用とし，残りの $k-1$ グループのデータを学習用とする．

（3）　全てのグループを一度テスト用のデータとして利用し，(2) の検定を k 回繰り返す．

最終的な精度等の指標は，各検定で得られる指標の平均値として求める．k–分割交差検証は検知モデル（分類器）の基本的な評価手法であり，テストデータは学習データに含まれないため，未知のデータに対する検知・分類がそのモデルでどの程度できているかを測る有効な検証法である．

比較対象である Jiang ら [4] の研究と同様に，k–分割交差検証において，k 個のグループのそれぞれに RAT の特徴ベクトルが一つずつ含まれるようにして実験を行った．したがって，本実験では $k = 15$ となる．

検知モデルの評価で用いた指標は以下の 7 種である．

$$ACC = \frac{TruePositive + TrueNegative}{TotalNumber}$$
$$FPR = \frac{FalsePositive}{FalsePositive + TrueNegative}$$
$$FNR = \frac{FalseNegative}{TruePositive + FalseNegative}$$
$$PRC = \frac{TruePositive}{TotalPositive + FalsePositive}$$
$$REC = \frac{TruePositive}{TotalPositive + FalseNegative}$$
$$F1 = \frac{2 \cdot Recall \cdot PRC}{REC + PRC}$$
$$AUC = \text{Area Under the (ROC) Curve}$$

表 7　k–分割交差検定による提案手法と先行研究の比較
Table 7　Comparison of experimental results with k-fold cross validation using each classifier.

提案手法							
	ACC	FPR	FNR	PRC	REC	F1	AUC
SVM	0.921	0.007	0.800	0.200	0.200	0.200	0.740
NB	0.164	0.907	0.133	0.088	0.867	0.159	0.387
KNN	0.945	0.027	0.333	0.567	0.667	0.600	0.900
DT	0.952	0.033	0.200	0.667	0.800	0.711	0.920
RF	0.964	0.007	0.333	0.667	0.667	0.667	0.917
Jiang ら [4]							
	ACC	FPR	FNR	PRC	REC	F1	AUC
SVM	0.909	0.000	1.000	0.000	0.000	0.000	0.797
NB	0.152	0.920	0.133	0.085	0.867	0.154	0.427
KNN	0.909	0.000	1.000	0.000	0.000	0.000	0.843
DT	0.921	0.053	0.333	0.489	0.667	0.544	0.857
RF	0.958	0.007	0.400	0.567	0.600	0.578	0.947

ACC は精度 (accuracy) を表し，その検知モデルの検知精度を表す．FPR は誤検知率 (false positive rate) であり，正常なアプリケーションの通信を RAT のものと誤って分類してしまう率である．FNR は見逃し率 (false negative rate) であり，RAT の通信を正常なアプリケーションのものとして見逃してまう率である．PRC は適合率 (precision) であり，RAT の通信として判別したサンプルの正確度を表す．REC は再現率 (recall) であり，true positive rate と同じで RAT 通信の検知率である．F1 は F1-score と呼ばれるものであり，PRC と REC の調和平均によって定義される．AUC は ROC (Receiver Operator Characteristic) 曲線の曲線下面積によって与えられる指標で，与えられたサンプルに対し，どの程度良い分類器が得られているかを示す一つの評価軸となる．

5.1　検知モデルと RAT の検知精度に関する評価

本節では，k–分割交差検証による各検知モデルと RAT の検知精度に関する評価を与える．表 7 に提案手法と先行研究の各種機械学習アルゴリズムを用いた場合のそれぞれの指標を示す．

検知モデル SVM と NB に関しては，提案手法，Jiang ら [4] の手法共に FPR あるいは FNR が非常に高く，RAT の検知に有効的ではない．更に，Jiang らの手法による実験結果において，検知モデル SVM, KNN の対して全てのサンプルデータが（すなわち全ての RAT の通信が）正常な通信として判断されている．本実験は，Jiang らが実際に [4] で用いたデータとは異なる RAT を利用しており，上記の結果は [4] で示されている FPR, FNR の指標値に差が見られる．ただし，[4] (Table 5) で示されているように，利用する特徴の数が少ない場合，検知モデル SVM, KNN において FNR の値が非常に高い結果となることが分かる．今回用いた RAT とその通信データに対しては，特にその傾向が顕著に現れたと考えられる．

全体の分類精度 ACC に関して，全ての検知モデルにおいて提案手法の方が高い精度で検知が行えていることが分かる．また，RF による検知モデルの精度が 96.4%で，一番高い値が得られている．

誤検知率 FPR に関しては，提案手法が全てのモデルにおいて優位な値が得られ，RF による 0.7%が最小となる．

見逃し率 FNR についても，提案手法が優れており，今回の検知モデルとして不適な NB を除けば，DT による 20.0%が最小値である．

また，AUC の値から，提案手法において，検知モデル KNN, DT, RF は良い分類が行えていることが分かる．

提案手法において，最も検知精度が高く FPR が低いモデルは RF であるが，見逃し率 FNR が一番低いのは DT であり，AUC もわずかながら RF に比べて高い値を取っている．RAT の通信検知において，悪性の通信を見逃す場合の方が，正常な通信に対して誤検知する場合に比べてより重大な問題となる．この観点からは，システムで利用する検知モデルとして DT が適切である．

5.2　利用した特徴に対する評価

本手法では，表 3 に示した 8 種類の通信の特徴を利用した．本節では，特にエントロピーが生成された検知モデル，分類精度に重要な貢献をしていることを示す．

決定木学習法において，木構造の上部に存在する質問ほど情報利得が高く，データの分類を行う上で質問

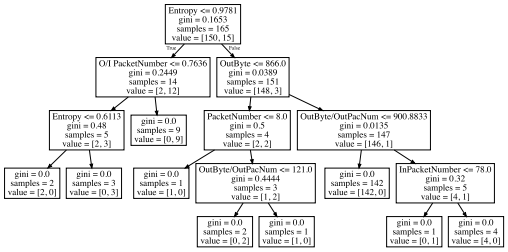

図 5　決定木の構造
Fig. 5　Construction of DT.

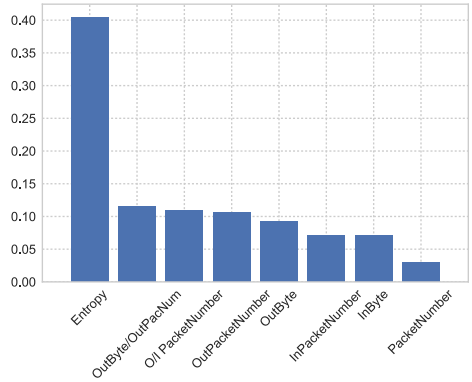

図 6　RF における特徴の重要度
Fig. 6　Feature importances in RF.

として優れている．本研究で用いたサンプルデータに対し，学習された分類器 DT の木構造を表したものが図 5 である．

特徴の一つエントロピー $H(X)$ が木構造の最も上位に位置し，分類に最も大きな影響を与えている事がわかる．次点で OutByte/OutPacNum と OutByte が分類に利用されている．また，エントロピーによる分類が続いていることも確認できる．

更に，検知モデル RF について，同様に今回のサンプルによって学習を行った際の，各特徴の重要度を出力することができる．その結果を図 6 に示す．ランダムアルゴリズムのため，エントロピーを除く特徴の重要度は，分類器の学習結果によってその大小関係が変わるが，エントロピーの重要度は他と一定の差を保ち，安定して大きい．

これらの結果より，本手法において用いた特徴の中で，エントロピーは RAT と通常のアプリケーションの通信を分類するのに最も影響を与え，初期侵入段階から端末制御段階までの RAT の通信の検知に有用であると言える．

表 8　実環境で観測した FPR の比較
Table 8　Comparison of FPR using real network data.

	SVM	NB	KNN	DT	RF
提案手法	0.15	0.66	0.05	0.08	0.01
先行研究	0.28	0.47	0.19	0.23	0.01

更に，分類において悪影響を与える特徴の有無について考察する必要がある．本研究では [4] (Fig. 5) と同様に，全ての特徴の組み合わせに対する精度の比較をそれぞれの分類器に対して行った．また，特徴の組み合わせとして，必ずエントロピーを使用するという制限を与えた場合の結果も確認した．比較的精度の高い DT と RF に対して，必ずエントロピーを使用した場合，特に FNR が安定して低く，全体的に検知精度が高い傾向が見られた．また，比較的精度が低くなる場合のほぼ全ては，エントロピーを特徴として選んでいない場合であった．しかし，本研究で用いたサンプルデータと本実験結果からは，エントロピーを除いた特徴のうち，分類に明らかに悪影響を与えている特徴を特定することはできなかった．

本研究では，Jiang ら [4] が使用した通信特徴にエントロピーを加え，特徴ベクトルの次元が増加しており，検知モデルを生成する計算量も増加している．ただし，上記の実験において，使用する特徴の数が [4] における特徴次元 7 に対応する場合も，使用する特徴にエントロピーを含めた場合は，本提案手法の 8 種の全ての特徴を使用した場合とほぼ同等の検知精度が得られ，[4] の提案手法に対して，本研究で使用したデータに関しては優位性があることを確かめた．

5.3　実環境における正常アプリケーション通信の誤検知率

本節では，本研究で使用したサンプルデータとそれによる検知モデルに対して，実環境のネットワーク通信データにおける誤検知率についての実験結果を述べる．正常なアプリケーションの通信を悪性のものと誤って判断する誤検知の多発は，本研究において提案する RAT 検知システムの実環境での運用に大きな悪影響を与える．テストデータとして使用する正常なアプリケーションの特徴ベクトルは，普段の我々の研究室内で使用するネットワークの通信のパケットデータから抽出を行い，実験に用いた．これらの入力データから FPR の測定を行った結果を表 8 に示す．

表 8 より，k–分割交差検証の結果と同様に，DT と RF の結果が優れており，NB のみ他と比較して値が

高くなっている．先行研究と比較して提案手法は，おおむね良好な値を示している．提案手法では先行研究と比較して，入力が学習に用いられていない未知の通信の特徴ベクトルでも FPR が低く誤検知が少ない．

5.4 考　　察

本節では，検知システムの評価実験において，見逃し率を上げている判別できなかった RAT と，リアルタイム性に注目した検知システムの処理能力について考察を与え，評価のまとめを行う．

5.4.1 判別できなかった RAT

本提案手法において，DT を使用した際，先行研究では検知できなかった RAT を正しく分類している反面，幾つかの別の RAT を検知することができていない．特に，今回用いたデータに対しては，非常に高い確率で Imminent Monitor と Turko jan を検知することができなかった．それは，これらの RAT の使用した特徴ベクトルのエントロピーが，他の RAT のものと比べて高い値を取っており，DT においてはエントロピーの特徴としての重要度が高いため，分類に失敗しているためである．これらの RAT は 3 ウェイハンドシェイクが完了した後も連続した通信が行われており，通信パケットが多く，偏りが発生していなかった．ただし，先行研究の提案手法である，通信の初期段階においたエントロピーを考慮しない特徴ベクトルを用いた場合に検知できなかった RAT を，エントロピーの差を利用することにより検知することができている．

特徴としてエントロピーを利用する際に起こるこれらの見逃しを避けるために，分類器におけるエントロピーの特徴としての重要度を適切に和らげる必要がある．そのためには，一つは決定木以外の弱学習器も取り入れたアンサンブル学習を利用して評価を行うことが挙げられる．また，本研究で定義したエントロピーは今回利用したサンプルデータから最も適切と思われる値 s, t を設定して定めたものだが，複数のパラメータに対するエントロピーを定義し，それぞれのエントロピーを同時に特徴として用いて，より多くの RAT が分類できるか確かめる必要がある．

5.4.2 検知のリアルタイム性

5.3 で述べた正常通信の FPR 測定において，キャプチャしたパケットデータのサイズに対し，提案手法における特徴ベクトルの抽出，DT によるテスト（分類）に掛かる時間の測定を行った．その結果を表 9 に示す．実験におけるそれぞれの計算は，動作周波数が 2.8GHz の Intel Core i7 CPU を用いてシングルスレッドで行った．特徴抽出に掛かる時間は，実際にはその大部分がパケットキャプチャデータからセッション（TCP コネクション）ごとにパケットを整理するところにあり，得られたセッションのデータから特徴ベクトルを計算するコストは小さい．また，分類時間は特徴抽出時間に比べて非常に小さい．実際の検知システムでは，検知モデルは事前にラーニングフェーズにおいて学習が行われ調整されており，リアルタイムに観測したデータの特徴抽出と分類を合わせた計算に掛かる時間が問題となる．表 9 の結果から，DATA1, 2, 3 のサイズはそれぞれ 0.4, 4.7, 45.4MB であり，一秒あたりの平均的な処理量はそれぞれ，5.71, 12.05, 9.50MB/s となる．それぞれのデータは，研究室ネットワークの正常な通信をキャプチャしたものであり，その際の平均的なトラヒック量は 1MB/s から 2MB/s 程度であった．実際に，DATA1, 2, 3 のキャプチャ時間は，それぞれ 0.21, 3.92, 26.01 秒であった．したがって，それぞれのパケットデータによって，TCP セッション数等の差から，特徴抽出の処理性能が異なるが，上記程度のトラヒック量の場合，リアルタイムに特徴抽出・テストデータの分類が行える．リアルタイム検知システムの構築においては，特徴抽出フェーズがボトルネックとならないよう，特徴抽出計算の高速化，並列化等を考える必要がある．

表 9　通信のデータサイズと検知に掛かる計算時間
Table 9　Calculation times to extract feature vectors and classify them for some network data.

通信データ	データサイズ (MB)	特徴抽出時間 (sec)	分類時間 (ms)
DATA1	0.4	0.07	1.32
DATA2	4.7	0.39	1.29
DATA3	45.4	4.78	2.01

5.4.3 評価のまとめ

提案手法に対し，検知モデルとして，ACC, FPR が最良だったモデルは RF であり，FNR は DT が最良であった．また，RF, DT は他の検知モデル評価指標に対しても良好であった．更に，実環境の通信データに対する FPR についても同様の結果であった．以上より，RF と DT が機械学習アルゴリズムにおいて提案手法に適していると考えられる．

検知に用いた特徴において，実験結果よりパケットの偏りを数値化したエントロピーが最も分類に影響していた．DT による検知においては，先行研究に対してより低い FNR を得られることから，エントロピーを特徴として用いることは有用であると言える．また，

その他の指標も全て先行研究の結果より優れている．

エントロピーの特徴の重要度が高いことから，通信の偏りが正常なアプリケーションと似ている，すなわち，エントロピーの値が近い RAT は検知することができなかった．これらに対応するためには，決定木以外の弱学習器も取り入れたアンサンブル学習による検知や，新たな特徴を考える必要がある．

6. むすび

標的型攻撃における RAT の通信検知は初期侵入段階から端末制御段階までに検知を行うことが有効とされている．しかし既存手法では，特定のプロトコルや，挙動に依存し，端末制御段階までに汎用的な検知をすることはできなかった．Jiang ら [4] の研究では検証に用いられたデータが少なく，事前実験で得られた結果より誤検知を非常に生みやすいことが分かった．そこで本研究では，攻撃者が操作を行う前の RAT の通信パケットの偏りをエントロピーを用いて数値化し，新たに特徴として加え，通信の検知実験を行った．評価実験より，エントロピーを特徴として用いることが有用であることが示された．また，RAT の初期侵入段階から端末制御段階までの間で，先行研究より多くの RAT の通信サンプルを用いた上で，より高い検知精度 96.4%を得た．更に，正常な通信の誤検知率 FPR に関しても最小でおよそ 0.7%となり，先行研究の手法による結果より低い値が得られた．RAT の見逃し率 FNR は DT による 20.0%が最小値であり，先行研究と比較して，より低い値となった．

今後の課題として，特に本研究で定義したエントロピーが RAT と正常なアプリケーションとで区別がつかないような通信に対して，適切な分類を可能とするための手法を考える必要がある．特に，RAT が TCP セッションの初期段階に，正常なアプリケーションを模したダミー通信を行う機能をもつ場合は，本提案手法で定義したエントロピーによる通信検知が困難になる．したがって，様々な弱学習器を用いたアンサンブル学習，より大規模なデータを利用したエントロピーのパラメータ調整，新たな特徴の追加，ホストベースの検知手法の検討をすべきである．

また，実際にリアルタイム検知システムの構築を行い，実ネットワーク環境で詳細な性能評価を行う必要がある．

謝辞　本研究を行うにあたり，第一著者は JST, CREST（研究課題番号：JPMJCR14D6）の支援を受けている．

文　献

[1] 特定非営利活動法人日本セキュリティ監査協会，APT による攻撃対策と情報セキュリティ監査研究会 APT 対策入門：新型サイバー攻撃の検知と対応，Next Publishing，株式会社インプレス R&D，2012.

[2] トレンドマイクロ株式会社，“国内標的型サイバー攻撃分析レポート 2016 年版状況と目的に応じて攻撃を変化させる攻撃者，” https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=194. Accessed: 2017-07-27.

[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，第 2015 巻，pp.1387–1393, Oct. 2015.

[4] D. Jiang and K. Omote, “A RAT detection method based on network behavior of the communication’s early stage,” IEICE Trans. Fundamentals, vol.E99-A, no.1, pp.145–153, Jan. 2016. http://search.ieice.org/bin/summary.php?id=e99-a_1_145

[5] McAfee 株式会社，“McAfee 脅威レポート 2016 年第 4 四半期，” https://www.mcafee.com/jp/resources/reports/rp-quarterly-threats-mar-2017.pdf. Accessed: 2017-07-27.

[6] C.I. Fan, H.W. Hsiao, C.H. Chou, and Y.F. Tseng, “Malware detection systems based on api log data mining,” 2015 IEEE 39th Annual Computer Software and Applications Conference, vol.3, pp.255–260, July 2015.

[7] 三村　守，大坪雄平，田中英彦，“HTTP ベースの通信挙動に基づく RAT 検知システムの試作，” コンピュータセキュリティシンポジウム 2016 論文集，第 2016 巻，pp.488–495, Oct. 2016.

[8] D. Adachi and K. Omote, “A host-based detection method of remote access trojan in the early stage,” pp.110–121, Springer International Publishing, Cham, 2016. http://dx.doi.org/10.1007/978-3-319-49151-6_8

[9] 大家政胤，面　和成，“ソフトウェアの通信挙動に基づく Remote Access Trojan の早期検知手法，” The 34th Symposium on Cryptography and Information Security (SCIS 2017), 2017.

[10] 山田正弘，森永正信，海野由紀，鳥居　悟，武仲正彦，“動的解析ログの API を用いた機能に基づくマルウェア分類，” The 31st Symposium on Cryptography and Information Security (SCIS 2014), 2014.

[11] 山内一将，川本淳平，堀　良彰，櫻井幸一，“機械学習を用いたセッション分類による C&C トラフィック抽出，” The 31st Symposium on Cryptography and Information Security (SCIS 2014), 2014.

[12] S. Li, X. Yun, Y. Zhang, J. Xiao, and Y. Wang, “A general framework of trojan communication detection based on network traces,” 2012 IEEE Seventh International Conference on Networking, Architecture, and Storage, pp.49–58, June 2012.

[13] S. Wu, S. Liu, W. Lin, X. Zhao, and S. Chen, “De-

tecting remote access trojans through external control at area network borders," Proc. Symposium on Architectures for Networking and Communications Systems, pp.131–141, ANCS '17, IEEE Press, Piscataway, NJ, USA, 2017. https://doi.org/10.1109/ANCS.2017.27
[14] dpkt, https://dpkt.readthedocs.io/en/latest/
[15] scikitlearn, http://scikit-learn.org/stable/

（平成 29 年 7 月 27 日受付，11 月 5 日再受付，
11 月 27 日早期公開）

石井　将大　（正員）

2009 年広島大学理学部数学科卒業．2011 年名古屋大学多元数理科学研究科修士課程修了．2013 年奈良先端科学技術大学院大学情報科学研究科修士課程修了．2016 年同大学大学院博士後期課程修了．工学博士．2016 年東京工業大学情報理工学院特任助教．2018 年同大学学術国際情報センター助教．暗号の理論と実装に関する研究に従事．情報処理学会会員．

宇野　真純

2015 年九州工業大学情報工学部知能情報工学科卒業．2017 年奈良先端科学技術大学院大学情報科学研究科修士課程修了．ネットワークセキュリティに関する研究に従事．

猪俣　敦夫　（正員）

平成 14 年北陸先端科学技術大学院大学情報科学研究科博士後期課程修了，平成 16 年独立行政法人科学技術振興機構研究員，平成 20 年奈良先端科学技術大学院大学情報科学研究科を経て平成 23 年同総合情報基盤センター准教授，平成 28 年東京電機大学教授，現在に至る．博士（情報科学）．情報セキュリティの研究開発に従事．一般社団法人 JPCERT/CC 理事，一般社団法人公衆無線 LAN 認証管理機構代表理事，情報処理学会，日本セキュリティマネジメント学会，各会員．

新井イスマイル

2002 年明石工業高等専門学校専攻科機械・電子システム工学専攻修了．2008 年奈良先端科学技術大学院情報科学研究科博士課程修了．博士 (工学)．2008 年立命館大学ポスドク研究員，2011 年明石工業高等専門学校助教・講師・准教授を経て，2016 年より奈良先端科学技術大学院大学総合情報基盤センター准教授．屋内測位システム，センサネットワーク，データ解析等，ユビキタスコンピューティングの研究開発に従事．情報処理学会，ACM，IEEE 各会員．

藤川　和利　（正員）

昭和 63 年阪大・基礎工・情報卒．平成 3 年同大学院基礎工学研究科博士後期課程退学後，同年阪大・基礎工・助手等を経て，平成 14 奈良先端大・情報科学センター・助教授，平成 17 年同大・情報科学研究科助教授，平成 23 年同大・情報科学研究科教授，現在に至る．博士（工学）．分散処理システム，マルチメディアシステム，ユビキタスコンピューティングの研究開発に従事．IEEE, ACM 各会員．