ホストベースによる Remote Access Trojan (RAT) の早期検知手法

足立 大地 †　　面 和成 †

† 北陸先端科学技術大学院大学 情報科学研究科
923-1292 石川県能美市旭台 1-1
{d-adachi,omote}@jaist.ac.jp

あらまし 近年，特定の組織を狙う標的型攻撃と呼ばれる攻撃が増加している．標的型攻撃では遠隔操作で組織の機密情報の窃取を行う Remote Access Trojan (RAT) というマルウェアが用いられ，感染を完全に防ぐことは難しいと言われている．そのため，感染後にできるだけ早く検知する出口対策が重要である．RAT の検知手法にはネットワークベースとホストベースがあり，ホストベースの方がより多くの情報を取得できるため検知に有効だと考えられる．しかしながら，既存のホストベース検知手法では RAT を早期に検知できるかどうかが明らかになっていない．本研究では，RAT と正常アプリケーションの通信の目的の違いに着目し，RAT 感染後の初期段階にホスト上で RAT を検知する手法を提案する．提案手法では初期段階の情報のみを用いるため，早期検知が可能となるだけでなく，既存研究よりも処理時間が少なくて済む．

Early Detective Method of Remote Access Trojan by Host Base

Daichi Adachi†　　Kazumasa Omote†

†School of Information Science, Japan Advanced Institute of Science and Technology
1-1, Asahidai, Nomi-shi, Ishikawa, 923-1292, JAPAN
{d-adachi,omote}@jaist.ac.jp

Abstract The attacks called Advanced Persistent Threat (APT) attack targeting a specific organization is increasing. The APT attack uses malware called Remote Access Trojan (RAT) stealing the confidential information of the organization by remote control and it is said that completely preventing infection is difficult. Therefore, the exit measures to detect after infection as soon as possible are important. There are a network-based and a host-based, RAT detection method and the host-based one is effective because it can acquire more information. However, it is not revealed whether you can early detect RAT by the existing host-based detection method. In this paper, we focus on objective difference between RAT and communication of the normal application and propose method early to detect RAT on a host for an initial stage after the RAT infection. The proposal method is not only possible to early detection but also less processing time than existing study because it use only information of the initial stage.

1　はじめに

インターネットの普及に伴いネットワーク犯罪も多様化している．対象となる特定の情報を盗むことを目的とする，サイバー犯罪の一種である標的型攻撃の被害が増加している．標的型攻撃は，特定の組織や企業の機密情報の窃取やシステムの破壊を目的とする攻撃手法である．

標的型攻撃では企業の機密情報や企業が管理している多くの個人情報が狙われるため，被害が甚大である．また，標的型攻撃は機密情報などを窃取することが目的であり，見つからないように行動するため，攻撃を受けていることに気づきにくいという特徴がある [1].

標的型攻撃ではメール，USB メモリ，Web サイトなどの感染経路を通して，脆弱性を突くマルウェアを送り込む．この攻撃に用いられるマルウェアとして, Remote Access Trojan (RAT) がある．RAT とは，リモートアクセス機能を持ち, 遠隔から被害者 PC の監視や操作ができるマルウェアである．標的型攻撃ではセキュリティソフトなどに検知されないような工夫がされているため従来の入り口対策での検知が難しい．現在，標的型攻撃などの入り口対策だけでは防ぎきれない攻撃が増えているため，出口対策が重要になっている．

RAT の検知手法としては, ネットワークベース検知手法とホストベース検知手法がある．ホストベース検知手法の場合, 各端末に RAT の検知ソフトをインストールする必要があるので運用方法などを考慮しなければならないが，ネットワークベース検知手法よりも多くの情報を取得できるので検知に有効である．ホストベース検知手法ではネットワーク情報の他に端末のプロセス情報やプロセスごとの宛先 IP アドレス, コネクション数などの情報を取得できる．よって，本研究ではホストベース検知手法で RAT 感染後の初期段階で検知する手法を提案する．本手法では，初期段階で検知することにより，被害を最小限に抑えることが期待できる．そのため，インシデント対応のための時間も確保でき情報漏洩などのリスクを低減できる．

本稿では，2 章で既存研究について述べ，3 章で準備として RAT および機械学習，交差検定について説明する．4 章では，RAT を検知するための提案手法について述べる．5 章では実験について述べ，6 章で考察を行う．そして，最後に 7 章で本研究のまとめについて述べる．

2 既存研究

RAT 検知に関する研究として，ネットワークベースとホストベースの検知手法がある．ネットワークベース検知手法ではネットワークから得られる情報を用いて検知を行う．ネットワークベース検知手法では組織のネットワーク全体の通信を一カ所で検知できるため管理やコストが容易という利点がある．一方，ホストベース検知手法では，各端末に RAT の検知ソフトをインストールする必要があるが，ネットワーク情報の他にホストの情報も特徴として使えるという利点がある．

ホストベース検知手法の既存研究として [4][7] の研究が挙げられる．ホストベース検知手法としては，主にホスト上で取得できる，プロセス情報（実行 CPU 使用率，メモリ使用率，プロセス実行パス，プロセス ID，API 呼び出し，ネットワーク状況等）を用いる検知手法が提案されている．中里らの研究 [4] では，RAT などマルウェアは未知のプロセスであるため，日常で利用されないプロセスであるという挙動から，普段利用しているプロセスか否かをプロセス情報から判断し，不審なプロセスを特定する手法を提案している．ここでは，プロセス情報からプロセスツリーを作成し，その構造の変化から不審なプロセスを特定する．Yu らの研究 [7] ではネットワーク情報の他にホストから得られる情報として並列コネクション数や宛先 IP アドレス数も用いて RAT の検知を行っている．正常アプリケーションはマルチセッションで通信するが，RAT は主にシングルセッションで通信するという特徴から並列コネクション数や宛先 IP アドレスの特徴を選んでいる．しかし，これらの研究ではどのぐらいの時間で特徴を収集すべきなのかが分からないため，早期に検知できるかが明らかでない．

ネットワークベース検知手法の既存研究としては [2][3] [5][6] が挙げられる．ネットワークベース検知手法としては，RAT と正常アプリケーションの通信特徴の違いに着目して検知を行っている．Li らの研究 [3] では，正常アプリケーションと比べて RAT は Outbound の通信量が Inbound より多いという特徴を用いてい

る．しかし，この研究では通信接続の確立から通信終了/切断までの情報が必要であるため，すでに機密情報が漏洩している可能性がある．山内らの研究 [6] では，正常通信がボットネットのロボット的な通信よりもランダム性があるということから，アクセス回数とアクセス時間の標準偏差の特徴を用いて，HTTP 型ボットネットを検知する手法を提案している．しかし，RAT の攻撃者は人間であるため，ランダム性の違いはあまり見られないと考えられる．この手法では RAT を検知することは難しい．Jiang らの研究 [2] では，ネットワークベース検知手法で接続初期段階という RAT の接続時の通信を用いた検知手法を提案している．山田らの研究 [5] では，内部対策として，攻撃者からの命令と，RAT から別の標的ホストへの攻撃通信，攻撃の結果の通信がそれぞれ連動して発生することに着目して，他のホストへの RAT 拡散や諜報活動等の攻撃検知手法を提案している．

3 準備

3.1 Remote Access Trojan (RAT)

RAT は遠隔操作で情報を窃取するためのマルウェアで，サーバの被害者 PC とクライアントの攻撃者 PC で構成されている．RAT は諜報活動などに使われるため，ファイルのアップロード，キーロガー，画面監視などの機能を持っている．RAT は感染後に RAT 側から攻撃者に対して接続を要求する．接続が確立した後は，攻撃者側から命令の通信を送り RAT とやりとりをする．

3.2 機械学習

機械学習とは，膨大な量のデータから重要なパターンや傾向を抽出し，データがどのような意味を持っているかを解析する手法である．機械学習には，教師あり学習と教師なし学習がある。

教師あり学習はデータとデータを分類するための情報であるラベルを用いて，未知のデータが与えられたときに，対応するラベルを予測して分類するための規則を獲得する学習方法である．教師なし学習はラベルなどの情報は与えられず，データだけが与えられ，データの分布などからデータの特徴的なパターンを見つけ出す学習方法である．

本研究では，RAT であるか正常アプリケーションであるかの教師情報が使えるので，RAT の検知に教師あり学習を用いる．

3.3 交差検定

交差検定は，機械学習によって作成されたモデルの妥当性の検証を行うための手法である．本研究では，K-Fold 交差検定を用いる．K-Fold 交差検定はデータを K 個に分割し，K-1 個を学習データとして用いて，残りの 1 個を検知データとして検知を行う．交差検定の評価指標として，Accuracy (精度)，FPR (誤検知率)，FNR (見逃し率) を用いる．

$$Accuracy = \frac{TrueDetectionNumber}{TotalNumber}$$

$$FRP = \frac{FalseDetectionNumberof'1'}{LegitimateSampleNumber}$$

$$FNR = \frac{FalseDetectionNumberof'0'}{RATSampleNumber}$$

4 提案手法

4.1 目的

標的型攻撃の検知が遅れると情報漏洩の被害が拡大する．したがって，RAT の感染後にできるだけ早く検知することが重要である．早期に検知することで窃取した情報が外部に漏洩する前に対策を行う時間も稼ぐことができ，情報が漏洩するリスクも減らすことができる．

RAT の検知手法として，ネットワークベース検知手法とホストベース検知手法がある．2 種類の検知手法があるが，ホストベース検知手法の方がネットワークベースよりも多くの情報が取得できるので検知に有効であると考えられる．よって，本研究ではホストベースで初期段階の情報を用いて RAT の不正アクセスを検知する手法を提案する．

4.2 初期段階

ここで，初期段階について定義する．

定義１（初期段階 [2]） 初期段階は，$TCP3-way$ ハンドシェイクから始まり，間隔時間が t 秒未満の連続した TCP パケット列である．

RAT の検知で初期段階を用いる理由としては次の通りである．RAT は情報窃取のためのマルウェアであり，目立たないように通信するという特徴がある．この特徴は正常アプリケーションの通信と正反対である．初期段階は RAT と攻撃者の接続を確立するための段階であり，できるだけ無駄な通信をせず必要最小限の通信のみを行うため，正常アプリケーションの通信と反対にデータ量は少なく，初期段階の時間も短い．

以上のような理由から初期段階は RAT 検知に有効だと考えられる．また，初期段階の特徴を用いるため，検知後に対策を施す時間が多く確保できる．

4.3 概要

本手法では，初期段階の情報をホスト上で取得し，その情報を用いて検知を行う．ネットワーク上ではなくホスト上で検知を行う利点として，ネットワーク情報だけでなくホスト情報も用いて検知できることが挙げられる．具体的には，ネットワークから取得できるデータ量やパケット数などだけでなく，ホストのプロセスごと宛先 IP アドレスやポート番号などを取得できる．ホスト情報も用いることでより高い精度で RAT が検知できると考える．

正常アプリケーションはマルチセッションが多いが RAT はシングルセッションの通信を行うため [7]，ホスト上で取得できるプロセス毎の宛先 IP アドレスやコネクション数の特徴が初期段階における RAT 検知にも有効な特徴だと言える．また，これらの特徴とプロセス ID を結びつけることで，RAT のプロセス ID を特定することができる．

4.4 手法の詳細

本手法は，3 つの段階（特徴抽出段階，学習段階，検知段階）で構成されている．

4.4.1 特徴抽出段階

特徴抽出段階ではネットワーク情報やプロセス情報から特徴ベクトルを作成する．特徴ベクトルは 11 次元ベクトルとして作成する（表 1 参照）．

次に図 1 を用いて特徴ベクトルの計算方法を説明する．本手法では DstIP と Conn はプロセス全体で計算し，残りの特徴はセッション毎に計算する．セッションとは，送信元 IP アドレスと宛先 IP アドレスのペアを一つのセッションとする [2][3]．まず，パケットが届くたびにパケットからポート番号を取り出し，取り出したポート番号を使っているプロセス ID を特定する．そして，プロセス ID からアプリケーション名を検索し，パケットとアプリケーション名を関連付ける．次にそのパケットのセッションを特定して，新しいセッションなのか既に通信を行っているセッションなのかを特定する．セッションの特定が終れば，PacNum，OutByte，InByte，OutPac，InPac，DstIP，Conn の値を更新する．パケット間の間隔時間が閾値 t 秒を超えれば，初期段階の終了と判断し，O/Ibyte，O/Ipac，OB/OP，IB/IP を計算する．最後に特徴ベクトルとして用いるセッションを選別する．

特に正常アプリケーションでは，アプリケーションごとに複数のセッションが存在するが，その中で主要なセッションを一つ選び，それを特徴として用いる．RAT はできるだけ目立たないように通信するが正常アプリケーションは目立つような通信が多く，主要なセッションを用いることで RAT との差が明確になると考えられる．主要なセッションとは時間が最も長いセッションである．

4.4.2 学習段階

学習段階では特徴抽出段階で抽出した特徴ベクトルを用いて検知モデルを構築する（図 2 参

表 1: 検知に用いる特徴

特徴	説明
PacNum	合計パケット数
OutByte	Outbound のデータ量
InByte	Inbound のデータ量
OutPac	Outbound のパケット数
InPac	Inbound のパケット
O/Ibyte	Outbound と Inbound のデータ量の比率
O/Ipac	Outbound と Inbound のパケット数の比率
OB/OP	Outbound での一つのパケット平均データ量
IB/IP	Inbound での一つのパケットの平均データ量
DstIP	宛先 IP の数
Conn	コネクションの数

照)．本手法では，教師あり機械学習を用いて正常アプリケーションと RAT の特徴ベクトルを学習させる．学習では特徴ベクトルにラベルを付ける．ラベルは 0 と 1 の二値があり，正常アプリケーションは 0 のラベル，RAT は 1 のラベルを付与する．教師あり機械学習を用いて検知モデルを学習させることによって，対象の通信が正常通信か RAT 通信かを分類することができる．

4.4.3 検知段階

検知段階では検知対象の通信情報から特徴ベクトルを作成し，検知モデルに入力として与える．検知モデルからの出力が 0 の場合，検知対象は正常通信と判断され，出力が 1 の場合，検知対象は RAT 通信であると判断される（図 3 参照)．

5 実験

5.1 目的

本実験では提案手法であるホストベース検知手法で初期段階の情報を用いた RAT の検知の評価を行う．手法の実験評価では機械学習を用いて 5-Fold 交差検定を行い，初期段階が RAT 検知に有効かを検証する．また，初期段階における RAT 検知に有効な特徴を評価する．

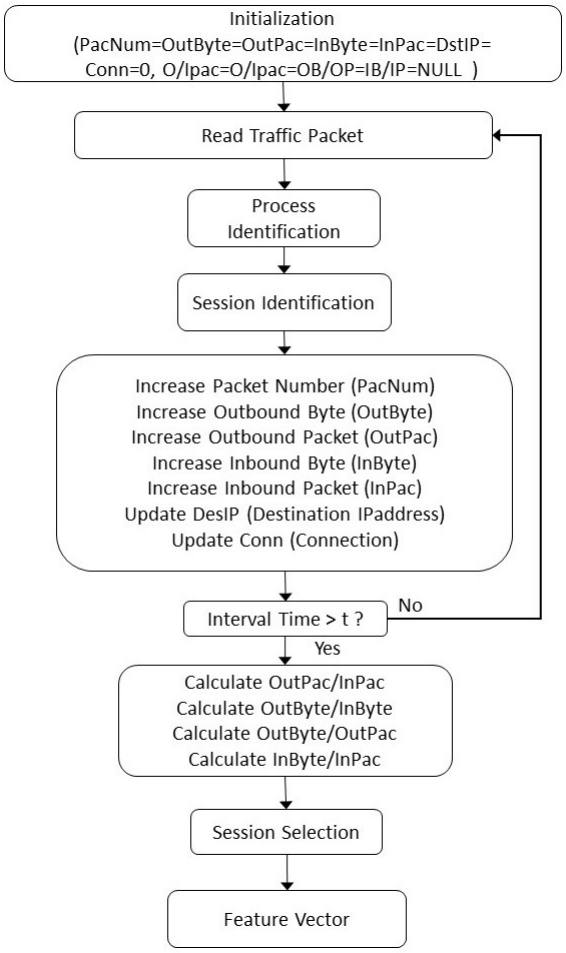

図 1: 特徴抽出段階

5.2 実験データ

本実験では 20 種類の RAT と 12 種類の正常アプリケーションの通信データを用いる．実験に用いる正常アプリケーションは通信形態（push 型 or pull 型)，keep-alive の有無，暗号化の有無の観点から RAT の特徴に似ているものを選んだ．具体的には HTTP，HTTPS，P2P，チャット，クラウドサービスなどのよく使用されているものを選んだ．さらに，RAT は push 型通信を行うので，同じように push 型通信を行うクラウドサービスのアプリケーションも選んだ．push 型通信とはクライアント側からの要求が

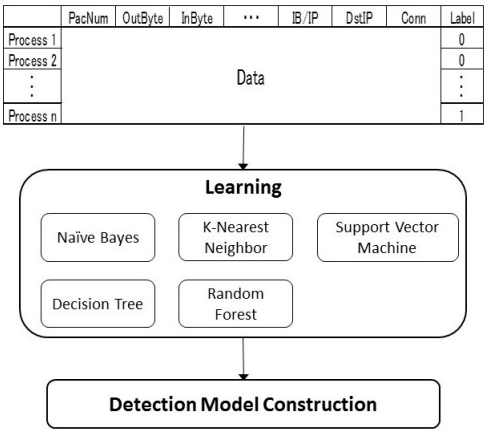

図 2: 学習段階

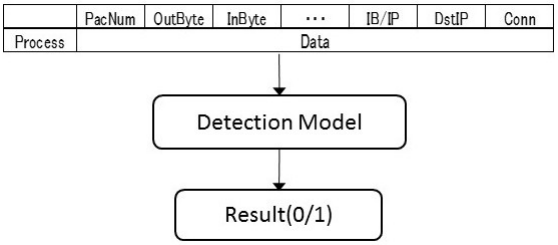

図 3: 検知段階

ない場合でもサーバ側からデータを送信するような通信である．また，RAT と同じような遠隔操作の機能を持っている正常アプリケーションとして Secure Shell (SSH) や Remote Desktop を選んだ．表 2 に実験に使用した RAT を，表 3 に正常アプリケーションを示す．

5.3 手順

5.3.1 前処理

実験の準備として，実験環境について説明する．RAT の通信データは仮想環境上で動作させて収集し，正常アプリケーションの通信データは大学の実ネットワークで動作させて収集した．仮想環境は 2 台の PC を接続することで，攻撃者と感染ホストの環境を構築した．仮想環境は Windows がインストールされた PC で 2 台だけの閉じられたネットワークを使用している．実験に用いる通信データは仮想環境上で RAT を動作させ，その通信を Wireshark でキャプチャして収集した．

収集したデータは，プロセス単位に分割して実験に用いる．通信データからポート番号を使っているプロセス ID を検索し，アプリケーション名と関連付けることによってプロセス単位に分割を行う．プロセスは RAT が 20 プロセス，正常アプリケーションが 12 プロセス，合わせて 32 プロセスのデータを収集した．

表 2: 20 種類の RAT

名称	Push or Pull	Keep-alive	Encryption
Bandook	Push	Yes	Yes
Bozok	Push	Yes	Yes
BX	Push	No	Yes
Cerberus	Push	Yes	Yes
Cyber Gate	Push	No	Yes
DarkNET	Push	No	Yes
Dark Comet	Push	No	Yes
Gh0st	Push	Yes	Yes
LeGeNd	Push	No	Yes
Mega	Push	No	Yes
Netbus	Push	No	No
njRAT	Push	No	Yes
Nuclear	Push	Yes	Yes
OptixPro	Push	No	No
Orion	Push	No	No
PoisonIvy	Push	Yes	Yes
ProRat	Push	No	No
Turkojan	Push	Yes	Yes
ucuL	Push	Yes	Yes
Wi RAT	Push	No	Yes

5.3.2 特徴抽出

特徴抽出では，前処理で準備した RAT と正常アプリケーションのプロセスから提案手法で述べている特徴を抽出する．パケットから特徴を抽出する際，初期段階の時間を決めるために閾値を設定する必要がある．準備実験で閾値を $t = 0.5$, $t = 1$, $t = 2$ として実験を行った結果，閾値が $t = 1$ の時に RAT と正常アプリケーションの特徴の差が大きいことが分かった．よって，

表 3: 12 種類の正常アプリケーション

名称	Push or Pull	Keep-alive	Encryption
BitComet(P2P ダウンロードツール)	Push	Yes	No
BitTorrent(P2P ダウンロードツール)	Push	Yes	No
Chrome(Web ブラウザ)	Pull	Yes	No
Dropbox(クラウドサービス)	Push	Yes	Yes
Firefox(Web ブラウザ)	Pull	Yes	Yes
PPTV(P2P ビデオ共有ツール)	Push	Yes	No
Remote Desktop(遠隔管理ツール)	Push	No	Yes
Skype(IM ツール)	Push	Yes	Yes
Secure Shell(遠隔管理ツール)	Push	No	Yes
Teamviewer(P2P 遠隔管理ツール)	Push	Yes	Yes
TorBrowser(匿名 Web ブラウザ)	Push	Yes	Yes
YahooMessenger(IM ツール)	Push	Yes	Yes

本実験では，初期段階の閾値である間隔時間を $t = 1s$ とする．提案手法で述べたようにプロセスから学習に用いる 11 種類の特徴を抽出して特徴ベクトルを作成する．

5.3.3 交差検定

学習では，特徴抽出で作成した特徴ベクトルを用いる．学習に用いるプログラムは Python の機械学習ライブラリである scikit-learn を用いて実装した．本実験では, 6 つの機械学習の分類器（Support Vector Machine (SVM)，Naive Bayes (NB)，K-nearest neighbor (KNN)，Decision Tree (DT)，Random Forest (RF)）を用いて，11 次元ベクトルの特徴ベクトルを学習させる．

5.3.4 実験結果

本実験では, Python の機械学習ライブラリを用いて交差検定を行う．交差検定は K-Fold 交差検定を用いる．K の値として，K = 5 として交差検定を行う．交差検定では，予測結果を評価するために，Accuracy，FPR，FNR を算出する．

6 種類の機械学習アルゴリズムを用いて，11 種類の特徴のすべての組み合わせである 2047 通りで 5-Fold 交差検定を行った．6 種類の機械学習アルゴリズムで最も平均精度が高かった組み合わせは「DstIP」,「Conn」,「O/Ipac+DstIP」,「O/Ipac+Conn」,「DstIP+Conn」,「O/Ipac+DstIP+Conn」である．6 種類のアルゴリズムで最も平均精度が高かった組み合わせの結果を表 4 に示す．その中で SVC と NB の精度が Accuracy=0.967，FPR=0.100，FNR=0.000 と一番精度が良かった．また，全体的に FNR が低く，誤検知が少ないという結果になった．精度の良かった組み合わせには DstIP や Conn の特徴が共通して含まれている．実験結果から DstIP や Conn の特徴が早期段階での RAT 検知に有効であることが分かった．

表 4: 平均精度が最良となった結果

name	Accuracy	FPR	FNR
NB	0.967	0.100	0.000
RF	0.933	0.200	0.000
LSVC	0.933	0.200	0.000
DT	0.933	0.200	0.000
SVC	0.967	0.100	0.000
KNN	0.933	0.200	0.000

6 考察

6.1 特徴について

実験結果より, 正常アプリケーションはマルチセッションでコネクションも複数使うが，RAT はシングルセッションでコネクションも少ないという傾向が明らかになった．本研究では，正常アプリケーションの特徴はアプリケーションごとに複数のセッションの中で主要なセッションを一つ選び，それを特徴として用いている．主要なセッションのみを用いることで, RAT と正常アプリケーションの特徴の差がはっきりと判別できると考えられる．したがって，DstIP や Conn の特徴が RAT 検知に有効な特徴だと言える．

6.2 誤検知について

FPR として誤検知した正常通信は ssh とリモートデスクトップである．この 2 つのアプリケーションはパケット数, セッション数, コネクション数などの特徴が RAT の特徴と似ているため誤検知したと考えられる．ssh は DstIP や Conn が RAT の特徴に近い．リモートデスクトップは DstIP と Conn 以外の特徴が RAT の特徴に近い．ssh やリモートデスクトップは遠隔操作で PC を操作するためのアプリケーションであり，RAT と機能的には同じことを行うために特徴も類似していると考えられる．しかし，FNR は 0 に抑えることができた．

RAT の初期段階の特徴として，セッション数とコネクション数は 1 つであり，正常アプリケーションでは多くののアプリケーションが複数セッション，複数コネクションなので RAT と正常アプリケーションを区別するための有力な特徴であると考えられる．

7 まとめ

本研究では, RAT を早期に検知するためにホストベース検知手法で初期段階の特徴を用いた検知手法を提案した．実験は，6 種類の機械学習アルゴリズムを用いて行った．実験の結果，93.3%以上の検知精度が得られた．また，FNR も低く抑えることができた．実験結果より，早期段階での検知が有効であることが示された．

正常アプリケーションではセッションやコネクションが複数生成されるが, RAT ではシングルセッションで, コネクションも初期段階に限定すれば一つしか生成されていないことが分かった．したがって，セッション数やコネクション数が特徴として適していると考えられる．今後の課題としては，FPR の値が高いため，FPR を下げる工夫が必要になる．

参考文献

[1] IPA 情報処理推進機構, ”2015 年版 情報処理セキュリティ 10 大脅威”, 2015

[2] D. Jiang and K. Omote, ”An Aproach to Detect Remote Access Trojan in Early Stage of Communication”, Advanced Information Networking and Applications (AINA), 2015.

[3] S. Li, X. Yun, Y. Zhang, J. Xiao and Y. Wang, ”A General Framework of Trojan Communication Detection Based on Network Traces”, IEEE 7th International Conference on Networking, Architecture, and Storage (NAS), 2012.

[4] 中里純二, 津田侑, 高木彌一郎, 衛藤将史, 井上大介, 中尾康二, ”ホスト型 IDS を用いた不審プロセスの特定” The 32nd Symposium on Cryptography and Information Security (SCIS), 2015.

[5] 山田正弘, 森永正信, 海野由紀, 鳥居悟, ”組織内ネットワークにおける標的型攻撃の振る舞い検知に向けた複数センサ連携手法”, The 32nd Symposium on Cryptography and Information Security (SCIS), 2015.

[6] K. Yamauchi, J. Kawamoto, Y. Hori, K. Sakurai, ”Extracting C&C Traffic by Session Classification Using Machine Learning”, The 7th Workshop among Asian Information Security Labs (WAIS), 2014.

[7] L. Yu, P. Guojun, Z. Huanguo and W. Ying, ”An Unknown Trojan Detection Method Based on Software Network Behavior”, Wuhan University Journal of Natural Sciences, 2013.