# RAT 通信監視手法の提案

鳥居 悟† 清水 聡‡ 森永 正信†

†株式会社富士通研究所
211-8588 川崎市中原区上小田中 4-1-1
{torii.satoru, morinaga}@jp.fujitsu.com

‡株式会社富士通ソーシアルサイエンスラボラトリ
211-0063 川崎市中原区小杉町 1-403 武蔵小杉タワープレイス
shimizu_satoru@jp.fujitsu.com

**あらまし** 近年のサイバー攻撃は，その手口が巧妙になってきている．例えば組織内に侵入した後のマルウェアの挙動において，外部サーバと通信路を確立する新しいタイプのトロイの木馬（RAT）が出始めている．プロキシのログでは，このような通信を特定する有効な情報が不足しており，業務アプリケーション通信をマルウェアのものと誤検知してしまうという問題がある．本稿では，このような誤検知を解決する手法を提案する．本方式は，プロキシを経由して外部と通信を行う組織内ネットワークにおいて，従来のようなプロキシのログを用いず，通信セッションの特徴に着目することで，通信要求元のアプリケーションを識別することが可能である．

# Extrusion Detection for Remote Access Trojan

Satoru TORII† Satoru SHIMIZU‡ Masanobu MORINAGA†

†FUJITSU LABORATORIES LTD.
1-1 Kamikodanaka 4-chome, Nakahara-ku, Kawasaki 211-8588, JAPAN
{torii.satoru, morinaga}@fujitsu.com
‡FUJITSU SOCIAL SCIENCE LABORATORY LIMITED
1-403 Kosugi-cho, Nakahara-ku, Kawasaki 211-0063, JAPAN
shimizu_satoru@jp.fujitsu.com

**Abstract** Recently, a crafty cyber attack becomes common. The intruded malware has set up communication path to the external C&C server. The number of the incident by such a malware, Remote Access Trojan (RAT), has increased. However, it is difficult to identify such a communication. Because, RAT speaks with crafty manner, so the proxy would not record the information to specify such a communication. There is a problem to misunderstand the business communication as the malware communication. In this paper, we propose the detection technique for solving such a false negative. Our method identifies the communicated application by analyzing network captured data at the edge of network. By paying attention to the feature of the communication session, we can pick a malicious message up where the business messages exist together.

# 1　はじめに

近年のサイバー攻撃は，その手口が巧妙になってきている．組織内に侵入した後のマルウェアの挙動において，外部サーバと通信路を確立する新しいタイプのトロイの木馬(RAT: Remote Access Trojan)が複数発見されており，これらによる被害事例も増加傾向といえる．一方で，新種の RAT を検知する有効な手段がまだ確立されていない状況である．

本論文では，このような検知が困難な新種の RAT が組織内ネットワークに侵入していないかどうかを監視する手法を提案する．本手法は，すでに試作した HTTP トンネリング通信検知システムをベースとして，RAT 通信も特定可能となるように機能拡張したものである．本稿で提案する監視手法は，組織内ネットワークを管理するセキュリティ管理者にとって，内部に RAT に感染した計算機がないかどうかを確認するひとつの有効な手段になりうると我々は考えている．

本稿では，2 章で新種の RAT がどのようなものであるかを整理し，3 章でその通信挙動の特徴を明らかにすると共に，実環境での特定に向けた実現可能性を検討する．4 章で提案する監視手法について述べ，すでに提案した HTTP トンネリング通信検知システムと共に，実現に向けた機能拡張について述べる．5 章で RAT 通信の監視に関する実証実験とその結果について述べる．6 章で現状の検知手法とその課題を整理し，最後にまとめと今後の課題について述べる．

# 2　RAT とは

RAT とは，Remote Access Trojan もしくは Remote Administration Tool と呼ばれるマルウェアのことである[1]．感染した PC に対して，遠隔から様々な操作をすることが可能なトロイの木馬プログラムである．近年，RAT による様々な被害事例が報告されている[2][3][4][5].

侵入したシステムを遠隔から操作できる RAT の脅威は，すでに 2002 年に BackOrifice の脅威として公開されている[6]．この頃と比べて最近の RAT は，組織内の侵入した計算機からファイアウォールを通過して外部の制御サーバと通信を行う機能を備えている[7][8]．これにより，被害事例の報告が増えたものと考えられる．さらには，特定の OS に限定されないマルチプラットフォームに対応するものも現れている[9].

このような状況の下，RAT の脅威は今後さらに増大するものと考えられる．すでに組織内ネットワークに感染した計算機が存在していてもおかしくない状況といえる．組織内ネットワークを管理するセキュリティ管理者にとって，内部に RAT に感染した計算機がないかどうかを確認することが必要であり，そのための手段が求められている．

# 3　フィージビリティスタディ

組織内に RAT に感染した計算機がないかどうかを確認する監視技術の確立を目指し，RAT に感染した計算機が行う通信の挙動の特徴を明らかにすると共に，得られた特徴が実環境での検知に有効であるかどうかを見極めることとした．

調査検討にあたり，実在する RAT を入手して行うこととした．一般的な組織内ネットワークにはファイアウォールが設置され，外部サーバとのアクセスは proxy を経由して行われることが多いと想定し，対象とする RAT として，ファイアウォールを通過する機能を供えているものを候補とした．その結果，proxy を経由する機能を持ち，誰でも入手が容易な Poison Ivy[7]を用いることとした．

## 3.1 実験室内での挙動解析

実験室内に閉じたネットワーク環境を用意し，proxy やファイアウォールを配置して，組織内ネットワークを模した仮想的な環境を構築した．ファイアウォールの内側に Poison Ivy に感染された PC を配置し，ファイアウォールの外側に制御サーバを配置し，どのような通信が発生するかを観測した（図 1）．

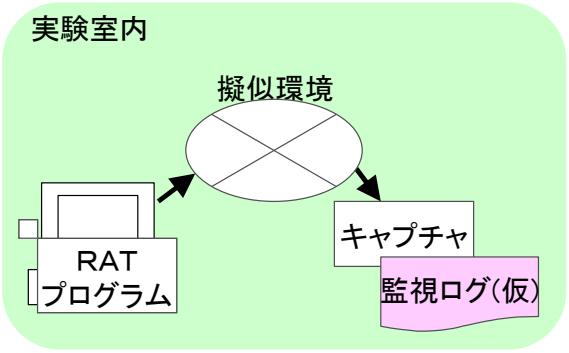


**図 1: 閉じたネットワークの実験環境**

観測の結果，情報処理推進機構(IPA)による調査資料[10]と同様の特徴を観測することができた．具体的には，以下の通りである．

- CONNECT 先 URL に接続先ディレクトリがなく，「IP アドレス:ポート番号」のみ
- User-Agent ヘッダは見つからず
- サーバ・クライアント間で交互に 48byte のペイロードを送信しあう
- 送信ペイロードの内容はサーバ・クライアントでは異なるが，それぞれ毎回同じ

## 3.2 実環境での通信観測

次に，実験室内での観測で得られた Poison Ivy 通信の特徴が，実環境での検知に有効であるか検証した．具体的には，実際の組織内ネットワークにおけるインターネットとの境界点で，どのような通信が発生するかを 1 日間（6 時～24 時）観測した（図 2）．

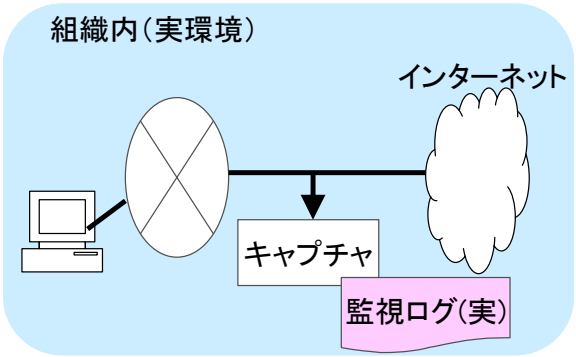


**図 2: 実環境での監視環境**

### 3.2.1 CONNECT メソッド

Poison Ivy が行う通信の特徴のひとつに，接続先ディレクトリ名が明記されずに「CONNECT <IP アドレス>:<ポート番号>」と指定する通信リクエストが発行される，というものがある．そこで，取得した監視ログを分析し，このようなリクエストがどの程度存在するかを調査した．

その結果，画像を含むすべての通信リクエストのなかで 1.2%のものが，このような，ディレクトリ名を明記しないものであった．

これらの通信リクエストは，Skype，メッセンジャー，SSL-VPN などのアプリケーションが行うものであった．また，ポート番号 443 を指定するものが大部分ではあるものの，それ以外のポート番号を指定する通信も見つかった．

### 3.2.2 User-Agent ヘッダ

得られた特徴に，「User-Agent ヘッダが明記されていない」というものもある．そこで，取得した監視ログを分析し，このようなリクエストがどの程度存在するかを調査した．

その結果，画像を含むすべての通信リクエストのなかで 0.097%のものが，User-Agent 情報を取得できない通信であった．但し，これらのなかには User-Agent ヘッダはあるもののその値が空白であるものも含まれている．

User-Agent の値を変更できる Web ブラウザや，外部と通信を行うアプリケーションなどが，このような通信リクエストを発行しているものと

思われる.

### 3.2.3 実環境の観測結果のまとめ

これらの観測結果から，Poison Ivy が行う通信の特徴である，CONNECT 先 URL に接続先ディレクトリ名が明記されていない通信，および，User-Agent 情報が取得できない通信が，定常的に発生していることが明らかになった．外部に接続する業務アプリケーションなどがこのような通信を行っているものと思われる.

すなわち， proxy ログなどから容易に取得可能なこれらの特徴だけでは，誤検知する恐れがあることが明らかになった．言い換えると，RAT が使用している通信メッセージは，定常的に行われている業務アプリケーションが使用するものと同様のものであると考えられる．業務アプリケーションを RAT と誤検知しないような，新たな監視手段を構築することが必要である.

## 4 RAT 通信の監視手法

近年の RAT は，内部から通信リクエストを発行し，リモートから操作を行うための通信路を維持するという特徴を持つ．この点に着目した新たな監視手段の実現について述べる.

## 4.1 監視手法の考え方

初期の RAT は PC を乗っ取った後に，その PC の通信ポートを開放し，外部からはこの通信ポートにアクセスして乗っ取った PC の制御を行う．一方，近年の RAT は乗っ取った PC から外部の制御サーバに通信リクエストを発行し，双方向にデータがやり取りできる通信路を確立する．これにより，ファイアウォールに守られた組織内ネットワークの内部の踏み台 PC に対して外部から制御が可能となる．さらに，確立した通信路を維持するために，外部の制御サーバと内部の踏み台 PC との間で，定期的にデータのやり取り（keep-alive 通信）を行う.

我々は，双方向通信が可能な通信路を内部から確立すること，定期的に keep-alive 通信を行うことの二点に着目する．このような通信に着目して監視することで，内部に RAT に感染した計算機がないかどうかを見極めることが可能と考える．この特徴は，Poison Ivy に限定されるものでなく，ファイアウォールを通過して外部の制御サーバと通信路を構築する機能を有する，近年の多くの RAT に共通するものと考えられる

### 4.1.1 持続的通信路の監視

proxy を経由して外部サーバと通信を行う場合，HTTP 1.1 から規定された CONNECT メソッドを用いることで，持続的な通信路を構築することが可能である[11].

そこで，CONNECT メソッドが指定された通信リクエストを監視対象として収集する.

### 4.1.2 Keep-Alive 通信の監視

フィージビリティスタディで明らかになったとおり，Poison Ivy の場合には，IP ヘッダを除く 48byte の通信パケットが繰り返し送受信される．この通信が keep-alive 通信と見受けられる．この通信ペイロードは，外向きと内向きとでは異なるが，それぞれ毎回同じ内容である.

そこで，同一サイズの通信パケットが繰り返し送受信され，それぞれの内容が毎回同じである場合，RAT による通信の可能性が高いと判断する.

## 4.2 監視手法の試作

CONNECT メソッドを用いて確立された持続的通信路を監視対象とし，この通信路において送受信される keep-alive 通信の特徴を抽出することで RAT 通信を監視するシステム（RAT 通信監視システム）を試作した.

### 4.2.1 HTTP トンネリング通信検知

我々はすでに，ネットワークの挙動を監視

することで，HTTP プロトコルを使用した VPN やファイル共有を行う通信，すなわち，不適切な HTTP トンネリング通信を検出する手法を提案・試作している[12].

先に試作した HTTP トンネリング通信検知システムは，ネットワークを監視し，観測された通信データを解析することで，トンネリング通信を行うアプリケーションの特定とその特徴（パケット数やバイト列など）を抽出することが可能なものである.

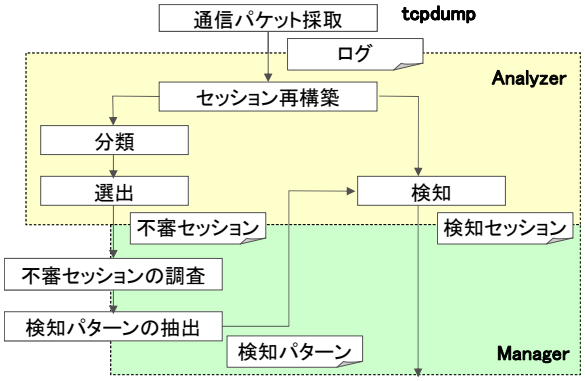


**図 3: 検知システムのシステム構成図**

具体的には，図 3 に示すシステム構成となっている. tcpdump で取得した通信パケットを入力とし，通信セッションを再構築し，CONNECT ヘッダが含まれているものを抽出する. 抽出されたセッション内容を解析し，User-Agent，SSL プロトコルとの整合性，アクセス先 URL，SSL 暗号化方式，SSL 証明書，などの情報を取得する. これらの得られた情報を元に分類し不振なセッションを抽出する. アプリケーションを特定する特徴的なキーワードやパターンが抽出できた場合には，検知用のパターンに登録することも可能である.

### 4.2.2 RAT 監視機能の追加

この HTTP トンネリング通信検知システムをベースに，RAT 通信も特定可能とすべく，繰り返し現れるバイナリ列と同じバイト数を抽出し、それを可視化する機能を追加した.

すなわち，RAT のような特徴を持つ通信セッションの特定が容易となるよう，繰り返し現れるバイナリ列，および，同じバイト数のパケットが出現する部分を抽出し，表示方法に視覚的な変化を加えた.

具体的には図 4 に示すように，抽出した不審セッションの内容表示において，繰り返し現れるバイナリ列を赤地の白抜きで，同じバイト数のパケットにはそのパケット数を青地の白抜きで表示される.

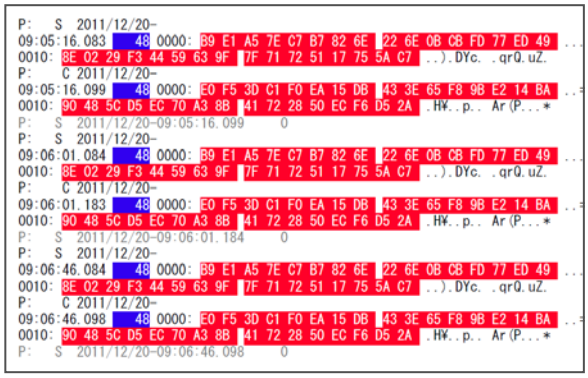


**図 4: 通信セッション内の可視化（Poison Ivy）**

## 5 試行実験

試作した RAT 通信監視システムを用いて，RAT 通信が特定であるかどうか，前述のフィージビリティで用いた環境で評価実験を行った.

### 5.1 実験室内での検知実験

組織内ネットワークを模した仮想的な環境に RAT 通信監視システムを設置し，RAT に感染した PC と制御サーバとの間で通信を発生させ，当該通信が抽出可能かどうかを実験した.

図 4 に示した内容は，この検知実験で得られたものである. RAT 感染 PC と制御サーバとの間で交互に 48byte のペイロードを送信しあう様子が，多数の青地に白抜きの部分として確認できた. また，送信ペイロードの内容がサーバ・クライアントでは異なるがそれぞれ毎回同じである様子が，多数の赤地に白抜きの部分として確認できた.

これらの結果から，RAT 通信監視システム

は，Poison Ivy が行う通信を捕捉することが可能とみなすことができる.

## 5.2 実環境での試行実験

さらに，実在する組織内ネットワークとインターネットとの境界点に RAT 通信監視システムを設置し，25 日間の試験運用を行った.

監視システムは，試験運用期間中に安定して稼動し続けたが，RAT と思われる通信は抽出されなかった. 少なくとも，業務アプリケーションによる通信を RAT によるものと誤検出することがなく，また，当該組織内に RAT に感染している計算機が存在していないと仮定すれば，正しい動作結果であったとみなすことが出来る.

### 5.2.1 Keep-Alive 通信の状況

RAT 通信の特定精度を見極めるため，試験運用中の通信履歴を精査し，RAT 通信と類似した通信が存在しないかどうか調査した. 具体的には，通信の特徴のひとつである 48byte のペイロードを持つパケットが大量に送受信される通信セッションを抽出しその内容を精査した.

その結果，通信セッション中に 48byte のペイロードを持つパケットを 10 回以上行うものが，試験運用期間中(25 日間)に 180 回存在していた. さらに当該セッションの内容を精査したところ，以下のような状況であった.

- SSH トンネリング通信と思われるものが，35 個見つかった
- SIP トンネリング通信と思われるものが，3 個見つかった
- 残りのものには，特徴的なキーワードが含まれていなかったため，アプリケーションの特定は出来なかった
- RAT 通信に類似した毎回同じ内容のパケットを送信するものは見つからなかった

すなわち，48byte のペイロードを持つパケットを大量に送信するという観点だけでは，RAT 通信を特定するには問題が生じる可能性があると言える. RAT による keep-alive 通信と一部の SSH アプリケーションや SIP アプリケーションによる keep-alive 通信と区別できることが必要であり，そのひとつの判断として毎回同じ内容のパケットを送信するかどうかという観点が有効であると言える.

### 5.2.2 RAT 通信監視システムの効果

試験運用を通じて，以下のような特徴を持つ不審な通信を抽出することが可能であることが分かった. HTTP トンネリング通信検知システムが有する機能によるものが大きいが，組織内ネットワークにおけるコンプライアンスの遵守状況の監視にも有効であるといえる.

- 仕様違反の通信（プロトコルの偽装）
- User-Agent の偽装
- 不自然な SSL ネゴシエーション
- 送受信パケットの大きさ，頻度，ビットパターン
- IP アドレス直打ちの通信
- SSL-Proxy 通過だけを目的にした通信
- オレオレ証明書サイト

## 5.3 試行実験のまとめ

試作した RAT 通信監視システムを用いた試行実験で得られた結果を以下に整理する.

実験室内の仮想的なネットワーク環境において，RAT 通信を捕捉することができた. 実環境においては，RAT 通信を抽出することができなかったが，これは当該ネットワーク内に RAT に感染した計算機が存在していなかったと想定すれば，正しい結果であったとみなすことができる.

実環境の通信履歴から，48byte のペイロードを持つパケットを送信しあうことは，一部の SSH アプリケーションや SIP アプリケーションにおいて，keep-alive 用に使用されている可能性があることが分かった. すなわち，特定サイズの通信パケットの出現頻度だけではなく，RAT の挙動解析で得られた毎回同じ内容のパ

ケットを送信するという観点で判断し識別することが必要であることが明らかになった.

## 6 現状の検知手法

RAT が備えているリモート制御機能は，適切に統制された使い方であれば，有効に活用することが可能である. そのために，一部のアンチウィルスソフトのみが RAT を検知する. RAT に有効活用の余地があるため，引き続き，すべてのアンチウィルスソフトが検知パターンを用意するとは限らないと思われる.

RAT やトロイの木馬に感染した PC を特定する検知手法として，これらのマルウェアが開放するポートの状況を監視する方法が提案されている. しかしながら，この検知手法は，制御サーバからの通信を受信する旧来型の RAT には有効であるが，近年型の RAT 側から制御サーバへ通信を発信するものには有効ではない. RAT 側からの発信を契機として確立された通信路を特定する手法が求められる.

一部の侵入検知ツール(IDS)において，RAT の通信ペイロードをパターンとするシグネチャが用意されている. しかしながら，すでに数十種類の RAT の存在が確認されており，また，通信ペイロードは RAT に少し手を加えるだけで変更することが容易である. これらを踏まえて，それぞれの RAT 毎にそれぞれの通信ペイロードをパターンとして用意することは，非常に高コストになると思われる. 我々が提案する監視手法は，近年の RAT に共通するふるまいに着目するものであり，個々の RAT 毎にパターンを用意する必要性は低い手法である.

悪意の制御サーバのリストを用意し，RAT 側からそれらへの通信を監視制御する方法が提案されている. この手法は，複数の BOT マルウェアを一括制御する形態では有効であるが，個別に RAT を制御するような形態では制御サーバの情報を入手することは困難である. また，制御サーバのドメイン名は動的に変化させることが可能であり，ブラックリストが用意されたときには，すでに当該制御サーバが存在していない可能性もある. このようなブラックリストによらない監視制御の手法が求められる. 我々が提案する監視手法は，通信セッションが継続されている点に着目しており，ブラックリストによらない監視制御のひとつの手法であると言える.

IPA が提唱する出口対策[14]として，proxy ログ監視等が提案されている. 本研究と方向性を同じとするものではあるものの，これらの実現可能性については本論文で議論した通りである. 本研究で試作した RAT 通信監視システムは，出口対策を実現するひとつの手段に位置づけられると我々は考えている.

## 7 まとめ

本論文では，Poison Ivy を例にして，双方向通信が可能な通信路を内部から確立すること，定期的に keep-alive 通信を行うことの二点に着目した監視手法が，RAT 通信監視に有効であることを明らかにした. proxy を経由する機能を有する RAT は他にも複数確認されており，今後はこれらの通信挙動の特徴を明らかにすると共に. 提案監視手法の品質を向上していく予定である.

今回の試行で用いた実環境においては，CONNECT メソッドや User-Agent ヘッダに関して，RAT の通信に類似するものが確認された. これは，様々な業務アプリケーションが外部ネットワークとの通信機能を備え始めているためであると言える. 一方で，業務アプリケーションの利用を統制する組織もあると考えられる. 様々な組織内ネットワークを対象として，どのような通信傾向が見られるかを明らかにする必要がある.

本研究では，keep-alive 通信で繰り返し送受信される通信パケットの内容に着目した. 踏み台 PC と制御サーバとの間で交互に送信される通信のタイミングに着目することも有効であると考えられる. このような特徴の抽出が容易となるように，通信セッションにおける送受信が行われるタイミングを可視化する手段を提供することも有効と考えられる.

組織内ネットワークを管理するセキュリティ管理者にとっては，内部に RAT に感染した計算機がないかどうかを確認することが急務である．本研究で提案する監視手法は，この確認作業に対するひとつの有効な手段になりうると我々は考えている．

## 参考文献


[1] “What is RAT (remote access Trojan)?” Definition from WatIs.com
http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan
[2] Dmitri Alperovitch, “Operation Shady RAT の全貌,” McAfee white paper
[3] “Tracking GhostNet：Investigating a Cyber Espionage Network,” Information Warfare Monitor, JR02-2009
[4] “Anatomy of an Attack,” RSA 公式ブログ
http://blogs.rsa.com/rivner/anatomy-of-an-attack/
[5] “Computer spyware is newest weapon in Syrian conflict,” CNN.com
http://edition.cnn.com/2012/02/17/tech/web/computer-virus-syria/
[6] “Danger: Remote Access Trojans,” Microsoft Technet
http://technet.microsoft.com/en-us/library/dd632947.aspx
[7] Poison Ivy
http://www.poisonivy-rat.com/
[8] Xtreme RAT
https://sites.google.com/site/nxtremerat/
[9] "NetWire first Multi-platform RAT,”
http://www.xylibox.com/2012/07/netwire-first-multi-platform-rat.html
[10] “「新しいタイプの攻撃」の対策に向けた設計・運用ガイド（改訂第 2 版,” 情報処理推進機構, 2011 年 11 月
[11] Fielding, et al., “RFC2616 - Hypertext Transfer Protocol -- HTTP/1.1,” June 1999
[12] 鳥居悟，他 “不適切な HTTP トンネリング通信を検出する手法の提案,” 情報処理学会研究報告 2009-CSEC-46(15)