長期間観測した通信データを用いた サイバー攻撃活動と推定されるプログラムの分類による 攻撃者像の一考察

鮫島 礼佳[1]　芦野 佑樹[1]　須尭 一志[1]　矢野 由紀子[1]　中村 康弘[2]

概要：近年，サイバー攻撃対策技術を回避するために，サイバー攻撃前後で被害端末の通信や振る舞いに急激な変化を発生させず，長期間にわたって慎重に攻撃を行っているサイバー攻撃や調査活動が存在する．このようなサイバー攻撃や調査活動は，サイバー攻撃の直前直後といった変化のある部分のみを分析するのではなく，長期間観測したデータを分析する必要があるといえる．また，サイバー攻撃はインターネットプロトコルの性質上必ず通信データが発生することから，送信者が送信者の意図通りの挙動をするプログラムを必ず使用しているといえる．

そこで，本論文では，長期間観測した通信データを分析し送信者が使用しているプログラムを分類することで，サイバー攻撃または調査活動目的と思われる通信を見つける手法を提案する．併せて，実際に筆者らがサイバー空間上に設置したセンサーで長期間観測した通信データを用いて提案手法の評価を行い，評価の結果作成されたプログラムの分類から攻撃者像に関する考察を行う．

キーワード：通信データ分析，サイバー攻撃，センサー，攻撃者像

A Study of Attacker's Image Based on Classification of Programs Presumed Cyber Attack Used Packet Data Observed Long Term

Samejima Ayaka[1]　Ashino Yuki[1]　Sugyo Kazushi[1]　Yano Yukiko[1]　Nakamura Yasuhiro[2]

Abstract: I suggested the analysis method of the communication data for the purpose of finding a cyber attack and the research activity that I attacked slowly for a long term without letting communication and the behavior of the damage terminal produce a sudden change in approximately a cyber attack in late years to evade the cyber attack measures technology that became mainstream in this article. It suggested technique to classify the programs that a sender used from communication data that a sender used the program that behaved according to intention of the sender by all means in that communication data existed. At the same time, using the analysis technique that I suggested, I classified programs from communication data by analyzing the communication data which I observed with the sensor which the writers installed on Cyberspace and showed the effectiveness of the suggestion technique. Furthermore, I report it because I considered the assailant image using the program from the communication data which I classified.

Keywords: Communication Data Analysis, Cyber Attack, Sensor, Image of Attacker

1. はじめに

近年，インターネットを経由したサイバー攻撃は日々

[1] 日本電気株式会社　ナショナルセキュリティ・ソリューション事業部　サイバーセキュリティ・ファクトリ
Cyber Security Factory, National Security Solution Division, NEC Corporation
[2] 防衛大学校　情報工学科
Computer Science, National Defense Academy

増加しており，その被害と危険性は社会問題となっている [1]．近年のサイバー攻撃対策技術として，サイバー攻撃を受けた際に，検知やフィルタリングといった対策を行う技術がある．しかし，この対策技術はサイバー攻撃を受けた際に発動するため，サイバー攻撃を受けた前後で，被害端末の通信や振る舞いに急激な変化が発生しない攻撃や調査活動の場合，もしくは過去に観測されず分析されていない攻撃手法が用いられた場合において，攻撃と識別し対策を行うことは困難であるといわれている [2], [5]．そこで，筆者らは，このような攻撃活動や調査活動を見つけるためには，サイバー攻撃の直前直後といった変化のある部分のみを分析するのではなく，長期間観測したデータを分析する必要があるのではないかと考えた．

長期間観測したデータを分析するにあたって，インターネットを経由したサイバー攻撃は必ず通信データが発生する [8] ことから，本研究では長期間観測した通信データを扱う．また，通信データが発生する際には，必ず送信者が，送信者の意図通りの挙動をするプログラムを使用している [9] ことから，本研究では，長期間観測した通信データを分析することで，送信者が使用しているプログラムを分類し，対策困難とされる攻撃活動や調査活動を見つけることを目的とする．以上のことより，本研究では，長期間観測した通信データを分析し送信者が使用しているプログラムを分類することで，サイバー攻撃または調査活動目的と思われる通信を見つける手法を提案する．併せて，実際に筆者らがサイバー空間上に設置したセンサーで長期間観測した通信データを用いて提案手法の評価を行い，評価の結果作成されたプログラムの分類から攻撃者像に関する考察を行う．

本論文の構成は以下のようになっている．2 章では関連研究を元に本研究で行う分析の方針について検討し，3 章で本研究の位置付けを述べる．4 章では攻撃活動や調査活動を見つけることを目的として，長期間観測した通信データからプログラムを分類する手法を提案し，5 章で提案手法の評価を行う．6 章では，評価実験の結果から通信データの分析により分類できたプログラムと攻撃者像について考察し，7 章で本論文全体についてまとめる．

2. 関連研究

インターネットを経由して行われるサイバー攻撃は，インターネットプロトコルに則る必要があることから，インターネットプロトコルの性質上，必ず通信データが発生する [8]．このことから，インターネットを経由して行われるサイバー攻撃を見つけるためには，通信データの分析が必要不可欠であると考える．そこで，本研究では，サイバー攻撃の攻撃活動や事前調査活動を見つけることを目的としていることから，分析対象として，通信データを扱う．

本章では，サイバー攻撃を見つける観点で通信データを分析している関連研究について述べ，本研究で行う分析の方針について検討する．

2.1 長期間観測した通信データの分析

2.1.1 長期間観測した通信データの分析に関する検討

近年のサイバー攻撃対策技術として，サイバー攻撃を受けた際に，検知やフィルタリングといった対策を行う技術が主流となっている．この対策技術は，世界中で共有されているサイバー攻撃の被害や使用された脆弱性といった脅威情報をはじめ，マルウェアなどの攻撃プログラムを解析することで得られる，攻撃プログラムのバイナリや攻撃プログラム実行時の通信データ，ログなどのデータを分析した情報を対策に活用している．このようなサイバー攻撃対策技術は，侵入検知システム (IDS) やファイアウォール，アンチウイルスソフトなどとして広く普及しており，分析済みの攻撃手法や，分析済みの攻撃に類似した攻撃手法に対しては，有効な対策技術となっている．

しかし，この対策技術はサイバー攻撃を受けた際に発動するため，サイバー攻撃を受けた前後で，被害端末の通信や振る舞いに急激な変化が発生しない場合や，過去に観測されず分析されていない攻撃手法が用いられた場合，攻撃と識別し対策を行うことは困難であるといわれている [2]．

実際に，対策が困難であったサイバー攻撃の被害事例として，攻撃を受けてから対策が行われるまでに一年以上の時間を要した事例がある [3]．この事例の被害端末は，アンチウイルスソフトを導入していたにも関わらずマルウェアに感染し，一年以上にわたってユーザーが意図していない外部との不信通信を行なっていた．この事例から，アンチウイルスソフトなどの現在普及している対策技術では，対策の困難な攻撃手法が存在していることがわかる．このように，まだ防護側に分析されておらず対策の講じられていない攻撃手法を用いた方が，攻撃が成功する可能性は高いと考えられる．そのため，攻撃者は，攻撃を成功させるために，攻撃対象が持つ脆弱性や使用している対策技術などを事前に入念に調査している可能性が高いといえる．

攻撃者が攻撃を実行する際の手順をモデル化したサイバーキルチェーンによると，第一段階として Reconnaissance(事前調査) という手順が定義されている [4]．事前調査段階の活動は，攻撃対象に検知されないように，攻撃対象の通信や振る舞いに急激な変化を発生させないよう慎重に，長期間かけて行われているといわれており，発見することが困難であるといわれている [5]．そのため，事前調査活動もまた，現在普及している対策技術では対策が困難なサイバー攻撃の一つであるといえる．しかし，事前調査活動によって搾取された情報が，被害の深刻なサイバー攻撃に利用される危険性があることから，事前調査活動を観測

し，対策を講じることの重要性は高まっている [5].

本研究では，攻撃前後で被害端末の通信や振る舞いに急激な変化が発生しないよう慎重に，長期間かけて行われるような攻撃や調査活動の対策を講じるために，このような攻撃や調査活動を見つけ，分類することを目的としている．以上のことから，筆者らは，本研究の目的を達成するためには，サイバー攻撃の直前直後といった通信データに変化のある部分のみを分析するだけではなく，長期間観測した通信データを分析することも必要であると考えた．

2.1.2 節では，長期間観測した通信データを分析することで，サイバー攻撃もしくは事前調査活動と思われる通信を見つけている関連研究について述べる．

2.1.2 長期間観測した通信データを分析している研究

梶川ら [6] は，独自に設置したセンサーで 1 年間観測した通信データを用いて，同一送信元における宛先の変化数を分析することで，調査活動の一手法であると思われる分散走査活動の通信を発見している．

筆者ら [7] は，長期間観測した通信データを詳細に分析する手法を提案している．実際に，提案手法を用いて独自に設置したセンサーで 1 年間観測した通信データを詳細分析することで，1 ヶ月のうちのある 4 日間において，センサーの応答に応じて反応を変えてくる調査活動と思われる通信を発見している．

これらの関連研究から，長期間観測した通信データを分析することで，サイバー攻撃もしくは調査活動と思われる通信を見つけることが可能であるといえる．

2.2 通信データの分析によるプログラムの分類

2.2.1 通信データの分析によるプログラムの分類に関する検討

インターネットを経由して行われるサイバー攻撃は，インターネットプロトコルに則る必要があることから，プロトコルの性質上，必ず通信データが発生する [8]．このことから，インターネットを経由して行われるサイバー攻撃や調査活動を見つけるためには，通信データの分析が必要不可欠であると考える．

通信データは，送信者 (攻撃者) と受信者 (センサー) の間で伝達される情報である．この情報の伝達はモデル化されており，そのモデルの一つにシャノン・ウィーバーモデルというモデルがある (**図 1**)[9].

シャノン・ウィーバーモデルは，電話やラジオなどの通信において，情報を早く正確に伝達することを目的とした研究で発明されたモデルである．シャノンらによると，通信には必ず送信者 (Information Source) と受信者 (Destination) がおり，送信者は自身の意図 (Message) を送信機 (Transmitter) で信号 (Signal) にエンコードすることで，受信者へ伝達している．受信者は，受け取った信号 (Received Signal) を受信機 (Receiver) でデコードすることで，送信者の意図を解釈している．

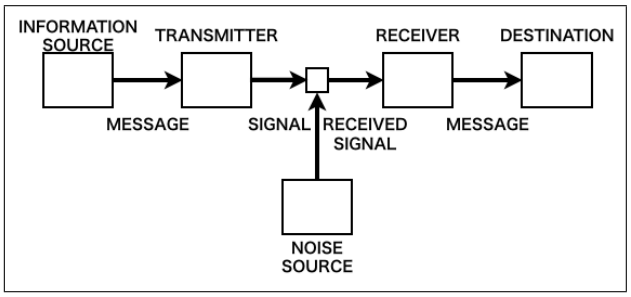

図 1 シャノン・ウィーバーによる情報伝達モデル
Fig. 1 Communication Model from Shannon and Weaver

本研究で扱う通信とは，インターネット通信である．そこで，シャノン・ウィーバーモデルをインターネット通信に適用すると，送信機は送信者の意図通りの挙動をするプログラムとそのプログラムを実行する計算機であり，信号は通信データであるといえる．また，サイバー攻撃の観点からシャノン・ウィーバーモデルをインターネット通信に適用すると，送信者は攻撃者であり，送信機は攻撃者の意図通りの挙動をする攻撃プログラムとそのプログラムを実行する計算機といえる．受信者は防護側の人間であり，受信機は防護側で設置しているセンサーであるといえる．つまり，受信機 (センサー) で観測可能な通信データが発生しているということは，送信者 (攻撃者) は，送信者の意図通りの挙動をするプログラム (攻撃プログラム) を必ず使用しているといえる．以上のことから，筆者らは，受信した通信データから，送信者が使用しているプログラムを分類することができれば，本研究の目的であるサイバー攻撃活動や調査活動を見つけることができ，その活動の分類が対策の検討に活用できるのではないかと考えた．

2.2.2 節では，通信データを分析することで，サイバー攻撃もしくは調査活動と思われるプログラムを分類している関連研究について述べる．

2.2.2 通信データの分析によりプログラムを分類している研究

桑原ら [10] は，ハニーポットで観測した通信データを用いて，マルウェアの感染判別と，感染したマルウェアの種類を分類する手法を提案している．

林ら [11] は，マルウェア実行時の通信データを用いて，マルウェアをファミリごとに分類する手法を提案している．

芦野ら [12] は，独自に設置したセンサーで 1 年間観測した通信データを用いて，情報収集活動で用いられているプログラムを分類する手法を提案している．

これらの関連研究から，通信データを分析することで，サイバー攻撃もしくは調査活動と思われるプログラムを分類することが可能であるといえる．

2.3 攻撃者像の分類

2.3.1 攻撃者像の分類に関する検討

2.2.1 節で述べたシャノン・ウィーバーモデルによると，送信者は，送信者の意図通りの挙動をするプログラムを用いることで，受信者へ意図を伝達している．また，筆者らの研究 [13] より，通信データから送信者の意図を推測できる可能性があることが示されている．そこで，筆者らは，2.2 節で述べた通り，通信データから送信者 (攻撃者) の意図通りの挙動をするプログラム (攻撃プログラム) を分類することができれば，同じ意図を持つと推測できる送信者 (攻撃者) を分類できるのではないかと考えた．

攻撃者は，目的や所属，組織構成によって分類できると言われている [14]．しかし，攻撃者の目的や所属，組織構成を，通信データのみから推測，考察することは非常に困難であると考える．そこで，本研究では，通信データを分析することでサイバー攻撃活動や調査活動を分類することができれば，その活動によって攻撃者像を分類し考察できるのではないかと考えた．

2.3.2 攻撃者像を分類している研究

笹渕ら [15] は，ダークネット上にハニーポットを設置し SSH を使用する攻撃を観測することで，複数の自動化ツールを用いて攻撃を行なう攻撃者と，自動化ツールを使用したのちに手動で攻撃を行う攻撃者を分類している．

梶川ら [16] は，独自に設置したセンサーで 1 年間観測した通信データを分析することで，類似した分散型操作活動を行っている送信元 IP アドレスを分類している．

これらの関連研究から，サイバー攻撃もしくは調査活動を行なっている攻撃者像を分類できる可能性があるといえる．

3. 本論文の位置付け

本章では，2 章で検討した，サイバー攻撃の攻撃活動や調査活動を見つけることを目的とした通信データの分析方針と関連研究から，本論文の位置付けを述べる．

近年，サイバー攻撃対策技術を回避するために，攻撃前後で被害端末の通信や振る舞いに急激な変化が発生しないよう慎重に，長期間かけて行われるような攻撃手法や調査活動が存在していると言われている．2.1 節より，このような攻撃手法や調査活動は，近年普及している攻撃前後の変化や事前に分析済みの攻撃情報に基づいて，サイバー攻撃を受けた際に対処する IDS やアンチウイルスソフトといった技術では，攻撃と識別し対処を行うことは困難であるという課題があることがわかった．

本研究ではこの課題を解決するために，このような攻撃活動や調査活動を見つけることを目的として，サイバー攻撃前後の通信データに変化のある部分のみを分析するだけでなく，長期間観測した通信データを分析する手法を提案する．分析手法を提案するにあたって，2.2 節より，インターネットを経由するサイバー攻撃は，常に通信データが発生することから，このようなサイバー攻撃や調査活動を見つけるためには，通信データの分析が不可欠であると考えた．また，シャノン・ウィーバーモデルより，通信データは送信者の意図通りの挙動をするプログラムによって発生するといえることから，受信データからプログラムを分類することができれば，その中から本研究の目的である攻撃活動や調査活動を見つけることが期待できると考えた．

さらに，2.3 節より，通信データからわかる攻撃活動や調査活動の種類，つまり送信者が使用しているプログラムの種類によって，攻撃者像を分類できる可能性があるとわかった．

そこで，本研究では，長期間観測した通信データを分析し送信者が使用しているプログラムを分類することで，サイバー攻撃もしくは調査活動目的と思われる通信を見つけ出す手法を提案し，実際に筆者らがサイバー空間上に設置したセンサーで長期間観測した通信データを用いて提案手法の評価を行う．併せて，評価の結果作成されたプログラムの分類から，攻撃者像に関する考察を行う．

4. 提案手法

本章では，長期間観測した通信データを分析し送信者が使用しているプログラムを分類することで，サイバー攻撃もしくは調査活動目的と思われる通信を見つけ出す手法を提案する．

2.1 節で述べた通り，攻撃前後で被害端末の通信や振る舞いに急激な変化が発生しないよう慎重に，長期間かけて行われるような攻撃や調査活動は，攻撃の直前直後といった通信データに変化のある部分のみを分析するだけではなく，長期間観測した通信データを分析する必要がある．しかし，長期間観測した通信データ全てを 1 パケットずつ詳細に分析することは，分析に膨大な時間がかかることが想定されるため，現実的な分析手法ではない．この問題を解決するために，筆者らは，長期間観測した大容量の通信データを詳細分析する手法を過去に提案している [7]．本研究では，過去に提案した大容量通信データの分析手法を元に，プログラムを分類する手法を提案した．本研究で提案する通信データの分析手法を**図 2** に示す．

(1) 長期間観測した通信データから，事前に選定しておいたプログラムの分類に有効と思われる特徴を抽出し，統計処理を行う．

(2) 統計情報を分析することで，通信データを分類するあたりをつけ，その特徴からフィルタルールを作成する．

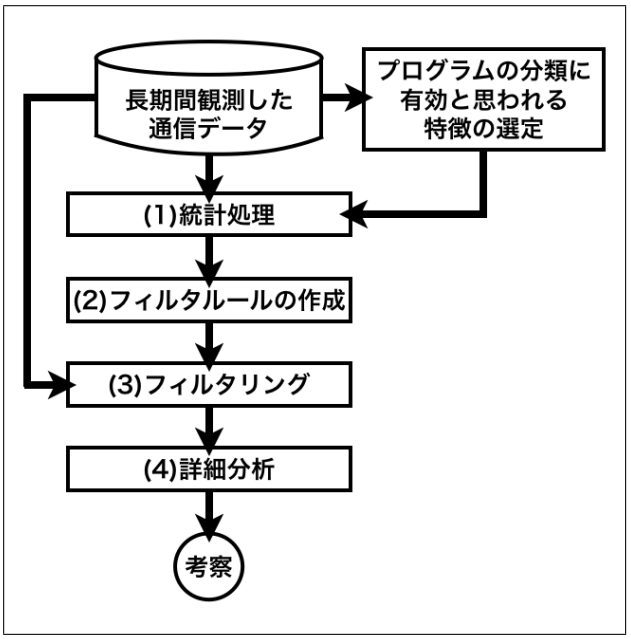

図 2 提案する分析手法
Fig. 2 Proposed Analysis Technique

(3) (2) で作成したフィルタルールを，元の長期間観測した通信データに適用し，詳細に分析するべき通信データを抽出する．

(4) 抽出した通信データを詳細に分析し，プログラムを分類することで，サイバー攻撃もしくは調査活動目的と思われる通信を見つける．

以上の手法により，長期間観測した通信データからプログラムを分類し，サイバー攻撃もしくは調査活動目的と思われる通信を見つけ出す．

最後に，詳細分析を行った結果を元に，プログラムの挙動やそのプログラムを使用している攻撃者像について考察を行う．

5. 評価実験

本章では，実際に筆者らがサイバー空間上に設置したセンサーで長期間観測した通信データを用いて，4 章で述べた提案手法の評価を行った手順とその結果について述べる．

5.1 実験使用データ

本節では，評価実験で使用した通信データの概要を述べる．このデータは，筆者らがサイバー空間上に設置した，約 1700 個のグローバル IP アドレスを観測しているセンサーの通信を収集したものである．このセンサーは，SYN フラグの立った TCP/IP パケットを受信した際に，その送信元に対して，SYN フラグと ACK フラグを立てた TCP/IP パケットと，RST フラグと ACK フラグを立てた TCP/IP パケットを，1 パケットずつ返送している．データの概要を，以下の**表 1** に示す．

表 1 実験で使用するデータの概要
Table 1 About Using Data of Exeriment

観測期間	2017/01/01〜2017/01/07
データサイズ	約 409GB
TCP/IP パケット数	約 33.8 億パケット
UDP/IP パケット数	約 1120 万パケット
総パケット数	約 34.0 億パケット

5.2 特徴の選定

本節では，通信データからプログラムを分類する際や，サイバー攻撃もしくは調査活動目的と思われるプログラムを見つける際，攻撃者像を考察する際に，有効と思われる特徴の選定について述べる．

5.2.1 IP アドレス

まず，送信元 IP アドレスについて検討する．近年，脅威情報の共有が進むにつれて，ボットネットやマルウェア配布サーバなど，サイバー攻撃の発信元となっている IP アドレスがブラックリスト化され，公開されている [17]．また，IP アドレスから，ドメインや所有者情報，地域といった送信者に関連する可能性のある情報を得ることができる．しかし，送信元 IP アドレスは，クラウドシステムなどの環境や踏み台を用いることで，容易に変更することが可能である [18]．そのため，送信元 IP アドレスから送信者の所属や所在地を特定することは困難であると考えるが，同じプログラムによると思われる通信ごとに送信元 IP アドレスを分類することで，攻撃者の分類や考察には活用可能であると考える．

次に，宛先 IP アドレスについて検討する．本実験で宛先となるセンサーの IP アドレスは，5.1 節で述べた通り，約 1700 個ある．そのため，同じプログラムによると思われる通信が，何種類のセンサーの IP アドレスで観測できるか，どのような順番で宛先 IP アドレスを変化させているか，といった情報からプログラムの挙動や攻撃対象の範囲を推測でき，プログラムを分類するのに活用可能であると考える．

5.2.2 ポート番号

まず，送信元ポート番号について検討する．送信元ポート番号は，送信側で任意に変更可能な場合や，セッションを貼りなおすたびに送信端末の OS によって自動で遷移していく場合がある．そのため，送信元ポート番号は，プログラムの分類や攻撃者の考察には活用困難であると考える．

次に，宛先ポート番号について検討する．宛先ポート番号は，TCP プロトコルや UDP プロトコルの性質上，特定のサービスで利用するために予約されている well-known ポートが存在する．また，走査活動の分類などで利用されているように [6], [16]，同じプログラムによると思われる

通信が何番のポート宛にきているのか，どのような順番で宛先ポート番号を変化させているか，といった情報からプログラムの挙動や攻撃対象の範囲を推測でき，プログラムを分類するのに活用可能であると考える．

5.2.3 プロトコルとフラグ

まず，プロコトルについて検討する．プロトコルは，OSI 参照モデル [19] でモデル化されているように，各プロトコルによって通信機能が分担されている．そのため，本実験では，OSI 参照モデルのトランスポート層以上のプロトコル，つまり，TCP/IP と UDP/IP を対象として分析を行う．

次に，フラグについて検討する．TCP/IP パケットの場合，プロトコルの性質上，ヘッダ内にパケットの役割を示す SYN や ACK といったフラグが存在する．このフラグは，TCP/IP の 3Way-Handshake のコネクション確立などでも利用されているように，送受信する順番が定められている場合がある．そこで本実験では，一定時間内に同一の送受信 IP アドレスと送受信ポート番号の組み合わせで行われた通信内で受信した TCP/IP パケットのフラグを，受信した順番に並べたものをフラグパターンと名付け，特徴として活用する．例えば，**図 3** の場合，フラグパターンは SYN - ACK - FIN/ACK - RST となる．

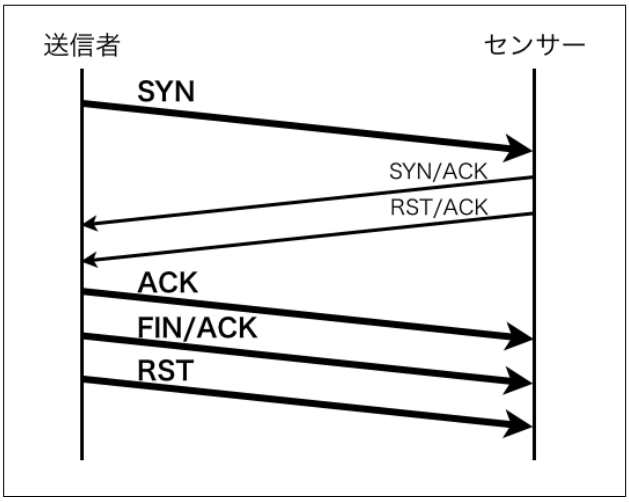

図 3 フラグパターンの例
Fig. 3 Example of Flag-Pattern

5.2.4 パケットの受信時間

パケットの受信時間について検討する．送信者が，意図的にパケットの送信日時や送信時間間隔を調整するプログラムを使用している場合，センサーで受信したパケットの受信時間を見ることで，プログラムの挙動を推測でき，プログラムを分類するのに活用可能であると考える．

5.2.5 本実験で使用する特徴

5.2.1 節から 5.2.4 節で行なった検討により，本実験では，以下の特徴を使用する．

- 送信元 IP アドレス
- 宛先 IP アドレス
- 宛先ポート番号
- プロトコル
- 受信順に並べた TCP/IP パケットのフラグ (フラグパターン)
- パケットの受信時間

5.3 評価実験の手順

本節では，実際に 5.1 節で述べた通信データを用いて，4 章で述べた提案手法の評価を行った手順の一例について述べる．

(1) 統計処理

5.1 節で述べた通信データの各パケットから，5.2 節で選定した 6 つの特徴のうちの，送信元 IP アドレス，宛先 IP アドレス，宛先ポート番号，プロトコル，パケットの受信時間の 5 つの特徴と，フラグ (TCP/IP パケットの場合のみ) を抽出した．

抽出した情報を元に，各パケットの情報をセッションごとにまとめた．ここで，セッションとは，送受信 IP アドレスと送受信ポート番号の組み合わせごとに，一度目の TCP/IP パケットもしくは UDP/IP パケットから 30 秒以内に発生した通信のことと定める．セッションごとにまとめる際に，TCP/IP パケットから抽出したフラグは，5.2.3 節で述べたフラグパターンとしてまとめた．

(2) フィルタルールの作成

(1) で抽出，作成した 6 つの特徴を用いて 5.1 節で述べた通信データを分析することで，通信データからプログラムを分類できるようなフィルタルールを作成した．

ここで，本実験で使用したフィルタルールの一例を示す．

本実験では，同一の送信元 IP アドレスから複数の送信元ポート番号を用いて，特定の宛先に同じフラグパターンで送られている通信をフィルタルールと定めた．

(3) フィルタリング

(2) で作成したフィルタルールを用いて，5.1 節で述べた通信データをフィルタリングした．このフィルタリングにより，長期間観測した通信データから，統計情報だけでなく，1 パケットずつ詳細に分析するべき通信データを抽出した．

(4) 詳細分析

(3) でフィルタリングした通信データを，1 パケットずつ詳細に分析し，プログラムを分類することで，サイバー攻撃もしくは調査活動目的と思われる通信を見つけた．

5.4 評価実験の結果

本節では，5.3 節で述べた実験手順に則って実験を行った結果について述べる．

5.3 節で述べた実験を行なった結果，3389 番ポート宛に，同じプログラムによるとみられる通信が分類できた．この分類において，同じ送受信 IP アドレスの組み合わせにおける通信の特徴を以下に示す．

- 送信元ポート番号は約 50 種類から約 350 種類
- 宛先ポート番号は 3389 番
- 同じフラグパターン

この通信で観測されたフラグパターンについて，**表 2** に示す．

表 2 観測されたフラグパターン
Table 2 Observed Flag-Pattern

1 回目	2 回目	3 回目	4 回目
CWR/ECE/SYN	CWR/ECE/SYN	SYN	ACK
5 回目	6 回目	7 回目	8 回目
PSH/ACK	PSH/ACK	PSH/ACK	RST/ACK

このような通信は一ヶ月間の 14 日間で観測されており，送信元 IP アドレスは合計で 13 種類あった．

観測された通信の観測日時ごとのパケット数の変化を**図 4** に示す．

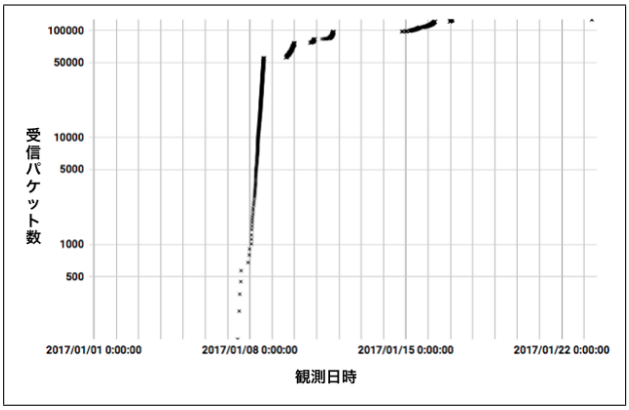

図 4 同一プログラムによるとみられるパケット数の変化
Fig. 4 Transition of Packets by Common Program

上記の特徴を持つ通信を 1 パケットずつフィルタリングし，選出した特徴以外の情報も詳細に分析した．その結果，どの送信元 IP アドレスからくるパケットにも，PSH/ACK パケットのペイロードには全て，**図 5** に示すようなデータが入っていた．

```
00 43 6f 6f 6b 69 65 3a  20 6d 73 74 73 68 61 73   Cookie:  mstshas
68 3d 68 65 6c 6c 6f 0d  0a 01 00 08 00 03 00 00   h=hello·  ·····
00
```

図 5 ペイロードに共通していたデータ
Fig. 5 Common Data from Payload

6. 考察

本節では，5.4 節で述べた評価実験結果について考察を述べる．

6.1 プログラムの分類の観点による考察

本節では，5.4 節で述べた評価実験結果について，プログラムの分類の観点で考察する．**??**節で述べた通り，この通信は，同一送信元 IP アドレスから同一宛先 IP アドレスとポートに対して，約 50 種類から約 300 種類もの送信元ポート番号から同じフラグパターンの通信を行なっていた．どの送信元 IP アドレスからの通信も同様のフラグパターンであり，また詳細分析を行ったところペイロードも類似していることがわかった．以上のことより，これらの通信は，送信元ポート番号のみランダムに変更して実行された同一プログラムによるものとみなせる．

6.2 攻撃者の分類の観点による考察

本節では攻撃者の観点で考察を行う．この通信は 3389 番の宛先ポート番号に集中していた．3389 番ポートは WindowsOS がリモートデスクトップのサービスで使用していることで知られている Well-Known ポートである．また，フラグパターンを見るとどの送信元からの通信も，1 回目と 2 回目のパケットのフラグは CWR/ECE/SYN と，通常の 3Way-HandShake では使用しないフラグが立っていた．このようなフラグを立てたパケットを，このフラグパターンになるように送り，かつ，ペイロードに同じ値を入れているパケットは，一般に使用されている製品の通信ではなく，送信者が何らかの意図を持ってこの通信を行うプログラムを作成し，使用している確率が高い．さらに，パケットの受信時間を見ると，一定時間内に送信元ポート番号を変えて 3way-handshake を行いコネクションの確立を試みている．

以上のことから，このプログラムを使用している送信者の意図として以下の 2 つの可能性が挙げられる．一つ目は，3389 番ポートに複数の送信元ポートから同時にコネクションを張ることで回線を遅延または停止させることを意図した攻撃者が使用している可能性が考えられる．二つ目は，このフラグパターンを送ることで 3389 ポートが開くシステムがどこかに存在し，そのシステムの特性を知っている攻撃者がそのシステムが存在する IP アドレスを調査するためにこのプログラムを使用している可能性が考えられる．

これらの可能性を持つ通信において，送信元 IP アドレスを攻撃者の識別子とみなすと，今回一ヶ月の期間のうちに観測された 13 種類の送信元 IP アドレスは，上記の目的

を持つ攻撃者の集団であると分類できる．

7. まとめ

本論文では，近年主流となっているサイバー攻撃対策技術を回避するために，サイバー攻撃前後で被害端末の通信や振る舞いに急激な変化を発生させず，長期間にわたってゆっくり攻撃を行っているサイバー攻撃や調査活動を見つけることを目的とした，通信データの分析方法を提案した．通信データが存在しているということは，必ず送信者が送信者の意図通りの挙動をするプログラムを使用しているということから，通信データから送信者が使用しているプログラムを分類する手法を提案した．併せて提案した分析手法を用いて，筆者らがサイバー空間上に設置したセンサーで観測した通信データを分析することで，通信データからプログラムを分類し，提案手法の有効性を示した．さらに，分類した通信データから，そのプログラムを使用している攻撃者像についても考察を行なった．

参考文献

[1] JPCERT/CC：JPCERT/CC インシデント報告対応レポート (online)，入手先 ⟨https://www.jpcert.or.jp/pr/2018/IR_Report20180712.pdf⟩ (参照 2018.08.10)．

[2] 大谷尚通，北野美紗，重田真義：企業内ネットワークの通信ログを用いたサイバー攻撃検知システム，コンピュータセキュリティシンポジウム 2013(2013)．

[3] 情報処理推進機構セキュリティセンター：サイバーレスキュー隊 (J-CRAT) 分析レポート 2016 長期感染の実態 ～1 台の感染 PC に残された攻撃痕跡の分析～(online)，入手先 ⟨https://www.ipa.go.jp/files/000057175.pdf⟩(参照 2018.08.10)．

[4] Lockheed Martin Corporation：*THE CYBER KILL CHAIN*(online)，入手先 ⟨https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html⟩(参照 2018.08.10)．

[5] 海野由紀，森永正信，山田正弘，鳥居悟：標的型サイバー攻撃におけるシステム内部の諜報活動検知の提案，コンピュータセキュリティシンポジウム 2012(2012)．

[6] 梶川慶太，中村康弘：宛先変化数に着目した分散走査活動の検出，2018 年電子情報通信学会総合大会 (2018)．

[7] 鮫島礼佳，芦野佑樹，矢野由紀子，島成佳，中村康弘：長期間の観測データを用いたサイバー攻撃と推定される通信を分析する手法の提案，2018 年暗号と情報セキュリティシンポジウム (2018)．

[8] 日本ネットワークインフォメーションセンター：IP(Internet Protocl) とは (online)，入手先 ⟨https://www.nic.ad.jp/ja/basics/beginners/ip.html⟩(参照 2018.08.10)．

[9] Claude E. Shannon，Warren Weaver：*The Mathematical Theory of Communication*，The University of Illinois(1949)．

[10] 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ーから感染種類を判定する発見的手法について，コンピュータセキュリティシンポジウム 2009(2009)．

[11] 林孝英，山口由紀子，嶋田創，高倉弘喜：ネットワークトラフィックフローにおけるシーケンスパターンに基づくマルウェア分類手法，コンピュータセキュリティシンポジウム 2014(2014)．

[12] 芦野佑樹，中村康弘，矢野由紀子，島成佳：サイバー攻撃の初期段階と推定される活動で使用されるプログラムの分類手法の提案と評価，コンピュータセキュリティシンポジウム 2017(2017)．

[13] 鮫島礼佳，芦野佑樹，須尭一志，矢野由紀子，中村康弘：サイバー攻撃の有無が不明な通信データからサイバー攻撃目的と推定される通信を抽出する手法の提案，第 82 回 CSEC 研究発表会 (2018)．

[14] 谷口星彦：攻撃者の分類の一考察，日本セキュリティ・マネジメント学会学会誌第 31 巻第 2 号 (2017)．

[15] 笹渕美寛，曽根直人，森井昌克：ダークネットに設置したハニーポットへのアクセス解析，コンピュータセキュリティシンポジウム 2013(2013)．

[16] 梶川慶太，中村康弘：分散型走査グループの検知と攻撃ペイロードの分類，第 16 回情報科学技術フォーラム (2017)．

[17] NTT PC Communications：用語解説辞典 ブラックリスト方式 (online)，入手先 ⟨https://www.nttpc.co.jp/yougo/ブラックリスト方式.html⟩(参照 2018.08.10)．

[18] Amazon：Amazon EC2 インスタンスの IP アドレッシング (online)，入手先 ⟨https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/using-instance-addressing.html⟩(参照 2018.08.10)．

[19] JPNIC：OSI 参照モデルとは (online)，入手先 ⟨https://www.nic.ad.jp/ja/basics/terms/osi.html⟩(参照 2018.08.10)．