Vol.2017-CSEC-78 No.6
Vol.2017-SPT-24 No.6
2017/7/14

長期間に渡るインターネットノイズの観測に基づいたサイバー攻撃の初期活動と推定される通信の発信源を分類する手法の提案

芦野佑樹[†1]　山根匡人[†1]　矢野由紀子[†1]　島成佳[†1]

概要：インターネット上には一見すると影響がなく意図の不明なインターネットノイズと呼ばれる通信が存在する．かつて筆者らは，インターネットノイズの分類に基づいた内容を応答することで，高度な技術を有する組織的な活動が存在する可能性を示した．このようなインターネット上での活動がサイバー攻撃の初期段階と仮定すれば，インターネットノイズの分析は攻撃者の活動の推測を可能とし，過去の事例に基づく分析が中心であったサイバーセキュリティにおけるリスク分析の精度向上に期待できる．本論文では，180 日間に渡って観測されたインターネットノイズの調査を通じて，サイバー攻撃の初期段階を捉えることを目的としたインターネットノイズ発信源の分類方法を提案する．併せてインターネットノイズの分析をサイバーセキュリティ対策の検討に活用できる可能性について考察する．

キーワード：インターネットノイズ，サイバーセキュリティ，偵察活動，攻撃者の分析，パケット解析，リスク分析

Proposal of a Communication Source Classification Method of the Cyber Attack in the Initial Stage based on a Long Term Internet Noises Observation

YUKI ASHINO[†1]　MASATO YAMANE[†1]
YUKIKO YANO[†1]　SHIGEYOSHI SHIMA[†1]

Abstract: On the Internet, there are packets of unclear intentions which are called the Internet Noises. Authors presented a possibility of an organization activities on the Internet, based on classification communication source and observation of the Internet Noises with reactive sensors. If these activities are the first stage of cyber attack phases, accuracy of cyber risk estimate will be improved by analysis of the Internet Noises. In this paper, in order to analyze the Internet Noises we propose a method for communication source classification of the Internet Noises using observation the Internet Noises data set for 180 days. Also we consider about measures of cyber security using estimation of enemies.

Keywords: Internet Noises, Cyber Security, Reconnaissance, Estimation of enemies, Packets Analysis, Risk Analysis

1. はじめに

インターネット上にはインターネットノイズ[1][2]と呼ばれる意図が不明な通信が存在する．インターネットノイズを受け取っても影響がないことから無視される対象とされる．しかし，インターネットノイズの発信源の中には，応答内容によって通信パターンに変化が生じるものがある．かつて筆者らは，発信源を分類した上で特定の内容を返した後の通信パターンの変化を長期間捉えた結果，インターネット全体のウェブサーバを調査することを目的とした高度な開発技術能力を有する組織的な活動が存在する可能性を示した[3]．このようなインターネット上の活動は，ロッキードマーチン社によって発表されたサイバーキルチェーン[4]によるとサイバー攻撃の初期段階である偵察活動だった可能性があると筆者らは考える．

このようなインターネット上での活動がサイバー攻撃の初期段階と仮定すれば，インターネットノイズの分析は攻撃者の活動の推測を可能とし，過去の事例に基づく分析が中心であったサイバーセキュリティにおけるリスク分析の精度向上に期待できる．

筆者は，インターネットノイズを分析するためにはインターネットノイズの分類に基づいた内容を応答する必要があると考えた．そこで，本研究ではインターネットノイズの発信源の分類に課題と定め，180 日間に渡って観測したインターネットノイズに基づいて発信源を分類する方法について提案する．併せてインターネットノイズがサイバー攻撃活動の初期段階である場合において，サイバーセキュリティ対策におけるインターネットノイズの分析結果の活用についても考察したので併せて報告を行う．

2. 関連研究

インターネットを介したサイバー攻撃を観測すること

†1 NEC 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・ファクトリー

を目的とした関連研究は，サイバー攻撃の通信を一方的に記録するパッシブセンサーを用いた研究と，通信に対して応答するリアクティブセンサーを用いた研究に分類できる．また，分析対象に関しては，攻撃の意図が攻撃であると明確である場合と，意図自体が不明な場合とで分類できる．各関研究の関係性を図 1 で示す．本章では，各関連研究の例を挙げた後に本論文で取り扱う課題について述べる．

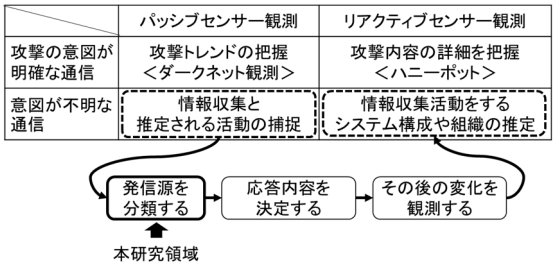

図 1　観測する関連研究の分類

2.1 パッシブセンサーによる攻撃意図通信の観測

代表的なパッシブセンサーのアプローチとして，NICTer プロジェクト[5]に代表されるように未使用のグローバル IP アドレス宛ての通信を観測するダークネット観測がある. 通常利用において未使用の IP アドレス宛の通信は発生しないことから，ダークネット観測において受信した通信は基本的に攻撃を意図している可能性が高いと考える．ダークネット観測に基づいた大容量の通信を分析することで，インターネット全体で行われている攻撃手段や発信源の傾向を捉えることが可能とされる[6].

2.2 リアクティブセンサーによる攻撃の意図が明確な通信の観測

代表的なリアクティブセンサーのアプローチとして，攻撃の意図のある通信に対して応答するハニーポットがある．代表的なハニーポットである Dionaea[7]は，脆弱性を持つ OS やサービスのように振る舞うことにより送り付けられたマルウェアを捕獲することが可能である．ハニーポットによっては，マルウェアの捕獲以外にも，マルウェア本体の挙動や不正侵入活動の記録を採ることも可能である．

2.3 パッシブセンサーによる意図が不明な通信の観測

実際に利用しているグローバル IP アドレス帯(以下，ライブネット)には, サービス提供の有無に限らず意図が不明な通信が多く送られている．このような通信はインターネットノイズと呼ばれ，ファイアウォールによって遮断されたり，サービスに対して影響がないことから無視される対象となる．

パッシブセンサーによってインターネットノイズを観測する関連研究に Shinoda らの研究がある．Shinoda らは，単位時間当たりのパケット送信量に意味を持たせることでパッシブセンサーの IP アドレスを割り出そうとする攻撃の存在を示している[8].

ゴらの研究では，ライブネットワークのアドレス帯に発信される膨大な TCP/IP パケットの分析し，大規模なポートスキャンを捉えている[9].

2.4 リアクティブセンサーによる意図が不明な通信の観測

意図が不明な通信であるインターネットノイズの発信源に対して適切な内容をリアクティブセンサーによって応答する先行研究は，筆者らが調べた範囲では筆者らの先行研究[3]以外は見つからなかった．筆者らの先行研究では，リアクティブセンサーによってインターネットノイズを観測することで，発信源を構成するシステム構成やそのシステムを開発・運用する者の能力の推定ができる場合があることを示した.

2.5 本論文における研究領域

インターネットノイズの発信源を詳細に調査するためには, リアクティブセンサーによって観測する必要がある．しかし，筆者らの先行研究によればリアクティブセンサーが応答する内容は発信源の分類に適する必要がある．そのため，応答する内容が限定されているハニーポットでは，インターネットノイズの発信源の分析は難しい可能性がある．さらに，インターネットノイズを全て確認し，一つずつ適した応答を推定しながらリアクティブセンサーを実装することは現実的ではない.

そこで，本論文における研究領域は，インターネットノイズの分析に向けて，リアクティブセンサーで応答する内容を決定するために必要な要素である発信源の分類をする手法を提案することと定める(図 1 の太枠).

3. 発信源の分類手法確立に向けた調査

本章では，実際のインターネットノイズを観測したデータセットを用いて発信源の分類手法の確立に向けた調査について述べる.

3.1 ライブネットワークにおけるパッシブセンサーで取得したインターネットノイズのデータセット

本章で扱うデータセットは，ライブネットワークに属するグローバル IP アドレスを 1 つ割り当てたパッシブセンサーが捉えた通信データを pcap ファイルとして記録したものである．データセットには管理目的の通信は含まれないようにした. このデータセットの緒元を表 1 にまとめる.

表 1　データセットの緒元

期間	2016/03/06～2016/09/02(180 日間)
容量	約 7GB
パケット数	約 2,455 万(IP パケット)

3.2 調査に用いる属性

かつて筆者らは，複数の発信源が協調して 24 時間ごとに同じ内容を発信するインターネットノイズを発見している．このようなインターネットノイズが存在する可能性もあることから，通信の発着点に関する情報と受信した時刻を処理できる必要があるとした．以降，本論文では発信元

Vol.2017-CSEC-78 No.6
Vol.2017-SPT-24 No.6
2017/7/14

IP アドレスを発信源と称する．通信データの調査に関してプロトコルごとの取り扱う属性について表 2 にまとめる．

表 2　調査に用いる属性

プロトコル名	属性
IP	受信時刻 発信元 IP アドレス(発信源) 宛先 IP アドレス 種類(IP，TCP/IP，UDP/IP)
TCP/IP	宛先ポート，フラグ

3.3　調査手法

本節ではデータセット全体の調査について述べる．調査手法は発信源の数，同一発信源による発信回数，観測期間である．観測期間の定義については 3.3.3 で述べる．

3.3.1 発信源の数と通信プロトコル

発信源の数は 79,532 であった．表 3 には通信プロトコルごとの発信源数と全体に対する割合を示す．通信プロトコル別の発信源数の合計が 79,532 を超えるのは，同一の発信源が複数の通信プロトコルを発信する場合が存在するためである．通信プロトコルの分類は，TCP/IP，UDP/IP と，それ以外(以下，非 TCP/IP・非 UDP/IP)とする．

表 3　通信プロトコルごとの発信源数

通信プロトコル名	IP アドレス数(割合)
TCP/IP	69,444 (89.0%)
UDP/IP	10,023 (10.0%)
非 TCP/IP・非 UDP/IP	1,087 (1.1%)

3.3.2 同一発信源からの通信回数の分布

発信回数ごとの発信源数と全体に対する割合を表 4 に示す．併せて横軸を発信源が発信した回数とし縦軸に発信源の累積度数とした累積度数分布を図 2 に示す．なお，横軸は 10 を基数とする対数軸である．

表 4　発信源からの発信回数と割合

発信回数	発信源数(割合)	発信回数	発信源数(割合)
1	27,130 (34.1%)	6	1,110 (1.4%)
2	26,912 (33.8%)	7	281 (0.4%)
3	18,450 (23.2%)	8	302 (0.4%)
4	2,476 (3.1%)	9	331 (0.4%)
5	769 (1.0%)	10 以上	1,762 (2.1%)

同一発信源から通信が発せられた回数については，発信回数が多くなるにつれ発信源の数は減っていき，10 回以上発信する発信源は 1,762 個であり全体の約 2.1%だった．

3.3.3 同一発信源からの観測期間

同一の発信源が使用されている期間を調査する．水谷の研究[10]では同一の発信源から発信された通信を最初に受け取ってから最後に受け取った時刻の差を観測期間と定義している．本論文でもこの観測期間の定義を準用する．観測期間を調査する対象は 2 回以上発信する 52,402 個の発信源とした．横軸に観測期間とし縦軸に発信源の累積度数とした累積度数分布を図 3 に示す．横軸は 10 を基数とする対数軸である．大きな特性として観測期間が 3.0±0.5 秒における累積度数が顕著に上昇している(図 3(1))．

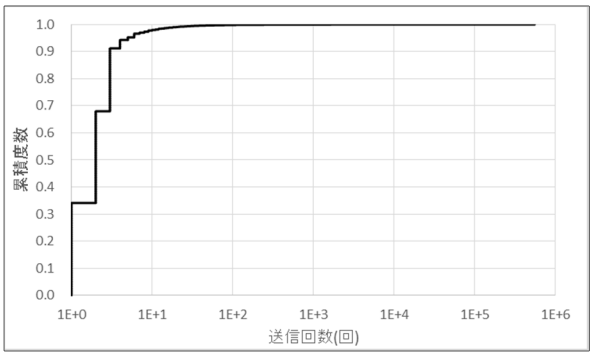

図 2　発信源の発信回数の累積度数分布

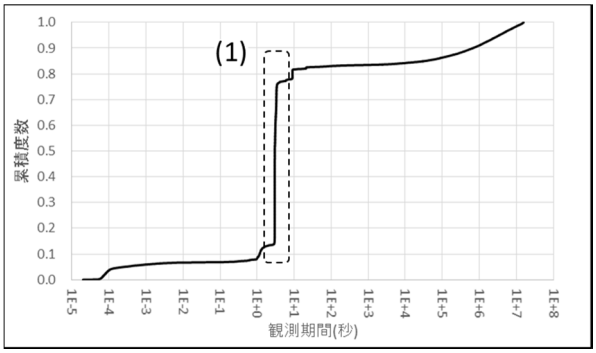

図 3　発信源と観測期間の累積度数分布

3.4　観測期間が 3.0±0.5 秒となる発信源の分析

3.3.3 で述べた通り，観測期間が 3.0 秒付近の発信源が多く存在している．本節では 3.0±0.5 秒を観測期間とする発信源について調査した内容をまとめる．

3.4.1 通信プロトコルごとの発信源数

表 5　3.0±0.5 秒を観測期間とする発信源のうち
通信プロトコル別における発信源の数

通信プロトコル名	発信源数(割合)
TCP/IP	32, 870 (99.9%)
UDP/IP	47 (0.1%)
非 TCP/IP・非 UDP/IP	3 (0.0%)

3.0±0.5 秒を観測期間とする発信源は 32,920 個であった．この期間において通信プロトコルごとの発信源数を集計した結果を表 5 に結果を示す．

3.0±0.5 秒を観測期間となる UDP/IP を発した発信源の割合は約 0.1%であった．表 3 でまとめたデータセット全体における UDP/IP を発する発信源の数は約 10.0%であり，両者の差は約 100 倍であった．この結果から，発信源の観測期間によって発信される通信のプロトコルに偏りが存在す

ることがわかった.

同一発信源からの発信回数

同観測期間内における同一発信源の発信回数の割合を表 6 に示す．データセット内におけるすべての発信源における発信回数を示した表 4 に比べると，4 回以上発信している割合が非常に少ないことが言える．このことから，観測期間と発信回数には偏りがあることがわかった.

表 6　観測期間が 3.0±0.5 秒の発信源における
発信回数ごとの発信源の数と割合

発信回数	発信源数(割合)
2	19,987 (61.1%)
3	12,309 (37.6%)
4	414 (1.3%)
5 回以上	15 (0.0%)

3.4.2 観測期間が 3.0±0.5 秒に集中する理由

観測期間が 3.0±0.5 秒となる発信源が発した TCP/IP のパケットを調査した所，SYN パケットが約 99.8%を占めていた．この結果は，TCP/IP の特性に起因されるものと考えられる．TCP/IP パケットは，OS 等によって自動的に再送処理が行われることが知られている．例えば，Windows の場合，TCP/IP パケットの再送時間は 3.0 秒が規定値とされており[11]，このような環境から発信された TCP/IP パケットは，何も応答を返さないパッシブセンサーに対しては規定された間隔でパケットを再送する.

したがって，観測期間が 3.0±0.5 秒となる発信源が多かった理由は，再送処理の間隔が 3.0 秒と規定した環境が多かったためと考えられる.

3.5 通信プロトコルごとの発信回数

3.4 節によって, 発信源が発信する通信プロトコルによって観測期間に偏りのあることがわかったことから，本節では通信プロトコルごとの発信回数の偏りを調査する．データセット全体から TCP/IP，UDP/IP，非 TCP/IP・非 UDP/IP における同一発信源からの発信回数とその割合を集計する. 発信回数は，5 回以上発信する送信源の割合は各通信プロトコルにともに累計して 10%に満たなかったことから，1 回から 4 回までの各回と 5 回以上の 5 種類とする(図 4).

図 4 の通り総じて発信回数が多くなるほど発信源数の割合は減る傾向であるが，非 TCP/IP・非 UDP/IP は 3 回発信する発信源の割合よりも 4 回発信する発信源の方が約 7.2 倍多い．TCP/IP を発信する発信源の発信回数については, 1 回から 3 回までの平均は約 30.6%となりほぼ同じである. 一方で, UDP/IP を 2 回以下発信する発信源の割合は合計で約 85.0%を占め 3 回発信する発信源の割合は約 3.6%となる.

この結果から，発信源の発信する通信プロトコルによって発信回数に偏りが存在することがわかった.

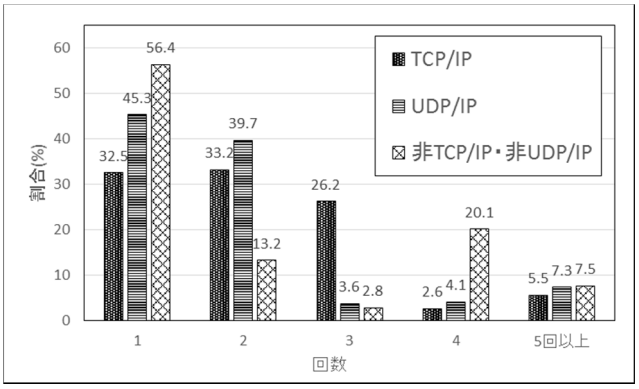

図 4　通信プロトコルごとの発信回数の割合

3.6 調査のまとめ

データセットの通信データは, 全て IP に則って発信源から発信されており，電気的なノイズ等によって自然発生するものではない．したがって，インターネットノイズは明確な意図に沿って特定の宛先に発信された通信であると言える.

3.4 節と 3.5 節の結果に基づけば発信源の発信回数と観測期間は，発信源の環境や実装に依存する可能性を示している．このことから，発信回数と観測期間が近い発信源を集めることで発信源の分類ができる可能性がある.

3.7 発信源を分類に向けた要件

3.6 節の通り発信源は, 通信の発信回数と観測期間で特性付けられ，同様の特性を有する発信源は複数存在することもわかった. 以上のことから, 発信源を分類するためには, 発信源ごとの発信回数と観測期間を表現でき，かつ，発信回数と観測期間の近い発信源が複数存在することを確認できる必要があると考えた．発信源の分類するための要件を表 7 にまとめた.

表 7　発信源を分類するための要件

要件 1	発信源の発信回数と観測期間を表現
要件 2	同様の特性を持つ複数の発信源の存在を確認

4. 発信源の分類を見える化する提案手法

発信源の特性を表現することを目的として，縦軸に観測期間と定め横軸に観測回数と定めて発信源の特性を二次元平面上に投影する手法を提案する．発信源の発信回数と観測期間を表現できることから，表 7 で示した発信源を分類する要件 1 を満たすことを目指す.

さらに，二次元平面上に投影する以上，二次元平面の分解能によっては同一座標上に複数の発信源が重複する場合がある．この場合は，同一の特性を有する発信源が複数存在することを意味していることから，発信源の重複度合に応じて色を変化させる．このことで, 3.7 節で述べた発信源を分類する要件 2 を満たすことを目指す.

以降，上記の手法をスペシャルパターンと称し，その基本的な考え方を図 5 に示した．図 5 を例にすると，観測期

間が 1 秒から 10 秒であり発信回数が 2 回となる発信源が 6 つある際は，その数に該当する領域の色は図 6 下部のカラーパターンを参照する．このことで，同一領域の発信源数を表現する．

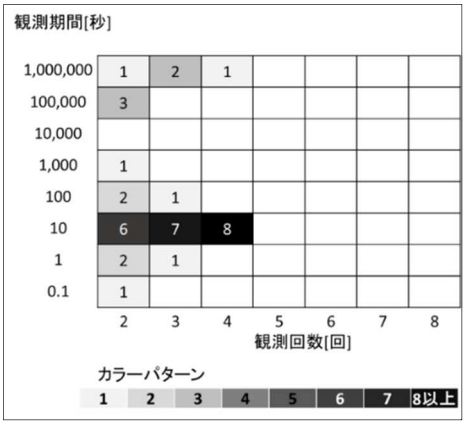

図 5　スペシャルパターンの例

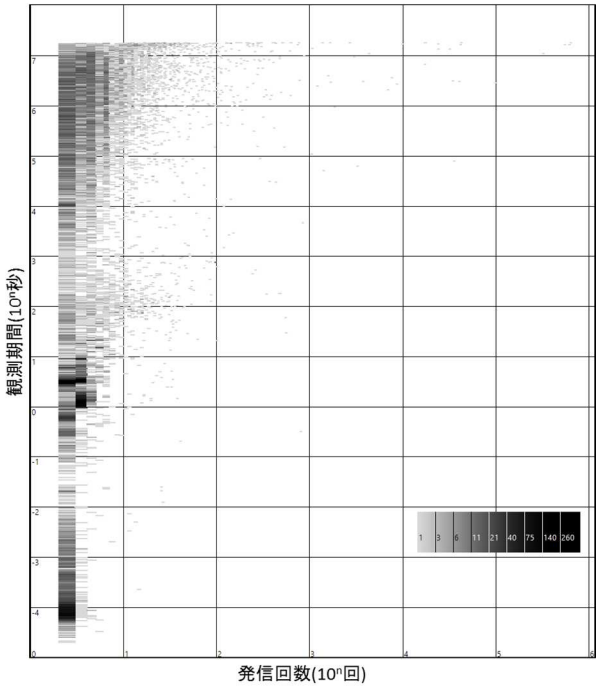

図 6　データセット全体のスペシャルパターン

データセットに含まれるすべての発信源について，発信回数と観測期間を集計し，スペシャルパターンとして表示した結果を図 6 に示す．発信回数及び観測期間は 3.3 節での調査に基づくと，各数値が大きくなるほど発信源数が減ることから各軸は対数軸とし基数は 10 とする．

同一領域における発信源の数は色の変化で表現し，各スペシャルパターン色と数値の目安をカラーパターンとして図中に示す．

5. 検証実験

5.1 通信プロトコルごとのスペシャルパターン

第 3 章で述べた通り通信プロトコルごとによって発信回数と観測期間に偏りがあることがわかっている．そこで，本節では 5.1.1 において TCP/IP のスペシャルパターンを作成してその特徴を述べる．TCP/IP 以外の通信プロトコルを発信する発信源が全体の約 11.5%しか存在しないことから，5.1.2 で UDP/IP と非 TCP/IP/IP・非 UDP/IP/IP を非 TCP/IP と称してまとめたスペシャルパターンを作成しその特徴を述べる．

5.1.1 TCP/IP

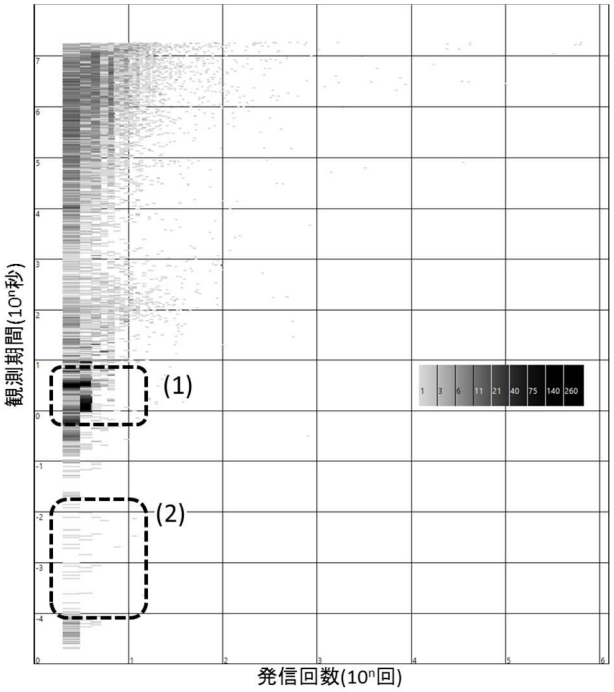

図 7　TCP/IP のスペシャルパターン

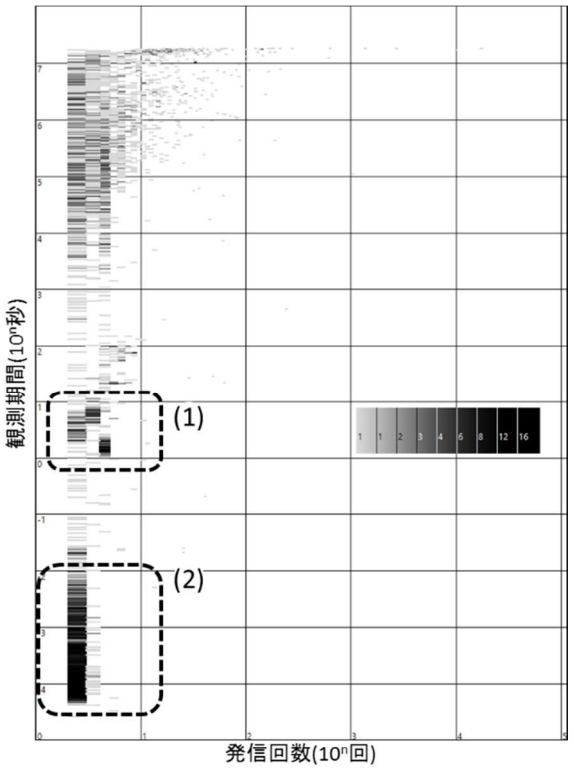

図 8　非 TCP/IP のスペシャルパターン

Vol.2017-CSEC-78 No.6
Vol.2017-SPT-24 No.6
2017/7/14

TCP/IP のスペシャルパターンを図 7 に示す．TCP/IP パケットを発する発信源は全発信源の 89.0%を占めていることから，データセット全体のスペシャルパターンである図 6 と似ている．

縦軸が 0（1 秒）から 1（10 秒）の観測期間を持つ発信源は非常に多い（図 7(1)）．しかしながら，縦軸-4(100 マイクロ秒)から-2(10 ミリ秒)の観測期間を持つ発信源が少ない(図 7(2))．そのため，100 マイクロ秒から 10 ミリ秒を観測期間とする発信源は TCP/IP 以外であることがスペシャルパターンから確認できた．

5.1.2 非 TCP/IP

非 TCP/IP のスペシャルパターンを図 8 に示す．縦軸が 0(観測期間 1 秒)から 1(同 10 秒)となる発信源のパターンは TCP/IP とは異なっていることが確認できた(図 8(1))．また，縦軸が-4(100 マイクロ秒)から-2(10 ミリ秒)付近の観測期間となる発信源が多いことが確認できた(図 8(2))．

5.2 宛先 TCP ポート別のスペシャルパターン

通信プロトコルによってスペシャルパターンに差異が存在することが確認できたため，宛先の TCP ポートによるスペシャルパターン差異についても調査する．スペシャルパターンを作成する対象を決定するために，宛先の TCP ポートごとの発信源の数を集計した(表 8)．本節では，発信源数の上位の 2 つである 23 と 1433 を取り上げスペシャルパターンの作成しその特性を述べる．

表 8　宛先 TCP ポート番号別発信元 IP アドレス数

ポート番号(用途)	発信元 IP アドレス数
23 (telnet)	67,422
1433 (MSSQL)	4,922
22 (SSH)	2,237

5.2.1 23/TCP のスペシャルパターン

データセットの中から 23/TCP 宛の通信を表現しスペシャルパターンを作成した(図 9)．図 9(1)の通り 3.0 秒付近に色濃く出ている．また，縦軸 2(100 秒)から 3(1,000 秒＝約 16 分 40 秒)を観測期間とする発信源が多くあることが確認できた(図 9(2))．

5.2.2 1433/TCP のスペシャルパターン

1433/TCP は Microsoft SQL Server[12]が標準で用いる TCP ポートである．データセットの中から 1433/TCP 宛の通信を表現しスペシャルパターンを作成した(図 10)．22/TCP と同様に 3.0 秒付近に多くの発信源が存在する(図 10(1))一方で，23/TCP と比較すると縦軸 2(100 秒)から 3(1,000 秒＝約 16 分 40 秒)を観測期間とする発信源がほとんどないことが確認できた(図 10(2))．また，横軸 1(発信回数 10 回)から 2(発信回数 100 回であり縦軸 5(観測期間が 100,000 秒＝約 1 日)から 7 付近(同 10,000,000 秒＝100 日以上)となる発信源が多く存在することが確認できた(図 10(3))．

6. 考察

6.1 提案手法の有効性

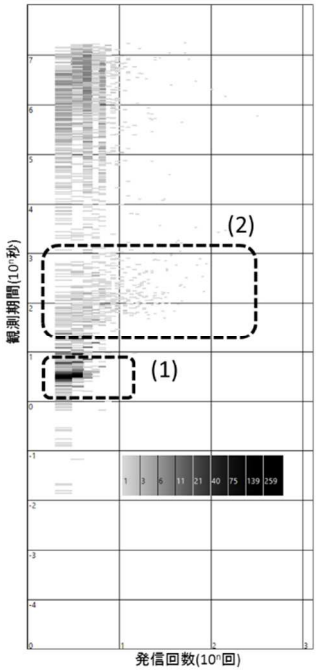

図 9　23/TCP

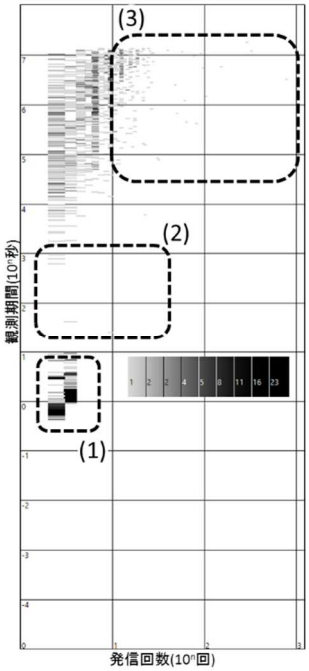

図 10　1433/TCP

第 5 章の検証実験の通り，通信プロトコルや宛先 TCP ポートによってスペシャルパターンに差異が存在することを示した．この差異によって，提案手法の特性から発信回数と観測期間の偏りが異なることを表現できたと言える．以上の結果から，3.7 節で述べた分類の要件 1 を満たせたと言える．

併せて，色の濃淡により同様の特性を持つ発信源の重複度合を表現できた．このことにより，3.7 節で述べた要件 2 を満たせたと言える．

以上の結果から，第 4 章で提案した発信源の分類手法は有効であると考えられる．

6.2 IP アドレスや観測時間帯によるインターネットノイズの特殊性

清水らは大分大学における 2016/04/06 から約 24 時間観測した通信データの集計を発表している．その集計によると，最も多かった SYN パケットの宛先の TCP ポートは 50382 であった[13]. 警察庁による@police[14]や情報通信研究機構による NICTER WEB 2.0[15]においては，リアルタイムで定点観測結果を公表している．両者の観測結果は，同じ時間帯であっても一致していない．@police においてまれに well-known ports[16]以外の TCP ポート宛の通信が大量に発生している時間帯の存在を確認できことから，宛先の TCP ポートの傾向は時間帯によっても異なると言える．

上記のように，インターネットにおける通信は，IP アドレスや時間帯によって変化すると言える．インターネットノイズも同様に観測する IP アドレスや時間帯によって異

なることも考えられることから，今後は観測点を増やしてIP アドレスや時間帯の変化を捉えていきたい．

6.3 過去の事例だけに基づかないリスク分析の可能性

セキュリティ対策の検討手法は現在に至るまで多くの研究が存在する．佐々木らは，経営者や情報システム部門のほか従業員と言った利害が複雑に絡む複数の関与者間におけるセキュリティ対策案の選択手法として多重リスクコミュニケータ(MRC)を提案している[17]．MRC では，専門家が過去のセキュリティインシデントの事例に基づいて対策案候補の列挙や対策案の効果を決定する[18]．しかし，専門家は世の中で発生したすべての事例を網羅することは困難であったことから，対策案効果の数値は定性的であった．また，未だに知られていない事例に適した対策案候補の列挙も難しかった．

そこで筆者らは，インターネットノイズの分析を通じて発信源を構成するシステムやそのシステムを開発・運用する者の能力を推定した結果をリスク分析に役立てられないかと考えた．例えば，ある分類された発信源から常に最新の脆弱性を突く通信を特定のサーバに対して発信していたことが確認できた場合，脆弱性情報の公開時刻，その脆弱性を突いた通信を観測した時刻，パッチ公開時刻，パッチ適用の時刻等から定量的な攻撃成功率の算出が可能であると考えられる．また，ある分類された発信源がウェブサーバのバージョン情報を調査している可能性が確認できれば，バージョン情報を偽装するといった新しい対策の導出が可能となる．

以上のように攻撃者の活動を捉えた結果をリスク分析への応用は，過去の事例に基づかないリスク分析を可能とし，結果として防御側の活動に有効ではないかと筆者らは考えた．第 7 章では攻撃者によるサイバー攻撃における初期段階を捉える研究の今後について述べる．

7. 本研究の今後について

7.1 検知されにくい攻撃手段

確たる目的に基づいて特定の目標に対して行われるサイバー攻撃は標的型攻撃(APT 攻撃)と呼ばれる．近年のAPT 攻撃は，サイバー攻撃が開始されてから被害が発覚するまでに半年以上の時間を要するケースがあるとされる[19][20]. 被害が発覚するまでに長時間を要する理由として，攻撃者が検知されてしまうような攻撃手段を選択していないと考えられる．すなわち，攻撃者は，攻撃目標の検知能力を把握した上で適切な攻撃手段を選択していると考えられる．攻撃者が，攻撃目標の検知能力をどのように把握しているのかは不明ではある一方で，攻撃者は徹底的な攻撃目標に関する情報収集を実施しているとも言われている[21].

7.2 節ではサイバーキルチェーンに基づいて，情報収集から武器化に至るまでの過程について述べる．

7.2 サイバーキルチェーンにおける情報収集の位置付け

サイバーキルチェーンとは，軍事行動をモデルにサイバー攻撃を 7 つのフェーズで表現したものである[4]．サイバーキルチェーンによると，攻撃手段の選択は第 2 段階目の武器化フェーズであるとされる．攻撃手段の選択に資する情報は，第 1 段階目の偵察フェーズにあるとされる．

サイバーキルチェーンに関するドキュメントには偵察フェーズにおける具体的な活動内容に関する記載がない．一般に偵察活動は見つけにくい活動であると言われている[22]．このことからも攻撃者が実施しているとされる偵察活動内容に関してはあまり知られていない．

そこで，筆者らは，サイバーキルチェーンが軍事行動をモデルにしている点に着目した．軍事行動における偵察活動に関する情報があれば，サイバーキルチェーンにおける偵察活動の具体的な内容を推定できるのではないかと考えた．7.3 節において，公開されている軍事行動に関するドキュメントから軍事行動における偵察活動について述べ，7.4 節において，サイバー空間における偵察活動の要件の例について述べる．

7.3 軍事行動における偵察活動の特性

軍事行動の基本的な方針はドクトリンと呼ばれる[23]．インターネット上で入手可能であり偵察活動に関する記載のあるドクトリンの一つにアメリカ合衆国陸軍の Field Manual 6(FM6)[24]がある．FM6 では，任務を達成する上で考慮すべき点(Mission Variable)として，達成すべき任務(Mission)，敵(Enemy)，地形と気象(Terrain and Weather)，効果的な友軍と支援(Troops and Support Available)，有効な時間(Time Available)，民間への考慮(Civil Considerations)を挙げている．偵察に関する記述は敵(Enemy)の中に存在し，敵に関して各方面から情報を得ることや偵察する必要性が記載されている．

偵察活動の実施方法は，敵に悟られずに情報収集を試みる狭義の偵察のほかに，敵に対してわざと気付かれるような行動を取って相手の出方を観測する威力偵察に区分されるとされる[25]. 偵察活動は，任務の達成に必要な情報を得るための活動であることから，活動の結果が任務の達成に悪影響を与えてはならないと言える．

7.4 サイバー空間における偵察活動の要件

表 9　サイバー空間における偵察活動の要件例

要件 1	サイバー攻撃の目標に関する情報をあらゆる方面から集めること
要件 2	サイバー攻撃の目標に対策を取られない範囲で偵察活動を行うこと

伊東は，各国の軍事組織は従来のサイバー空間におけるドクトリンを開発していると見解を述べている[26]．サイバー空間における軍事活動は，従来の軍事組織が実施する．そのため，サイバー空間におけるドクトリンは，従来の組

織構成や組織文化等に適して作成されていると考えられる．すなわち，既存のドクトリンをサイバー空間におけるドクトリンに応用したのではないかと考えられる．

サイバーキルチェーンが軍事行動をモデルに作成したように，軍事行動における偵察活動も，サイバー空間における偵察活動に適用できるのではないかと筆者らは考えた．

上記の議論を踏まえ，7.4 節で述べた軍事行動における偵察活動をサイバー空間における偵察活動に応用した際の要件の例を表 9 に示す．今後は，この要件の妥当性について検討を進め，偵察活動の捕捉に努めたい．

7.5 サイバー空間における敵情分析に向けて

現代のサイバーセキュリティ対策は，サイバーキルチェーンにおける 7 つのフェーズの内，3 段階目である配送(Delivery)以降で攻撃と識別できた事象に基づいた対策案の組み合わせを基本としている．一方で攻撃者は表 9 に示す要件を満たす偵察活動で得た情報に基づいて最適な攻撃手法を用いて検知されにくいサイバー攻撃を実施していると考えられる．このような状況から，今後の高度なサイバー攻撃は，より一層検知が難しくなると考えられる．

そこで筆者らは，サイバーキルチェーンにおける偵察活動を捉る敵情分析が必要であると考える．今後は，今回の提案手法に基づいたリアクティブセンサーを実装した上でインターネットノイズの観測を行い敵情分析に向けた検討を進めたい．

8. まとめ

本研究では，サイバー攻撃の初期段階を捉えることを目的として，インターネットノイズの発信源の分類に取り組んだ．パッシブセンサーで 180 日間に渡って観測したインターネットノイズを調査した結果，通信プロトコルや宛先の TCP ポートによって発信源における発信回数と観測期間に偏りが存在することを確認した．この偏りを可視化する手法を提案し，発信源の分類ができる可能性が高いことを確認した．インターネットノイズのようなインターネット上の活動の中には，サイバーキルチェーンにおける偵察活動が含まれている可能性があり，こうした攻撃者の活動を捉えることの重要性を示した．

今後は，今回提案した発信源の分類手法に基づいて応答内容を決定するリアクティブセンサーを実装し，偵察活動の捕捉に取り組みたい．

参考文献

[1] David W. Richardson, Steven D. Gribble, Edward D. Lazowska : The limits of global scanning worm detectors in the presence of background noise, WORM '05 Proceedings of the 2005 ACM workshop on Rapid malcode, pp. 60-70, 2005.
[2] “Internet background noise”. http://malwareanalysis.tech/category/internet-background-noise/, (参照 2017-05-08).
[3] 芦野佑樹, 島成佳：インターネットノイズに対する偽装応答機能の実装と観測に基づいた意図が不明なリクエストに関する考察, SCIS2015, 2015.
[4] “Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform”. http://lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.PDF, (参照 2017-05-08).
[5] 中尾康二, 井上大介, 衛藤将史, 吉岡克成, 大高一弘：ネットワーク観測とマルウェア解析の融合に向けて-インシデント分析センター –nicter-, 情報処理学会論文誌第 50 第 3 号, pp. 235-242, 2009.
[6] “国際連携によるサイバー攻撃予知・即応技術の研究開発”. http://www.soumu.go.jp/main_content/000427055.pdf, (参照 2017/05/08).
[7] “Dionaea”. https://github.com/DinoTools/dionaea, (参照 2017-05-08).
[8] Yoichi Shinoda, Ko Ikai, Motomu Itoh : Vulnerabilities of passive internet threat monitors, 14th USENIX Security Symposium, pp. 209-224, 2005.
[9] ゴ・キムクォン, 中村 康弘：走査活動観測に基づくネットワーク攻撃意図の推定, CSS2016, pp. 403-407, 2016.
[10] 水谷正慶：長期的な攻撃元ホストの振る舞い調査, CSS2016, pp. 1033-1039, 2016.
[11] “TCP/IP の再送タイムアウトの最大値を変更する方法”. https://support.microsoft.com/ja-jp/help/170359/how-to-modify-the-tcp-ip-maximum-retransmission-time-out, (参照 2017-05-08).
[12] ”特定の TCP ポートで受信待ちするようにサーバーを構成する方法 (SQL Server 構成マネージャー) “. https://msdn.microsoft.com/ja-jp/library/ms177440.aspx, (参照 2017-05-08).
[13] 清水光司, 小刀稱知哉, 池部実, 吉田和幸：SSH パスワードクラッキング攻撃におけるデータサイズを用いる検知手法の提案と運用評価, 情報処理学会論文誌 Vol.58 No.3, p.695-707, 2017.
[14] “警察庁セキュリティポータルサイト@policeーインターネット定点観測”. https://www.npa.go.jp/cyberpolice/detect/observation.html, (参照 2017-05-08).
[15] “NICTER WEB 2.0”. http://www.nicter.jp/, (参照 2017-05-08).
[16] “Service Name and Transport Protocol Port Number Registry”. https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml, (参照 2017-05-08).
[17] 佐々木良一, 石井真之, 日高悠, 矢島敬士, 吉浦裕, 村山優子：多重リスクコミュニケータの開発構想と試適用, 情報処理学会論文誌第 46 第 8 号, pp.2120-2129, 2005.
[18] 金子紀之, 佐々木良一：イベントツリー分析法に基づく標的型攻撃の分析評価ツールの開発と適用, 2013-DPS-154, pp.1-7, 2013.
[19] “2015 年第 2 四半期　セキュリティラウンドアップ”. http://www.trendmicro.co.jp/jp/security-intelligence/sr/sr-2015q2/index.html, (参照 2017-05-08).
[20] FireEye. M-TRENDS 2016. 2016.
[21] “ネットワークビギナーのための情報セキュリティハンドブック Ver.2.11”. https://www.nisc.go.jp/security-site/handbook/index.html, (参照 2017-05-08).
[22] “高度サイバー攻撃への対処におけるログの活用と分析方法”. https://www.jpcert.or.jp/research/APT-loganalysis_Report_20161019.pdf, (参照 2017-05-08).
[23] 田村尚也：各国陸軍の教範を読む, イカロス出版, 2015
[24] “FM-6, COMMANDER AND STAFF ORGANIZATION AND OPERATIONS Appendix A OPERATIONAL AND MISSION VARIABLES”. http://www.milsci.ucsb.edu/sites/secure.lsit.ucsb.edu.mili.d7/files/sitefiles/fm6_0.pdf, (参照 2017-05-08).
[25] あかぎひろゆき：戦車男入門: 元陸上自衛官だから語れる戦車論, Panda Publishing, 2016.
[26] 伊東寛：第 5 の戦場, 祥伝社, 2012.