Vol.2018-CSEC-82 No.40
Vol.2018-SPT-29 No.40
2018/7/26

インターネットに接続された サイバー攻撃観測用センサーの環境に関する考察

芦野佑樹[†1]　鮫島礼佳[†1]　須堯一志[†1]　矢野由紀子[†1]　中村康弘[†2]

概要：近年，インターネット経由のサイバー攻撃が深刻化しており社会問題となっている．サイバー攻撃に対処するためには，サイバー攻撃に関する通信の分析に基づいたセキュリティ対策が必要であることから，サイバー攻撃に関する通信を観測するセンサーの研究が行われている．本論文では，サイバー攻撃を観測することを目的としたセンサーの設置環境について1,700のグローバルIPアドレスに設置したセンサーが観測したデータセットの分析を通じて考察を行う．その結果，センサーの数，観測期間，グローバルIPアドレスによって観測できる内容に差があることを確認できたので報告する．併せてセンサーの設置に関して考慮するべき点を考察したので併せて報告を行う．

キーワード:サイバー攻撃, 観測, センサー, 発信源数, グローバルIPアドレス

Consideration About Internet Sensor Environment for Observation of Cyber Attack Packets

YUKI ASHINO[†1]　AYAKA SAMEJIMA[†1]　KAZUSHI SUGYO[†1]
YUKIKO YANO[†1]　YASUHIRO NAKAMURA[†2]

Abstract: Sensors which are connected the Internet can obtain and store packets of cyber-attakcs. In order to obtain many types of cyper-attacks, sensor must be operated to obtain packets on many global IP addresses for long terms. However sensors operation costs are increase by count of sensor and observation term. In this paper, considering sensor operation based on analyze data set which observation Internet noises using about 1,700 global IP addresses.

Keywords: Cyber-attacks, Observation, Internet Sensor, Number of Source IP Addresses, Global IP Address

1. はじめに

インターネット経由で行われるサイバー攻撃(以下，「サイバー攻撃」)は年々巧妙化しており，その被害は増加傾向にあるとされる[1].

しかし，どのような巧妙なサイバー攻撃であっても，サイバー攻撃に関する通信(以下，「攻撃通信」)を伴うのであれば通信規約に則った通信が必ず発生する．インターネットを経由した通信を伴うものであれば，攻撃通信はIP(Internet Protocol)に則っている必要があり，IPに則った通信データ(以下，「IPパケット」)として必ず観測される制約がある．

さらに，サイバー攻撃は，人の意思が介在して行われるとさており[2]，その意思を事前に把握することは非常に困難である．したがって，サイバー攻撃はその発生を事前に把握することは困難であるといった特徴を持つ．

以上の制約と特徴から，インターネットに接続されたコンピュータは，常にサイバー攻撃を受ける可能性があり，送り付けられた攻撃通信は必ず観測できる性質を持っていると言える．このような性質から，センサーと呼ばれるインターネットに接続されたコンピュータを用いた攻撃通信を観測する研究が存在する．

サイバー攻撃は年々巧妙化していることから攻撃通信も同様に日々変化していると考えられる．セキュリティ対策のために，センサーはできるだけ多くの種類の攻撃通信を補足することが望ましいと言える．

しかし，センサーに割り当てたグローバルIPアドレスや観測期間といった環境によって観測できる通信内容に差が存在することが知られている[3][4][5]．センサーに割り当てられるセンサー数や観測期間は，経済的な範囲に抑えられることから，センサーを設置した環境に関する評価は必要である．

そこで筆者らは，筆者らのセンサーによって観測された通信データの分析を通じて，センサーの環境について考察を行ったので報告を行う．

2. サイバー攻撃の制約と特徴

インターネットを経由した通信は，通信規約であるIP(Internet Protocol)に必ず則る必要がある．したがって，どのような巧妙なサイバー攻撃であっても，インターネット

†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
Cyber Security Factory, National Security Solution Division, NEC Corporation.

†2 防衛大学校情報工学科
Computer Science, National Defense Ascademy

を経由した攻撃通信であればIPに則った通信データ(以下,「IP パケット」)の存在自体を隠すことができない. 一方で, サイバー攻撃は，人の意思が介在していることから，人の考えを事前に把握できない以上はサイバー攻撃の発生を事前に知ることができないといった特徴を有している．

本節では，攻撃通信の制約と特徴を述べる．

2.1 通信規約による制約

ある 2 点間で情報の交換を目的とした情報通信は，手順や書式を定めたプロトコルが存在する．インターネットを介した 2 つのコンピュータ同士の情報通信は，IP に則って通信する必要がある．IP の詳細な内容は RFC791[6]に記載されている．なお，本論文では特に断りがない限り IP を RFC791 に記載されているバージョン 4 として扱う．

IP は，コンピュータの識別に IP アドレスと呼ばれる 32 ビットで表現された識別情報を用いる．インターネットに直接接続されたコンピュータに割り当てる IP アドレスは，特にグローバル IP アドレスと呼ばれており重複することなく各コンピュータに割り当てられる．

したがって，インターネット上に接続されたコンピュータに攻撃通信を送る場合は，攻撃目標となるコンピュータにはグローバル IP アドレスが割り当てられている必要がある．

これは，どのような巧妙なサイバー攻撃であったとしても，インターネットを介してインターネットに接続されたコンピュータに対して送られる攻撃通信は，IP の制約から逃れることができず，攻撃通信の存在を隠すことができない特性を持つ．

2.2 事前予測が困難である特徴

通信は，異なる二者間の情報交換であるとされシュラムモデルで表現されることがある[7]．シュラムモデルに基づけば，通信は自然発生するものではなく人の意思が存在するとされる．したがって，サイバー攻撃も同様に人の意思が存在していると言え，攻撃通信モデルの検討がされている[2]．人の意思は通信が事前に他者が知ることがないので, サイバー攻撃も同様にその発生は事前に把握することが困難と言える．

以上のことから，サイバー攻撃は基本的に事前にその存在を把握することが困難という特徴がある．

3. 本研究の位置づけ

3.1 サイバー攻撃を観測するためのセンサー

2.1 節で述べた制約から, サイバー攻撃に伴う攻撃通信が自分のコンピュータに対して送信された場合は，IP パケットとして必ず観測できると言え，tcpdump[8]などに代表されるキャプチャリングツールを用いることで記録することが可能である．

2.2 節の特徴から, 攻撃通信の宛先や観測時刻を事前に把握することができない．その一方でインターネットに接続しているコンピュータは常に攻撃通信によって送り付けられる可能性があると言える．

以上のことから，インターネットに接続したコンピュータは，インターネットを経由して自分宛に送られた攻撃通信を必ず観測できる性質を持っていると言える．

この性質から，インターネットに直接接続されたコンピュータがサイバー攻撃を観測することを目的としたセンサーとして扱われることもある．

3.2 関連研究

本節では，攻撃通信を観測するセンサーと呼ばれるインターネットに接続されたコンピュータを用いた関連研究について述べる．

池部らは，クラス C 相当のアドレス空間に設置したハニーポットで観測した攻撃通信を分析している[3]. 池部らのセンサーは，第 4 オクテットが 3 から 253 までの計 251 個のアドレスが割り当てられており, 複数のグローバル IP アドレスで観測することで IP アドレスによって観測されるパケット数や，TCP パケットの宛先ポート番号に差があることを示している．

橋本らは，2 か月間に渡り/16 の未使用のグローバル IP アドレスで観測した約 26 億パケットを分析している[4]. このように長期間に渡る観測結果の分析から，1 か月以上に渡り特定の属性値を持つパケットが増えるといった現象を報告している．

沖野らは，観測されるサイバー攻撃の種類は，センサーに割り当てたグローバル IP アドレスの過去の用途に依存していることを示している[5].

サイバー攻撃は年々巧妙化していることから攻撃通信も同様に日々変化していると考えられる．セキュリティ対策のためには，できるだけ多くの種類の攻撃通信を観測する必要があると言える．

多くの種類の攻撃通信を観測するためには，上述した関連研究のとおり, できるだけ多くのグローバル IP アドレスをセンサーに割り当て，できるだけ長期間に渡り観測し，かつ，センサーによって観測された攻撃通信の差を分析できるような形が望ましいと言える．

3.3 本論文の領域

本論文の目的は，インターネットに設置したセンサーが攻撃通信を観測する際に考慮するべき環境について考察を行う．

以下に，本論文の領域における，センサーが観測する対象や, 分析する観点および IP パケットにおける分析する属性について述べる．

3.3.1 センサーが観測する通信データの対象

攻撃通信をできるだけ多く観測する必要があるが，実際

に攻撃通信であるかを識別することは観測時点で判断できるとは限らない．実際に，インターネット上にはインターネットノイズと呼ばれる意図が不明な通信が存在し[9]，その中には組織的に開発された大規模な分散システムによって発信されていると推定される通信も確認されている[10]．したがって，本論文におけるセンサーが観測するべき通信の対象は，センサー宛のすべての通信とする．

3.3.2 センサーの環境と分析する観点

インターネットノイズの発信源には，1 つのグローバル IP アドレス数だけを宛先にするものからネットワーク全体に対するものがあったり[11], 3 秒ほどの短期間で発信を止めるものから数か月以上にも渡っての発信を継続するものが存在する[12]. したがって, センサーに割り当てたグローバル IP や観測期間などのセンサーの環境によって観測できる攻撃通信に差が生じることが知られている．

そこで筆者らは，センサーがサイバー攻撃を多く観測できるように設置されていることを評価できるようにするためには, センサーに割り当てたグローバル IP アドレスや観測期間といったセンサーの環境についての評価が必要であると考えた．

本論文では, センサーに割り当てたグローバル IP アドレスや観測期間をセンサーの環境と定義し，多くの攻撃通信を観測することを目的として，筆者らのセンサーによって観測された通信から表 1 に示す関係を明らかにするものである．

表 1　分析の観点

(1) センサー数と観測できる通信の種類
(2) 観測期間と観測できる通信の種類
(3) センサーごとに観測できる通信の種類

上記の関係を明らかにした上で，効率の良いセンサーの設置方法について検討する．

3.3.3 分析対象の IP パケットの属性

筆者らは，センサー宛に送られる通信は送信プログラムに依存しており, 通信の発信元 IP アドレスおよび宛先における送信回数や観測されている期間によって分類ができる可能性を示している[12].

以上のことから, 本論文で分析対象とする IP パケットの属性を表 2 に示す.

表 2　分析対象

(1) IP パケットの受信時刻
(2) 発信元 IP アドレス
(3) 宛先 IP アドレス
(4) プロトコル番号

4. データセット

本章では，筆者らがインターネット上に設置したセンサーによって観測した通信データ(以下,「データセット」)を用いて 3.3.2 で述べた観点で分析を進める．

4.1 概要

筆者の一人が所属する組織が管理している到達可能なネットワークの内, センサーとして利用が可能な IP アドレスにセンサーが設置されている. このグローバル IP アドレスは，観測時点でサーバ等の運用はされておらず，ドメイン等の登録も行っていない．そのため，このセンサー宛に送られた通信は，正規のユーザから発せられたものとは考えにくく，攻撃通信である可能性も否定できない．このことから，本論文では，3.3.1 で述べたとおり，センサー宛の通信をすべて分析する．

表 3　データセット概要

データ形式	pcap(1 日 1 ファイル)
観測期間	2017/12/01～ 2018/04/30(151 日間)
グローバル IP アドレス数	約 1,700 個
容量	約 2.73TB
パケット数	約 256.7 億パケット
ユニーク IP アドレス数 (発信源数)	約 1,333.6 万個

センサーに割り当てている IP アドレスは, ほぼ連続した約 1,700 の IP アドレスであり，インターネット側から TCP の SYN パケットを受信した場合，発信元の IP アドレスに対して SYN/ACK を応答する機能を持つ[11].

本論文で使用するデータセットは，表 3 に示すとおり 2017 年 12 月 1 日から 2018 年 4 月 30 日に至るまでの 151 日間で，パケット数は約 256.7 億であった．観測期間中，1,333.6 万の発信元のユニーク IP アドレス(以下,「発信源」)を観測できた．

データセットにおけるプロトコルごとのパケット数および割合を表 4 に示す. 全体の 99.0%が TCP/IP の通信であり，それ以外は 1.0%であった．

表 4　プロトコルごとのパケット数と割合

プロトコル名	パケット数(割合%)
UDP/IP	約 1.7 億パケット(約 0.67%)
TCP/IP	約 253.1 億パケット(約 99.0%)
それ以外のプロトコル	約 0.6 億パケット(約 0.37%)

4.2 パケット数の時間変化

観測期間中に各センサーが観測した 1 日当たりのパケット数の推移を図 1 に示す.

1 日当たりで観測した最大のパケット数は 2018/04/26 の

Vol.2018-CSEC-82 No.40
Vol.2018-SPT-29 No.40
2018/7/26

約 3.0 億パケットであった．図 1 中には，観測されたパケット数が記されていない日がある．これはセンサーが停止しており観測できなかった欠測が 24 時間以上継続していたことが原因である．観測パケット数が 0 の日は 13 日あったため，実質的な観測日数は 137 日であった．なお，本論文では 24 時間未満の欠測時間は無視する．

実質観測日数が 137 日であったことから，1 日当たり平均して約 1.9 億パケット(256.7 億パケット/137 日=約 1.9 億パケット/日)を観測しており，1 アドレス 1 日平均では約 11.9 万パケット(1.9 億パケット/1,700 センサー=約 11.9 万パケット/センサー)を観測している．

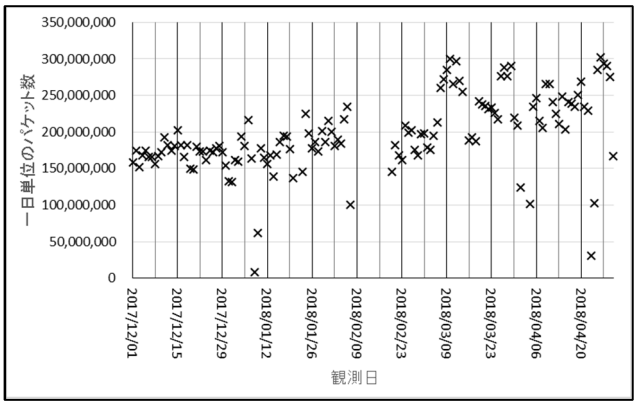

図 1　日単位の観測したパケット数

4.3 ユニーク送信数の時間変化

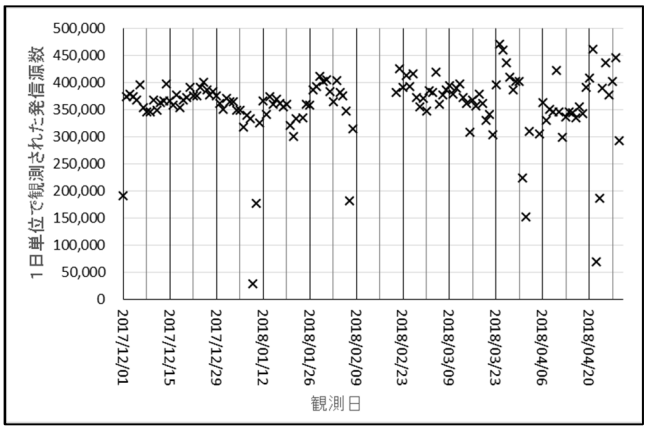

図 2　日単位の観測した発信源数の推移

図 2 は，日ごとに観測された発信源数を示したものである．なお，同一の発信源であっても異なる日で観測されていれば，それぞれの日で 1 個の発信源として扱う．

最も発信源数が多く観測された日は，2017/12/02 であり約 60.6 万の発信源が観測された

5. 分析

本章では，第 4 章で述べたデータセットを 3.3.2 で述べたセンサーの環境を分析する観点に基づいて分析した結果を述べる．

5.1 センサー数と観測できる発信源数

センサー数によって観測される発信源数の分析手順を表 5 に示す．

表 5　センサー数と観測できる発信源数の分析手順

(1) センサーはほぼ連続したグローバル IP アドレスが割り当てられているので，各センサーのグローバル IP アドレスと最も小さいグローバル IP アドレスの差をセンサーID と定義する
(2) センサーID:0 から 1 個ずつセンサーID を増やしていきそのセンサー群で観測された発信源数を調査する

表 5 の手順に基づいた分析について，横軸にセンサー数とし縦軸が観測された全発信源数に対する累積度数として図 3 に示す．図 3 が示すとおり，センサー数と発信源数は比例しない傾向が確認された．

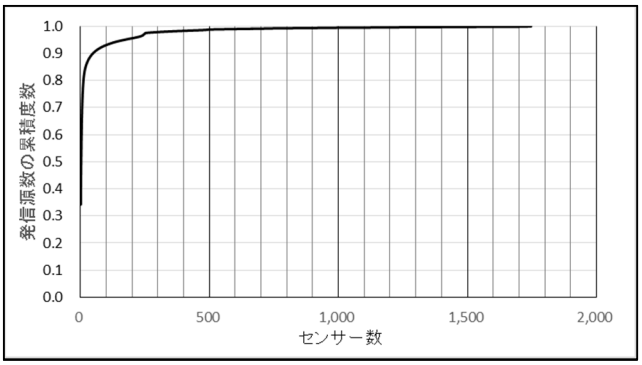

図 3　センサー数と発信源数の関係

表 6　センサー数と観測できる発信源数の割合

センサー数(個)	発信源数(個)	全体の発信源数との割合(%)
1	4,565,585	34.2
4	8,097,413	60.7
10	10,477,251	78.6
100	12,414,123	93.1
200	12,745,624	95.6
400	13,109,299	98.3
800	13,237,794	99.3

表 6 は，上記分析結果の内，特に特徴のあるセンサー数と発信源数の割合について示したものである．表 6 の通り，センサー数が少ない場合は，センサー数の増加に伴い観測される発信源数も増加するが，センサー数が大きくなるにつれ観測できる発信源数は増え方が鈍化する．例えば，センサー数が 100 個で観測される発信源数は全体の 93.1%であるが，200 個に増やしても観測できる発信源数は全体の 95.6%となり，100 個との差は 2.5%の増加のみとなる．したがって，センサーの数が多くなるほど観測でき

Vol.2018-CSEC-82 No.40
Vol.2018-SPT-29 No.40
2018/7/26

る発信源数の増え方は鈍化する傾向になることがわかった.

5.2 観測期間と観測できた発信源数

観測日数と観測された発信源数の累積度数を図 5 に示す. 観測された発信源数は 1,333.7 万であった.

観測日 70 日目から 84 日目近辺の線が途切れているように見えるのは，欠測の日が連続して続いたためである．欠測の日を挟んでも，観測された累積の発信源数の割合は観測日と比例する傾向が続くことが確認できた．この傾向から，観測される発信源数は，観測を開始してからの時間ではなく，実際に観測した時間に比例することがわかった.

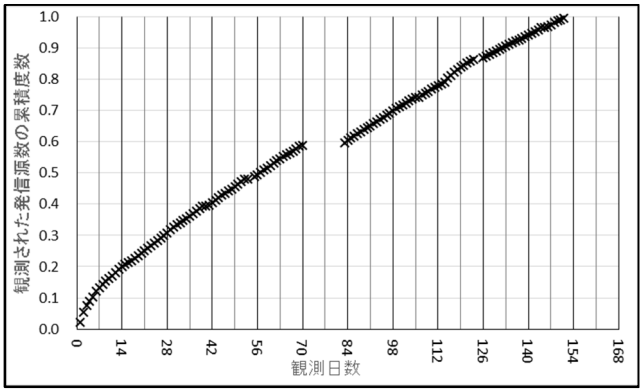

図 5　観測期間と発信源数の関係

5.3 センサーごとの観測された発信源数

個々のセンサーと観測した発信源数の関係を図 6 に示した. 横軸のセンサーID は，表 5 の(1)で示した方法で割り当てたセンサー名である．図 6 が示すとおり，一定の間隔で特徴的なカーブが描かれており, その間隔は 256 であった.

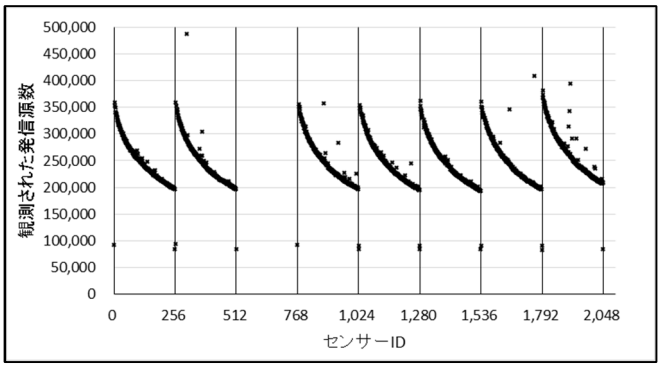

図 6　センサーごとの観測された通信の種類数

センサーID0 に割り当てられたグローバル IP アドレスの第 4 オクテットが 0 であったことから，第 4 オクテットごとに観測された発信源数を図 7 に示す.

観測された発信源数が最小であったのは第 4 オクテットが 255 の約 36.9 万であり，次に少なかった第 4 オクテットが 0 の約 40.7 万であった．それ以外はすべて 80 万発信源を観測しており最大は第 4 オクテットが 7 のときで 152.1 万発信源であった．また，全体として第 4 オクテットが大きくなるほど観測される発信源数は減少の傾向にあり, 0～63 の平均は約 127.0 万発信源であったのに対して 192～255 の平均は約 87.6 万発信源となりその差は約 1.4 倍であった.

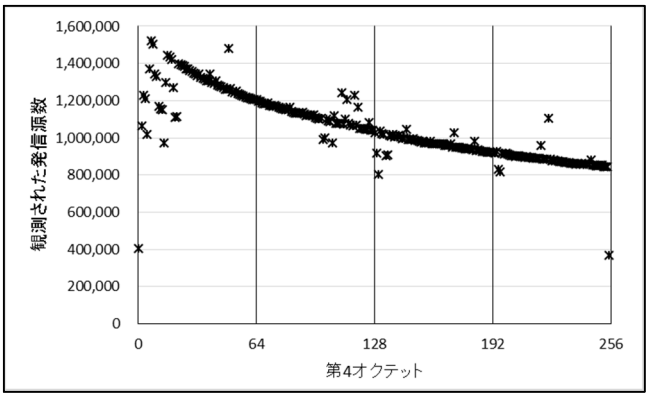

図 7　センサーの第 4 オクテットで集計

6. 考察

6.1 センサー数と観測された発信源数

5.1 節で述べたとおり，センサーの数を 5 以上に増やしても観測できる発信源の数が比例する傾向は得られなかった.

このような傾向は，同一の発信源からの通信を複数のセンサーが観測していることが原因であると考えられる．そこで，その原因を確かめるために，発信源ごとの宛先センサー数を集計した結果を図 8 に示す．図 8 は，横軸を同一発信源が送信したセンサー数とし，縦軸を宛先センサー数における全発信源の累積度数を示した．その結果から 1 個のセンサーのみに送付する発信源は全体の 34.2%であり, 2 回以上送信する発信源は全体の 65.8%存在した.

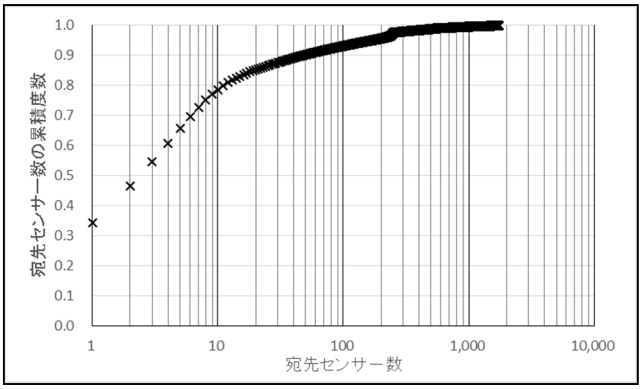

図 8　発信源における宛先センサー数の関係

実際にインターネット全体を探索するような通信は過去に確認されている[13][14]．このため，センサー数を増やしても同一の発信源からの通信を補足してしまい，結果としてセンサー数と観測される発信源数は比例しないものと考えられる.

6.2 観測時間と発信源数

5.2 節で述べたとおり, 観測期間と観測された発信源数は比例の関係であることがわかった．同一の発信源が長期間

利用されていれば，観測期間を長くするほど観測される累積の発信源数の伸びは観測時間に比例しなくなると考えられる．そこで，本節では 5.2 節で示した傾向の原因を探るため，各発信源の観測され続けた時間を分析した．

観測され続けた時間を分析するに当たり，水野が定義した発信源の振る舞いに関する評価指標の一つである活動時間[15]を参考にする．活動期間 T_a は，1 個の発信源から初めて通信が観測された時刻 T_b と定義し最後に観測された時刻 T_e の差として定義される(式 1).

$$T_a = T_e - T_b \quad \text{(式 1)}$$

観測された全発信源の活動期間の分析結果について，縦軸に全発信源における累積度数，横軸に活動期間を秒として図 9 に示す．1 パケットしか発信しない発信源の活動期間は 0 秒とした．図 9 のとおり，全発信源の 50%は活動期間が 20,000 秒(5 時間 33 分 20 秒)以下であった．また，活動期間が約 1 日(図中 86,000 秒(24 時間×60 分×60 秒=1 日))となる発信源の割合は全体の 59.6%であることがわかった．

このことから，観測期間を長くすると，活動期間が 1 日以下となるような短命な発信源が多く観測され，結果として観測期間と発信源数が比例すると考えられる．

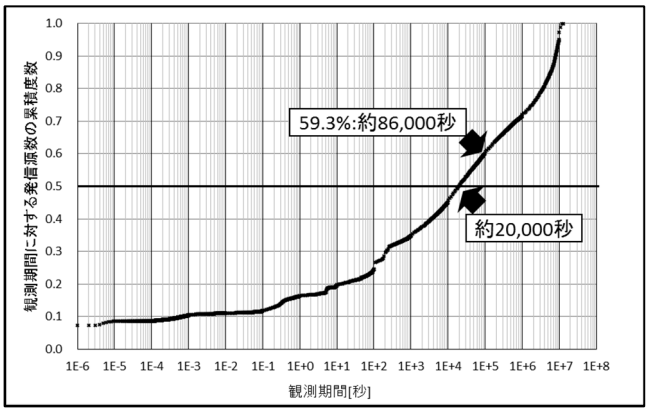

図 9　全発信源の活動期間の累積度数分布

しかし，グローバル IP アドレスは有限であることから，今回のデータセットにおける観測期間よりもさらに長期間観測にすることで，観測される発信源数の伸びは観測期間に比例しなくなると考えられる．

一方で，グローバル IP アドレスの用途は恒久的ではなく，特にクラウド事業者のグローバル IP アドレスは，長期間観測している間に利用者が入れ替わることが考えられる．

したがって，発信源の活動期間の分析については，発信源の IP アドレスが同一の用途で利用される期間を考慮する必要があるものと考えられる．

6.3 割り当てるグローバル IP アドレスと発信源数

5.3 節で述べたとおり，センサーに割り当てたグローバル IP アドレスの第 4 オクテットが 0 や 255 で観測された発信源数は，ほかの第 4 オクテットのアドレスよりも少なかった．本節では，第 4 オクテットが 0 と 255 のときに観測された発信源数の原因について考察する．

第 4 オクテットが 0 や 255 宛の発信源が少ない理由として，BGP と呼ばれるインターネットの経路制御で扱う最大のサブネットマスクが/24 であった時代の名残である可能性が考えられる．2014 年にサブネットマスクが最大で/28 になるアナウンスが ARIN(American Registry for Internet Numbers)[16]からなされるまでは/24 でインターネットの経路制御は管理されていた[17]. そのため，発信源で動作するプラムのいくつかは第 4 オクテットが 0 や 255 を避けるように実装されているのではないかと考えた．

宛先 IP アドレスの第 4 オクテットを 255 とする発信源が少ないもう一つの理由としては，UDP/IP パケットであった場合に Fraggle Attack と呼ばれる攻撃[18]として IDS に検知されることを避けていた可能性も考えられる．

このようにセンサーに割り当てたグローバル IP アドレスの第 4 オクテットによって観測できる発信源に差が存在していることから，センサーを設置する際は第 4 オクテットへの考慮が必要である．

6.4 ほかのセンサーでの観測

6.1 節から 6.3 節の考察は，第 4 章で観測された発信源の傾向を示したに過ぎない．

そこで本節では，ほかのセンサーで同時期に観測したデータセットの分析を通じて 6.1 節から 6.3 節で述べた傾向と同様になるのかを調査した．筆者らが別途保有している 7 か所のセンサーが観測したデータの分析を通じて考察する．

表 7　データセット B の概要

データ形式	pcap (1 センサー1 ファイル)
観測期間	2018/05/01～2018/06/01 (32 日間)
グローバル IP アドレス数	約 7 個
容量	約 2.2GB
パケット数	約 1,198.9 万パケット
ユニーク IP アドレス数 (発信源数)	約 31.0 万個

本論文では説明しやすいように，本節で述べる 7 か所で観測したデータセットをデータセット B と称し概要を表 7 にまとめる．データセット B における各センサーが観測したパケット数やプロトコルの種類を図 10 に示した．最も多くのパケットを観測したのはセンサーA であり約 526.1 万パケットを観測しているが，最小のセンサーG は約 66.1 万パケットを観測であった．また，観測できたパケットの種類に関しては，センサーA は 93.0%が UDP/IP である一方で，センサーF は 99.5%が TCP/IP であった．

以上のことから，センサーごとに観測される通信の種類に差があることが確認できた．

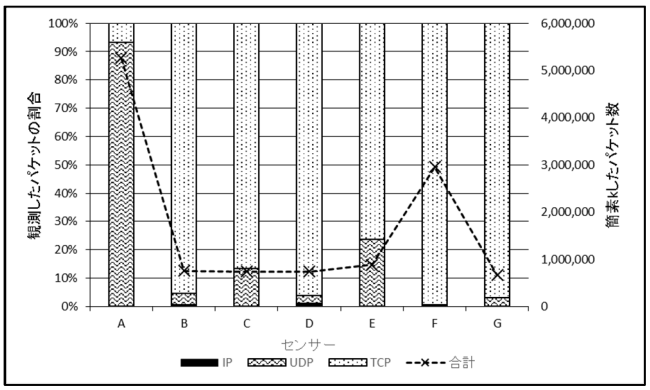

図 10　センサーごとのパケットの種類とパケット数

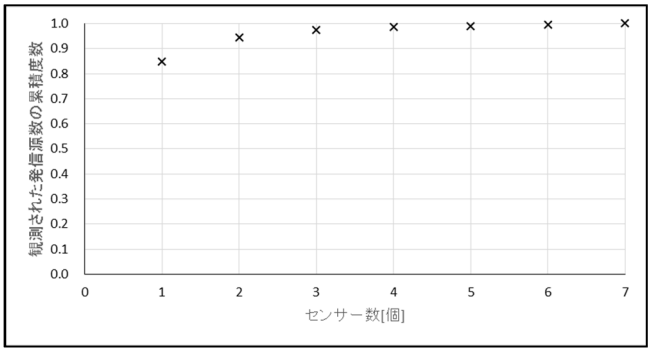

図 11　センサー数と発信源数の関係

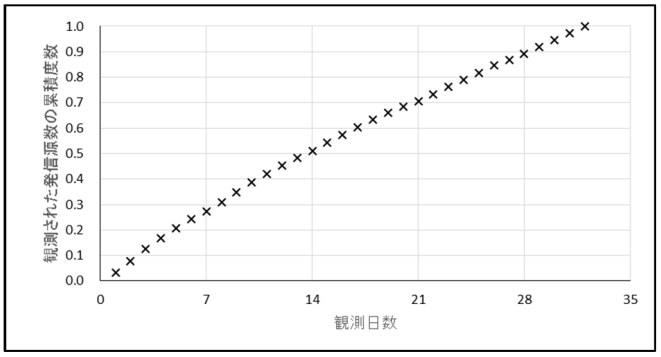

図 12　観測日数と観測された発信源数の推移

データセットBにおけるセンサー数と発信源数の関係を5.1 節で述べた方法で分析した結果を図 11 に示す．

この結果から，データセット B でも 5.1 節と同様の傾向があることがわかった．センサーが 1 個のときで観測できた発信源数の割合が 84.4%であり，表 6 で示した数値よりも大きかった．このことから，データセット B には，複数のグローバル IP アドレスに対して通信を発信する発信源からの IP パケットが多く含まれていたと考えられる．

しかし，単純に観測期間がデータセット B は，データセットの観測期間に対して約 5 分の 1 であった．そのため，データセットの観測期間を 5 倍に増やして分析した場合，表 3 と同じような数値になっていた可能性もあるので今後の課題としたい．

次に，観測期間と観測された発信源数の累積度数を図 12 に示した．この結果から，5.2 節で示したとおりデータセット B も観測期間に比例することがわかった．

以上のことから，第 4 章の述べたデータセットとデータセット B の傾向は定性的に同様である．したがって，インターネット上に設置したセンサーは，6.1 節から 6.3 節で述べたような傾向を示す可能性が高いと考えられる．

6.5 センサーを設置する際の考慮すべき点

6.4 節までの議論に基づいて，センサーを設置する際の考慮するべき点について述べる．

(1) センサー数と観測できる種類は比例しない

筆者らの分析結果から，センサー数と観測できる発信源数は比例しない傾向があることが確認された．

センサー数は，確保したグローバル IP アドレス数と同義であることから，センサー数と観測期間に比例してセンサーの運用にはコストがかかる．詳細な運用コストについては，ネットワークを管理している組織や契約業者によって観測期間を変数にした関数として表現できると考えられる．併せて，観測できた 1 つの発信源数に対する価値を定義した上で，費用対効果の見積もりを実施する必要性があると考える．今後は，費用対効果の定量的な方法についての分析も進めていきたい．

(2) 観測期間と観測できる発信源数は比例する

発信源の約 59.3%が，1 日以下の活動期間であることから発信源は 1 日程度で役目を終えて破棄されるものと推定される．したがって，観測期間は可能な限り長く設定するべきであると考えられる．

(3) IP アドレスによって観測できる発信源数は異なる

連続したグローバル IP アドレスであっても離れたグローバル IP アドレスであっても，アドレスによって観測される内容に差がある．したがって，IP アドレスによる観測される内容の差を分析できるようにしておく必要がある．

(4) 大容量の分析に備える

サイバー攻撃は今後も巧妙化し続けることが予想されることから，より多くのセンサーによる長期間の観測をし続ける必要があると考えられる．その結果，分析対象はより大容量になるものと予想される．大容量の観測データを分析するためには，第一段階としてマクロ的な解析を通じて詳細に解析をする対象の絞り込みを図った後，第二段階として絞り込んだ対象をミクロ的に解析するといった手法[19]が有効であると考えられる．

さらに，発信源からの通信をより詳細に分析するためには，IP パケットの特定の属性だけではなく TCP のペイロード等を分析対象として扱う必要がある．

今後は，大容量のデータをより詳細に分析した結果に基

づいた考察の実施を考えている．

7. まとめ

本論文では，インターネットを経由したサイバー攻撃を観測する必要性について述べた．また，センサーに割り当てたグローバル IP アドレスや観測期間といったセンサーの環境によって観測できるサイバー攻撃に関する通信の種類に変化がある可能性があることについて述べた．センサーの環境を評価することは，効率の良いセンサーの設置を計画できる可能性があることから，本論文では筆者らの設置したセンサーで観測したデータを用いて通信の発信源の分析を行った．また，分析結果に基づいて，センサーの設置をする際に考慮するべき点について考察をした．

今後はよりセンサーを長期間運用した結果や，IP パケットの属性値以外のデータ分析が必要となる可能性があることから，大容量の通信データの分析をしていきたい．

参考文献

[1] https://www.npa.go.jp/hakusyo/h29/, (参照 2018-06-20 確認).
[2] 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 論文集, 2017(2), 2017.
[3] 池部実, 宮崎桐果, 吉田和幸. ハニーポットによる大分大学におけるダークネット宛通信の分析. 情報処理学会研究報告. IOT, [インターネットと運用技術] 2015-IOT-29(17), 2015, p.1-8.
[4] 橋本直輝, 小澤誠一, 班涛, 中里純二, 島村隼平. ダークネットトラフィックデータの頻出パターン解析. 研究報告コンピュータセキュリティ(CSEC), 2017-CSEC-78(6), p.1-8.
[5] 沖野浩二, 片山昌樹, 占部優希. IP アドレスの履歴が攻撃に与える影響に関する考察. コンピュータセキュリティシンポジウム 2014 論文集, 2014(2), 2014, p.56-63.
[6] https://tools.ietf.org/html/rfc791, (参照 2018-06-20 確認).
[7] Wilbur Lang Schramm. The Process and Effects of Mass Communication. Univ of Illinois Pr; Revised edition, 1971.
[8] https://www.tcpdump.org/, (参照 2018-06-20 確認).
[9] 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, 2005, p.60-70.
[10] 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 暗号と情報セキュリティシンポジウム, 2015.
[11] 中村康弘. 初期ペイロードに着目したネットワーク走査活動の分析. 第 79 回全国大会講演論文集, 2017(1), 2017, p.523-524.
[12] 芦野佑樹, 山根匡人, 矢野由紀子, 島成佳. 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. 研究報告コンピュータセキュリティ(CSEC), 2017, p.1-8.
[13] https://www.npa.go.jp/cyberpolice/detect/pdf/20140925-2.pdf, (参照 2018-06-20 確認).
[14] https://blog.erratasec.com/2014/09/bash-shellshock-scan-of-internet.html, (参照 2018-06-20 確認).
[15] 水谷正慶, 長期的な攻撃元ホストの振る舞い調査, コンピュータセキュリティシンポジウム 2016 論文集, 2016(2), 2016, p.1033-1039. https://ddos-guard.net/en/terminology/fraggle-attack-broadcast-udp-packets-attack, (参照 2018-06-20 確認).
[16] https://www.arin.net/, (参照 2018-06-20 確認).
[17] https://www.arin.net/vault/announcements/2014/20140130.html, (参照 2018-06-20 確認).
[18] https://ddos-guard.net/en/terminology/fraggle-attack-broadcast-udp-packets-attack, (参照 2018-06-20 確認).
[19] 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. SCIS2018 暗号と情報セキュリティシンポジウム, 2018.