サイバー攻撃観測用センサーの静的特性に関する考察

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：インターネットを経由したサイバー攻撃に伴う攻撃通信に対処するためには，攻撃通信の実体を入手し解析する必要がある．攻撃通信の実体を入手するための一つの方法として，センサーと呼ばれるコンピュータを用いて攻撃通信を観測する方法が知られている．センサー観測できる攻撃通信を含む通信内容は，観測対象である IPv4 のグローバル IP アドレスの利用状況に依存する動的特性が知られている．その一方で，筆者らは，5 か月間のデータセットの分析を通じて，観測できる通信内容がグローバル IP アドレスの第 4 オクテットに依存する静的特性が存在する可能性を示した．この偏りが長期間に渡り確認できるならば，センサーの動的特性に加えて静的特性に基づいた分析ができるようになるのではないかと考えた．本論文では，2 年 5 か月間のデータセットの分析を通じて，第 4 オクテットによる静的特性の存在を確認したので報告する．

キーワード：サイバー攻撃，パケット解析，センサー，第 4 オクテット，観測

A Study of Static Character of Internet Sensors for Cyber Attacks

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

Abstract: In order to counter measure for cyber attacks via Internet, it is necessary to obtain and analyze attack packets. One way to obtain attack packets is packets observation using attached Internet computers. Some researchers show that observation results are depended by a conditions of the global IP address. Authors found a dependency of observation result by fourth octet of the global IP address, named "Octet Pattern" using 5 months data set. This paper shows a presence of "Octet Pattern" by packets analysis of 2 years 5 months data set.

Keywords: Cyber-Attacks, Packet Analysis, Sensor, Fourth Octet, Observation

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(以下,「サイバー攻撃」)が脅威となっている[1]. サイバー攻撃への対処としては, サイバー攻撃に関する通信(以下,「攻撃通信」)をできるだけ早く検知し，攻撃通信による影響を最小限に抑えるよう対処するアプローチが必要である．攻撃通信を検知する代表的なものに，IDS(Intrusion Detection System: 侵入検知装置)がある[2].

IDS はシグネチャと呼ばれる攻撃通信の特徴を格納したデータベースを用いて，攻撃通信の存在を検知するものである．攻撃通信の特徴を得るためには，攻撃通信の実体を入手する必要がある．攻撃通信の実体の入手に関しては，攻撃通信を含めた通信を観測するコンピュータを用いる．

本論文では，攻撃通信を観測することを目的としたコンピュータをセンサーと呼ぶ.

センサーは， 観測対象である 1 つまたは複数のグローバル IP アドレスに対して送られる通信(以下,「インバウンドパケット」)や，その応答の通信(以下,「アウトバウンドパケット」)を観測する．なお，本論文では，グローバル IP アドレスは IPv4 として議論する．

攻撃通信がセンサーによって観測しているグローバル IP アドレスに対して送信された場合は，インバウンドパケットとして観測でき，結果として攻撃通信の実体の入手が期待できる．

しかしながら，センサーが観測できる攻撃通信は，観測対象であるグローバル IP アドレスに対するインバウンドパケットおよびアウトバウンドパケットに限られる．

グローバル IP アドレスの過去の利用状態によって観測できる攻撃通信に偏りがあることが知られている[3]. また，同一のグローバル IP アドレスを観測するセンサーを一方的にインバウンドパケットのみを観測するパッシブモードから，ある特定のインバウンドパケットに対して応答するリアクティブモードに切り替えることによって，観測できる通信の種類が変動する可能性があることも知られている[4].

このように, センサーの観測対象であるグローバル IP アドレスから発信されるアウトバウンドパケットが，インバウンドパケットに変化を与えたと言える．このような特性

†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 防衛大学校工学部通信工学科
Computer Science, National Defense Academy.

を本論文では，グローバル IP アドレスの動的特性と言う．

その一方で，筆者らは，センサーの観測対象であるグローバル IP アドレスの第 4 オクテットによってインバウンドパケットの発信源数に偏りがあることを確認している[5]．この傾向は，特定の期間にだけ存在している現象であることを否定できない．しかし，第 4 オクテットによる偏りが長期間に渡って存在するのであるならば，グローバル IP アドレスには第 4 オクテットによる静的特性が存在していると言える．

動的特性に加えて静的特性の存在が確認できれば，センサーの設置や運用に関する計画が立てられるようになるほか，センサーが観測した通信データの分析にも役立てられるのではないかと考えた．

本論文では，筆者らが設置したセンサーが長期間に渡って観測した通信データの分析に基づいて，センサーの観測対象であるグローバル IP アドレスの第 4 オクテットに基づく静的特性の存在を確認する．

2. サイバー攻撃の観測

2.1 サイバー攻撃の制約と特徴

インターネットを経由したサイバー攻撃に伴う攻撃通信は，インターネット上の異なる 2 点間で情報を伝える通信であり，通信規約である IP(インターネット・プロトコル)[6]に則らなければならない制約がある．この制約のため，非常に高度な攻撃技術を搭載した攻撃プログラムが送信した攻撃通信であったとしても，IP パケットして観測が可能である．

また，攻撃通信を送信する攻撃プログラムは，ある目的によって開発されおり，人の意思によって実行されているものと考えられる[7]．第三者である攻撃プログラムを実行する人の意思をインターネット越しに伺い知ることは非常に困難であるため，攻撃通信の存在を事前に把握することは非常に困難という特徴があると言える．

2.2 センサー

サイバー攻撃は，2.1 節で述べたような制約と特徴があることから，インターネットに接続されたコンピュータは，いつかは攻撃通信が送り付けられてくる可能性があり，仮に攻撃通信が送り付けられた場合は IP パケットとして必ず観測できる性質を持っていると言える．

サイバー攻撃は前述のような性質があることから，インターネットに接続されたコンピュータはいずれ攻撃通信を受け取る可能性がある．攻撃通信を観測することに特化したコンピュータを本論文ではセンサーと呼ぶ．

センサーの単位は，観測対象となる 1 つのグローバル IP アドレスと同義に扱われることがあることから[8]，本論文でもその扱いに準じる．

センサーの仕組みは図 1 で示すとおり，発信源と観測対象となるグローバル IP アドレスとの間の通信を観測し通信データとして記録するものである．本論文では発信源から観測対象のグローバル IP アドレスに対して送信される通信をインバウンドパケットとし，逆方向の通信をアウトバウンドパケットとする．

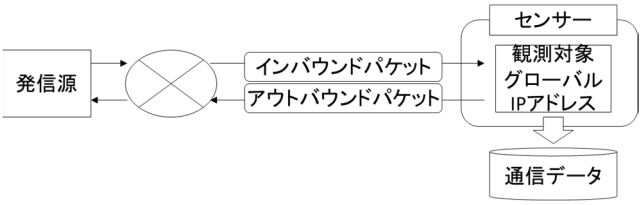

図 1　センサーの仕組み

2.3 関連研究

センサーが観測する通信内容について，グローバル IP アドレスによって偏ることが知られている．この偏りに関する研究は，グローバル IP アドレスの利用状況によって変化する動的特性の研究と，グローバル IP アドレスそのものの属性に基づく静的特性の研究に分類できる．本節では，動的特性と静的特性について述べる．なお，本論文では，グローバル IP アドレスは IPv4 として議論を進める．

2.3.1 動的特性に関する研究

センサーが観測対象であるグローバル IP アドレスの利用状況によって，観測される内容が変化することが知られている．本論文では，グローバル IP アドレスの利用状況によって観測内容が変化する特性を動的特性と呼ぶ．

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[3]．用途の切り替わりによる変化に関しては，センサーの動作を一方的にインバウンドパケットのみを観測するパッシブモードから応答するリアクティブモードに切り替えたことにより，観測できる通信の種類が変動した可能性を示す研究を小堀らが報告している[4]．

以上のことから，動的特性は，観測対象のグローバル IP アドレスが発信するアウトバウンド通信によって変化することが考えられる．

2.3.2 静的特性

センサーの観測対象であるグローバル IP アドレスは，変更できない属性値である．この属性によって，観測される内容が偏ることが知られている．本論文では，グローバル IP アドレスの属性によって観測内容が偏る特性を静的特性と呼ぶ．

静的特性については，鈴木らの分析によると，あるボットが発信する通信の宛先グローバル IP アドレスは，第 4 オクテットが 128 よりも大きいアドレスに対しては送られないことを確認している[9]．

筆者らは, 表 1 に示すデータセットの分析から IP アドレスの第 4 オクテットによって観測された通信の発信源に偏りがあることを確認している[5].

筆者らは第 4 オクテットの偏りの可視化を行っている. 横軸に第 4 オクテットと置き，縦軸に観測された発信源数として図 2 に可視化した. 図 2 が示すとおり，第 4 オクテットが小さいほど発信源数が多く，第 4 オクテットが大きくなるほど発信源数が緩やかに下降していく傾向が確認できた. また，図 2(1)の第 4 オクテットが 0 の時と，図 2(2)の第 4 オクテットが 255 は，ほかの第 4 オクテットよりも極端に少ないことがわかる.

表 1　オクテットパターンを調査した際のデータセット

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

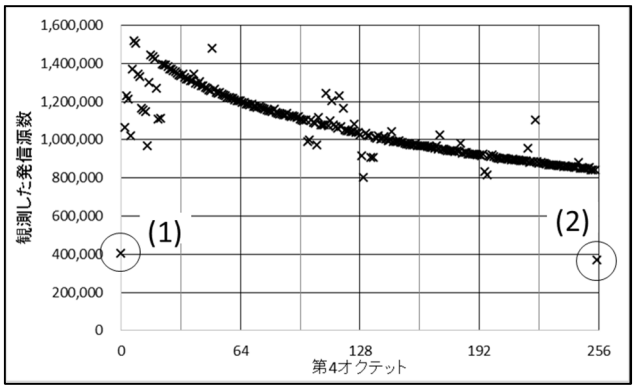

図 2 第 4 オクテットによる観測された発信源数

本論文では，図 2 で示されるような傾向をオクテットパターンと名付けた. オクテットパターンは，グローバル IP アドレスの第 4 オクテットに依存することから，センサーにとって静的特性の一つが表現できている可能性がある.

しかし，このオクテットパターンは，表 1 で示す観測期間よりも前の状態を確認していないことから，動的特性の結果である可能性を排除できないでいた.

2.4 本研究の位置付け

2.3.2 で述べたオクテットパターンが長期に渡って確認できるのであるならば，センサーは動的変化のほかにオクテットパターンとして表現される静的特性も存在する可能性がある

そこで筆者らは, センサーの静的特性が明らかになれば, 動的特性と併せてセンサーの設置および運用に際しての計画が立てられるようになるほか，センサーが観測した通信の分析にも役立てられるのではないかと考えた.

本論文では，より長期間に渡って筆者らが設置したセンサーが観測した通信の分析に基づいて，センサーの観測対象であるグローバル IP アドレスの第 4 オクテットに基づく静的特性を確認する.

3. 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」)について述べる.

3.1 センサー

筆者らは，到達可能なネットワークの内，ドメイン登録やサーバとしての運用のほか，インターネット接続用としても用いられていないグローバル IP アドレスにセンサーを設置している. このため，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，このセンサーはセンサー宛の通信をすべて観測する.

センサーの観測対象となっているグローバル IP アドレスは，ほぼ連続した約 1,700 の IP アドレスである. センサーは，インバウンドパケットの内，プロトコルが TCP であり，かつ SYN フラグが立ったパケットを受信した場合のみ, 発信源の IP アドレスに対して SYN/ACK を応答する機能を持つ[10].

3.2 概要

表 2　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	2016/01/01　～　2018/05/31 (881 日間)
グローバル IP アドレス数	約 1,700 個
容量	約 8.0TB
総パケット数	約 756 億
インバウンドパケット数	約 598 億
ユニーク IP アドレス数 (発信源数)	約 6,695 万個

本論文で使用するデータセットは，表 2 に示すとおり 2016 年 1 月 1 日から 2018 年 5 月 31 日に至るまでの 881 日間で，パケット数は約 756 億であった. ただし，このパケット数は，インバウンドパケットのほかにセンサーが応答したアウトバウンドパケットを含む. インバウンドパケットに限ると約 596 億パケットである. 観測期間中, 約 6,695 万の発信元のユニーク IP アドレス(以下,「発信源」)の観測ができた.

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 3 に示す. 全体の約 99.0%が TCP/IP の通信であり，それ以外は約 1.0%であった.

表 3　プロトコルごとの受信パケット数と割合

プロトコル名	パケット数(割合%)
UDP/IP	約 1.5 億パケット(約 0.3%)
TCP/IP	約 592.2 億パケット(約 99.0%)
それ以外のプロトコル	約 4.6 億パケット(約 0.7%)

3.3 1 日当たりのパケット量

各センサーは，ネットワークやセンサーシステムの定期点検等の理由により停止している時期がある．センサーが 24 時間以上停止していた場合，日単位で集計している観測したパケット数が 0 となる．このように集計したパケット数が 0 となる観測日は欠測日として扱う.

観測期間における欠測日は 69 日あったことから，実質観測日数は 812 日(観測期間 881 日-観測日数 69 日=実施津観測日数 812 日)である. 総観測パケット数から実質観測日数で割ると 1 日当たりの観測したパケット数が得られる. 1 日当たりの観測パケット数は, 約 9,310 万パケット(756 億パケット/812 日=約 0.931 億パケット/日)である．インバウンドパケットのみとすると, 1 日当たり平均して約 7,365 万パケット(598 億÷812 日＝約 0.7365 億パケット/日)を観測している．1 アドレス 1 日平均では約 4.3 万パケット(7,365 万パケット/1,700 センサー=約 4.3 万パケット/センサー)を観測している.

1 日当たりで観測した最大のパケット数は 2017/09/16 の約 3.6 億パケットであった.

3.4 パケット数の時間変化

観測期間中に全センサーが観測した 1 日当たりのパケット数の推移を，横軸に観測を開始してからの日数とし，縦軸に日単位における全センサーが観測したパケット数を図に示す(図 3). 図 3 のとおり，日を追うごとに観測されたパケット数は増加傾向にあることがわかる.

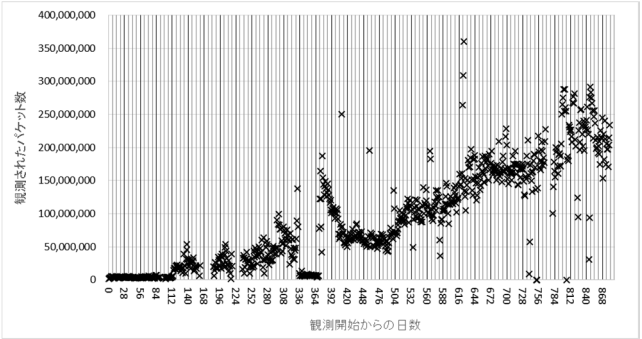

図 3　日単位の観測したパケット数

4. 分析

本章では，2.4 節で述べたオクテットパターンが，第 3 章で述べたデータセットを用いて確認するための分析について述べる.

4.1 集計方法

集計するには各センサーを識別する必要があることから，約 1,700 個存在するセンサーを識別する方法について述べる.

観測対象となっているグローバル IP アドレスの内, 最も小さいグローバル IP アドレスを IP_{min} とし，IP_{min} を観測対象としているセンサーを ID:0 と名付けた. 各センサーの命名については, 観測対象となっているグローバル IP アドレスと IP_{min} の差を ID とした. 例えば, ID:100 のセンサーは, IP_{min} に 100 を加えたグローバル IP アドレスを観測しているセンサーを指す.

4.2 発信源数

各センサーにおける観測した発信源数の分布を図 4 に示す．図 4 は，横軸にセンサーID として縦軸に各センサーで観測された発信源数とした.

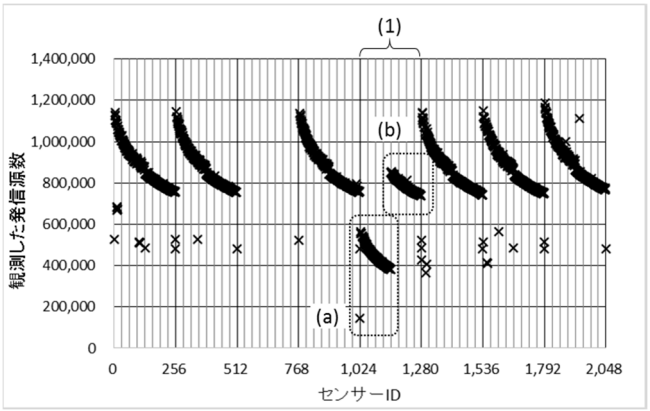

図 4　センサーID 単位の観測された発信源数

図 4 のとおり，256 センサーごとにオクテットパターンが繰り返されることを確認できた．図 4 中(1)に示す区間では，ID:1024 から ID:1280 の間であり，オクテットパターンが(a)と(b)の 2 つに分かれている．発信源数は，観測された期間に比例することが筆者らの分析によって確認されている[5]. 観測期間と共に観測したパケット数も多くなるため, 4.3 節でパケット数に関する分析を行う.

4.3 センサーごとのパケット数

4.3.1 全期間におけるパケット数

センサーごとに観測されたパケット数を図 5 に示す. 図 5 は横軸にセンサーID を置き，縦軸に各センサーで観測されたパケット数である．図 5 が示すとおり，パケット数においてもオクテットパターンが確認できた.

図 5 中の(1)に示す区間は 4.2 節と同じく ID:1024 から ID:1280 であり，オクテットパターンが(a)と(b)の 2 つに分断されている．つまり，図 5 中の(a)と(b)とで観測できたパケット数に差が存在することを意味する．この観測され

たパケット数の差が，観測された発信源数の差となって表れたものと考えられる．

図 5 中の(2)に示す区間は，センサーID:256 から ID:511 のパケット数がほかのセンサーに比べて多い．この傾向が 2016 年 1 月 1 日以降から継続している場合は静的特性であり，観測期間の途中から確認されれば動的特性と言える．

そこで，4.3.2 では日単位におけるパケット数について分析を行う．

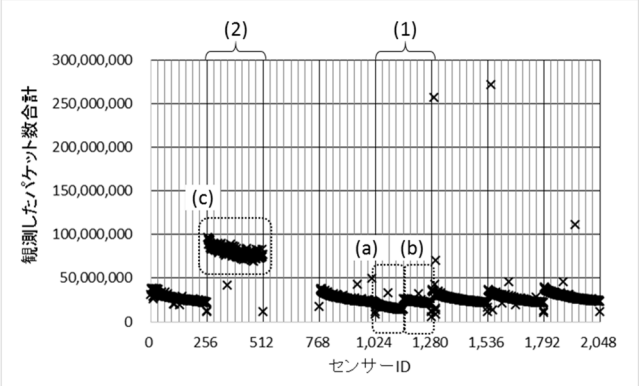

図 5　センサーID 単位の観測されたパケット数

4.3.2 日単位におけるパケット数

センサーID:256 から ID:511 のパケット数がほかと比べて多い点に関して，観測期間開始からその傾向として観測がされる静的特性によるものか，観測期間の途中からその傾向が始まっている動的特性のいずれかは，集計したパケット数からはわからなかった．そこで，全期間における日単位のパケット数を集計する．

各センサーにおける日単位の観測されたパケット数を表に出力すると，センサーの数分の列と観測日数である 2 行が必要であることから，約 138 万(約 1,700×810 日)N 要素がある表として出力される．人は，138 万の要素を見て傾向をつかむことが困難である．

そこで，筆者らが考案した二次元平面上に全センサーの各観測した日毎のパケット数を描画する手法を用いる[12]．この手法に基づいて，横軸にセンサーID を置き，縦軸に観測した日を置き，各センサーの日単位で観測したパケット数を色(図 6)で表現した図を出力する(図 7:最終ページ参照)．背景色である黒色の領域は，観測対象のグローバル IP アドレスか欠測日である．この黒色部分に灰色の横線が等間隔で描かれているが，これは 28 日ごとの補助線である．

図 6　カラーパターン

図 7 によれば，観測期間開始は横方向に各センサーで観測したパケット数は少なく図 6 に示すカラーパターンに基づけば 10 万パケット以下となっているセンサーが多いことがわかる．観測開始から 112 日目からセンサーID:256 から ID:511(図 7(1))の区間が青から緑色に変化する．緑色は，図 7 のカラーパターンに基づけば 100 万である．実際に図 3 を確認すると観測開始から 112 日目で大きくパケット数が増加していることがわかる．

また，観測開始から 363 日目では(図 7(1))の区間で橙色が出現している．図 7 のカラーパターンに基づけば 1,000 万以上のパケットが観測されていることを意味している．この期間は，図 3 でも 364 日目付近で合計で 1 億以上のパケットを観測していることが確認されている．なお，センサーID:256 から ID:511(図 7(1))の区間はほかのセンサーと比べてポアケット数が多く，観測開始から終了に至るまで同様の傾向を示している．したがって，図 7(1)の区間のパケット数の多さは静的特性であると言える．

5.　考察

本章では，第 4 章で述べたデータセットを分析した結果から考察できる点について述べる．

5.1　全体を通じたオクテットパターンの確認

図 7 中の観測日の 616 日から 672 日, ID:768 から ID:1024 のセンサーの範囲を拡大をし，併せてパケット数を表現する色調整を実施した図を示す(図 8:最終ページ参照)．図 8 中の(1)から(5)の各区間において, 左端から右端にかけての色が緩やかに変化していることが確認できる. この変化は，パケット数が区間内で左端から右端にかけてパケット数が減少していくことを表している．また，この色の変化が縦方向にも継続していることが確認できる．このことから，図 8 が示す観測期間内である約 100 日間は，オクテットパターンが継続していることを意味している．

したがって, センサーの観測対象でありグローバル IP アドレスの第 4 オクテットには静的特性が存在することが確認できた．

5.2　各センサーのパケット数の増減

図 7 には横方向の筋が多く存在していることが確認できる．一部を拡大すると横方向の筋が不規則に並んでいるのがわかる(図 9).

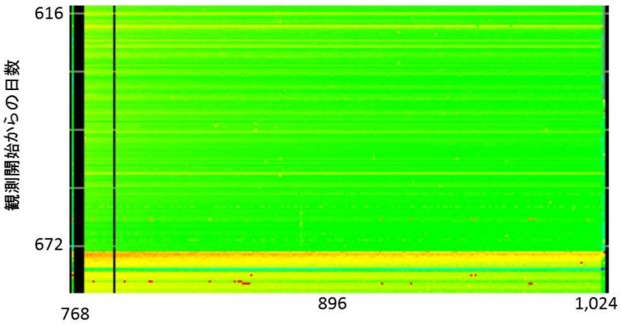

図 9　特定期間で同期する日毎のパケット量

この横の筋は，同 1 日に異なるセンサーにおいてパケット数の増減が同期が取れていることを意味している．筆者らによる表 1 のデータセットの分析に基づけば，一つの発信源の 65.8%は箇所以上のセンサーに送信していることがわかっている．また，複数のホストが一斉にパケットを送信する現象も村上らによって確認されている[13]．このことから，観測対象となっているグローバル IP アドレスで観測されるパケット数の増減が同期している現象は，動的特性でも静的特性ではなく，インターネット全体の傾向であると言える．

5.3 グローバル IP アドレスの用途に依存しない動的特性

図 8 には，縦方向の筋がいくつか確認できる．縦方向の筋は，5.2 節で述べたような観測日による増減とは異なり，センサー固有の傾向である．図 10 は，観測日 168 から 224 日付近のセンサーID:1950 近傍部分を拡大したものである．

ID:1950 近傍のセンサーは 3.2 節で述べたとおり，TCP の SYN パケットに対して応答を返すのみのである．

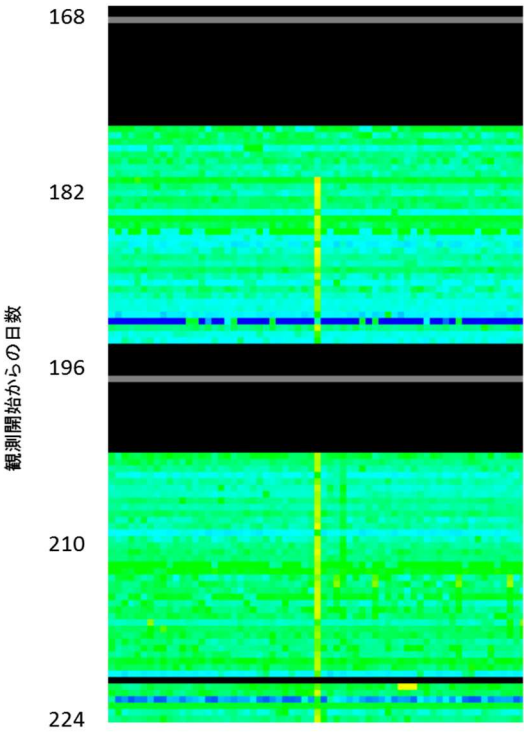

図 10　IP アドレスの状況

しかし，図 10 が示すとおり，観測日数が 182 日目付近から ID:1950 近傍で縦方向の筋が入っている．これは，ID:1950 近傍の 1 つのセンサーが観測するパケット数が，近傍のセンサーに比べて突然増加する傾向が継続していることを意味している．

2.3 節で述べたとおり，動的特性は，観測対象のグローバル IP アドレスから発信されるアウトバウンド通信の内容に依存すると考えられていた．今回の傾向は，アウトバウンド通信を変更しなくても，動的特性が変更しうる可能性を示すものであ．

今後は，この動的特性が変化する前後の通信内容を解析し，動的特性の原因について調査したい．

5.4 動的特性と静的特性に基づく分析への応用

本論文では，センサーの観測対象であるグローバル IP の第 4 オクテットによる静的特性が長期間に渡り存在していることが確認できたことについて述べた．また，グローバル IP アドレスの利用状況によって通信内容が変化する経年変化が，グローバル IP アドレスの利用状況に関係なく発生し得ることが確認された点についても述べた．

これらセンサーの観測対象であるグローバル IP アドレスの静的特性と動的特性を考慮すれば，より多くの攻撃通信を観測できるようになるのではないかと考えられる．

今後は，静的特性と動的特性に基づく，センサーの設置および運用方法について検討を進めたい．

6. まとめ

本論文では，センサーと呼ばれるインターネット経由で行われるサイバー攻撃に伴う攻撃通信を観測するコンピュータを用いる必要性について述べた．また，センサーが観測できる通信内容は，観測対象であるグローバル IP アドレスによって偏る点についても述べた．観測できる通信内容の偏りは，グローバル IP アドレスの過去の利用状況に伴う経年変化が知られている一方で，筆者らはグローバル IP アドレスの第 4 オクテットによって偏りの可能性について述べた．

そこで，本論文では，2 年 5 か月に渡って観測したデータセットを用いて，グローバル IP アドレスの第 4 オクテットによる観測内容の偏りが長期間に渡っても存在することを示した．また，グローバル IP アドレスの用途に関係なく，一部のグローバル IP アドレスが経年変化することも示した．

今後は，このような静的特性と動的特性に基づいた，センサーの設計および運用方法について検討を進めていきたい．

参考文献

[1] https://www.npa.go.jp/hakusyo/h29/, (参照 2018-08-20 確認).

[2] https://www.ipa.go.jp/security/fy18/reports/contents/remote/Chapter7/8.htm, (参照 2018-08-20 確認).

[3] 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), p.56-63, 2014/10.

[4] 小堀 佳和子, 稲村 勝樹, “状態変化型リアクティブセンサーを用いた攻撃ロジック観測手順の提案”, コンピュータセキュリティシンポジウム 2017 論文集, Vol.2017, No.2, 2017/10.

[5] 芦野 佑樹, 鮫島 礼佳 , 須堯 一志 , 矢野 由紀子 , 中村 康弘 , “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”, 第82回コンピュータセキュリティ(CSEC)研究会発表資料, Vol. 2018-CSEC-82, No.40, 2018/07.
[6] https://tools.ietf.org/html/rfc791, (参照 2018-08-20 確認).
[7] 芦野 佑樹, 島 成佳 , 矢野 由紀子 , 中村 康弘 ,”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, pp.1238-1245, 2017/10.
[8] https://www.nict.go.jp/cyber/report/NICTER_report_2017.pdf (参照 2018-08-20 確認).
[9] 鈴木 将吾, 小出 駿, 牧田 大佑, 村上 洸介, 笠間 貴弘, 島村 隼平, 衛藤 将史, 吉岡 克成, 松本 勉, 井上 大介. "複数国ダークネット観測による攻撃の局地性分析", コンピュータセキュリティシンポジウム2014論文集, Vol.2014, No.2, 2014/10.
[10] 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, 鮫島礼佳, 矢野由紀子, 島成佳, 中村康弘, “センサーが捕捉した通信データの解析を支援する可視化手法の提案”, 2018 年情報とセキュリティシンポジウム(SCIS 2018), IE1-2, 2018/01.
[13] 村上 洸介, 蒲谷 武正, 千賀 渉, 鈴木 将吾, 小出 駿, 島村 隼平, 牧田 大佑, 笠間貴弘, 衛藤 将史, 吉岡 克成, 井上 大介, 中尾 康二, “複数のダークネット観測拠点で同時期に急増する攻撃を検知する手法の提案”, コンピュータセキュリティシンポジウム 2014 論文集, Vol.2014, No.2, 2014/10.

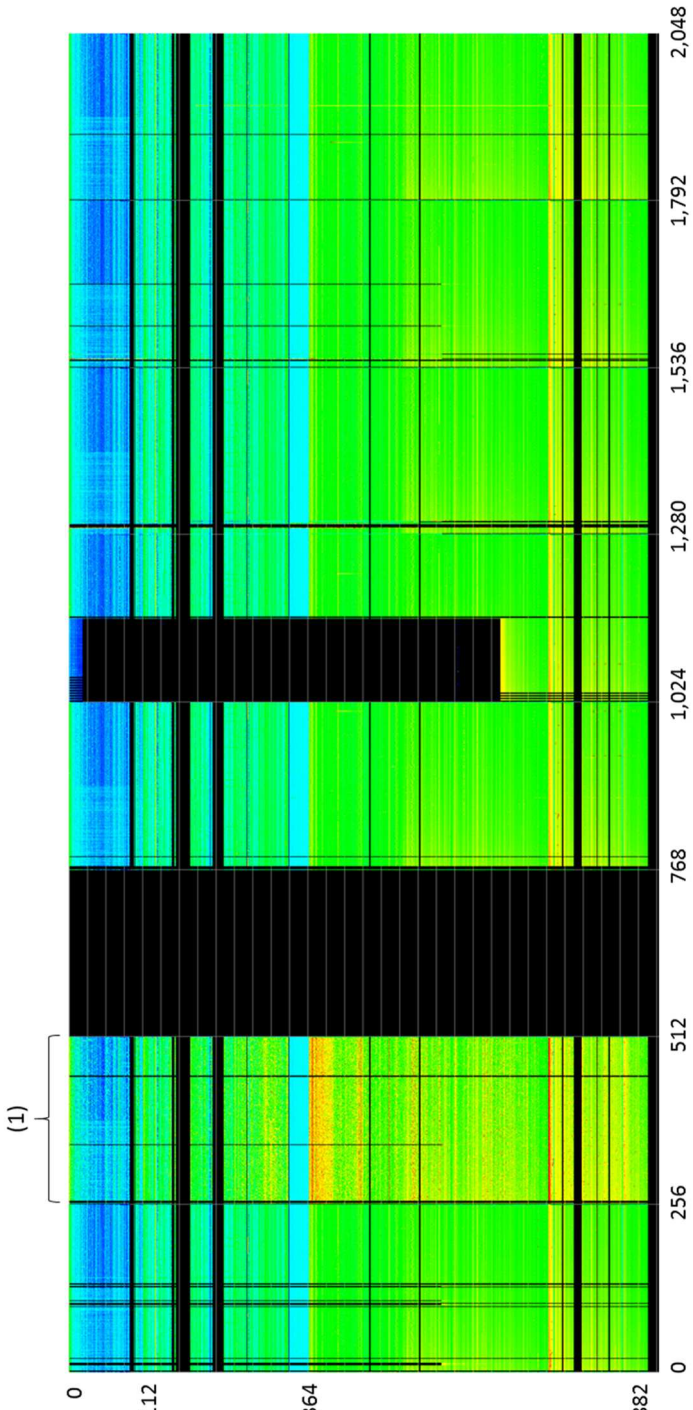

図 7　センサーごとの観測されたパケット数の推移

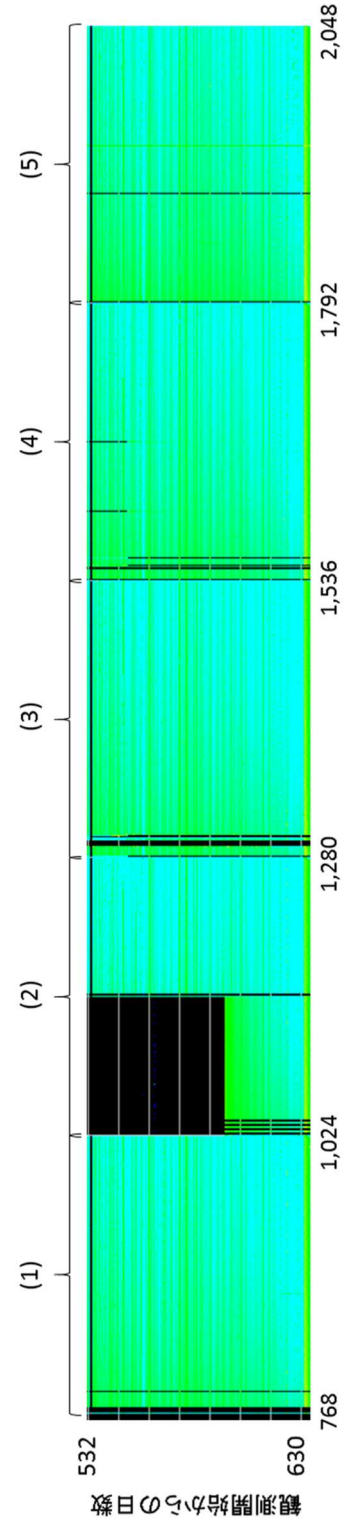

図 8　センサーごとの観測されたパケット数の推移