Computer Security Symposium 2016
11 - 13 October 2016

長期的な攻撃元ホストの振る舞い調査

水谷 正慶[1]

概要：攻撃者がインターネット上で悪意ある活動をする際、多くの場合は自身が直接操作する端末ではなく踏み台となる第三者のホストを経由して攻撃を実施する。これは攻撃者が自身を特定されるのを防いだり、攻撃元を限定されることでその端末からの攻撃対象への通信が拒否されるのを防ぐことが目的と考えられる。そのため、攻撃者は踏み台となるホストを次々と変更するのが効果的だが、一方で長期的に攻撃に利用されているホストも存在している。本稿では攻撃元となるホストの生存時間や挙動について調査した結果をまとめる。

キーワード：ネットワークセキュリティ、侵入検知システム、ログ分析

Investigation of Long-term Attacker Host's Behaviour

Masayoshi Mizutani[1]

Abstract: When attackers does malicious activity on Internet, they attack victim via bot or other compromised host, not directly. The purpose to use the compromised host is to prevent detection of attacker's identity and rejection of communication to victim by ACL. Therefore it may be effective for attacker to change the host to attack victim. However the hosts to be used long-term by attackers are also observed. In the paper, I summarize our investigation of the host to be used for attack.

Keywords: Network Security, Intrusion Detection System, Log Analysis

1. はじめに

ネットワーク上におけるセキュリティ侵害を目的とした攻撃方法は，インターネットやネットワークに接続するホストの状況に応じて変化を続けている．2000 年初頭には，ユーザが個人で利用するホスト (Personal Computer, PC) か常時稼働しネットワーク上でサービスを提供するホスト (サーバ) かにかかわらず，攻撃対象のホストが開放しているサービスを狙った攻撃は多く発生した．しかしその後，PC を標的としたそのような攻撃は 2010 年頃までに減少しており，ドライブバイダウンロード (DbD) やメールを起点とした攻撃に推移した．これは，ネットワーク型およびホスト上で動作するファイヤウォールや侵入検知システム (Intrusion Detection System, IDS)， 侵入防止システム (Intrusion Prevention System) の対策導入が進んだことにより，攻撃の成功率が低下したためだと考えられる．一方で，多くのソフトウェアやサービスがクラウドをはじめとする Web サービスへと移行していることもあり，外部からの接続を受け付ける必要があるサーバは増加している．このようなサーバに対する攻撃は継続的に発生している．

サーバに対する攻撃は，踏み台と呼ばれる中継ホストを経由して実施される場合が多い．インターネットにおいて遠隔から攻撃する際，DoS 攻撃や UDP を利用した双方向の通信を必要としない場合を除いて，攻撃側と攻撃対象は互いに IP アドレスを認識しなければならない．これは TCP に代表されるセッション管理のプロトコルを利用する場合，双方向でセッション管理のための情報を送受信する必要があるためである．国ごとに対応は異なるが，IP アドレスは地域インターネットレジストリやインターネット・サービス・プロバイダが管理・運用しており，攻撃者自

[1] 日本 IBM 東京基礎研究所
Tokyo Research. IBM, Japan

身が直接利用している IP アドレスが露呈した場合に利用している地域や組織，あるいは身元が追跡される可能性がある．しかし，経路情報をインターネット接続事業者が相互に管理しているインターネットを介した通信において，TCP などセッション管理を伴う場合に IP アドレスを偽装することは困難である．そのため，攻撃者は自身が直接操作するホストではなく第三者のホストを不正に操作し，踏み台ホストとしてそのホストに割り当てられた IP アドレスを用いて攻撃を実施する場合が多い．

このような踏み台ホストが長期的にどのような利用をされているのか調査する必要がある．2005 年頃からインターネット上の攻撃に利用されるようになったボットネットでは，不正に侵入したホストをまとめて管理・運用し，攻撃者の必要に応じて攻撃などの不正活動に利用されるようになった [4]．また，サーバが開放しているサービスに対して攻撃を実施する場合，攻撃者側から能動的に接続を開始する．そのため，DbD 攻撃に利用されるような攻撃コードを設置して待機しているホストと比べて，攻撃に利用するホストを取り替えるのは比較的容易であると言える．これらの理由により攻撃者はサーバを攻撃する際に利用するホストを流動的に変更できる実態がある．

一方でネットワークにおけるセキュリティ対策として IP アドレスを基準として脅威を判定するものもある．ブラックリスト方式による IP アドレスの判定サービス [1] や，IP アドレスのレピュテーション情報を提供するサービス [2] があり，これらを利用して通信の制限や通信発生後のログの調査などに役立てることができると考えられる．このような対策をするにあたり，サーバへの攻撃に利用される IP アドレスがどのような挙動をしているかを明らかにすることで，その有効性を議論できる．

本稿では IBM Tokyo SOC において観測されたサーバに対する攻撃データを元に，サーバに対する攻撃がどのように実施されているかを調査・分析した結果について報告する．本稿で提示するデータは複数環境をまたがったデータを用いて，観測環境の違いがどのような影響をおよぼすのか調査する．IP アドレスがどれくらい継続的に利用されるかという点を明らかにすることで，IP アドレスによるブラックリスト型の対策がどの程度有効であるかを論じる．また，これによってダークネットやハニーポットによる観測にどのような影響があるのかを論じる．

2. データの収集条件と事前処理

本稿では IBM Tokyo SOC で 2016 年 1 月 1 日から 2016 年 6 月 30 日まで観測された IDS および IPS によって検知されたイベントのデータを分析する．データは基本的に日本の組織に関係がある環境のネットワークで観測されたイベントとなる．IDS および IPS には IBM Proventia GX シリーズおよび XGS シリーズが用いられており，シグネチャは常に最新のものが適用されている．

また，本稿での分析を実施する前に分析の正確性を向上させるため，収集したデータに対して以下の処理を実施した．

2.1 サーバに対する攻撃と考えられるイベントの抽出

データ収集に利用した IDS および IPS はサーバに対する攻撃のみではなくクライアントに対して実施される DbD 攻撃やメールを起点とした攻撃のイベント，さらに攻撃成功後に発生する Command & Control サーバに対するコールバック通信なども検知する．本稿では固定的に設置されサービスを提供するサーバに対しての不正行為を分析するため，以下の 3 種類のいずれかに属するイベントのみを抽出した．

1. サーバに対するスキャン
2. サーバに対する DoS 行為
3. サーバに対する侵入の試み

特に (3) については Web サーバやメールサーバといったミドルウェアに対する攻撃だけではなく，Web アプリケーションに対する SQL インジェクションやクロスサイトスクリプティングなどの攻撃についても対象とした．本稿ではこれらのイベントを総称して**攻撃**と呼ぶ．

2.2 不要なイベントの除外

本稿で利用するデータは一般的な IDS や IPS と同様に誤検知 (False Positive, FP) のイベントと，脆弱性診断などに代表される悪意のない通信によるイベントが含まれる．そのためこれらを不要なイベントとして除外する必要がある．

まず，脆弱性診断であると考えられる通信は送信元 IP アドレスの所属から判定した．現在，様々なシステムインテグレータやセキュリティ対策ベンダが脆弱性診断を実施している．脆弱性診断の通信によって発生するイベントは攻撃と同様に通信であり FP ではないが，対象となるホストの所有者が意図したものであり，第三者による攻撃を分析する上ではノイズとなるため，これらのイベントを除外した．

さらに Content Delively Network (CDN) からの通信によるイベントも除外した．CDN は Web サービスなどの負荷を分散するため，必要に応じてコンテンツデータを部分的に CDN 事業者のシステムに転送し，サーバ側のデータ転送の負荷を軽減するものである．攻撃者によるリクエストを CDN 事業者側のシステムが受信した場合，CND 事業者のシステムはサーバに必要となるデータの取得を試みる場合があり，これが攻撃として検知される可能性がある．このようなイベントは元は悪意のある攻撃であるが，観測地点からは本来の送信元 IP アドレスが不明となってしま

うため，本稿における分析の観点からこれらのイベントを除外した．

また，監視環境内においてインシデントが発生していない限り，監視環境内で利用されている IP アドレスから発生したイベントは除外した．

3. 分析および結果

3.1 対象となるデータ全体の傾向

第 2 節で述べた方法によりデータ収集および事前処理を実施し，抽出されたイベントを集計した．抽出されたイベントにおいて観測された攻撃元となる IP アドレスは 1,285,685 件であった．本稿では，これらの IP アドレスをキーとして時系列でイベントを並べた時に最初に検知されたイベントと最後に検知されたイベントの時間差分をその IP アドレスの観測期間と呼ぶこととする．

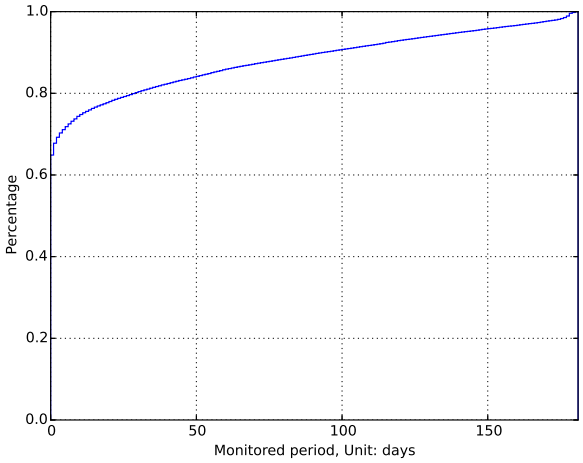

図 1: 同一の IP アドレスからの活動の初登場時刻を 0 とした場合の観測期間の累積度数分布 (単位:日)

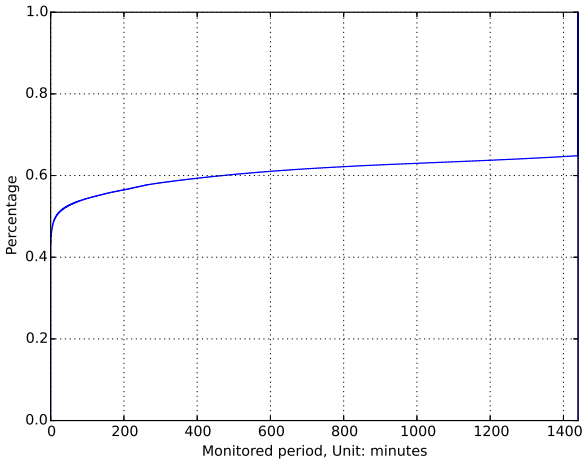

図 2: 同一の IP アドレスからの活動の初登場時刻を 0 とした場合の観測期間の累積度数分布 (1440 分まで，単位:分)

表 1: 観測期間の長さにもとづく IP アドレスの分類

観測期間	表記	件数 (割合)
$0 \leq d < 60$	`< 1min`	597,405 (46.46%)
$60 \leq d < 86400$	`< 1day`	260,933 (20.29%)
$86400 \leq d < 2592000$	`< 30days`	190,865 (14.84%)
$2592000 \leq d$	`>= 30days`	236,482 (18.39%)

割合は小数点第 3 位以下切捨

図 1 および図 2 では，各 IP アドレスの観測期間を累積度数分布によってグラフ化したものである．図 1 がデータ収集対象期間の 6 ヶ月間の累積度数分布を表しており，図 2 では先頭 24 時間分を拡大したグラフとなっている．このグラフでは観測期間が長い IP アドレスほど少なくなるという傾向を示す一方で，短期間でしか登場しない IP アドレスが大きな割合を占めていることを示している．図 1 では X 軸の単位が日数となっており，観測期間が 24 時間未満の IP アドレスが全体の約 66.76%であった．さらには全体の約 46.49%の IP アドレスの観測期間が 60 秒未満となっていた．このような短期間にしか観測されない IP アドレスについては，第 3.3 節で詳細に述べる．

また，全体の 20%ほどの IP アドレスは 20 日以上たった後でも観測されている．ただし，これについては一度観測された後に活動がなく，長期間たった後に再び観測された IP アドレスも含まれている．個人で契約しているインターネット・サービス・プロバイダや組織内ネットワークのユーザセグメントなどでは，IP アドレスの効率的な利用のために IP アドレスを動的に割り当てている．このようなネットワーク環境の場合，攻撃者の踏み台として利用しているホストの IP アドレスが変更されている可能性があり，図 1 および図 2 ではこれについて考慮されていない．これについての詳しい考察・分析は 3.4 節で述べる．

3.2 観測期間別の IP アドレスの特徴

本節では IP アドレスの観測期間ごとの特徴について調査し，観測期間の違いによって攻撃元 IP アドレスの挙動に差があるのかについて議論する．第 3.1 節で述べた通り，本稿で対象としているデータでは観測期間が短い IP アドレスが多く出現する傾向がある．そのことから，IP アドレスの観測期間を 60 秒未満，60 秒以上 24 時間未満，24 時間以上 30 日未満，30 日以上の 4 つのグループに分けて傾向を比較した．観測期間 (秒) を d として詳細を表 1 に示す．

図 3 は観測期間別に，IP アドレスが観測された環境数の分布を示している．本稿で分析に用いているデータは複数環境において観測された IDS および IPS のデータとなっている．各環境は互いに独立しているため，複数環境で同じ IP アドレスからのイベントが検知されるということは，攻撃者がその IP アドレスを利用して広範囲に攻撃を実施している可能性があるということになる．図 3 では観測さ

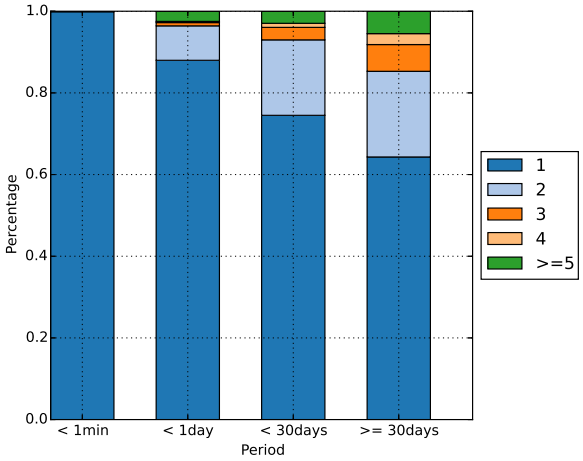

図 3: 活動期間別でみる IP アドレス観測環境数の割合

れた環境数は 1 から 4，および 5 以上の 5 段階に分類した．観測期間別に分類した IP アドレスのグループごとに，観測された環境数の割合がどのように分布していたかを示している．

図 3 ではいずれか 1 環境のみで観測されている IP アドレスが多くの割合を占めているのがわかる．特に 1 分未満のグループ (< `1min`) については約 99.89%が 1 環境のみでの観測となっている．観測期間の長さに応じて 2 環境以上で観測された IP アドレスは増加しており，1 日未満 (< `1day`) では約 10.57%，30 日未満 (< `30days`) で約 25.10%，30 日以上 (>= `30days`) で約 36.90%となっている．このことから長期間にわたって攻撃に利用される IP アドレスは複数の環境に対する攻撃を目的としている傾向があると分かる．しかし，実態としては 30 日以上観測され続けた IP アドレスでも 60%以上が 1 環境でしか観測されていない．観測期間に関係なく分布を調べても全体の約 87.28%が 1 環境のみで観測された IP アドレスであった．

攻撃が検知された IP アドレスの大部分が 1 環境のみで観測されていたのは，1 つの IP アドレスから複数の環境に対して攻撃するという傾向ではなくなりつつあることを示唆していると考えられる．インターネット上のサーバに対する攻撃は自動化することで大量の宛先に対して定形の攻撃コードを送信するのが容易である．実際に 2010 年以前に流行した感染後に攻撃を拡散させるマルウェアなどが代表的な例である．しかし今回の分析結果から，攻撃者は無闇に攻撃を拡散させているわけではなく，宛先を限定しながら攻撃を実施しているのではないかと考えられる．

図 4 は観測期間別の IP アドレスが所属していた国の割合を示している．図 3 と同様に観測期間別のグループに分割し，出現した国の上位 10 カ国についての割合を出しており，その他は Others としてまとめている．IP アドレスから所属する国名の判定には GeoIP[3] を利用した．所属国の分布については観測期間によって大きな差が生じにく

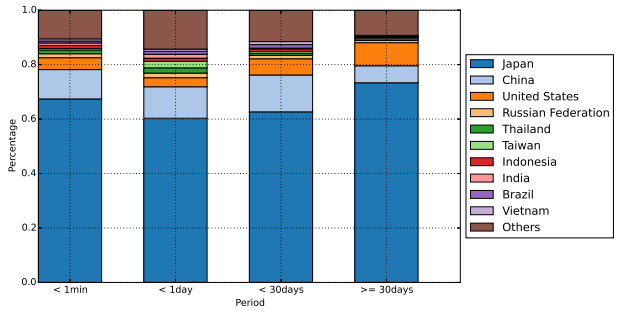

図 4: 活動期間別でみる IP アドレス所属国の割合

いことが分かる．30 日以上のグループにおいて国内からのアクセスが多くなっている点には着目できる．

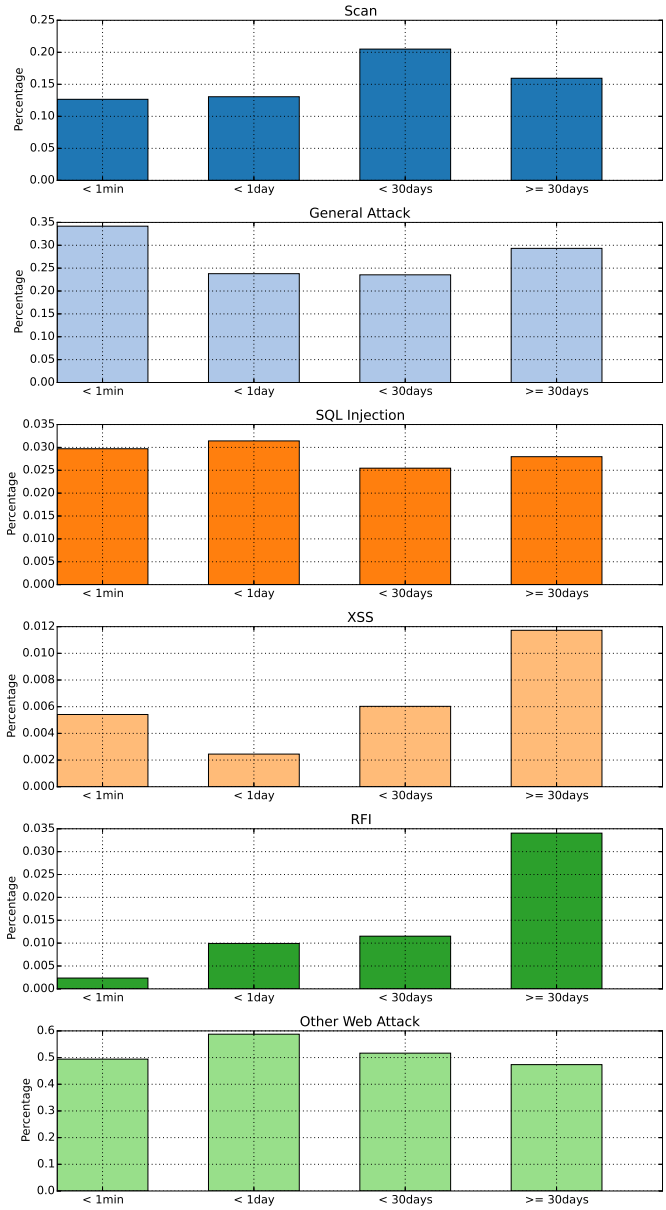

図 5: 期間別の IP アドレスに含まれるイベント種別

図 5 も観測期間別に IP アドレスをグループ分けし，そ

の IP アドレスから検知されたイベントがどのようなシグネチャによって検知されたものなのかを示している．1 つの IP アドレスから複数のイベントが検知される場合があるため，シグネチャを 6 つにカテゴリ分けし，グループ内で何割の IP アドレスが当該カテゴリのシグネチャによるイベントを発生させていたかを示している．シグネチャのカテゴリは以下の 6 種類に分類している．

- `Scan`: サーバやサービスの死活を確認する行為を検知するシグネチャ．ポートスキャンや Ping スイープなど．
- `General Attack`: 各種サーバのミドルウェア (Web, DB) や Web 以外のサービス (メール，リモートアクセスなど) に対する攻撃を検知するシグネチャ．
- `SQL Injection`: Web アプリケーションに対する SQL インジェクション全般を検知するシグネチャ．
- `XSS`: クロスサイトスクリプティング全般を検知するシグネチャ．
- `RFI`: リモート・ファイル・インククードに関連するイベントを検知するシグネチャ．
- `Other Web Attack`: 上記以外で Web アプリケーションに関連する攻撃を検知するシグネチャ．フレームワークの脆弱性を狙った攻撃など．

図 5 からは観測期間の変化にともなって検知されるイベントの傾向の違いがいくつか見られる．`Scan` に関しては 1 日以上の観測期間の方が比較的多く検知されている傾向がある．いくつかの攻撃元 IP アドレスについて確認したところ，継続的に特定の環境に対してポートスキャンなどを実施していた．観測期間が短い IP アドレスでも同様にスキャンのイベントが確認されているが，継続的にスキャンを実施する IP アドレスが割合を引き上げているとみられる．一方で `General Attack` については短期，特に 1 分未満のグループが顕著に高い傾向が見られた．ただしこのカテゴリにはメールやリモートアクセスに関するイベントも含まれており，正規のユーザによるアクセスに関連したイベントも検知していると考えられる．そのほかでは `XSS`, `RFI` については観測期間の長さに応じてイベントが発生している割合が増えているが，`Scan` や `General Attack`, `Other Web Attack` のカテゴリに比べて割合が少なく，他のカテゴリでででている差分と比べて大きな差分は無いといえる．

本節において述べた観測期間ごとの違いをまとめると，観測環境数のように観測期間に影響されやすいものについては違いが現れるものの，送信元の国や攻撃を検知したシグネチャについては大きな変化が見られなかった．このことから，攻撃者が長期間運用している踏み台と短期的な踏み台というものを区別せず，単純に制御下にある限りは攻撃に利用し，踏み台となっているホストが検疫されるなどの理由で制御下から離れた場合には観測期間が短くなる，という状況なのではないかと考えられる．

3.3 短期的に活動する IP アドレスの特徴

本節では観測期間が 60 秒未満の IP アドレスを対象にした分析について述べる．これは今回のデータで観測された IP アドレス全体の約 46.49%にあたる．

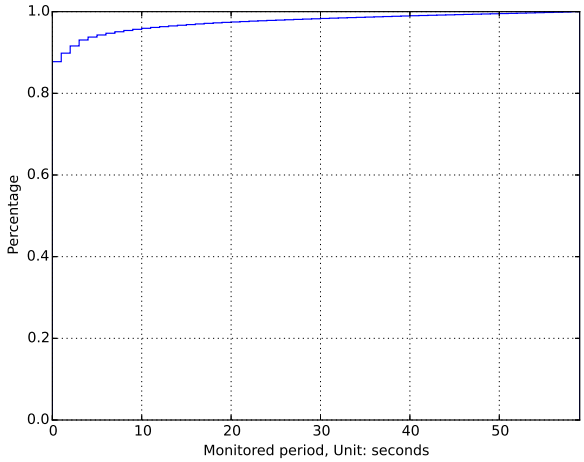

図 6: 期間が 60 秒未満の同一 IP アドレスの観測期間の累積度数分布 (単位:秒)

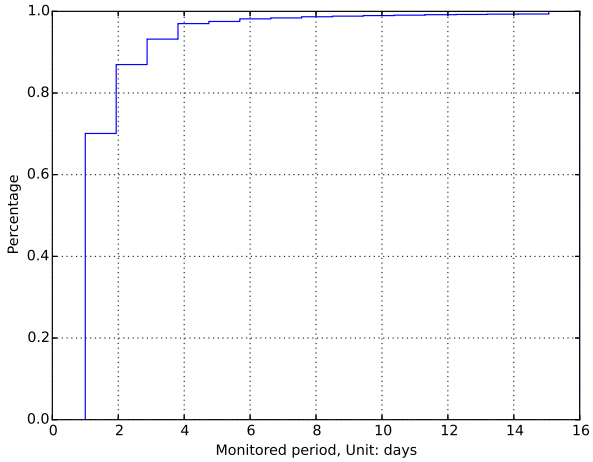

図 7: 期間が 60 秒未満の同一 IP アドレスから観測されたイベント数の累積度数分布

図 6 と図 7 はそれぞれ 60 秒未満のデータの出現の傾向を表している．図 6 は秒単位での観測期間の累積度数分布をあらわしている．図 7 は各 IP アドレスから検知されたイベント数の累積度数分布を表している．イベント数の最大値は 16 以上だったが，視認性のためにグラフ描画の最大値を 15 に設定した．16 以上のイベントが検知された IP アドレスは観測期間が 60 秒未満の IP アドレスの 1%未満である．

3.4 長期的に活動する IP アドレスの個別分析

グローバル IP アドレスはインターネット上で一意な識別子となるが，これは恒久的に同じホストのインターフェースを指し示すものではない．動的なアドレス割り当てやネットワークの構成変更にともなって，IP アドレスは異なる OS や異なる物理インターフェースを指し示すようになる可能性がある．第 3.1 節において示した IP アドレスの観測期間の分布に関する調査はこのような IP アドレスの変更については考慮していなかった．そこで，IDS および IPS によって収集されたイベントの内容を元に観測された IP アドレスが以前のものと同様であったかという点について検証を試みた．検証においては以下の 2 つの前提を設定した．

1. 24 時間以上イベントが観測されなかった場合，異なるホストに切り替わった可能性があるものとする．24 時間以上のイベント無検知状態で句切られたイベントの集合をイベント郡と呼ぶ．
2. 24 時間以上経過した後に再び同じ IP アドレスからの通信が観測された場合，検知したイベント郡の観測された環境かイベントの種類を過去のイベント郡と比較し，ある程度の一致があれば同じホストによる活動だとみなす．

2 の前提から以前に発生したイベント郡と現在のイベント郡を比較するために，式 1 と式 2 を用いた．

$$r_l = \frac{2|L_p \cap L_n|}{|L_p \cup L_n|} \tag{1}$$

$$r_e = \frac{2|E_p \cap E_n|}{|E_p \cup E_n|} \tag{2}$$

L_p は以前に発生したイベント郡を検知した環境の集合，L_n は現在のイベント郡を検知した環境の集合，E_p は以前に発生したイベント郡に含まれるイベントの種類の集合，E_n は現在のイベント郡に含まれるイベントの種類の集合となる．これらを用いて計算した r_l と r_e を観測環境とイベントの種類の一致率とし，事前に与えたしきい値 t_l および t_e と比較する．t_l と t_e はそれぞれ 0 以上 1 以下の値をとるものとする．$(t_l \leq r_l)\&(t_e \leq r_e)$ を満たしていた場合，前後のイベント郡が連続していたとみなすこととした．

この時，t_l と t_e の値を変化させた場合に連続するイベントの割合がどのように変化したかを図 8 に示す．イベントの観測期間が 24 時間を超えており，かつ 24 時間以上の無検知期間を 1 度以上持つ IP アドレスを対象に，分割されたイベント郡が全て連続していると判断できるかを調査した．図では t_l の値を 0.0，0.1，0.3，0.5，0.7，0.9，1.0 にそれぞれ固定し，t_e を 0.05 刻みで変化させた場合に全てのイベント郡が連続する IP アドレスの割合の変化を示している．図は大きく 3 つのグループに分離しており，一番

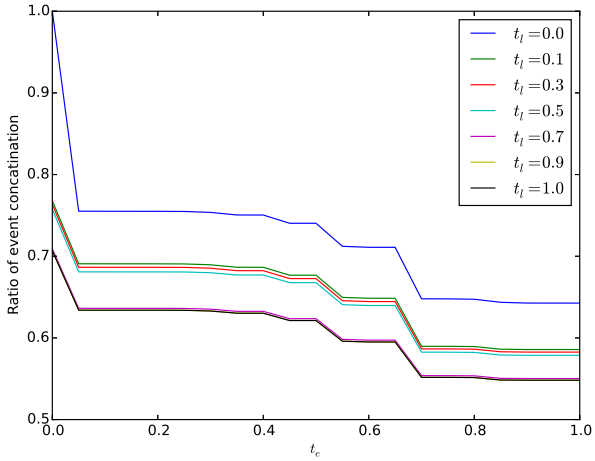

図 8: t_l と t_e を変化させた場合に連続するイベントの割合 (24 時間以上のイベントが対象)

上が t_l が 0.0 のグループ，真ん中が 0.1，0.3，0.5 のグループ，下が 0.7，0.9，1.0 のグループとなっている．

この結果から，対象となっている IP アドレスの半分以上は 24 時間以上検知がなかったとしても，同じホストのまま活動しているということが推定される．まず，もっとも条件の厳しい $t_l = 1.0$ かつ $t_e = 1.0$ の点では全て連続しているとみられる IP アドレスは全体の約 54.81%となっている．この条件が成立するということは同じ IP アドレスに属する全てのイベント郡の検知環境および検知したイベントの種類が完全に一致している状態である．ランダムにインターネット上の広範な IP アドレスから同じ監視対象となる環境で同じイベントを検知するのは極めて稀であると考えられ，同じホストによる活動であると判断できる．また，より容易な条件として $t_l = 0.5$ かつ $t_e = 0.5$ の点でも，対象となる IP アドレスの約 66.76%に対してイベント郡が連続していると判断できる．この条件でも半分以上は同じ環境に対して，半分以上は同じシグネチャで検知されるという条件をみたす必要があり，同じホストによる活動と判断することは妥当ではないかと考えられる．さらに，この調査では同じ IP アドレスに属する全てのイベント郡が連続していることを条件としており，部分的な連続で見ればより高い割合の IP アドレスが継続して使われているのではないかと予想できる．

これらの結果から，ある IP アドレスの観測期間が長くかつ何もイベントが検知されない期間が 24 時間以上あったとしても，同じホストとして活動している可能性が高いということが明らかになった．

4. 考察および今後の課題

第 3.1 節および第 3.3 節で述べたとおり，今回の分析で用いたデータの IP アドレスのうち約 46.49%が 1 分以内のみに観測されたものであった．さらのその中でも 1 度しか

イベントが観測されなかった IP アドレスも多く存在した．これらの IP アドレスは攻撃者が攻撃に使うのを中止した，あるいはホストの IP アドレスが変化したことにより再度観測されることがなかった可能性もあるが，False Positive として悪意のない通信を検知してしまっている可能性もある．非常に短期間にのみ観測されている IP アドレスは全体のうち大きな部分を占めるため，今後 False Positive のように分析のノイズとなるようなイベントのデータを適切に除去する方法を検討する必要がある．

第 3.2 節では，観測期間によって違いはあるものの特定の IP アドレスが観測された環境の数は極めて少ないという点について述べた．1 つの IP アドレスが広範なネットワークを攻撃していない傾向があるという事実は，研究やセキュリティ対策のためのデータ収集の観点から懸念がある．まず，同じ IP アドレスが観測される環境が限定されることで，ブラックリスト型の対策に影響がある可能性がある．ブラックリストを利用した防御では他環境で検知された攻撃の情報を元にブラックリストを作成し，それを共有することで効果を発揮する．しかし，環境をまたがった攻撃が少ないということはブラックリストに掲載されている IP アドレスからの攻撃を受ける可能性が少なくなることを示している．また，攻撃データの収集の観点から，ハニーポットやダークネットによるデータ収集にも影響があるのではないかと考えられる．ハニーポットやダークネットは攻撃関連のデータをあえて受信することでインターネット上の攻撃を把握しようとする試みだが，このように環境をまたがった攻撃が多く実施されないのだとすると，より多数の環境での観測をしていかなければならない．これらの研究では，より広範な環境でデータの収集が必要になると考えられる．

一方で第 3.4 節で示したように，長期で観測される IP アドレスの多くは一定時間検知が無い状況が続いても継続して類似した攻撃に使用されていた．このことから攻撃者も頻繁に攻撃用の踏み台を切り替えながら攻撃を実施しているわけではなく，同じ目的で使い始めた踏み台はそのまま継続して利用する傾向が強いことを示している．よって，攻撃者が利用する IP アドレスを広く防御側で共有するのは有意義であると見られ，研究の面からも実務的なセキュリティ対策の面からも，今後そのような取り組みがより一層重要になるのではないかと考えられる．

5. まとめ

本稿では 2016 年 1 月から 6 月までに複数環境において検知された IDS・IPS のイベントをもとに，攻撃元 IP アドレスがどのように利用されていたのかについて調査，分析を行った．その結果，非常に短期間でのみ攻撃を検知した IP アドレスが多かった一方で，長期的に攻撃が検知された IP アドレスは動的な IP アドレスの割当などに影響されず，同じホストが攻撃を継続していることが明らかになった．さらに複数の監視環境を持っていたとしても，それらをまたがって観測できる IP アドレスはごく一部であるということも明らかになった．今後は組織を超えて，セキュリティ関連の情報を共有していく取り組みがより重要になると考えられる．

参考文献

[1] What Is My IP Address. Blacklist Check, 2000. `http://whatismyipaddress.com/blacklist-check`.

[2] IBM. IBM X-Force Exchange, 2014. `https://exchange.xforce.ibmcloud.com/`.

[3] MaxMind. Geoip, 2012. `https://www.maxmind.com/ja/geoip2-services-and-databases`.

[4] 須藤年章. マルウェア：3．マルウェア観察日記（2）-サービスとして提供される攻撃-. **情報処理**, 51(3):252–260, mar 2010.