Computer Security Symposium 2017
23 - 25 October 2017

調査対象のIPアドレス属性を考慮した長期的な攻撃元ホストの振る舞いの分析

水谷 正慶[1]　渡邊 裕治[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。本稿では大規模運用されている侵入検知・防止システムのログから攻撃者の挙動を調査するにあたり、攻撃元となるIPアドレスが所属するネットワークの情報を取得し、分析に利用した。これによって攻撃者が利用している資源にどのような傾向があるかを確認することができた。

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 with IP address attribution

Masayoshi Mizutani[1]　Yuji Watanabe[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. In this paper, we use information of IP address that is detected as malicious host such as IP address registration. Then, we summarize our investigation of attacker's behaviour.

Keywords: Network Security, Intrusion Detection System, Log Analysis

1. はじめに

インターネットにおけるセキュリティ侵害を目的とした攻撃方法は年々変化を続けている．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，ファイヤウォールや侵入検知・防止システム (Intrusion Detection and Prevention System, IDPS)，アンチウィルスソフトウェアをはじめとするPC上のセキュリティソフトの普及などによって，PCを標的としたそのような攻撃は2010年頃までに現象の傾向にあった．一方でPCを標的とした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．これは各種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，デジタルビジネスの普及やサービスのクラウド化などにともない，定常的に稼働する公開サーバへの攻撃は継続的に発生している．

一方ネットワーク上で悪意ある行為をする場合には，PCをマルウェアに感染させて攻撃者からの任意の命令を実行させるボット，そしてその集合体であるボットネットが利用されるようになった．2000年頃からボットネットによる攻撃は増加し，インターネット上における悪意ある行為の中核を占めていた．攻撃者はボットネットを用いて分散型サービス妨害攻撃 (Distributed Denial of Service, DDoS)

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

や情報搾取，さらにボットネットを拡大させる攻撃に利用してきた．しかし，近年ではボットネットだけが攻撃の中核ではなく，ランサムウェアや金融マルウェアの増加 [4] による被害の拡大や，イントラネット内の PC を狙った DbD 攻撃は減少し [6] メールを利用した攻撃へと推移しており，ボットネットの拡大とは違った方向で個人の PC などが脅威にさらされている．またクラウドサービスの増加にともない，クラウド上のホストを不正に利用しての攻撃も増加しつつある．

本稿では，このような環境において公開サーバへの攻撃してくるホストにどのような特徴があるのかを調査し，報告する．筆者らは以前に攻撃元 IP アドレスを起点として長期的な振る舞いの調査 [5] を実施したが，その結果には大きくわけて 2 つの課題があった．まず 1 つ目は送信元 IP アドレスの特性を考慮していない，という点である．誤検知を除去するために脆弱性診断を実施していると考えられる通信元や Content Delively Network (CDN) からの通信によるイベントは除去したが，それ以外の送信元 IP アドレスについては均一的に扱っている．インターネットプロトコルにおいて IP アドレスはホストの抽象化された形ではあるが，セキュリティを論ずる上でより詳しいホストの分類をしなければならないと考えられた．2 つ目は検知内容の精査が不十分な点である．攻撃内容の大まかな分類を示して見せたが，検知結果から誤検知であるかどうかの判定はしていなかった．また，分類のみで個々のイベントに対する深い分析までは実施しなかった．そのため本稿では次の 2 点について考慮した上で，分析を実施した．

- 送信元 IP アドレスの調査: 分析の対象となる IP アドレスがどのような特性をもつかについて，その IP アドレスが所属する組織や IP アドレスに紐付けられた逆引き名などから分類を実施した．今回は日本の ISP が所有しているクライアント用とみられる IP アドレス郡，クラウドおよびホスティング事業者が所有する IP アドレス郡の 2 つを抽出し，それらの比較や分析結果について論じた．
- 検知内容のより深い調査: 検知内容に対して誤検知と判断されるものを除去した上で分析を実施した．誤検知の判定には検索エンジン向けのクローラーによるアクセスを利用し，悪意ないアクセスであっても検知をしてしまうイベントを特定し，それらを分析前に除去するようにした．

これらの結果から日本国内の ISP と大手クラウドおよびホスティング事業者から発せられるイベントの傾向の違いが明らかになった．また，公開サーバへの攻撃はクライアント PC に感染したボットによるものだけではなく，クラウドおよびホスティングサービスが積極的に使われるようになっているといった傾向が確認できた．

2. データの収集条件と事前処理

本稿では IBM Tokyo SOC で 2016 年 10 月 1 日から 2017 年 6 月 30 日まで観測された IDPS 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．観測している組織には商業，金融業，製造業，電気・ガス業，情報通信業などの企業を含む．IBM Proventia GX シリーズおよび XGS シリーズを監視機器として用いており，シグネチャは常に最新のものが適用されている．

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 IDPS は，ネットワーク上で発生するセキュリティ関連のイベントを広く検知する機能を持つ．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，あるいは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，定常的に稼働しているサーバに対しての不正行為を分析するため，検知された全てのイベントから以下の 3 種類のイベントを抽出した．

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．対象となる攻撃を抽出したところ，233,705,901 件のイベントが確認された．このイベントの集合を D_{all} とする．D_{all} には 2,086,007 件の攻撃元 IP アドレスが確認された．

2.2 対象となる送信元の抽出

本稿では攻撃元の IP アドレスの特性を分析するために，D_{all} から日本国内の ISP が所有する IP アドレスおよび，クラウドおよびホスティング事業者が所有する IP アドレスからのイベントを抽出した．

2.2.1 日本国内の ISP からのイベントの抽出

日本国内の ISP から 21 社を対象として，イベントの抽出を実施した．対象となった ISP は D_{all} において観測された IP アドレス数の上位 21 社となっている．IP アドレスの特定は X-Force Exchange[2] で提供される API を経由した IP アドレス登録者情報の問い合わせ，および IP アドレスの DNS 逆引きによって得られた名前を参考としている．これは IP アドレスが ISP 事業を展開している企業に所属しているものであったとしても，別の事業で利用され

ているケースや管理用の IP アドレスとして利用されるものも含まれるためである．対象には家庭用のインターネットサービスおよび携帯電話など移動体通信用のインターネットサービスも含めている．この手順によって抽出されたイベントを D_i とする．$|D_i| = 14,471,906$ である．

2.2.2 クラウドおよびホスティング事業者からのイベントの抽出

クラウドおよびホスティング事業者からの IP アドレスは，各社が公表している IP アドレスレンジの情報，IP アドレス登録者情報および IP アドレスの DNS 逆引きを利用した．本稿ではクラウドを API 経由でサーバ (インスタンス) 起動できるサービス，ホスティングがそれ以外だと識別しているが，議論の上ではこの 2 つを区別しないものとする．クラウド事業者は自身が所有しユーザが利用する想定の IP アドレスレンジが公開されており，本稿では 2017 年 8 月 15 日時点の IP アドレスレンジのリストを利用した．対象とした事業者は 7 社である． D_c とする．$|D_c| = 3,230,065$ である．

2.3 誤検知イベントの除去および高脅威イベントの抽出

本稿で利用するデータは通常の IDPS の運用から得られたものであり，誤検知 (False Positive, FP) のイベントが含まれている．本稿では FP を「攻撃の意図がない通信を攻撃と判断してしまった検知」と定義する．攻撃の意図があったが攻撃が失敗に終わったものについては誤検知とはしない．FP のイベントは分析結果に対するノイズとなるため，目視による確認および Web クローラを利用した誤検知判定の 2 つの方法で FP のイベントの除去を実施した．

2.3.1 目視による FP の除去

今回の分析に使うイベントを収集した IBM Proventia GX シリーズおよび XGS シリーズには検知したイベントに関する通信のパラメータを一部保存する機能が実装されている．これを利用し，`HTTP_JBoss_JMX_Console_Exec` および `HTTP_Apache_Struts2_Exec` のシグネチャによって検知されたイベントに攻撃コードと考えられるデータが付随していなかったものについて FP であると判断した．

また，`TLS_OpenSSL_Ticket_DoS` のシグネチャについても誤検知を発生させる可能性があることがリリースノートにおいて報告されているため，一括して FP として除外した．

2.3.2 Web クローラを利用した FP の除去

しばしば Web サービスでは攻撃の意図無くアクセスしたにも関わらず，攻撃と判定されてしまうような通信が発生する場合がある．これは当該 Web サービスが攻撃と判定されてしまいやすい URL が生成される，あるいは送信するデータにそのようなコードが必然的に含まれてしまう，といった場合がある．

このような FP を除外するため，本稿では検索エンジンのための Web クローラからのアクセスに着目した．Web クローラは基本的に Web ページ上に設置されたリンクを巡回し，インターネット上の Web コンテンツを収集することを目的に動作している．そのため攻撃の通信を意図的に生成することは考えづらく，攻撃として検知された場合，それは正規のアクセスによるものであったと考えられる．よって Web クローラがアクセスした宛先と検知したイベントのシグネチャを組み合わせることで FP と判定するためのパターンを作成することができる．

本稿では D_{all} に出現した IP アドレスから，IP アドレスの逆引きによって 3,421 件の IP アドレスを Web クローラと特定した．この IP アドレスから発生した 363,201 件のイベントを用いて 15,977 件のパターンを作成した．パターンには検知したイベントのシグネチャ，宛先となったホストのホスト名，もしくは宛先 IP アドレス，および存在する場合は URL を含めた．このパターンのシグネチャとホスト名，および存在する場合は URL に一致するイベントは FP と判断し，除去した．

2.3.3 高脅威イベントの抽出

第 2.3.1 節，第 2.3.2 節での手順により明らかな FP は除去できるが，実際には IDPS から検出されるイベントはそれが攻撃なのか判断するのが難しいイベントが多く発生する．そのため，システムへの侵入や改竄を目的としていると考えられる表 1 に掲載されたシグネチャによるイベントを高脅威イベントし，このイベントを含む IP アドレスを高脅威であると判断した．シグネチャは Struts2[1] の脆弱性に関連したもの，SQL インジェクションに関連したもの，JBoss の脆弱性に関連したもの，Joomla![3] の脆弱性に関連したもの，SSH に対する BruteForce 攻撃を対象としたものを含む．これらのイベントで検知された IP アドレスを抽出し，さらに当該 IP アドレスから発生した全てのイベント群を抽出した．

3. 分析および考察

3.1 イベントの分類

第 2 節で述べた手順に従って D_{all} を分類した結果を表 2 に示す．FP の除去を実施したことにより，D_{all} は 24.00%，D_c は 72.06%，D_i は 33.76%のイベントを取り除いた．D_{all}, D_c, D_i から FP を除去して残ったイベントをそれぞれ E_{all}, E_c, E_i とする．また，第 2.3.3 節の方法で E_{all}, E_c, E_i から高脅威のイベントを抽出したものを，H_{all}, H_c, H_i とした．E および H のイベント郡に関するデータの概要を表 3 に示している．

表 2 および表 3 において特徴的なのが H_i および H_c における IP アドレス数である． E_i は国内の ISP 21 社からの通信で観測されたイベントから FP を除外したものとなっており，観測された IP アドレスは 530,886 件におよんでいる．しかし高脅威のイベントが観測された IP アド

表 1: 高脅威と判断するために着目したシグネチャ一覧

HTTP_Apache_Struts2_Exec
HTTP_Apache_Struts2_FilePath_Exec
HTTP_GET_SQL_Convert_Int
HTTP_GET_SQL_OpenRowSet
HTTP_GET_SQL_Select_Count
HTTP_GET_SQL_UnionAllSelect
HTTP_GET_SQL_UnionSelect
HTTP_GET_SQL_WaitForDelay
HTTP_JBoss_Console_Authentication_Bypass
HTTP_JBoss_JMX_Console_Exec
HTTP_Joomla_SessionDeserialization_Exec
HTTP_POST_SQL_Convert_Int
HTTP_POST_SQL_OpenRowSet
HTTP_POST_SQL_Select_Count
HTTP_POST_SQL_UnionAllSelect
HTTP_POST_SQL_UnionSelect
HTTP_POST_SQL_WaitForDelay
HTTP_Ruby_on_Rails_Hash_SQL_Injection
SSH_Brute_Force

レスは H_i において 835 件であり，元の約 0.16% となっている．一方で，クラウドおよびホスティング事業者 7 社からの通信から検知され FP を除外したイベントの E_c では観測された IP アドレスが 6,639 件であったのに対し，高脅威イベント H_c の IP アドレスは 1,163 件となっており，元の約 17.52% となっており，国内 ISP からのイベントと比較すると著しく割合が大きい．

これは PC に感染するマルウェアによる経済的利益を得るアプローチが，ボットネットではなくランサムウェアや金融マルウェアにシフトしたのではないかと推測される．国内の ISP から観測される攻撃もクラウドおよびホスティング事業者から観測される攻撃も同等の確率で観測されると仮定した場合，主に PC，あるいはスマートフォンである推定される国内の ISP に所属するホストが直接的に攻撃に利用されにくい状況となっているのではないかと考えられる．未だに PC に感染するボットは存在するものの，近年ではランサムウェアや金融マルウェアによる被害も増加しており [4]，攻撃者の経済的利益を得る手段として確立しつつある．ランサムウェアや金融マルウエアと外部に攻撃をかけるようなボットへの感染は技術的に可能だが，ある時点でユーザ自身に発覚しやすいランサムウェアや金融マルウエアと潜伏を続けたいボットでは相性が悪いと考えられる．このような背景を踏まえると，ユーザが利用する PC ではなくクラウドやホスティングのホストの方が攻撃者にとって利用しやすくなっているのではと推定される．

3.2 IP アドレス毎のイベント検出期間

図 1 は $E_{all,i,c}$ において，各 IP アドレスからのイベントが観測された最初の時刻と最後の時刻の差を秒で表し，累

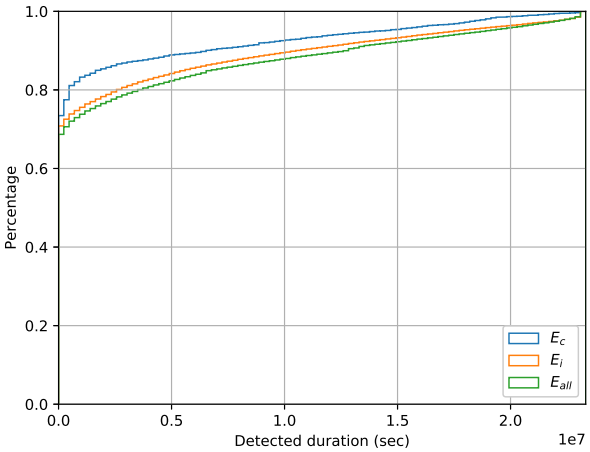

図 1: $E_{all,i,c}$ における IP アドレス毎の検知期間 (270 日)

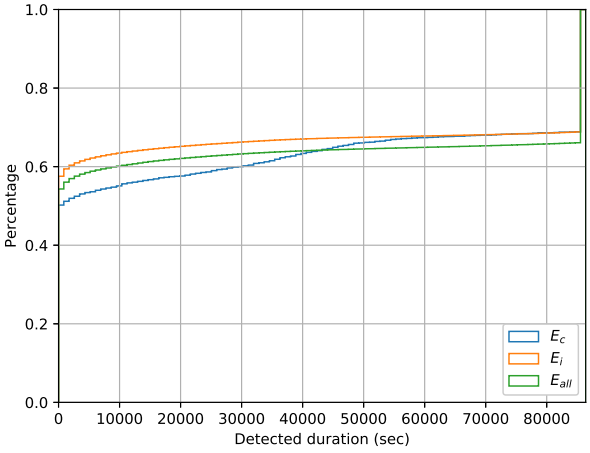

図 2: $E_{all,i,c}$ における IP アドレス毎の検知期間 (1 日)

データセット	イベント数	FP 除外後イベント数 ($\|E_x\|$)	FP イベント数	攻撃元 IP アドレス数
D_{all}	233,705,901	177,618,254 (76.00%)	56,087,647 (24.00%)	2,086,007
D_c	3,230,065	902,474 (27.94%)	2,327,591 (72.06%)	17,879
D_i	14,471,906	9,585,697 (66.24%)	4,886,209 (33.76%)	1,009,754

表 2: データセット一覧，IBM Tokyo SOC で 2016 年 10 月 1 日から 2017 年 6 月 30 日まで IDPS によって検知されたイベントより．イベント数のパーセンテージ表示は元となったイベント数に対する割合，小数点第 3 桁を切り捨て

データセット	イベント数	攻撃元 IP アドレス数
E_{all}	177,618,254	1,227,455
E_c	902,474	6,639
E_i	9,585,697	530,886
H_{all}	24,936,938	32,047
H_c	295,698	1,163
H_i	163,008	835

表 3: 分類後のデータセット一覧

積度数分布で示している．このグラフでは観測された最初の時刻と最後の時刻の間に発生したイベントの回数は考慮されていない．X 軸の最大値は 23,328,000 秒であり，270 日を表している．また，図 2 は図 1 と同じ方式で累積度数分布を示したものから最初の 1 日分（86400 秒以下）の部分を切り出している．

図 1 および図 2 の結果は，筆者らが 2016 年 1 月 1 日から 2016 年 6 月 30 日までのイベントを調査した結果 [5] と類似している．検知されたイベントが 60 秒未満でそれ以降出現しなかった IP アドレスは D_{all} で約 42.42%，E_{all} で約 46.28%であった．FP が除去されることで 60 秒未満しか観測されなかった IP アドレスは増加する傾向が見られるが，2016 年 1 月 1 日から 2016 年 6 月 30 日のデータでは約 46.49%とほぼ類似した結果が得られている．

図中では同様に E_c, E_i のデータも示している．図 2 において前半では IP アドレスに対してややずれが見られるが，後半は収束する傾向にある．しかし図 1 ではクラウドおよびホスティング事業者からのイベントである E_c が E_{all} および E_i より全体的に観測期間が短くなっている傾向が分かる．これは第節においても述べるが，クラウドおよびホスティング事業者においてはネットワーク内で発生しているインスタンスが外部に対して問題行為を実施した場合に事業者として措置をとれるようになっており，問題を迅速に対処できるのが要因なのではないかと考えられる．一方で ISP の場合は契約している端末がマルウェアに感染していたとしても積極的に介入できないため，継続して攻撃が発生しやすいのではないかと考えられる．

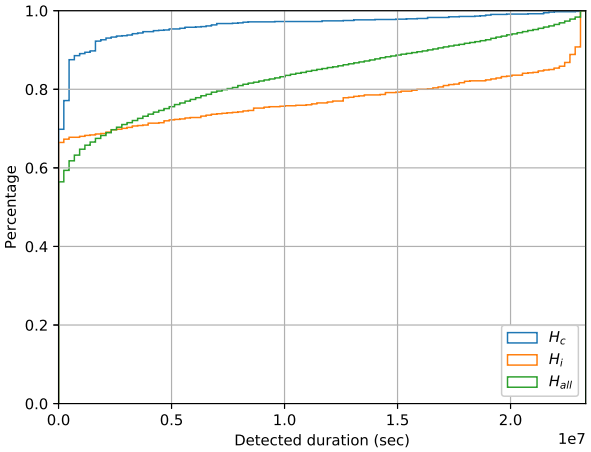

図 3: $H_{all,i,c}$ における IP アドレス毎の検知期間 (270 日)

3.3 高脅威の攻撃が検知された IP アドレスについての分析

第 2.3.3 節で述べた通り，IDPS で検知するイベントには攻撃か誤検知かを判断するのが難しいイベントも多いた

め，本稿では特に攻撃と判断できるイベントの分析をするため高脅威のイベントを特定した上で，その IP アドレスが発生させるイベント郡をそれぞれ H_{all}, H_c, H_i として分類した．図 3 は H_{all}, H_c, H_i を用いて 図 2, 1 と同じ方式で観測された期間の累積度数分布を示している．

全体のイベントから高脅威イベントを抽出した H_{all} は図 2, 1 と類似した 傾向となっているが，H_c, H_i については異なる傾向が現れている．国内の ISP からの通信で観測されたイベントの H_i は約 2,500,000 秒 (約 29 日) 近くまでは全体の H_{all} と比べて継続して発生するイベントは少ないが，そこからは上昇が遅く 20%以上の IP アドレスが約 15,000,000 秒後 (約 173 日後) にも イベントが検知されている．一方でクラウドおよびホスティング事業者である H_c は約 2,000,000 秒 (約 23 日) 以上検知が見られた IP アドレスは 10%未満となっており，長期間に渡って活動していたホストは ISP でのホストに比べて少ない割合になっていることがわかる．

同様の手法で検知期間を描画した図 2, 1 と比較しても顕著な違いがあらわれており，第 3.3 で述べたようにクラウドおよびホスティング事業者が特に高脅威として捉えられるような攻撃に対し，迅速に対応しているものと考えられる．一方，第 3.1 節と第節で述べたように，高脅威イベントが発生した IP アドレスは割合および絶対数ともにクラウド・ホスティング事業者より ISP の方が少ないものの，事業者が積極的に対処しにくいという点で攻撃が持続しやすい傾向があると見られる．

3.4 イベントの無検知期間

イベントの最初の検知と最後の検知が長期間になる IP アドレスも一定数いることが図 1 で示されているが，これらは全てが継続的にイベントを発生させているわけではない．そのため，期間中にイベントが検知されない時間の割合を調査した．図 4 が $E_{all,i,c}$ のイベントを対象とした場合，図 5 が $H_{all,i,c}$ のイベントを対象とした場合のイベント無検知時間割合の累積度数分布を示している．無検知時間は，ある IP アドレスに対して検知したイベントの時刻が $t_1, t_2, ...t_{e-1}, t_e$ であったとして，$t_n - t_{n-1} > 86400$ の場合，$t_n - t_{n-1}$ を無検知時間 T_s に加算し，$t_n + 86400 < t_x$ となる t_x が現れた場合に再び無検知時間の加算の条件判断に戻る．無検知時間割合は $\frac{T_s}{t_e - t_1}$ で計算される．これによって期間中の何日程度活動していたかを知る指標とする．無検知時間割合が高い IP アドレスは期間が長かったとしてもまれにしかイベントを発生させていなかったということが分かる．一方で無検知時間割合が低ければ頻繁に活動していたと判断できる．

$E_{all,i,c}$ を対象としている図 4 では若干の差はあるものの概ねそれぞれ同じ傾向が見られる．一方，高脅威イベントを対象としている図 5 では H_{all} が示す全体の傾向と

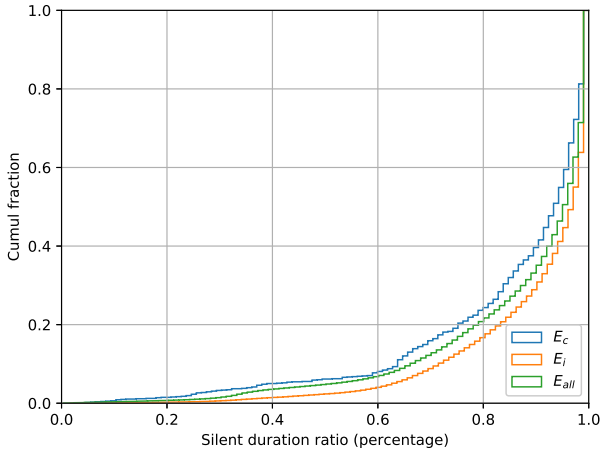

図 4: $E_{all,i,c}$ における IP アドレス毎のイベント無検知時間割合の累積度数分布

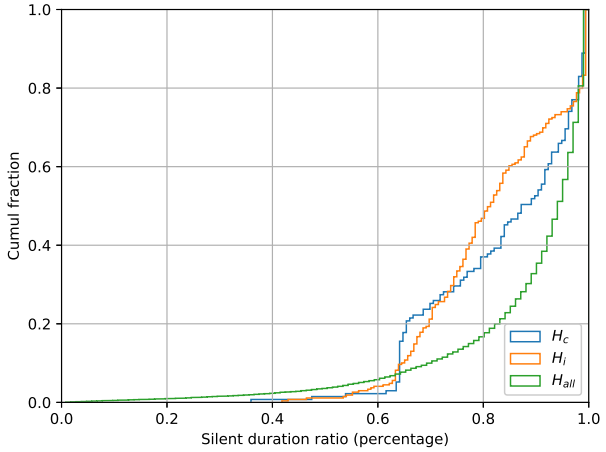

図 5: $H_{all,i,c}$ における IP アドレス毎のイベント無検知時間割合の累積度数分布

H_c, H_i に差が見られる．図 5 では無検知時間割合がおよそ 64%の時点で H_c が全体の 20%以上の IP アドレスが該当し，H_i も無検知時間割合がおよそ 70%を超えた段階で全体の 20%以上の IP アドレスを含んでいる．これは H_{all} および $E_{all,i,c}$ の結果と比較すると無検知時間が低めの IP アドレスが多いということを示している．

図 5 において H_c と H_i に活発に攻撃をしている IP アドレスが多い理由として，攻撃者は明確な攻撃をする際にできるだけ攻撃に利用するホストの稼働率をあげていることが考えられる．攻撃をするホストの場合，特にクラウドなどの環境だと検知・駆除される可能性が高いため，攻撃をはじめたホストはなるべく多くの攻撃対象に対して攻撃を仕掛けた方が有利である．そのため，他の攻撃活動に比べてより活発にイベントが発生するという推測が考えられる．

4. 考察

本稿では IDPS が検知した IP アドレスの挙動を調べるにあたり，対象となる IP アドレスの属性について調査し，さらに検知したシグネチャに基づいて FP の除去や高脅威イベントの抽出を実施した上で分析を実施した．本稿の対象とした 2016 年 10 月 1 日から 2017 年 6 月 30 日までのデータは全体の傾向として 2016 年 1 月 1 日から 2016 年 6 月 30 日のデータの検知結果と類似していた．一度観測された IP アドレスの約 40%から 50%は最大で 9 ヶ月間再度観測されることはない一方で，約 10%から 20%の IP アドレスについては 30 日間たった後も再び観測されている．対象となる IP アドレスが日本国内の ISP であるかクラウドおよびホスティング事業者であるかによってやや差分はあるが，観測された攻撃全般では全体と似た傾向を示した．一方で任意のコマンド実行を可能にするフレームワークの脆弱性を狙った攻撃や SQL インジェクション，あるいはリモートログインの Burte Force 攻撃など，高い脅威であると考えられる攻撃に注目することによっていくつかの傾向が明らかになった．

まず，公開サーバに対して高脅威な攻撃をするホストは，全体からするとかなり小さい集合であるということがわかる．インターネット全体を対象としても 32,047 件で検知したイベント 2,086,007 件に対して約 1.54%となっている．観測期間が 9 ヶ月であり，ある程度の規模の観測をしていることを考慮してもこのような攻撃をしているホストは限られているということが分かる．さらに国内 ISP やクラウドを対象に見れば合計で 1,998 件とさらに規模が小さくなる．これは高脅威のイベントを検知させる IP アドレスを抽出する前と比較しても約 0.37%となっており，インターネット全体から見ても脅威となるホストが少ないネットワークであると言える．

高脅威イベントの合計数は少ないものの，クラウドおよびホスティング事業者からの IP アドレスが国内 ISP より多く発生していたのは注目すべき点であると考えられる．第 3.1 節で示した通り，検知されていた全体の IP アドレスは国内 ISP の方が多かったにも関わらず，高脅威攻撃に利用されていた IP アドレスはクラウドおよびホスティング事業者の方が多かった．一方，第 3.3 節で示した通り，クラウドおよびホスティング事業者上で高脅威の攻撃が発生した場合は比較的速い段階で検知，対応されている．今回，調査の対象としたのが比較的大きい規模の事業者であったため，悪意ある行動をしているホストへの対応が迅速に執り行われているということが分かる．これらの事象から，以下の点が推測される．

- 公開サーバへの攻撃はクライアント PC に観戦したボットによるものだけではなく，クラウドおよびホスティングサービス上のリソースが積極的に利用されるようになっている
- しかしクラウドおよびホスティングサービス上のリソースは不正行為を迅速に検出・対応されている傾向があり，少なくとも正規の事業者のものは攻撃者にとって利用しやすいとは言えない状況である

5. 今後の課題

今後の課題として，より多様な IP アドレスの属性を調査する必要がある．今回は国内の ISP とクラウドおよびホスティング事業者を対象としたが，検知された IP アドレスのごく一部である．特に近年では Bulletproof ホスティングが積極的に利用されるようになっているため，大手のクラウドだけではなくより多様な事業者について調査する必要がある．

また，本稿ではより攻撃のみに着目して分析ができるよう検知結果から FP を除去する作業を実施したが，十全に FP が除去できているとは言い難い状況である．これはイベント数の多さだけではなく，攻撃対象となる公開サーバのログなど，イベント以外の情報が利用できない場合における FP 除去手法が乏しいためである．今後は，本稿で試みた Web クローラを利用した手法など，イベント情報を中心とした手法を検討する必要がある．

6. まとめ

本稿では IP アドレスを基点とした長期的な攻撃の振る舞いの分析において，より詳細な分析を実施するために IP アドレスの特性や検知したイベントの特性を考慮した分析を実施した．これによって近年の攻撃者がクラウドおよびホスティングといったリソースを積極的に利用している傾向を発見した．

参考文献

[1] The Apache Software Foundation. Apache struts, 2000. https://struts.apache.org.

[2] IBM. IBM X-Force Exchange, 2014. https://exchange.xforce.ibmcloud.com/.
[3] Inc. Open Source Matters. Joomla!, 2005. https://www.joomla.org/.
[4] トレンドラボ. *Trend Labs 2016* **年年間セキュリティラウンドアップ**. トレンドマイクロ株式会社, 2017.
[5] 水谷 正慶. 長期的な攻撃元ホストの振る舞い調査. **情報処理学会** *Computer Security Symposium 2016*, Oct 2016.
[6] 窪田 豪史 茂木 大輔 柳 優 藤田 香凛 野ヶ山 尊秀 小倉秀敏 水谷 正慶 鳥谷部 彰則, 猪股 秀樹. *2016* **年下半期** *Tokyo SOC* **情報分析レポート**. 日本アイ・ビー・エム セキュリティサービス, 2017.