研究指導　中澤 真 准教授

悪性通信に対するパケットの収集と分析 –パケットの発信元国と攻撃パターンの関係–

樋口　風音

1.　はじめに

インターネットによって人々の生活は便利なものになったが，それを悪用して企業や官公庁にサイバー攻撃を仕掛けるといったことも起きている[1][2][3]．このため，個人，法人等にかかわらず不正アクセスなどのサイバー攻撃への対応策をとることが必要になっている．しかし，対策をしていてもサイバー攻撃による事件は増加しており[4]，被害の影響も大きくなっている．このような被害を防ぐためには，攻撃の特徴を詳細に把握しなければならず，そのためにはネットワーク上を流れるパケットを取得・分析する必要がある．

そこで，本研究ではネットワーク上のパケットを収集・分析し，攻撃パケットの発信元となる地域の特性や攻撃対象となるサービスの特徴を明らかにする．傾向を把握できれば，特定の対象に絞った監視や防御が可能になり，監視や注意を集中できるため，コストと効果のバランスが取れたセキュリティ対策が期待できる．

2.　近年のサイバー攻撃

2.1　インターネットを悪用した犯罪

パソコンやスマートフォンの普及により，多くの人々がインターネットを利用できるようになった．しかし，人々の生活にインターネットが欠かせないものになっていることを逆手に取り，DoS/DDoS 攻撃や標的型攻撃メールなどのサイバー攻撃に利用されてしまうことも多くなり社会問題となっている[4]．2015 年にはセブン銀行などにDDoS 攻撃がしかけられたこと[1]や，最近では，通信販売サイトで不正アクセスが行われ，顧客のクレジットカード情報が流出した可能性があると発表されている[3]．

2.2　不正アクセスへの対策

不正アクセスの対策には，ファイアウォールや IDS(不正侵入検知システム)が一般的に用いられる．これらのシステムは，コンピュータにアクセスしようとする不正な侵入やマルウェアなどの悪性な通信を判別し，遮断する機能を持っている．しかし，セキュリティを厳重にしても，近年のサイバー攻撃では，ウェブサイトの閲覧者へのウイルス感染やフィッシングサイトへの誘導を狙ってウェブページを改ざんするなど攻撃者の手口が巧妙化しているため[5]，サイバー攻撃による被害が後を絶たない．

このような不正アクセスの被害を防ぐためには，攻撃パケットの内容を詳細に把握する必要がある．パケットを分析することで，時間や攻撃元，攻撃先のポートなどがわかる．それらに特徴があれば，その国からのアクセスを注意深く監視することやポートのセキュリティを厳しくするなどの対応ができ，サイバー攻撃を未然に防ぐことや被害を軽減することが可能になる．

そこで本研究では，ネットワーク上に流れるパケットを取得・分析するためのツールである Wireshark[1]を用いて，どのような攻撃パケットがネットワーク上を流れているのか分析し，地域やポート番号等の特徴を明らかにする．

3.　不正アクセス対策としてのパケットとアクセスログの分析

不正アクセスへの対策として攻撃を分析する方法には，パケットの分析の他にアクセスログを分析する方法もある．アクセスログ型では，サービス内容と直結したログを記録するため，攻撃手段の解明が比較的容易にできる．しかし，特定のサービスについての記録しかないため，網羅的に攻撃に関する情報を集めることが難しい．一方で，パケットキャプチャ型では網羅的に情報を収集できるが，パケット単位のデータとなるため解析の手間がかなり大きくなってしまうという短所がある．

以下では，これら二つの方法を用いた研究事例について述べる．

3.1　攻撃パケットの特徴抽出分析

不正アクセス対策としてのパケット分析を用いた事例としては田中らの研究[6]が挙げられる．田中らはマルウェア 5 検体を長期観測したパケットを分析している．そこから，正常通信と悪性通信との差異を検出し悪性通信の判定に使用できる可能性のある特徴を抽出している．この研究では，マルウェアに感染したコンピュータからは定期的なパケットが送信されていることや，特定のサイズのパケットの割合が高くなるなど悪性通信と判別できるパターンを示している．しかし，この研究の目的は，マルウェアに感染した端末の挙動を分析することであるため，多種多様な攻撃に対して網羅的に分析するには適していない．

3.2　Honeypot のアクセスログの分析

Honeypotはクラッカーの侵入手法やウイルスの挙動などを調査するために，インターネット上に設置されたセキュリティが甘いサーバやネットワーク機器を指す．悪意のある攻撃者からの攻撃を誘うために，何らかの有益な情報を保有させたり，故意にセキュリティを甘く設定したりすることで，おとりとして稼動させるのである．このため，本来であればHoneypotに正規の通信が届くことがないことから，アクセスが試みられた記録はすべて悪意のある攻撃とみなすことができる．

この性質を利用して安藤ら[7]は，Honeypot として設置したサーバへのアクセスログを分析することで，攻撃元がどこなのか，時間帯による攻撃数の変化，どのサービスへの攻撃が多いのかを明らかにしている．

1　https://www.wireshark.org/

しかし，攻撃国を特定しただけで，国別あるいは地域別で共通する特徴や相違点などについて明らかになっていない．さらに，サービス内容と直結したログしか記録できずデータを網羅的に取得できないため，ネットワーク全体の傾向をつかむことができない．

そこで，網羅的にデータを取得できるパケットキャプチャ方式を用いて国や地域別にパケットを分析し，パケットの発信元国と攻撃パターンを本研究で明らかにする．

4.　Honeypotを用いたパケット収集実験

パケットの発信元国と攻撃パターンの関係を明らかにするために，まずHoneypotによるパケット収集実験を実施した．2016年10月25日に，会津大学短期大学部のDMZ2[2]という実験用のネットワーク[3]にHoneypotを設置し，2016年11月27日までに受信したパケットをすべて記録した．今回の実験ではパケットを悪性・正常な通信にかかわらずすべて収集している．通常のHoneypotでは，サービスアプリを起動させるが，今回の実験ではサービスを稼動させずにポートをすべてオープンとすることで無防備な状態にし，外部から送られてくるパケットを収集している．なお，パケットの収集にはWiresharkとPcap[4]の二つのソフトウェアを用いている．

設置したHoneypotマシンは何のサービスも提供していないため，このマシンのリクエストに対する応答パケットしか届かないはずである．このため，提供していないサービスのプロトコルであるHTTP，Telnet，SMTPなどのパケットが届いた場合は悪性通信であると判断できる．なお，今回の実験では同一のIPアドレスからの攻撃パケットは，数にかかわらず1回の攻撃とカウントした．

実験で用いたPCやソフトウェアの環境は表1のとおりである．

表1：実験で使用したHoneypot環境

ハードウェア	JP Compaq dc7800p Small Form Factor
OS	Windows Vista Business
ソフトウェア	Wireshark　バージョン2.2.0
	Pcap　　バージョン4.1.3
ポートの状態	すべてオープン

5.　パケット収集実験の結果の分析

5.1　収集した全攻撃パケットの傾向

攻撃パケットの解析することにより，その送信元IPアドレスから発信元の国を特定出ることが可能である．そこでまず，収集した全パケットについて地域ごとに分類し，それぞれのエリアごとの攻撃数を表2に示す．

表2：地域ごとの攻撃パケットの発信数

州	攻撃数	IPアドレス数	攻撃数/IPアドレス数（10万個あたり）
北アメリカ州	3336	1721768448	0.19
南アメリカ州	5168	146937856	3.52
アジア州	16962	862772288	1.97
ヨーロッパ州	9155	749830224	1.22
アフリカ州	587	97914368	0.60
オセアニア州	255	55692544	0.46

表2から，割り当てられているIPアドレス数と攻撃数が比例していないことがわかる．南アメリカやアジアはIPアドレス数が少なくても攻撃数が多くなっていることから，サイバー攻撃に積極的な地域といえる．また，情報技術に疎い途上国を狙って，これらの国のIPアドレスを踏み台にして攻撃を仕掛けていることも予想される．

次に，国別の攻撃数の割合を図1に示す．また．各国に振り分けられたIPアドレス数10万個あたりの攻撃パケットの割合を図2に示す．

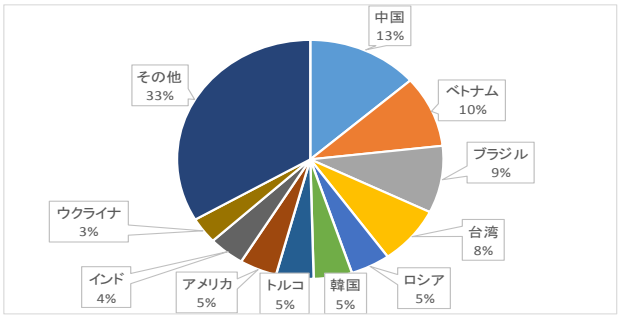

図1：攻撃数が多い上位10カ国

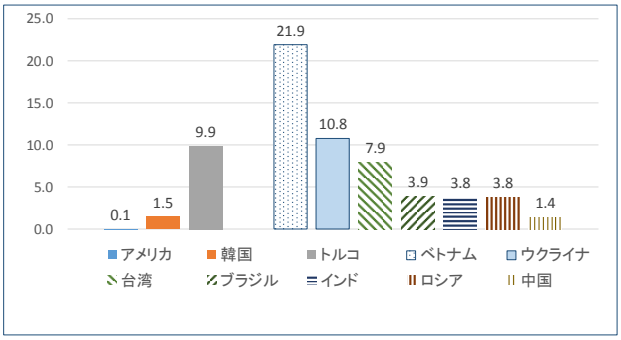

図2：10万個あたりのパケット数

図1から，全体の攻撃数の6割強を10カ国が占めており，アジアの国々からの攻撃が多いことがわかる．特に中国は近年，発展を遂げており，多くの人がインターネットを利用できるようになったため，攻撃数が多くなったのではないかと考えられる．また，図2から，アメリカや韓国といった先進国と比べ，途上国は割り振られているIPアドレス数に対して不正攻撃に利用されるIPアドレスの割合が高い傾向にあることが示された．

さらに，上位10カ国の中から日本と外交的に多くの問題を抱えている国と，日本と良好な関係にある国をそれぞれ3カ国抽出して比較した結果を表3に示す．

表3：日本と問題を抱える国と友好的な国の比較

日本と問題がある	攻撃数	関係が良好	攻撃数
中華人民共和国	4846	ベトナム	3468
ロシア	1721	ブラジル	3260
韓国	1669	台湾	2822
平均	2745.3	平均	3183.3

日本と領土や歴史認識等で問題がある国ならば，攻撃数が多いのではないかと考えたが，実際には友好的

[2] DMZ：DeMlitarized Zoneの略称で，インターネットなどの外部ネットワークと社内等の内部ネットワークから隔離され，中間に置かれた区域のこと．

[3] 学外ネットワークからのすべてのパケットをファイアウォールで遮断することなく通過させる設定にした実験用のネットワーク環境．

[4] http://www.winpcap.org/install/

な国からの攻撃数が多く，政治的な国同士の関係性と攻撃数の間に明確な関係性は示せなかった．

他にも，上位 10 カ国の中に先進国よりも途上国が多いことから，先進国と途上国の攻撃数が多い上位 10 カ国で比較したものを表 4 に示す．なお，先進国，途上国の定義については，OECD に加盟している国を先進国，加盟していない国を途上国としている[8]．

表 4:先進国と途上国の攻撃数の比較

先進国	攻撃数	途上国	攻撃数
韓国	1669	中国	4846
トルコ	1630	ベトナム	3468
アメリカ	1628	ブラジル	3260
メキシコ	1100	台湾	2822
ポーランド	681	ロシア	1721
フランス	468	インド	1571
イタリア	375	ウクライナ	1266
イスラエル	306	ルーマニア	972
イギリス	281	アルゼンチン	691
チリ	277	コロンビア	528
平均	841.5	平均	2114.5

攻撃回数の平均は，途上国の攻撃数が先進国のおよそ 2.5 倍となっており，差があることがわかる．

サイバー攻撃の中には，攻撃者が他の国のサーバを踏み台にすることで，攻撃対象となるサーバやコンピュータに攻撃を仕掛けるものがある．途上国は犯罪などの司法の手が届きにくいことから，先進国が途上国のサーバを踏み台にすることで攻撃元の国を偽装して攻撃を行っていることが考えられる．

5.2　ポート番号に関する分析

ポート番号を分析することで，狙われやすいサービスがどのようなものであるかがわかる．傾向がわかれば，セキュリティ監視などを特定のサービスに集中させることにより，費用対効果の高い対策をとることができる．

まず，ポート別攻撃数の割合を図 3 に示す．次に表 4 に記載した先進国と途上国の国別のポート番号別の攻撃パケットの割合を図 4，図 5 に示す．なお，悪性通信と判断したポートの種別は参考文献[12]を参照している．

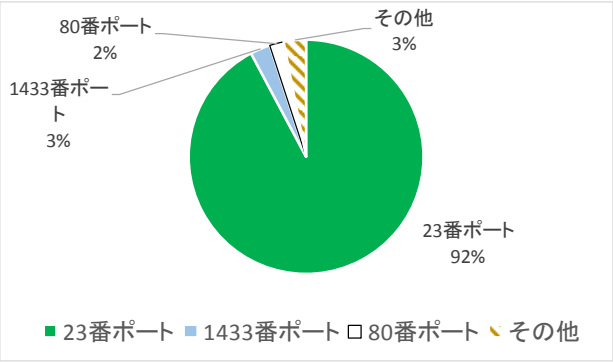

図 3:同一 IP アドレスのポート別攻撃数

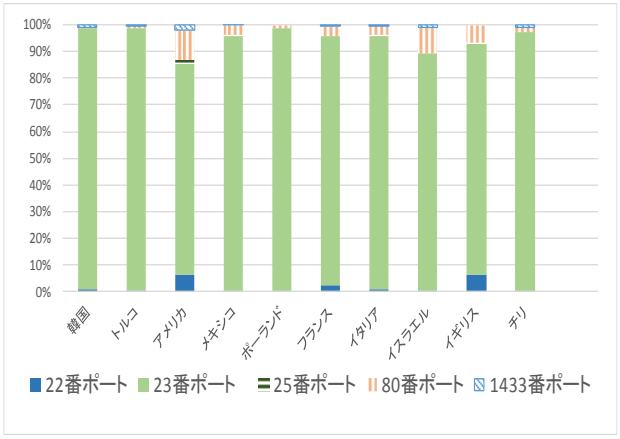

図 4:先進国のポート番号別の攻撃数の割合

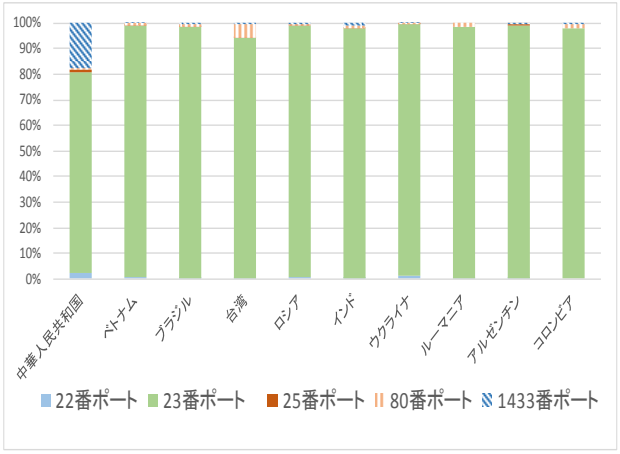

図 5:途上国のポート番号別の攻撃数の割合

これらの図から23番ポートへの攻撃が全体でも，国別でも非常に多いことがわかる．また，先進国と途上国を比較しても構成するポート番号の割合にほとんど差はなかった．

この 23 番ポートは Telnet と呼ばれる，遠隔地のコンピュータを操作するサービスに使われ，悪用すると他人のコンピュータやサーバを乗っ取ることもできてしまう．このような性質から，特に攻撃されやすいポート番号になっていることが考えられる．

5.3　同一IPアドレスからの攻撃回数の偏り

悪性パケットの送信元の IP アドレスは様々だが，同じ IP アドレスから何度も攻撃を受ける場合もある．同一 IP アドレスから受ける攻撃回数は最も少なくて 1 回，多いものは 100 回を超える．そこで，同一 IP アドレスからの攻撃回数にどのような偏りがあるか，その構成比を分析する．まず，全体の傾向をつかむために，収集した全パケットの攻撃回数別の構成比を図 6 に示す．同一の IP アドレスからの攻撃回数が 30 回以下の割合が 99%以上となっており，30 回を超えて攻撃をしてくる IP アドレスはごくわずかである．そこで，攻撃数が 30 回以下の IP アドレスに焦点をあて国別の攻撃回数の構成比を図 7，図 8 に示す．

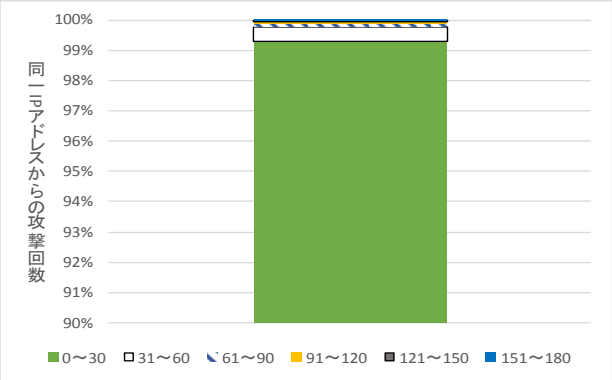

図 6:パケット全体の攻撃回数の構成

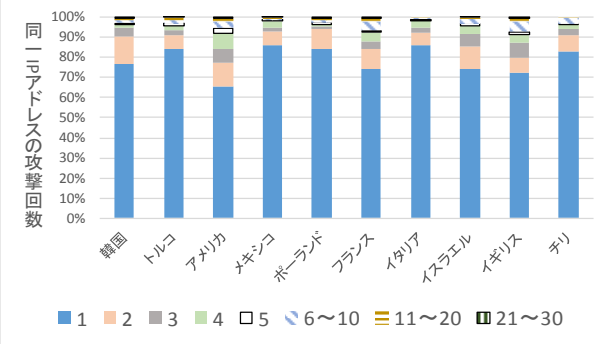

図 7:攻撃回数が 30 回以下の構成(先進国)

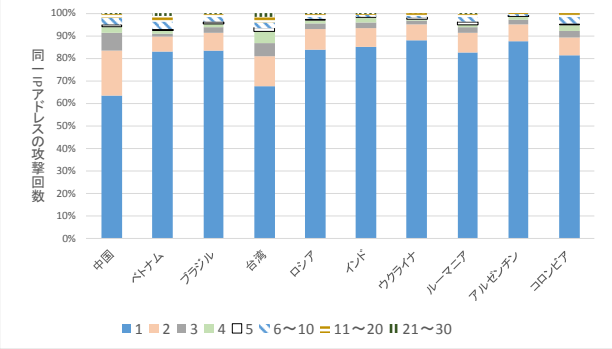

図 8:攻撃回数が 30 回以下の構成(途上国)

先進国と途上国を比較すると，攻撃回数が 1 回限りの IP アドレスの割合が非常に大きく，攻撃回数の増加とともにその割合が小さくなることも共通している．

同一 IP アドレスからの攻撃に偏っているのであれば，IP アドレスを識別して特定の IP アドレスからの攻撃を遮断することができる．しかし，毎回異なる IP アドレスからの攻撃が展開されている場合では，この方法が必ずしも有効になるわけではない．そのため，常に通信の状況を監視して，異常が起きたかどうかを把握し，異常が起きた際にはすぐに対処できるような状態にしなければならない．

6. 研究のまとめ

本研究では，悪性な通信の発信元やポート番号に差があるかを，パケットを収集・分析することで明らかにした．ポート番号には差が見られなかったが，攻撃数については先進国よりも途上国の攻撃数が多いことがわかった．このことから途上国のサーバが先進国の攻撃者の踏み台になっている可能性が考えられる．サイバー攻撃の対策においては情報通信技術が発達しているかどうかに注意する必要があるが，それだけでなく，司法の手が届くかどうかも重要な要素になることが考えられる．

今回は地域とポート番号を対象に分析したが，パケットの情報からは他にも分析できる項目がある．今後は，国ごとの攻撃の時間差やプロトコルなどについても分析をしたい．

参考文献

[1] ITpro, 2016, 1, 18, 金融庁の Web サイトに DDoS 攻撃、「アノニマス」の犯行声明も
http://itpro.nikkeibp.co.jp/atcl/news/16/011800135/?rt=nocnt

[2] 産経ニュース, セブン銀などに DDoS 攻撃　ネットバンク接続不良に警視庁が捜査へ, 2015/7/13,
http://www.sankei.com/affairs/news/150713/afr150713

[3] 日本経済新聞, 資生堂不正アクセスの原因発表, 2017/1/31,
http://www.nikkei.com/article/DGXLASDZ31HQZ_R30C17A1TI5000/

[4] 警察庁, 平成 27 年におけるサイバー空間をめぐる脅威の情勢について,
https://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf

[5] 日本経済新聞, トヨタのサイト改ざん　閲覧でウイルスに感染　情報流出など被害を調査中, 2013/619
http://www.nikkei.com/article/DGXNASDG19048_Z10C13A6000000/

[6] 田中恭之, 畑田充弘, 稲積孝紀, ”パケットキャプチャからみた悪性通信に関する特徴の考察”, コンピュータセキュリティシンポジウム 2013 論文集, pp. 118-124, 2013.

[7] 安藤純一, 壁屋喜槻, 後藤邦夫, ”仮想ホストを用いた攻撃パターンの収集と分析”, アカデミア数理情報編, 第 4 巻, pp. 1-16, 2004.

[8] 内閣府,内閣府ホーム,内閣府の政策,白書等(経済財政白書, 世界経済の潮流), 世界経済の潮流 2016 年
http://www5.cao.go.jp/j-j/sekai_chouryuu/sh16-01/s1_16_0_2.html

[9] IT トレンド, ネットワークセキュリティ, 不正侵入. 防御システム(IDS・IPS), IDS・IPS はファイアウォール, WAF とどう違う？,
http://it-trend.jp/ids-ips/article/difference

[10] 八木毅, 青木一史, 秋山満昭, 幾世知範, 髙田雄太, 千葉大紀, 実践サイバーセキュリティモニタリング, コロナ社, 2016.

[11] 竹下恵, パケットキャプチャ実践技術 Wireshark によるパケット解析応用編, 株式会社リックテレコム, 2009.

[12] Michael Collins, 中田秀基監訳, 木下哲也訳, データ分析によるネットワークセキュリティ, オライリー・ジャパン, 2016.

[13] Chris Sanders, 高橋基信, 宮本久仁男監訳, 岡真由美訳, 実践パケット解析第 2 版-Wireshark を使ったトラブルシューティング, 2012.

[14] 日立ソリューションズ情報セキュリティブログ, セキュリティ用語解説,
http://securityblog.jp/words/