DRDoS ハニーポットが観測した攻撃の履歴を用いた攻撃対象の傾向分析

牧田大佑†‡　西添友美‡　吉岡克成‡
松本　勉‡　井上大介†　中尾康二†‡

†国立研究開発法人　情報通信研究機構
184-8795　東京都小金井市貫井北町 4-2-1
{d.makita, dai, ko-nakao}@nict.go.jp

‡国立大学法人　横浜国立大学
240-8501　神奈川県横浜市保土ケ谷区常盤台 79-1
{makita-daisuke-jk, nishizoe-tomomi-ny}@ynu.jp
{yoshioka, tsutomu}@ynu.ac.jp

あらまし　本稿では，DRDoSハニーポットが2015年1月から6月までに観測したDRDoS攻撃の履歴情報を用いて，DRDoSの攻撃対象の傾向を分析する．分析の結果，期間中にDRDoSハニーポットが観測した73万件の攻撃のうち，24万件（33%）の攻撃は特定の10個のAS（全ASの0.02%）に集中している等，DRDoSの攻撃対象には大きな偏りがあることがわかった．また，定常的に攻撃に晒されていた組織だけでなく，短期間に集中して攻撃を受けた組織が存在することを確認した．本分析結果はDRDoSの攻撃対象にはネットワーク的・時間的な局所性があることを示しており，本知見はDRDoSハニーポットが観測した攻撃の履歴情報を用いたDRDoS攻撃対策技術への応用に期待できる．

An Analysis of Attack Targets Observed by DRDoS Honeypots

Daisuke Makita†‡　Tomomi Nishizoe‡　Katsunari Yoshioka‡
Tsutomu Matsumoto‡　Daisuke Inoue†　Koji Nakao†‡

† National Institute of Information and Communications Technology.
4-2-1, Nukui-Kitamachi, Koganei, Tokyo, 184-8795, Japan
{d.makita, dai, ko-nakao}@nict.go.jp

‡ Yokohama National University.
79-1, Tokiwadai, Hodogaya, Yokohama, Kanagawa, 240-8501, Japan
{makita-daisuke-jk, nishizoe-tomomi-ny}@ynu.jp
{yoshioka, tsutomu}@ynu.ac.jp

Abstract　In this paper, we analyze the trends of DRDoS attack targets using the historical information of DRDoS attacks that our DRDoS honeypots observed from January to June in 2015. As a result, we found that attack targets are heavily biased such as 238,000 attacks (33%) out of 726,000 attacks are concentrated only in 10 ASes (0.02% of all ASes). In addition, we confirmed that there are not only targets that were exposed to attacks regularly but also targets that were attacked many times in a short

term. These results show that some attacks have localities on their target networks and their lives, and it can be expected to develop countermeasures against DRDoS attacks by sharing information of attacks that DRDoS honeypots observe.

1 はじめに

近年，分散反射型サービス妨害攻撃（Distributed Reflection Denial-of-Service Attack; DRDoS 攻撃）がインターネット上の大きな脅威になっている．本攻撃は，インターネット上に不適切な設定で公開されているサーバを踏み台にして多量の通信を攻撃対象に送りつけることにより，攻撃対象の機器のリソースを圧迫してそのサービスを妨害する．

DRDoS 攻撃により発生する通信量は攻撃により様々であるが，2013 年 3 月に発生した Spamhaus への攻撃では 300Gbps，2014 年 2 月の攻撃では 400Gbps もの攻撃通信が観測されたと報告されている[8][9]．このように DRDoS 攻撃の被害は深刻化しているが，その一方で，Booter や Stresser と呼ばれる DDoS 攻撃代行サービスが登場しており[3][4]，攻撃の知識を持たないユーザでも DDoS 攻撃を容易に実行可能な状況になっている．このほかにも，昨今話題となっているハッカー集団の Anonymous や Lizard Squad，企業を脅迫し Bitcoin で身代金を要求する DD4BC[10]の活動でも DRDoS 攻撃が使用されており，今後も本攻撃の脅威は拡大するものと予想される．

そこで我々は，DRDoS 攻撃を観測しその傾向を把握するため，DRDoS ハニーポットを提案し，攻撃の継続的な観測・分析をおこなっている[5][6][7]．本稿では，DRDoS ハニーポットが 2015 年 1 月から 6 月までの半年間に観測した DRDoS 攻撃の履歴を用いて，DRDoS の攻撃対象の傾向を分析する．

分析の結果，DRDoS ハニーポットが半年間に観測した 73 万件の DRDoS 攻撃のうち，24 万件（33%）の攻撃は特定の 10 個の AS（全 AS の 0.02%）に集中している等，攻撃対象の組織や攻撃対象となるネットワークには大きな偏りがあることがわかった．また，多数の攻撃の被害にあっていたネットワークの中には，定常的に攻撃に晒されていた組織だけでなく，短期間に集中して攻撃を受けた組織が存在することを確認した．本稿の分析結果は DRDoS の攻撃対象にはネットワーク的・時間的な局所性があることを示しており，本知見は DRDoS ハニーポットが観測した攻撃の履歴情報を用いた DRDoS 攻撃対策技術への応用に期待できる．

本稿の構成は次のとおりである．まず，2 章で本研究の背景として DRDoS 攻撃と DRDoS ハニーポットについて説明する．次に，3 章で DRDoS 攻撃の観測環境および観測結果をまとめ，4 章で攻撃対象の傾向を分析する．5 章で分析結果について考察し，6 章でまとめと今後の課題を記す．

2 背景

2.1 DRDoS 攻撃

DRDoS 攻撃は，インターネット上に不適切な設定で公開されているサーバを踏み台にして多量の通信を攻撃対象に送りつけることにより，攻撃対象の機器のリソースを圧迫する DoS 攻撃である．効果的な攻撃を実行するため，攻撃者は二つの通信の性質を悪用する．

増幅効果（Amplification）
: 通信の増幅器としての効果．要求よりも応答のサイズが大きくなるプロトコルを悪用することにより，攻撃者は攻撃通信量を増幅させることができる．

反射効果（Reflection）
: 通信の反射板（リフレクタ）としての効果．要求パケットの送信元を確認せずに応答パケットを送信する性質を持つプロトコルを悪用するにより，攻撃者は要求パケットの実際の送信元とは別のホストに応答パケットを送信

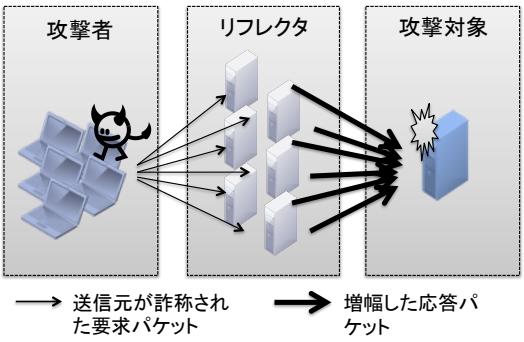

図 1　DRDoS 攻撃

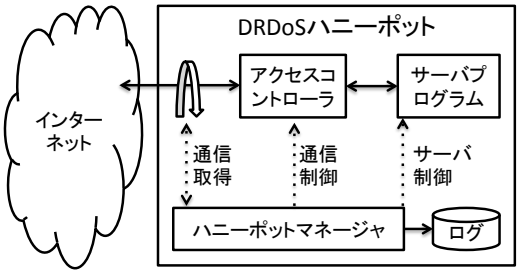

図 2　DRDoS ハニーポットの構成

させることができる.

攻撃者はこれらの性質を悪用し，次の手順で DRDoS 攻撃を実行する（図 1）. まず，攻撃者は，自身が操作可能なホストを利用し，送信元の IP アドレスを攻撃対象のものに詐称した要求パケットをリフレクタへ送信する. リフレクタは応答パケットを実際の送信元ではなく攻撃対象へ送信することになる（反射効果）が，このとき応答パケットは要求パケットよりも大きくなる（増幅効果）ため，攻撃対象のネットワークには増幅した多量の応答パケットが到達する. その結果，攻撃対象のネットワークは飽和しサービス不能状態に陥る.

文献[1]では，インターネット上に存在するリフレクタの数や応答の増幅率等の条件から，UDP 上でサービスを提供する DNS や NTP 等，14 種類のプロトコルが DRDoS 攻撃に悪用可能であると報告されている. また，最近の研究により，これらのプロトコル以外にも，MSSQL や RIPv1，TCP の 3-way handshake 等のプロトコルも攻撃に悪用可能であることが確認されている[2][11][12].

2.2　DRDoS ハニーポット

DRDoS ハニーポットは，DRDoS 攻撃の観測を目的とした囮のリフレクタであり，踏み台の視点から DRDoS 攻撃を観測する.

DRDoS ハニーポットの構成を図 2 に示す. DRDoS ハニーポットは，要求に対する応答を返す「サーバプログラム」，外部への攻撃通信を遮断する「アクセスコントローラ」，これらを制御する「ハニーポットマネージャ」からなる. 2015 年 8 月現在，サーバプログラムにはオープンソースソフトウェアやプロトコルを模擬する簡易スクリプトを使用しており，QOTD (17/udp)，CHG (19/udp)，DNS (53/udp)，NTP (123/udp)，SNMP (161/udp)，SSDP (1900/udp)の 6 種類のプロトコルに対応している. また，上記以外のプロトコルを悪用する攻撃を観測するため，プロトコルに準拠しない独自のサーバプログラムを用いた DRDoS 攻撃の観測もおこなっている[7].

3　DRDoS 攻撃の観測

DRDoS ハニーポットが観測する通信には，DRDoS 攻撃以外にも，リフレクタの探索活動やサーバの脆弱性を狙った攻撃等が含まれる. また，DRDoS 攻撃が発生すると，ハニーポットは多量のパケットを受信するため，パケット単位での分析は困難である. そこで本稿では，ハニーポットが受信した一連のパケットをグループ化し，これを「攻撃イベント」（もしくは単に「攻撃」と呼ぶ）として処理することにより DRDoS 攻撃の分析をおこなう.

本章の構成は次のとおりである. まず 3.1 節で，本稿で分析の対象とする DRDoS ハニーポットの観測環境を説明し，3.2 節で攻撃イベントを定義する. そして，3.3 節で観測結果の概要をまとめる.

3.1　観測環境

本稿では，我々が運用する 6 台の DRDoS ハ

表 1　DRDoS ハニーポットの観測環境と観測結果

ハニーポット ID	稼働日数	IP アドレスの変更回数	観測した攻撃件数						
			QOTD	CHG	DNS	NTP	SNMP	SSDP	計
H01	179	5	16	25,713	35,029	159,535	9	40,845	261,131
H02	180	3	20	39,563	57,204	173,027	7	64,284	334,085
H03	161	5	4	17,448	30,130	118,740	8	46,577	212,903
H04	179	0	26	45,807	46,910	206,384	391	33,948	333,440
H05	178	0	17	45,457	33,538	198,202	8	13,908	291,113
H06	178	2	14	53,591	51,413	170,390	6	41,280	316,680
全体※	181	-	37	92,602	133,963	344,730	400	153,971	725,703

※複数のハニーポットが同じ攻撃を観測する事例も存在するため，各ハニーポットの攻撃件数の和は全体の攻撃件数と一致しない．

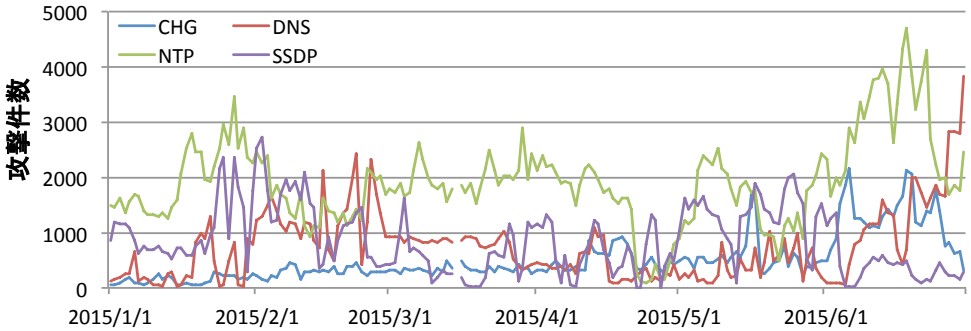

図 3　日ごとの DRDoS 攻撃件数の推移

ニーポット[1]が観測した DRDoS 攻撃を分析する．これらのハニーポットは，日本国内の異なる ISP ネットワークで稼働しており，QOTD・CHG・DNS・NTP・SNMP・SSDP の 6 種類全てのプロトコルに対応している．分析対象とする期間は，2015 年 1 月 1 日から 2015 年 6 月 30 日までの 181 日間である．

3.2　攻撃イベントの定義

本稿では，DRDoS ハニーポットが観測した攻撃を分析するため，次のように DRDoS の攻撃イベントを定義する．

まず，DRDoS ハニーポットが受信したパケットを，受信したハニーポット，プロトコル，送信元 IP アドレス（i.e. DRDoS 攻撃のパケットであれば攻撃対象の IP アドレス）ごとにグループ化する．次に，グループ化された一連のパケットを受信時刻順に並び替え，隣り合うパケットの間隔が閾値 t 秒以下の場合は同じグループのままとし，t 秒を超えたものは別のグループとして分離する．その結果生成されたグループの集合のうち，パケット数が N_{attack} 以上のグループをハニーポットが観測した DRDoS 攻撃イベントとする．ただし，複数のハニーポットが同じ攻撃を観測することがあるため，複数のハニーポットが同時刻に同じ IP アドレス宛の攻撃イベントを観測していた場合には，それらを統合して一つの攻撃イベントとする．

本稿では，暫定的に閾値 t =3600 秒，N_{attack}=100 パケットとして DRDoS 攻撃イベントを抽出した．この閾値の妥当性は別途検証する必要があるが，リフレクタの探索活動やサーバの脆弱性を狙った攻撃等はこの閾値で十分に除外できると考えられる．

3.3　観測結果

DRDoS ハニーポットが観測した DRDoS 攻撃の件数を表 1 にまとめる．DRDoS ハニーポットは，2015 年 1 月から 6 月までの 181 日間に計 725,703 件の攻撃を観測した．プロトコルごとの攻撃件数は，QOTD が 37 件（0.00005%），CHG が 92,602 件（13%），DNS が 133,963 件（18%），NTP が 344,730 件（48%），SNMP が 400 件（0.0006%），SSDP が 153,971 件

[1] これらのハニーポットのほかに，異なる条件で動作するハニーポットを 4 台，計 10 台のハニーポットを運用している．

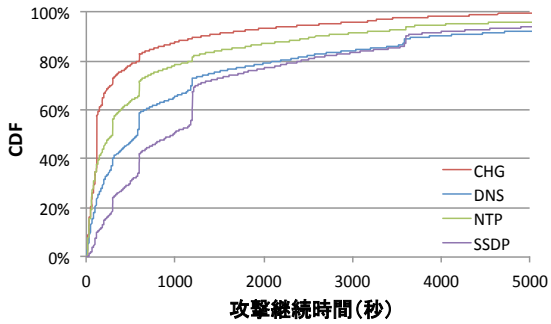

図 4　攻撃継続時間の分布

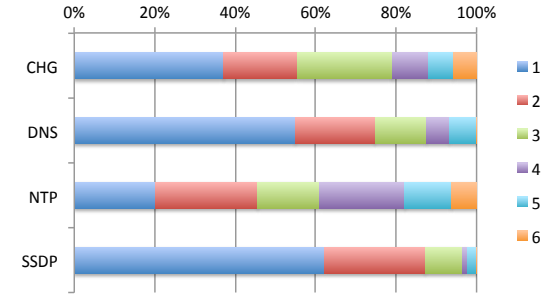

図 5　攻撃を観測したハニーポット数の割合

(21%)であった. QOTD・SNMP を悪用する攻撃はほとんど観測されなかったため，本稿では CHG・DNS・NTP・SSDP の 4 種類のプロトコルを悪用する DRDoS 攻撃を分析する.

まず，日ごとの DRDoS 攻撃件数の推移を図 3 に示す. 2015 年以降，一日平均 4000 件の攻撃が観測されており，最も高頻度で悪用された NTP においては，一日平均 1900 件以上の攻撃が観測された.

次に，攻撃の継続時間の累積分布関数(CDF)を図 4 に示す. 攻撃の継続時間は，300 秒，600 秒，900 秒，1200 秒，3600 秒のような切りのよい時間に分布が偏っていたものの，15 分以下の攻撃が全体の 70%を占めた.

攻撃を観測したハニーポット数(＝何台のハニーポットがその攻撃を観測していたか？)の割合を図 5 に示す. NTP を悪用した攻撃では，全攻撃の 80%以上が複数のハニーポットで観測されていたのに対し，DNS を悪用した攻撃では，攻撃が複数のハニーポットで観測された事例は 40%程度であった.

最後に，同時に複数のプロトコルを悪用する攻撃も観測されていたが，その割合は攻撃全体の 1%程度であったため，本稿では別の攻撃として扱う.

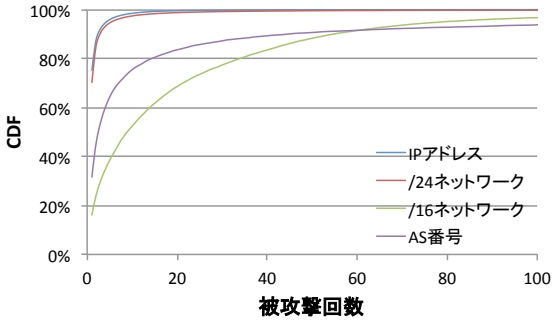

図 6　被攻撃件数の分布

4　攻撃対象の傾向

DRDoS ハニーポットは，2015 年 1 月 1 日から 6 月 30 日までの間に約 73 万件の DRDoS 攻撃を観測した. 攻撃対象になった IP アドレスは約 40 万，AS(Autonomous System)は 10,019，国や地域は 197 に達した[2].

本章では，ハニーポットが観測した攻撃の履歴を使用し，DRDoS の攻撃対象の傾向を分析する.

4.1　被攻撃件数

DRDoS ハニーポットが観測した DRDoS 攻撃の件数の分布を，攻撃対象の IP アドレス，/24 ネットワーク，/16 ネットワーク，AS ごとに集計した結果を図 6 に示す. IP アドレス単位で見ると，攻撃対象の 80%は半年間に 1 件の攻撃しかを受けておらず，10 件以上の攻撃を受けた被害者はわずか 1.5%であった. また，/24 のネットワーク単位で集計した結果も IP アドレスの場合と同様の結果であったが，/16 のネットワーク単位や AS 単位で集計すると，攻撃を受けたネットワーク・AS の 50%以上が半年間に 10 件以上の攻撃を受けていた.

4.2　攻撃対象の偏り

IP アドレス，/16 ネットワーク，AS，国ごとに集計した被攻撃件数の上位 5 位を表 2 にまとめ

[2] IP アドレスが属する AS・国情報は MaxMind 社の GeoIP データベース[13]を用いて推定した.

表 2　IP アドレス・/16 ネットワーク・AS・国ごとの被攻撃件数 Top5

件数	IP アドレス	件数	ネットワーク(/16)	件数	AS（国）	件数	国名
334	[redacted].31.20.35	7,517	11[redacted].28.0.0/16	46,270	AS [redacted]134 (CN)	214,578	United States
333	[redacted].31.103.172	6,117	18[redacted].60.0.0/16	34,949	AS [redacted]7963 (CN)	186,609	China
325	[redacted].163.224.34	4,696	11[redacted].231.0.0/16	30,656	AS [redacted]922 (US)	43,524	France
298	[redacted].28.132.69	4,686	18[redacted].96.0.0/16	30,083	AS [redacted]837 (CN)	26,899	United Kingdom
297	[redacted].1.1.1	4,564	11[redacted].29.0.0/16	27,165	AS [redacted]6276 (FR)	26,420	Germany

表 3　被攻撃件数の上位が占める攻撃件数の割合

攻撃対象	攻撃件数	攻撃対象の総数	攻撃件数の割合		
			Top10	Top100	Top1000
IP アドレス	725,666	398,756	0.4%	1.9%	7.3%
/16 ネットワーク		23,972	6.6%	24.9%	47.9%
AS		10,019	32.9%	66.5%	92.7%

る. 分析対象期間に最も多くの攻撃が観測された IP アドレスは，CDN のサービスを提供するアメリカの会社が所有しており，181 日間に 334 回の攻撃が観測された. また，/16 のネットワークで集計すると，中国の IT 企業が所有するネットワークが最も多く攻撃を受けており，AS 単位でも同様の傾向が見られた. 国単位で集計すると，アメリカ宛と中国宛の攻撃のみで，全体の 50%以上を占めた.

次に，IP アドレス，/16 ネットワーク，AS ごとの上位 10，上位 100，上位 1000 が占める攻撃件数の割合を表 3 に示す. IP アドレス単位で見ると，被攻撃件数の多い上位 10 のアドレスで攻撃全体の 0.4%を占めていたが，AS 単位で見ると，被攻撃件数の多い上位 10 の AS（全 AS の 0.02%[3]）が全攻撃の 32.9%，上位 100 の AS（全 AS の 0.2%）が全攻撃の 66.5%を占めていた. この結果から，AS の規模や GeoIP の精度等を考慮する必要はあるものの，DRDoS の攻撃対象ネットワークには大きな偏りがあることがわかる.

4.3　攻撃対象の時間変化

4.1 節で述べたように，一度，攻撃対象となった IP アドレスが，再度攻撃の対象となるケースは少ないが，一部の攻撃対象に関しては多数の攻撃が観測されていた. これらの攻撃対象

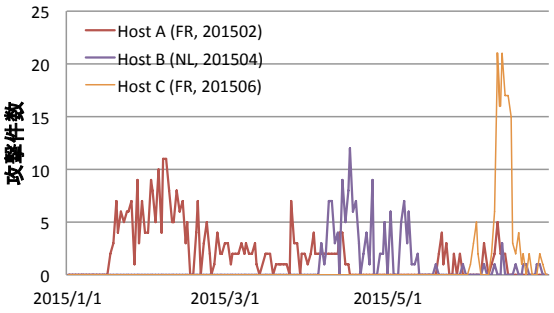

図 7　日ごとの被攻撃件数の推移（括弧内は国コードと最も被攻撃件数の多かった月）

の中には，定常的に DRDoS 攻撃に晒されていた組織だけでなく，短期間に集中して攻撃を受けていた組織も存在した.

2015 年 1 月から 6 月の偶数月に最も被攻撃件数の多かった 3 つの IP アドレスの日毎の被攻撃件数の推移を図 7 に示す. これらの IP アドレスに対する攻撃は短期間に集中する傾向にあることから，DRDoS の攻撃対象の中には，攻撃件数に時間的な局所性があるケースが存在することがわかる.

4.4　攻撃対象のサービス

DRDoS ハニーポットが観測した攻撃の中には，要求パケットの送信元ポート番号（i.e. 攻撃の宛先ポート番号）が特定の値に設定されている攻撃が存在した.

具体的には，全攻撃件数の 35%にあたる約 25 万件の攻撃では宛先ポート番号が Web サーバで使用される 80 番に設定されており，このほかにも，DNS サーバ（53 番）宛に 8,193 件，

[3] 全 AS の数は，CAIDA の AS Rank[15]に登録されている AS 数（2015 年 8 月現在）とした.

NTP サーバ（123 番）宛に 1,462 件，Xbox（3074 番）宛に 13,822 件，Minecraft（25565 番）宛に 5,793 件の攻撃が観測された．

5 考察

本稿の分析対象期間中，DRDoS ハニーポットは一日平均 4000 件の DRDoS 攻撃を観測した．非常に多くの攻撃が観測されていたものの，その多くは継続時間が短く，期間内に何度も攻撃された攻撃対象は少なかった．これらの結果から，ハニーポットが観測した攻撃の中には，サービスの妨害を意図した攻撃だけでなく，テスト攻撃の通信が含まれているものと予想される．実際，Booter サービスの中には，無料あるいは手頃な値段で，条件付きの DDoS 攻撃を試し打ちできるサービスが提供されており，これらが攻撃件数を引き上げる要因になっていると考えられる．

また，4.4 節で述べたように，一部の攻撃では宛先ポート番号が設定されており，これらの攻撃はそのポートで動作するサービスの妨害を狙ったものと推測される．攻撃の宛先ポート番号を設定することが，攻撃にどのような影響を与えるのかははっきりしないが，攻撃対象の組織に設置されたファイアウォールの回避や，サービスのデーモンプロセスに負荷をかけるための対応であると考えられる．

最後に，4.2，4.3 節で分析したように，DRDoS の攻撃対象にはネットワーク的・時間的な局所性が存在するため，DRDoS ハニーポットが観測した攻撃の履歴を分析することにより，DRDoS 攻撃で現在狙われている組織やネットワークを推定することが可能である．この情報の精度等の評価については今後の課題であるが，これらの情報を共有することにより，ISP をはじめとしたネットワークを運用する組織による DDoS 攻撃対策を支援できると考えている．

6 まとめと今後の課題

本稿では，DRDoSハニーポットが2015年1月から6月までに観測したDRDoS攻撃の履歴を用いて，DRDoSの攻撃対象の傾向を分析した．本稿の分析結果は，DRDoSの攻撃対象はネットワーク的・時間的な局所性があることを示しており，本知見は攻撃の履歴情報を用いたDRDoS攻撃対策技術への応用に期待できる．

今後の課題としては，DRDoS 攻撃の観測・分析を継続するとともに，本研究で得られた知見をもとに，DRDoS 攻撃の対策技術について検討する予定である．また，攻撃のパケットなどに見られる特徴から攻撃者の分類をおこない，Booter サービスをはじめとする DRDoS 攻撃を実行するインフラの実態を明らかにしていきたい．

謝辞

本研究の一部は，総務省情報通信分野における研究開発委託／国際連携によるサイバー攻撃の予知技術の研究開発／サイバー攻撃情報とマルウェア実体の突合分析技術／類似判定に関する研究開発により行われた．

参考文献

[1] Christian Rossow: "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," In the Proceedings of Network and Distributed System Security Symposium (NDSS), 2014.

[2] Marc Kuhrer, Thomas Hupperich, Christian Rossow, Thorsten Holz: "Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks," In the Proceedings of 8th Usenix Workshop on Offensive Technologies (WOOT 14), 2014.

[3] Jose Jair Santanna, Roland van Rijswijk-Deij, Rick Hofstede, Anna Sperotto, Mark Wierbosch, Lisandro Zambenedetti Granville, Aiko Pras: “Booters - An Analysis of DDoS-as-a-Service Attacks,” In the Proceedings of the 14th IFIP/IEEE Symposium on Integrated Network and Service Management, 2014.

[4] Jose Jair Santanna, Romain Durban, Anna Sperotto, Aiko Pras: "Inside Booters: An Analysis on Operational

Databases," Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on, IEEE, 2015.
[5] 牧田大佑, 吉岡克成, 松本勉:DNS ハニーポットによる DNS アンプ攻撃の観測, 情報処理学会論文誌, Vol.55, No.9, pp.2021-2033, 2014.
[6] 牧田大佑, 西添友美, 小出駿, 筒見拓也, 金井文宏, 森博志, 吉岡克成, 松本勉, 井上大介, 中尾康二:早期対応を目的とした統合型 DRDoS 攻撃観測システムの構築, 2015 年暗号と情報セキュリティシンポジウム(SCIS2015).
[7] 西添友美, 牧田大佑, 吉岡克成, 松本勉: プロトコル非準拠のハニーポットによる DRDoS 攻撃の観測, 2015 年暗号と情報セキュリティシンポジウム(SCIS2015).
[8] CloudFlare: "The DDoS That Almost Broke the Internet," http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/, accessed 2015/08/21.
[9] CloudFlare: "Technical Details Behind a 400Gbps NTP Amplification DDoS Attack," http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/, accessed 2015/08/21.
[10] The Akamai Blog: "DD4BC: PLXsert warns of Bitcoin extortion attempts," https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html, accessed 2015/08/21.
[11] Default Deny: "MC-SQLR Amplification: MS SQL Server Resolution Service enables reflected DDoS with 440x amplification," http://kurtaubuchon.blogspot.jp/2015/01/mc-sqlr-amplification-ms-sql-server.html, accessed 2015/08/21.
[12] The Akamai Blog: "RIPv1 Reflection DDoS Making a Comeback," https://blogs.akamai.com/2015/07/ripv1-reflection-ddos-making-a-comeback.html
[13] MaxMind: GeoIP2 Downloadable Databases, http://dev.maxmind.com/geoip/geoip2/downloadable/, accessed 2015-08-21.
[14] The Measurement Factory: "IPv4 Heatmaps," http://maps.measurement-factory.com/, accessed 2015/08/21.
[15] CAIDA: AS Rank, http://as-rank.caida.org/, accessed 2015/08/24.

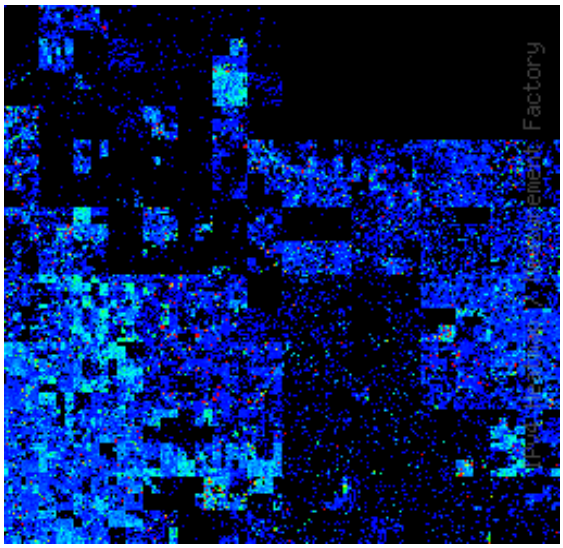

図 A DRDoS の攻撃対象の分布

付録 A. 攻撃対象ネットワークの可視化

Hilbert 曲線を用いて IPv4 空間を可視化する手法が考案されている[14]. IPv4 のアドレスを二次元平面の Hilbert 曲線上にマッピングすると, 数的に距離の近い IP アドレスが空間的に近い位置にマッピングされるため, この手法は IP アドレスの局所性等の表現に適している.

本付録では, この手法を用いて DRDoS の攻撃対象ネットワークを可視化する. 可視化には[14]で公開されているプログラムを使用し, 次のように画像が出力されるよう設定した.

- /16 ネットワークを 1 pixel で表し, 256×256 の画像に IPv4 空間全体を描画する.
- 各 pixel の色は, その/16 ネットワークへの攻撃件数を表現する(黒:0 件, 青:1 件, 赤:256 件以上, 赤に近いほど攻撃件数は多い)

本稿で分析した DRDoS の攻撃件数を可視化した結果を図 A に示す. インターネット上の多くのネットワークが攻撃されている一方で, 一部のネットワークが頻繁に攻撃されていることがわかる.