ハニーポットによるTCPリフレクション攻撃の観測と分析

小出 駿† 牧田 大佑†* 吉岡克成‡ 松本勉‡

† 横浜国立大学
‡ 横浜国立大学大学院環境情報研究院/横浜国立大学先端科学高等研究院
240-8501 神奈川県横浜市 保土ケ谷区常盤台 79-1
{koide-takashi-mx, makita-daisuke-jk}@ynu.jp, {yoshioka, tsutomu}@ynu.ac.jp
* 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@nict.go.jp

あらまし TCPの再送機能を悪用したリフレクション攻撃（TCPリフレクション攻撃）の可能性が指摘されている. そこで我々は, 攻撃の踏み台になるインターネット上のホストを調査した結果, 最大で13万倍の増幅効果を持つTCP実装を有するホストが特定のISPネットワーク内に多数存在することが分かった. また, TCPリフレクション攻撃を観測するハニーポットを実装し, 1つのハニーポットセンサを用いて攻撃の現状を把握するための実験を行なった. その結果, 22日間で276のIPアドレスに対する合計140万のTCPリフレクション攻撃パケットを観測し, 当該攻撃は既に攻撃者によって実行されていることを確認した.

Observation and Analysis of TCP-based Reflection Attacks Using Honeypot

Takashi Koide† Daisuke Makita†‡ Katsunari Yoshioka†
Tsutomu Matsumoto†

† Yokohama National University
‡Graduate School of Environment and Information Sciences/Institute of Advanced Sciences, Yokohama National University
79-1 Tokiwadai, Hodogaya-ku, Yokohama-shi, Kanagawa, 240-8501, Japan
{koide-takashi-mx, makita-daisuke-jk}@ynu.jp, {yoshioka, tsutomu}@ynu.ac.jp
* National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo, 184-8795, Japan
d.makita@nict.go.jp

Abstract The possibility of TCP-based reflection attacks has been addressed but not well documented. In this paper, we first report the existence of reflectors with very high amplification factor of approximately 130,000, all located in an ISP. Furthermore, we design and deploy a first honeypot that observes TCP-based reflection attacks. With the deployment of 22 days, we observed over 140 million packets targeting 276 IP addresses, which indicate that TCP-based reflection attacks are indeed conducted in the wild.

1 はじめに

DDoS 攻撃(Distributed Denial-of-Service Attacks)は複数のホストからインターネットに接続されたホストに対し，過剰に負荷を掛けサービスを妨害する攻撃であり，インターネット上の脅威として知られている．近年，リフレクタと呼ばれるサーバを踏み台として，攻撃対象に大量の通信を送りつける DRDoS 攻撃(Distributed Reflection Denial-of-Service Attacks)による被害が増えており，DNS サーバを悪用した 2013 年 3 月の事例では Spamhaus に対して最大 300Gbps の攻撃を記録し，NTP サーバを悪用した 2014 年 2 月の事例では最大 400Gbps を記録している[10, 11].

DRDoS 攻撃で悪用される事が多い DNS や NTP などのプロトコルではコネクションレス型の UDP で通信を行っているため，クライアントが送信元 IP アドレスを詐称した要求パケットを送信すると，サーバは応答パケットを詐称された IP アドレスへ送信する．これを利用し，要求パケットに対して応答パケットのサイズが大きくなるクエリをサーバへ送信することで攻撃者は効果的に攻撃を増幅させることができる．

一方，TCP は 3WAY ハンドシェイクを用いてセッション確立を行うため，送信元 IP アドレスを詐称したパケットを送信しても，UDP のように増幅されたペイロードを持つパケットを攻撃対象へ送りつける事は出来ない．しかし，TCP の再送機能を悪用したリフレクション攻撃の可能性が指摘されており，2002 年に TCP リフレクション攻撃の PoC(Proof of Concept:概念実証)コードである BANG.c[1]が公開されている[2]．このプログラムは，送信元 IP アドレスを詐称した SYN パケットを送信する機能を持ち，そのパケットを受信したサーバは SYN-ACK パケットを詐称された IP アドレスへ送信し，再送回数の上限まで繰り返す．つまり，ペイロードを増幅させるのではなく，パケット数を増やすことで結果的にトラフィックを増幅することができる．さらに，TCP リフレクション攻撃に悪用される可能性のあるインターネット上のホストに関する既存研究として，文献[3]では，ランダムに生成した 2000 万の IP アドレスへ向けて TCP の 13 種のポート番号に対して SYN パケットのみを送信するネットワークスキャン(TCP SYN スキャン)を行い，応答パケットの分析を行っている．その結果，プロトコルによっては全体の約 2%のホストが 20 回以上応答パケットを送信するなど，高い増幅率を持つホストが多く存在すると報告している．また，SYN-ACK パケットだけではなく，接続拒否の RST パケットやペイロードを持った PSH パケットを SYN パケットの応答として返すホストも存在すると述べている．さらに，独自のフィンガープリントを用いて応答ホストを分類した結果，増幅率の高いホストの中には，ルータや組み込み機器などの IoT デバイスが存在すると報告している．

また，文献[4，5]では金銭を支払うことで DDoS 攻撃を代行する，Booter または Stresser と呼ばれるサービスの中には，選択可能な攻撃種別の項目として「TCP AMP」が存在している事を報告しており，実際に我々がいくつかの Booter サービスを調査したところ，twBooter2, DestressBooter, inBOOT といった Booter は，TCP リフレクション攻撃を発生させる機能を持つことが分かった．

以上のことから，すでに TCP リフレクション攻撃がインターネット上で発生しており，攻撃者によって TCP で動作するサーバ機器が悪用されている可能性は高いと考えられる．さらに，増幅率の高いホストは多数存在しているため，今後 DNS や NTP のように大規模な攻撃に利用されることは十分考えられる．

TCP リフレクション攻撃はその実態が未だ明らかになっていないため，我々は TCP リフレクション攻撃の実態と傾向を把握するために，2 つの実験を行った．まず，文献[3]と同様にインターネット上のホストに対してネットワークスキャンを行い，TCP リフレクション攻撃に悪用される可能性の高いホストについて分析する追実験を行った．その結果，高い増幅率を持つリフレクタを多数発見し，実際の攻撃に悪用された場合に脅威になり得ることを確認した．次に，TCP リフ

レクション攻撃を観測するため，リフレクタを模擬した TCP リフレクションハニーポットを構築し，通信を分析した．その結果，TCP リフレクション攻撃と思われる通信を多数観測した．また，観測した攻撃にはそのパケットの各種ヘッダに特徴や傾向があることを確認した．

本稿の構成は次の通りである．2 章で TCP リフレクション攻撃に悪用される可能性のあるインターネット上のホストについてネットワークスキャンを用いて分析する．次に，3 章で我々が構築した TCP リフレクションハニーポットの概要とその観測結果について述べ，4 章でまとめと今後の課題を述べる．

2 ネットワークスキャンによるリフレクタの分析

本章では，インターネット上に存在する TCP リフレクション攻撃に悪用される可能性のあるホストを探索するためネットワークスキャンを行い，応答パケットを分析した結果について報告する．

2.1 実験方法

RST パケットを受け取ったホストは SYN-ACK パケットの再送を中断させるため，RST パケットの送信を許可しないように設定したホストにグローバル IP アドレスを割り当て，このホストから，FTP（21/tcp），SSH（22/tcp），Telnet（23/tcp），DNS（53/tcp），HTTP（80/tcp），NetBIOS（139/tcp），HTTPS（443/tcp），SIP（5060/tcp），8080/tcp，10000/tcp の 10 種のポートに対して，それぞれランダムに生成した 1000 万個の IP アドレスを宛先に設定し，TCP SYN スキャンを行った．次に，これらの SYN パケットに対する応答パケットを同一ホスト上で観測し，具体的な応答パターンやパケットの増幅率，リフレクタの所属するネットワークの傾向やネットワーク機器の特徴を分析する．ここで，増幅率は受信したパケットの総データ量を，送信した SYN パケットのデータ量（=54byte）で割った値と定義する．

表 1 ネットワークスキャンに対するポート番号ごとの応答ホスト数

宛先ポート番号	応答パケット数別送信元 IP アドレス数				
			>20（TCP リフレクタ）		
	>1	>10	SYN-ACK リフレクタ	PSH リフレクタ	RST リフレクタ
21	430674	5126	4049	0	2
22	411575	557	301	0	10
23	339278	3473	2891	5	4
53	369659	92	8	0	24
80	435708	1415	953	0	8
139	258805	64	34	0	7
443	489899	1018	815	0	8
5060	427905	91	62	0	14
8080	364860	568	346	0	3
10000	409805	105	78	0	11

2.2 実験結果

スキャン対象のホストを応答パケットの数で分類し，ポート番号ごとに，それぞれ一回以上，10 回以上，20 回以上応答パケットを送信した IP アドレスの数を表 1 に示す．ここで，応答パケットを 20 回以上送信しているホストを「TCP リフレクタ」とする．また，TCP リフレクタの条件を満たし，かつ SYN-ACK パケット，PSH パケット，RST パケットを主に返すホストをそれぞれ，「SYN-ACK リフレクタ」，「PSH リフレクタ」，「RST リフレクタ」とする．これらの TCP リフレクタの中で最も多いのは SYN-ACK リフレクタであり，RST リフレクタとともに全てのプロトコルで観測することが出来た．また，少数の PSH パケットを返すホストはいくつかのプロトコルで観測しているが，20 回以上の PSH パケットを送信しているホストを発見できたのは，本実験では Telnet のみであった．

2.2.1 PSH リフレクタの分析

Telnet に対するスキャンで今回観測した 5 つの PSH リフレクタのすべてが，SYN パケットに対し SYN-ACK パケットを応答として返し，その後 ACK パケットを受信していないにも関わらず PSH パケットを送信するという，TCP の仕様に従っていない動作を行っていた．実際に Linux の Telnet コマンドを用いてこれらの PSH リフレクタに接続を試みたところ，「Lockout for

表 2 ある AS 内の RST リフレクタ数とプロトコルごとの重複割合

宛先ポート番号	RST リフレクタ数	IP アドレスの重複割合(%)			
		21	22	23	10000
21	1763	-	59%	53%	57%
22	2337	78%	-	71%	74%
23	2901	87%	88%	-	87%
10000	2830	91%	90%	84%	-

508948 seconds.」といった，サーバによってユーザのアカウントがロックされたと思われる文字列が表示され，その後毎秒，数字部分がカウントダウンされることを確認した．この文字列はネットワークスキャン時に観測された PSH パケットのペイロードと同様のものであったため，これらの PSH ホストは 3WAY ハンドシェイクによるコネクションが確立したかを確認せずに同様の PSH パケットを送信し続ける事がわかった．そこで，ある PSH リフレクタに対して，1 回の SYN パケットの送信と，5 回の SYN パケットの送信で増幅率にどのような影響があるかを調べた．まず SYN パケットを 1 回のみ送信すると，PSH パケットを含む応答パケットを約 40 秒間観測した．この時の応答パケットの合計データ量は 11,227Byte であり，約 208 倍の増幅率となった．次に，送信元ポート番号の異なる 5 つの SYN パケットを短時間のうちに送信したところ，約 40 秒間に合計 56,479Byte のパケットを受信し，約 209 倍の平均増幅率となった．

以上の結果から，このホストは送信する SYN パケット数を増やしても増幅率は減少せず，安定してトラフィックを増幅できるリフレクタとして悪用される可能性があると考えられる．

2.2.2 RST リフレクタの分析

次に，RST リフレクタの IP アドレスの分布を調べると，大量の RST パケットを送信するホストが特定の IP アドレス範囲に多く含まれていることが分かった．そこで，これらの IP アドレスを含む/16 ネットワーク(65,536IP アドレス)の全 IP アドレスに対して，FTP(21/tcp)，SSH(22/tcp)，Telnet(23/tcp)，10000/tcp 宛へ TCP SYN スキャンを行ったところ，ナイジェリアのある ISP の所有する 30,208 個の IP アドレスで構成される AS(Autonomous System)に範囲を限定することができ，さらに多数の RST リフレクタを発見した．表 2 はこのナイジェリアのネットワークに存在する RST リフレクタについて，各プロトコルの RST リフレクタ群が，他のプロトコルの RST リフレクタ群と同一の IP アドレスを含む割合を示す．プロトコルごとに RST リフレクタの総数は異なるものの，全てのプロトコルにおいて 50%以上の IP アドレスが共通しているため，接続許可をしていないポートに対しては，ポート番号に関係なく RST パケットを大量に返すのではないかと予想した．

そこで，この AS 内のある 1 つの RST リフレクタに対して，ランダムに選択した 500 ポートに向けて 1 回ずつ，合計 500 パケットの SYN パケットの送信を行い，応答パケットを観測する実験を行った．その結果，498 個のポートから 8 分間にわたり合計約 805 万回の RST パケットを受信した．ポートごとに応答回数は大きく異なるものの，最も多い応答回数は約 13 万回であり，受信した総パケット数は送信したパケット数の約 1.6 万倍となった．すべての RST パケットのサイズが SYN パケットと同一の 54byte であったため，平均増幅率も約 1.6 万倍となった．また，同一の実験をこの AS 内の他のホストに対しても行った．ネットワークへの影響を懸念し，すべてのホストを網羅的に対象としていないが，500 個のポートのうちほぼ全てのポートから合計 100 万回以上の RST パケットを応答するホストを多数発見した．DNS，NTP，SNMP などを悪用した際の増幅率は最大で数百～千倍と言われており[6]，それと比較すると，この RST リフレクタが記録した増幅率がいかに強力であるかが分かる．以上の分析結果は，ポート番号に関係なく RST パケットを大量に返すという前述の仮説を支持するものであり，この AS に属する他の RST リフレクタも，一般的な OS の応答としては考えられないほど異常に大量の RST パケットを送信するため，同様のネットワーク機器や類似した設定が使用されていると推察される．したがって，このネット

表 3 ポート番号ごとのユニークな IoT 機器数と IoT リフレクタ数

宛先ポート番号	IoT 機器の製品数	IoT ホスト数
21	104	731
22	10	51
23	31	44
80	66	159
8080	15	20

ワーク全体が強力なリフレクタとして悪用される可能性は高いと思われる.

2.2.3 IoT 機器の分析

最後に, TCP リフレクタがどのような機器で動作しているかを調べるために, FTP(21/tcp), SSH (22/tcp), Telnet (23/tcp), HTTP (80/tcp), 8080/tcp へのスキャンで発見した TCP リフレクタに各ポートで接続を行い, ログイン前に送信される Telnet バナー情報や FTP ウェルカムメッセージなどの文字列, Web ブラウザを用いたアクセスによるログイン画面や BASIC 認証の際に送られるメッセージなどから使用されている機器の分析を行った. その結果, 有線・無線ルータ, モデム, ファイアウォール, プリントサーバ, ネットワークカメラ, DVR など様々な IoT 機器を確認し, 具体的な製品名が特定できる IoT 機器を多数発見することができた. プロトコルごとのユニークな IoT 機器の製品数と IoT 機器が使用されているホスト数を表 3 に示す.

その中で, 最も多くの製品名を取得できたのは FTP であり, FTP のウェルカムメッセージから, 100 件以上のユニークな IoT 機器と, それらを使用している 700 のホストを発見した. 特に多くの FTP ホストで使用されていた IoT 機器メーカは, TP-LINK 社, Huawei 社, ZyXEL 社, ZTE 社であり, それぞれ 161 ホスト, 104 ホスト, 92 ホスト, 85 ホストであった. これらのメーカの製品は他のプロトコルでも多く使用されており, 他にも Cisco, D-Link, Hikvision, MikroTik, moxa, Seagate, Trendchip といったメーカによる製品も多数確認している. これらの機器の応答パケットの回数や送信のタイミングはメーカごとに異なるが, 同一のメーカの異なる製品ではそれらが類似している事が多いため, ZyXEL 製のルータなどが ZynOS という独自の OS によって通信の管理を行っているように[3, 7], その他のメーカもそれぞれ共通の OS や設定が使用されている可能性は高い.

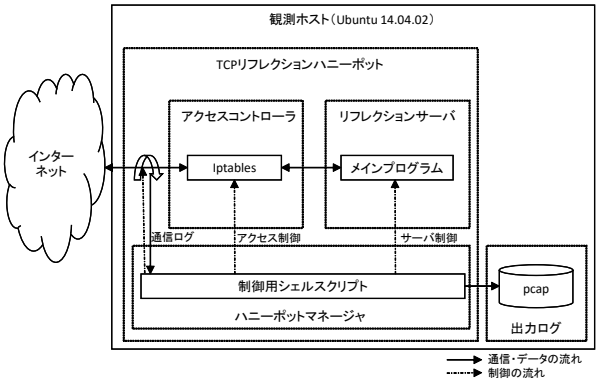


図 1 TCP リフレクションハニーポットの構成

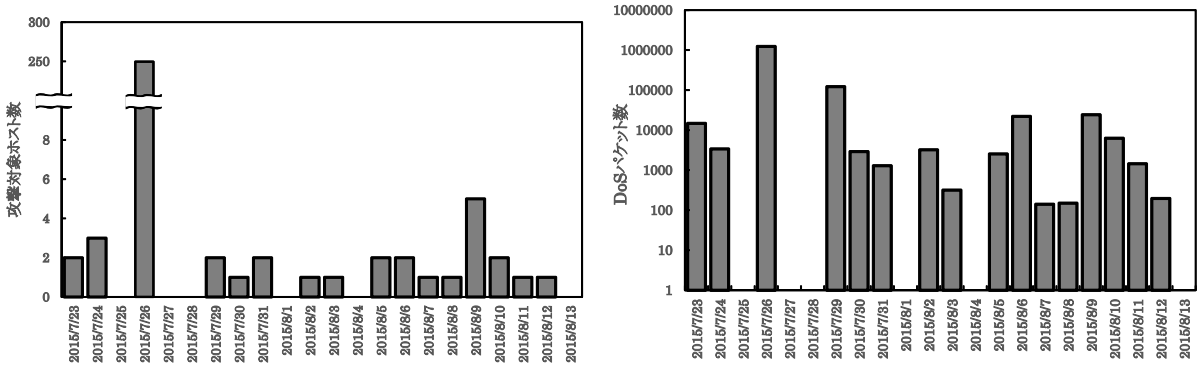
IoT の普及に伴い, 今後インターネットへ様々な種類のデバイスが接続されることが予想され, 今回の実験で判明したように, 多くのメーカが独自に設計・開発した TCP/IP の実装を製品に組み込むことで, TCP リフレクション攻撃に悪用される可能性のある脆弱なホストがさらに増加すると推察される.

3 TCP リフレクションハニーポットを用いた攻撃の観測

本章では, 我々が独自に構築した TCP リフレクタを模擬したハニーポットである TCP リフレクションハニーポットを用いて, 実際の攻撃の観測を行った結果について述べる.

3.1 構成と実装

TCP リフレクションハニーポットの構成を図1に示す. TCP リフレクションハニーポットはグローバル IP アドレスを割り当てたマシン(Ubuntu 14.04.2 LTS)で稼働し, 「リフレクションサーバ」, 「アクセスコントローラ」, 「ハニーポットマネージャ」の 3 つの要素から構成される. リフレクションサーバは, インターネットから到達した TCP の全ポート(65536 個)の SYN パケットに対して,



(a) 攻撃対象ホスト数　　(b) DoS パケット数

図 2 TCP リフレクションハニーポットで観測された攻撃対象ホスト数と DoS パケット数の推移

1 パケットあたり 100 回の SYN−ACK パケットを RAW ソケット(SOCK_RAW)によって送信し，100 倍の増幅率を持ったリフレクタ(SYN-ACK ホスト)として動作するようにする．なお，メインとなるプログラムは Python とそのライブラリ dpkt, pcapy によって実装した．アクセスコントローラは，インターネットとリフレクションサーバ間の通信を，パケットフィルタリングツール iptables を用いて制御する．ここで，実際の TCP リフレクション攻撃の被害を最小限に抑えるため，iptables の hashlimit モジュールを使用し，同一の宛先 IP アドレスに対して，1000 回以上 SYN-ACK パケットが送信された場合，その IP アドレスへの SYN-ACK パケットの送信を毎秒 100 回に制限するようにする．ハニーポットマネージャはリフレクションサーバの制御・管理や通信ログの取得を行う．通信ログは tcpdump で取得し，pcap 形式のファイルを出力として保存する．

3.2 観測方法

TCP リフレクション攻撃の観測は，国内の動的グローバル IP アドレスを割り当てた 1 つのハニーポットセンサを使用した．この IP アドレスでは本センサ以外の外部向けのサービスは稼働していないため，SYN Flood 攻撃の対象となることは無いと考えられ，到達する SYN パケットは主に，

ⅰ ネットワークスキャン
ⅱ マルウェアや攻撃者による侵入と感染
ⅲ TCP リフレクション攻撃

表 4 国ごとの攻撃対象ホスト数

国コード	攻撃対象ホスト数
RU	263
CN	3
US	2
UA	2
DE	2
IN	1
GB	1
FR	1
EE	1
計	276

のいずれかを目的としていると考えられる．2015 年 7 月 23 日から観測を始め，8 月 13 日までの通信トラフィックについて，IP アドレスごとのパケット数や所属国を分類し，我々が提案した独自の通信実装から送信されたパケットの分類手法[8]を用いてその特徴を分析した．なお，観測期間中に IP アドレスの変更は無かった．

3.3 観測結果

前節のⅲのトラフィックと，ⅰ，ⅱのトラフィックを区別するため，一日分のパケットキャプチャデータに対して，SYN パケットの送信元 IP アドレスのうち，ACK パケットを送信していないホストを抽出し，それぞれの SYN パケットの数が 100 を超えたものを「攻撃対象ホスト」とし，その IP アドレスが送信元に設定されている SYN パケットを「DoS パケット」として分析を行った．1 日あたりの攻撃対象ホスト数と DoS パケット数をそれぞれ図 2 に示し，全期間で観測された攻撃対象ホストについて，所属国ごとのユニークな IP アドレス数を表 4 に示す．

国ごとのアドレス数を分析すると，ロシアの IP

表 5 ハニーポットで観測された DoS パケットのシグネチャ

Signature	IP ヘッダ		TCP ヘッダ		
	ID	TTL(予想初期値)	送信元ポート番号	ウィンドウサイズ	シーケンス番号
Tcp_reflection_1	ランダム値	86~129(範囲値)	ランダム値	8192	ランダム値
Tcp_reflection_2	26437	19(64 以下)	固定値	50723	3324214066
Tcp_reflection_3	1~255, 3092~3100, 60807~60813	237(255)	ランダム値	0 または ランダム値	ランダム値

アドレスを多く観測しており，263 個の IP アドレスのうち 258 個は DDoS 対策を重視したホスティング事業を主なサービスとする企業が保有する IP アドレスであった．分析対象としたトラフィックの中で最も大量の DoS パケットを観測したのは 7 月 26 日であり，約 2 時間，総数 113 万の SYN パケットを受信し，送信元 IP アドレスにはこの企業の 255 個の IP アドレスが設定されていた．これらの通信の DoS パケットの宛先ポート番号は 16 種あり，この通信が発生する約一時間前に異なるロシアの IP アドレスから同一の 16 ポートへ，1 回ずつの SYN パケットを確認している．この結果から，攻撃者は自らが制御可能なホストからポートスキャンもしくはネットワークスキャンによるホスト探索を事前に行い，その後 TCP リフレクション攻撃に我々のハニーポットを利用したと考えられる．

また，8 月 6 日に 13 種のポートに対する DoS パケットを 2 万以上観測しており，その送信元 IP アドレスはイギリスとフランスのアドレスが設定されていた．この DoS パケットが観測された約 15 分前に，ウクライナの IP アドレスから同一の 13 種のポート宛に 1 回ずつ SYN パケットを観測している．ここで，文献[8]の手法によりこの DoS パケットの IP ヘッダと TCP ヘッダを分析すると，シーケンス番号と IP ヘッダの ID 値がランダム生成による値であり，ウィンドウサイズが 8192 に固定され，TTL(Time to Live)値は 86 から 129 の範囲内に分布するという特徴を持っていた．通常 OS ごとに初期値が決められている TTL の値が大きく分散していることに加え，高速に大量のパケットを送信していることから，独自の実装によってパケットヘッダを作成していることが予想されるため，このパケットのシグネチャを **Tcp_reflection_1** とする(表 5)．また，前述の企業の保有する IP アドレスを狙った攻撃の DoS パケットを分析すると，シーケンス番号，ウィンドウサイズと IP ヘッダの ID 値が **Tcp_reflection_1** と同様であり，TTL は 86 から 127 の範囲内の値という類似した特徴を持っていた．事前のネットワークスキャンを行い，複数のポートを悪用するという同様の攻撃の傾向を持ち、DoS パケットのヘッダパターンが類似していることから，2 つの攻撃は共通の攻撃ツールやマルウェアによって行われたと推測できる．

パケットヘッダに特徴を持った DoS パケットをさらに分析すると，複数種類に分類することができ，このうち特に大量の通信を頻繁に観測した 2 種のヘッダパターンを **Tcp_reflection_2**，**Tcp_reflection_3** とした．

また，パケット数が数十程度のホストによる少量の通信であっても独自のネットワーク実装によるパケットを複数確認でき，表 5 に示したシグネチャでマッチング可能なパケットも観測できた．したがってこれらの通信は，攻撃通信と同様の特徴を持つことがあることから，攻撃者の所有するホストから送信された，または攻撃者の操作可能な別のホストから送信元を詐称して送信された，攻撃テストの可能性がある．

3.4 考察

攻撃者は攻撃を発生させる前に，ネットワークスキャンやポートスキャンを行い攻撃に悪用可能なホストを探索することと，増幅効果があるかを確かめるために攻撃テストを行うことがあると分かった．それらと実際の TCP リフレクション攻撃を共通の攻撃ツールやマルウェアを使用して実行しているため，DoS パケットのヘッダパターンから通信を分類することで，攻撃と攻撃者の所有するホストを結び付けられる可能性がある．

4　まとめと今後の課題

本稿では，TCP リフレクション攻撃に悪用される可能性のあるリフレクタの調査を行い，実際の攻撃に利用された際に高い増幅効果を持つホストを発見した．また，我々が構築した TCP リフレクションハニーポットを用いた観測の結果，実際の TCP リフレクション攻撃の観測に成功し，詐称の可能性のある送信元 IP アドレスに依存しない分析方法を用いて攻撃に特徴や傾向があることを確認した．

本研究で行ったリフレクタホストの調査はインターネットの網羅的な調査ではないため，他にも増幅率の高いホストが多く存在する TCP のプロトコルがある可能性がある．そこで，ハニーポットで観測される通信から悪用されやすいポートを分析し，その結果を基にさらなるリフレクタホストの調査を行うことが今後の課題である．また，本稿では1つの TCP リフレクションハニーポットでのみ観測を行ったが，応答回数の変更や RST パケットを応答する機能を追加するなど複数種類のハニーポットセンサを設置することで，攻撃観測の効率を高めていきたい．さらに，我々が開発し運用を行っている DRDoS 攻撃観測システム[9]は複数種類の DRDoS ハニーポットによって攻撃の観測を行っており，これに TCP リフレクションハニーポットを組み込み，他のプロトコルの観測結果と相関分析を行うことで，DRDoS 攻撃の予知・対策技術への貢献を行いたい．

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．

また，本研究の一部は，文部科学省国立大学改革強化推進事業の支援を受けて行われた．

参考文献

[1] BANG.c, https://www.exploit-db.com/exploits/343.

[2] M. Handley, Internet Denial-of-Service Considerations, https://tools.ietf.org/html/rfc4732, 2006.

[3] M. Kührer, T. Hupperich, C. Rossow, T. Holz, "Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks," In Proceedings of the 8th Usenix Workshop on Offensive Technologies (WOOT 14), 2014.

[4] J. J. Santanna, R. Durban, A. Sperotto, and A. Pras, “Inside Booters: An Analysis on Operational Databases,” In proceedings of the 14th IFIP/IEEE International Symposium on Integrated Network Management (IM 2015), 2015.

[5] An Analysis of DrDoS SYN Reflection Attacks, http://www.prolexic.com/kcresources/white-paper/white-paper-syn-ssyn-reflection-attacks-drdos/Analysis_of_DrDoS_SYN_Reflection_Attacks_White_Paper_062513.pdf.

[6] Internet Infrastructure Review Vol.21, http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol21_internet.pdf, 2013.

[7] M. Kührer, T. Hupperich, C. Rossow, T. Holz, "Exit from Hell? Reducing the Impact of Amplification DDoS Attacks," In Proceedings of the 23rd Usenix Security Symposium, 2014.

[8] 小出駿，鈴木将吾，牧田大佑，村上洸介，笠間貴弘，島村隼平，衛藤将史，井上大介，吉岡克成，松本勉，”通信プロトコルのヘッダの特徴に基づく不正通信の検知・分類手法”，情報処理学会，コンピュータセキュリティシンポジウム 2014 論文集，pp. 48-55，2014.

[9] 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“，電子情報通信学会，2014 年 暗号と情報セキュリティシンポジウム，2014.

[10] Matthew Prince, The DDoS That Almost Broke the Internet, https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/, 2013.

[11] Matthew Prince, Technical Details Behind a 400Gbps NTP Amplification DDoS Attack, https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/, 2014.