# 5-3　DRDoS 攻撃を観測するハニーポット技術の研究開発

牧田大佑　吉岡克成

我々は、インターネット上の大きな脅威となっている DRDoS 攻撃を観測するためのハニーポット（以降、AmpPot）の研究開発を行っている。本稿では、AmpPot の概要を説明するとともに、我々の運用する AmpPot が観測した DRDoS 攻撃を分析し、攻撃の傾向や特徴を示す。また、AmpPot を応用した DRDoS 攻撃対策技術の 1 つとして、我々が開発・運用を行っている DRDoS 攻撃アラートシステムについて説明する。

## 1　はじめに

インターネットを利用するサービスの普及に伴い、そのサービスを妨害するサイバー攻撃（DoS 攻撃：Denial-of-Service Attack: サービス妨害攻撃）がインターネット上の大きな脅威となっている。DoS 攻撃の実行方法は、サービスを提供するプログラムの脆弱性を攻撃してサービスを妨害するものと、大量の通信を送信することにより高負荷をかけてサービスを妨害するものの 2 種類に大別されるが、特に後者は、攻撃者が事前に準備したボット*1 を用いて分散して実行されることが多く（DDoS 攻撃：Distributed Denial-of-Service: 分散型サービス妨害攻撃）、その被害を防止することは難しい。DDoS 攻撃の実行方法としては、TCP の SYN パケットを大量に送りつける SYN-FLOOD 攻撃や、UDP パケットを大量に送りつける UDP-FLOOD 攻撃等、その手法は多数存在するが、近年、DRDoS 攻撃（Distributed Reflection Denial-of-Service Attack: 分散反射型サービス妨害攻撃）と呼ばれる攻撃手法が大きな脅威となっている。

DRDoS 攻撃とは、インターネット上に存在するマシン群に通信を反射させて、大量のパケットを攻撃対象に送信する DDoS 攻撃である。攻撃者は、要求パケットの送信元 IP アドレスを攻撃対象の IP アドレスに詐称し、これをインターネット上に存在するマシン群へ送りつけることにより、その応答パケットを攻撃対象に集中させる。その結果、攻撃対象のネットワーク等のリソースが圧迫され、サービスが妨害される。DRDoS 攻撃は、2000 年頃からその存在が既に認知されていたが、2013 年 3 月に実行された Spamhaus*2 への攻撃 [1] をきっかけに、DDoS 攻撃の代表的な実行方法として広く使用されるようになった。例えば、昨今問題となっているハッカー集団の Anonymous*3 や、DDoS 攻撃で脅迫して身代金を要求する DD4 BC[2] 等のグループは、DDoS 攻撃の実行方法の 1 つとして DRDoS 攻撃を利用している。また、近年、Booter や Stresser と呼ばれる DDoS 攻撃代行サービス*4 が登場しており [3][4]、攻撃に関する知識を持たないユーザでも DRDoS 攻撃を容易に実行できる状況になっている。

DRDoS 攻撃の現状を把握し、その対策を講じるため、我々は DRDoS 攻撃を観測するためのハニーポット（以降、AmpPot）の研究開発を行っている [5][6]。本稿では、AmpPot の概要を説明するとともに、我々の運用する AmpPot が観測した DRDoS 攻撃を分析し、DRDoS 攻撃の傾向や特徴を示す。また、AmpPot を応用した DRDoS 攻撃対策技術の 1 つとして、我々が開発・運用を行っている DRDoS 攻撃アラートシステムについて説明する。

本稿の構成は次のとおりである。まず、**2** で本研究の背景として、DRDoS 攻撃について説明する。次に、**3** で我々が開発を進めている AmpPot の構成と実装、その運用について述べる。**4** で AmpPot が観測した DRDoS 攻撃を分析し、**5** で AmpPot を応用した DRDoS 攻撃アラートシステムを説明する。最後に、**6** でまとめと今後の課題を記す。

## 2　DRDoS 攻撃

DRDoS 攻撃とは、インターネット上に存在するマ

＊1　攻撃者の指令に従い動作する不正プログラム（マルウェア）の一種。
＊2　スパムメール対策を中心としたサイバー攻撃対策に関する情報を提供する非営利組織（https://www.spamhaus.org/）。
＊3　匿名（Anonymous）の名の下に抗議活動を行う国際的な集団。一部の構成員は、抗議活動の手段として、DDoS 攻撃等のサイバー攻撃を実行する。
＊4　Booter/Stresser は、負荷テストを名目としてサービスを提供しているが、実際には DDoS 攻撃を代行するサービスとして利用されている。

シン群に通信を反射させて、大量のパケットを攻撃対象に送信することにより、攻撃対象のネットワーク等のリソースを圧迫する DDoS 攻撃である。この攻撃では、次の 2 つの性質を持つサービスが悪用される。

- 増幅効果（Amplification）
  サーバが通信の増幅器となる性質。要求パケットの長さよりも応答パケットの長さが大きくなるプロトコルを使用することにより、攻撃者はそのサーバを経由して通信量を増幅させることができる。この性質から、この攻撃はアンプ攻撃とも呼ばれる。
- 反射効果（Reflection）
  サーバが通信を反射する性質。要求パケットの送信元 IP アドレスを確認しないプロトコル*5 を使用することにより、攻撃者は応答パケットを任意のホストへ送信させることができる。この攻撃で踏み台にされるサーバはリフレクタと呼ばれる。

攻撃者はこれらの性質を利用し、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マシンを利用し、送信元 IP アドレスを攻撃対象の IP アドレスに詐称した要求パケットを大量に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サイズが大きくなる（増幅効果）。そのため、攻撃対象のアドレスには増幅した応答パケットが大量に到達し、その結果、攻撃対象のネットワークは、リフレクタからのパケットで飽和し、サービス不能状態に陥る。

文献 [7] 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、DNS や NTP 等、14 種類のプロトコルが DRDoS 攻撃に利用される可能性があると報告されている。また、これらのプロトコル以外にも、TCP の 3 -way handshake 等のプロトコルも DRDoS 攻撃に悪用できることが指摘されており [8]–[11]、今後も DRDoS 攻撃の脅威は拡大することが予想される。

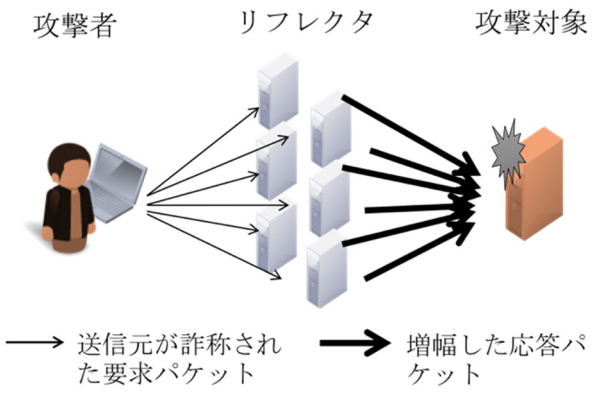


図 1　DRDoS 攻撃

## 3　AmpPot（DRDoS ハニーポット）

ハニーポットとは、不正アクセスの手法やその傾向の観測・分析を目的とした、不正使用されることに価値を持つ情報システムである。我々が研究開発を進めている AmpPot（DRDoS ハニーポット）は、DRDoS 攻撃を観測することを目的としたおとりのリフレクタであり、これをセンサとしてインターネット上に設置して運用することにより、攻撃の踏み台にされるリフレクタの視点から DRDoS 攻撃を観測する。

### 3.1　構成

攻撃者は、インターネット上で定常的なスキャンを実行することにより、攻撃に使用するリフレクタを探索していると予想される。そのため、DRDoS ハニーポットは、攻撃者のスキャンの要求パケットに応答しつつも、実際の攻撃には加担しないように設計する必要がある。

以上の要件を満たすため、AmpPot を図 2 ように構成する。AmpPot は、「サーバプログラム」「アクセスコントローラ」「ハニーポットマネージャ」の 3 つの要素からなる。まず、サーバプログラムは受信する要求パケットに対して応答パケットを送信する。次に、アクセスコントローラはサーバプログラムとインターネットの間で動作し、ハニーポットが攻撃に利用され

表 1　AmpPot が提供するサービスと使用する実装の一覧

| プロトコル名 | ポート | 実装 |
|---|---|---|
| QOTD | 17 /UDP | quoted*6 |
| CHG | 19 /UDP | xinetd*7 |
| DNS | 53 /UDP | BIND*8, Unbound*9 |
| NTP | 123 /UDP | NTP Project*10 |
| SNMP | 161 /UDP | Net-SNMP*11 |
| SSDP | 1900 /UDP | 簡易スクリプト |

*5　TCP/IP のトランスポート層に、UDP（User Datagram Protocol）を使用するプロトコルがこれに該当する。
*6　http://www.mrp3.com/webutil/quoted.html
*7　http://www.xinetd.org/
*8　https://www.isc.org/downloads/bind/
*9　https://www.unbound.net/
*10　http://www.ntp.org/
*11　http://www.net-snmp.org/

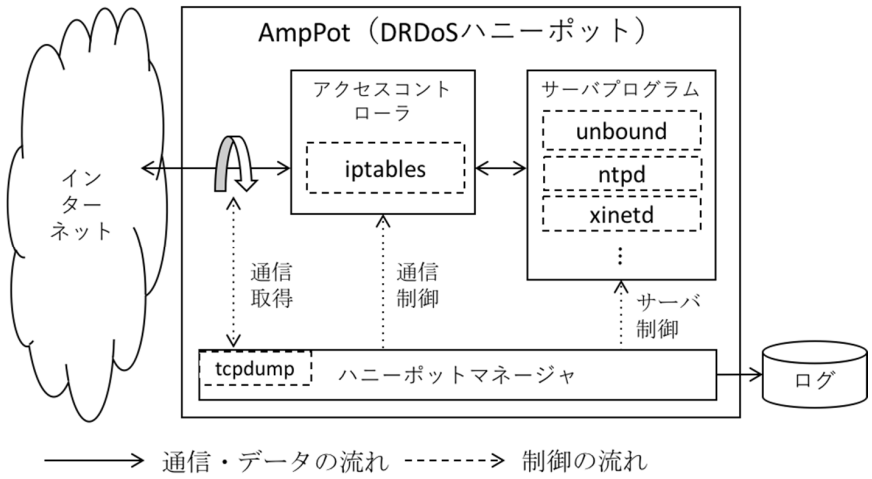


図 2　AmpPot (DRDoS ハニーポット)

表 2　運用中の AmpPot センサの概要

| ID | 設置日 | 追加日（日付の記載がないものは、設置日から観測） |
|---|---|---|
| H01 | 2012 /10 /06 | DNS、CHG（2013 /07 /26 ～）、QOTD・NTP・SNMP・SSDP（2014 /09 /25 ～） |
| H02 | 2013 /05 /13 | DNS のみ |
| H03 | 2014 /05 /13 | QOTD・CHG・DNS・NTP、SNMP（2014 /09 /17 ～）、SSDP（2014 /10 /03 ～） |
| H04 | 2014 /05 /13 | QOTD・CHG・DNS・NTP、SNMP・SSDP（2014 /09 /17 ～） |
| H05 | 2014 /05 /10 | QOTD・CHG・DNS・NTP、SNMP・SSDP（2014 /10 /18 ～） |
| H06 | 2014 /05 /10 | |
| H07 | 2014 /05 /10 | |

た場合に、攻撃に加担しないように通信を制御する。ハニーポットマネージャは、サーバプログラムとアクセスコントローラの制御及び通信ログの出力を担当する。

### 3.2　実装

我々が運用する AmpPot は、2016 年 3 月現在、DRDoS 攻撃に利用される可能性のある 6 種類のプロトコルを観測している（表 1）。AmpPot の実装においては、表 1 のサーバプログラムを Ubuntu Server*12 上にインストールし、アクセスコントローラとして iptables*13、ハニーポットマネージャには自作のシェルスクリプトを使用した。通信ログは、tcpdump*14 を用いて PCAP 形式で取得し、その PCAP ファイルを AmpPot の出力とした。

### 3.3　運用

我々が現在運用している AmpPot センサの一覧を表 2 に示す。2016 年 3 月現在、我々は 6 種類のサービスを 7 台のハニーポットセンサで観測を行っている。いずれのハニーポットも、日本国内で一般利用者向けにサービスを提供する ISP 回線に設置しており、DNS のみを観測する 1 台を除いて、表 1 の 6 種類のプロトコルを観測している。最も古いものは 2012 年 10 月から運用を開始しており、それ以降、より多くの攻撃を観測するため、ハニーポット数や対応するサービスを随時追加している。

## 4　DRDoS 攻撃の分析

AmpPot センサが観測した DRDoS 攻撃件数（AmpPot 1 台平均）の推移を図 3 に示す。観測開始当初の 2012 年 10 月には攻撃がほとんど観測されなかったが、2013 年半ば頃から攻撃が増加しはじめ、2015 年 10 月には 1 日平均 2,600 件の DRDoS 攻撃が観測されている。また、2015 年 10 月に観測された DRDoS 攻撃件数をそのプロトコルごとで比較すると、センサ 1 台あたりで、QOTD が 76 件（0.1 %）、CHG が 10,896

*12 http://www.ubuntu.com/
*13 http://www.netfilter.org/projects/iptables/index.html
*14 http://www.tcpdump.org/.

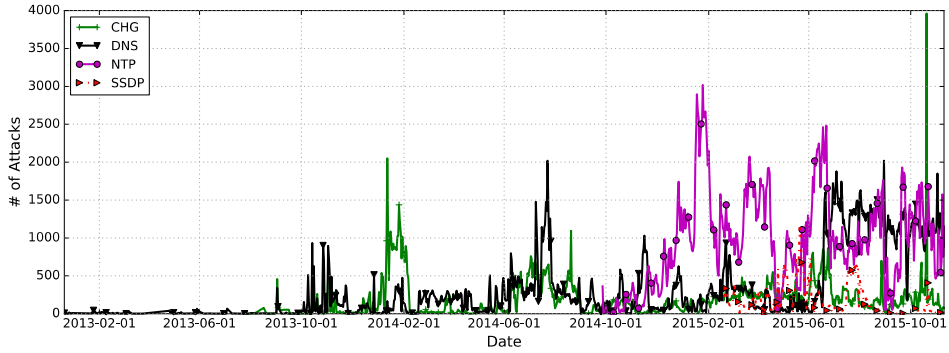


図 3　DRDoS 攻撃件数の推移 (AmpPot センサ 1 台平均)

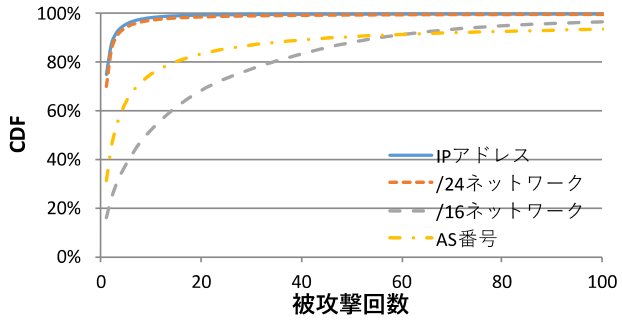


図 4　被攻撃回数の分布

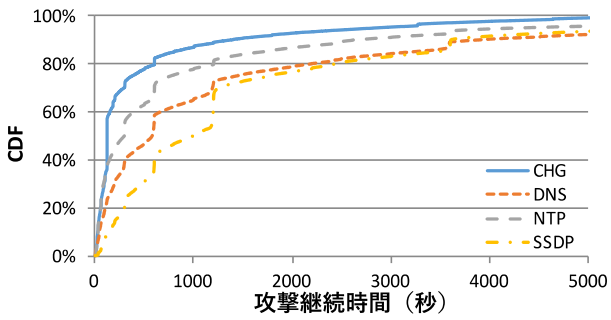


図 5　攻撃継続時間の分布

件 (12.9 %)、DNS が 34,467 件 (40.7 %)、NTP が 37,488 件 (44.3 %)、SNMP が 27 件 (0.03 %)、SSDP が 1,656 件 (2.0 %) であった。

本章では、AmpPot センサが観測した攻撃のうち、2015 年 1 月から 6 月までの半年間 (181 日間) に観測した攻撃を「被攻撃回数 (**4.1**)」「攻撃の継続時間 (**4.2**)」「攻撃を観測したハニーポット数 (**4.3**)」の 3 点に着目して分析し、**4.4** で分析結果を考察する。なお、QOTD・SNMP を利用する攻撃はほとんど観測されなかったため、以降の分析では、CHG・DNS・NTP・SSDP の 4 種類のプロトコルの分析結果を記載する。

## 4.1　被攻撃回数

分析対象期間における被攻撃回数の分布を、IP アドレス、/24 ネットワーク、/16 ネットワーク、AS 番号ごとに集計した結果を図 4 に示す。IP アドレス単位でみると、DRDoS 攻撃の被害者の 80 % は半年の間に 1 件の攻撃しかを受けておらず、半年間に 10 件以上の攻撃を受けた被害者は全体のわずか 1.5 % であった。また、/24 のネットワーク単位で攻撃を集計した結果も IP アドレスの場合と同様の推移を示したが、/16 のネットワーク単位や AS 単位で攻撃を集計すると、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　攻撃の継続時間

攻撃継続時間の分布を図 5 に示す。攻撃継続時間はプロトコルごとに多少傾向が異なっていたものの、300 秒、600 秒、900 秒、1,200 秒、3,600 秒のようなきりのよい時間に分布が偏っていた。プロトコルごとで比較すると、CHG の攻撃継続時間が最も短い傾向にあり、SSDP の攻撃継続時間が最も長い傾向にあった。攻撃全体でみると、継続時間が 1 分以下の攻撃が 18 %、5 分以下の攻撃が 48 %、10 分以下の攻撃が 63 % を占め、1 時間を超える攻撃はわずか 8 % であった。

## 4.3　攻撃を観測したハニーポット数

DRDoS 攻撃は、多数のリフレクタを踏み台とした攻撃であるため、同じ攻撃を複数のハニーポットが同時に観測することがある。DRDoS 攻撃を観測したハニーポット数の割合を図 6 に示す。NTP を利用する攻撃では、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 や SSDP を踏み台にする攻撃では、全攻撃の 40 % 程度しか複数のハニーポットで観測されていなかった。

### 4.4　考察

本章の冒頭で述べたように、観測開始当初、DRDoS 攻撃はほとんど観測されていなかったが、2015 年 10 月には 1 日平均 2,600 件の DRDoS 攻撃が観測されている。これは、AmpPot が観測するサービスを増やしたことも影響するが、図 3 の推移より、ここ数年で DRDoS 攻撃が DDoS 攻撃の実行手法として頻繁に利用されるようになったためであると推測される。また、サービスごとの攻撃件数を比較すると、DNS や NTP を悪用する攻撃は多く観測されていたが、QOTD や SNMP を悪用する攻撃はほとんど観測されていなかった。QOTD や SNMP が攻撃に悪用されない理由としては、ハニーポットの実装や設定の不備の可能性も考えられるが、これらのサービスはインターネット上のリフレクタ数や通信の増幅率の観点から、攻撃者にとって有用なサービスではなかったからであると考えられる。

AmpPot は多くの DRDoS 攻撃を観測しているが、**4.1** と **4.2** で述べたように、複数回攻撃される被害者は少なく、攻撃継続時間も短い傾向がみられた。この理由について、はっきりとした結論は得られていないが、これらの攻撃の中にはテスト攻撃が含まれていると我々は考えている。例えば、DDoS 攻撃を代行する Booter や Stresser と呼ばれるサービスでは、無料あるいは安価な値段で、攻撃通信量や攻撃時間に制約のある DDoS 攻撃を試し打ちできるサービスが提供されており、これらが攻撃数を引き上げる要因になっていると推測される。また、**4.3** の結果より、1 つのハニーポットでしか観測できていない攻撃が多数存在していたことから、現在設置している 7 台のハニーポットでは観測できていない攻撃が一定数存在すると考えられる。そのため、今後、ハニーポットの台数を増やす等して、観測する攻撃事例を増やしつつ、何台のハニーポットがあれば DRDoS 攻撃を網羅的に観測できるかを検証する必要がある。

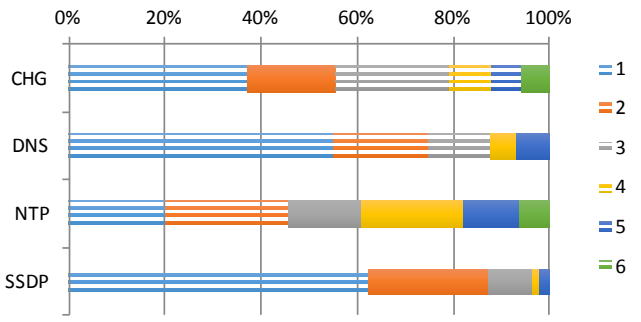


図 6　攻撃を観測したハニーポット数の割合

## 5　DRDoS 攻撃アラートシステム

AmpPot が提供するサービスは、一般に公開されている正規のサービスではないため、AmpPot が受信する通信は不正通信に関する可能性が高い。そのため、AmpPot が観測する通信を収集・分析して DRDoS 攻撃を検知しその情報を共有することにより、DRDoS 攻撃のアラートシステムを構築することができる。

DRDoS 攻撃アラートシステムの構成を図 7 に示す。システムは、「攻撃観測部」「攻撃分析部」「アラート送信部」の 3 つの要素からなる。攻撃観測部では、**3** で述べた AmpPot を運用し DRDoS 攻撃を観測する。AmpPot が観測した通信ログは攻撃分析部へ転送され、攻撃分析部では、通信ログから分析に必要な情報が抽出され、通信が分析される。分析の結果、攻撃と判断された通信情報はアラート送信部に転送され、連携先の組織へアラートが送信される。アラートの送信にあたっては、連携先の組織に不要なアラートを送信しないようにアラートをフィルタリングしたり、アラート

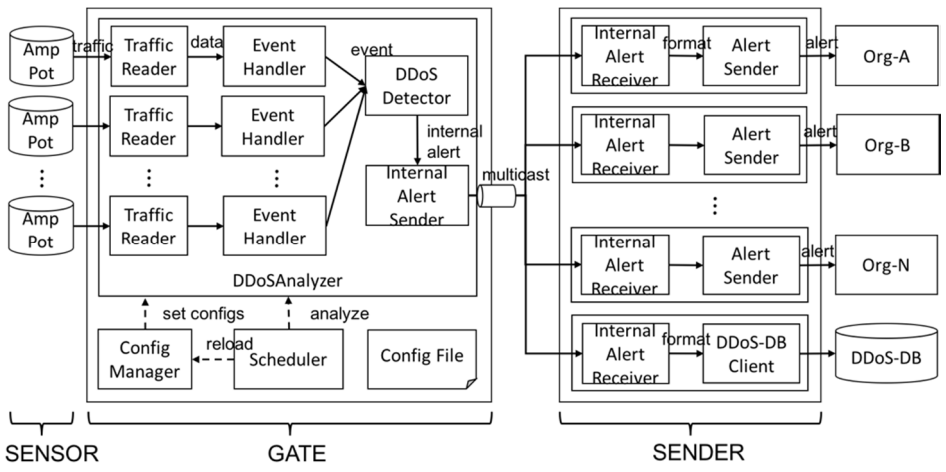


図 7　DRDoS 攻撃アラートシステムの構成

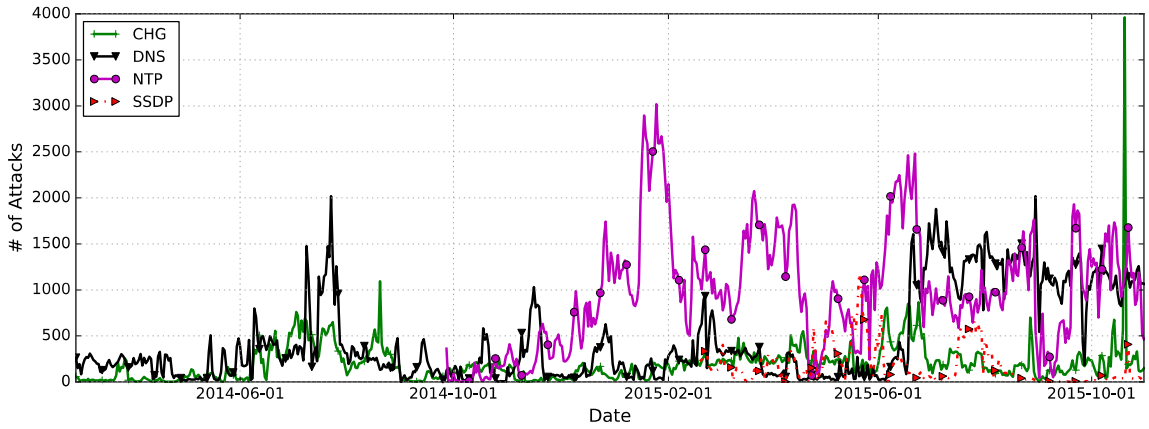


図 8　アラートシステムが送信したアラート数の推移

の出力形式を連携先の組織ごとに整形したりできるようにし、送信方法にはオープンソースのログコレクタである fluentd[*15] や電子メールを用意した。

我々は、国内の研究開発プロジェクトの枠組みにおいて、2014 年 2 月から提案システムの運用を行っており、2016 年 3 月現在、日本国内の複数の組織に DRDoS 攻撃のアラート情報を提供している（図 8）。AmpPot は一般に非公開のサービスであり、攻撃通信の検知が比較的容易であるため、正確で速報性のあるアラートの提供を期待できる。そのため、アラート情報をネットワーク運用者に提供することにより、本アラートシステムは DRDoS 攻撃の早期対応を支援するシステムとして期待できる。

## 6　まとめ

本稿では、我々が研究開発を進めている AmpPot の概要を説明し、AmpPot が観測した DRDoS 攻撃の分析結果を示した。また、AmpPot を応用した DRDoS 攻撃対策技術の 1 つとして、DRDoS 攻撃アラートシステムの取組について紹介した。

今後の課題としては、AmpPot センサの運用を継続するとともに、センサの台数や対応するプロトコルの増強等、より多くの攻撃を観測できるようにシステムの改良を行っていきたい。また、DRDoS 攻撃アラートシステムでアラート情報を提供するだけでなく、定期的な攻撃観測レポートを作成・公開することにより、DRDoS 攻撃の傾向を継続的に分析するとともに、Booter サービス等の DRDoS 攻撃を実行するインフラの実態解明や DRDoS 攻撃の対策技術に関する研究開発に取り組んでいきたい。

## 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（PRACTICE）」における研究開発により実施された。

### 【参考文献】

1　CloudFlare, "The DDoS That Almost Broke the Internet," http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/, 閲覧日 2016/04/21.
2　Akamai, "DD4BC: PLXsert warns of Bitcoin extortion attempts," https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html, 閲覧日 2016/04/21.
3　Jose Jair Santanna, Roland van Rijswijk-Deij, Rick Hofstede, Anna Sperotto, Mark Wierbosch, Lisandro Zambenedetti Granville, and Aiko Pras, "Booters - An Analysis of DDoS-as-a-Service Attacks," Integrated Network Management (IM), IFIP/IEEE Symposium, 2014.
4　Jose Jair Santanna, Romain Durban, Anna Sperotto, and Aiko Pras, "Inside Booters: An Analysis on Operational Databases," Integrated Network Management (IM), IFIP/IEEE Symposium, 2015.
5　Lukas Krämer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, and Christian Rossow, "AmpPot: Monitoring and Defending Amplification DDoS Attacks," Research in Attacks, Intrusions, and Defenses (RAID), Springer International Publishing, pp.615–636, 2015.
6　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.
7　Christian Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," Symposium on Network and Distributed System Security (NDSS), 2014.
8　Marc Kührer, Thomas Hupperich, Christian Rossow, Thorsten Holz, "Exit from Hell? Reducing the Impact of Amplification DDoS Attacks," USENIX Security Symposium, (2014).
9　Marc Kührer, Thomas Hupperich, Christian Rossow, and Thorsten Holz, "Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks," USENIX Workshop on Offensive Technologies (WOOT), 2014.
10　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, 閲覧日 2016/04/21.
11　The Akamai Blog, "RIPv1 Reflection DDoS Making a Comeback," https://blogs.akamai.com/2015/07/ripv1-reflection-ddos-making-a-comeback.html, 閲覧日 2016/04/21.

＊15 http://www.fluentd.org/

**牧田大佑**　（まきた　だいすけ）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究員
横浜国立大学大学院
サイバーセキュリティ

**吉岡克成**　（よしおか　かつなり）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
招聘研究員
横浜国立大学大学院
博士（工学）
サイバーセキュリティ