情報処理学会論文誌 Vol.57 No.9 1974–1985 (Sep. 2016)

早期インシデント対応を目的とした DRDoS攻撃アラートシステム

牧田 大佑[1,2,a)] 西添 友美[1] 吉岡 克成[3] 松本 勉[3] 井上 大介[2] 中尾 康二[2]

受付日 2015年12月3日, 採録日 2016年6月2日

概要：近年，DRDoS 攻撃がインターネット上の大きな脅威となっている．DRDoS 攻撃による被害を軽減するためにはその早期対応が重要となるが，通常のネットワークには攻撃とは無関係の大量の通信が流れているため，攻撃の判断は難しく，その処理に時間を要する．そこで本論文では，DRDoS 攻撃を観測するハニーポット（DRDoS ハニーポット）を利用した DRDoS 攻撃アラートシステムを提案する．提案システムは，DRDoS ハニーポットが観測した通信からリアルタイムに DRDoS 攻撃を検知し，そのアラート情報を連携組織へ送信することにより，DRDoS 攻撃への早期対応を支援する．我々は，国内の研究開発プロジェクトの枠組みで提案システムの運用を行っている．本論文では，その運用結果を報告するとともに，提案システムが観測した DRDoS 攻撃の傾向を分析する．また，提案システムが観測した DRDoS 攻撃と国内のある ISP において観測された大量通信の観測結果を比較した結果，提案システムが正確で速報性の高いアラートを提供できた事例を示す．この結果は，提案システムが DRDoS 攻撃の早期対応に有用な情報を提供できる可能性を示しており，提案システムは 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．

キーワード：サイバーセキュリティ，DRDoS 攻撃，DDoS 攻撃対策

DRDoS Attack Alert System for Early Incident Response

Daisuke Makita[1,2,a)] Tomomi Nishizoe[1] Katsunari Yoshioka[3] Tsutomu Matsumoto[3] Daisuke Inoue[2] Koji Nakao[2]

Received: December 3, 2015, Accepted: June 2, 2016

Abstract: In recent years, DRDoS attack has become a major threat on the Internet. To mitigate the damage caused by DRDoS attack, its early response is important. However, because a lot of traffic that is not related to attacks is observed in a normal network, detecting DRDoS attacks is a hard and time-consuming task. In this paper, we propose a DRDoS attack alert system using honeypots that observe DRDoS attack (DRDoS honeypot). Our system detects DRDoS attacks from traffic that DRDoS honeypots collects in real time, and sends their alert information to collaborating organizations in order to support early response against DRDoS attacks. We have operated this system in the framework of an R&D project in Japan. In this paper, we report the operational results and analyze the trend of DRDoS attacks our system observed. In addition, as a result of comparison between our system and an ISP's mass communication detector, we show that our system is able to provide accurate and rapid alerts. This result shows that our system can provide useful information for early responses, and therefore our system can be expected as a system for supporting early responses against DRDoS attacks.

Keywords: Cybersecurity, DRDoS Attack, DDoS Mitigation

1. はじめに

近年，DRDoS 攻撃（Distributed Reflection Denial-of-

[1] 横浜国立大学大学院環境情報学府
Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 情報通信研究機構
National Institute of Information and Communications Technology, Koganei, Tokyo 184–8795, Japan
[3] 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
Graduate School of Environment and Information Sciences, Yokohama National University/Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[a)] makita-daisuke-jk@ynu.jp

Service Attack；分散反射型サービス妨害攻撃）がインターネット上の大きな脅威となっている．DRDoS 攻撃とは，インターネット上のサーバを踏み台にして大量のパケットを攻撃対象組織に送信することにより，その組織のネットワーク等のリソースを圧迫するサービス妨害攻撃である．DRDoS 攻撃では，攻撃者は攻撃の通信量を非常に大きくすることが可能であり，2013 年 3 月に実行された攻撃では 300 Gbps，2014 年 2 月に実行された攻撃では 400 Gbps もの攻撃通信が観測されている [13], [14]．このように，DRDoS 攻撃による被害は深刻さを増しているが，その一方で，Booter や Stresser と呼ばれる DDoS 攻撃代行サービス[*1]が登場しており [5], [6]，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．また，昨今問題となっているハッカー集団の Anonymous や Lizard Squad，DDoS 攻撃で企業を脅迫して身代金を要求する DD4BC や Armada Collective の攻撃活動においても，DRDoS 攻撃が攻撃の実行手段として利用されており [15], [16]，今後もこの攻撃による脅威は拡大することが予想される．

しかし，DRDoS 攻撃は大量のパケットで攻撃対象組織のリソースを枯渇させる攻撃であるため，この攻撃による被害を防ぐ方法は確立されておらず，ひとたび攻撃が実行されると，被害側はその攻撃が終わるのを待つか，ブラックホールルーティングやパケットフィルタリング等の技術を利用して被害を軽減させつつ，攻撃が終わるまで耐えるしかないのが現状である．また，攻撃で発生する通信量によっては，攻撃対象の組織だけでなくその周囲の組織のネットワークにも影響を及ぼしうるため，被害組織だけでなくその周囲の組織と協力して攻撃に対処することが必要になる場合もある．

このような状況の中で，DRDoS 攻撃への早期対応は，攻撃の被害を軽減させつつネットワークを安定運用するための重要な要素である．しかし，様々なサービスを提供するネットワークでは，攻撃とは無関係の正常な通信が大量に流れているため，定常的な通信監視による DRDoS 攻撃の検知は，攻撃の判断が困難でその処理に時間を要する．

本論文では，DRDoS 攻撃を観測するハニーポット（以降，DRDoS ハニーポット）を利用した DRDoS 攻撃アラートシステムを提案する．提案システムは，インターネット上に設置した DRDoS ハニーポットからリアルタイムに通信情報を収集し，それに含まれる DRDoS 攻撃を検知することにより，そのアラート情報を連携組織へ送信する．DRDoS ハニーポットは一般に公開されているサービスではなく正規のユーザが存在しないため，攻撃通信の検知が比較的容易であり，正確で速報性の高いアラートを提供することができる．このアラート情報を利用することにより，ネットワーク管理者は状況を把握し迅速に対応を決定することが可能になる．

提案システムの有用性を検証するため，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，2015 年 11 月現在，日本国内の複数の ISP（Internet Service Provider）に DRDoS 攻撃のアラート情報を提供している．本論文では，その運用結果を報告するとともに，提案システムが観測した DRDoS 攻撃の傾向を分析する．また，この研究開発プロジェクトの枠組みにおいて，提案システムが観測した DRDoS 攻撃と国内のある ISP において観測された大量通信の観測結果を比較した結果，提案システムが正確で速報性の高いアラートを提供できた事例を確認したのでその結果をまとめる．

本研究の貢献としては，まず，DRDoS ハニーポットを利用した DRDoS 攻撃アラートシステムを構築し，そのアラート情報をリアルタイムに連携組織に提供する枠組みを構築したことがあげられる．ハニーポット技術を用いたサイバー攻撃観測システムはすでに多数存在するが，DRDoS 攻撃を観測・通知するアラートシステムは我々の知る限り初めてのシステムである．また，提案システムを 1 年半以上の長期にわたって運用し，連携先の組織に攻撃情報を提供することにより，その組織内でのインシデント対応に貢献したことも意義のある成果である．さらに，提案システムが観測した DRDoS 攻撃と ISP において観測された大量通信と比較した結果として，提案システムが正確で速報性の高いアラートを提供できた事例を示す．この結果は，提案システムが DRDoS 攻撃の早期対応に有用な情報を提供できる可能性を示しており，提案システムは 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．

本論文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．3 章で，本論文で提案する DRDoS 攻撃アラートシステムの構成と実装について説明し，4 章で提案システムの実運用結果と DRDoS 攻撃の分析結果を述べる．5 章で提案システムとその運用結果について考察し，6 章で DRDoS 攻撃対策の関連研究を述べる．最後に，7 章でまとめと今後の課題を記す．

2. 背景

2.1 DRDoS 攻撃

DRDoS 攻撃とは，インターネット上に公開されているサーバを踏み台にして大量のパケットを攻撃対象組織に送信することにより，その組織のネットワーク等のリソースを圧迫するサービス妨害攻撃である．この攻撃では，次の 2 つの性質を満たすサービスが悪用される．

[*1] Booter/Stresser は，負荷テストの名目で DDoS 攻撃のサービスを提供しているが，その実態を端的に表現するため，本論文では「DDoS 攻撃代行サービス」と表記した．

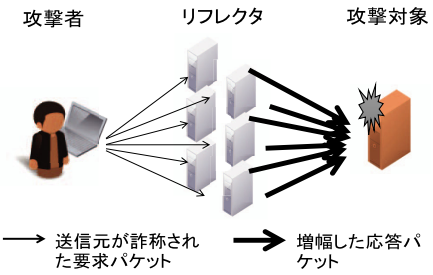

図 1 DRDoS 攻撃
Fig. 1 DRDoS attack.

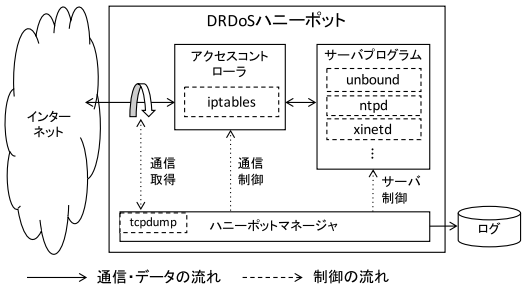

図 2 DRDoS ハニーポットの構成
Fig. 2 Architecture of DRDoS honeypot.

- 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，DRDoS 攻撃はアンプ攻撃とも呼ばれる．
- 反射効果（Reflection）
  サーバが通信の反射板となる性質．要求パケットの送信元アドレスを確認せずに応答パケットを送信するプロトコル[*2]を使用することにより，攻撃者はそのサーバに任意のホストに応答パケットを送信させることができる．この性質から，DRDoS 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マシンを利用し，送信元の 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）ため，攻撃対象のアドレスには大量の増幅した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 [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，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，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 DRDoS 攻撃に悪用できることが最近の研究によって指摘されており [3], [17], [18]，今後も DRDoS 攻撃による脅威は拡大することが予想される．

2.2 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・分析を主な目的とした，不正使用されることに価値を持つ情報システムである．

本論文で使用する DRDoS ハニーポットは，DRDoS 攻撃の観測を目的とした囮（おとり）のリフレクタであり，これをインターネット上に設置することにより，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 [2][*3]．攻撃者は，インターネット上で定常的なスキャンを実施することにより，攻撃の踏み台と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，DRDoS ハニーポットを**図 2** のように構成する．DRDoS ハニーポットは，「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する役割を担う．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，サーバプログラムが攻撃に悪用された場合に，外部に与える影響を抑えるように通信を制御する役割を担う．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，および，通信ログの出力を担当する．

我々が運用する DRDoS ハニーポットは，2015 年 11 月現在，DRDoS 攻撃に利用される可能性の高い 6 種類のサー

表 1 DRDoS ハニーポットが提供するサービスと使用する実装の一覧
Table 1 List of services and implementations that DRDoS honeypot provides.

サービス名	ポート	実装
QOTD	17/UDP	quoted[24]
CHG	19/UDP	xinetd[25]
DNS	53/UDP	BIND[26],Unbound[27]
NTP	123/UDP	NTP Project[28]
SNMP	161/UDP	Net-SNMP[29]
SSDP	1900/UDP	簡易スクリプト

[*2] 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．

[*3] 文献 [2] は，DRDoS 攻撃を観測するハニーポットを AmpPot と表記しているが，本論文では「DRDoS ハニーポット」と表記する．

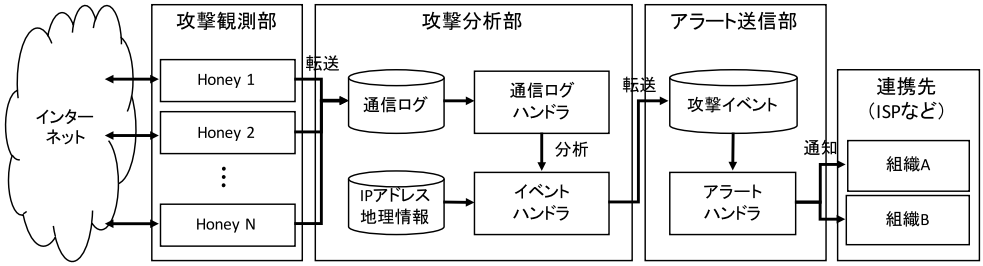

図 3 DRDoS 攻撃アラートシステムの構成
Fig. 3 Architecture of DRDoS attack alert system.

ビスを観測している（**表 1**）．DRDoS ハニーポットの実装にあたっては，表 1 のサーバプログラムを Linux のディストリビューションの 1 つである Ubuntu [21] 上にインストールし，アクセスコントローラとして iptables [22]，ハニーポットマネージャとして自作のシェルスクリプトを使用した．通信ログは，tcpdump [23] を用いて PCAP 形式で取得し，その PCAP ファイルを DRDoS ハニーポットの出力とした．

3. DRDoS 攻撃アラートシステム

本章では，DRDoS ハニーポットを利用した DRDoS 攻撃アラートシステムを提案し，その構成と実装について説明する．提案システムは，インターネット上に設置した DRDoS ハニーポットからリアルタイムに通信情報を収集し，それに含まれる DRDoS 攻撃を検知することにより，そのアラート情報を連携組織へ送信する．アラートシステムが DRDoS 攻撃の早期対応の役に立つためには，アラートが正確でかつ速報性が高いことが必要である．ここでいう「正確」とは，送信されるアラートが示す攻撃通信が被害側にも実際に到達していることを指し，「速報性が高い」とは既存の検出エンジンと比較して同等かそれよりも早く攻撃を検知できていることを指すこととする．このような要件を満たすアラートシステムを構築・運用することにより，ネットワーク管理者は受信したアラート情報をもとに状況を把握し，迅速に対応を決定することができるようになる．

本章の構成は次のとおりである．まず，3.1 節で提案システムの構成を説明する．次に，3.2 節で提案システムにおける分析の単位である「イベント」を定義し，3.3 節で提案システムが提供するアラートに含まれる情報を示す．そして，3.4 節で本論文におけるシステムの実装を説明する．

3.1 システムの構成

提案システムの構成を**図 3** に示す．提案システムは，「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，2.2 節で述べた DRDoS ハニーポットを運用し，DRDoS 攻撃を観測する．グローバル IP アドレスごとにハニーポットに識別子を割り当て，各ハニーポットが観測した通信ログを攻撃分析部へ転送する．

攻撃分析部では，攻撃観測部で収集した通信ログから分析に必要な情報を抽出し，通信をイベント単位で集約・分析する．図 3 の通信ログハンドラは通信ログの形式の差異を吸収して必要な情報を抽出する役割を担い，イベントハンドラは通信の整理・分析を担当する．なお，イベントハンドラでは，攻撃対象の分析のために IP アドレスからその地理情報（国や組織）を特定するデータベースを使用する．

イベントハンドラによって攻撃と判断されたイベントはアラート送信部に転送され，アラートハンドラが連携先の組織へアラートを送信する．アラートハンドラは，不要なアラートを転送しないようにアラートをフィルタリングしたり，アラートの出力形式を連携先の組織ごとに整形したりする役割も担う．また，アラートの送信にあたっては，オープンソースのログコレクタである fluentd [30] や電子メール等，複数の送信方法を用意する．

3.2 イベントの定義

DRDoS ハニーポットが観測する通信の中には，DRDoS 攻撃だけでなくリフレクタの探索活動やサーバの脆弱性を攻撃する通信が含まれる．そのため，提案システムではこれらの DRDoS 攻撃ではない通信を取り除く必要がある．また，DRDoS 攻撃が発生すると，DRDoS ハニーポットは大量の要求パケットを受信するため，パケット単位でのアラートの通知は困難である．そこで提案システムでは，DRDoS ハニーポットが受信する一連のパケットを「イベント」として処理し，そのイベントごとに攻撃か否かを判断してアラートを送信する．

提案システムにおけるイベントの概念は次のとおりである．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，サービス，送信元アドレス」の組をキーとして整理する．次に，受信時刻順に整理された一連のパケットにおいて，隣り合うパケットの受信時刻の間隔 Δt が閾値 T 以下の場合は同じグループとし，T を超えたものは別のグループとして分離する（**図 4**）．この処理の結果，生成されたパケットのグループがイベントであり，このイベントの集合のうち，パケット数が閾値 N_{attack}

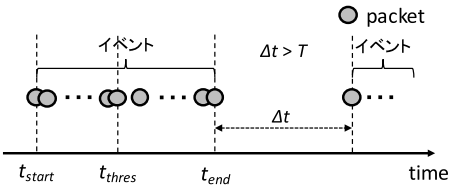

図 4 提案システムにおけるイベントの概念
Fig. 4 Concept of event in the system.

以上のイベントをハニーポットが観測した DRDoS 攻撃のイベントとする．

3.3 アラートに含まれる情報

提案システムでは，DRDoS 攻撃に関する次の 2 種類のアラートを提供する．

- 攻撃開始アラート
  攻撃が始まったことを通知するアラート．イベントのパケット数が閾値 N_{attack} に達すると，提案システムはそのイベントを攻撃と判断して攻撃開始アラートを送信する．図 4 の例では，$t = t_{thres}$ の直後にアラートを送信する．
- 攻撃終了アラート
  攻撃が終わったことを通知するアラート．攻撃と判断されたイベントにおいて，新しいパケットが閾値 T 秒以上観測されなかった場合に，提案システムはそのイベントを攻撃終了と判断して攻撃終了アラートを送信する．図 4 の例では，$t = t_{end} + T$ の時刻にアラートを送信する．

各種アラートに含まれる情報と攻撃終了アラートの例を**表 2** と**図 5** に示す．アラートには，観測したハニーポットの ID 等のメタ情報をはじめ，攻撃対象の IP アドレスやその地理情報，攻撃の開始・終了時刻等の情報が含まれる．

3.4 システムの実装

提案システムの各部の実装は次のとおりである．

まず，攻撃観測部は DRDoS ハニーポットからなるが，その実装は 2.2 節で述べたとおりである．DRDoS ハニーポットが出力する PCAP ファイルを使用し，この PCAP ファイルは 1 分ごとに攻撃分析部へ転送するように設定した．

攻撃分析部は，DRDoS ハニーポットと同様に Ubuntu 上に実装した．通信ログの分析にはスクリプト言語の Python [31] を使用し，そのライブラリとして，PCAP ファイルを扱う pcapy [32] とパケットを分析する dpkt [33] を使用した．また，攻撃対象の地理情報（国や AS 情報等）の取得には MaxMind 社 [34] の GeoIP データベースを使用した．

アラート送信部は，攻撃分析部と同じマシン上に Python を用いて実装した．アラートの送信方法としては，オープンソースのログコレクタである fluentd と電子メールに対応した．なお，fluentd のクライアントライブラリには fluent-logger-python [35] を使用し，電子メールの送信処理には Python の標準ライブラリを使用した．

表 2 アラートに含まれる情報の一覧
Table 2 List of alert information.

(a) 攻撃開始アラート
(a) Attack-Start Alert

値	値の意味
alerttime	アラート送信時刻
as	攻撃対象の AS 情報
country	攻撃対象の国情報
detecttime	攻撃検知時刻（図 4 の t_{thres}）
query (DNS のみ)	DNS クエリ数（ドメイン，型，クラスごと）
sensorid	攻撃を観測したハニーポットの識別子
service	攻撃を観測したサービス
starttime	攻撃開始時刻（図 4 の t_{start}）
target	攻撃対象の IP アドレス
totalpacket	観測パケット数

(b) 攻撃終了アラート
(b) Attack-End Alert

値	値の意味
（開始時アラートの情報を更新したもの）	
elapsedtime	継続時間（秒）
stoptime	攻撃終了時刻（図 4 の t_{end}）
maxpps	ハニーポットが観測した通信の最大 PPS
avepps	ハニーポットが観測した通信の平均 PPS
hostname	IP アドレスの逆引きで得られるホスト名


```
{
    "hostname": "[redacted].net",
    "elapsedtime": 3600,
    "as": "AS1[redacted]",
    "stoptime": "2015-10-31T08:09:49+09:00",
    "alerttime": "2015-10-31T08:11:37+09:00",
    "query": {
        "1x1.cz    ANY    IN": 59966
    },
    "maxpps": 23.35,
    "detecttime": "2015-10-31T07:09:59+09:00",
    "target": "[redacted].216.192",
    "service": "dns",
    "country": "Canada",
    "avepps": 16.38415300546448,
    "starttime": "2015-10-31T07:09:49+09:00",
    "sensorid": "sensor007",
    "totalpacket": 59966
}
```


図 5 攻撃終了アラートの例（fluentd で利用される JSON 形式）
Fig. 5 Example of attack-end alert (JSON format used by fluentd).

4. 実運用結果と攻撃の分析

提案システムの有用性を検証するため，我々は，国内の研究開発プロジェクトの枠組みで 2014 年 2 月から提案シ

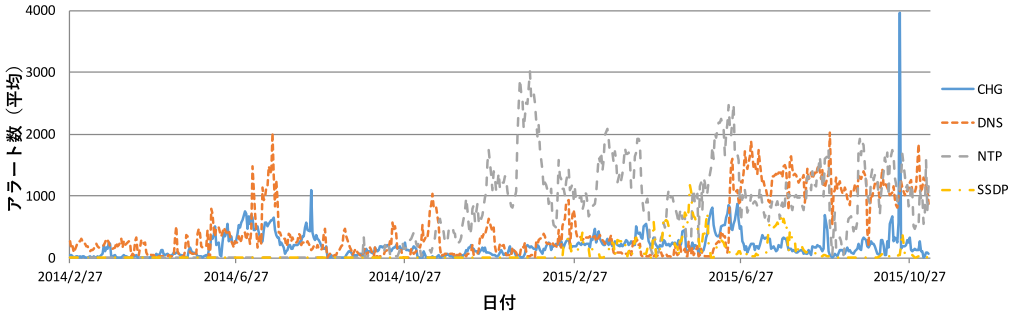

図 6 日ごとの DRDoS 攻撃アラート数（ハニーポット 1 台平均）の推移
Fig. 6 The number of daily DRDoS attack alerts per honeypot.

表 3 提案システムの主な運用履歴
Table 3 Operation history of the system.

日付	変更点
2014/02/27	攻撃終了時アラートの提供を開始．観測するハニーポットは 2 台．対応サービスは DNS と CHG．
2014/05/10	観測するハニーポットを 4 台に増強．
2015/05/17	観測するハニーポットを 7 台に増強．
2014/09/27	攻撃検知時アラートの提供を開始．NTP と QOTD に対応．
2015/02/19	SNMP・SSDP に対応．

ステムの運用を行っており，2015 年 11 月現在，国内の複数の ISP に DRDoS 攻撃のアラート情報を提供している．本章では，提案システムを 1 年半以上の長期にわたって運用した結果を報告するとともに，提案システムが観測した DRDoS 攻撃の傾向を分析する．また，この研究開発プロジェクトの枠組みにおいて，提案システムが観測した DRDoS 攻撃と国内のある ISP において観測された大量通信の観測結果を比較したのでその結果をまとめる．なお，4.2 節以降に記載する統計値は，簡単のために，提案システムと同じ処理を行うプログラムを別途用意して後日集計した値を使用した．

4.1 運用状況

提案システムの主な運用履歴を時系列順に記したものを**表 3** にまとめる．2014 年 2 月 27 日から攻撃終了アラートの提供を開始し，同年 9 月 27 日から攻撃検知アラートの提供を開始した．提供開始当初は，2 台のハニーポットで攻撃を観測していたが，ハニーポットの台数を増やすことにより観測可能な攻撃が増えるのかを検証するため，2014 年 5 月に観測するハニーポットの台数を 7 台に増強した．これらのハニーポットはいずれも日本国内で一般向けにサービスを提供する異なる ISP 回線に設置しており，DNS のみを観測する 1 台を除いては，DRDoS ハニーポットは表 1 の 6 種類のサービスを観測している．

実際の運用における閾値に関しては，アラートの速報性を維持しつつもイベントを必要以上に分割してしまわないように $T = 60$ [sec] とし，スキャン等の通信を確実に除外するために $N_{attack} = 100$ [packets] と設定した．これらの閾値については 5.1 節で議論するが，4 章で述べる実運用の結果から，これらの暫定値で提案システムは機能していると我々は考えている．

4.2 アラート数の推移

提案システムが送信したアラート数（ハニーポット 1 台平均）の推移を**図 6** に示す．提供開始当初の 2014 年 2 月には，1 日 260 件程度の攻撃しか観測されなかったが，2014 年 6 月頃から攻撃数が増加し，2015 年 10 月現在では 1 日平均 2,700 件の DRDoS 攻撃が観測されている．

2015 年 10 月に観測した DRDoS 攻撃件数をそのサービスごとで比較すると，ハニーポット 1 台あたりで，QOTD が 76 件（0.1%），CHG が 10,896 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．最も多く攻撃が観測された DNS に関しては，1 日平均 1,100 件以上の攻撃が観測されたが，QOTD・SNMP を悪用する攻撃はほとんど観測されなかった．そのため，本論文では，CHG・DNS・NTP・SSDP の 4 種類のサービスを悪用する DRDoS 攻撃の結果のみを記載する．

4.3 DRDoS 攻撃の分析

本節では，提案システムが観測した攻撃のうち，2015 年 1 月（ただし，SSDP は 2 月 19 日以降）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」「攻撃の継続時間」「観測したハニーポット数」の 3 点に着目して分析する．なお，本節の分析では，複数のハニーポットが同時刻に同じアドレス宛の攻撃を観測していた場合には，それらのイベントを事前に 1 つのイベントにまとめて分析を行っている．

4.3.1 被攻撃回数

半年間の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

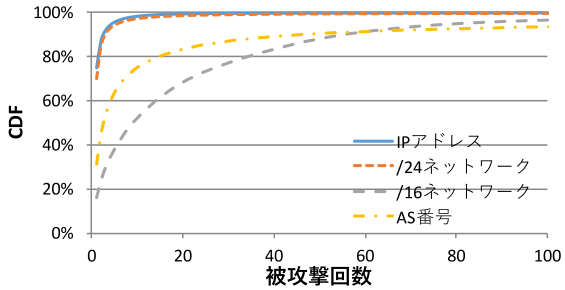

図 7 被攻撃回数の分布

Fig. 7 CDF of the number of attacks per victim.

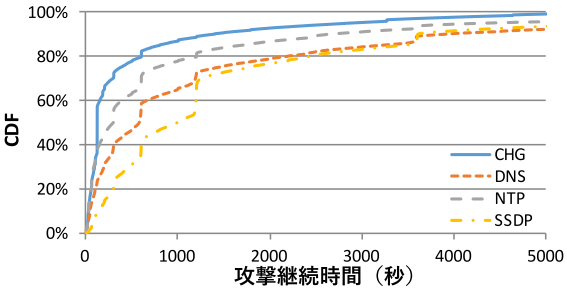

図 8 攻撃継続時間の分布

Fig. 8 CDF of attack durations.

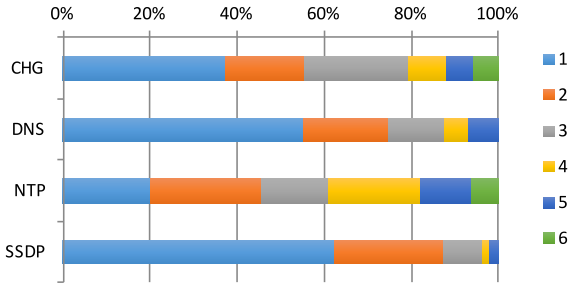

図 9 攻撃を観測したハニーポット台数の割合

Fig. 9 Ratio of the number of honeypots that observed the attack.

表 4 提案システムの攻撃検知時刻と ISP における大量通信検知時刻の比較

Table 4 Comparison of attack detection time between our system and ISP.

提案システムの攻撃検知時刻	ISP における大量通信検知時刻	時間差（秒）
2014/10/XX 00:10:46	2014/10/XX 00:15:54	308
2014/11/XX 21:41:16	2014/11/XX 21:44:30	194
2014/11/XX 23:57:34	2014/11/XX 23:59:20	106
2014/11/XX 17:02:21	2014/11/XX 17:04:44	143

果を図 7 に示す．IP アドレス単位でみると，DRDoS 攻撃の被害者の 80%は半年間に 1 件の攻撃しか受けておらず，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．

4.3.2 攻撃の継続時間

攻撃継続時間の分布を図 8 に示す．攻撃継続時間はサービス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．サービスごとで比較すると，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．

4.3.3 観測したハニーポット数

攻撃を観測したハニーポット数（＝その攻撃を何台のハニーポットが観測していたのか）の割合を図 9 に示す．NTP を踏み台にする攻撃では，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 ISP における大量通信検知時刻との比較

提案システムは，2014 年 10 月 9 日から 2014 年 11 月 10 日までの間に，国内のある ISP 宛の 11 件の DRDoS 攻撃を観測した．この 11 件の攻撃について調査した結果，そのうちの 4 件の攻撃については ISP においても大量通信に該当する攻撃として検知されていた．この 4 件の攻撃について，提案システムが攻撃を検知した時刻と ISP において大量通信が検知された時刻を比較した結果を表 4 に示す．分析の結果，4 件の攻撃のすべてにおいて ISP での大量通信検知前に提案システムが攻撃を検知しており，その時間差は平均して 188 秒存在した．また，残りの 7 件の攻撃においても，その ISP が定める大量通信の定義には達していなかったものの，同時刻にある程度の規模の通信が観測されていたことを確認した．

5. 考察

本章では，提案システムとその運用結果について考察する．まず，提案システムに関して，5.1 節でイベントの定義と各種閾値の妥当性，5.2 節で処理の遅延について考察する．次に，提案システムの運用結果に関して，5.3 節で DRDoS 攻撃の分析結果，5.4 節でアラートの正確性と速報性について考察する．そして最後に，5.5 節でアラートの有用性について議論する．

5.1 イベントの定義と各種閾値

提案システムは，3.2 節で定義した「イベント」単位で通信を分析し，攻撃のアラートを送信する．イベントは送信

元アドレスごと整理された一連のパケットであり，T 秒以上の間隔を開けずに N_{attack} 個以上のパケットが観測された場合に，そのイベントは攻撃と判断される．本節では，このイベントの定義と閾値の妥当性について考察する．

イベントの定義では，送信元アドレスごとにパケットを集約しているが，これは我々の経験則によるものである．これまで観測してきたDRDoS攻撃は，単一のIPアドレスからの大量の要求パケットを観測するものがほとんどであった．しかし，ネットワーク帯域の枯渇を目的としたDRDoS攻撃の中には，単一のIPアドレスではなく，特定のアドレス帯（たとえば，/24のネットワーク全体）を攻撃対象にする攻撃が存在する．そのような攻撃では，単一のIPアドレスではあまりパケットが観測されずに攻撃と判断されなかったり，逆に，本来は同じ攻撃として処理すべき攻撃に対して大量に攻撃を検知したりしてしまう．そのため，特定のアドレス帯を攻撃対象にするような攻撃に対しては，本論文のイベントの定義は不適切であると考えられる．

また，提案システムの運用で暫定的に使用している閾値（$T = 60\,[\mathrm{sec}]$，$N_{attack} = 100\,[\mathrm{packet}]$）も，我々の経験則で決定した値である．閾値 T は，その値を小さく設定することにより，アラートの速報性を高めることができるが，一方で，一連の攻撃イベントを不必要に細かく分割してしまう可能性がある．逆に，閾値 T に大きな値を設定すると，アラートの速報性が失われるが，攻撃の小休止等を考慮せずに攻撃の全体をとらえることができる．現状の運用では，アラートの速報性を優先しつつも攻撃全体をとらえることができるように，$T = 60\,[\mathrm{sec}]$ と設定している．また，閾値 N_{attack} は，その値を小さく設定することにより，攻撃と判断するまでの時間が短くなりアラートの速報性を高めることができるが，一方で，DRDoS攻撃でないスキャン等の通信を攻撃と判断する可能性がある．逆に，閾値 N_{attack} に大きな値を設定すると，パケット数が N_{attack} まで到達するのに時間がかかるためアラートの速報性は失われてしまうが，高い確度でDRDoS攻撃と判断することができる．提案システムの運用において，アラートの速報性を失わないようにしつつも，スキャン等の通信を確実に除外するために，$N_{attack} = 100\,[\mathrm{packet}]$ と設定している．

これらの定義や閾値を調整することによって，アラート数やその精度がどの程度変化するのかを検証することは今後の課題であるが，これまでの結果から，これらの暫定値で提案システムは機能していると我々は考えている．

5.2 実装にともなう遅延

提案システムは，攻撃観測部で観測した通信を攻撃分析部に転送し，そこで検知した攻撃をアラートとして送信するが，観測からアラート送信までの処理の過程で遅延が発生する．本節では，この遅延について考察する．

まず，攻撃観測部では，DRDoSハニーポットの通信をtcpdumpで取得し，1分ごとに攻撃分析部へと転送しているため，ログの収集と転送で1分程度の遅延が見込まれる．次に，攻撃分析部では，通信ログの分析に要する時間とアラートの送信条件を満たすまでの待機時間[*4]が存在するため，ここでも1分程度の遅延が想定される．

これらの遅延を考慮すると，DRDoS攻撃が実際に開始・終了してからアラートを送信するまでに約2分の遅延が発生すると推測される．この処理の遅延は，通信ログの収集・転送方法を変更したり分析プログラムの処理を高速化したりすることによって，ある程度改善することはできるが，4.4節の表4の比較結果を考えると，アラートシステムは遅延を考慮してもISPで大量通信が検知されるよりも早くアラートを送信した事例が存在しており，現状のシステムでも早期対応に有用なアラートを提供できた例があるといえる．

5.3 観測結果と攻撃の分析

4.2節で述べたように，アラート提供開始当初の2014年2月には1日260件程度の攻撃しか観測されていなかったが，2015年10月には1日平均2,700件のDRDoS攻撃が観測されている．ハニーポットが対応するサービスを増やしたことも影響するが，図6より，ここ数年でDRDoS攻撃が攻撃の実行手法として頻繁に利用されるようになってきていると考えられる．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いからだと我々は考えている．

提案システムは非常に多くのDRDoS攻撃を観測しているが，4.3節で述べたように，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．たとえば，DDoS攻撃を代行するBooterやStresserと呼ばれるサービスでは，無料あるいは手頃な値段で，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考えられる．実際，4.4節の分析結果より，連携しているISP宛の11件の攻撃のうち，4件はISP側でも大量通信として検知されていたが，残りの7件は大量通信の閾値に達しておらず，これらの7件の攻撃は

[*4] 攻撃開始アラートの場合はパケット数が閾値 N_{attack} に到達するまでの時間．攻撃終了アラートの場合は，攻撃終了と判断するまでの閾値 T 秒間．

テスト攻撃であった可能性があると考えられる．

5.4 アラートの正確性と速報性

4.4 節で述べたように，提案システムが観測したある ISP 宛の 11 件の攻撃は，その ISP でも観測されていた．このことから，提案システムのアラートは正確であるといえる．すべての攻撃が ISP 側で大量通信として検知されたわけではなく，11 件中 7 件の攻撃はその ISP が定義する大量通信に達していなかったが，同時刻にある程度の規模の通信が観測されていたことから，これらのアラートはネットワーク管理者に有用な情報を提供できていたといえる．一方で，4.3.3 項の結果より，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ることから，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推測される．そのため，今後，ハニーポットの台数を増やすことにより，観測する事例を増やしつつ，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と考えている．また，ハニーポットの台数以外にも，ハニーポットがより多くの攻撃を観測するための条件（たとえば，ハニーポットを設置する国や AS，ISP 回線等）がないかについても，今後検証を進めたい．

また，表 4 の比較結果より，ハニーポットと ISP の両方で検知された 4 件の攻撃（大量通信）については，いずれもハニーポットの方が早く検知できたことを確認した．提案システムの検知時刻の方が早い理由については様々な要因が考えられるが，正常の通信をほとんど含まないハニーポットの方が，ISP の観測よりも攻撃の検知が容易で分析の時間が短く済むことが大きいと考えられる．ただし，この結果に関しては比較件数が少ないため，今後，このような分析を継続することにより，アラートの速報性についてより正確な分析を行う必要があると考えている．

5.5 アラートの有用性

まず，これまで議論してきたように，提案システムは正確で速報性が高いアラートを提供できた事例があるため，攻撃開始アラートはインシデントの初期対応に有用な情報を提供できる可能性があると考えられる．このアラート情報を用いることで，具体的にどのような対応ができるかの検討については今後の課題であるが，アラートにより，攻撃が発生したこと，どこが攻撃されているか，どのサービスが悪用されているか等の基本的な情報が分かるため，ネットワーク管理者が状況を把握し対応を判断するうえで有用な情報であるといえる．

また，攻撃終了アラートもインシデントの対応を終了するうえで有用な情報を提供できる．たとえば，攻撃が発生した際にネットワークのゲートウェイで攻撃通信を遮断する対応を実施した場合，攻撃終了後に迅速に復旧作業を行う必要がある．このような場合に，攻撃終了アラートは，攻撃が終了したことを客観的に判断する情報として活用できる．このほかにも，攻撃終了アラートは，攻撃対象に関する情報をはじめ，開始時刻や終了時刻等，攻撃に関する様々な情報を含むため，このアラートをデータベースに蓄積することにより，過去の攻撃情報を共有することができる点でも有用である．

このように，提案システムが提供するアラート情報は，DRDoS 攻撃の早期対応に有用であると考えられるため，提案システムは 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. DRDoS 攻撃対策の関連研究

DRDoS 攻撃は，インターネット上に存在するリフレクタを踏み台にする攻撃であるため，そのリフレクタの数を減らすことにより，攻撃の被害を少なくすることができる．そこで，Open Resolver Project [36] はじめとする様々な組織が，リフレクタの数を減らす活動に取り組んでいるが，リフレクタの中には，設定の不備によりリフレクタとして動作するサーバだけでなく，ホームルータ等のネットワーク機器の不具合でリフレクタとして動作する機器も多く存在するため，多くのリフレクタがまだインターネット上に存在しているのが現状である．ホームルータ等の一般家庭向けのネットワーク機器がリフレクタとして動作する問題を解決するため，一般家庭向けにサービスを提供する ISP の一部では，53/UDP や 123/UDP 等の特定ポート宛の外部からの通信を遮断する措置が検討されている [20]．これにより，DRDoS 攻撃に利用可能なリフレクタの数を減らすことができるため，DRDoS 攻撃の被害を部分的に抑えることができると考えられる．

また，DRDoS 攻撃は，送信元アドレスを詐称したパケットを利用する攻撃であるため，送信元アドレスを詐称できないネットワークでは攻撃を実行することはできない．そこで，送信元アドレスを各ネットワークで検証し，送信元を詐称した IP パケットの転送を防止する技術（Ingress Filtering，BCP38）[19] の導入が検討されている．しかし，インターネット上には，コスト面等の理由から Ingress Filtering を導入しないネットワークが一定数存在するため，インターネット全体で DRDoS 攻撃を実行できないネットワークを実現することは困難である．

文献 [7], [8] では，DRDoS 攻撃における要求パケットと応答パケットの関係から DRDoS 攻撃を検知し，攻撃パケットを遮断する手法がそれぞれ提案されている．また，文献 [9] では，通信のフローを解析してその順位相関を計算することにより，DRDoS 攻撃を検知する手法が提案されており，文献 [10] では，これを発展させて攻撃を検知および攻撃の種類を分類する手法を提案している．これらの手法は，いずれも被害者側のネットワークで実施する検知

手法・対策である．

文献 [2], [12] では，DNS サーバを踏み台にする DRDoS 攻撃（DNS リフレクション攻撃）の対策として，攻撃に使用されるドメイン名ブラックリストの作成が検討されている．この対策は DNS リフレクション攻撃に限定されるが，このブラックリストを使用することにより，応答パケットの増幅率を小さくしたり応答パケットそのものを送信しないように設定したりすることができるため，攻撃の被害を抑制することができる．また，文献 [12] は，大規模なダークネットセンサで観測される DNS 通信と DNS ハニーポット[*5]で観測される DNS リフレクション攻撃の相関を分析し，攻撃に使用されるドメイン名を用いたスキャンが攻撃前にインターネット上で観測される可能性が高いことを明らかにしている．ドメイン名のブラックリストによる対策とこの知見を合わせることにより，DNS リフレクション攻撃の事前対策を実施することができる．

本論文で提案したアラートシステムは，攻撃が発生することを前提としたうえで，その攻撃情報を正確かつ迅速にネットワーク管理者に通知することを目的としたシステムであり，DRDoS 攻撃が発生した際に，ネットワーク管理者の状況把握・対応判断を支援する．

7. まとめと今後の課題

本論文では，DRDoS ハニーポットを利用した DRDoS 攻撃アラートシステムを提案し，国内の研究開発プロジェクトの枠組みで 1 年半以上の長期にわたって提案システムを運用した結果として，提案システムは正確で速報性の高い DRDoS 攻撃アラートを提供できた事例を示した．この結果は，提案システムが DRDoS 攻撃の早期対応に有用な情報を提供できる可能性を示しており，提案システムは 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．

今後の課題としては，提案システムの運用を継続するするとともに，より正確で速報性の高いアラートを提供できるようにシステムの改良に取り組みたい．5 章の考察でも述べたように，提案システムには改良の余地が残されており，これらを解決することにより正確で速報性の高いアラートを提供することができるようになると考えられる．また，攻撃の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・公開して DRDoS 攻撃の傾向を分析するとともに，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 攻撃の対策技術の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．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．

[*5] DNS リフレクション攻撃を観測するハニーポット [11]．DRDoS ハニーポットは DNS ハニーポットを含む．

参考文献

[1] Rossow, C.: Amplification Hell: Revisiting Network Protocols for DDoS Abuse, *Symposium on Network and Distributed System Security* (*NDSS*) (2014).
[2] Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K. and Rossow, C.: AmpPot: Monitoring and Defending Amplification DDoS Attacks, *Research in Attacks, Intrusions, and Defenses* (*RAID*), pp.615–636, Springer International Publishing (2015).
[3] Kührer, M., Hupperich, T., Rossow, C. and Holz, T.: Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks, *USENIX Workshop on Offensive Technologies* (*WOOT*) (2014).
[4] Kührer, M., Hupperich, T., Rossow, C. and Holz, T.: Exit from Hell? Reducing the Impact of Amplification DDoS Attacks, *USENIX Security Symposium* (2014).
[5] Santanna, J.J., van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L.Z. and Pras, A.: Booters – An Analysis of DDoS-as-a-Service Attacks, *Integrated Network Management* (*IM*), *IFIP/IEEE Symposium* (2014).
[6] Santanna, J.J., Durban, R., Sperotto, A. and Pras, A.: Inside Booters: An Analysis on Operational Databases, *Integrated Network Management* (*IM*), *IFIP/IEEE Symposium* (2015).
[7] Tsunoda, H., Ohta, K., Yamamoto, A., Ansari, N., Waizumi, Y. and Nemoto, Y.: Detecting DRDoS attacks by a simple response packet confirmation mechanism, *Journal of Computer Communications*, Vol.31, No.14, pp.3299–3306 (2008).
[8] Priya, P.M., Akilandeswari, V. and Shalinie, S.M.: Detecting DRDoS attack by Log File based IP pairing mechanism, *WSEAS Trans. Computers*, Vol.13, pp.538–548 (2014).
[9] Wei, W., Chen, F., Xia, Y. and Jin, G.: A rank correlation based detection against distributed reflection DoS attacks, *Communications Letters*, IEEE 17.1, pp.173–175 (2013).
[10] Priya, P.M., Akilandeswari, V., Shalinie, S.M., Lavanya, V. and Priya, M.S.: The Protocol Independent Detection and Classification (PIDC) system for DRDoS attack, *International Conference on Recent Trends in Information Technology* (*ICRTIT*) (2014).
[11] 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).
[12] 牧田大佑，吉岡克成，松本 勉，中里純二，島村隼平，井上大介：DNS アンプ攻撃の事前対策へ向けた DNS ハニーポットとダークネットの相関分析，情報処理学会論文誌，Vol.56, No.3, pp.921–931 (2015).
[13] CloudFlare: The DDoS That Almost Broke the Internet, available from ⟨http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/⟩ (accessed 2015-12-01).
[14] CloudFlare: Technical Details Behind a 400Gbps NTP Amplification DDoS Attack, available from ⟨http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/⟩ (accessed 2015-12-01).
[15] Akamai: DD4BC: PLXsert warns of Bitcoin extortion attempts, available from ⟨https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html⟩ (accessed 2015-12-01).

[16] Akamai: Operation Profile: Armada Collective, available from ⟨https://blogs.akamai.com/2015/11/operation-profile-armada-collective.html⟩(accessed 2015-12-01).
[17] Default Deny: MC-SQLR Amplification: MS SQL Server Resolution Service enables reflected DDoS with 440x amplification, available from ⟨http://kurtaubuchon.blogspot.jp/2015/01/mc-sqlr-amplification-ms-sql-server.html⟩ (accessed 2015-12-01).
[18] The Akamai Blog: RIPv1 Reflection DDoS Making a Comeback, available from ⟨https://blogs.akamai.com/2015/07/ripv1-reflection-ddos-making-a-comeback.html⟩ (accessed 2015-12-01).
[19] Ferguson, P. and Senie, D.: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, available from ⟨http://tools.ietf.org/rfc/bcp/bcp38.txt⟩ (accessed 2015-12-01).
[20] JAIPA：電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン，入手先 ⟨http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf⟩（参照 2015-12-01）.
[21] Ubuntu, available from ⟨http://www.ubuntu.com/⟩.
[22] iptables, available from ⟨http://www.netfilter.org/projects/iptables/index.html⟩.
[23] tcpdump, available from ⟨http://www.tcpdump.org/⟩.
[24] quoted, available from ⟨http://www.mrp3.com/webutil/quoted.html⟩.
[25] xinetd, available from ⟨http://www.xinetd.org/⟩.
[26] BIND, available from ⟨https://www.isc.org/downloads/bind/⟩.
[27] Unbound, available from ⟨https://www.unbound.net/⟩.
[28] NTP Project, available from ⟨http://www.ntp.org/⟩.
[29] Net-SNMP, available from ⟨http://www.net-snmp.org/⟩.
[30] fluentd, available from ⟨http://www.fluentd.org/⟩.
[31] Python, available from ⟨https://www.python.org⟩.
[32] pcapy, available from ⟨https://github.com/CoreSecurity/pcapy⟩.
[33] dpkt, available from ⟨https://github.com/kbandla/dpkt⟩.
[34] MaxMind, available from ⟨https://www.maxmind.com/⟩.
[35] A Python structured logger for Fluentd, available from ⟨https://github.com/fluent/fluent-logger-python⟩.
[36] Open Resolver Project, available from ⟨http://openresolverproject.org/⟩.

牧田 大佑 （学生会員）

2014 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期修了，修士（情報学）．同年 4 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期に進学．同年 4 月より独立行政法人情報通信研究機構で研究員として勤務．ネットワーク攻撃観測等のネットワークセキュリティの研究に従事．

西添 友美

2015 年 3 月横浜国立大学理工学部数物・電子情報系学科卒業，学士（工学）．同年 4 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程前期に進学．ネットワーク攻撃観測等のネットワークセキュリティの研究に従事．

吉岡 克成 （正会員）

2005 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了，博士（工学）．同年 4 月独立行政法人情報通信研究機構研究員．2007 年 12 月より横浜国立大学学際プロジェクト研究センター特任教員（助教）．2011 年 4 月より横浜国立大学大学院環境情報研究院准教授．マルウェア解析やネットワーク攻撃観測・検知等のネットワークセキュリティの研究に従事．2009 年文部科学大臣表彰・科学技術賞（研究部門）受賞．

松本 勉

1986 年 3 月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年 4 月横浜国立大学講師．2001 年 4 月より同大学院環境情報研究院教授．2014 年 12 月より同大学先端科学高等研究院主任研究者を兼務．ネットワーク・ソフトウェア・ハードウェアセキュリティ，暗号，耐タンパー技術，生体認証，人工物メトリクス等の「情報・物理セキュリティ」の研究教育に 1981 年より従事．1982 年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を 4 名で創設．2005 年～2010 年国際暗号学会 IACR 理事．1994 年第 32 回電子情報通信学会業績賞，2006 年第 5 回ドコモ・モバイル・サイエンス賞，2008 年第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞（研究部門）受賞．

井上 大介

2003 年横浜国立大学大学院工学研究科博士課程後期修了．2003 年通信総合研究所（現，情報通信研究機構）に入所．2006 年よりインシデント分析センター NICTER の研究開発に従事．現在，情報通信研究機構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室長．2002 年暗号と情報セキュリティシンポジウム論文賞，2009 年科学技術分野の文部科学大臣表彰（科学技術賞），2013 年グッドデザイン賞，2014 年 Asia-Pacific Information Security Leadership Achievements 等を受賞．博士（工学）．

中尾 康二 （正会員）

1979 年早稲田大学卒業後，国際電信電話（株）に入社．KDD 研究所を経て，現在 KDDI（株）顧問，および国立研究開発法人情報通信研究機構（NICT）サイバーセキュリティ研究所主管研究員兼務．ネットワークおよびシステムを中心とした情報セキュリティ技術の研究開発に従事．電子情報通信学会等の会員．経済産業省大臣表彰賞，KPMG 情報セキュリティアウォーズ，文部科学省大臣表彰賞，情報セキュリティ文化賞，総務大臣表彰等を受賞．