情報処理学会論文誌 Vol.56 No.3 921–931 (Mar. 2015)

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

牧田 大佑[1,2,a)] 吉岡 克成[1] 松本 勉[1] 中里 純二[2] 島村 隼平[3] 井上 大介[2]

受付日 2014年6月30日, 採録日 2014年11月10日

概要：近年，DNS アンプ攻撃による被害が深刻化しており，早急な対策が求められている．我々は，DNS アンプ攻撃を観測する手法として DNS ハニーポットを提案し，DNS アンプ攻撃の観測・分析を行っている．DNS アンプ攻撃では通信を増幅するためにインターネット上のオープンリゾルバが用いられるため，攻撃者は広範囲なスキャンによりオープンリゾルバを探索することが予想される．しかし，DNS ハニーポットは，DNS サーバとして動作するための運用コストが高く，大規模な観測に不向きであるため，攻撃者によるスキャン活動の全体的な傾向を把握することが困難である．本論文では，DNS ハニーポットが観測した DNS アンプ攻撃と，広範囲のアドレス空間を監視するダークネットセンサが観測したスキャン活動を突合し，その相関を分析する．分析の結果，分析対象期間内に DNS ハニーポットで観測された 33 個の攻撃用ドメイン名のうち 87%にあたる 29 個のドメイン名は，攻撃と同一のドメイン名を用いたスキャン活動がダークネットセンサでも観測され，そのうち 22 個のドメイン名は，DNS アンプ攻撃が観測される 1 日以上前に，同様のスキャン活動がダークネットセンサでも観測された．本分析結果は，スキャン情報を用いた DNS アンプ攻撃の早期対策技術への応用に期待できる．

キーワード：サイバーセキュリティ，DNS アンプ攻撃，DNS ハニーポット，ダークネット観測，DDoS 攻撃対策

Correlation Analysis between DNS Honeypot and Darknet toward Proactive Countermeasures against DNS Amplification Attacks

Daisuke Makita[1,2,a)] Katsunari Yoshioka[1] Tsutomu Matsumoto[1]
Junji Nakazato[2] Jumpei Shimamura[3] Daisuke Inoue[2]

Received: June 30, 2014, Accepted: November 10, 2014

Abstract: In recent years, problems posed by DNS amplification attacks have become serious and there is a compelling need for effective countermeasures. We have proposed DNS honeypot, a method for observing DNS amplification attacks, and have been conducting the observation and analysis of DNS amplification attacks. In order to conduct DNS amplification attacks, attackers need to know where open resolvers are and therefore it is expected that they conduct network scans for finding open resolvers before conducting amplification attacks. However, since a DNS honeypot requires operational costs to work as a DNS server and it is unfit for large-scale monitoring, it is difficult to grasp the trends of scans for open resolvers by DNS honeypots. In this paper, we compare the DNS amplification attacks that DNS honeypot observed with the scans that darknet sensor observed, and analyze the correlation between them. As a result, out of 33 domain names used for DNS amplification attacks that DNS honeypots observed during the analysis period, 29 domain names (87%) were used for scans that darknet sensor observed, and 22 domain names out of them were observed by darknet sensor one or more days before the actual attacks occurred. From this result, it can be expected to develop proactive countermeasures against DNS amplification attacks using scan information.

Keywords: cybersecurity, DNS amplification attack, DNS honeypot, darknet monitoring, DDoS attack prevention

1. はじめに

Domain Name System（DNS）は，インターネット上でドメイン名と IP アドレス等の情報を対応付ける重要な役割を果たしている．DNS はインターネット上の不正活動にも利用されており，特に，インターネット上の任意のホストからの再帰的な名前解決を許可する DNS キャッシュサーバ（オープンリゾルバ）は，DNS アンプ攻撃と呼ばれる分散型サービス妨害攻撃（Distributed Denial-of-Service Attack; DDoS 攻撃）の要因となっている [1]．

Open Resolver Project [2] によると，DNS サーバの待ち受けポートである 53/UDP への要求に対して応答するサーバのうち，インターネット上の任意のホストからの名前解決要求に応答するサーバは，2014 年 6 月現在，インターネット上に 2,000 万台近く存在しており，これらが DNS アンプ攻撃の踏み台として悪用されている．2013 年 3 月の Spamhaus [3] を標的とした DDoS 攻撃では，DNS アンプ攻撃が実行手段として利用され，ピーク時には 120 Gbps もの通信が関係するネットワークに流れ込み，上流の Tier1 プロバイダでは一時 300 Gbps の通信が観測されたと報告されている [4]．また，DDoS 攻撃対策サービスを提供する Prolexic 社 [5] も，2013 年 5 月末に，167 Gbps に達する DNS アンプ攻撃に対処したことを公表している [6]．このように，DNS アンプ攻撃による被害が深刻化しており，早急な対策が求められている．

我々は，DNS アンプ攻撃を観測する手法として DNS ハニーポットを提案している [7]．DNS ハニーポットは，囮（おとり）の DNS サーバを中心にしたシステムであり，我々はこれをインターネット上で運用することにより，DNS アンプ攻撃の観測・分析を行っている．この観測・分析においては，DNS アンプ攻撃自体の観測に加えて，攻撃者によるオープンリゾルバの探索の状況を把握することが重要である．しかし，DNS ハニーポットは，DNS サーバとして動作するための運用コストが高く，大規模な観測に不向きであるため，オープンリゾルバの探索を目的としたスキャン活動の全体的な傾向を把握することが困難である．

本論文では，DNS ハニーポットが観測した DNS アンプ攻撃と，広範囲のアドレス空間を監視するダークネットセンサが観測した DNS サーバのスキャン活動を突合し，その相関を分析する．2 台の DNS ハニーポットと，/16 規模のネットワークを監視するダークネットセンサがそれぞれ観測した 6 カ月間の DNS 通信を突合した結果，DNS アンプ攻撃が DNS ハニーポットで観測される前には，攻撃に利用されるドメイン名と同じドメイン名を用いたスキャン活動がダークネットセンサで観測される可能性が高いことを確認した．

本研究の特筆すべき貢献は，DNS ハニーポットとダークネットセンサでそれぞれ観測される DNS 通信に着目し，DNS アンプ攻撃とスキャン活動の関係を明らかにしたことである．分析結果は，DNS アンプ攻撃が実行される前に，攻撃と同じドメイン名を用いたスキャン活動がインターネット上で観測される可能性が高い，すなわち，DNS アンプ攻撃が実行される前に，攻撃に利用されるドメイン名を特定できる可能性が高いことを示している．この知見は，DNS アンプ攻撃の早期対策技術への応用に期待できる．

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 DNS アンプ攻撃，DNS ハニーポット，ダークネットについて説明する．3 章では，本論文で分析する DNS ハニーポットとダークネットの観測環境，および，各システムが観測した DNS 通信の概要を説明する．4 章で DNS ハニーポットとダークネットが観測した DNS 通信の突合分析の結果をまとめ，5 章で本研究に関する考察を行う．最後に，6 章でまとめと今後の課題を記す．

2. 背景

2.1 DNS アンプ攻撃

DNS アンプ攻撃とは，DNS サーバを通信の増幅器（Amplifier）として利用する攻撃である [8]．DNS 通信は，要求（クエリ）とそれに対する応答（レスポンス）からなり，応答には要求とその回答が含まれる．そのため，DNS 通信では要求パケットよりも応答パケットのデータサイズが大きくなるという性質がある（増幅効果）．その性質を利用し，増幅率が高いドメイン名の DNS クエリを多量に DNS サーバに送信することにより，DNS 通信を増幅させ，攻撃対象のネットワーク帯域を圧迫する DoS 攻撃が可能になる．

また，DNS 通信は，主に User Datagram Protocol（UDP）上で行われる．UDP はコネクションの確立を行わないため，送信元 IP アドレスを詐称した通信が可能である．そのため，送信元 IP アドレスを攻撃対象の IP アドレスに詐称した DNS クエリを多量に DNS サーバに送信することにより，応答パケットを攻撃対象に集中させ，攻撃対象のネットワーク帯域を圧迫する DoS 攻撃が可能になる．このとき，送信元 IP アドレスを詐称した DNS クエリは，その応答が DNS サーバで反射（Reflection）しているように見えることから，この攻撃は DNS リフレクション攻撃と呼ばれる．DNS サーバを踏み台にする DDoS 攻撃では，DNS 通信の増幅効果と，UDP のコネクションレス型の性質の両方が利用されるため，DNS アンプ攻撃と DNS リフレク

[1] 横浜国立大学
Yokohama National University, Yokohama, Kanagawa 240–8501, Japan.
[2] 独立行政法人情報通信研究機構
National Institute of Information and Communications Technology, Koganei, Tokyo 184–8795, Japan.
[3] 株式会社クルウィット
clwit, Inc., Mitaka, Tokyo 181–0013, Japan.
[a)] makita-daisuke-jk@ynu.jp

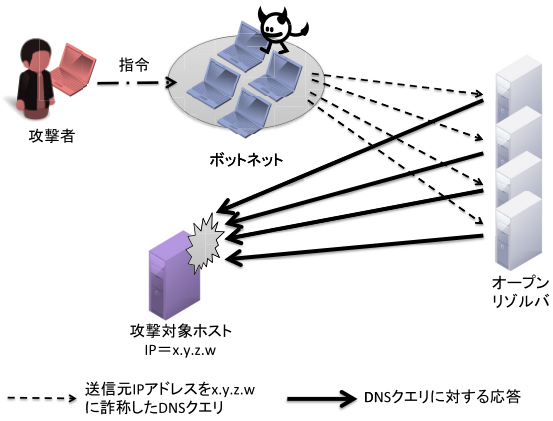

図 1 DNS アンプ攻撃
Fig. 1 Model of DNS amplification attack.

ション攻撃は同義として使用されることが多い．本論文では，以降，DNS アンプ攻撃に記述を統一する．

DNS アンプ攻撃のシナリオを図 **1** に示す．DNS アンプ攻撃では，攻撃者が操作するボットネットとインターネット上に多数存在するオープンリゾルバが利用される [9], [10]．攻撃者は，ボットネットを操り，送信元 IP アドレスを攻撃対象の IP アドレスに詐称した DNS クエリを多数のオープンリゾルバに送信する．オープンリゾルバは詐称された IP アドレスに応答を返すが，このとき，応答のデータサイズが大きくなるドメイン名を要求することにより，攻撃対象に多量の増幅した応答が集中する．その結果，攻撃対象のネットワーク帯域がオープンリゾルバからの応答で飽和し，サービス不能状態に陥る．

このように，DNS アンプ攻撃は特定のプログラムの脆弱性を狙う攻撃ではなく，攻撃対象となるネットワークの帯域等の資源に対する攻撃である．DNS アンプ攻撃では，オープンリゾルバが踏み台として利用されるため，被害者は攻撃者の特定が困難である．また，踏み台となるオープンリゾルバの中には，設定の誤りによりオープンリゾルバとして動作している DNS キャッシュサーバだけでなく，オープンリゾルバとして機能する問題を有するネットワーク機器も存在する [11] ため，インターネット上のすべてのオープンリゾルバに対処することも難しい．

増幅効果とコネクションレス型の性質をあわせ持つサービスであれば，DNS 以外のサービスでも同様の攻撃を実行することが可能である．論文 [12] では，UDP 上で通信を行う 14 種類のサービスについて，通信の増幅率等を調査し，攻撃に利用可能なサービスを検証している．また，Prolexic 社によると，CHARGEN（19/UDP）や NTP（123/UDP），SNMP（161/UDP）等のサービスが攻撃に悪用されはじめていると報告されている [13]．本論文では，UDP 上でサービスを提供する DNS 通信のみを研究の対象とし，他のサービスを悪用する攻撃については今後の課題とする．

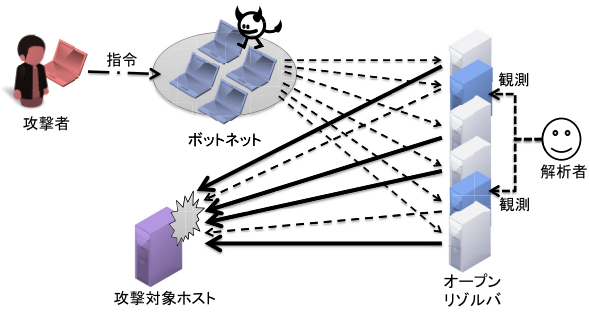

図 2 DNS ハニーポットのアイディア
Fig. 2 Idea of DNS honeypot.

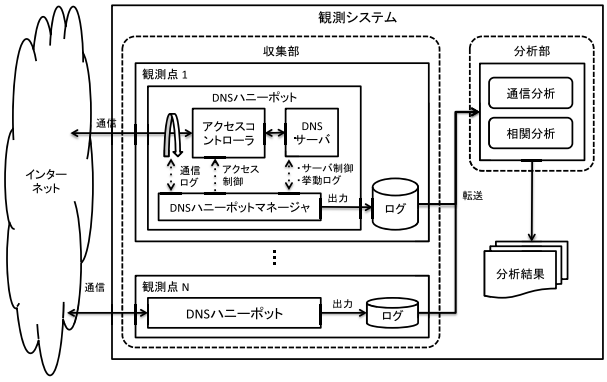

図 3 DNS ハニーポットと観測システムの構成
Fig. 3 Architecture of DNS honeypot and observation system.

2.2 DNS ハニーポット

ハニーポットとは，不正使用されることに価値を持つ情報システム資源であり [14]，不正アクセスの手法やその傾向の観測・分析を主な目的する．我々が提案している DNS ハニーポットは，DNS アンプ攻撃等の DNS サーバを悪用する不正活動の観測・分析を主な目的としている．提案システムは，囮（おとり）の DNS サーバを中心とするシステムであり，これをインターネット上で運用することにより，DNS サーバを悪用する不正活動の観測・分析を行う．DNS アンプ攻撃の観測を想定した場合，図 **2** のように，攻撃者が DNS ハニーポットを攻撃の踏み台として利用することにより，攻撃の観測・分析が可能になる．

2.2.1 システムの構成

DNS ハニーポットと観測システムの構成を図 **3** に示す．DNS ハニーポットは，「DNS サーバ」「アクセスコントローラ」「DNS ハニーポットマネージャ」の 3 つの要素からなる．DNS サーバは，DNS クエリに対して応答する役割を担い，インターネット上の任意のホストから名前解決ができるように設定する．次に，アクセスコントローラは，DNS サーバとインターネットの間で動作し，DNS サーバが悪用された場合に外部ネットワークに与える影響を少なくするように，通信を制御する役割を担う．DNS ハニーポットマネージャは，DNS サーバやアクセスコントローラの制御，および，ログの出力を担当する．

ハニーポットを用いて不正活動の分析を行う場合，単体ではなく複数のハニーポットの通信を分析することにより，各観測点の観測結果の比較や相関等，詳細な分析が可能になる．そこで，DNS ハニーポットを運用する観測システムにおいても，図 3 のように，システムを「収集部」と「分析部」の 2 つに分離して観測を行う．

「収集部」は，インターネットに接続された複数の観測点から構成される．各観測点で，DNS ハニーポットを動作させ，そこで DNS 通信のログを収集する．そして，各観測で収集したログを「分析部」に転送し，そこで各観測点の DNS 通信の分析，および，複数の観測点の DNS 通信の相関分析を行い，分析結果を出力する．

2.2.2 実装

本研究における DNS ハニーポットの実装を**図 4** に示す．Ubuntu [15] をインストールしたマシンを各観測点に 1 台ずつ用意し，それぞれのマシン上に DNS ハニーポットを実装した．DNS ハニーポットは，DNS サーバとして BIND [16]，アクセスコントローラとして iptables [17]，DNS ハニーポットマネージャとして Linux 標準のコマンド，および，制御用のシェルスクリプトを用いて実装した．DNS サーバは，インターネット上の任意のホストからの再帰的な名前解決を許可，すなわち，オープンリゾルバとして動作するように設定し，DNS ハニーポットマネージャは解析者が操作できるようにした．また，通信ログは tcpdump [18] を用いて取得し，BIND のクエリログ，および，tcpdump が出力する pcap ファイルを DNS ハニーポットの出力とした．

2.3 ダークネットセンサ

ダークネットとは，インターネット上の未使用の IP アドレス空間のことである [19], [20]．未使用のアドレス空間であるため，通常のインターネット利用で発生する通信がダークネットに流れ込む可能性は低い．しかし，実際には相当数のパケットがダークネットに到達している．これらの通信は，ホストの探索を目的としたスキャンや送信元 IP アドレスが詐称された DoS 攻撃の跳ね返り（バックスキャッタ）等，不正活動に起因するものが多い．そのため，ダークネット観測はインターネット上で発生している不正活動の傾向の把握に利用されている[*1]．

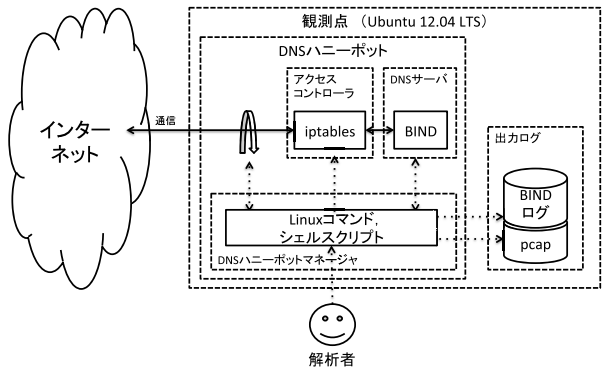

図 4 DNS ハニーポットの実装
Fig. 4 Implementation of DNS honeypot.

ダークネットを用いた DNS 通信の分析に関する研究としては，論文 [21], [22] があげられる．論文 [21] では，ダークネットで観測される DNS クエリに着目し，ダークネットで観測される不正活動と DNS クエリの関係を分析している．論文 [22] では，ダークネットに到達する DNS クエリ（DNS サーバを探索するスキャン）と送信元 IP アドレスをダークネットのアドレスに詐称した DNS クエリに対する応答（DNS サーバからのバックスキャッタ）に着目し，それぞれの傾向や特徴を分析している．本論文では，DNS ハニーポットと，広範囲のアドレス空間を監視するダークネットセンサでそれぞれ観測される DNS 通信の関係に着目し，DNS アンプ攻撃とスキャン活動の相関を分析する．

3. DNS 通信の観測

本章では，DNS ハニーポットとダークネットセンサの観測環境の概要と，各システムが分析対象期間中に観測した DNS 通信の概要を述べる．

表 1 DNS ハニーポットの観測環境
Table 1 Overview of DNS honeypots.

	DNS ハニーポット 1 (DNS-HONEY1)	DNS ハニーポット 2 (DNS-HONEY2)
ネットワーク	ISP-A	ISP-B
動作	オープンリゾルバ	
IP アドレス数	それぞれ 1 つの IP アドレス	
観測開始日	2012 年 10 月 7 日	2013 年 5 月 20 日
分析対象期間	2013 年 6 月 1 日〜2013 年 11 月 30 日	
分析対象日数	182 日間	
通信制御（全観測期間）	・制御なし（手動）：2012 年 10 月 7 日〜2013 年 8 月 3 日，2013 年 8 月 25 日〜9 月 7 日 ・同一 IP アドレスに対する応答を 1pps に制限：2013 年 8 月 3 日〜8 月 25 日．2013 年 9 月 7 日〜現在	・制御なし（手動）：2013 年 5 月 20 日〜5 月 27 日 ・同一 IP アドレスに対する応答を 1pps に制限：2013 年 5 月 27 日〜現在
IP アドレスの変更（分析対象期間）	3 回（2013 年 7 月 25 日，8 月 25 日，9 月 9 日）	12 回（2013 年 8 月 22 日×2 回，10 月 10 日，10 月 20 日，10 月 28 日，11 月 4 日，11 月 5 日×2 回，11 月 10 日，11 月 21 日，11 月 22 日，11 月 27 日）

[*1] ダークネットに設置するセンサは，受信パケットに対する応答の程度により，ブラックホールセンサ，低インタラクションセンサ，高インタラクションセンサの 3 つに分類される．本論文では，受信パケットに対して応答をいっさい行わないブラックホールセンサをダークネットセンサと呼称している．

3.1 観測環境

本論文では，我々が運用している 2 台の DNS ハニーポットが観測した DNS クエリと，NICTER [23] の NONSTOP [24] で提供される /16 規模のダークネットセンサが観測した DNS クエリを分析の対象とした．分析対象の期間は，2013 年 6 月から 2013 年 11 月までの半年間である．各システムの観測環境の概要を**表 1**，**表 2** に示す．

我々が運用している 2 台の DNS ハニーポット（DNS-HONEY1，DNS-HONEY2）は，それぞれ別の ISP ネットワークに属しており，オープンリゾルバとして動作している．観測開始当初は，観測を優先するため通信制限を行わず，手動で制御する程度にとどめたが，DNS-HONEY1 では 2013 年 8 月 3 日以降，DNS-HONEY2 では 2013 年 5 月 27 日以降，外部ネットワークへの影響を考慮し，同一 IP アドレスへの応答の上限を 1 pps（Packet Per Second）に制限した．また，分析対象とした半年間に，DNS-HONEY1 では 3 回，DNS-HONEY2 では 12 回，各観測点の IP アドレスが変更されている．

また，本論文で分析した NICTER が保有するダークネットセンサは，/16 ネットワークのアドレス空間（= 65,536 個の IP アドレス）の通信を観測しており，パケットの送信元に応答を返さないブラックホールセンサとして動作している．なお，分析対象期間の 182 日間のうち 9 日間はダークネットセンサが停止していたため分析の対象から除外している．

表 2 ダークネットセンサの観測環境
Table 2 Overview of darknet sensor.

	NICTER ダークネットセンサ (DARKNET)
動作	ブラックホールセンサ
IP アドレス数	65536（/16 規模のネットワーク）
分析対象期間	2013 年 6 月 1 日〜2013 年 11 月 30 日
分析対象日数	173 日間 （182 日間のうち，9 日間はシステム停止）

3.2 観測結果

DNS ハニーポットとダークネットが分析対象期間中に観測した DNS クエリの概要を**表 3** に，DNS クエリ数の日ごとの推移を**図 5** に示す．

2 台の DNS ハニーポットは，182 日間の分析対象期間中に，累計で 6,400 万以上，1 日平均十数万の DNS クエリを観測した．一方，ダークネットセンサは，173 日間の分析対象期間中に，累計で 8,900 万以上の DNS クエリを観測したが，1 つの IP アドレス平均では，173 日間で約 1,400 クエリ，1 日平均では約 8 クエリであった．また，受信した DNS クエリの送信元 IP アドレス数は，2 台の DNS ハニーポットはそれぞれ数万に達したのに対し，65,536 個の IP アドレスを監視するダークネットセンサは 6,867 個であった．このように，ダークネットセンサが観測した DNS クエリ数や送信元 IP アドレスの数は，DNS ハニーポットが観測した数と比較すると少数であった．これは，ダーク

表 3 DNS ハニーポットとダークネットで観測された DNS クエリの概要
Table 3 Overview of DNS queries that DNS honeypots and darknet sensor observed.

	DNS-HONEY1	DNS-HONEY2	ダークネット（65536 アドレス）	ダークネット（1 アドレス平均）
DNS クエリ数（累計）	34,838,637	29,510,478	89,408,057	約 1,364
DNS クエリ数（1 日平均）	約 191,421	約 162,145	約 516,809	約 8
送信元 IP アドレス数	29,129	12,948	6,867	—
ドメイン名の数	1,369	431	488,678	—

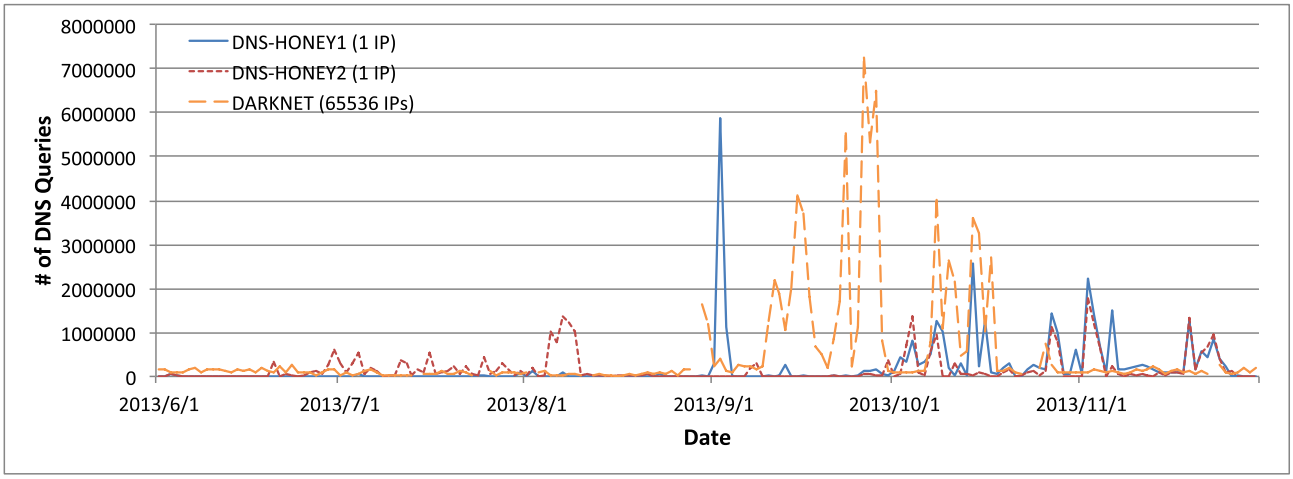

図 5 DNS クエリ数の推移（日ごと）
Fig. 5 Changes in the number of DNS queries (Daily).

ネットセンサが観測したDNSクエリは，DNSサーバの探索を目的としたスキャンがほとんどであったのに対し，DNSハニーポットが観測したDNSクエリは，スキャンに加え，DNSアンプ攻撃で発生する多量のDNSクエリが含まれていたためである．

一方，各システムが観測したドメイン名の数を比較すると，65,536個のIPアドレスを監視するダークネットセンサは，DNSハニーポットより多くのドメイン名を観測していた．これは，観測しているIPアドレスによって異なるドメイン名（たとえば，逆引きに利用されるドメイン名や，オープンリゾルバの探索を目的としたプロジェクトがスキャン目的で利用するドメイン名）がダークネットのアドレス空間全体で観測された結果，観測しているIPアドレスの数だけドメイン名の数が存在したためである．

表 4 一般的なドメイン名の応答サイズと増幅率（2013年11月25日現在）
Table 4 Response sizes and amplification factors of general domain names (as of November 25th, 2013).

ドメイン名	型	増幅率※1（%）
google.com	ANY	847%
facebook.com	ANY	361%
youtube.com	ANY	796%
yahoo.com	ANY	610%
baidu.com	ANY	648%
wikipedia.org	ANY	486%
qq.com	ANY	165%
live.com	ANY	818%
linkedin.com	ANY	1167%
twitter.com	ANY	1002%

※1 増幅率はEthernetヘッダ14オクテット，IPヘッダ20オクテット，UDPヘッダ8オクテットとして，増幅率＝（応答のパケットサイズ）／（要求のパケットサイズ）×100 [%]の式で計算した．

3.3 DNSアンプ攻撃に利用されるドメイン名

DNSハニーポットで観測されたドメイン名のうち，その回数が多い上位10個のドメイン名とその増幅率を**表 5**に，一般的なドメイン名のDNS通信の増幅率を**表 4**に示す．なお，ここではAlexa [27] で公開されている人気サイトランキング上位10個のドメイン名を一般的なドメイン名として利用した．

表より，DNSハニーポットで多く観測されたドメイン名の増幅率は，一般的なドメイン名の増幅率と比較して大きく，DNSアンプ攻撃に悪用されやすいドメイン名であることが分かる．また，DNSハニーポットが観測したDNSアンプ攻撃では，isc.org [25] やripe.net [26] のように正規の目的で使われているドメイン名（表5では「正規」と表記）が悪用される事例も観測されたが，その一方で，100個以上のIPアドレスや大きなサイズのTXTレコードが登録されており，著者らがWeb検索エンジンを用いて検索しても，そのドメインを所有する組織を特定することができないドメイン名が使用される事例も観測された．後者のドメイン

表 5 DNSアンプ攻撃に利用されていたドメイン名の情報（DNSクエリ数の多い上位10個）
Table 5 Information of domain names used for DNS amplification attacks (TOP 10 in descending order of the number of DNS queries).

ドメイン名	型	DNSクエリ数※1	増幅率※2	応答（DNSアンプ攻撃観測時）	応答コード（2014年1月22日現在）	正規／独自
isc.org	ANY	14,414,573	4541%	様々な種類の応答	NOERROR	正規
pkts.asia	ANY	12,262,517	5070%	245個の応答	NXDOMAIN	独自
anonsc.com	ANY	7,323,906	—※3	201個の応答	NXDOMAIN	独自
aa3247.com	A	3,790,906	5379%	256個の応答	NXDOMAIN	独自
babywow.co.uk	ANY	3,772,660	5488%	246個の応答	NOERROR（応答小）※4	独自
eschenemnogo.com	ANY	3,217,076	4739%	246個の応答	—※5	独自
ym.rctrhash.com	ANY	2,396,101	—※3	大きなサイズのTXT応答	NXDOMAIN	独自
a.packetdevil.com	ANY	2,396,055	4723%	252個の応答	SERVFAIL	独自
irlwinning.com	ANY	2,279,340	4778%	245個の応答	NOERROR（応答小）※4	独自
fkfkfkfa.com	ANY	2,201,520	4900%	245個の応答	NXDOMAIN	独自

※1 DNS−HONEY1とDNS-HONEY2で分析対象期間中に観測したDNSクエリ数の和を記載した．
※2 観測期間の中で最大の増幅率を記載した．なお，増幅率は表4の※1と同様の手順で計算した．
※3 観測結果から正確な応答のサイズを算出できなかったため不定とした．
※4 攻撃者は既にこのドメインを所有しておらず，ドメインの管理業者によりパーキングされているものと推測される．
※5 権威DNSサーバからの応答パケットを受信できなかったため不定とした．

表 6 aa3247.com，pkts.asia，bitstress.comの初観測日とDNSアンプ攻撃の観測日
Table 6 First observation date in darknet and observation date of DNS amplification attack (aa3247.com, pkts.asia, bitstress.com).

ドメイン名	型	ダークネットでの初観測日	DNSアンプ攻撃の初観測日※1	DNSクエリ数のピーク※1
aa3247.com	A	2013年9月23日	2013年10月2日（9日後）	2013年10月4日（11日後）
pkts.asia	ANY	2013年10月2日	2013年10月3日（1日後）	2013年11月2日（31日後）
bitstress.com	ANY	2013年9月19日	2013年9月23日（4日後）	2013年9月28日（9日後）

※1 括弧内はダークネットで初めて観測された日からの日数を表す．

名は，攻撃者が DNS アンプ攻撃のために独自に用意したもの（表 5 では「独自」と表記）であると考えられ，本論文では，これらのドメイン名に着目して，以降の分析を行う．

4. DNS 通信の突合分析

本章では，DNS ハニーポットが観測した DNS アンプ攻撃と，ダークネットセンサが観測した DNS サーバのスキャン活動を突合し，その相関を分析する．本分析の目的は，DNS アンプ攻撃とスキャン活動の相関を分析することであり，本論文では，DNS クエリに含まれるドメイン名に着目して分析を行った．

なお，本論文では，DNS ハニーポットが観測した DNS 通信のうち，同一の送信元 IP アドレスからの連続した 100 以上の DNS クエリを DNS アンプ攻撃，ダークネットセンサが観測した DNS クエリをスキャンと判断した．

4.1 スキャンと DNS アンプ攻撃の相関

本節では，DNS ハニーポットが観測したドメイン名のうち，DNS アンプ攻撃に使用されていた 3 つのドメイン名（aa3247.com，pkts.asia，bitstress.com）に着目し，スキャンと DNS アンプ攻撃の相関を分析する．

4.1.1 aa3247.com

aa3247.com の DNS クエリは，分析対象期間中に 2 台の DNS ハニーポットで約 380 万回観測された．その応答には，256 個の IP アドレスが登録されており，通信の増幅率は約 54 倍であった．

DNS ハニーポットとダークネットセンサが観測した aa3247.com の DNS クエリ数の時間推移を**図 6** に示す．aa3247.com を用いたスキャンは，2013 年 9 月 23 日に，ダークネットセンサと DNS ハニーポットの両方で初めて観測された．その後，ダークネットセンサでは，aa3247.com を用いた大規模なスキャンが 1 週間近く継続して観測された．一方，DNS ハニーポットでは，スキャンの初観測日から 9 日後の 10 月 2 日に，aa3247.com を用いた DNS アンプ攻撃が初めて観測され，11 日後の 10 月 4 日に，aa3247.com. の DNS クエリ数はピークに達した．

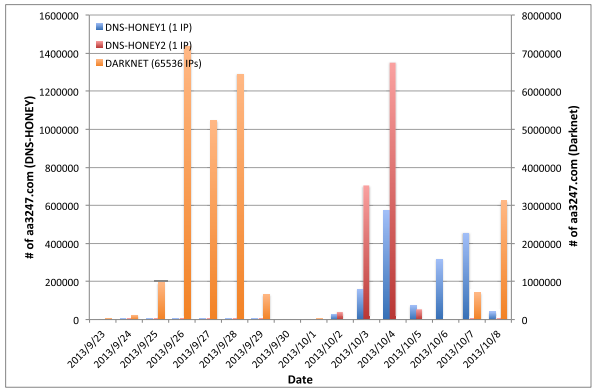

図 6 aa3247.com の DNS クエリ数の推移
Fig. 6 Changes in the number of DNS queries of aa3246.com.

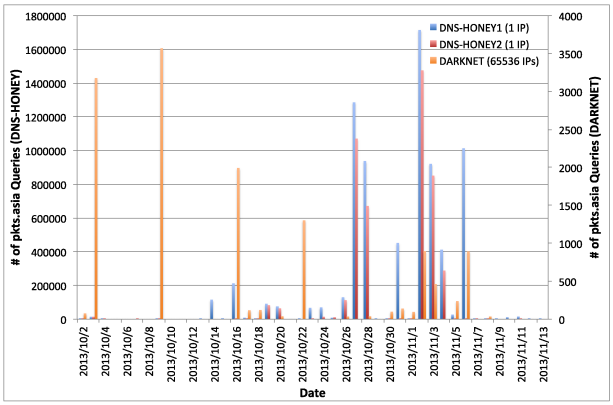

図 7 pkts.asia の DNS クエリ数の推移
Fig. 7 Changes in the number of DNS queries of pkts.asia.

4.1.2 pkts.asia

pkts.asia の DNS クエリは，2 台の DNS ハニーポットで分析対象期間中に約 1,200 万回観測された．その応答には，IP アドレスを中心に 245 個のレコードが登録されており，通信の増幅率は約 50 倍であった．

DNS ハニーポットとダークネットセンサが観測した pkts.asia の DNS クエリ数の時間推移を**図 7** に示す．pkts.asia を用いたスキャンは，2013 年 10 月 2 日に，ダークネットセンサと DNS ハニーポットの両方で初めて観測され，その翌日の 10 月 3 日に，pkts.asia を用いた DNS アンプ攻撃が DNS ハニーポットで初めて観測された．その後，ダークネットセンサでは pkts.asia の大規模なスキャンが 5〜6 日おきに観測された．DNS ハニーポットでは，10 月 14 日以降に pkts.asia を用いた攻撃が増加し，スキャンの初観測日から 31 日後の 11 月 2 日に pkts.asia の DNS クエリ数はピークに達した．

4.1.3 bitstress.com

bitstress.com の DNS クエリは，2 台の DNS ハニーポットで分析対象期間中に約 17 万回観測された．その応答には，IP アドレスを中心に 242 個のレコードが登録されており，通信の増幅率は約 48 倍であった．

DNS ハニーポットとダークネットセンサが観測した bitstress.com の DNS クエリ数の時間推移を**図 8** に示す．bitstress.com を用いたスキャンは，2013 年 9 月 19 日に，ダークネットセンサと DNS ハニーポットの両方で初めて観測され，ダークネットセンサでは，その後も継続したスキャンが観測された．DNS ハニーポットでは，スキャンの初観測日から 4 日後の 9 月 23 日に bitstress.com を用いた DNS アンプ攻撃が初めて観測され，9 日後の 9 月 28 日に bitstress.com の DNS クエリ数はピークに達した．

4.2 スキャンから DNS アンプ攻撃までの日数

本節では，分析対象期間中に DNS ハニーポットが 1,000 回以上の DNS クエリを観測したドメイン名を攻撃に利用

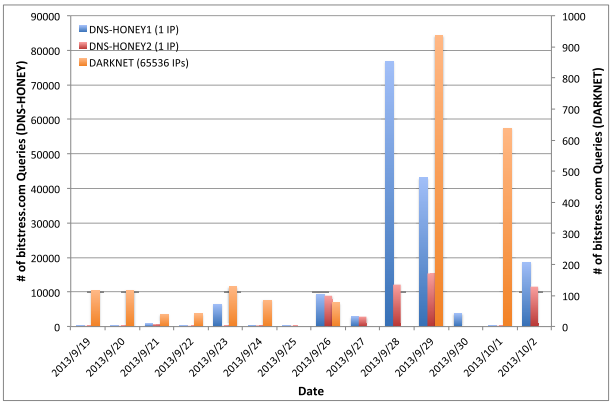

図 8 bitstress.com の DNS クエリ数の推移
Fig. 8 Changes in the number of DNS queries of bitstress.com.

表 7 スキャンから攻撃までの日数の分布
Table 7 Distribution of days from scan to attack.

日数※1	ドメイン名の数
0 日（攻撃と同日にダークネットで観測）	4（12.1%）
1 日	5（15.2%）
2 日〜7 日	7（21.2%）
8 日〜30 日	6（18.2%）
31 日以上	4（12.1%）
攻撃観測後にダークネットで観測	3（9.1%）
ダークネットで観測されず	4（12.1%）

されたドメイン名とし，そのうち，攻撃者が DNS アンプ攻撃のために独自に用意したと想定される 33 個のドメイン名について，4.1 節と同様で，次の 2 つの日数を分析する．なお，3.3 節と同様の手順で，攻撃者が独自に用意したドメイン名か否かを判断し，日数の計算は観測した日付に基づいて計算している．

(1) スキャンから攻撃までの日数

ダークネットセンサでスキャンが初めて観測された日から，DNS ハニーポットで同じドメイン名を用いた DNS アンプ攻撃が観測された日までの日数．

(2) スキャンから攻撃のピークまでの日数

ダークネットセンサでスキャンが初めて観測された日から，DNS ハニーポットで同じドメイン名の DNS クエリが最も多く観測された日までの日数．

33 個のドメイン名に関する 2 つの日数の分布を**表 7**，**表 8** に示す．分析の結果，DNS ハニーポットで DNS アンプ攻撃が観測されるよりも 1 日以上前に，66.7%（33 個のうち 22 個）のドメイン名がダークネットセンサで観測されていた．また，DNS ハニーポットで観測された攻撃がピークに達する 1 日以上前に，81.8%（33 個のうち 27 個）のドメイン名がダークネットセンサで観測されていた．これらの結果から，DNS アンプ攻撃が DNS ハニーポットで観測される前には，攻撃と同じドメイン名を用いたスキャン活動がダークネットセンサでも観測される可能性が高いことが分かる．

表 8 スキャンから攻撃のピークまでの日数の分布
Table 8 Distribution of days from scan to peak of attacks.

日数※1	ドメイン名の数
0 日（攻撃と同日にダークネットで観測）	1（3.0%）
1 日	4（12.1%）
2 日〜7 日	9（27.3%）
8 日〜30 日	7（21.2%）
31 日以上	7（21.2%）
ピーク後にダークネットで観測	1（3.0%）
ダークネットで観測されず	4（12.1%）

※1 本論文では，各観測日の日付の差分のみで日数を計算している．

5. 考察と対策

本章では，4 章の分析結果に関する考察と，分析結果から得られた知見を用いた DNS アンプ攻撃の早期対策技術に関する考察を記述する．

5.1 攻撃者が独自に用意したドメイン名

攻撃者が DNS アンプ攻撃のために独自に用意したと我々が判断したドメイン名は，攻撃観測時には大きな応答を有していたものの，2014 年 1 月 22 日現在では，応答が存在しない（NXDOMAIN）か，応答のサイズが小さく変更されており，DNS アンプ攻撃には適さない応答サイズになっていた（表 5）．これは，攻撃者が DNS アンプ攻撃に使うドメイン名を短期間で使用しなくなる傾向にあるためであり，この傾向は他の不正活動に使用されるドメイン名（たとえば，ボットネットの C&C サーバで用いられるドメイン名）の特徴と合致する [29]．なお，応答サイズが小さく変更された理由は，攻撃者がそのドメインの所有権を放棄し，ドメインがレジストラ等の管理業者によってパーキングされていたためであると推測される．

5.2 攻撃者が攻撃と同じドメイン名を用いたスキャンを行う目的

4 章の分析結果より，DNS ハニーポットが観測したドメイン名のうち，DNS アンプ攻撃で利用されていたドメイン名の約 9 割（33 個中 29 個）が，ダークネットセンサでも観測されていたことが分かる．本節では，攻撃者が攻撃と同じドメイン名を用いたスキャンを実行する理由を考察する．

攻撃者が DNS アンプ攻撃を実行するためには，踏み台にするオープンリゾルバの IP アドレスをあらかじめ把握している必要がある．しかし，オープンリゾルバの中には，オープンリゾルバとしてのサービスの提供を停止するものや，オープンリゾルバとしてのサービスを新たに開始するもの，ISP から動的に IP アドレスが割り当てられる環境下で動作しているため機器の IP アドレスが不定期で変わるものが存在する．そのため，攻撃者は定期的にスキャンを行い，攻撃の踏み台にするオープンリゾルバのリストを

更新する必要がある．

また，攻撃者は，DNS アンプ攻撃のために用意したドメイン名が踏み台にするオープンリゾルバで実際に名前解決可能か否かを事前に確認する必要がある．これは，DNS キャッシュサーバの中には，応答のサイズや一部の DNS クエリが制限されているものが存在するためである．たとえば，EDNS0（Extension Mechanisms for DNS）[30] と呼ばれる DNS の拡張規格に対応していない DNS キャッシュサーバは，UDP 上では 512 オクテットまでの応答しか返すことができないため，通信を増幅させる DNS アンプ攻撃の踏み台として不向きである．また，Google 社が提供する Public DNS サービス [28] のように，isc.org（ANY）等の一部のクエリの応答を制限する DNS キャッシュサーバも存在しており，これらのオープンリゾルバも DNS アンプ攻撃の踏み台として利用することは困難である．

以上のような理由から，攻撃者は，攻撃の踏み台とするオープンリゾルバの IP アドレスを収集するとともに，そのオープンリゾルバが踏み台として利用可能か否かを検査するために，攻撃と同じドメイン名を用いてスキャンを行っているものと考えられる．

5.3 スキャンが観測されなかったドメイン名

DNS ハニーポットが観測したドメイン名のうち，DNS アンプ攻撃で利用されていたドメイン名の約 9 割は，ダークネットセンサでも観測されていた．しかし，残りの 4 個のドメイン名は，DNS ハニーポットでは攻撃が観測されたものの，ダークネットセンサではスキャンが観測されなかった．その理由としては，次の 2 つが考えられる．

まず，攻撃者が別のドメイン名を用いてスキャンを行った場合である．この場合，ダークネットセンサでは DNS アンプ攻撃に利用されるドメイン名を観測することができず，そのドメイン名を事前に特定することができない．しかし，この場合，攻撃者は DNS アンプ攻撃のために用意したドメイン名が踏み台にするオープンリゾルバで実際に使用可能か否かをあらかじめ確認することが困難であるため，攻撃者は DNS アンプ攻撃に失敗するリスクを負うことになる．

もう 1 つは，実際には攻撃と同じドメイン名を用いたスキャンが実行されていたが，観測しているダークネットにはスキャンが到達していなかった場合である．この場合，本論文で分析したダークネットセンサがスキャンを観測していなくても，他のダークネットセンサはスキャンを観測している可能性があるため，複数箇所のダークネットセンサを分析することにより，DNS アンプ攻撃に使用されるドメイン名を事前に特定できる可能性が向上すると考えられる．

5.4 早期対策へのアプローチ

本論文の分析結果は，DNS アンプ攻撃が観測される前に，攻撃と同じドメイン名を用いたスキャン活動がインターネット上で観測される可能性が高い，すなわち，DNS アンプ攻撃に利用されるドメイン名を事前に特定できる可能性が高いことを示している．これらのドメイン名は，その応答に多数のレコードや大きなサイズの TXT レコード等を保持しているため通信の増幅率が高く，かつ，そのドメイン名を用いたスキャンがインターネット上の広範囲で観測されていた．したがって，応答の増幅率が高く，かつ，ダークネットの広範囲で観測されているといった条件を設定することにより，ダークネットで観測される DNS クエリから，DNS アンプ攻撃に利用されるドメイン名を抽出できる可能性が高い．これらの条件により，どの程度の精度で DNS アンプ攻撃に使用されるドメイン名を特定できるかの評価は今後の課題であるが，本論文で得られた知見をもとに，ISP をはじめとするネットワークを運用する組織で早期対策を実施する枠組みを構築し，このようなフィールドワークを進めながら，精度の評価・向上を図っていくことは意義があると考えられる．以降，本節では，本研究から得られた知見を応用した早期対策技術について，ドメインを管理するレジストラの立場と DNS キャッシュサーバの管理者の立場で実行可能な対策を考察する．

まず，ドメインを管理するレジストラの立場であれば，スキャン情報から DNS アンプ攻撃に利用されるドメイン名を事前に特定することにより，攻撃が実行される前に，該当するドメインの登録を抹消，あるいは，ドメインの所有者に通告することが可能である．

また，DNS キャッシュサーバの管理者であれば，該当するドメインの応答を事前に変更することにより，応答を無効化あるいは縮小させ，被害を抑えることが可能である．これは，何らかの事情でオープンリゾルバとしての機能を停止できない DNS キャッシュサーバや，その DNS キャッシュサーバ自体はオープンリゾルバとして動作していないものの，そのネットワーク内で DNS キャッシュサーバへのフォワーダ（あるいはプロキシ）として動作するネットワーク機器が存在する場合の対処方法として有効である．

6. まとめと今後の課題

本論文では，DNS ハニーポットが観測した DNS アンプ攻撃と，ダークネットセンサが観測した DNS サーバのスキャン活動を突合し，その相関を分析した．分析の結果，DNS アンプ攻撃が DNS ハニーポットで観測される前に，攻撃と同じドメイン名を用いたスキャン活動がダークネットセンサでも観測される可能性が高いことを確認した．本論文の分析結果は，インターネット上で観測される DNS サーバのスキャン活動から DNS アンプ攻撃に利用されるドメイン名を攻撃の前に特定できる可能性を示しており，

本研究で得られた知見は，スキャン情報を用いたDNSアンプ攻撃の早期対策技術への応用に期待できる．

今後の課題としては，DNSハニーポットとダークネットセンサで観測されるDNS通信の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，DNSアンプ攻撃の早期対策技術，および，その評価手法について具体的な検討を行う予定である．また，DNSハニーポットで観測される通信を分析するだけでなく，DNSアンプ攻撃を実行するマルウェアの分析や，DNSアンプ攻撃の被害者側の通信の相関を分析することにより，DNSアンプ攻撃の全体像を明らかにし，そ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/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，本研究では，NICTERが保有しているサイバーセキュリティ情報を遠隔から安全に利用するための分析基盤（NONSTOP）で提供されるダークネットデータを利用した．貴重なデータセットを提供していただいたNICTERの関係者各位に深く感謝する．

参考文献

[1] JPCERT CC：DNSの再帰的な問い合わせを使ったDDoS攻撃に関する注意喚起，入手先 ⟨http://www.jpcert.or.jp/at/2013/at130022.html⟩（参照 2014-06-22）．
[2] Open Resolver Project, available from ⟨http://openresolverproject.org/⟩ (accessed 2014-06-22).
[3] The Spamhaus Project, available from ⟨http://www.spamhaus.org/⟩ (accessed 2014-06-22).
[4] CloudFlare: The DDoS That Almost Broke the Internet, available from ⟨http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet⟩ (accessed 2014-06-22).
[5] Prolexic Technologies, available from ⟨http://www.prolexic.com/⟩ (accessed 2014-06-22).
[6] Prolexic Technologies: Prolexic Stops Largest-Ever DNS Reflection DDoS Attack, available from ⟨http://www.prolexic.com/news-events-pr-prolexic-stops-largest-ever-dns-reflection-ddos-attack-167-gbps.html⟩ (accessed 2014-06-22).
[7] 牧田大佑，吉岡克成，松本 勉：DNSハニーポットによる不正活動観測，情報処理学会研究報告，Vol.2013-CSEC-62, No.54, pp.1–8 (2013).
[8] 寺田真敏：DoS/DDoS攻撃とは，情報処理学会誌，Vol.54, No.5, pp.428–435 (2012).
[9] Internet Initiative Japan (IIJ): Internet Infrastructure Review (IIR), Vol.21, pp.28–31, available from ⟨http://www.iij.ad.jp/company/development/report/iir/021.html⟩ (accessed 2014-06-23).
[10] Japan Registry Services（JPRS）：DDoSにあなたのDNSが使われる〜DNS Ampの脅威と対策〜，入手先 ⟨http://jprs.jp/related-info/guide/003.pdf⟩（参照 2014-06-23）．
[11] Japan Vulnerability Note（JVN）：JVN#62507275 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題，入手先 ⟨http://jvn.jp/jp/JVN62507275/⟩（参照 2014-06-23）．
[12] Rossow, C.: Amplification Hell: Revisiting Network Protocols for DDoS Abuse, *Proc. 2014 Network and Distributed System Security* (*NDSS*) *Symposium* (2014).
[13] Prolexic Technologies: Second white paper in the DrDoS Attacks series: SNMP, NTP and CHARGEN attacks, available from ⟨http://www.prolexic.com/knowledge-center-white-paper-series-snmp-ntp-chargen-reflection-attacks-drdos-ddos.html⟩ (accessed 2014-06-23).
[14] Spitzner, L.: Honeypots –Definitions and Value of Honeypots, available from ⟨http://www.tracking-hackers.com/papers/honeypots.html⟩ (accessed 2014-06-22).
[15] Ubuntu, available from ⟨http://www.ubuntu.com/⟩ (accessed 2014-06-23).
[16] BIND, available from ⟨http://www.isc.org/⟩ (accessed 2014-06-23).
[17] iptables, available from ⟨http://www.netfilter.org/projects/iptables/⟩ (accessed 2013-11-24).
[18] tcpdump, available from ⟨http://www.tcpdump.org/⟩ (accessed 2013-11-24).
[19] Bailey, M., Cooke, E., Jahanian, F., Nazario, J. and Watson, D.: The Internet Motion Sensor: A Distributed Blackhole Monitoring System, *Proc. 12th Annual Network and Distributed System Security* (*NDSS*) *Symposium* (2005).
[20] 井上大介：情報セキュリティ技術動向調査（2008年下期）7 ダークネット観測の技術動向と観測事例，IPA, 入手先 ⟨http://www.ipa.go.jp/security/fy20/reports/tech1-tg/2_07.html⟩（参照 2014-06-23）．
[21] Oberheide, J., Karir, M. and Mao, Z.M.: Characterizing Dark DNS Be-havior, *DIMVA 2007*, LNCS, No.4579, pp.140–156 (2007).
[22] 中里純二，島村隼平，衛藤将史，井上大介，中尾康二：ダークネットモニタリングによるDNSトラフィック分析，情報処理学会コンピュータセキュリティシンポジウム2013（CSS2013）論文集，pp.971–977 (2013).
[23] NICTER, available from ⟨http://www.nicter.jp/⟩ (accessed 2014-06-23).
[24] 竹久達也，井上大介，衛藤将史，吉岡克成，笠間貴弘，中里純二，中尾康二：サイバーセキュリティ情報遠隔分析基盤NONSTOP，信学技報，Vol.113, No.95, ICSS2013-15, pp.85–90 (2013).
[25] Internet Systems Consortium, available from ⟨https://www.isc.org/⟩ (accessed 2014-06-23).
[26] RIPE Network Coordination Centre, available from ⟨http://www.ripe.net/⟩ (accessed 2014-06-23).
[27] Alexa, available from ⟨http://www.alexa.com/⟩ (accessed 2014-06-23).
[28] Google: Public DNS – Google Developers, available from ⟨https://developers.google.com/speed/public-dns/⟩ (accessed 2014-06-23).
[29] Bilge, L., Kirda, E., Kruegel, C. and Balduzzi, M.: EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis, *Proc. 18th Network and Distributed System Security* (*NDSS*) *Symposium* (2011).
[30] Vixie, P.: Extension Mechanisms for DNS (EDNS0) (RFC2671), IETF (online), available from ⟨http://www.ietf.org/rfc/rfc2671.txt⟩ (accessed 2014-06-26).

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．

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（IAS-YNU）情報物理セキュリティ研究ユニットリーダーを兼務．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．2005〜2010 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）各受賞．

中里 純二 （正会員）

2001 年東海大学工学部電気工学科卒業．2003 年同大学大学院博士前期課程修了．2006 年同大学院博士後期課程修了，博士（工学）．同年独立行政法人情報通信研究機構入所．現在，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

島村 隼平

2004 年 3 月芝浦工業大学電気工学科卒業．2011 年 4 月より株式会社クルウィット勤務．2005 年からダークネットをはじめとするインターネット上の不正通信の観測・分析作業に従事．

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，情報通信研究機構ネットワークセキュリティ研究所サイバーセキュリティ研究室室長，同機構サイバー攻撃対策総合研究センター（CYREC）サイバー防御戦術研究室室長（兼務）．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）．