情報処理学会論文誌 Vol.55 No.9 2021–2033 (Sep. 2014)

DNSハニーポットによるDNSアンプ攻撃の観測

牧田 大佑[1,a)] 吉岡 克成[1] 松本 勉[1]

受付日 2013年12月2日, 採録日 2014年6月17日

概要：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よっても利用されており，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キャッシュサーバは，DNSアンプ攻撃と呼ばれる分散型サービス妨害が行える要因となっている．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．しかし，DNSアンプ攻撃の実態には不明確な部分が多いため，攻撃を観測して分析し，その傾向や特徴を把握することがその対策を行うために重要である．本論文では，DNSサーバを悪用する不正活動を観測する手法としてDNSハニーポットを提案する．DNSハニーポットとは，囮（おとり）となるDNSサーバソフトウェアを中心としたシステムであり，このシステムをインターネット上で運用し，DNSサーバを悪用する不正活動を観測する．我々はDNSアンプ攻撃と推測される通信をDNSハニーポットが多数観測できていることを検証実験により確認した．また，DNSハニーポットを用いた1年間以上の長期観測の事例からDNSアンプ攻撃の傾向や特徴を分析する．この結果，DNSハニーポットを用いてDNSアンプ攻撃の動向を継続的に観測・分析することは，DNSアンプ攻撃への対策技術を検討するにあたり有効であることを示す．

キーワード：DNSアンプ攻撃，DNSハニーポット

Observing DNS Amplification Attacks with DNS Honeypot

Daisuke Makita[1,a)] Katsunari Yoshioka[1] Tsutomu Matsumoto[1]

Received: December 2, 2013, Accepted: June 17, 2014

Abstract: Domain Name System (DNS) plays an important role to map domain names to their information such as IP addresses on the Internet. DNS is also used for malicious activities. In particular, DNS cache servers which allow recursive queries from anywhere on the Internet can be the root cause of DNS amplification attack, a kind of Distributed Denial-of-Service attack. These days, problems posed by DNS amplification attacks become serious and there is a compelling need for effective countermeasures. However, since the details of these attacks are not well studied or reported, it is important to observe and understand their trends and characteristics. In this paper, we propose a concept of DNS honeypot - a method for observing malicious activities that abuse DNS servers. DNS honeypot is a system based on a dummy DNS server, and observes malicious activities that abuse DNS servers on the Internet. The result of our experiment with DNS honeypots shows that our method is effective for observing and analyzing DNS amplification attacks. As a result of long-term evaluation experiment over one year, we also analyze the trends and characteristics of DNS amplification attacks which our DNS honeypots observed.

Keywords: DNS amplification attack, DNS honeypot

1. はじめに

Domain Name System（DNS）[1] 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

[1] 横浜国立大学
Yokohama National University, Yokohama, Kanawaga 240–8501, Japan.
[a)] makita-daisuke-jk@ynu.jp

活動によっても利用されており，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（DDoS）攻撃が行える要因となっている [2].

Open Resolver Project [3] によると，DNSの待ち受けポートである53/UDPへのインターネット上の任意のホストからのDNSクエリに対して応答するサーバは，2013年11月現在，インターネット上に2,800万台近く存在しており，これらがDNSアンプ攻撃の要因となっている．2013年3月に発生したスパム対策組織Spamhaus [4] 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Tier 1プロバイダでは一時300 Gbpsの通信を観測したと報告されている [5], [6]．また，DDoS攻撃対策サービスを提供するProlexic社 [7] も，2013年5月末に167 Gbpsに達するDNSアンプ攻撃の対応にあたったことを公表している [8]．このように，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．

DNSアンプ攻撃の負荷を軽減する技術に関する研究としては論文 [9], [10] が，DNSに関係する不正活動を，未使用のアドレス空間であるダークネットの通信に着目して分析した研究としては論文 [11], [12] があげられる．しかし，DNSアンプ攻撃の実態には不明確な部分が多いため，これらの攻撃を観測して分析し，その傾向や特徴を明らかにすることがその対策を行うために重要である．

本論文では，DNSサーバを悪用する不正活動を観測する手法としてDNSハニーポットを提案する．DNSハニーポットは囮（おとり）となるDNSサーバソフトウェアを中心にしたシステムである．本システムをインターネット上で運用することにより，DNSアンプ攻撃等のDNSサーバを悪用する不正活動を観測する．

提案手法を一般ISP回線下で運用した結果，DNSハニーポットはDNSアンプ攻撃と推測される通信を多数観測しており，提案手法がDNSアンプ攻撃の観測・分析に有用であることを確認した．また，DNSハニーポットを用いた1年間以上の長期観測の事例から，提案手法が観測したDNSアンプ攻撃を分析した結果として，オープンリゾルバを悪用するDNSアンプ攻撃の傾向，攻撃対象となる国や組織，DNSアンプ攻撃に利用されるドメイン名，DNSアンプ攻撃のDNSクエリパケットに含まれる特徴等を明らかにした．

本研究の貢献としては，まずDNSアンプ攻撃等のDNSサーバを利用する不正活動を観測する手段として，DNSハニーポットの概念を提案し，本手法が一般ISP回線下での運用においても，DNSアンプ攻撃の観測・分析に有用であることを確認したことがあげられる．また，長期観測の結果として，一般ISP回線下に存在するオープンリゾルバを悪用するDNSアンプ攻撃の傾向や，観測されるDNSアンプ攻撃のDNSクエリに含まれる特徴を明らかにしたことも，DNSアンプ攻撃を分析するうえで重要な指標になると考えられる．DNSハニーポットを用いてDNSアンプ攻撃の動向を継続的に観測・分析することは，DNSアンプ攻撃の対策技術への応用が期待できる．

本論文の構成は次のとおりである．2章でDNSアンプ攻撃について説明する．3章でDNSハニーポットの概要と，本研究における実装を説明し，4章で検証実験とその結果を述べる．5章で我々のDNSハニーポットが観測したDNSアンプ攻撃と推測される通信の具体例を述べ，最後に，6章でまとめと今後の課題を述べる．

2. 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 [13]．DNSの通信は，主に要求（クエリ）とそれに対する応答（レスポンス）からなり，DNSのフォーマットに則った通信であれば，要求よりも応答のデータサイズが大きくなる性質がある．そのため，応答のデータサイズが大きいドメイン名の名前解決を多量にDNSサーバに要求することにより，その通信を増幅させ，ネットワークの帯域を圧迫する攻撃が可能になる．また，DNSの通信は主にUDPで行われるため，送信元IPアドレスの詐称することが容易である．そのため，送信元IPアドレスを攻撃対象に詐称したDNSクエリをDNSサーバに送信することにより，その応答を攻撃対象に集中させ，ネットワーク帯域を圧迫する攻撃が可能になる．送信元IPアドレスを詐称したDNSクエリは，その応答がDNSキャッシュサーバで反射（Reflection）しているようにみえることから，DNSリフレクション攻撃とも呼ばれる．DNSを用いたDDoS攻撃では，DNSの増幅する性質とUDPの送信元が偽装可能な性質の両性質が利用されるため，DNSアンプ攻撃とDNSリフレクション攻撃はほぼ同義として用いられることが多い．本論文では，以降，DNSアンプ攻撃に記述を統一する．

DNSアンプ攻撃に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ことが多い [14], [30]．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で，攻撃対象には多数の増幅された応答が集中する．その結果，攻撃対象のネットワーク帯域が飽和し，サービス不能状態に陥る（**図 1**）．

このように，DNSアンプ攻撃は特定のサービスの脆弱性を狙う攻撃ではなく，標的のネットワークに対する攻撃で

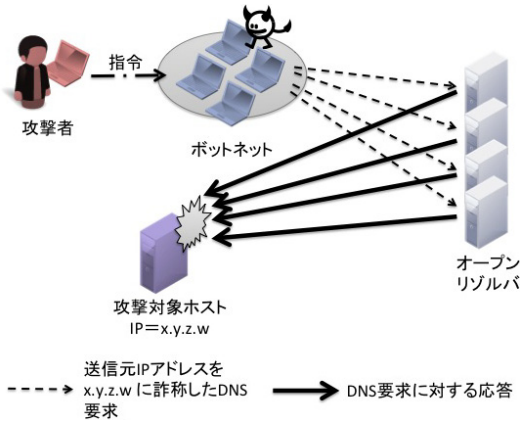

図 1 DNS アンプ攻撃
Fig. 1 Model of DNS amplification attack.

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には，設定の誤りによりオープンリゾルバと動作している DNS 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 [31] 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．

増幅効果があり，かつ，UDP を使うサービスであれば，同様の攻撃は可能であり，DNS 以外でも CHARGEN（19/UDP）や NTP（123/UDP），SNMP（161, 162/UDP）等のサービスが悪用され始めている [14], [15]．本論文では，UDP でサービスを提供する DNS 通信のみを研究の対象とし，他のサービスに関しては今後の課題とする．

3. DNS ハニーポット

本章では，DNS を利用する不正活動を観測する手法として，DNS ハニーポットを提案する．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，不正アクセスの手法やその傾向等を観測，分析することを主な目的としている [32]．本論文で提案する DNS ハニーポットは，DNS サーバソフトウェアを中心とするシステムである．たとえば，DNS アンプ攻撃の観測を想定した場合，攻撃者が本システムを踏み台として利用することにより，不正活動の観測，分析が可能となる（**図 2**）．

本章の構成は次のとおりである．まず，3.1 節で DNS ハニーポットの要件をまとめる．3.2 節で，DNS ハニーポットのシステム概要を説明し，3.3 節で本研究における実装を説明する．

3.1 システムの要件

DNS ハニーポットに求められる要件としては，「観測可能性」と「安全性」の 2 つがあげられる．

観測可能性とは，提案手法により攻撃者の不正使用を観測できる性質である．本研究では，DNS アンプ攻撃を主

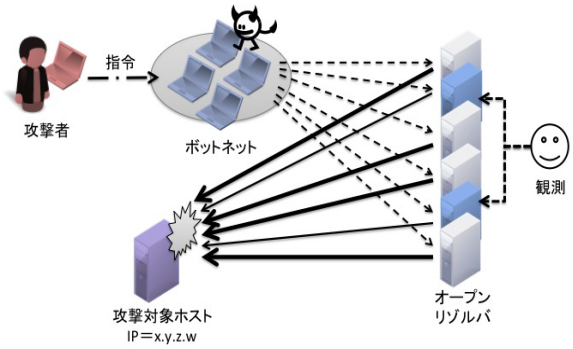

図 2 提案手法のアイディア
Fig. 2 Idea of our proposed method.

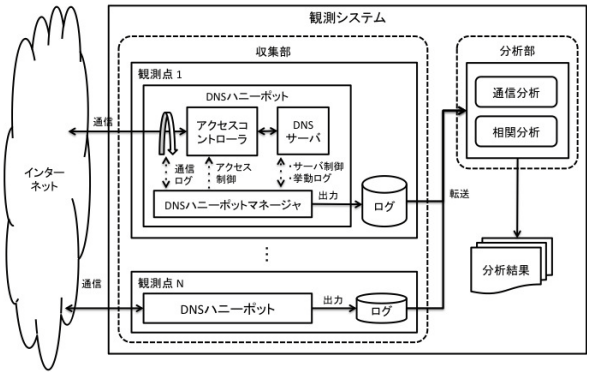

図 3 DNS ハニーポットの構成と観測システム
Fig. 3 Architecture of DNS honeypot and observation system.

な観測対象とするが，他の不正使用に関しても観測できることを目標とする．次に，安全性とは，観測地点で動作しているシステムが外部の環境になるべく影響を与えず，安全に観測，分析できる性質である．安全性を満たすためには，通信量やその内容によって外部への通信を制限する必要がある．

DNS アンプ攻撃の観測を想定する場合，踏み台とするオープンリゾルバの応答能力を事前に検査する攻撃者の存在を仮定すると，通信量を制限することにより，DNS ハニーポットで攻撃が観測できなくなる可能性がある．その場合，観測可能性と安全性はトレードオフの関係にあり，目的に応じてこれらの要件を調整していく必要がある．

3.2 DNS ハニーポットの構成

DNS ハニーポットの構成と観測システムの概要を**図 3** に示す．DNS ハニーポットは，DNS サーバを悪用する不正活動を観測，分析することを目的としており，「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 つの要素から構成される．なお，図 3 では，実線が通信・データの流れを，破線はシステム制御を表す．

まず，DNS サーバは外部からの DNS クエリに対して応答する役割を担う．ここでは，DNS サーバはインターネット上の任意の場所から不正利用が可能になるように設定する．次に，アクセスコントローラは DNS サーバとインター

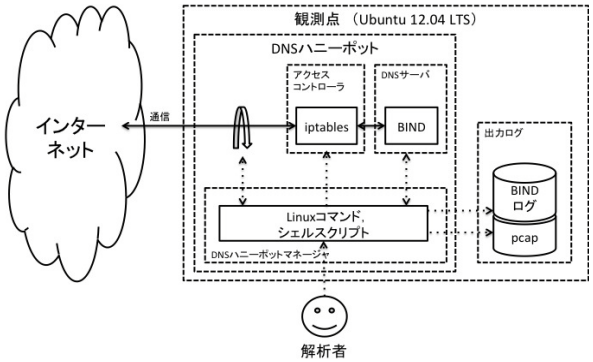

図 4 DNS ハニーポットの実装
Fig. 4 Implementation of DNS honeypot.

ネットの間に介在し，DNS サーバに悪用された場合に外部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．そして，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といった DNS ハニーポットを構成する要素の制御，および，ログの出力を担当する．

ハニーポットを用いて通信の分析を行う場合，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で，各観測点の観測結果の比較や相関等，より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「収集部」と「分析部」の 2 つにわけて複数のハニーポットを運用する．

「収集部」は，インターネットに接続し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，DNS の要求や応答のログを収集する．各観測点で収集したログは「分析部」に転送され，そこで各観測点の DNS 通信の分析，および，複数点の DNS 通信の相関分析を行い，分析結果を出力する．

3.3 実装

本論文の検証実験では，**図 4** のように DNS ハニーポットを実装した．各観測点に Linux ディストリビューションの 1 つである Ubuntu [16] がインストールされたマシンを 1 台割り当て，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 [17]，アクセスコントローラとして iptables [18]，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．通信ログのキャプチャには tcpdump [19] を用い，BIND から出力されるクエリログ，および，tcpdump によって出力した pcap ファイルを DNS ハニーポットの出力とした．

4. 検証実験

本章では，3 章で説明した DNS ハニーポットの検証実験，および，実験結果について述べる．

本章の構成は次のとおりである．まず，4.1 節で実験の目的をまとめ，4.2 節で実験方法を述べる．4.3 節で実験結果を説明し，4.4 節で，DNS ハニーポットが観測した DNS クエリに含まれる各種プロトコルのフィールド値の分析結果を述べる．そして，4.5 節で実験結果に関する考察を述べる．

4.1 実験の目的

本実験の目的は，DNS ハニーポットが DNS サーバを悪用する不正活動を観測可能か否か検証すること，および，DNS ハニーポットで観測される通信の特徴を分析することである．本実験では，DNS アンプ攻撃を主な観測対象ととらえ，その傾向と特徴の分析を行う．具体的には，DNS ハニーポットが観測した日ごとの DNS クエリ数の推移，DNS クエリの送信元 IP アドレスが属する国および AS（Autonomous System）番号，DNS アンプ攻撃で利用されるドメイン名等を分析する．なお，DNS アンプ攻撃の場合，送信元の IP アドレスは，詐称された攻撃対象の IP アドレスである．

また，DNS ハニーポットで観測した DNS クエリに含まれる各種フィールド値の統計情報を分析し，DNS アンプ攻撃に含まれる特徴を明らかにする．これは，フィールド値に見られる特徴が，DNS アンプ攻撃を行う実体（マルウェアや攻撃ツール）の特定や，攻撃の分類に有効な指標として期待できるためである．

4.2 実験方法

検証実験では，まず攻撃者が一般 ISP 回線下の DNS サーバを不正使用するか否かを 1 台の DNS ハニーポットを用いて検証した（観測点 1，DNS-HONEY1）．この実験において，DNS アンプ攻撃と推測される通信を観測したことを確認したのち，別の一般 ISP 回線下に DNS ハニーポットを 1 台追加した（観測点 2，DNS-HONEY2）．本研究では，これらの 2 台の DNS ハニーポットが観測した DNS 通信を分析する．

各観測点の概要を**表 1** に示す．2 つの観測点は別の ISP ネットワークに属しており，各 DNS ハニーポットは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可能性を優先するため通信制限は行わず，手動で制御する程度にとどめたが，観測点 1 では 2013 年 8 月 3 日以降（8 月 25 日～9 月 7 日を除く），観測点 2 では 5 月 27 日以降，外部環境への影響を考慮し（安全性の確保），iptables の hashlimit 機能を用いて同一 IP アドレスへの応答を 1 pps（Packet Per Second）に制限した．また，観測点 1 では，

表 1 各観測点の概要
Table 1 Overview of observation points.

	観測点 1（DNS-HONEY1）	観測点 2（DNS-HONEY2）
ISP	一般 ISP-A	一般 ISP-B
動作	オープンリゾルバ	
観測期間※1	2012 年 10 月 7 日〜2013 年 10 月 31 日	2013 年 5 月 20 日〜2013 年 10 月 31 日
観測日数	390 日間	165 日間
通信制御	・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	9 回（2012 年 12 月 11 日, 2013 年 3 月 13 日, 3 月 22 日×3 回, 4 月 19 日，7 月 25 日，8 月 25 日，9 月 9 日）	5 回（2013 年 8 月 22 日×2 回, 10 月 10 日, 10 月 20 日，10 月 28 日）

※1 観測期間は本論文で分析の対象とした期間であり，DNS ハニーポットは 2013 年 11 月 30 日現在も継続して運用中である．

観測期間中に 9 回，観測点 2 では 5 回，IP アドレスが変更されている．

4.3 実験結果

DNS ハニーポットは一般に公開しているサービスではないため，そこで観測される通信は，DNS サーバの探索を目的とするスキャンや DNS アンプ攻撃等，不正活動に関係する可能性が高い．また，我々がこれまでに観測してきた DNS アンプ攻撃と推測される通信は，その実行方法（たとえば，攻撃で発生する通信量や，攻撃対象の IP アドレス数，攻撃の継続時間等）が様々であり，一連の通信が DNS アンプ攻撃か否かの閾値を決定することは困難である．そこで，本論文では，暫定的に，1 から数十パケットの DNS クエリを DNS サーバの探索を目的としたスキャン，数百から数十万の連続した DNS クエリを DNS アンプ攻撃とし，DNS ハニーポットで観測される DNS 通信はこの 2 種類であると仮定する．また，スキャンよりも DNS アンプ攻撃で発生する DNS クエリの数が多いことから，以降の分析では，DNS ハニーポットで観測した DNS クエリを分析して得られる統計値は，DNS アンプ攻撃の傾向や特徴が強く反映されていると考える．

なお，DNS アンプ攻撃の観測例は 5 章で取り上げ，以降では，DNS ハニーポットが観測した DNS クエリ数の推移，DNS クエリの送信元 IP アドレス（DNS アンプ攻撃の場合は，攻撃対象の IP アドレスを指す）の国名および AS 番号情報，DNS アンプ攻撃で利用されるドメイン名を分析する．

表 2 各観測点で観測した DNS クエリの概要
Table 2 Overview of DNS queries that DNS honeypots observed.

	観測点 1（DNS-HONEY1）	観測点 2（DNS-HONEY2）
クエリ数（累計）	24,600,390	22,169,789
送信元 IP アドレス数（ユニーク）	16,546	8,145
要求されたドメイン数（ユニーク）	1,363	174

4.3.1 DNS クエリ数の推移

表 2 に各観測点で観測した DNS クエリの概要を示す．2 地点の DNS ハニーポットは，2013 年 10 月 31 日までに合わせて 4,700 万近くの DNS クエリを観測した．これらの DNS クエリを分析したところ，99.9%以上のクエリが再帰的な問合せを要求していたことから，ほとんどの DNS クエリは DNS キャッシュサーバに対するクエリであった．また，99.5%以上のクエリが EDNS0（Extension Mechanisms for DNS）による拡張クエリであった．EDNS0 とは，DNS で 512 オクテット以上の大きなデータを転送する際に用いられる規格 [28] である．このことから，ほとんどの DNS クエリは大きな応答を取得しようとしていたといえる．

2 つの観測点で観測した日ごとの DNS クエリ数の推移を**図 5** に示す．DNS クエリがほとんど観測されない日もあれば，1 日で非常に多く DNS クエリが観測される日も存在した．全体の傾向として，観測開始当初（2012 年 10 月）は，DNS クエリがほとんど観測されていなかったが，2013 年以降，特に，2013 年 4 月後半以降にクエリ数が増加していた．その中でも，2013 年 9 月 2 日には，観測点 1（DNS-HONEY1）で 1 日あたり 500 万以上の DNS クエリを観測しており，2013 年 10 月以降も 1 日数十万の DNS クエリを観測していた．

4.3.2 送信元 IP アドレスの国および AS 番号

DNS クエリの送信元 IP アドレスから送信元の国情報と AS 番号を特定し，送信元の国名および AS 番号別に全観測期間の DNS クエリ数を整理した．**図 6**，**図 7** に DNS クエリ数の多い上位 10 の国名および AS 番号を示す．多量の DNS クエリを送信してくる国名および AS 番号は，送信元が詐称された DNS アンプ攻撃の被害者であると考えることができる．なお，国情報および AS 番号は，2013 年 10 月 28 日に取得した MaxMind 社の GeoLite [20] のデータベースを用いて特定し，IP アドレスが属する国情報や AS 番号が観測時から変更されている可能性については考慮しない．

DNS アンプ攻撃の被害を受けている国名と AS 番号には顕著な偏りが確認できる．国別で見ると，アメリカ合衆国が一番多く，これにフランス，ルーマニア等の欧米諸国が続く．また，AS 番号別では，欧米を中心に展開する Web ホスティング会社の OVH Systems（AS16276）が一番多

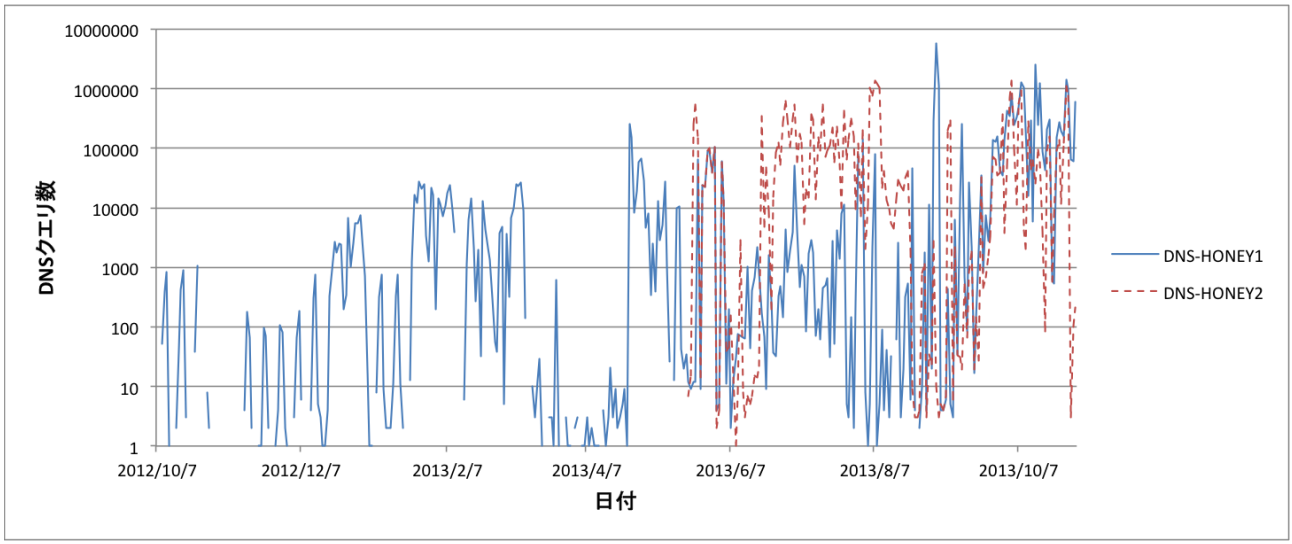

図 5 DNS ハニーポットで観測した DNS クエリ数の推移（日ごと，縦軸対数）
Fig. 5 Changes in the number of DNS queries that DNS honeypots observed (Daily, axis of ordinate is logarithmic).

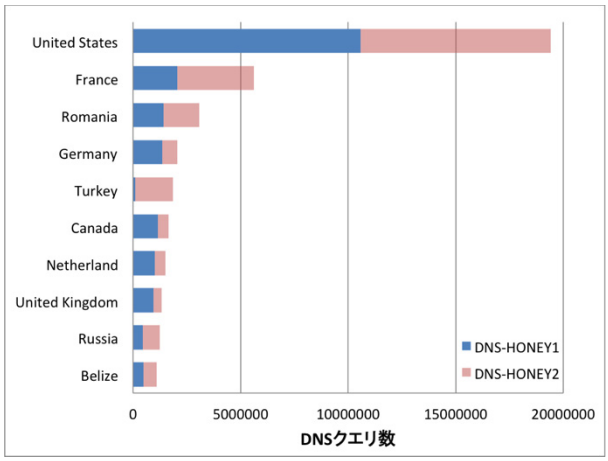

図 6 DNS ハニーポットで観測した DNS クエリの送信元の国名（上位 10）
Fig. 6 Source countries of DNS queries (TOP 10).

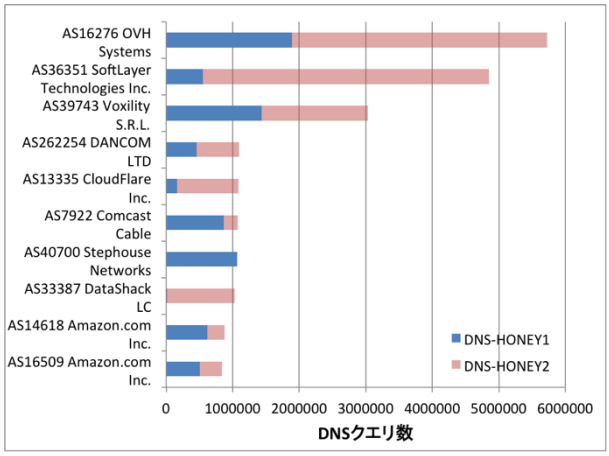

図 7 DNS ハニーポットで観測した DNS クエリの送信元の AS 番号（上位 10）
Fig. 7 Source ASes of DNS queries (TOP 10).

く，以降，Web ホスティングサービスやクラウドサービス等を運営する企業が続いており，これらの企業が主な攻撃対象となっていることが分かる．

4.3.3 利用されるドメイン名

DNS ハニーポットで観測した DNS クエリの中で，要求された回数が多い上位 10 個のドメイン名を図 8 に示す．両観測点とも，ドメイン名に対する ANY の要求が多く確認された．DNS クエリでは，ドメイン名と同時に取得する情報の種類を表す資源レコードの型（たとえば，A レコードは IP アドレス，NS レコードは権威サーバのホスト名）を要求する．その型に ANY を指定することにより，対応するすべてのレコードの応答を取得することが可能であり，ドメイン名によっては ANY の要求に対する応答は非常に増幅率が高くなることがある．

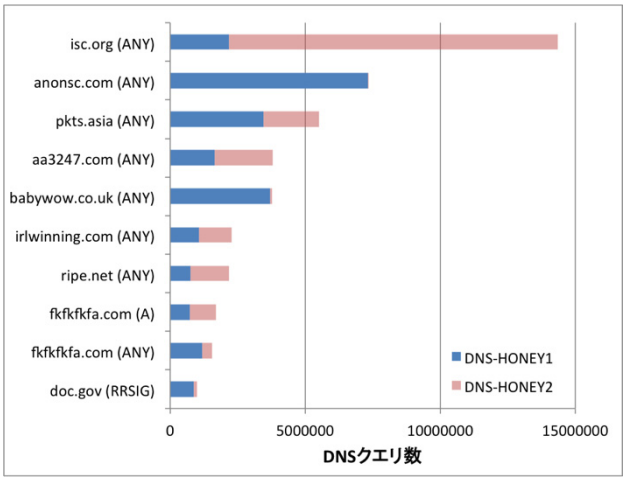

図 8 DNS ハニーポットで観測したドメイン名（上位 10）
Fig. 8 Domain names that DNS honeypot observed (TOP10).

表 3 DNS ハニーポットで観測したドメイン名の応答サイズと増幅率

Table 3 Response sizes and amplification factors of domain names that DNS honeypots observed.

ドメイン名	型	応答サイズ※2 (Byte)	増幅率※3 (%)
isc.org	ANY	3542	4541%
anonsc.com	ANY	-※4	-
pkts.asia	ANY	4056	5070%
aa3247.com	ANY	4357	5379%
babywow.co.uk	ANY	4610	5488%
irlwinning.com	ANY	4061	4778%
ripe.net	ANY	3266	4134%
fkfkfkfa.com	A	3993	4811%
fkfkfkfa.com	ANY	4067	4900%
doc.gov	RRSIG※5	11390	14603%

※2 UDP パケットのペイロード部分のバイト数．観測期間の中で，応答のパケットサイズが最大時のものを記載した．
※3 増幅率は次式で計算した．

$$\text{増幅率} = \frac{\text{DNS 応答パケットのバイト数}}{\text{DNS 要求パケットのバイト数}} \times 100\ [\%]$$

また，各パケットのバイト数は，Ethernet ヘッダ 14byte，IP ヘッダ 20byte，UDP ヘッダ 8byte と仮定し，これらに UDP のペイロード部分のバイト数を加算することで算出した．
※4 anonsc.com の応答サイズを正確に測定できなかったため，本検証では不定としている．
※5 資源レコードの電子署名を要求するための型である．

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.

ドメイン名	型	応答サイズ※2 (Byte)	増幅率※3 (%)
google.com	ANY	644	847%
facebook.com	ANY	258	361%
youtube.com	ANY	611	796%
yahoo.com	ANY	446	610%
baidu.com	ANY	476	648%
wikipedia.org	ANY	366	486%
qq.com	ANY	85	165%
live.com	ANY	604	818%
linkedin.com	ANY	927	1167%
twitter.com	ANY	780	1002%

図 8 に示したドメイン名の要求に対する応答サイズおよび増幅率を**表 3** に，一般的なドメイン名の要求に対する応答サイズおよび増幅率を**表 4** に示す．なお，ここでは Alexa [23] で公開されている人気サイトランキングの上位 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．

DNS ハニーポットで多く観測されたドメイン名の応答のデータサイズは，一般的なドメイン名の応答に比べ増幅率が高く，DNS アンプ攻撃に悪用しやすいものであることが分かる．

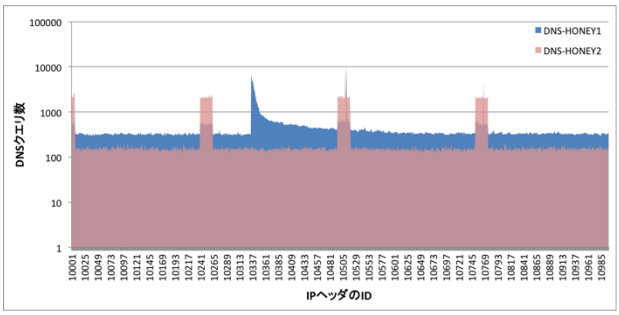

図 9 IP ヘッダの ID 値の分布（ID = 10001～11000 までを抜粋，縦軸対数）

Fig. 9 Distribution of ID field's values in IP header (from 10001 to 11000, axis of ordinate is logarithmic).

4.4 DNS クエリパケットの分析

本節では，DNS ハニーポットで観測した DNS クエリについて，各種通信プロトコルに含まれるフィールド値の分析を行う．本分析で対象とするものは，IP，UDP，DNS の各種ヘッダ，および，DNS メッセージに含まれるフィールド値である．ただし，IP ヘッダに含まれる送信元 IP アドレス，DNS のメッセージに含まれるドメイン名および資源レコードの型は 4.3 節で分析したため，本節では分析の対象としない．

分析の結果，IP ヘッダの ID 値，TTL 値，UDP ヘッダの送信元ポート番号，DNS ヘッダの ID 値等に顕著な特徴を確認した．以下で各フィールド値の概要とその特徴を説明する．

4.4.1 IP ヘッダの ID 値

IP ヘッダに含まれる ID フィールドの値は，IP パケットの分割，再構成で利用される 16 bit の識別子である．この ID 値の割当てはシステムの実装依存であるが，識別子の性質上，同じ通信の他の IP パケットと ID の値が重複しないような実装が求められている [24] ため，特定の ID 値が突出して高い頻度で利用されることはないはずである．

DNS ハニーポットで観測した DNS クエリパケットに含まれる IP ヘッダの ID 値の頻度分布の一部を**図 9** に示す．各 ID 値を有するパケットは平均的に観測されていたが，一部の ID 値が高頻度で観測された．特に，DNS-HONEY2 では，高頻度で観測される ID 値は規則的であり，256 ごとに確認され，図 9 で示す以外の範囲の ID 値においても同様の規則性がみられた．そこで，高頻度に観測された ID 値を含む DNS クエリを分析した結果，単一あるいはある範囲の ID 値のみを使用する DNS アンプ攻撃が多数確認された．

4.4.2 IP ヘッダの TTL 値

IP ヘッダに含まれる TTL フィールドの値は，IP パケットの残りの生存時間を表す 8 bit の数値である．現在の実装では，パケットがルータを 1 つ経由するごとに 1 ずつ TTL 値が減少され，TTL が 0 になるとパケットは破棄さ

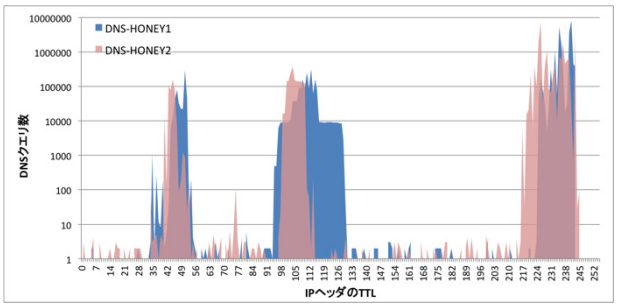

図 10 IP ヘッダの TTL 値の分布（縦軸対数）
Fig. 10 Distribution of TTL values in IP header (axis of ordinate is logarithmic).

れる．このようにすることで，IP パケットがネットワーク上を無限に巡回することを防止している．

この TTL の初期値は OS ごとに特徴的であり，UDP パケットの場合，Windows XP 以降の Windows OS は 128，MacOS X や Ubuntu 12.04 は 64 である．現在のインターネットでは，パケットが対象ホストに到達するまでに経由するルータ数は最大 30 台程度といわれており，多くの実装では，初期値として 30 以上の 2 のべき乗値（具体的には，32，64，128，255[*1]）周辺の値を採用している [25]．

DNS ハニーポットで観測した DNS クエリパケットに含まれる IP ヘッダの TTL 値の分布を**図 10** に示す．図より，DNS ハニーポットで観測される DNS クエリの多くは，初期値を 64，128，255 とするものの 3 つに分類できることが分かる．ただし，DNS-HONEY1 では，TTL の初期値がこの 3 つにあてはまらない DNS クエリも一定数存在した．

4.4.3 UDP ヘッダの送信元ポート番号

UDP ヘッダに含まれる送信元ポート番号は，コンピュータどうしの通信で利用される 16 bit の番号である．DNS サーバ側は通常 53 番ポートで待ち受けるが，クライアント側で使用するポート番号はシステムの実装依存であり不定である．近年のシステムでは，DNS キャッシュポイズニング攻撃の対策のため，送信元ポート番号をランダムに選択することが求められている [26], [27]．そのため，観測される通信では，UDP ヘッダの送信元ポート番号の分布は一様になるはずである．ただし，TCP/IP ネットワークの主要プロトコルで使用されるウェルノウンポート（0 から 1023 番）は使用されない．

DNS ハニーポットで観測した DNS クエリパケットの送信元ポート番号の分布の一部を**図 11** に示す．図より，DNS クエリ数はほとんどのポート番号で平均的に分布しているが，一部のポート番号が頻繁に利用されていることが確認できる．頻繁に利用されていた値を送信元ポート番号とする DNS クエリパケットを分析したところ，その値を送信元ポート番号とする DNS アンプ攻撃と推測される

[*1] 8 bit で表せる最大値 255 であるため，256 ではなく 255 が利用される．

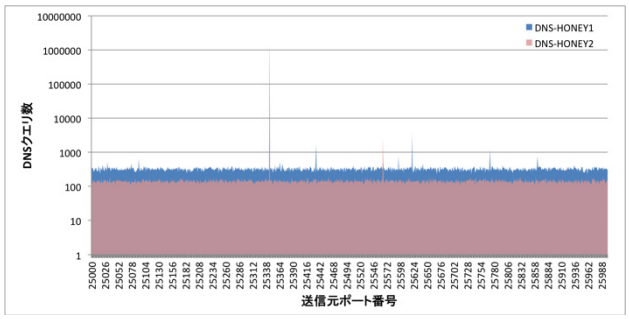

図 11 UDP ヘッダの送信元ポート番号の分布（ポート番号 = 25001～26000 を抜粋，縦軸対数）
Fig. 11 Distribution of source port numbers in UDP header (from 25001 to 26000, axis of ordinate is logarithmic).

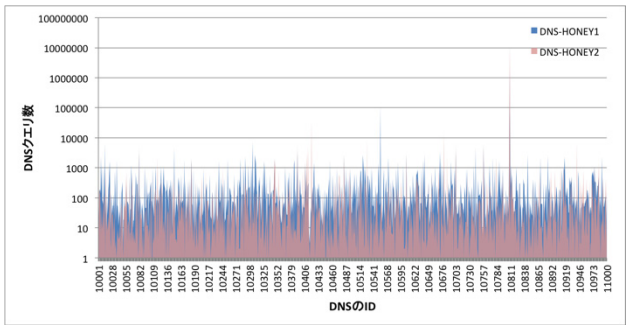

図 12 DNS ヘッダの ID 値の分布（ID = 10001～11000 を抜粋，縦軸対数）
Fig. 12 Distribution of ID field's values in DNS header (from 10001 to 11000, axis of ordinate is logarithmic).

通信が多数確認された．また，ウェルノウンポートを送信元とする攻撃も多数観測されていた．

4.4.4 DNS ヘッダの ID フィールド値

DNS ヘッダに含まれる ID フィールドの値は，DNS の要求と応答を対応付けるための 16 bit の識別子である．この ID 値の割当てはシステムの実装依存であるが，識別子の性質上，他の DNS クエリと ID の値が重複しないような実装が必要である．また，送信元ポート番号と同様に，DNS キャッシュポイズニング攻撃対策のため，ID 値はランダムに選択することが求められている [26], [27]．そのため，観測される通信では DNS ヘッダの ID フィールド値の分布は一様になるはずである．

DNS ハニーポットで観測した DNS クエリのヘッダに含まれる ID 値の分布の一部を**図 12** に示す．DNS ヘッダの ID 値は，IP ヘッダの ID 値や UDP ヘッダの送信元ポート番号に比べて平均的な分布をとっておらず，一部の値が頻繁に利用される傾向があった．そこで，頻繁に使用されていた値を DNS ヘッダの ID に持つ DNS クエリを分析したところ，その ID 値の DNS クエリのみを継続して使用する DNS アンプ攻撃が多数確認された．

4.5 実験結果に関する考察

4.5.1 DNS アンプ攻撃の傾向と特徴

DNS ハニーポットが観測した DNS クエリ数は，観測開始当初の 2012 年 10 月は 1 日平均 189 クエリ，2013 年 10 月現在は 1 日平均 34 万クエリであった．観測したクエリ数は日によって多少の変動があるものの，1 日の平均クエリ数は 1 年間で約 1,800 倍に増加していた．我々が観測している DNS クエリは，DNS ハニーポットが観測する DNS クエリのみであるため，その結果から全体的な傾向を把握することは困難だが，DNS ハニーポットで観測される傾向がインターネット上のオープンリゾルバにあてはまると仮定すると，この 1 年間で DNS アンプ攻撃による被害が深刻化していると考えることができる．

また，攻撃対象となる AS には顕著な偏りがみられた．これらの AS に対する攻撃を分析したところ，観測期間中に最も多くの DNS クエリの送信元であった OVH Systems は，2013 年のはじめから観測期間終了時まで継続して攻撃を受けており，攻撃者によって執拗に攻撃が行われていたことが分かる．

DNS アンプ攻撃に利用されていたドメイン名（表 3）は，通常のドメイン名（表 4）と比較して，いずれも増幅率が高かった．DNS アンプ攻撃には，isc.org や ripe.net，doc.gov 等正規の目的で利用されているドメイン名が悪用される場合もあったが，それ以外のドメイン名も存在していた．後者のドメイン名は，DNS ハニーポットで多量に名前解決されていたことに加え，200 以上の IP アドレスや大きな TXT レコードが応答として登録されていたため，増幅率は非常に高いものであった．また，これらのドメイン名を Web 検索エンジンで検索したところ，特定の組織に関係する記述を見つけることができなかった．以上のことから，これらのドメイン名は攻撃者が DNS アンプ攻撃のために独自に用意したものであると我々は考えている．

4.5.2 各種フィールド値の分布

4.4 節で見たように，DNS ハニーポットで観測した DNS クエリには，IP ヘッダの ID フィールド値，UDP ヘッダの送信元ポート番号，DNS ヘッダの ID フィールド値に顕著な偏りがみられた．頻繁に使用されていたフィールド値を持つ DNS クエリを分析したところ，DNS ハニーポットが観測した攻撃の一部では，固定あるいはある範囲のフィールド値が継続して使用されていた．このフィールド値の偏りは，攻撃者が使用したボット等のパケットを送信するプログラムの特徴が現れたものであると我々は考えている．また，IP ヘッダの TTL 値も，その初期値を推測することにより，送信元の OS や独自のパケット送信プログラムの指標にすることができる．

これらの特徴の分析を進めることにより，DNS アンプ攻撃を実行するマルウェアや攻撃ツールのような実体の特定や，DNS アンプ攻撃の分類への応用が期待できる．

表 5 ダークネットと DNS ハニーポットの DNS クエリ数の比較（2013 年 10 月分）

Table 5 Comparison of the number of DNS queries between darknet and DNS honeypot (October, 2013).

	ダークネット	観測点 1 (DNS-HONEY1)	観測点 2 (DNS-HONEY2)
DNS クエリ数（31 日間）	約 380	14,298,706	6,841,852
DNS クエリ数（1 日平均）	約 12	461,249	220,705

4.5.3 ダークネット観測との比較

受信パケットに対してまったく返答を行わないダークネット観測において観測される DNS クエリ数と，受信パケットに対して正しい応答を返す DNS ハニーポットにおいて観測される DNS クエリ数を比較する．DNS ハニーポットは ISP 回線下で動作するが，ISP から割り当てられる IP アドレスは，そのアドレスで応答を返すホストがいなければ，ダークネットと考えることができる．そのため，これらのクエリ数を比較することにより，DNS クエリに対する応答の有無が観測結果に与える影響，すなわち，DNS ハニーポットを設置したことによる効果を検証することが可能だと考える．

本検証では，DNS ハニーポットが観測した DNS クエリと，nicter [21] の NONSTOP [22] 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 クエリの 2013 年 10 月分を用いた．2013 年 10 月の 31 日間に DNS ハニーポットが観測した DNS クエリ数，および，ダークネットセンサが観測した DNS クエリ数を**表 5** に示す．31 日間のダークネット観測で，53/UDP 宛の通信は約 2,500 万パケット存在した．DNS クエリは各 IP アドレスに平均的に分布しており，1 つの IP アドレスで 1 カ月に観測する DNS クエリ数は平均 380 パケット，1 日あたりに換算すると 12 パケット程度であった．一方，オープンリゾルバとして動作する DNS ハニーポットでは，2013 年 10 月に 1 日平均 34 万の DNS クエリを観測した．このことから，DNS ハニーポットを設置することにより，DNS アンプ攻撃を中心とする多くの不正活動が観測可能になったと考えている．

なお，比較対象としたダークネットは長期間にわたり，応答を返さない状態であるのに対して，ISP 回線では DNS ハニーポットにアドレスが割り当てられる前は，他のユーザにより使用されているため，完全に同一の条件での比較ではないが，このような条件の差異を考慮しても DNS ハニーポット設置に起因する DNS クエリ数の増加は顕著といえる．

4.5.4 通信制御と IP アドレスの変更の影響

検証実験では，外部に与える影響を考慮し，各観測点で同一 IP アドレスに対し 1 pps の出力制限を行った．この通信制御が観測に与えた影響については不明であるが，通

信制御後も継続して DNS アンプ攻撃と推測される通信が多数観測されていることから，通信制御の有無を確認せずにオープンリゾルバを悪用する攻撃者が相当数存在すると我々は考えている．しかし，提案手法のような技術が広く展開されるに従い，攻撃者が事前に DNS サーバの応答能力を確認することが十分に考えられるため，今後は観測可能性と安全性の調整がより重要になることが予想される．

また，4.2 節で述べたように実験期間中に，観測点 1 では 9 回，観測点 2 では 5 回，観測点の IP アドレスが変更されている．IP アドレスの変更により，攻撃者は踏み台とするオープンリゾルバ（この場合は DNS ハニーポット）の IP アドレスを把握できなくなるため，DNS ハニーポットでは攻撃が観測されなくなるはずである．実際，IP アドレスの変更直後に観測される DNS クエリは，1 日あたり 0〜数百クエリ程度であり，これらはスキャンと考えられる．しかし，多量のクエリが DNS ハニーポットで観測されるようになった 2013 年 4 月以降，IP アドレス変更の数日後には，DNS アンプ攻撃と考えられる多量の名前解決が観測されるようになっていた．このことは，攻撃者がオープンリゾルバの探索を継続的に実施しており，その活動が以前と比べて活発化していることを示唆している．

5. DNS アンプ攻撃の観測例

本章では，検証実験において我々の DNS ハニーポットが観測した DNS アンプ攻撃のうち，2 つの具体的な事例を取り上げる．

5.1 事例 I：CloudFlare に対する攻撃

我々が観測する DNS ハニーポットは，CloudFlare 社，Prolexic 社（1 章参照）をはじめとするホスティングサービスや DDoS 対策サービスに関連するネットワークへの攻撃を定常的に多数観測している．本節では，2013 年 5 月に観測した CloudFlare 関連ネットワークへの DNS アンプ攻撃について記述する．

この攻撃は 2013 年 5 月 22 日午前 5 時 34 分（JST）から DNS-HONEY2 で観測された．攻撃対象は CloudFlare が所有すると推定される 5 つの IP アドレスであり，利用されたドメイン名と型は www.58wgw.com（ANY）と ripe.net（ANY）の 2 種類である．応答のログから，ripe.net（ANY）には十分な増幅効果があることを確認したが，www.58wgw.com（ANY）は増幅効果が小さかった．ただし，www.58wgw.com の応答に含まれる IP アドレスは，攻撃対象の IP アドレスのうちの 2 つを指しており，攻撃と何らかの関係があるものと我々は考えている．

5 つの IP アドレスから DNS ハニーポットへの DNS クエリ数[*2]の推移を図 **13** に示す．この攻撃は数回の小休止をはさみつつ，約 1 日半にわたって実行されていた．このときの DNS クエリの IP ヘッダに含まれる TTL 値の分布

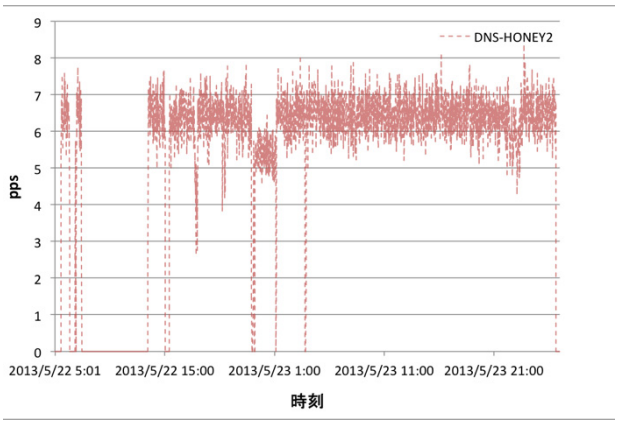

図 13 事例 I：CloudFlare に対する DNS アンプ攻撃で観測されたクエリ数の推移

Fig. 13 Case I: Changes in the number of queries that were observed in a DNS amplification attack against CloudFlare.

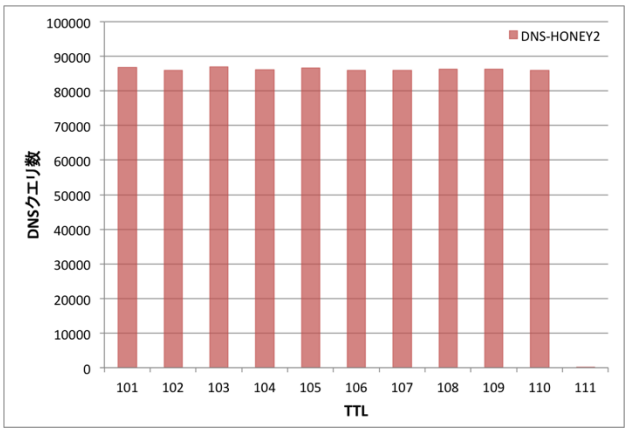

図 14 事例 I：CloudFlare に対する DNS アンプ攻撃で観測された DNS クエリパケットの TTL 値の分布

Fig. 14 Case I: Distribution of TTL field's values in DNS queries that were observed in a DNS amplification attacks against CloudFlare.

は，図 **14** のように 101〜110 に平均的に分散していた．これは，実際に DNS クエリを送信したホストから DNS ハニーポットまでにパケットが通過した経路が 10 以上存在していており，この結果は，実際の送信元が 10 以上のホストであることを示唆している．さらに，この攻撃で観測された DNS ヘッダに含まれる ID 値の分布には大きな偏りがみられたことから，これらは同じパケット送信プログラムによって生成されていると考えられる．以上のことから，この攻撃ではボットネットが利用されていたものだと考えている．

[*2] ここでは，DNS アンプ攻撃で踏み台とされたオープンリゾルバ 1 台あたりから，攻撃対象に流れ込む応答の数と考えることができる．また，このクエリ数は 1 分間に観測した DNS クエリ数を 60 秒で割った値（1 分あたりの平均の pps）を記載している．事例 II の図 15 も同様．

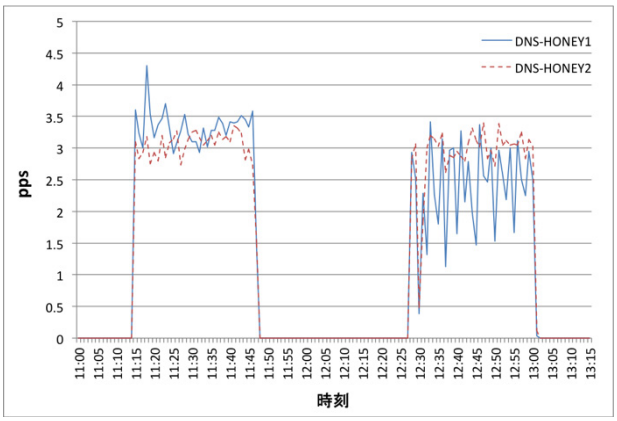

図 15 事例 II：ネットワーク分散型の DNS アンプ攻撃で観測されたクエリ数の推移

Fig. 15 Case II: Changes in the number of queries that were observed in a DNS ampification attack to distributed network.

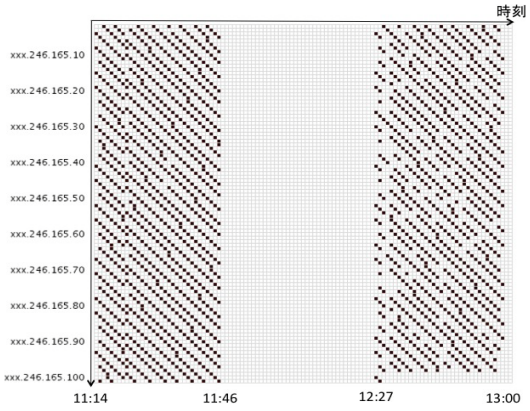

図 16 事例 II：ネットワーク分散型の DNS アンプ攻撃で観測された DNS クエリの送信元 IP アドレスの推移

Fig. 16 Case II: Changes in source IP addresses of DNS queries that were observed in a DNS ampification attack to distributed network.

5.2 事例 II：ネットワーク分散型の DNS アンプ攻撃

我々の DNS ハニーポットが観測した DNS アンプ攻撃では，攻撃対象の IP アドレスは 1〜数個程度であることが多い．しかし，2013 年 5 月 29 日に観測した攻撃では，攻撃対象の IP アドレスが同一ネットワーク内の 100 個に分散していた．

この攻撃は，2013 年 5 月 29 日午前 11 時 14 分（JST）から DNS-HONEY1 と DNS-HONEY2 の両方で観測された．利用されたドメイン名は ripe.net（ANY）である．観測された DNS クエリの送信元 IP アドレスは第 1 から第 3 オクテットが同一であり，第 4 オクテットには 1 から 100 までの値が使用されていた．

これらの IP アドレスからの DNS ハニーポットへの DNS クエリ数の時間推移を**図 15** に示す．DNS-HONEY1 と DNS-HONEY2 で攻撃の開始時刻，終了時刻は同期していた．また，DNS クエリの IP ヘッダに含まれる TTL 値も DNS-HONEY1 では 107〜116，DNS-HONEY2 では 101〜110 に平均的に分散していた．

この攻撃で観測された DNS クエリの送信元 IP アドレスの時間変化を**図 16** に示す．横軸が時刻，縦軸が DNS クエリの送信元の IP アドレスを表しており，時刻 t に IP アドレス a からの DNS クエリを観測した場合，その座標（t, a）に点をプロットしている．図 16 より，DNS クエリの送信元 IP アドレスは時刻とともに機械的に推移していることが確認できる．これは，攻撃者が意図的に攻撃対象となる IP アドレスを分散させていたためだと考えている．

以上のことから，事例 II の攻撃では，事例 I と同様に，DNS クエリを送信した実ホストはボットに感染したホスト群であると考えている．

6. まとめと今後の課題

本論文では，DNS サーバを悪用する不正活動を観測する手法として DNS ハニーポットを提案し，検証実験により，提案手法は DNS アンプ攻撃と推測される通信を多数観測していることを確認した．また，DNS ハニーポットを用いた 1 年間以上の長期観測の事例から，DNS ハニーポットが観測した DNS クエリを分析し，観測開始当初である 2012 年 10 月に比べ，DNS アンプ攻撃の被害が深刻化していること，DNS アンプ攻撃の攻撃対象となっている国や組織，DNS アンプ攻撃に利用されるドメイン名を明らかにした．さらに，DNS クエリに含まれるフィールド値を分析した結果，パケットに含まれる各種プロトコルに，顕著な偏りがみられることを明らかにし，これらが DNS アンプ攻撃の実態解明や，その分類に期待できることを示した．以上のことから，DNS ハニーポットを用いて DNS アンプ攻撃の動向を継続的に観測・分析することは，DNS アンプ攻撃への対策技術を検討するうえで有効である．

今後の課題としては，DNS ハニーポットによる DNS アンプ攻撃の観測・分析を継続するとともに，検証実験で観測した DNS アンプ攻撃を，ISP をはじめとするインターネットを運用する組織の実トラフィックと比較する等して，より広い視点から観測した攻撃を裏付けることが必要であると考えている．また，本研究の分析結果より得られた DNS アンプ攻撃の特徴の分析を進めることにより，DNS アンプ攻撃の実体を明らかにするとともに，本研究から得られる知見をもとにした DNS アンプ攻撃への対策技術を検討していきたいと考えている．

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）にて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] Mockapetris, P.: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION (RFC1035), IETF (online), available from ⟨http://www.ietf.org/rfc/rfc1035.txt⟩ (accessed 2013-11-24).

[2] 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 2013-11-24）．

[3] Open Resolver Project, available from ⟨http://openresolverproject.org/⟩ (accessed 2013-11-24).

[4] The Spamhaus Project, available from ⟨http://www.spamhaus.org/⟩ (accessed 2013-11-24).

[5] CloudFlare: The DDoS That Almost Broke the Internet, available from ⟨http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet⟩ (accessed 2013-11-24).

[6] TrendLabs SECURITY BLOG：DNS Amp 手法による過去最大規模の DDoS 攻撃，スパム対策組織「Spamhaus」がターゲットに，入手先 ⟨http://blog.trendmicro.co.jp/archives/7012⟩ （参照 2013-11-24）．

[7] Prolexic Technologies, available from ⟨http://www.prolexic.com/⟩ (accessed 2013-11-24).

[8] 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 2013-11-24).

[9] Kambourakis, G., Moschos, T., Geneiatakis, D. and Gritzalis, S.: Detecting DNS Amplification Attacks, *CRITIS 2007*, LNCS 5141, pp.185–196 (2008).

[10] Sun, C., Liu, B. and Shi, L.: Efficient and Low-Cost Hardware Defense Against DNS Amplification Attacks, *Proc. IEEE Global Telecommunications Conference* (*GLOBECOM*), pp.1–5 (2008).

[11] Oberheide, J., Karir, M. and Z. Mao, M.-L.: Characterizing Dark DNS Behavior, *DIMVA 2007*, LNCS 4579, pp.140–156 (2007).

[12] 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).

[13] 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).

[14] 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 2013-11-25).

[15] 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 2013-11-24).

[16] Ubuntu, available from ⟨http://www.ubuntu.com/⟩ (accessed 2013-11-24).

[17] BIND, available from ⟨http://www.isc.org/⟩ (accessed 2013-11-24).

[18] iptables, available from ⟨http://www.netfilter.org/projects/iptables/⟩ (accessed 2013-11-24).

[19] tcpdump, available from ⟨http://www.tcpdump.org/⟩ (accessed 2013-11-24).

[20] MaxMind: GeoLite Free Downloadable Databases, available from ⟨http://dev.maxmind.com/geoip/legacy/geolite/⟩ (accessed 2014-04-06).

[21] nicter, available from ⟨http://www.nicter.jp/⟩ (accessed 2013-11-24).

[22] 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).

[23] Alexa, available from ⟨http://www.alexa.com/⟩ (accessed 2013-11-25).

[24] West, M. and McCann, S.: TCP/IP Field Behavior (RFC4413), IETF (online), available from ⟨http://www.ietf.org/rfc/rfc4413.txt⟩ (accessed 2013-11-25).

[25] Sebastian, A.: Default time to live (TTL) values, available from ⟨http://www.binbert.com/blog/2009/12/default-time-to-live-ttl-values/⟩ (accessed 2013-11-25).

[26] Atkins, D. and Austein, R.: Threat Analysis of the Domain Name System (DNS) (RFC3833), IETF (online), available from ⟨http://www.ietf.org/rfc/rfc3833.txt⟩ (accessed 2013-11-25).

[27] Hubert, B. and van Mook, R.: Measures for Making DNS More Resilient against Forged Answers (RFC5452), IETF (online), available from ⟨http://www.ietf.org/rfc/rfc5452.txt⟩ (accessed 2013-11-25).

[28] Vixie, P.: Extension Mechanisms for DNS (EDNS0) (RFC2671), IETF (online), available from ⟨http://www.ietf.org/rfc/rfc2671.txt⟩ (accessed 2013-11-25).

[29] CloudFlare, Inc., available from ⟨http://www.cloudflare.com/⟩ (accessed 2013-11-27).

[30] 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 2013-11-29）．

[31] 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 2013-11-29）．

[32] Spitzner, L.: Honeypots – Definitions and Value of Honeypots, available from ⟨http://www.tracking-hackers.com/papers/honeypots.html⟩ (accessed 2013-11-26).

牧田 大佑

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．2007 年 4 月～2011 年 3 月は同大学教育研究評議員を兼務．2011 年 4 月～2013 年 3 月は同大学理工学部副学部長を兼務．日本学術会議連携会員．暗号アルゴリズム・プロトコル，耐タンパ技術，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）受賞．