Vol.2013-CSEC-62 No.54
Vol.2013-SPT-6 No.54
2013/7/19

DNS ハニーポットによる不正活動観測

牧田大佑† 吉岡克成† 松本勉†

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悪用されており，特に，外部からの再帰的問い合わせを許可する DNS キャッシュサーバは，DNS アンプ攻撃の踏み台として悪用され，分散型サービス妨害の要因となっている．本稿では，DNS サーバを悪用する不正活動を観測する手法を提案する．提案手法では，インターネット上に複数の観測地点を用意し，各地点で囮となる DNS サーバをハニーポットとして運用することにより，DNS サーバを悪用する不正活動を観測，分析する．半年以上の検証実験の結果，本提案手法が DNS アンプ攻撃と推測される不正活動を観測可能であることを確認した．

Observing Malicious Activities with DNS Honeypot

DAISUKE MAKITA† KATSUNARI YOSHIOKA†
TSUTOMU MATSUMOTO†

Domain Name System (DNS) plays an important role to map domain names to their information such as IP addresses on the Internet. Meantime, DNS is also abused for malicious activities. Especially, DNS cache servers which allow recursive queries from anywhere on the Internet (Open Resolver) are abused as steppingstones for DNS amplification attacks, a type of DDoS attacks. In this paper, we propose a method for observing malicious activities that abuse DNS servers. In this method, we prepare several monitoring points on the Internet, run a dummy DNS server as a honeypot at each point, observe and analyze malicious activities from their traffic. As a result of long-term evaluation experiment in ISP networks, we confirm that out method can observe a series of suspicious activities that appear to be related to DNS amplification attacks.

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活動にも悪用されており，特に，外部からの再帰的問い合わせを許可する DNS キャッシュサーバ(オープンリゾルバ)は，DNS アンプ攻撃の踏み台として悪用され，分散型サービス妨害（DDoS）攻撃の要因になっている[2].

Open Resolver Project[3]によると，外部からの DNS のデフォルトポートである UDP/53 への問い合わせに対して何らかの形で応答するサーバはインターネット上に 3300 万以上存在しており，これらが DNS アンプ攻撃を引き起こす要因となっている．2013 年 3 月に発生したスパム対策組織の Spamhaus[4]をターゲットにした 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 120Gbps もの通信量が関係するネットワークに流れ込み，上流のインターネット相互接続点（IX）では一時 300Gbps の通信量を観測したと言われている[5, 6].

このような脅威に対抗するためには，DNS サーバを悪用する不正活動を観測し，その傾向や特徴を把握することが重要になる．そこで，本稿では，DNS サーバを悪用する不正活動を観測する手法を提案する．提案手法では，インターネット上に複数の観測地点を用意し，各地点で囮となる DNS サーバをハニーポットとして運用することにより，DNS サーバを悪用する不正活動を観測する．そして，各観測地点の通信，及び，複数地点の通信の相関を分析することにより，DNS サーバを悪用する不正活動の傾向や特徴の把握を試みる．提案手法を実装したシステムを一般 ISP 回線下に設置し，半年以上の検証実験を行った結果，本提案手法が DNS アンプ攻撃と推測される不正活動を観測可能であることを確認した．

本稿の構成は次の通りである．2 章で既存の不正活動手法として，ハニーポットとダークネットを用いた不正活動観測について説明する．3 章で提案手法を概説し，4 章で検証実験と実験結果を示す．5 章で検証実験にて観測した DNS アンプ攻撃と思われる通信の例をまとめ，6 章で考察を行う．最後に，7 章でまとめと今後の課題とする．

2. 既存の不正活動観測手法

2.1 ハニーポット

ハニーポットとは，不正使用をされることに価値を持つ情報システム資源であり[7]，不正アクセスの手法やその傾向等を分析することを主な目的としている．

ハニーポットには分析の目的に応じて様々な種類が存在している．例えば，リモートエクスプロイトにより感染を拡大させるマルウェアの観測や検体入手を目的とするサーバ型のハニーポットや，Web ブラウザやそのプラグインの脆弱性を悪用する攻撃を観測するクライアント型のハニーポット等が運用されている．エミュレータ等で脆弱性を模

†横浜国立大学
Yokohama National University

ⓒ2013 Information Processing Society of Japan

擬し不正使用を観測する（低対話型）ものから，実システムを用いて不正使用を観測する（高対話型）ものまで，その形態も目的に応じて様々であるが，インターネットで発生するセキュリティ上の脅威の観測やその対策の導出に有効な手段である．

2.2 ダークネット

ダークネットとは，インターネット上から到達可能なものの，特定のホストに割り当てられていないアドレス空間のことである．ダークネットは未使用アドレス空間であるため，本来ならばそのアドレス空間への通信は発生しないはずであるが，マルウェアの感染拡大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通信が観測されている．これらの通信を観測することによりインターネット上で発生しているスキャンや攻撃を検知することが可能であり，ハニーポットと同様，インターネットで発生しているセキュリティ上の脅威の分析に利用されている．

3. 提案手法

本章では，DNS サーバを悪用する不正活動を観測する手法を提案する．まず，3.1 節では提案手法により観測を想定している不正活動について述べる．次に，3.2 節で提案手法の要件を述べ，3.3 節で提案手法を概説する．

3.1 観測を想定している不正活動

提案手法により観測することを想定している不正活動として次の 2 つを挙げる．

3.1.1 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として利用する攻撃である[8]．一般に，DNS では問い合わせ（クエリ）よりも応答（レスポンス）のパケットサイズが大きくなるため，小さなクエリから大きなレスポンスを発生させることが可能である．また，DNS 通信は主に UDP パケットで行われるため, 送信元 IP アドレスの詐称することが可能である．これらの性質を利用することにより，送信元 IP アドレスを攻撃対象の IP アドレスに偽装し，予め選定したパケットサイズの大きい DNS 応答を攻撃対象に集中させることで，攻撃対象ホストの周辺の通信帯域を圧迫する DDoS 攻撃が可能になる．

DNS アンプ攻撃には攻撃者が所有するボット，及び，オープンリゾルバが利用されることが多い．そのため，このような攻撃を観測することができれば，攻撃の傾向や特徴を把握する上で有効な手段になる．

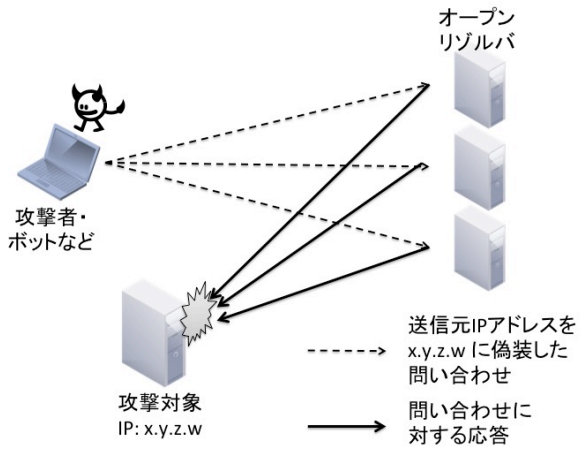

図 1　DNS アンプ攻撃の例

3.1.2 オープンリゾルバを悪用するマルウェアの DNS 通信

近年のマルウェアは，C&C（Command &Control）サーバを通して攻撃者からの指令を受け取る機能を有している物が多い．W32.Morto（Symantec 名）は，DNS の TXT レコードを通じて指令を受け取ることが確認されており[9]，また，我々の解析において，このマルウェアは OS に設定されている DNS キャッシュサーバだけでなく, インターネット上のオープンリゾルバを利用することを確認している．このような DNS 通信を観測することができれば, そのマルウェアの感染数やその動向を把握する上で有効な手段になる．

3.2 提案手法の要件

DNS サーバを悪用する不正活動を観測する手法に求められる要件として,「観測可能性」と「安全性」の 2 つを挙げる．

観測可能性とは, 提案手法により DNS サーバを悪用する様々な挙動を観測できる性質を指す．3.1 節に我々が現在想定している不正活動を述べたが，これ以外の不正活動についても観測，分析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影響を与えず，安全に観測，分析できる性質を指す．安全性を満たすためには，通信量やその内容によって応答を制限する必要がある．

DNS サーバを悪用する不正活動の場合, 攻撃者によって事前に DNS サーバの応答能力等が検査されることが十分に考えられ，観測可能性と安全性はトレードオフの関係になる．そのため，目的に応じてこれらの要件を調整していくことが重要になる．

3.3 提案手法の概略図

提案手法の概要を図 2 に示す．提案手法は大きく「収集部」と「分析部」からなる.「収集部」は，インターネット上から接続可能な複数の観測地点のマシンから構成され，マシン上では，不正使用が可能な DNS サーバ（DNS ハニーポットと呼ぶ，後述）がサービスを提供しており，DNS

の問い合わせや応答のログを収集する．各観測地点で収集されたログは「分析部」に転送され，そこで各観測地点の通信分析，及び，複数地点の通信の相関分析を行い，最後に分析レポートを出力する．

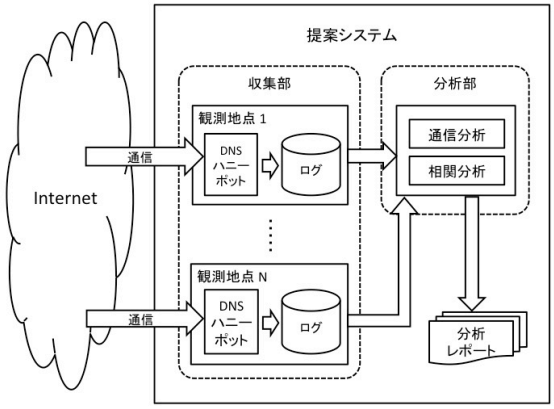

図 2　提案手法の概念図

提案手法で使用する 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，実線がネットワーク通信の流れを，破線はシステム制御の流れを表す．

まず，DNS サーバは外部からの DNS の問い合わせに対して応答する役割を担う．この DNS サーバは，インターネット上の任意の地点から使用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に存在し，DNS サーバに悪用された場合に，外部に影響を与えない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，及び，ログの出力を行う．

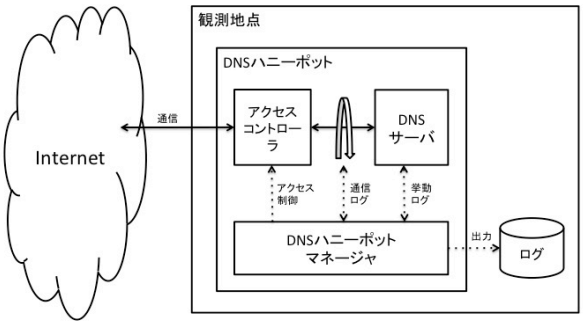

図 3　DNS ハニーポットの概念図

4. 検証実験

本章では，提案手法の有効性を検証するため行った実験について記述する．まず，4.1 節で検証実験に使用したシステムの実装を述べる．次に，4.2 節で検証実験の方法をまとめ，4.3 節で観測結果を，4.4 節で観測された不正活動をまとめる．

4.1 提案手法の実装

検証実験では，各観測地点に Linux ディストリビューションの一つである Ubuntu 12.04 Desktop 版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．検証実験で実装した DNS ハニーポットシステムの概要を図 4 に示す．DNS ハニーポットは，DNS サーバとして BIND 9.8.1 [11]，アクセスコントローラとして iptables [12]，DNS ハニーポットマネージャとして Linux 標準のコマンド，及び，その制御用のシェルスクリプトを用いて実装し，解析者が DNS ハニーポットマネージャを操作できるようにした．また，検証実験では，DNS サーバである BIND を外部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た．通信ログのキャプチャには tcpdump [13]を用い，BIND から出力されるクエリログ，及び，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．

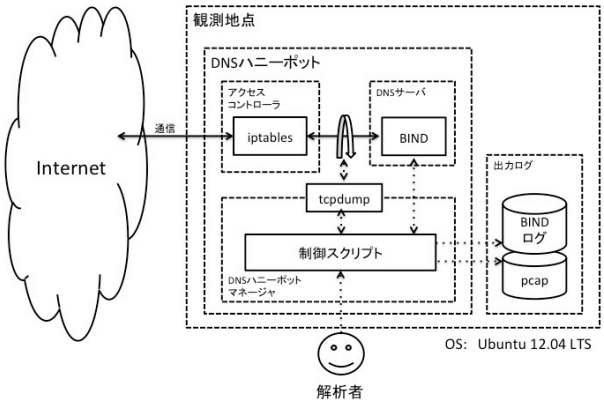

図 4　DNS ハニーポットの実装

4.2 実験方法

まず，攻撃者が一般 ISP 下の DNS サーバを不正使用するかを 1 つの観測地点を用いて検証した．この実験において，システムが不正活動に利用されていることを確認した後に，新たに観測地点を追加した．そして，これらの 2 つの観測地点で観測した通信の分析，及び，2 地点で観測した通信の相関分析を行った．

各観測地点の環境の概要を表 1 に示す．2 つの観測地点は別の ISP のネットワークに属しており，4.1 節で記述したように OS，DNS サーバ等は同様のものを用いた．また，アクセス制御は，観測可能性を優先するために手動で制御する程度にとどめた．ただし，観測地点 2 では，5 月 27 日以降は iptables の hashlimit 機能を用いて同一 IP アドレスへの応答を 1pps 程度に制限した．

なお，2 つの観測地点のマシン間にはシステム時刻（Unix Time）に 30 秒程度のずれが存在していた．また，観測地点 1 では，観測期間中に 3 回（2013 年 3 月 13 日，3 月 22

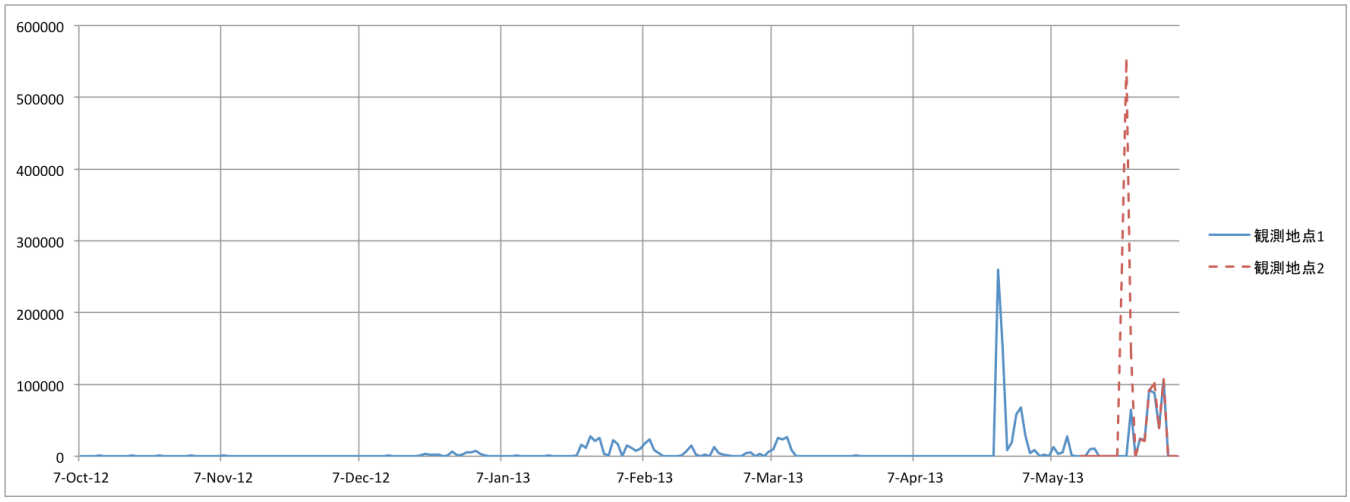

図 5　各観測地点で観測した問い合わせ数の推移

日，4 月 9 日)，IP アドレスが変更されている．

表 1　各観測地点の環境

	観測地点 1	観測地点 2
回線	一般 ISP①	一般 ISP②
OS	Ubuntu 12.04	Ubuntu 12.04
DNS サーバ	BIND 9.8.1	BIND 9.8.1
観測期間	2012 年 10 月 7 日～2013 年 6 月 2 日（237 日間）	2013 年 5 月 13 日～2013 年 6 月 2 日（19 日間）
アクセス制御	手動	手動，2013 年 5 月 27 日以降は同一 IP アドレスに対して 1pps が上限

4.3 実験結果

本節では，2 つの観測地点で観測した DNS 通信の分析結果を述べる．表 2 に各観測地点で観測期間中に観測した問い合わせ数，問い合わせ元の IP アドレス数，問い合わされたドメイン数を示す．以下，問い合わせ数の推移，問い合わせ元の IP アドレス，問い合わされたドメイン名についてまとめる．

表 2　各観測地点で観測した DNS 通信の概要

	観測地点 1	観測地点 2
問い合わせ数（累計）	1,578,121	1,340,039
問い合わせ元の IP アドレス数	919	326
問い合わされたドメイン名の数	1,001	49

4.3.1 問い合わせ数の推移

2 つの観測地点における日毎の問い合わせ数の推移を図 5 に示す．DNS の問い合わせがほとんどない日もあれば，一日で非常に多く問い合わせが観測される日も存在した．全体の傾向としては，2013 年以降，特に 4 月後半以降に問い合わせ数が急増している．また，2013 年 5 月末の 2 つの観測地点における問い合わせ数はほぼ同じ数値を示しており，この期間に 2 つの地点で観測された問い合わせには相関があることを確認した（5.2 節，5.3 節参照）．

4.3.2 問い合わせ元の IP アドレス

観測地点 1，2 で観測された通信の中で，問い合わせ数が多かった IP アドレスとその問い合わせ回数，及び，その IP アドレスが属する国名をそれぞれ表 3，4 示す．なお，国名は，GeoIP[14] を用いて推定した．

問い合わせ回数の多い IP アドレス，及び，その IP アドレスが割り当てられている国には大きな偏りが存在しており，観測地点 1 では主に欧州の国が，観測地点 2 では主に米国が問い合わせ元になっている．

表 3　IP アドレス毎の問い合わせ回数（観測地点 1）

問い合わせ回数	IP アドレス	国
121,409	xxx.33.217.9	United Kingdom
114,785	xxx.165.154.75	Poland
72,866	xxx.3.51.194	France
61,660	xxx.165.94.155	France
61,402	xxx.33.2.164	Poland
54,945	xxx.217.113.202	-
53,316	xxx.165.94.153	France
31,935	xxx.135.134.141	-
31,507	xxx.172.179.21	Germany
29,051	xxx.171.170.1	United States

表 4　IP アドレス毎の問い合わせ回数（観測地点 2）

問い合わせ回数	IP アドレス	国
309,527	xxx.93.248.10	-
308,389	xxx.93.249.10	-
70,514	xxx.245.59.142	United States
58,663	xxx.245.58.138	United States
58,105	xxx.245.58.99	United States
57,751	xxx.245.59.99	United States
29,758	xxx.171.170.1	United States
28,198	xxx.171.179.1	United States
21,636	xxx.125.31.121	United States
17,857	xxx.18.190.126	United States

ⓒ2013 Information Processing Society of Japan

4.3.3 問い合わされたドメイン名

観測地点 1，2 で観測された通信の中で，問い合わせ数の多かったドメイン名とレコードの型，及び，その問い合わせ回数を表 5，6 に示す．

両地点とも，特定のドメイン名に関する ANY の問い合わせが多く見られた．ANY 問い合わせとは，ドメイン名に対応する全てのレコードを取得するものであり，ドメインによっては大きな応答を返すことになる（表 7）．

表 5　ドメイン名毎の問い合わせ回数（観測地点 1）

問い合わせ回数	ドメイン名	型
1,105,518	isc.org	ANY
332,358	ripe.net	ANY
32,196	www.2sf999.com	ANY
31,330	8845.582878.com	ANY
28,298	www.ntdtv.com	ANY
7,877	kkkfu.sylytz.com	ANY
7,735	120sf.0755nk.net	ANY
7,630	hao-119.51shop6.com	ANY
1,768	dmd8j1rexm7yf.cloudfront.net	ANY
1,353	sf678.0755nk.net	ANY

表 6　ドメイン名毎の問い合わせ回数（観測地点 2）

問い合わせ回数	ドメイン名	型
827,664	ripe.net	ANY
382,190	www.58wgw.com	ANY
31,553	www.2sf999.com	ANY
31,187	8845.582878.com	ANY
28,019	www.ntdtv.com	ANY
13,600	120sf.0755nk.net	ANY
7,652	kkkfu.sylytz.com	ANY
7,443	hao-119.51shop6.com	ANY
5,469	www.sf86.com	ANY
2,534	dmd8j1rexm7yf.cloudfront.net	ANY

表 7　isc.org，ripe.net の問い合わせ，応答のパケットサイズとその増幅率（ANY，2013 年 6 月 17 日現在）

ドメイン名	問い合わせ	応答（最大[a]）	増幅率[b]
isc.org	78byte	3,497byte	4483.3%
ripe.net	79byte	2,882byte	3648.1%

4.4 観測された不正活動

検証実験では，特定の IP アドレスから特定のドメイン名に関する大量の問い合わせが多数観測された．これらの通信を分析したところ，ある期間継続して増幅率の高い isc.org や ripe.net を ANY で問い合わせているホストが多く，DNS アンプ攻撃が行われているものと推測される．なお，検証実験において，DNS アンプ攻撃と推測される通信は多数確認したが，それ以外の不正活動に関しては現状では確認できていない．

a) 付録 A.1 参照
b) 増幅率＝応答パケットサイズ÷問い合わせパケットサイズ×100%

4.4.1 不正活動を観測するまでの日数

各観測地点において，観測開始日から不正活動が観測されるまでの日数を調べるため，問い合わせ数が多かった isc.org または ripe.net の ANY の問い合わせを初めて観測した日，及び，DNS アンプ攻撃を初めて観測した日を調査した．なお，isc.org または ripe.net の ANY の問い合わせの DNS クエリが 1 分間あたり 60 回を超えたものを DNS アンプ攻撃とみなした．

各観測地点における，isc.org または ripe.net の ANY の問い合わせの初観測日，及び，DNS アンプ攻撃の初観測日を表 7 に示す．観測地点 1 では，isc.org または ripe.net の ANY の問い合わせが観測されるまでに 21 日，DNS アンプ攻撃が観測されるまでに 54 日かかったのに対し，観測地点 2 では，isc.org または ripe.net の ANY の問い合わせが観測されるまで 3 日，DNS アンプ攻撃が観測されるまでに 9 日程度であった．観測地点が 2 箇所程度であることから断定はできないが，図 5 に示した問い合わせ数の推移を合わせて考えると，オープンリゾルバを用いた DNS アンプ攻撃の頻度が実験期間を通じて増加していることが推測される．

表 8　観測開始日から不正活動が観測されるまでの日数

	観測地点 1	観測地点 2
観測開始日	2012 年 10 月 7 日	2013 年 5 月 13 日
isc.org/ripe.net の初観測日	2012 年 10 月 28 日（＋21 日）	2013 年 5 月 16 日（＋3 日）
DNS アンプ攻撃の初観測日	2012 年 12 月 21 日（＋54 日）	2013 年 5 月 22 日（＋9 日）

5. DNS アンプ攻撃の分析

4 章の検証実験の結果，DNS アンプ攻撃の踏み台になっていると推測される通信が多く観測された．本章では DNS アンプ攻撃と推測される通信の分析結果をまとめる．なお，以下に記載する時刻はいずれも日本標準時（JST）である．

5.1 観測された DNS アンプ攻撃

検証実験で観測された DNS アンプ攻撃の挙動は，大きく 2 つに分類可能であった．1 つは，1 秒あたり数回程度の低いレートで問い合わせが続くもの，もう一つは，1 秒あたり数十回もの高いレートで問い合わせが続くものである．以下にそれぞれの例を取り上げる．

5.1.1 低いレートで行われる DNS アンプ攻撃の例

低いレートで行われる DNS アンプ攻撃の例として，観測地点 1 で 2013 年 1 月 31 日夜から 2 月 1 日朝に観測された通信を取り上げる．

問い合わせ元 IP アドレス（xxx.33.217.9）は，観測地点 1 で問い合わせ回数が最も多かったホストである．この IP アドレスは，逆引き結果，及び，WHOIS 情報から欧州を中心に展開する Web ホスティングサービスのものと推測された．この DNS アンプ攻撃では，isc.org の ANY の問い合わせが悪用されていた．

ⓒ2013 Information Processing Society of Japan

観測地点 1 から xxx.33.217.9 への通信の pps（packets per second）と bps（bits per second）の時間推移を図 6 に示す．図より，1pps 程度の問い合わせが継続的に，小休止を挟みつつ数時間にわたって行われていることが確認できる．また，このホストへの DNS アンプ攻撃は，観測期間中の 13 日で観測された．

この期間の DNS 通信を分析したところ，DNS 通信のヘッダに含まれる ID は 10809 で固定であり，IP ヘッダに含まれる TTL は 99〜128 または 227 と幅広く分布していた．これはボットのようなホスト群が送信元 IP アドレスを偽装していたためと推測される．

また，観測地点 2 で観測された xxx.93.248.10 や xxx.93.249.10 への通信では，ripe.net の ANY の問い合わせが利用されていたものの，同様に低いレートの DNS アンプ攻撃が確認された．

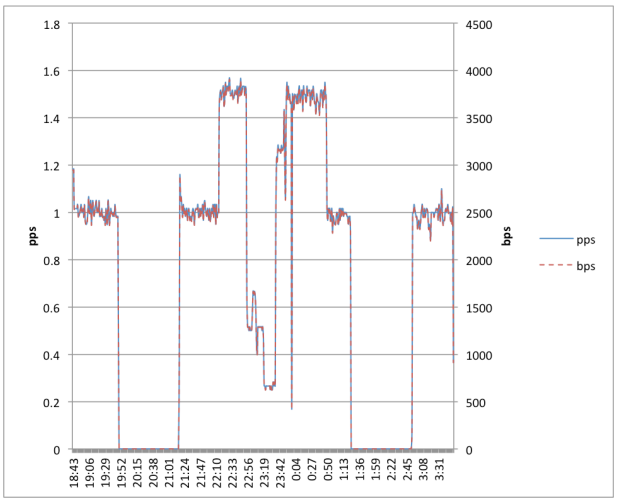

図 6　観測地点 1 から xxx.33.217.9 への通信の推移

5.1.2 高いレートの DNS アンプ攻撃の例

高いレートで行われる DNS アンプ攻撃の例として，観測地点 1 で 2013 年 4 月 25 日に観測された通信を取り上げる．

問い合わせ元 IP アドレス（xxx.165.154.75）は，観測地点 1 で 2 番目に問い合わせ回数が多かったホストである．IP アドレスの逆引き結果，及び，WHOIS 情報から先と同じホスティングサービスが保持する IP アドレスであることが推測された．この DNS アンプ攻撃でも，isc.org の ANY の問い合わせが悪用されていた．

観測地点 2 から xxx.165.154.75 への通信の pps と bps の時間推移を図 7 に示す．図より，40〜50pps，10 万 bps 程度の通信が小休止を挟みつつ数時間行われていることが確認できる．このホストへの DNS アンプ攻撃は観測期間中の 3 日で観測された．

また，この期間の DNS 通信を分析したところ，DNS 通信のヘッダに含まれる ID は 7490 で固定であり，IP ヘッダに含まれる TTL は，109, 111, 113, 115 とわずかではあるが分散していた．

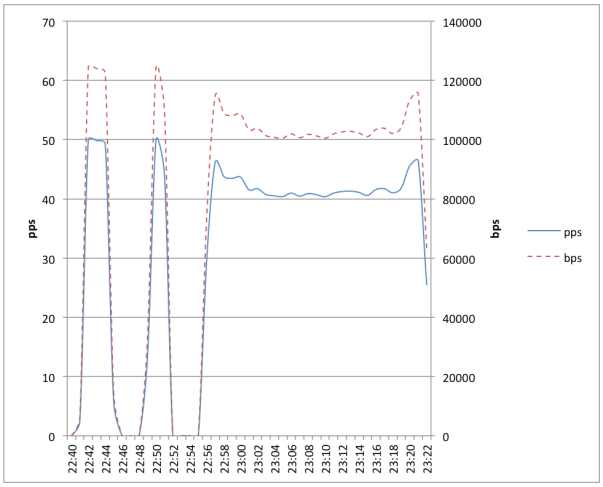

図 7　観測地点 1 から xxx.165.154.75 への通信の推移

5.2 2 つの観測地点で相関のある DNS アンプ攻撃の例

検証実験では，2013 年 5 月 13 日以降，2 つの観測地点で観測を行っている．ここでは，この 2 地点で相関のあった DNS アンプ攻撃の例として，5 月 28 日に観測された通信を取り上げる．

問い合わせ元の IP アドレス（xxx.171.170.1）は，観測地点 1 では 10 番目，観測地点 2 では 7 番目に問い合わせ回数が多かったホストである．IP アドレスの逆引き結果，及び，WHOIS 情報からホスティングサービスの DNS サーバであることが推測された．この DNS アンプ攻撃では，ripe.net の ANY の問い合わせが利用されていた．

観測地点 1，2 から xxx.171.170.1 への通信の pps と bps の時間推移を図 8，図 9 にそれぞれ示す．観測地点 1，観測地点 2 ともに DNS アンプ攻撃の開始時刻，終了時刻は同じである．観測地点 1 では平均して 1.5pps 程度の通信が流れ込んでいるのに対し，観測地点 2 では同一ホストへの通信は 1pps 程度に制限しているため，平均して 1.0pps 程度であった．なお，各観測地点である時期に bps のみが急増しているのは，DNS キャッシュサーバ内に存在するキャッシュが応答の大きさに影響しているためである（付録 A.1 参照）．

また，2 つの観測地点で観測した DNS 通信のヘッダに含まれる ID を調べたところ，パケットごとに様々な値であったものの，2 地点間の問い合わせで使用された ID 群は完全に一致しており，同一のボットネットからの通信であることが予想される．また，IP ヘッダに含まれる TTL は，観測地点 1 では 107〜116，観測地点 2 では 101〜110 に分散していた．

ⓒ2013 Information Processing Society of Japan

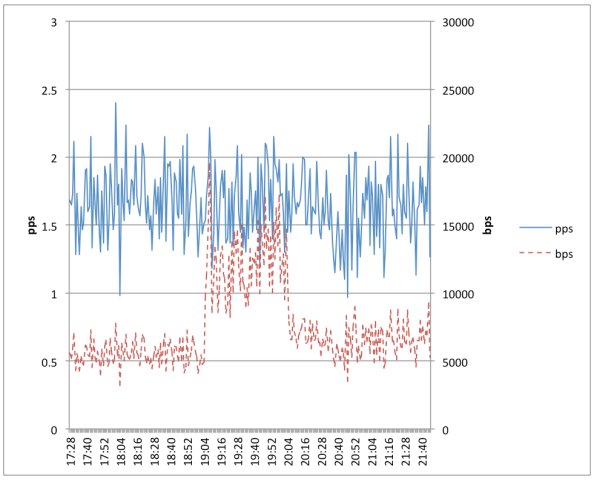

図 8　観測地点 1 から xxx.171.170.1 への通信の推移

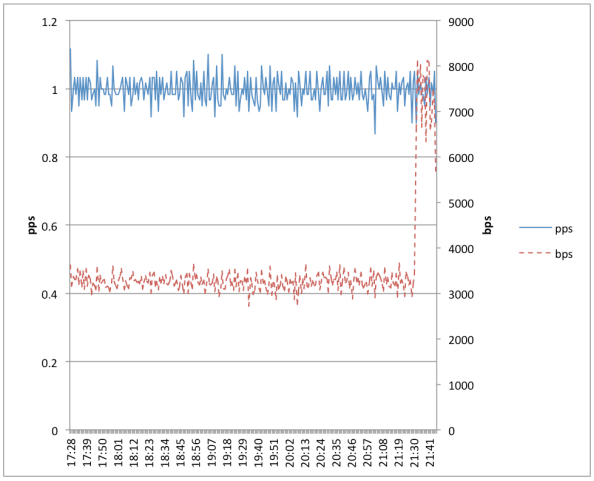

図 9　観測地点 1 から xxx.171.170.1 への通信の推移

5.3 同一ネットワークへの DNS アンプ攻撃の例

5.1 節，5.2 節では単一の IP アドレスに対する DNS アンプ攻撃を取り上げたが，本節では，観測地点 1，2 で 2013 年 5 月 29 日に観測された同一ネットワーク内の複数の IP アドレスに分散した DNS アンプ攻撃について説明する．

観測された通信の問い合わせ元 IP アドレスは第 1 から第 3 オクテットが同一（xxx.246.165）で，第 4 オクテットのみが異なっており，その値には 1～100 までが用いられていた．IP アドレスの逆引き，及び，WHOIS 情報から，この IP アドレス群一帯は同一のホスティングサービスが保持しており，そのネットワークへの DNS アンプ攻撃であることが推測された．また，この DNS アンプ攻撃では，ripe.net の ANY の問い合わせが悪用されていた．

観測地点 1，2 からこの同一ネットワーク内への通信の pps の時間推移を図 10 にそれぞれ示す．観測地点 1，観測地点 2 ともに通信の開始時刻，終了時刻は同じであり，観測地点 1, 2 からそれぞれ 2～4pps 程度の通信が対象のネットワークに流れ込んでいた．また，問い合わせ元 IP アドレスは，図 11 のように時刻とともに順に変化していた．

また，2 つの観測地点で観測した DNS 通信のヘッダに含まれる ID を調べたところ，5.2 節の例と同様，ID の値は様々であったものの，2 地点間の問い合わせで観測された ID 群は一致していた．また，このネットワークからの通信の IP ヘッダに含まれる TTL は，観測地点 1 では 107～116,観測地点 2 では 101～110 に分散していた．

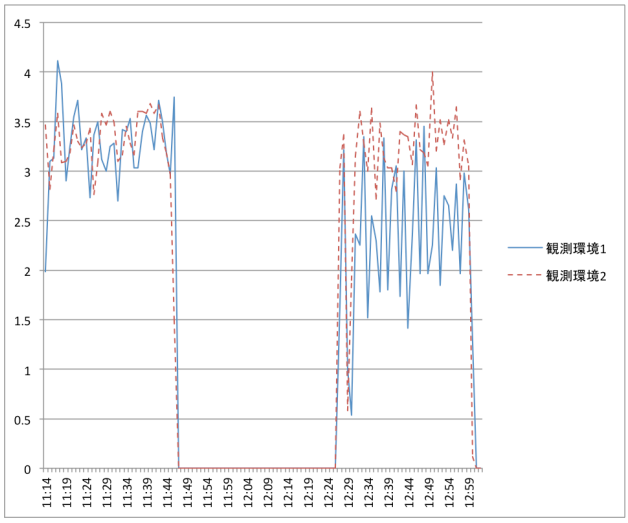

図 10　観測地点 1，2 から xxx.246.165.1～xxx.246.165.100 への通信の推移

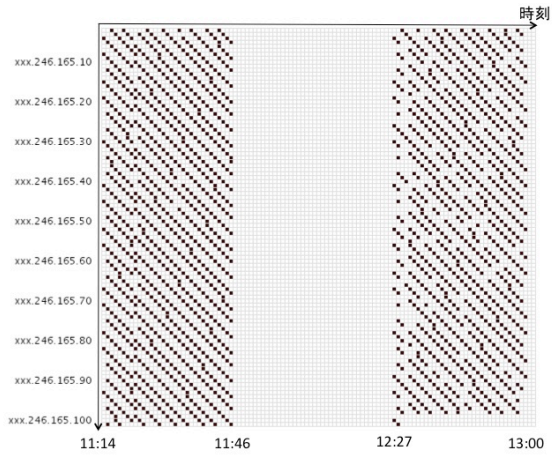

図 11　xxx.246.165.1～xxx.246.165.100 からの問い合わせ
（横軸：時刻，縦軸：問い合わせ元 IP アドレス）

6. 考察

4 章，5 章の分析結果から，提案手法により DNS サーバを悪用する不正活動を観測できることが示されたといえる．5 章では，DNS アンプ攻撃と推測される 4 つの通信の例を取り上げたが，その他にも DNS アンプ攻撃と推測される通信を多数観測した．特に，2013 年以降はその数も増加する傾向が見られ，その DNS アンプ攻撃自体も，単一の IP アドレスを対象としたものから，複数のアドレスからなるネットワークを対象にしたものまで，多様化する傾向にあった．また，攻撃対象となる IP アドレスは，ホスティングサービスのものと推測されるものが多くみられた．

ⓒ2013 Information Processing Society of Japan

1 つの観測地点の通信のみでも，isc.org と ripe.net のドメインを中心とした DNS アンプ攻撃と推測される挙動を多数確認されたが，複数の観測地点での相関も見られたことから，観測地点を増やすことによって，より確度の高い情報が得られると考えられる．

また，5 章の分析結果から，DNS アンプ攻撃の通信に含まれる IP ヘッダの TTL や DNS 通信のヘッダに含まれる ID には，それぞれに傾向が見られることが確認できる．そのため, これらの特徴を用いて DNS アンプ攻撃の更なる分析が可能になると考えられる．

最後に, 観測地点 2 では, 5 月 27 日より iptables の hashlimit 機能を用いたアクセス制限を行ったが，以降の 7 日間に関して，予想に反してアクセス制限により攻撃が減少する実は確認できなかった．

7. まとめと今後の課題

インターネット上に複数の観測地点を用意し，各地点で DNS ハニーポットを運用することにより, DNS サーバを悪用する不正活動を観測，分析する手法を提案し，本提案手法が DNS アンプ攻撃と推測される不正活動を観測可能であることを確認した．

今後は，提案手法を用いた分析を継続するとともに，観測可能性と安全性の 2 つの要件を満たす閾値の検討する予定である．また，ハニーポットやダークネット等の既存の不正活動観測結果との分析結果の突合や DNS アンプ攻撃の予兆となる挙動についても検討していきたい．

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．

参考文献

1) P. Mockapetris, “DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION,” http://www.ietf.org/rfc/rfc1035.txt, last visited 2013/06/10
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,” http://www.jpcert.or.jp/at/2013/at130022.html, last visited 2013/06/12.
3) Open Resolver Project, http://openresolverproject.org/, last visited 2013/06/10.
4) The Spamhaus Project, http://www.spamhaus.org/, last visited 2013/06/10.
5) The DDoS That Almost Broke the Internet, http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet, last visited 2013/06/13.
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,” http://blog.trendmicro.co.jp/archives/7012, last visited 2013/06/10.
7) Honeypots –Definitions and Value of Honeypots-, http://www.tracking-hackers.com/papers/honeypots.html, last visited 2013/06/09.
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.
9) Symantec Official Blog, “DNS レコードを利用する Morto ワーム,” http://www.symantec.com/connect/blogs/dns-morto, last visited 2013/06/12.
10) Ubuntu, http://www.ubuntu.com/, last visited 2013/06/14
11) BIND, http://www.isc.org/downloads/bind/, last visited 2013/06/10.
12) iptables, http://www.netfilter.org/projects/iptables/, last visited 2013/06/13.
13) tcpdump, http://www.tcpdump.org/, last visited 2013/06/14.
14) GeoIP, http://www.maxmind.com/ja/home, last visited 2013/06/16.

付録

付録 A.1　ANY の問い合わせに対する DNS キャッシュサーバの応答

DNS キャッシュサーバは，取得したレコードをキャッシュとして一定期間保持することにより，負荷の軽減や高速化を実現している．キャッシュの保持時間は，資源レコード内に記述された TTL（Time To Live）値により決定されるが, あるドメイン名に対して異なる TTL 値を持つ資源レコードの集合が存在した場合，一部だけがキャッシュから消滅した状態が発生する．そのため，異なる TTL 値を含む資源レコードが存在すると，ANY の問い合わせに対する DNS キャッシュサーバの応答の大きさは時間とともに小さくなる．

例えば，example.com に表 A.1 のような資源レコードが割り当てられていた場合，example.com の ANY の問い合わせに対する DNS キャッシュサーバの応答は図 A.1 のようになる．

表 A.1　example.com の資源レコードの例（クラスは省略）

ドメイン名	レコードの型	TTL	応答
example.com	A	60	1.2.3.4
example.com	NS	120	ns.example.com
example.com	MX	90	mail.example.com

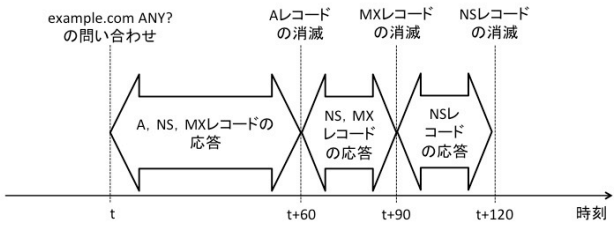

図 A.1　example.com の ANY の問い合わせに対する DNS キャッシュサーバの応答の変化

ⓒ2013 Information Processing Society of Japan