DNS ハニーポットによる DNS Water Torture の観測

牧田 大佑†‡　吉岡 克成†‡　松本 勉†
島村 隼平*　井上 大介‡　中尾 康二‡

†横浜国立大学
240-8501　神奈川県横浜市保土ケ谷区常盤台 79-1
makita-daisuke-jk@ynu.jp, {yoshioka, tsutomu}@ynu.ac.jp

‡情報通信研究機構
184-8795　東京都小金井市貫井北町 4-2-1
{d.makita, yoshioka, dai, ko-nakao}@nict.go.jp

*株式会社 クルウィット
181-0013　東京都三鷹市下連雀 3-34-8　三鷹ハイデンス 509 号
shimamura@clwit.co.jp

あらまし 本稿では，我々のDNSハニーポットが観測した，DNS Water Tortureと呼ばれるDDoS攻撃を分析する．本攻撃は，特定ドメインに属する多量のFQDNの名前解決をDNSキャッシュサーバに要求することにより，そのドメインを管理する権威サーバ，及び，再帰的な名前解決を行なうキャッシュサーバのサービスを妨害する．本攻撃は，その実行方法や傾向等，攻撃の実態には不明確な部分が多いため，本研究を通して攻撃の特徴や傾向を把握することにより，今後の対策技術への応用が期待される．

Observing DNS Water Torture by DNS Honeypot

Daisuke Makita†‡　Katsunari Yoshioka†‡　Tsutomu Matsumoto†
Jumpei Shimamura*　Daisuke Inoue‡　Koji Nakao‡

† Yokohama National University.
79-1, Tokiwadai, Hodogaya-ku, Yokohama-shi, Kanagawa 240-8501, JAPAN
makita-daisuke-jk@ynu.jp, {yoshioka, tsutomu}@ynu.ac.jp

‡ National Institute of Information and Communications Technology.
4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo 184-8795, JAPAN
{d.makita, yoshioka, dai, ko-nakao}@nict.go.jp

* clwit, Inc.
3-34-8-509, Shimo-Renjaku, Mitaka-shi, Tokyo 181-0013, JAPAN
shimamura@clwit.co.jp

Abstract In this paper, we analyze DDoS attack called DNS Water Torture that our DNS honeypots observed. This attack prevents the service of name servers (both authoritative name servers that have the authority of the domains and caching name servers that conduct recursive name resolutions) by requesting a large amount of FQDNs belonging to specific domains. Since this kind of attacks is not well studied or reported, it is expected to develop countermeasures by understanding the trends and characteristics through this study.

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アドレス等の情報の対応付けを管理す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，オープンリゾルバ（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，インターネット上で実行される DDoS 攻撃 (Distributed Denial of Service Attack)の踏み台として利用されている．

我々は，このような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，DNS アンプ攻撃を中心とした不正活動の観測・分析を行なっている [1][2][3]．本稿では，我々の DNS ハニーポットが観測した，DNS Water Torture [4][5][6]と呼ばれる DDoS 攻撃を分析する．本攻撃は，応答の増幅率が高い FQDN（Fully Qualified Domain Name）を用いて通信帯域を圧迫する DNS アンプ攻撃とは異なり，特定ドメインに属する多量の FQDN の名前解決を DNS キャッシュサーバに要求することにより，そのドメインを管理する権威サーバ，および，再帰的な名前解決を行なうキャッシュサーバのサービスを妨害する．

DNS Water Torture は，その実行方法や傾向等，攻撃の実態には不明確な部分が多いため，本研究を通して攻撃の特徴や傾向を把握することにより，今後の対策技術への応用が期待される．

本稿の構成は次の通りである．まず，2 章で DNS Water Torture の概要を説明する．3 章で DNS ハニーポットの構成を説明し，4 章で DNS ハニーポットの観測結果をまとめる．5 章で DNS Water Torture の観測例をまとめ，最後に，6 章でまとめと今後の課題を述べる．

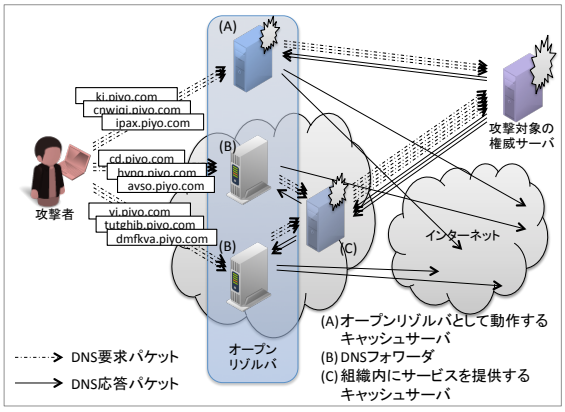

図 1　DNS Water Torture

2　DNS Water Torture[a)]

DNS Water Torture（Slow Drip DDoS 攻撃）[4]とは，特定のドメインに属する多量の FQDN の名前解決をキャッシュサーバに要求することにより，そのドメインを管理する権威サーバのサービスを妨害する DDoS 攻撃である．再帰的な名前解決を行なうキャッシュサーバは，受信した要求に対する応答を自身のキャッシュ内に保持しない場合，権威サーバへの要求を行なう．そのため，あるドメインに属する FQDN を要求毎に変更してキャッシュサーバへ要求する（例えば，*.piyo.com の*の部分を，要求毎に異なる文字列にした FQDN を要求する）と，キャッシュサーバは要求を受信するたびに権威サーバへの要求を行なう．これを多数のキャッシュサーバから継続的に実行されると，権威サーバはその要求を正常に処理できずに，権威サーバからの応答に遅延・損失が発生する．その結果，キャッシュサーバは多量の応答の待ち状態になるため，キャッシュサーバのリソースが枯渇し，障害が発生する．また，同時に，攻撃で発生する多量の要求・応答パケットにより，通信帯域が圧迫され，通信障害につながる．

DNS Water Torture を実行するための踏み台として，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ている．オープンリゾルバの中には，不適切な設定によりオープン

a) Water Torture（水責め）とは，「水を絶えず顔にかけたり，多量に飲ませたりする拷問」である[12]．

リゾルバとして動作するキャッシュサーバ(図 1 の(A))も存在するが，一方で，キャッシュサーバへのフォワーダ機能がオープンリゾルバとしての役割を果たしているネットワーク機器(図 1 の(B))も存在する[7]．後者の機器が多数存在するネットワークでは，DNS Water Torture の発生に伴い，そのネットワーク内にサービスを提供するキャッシュサーバ(図 1 の(C))の通信も増加するため，副次的にキャッシュサーバへの DoS 攻撃にもなる．

DNS Water Torture は，2014 年 2 月頃から海外のフォーラム等で報告されており[8][9]，我々が運用する DNS ハニーポットでも，2014 年 5 月末から攻撃が観測されている．また，国内の ISP が提供する DNS キャッシュサーバにおいても，本攻撃の影響と推測される通信障害が複数報告されている[10][11]．4・5 章で示すように，DNS Water Torture で使用される DNS クエリの送信元 IP アドレスは広い範囲で詐称されるため，その応答パケットはダークネット等でも観測されている．

3 DNS ハニーポット

本章では，我々が運用している DNS ハニーポットの構成と実装例を示す．我々の DNS ハニーポットは，オープンリゾルバとして動作する囮(おとり)の DNS サーバを中心とするシステムであり，オープンリゾルバの視点から DNS アンプ攻撃や DNS Water Torture を観測する．

本稿では，DNS Water Torture による外部への影響を軽減するため，論文[1]の実装に，「DNS コントローラ」を追加した．

3.1 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 2 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 つの要素から構成される．

まず，DNS サーバは外部からの DNS クエリに応答する．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 サーバが不正利用された場合に，通信制御を行なう．そして，DNS ハニーポットマネージャは，DNS サーバと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．

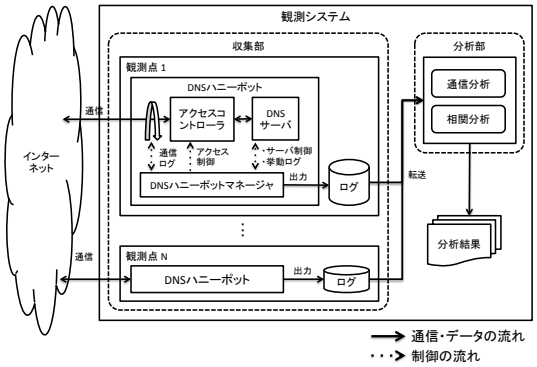

図 2 DNS ハニーポットと観測システム

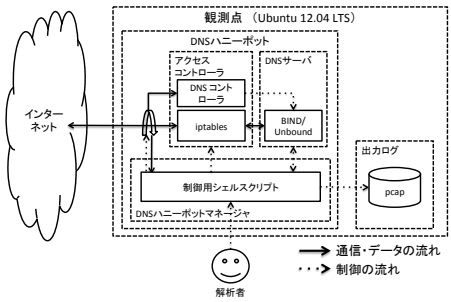

図 3 DNS ハニーポットの実装

ハニーポットを用いて観測を行なう場合，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など，より詳細な分析が可能になる．そこで，DNS ハニーポットの観測においても，図 2 のように，システムを「収集部」「分析部」の二つに分け，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，各観測点では，DNS ハニーポットを用いて通信のログを収集する．収集したログは「分析部」に転送され，そこで各観測点の通信の分析，および，複数点の通信の相関を分析する．

3.2 システムの実装

DNS ハニーポットの実装を図 3 に示す．各観測点に Ubuntu[13]をインストールしたマシンを設置し，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[14]，または，

表 1 DNS ハニーポットの観測環境

センサ名	sensor001	sensor002	sensor003	sensor004	sensor005	sensor006	sensor007
DNS サーバ	BIND	Unbound					
ISP	ISP-A	ISP-B	ISP-C	ISP-D	ISP-E	ISP-F	
観測開始日	2012/10/07	2013/05/13	2014/05/13		2014/05/10		
分析対象期間	2014 年 5 月 1 日(または観測開始日)～7 月 31 日						
通信制御	iptables: /24 ネットワークへの応答を，次の何れかの通信量に制限※1(1pps，6ppm，1pph※2)． DNS コントローラ(2014 年 7 月 10 日以降)：各種パラメータは T_{node}=20，$t_{refresh}$=600，$t_{timeout}$=3600．						
IP アドレスの変更回数と変更日	5 回:2014 年 6 月 2 日，3 日，4 日，5 日，29 日	4 回:2014 年 5 月 11 日，6 月 14 日，29 日，7 月 22 日	2 回:2014 年 5 月 16 日，6 月 6 日	1 回:2014 年 6 月 6 日	なし	1 回:2014 年 6 月 5 日	1 回:2014 年 6 月 5 日

※1 正確には，最初の 5 または 10 パケットを許可し，それ以降の通信量を上記の値に制限している．
※2 pps = packet per second, ppm = packet per minute, pph = packet per hour.

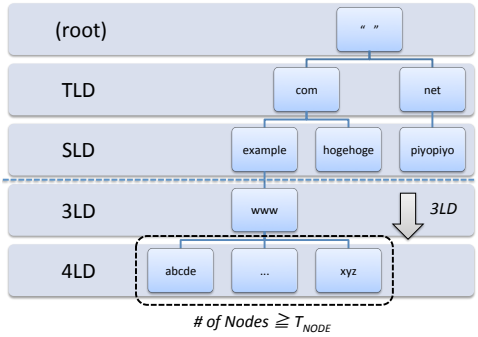

図 4 ドメイン名空間と DNS コントローラ

Unbound[15]，アクセスコントローラとして iptables[16]，及び，DNS Water Torture 対策のために導入した DNS コントローラ(3.3 節参照)，DNS ハニーポットマネージャとして制御用のシェルスクリプトを用いて実装した．また，DNS サーバは，インターネット上の任意のホストから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，解析者が制御できるようにした．通信ログの取得には tcpdump[17]を使用し，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．

3.3 DNS コントローラ

本稿における DNS コントローラの実装は以下の通りである．まず，DNS ハニーポットで観測される通信をリアルタイムで取得し，観測された FQDN を木構造で表現されるドメイン名空間に追加する．次に，木構造を探索し，あるノードの子ノードの数が 3LD[b)]より深いレベルで閾値 T_{node} を超えたドメインを DNS Water Torture のドメインとして検知する．最後に，検知されたドメインに属する FQDN の応答として NXDOMAIN を返すように，DNS サーバの設定を変更する．ただし，DNS Water Torture では，多量の FQDN が要求され，ドメイン名空間の木構造が非常に大きくなるため，木構造を $t_{refresh}$ 秒間隔でリセットするようにし，上記で変更した応答は，攻撃観測終了の $t_{timeout}$ 秒後に，再度設定を書き換え，通常の応答を返すようにした．なお，DNS コントローラは，Python[18]，及び，そのライブラリの pcapy[19]，dpkt[20]を用いて実装した．

4 DNS 通信の観測

4.1 観測環境

本稿における DNS ハニーポットの観測環境を表 1 に示す．我々は 7 台の DNS ハニーポット(センサ)を運用しており，各センサは日本国内の ISP ネットワークで動作している．本稿では，2014 年 5 月 1 日(それ以降に観測を開始したものは，観測開始日)から 7 月 31 日までの約 3 ヶ月間に，DNS ハニーポットが観測した DNS 通信を分析する．

b) ドメイン名空間のノードは，ルートから近い順にトップレベルドメイン(TLD)，セカンドレベルドメイン(SLD)，サードレベルドメイン(3LD)…と表現される．TLD の取得には，ICANN[22]の承認が必要であり，一般の組織は SLD 以下を取得するため，現在の DNS Water Torture で変更される文字列は 3LD より深いレベルの部分になる．

表 2 DNS ハニーポットが観測した DNS クエリの概要

センサ名	sensor001	sensor002	sensor003	sensor004	sensor005	sensor006	sensor007
DNS クエリ数 （一日平均）	43,503,558 (472,865)	173,693,901 (1,887,977)	208,461,285 (2,605,766)	13,609,367 (170,117)	114,213,058 (1,376,061)	56,062,081 (675,447)	821,433,712 (9,896,792)
FQDN 数	1,156,155	1,595,345	1,381	337	863	10,661	520,139,438
送信元 IP アドレス数	1,572,670	693,148	84,289	34,649	41,846	23,443	586,297,891

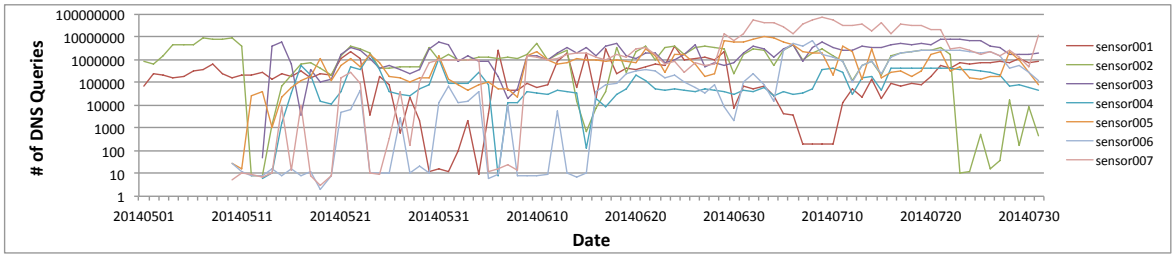

図 5 DNS クエリ数の推移（日ごと，縦軸対数）

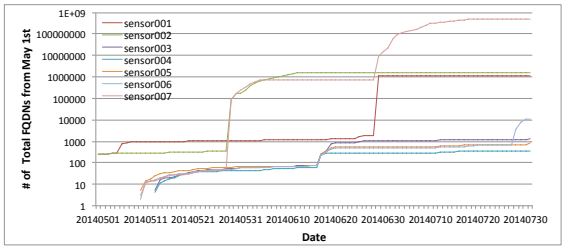

図 6 2014 年 5 月 1 日以降の FQDN の累積個数の推移（日ごと，縦軸対数）

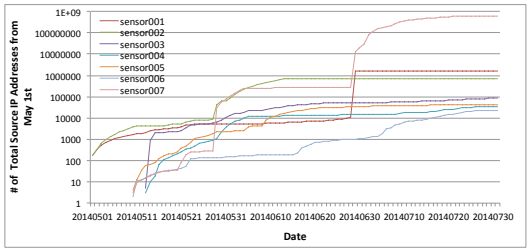

図 7 2014 年 5 月 1 日以降の送信元 IP アドレスの累積個数の推移（日ごと，縦軸対数）

4.2 観測結果

分析対象期間中に DNS ハニーポットが観測した DNS クエリの概要を表 2 に，DNS クエリ数の日ごとの推移を図 5 に示す．各センサは一日平均で数十万から数百万の DNS クエリを観測しており，特に，sensor007 では期間中に 8 億以上の DNS クエリを観測した．また，各センサが観測した FQDN 数と送信元 IP アドレス数を比較すると，sensor001・sensor002・sensor007 は他のセンサよりも多数の FQDN・IP アドレスを観測しており，特に，sensor007 では期間中にそれぞれ 5 億以上の FQDN・IP アドレスを観測した．

次に，各センサが観測した FQDN と送信元 IP アドレスの累積個数の推移（2014 年 5 月 1 日基準）を図 6，図 7 に示す．sensor003～sensor006 が観測した FQDN・IP アドレスの累積個数は，多少の誤差はあるものの，同じように緩やかに増加した．一方，sensor001 は 6 月 29 日に，sensor002 は 5 月 29 日から 6 月 14 日に，sensor007 は 5 月 29 日から 6 月 4 日，6 月 29 日から 7 月 23 日にかけて，観測した FQDN・IP アドレスの数が急増した．この時期に，これらのセンサが観測した通信を分析した結果，DNS Water Torture と推測される多量の DNS 通信が確認された[c]．なお，本稿では，分析対象期間中に，3LD 以下の子ノードの数が 100 を超えたドメインを，DNS Water Torture で使用されたドメインとして分析する．

DNS Water Torture の観測例は 5 章で取り上げ，本章では，DNS ハニーポットが観測した DNS Water Torture の特徴を分析する．

4.3 DNS Water Torture の分析

分析対象期間中に，DNS ハニーポットは計 245 のドメインで DNS Water Torture と推測される通信を観測した．本節では，これらの通信

[c] sensor001 では 6 月 29 日に，sensor002 では 6 月 14 日に，sensor007 では 6 月 4 日に，センサの IP アドレスが変更されたため， DNS Water Torture が観測されなくなったと推測される．

表 3 DNS ハニーポットが観測した DNS Water Torture の概要(クエリ数上位 5 位)

観測したセンサ	FQDN(*は任意の文字列)※1	クエリ数	FQDN 数	送信元 IP アドレス数	権威サーバ(2014 年 8 月 18 日現在)	応答(2014 年 8 月 18 日現在)※2
sensor007	*.www.tanw■.com	96,365,281	68,190,123	93,851,060	権威サーバ A	NOERROR
sensor007	*.st.xingx■.com	42,916,882	32,322,982	42,409,252	権威サーバ B	NXDOMAIN
sensor007	*.wushuang.ta■.com	38,359,321	27,189,996	37,956,885	権威サーバ C	NOERROR
sensor007	*.71.apple■.com	23,736,513	17,882,117	23,580,914	権威サーバ D	NOERROR
sensor007	*.wwmd.9■.net	23,682,112	17,844,634	23,532,045	権威サーバ C	NOERROR

※1 ドメインの一部をマスキングしている. 以降のドメインも, 文字列の一部をマスキングしている.
※2 FQDN のドメイン部分の A・NS・SOA レコードを問い合わせ, その応答に含まれる情報から判断した.

の特徴を分析する.

4.3.1 FQDN と送信元 IP アドレス

各センサが観測した攻撃のうち, クエリ数の多い上位 5 つの攻撃の概要を表 3 に示す. 観測された DNS クエリ数, FQDN 数, IP アドレス数から, これらの攻撃ではクエリ毎に異なる FQDN・IP アドレスが使用される傾向にあることがわかる. この特徴は, DNS Water Torture の通信に共通していたが, FQDN のホスト部(表 3 の*の部分)の長さや, 送信元 IP アドレスの範囲は, 攻撃によって偏りが存在した.

また, 送信元 IP アドレスは, 広い範囲の IP アドレスが使用されており, その IP アドレスの数からも, 攻撃者がこれらの全ての IP アドレスを保持できる可能性は低い. そのため, これら送信元 IP アドレスの多くは詐称されているものと考えられる. 実際, sensor007 で観測された IP アドレスの中には, NICTER[21]が保有するダークネット観測網の IP アドレスも含まれており, そのダークネットセンサでは, sensor007 からの応答パケットも観測されていた.

4.3.2 ドメインと権威サーバ

DNS Water Torture で使用された 245 個のドメインのうち, 2014 年 8 月 20 日現在, whois 情報を取得できたドメインは 189 個で, そのうち 165 個は中国で取得されたものと推測される. これらのドメインの中には正規の目的で使用されていると推測されるドメインも存在したが, 2014 年 8 月 18 日現在では使用されていないもの(NXDOMAIN)や権威サーバから応答がないものも存在した. また, 攻撃に使用されたドメインの中には, 権威サーバが共通のものも存在した. 権威サーバに関する情報は, 2014 年 8 月 18 日に取得したため, 攻撃発生時とは異なる可能性もあるが, 攻撃者は異なるドメインを用いて, 同一の権威サーバを狙った攻撃を実行したことが予想される.

4.3.3 通信量と権威サーバからの応答

DNS ハニーポットが観測した DNS Water Torture に関する単位時間の通信量は, 5 月 29 日からの攻撃では 0～5pps 程度であったが, 6 月 29 日からの攻撃では数百 pps に達した. また, 攻撃時の権威サーバから DNS ハニーポットへの応答は, NXDOMAIN や SERVFAIL 等が多く, 応答パケットがハニーポットに到達しない DNS クエリも多数存在した.

4.4 考察

我々が運用している 7 台の DNS ハニーポットのうち 3 台において, DNS Water Torture と推測される通信が観測された. しかし, これらのハニーポットでは, IP アドレス変更後, 攻撃が観測されない傾向にあったことから, 攻撃者はオープンリゾルバのリストを頻繁には更新していないことが予想される. また, 攻撃が観測されなかったハニーポットも複数存在していたことから, 攻撃者は一部のオープンリゾルバしか悪用していないことが推測される. 以上のことから, 今後, 攻撃者がより効率的な攻撃を実行することにより, 被害が更に深刻化する可能性があると考えられる.

また, DNS Water Torture は権威サーバにへの攻撃と考えられているが, キャッシュサーバへの攻撃としても有効である. そのため, 攻撃者が権威サーバを用意して意図的に応答を遅延・損失させたり, 増幅効果の高い応答を用意したりすることで, キャッシュサーバの負荷を

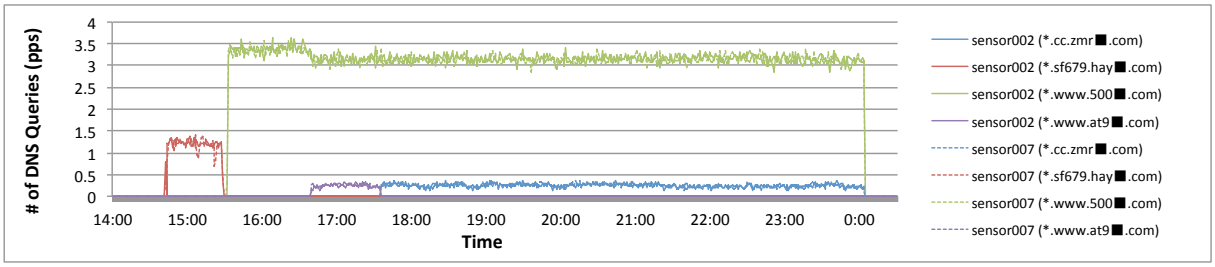

図 8 DNS クエリ数の推移（2014 年 5 月 29 日～30 日）

表 4 各ドメインの DNS クエリの概要

	*.cc.zmr■.com		*.sf679.hay■.com		*.www.500■.com		*.www.at9■.com	
	sensor002	sensor007	sensor002	sensor007	sensor002	sensor007	sensor002	sensor007
DNS クエリ数	5,975	6,124	3,328	3,204	97,554	97,366	850	912
FQDN 数	5,395	5,532	3,328	3,204	83,262	83,154	824	882
送信元 IP アドレス数	4,086	4,131	1,066	1,046	25,861	25,499	588	620

高めたり，その通信帯域を圧迫したりする DoS 攻撃が実行されることも予想される．

我々が観測する DNS ハニーポットでは，2014 年 7 月 23 日以降，2014 年 8 月 24 日現在まで，DNS Water Torture と推測される通信は観測されていない．しかし，NICTER のダークネット観測網では，2014 年 8 月 24 日現在も，DNS Water Torture の跳ね返りと推測されるパケットが観測されているため，DNS Water Torture は継続していると考えられる．

最後に，DNS コントローラを DNS ハニーポットに導入した結果，DNS Water Torture の影響で不安定だった DNS ハニーポットの動作が安定した[d)]ことに加え，DNS ハニーポットは DNS Water Torture に関連する権威サーバへの要求を送信しなくなったため，外部に与える影響を軽減しつつ観測を行なうことが可能になった．DNS コントローラの導入が以降の観測に与えた影響は不明だが，導入後も継続して攻撃が観測されていたことから，観測への影響は小さいと推測される．なお，DNS コントローラで設定した各種パラメータの値の妥当性の検証は不十分であるため，これらの閾値の検討を今後行なう予定である．

5 DNS Water Torture の観測例

本章では，DNS ハニーポットが 2014 年 5 月 29 日から 30 日にかけて観測した DNS Water Torture の事例を分析する．

本攻撃は，2014 年 5 月 29 日 14 時 33 分頃から翌 30 日の 0 時 4 分頃まで，sensor002 と sensor007 で観測された．この期間に観測された 4 種類のドメインのクエリ数の推移を図 8 に，各ドメインの DNS クエリの概要を表 4 に示す．

まず，本攻撃では，*.sf679.hay■.com（*は任意の文字列）を用いた DNS クエリが 14 時 33 分から 15 時 28 分まで観測され，次に，*.www.500■.com のクエリが 15 時 33 分から 0 時 4 分まで継続して観測された．その途中，*.www.at9■.com のクエリが 16 時 40 分から 17 時 35 分まで観測され，その直後の 17 時 36 分から 0 時 4 分まで，*.cc.zmr■.com のクエリが観測された．

DNS クエリの送信元 IP アドレスは，一部に偏りが存在したものの，広い範囲の IP アドレスが使用されており，これらの多くのクエリの送信元 IP アドレスは詐称されていたことが推測される．また，この期間の DNS クエリの IP ヘッダに含まれる TTL（Time To Live）値は，sensor002 では 228～243 に，sensor007 では 229～241 に分散しており，DNS クエリの実際の送信元ホストも多数存在したことがわかる．以上のことから，この攻撃にはボットに感染した

d) DNS ハニーポットで動作する DNS サーバは，再帰的な名前解決を行なう DNS キャッシュサーバであるため，DNS Water Torture の影響で DNS サーバプログラムが異常終了する現象が発生していた．

マシンが使用されていることが推測される.

6 まとめと今後の課題

本稿では，我々の DNS ハニーポットが観測した，DNS Water Torture と呼ばれる DDoS 攻撃の通信を分析し，攻撃に使用される FQDN や送信元 IP アドレス，ドメイン等の特徴を示した.

今後の課題としては，DNS Water Torture の分析を継続するとともに，DNS ハニーポットの観測結果とダークネットセンサ等の観測結果との相関を分析し，よりマクロな視点からこの攻撃を分析したいと考えている. また，DNS Water Torture を実行するマルウェア等の実態の解明や，対策技術の研究開発にも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.

参考文献

[1] 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，コンピュータセキュリティ研究会（CSEC），2013-CSEC-62，2013.

[2] 筒見拓也，野々垣嘉晃，田辺瑠偉，牧田大佑，吉岡克成，松本勉：複数種類のハニーポットによる DRDoS 攻撃の観測，情報処理学会，コンピュータセキュリティ研究会（CSEC），2014-CSEC-65，2014.

[3] 牧田大佑，吉岡克成，松本勉：DNS アンプ攻撃の早期対策を目的とした DNS ハニーポットとダークネットの突合分析，電子情報通信学会，2014 年暗号と情報セキュリティシンポジウム（SCIS2014），2014.

[4] Secure64 Software Corporation: Water Torture: A Slow Drip DNS DDoS Attack, available from <https://blog.secure64.com/?p=377> (accessed 2014-08-15).

[5] DNS Amplification Attacks Observer: Authoritative Name Server Attack, available from <http://dnsamplificationattacks.blogspot.jp/2014/02/authoritative-name-server-attack.html> (accessed 2014-08-15).

[6] A10 Networks, Inc: ランダム DNS クエリー攻撃（DNS Water Torture）対策について，入手先<http://www.a10networks.co.jp/files/140731/dns_water_torture.pdf>（参照 2014-08-15）.

[7] Japan Vulnerability Notes (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 2014-08-15）.

[8] GOSSAMER THREADS: random dns queries with random sources, available from <http://www.gossamer-threads.com/lists/nanog/users/169123> (accessed 2014-08-15).

[9] SPICE WORKS: What Does a DNS Amplification DDoS attack look like?, available from <http://community.spiceworks.com/topic/441721-what-does-a-dns-amplification-ddos-attack-look-like> (accessed 2014-08-15).

[10] Cyber Force Center, NPA JAPAN（@police）：日本国内のオープン・リゾルバを踏み台とした DDoS 攻撃発生に起因すると考えられるパケットの増加について，入手先< http://www.npa.go.jp/cyberpolice/detect/pdf/20140723.pdf>（参照 2014-08-15）.

[11] JPCERT/CC: インターネット定点観測レポート（2014 年 4～6 月），入手先< https://www.jpcert.or.jp/tsubame/report/report201404-06.html>（参照 2014-08-15）.

[12] 三省堂大辞林（第三版）：水責め，2006.

[13] Ubuntu, http://www.ubuntu.com/.

[14] BIND, http://www.isc.org/.

[15] Unbound, http://unbound.net/.

[16] iptables, http://www.netfilter.org/.

[17] tcpdump, http://www.tcpdump.org/.

[18] Python, https://www.python.org/.

[19] pcapy, http://corelabs.coresecurity.com/.

[20] dpkt, https://code.google.com/p/dpkt/.

[21] NICTER, http://www.nicter.jp/.

[22] ICANN, https://www.icann.org/.