「マルチメディア，分散，協調とモバイル
(DICOMO2017)シンポジウム」 平成29年6月

ダークネット観測データを用いた接続機器の調査と分類

杉生 貴成[1] 佐々木 良一[1] 猪俣 敦夫[1]

概要: 近年，IoT(Internet of Things)を用いた「DNS アンプ攻撃」のような大規模な DDoS(distributed Denial of Service)攻撃が増加している．DNS アンプ攻撃を成立させるため，事前に広範囲にオープンリゾルバの探索スキャンがされる傾向がある．広範囲に渡るスキャンの傾向を捉える手段としてダークネット分析がある．本論文はダークネットの DNS（53/UDP）パケットを抽出して到着間隔や総パケット数などを特徴として同様の動きをするボットネットを可視化した．具体的には，予め対象とする IP アドレスに対して DNS 逆引きを行い調査組織の IP アドレスと分けた．また，観測された IP アドレスに対してアクティブスキャンを行い DNS アンプ攻撃時に踏み台とされる機器の調査を行った．さらに対象とする IP アドレスに対してオープンリゾルバ状態かどうかの判別も行った． 結果，サーバ以外では家庭用のルータが多くを占め Web カメラや DVR などの IoT 機器も見つかった．市販されている多くのルータは標準で DNS をサポートすることから，本論文ではユーザによる設定の不備等について言及した．

Survey and classification of connected equipment using Data observation Darknet

TAKAAKI SUGIU RYOICHI SASAKI ATSUO INOMATA

1. はじめに

近年，IoT（Internet of Things）機器が増加しており，シスコシステムズによるインターネットに接続されるデバイス数を調査した結果 2003 年では世界人口 63 億人に対して接続デバイス数が 5 億だが，指数関数的に増加し 2015 年では世界人口 72 億人に対して接続デバイス数が 250 億と 1250 倍に増え，1 人当たりの接続デバイス数が 3.47 となった．それらのデバイスの中にはセキュリティアップデートやパスワード設定などが十分にされていないため，容易にマルウェアに感染しボットと化している．多くのデバイスを踏み台にした DDoS(Distributed Denial of Service)攻撃は規模が大きくなり無視できない問題となっている．

近年，特に著しい被害をもたらしている DDoS 攻撃の 1 つに DNS アンプ攻撃がある．本論文では DNS アンプ攻撃に踏み台として悪用されるオープンリゾルバに対してアクティブスキャンを行い機器の調査を行った．また，非オープンリゾルバ状態の機器に対しても同様の分析を行った．ここで、オープンリゾルバとは DNS の名前解決を行う機器のうち，アクセス元を限定しない不特定多数のインターネット全体から利用可能な状態のものである．

DNS アンプ攻撃が発生する前にオープンリゾルバを探索するスキャンが事前に観測される可能性がある．そのためインターネット空間を広範囲に捉えたデータが必要だが，本論文は NICT[1]が観測したダークネットデータセット 2016 を使用する．これは，NICT が観測しているダークネットのうち，4096 の連続 IP アドレスに届いたトラフィックデータであり，マルウェア対策人材育成ワークショップ 2016[1]にて配布されたデータセットの一つである．

2. 攻撃事例

IoT 機器を用いた DDoS 攻撃の事例として 2016 年 8 月下旬～9 月上旬にかけて大手企業を含む複数のサイトにつながりにくい状況が起きた．標的とされたサイトへ大量の応答があり，DNS アンプ攻撃と報告された．同年 9 月，セキュリティ専門である Brain Krebs 氏のブログ[2]である「Krebs on security」が約 620Gbps 攻撃を受け話題になった．この攻撃は Mirai というマルウェアに感染したボットネットによるものと指摘されている．Mirai は Router や Web Camera・DVR など IoT 機器をターゲットとし脆弱なパスワードやデフォルトパスワードを利用して感染する．

JPCERT/CC[2]によれば，2016 年第四半期の定点観測レポート[3]において DNS の応答パケットが国内外の多数の IP アドレスから受信している．受信したパケットを分析したところ，存在しないランダムなホスト名の名前解決要求パケットに対する応答パケットであることが分かった．これは，DNS 水責め攻撃（ランダムサブドメイン攻撃）と推測される．

1 東京電機大学

3. 関連研究

ダークネットにて観測された機器へアクティブスキャンをする関連研究として笠間らの研究[4]があげられる．この研究ではダークネット観測により取得した約 24 万の IP アドレスに対して調査した．特に，Telnet(23/TCP)を狙う攻撃を行うホストを調べるためパッシブ OS フィンガープリントを用いて OS の判定を行った．結果，Linux 系に対する攻撃活動と Windows OS に感染したマルウェアによる攻撃活動とは異なることが分かった．また，攻撃元ホストに対して Nmap によるポートスキャンを実施し，多くがルータやネットワークカメラなどの IoT 機器だということが判明した．我々の研究との違いは着目したプロトコルである．今回，我々は DDoS 攻撃の中で特に DNS を用いた攻撃を調べるため DNS (53/UDP) に焦点を当てて調べた．DNS に絞ることにより DNS を狙った攻撃またはオープンリゾルバ状態の機器からの攻撃が観測できる．

ダークネット観測データを分析というと福島ら研究[5]があげられる．この研究は長期間にわたって少量のパケットしか観測されないような気づきにくい攻撃を検知するため，平均送信パケット数と送信元 IP アドレスの出現頻度に着目する手法を提案した．また，クラスタリング分析によって抽出した攻撃パターンから同じような特徴を持った攻撃を抽出・分離することができた．我々の研究との違いは攻撃パターンを調べる際の特徴である．著者らはスロースキャンを調べるため IP アドレスの頻度と平均送信パケット数に着目しクラスタリングを行ったが，我々は IP アドレスの攻撃間隔と頻度を特徴とし，クラスタリングによる分類はしていない．

4. DNS アンプ攻撃

4.1 オープンリゾルバ

オープンリゾルバとは DNS の名前解決を行う機器のうち，アクセス元を限定しない不特定多数のインターネット全体から利用可能な状態のものである．さらに，再帰的に名前解決ができ，応答結果を対象とする DNS サーバに回答できる

4.2 DNS アンプ攻撃

DNS アンプ攻撃について説明する．図 1 において青矢印が問い合わせで赤矢印が応答である．攻撃者はまず，乗っ取ったサーバまたは攻撃用の DNS サーバを用意する．そして表 1 のように悪意のある DNS レコードを登録する．

表 1　ゾーンファイルレコード例

example.com　21600　IN　A　1.1.1.1
example.com　21600　IN　A　1.1.1.2
example.com　21600　IN　A　1.1.1.3

次に，攻撃者はオープンリゾルバ状態の機器を踏み台として悪意のあるレコードを登録してある DNS サーバに対して DNS の問い合わせを行う．乗っ取られた DNS サーバは悪意のあるレコード返し，オープンリゾルバ状態の機器は悪意のあるレコードをキャッシュする．その様子を図 1 に示す．

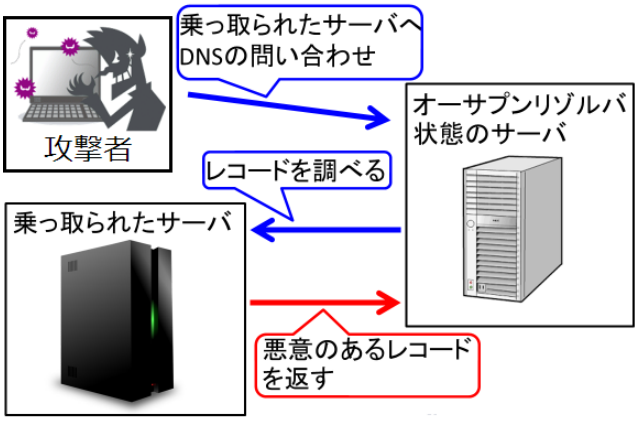

図 1　DNS アンプ攻撃手順 1

最後，攻撃者が攻撃対象のサーバになりすましてオープンリゾルバ状態のサーバへ攻撃されたサーバの情報の問い合わせを行う．問い合わせが攻撃対象サーバからだと勘違いしたオープンリゾルバ状態のサーバは，攻撃者が作った悪意あるレコードのキャッシュを攻撃対象のサーバに送信することで攻撃が成立する．その様子を図 2 に示す．

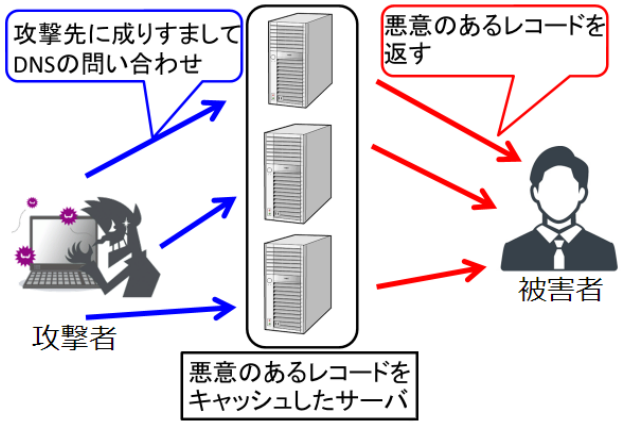

図 2　DNS アンプ攻撃手順 2

5. ダークネット観測

ダークネットとはインターネット上で到達可能な IP アドレスのうち未使用な IP アドレス群である．ダークネット

2 JPCERT コーディングセンター

で観測されるトラフィックは多くがマルウェアなどに感染した機器からのスキャンやバックスキャッタなど攻撃活動に起因するため，ダークネットを監視・分析することで大規模なサイバー攻撃が起きるきっかけやボットネットの攻撃活動を把握することができる．ここで，DNS（53/UDP）に絞ったダークネット空間のトラフィックを図 3 に示す．

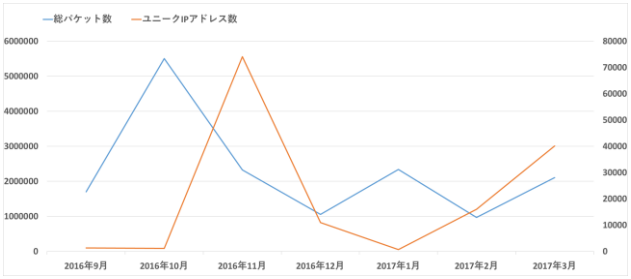

図 3　ダークネット観測統計（53/DNS）

6.　調査手法

使用するデータは NICTER[3] によって観測された研究用ダークネットデータセットであり，本論文では 2016 年 9 月から 2016 年 12 月までのデータを対象とする．

(1) データセットからパケットデータを抽出する際，送信元ポート番号が 53 番，または送信先ポート番号が 53 のトラフィックのみ抽出する．

(2) (1)で抽出したトラフィックの IP アドレスに対してオープンリゾルバ状態の有無を調べる．その際「openresolver.com」[6]というサイトを使用し調べる．dig コマンドを使用し調査する．その際，検索に利用するドメイン名を「test.openresolver.com」と指定し，検索タイプを「TXT」に指定する．具体的には「dig +short test.openresolver.com TXT @調査先 IP アドレス」となる．調査機器がオープンリゾルバ状態であれば「open-resolver-detected」と応答がくる．このようにして IP アドレスをオープンリゾルバ・非オープンリゾルバ・応答なしの 3 種類に分類する．

(3) (2)で分類した IP アドレスのうちオープンリゾルバの集団に対してポートスキャンを行う．ポートスキャンを行う際，オプションの指定として「-sV（ソフトウエア名とバージョンの表示）」と「-O（OS の検出）」を指定する．また，Nmap[4] には NSE があり「--script banner」も加えて実行することでバナー情報も取得できる．

(4) ポートスキャンにより，開いているポート番号，サービス名，OS の推定からデバイスを推測し分類する．ポートスキャンの実行例の一部を図 4 に示す．図 4 より開いているポート番号やサービスの名前，情報から調査したデバイスは MikroTik 社のルータだと分かる．

```
25/tcp   filtered smtp
53/tcp   open     domain         MikroTik RouterOS
80/tcp   open     http           MikroTik router co
1723/tcp open     pptp           MikroTik (Firmware
2000/tcp open     bandwidth-test MikroTik bandwidth
```

図 4　ポートスキャン実行例

7.　調査結果

7.1　送信元機器一覧

ポートスキャンによる機器の分類結果を表2に示す. ポートスキャンによる調査はダークネットに飛来する機器の傾向を捉えるためとし，本論文で扱う期間に対して全ては行わず，2016年の9月～10月のみとする．

表 2　ポートスキャン結果

機器	件数
サーバ	132
ルータ	87
プリンタ	5
ネットワークカメラ	3
NAS	2
DVR	2
ロードバランサ	2
判別不能	86
Block	124

関連研究で述べた笠間らの研究[4]では，ダークネット空間中のTelnet（23/TCP）とHTTP（80/TCP）で収集されたIPアドレスに対してポートスキャンを行った．判別する方法としてバナー情報に含まれる文字列からの推測やHTMLタイトル情報，WWW-Authenticate，Serverヘッダなどから判断している．結果，最も多い機器がDVRであり次にルータ，ネットワークカメラ，ゲートウェイ，サーバ，その他の順であった．

ダークネット空間中のDNS（53/UDP）で収集されたIPアドレスに対してポートスキャンによる調査を行ったところ，サーバと思われる機器が最も多く次にルータだった．またプリンタやネットワークカメラ、NASなど少数だが発見することができた．関連研究との調査結果の違いだが，関連研究ではTelnetとHttpがサービスとして稼働している機器を対象としそれらのプロトコルは多くの汎用的な機器に備わっているため，このような結果が出た．また，我々の調査結果でサーバやルータが多く見つかったのは，それらの多くは標準でDNSをサポートしているためと考えられ，設定の不備が疑われる．

7.2　オープンリゾルバ数

次にオープンリゾルバ，非オープンリゾルバ状態の総パケット数とユニーク IP アドレス数の調査結果を表 3 に示す．総パケット数は 2016 年 10 月が最も多いが，ユニーク IP アドレス数は 2016 年 11 月が最も多い．オープンリゾルバ状態の IP アドレス数が最も多い月は 2016 年の 11 月である．

3　Network Incident Analysis Center for Tactical Emergency Response

4 ネットワーク調査ツールおよびポートスキャナ

表 3　結果

date	Open total	Non open total	Open unique	Non open unique
2016/9	421,867	1,153,808	131	695
2016/10	3,680,839	1,820,392	270	850
2016/11	102,009	4,426,163	38,222	35,853
2016/12	6226	1,050,258	5,347	5,592
2017/1	0	2,336,967	0	655
2017/2	14,787	954,041	13,461	2,585
2017/3	728,599	1,379,392	21,301	18,839

8.　詳細分析

8.1　2016 年 11 月の動向

2016 年 11 月は調査期間中最もオープンリゾルバ状態の IP アドレス数が多く異常な月と言える．よって 11 月について詳細な結果を示す．11 月の DNS パケットの総数は 2322954，ユニークな IP アドレス数は 74075 件であった．総パケット数は 9～10 月と比べて減少しているが，ユニークな IP アドレス数が約 66 倍に増加し 74075 件であった。これは明らかに異常な値である．JPCERT/CC のインターネット定点観測レポート(2016 年 10～12 月)[3]によれば，存在しないランダムなホスト名の名前解決要求パケットに対する応答パケットが多数受信した．この攻撃はランダムサブドメイン攻撃，または DNS 水責め攻撃と考えられている．また，オープンリゾルバに送信された名前解決要求パケットに対する応答パケットと推測できる．

図 5 に 2016 年 11 月のダークネット統計データ(53/DNS)を示す．日毎にユニーク IP アドレスと総パケット数を見ると 11 月 28 日から急激に増加していることが分かる．9，10 月同様にオープンリゾルバがどうか分類する．ただし，11 月は異常な月であるため日毎にカウントする．図 6 に日毎のオープンリゾルバのユニーク IP アドレス数と総パケットの図を示す．ユニーク IP アドレス数と総パケットの差が少ないことからオープンリゾルバである IP アドレスは多くのパケットを送信してないことが分かる．最も多くのオープンリゾルバが現れた 11 月 28 日を注目して見ても 1 つの IP アドレスは平均して約 1.3 個のパケットしか発してない．対して，図 7 に日毎の非オープンリゾルバのユニーク IP アドレス数と総パケットの図を示す．ユニーク IP アドレス数と総パケットの差が大きいことから 1 つの IP アドレスが多くのパケットを送信していると分かる．同様に 11 月 28 日に注目して見ると 1 つの IP アドレスは平均して約 3.0 個のパケットを発していることが分かる．

また，11 月は 18 日～21 日と 28 日～30 日はユニーク IP アドレス数が増加しているが，増え方や総パケット数とユニーク IP アドレス数の比が大きく異なるため，別の手法で見てみる．送信元ポート番号が 53 で宛先ポート番号がランダムなハイポートな場合，「DNS 応答パケット」，送信元がランダムなハイポートで宛先ポート番号 53 の場合「DNS 問い合わせパケット」と判断する．また，そのパケットがオープンリゾルバ状態かどうかでも判断した結果を表 4 に示す．11 月 1 日～11 月 17 日までは多くのパケットが DNS 問い合わせパケットであるのに対して，11 月 18 日～11 月 21 日はオープンリゾルバ状態の IP アドレスからのパケットが急激に増えている．オープンリゾルバと非オープンリゾルバの割合は，およそ 80：1 でオープンリゾルバ状態の IP アドレスが多数を占めているのが分かる．それに対して 11 月 28 日～11 月 30 日は非オープンリゾルバ状態の IP からのパケット急激に増えている．前者はオープンリゾルバ状態の IP アドレスから多数きていることから反射型の攻撃と推測でき，後者は非オープンリゾルバ状態のパケットが多くを占めることから何らかの探索を行っていると推測される．

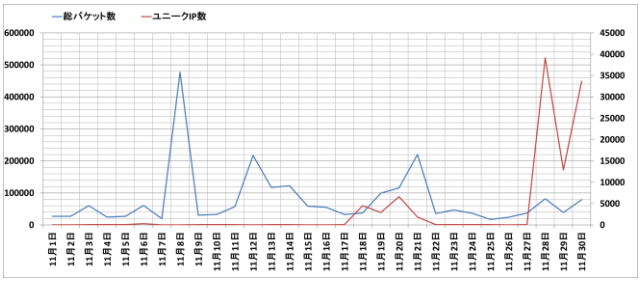

図 5　2016 年 11 月　ダークネット観測統計（53/DNS）

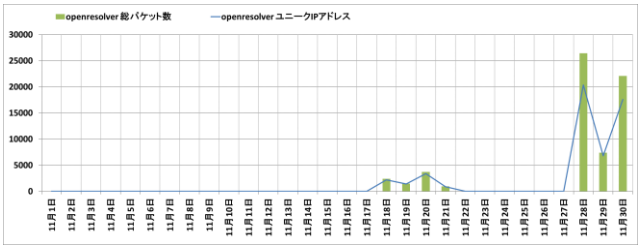

図 6　2016 年 11 月　オープンリゾルバ

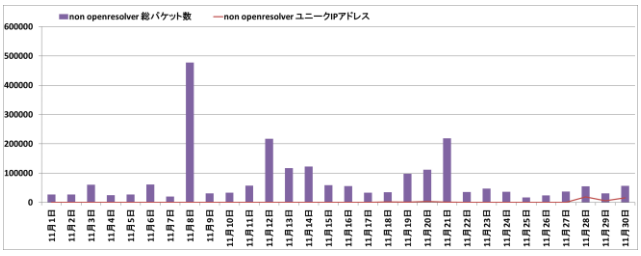

図 7　2016 年 11 月　非オープンリゾルバ

8.2　詳細分析結果の可視化

ダークネット空間上のボットネットやDNSアンプ攻撃の可視化に関する研究として，土性らの研究[7]がある．彼らは可視化を行う際，IPアドレスに出現順にソートしラベル

を付ける．しかし，shodan[8]やShadowsever[9]など機械化された調査組織らしきボットのスキャンがノイズとなり表れてしまう．そこで我々の研究では可視化をする際，対象とするIPアドレスに対してドメインの逆引きをしてIPアドレスに割り当てられているドメインを調べる．そして表6に示すドメインが存在した場合，調査組織と判断する．

表 6　調査組織のドメイン

ドメイン
.rapid7.
.edu.
.shadowserver.
.shodan.
.censys.
. openresolverproject.
.google.
.dnsserach.

ダークネット空間から取得したIPアドレスをオープンリゾルバ・非オープンリゾルバに分類し，平均到達間隔（Sec）と総パケット数を特徴として可視化する．2016年9月の結果を図8に示す．次に表6にしたがって調査組織を分類した結果を図9に示す．黒い点は調査組織のドメインと判断したIPアドレスである．

調査組織はプログラムによって定期的に一定の間隔・パケット数でスキャン行為を行っていると言える．また，赤色の点はオープンリゾルバ状態のIPアドレスであるが，パケットの到達間隔が短いと言える．同様の方法で2016年10月を図10に示す．9月同様にオープンリゾルバ状態のIPアドレスである赤色の点は比較的Y軸の近くにあることから短い間隔でパケットを発信していると言える．

2016年11月はDNS問い合わせパケットとDNS応答パケットの増え方に違いがあることから，DNS問い合わせパケットとDNS応答パケットに分類しそれを図11に示す．オレンジ色の点はDNS応答パケットのIPアドレスであり，オープンリゾルバ状態のIPアドレスと同様に到達間隔が短い傾向がある．また，水色の点はDNS問い合わせパケットのIPアドレスであり，非オープンリゾルバ状態のIPアドレスと似た位置にあることからDNS問い合わせパケットは多くが非オープンリゾルバ状態であると言える．

総パケット数にはばらつきがあり，平均到達間隔は短いという特徴がある．よってオープンリゾルバのような到達間隔の短いIPアドレスは不特定多数の攻撃者によって反射型の攻撃の踏み台として利用され，非オープンリゾルバ状態の機器は乗っ取られ内部からウイルスによってパケットを飛ばしていると推測できる．

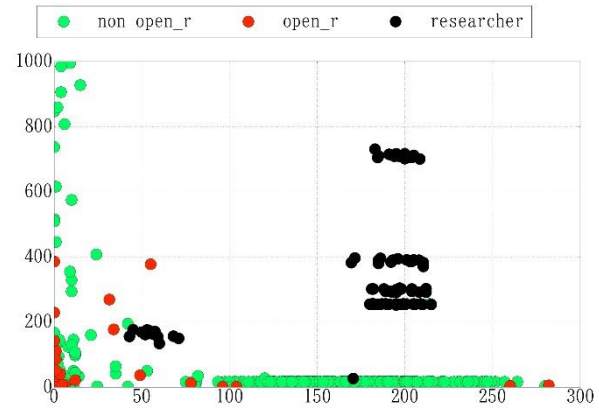

図8　2016年9月　散布図　1

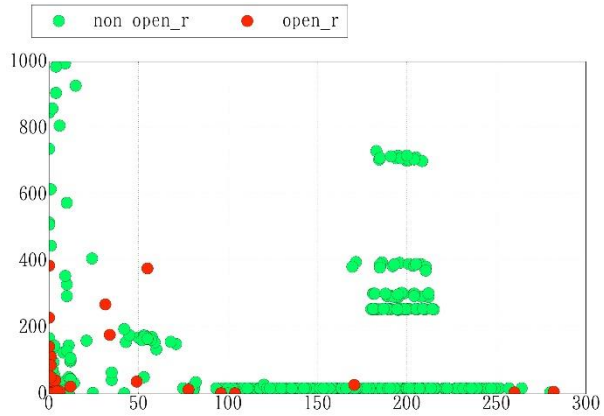

図9　2016年9月　散布図　2

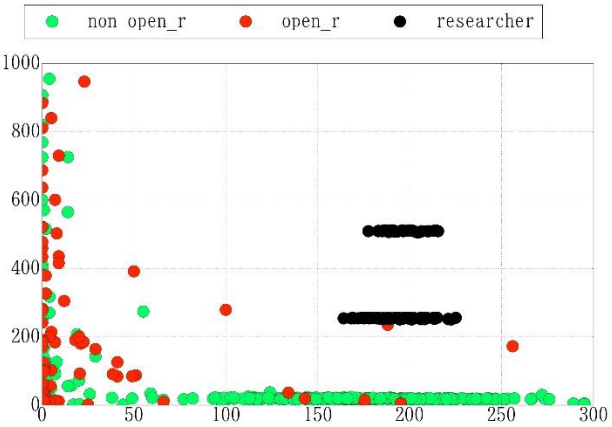

図10　2016年10月　散布図

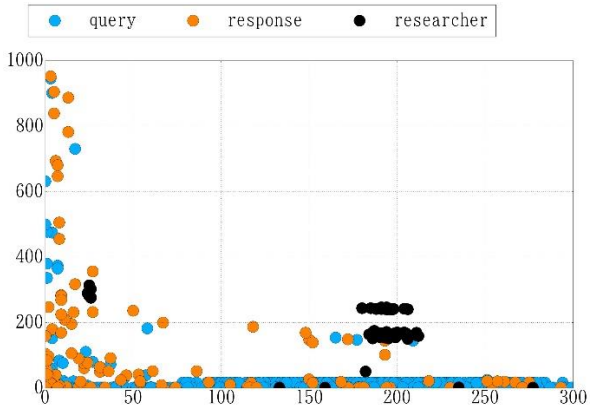

図11　2016年11月　散布図

9.　考察

本論文はDNSアンプ攻撃が発生する際，踏み台として利用されるオープンリゾルバとして稼働する機器について調べた．機器のトラフィックの状態を観測するため，ダークネット観測データとアクティブスキャンを組み合わせてオープンリゾルバとなっている機器の調査を実施した．結果，サーバとして稼働している機器が最も多いが，機器の種類が明確に判別できた中ではルータが多くを占めていた．

また，調査した端末の一部にIoTが含まれていることや，Krebs on Security[2]へのDDoS攻撃をみても，今後IoTデバイスが大規模なサーバ攻撃に利用されることは必至であり，今後注目して監視・分析する必要がある．

可視化を行った際，オープンリゾルバ状態の機器の特徴としてパケットの到達間隔が短く総パケット数には偏りがないという点が挙げられる．理由としては反射型の攻撃であるから機器内部からの攻撃というよりは外部からの跳ね返りの攻撃が多く占めているからである．また，DNS問い合わせパケットとDNS応答パケットに分けて表した際，オープンリゾルバ・非オープンリゾルバ状態の機器と類似した結果になった．そのことから応答パケットの多くはオープンリゾルバ状態と言える．

10.　まとめ

本論文では，DNSアンプ攻撃に悪用されるオープンリゾルバ状態の機器に対してポートスキャンを行い，機器の分類を行った．オープンリゾルバ・非オープンリゾルバ状態のIPアドレスに対して平均到達間隔と総パケットを特徴として可視化を行った．その際，事前に対象とするIPアドレスに対してDNS逆引きを行いドメイン名から調査組織のIPアドレスか否かを考慮した．また，トラフィックをDNS問い合わせパケットとDNS応答パケットで分類し同様に可視化した．

因果関係は明確に説明できないがポートスキャンによる調査を行っている最中，調査サーバに対して不正なリクエストが増加した．サーバを外部に設置する関係上，不正なリクエストは自然と観測されるが，明らかにポートスキャンがトリガーとなっている．現状，不正なリクエストが自然と飛来してきたアクセスかポートスキャンに起因するアクセスかどうかは区別できない．今後これらの機器を更に調査することでボットネットの一部を垣間見ることができると考える．

表 4　2016年11月 送信・宛先ポート別

Day	Query non open	Query open	Response non open	Response open
11/1	49	4	0	0
11/2	47	5	0	0
11/3	64	20	0	0
11/4	75	8	0	0
11/5	63	18	0	1
11/6	288	50	0	0
11/7	47	9	0	0
11/8	44	16	0	0
11/9	8	64	0	0
11/10	22	64	0	0
11/11	23	42	0	0
11/12	15	44	0	0
11/13	14	67	0	0
11/14	16	47	0	0
11/15	16	47	0	0
11/16	7	52	0	0
11/17	8	60	0	0
11/18	41	2251	25	2199
11/19	30	1475	18	1423
11/20	40	3202	21	3357
11/21	50	909	21	893
11/22	64	9	0	0
11/23	63	8	0	0
11/24	77	4	1	0
11/25	73	2	0	0
11/26	4	57	0	3
11/27	6	73	0	1
11/28	18716	25	20344	28
11/29	6082	22	6791	30
11/30	16037	21	17572	43

参考文献

[1] マルウェア対策のための研究用データセット～MWS Datasets 2016～
[2] Krebs on Security, https://krebsonsecurity.com/
[3] 一般社団法人JPCERTコーディネーションセンター，“インターネット定点観測レポート(2016年 10～12

月）“,
https://www.jpcert.or.jp/tsubame/report/report201610-12.html
[4] 笠間　貴弘，島村　隼平，井上　大介，“パッシブ観測とアクティブ観測を組み合わせた組込み機器の攻撃活動状況の把握”，電子情報通信学会論文誌 A Vol.J99-A No.2 pp.94-105，2016/02/01
[5] 福島　祥郎，堀　良彰，櫻井　幸一，“ダークネット観測データに基づく攻撃挙動の特徴抽出に関する考察”，電子情報通信学会技術研究報告，2009/11/13
[6] Open recursive DNS resolver test, http://openresolver.com/
[7] 土性　文哉，杉生　貴成，笠間　貴弘，佐々木　良一，“ダークネット観測データを用いたボットネット抽出手法の提案”，分散協調とモバイルシンポジウム2016論文集，2016，826-831
[8] Shadowsever, https://www.shadowserver.org/wiki
[9] Shodan, https://www.shodan.io/