

## DNS の再帰的な問い合わせを悪用した DDoS 攻撃手法の検証について

### 1 はじめに

分散サービス不能(Distributed Denial of Service:DDoS)攻撃は、複数のコンピュータから大量のデータを送信することで攻撃対象を過負荷状態に陥れる攻撃であり、国内では昨年4月に複数の中央省庁の Web サイトが一時閲覧不能となるなどの被害が発生しており、今年5月に島根県庁の Web サイトにおいても同様の被害が発生している。

この DDoS 攻撃手法の一種として、インターネットの基幹システムである Domain Name System(DNS)を踏み台として利用する攻撃手法がある。DNS のサービスを提供する DNS サーバは世界中に無数に存在しているが、その多くが踏み台として悪用される危険性を抱えており、今後大きな脅威となる可能性がある。

この攻撃手法は、攻撃者が攻撃対象を装って DNS サーバに問い合わせデータを送信することで、DNS サーバから攻撃対象に問い合わせデータの数十倍の応答データを送信させる。これにより、DNS サーバはあたかもマイクに喋った声をスピーカーから大きな音で出力するアンプ(増幅器)のような役割をすることになる。

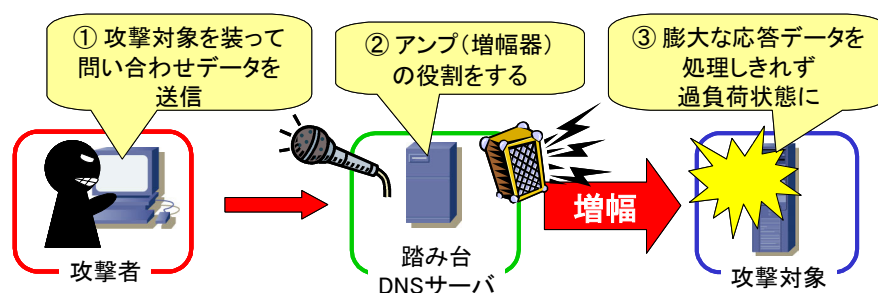


図 1.1 攻撃手法の概要

この攻撃手法による攻撃は既に行われており、昨年12月に米国の国土安全保障省のコンピュータ緊急対応チームである US-CERT からこの攻撃手法についての注意喚起が行われ(「6 参考文献」の[1]を参照)、今年3月に日本の民間のコンピュータ緊急対応チームである JPCERT から国内の DNS サーバが悪用されているとの注意喚起が行われたところである。(「6 参考文献」の[3]を参照)。そこで当庁においてこの攻撃手法の検証を行った結果、攻撃者の送信データの約40倍のデータを踏み台DNSサーバから送信させ、攻撃対象の通信を困難にすることが可能であることが判明した。

## 2 攻撃手法

### (1) DNS の再帰的な問い合わせ

DNS は、利用者からのホスト名の問い合わせに対して DNS サーバがホスト名に対応する IP アドレスを応答する仕組みになっている (図 2.1)。

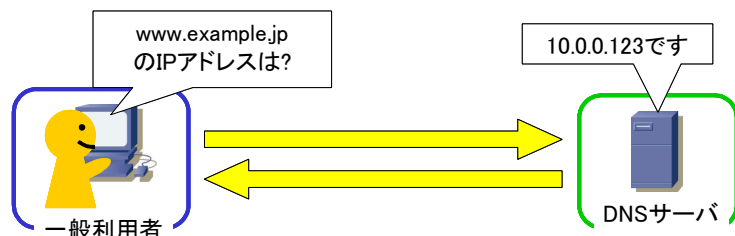


図 2.1 DNS の問い合わせ

問い合わせを受けた DNS サーバが該当するホスト名に関する情報を持っていない場合、DNS サーバは利用者に代わってルート DNS サーバから該当するホスト名の情報を管理している DNS サーバまで順番に問い合わせを行い、得られた結果を利用者のコンピュータに応答する。これが再帰的な問い合わせである (図 2.2)。

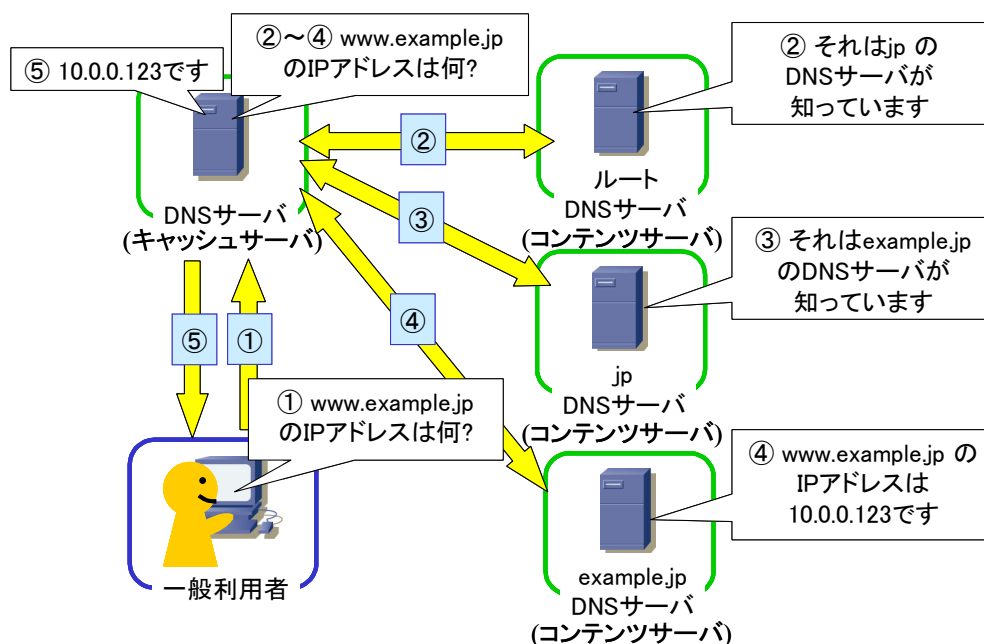


図 2.2 再帰的な問い合わせ

DNS サーバは役割によって分類されており、「jp」や「example.jp」などの各ドメインの情報を管理している DNS サーバはコンテンツサーバと呼ばれている。それに対して、自らはドメインの情報を管理せずに利用者の問い合わせに対して再帰的な問い合わせを行って結果を応答する DNS サーバはキャッシュサーバと呼ばれている。



キャッシュされた TXT レコードは、攻撃者の DNS サーバの TTL で設定された期間踏み台 DNS サーバに保持される。DNS サーバの推奨設定が書かれている RFC 1537（「6 参考文献」の[12]を参照）において一般的な DNS サーバの設定として推奨されている TTL の値は 1 日であるが、攻撃者はさらに長い TTL を設定することで、踏み台 DNS サーバに TXT レコードを長期間キャッシュさせ続けることができる。

#### イ 攻撃段階

実際に攻撃を行う段階では、攻撃者は送信元 IP アドレスを攻撃対象の IP アドレスに詐称し、踏み台 DNS サーバに対して大量に再帰的問い合わせを送信する（図 2.5）。問い合わせを受信した踏み台 DNS サーバは、準備段階においてキャッシュした攻撃者の TXT レコードを攻撃対象に応答する。TXT レコードのサイズを大きくするほど、攻撃者の送信トラフィックは踏み台 DNS サーバによって大きく増幅されることになる。

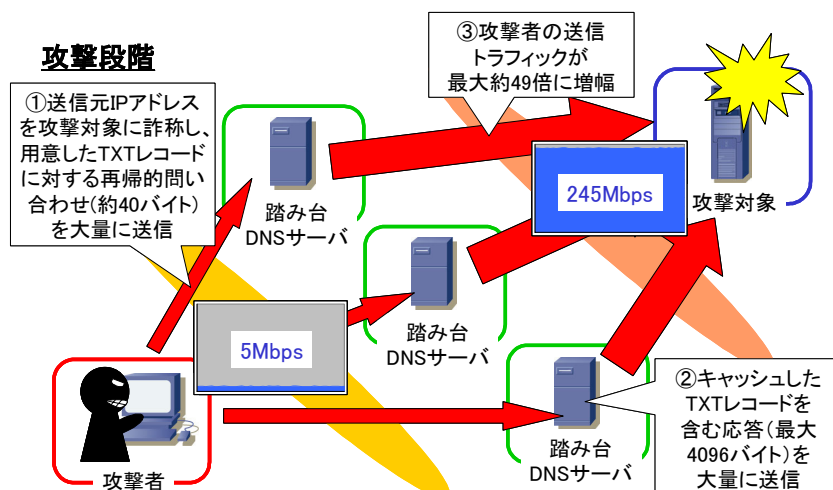


図 2.5 実際に攻撃を行う段階

DNS では UDP を使用して通信を行うが、DNS サーバからの応答のサイズが 512 バイトを超える場合、サーバはクライアントに TCP を使用して再度問い合わせを行うよう通知する。このため、攻撃者が踏み台 DNS サーバから UDP で送信させることのできる応答は最大 512 バイトまでとなる。

ネットワークでの通信には Ethernet という規格が広く使用されており、Ethernet ではデータに Ethernet ヘッダ、IP ヘッダなどが追加された Ethernet フレームの形で通信が行われている。攻撃者の問い合わせのサイズが 40 バイト、応答のサイズが 512 バイトのとき、攻撃者と踏み台 DNS サーバから送信される Ethernet フレームのサイズはそれぞれ 86 バイト、558 バイトとなり（図 2.6）、理論上攻撃者の送信トラフィックは踏み台 DNS サーバにおいて約 6.5 倍まで増幅される。

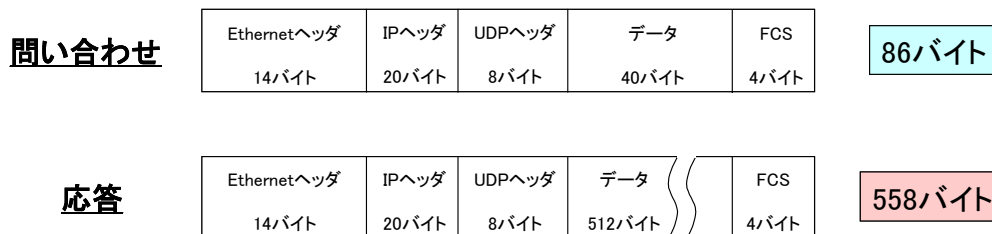


図 2.6 問い合わせと応答の Ethernet フレームサイズ

さらに、攻撃者は EDNS0（「6 参考文献」の[13]を参照）と呼ばれる DNS の拡張機能を使用して問い合わせを送信することで、踏み台 DNS サーバから最大 4096 バイトの応答を UDP で送信させることが可能となる（図 2.7）。

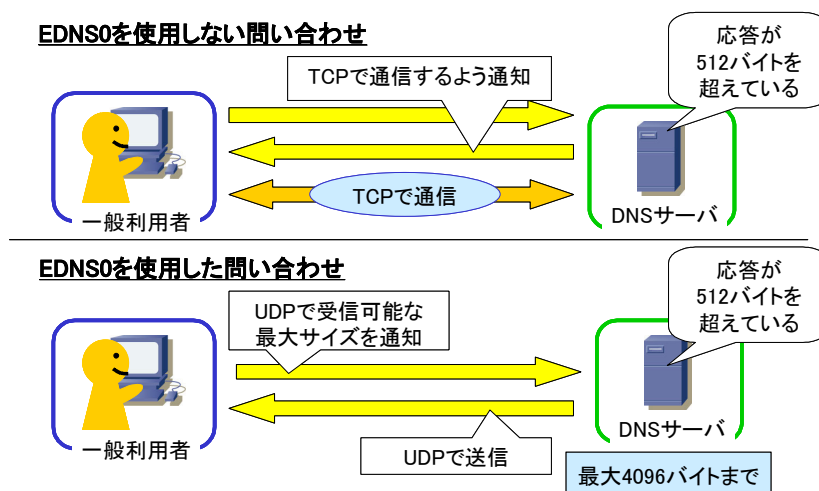


図 2.7 EDNS0

攻撃者の問い合わせのサイズが 40 バイト、応答のサイズが 4096 バイトのとき、応答の UDP パケットは 1 個の Ethernet フレームに入りきらないため、3 個に分割されて攻撃対象へ送信される。そのため攻撃者が 1 回の問い合わせで 1 個の Ethernet フレームを送信するのに対し、踏み台 DNS サーバは 3 個の Ethernet フレームを送信することになる。踏み台 DNS サーバから送信される 3 個の Ethernet フレームの合計サイズは 4218 バイトとなり（図 2.8）、理論上攻撃者の送信トラフィックは踏み台 DNS サーバにおいて約 49 倍まで増幅される。よって、EDNS0 を使用して攻撃が行われた場合、EDNS0 を使用しない場合に比べて高い攻撃力となる。

EDNS0 に対応している DNS サーバソフトウェアとしては、BIND のバージョン 9 や Windows Server 2003 の DNS サービスなどがあり、これらは現在インターネット上で広く使用されている。

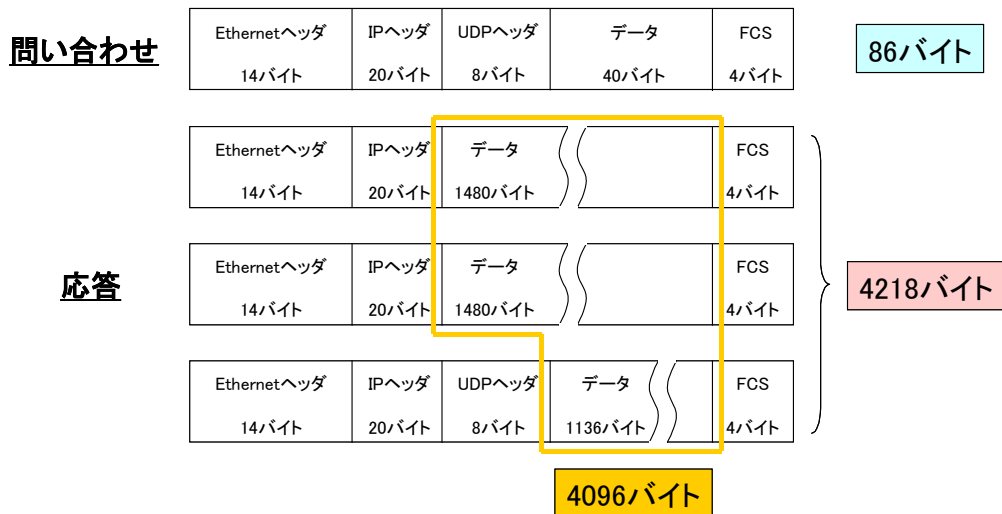


図 2.8 EDNS0 を使用する場合の Ethernet フレームサイズ

### 3 検証

#### (1) 検証環境

検証は、攻撃プログラムを作成して図 3.1 のような Fast Ethernet(100Mbps)のネットワークで行った。攻撃用 PC に 4086 バイトの TXT レコードを用意し、攻撃プログラムを実行して EDNS0 を使用した再帰的問い合わせを 3 台の踏み台 DNS サーバに対して大量に行い、LAN アナライザで攻撃用 PC の送信トラフィックと踏み台 DNS サーバの送信トラフィックを計測した。

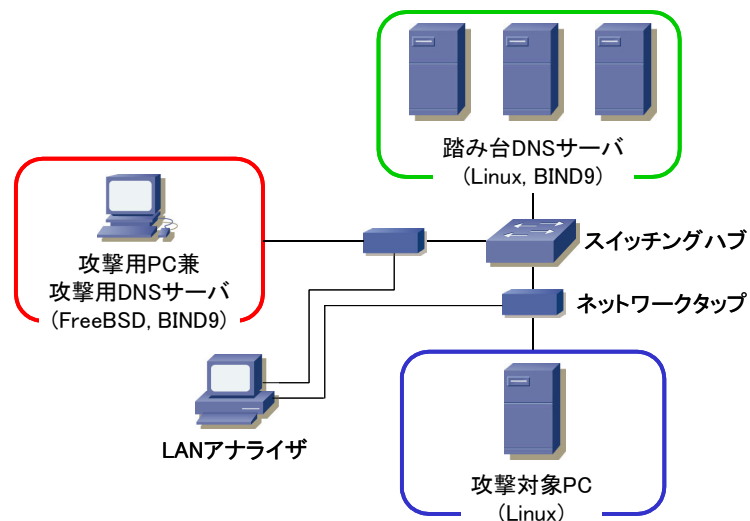


図 3.1 検証環境

## (2) 検証結果

攻撃用 PC で再帰的問い合わせによる送信トラフィックを変化させながら、1 台の踏み台 DNS サーバの送信トラフィックを測定したところ、踏み台 DNS サーバの送信トラフィックは攻撃用 PC の送信トラフィックにほぼ比例して増加しており、トラフィックは約 40 倍に増幅されている (図 3.2)。

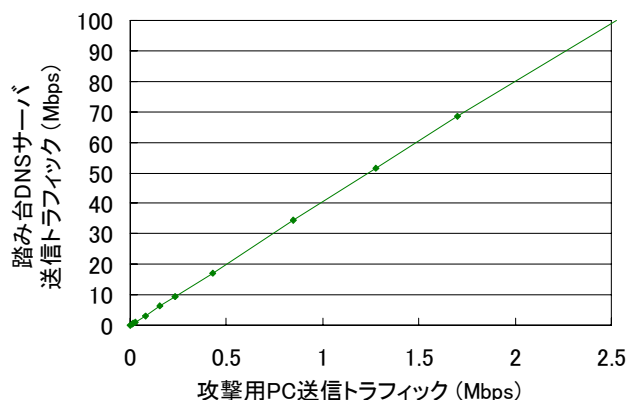


図 3.2 踏み台 DNS サーバ 1 台の送信トラフィック

次に 3 台の踏み台 DNS サーバを使用して、攻撃用 PC の送信トラフィックを変化させながら、ping コマンドを使用して攻撃用 PC から攻撃対象 PC へ 100 回ずつ ICMP echo request パケットを送信し、攻撃対象 PC から応答の ICMP echo reply パケットが返らずにパケットロスとなる割合を測定した。LAN アナライザで測定可能なトラフィックの上限が 100Mbps であるため、100Mbps 以降の踏み台 DNS サーバ 3 台の送信トラフィックは攻撃用 PC の送信トラフィックに増幅率 40 倍を掛けた推定値である。踏み台 DNS サーバの送信トラフィックが 100Mbps を超えるとパケットロス率は上昇を始め、通信が困難な状態となっている (図 3.3)。

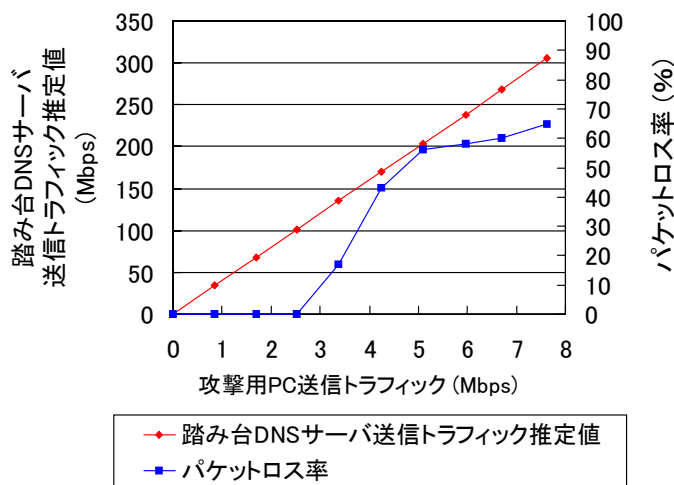


図 3.3 攻撃用 PC と攻撃対象間のパケットロス率

#### 4 攻撃を未然に防止するために

この DDoS 攻撃手法は、被害側の対策によって攻撃を防ぐことが困難であることから、インターネットに接続している各 DNS サーバやネットワークの管理者が攻撃を未然に防止するための対策をとることが重要である。

##### (1) DNS サーバの設定

DNS サーバはその役割によってキャッシュサーバとコンテンツサーバに分類される。また、両方を兼ねているものもある。（キャッシュサーバとコンテンツサーバの役割については「2 (1) DNS の再帰的な問い合わせ」を参照。）

BIND や Windows の DNS サービスといったインターネット上で広く使用されている DNS サーバソフトウェアは、起動するとキャッシュサーバとして動作し、初期設定では再帰的な問い合わせを制限していないため、DDoS 攻撃の踏み台に利用されるおそれがある。攻撃を未然に防止するため、キャッシュサーバとして使用している DNS サーバでは信頼できる利用者以外からの再帰的な問い合わせを受け付けられないよう設定する必要がある（図 4.1）。以下に、BIND と Windows の DNS サービスでの設定方法を示す。

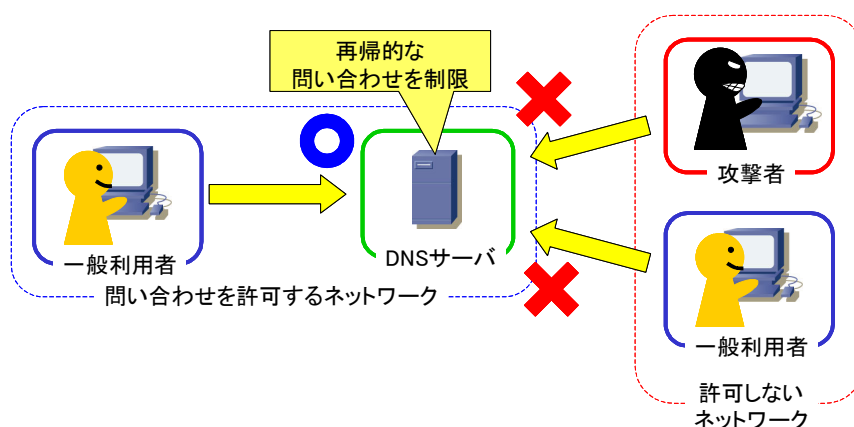


図 4.1 再帰的な問い合わせの制限

##### ア BIND での設定

BIND では、設定ファイルである `named.conf` の `options` ステートメントに `allow-query` サブステートメントを追加することで、問い合わせを受け付けるネットワークを制限する。ただし、コンテンツサーバとして外部に公開するゾーンが存在する場合には、外部からの問い合わせを受け付ける必要があるため、それぞれの `zone` ステートメントに `allow-query` サブステートメントを追加して制限を緩和する。

```

options {
    fetch-glue no: // BIND 8 の場合記述する
    recursion yes: // キャッシュサーバとして使用する場合は yes

    // 問い合わせを受け付けるネットワークを設定する
    allow-query {
        localhost;
        192.168.0.0/24;
    };
};

zone "example.jp" {
    type master;
    file "db.example";
    // コンテンツサーバとして外部に公開するゾーンは
    // どこからの問い合わせも受け付けるよう設定する
    allow-query { any; };
};

```

図 4.2 named.conf の設定例

#### イ Windows の DNS サービスの設定

Windows の DNS サービスでは、再帰的な問い合わせを受け付けるかどうかのみを設定でき、BIND のように問い合わせを受け付けるネットワークを設定することはできない。このため、キャッシュサーバとコンテンツサーバを分離して運用し、コンテンツサーバでは再帰的な問い合わせを受け付けられないよう設定する。キャッシュサーバについては、ファイアウォール製品などによるパケットフィルタリングで問い合わせを受け付けるネットワークを制限する。

Windows Server 2003 で再帰的な問い合わせを受け付けられないように設定するには、管理ツールの「DNS」で DNS サーバのプロパティを開き、「再帰を無効にする」のチェックボックス（図 4.3 の赤線で囲まれた部分）をオンにして「OK」をクリックする。

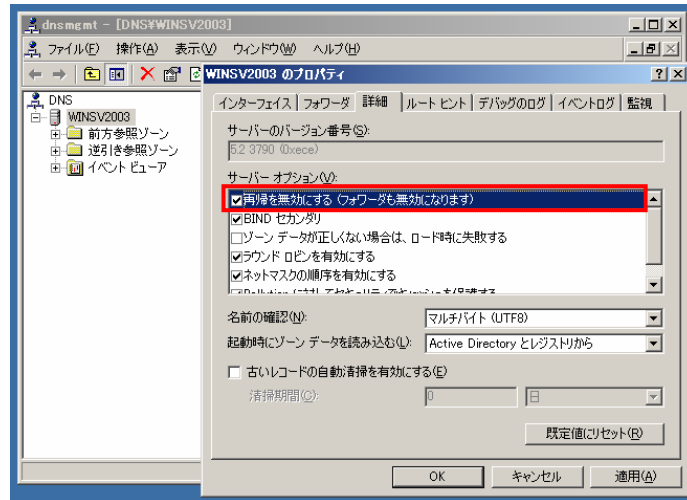


図 4.3 Windows Server 2003 での DNS サービスの設定変更

## (2) IP アドレスの詐称防止

攻撃者が DNS サーバを直接踏み台として利用する以外に、コンピュータにポットプログラムを感染させ、そのコンピュータに DNS サーバを踏み台にした DDoS 攻撃を行わせることも考えられる。この DDoS 攻撃手法では、送信元 IP アドレスを詐称した再帰的な問い合わせを大量に行うため、ファイアウォール、ルータなどで送信元 IP アドレスが詐称されているパケットが外部のネットワークに向けて送信されないよう設定する (egress filtering) ことで、攻撃パケットが DNS サーバに到達することを防ぎ、攻撃を未然に防止することができる (図 4.4)。また、egress filtering を行うことで、送信元 IP アドレスを詐称した SYN flood 攻撃や UDP flood 攻撃などの DoS 攻撃が自組織から外部に向けて行われることも防止することができる。

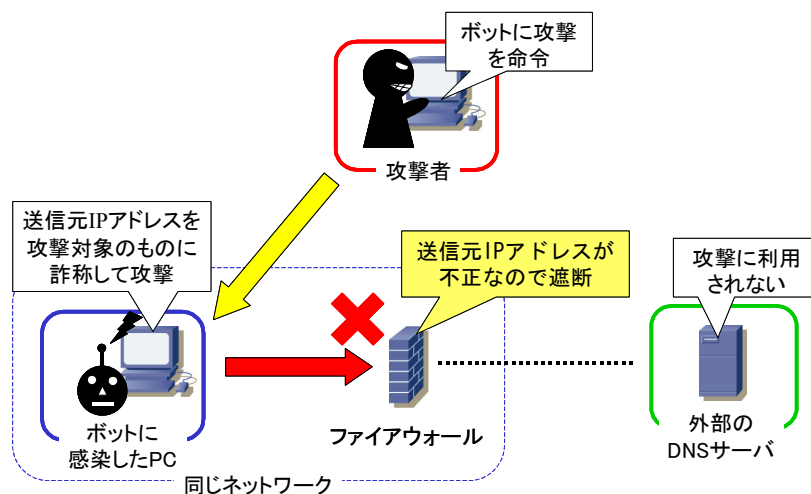


図 4.4 送信元 IP アドレスの詐称防止

## 5 おわりに

今回の検証で、攻撃者が再帰的な問い合わせを制限していない DNS サーバを踏み台として利用することで、自身の送信トラフィックを約 40 倍に増幅し、攻撃対象の通信を困難にできることを確認した。

この攻撃手法は、インターネット上でサービスを提供している DNS サーバを侵入することなく DDoS 攻撃の踏み台として利用することができる。ボットネットなどを使用して多数のコンピュータから大規模な攻撃が行われた場合は深刻な脅威となり、また多数の DNS サーバが踏み台に悪用された場合は、個々の DNS サーバに対する再帰的な問い合わせの頻度が低くなるため、DNS サーバの管理者は自分の管理する DNS サーバが踏み台として悪用されていることに気が付かないおそれがある。The Measurement Factory 社が昨年行った DNS サーバに関する調査の結果（「6 参考文献」の[8]を参照）によると、調査を行った約 130 万の DNS サーバの 75 パーセント以上が再帰的な問い合わせの制限を行っておらず、この攻撃手法を使用した DDoS 攻撃はいつ発生してもおかしくない状況にある。

この攻撃手法は被害を受けている側での対策が困難であることから、インターネットに接続している各 DNS サーバやネットワークの管理者が適切に設定を行うことで攻撃の発生を未然に防止することが重要である。

## 6 参考文献

### [1] US-CERT

The Continuing Denial of Service Threat Posed by DNS Recursion  
[http://www.us-cert.gov/reading\\_room/DNS-recursion121605.pdf](http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf)

### [2] US-CERT

The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0)  
[http://www.us-cert.gov/reading\\_room/DNS-recursion033006.pdf](http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf)

### [3] JPCERT/CC

DNS の再帰的な問合せを使った DDoS 攻撃に関する注意喚起  
<http://www.jpCERT.or.jp/at/2006/at060004.txt>

### [4] 日本レジストリサービス社 (JPRS)

DNS の再帰的な問合せを使った DDoS 攻撃の対策について  
<http://jprs.jp/tech/notice/2006-03-29-dns-cache-server.html>

- [5] Randal Vaughn, Gadi Evron  
DNS Amplification Attacks  
<http://www.isotf.org/news/DNS-Amplification-Attacks.pdf>
- [6] ICANN Security and Stability Advisory Committee  
SSAC Advisory SAC008 DNS Distributed Denial of Service (DDoS) Attacks  
<http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf>
- [7] ベリサイン社  
Anatomy of Recent DNS Reflector Attacks From the Victim and Reflector Points of View  
<http://www.verisign.com/static/037903.pdf>
- [8] The Measurement Factory 社  
The Measurement Factory DNS Survey  
<http://dns.measurement-factory.com/surveys/sum1.html>
- [9] Team Cymru  
Secure BIND Template  
<http://www.cymru.com/Documents/secure-bind-template.html>
- [10] マイクロソフト社  
DNS サーバーで再帰を無効にする  
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/ja/library/ServerHelp/e1fe9dff-e87b-44ae-ac82-8e76d19d9c37.msp?mfr=true>
- [11] Paul Ferguson, Daniel Senie  
Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing [BCP38 / RFC2827]  
<http://www.ietf.org/rfc/rfc2827.txt>
- [12] Piet Beertema  
Common DNS Data File Configuration Errors [RFC1537]  
<http://www.ietf.org/rfc/rfc1537.txt>

- [13] Paul Vixie  
Extension Mechanisms for DNS (EDNS0) [RFC2671]  
<http://www.ietf.org/rfc/rfc2671.txt>