Vol.2018-IOT-40 No.3
2018/3/5

柔軟な応答制御機構を持つ DNSサーバファイアウォールの提案と試作

瀬川 駿[1,a)]　桝田 秀夫[2,b)]　森 真幸[2,c)]　永井 孝幸[2,d)]

概要：DNS サーバは DDoS 攻撃や DNS リフレクター攻撃などの様々な攻撃の対象や，攻撃のための踏み台にしようとする不正通信にさらされている．また，不正通信が行われる際に，特徴的な DNS クエリパターンがみられる場合が知られている．このような不正な通信に繋がるものと正規のもののクエリに対して，レスポンスを適応的に制御できれば，DNS サーバの防御に繋がる．本稿では，DNS サーバの前段に DNS クライアントからの通信を監視するシステムを配置し，攻撃者からのクエリに対してレスポンスを適応的に制御することで DNS サーバへの攻撃を抑える手法を提案する．

Proposal and prototype of DNS server firewall with flexible response control mechanism

Shun Segawa[1,a)]　Hideo Masuda[2,b)]　Masayuki Mori[2,c)]　Takayuki Nagai[2,d)]

Abstract: DNS servers may be illegally accessed to make it target or springboard server for attacks such as DDoS attacks and DNS reflector attacks. It is known that characteristic DNS query patterns are seen when DNS servers are illegally accessed. Adaptive control of responses for queries leading to such illegal access and regular queries leads to defense of DNS servers. In this paper, We propose the method to suppress attacks to DNS servers by introducing the system to monitor access from DNS clients in front of the DNS server and adaptively controlling responses to queries from attackers.

1. はじめに

近年，クラウド化によるサービスの多様化やモバイル端末の普及により，インターネットの利用が増加している．インターネットの通信における重要なシステムとして DNS (Domain Name System) [1][2] がある．インターネットに接続されているすべてのコンピュータ間の通信は，固有の IP アドレスにより行われる．このため，IP アドレスを人間が覚えやすい名前で扱うために考案された機構がインターネットドメイン名である．DNS はドメイン名を分散管理・運用するためのシステムであり，IP アドレスとの対応付けや，メールの宛先ホストの指示などを行うことが可能である．また，ENUM (E.164 NUmber Mapping)[3] や IDN (Internationalized Domain Name)[4] のような，DNS における新しい技術の開発により，インターネット上の DNS が果たす役割は，今後ますます大きくなっていくと考えられる．

一方で，DNS サーバのサービスが停止してしまうことによる被害は大きく，インターネットの安定した運用のためには，安定した DNS サーバの運用が必須である．インターネットに接続したサーバは常に攻撃の危険にさらされており，DNS サーバも例外ではない．DNS への攻撃には，DNS サーバの負荷を上げて応答を得られなくする DoS (Denial of Service) 攻撃や DDoS (Distributed DoS) 攻撃 [5]，DNS サーバの機能を悪用した DNS アンプ攻撃 [6] などがある．

[1] 京都工芸繊維大学 工芸科学研究科 情報工学専攻
Department of Information Science, Kyoto Institute of Technology
[2] 京都工芸繊維大学 情報科学センター
Center for Information Science, Kyoto Institute of Technology
[a)] s-segw17@dsm.cis.kit.ac.jp
[b)] h-masuda@kit.ac.jp
[c)] morim@kit.ac.jp
[d)] nagai@kit.ac.jp

また，DNS を利用してポートスキャン攻撃を可能とする，IPv6 機器発見手法 [7] が見つかっている．これらの攻撃により，サービスの停止やネットワークの麻痺を引き起こす可能性がある．DNS サーバ運用者は，クライアントが要求しているサービスを提供しつつ，このような攻撃を防ぐ必要がある．

DNS サーバへの攻撃を防ぐ技術として，Paul Vixie らによって提案された DNSRRL (DNS Response Rate Limiting)[8] がある．この手法では，応答頻度を監視し，制限することで DNS サーバへの攻撃を防ぐ．DNS を用いた IPv6 機器発見手法に対しては， IPv6 Privacy Extensions[9] を用いた回避策が提案されている．一方，DoS 攻撃や DDoS 攻撃への対処として，DNS 応答を用いた不正通信誘導の手法であるアクセス元分別システム [10] が提案されている．この研究では DNS クエリに対する応答を変化させることで，攻撃性のある通信と正規の通信の分別が可能となり，不正通信誘導ができる手法を提案している．しかし，実装のために既存の DNS サーバに新たに機能を追加する方法では，セキュリティ対策などのバージョンアップに追従することが難しくなる．

そこで本研究では，既存の DNS サーバには手を加えずに，DNS サーバの前段に DNS クライアントからの通信を監視するシステムを配置し，攻撃者からのクエリに対してレスポンスを適応的に制御することで DNS サーバへの攻撃を抑える手法を提案する．また，このシステムにおいて，不正な通信に繋がるクエリを検知する手法を検討するために，実際にインターネット上で利用されている DNS サーバの通信を分析した．

2. DNS サーバへの攻撃

本研究では，DNS サーバへの以下のような攻撃に対する防御手段としてのシステムを提案する．

2.1 DoS 攻撃・DDoS 攻撃

DoS 攻撃は，サーバソフトウェアの脆弱性を利用してサービスを停止させたり，DNS サーバの負荷を上げて応答を得られなくさせたり，通信路を溢れさせて応答が戻らないようにする攻撃手法である．また，大量のマシンから 1 つのサーバに一斉に DoS 攻撃を仕掛ける DDoS 攻撃という類型もある．

2.2 DNS アンプ攻撃

DNS アンプ攻撃は，DNS サーバを通信の増幅器として利用する攻撃で，DNS サーバが送信元からの問い合わせに対し反射的に応答を返すという特性を悪用した攻撃手法である．DNS は UDP を使用するが，UDP は IP アドレスの詐称に弱い．送信元 IP アドレスを詐称したクエリを送ると DNS サーバは詐称された IP アドレスに応答を返すため，攻撃パケットを送ることになる．また，DNS は多くの場合クエリよりも応答のほうがデータが大きいので，DoS 攻撃や DDoS 攻撃をより効率よく行えるという特徴がある．

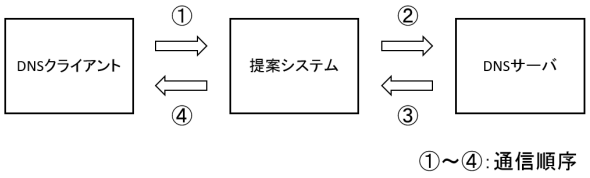

図 1 提案システムの概要

3. 要求

本章では，システムへの要求について述べる．

3.1 DNS プロトコルに変更を加えないこと

DNS プロトコルは広く使われているため，プロトコル自体を大きく変えることは現実的ではない．そのため，DNS プロトコルには変更を加えず，レスポンスのタイミングを変更したり，間引いたり，ペイロードの一部を書き換えたりといった適応的な制御に留める必要がある．

3.2 既存の DNS サーバに手を加えないこと

BIND[11] や NSD[12] などの既存の DNS サーバへ新たな機能を追加する方法では，セキュリティ対策などのバージョンアップに追従することが難しくなる．そのため，既存の DNS サーバに手を加えることは避ける必要がある．

4. 提案システム

本章では，3 章で挙げた要求を満たすために，図 1 のように DNS サーバの前段に DNS クライアントからの通信を監視するシステムを配置し，攻撃者からのクエリに対してレスポンスを適応的に制御することで DNS サーバへの攻撃を抑える手法を提案する．

4.1 DNS サーバへの攻撃の対策

提案システムでは，DNS プロトコルには変更を加えずに，パケットの中継や破棄，書き換えを行う．このシステムにおいて DNS クライアントからのクエリを監視し，分析することができれば，その結果に基づきクエリの攻撃性を検知し，適応的にレスポンスを制御することで，DNS サーバの防御が可能になる．これにより，DDoS 攻撃や DNS アンプ攻撃などの攻撃を防ぐことに繋がる．また，3.1 節の要求を満たすことができると考えられる．

4.2 DNS サーバから独立したシステム

このシステムが DNS サーバを防御するので，既存の DNS サーバには手を加えない．これにより，3.2 節の要求

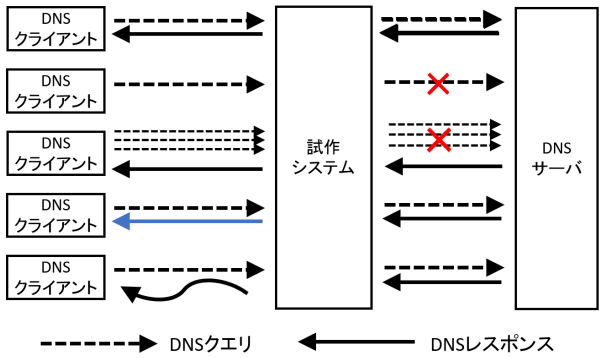

図 2　試作システム

を満たすことができると考えられる．

5. 試作

本章では，4 章で述べたシステムを実際に試作したものについて説明する．

5.1 制御機能

試作システムの実装には，Scapy[13] をライブラリとして利用できる Python を使用した．これにより，DNS パケットの送受信を行う処理を 400 行ほどのソースコードで実装できた．試作システムの概要を図 2 に示す．試作システムでは，以下のようなレスポンスの制御を行う．

制御 1　DNS クライアントと DNS サーバとの通信を無変更で中継する

制御 2　DNS クライアントからのクエリを DNS サーバには送らず破棄する

制御 3　DNS クライアントからの DNS サーバへのクエリ数を制限する

制御 4　DNS サーバからのレスポンスを書き換える

制御 5　DNS クライアントからのレスポンスを遅らせる

試作システムでは，これらの機能により適応的なレスポンスの制御を行う．

5.2 使用例

試作システムの制御機能の使用例を説明する．DNS クライアントからの正規のクエリに関しては，DNS クライアントと DNS サーバとの通信を中継する．不正な通信に繋がるクエリに関しては，DNS クライアントからのクエリを DNS サーバには送らず破棄することで，DNS サーバを防御することなどが考えられる．また，同一の IP アドレスから大量にクエリが送信された場合は，その DNS クライアントからの DNS サーバへのクエリ数の制限やレスポンスの遅延などを行い，DNS サーバを防御することなどが考えられる．

表 1　観測された DNS クエリの概要

クエリ数	1,593,411
通常の応答となったクエリ数	1,283,277
レスポンスエラーとなったクエリ数	310,134
送信元 IP アドレス数	33,313

6. 実験

本章では，6.1 節で実際の DNS サーバが受信したクエリの分析を行うことで，不正な通信に繋がるクエリと正規のクエリの判別方法についての検討を行う．また，6.2 節で試作システムの評価実験を行う．

6.1 実際のクエリの分析

不正な通信に繋がるクエリと正規のクエリを判別する手法を検討するために，実際にインターネット上で利用されている DNS サーバが受信しているクエリを分析する．本分析では，京都工芸繊維大学における kit.ac.jp ゾーンと kit.jp ゾーンの権威をもつ DNS サーバを対象とした．この DNS サーバの通信をモニタリングした結果を使用して分析を行った．分析対象期間は 2018 年 1 月 12 日から 2018 年 1 月 18 日までの 7 日間とした．また，提案システムにおいて，どの程度の処理性能が必要かの検討のために pps（packets per second）についての分析も行った．

6.1.1 クエリ内容の分析

観測された DNS クエリの概要を表 1 に示す．DNS サーバでは，1,593,411 個のクエリを観測した．その内，通常の応答となったクエリは 1,283,277 個，レスポンスエラーとなったクエリは 310,134 個となった．レスポンスエラーが非常に多いという結果になったが，その約半分は学内のプロキシサーバからのクエリであった．これは，プロキシサーバにおいて，クライアントから FQDN 名でクエリを受信し，実際のアクセス先の IP アドレスを探すクエリを DNS サーバに送信するが，リゾルバの設定上，名前解決に失敗した場合はドメイン名の末尾に cis.kit.ac.jp を補ったものでクエリを送信するため，レスポンスエラーとなるクエリが多くなったことによるものと思われる．

観測されたクエリにおいて，通常の応答となったクエリは正規のクエリとし，レスポンスエラーとなったクエリについて，詳しく分析する．

6.1.1.1 ゾーン外に対するクエリ

DNS サーバの応答がレスポンスエラーとなったもののひとつとして，クエリが問い合わせるドメイン名がゾーン外であるものが含まれていた．これらのクエリの例を表 2 に示す．これらのクエリは検索タイプにより大きく分けて 2 種類のクエリに分類できた．検索タイプが A であったクエリが問い合わせるドメイン名として analytics.ff.avast.com や dnsscan.shadowserver.org,

表 2　ゾーン外に対するクエリ

検索タイプ	ドメイン名
A	c.afekv.com
	analytics.ff.avast.com
	dnsscan.shadowserver.org
	cc595656.openresolverproject.org
	sttp.1f1f1085.wc.syssec.rub.de
ANY	activum.nu
	leth.cc
	svist21.cz
	isc.org
	(.)

表 3　一般的なドメイン名の増幅率

ドメイン名	増幅率
google.com	812%
youtube.com	909%
facebook.com	176%
baidu.com	400%
wikipedia.org	675%
reddit.com	104%
yahoo.com	400%
google.co.in	758%
qq.com	266%
amazon.com	981%
平均	642%

表 4　検索タイプが ANY のクエリの増幅率

ドメイン名	増幅率
activum.nu	8207%
leth.cc	15564%
svist21.cz	8922%
isc.org	4387%
(.)	3348%

cc595656.openresolverproject.org などはインターネット上のオープンリゾルバの調査を行っている調査機関の管理下のドメイン名であった．sttp.1f1f1085.wc.syssec.rub.de はルール大学ボーホムの管理下のドメイン名であり，これに関してもインターネット上の調査に利用されているものであった．検索タイプが A であったクエリの約 25%はこれらのような調査機関などの管理下のドメイン名に対するクエリであった．このようにクエリが問い合わせるドメイン名がゾーン外であり，かつ検索タイプが A のクエリは，DNS サーバの応答がレスポンスエラーとなったが，不正な通信に繋がるクエリではないものが多いと考えられる．

検索タイプが ANY であったドメイン名として activum.nu や leth.cc に関しては，フルリゾルバを使用して名前解決を行った．その結果を表 4 に示す．増幅率は，クエリのパケットサイズに対するレスポンスのパケットサイズである．また，検索タイプを ANY とした場合の一般的なドメイン名においての増幅率を表 3 に示す．一般的なドメイン名には Alexa[14] で公開されている人気サイトランキングの上位 10 個のドメイン名を利用した．一般的なドメイン名においての増幅率は 642%程度なので，検索タイプが ANY であったドメイン名に対する増幅率は非常に大きいことが分かる．このことから，これらのドメイン名は DNS アンプ攻撃に利用されやすいドメイン名であり，不正な通信に繋がるクエリであると考えられる．検索タイプが ANY であったクエリの約 99%は，このように増幅率が非常に大きくなるドメイン名に対するクエリであった．

また，検索タイプが A であるが調査機関などの管理下のドメイン名に対するクエリでないものや，検索タイプが ANY であるが増幅率が一般的なものと変わらないクエリに関しては今後さらに分析する必要がある．

6.1.1.2　ゾーン内に対するクエリ

DNS サーバの応答がレスポンスエラーとなったもののひとつとして，クエリが問い合わせるドメイン名がゾーン内であるものが含まれていた．これらのクエリの例を表 5 に示す．これらのクエリには，smtp.mail.edu.kit.ac.jp や resmail.cis.kit.ac.jp のようなゾーン内であるが定義されていないドメイン名に対する正引きのクエリと，xxx.yyy.16.133.in-addr.arpa のようなゾーン内であるがドメイン名に対応付けされていない IP アドレスに対する逆引きのクエリがあった．

imap.kit.ac.jp や smtp.mail.edu.kit.ac.jp のようなゾーン内であるが定義されていないドメイン名に対する正引きのクエリは，メールソフトなどが kit.ac.jp や kit.jp に対応するメールサーバを探す際に使用したクエリである可能性がある．また，このようなクエリは，過去に使用していたが現在は使用していないようなドメイン名に対するクエリであることも考えられる．そのため，不正な通信に繋がるクエリではないと考えられる．

xxx.yyy.16.133.in-addr.arpa. のようなゾーン内であるがドメイン名に対応付けされていない IP アドレスに対する逆引きのクエリは，登録されていない IP アドレスに対するスキャン準備行動の可能性がある．しかしながら，京都工芸繊維大学の IPv4 アドレスブロック (133.16.0.0/16) の運用では，必ずしもすべての利用中 IPv4 アドレスに対するドメイン名登録を行っていないため，存在しているアドレスからのアクセスに対する，アクセス元調査行動 (接続制限やログ記録) の場合が考えられる．学内の IP アドレスの利用状況調査システムと連携して，未登録アドレスの自動抽出を行ったり，自動生成応答を返すような応用が考えられる．

6.1.1.3　ドメイン名 version.bind

DNS サーバの応答はレスポンスエラーとはならなかったが，クエリが問い合わせるドメイン名の末尾が kit.ac.jp または kit.jp とならなかったものとしては，問い合わせるドメイン名が version.bind のクエリが確認された．DNS

表 5　ゾーン内に対するクエリ

問い合わせ方法	ドメイン名
正引き	imap.kit.ac.jp smtp.mail.edu.kit.ac.jp resmail.cis.kit.ac.jp ipc.kit.ac.jp www.ad-global.kit.ac.jp
逆引き	xxx.yyy.16.133.in-addr.arpa

表 6　試作システムの環境

CPU	Intel(R) Xeon(R) CPU E3-1240 V2 @ 3.40GHz
メモリ	8GB
NIC	1000Mbps Full Duplex (e1000e driver)
OS	Ubuntu 14.04.5 LTS
ソフトウェア	Python 2.7.6

サーバは，問い合わせるドメイン名が version.bind，検索タイプが TXT，ネットワーククラスが CH のクエリを受信すると応答として DNS サーバのバージョン情報を送信する．このようなクエリは，攻撃者が DNS サーバのバージョンを確認することで脆弱性のある DNS サーバの探索に利用している可能性がある．

6.2　試作システムの評価実験

DNS サーバの前段に配置した試作システムに対して，dnsperf[15] によりクエリを送信し，処理速度 pps を調べる．また，6.1 節のデータを用いて，実際の DNS サーバが受信したクエリの pps を調べる．この 2 つの pps を比較し，試作システムの性能を評価する．試作システムの pps の測定は 10 回行う．また，実際の DNS サーバが受信したクエリの pps については，1 日の最大 pps を調べる．

6.2.1　実験環境

試作システムとして PC を 1 台，DNS サーバとして研究室で運用している仮想化基板上の仮想マシンを用意した．それぞれの実験環境を表 6，表 7 に示す．

6.2.2　DNS サーバの設定

本研究では，DNS サーバとして NSD 4.0.1 を使用した．実際にドメイン名空間におけるドメインを委任されているわけではなく，ゾーンデータファイルには架空のゾーンに対する情報を記述した．www.example.com というドメイン名のクエリに対して回答部，権威部，付加情報部にそれぞれ 1 つずつリソースレコードを持つ応答を返すように設定した．

6.2.3　実験の結果と評価

試作システムでの実験結果を表 8 に，実際の DNS サーバでの実験結果を表 9 に示す．

実験結果より，試作システムの処理性能は平均 4.64pps となった．また，実際の DNS サーバの 1 日の最大処理性能は平均 224pps となり，試作システムの処理性能は実際の DNS サーバの処理性能に比べて非常に低いことが分かった．これは，Scapy が通信フレームを pcap を用いて直接取り扱っていることが遅くなる主因と考えられる．

表 7　DNS サーバの環境

CPU	Dual-Core AMD Opteron(tm) Processor 8222 3GHz x4
メモリ容量	128GB
NIC	1000Mbps Full Duplex (e1000 driver)
OS	Cent OS 6.3
仮想化ソフトウェア	KVM
仮想マシンのメモリ容量	1 GB
仮想マシンの OS	Ubuntu 14.04.5 LTS
ソフトウェア	NSD version 4.0.1

表 8　試作システムの pps

試行回数	試作システムの処理性能 pps
1	4.91
2	4.94
3	4.96
4	4.87
5	4.70
6	4.56
7	4.47
8	4.41
9	4.30
10	4.23
平均	4.64

表 9　DNS サーバの pps

日付	最大 pps
1/12	204
1/13	528
1/14	82
1/15	208
1/16	102
1/17	356
1/18	92
平均	224

7.　おわりに

本研究では，DNS サーバの前段に DNS クライアントからの通信を監視するシステムを配置し，攻撃者からのクエリに対してレスポンスを適応的に制御することで DNS サーバへの攻撃を抑える手法を提案し，試作した．また，提案システムにおいて不正な通信に繋がるクエリと正規のクエリを判別する方法を検討するために，実際の DNS サーバが受信したクエリの分析を行った．分析の結果，検索タイプが ANY であり，かつ DNS サーバがレスポンスエラーを返すドメイン名に対するクエリに関しては，そのドメイン名が DNS アンプ攻撃に悪用されやすいドメイン名であることが多いことを確認した．また，DNS サーバの

バージョンを確認するクエリも確認された．これらのクエリに対しては，通常のレスポンスではなく，適応的にレスポンスを制御する必要があると考えられる．また，試作システムの性能評価に関しては，試作システムの処理性能が実際の DNS サーバの処理性能と比較して非常に低くなってしまった．

今後の課題としては，不正な通信に繋がるクエリに対する適応的なレスポンスの検討，処理時間の短縮などが挙げられる．また，今後も DNS サーバへのクエリの分析を継続し，不正な通信に繋がるクエリと正規のクエリの判別方法を検討する必要がある．

参考文献

[1] Mockapetris, P. and ISI: DOMAIN NAMES - CONCEPTS AND FACILITIES, RFC 1034 (1987).
[2] Mockapetris, P.: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, RFC 1035 (1987).
[3] Faltstrom, P.: E.164 number and DNS, RFC 2916 (2000).
[4] Klensin, J.: Internationalized Domain Names for Applications (IDNA):Definions and Document Framework, RFC 5890 (2010).
[5] Handley, M. and Rescorla, E.: Internet Denial-of-Service Considerations, RFC 4732 (2006).
[6] Damas, J. and Neves, F.: Preventing Use of Recursive Nameservers in Reflector Attacks, RFC 5358 (2008).
[7] 曽我一喜，桝田秀夫：IPv4/IPv6 デュアルスタック環境における DNS を用いた IPv6 機器発見の手法とその回避策の一考察，インターネットと運用技術 (IOT) シンポジウム 2013 WIP，pp. 107–110 (2013).
[8] Vixie, P. and Schryver, V.: DNS Response Rate Limiting (DNS RRL), *ISC-TN-2012-1-Draft1*, pp. 1–5 (2012).
[9] Thomson, S. and Narten, T.: IPv6 Stateless Address Autoconfiguration, RFC 2462 (1998).
[10] 小川拓也，桝田秀夫：IPv6 環境におけるサーバ防御を目的とする DNS 応答を用いたアクセス元分別システムの提案，京都工芸繊維大学大学院工芸科学研究科修士論文，pp. 1–30 (2016).
[11] InternetSystemsConsortium: BIND, Internet Systems Consortium (online), available from ⟨https://www.isc.org/downloads/bind/⟩ (accessed 2018-1-25).
[12] NLnetLabs: NSD, NLnetLabs (online), available from ⟨https://www.nlnetlabs.nl/projects/nsd/⟩ (accessed 2018-1-25).
[13] Biondi, P., Valadon, G. and Lalet, P.: Scapy, (online), available from ⟨http://www.secdev.org/projects/scapy/⟩ (accessed 2018-1-25).
[14] AlexaInternet: Alexa, Alexa Internet (online), available from ⟨http://www.alexa.com/⟩ (accessed 2018-1-25).
[15] Nominum: dnsperf, Nominum (online), available from ⟨http://www.nominum.com/measurement-tools/⟩ (accessed 2018-1-25).