DNS オープンリゾルバの実態

高野　祐輝[†,††a)]　安藤　類央[†]　宇多　仁[†,††]　高橋　健志[†]
井上　朋哉[†,††]

The Ecology of DNS Open Resolvers

Yuuki TAKANO[†,††a)], Ruo ANDO[†], Satoshi UDA[†,††], Takeshi TAKAHASHI[†], and Tomoya INOUE[†,††]

あらまし　DNS アンプ攻撃は DNS オープンリゾルバを踏み台として利用した DDoS 攻撃であり，その増幅率は数十倍にのぼるため，少ないネットワーク帯域でも効果的に攻撃を行うことができるため大きな問題となっている．そこで我々は，DNS アンプ攻撃に利用されるオープンリゾルバの実態を調査するために，広域なアクティブ検索，サイレントモニタ運用，実オープンリゾルバ運用という三つの多角的な視点から観測を行った．我々が行ったアクティブ検索の結果，インターネット上に 3,000 万以上の DNS サーバが存在することが明らかとなり，そのうちの 2,500 万以上もの DNS サーバがオープンリゾルバであることが明らかとなった．また，サイレントモニタ運用，実オープンリゾルバの運用により，DNS サーバ探索には A レコード問い合わせが，攻撃には A レコード及び ANY レコードの問い合わせが多く利用されることが明らかとなり，更に，これら情報と BGP 情報を組み合わせることで，DNS アンプ攻撃の攻撃者が存在するネットワークを特定することが可能であることを示す．

キーワード　DNS，オープンリゾルバ，DNS アンプ攻撃，DDoS 攻撃

1. まえがき

Domain Name System (DNS) [1], [2] は人間の読みやすいホスト名と IP アドレスとを変換するために利用される分散型のデータベース・名前解決システムであり，今日のインターネット運用に必要不可欠なサービスである．DNS は，インターネット黎明期の 1987 年に RFC 1035 で策定された仕様を，2014 年の現在に至るまで様々なアップデートが施されつつ利用され続けている．これまでに DNS のセキュリティで大きな問題となったのは，偽の DNS 応答をする DNS スプーフィング攻撃や，DNS キャッシュサーバのキャッシュポイゾニング攻撃である．

DNS スプーフィング攻撃は，DNS のプロトコルに認証機能をないことを利用した攻撃であるが，実際に，中国の金盾と呼ばれる検閲システムでは DNS スプーフィング攻撃を行っていることが報告されている [3]．DNS スプーフィング攻撃はこのような大規模な検閲システムでなくても，比較的容易に行えるため問題となったが，これを解決するために DNSSEC [4] の提案がなされ，現在，多くの DNS サーバソフトウェアにて実装されている．また，DNS キャッシュに対する攻撃として，非常に実践的な Kaminsky 攻撃が 2008 年に報告され [5]，こちらも大きな問題となった．

更に，DNS スプーフィング攻撃，DNS キャッシュポイゾニング攻撃に続いて，DNS アンプ攻撃 [6] と呼ばれる DNS サーバを悪用した DDoS 攻撃が注目をあびるようになった．例えば，2013 年にアンチスパムメールの非営利団体である Spamhous が受けた，DNS アンプ攻撃を利用した 75Gbps もの DDoS 攻撃は大きな話題となった [7]．本来，DNS はパケットのサイズに 512 バイトの制限があったが，仕様のアップデートによって 512 バイトを超える大きな問い合わせ・応答パケットを送信できるようになり [8]，その結果，DNS サーバ（オープンリゾルバ）を増幅器とした反射型の DDoS 攻撃が可能となり大きな問題となっている．

† 情報通信研究機構，小金井市
National Institute of Information and Communications Technology, Koganei-shi, 184–8795 Japan
†† 北陸先端科学技術大学院大学，能美市
Japan Advanced Institute of Science and Technology, Nomi-shi, 923–1211 Japan
a) E-mail: ytakano@wide.ad.jp

そこで，本研究では DNS アンプ攻撃の踏み台として利用されるオープンリゾルバについて，アクティブ検索，サイレントモニタ観測，オープンリゾルバ運用という三つの側面から詳細に調査した．**2.** では関連研究について述べる．**3.** では，我々が設計・実装した DNS サーバのアクティブ探索システムについて説明する．**4.** と **5.** では，我々が行ったアクティブ検索の結果を示す．アクティブ検索の結果，インターネット上に約 3,000 万の DNS サーバが存在し，そのうちの約 2,500 万もがオープンリゾルバとなっていることが明らかとなった．更に，これらサーバに VERSION.BIND 問い合わせを行うことで，DNS サーバソフトウェア種類とバージョンについての傾向を得ることができた．また，**7.** にて，サイレントモニタによる観測を行った結果を示し，**8.** で実際にオープンリゾルバ運用を行った結果を示す．サイレントモニタによる観測では，多くの DNS サーバ探索パケットを観測することができ，オープンリゾルバ運用の結果 DNS アンプ攻撃が定常的に行われていることが明らかとなった．更に，本論文では，サイレントモニタ，オープンリゾルバ，及び BPG から得られた情報を組み合わせることで，攻撃元ネットワークの特定が可能であることを示す．

2. 関連研究

本節では，DNS アンプ攻撃及び，DNS サーバ調査研究について説明し，関連研究と本研究の差異について述べる．

2.1 DNS アンプ攻撃

DNS アンプ攻撃は，DNS の問い合わせパケットと応答パケットのサイズに大きく差があることを利用して行われる DDoS 攻撃の一種である．RFC 4732 [9] の分類によると，増幅攻撃の一種とされており，類似の攻撃手法として Smurf 攻撃や TCP アンプ攻撃などが存在する．

DNS アンプ攻撃は，インターネット上に存在する複数の DNS サーバに対して，送信元アドレスを攻撃対象に詐称したクエリを送信することで行われる．一般的に，DNS の問い合わせパケットは，数十バイトのサイズであるが，ANY クエリなど特定のクエリに対する応答パケットは 3,000 バイト以上となるため，攻撃者が送信したトラヒックが数十倍に増幅されて攻撃対象のネットワークに到達する．このように，DNS アンプ攻撃は，インターネット上にある DNS サーバを増幅器として利用して行われるが，この，インターネット上にオープンに存在して制限なく再帰問い合わせに答える DNS サーバの事は，一般的に DNS オープンリゾルバと呼ばれる．

DDoS 攻撃の踏み台となるオープンリゾルバは，だれでも自由に運用できるため，世界中に分布していると考えられるが，その実態を詳細に把握されてはいなかった．また，DNS アンプ攻撃の特性や防御方法などを研究する上でも，オープンリゾルバの実態を把握することは重要である．

2.2 DNS サーバ調査研究・プロジェクト

Open Resolver Project [10] は，2013 年の 3 月頃から世界中の DNS サーバをアクティブに調査し，ウェブ上で定期的にオープンリゾルバの統計情報を提供しているプロジェクトである．本プロジェクトのページから，2013 年 3 月から 2014 年 1 月現在に至るまでオープンリゾルバの情報を閲覧することができる．Shadowserver [11] は，インターネットセキュリティに関連した調査を行っている団体であるが，Shadowserver においてもオープンリゾルバのアクティブ計測を行っている．本プロジェクトの存在は **7.** で述べる，サイレントモニタを運用することで発見することができた．その他にも Steve Sntorelli [12] も同様に，オープンリゾルバの調査報告を行っているが，こちらは前者二つと違い，広域な調査を行っているわけではない．

前者二つのプロジェクトは，IPv4 アドレス空間をスキャンした結果のアドレス分布を大まかに報告している．本研究では，同様に，インターネット上の DNS サーバをスキャンした結果を述べるが，本論文では，前者二つが報告していない，DNS サーバのソフトウェア種類，バージョン情報，IP アドレスの逆引き情報について詳細な報告を行う．更に，我々は，アクティブスキャンのみならず，サイレントモニタと，実際のオープンリゾルバ両者を運用し観測を行ったので，本論文では，これら運用から得られた知見についても報告を行う．

3. DNS サーバのアクティブ検索システム

本節では，インターネット上にある DNS サーバをアクティブに検索するためのシステムとアーキテクチャについて説明する．図 1 は，我々が設計と実装を行った，DNS サーバ検索システムのシステムアーキテクチャとなる．本システムは以下で述べる，DB, DNS Prober, Reverse Lookupper, Statistical Analyzer の四つのコンポーネントから成り立っている．

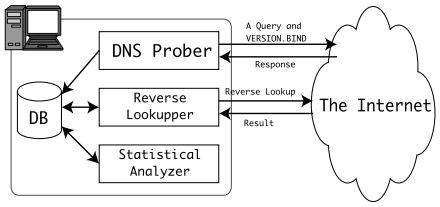


図 1　DNS サーバ検索システムのシステムアーキテクチャ
Fig. 1　System architecture of DNS server crawler.

DB

本システムでは，検索した結果や統計情報を NoSQL データベースに保存する．NoSQL データベースを採用した理由は，NoSQL データベースは SQL データベースのようにカラム定義などの制限にとらわれずに柔軟なレコードの追加が行えるため，ラピッドプロトタイピングなどで容易に利用可能であり，また，幾つかの NoSQL データベースは MapReduce [13] を利用して容易にデータ処理が行えるためである．我々の実装では，NoSQL データベースとして，MapReduce も備えており，C++，Python などと親和性の高い MongoDB [14] を利用した．

DNS Prober

DNS Prober は，全ての IPv4 グローバルアドレスの 53 番ポート宛に DNS の A レコード要求を送信して，インターネット上にある DNS サーバを検索するコンポーネントとなる．検索する際，再帰問い合わせ要求を意味する RD フラグ [2] をオフにしたクエリパケットを送信することで，極力インターネットに負荷をかけることを避けている．もし，この A レコード要求に対して，再帰問い合わせ可能であることを示す RA フラグ [2] がセットされた応答が返ってきた場合，その応答を返してきたアドレスに，オープンリゾルバが存在することを意味する．逆に，RA フラグがオフとなっていた応答を返してきた場合は，オープンリゾルバでない DNS サーバが存在するすることを意味する．

A レコード要求に対する応答を受信した場合，DNS Prober は続けて VERSION.BIND をキーとした TXT レコード要求を，応答したアドレスに送信する．幾つかの DNS サーバの実装では，DNS サーバのソフトウェアバージョンを VERSION.BIND の TXT レコード要求に対して返信する．実際にこの挙動は，dig コマンドを用いて，`$ dig @127.0.0.1 -t TXT -c CHAOS VERSION.BIND` とすると確認することができる．

我々は DNS Prober を C++で実装した．DNS Prober では，Boost [15]，libevent [16]，MongoDB C++ドライバ，Catenaccio DPI [17] を利用しており，得られた全ての結果は MonboDB に保存している．また，DNS Prober は IPv4 グローバルアドレス全てに対して探索するため，逐次問い合わせを行っていたのでは，処理の完了までに時間がかかってしまう．そのため，本実装では，クエリ発行処理と応答の処理を分離して探索の高速化を行っている．

Reverse Lookupper

Reverse Lookuper は，DNS Prober にて得られた IP アドレスの逆引きを行い，IP アドレスに結び付けられたドメイン名を取得する．我々は，Reverse Lookupper を同様に C++で実装した．Reverse Lookupper もまた，Boost, libevent, MongoDB C++ドライバ，Catenaccio DPI を利用している．逆引きするアドレスは数千万もの大量のアドレスとなる．そこで，我々は，同様に，libevent を利用して非同期に大量のクエリを処理できるように最適化した．同様に，全ての得られたドメイン名は MongoDB へと保存される．

Statistical Analyzer

DNS Prober 及び Reverse Lookupper から得られた結果は，Statistical Analyzer によって解析される．我々の実装では，解析に MongoDB の提供する MapReduce を利用した．MongoDB では，JavaScript に対応した MapReduce 用のインターフェースを提供しているため，Statistical Analyzer の実装では JavaScript を主として用い，補助的に Python を利用した．

我々は本システムを用いて，全 IPv4 アドレス空間に存在する DNS サーバの検索を，日本時間の 2013 年 7 月 5 日 17 時 26 分から 7 月 6 日 19 時 38 分にかけて行った．その結果，IPv4 アドレス空間に 3,000 万以上もの DNS サーバが存在し，更にそのうちの 2,500 万近くもの DNS サーバがオープンリゾルバとなっていることが明らかとなった．また，700 万の DNS サーバから DNS ソフトウェアとバージョン情報を取得することができた．これら結果の詳細については，**4.** と **5.** にて記述する．

4. DNS サーバソフトウェアと地域分布

本節では **3.** で説明したシステムを用いた，DNS サーバ検索の結果について述べる．

4.1 DNS サーバソフトウェア分布

我々は，得られたIPv4アドレスを地域インターネットレジストリ (RIR) [18] ごとに分類し，更に，VERSION.BIND 問い合わせで得られた結果を，表 1 に示す正規表現を用いてサーバ種類で分類した．

表 2 は，DNS サーバ種類の RIR ごとの分布となる．なお，can't detect の行は，表 1 の正規表現で分類できなかったサーバを示しており，no version info の行は，VERSION.BIND 問い合わせに対してエラーを返信してきたサーバを示している．

表 1 DNS サーバ種類判別のための正規表現
Table 1 Regex for detecting DNS server types.

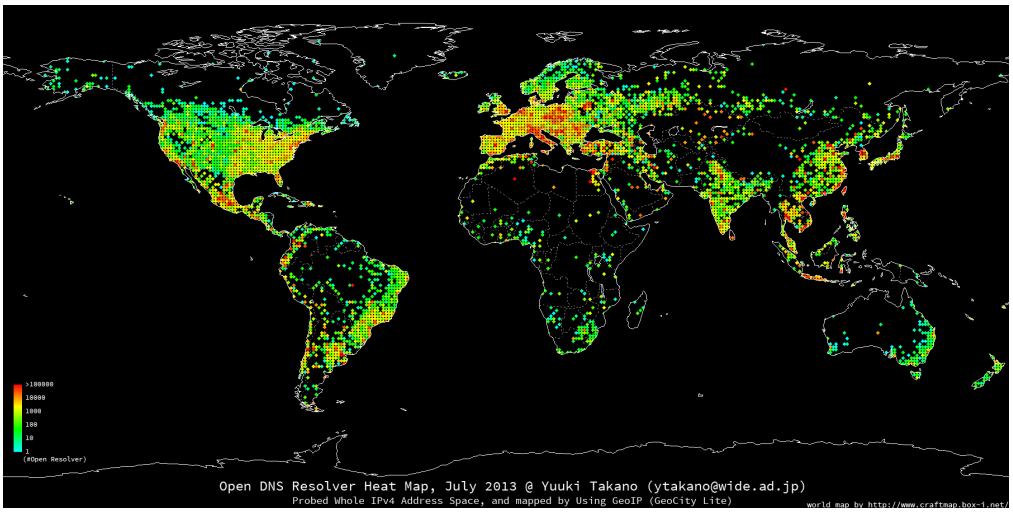
DNS 種類	正規表現
BIND 9.x	^9(\.[0-9])+
BIND 8.x	^8(\.[0-9])+
BIND 4.x	^4(\.[0-9])+
Dnsmasq	^dnsmasq
Nominum Vantio	^Nominum Vantio
Nominum ANS	^Nominum ANS
PowerDNS	^PowerDNS
Unbound	^unbound
NSD	^NSD
Windows series	.*Windows

我々が計測した結果，VERSION.BIND 問い合わせに応答したサーバの数は 15,357,412 となり，そのうち表 1 の正規表現で分類できたサーバの数は 7,075,527 となった．ただし，VERSION.BIND 問い合わせに対して応答する内容は，サーバ運用の際に自由に設定可能であるため，必ずしも正しいバージョンやソフトウェアでない場合もある．しかしながら，多くの場合，デフォルト設定では，自身のソフトウェア名とバージョンを応答することも注記しておく．DNS サーバは大きく分けて，ゾーンを管理するサーバ（コンテンツサーバ，スレーブサーバ）と，クライアントからの要求に答えるためのサーバ（フルサービスリゾルバ，フォワーダ）に分類される．本論文では，議論を明確にするために，前者を権威 DNS サーバ，後者をリゾルビング DNS サーバと呼ぶ．BIND シリーズ [19]，Nominum ANS [20]，PowerDNS [21]，NSD [22] は権威 DNS サーバが構築可能な DNS サーバソフトウェアであり，一方，Dnsmasq [23]，Nominum Vantio [24]，Unbound [25] は，リゾルビングサービスの

表 2 DNS サーバソフトウェア種類分布
Table 2 Distribution of DNS server types.

Type of DNS	#	Total %	APNIC #	RIPE #	ARIN #	LACNIC #	AFRINIC #	other #
BIND 9.x	4268442	(14.1%)	806357	1530177	1126501	169268	121556	514583
†	1851362	(6.1%)	551458	781954	176399	94385	117906	129260
BIND 8.x	35218	(0.1%)	4588	21348	6663	974	32	1613
†	30444	(0.1%)	4202	18958	5186	854	31	1213
BIND 4.x	3486	(0.0%)	121	2751	440	43	0	131
†	2765	(0.0%)	93	2256	348	11	0	57
Dnsmasq	1308653	(4.3%)	692042	216273	75201	226880	32676	65581
†	1308381	(4.3%)	692026	216028	75196	226877	32676	65578
Nominum Vantio	968041	(3.2%)	553404	284852	20142	21205	70861	17577
†	967044	(3.2%)	552650	284782	20125	21200	70736	17551
Nominum ANS	687	(0.0%)	18	34	79	42	2	512
†	13	(0.0%)	2	0	0	11	0	0
PowerDNS	373588	(1.2%)	14215	329994	14360	2952	91	11976
†	372684	(1.2%)	14207	329116	14354	2952	91	11964
Unbound	71781	(0.2%)	16230	43507	6941	1510	1585	2008
†	23220	(0.0%)	3281	14398	4638	315	312	276
NSD	33933	(0.1%)	1731	11077	17182	322	13	3608
†	17	(0.0%)	5	5	2	1	0	4
can't detect	8281885	(27.3%)	4012525	2367711	429450	690618	279903	501678
†	7658656	(25.3%)	3911886	2118455	244682	670597	278183	434853
Windows series	11698	(0.0%)	184	1077	85	10312	0	40
†	11342	(0.0%)	129	865	67	10257	0	24
no version info	14927910	(49.3%)	3457029	4505928	1442348	4025325	699029	798251
†	12746062	(42.1%)	3050589	3465814	1179188	3919438	668399	462634
Total	30285322	(100.0%)	9558444	9314729	3139392	5149451	1205748	1917558
†	24971990	(82.5%)	8780528	7232631	1720185	4946898	1168334	1123414

†: DNS オープンリゾルバ
2013 年 7 月 5 日 17 時 26 分 - 7 月 6 日 19 時 38 分 (JST)



https://github.com/ytakano/pictures/blob/master/dns/open_dns_resolver_heatmap_201307.png

図 2　DNS オープンリゾルバの地域別分布
Fig. 2　World heatmap of DNS open resolvers.

み提供する DNS サーバを構築するための DNS サーバソフトウェアである．表 2 から，権威 DNS サーバのみに特化した NSD と Nominum ANS では，オープンリゾルバとなっている割合が非常に少ないことがわかる．その一方，権威 DNS サーバとリゾルビング DNS サーバの両方に利用可能な BIND シリーズや，PowerDNS では，オープンリゾルバとなっている割合が高く，リゾルビングサービス専用の DNS サーバソフトウェアで運用されている DNS サーバの多くもオープンリゾルバとなっている．各サーバソフトウェアの詳細については **5.** で議論する．

4.2　RIR ごとの DNS サーバ分布

まずはじめに，RIR ごとの DNS サーバとオープンリゾルバの分布について議論する．我々は合計で 30,285,322 の DNS サーバアドレスを取得することができ，そのうちの，約 82.5%の 24,971,990 ものアドレスから，オープンリゾルバであることを意味する RA フラグがセットされた応答を得られることができた．APNIC と RIPE NCC に DNS サーバが多く集中しており，インターネット上に存在する DNS サーバの約 62.3%もが APNIC と RIPE NCC に存在し，更にそのうち，約 87%もがオープンリゾルバとなっている．LACNIC 及び AFRINIC は他と比較して DNS サーバが存在する数が少なく，それぞれ，5,149,451 と，1,205,748 アドレスとなっており，これは，インターネットユーザの数に起因すると考えられる．LACNIC と AFRINIC に存在する DNS サーバのうち，約 96%がオープンリゾルバとなっており，すなわち，LACNIC と AFRICIN に存在する DNS サーバのほとんど全てがオープンリゾルバである．一方，ARIN には 3,139,392 の DNS サーバが存在するが，オープンリゾルバと分類されたのは，そのうちの約 54.8%の 1,720,185 のみであり，他の RIR と比較して DNS サーバがオープンリゾルバである割合が低くなっている．

図 2 は，得られた DNS オープンリゾルバの IP アドレスから GeoIP Lite [26] を用いて緯度経度を算出した後，地図上にマッピングしたものである．この図から，世界中の非常に広範囲にわたって，オープンリゾルバが分布していることがわかる．

5.　DNS サーバソフトウェアとバージョン分布

本節では，BIND シリーズ，PowerDNS，Dnsmasq，Unbound，NSD，Nominum Vantio，Nominum ANS の DNS サーバソフトウェアとバージョン分布について議論を行う．

5.1　BIND シリーズ

BIND は最も有名な DNS サーバソフトウェアであり，権威 DNS サーバとリゾルビング DNS サーバの両方に利用可能である．我々の計測では，BIND 9.x，8.x，4.x シリーズで，それぞれ，417，86，71 のソフ

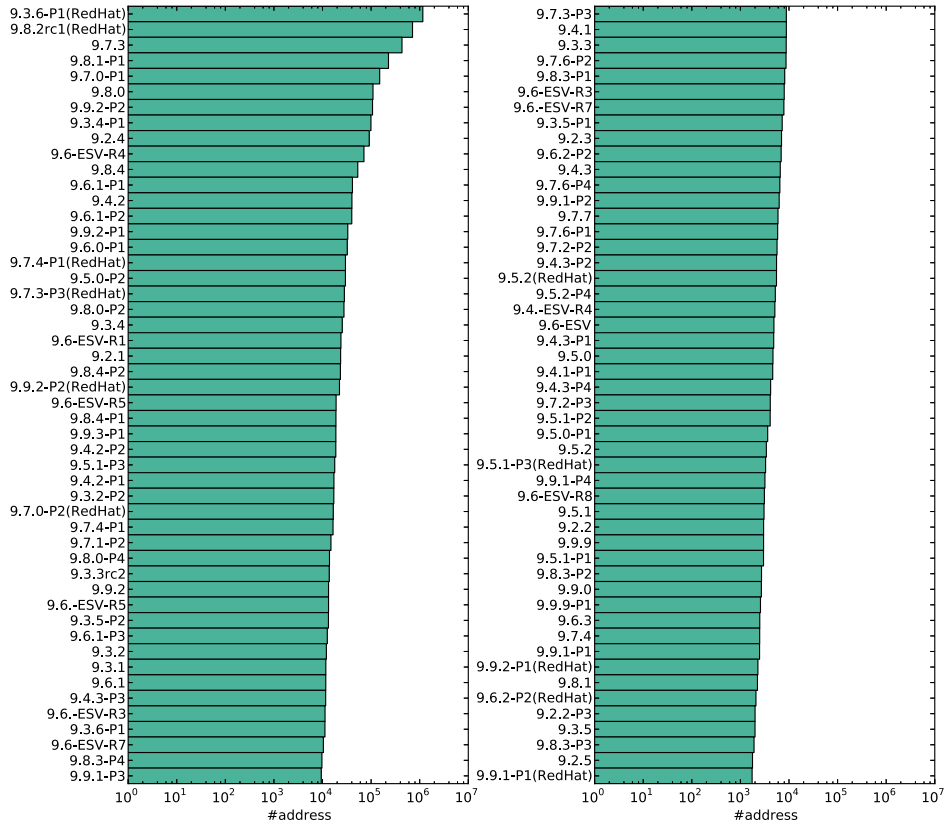


図 3　BIND 9.x シリーズのバージョン分布 (上位 100 位)
Fig. 3　Version distribution of BIND 9.x series (Top 100).

トウェアバージョンを確認することができた．図 3，図 4，図 5 に，それぞれの BIND シリーズのバージョン分布を示す．なお，ここでは，RedHat から提供された BIND のパッケージは，別のバージョンとして数えている．これは，RedHat Linux のために配布される BIND ソフトウェアは，RedHat Linux 独自にバックポーティングされているためである．

計測時の 2013 年 7 月時点で，BIND 9.x シリーズの最新バージョンは，9.9.3-P2，9.8.5-P2，9.7.7 (EOL)，9.6-ESV-R9-P1 となっていた [27]．図 3 から，多くのサーバが最新のバージョンにアップデートされていないことがわかる．また，BIND 8.x と 4.x の最終バージョンは，8.4.7 と 4.9.11 である．

表 2 から，運用されている BIND シリーズの多くが，オープンリゾルバとなっていることがわかる．しかし，BIND は権威 DNS サーバのみとしての運用も可能であるためか，半数以上の BIND シリーズによる DNS サーバはオープンリゾルバとなっていない．

BIND 4.x と BIND 8.x は非常に古い実装であり，2007 年の 8 月に BIND 8.x は the end of life に突入したと公式に発表されたが [28]，我々の計測から，未だに BIND 8.x と BIND 4.x がインターネット上に多く存在することが明らかとなった．更に，表 2 から，BIND 8.x と 4.x は，RIPE NCC に多く存在することがわかる．ただし，本結果をフランスで行われた GreHack 2013 にて発表したところ [29]，参加者から RIPE NCC に BIND 4.x シリーズが多いのはハニーポットであるという指摘を受けたことを注記しておく．

5.2　PowerDNS

図 6 は，PowerDNS のバージョン分布を示しており，我々の計測では合計 22 種類のバージョンを得られることができた．PowerDNS は，PowerDNS Authoritative Server と呼ばれる権威 DNS サーバと PowerDNS Recursor と呼ばれるリゾルビング DNS サーバとして配布されている．図 6 では，10 種類のバージョンしか示していないが，この理由は，PowerDNS は，ごく

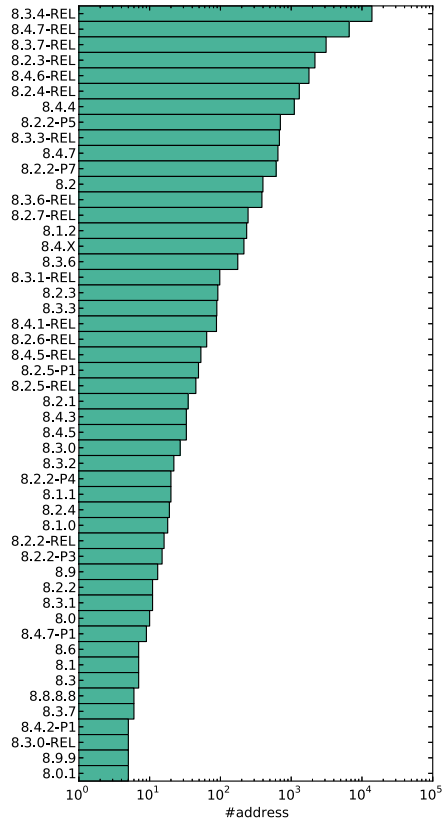


図 4　BIND 8.x シリーズのバージョン分布 (上位 50 位)
Fig. 4　Version Distribution of BIND 8.x series (Top 50).

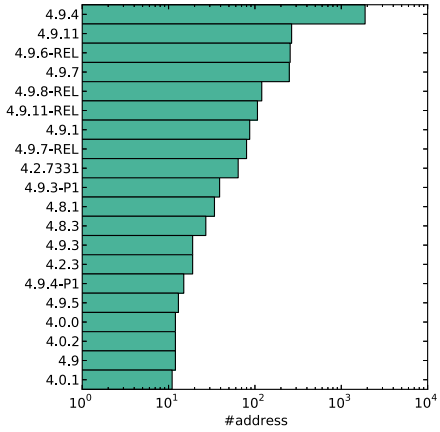


図 5　BIND 4.x シリーズのバージョン分布 (上位 20 位)
Fig. 5　Version distribution of BIND 4.x series (Top 20).

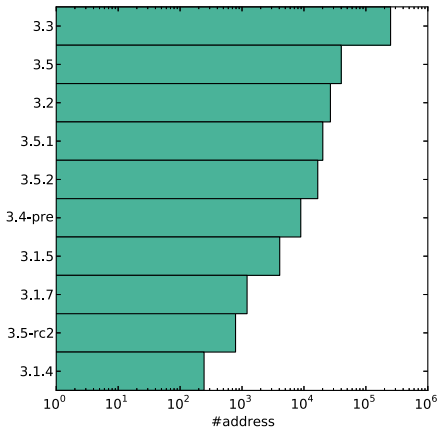


図 6　PowerDNS のバージョン分布 (上位 10 位)
Fig. 6　Version distribution of PowerDNS (Top 10).

最近のリリースであるバージョン 3.0 以降から VERSION.BIND 問い合わせに対応したからである [30]．なお，2013 年 7 月時点の，PowerDNS Authoritative Server と PowerDNS Recursor の最新バージョンは，それぞれ，3.3 と 3.5.2 であった．図 6 から，PowerDNS の場合，最新バージョンが最も多く使われている事がわかる．

表 2 から PowerDNS と判定された，多くのサーバがオープンリゾルバであることがわかる．PowerDNS は権威 DNS サーバとしても利用可能であるが，ほとんどがリゾルビング DNS サーバとして利用されていると考えられる．

5.3　Dnsmasq

Dnsmasq は，小さなネットワークのための，軽量な DNS フォワーダ及び DHCP のソフトウェア実装である．Dnsmasq は大規模なリゾルビング DNS サーバとしての利用は想定されていないにもかかわらず，表 2 から，多くの Dnsmasq がオープンリゾルバとなっておりインターネット上にリゾルビングサービスを提供していることがわかる．また，公開されている Dnsmasq サーバのほとんどがオープンリゾルバとなっていることもわかる．

NAT 下では，UDP/TCP ポートを有効に利用するため，DNS フォワーダが必須となるが，Dnsmasq は NAT を実現するホームルータなどに採用されている場合が多い．ホームルータなどは各家庭で設置されており，これがオープンリゾルバとなっていた場合は，インターネットキャリアなどで制限することは難しく，オープンリゾルバ問題の解決の難しさがわかる．

図 7 に，Dnsmasq のバージョン分布を示す．なお，

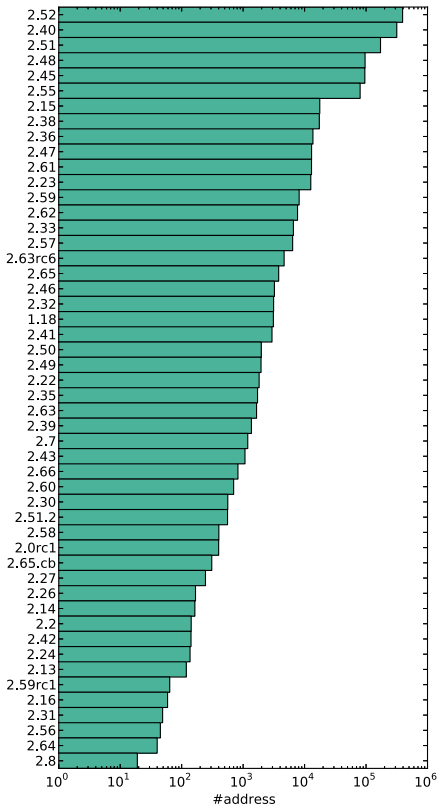


図 7　Dnsmasq のバージョン分布 (上位 50 位)
Fig. 7　Version distribution of Dnsmasq (Top 50).

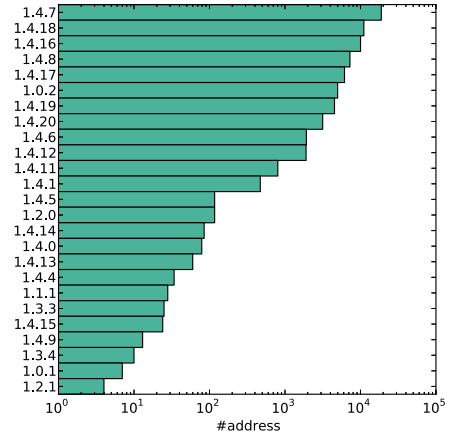


図 8　Unbound のバージョン分布 (上位 25 位)
Fig. 8　Version distribution of Unbound (Top 25).

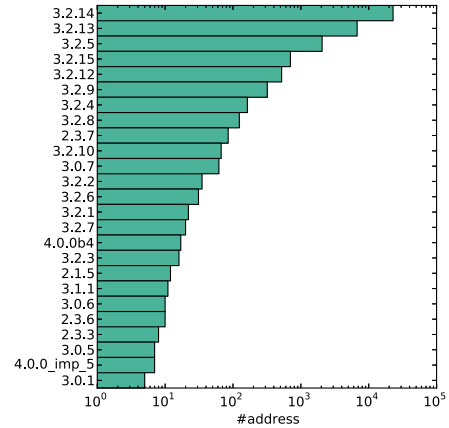


図 9　NSD のバージョン分布 (上位 25 位)
Fig. 9　Version distribution of NSD (Top 25).

我々の計測では，合計 86 のバージョンを取得できた．2013 年 7 月時点では，Dnsmasq の最新バージョンは 2.66 であるが，図に 2.66 は現れていない．

5.4　Unbound 及び NSD

Unbound は DNS キャッシュサーバであり，NSD は権威 DNS サーバであり，どちらも NLnet Labs によって開発されている [31]．図 8 と図 9 に，これらのバージョン分布を示す．我々の計測では，合計 30 の Unbound のバージョンと，42 の NSD のバージョンを取得できた．なお，2013 年 7 月時点の最新バージョンは，Unboud が 1.4.20 であり，NSD が 3.2.15 となる．また，図 8 中の，4.0.0b4 と，4.0.0_imp_5 は，ベータバージョンの NSD 実装であり，ベータバージョンの NSD が少数ではあるが運用されていることが明らかとなった．

表 2 から，Unbound もオープンリゾルバとなっては居るが，他のサーバソフトウェアと比較して，その割合が低くなっている．多くの場合，Unbound ではデフォルトインストール状態では，ローカルからの問い合わせしか受け付けておらず，また，仮に Unbound が利用する UDP ソケットを ANY アドレス (0.0.0.0) にバインドしたとしても，全ての IP アドレスからの問い合わせに応答するという特殊な設定をしなければ，サービスをオープンに公開する事ができない．このように，Unbound をオープンリゾルバとするためには幾ばくか煩雑な手順が必要であるため，このような結果となったと考えられる．また，NSD は基本的に権威 DNS サーバとしてのみ動作するためか，オープンリゾルバとなっている割合が非常に小さい．

5.5　Nominum Vantio 及び Nominum ANS

Nominum Vantio 及び Nominum ANS は，Nominum 社によって開発されている，商用の DNS

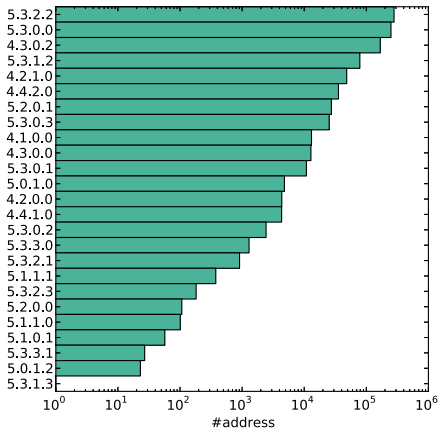


図 10　Nominum Vantio のバージョン分布 (全て)
Fig. 10　Version distribution of Nominum Vantio (All).

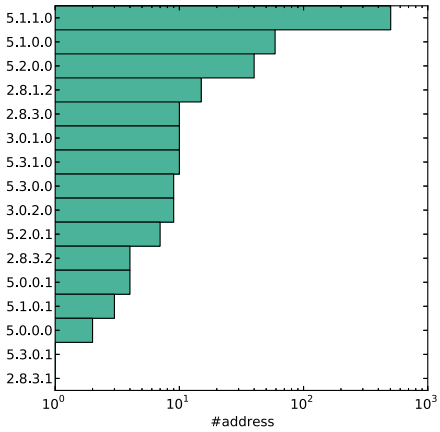


図 11　Nominum ANS のバージョン分布 (全て)
Fig. 11　Version distribution of Nominum ANS (All).

キャッシュサーバ及び権威 DNS サーバである．図 10 と図 11 は，Nominum Vantio 及び Nominum ANS のバージョン分布を示しているが，これらのソースコードは公開されておらず，インターネット上に最新バージョンの情報は公開されていない．しかし，我々の計測から，Nominum Vantio 及び Nominum ANS の最新バージョンは，それぞれ 5.3.3.1 と 5.3.1.0 であると予測できる．

表 2 から，100 万近くの Nominum Vantio によるオープンリゾルバが存在することがわかる．しかし，Nominum Vantio 及び Nominum ANS は非常に高価であり，このように多くのオープンリゾルバが Nominum Vantio であるとは考えにくい．Dnsmasq などの DNS フォワーダでは，VERSION.BIND 問い合わせもそのまま転送するように設定できるため，Nominum Vantio（あるいは他の DNS サーバ）の幾つかは実際には Dnsmasq などの DNS フォワーダである可能性も考えられる．

5.6　その他サーバ

表 2 の can't detect と no version info の行は，VERSION.BIND に対してソフトウェア種別とそのバージョンが判別可能な応答を返答しなかったサーバアドレスの数である．一般的に，セキュリティ対策として，ソフトウェア種別とバージョン情報を非公開にするように推奨されることもあるが，表 2 からもわかるとおり，実際には，VERSION.BIND に正しく応答しないサーバのほとんどがオープンリゾルバとなっており，オープンリゾルバ問題対策という視点から見ると，必ずしも，バージョン情報を非公開にしているサーバが正しい設定を行っているとは限らない事がわかる．

家庭用のルータや家庭用終端端末などには，リゾルビングサービスを行う DNS サーバ・フォワーダが内蔵されているが，これらは独自の実装や，Dnsmasq を流用したものが利用されている．これら機器の DNS サーバは，特殊なバージョン情報（ISP 名など）を返したり，あるいは，バージョン情報問い合わせに応答しない事がある．例えば，バージョン情報としてイタリアにある ISP 名を返す DNS サーバが多数存在することが，我々の調査結果から判明している (注1)．このように，can't detect や no version info にもオープンリゾルバが多いのは，適切な設定をされていない，家庭用ルータや家庭用終端端末が原因であると考えられる．

6.　DNS オープンリゾルバのドメイン毎分布

次に我々は，測定から得られた約 3,000 万の IPv4 アドレスを逆引きし，これらアドレスに関連付けられたドメイン名を調査した．当初，ローカルに設置した Unbound を利用した逆引き用のソフトウェアを実装したが，全ての逆引きが終わるまでに，推定で 2ヶ月以上かかる事が判明したためこの手法は諦めた．そこで，我々は libevent を用いた非同期に大量の逆引きを

(注1)：ちなみに，これが原因で，図 2 で，イタリア付近が赤くなっていると考えられる．

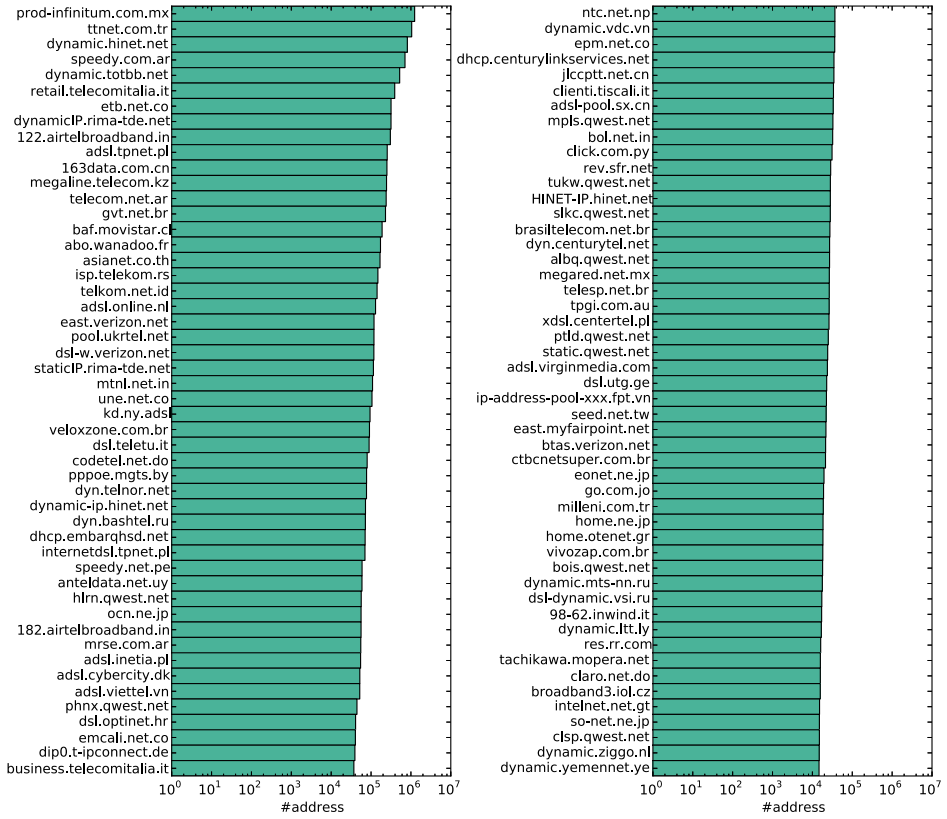


図 12　DNS オープンリゾルバのドメイン分布 (上位 100 位)
Fig. 12　Domain distribution of DNS open resolvers (Top 100).

行える Reverse Lookupper を C++にて作成した．その結果，3,000 万アドレスもの逆引きを，1 台の PC のみで約 5 日間という短い期間で終わらせることができた．

図 12 は，サードレベルドメインまでのオープンリゾルバのドメイン名分布であり，図 13 は，JP トップレベルドメイン (JP TLD) のみ見た，サードレベルドメインまでのオープンリゾルバのドメイン名分布である．

図 12 より，スパムメールの大量発信元とされる，163data.com.cn と hinet.net というドメイン名 [32] が発見することができ，スパムメールの発信元とされるドメインに，多くのオープンリゾルバが存在することが明らかとなった．

一方，JP TLD のオープンリゾルバは，我々の計測によると，合計で 381,387 アドレス取得することができた．図 13 より，NTT コミュニケーションズによるインターネットサービスプロバイダ（ISP）の OCN (ocn.ne.jp) に，JP TLD で最も多くのオープンリゾルバが存在することがわかる．OCN が最も多くなった理由は，OCN は日本で最大の顧客数を誇る ISP である [33] からと考えられる．この事実からも，だれでも自由にオープンリゾルバを運用できる現状，ISP などでコントロールすることが難しいということがわかる．

表 3　探索パケットのクエリタイプ統計
Table 3　Query types of probe packet.

タイプ	#
A	11,972
ANY	268
PTR	7
NS	5
TXT	1

7. サイレントモニタによる DNS サーバ探索パケット検出

DNS アンプ攻撃を行うためには，オープンリゾルバ

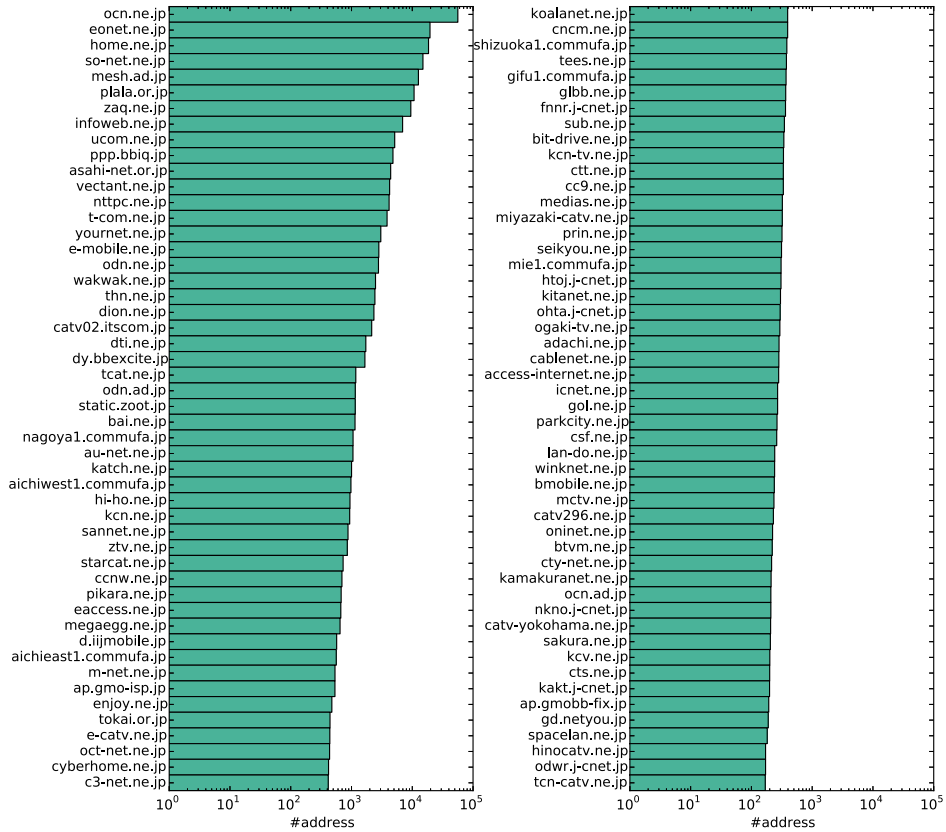


図 13　JP TLD 内におけるオープンリゾルバのドメイン分布 (上位 100 位)
Fig. 13　Domain distribution of DNS open resolvers in JP TLD (Top 100).

を利用する必要があり，オープンリゾルバを利用するためには，世界中に存在するオープンリゾルバを見つける必要がある．オープンリゾルバの発見には，我々が行ったように，IPv4 アドレス空間を探索して発見する方法があるが，この探索パケットは DNS サーバが利用する 53 番ポートを監視することで観測することができる．我々は，2013 年 9 月 28 日から 2014 年 1 月 6 日の約 3ヶ月間にかけて，53 番ポートを監視するサイレントモニタ (1 IP アドレス) を設置し，DNS サーバ探索パケットの観測を行った．

表 3 は，約 3ヶ月間の観測で見つかった DNS パケットのクエリタイプである．ほとんどの DNS 問い合わせは，A レコード問い合わせあることがわかる．表 4 は，探索パケットの問い合わせ名の統計である．我々は，合計で 12,255 リクエストの探索パケットを観測し，更に，そのうち 7,099 のドメイン名を観測した．その結果，問い合わせに使われるドメイン名は様々なものが用いられることが明らかとなった．

表 4　探索パケットのクエリ名統計
Table 4　Query names of probe packet.

クエリ名	#
www.ujiaoban.com.	1,145
vip3.gfdns.net.	666
dnsscan.shadowserver.org.	593
www.iana.org.	143
pay.13hp.com.	84
.	72
ghmn.ru.	48
loo1.ru.	29
isc.org.	28
fkfkfkfa.com.	21

観測を行っていると，定常的に，同一のネットワークから探索パケットが送信されることがわかる．特に顕著なのが，dnsscan.shadowserver.org と，openresolverproject.org からの探索パケット，及び AS 2xxx3 (注2) からの探索パケットである．これらか

(注2)：AS 番号の公開は敏感な問題であるため，本論文では明示的に AS 番号を記すことを避け，一部伏せ字にして表記する．詳細を知りたい場合は主著者の高野 (ytakano@wide.ad.jp) まで連絡されたい．

らは，観測した約 3ヶ月間の間，ほぼ毎日，少なくとも数日おきに探索パケットが観測された．なお，dnsscan.shadowserver.org のプロジェクトは，サイレントモニタによる観測で知ることができた．それ以外にも，オープンな分散型のネットワーク検証プラットホームである PlanetLab [34] からの DNS 探索パケットや，ホスティングサーバからの探索パケットを観測することができた．

8. DNS オープンリゾルバと踏み台利用

DNS アンプ攻撃はオープンリゾルバを踏み台として利用する攻撃手法であり，オープンリゾルバとなっている DNS サーバは攻撃者に勝手に悪用されてしまう．そこで我々は，実際にオープンリゾルバがどのように踏み台として利用されるかを知るために，オープンリゾルバに設定した DNS サーバを複数台用意して，2013 年 9 月 28 日から 2014 年 1 月 6 日の約 3ヶ月間にかけて観測を行った．

観測を行う際に，**7.** で述べた AS 2xxx3 からの問い合わせに応答しないように設定したオープンリゾルバを 2 台 (IP アドレス二つ) と，何も制限を行わないオープンリゾルバを 2 台 (IP アドレス二つ) 用意した．なお，AS 2xxx3 の IP アドレスは，AS 2xxx3 からの BGP (Border Gateway Protocol) 経路広告から割り出し，得られた IP アドレスに対して iptables の OUTPUT フィルタに drop と設定した．観測に利用した DNS サーバソフトウェアは Unbound となる．その結果，AS 2xxx3 からの問い合わせを破棄したオープンリゾルバと，何も制限しないオープンリゾルバで，利用のされ方に大きな違いがでた．

表 5 は，設置したオープンリゾルバに来た DNS 問い合わせのタイプを示している．なお，何も制限しないオープンリゾルバと，AS 2xxx3 を制限したオープンリゾルバは，それぞれ 2 台用意したが，それぞれで違いがみられなかったため，本節では，それぞれ代表の 1 台についてデータを示す．表 5 より，問い合わせに利用されるクエリは ANY クエリが非常に多いことがわかる．ANY クエリは，その増幅率から DNS アンプ攻撃に利用されることが非常に多く，我々の用意したオープンリゾルバが DNS アンプ攻撃の踏み台として利用された可能性が高いことを示している．次に多いのが，A クエリであるが，IP アドレスが大量に割り当てられたドメイン名の場合，これもまた増幅率が高くなることから，DNS アンプ攻撃に利用される．

表 5 オープンリゾルバの利用クエリタイプ統計
Table 5 Query types to open resolver.

タイプ	#	# (AS 2xxx3 破棄)
ANY	33,564,934	14,359,798
A	2,910,108	727,044
TXT	38,292	32,618
RRSIG	4,719	0
MX	1	0
SOA	1	0
SRV	1	1
TYPE0	0	78,088

表 6 ANY クエリ統計
Table 6 ANY query statistics.

クエリ	#queries	#queries (AS 2xxx3 破棄)
pkts.asia.	10,971,788	331
isc.org.	10,926,653	9,369,123
.	2,758,851	2,668,052
krasti.us.	1,974,023	3
fkfkfkfa.com.	1,701,773	20
ym.rctrhash.com.	916,113	1,346,231
ghmn.ru.	689,708	3
x.slnm.info.	650,039	1
lrc-pipec.com.	515,806	21,557
eschenemnogo.com.	452,167	444,744

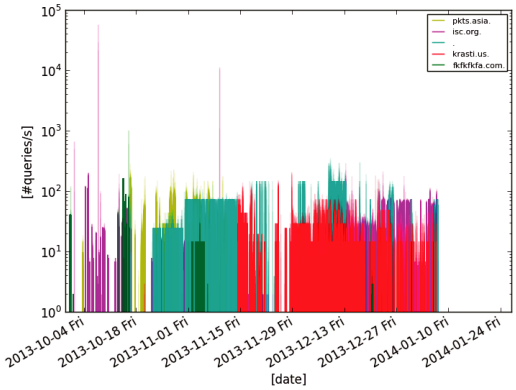
表 7 A クエリ統計
Table 7 A query statistics.

クエリ	#queries	#queries (AS 2xxx3 破棄)
reanimator.in.	873,583	11
ilineage2.ru.	863,495	6
eschenemnogo.com.	711,605	711,703
txt.fwserver.com.ua.	219,073	2
lrc-pipec.com.	210,354	9
ghmn.ru.	18,393	14,894
1x1.cz.	6,798	1
doc.gov.	5,963	0
aa.10781.info.	191	178
dnsscan.shadowserver.org.	101	91

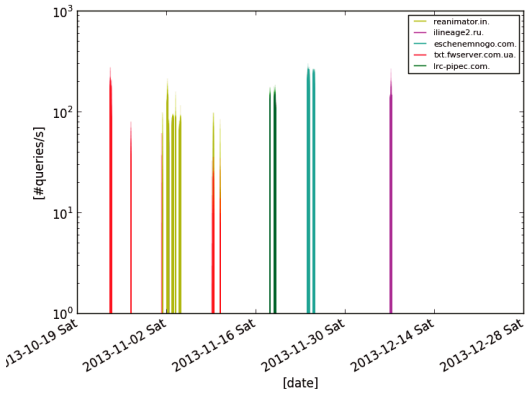
表 5 より，A クエリによる攻撃にも我々のオープンリゾルバが悪用された可能性が高いことがわかる．

次に，ANY クエリと A クエリの内訳を見てみる．表 6 が ANY クエリ，表 7 が A クエリの内訳である．この表からわかるように，AS 2xxx3 からの問い合わせを破棄した場合，pkts.asia. の ANY や，reanimator.in. の A クエリは制限しないオープンリゾルバと比較して非常に少なくなることが明らかとなった．

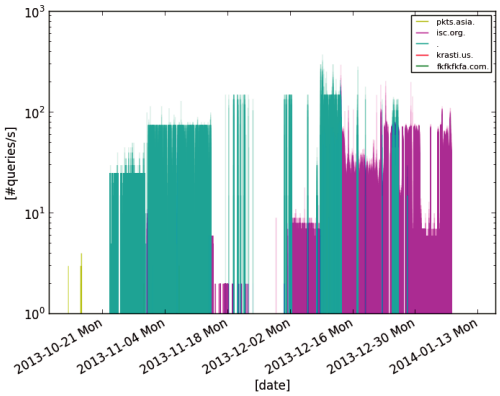
図 14 と図 15 は，用意したオープンリゾルバに来た ANY クエリと A クエリの時間推移を示している．図 14 の制限なしを見ると，ANY クエリを利用した DNS アンプ攻撃が定常的に行われている可能性が，極



(制限なし)
(No Restriction)

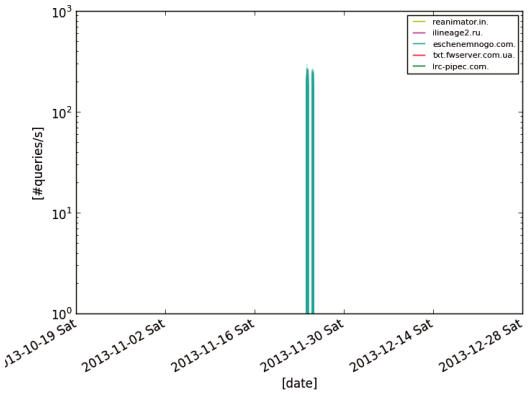


(制限なし)
(No Restricion)



(AS 2xxx3 破棄)
(Drop AS 2xxx3)

図 14　ANY クエリの時間推移
Fig. 14　Time transision of ANY queries.



(AS 2xxx3 破棄)
(Drop AS 2xxx3)

図 15　A クエリの時間推移
Fig. 15　Time transision of A queries.

めて高いことがわかる．その一方，図 15 より，A クエリを利用した DNS アンプ攻撃は集中的な利用のされ方となっている．更に，同様に，これらの図からも，AS 2xxx3 を制限した場合踏み台として利用される事が少なくなることが明らかとなった．

9. 議　　論

本節では，DNS アンプ攻撃に使われる攻撃パケットと，対策，オープンリゾルバ運用の結果について議論を行う．

9.1 攻撃パケットと DNSSEC

DNS アンプ攻撃が成立する理由は，ある特定の DNS クエリに対して，DNS サーバが問い合わせパケットと比較して，何十倍にも増幅された応答パケットを送信するからである．例えば，2013 年 8 月の時点で，isc.org や ripe.net に対する ANY クエリの問い合わせパケットは，それぞれ 64 と 65 バイトであるが，これらに対する応答パケットは，それぞれ，3,245 と 2,669 バイトとなっている．この事実は，dig コマンドを用いて `$ dig any isc.org +bufsize=4096` とすると確認できる．

表 8 に，isc.org と ripe.net に対する ANY クエリに対する応答パケットの内訳を示す．本表より，DNSSEC [35]～[37] 関連のレコードである RRSIG, DNSKEY, NSEC レコードが ANY クエリに対する応答の大部分を占めている事がわかる．これは，DNSSEC による，応答パケットの増大が，DNS アンプ攻撃の引き金となっていることを示唆している．DNSSEC は，インターネットユーザに正当な DNS サーバの応答であることを保証する技術である．例え

表 8　ANY クエリに対する DNS 応答パケットの内訳
Table 8　Breakdown of responce of ANY query.

	isc.org	ripe.net
RRSIG	1,965	1,304
DNSKEY	427	848
NSEC	53	38
SPF	112	-
TXT	181	-
NS	97	136
NAPTR	46	-
A	16	16
AAAA	28	28
MX	24	50
SOA	54	52
Total	3,005	2,472

(bytes)

ば，中国の金盾と呼ばれる検閲システムでは，AS レベルで DNS パケットのスプーフィング攻撃を行って居ることが匿名の著者により報告されたが [3]，DNSSEC を用いると，このようなスプーフィング攻撃を防ぐことができる．しかしながら，DNSSEC に対応するための DNS プロトコルの拡張 [8] が，DDoS 攻撃を可能にしたという負の側面ももつ．

実際に攻撃に使われる DNS パケットは，DNSSEC が要因となった以外にもある．例えば，表 6 にある，pkts.asia や fkfkfkfa.com は単一ドメインに大量の A レコードが割り当てられており，ANY クエリの応答が増大する理由は，A レコードとなっている．また，krasti.us の場合は，大量に割り当てられた MX レコードと，TXT レコードが増幅の原因となっている．これら事実からもわかるとおり，単純に ANY クエリを破棄するだけでは，根本的に DNS アンプ攻撃を防ぐことはできない．実際，我々が行ったオープンリゾルバの運用結果より，RRSIG や A クエリなどを用いて攻撃することが可能であることがわかる．したがって，DNS アンプ攻撃の対策を行うためには，より抜本的な解決が必要であると考えられる．

9.2　DNS アンプ攻撃への対策

DNS プロトコル自体を改良，アップデートすることが，オープンリゾルバ問題に対する最も抜本的な解決方法である．UDP パケットの送信元アドレスを詐称して行われる DNS アンプ攻撃を防ぐには，DNS プロトコルに送信元の正当性検査する機能を組み込む必要がある．これは，UDP ではなく TCP を用いることで，達成することができる．TCP はコネクション指向のプロトコルであるため，通信のはじめに 3 ウェイハンドシェイクによるコネクション確立を行うため，UDP と違って，容易に，送信元を偽装して通信することはできない．しかし，TCP を用いると DNS の応答時間が増大してしまう（UDP では 1 RTT のところ，TCP だと最低でも 2 RTT 必要となる）．これは極力応答時間を短くする必要がある DNS にとって問題となる．だが，これは，純粋な TCP を利用するのではなく，高速な TCP コネクション確立を実現する TCP Fast Open [38] や，ASAP [39] を用いることで，応答時間に関する問題は緩和可能であると考えられる．

インターネット上に存在する，2,500 万台近くにのぼる全てのオープンリゾルバを停止，あるいは正しく設定させることはもう一つの抜本的な解決方法である．しかしながら，本方法は自律分散的に管理されているインターネットの性質上困難であると予想される．たとえ日本中全てのオープンリゾルバを根絶できたとしても，それは，全体の一部にしか過ぎないため効果は薄い．更に，**6.** で述べたように，スパムメールの発信元とされるネットワークにオープンリゾルバが多いという事実や，**5.** で述べたように，BIND 4.x と 8.x という古い実装の DNS サーバが未だに運用される事実を鑑みるに，全ての DNS サーバを制御することは困難であると予想される．

各 ISP が，適切な Egress フィルタを設定し，送信元アドレスを詐称したパケットをインターネット上に送信できないようにする方法は，もう一つの解決方法である．本方式は，DNS アンプ攻撃のみではなく，送信元アドレスを偽装した他の攻撃にも有効であり，更に ISP のコアネットワークレベルで対策可能ある．しかし，適切な Egress フィルタの設定はそれなりのコストが必要となる．uRPF [40] はルーティングテーブルをフィルタリングに応用した技術であり，送信元アドレスとルーティングテーブルを照合し，送信元アドレスが経路として存在しなかった場合パケットを破棄する．uRPF の適用は，送信元アドレス偽装に対して効果が高い上に，比較的現実的であると考えられる．しかしながら，依然として，全ての ISP に強制するということはできないという問題は残る．

9.3　攻撃元の特定

8. で，サイレントモニタで観測した DNS サーバ探索パケットの送信元ネットワークへの通信を遮断することで，オープンリゾルバの利用され方に大きな違いが出ることが明らかとなったが，この原因には以下で述べる三つの仮説が考えられる．

一つめは，偶然，そうなったというものである．オー

プンリゾルバの利用のされ方が大きく異なるのは，ネットワーク通信の遮断とは何ら因果関係がなく，我々の設置したオープンリゾルバがたまたま異なる利用のされ方をしたに過ぎないという仮説である．我々は，実際に，偶然このような結果になったのではないかと疑ったため，他にも数カ所，ネットワーク的に異なる場所で，1 週間程度のオープンリゾルバ運用・観測を行ったが，やはり AS 2xxx3 を遮断したオープンリゾルバは利用されることが少なかった．そのため，本仮説が原因である確率は低いと考えられる．

二つめは，我々のオープンリゾルバで取得しているデータを損なわせる事を目的として，何者かが悪意のあるパケットを，我々の用意したサーバに送信したという仮説である．しかしながら，これも，他の場所で行った短期間のオープンリゾルバ運用の結果から，可能性は低いと考えられる．

三つめは，AS 2xxx3 のネットワークの所有者が行ったのか，あるいは AS 2xxx3 のネットワークが悪用されたのかは分からないが，攻撃者が AS 2xxx3 のネットワークを利用して DNS サーバ探索を行い DDoS 攻撃を行っているという仮説である．**7.** 及び **8.** の結果から，本仮説が有力であると考えられる．

もし，三つめの仮説が正しいとしたら，サイレントモニタ，オープンリゾルバ，BGP から得られるデータを組み合わせて利用することで，攻撃元ネットワークを特定することがある程度可能であり，DNS アンプ攻撃に対する防御技術にも利用可能であると考えられる．

9.4 攻撃対象

DNS アンプ攻撃は UDP の送信元アドレスを攻撃対象に詐称して行われるため，オープンリゾルバへと来た問い合わせパケットの送信元アドレスを調べると，何処に向けての攻撃か知ることができる．本研究の調査で得られた攻撃対象の詳細を公開することは，攻撃対象となったネットワークの不利益に繋がる可能性があるため，本節にて簡単に議論を行うに留める．

8. では，増幅率の大きい，ANY クエリや，特定ドメイン名に対する A クエリがオープンリゾルバへの問い合わせとして，非常に多く利用されていることを示した．これら問い合わせパケットの送信元アドレスを調べたところ，様々であったが，データセンタやクラウド・ホスティングサイトに対する攻撃が多いことが判明した．これは，サービス妨害攻撃という名前の示すとおり，昨今では，データセンタやクラウドサービス上にてインターネットサービスが多く運用されているからと考えられる．

10. むすび

DNS アンプ攻撃はオープンリゾルバと呼ばれる，オープンにサービスを公開しているリゾルビング DNS サーバを踏み台として利用した DDoS 攻撃であり大きな問題となっている．本研究では，そのオープンリゾルバについてアクティブ検索，サイレントモニタ観測，実際のオープンリゾルバ運用という多角的な視点から調査を行い，本論文にてオープンリゾルバの詳細を報告した．

我々が行ったアクティブ検索によると，約 3,000 万以上の DNS サーバがインターネット上に存在し，そのうち約 2,500 万もがオープンリゾルバとなっていることが明らかとなった．また，我々は，DNS サーバのバージョン調査をも行った．その結果，BIND 8.x や 4.x シリーズという非常に古いソフトウェア実装が未だに存在することが明らかとなり，小規模ネットワーク向けの DNS フォワーダである Dnsmasq や，DNS サーバソフトウェアの PowerDNS の多くがオープンリゾルバとなっていることが明らかとなった．また，他と比較して割合は少ないものの，Unbound や BIND 9.x シリーズの一部もオープンリゾルバとなっていることが明らかとなった．また，調査によって得られたオープンリゾルバの IP アドレスを逆引きした結果，スパムメールの発信元とされるドメインに多くのオープンリゾルバが存在することが明らかとなった．

更に，サイレントモニタを用いた観測を行うことで，DNS サーバ探索パケット観測することができることを示し，観測の結果，dnsscan.shadowserver.org，openresolverproject.org，AS 2xxx3 からの探索パケットを多く見つけることができた．また，探索に利用されるクエリは A レコード問い合わせであることも明らかとなった．

次に，我々は実際にオープンリゾルバ運用を行い，攻撃パケットの観測を行った．その結果，攻撃には増幅率の大きい ANY クエリと，特定の A クエリが多く利用されることが明らかとなった．また，AS 2xxx3 からの問い合わせを破棄するオープンリゾルバと，何も制限しないオープンリゾルバの 2 種類を用意し比較した結果，利用のされ方が大きく異なることが明らかとなり，AS 2xxx3 のネットワークが DNS アンプ攻撃に悪用された可能性が大きいことを示した．

謝辞　本研究を支えていただいた北陸先端科学技術大学院大学の篠田陽一教授に感謝します．また，本研究で利用したネットワークと PC 環境の整備を行っていただいた，北陸先端科学技術大学院大学の明石邦夫君に感謝します．

文　献

[1] P.V. Mockapetris, “Domain names - concepts and facilities,” RFC 1034 (INTERNET STANDARD), Nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936. http://www.ietf.org/rfc/rfc1034.txt

[2] P.V. Mockapetris, “Domain names - implementation and specification,” RFC 1035 (INTERNET STANDARD), Nov. 1987. Updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604. http://www.ietf.org/rfc/rfc1035.txt

[3] Anonymous, “The Collateral Damage of Internet Censorship by DNS Injection,” SIGCOMM Computer Communication Review, vol.42, no.3, pp.21–27, 2012. http://conferences.sigcomm.org/sigcomm/2012/paper/ccr-paper266.pdf

[4] M. Borella, D. Grabelsky, J. Lo, and K. Taniguchi, “Realm Specific IP: Protocol Specification,” RFC 3103 (Experimental), Oct. 2001. http://www.ietf.org/rfc/rfc3103.txt

[5] “Understanding Kaminsky’s DNS Bug - Linux Journal,” http://www.linuxjournal.com/content/understanding-kaminskys-dns-bug

[6] “US-CERT Alert(TA13-088A) DNS Amplification Attacks,” http://www.us-cert.gov/ncas/alerts/TA13-088A

[7] “CloudFlare - The DDoS That Knocked Spamhaus Offline (And How We Mitigated It),” http://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho

[8] J. Damas, M. Graff, and P. Vixie, “Extension Mechanisms for DNS (EDNS(0)),” RFC 6891 (INTERNET STANDARD), April 2013. http://www.ietf.org/rfc/rfc6891.txt

[9] M. Handley, E. Rescorla, and IAB, “Internet denial-of-service considerations,” RFC 4732 (Informational), Dec. 2006. http://www.ietf.org/rfc/rfc4732.txt

[10] “Open Resolver Project,” http://openresolverproject.org/

[11] “The Shadowserver Foundation: DNS Scanning Project,” https://dnsscan.shadowserver.org/

[12] Steve Santorelli, “The global open resolver picture,” http://www.securityacts.com/securityacts03.pdf#page=29

[13] J. Dean and S. Ghemawat, “MapReduce: Simplified Data Processing on Large Clusters,” OSDI, pp.137–150, USENIX Association, 2004.

[14] “MongoDB,” http://www.mongodb.org/

[15] “Boost C++ Library,” http://www.boost.org/

[16] “libevent,” http://libevent.org/

[17] “Catenaccio DPI,” https://github.com/ytakano/catenaccio_dpi

[18] “IANA IPv4 Address Space Registry,” http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.txt

[19] “Internet Systems Consortium — BIND,” http://www.isc.org/downloads/bind/

[20] “Authoritative DNS — Nominum,” http://www.nominum.com/products/core-engines/authoritative-dns/

[21] “Welcome to PowerDNS,” https://www.powerdns.com/

[22] “nlnetlabs.nl :: Name Server Daemon (NSD) ::,” http://www.nlnetlabs.nl/projects/nsd/

[23] “Dnsmasq - a DNS forwarder for NAT firewalls,” http://www.thekelleys.org.uk/dnsmasq/doc.html

[24] “Vantio Caching DNS — Nominum,” http://www.nominum.com/products/core-engines/caching-dns/

[25] “Unbound,” http://unbound.net/

[26] “GeoIP Products ≪ Maxmind Developer Site,” http://dev.maxmind.com/geoip/

[27] “Internet Systems Consortium — BIND Software Status,” http://www.isc.org/downloads/software-support-policy/bind-software-status/

[28] “BIND8 entering end of life,” https://lists.isc.org/pipermail/bind-announce/2007-August/000222.html

[29] R. Ando, Y. Takano, and S. Uda, “Unraveling large scale geographical distribution of vulnerable DNS servers using asynchronous I/O mechanism,” 2013.

[30] “PowerDNS Authoritative Server 3.0 Release Notes,” http://doc.powerdns.com/html/changelog.html#changelog-auth-3-0

[31] “nlnetlabs.nl :: Home ::,” http://nlnetlabs.nl/

[32] C.A. Shue, M. Gupta, J.J. Lubia, C.H. Kong, and A. Yuksel, “Spamology: A Study of Spam Origins,” The 6th Conference on Email and Anti-Spam (CEAS), 2009.

[33] “OCN Top Page,” http://www.ocn.ne.jp/

[34] “PlanetLab — An open platform for developing, deploying, and accessing planetary-scale services,” https://www.planet-lab.org/

[35] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, “DNS security introduction and requirements,” RFC 4033 (Proposed Standard), March 2005. Updated by RFCs 6014, 6840. http://www.ietf.org/rfc/rfc4033.txt

[36] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, “Resource records for the DNS security extensions,” RFC 4034 (Proposed Standard), March 2005. Updated by RFCs 4470, 6014, 6840, 6944. http://www.ietf.org/rfc/rfc4034.txt

[37] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, “Protocol modifications for the DNS security extensions,” RFC 4035 (Proposed Standard), March 2005. Updated by RFCs 4470, 6014, 6840. http://www.ietf.org/rfc/rfc4035.txt
[38] “TCP Fast Open (IETF Draft),” https://tools.ietf.org/html/draft-ietf-tcpm-fastopen-04
[39] W. Zhou, Q. Li, M. Caesar, and B. Godfrey, “ASAP: A low-latency transport layer,” CoNEXT, ed. K. Cho and M. Crovella, p.20, ACM, 2011.
[40] F. Baker and P. Savola, “Ingress filtering for multihomed networks,” RFC 3704 (Best Current Practice), March 2004. http://www.ietf.org/rfc/rfc3704.txt

（平成 26 年 1 月 30 日受付，5 月 12 日再受付）

高野　祐輝

2001 年石川工業高等専門学校電気工学科卒業．2003 年同学専攻科電子機械工学専攻修了．2005 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．2011 年同学博士後期課程修了（情報科学）．2011～2012 年同学高信頼ネットワークイノベーションセンターにて研究員として勤務．ネットワーク技術の研究に従事．2012 年より現在まで，情報通信研究機構にて，研究員として勤務．ネットワークセキュリティの研究に従事．2013 年より，北陸先端科学技術大学院大学プロジェクト研究員として，ネットワーク技術の研究に従事．

安藤　類央

2006 年慶應義塾大学政策・メディア研究科後期博士課程修了（政策・メディア）．同年情報通信研究機構所属．ネットワークセキュリティ，仮想化システムセキュリティの研究に従事．

宇多　　仁

2004 年北陸先端科学技術大学院大学博士後期課程修了，博士 (情報科学)．同年北陸先端科学技術大学院大学情報科学センター助手．2006 年同助教，情報通信研究機構北陸 StarBED 研究センター特別研究員．ネットワークアーキテクチャ並びにインターネット運用技術に関する研究に従事．

高橋　健志　（正員）

平 13 早稲田大学卒，平 14 同大大学院修士課程了，平 17 同大博士後期課程了．Tampere University of Technology(研究員)，日本学術振興会 (特別研究員)，株式会社ローランド・ベルガー (コンサルタント) を経て，現在，独立行政法人情報通信研究機構にて主任研究員．主として通信プロトコル，ネットワークセキュリティ，情報アーキテクチャの研究に従事．国際標準化活動にも従事し，ITU-T 及び IETF に技術提案，IETF MILE Working Group co-chair．ACM，IEEE，電子情報通信学会各会員．

井上　朋哉

2003 年石川工業高等専門学校専攻科電子機械工学専攻修了．同年株式会社 PFU 勤務，2006 年北陸先端科学技術大学院大学情報科学研究科博士前期課程修了．2009 年株式会社 Clwit 勤務．2012 年北陸先端科学技術大学院大学博士後期課程博士後期課程終了．同年北陸先端科学技術大学院大学高信頼ネットワークイノベーションセンター研究員．P2P ネットワーク，分散ネットワークソフトウェアの研究開発に従事．博士（情報科学）