Computer Security Symposium 2013
21 - 23 October 2013

ダークネットモニタリングによるDNSトラフィック分析

中里 純二† 島村 隼平‡ 衛藤 将史† 井上 大介† 中尾 康二†

†情報通信研究機構
184-8795 東京都小金井市貫井北町 40201
{nakazato, eto, 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 2013 年 3 月に，ロンドンのスパム対策組織 SPAMHOUSE に対して大規模な DNS リフレクション攻撃が行われ，ヨーロッパのインターネットが麻痺するなど DNS を用いた攻撃の対策が重要となってきている．本論文では，ダークネットモニタリングによる DNS トラフィック分析を行うことで，DNS サーバへのスキャンや，DNS サーバからのバックスキャッタ（送信元を詐称した問合せに対する応答）の特徴を分析する．スキャンや攻撃の目的を明らかにすることで今後の対策技術への応用が期待される．

DNS Traffic Analysis by Darknet Monitoring

Junji Nakazato† Jumpei Shimamura‡ Eto Masashi† Daisuke Inoue†
Koji Nakao†

†National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, JAPAN
{nakazato, eto, dai, ko-nakao}@nict.go.jp

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

Abstract In March 2013, large DNS reflection attack has been occured to the anti-spam organization SPAMHOUS of London. It is important to take measure for such a attack, because European Internet was paralyzed. In this paper, we analyze characteristics of a scan to the DNS server and a backscatter from the DNS server, by analyzing DNS traffic based on a darknet monitoring.

1 はじめに

2013年3月，スパム対策組織のSPAMHOUS[1]に対して大規模なサイバー攻撃が行われた．この攻撃には，オープンリゾルバとして動作するDNS サーバが利用された．送信元を詐称したDNS 要求パケットをオープンリゾルバに対して送信すると，そのサーバ内にキャッシュされている情報をIP アドレスの詐称されたホストへと返答する．このときDNS の特徴として，要求パケットサイズよりも返答パケットサイズの方が遥かに大きくなる事があるため，攻撃者は効

率よく標的に対して大量のデータを送りつけ攻撃する事が出来る．実際に，SPAMHOUS への攻撃では最大で 300Gbps にもなったと言われている．このように，DNS リゾルバを用いた攻撃は．DNS サーバの跳ね返りを使う事から DNS リフレクション攻撃や，通信量が増幅される事から DNS アンプ攻撃などとも呼ばれている．

DNS を用いた攻撃の対策技術としてさまざま研究が現在までにされている [2, 3, 4, 5, 6, 7, 8]．ダークネットを用いた DNS 分析では [4] がある．[4] では，ダークネットに到達する DNS 要求だけを対象としている．そこで本論文では，ダークネットで観測可能な DNS 要求（DNS スキャン）と送信元が詐称された DNS 要求に対する応答（DNS バクスキャッタ）の両方を対象とした分析を行う．対象とするダークネットデータには NICTER darknet Dataset 2013[9] の通信データと nicter で観測している同規模（/20）のダークネット通信データを用いる．

本論文では，2 節でデータセットに含まれる通信およびダークネットで観測された DNS 通信の統計データを示す．3 節では，DNS スキャンや DNS バックスキャッタの特徴を述べて，最後に 4 節でまとめる．

2 DNS トラフィック

ダークネット観測では，特定の IP アドレスに対するスキャンや IP アドレスを詐称した攻撃の跳ね返り（バックスキャッタ）を捉える事ができる．NICTER darknet Dataset 2013[9] では /20 のネットワーク（2048 個の IP アドレス）宛の通信の観測結果が含まれている．本論文では，特に DNS トラフィックに着目した分析を行う．ダークネットで観測可能な DNS 通信としては，

1. ダークネットアドレスへの DNS クエリ（DNS サーバスキャン）
2. ダークネットアドレスを詐称したクエリに対するレスポンス（DNS サーバからのバックスキャッタ）

を観測する事ができる．そこで，NICTER darknet Dataset 2013 から 53/UDP 宛の通信または 53/UDP からの通信を抽出し，2.1.2 節で説明する Question セクションに含まれる問合せドメインを分析する．

表 1: DNS ヘッダフィールド概要

フィールド		概要
ID		問い合わせと応答を識別するために用いられる．問い合わせ時にクライアントが設定し，応答にも同じ値が用いられる．
フラグ	QR	問い合わせ時に 0 を設定（クライアント）．応答時に 1 を設定（サーバ）．
	OPCODE	問い合わせ内容の詳細（Operation Code）．
	AA	応答内容が再帰的に探索されたか否か．返答したサーバが直接知っている情報（権威サーバ）であれば 1 が設定される（Authoritative Answer）．
	TC	応答内容が 512 byte を超えたかどうか．512 byte を超えた場合 1 が設定され，通常は TCP による接続が行われる（Truncated）．
	RD	再帰的な問い合わせを要求するか否か．要求する場合は 1 を設定する（Recursion Desired）．
	RA	サーバが再帰的な問い合わせに対応しているか否か．再帰的な問い合わせに対応している場合 1 を設定する（Recursion Available）．
	Z	予約．
	RCODE	応答ステータス（Return Code）．
Question セクション数		問い合わせ数．
Answer セクション数		応答数．
Authority セクション数		応答に対するオーソリティ数
Addition セクション数		追加情報数．

2.1 DNS パケットフォーマット

2.1.1 DNS パケットヘッダ

DNS は複数の RFC により定義されている．特に RFC 1035[10] には DNS パケットが 12 byte のヘッダと Question セクション，Answer セクション，Authority セクション，Additional セクションから構成される事が示されている．12 byte のヘッダの中には，2 byte の ID，2 byte のフラグ，各セクションの個数が 2 byte づつの情報で含まれている．**図 1** にヘッダ構成を，**表 1** に各フィールドの概要を示す．OPCODE や RCODE は RFC 6895[11] で詳細が規定されている．また，その他のパラメータも IANA（Internet Assigned Number Authority）にまとまっているので参照されたい [12]．

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ID															
QR	OPCODE				AA	TC	RD	RA	Z			RCODE			
Question セクション数															
Answer セクション数															
Authority セクション数															
Addition セクション数															

図 1: DNS パケットヘッダ構成

ダークネットに対して DNS 問い合わせを行う事は，DNS サーバへのスキャンであることが考えられる．また，DNS 問い合わせに対する応答は，送信元を詐称した問い合わせに対する応答である．そこで本論文では，DNS 問い合わせを行うパケット（QR フィールドに 0 が設定されたパケット）を DNS スキャン（パケット）と呼び，DNS 応答パケット（QR フィールドに 1 が設定されたパケット）を DNS バックスキャッタ（パケット）と呼ぶ．

2.1.2 Question セクション

Question セクションには，ユーザが問合せを行いたいドメイン，そのクラスとタイプが格納される．例えば，`www.example.com` の IP アドレスを問い合わせる場合（正引きの場合），ドメインは “`www.example.com`”，タイプは “A”，クラスはインターネットを表す “IN” が設定されて問合せが行われる．逆引きの場合（IP アドレスからドメイン名を問い合わせる場合）は，“IP アドレスの逆順．in-addr.arpa” というドメイン情報を設定する．例えば，a.b.c.d という IP アドレスからドメイン名を逆引きする場合は “d.c.b.a.in-addr.arpa” というドメインの問合せになる．

2.1.3 Answer セクション

Answer セクションには，ユーザの問合せに対する応答結果が格納される．問い合わせられたドメインに対する IP アドレスや別名（CNAME）を持っていればその別名と対応する IP アドレス情報などがセットされる．

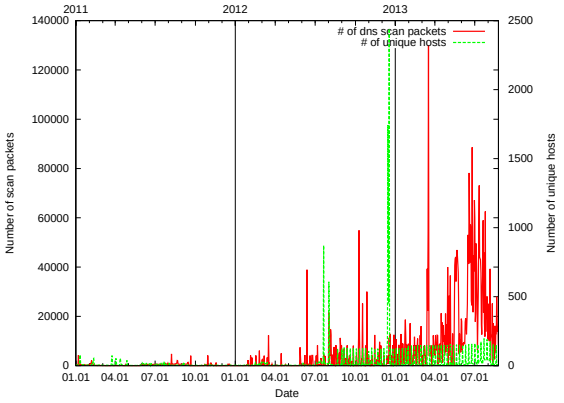

図 2: DNS スキャン統計（期間：2011/01/01 〜 2013/08/25）

2.1.4 Authority セクション

Authority セクションでは，問合せが行われた（Question セクションに指定された）ドメインを管理している DNS サーバ（権威サーバ）の情報がセットされる．

2.1.5 Addition セクション

Addition セクションでは，Authority セクションにセットされた DNS サーバの IP アドレスなどの追加情報が格納される．

2.2 DNS スキャン

ここでは，DNS スキャンの傾向を示す．**図 2** に 2011 年 1 月 1 日から 2013 年 8 月 25 日の間に /20 のダークネットで観測された DNS スキャンパケット数および，ユニークな DNS スキャン送信ホスト数を，**図 3** にそれぞれの 30 日間の移動平均を示す．**図 2**，**図 3** より，2011 年や 2012 年の 7 月頃までは目立ったスキャンは観測されていない．一方で，2012 年 8 月以降は，ユ

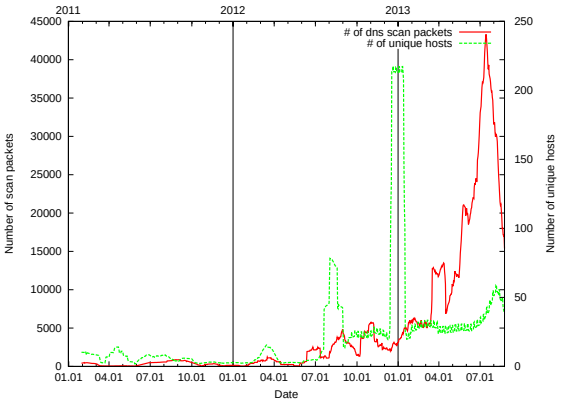

図 3: DNS スキャンの 30 日間の移動平均

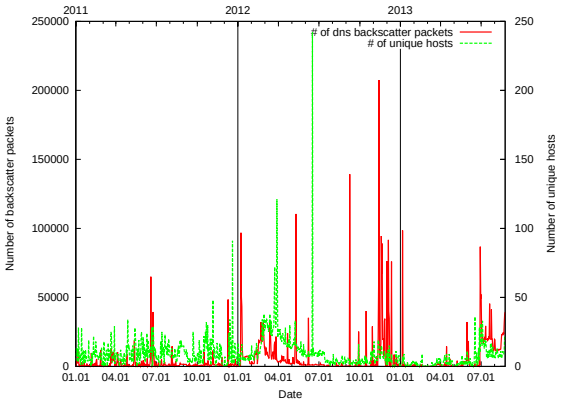

図 4: DNS バックスキャッタ統計（期間：2011/01/01 〜 2013/08/25）

ニークホスト数は周期性を持った増加が観測されている．実際にはほぼ 7 日間（1 週間）毎に 150 前後のホスト（IP アドレス）からのスキャンを観測している．また，これらの送信元は同一のネットワーク（/23）に属している IP アドレスであることを確認した．2012 年 12 月 18 日には観測期間で最大の 2,400 ホスト以上からのスキャンを観測した．1 ホスト辺りの送信パケット数は多くて 3 パケットであるため，ボットなどを利用した大規模な DNS スキャンまたは，送信元を詐称した DNS スキャンが行われた事が考えられる．

DNS スキャンパケットも 2012 年 8 月頃から 2013 年 6 月頃まで増加傾向にある事が分かる．しかし，2013 年 6 月末をピークに減少傾向になっている．2013 年 3 月 18 日には観測期間で最大の約 13 万パケットのスキャンを観測した．これらのパケットは 1 つのホストから送信されていた．また，2013 年 6 月 26 日に増加傾向のピークを迎えているが，このときスキャンパケット数は約 9 万であったのに対して，送信元ホスト数は 17 ホストと一つのホストが多くのスキャンを行っている事が分かる．

2.3 DNS バックスキャッタ

ここでは，DNS バックスキャッタの傾向を示す．**図 4** に 2011 年 1 月 1 日から 2013 年 8 月 25 日の間に /20 のダークネットで観測された DNS バックスキャッタパケット数および，ユニークな DNS バックスキャッタ送信ホスト数を，**図 5** に

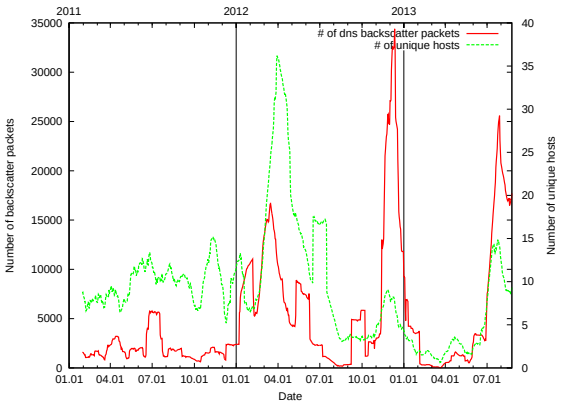

図 5: DNS バックスキャッタの 30 日間の移動平均

それぞれの 30 日間の移動平均を示す．**図 4**，**図 5** より，2012 年 2 月頃よりホスト数，パケット数共に急激な増加を観測したが，直ぐに減少傾向に転じていることが分かる．再び 2013 年 7 月頃にホスト数，パケット数共に急激な増加を観測している．ホスト数は 2012 年 6 月 17 日に観測期間で最大の約 200 ホスト観測した．このとき観測したホストの多くは 1 ホスト辺り 2〜4 パケット程度の非常に少ないパケットを送信していた．

DNS バックスキャッタパケット数は 2012 年 11 月 14 日に最大の約 20 万パケットを観測した．このとき，同一のネットワーク（/16）に属している 8 ホストから，全体の約 97% のパケットを観測した．

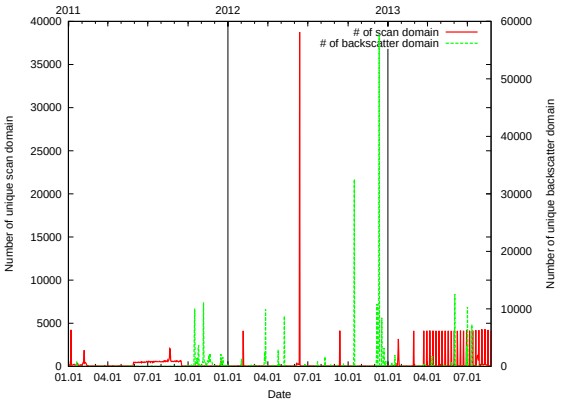

図 6: 問合せドメイン数統計（期間：2011/01/01 ～ 2013/08/25）

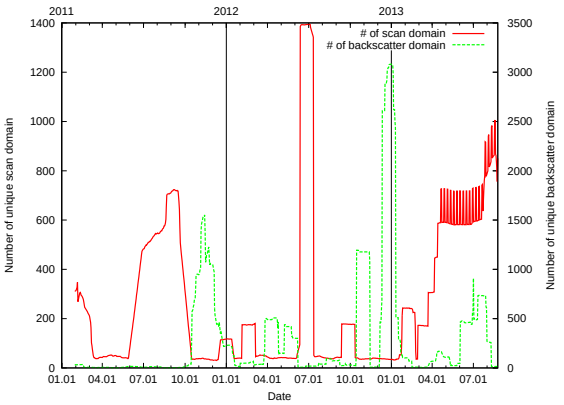

図 7: 問合せドメイン数の 30 日間の移動平均

3　DNS トラフィック分析

ここでは，ダークネットで観測可能な DNS トラフィックの分析を行う．特に 2.1.2 節で説明した Question セクションに格納されたドメイン名に着目した分析を行う．問合せドメイン名による分析を行う事で，DNS スキャンの目的や，DNS バックスキャッタの原因を分析する．

図 6，**図 7** に DNS スキャンに含まれるユニークなドメイン数と DNS バックスキャッタに含まれるユニークな問合せドメイン数の推移を示す．**図 6**，**図 7** より，DNS スキャンに用いられるドメイン数は周期的な増減がある事が分かる．また多くの場合，DNS スキャンのドメイン数が増えた後に，DNS バックスキャッタに現れるドメイン数が増えている事が分かる．

DNS スキャンに現れた総ドメイン数（観測期間中に現れた問合せドメインの種類数）は約 18 万ドメインであった．DNS バックスキャッタに現れた総ドメイン数は約 27 万ドメインであった．このうち，DNS スキャンと DNS バックスキャッタの両方に現れたドメイン数は 42 ドメインであった．DNS スキャンと DNS バックスキャッタの両方に現れるドメイン数が非常に少ない事から，DNS サーバを探索する様なスキャンでは，送信元 IP アドレスを詐称した問合せを行う事は非常に少なく，既に DNS サービスを提供している事が分かっているサーバに対しては，送信元 IP アドレスを詐称して問合せを行う事が多い事が考えられる．**表 2** に観測期間中に DNS スキャン，DNS バックスキャッタの両方に現れたドメインの第 2 レベルドメインまでの情報を示す（SLD.TLD）．

表 2: 共通 DNS ドメインリスト（第 2 レベルドメインまで）

134114.com
137fu.com
159119.com
6789pk.com
VERSION.BIND
baidu.com
com.tr
dnsresearch.us
facebook.com
google.com
huituzi.net
isc.org
microsoft.com
qq.com
taomir.com
wyb.name
yingzhoushi.com

3.1　DNS スキャン分析

ここでは，DNS スキャンに用いられる問合せドメインの分析を行う．**図 2**，**図 6** より，DNS スキャンでは送信元 IP アドレス数や問合せドメイン数に周期的な増減が確認できる．周期的なホスト数の増減は 2.2 節で前述したように，同一のネットワーク（/23）に属する IP アドレスからほぼ 1 週間毎にスキャンが行われている．ことのとき，問合せを行うドメインは “www.google.com” であり，ID 値（**表 1** 参照）は 2013 年 1 月までは全て同じ値が設定されていた．2013 年 2 月以降は ID 値が全て異なる値

に変更され，スキャンの方法に何らかの変更が加えられた事が考えられる．また，問合せドメインはDNSスキャンとDNSバックスキャッタ共通のドメイン（**表 2**）である事から，送信元IPアドレスが詐称されている事も考えられる．これらのスキャンがボットなどによるスキャンであった場合，2013年2月にボット自身のアップデートが行われた事が考えられる．

一方で，ドメイン数の周期的な増減は2013年3月末からホスト数の増減と同様にほぼ1週間周期で起こっている．しかし，ホスト数の増減とは異なるタイミングで起きており，同一の事象である事は考えにくい．このとき，問合せを行うドメインは“xxxxxxxx.openresolverproject.org”であり，ID値は全て異なるものであった．“xxxxxxxx”の部分には送信先IPアドレス毎に異なる英数列が用いられ，/20の全センサ宛てに1パケットづつ送信されている．また，全ての問合せに対してRDフラグ（**表 1** 参照）がセットされている事から，オープンリゾルバとなっているDNSサーバのプローブである事が考えられる．実際に，“openresolverproject.org”のドメインを所有しているOpen Resolver Projectでは，オープンリゾルバとなっているDNSサーバのリストを公開し，毎週そのデータをアップデートしている事が公表されている[13]．

2013年3月以前にも同規模程度の問合せ数を持つDNSスキャンが観測されているが，これらのスキャンも問合せDNSは異なるものの，送信先IPアドレスを識別可能な形でDNS問合せが行われている．従って，オープンリゾルバとなるDNSサーバの探索を行っているもである事が考えられる．

3.2 DNSバックスキャッタ分析

ここでは，DNSバックスキャッタに用いられた問合せドメインの分析を行う．**図 4**，**図 6** より，2012年6月17日に観測したバックスキャッタ送信ホスト数の最大を記録している．このとき，約200ホストから“isc.org”の名前解決の結果が送られて来ていた．全てのパケットにはAAフラグ（**表 1** 参照）が設定されておらず，問合せ結果を返答しているホストはRAフラグがセットされている事から，再帰的に問合せが行われた結果であることが分かる．従って，オープンリゾルバとして動作しているDNSサーバからの応答である事が分かる．“isc.org”は，DNSスキャン時にも見られるドメインであり，同時期に数多くのホストからDNSバックスキャッタを観測していることからisc.orgを管理する権威DNSサーバに対するDDoS攻撃である可能性が非常に高い．実際に，“isc.org”を問い合わせるDNSスキャンも16日，17日に非常に多く発生している．

2012年11月14日には最大バックスキャッタパケット数を観測した．このとき，特定の組織が保有する9ホストから30個の異なるIPアドレスを持つセンサに対して約20万パケットを観測している．しかし，このときのDNSパケットにはヘッダ情報しか無く，Questionセクション以下何も情報が入っていないパケットであった．送信元ポート番号は53番であったことから，DNS問合せに対する応答である可能性は非常に高いが，何らかのスキャンやDNSサーバの脆弱性を狙った攻撃である可能性もある．

目立った増加が確認された場合以外でも，AAフラグが設定された応答を返しているにも関わらず，現在（2013年8月現在）では応答を返さないホストや，TTL（キャッシュ生存期間）が非常に短く設定された応答をしているホストなども多く存在している．これらのホストは今後ドメインの乗っ取りや，本来の権威サーバへのDDoS攻撃などに利用される可能性が考えられる．

4 おわりに

本論文では，ダークネットモニタリングで観測可能なDNSトラフィックの分析を行った．ダークネットでは，DNSトラフィックのうちDNSサーバに対するスキャン（DNSスキャン）と詐称されたIPアドレスからのDNS問合せに対する応答（DNSバックスキャッタ）を観測可能である．DNSスキャン，DNSバックスキャッタのそれぞれのトラフィックは年々増加傾向にあることが分かり，今後も動向に注意する必要があ

る．特に，オープンリゾルバなどを利用した大規模なDDoS攻撃なども起こっているため，これらの予兆をいち早く捉え，対策を行う事が非常に重要になる．現在でも，オープンリゾルバとして動作するDNSサーバを探索する通信が定期的に観測され，実際にオープンリゾルバリストなども公開されている事から，それらのホストからの問合せを拒否するなど対策を行う必要がある．

DNSサーバからのバックスキャッタ分析では，複数のオープンリゾルバを用いたDDoS攻撃を観測した．DNSバックスキャッタを利用する事でもオープンリゾルバとして動作するホストを特定する事が可能である事が分かった．また，実際には権威を持っていないドメインに対して不正な応答を行うDNSサーバなどの存在を確認した．

今後は，ダークネットモニタリングを利用する事で，オープンリゾルバからの問合せや，不正DNSサーバからの問合せなどを検出し，それらのホストからの通信をフィルタリングするなど，大規模攻撃に備えた対策技術の開発が期待できる．

参考文献

[1] The Spamhous Project, `http://www.spamhaus.org`（2013年8月現在）.

[2] T. Callahan, M. Allman, and M. Rabinovich, “On Modern DNS Behavior and Properties,” ACM SIGCOMM Computer Communication Review, Vol. 43, No. 3, pp. 7 – pp. 15, 2013.

[3] V. Ramasubramanian and E. G. Sirer, “The Design and Implementation of a Next Generation Name Service for the Internet,” ACM SIGCOMM Computer Communication Review, Vol. 34, No. 4, pp. 331 – pp. 342, 2004.

[4] Jon Oberheide, Manish Karir, and Z. Morley Mao, “Characterizing Dark DNS Behavior,” DIMVA 2007, LNCS 4579, pp. 140 – 156, 2007.

[5] *Anonumous*, “The Collateral Damage of Internet Censorship by DNS Injection,” ACM SIGCOMM Computer Communication Review, Vol. 42, No. 3, pp. 21 – 27, 2012.

[6] T. Peng, C. Leckie, and K. Ramamohanarao, “Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problem,” ACM SIGCOMM Computer Communication Review, Vol. 39, No. 1, pp. 1 – 42, 2007.

[7] S. D. Paola and D. Lombardo, “Protectiong against DNS Reflection Attacks with Bloom Filters,” DMIVA 2011, LNCS 6739, pp. 1 – 16, 2011.

[8] G. Kambourakis, T. Moschos, D. Geneiatakis, and S. Gritzalis, “Detectiong DNS Amplification Attacks,” CRITIS 2007, LNCS 5141, pp. 185 – 196, 2008.

[9] 神薗 雅紀, 他, “マルウェア対策のための研究用データセット ～MWS Datasets 2013～”, MWS2013, 2013.

[10] RFC 1035, `http://www.ietf.org/rfc/rfc1035.txt`（2013年8月現在）.

[11] RFC 6895, `http://www.ietf.org/rfc/rfc6895.txt`（2013年8月現在）.

[12] Internet Assigned Number Authority (IANA), `http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml`（2013年8月現在）.

[13] Open Resolver Project, `http://openresolverproject.org`（2013年8月現在）.