社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＱＡＩ－25（７）
2007／10／25

改良型 iTrace 手法 (iTrace-PT 手法) の 反射型 DDoS 攻撃への適用とその効果

高田 友則† 中山 雅哉†

† 東京大学大学院 新領域創成科学研究科
〒 113-8658 東京都文京区弥生 2-11-16
E-mail: †takada@cnl.k.u-tokyo.ac.jp, ††nakayama@nc.u-tokyo.ac.jp

あらまし 近年 DNS サーバや Web サーバ等を踏み台 (リフレクタ) に用い，被害者を反射パケットにより攻撃する反射型 DDoS (DRDoS) 攻撃が新たな脅威となっている．現在提案されている反射型 DDoS 攻撃への Traceback 技術は，数多くのリフレクタやルータに新たな機能を持たせなければ有効に機能しないという問題がある．
本稿では，著者らが提案している iTrace-PT 手法を反射型 DDoS 攻撃に適用し，リフレクタへの追加機能を必要とせず，対応ルータの数が少ない場合でも有効に機能する手法を提案する．提案手法の特徴は，攻撃者-リフレクタ間の経路情報を持った iTrace パケットを攻撃パケットと同様にリフレクタで反射させることにある．シミュレーションにより，提案手法は対応ルータの数が少ない場合でも有効に機能することを示した．
キーワード DoS 攻撃，反射型 DDoS (DRDoS) 攻撃，iTrace-PT, Traceback

Application of the iTrace-PT Method to Reflector based DDoS Attack and Its Effect

Tomonori TAKADA† and Masaya NAKAYAMA†

† Graduate School of Frontier Sciences, The University of Tokyo
2-11-16 Yayoi, Bunkyo-ku, Tokyo, 113-8658 Japan
E-mail: †takada@cnl.k.u-tokyo.ac.jp, ††nakayama@nc.u-tokyo.ac.jp

Abstract Recently, reflector-based DDoS (DRDoS) attack has become a new threat. It uses DNS, Web, and other servers as reflectors to attack victims by using reply packet. Conventional traceback techniques against DRDoS attack have a problem that they are not effective if a lot of reflectors and routers don't have special functions for traceback.
In this paper, we propose a method which doesn't need for reflectors to have additional functions and can be effective even when a small number of routers for traceback are used, by applying the iTrace-PT, which we have been proposed, to reflector based DDoS attack. The characteristic of this method is that it reflects the iTrace packet, which has the path information between the attacker and reflector, at reflectors as well as the attack packet. We verify by simulation results that the proposal technique is effective even when a small number of routers for traceback are used.
Key words DoS attack, Reflector based DDoS (DRDoS) Attack, iTrace-PT, Traceback

1. はじめに

サービス妨害攻撃 (DoS 攻撃) は，一般的に送信元 IP アドレスを偽装したパケットによって行われる．そのため，被害者は受け取った攻撃パケットから攻撃元を特定することは困難であり，今日のインターネットにおける脅威の一つとなっている．IP Traceback 手法は，偽装したパケットを送出する攻撃元を特定する技術であり，これまでにさまざまな手法が提案されてきた [1]～[4].

しかし，近年になって，DRDoS (Distributed Reflective DoS) 攻撃 [5] と呼ばれる反射型の DDoS 攻撃が新たな脅威となってきた．DRDoS 攻撃の攻撃者は，インターネット上でサーバ機

能を持つ通常のホストを踏み台（リフレクタ）に利用し，送信元IPアドレスを標的ホストに偽装したパケットを用いて，サーバからの応答パケットで標的ホストを攻撃する．

これまで提案されてきたIP Tracebackの多くの手法は，攻撃者が標的ホストを直接攻撃するDoS攻撃に対するものなので，DRDoS攻撃では，リフレクタの特定はできても真の攻撃元を特定することができない．このため，DRDoS攻撃の真の攻撃元を特定する手法がいくつか提案されてきた[6], [7]．しかし，それらは数多くのリフレクタやルータに追加機能を持たせなければ有効に機能しないという問題がある．

本稿では，著者らが低レートのDoS攻撃にも有効な手段として提案を行っているiTrace-PT手法[4]をDRDoS攻撃に適用し，リフレクタに追加機能を持たせず，対応ルータの数が少ない場合でも有効に機能する手法を提案する．提案手法では，攻撃者-リフレクタ間に対応ルータがあれば，その経路情報を持ったiTraceパケットが攻撃パケットと同じ経路で被害者に到達するため，従来のDRDoS攻撃へのTraceback手法で問題となっていた対応ルータ数が少ない場合でも有効に機能する．

以下，本稿では，2章でDRDoS攻撃の特徴について述べ，3章でDRDoS攻撃の対策として関連研究を紹介する．4章でiTrace-PT手法の概要を述べ，5章で提案手法について述べ，6章で提案手法のシミュレーション結果を示し，7章で本論文の結論と今後の課題についてまとめる．

2. DRDoS攻撃

近年，DRDoS (Distributed Reflective DoS) 攻撃[5]と呼ばれる反射型のDDoS攻撃がインターネット上の新たな脅威となってきた．

DRDoS攻撃の概要を，以下で説明する．

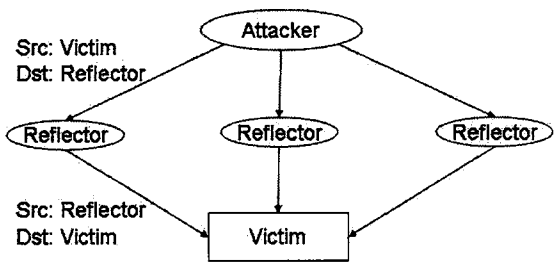

図1 DRDoS attack

図1のように，DRDoS攻撃の攻撃者は，リフレクタと呼ばれるインターネット上でサーバ機能を持つホストに，送信元IPアドレスを標的ホストのIPアドレスに偽装したパケットを送る．このパケットを受け取ったリフレクタは，その送信元IPアドレス，つまり標的ホストに対して応答パケットを返信する．このように被害者が，攻撃者からではなく，リフレクタからの応答パケットにより攻撃を受けるということが，DRDoS攻撃の最大の特徴である．この特徴のため，通常のIP Tracebackを用いても，被害者はリフレクタまでしか攻撃元を特定できず，その後ろの真の攻撃元を特定できない．

この攻撃で利用されるリフレクタは，パケットを受け取り応答パケットを返すホストであれば何でも良いので，インターネット上には無数のリフレクタが存在する．

実際に，DRDoS攻撃は2002年，Gibson Research Corporation[8]に対して行われ，この攻撃の脅威が示された．また，近年リフレクタにDNSサーバを用いて，DNSのReplyパケットによって攻撃を行うDRDoS攻撃が増えてきている[9]．

DRDoS攻撃の脅威な点をまとめると以下のような3点が挙げられる．

- インターネット上のほとんどのホストがリフレクタになりえる．
- パケットの増幅作用が生じる．
- 攻撃者から直接パケットを受け取らない．

第一に，インターネット上のほとんどのホストがリフレクタになりえることにより，被害者が特定のリフレクタからの通信を拒否するだけでは，この攻撃を防ぐことはできない．

第二に，DRDoS攻撃では，受信パケット数よりも多くの応答パケットを返したり，受信パケットのサイズよりも大きな応答パケットを返すリフレクタを用いることにより，攻撃パケットの数やサイズを数倍から数十倍に増幅することが可能である．これはつまり，攻撃パケットを少なくしても，非常に大きな攻撃を行えるということである．

最後は，上で述べたようにDRDoS攻撃の被害者は，攻撃者から直接パケットを受け取らないため，従来のIP Tracebackを用いても，リフレクタまでしか攻撃元を特定できず，その後ろの真の攻撃元を特定できない．

3. 関連研究

本章では，現在提案されているDRDoS攻撃に対するTraceback技術を紹介する．DRDoS攻撃へのTracebackは，リフレクタの後ろの真の攻撃元を特定することが目標である．

3.1 Reverse iTrace (r-iTrace)

Reverse iTrace (r-iTrace) は，ICMP Traceback (iTrace) [3]をDRDoS攻撃向けに改良した手法である．iTrace手法は，パケットがTraceback対応ルータに到着すると，そのルータのIPアドレス等をデータ部に記載したICMPメッセージ (iTraceパケット) を一定の確率で生成し，中継したパケットと同じあて先に送る．被害者は，受信したiTraceパケットのデータを基にして，攻撃元までの経路を特定できる．

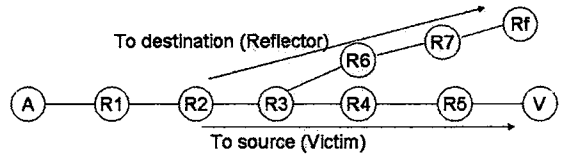

図2 When R2 generates iTrace packets

r-iTraceでは，iTraceパケットを中継したパケットのあて先だけでなく，送信元に対しても送る．例えば，図2において，R2が攻撃パケットに対してiTraceパケットを生成するとき，

そのあて先であるリフレクタと，送信元である被害者あての2パケット生成し，送信する．こうすることによりDRDoS攻撃の被害者は，攻撃者-リフレクタ間の経路情報を得ることができる．しかし，被害者から攻撃者の最寄の対応ルータまでの経路上の全ルータが，対応ルータでなければ攻撃元を特定できないという問題がある．

3.2 ICMP Caddie messages (iCaddie)

ICMP Caddie messages (iCaddie) [6] では，DRDoS攻撃へのIP Tracebackは，次のように2段階で行われる．

一段階目で，被害者が受け取ったリフレクタ-被害者間の経路情報を持ったiCaddieメッセージにより，リフレクタの最寄ルータを特定し，二段階目で，特定したそのルータに対してTraceback Requestを送り，Requestを受けたルータが真の攻撃元まで特定する (図3)．

iCaddieは，Traceback Requestを受けたルータが，攻撃者-リフレクタ間の経路情報を持ったiCaddieメッセージを受け取れなければ，真の攻撃元を特定することができない．例えば，図3において，R3,R6,R7が対応ルータでなければ，R4までしか特定できず，R4は攻撃者-リフレクタ間の経路情報を持ったiCaddieメッセージを受け取れないため，リフレクタの後ろの真の攻撃者を特定できない．

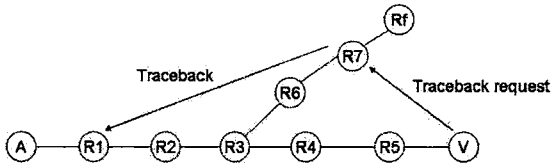

図3 iCaddie

4. iTrace-PT

iTrace with Periodical Transmission (iTrace-PT) [4] は，低レートのDoS攻撃に対応するために，iTraceを改良した手法である．iTraceは，ネットワークに与える負荷を考慮しiTraceパケットの生成確率を低い値としているため，低レートのDoS攻撃には向いていない．

iTrace-PTは，一度iTraceパケットを送ったあて先には，一定時間は再送しないという生成方式により，iTraceパケットの生成確率を上げながらネットワークに与える負荷を低く抑えることができる．これを実現するためiTrace-PTでは，Bloom Filterを用いて，一度送ったiTraceパケットのあて先IPアドレスを記憶し，記憶中は同じあて先にはiTraceパケットを送らず，一定時間経ったら，Bloom Filterをハッシュクリアする．この処理により，1回のハッシュクリア間隔では，同じあて先へのiTraceパケットは1パケットしか生成されない．

そして，攻撃元の特定は次のように行う．C 回のハッシュクリアが行われたとき，閾値を α として，$C\alpha$ 個以上のiTraceパケットを発生させたルータを，攻撃者の直近ルータと特定する．

iTrace-PTによる攻撃元特定手法は，攻撃の持続時間に基づいて攻撃元の特定が行われる．つまり，高ビットレートの攻撃も低ビットレートの攻撃も，C 回のハッシュクリアの時間だけ攻撃パケットが継続している場合，攻撃者の直近ルータから届くiTraceパケットは C 個である．よって，iTrace-PTでは，攻撃者の通信が小さくても，攻撃時間が長ければ，攻撃元を特定することができる．

5. 提案手法

本章では，iTrace-PT手法をDRDoS攻撃に適用し，リフレクタに新たな機能を持たせず，対応ルータの数が少ない場合でも有効に機能する手法を提案する．

本手法の主な考えは，iTraceパケット自体も攻撃パケットと同様にリフレクタに反射させるということである．この目的を達成するため，生成するiTraceパケットの送信元IPアドレスとあて先IPアドレスの組を，中継パケットと同一にし，ICMPの型をTraceback用に新たに定義するのではなく，現在広く使われているICMP echo (Ping) とする．ICMP echo Requestに含まれているデータは，Replyに含まれなければならない [10]．そのため，ICMP echo Requestのデータ部に記載した，攻撃者-リフレクタ間の経路情報が，リフレクタにおいて反射された後のICMP echo Replyに維持される．

図4を用いて本手法の概要を説明する．

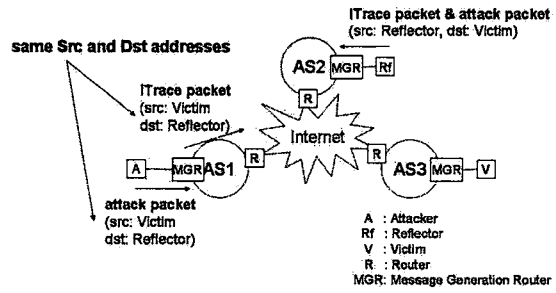

図4 Proposal method

パケットがMessage Generation Router (MGR) と呼ばれる対応ルータに到着すると，そのパケットと送信元・あて先IPアドレスが等しいiTraceパケットを確率的に生成し送信する．こうすることにより，攻撃パケットとiTraceパケットは，同じ経路を通り被害者に届くことが期待される．この時，経路中のMGRは，受け取ったiTraceパケットに自分のアドレスを追加してから中継する．この処理により，被害者は受け取ったiTraceパケットの情報により攻撃元までの経路を特定することができる．

提案手法におけるリフレクタの役割は，ICMP echo Requestに対して，ICMP echo Replyを返すだけなので，新たな機能を持つ必要はない．インターネット上の同一ネットワーク上にない100個のWebサーバに対して，ICMP echoを送ったところ，74個のサーバがReplyを返した．つまり，現時点においても大部分のリフレクタが協力してくれている状態であるといえる．

また，本手法は，攻撃経路中に一つでも対応ルータがあれば，

攻撃者の最寄の対応ルータを特定することが可能なので，対応ルータの数が少ない場合でも有効に機能することが期待される．例えば，図4においてAS1のみが対応ルータを置いており，他ASが置いていなくても，AS1で生成されたAS1の経路情報を持ったiTraceパケットのデータは，リフレクタからの応答パケットにおいても維持されるため，被害者はAS1の攻撃元を特定することが可能である．

続いて，図5に提案手法におけるiTraceパケットのフォーマットを示す．上2段は，ICMPヘッダであり，上述のように通常のICMP echo (ping) と同一である．Traceback Codeフィールドには，通常のpingと区別するため，Traceback用メッセージであることを識別できるように，一意な値を入れる．Authentication Codeフィールドは，このiTraceパケットを作り出したのがそのルータであるということを証明するフィールドである．各Router's IP addressフィールドには，iTraceパケットを生成したルータから被害者までの経路中の対応ルータのIPアドレスが入る．

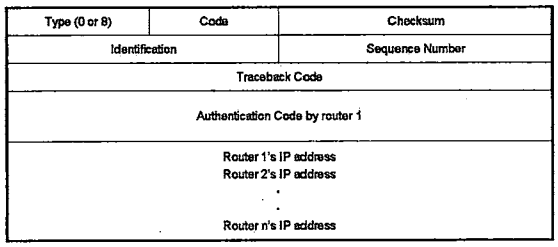

図5 Message format

6. シミュレーション

本章では，r-iTrace, iCaddie, iTrace-PTの3手法に関して，ルータの対応率が攻撃元の特定能力に与える影響を，シミュレーションによって評価した．

ルータの総数をN，対応率をβ $(0 \leqq \beta \leqq 1)$としたとき，$\lfloor \beta N \rfloor$個を対応ルータとして，ランダムに配置する．評価項目は，攻撃元の特定能力を調べるため，以下の式で表されるFalse Negative (検出漏れ) とした．

$$FalseNegative = \frac{\text{特定できなかった攻撃元の数}}{\text{検出すべき攻撃元の数}}$$

ここで検出すべき攻撃元とは，攻撃者に最も近い対応ルータとする．

図7は，図6の単純なトポロジで行ったシミュレーション結果とr-iTrace, iCaddieの理論値を示している．

シミュレーションは，各β毎に1000回行い，1回ごとに対応ルータの配置を変えた．

r-iTraceでは，被害者から攻撃元までの全ルータが対応ルータの時に攻撃元を特定できる．よって，nを対応ルータの数として，図6のトポロジにおけるr-iTraceのFalse Negativeの理論値$FN_1(n)$は，以下のように表せる．

$$FN_1(n) = \begin{cases} 1 & (n=0) \\ 1 - \frac{1}{{}_{10}C_n} & (n \geqq 1) \end{cases} \quad (1)$$

iCaddieは，Traceback Requestを受けたルータが，攻撃者-リフレクタ間の経路情報を持ったiCaddieメッセージを受け取ることができれば，攻撃元を特定できる．図6のトポロジでは，ルータ4,5が対応ルータだとすると，攻撃元を特定できる．nを対応ルータの数として，図6のトポロジにおけるiCaddieのFalse Negativeの理論値$FN_2(n)$は，以下のように表せる．

$$FN_2(n) = \begin{cases} 1 & (n=0) \\ 1 - \frac{{}_4C_n + 2\cdot{}_8C_{n-1}}{{}_{10}C_n} & (n=1) \\ 1 - \frac{{}_4C_n + 2\cdot{}_8C_{n-1} + {}_8C_{n-2}}{{}_{10}C_n} & (2 \leqq n \leqq 4) \\ 1 - \frac{2\cdot{}_8C_{n-1} + {}_8C_{n-2}}{{}_{10}C_n} & (5 \leqq n \leqq 9) \\ 0 & (n=10) \end{cases} \quad (2)$$

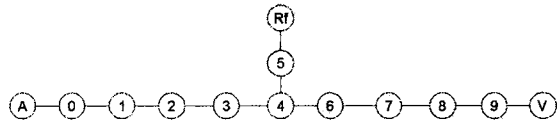

図6 simple topology

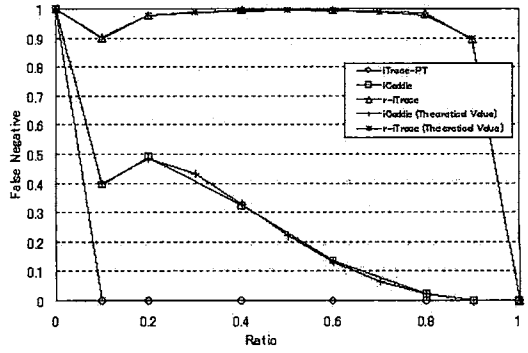

図7 False Negative on simple topology

図7より，提案手法は$\beta = 0.1$，つまり攻撃経路中にひとつでも対応ルータがあれば攻撃元を特定できることが示されている．一方r-iTraceは，90%のルータが対応していたとしても，ほとんど攻撃元を特定できない．また，iCaddieは，対応率が0.8以下になると性能が落ちている．これは，図6のトポロジにおいて，ルータ4,5に対応ルータが配置されなかったことによる．

続いて実ネットワークにおいて，提案手法が有効に機能するか調べるため，図8に示すSINET [11] をトポロジに用いてシミュレーションを行った．

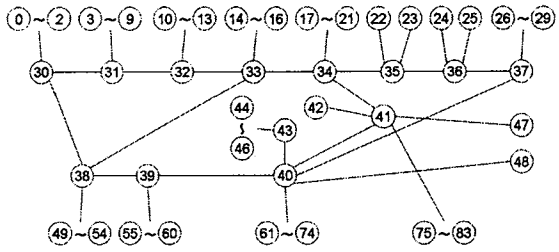

図 8 SINET

攻撃者をルータ 0，被害者をルータ 29 の下に配置し，攻撃者が 1 つのリフレクタ (ルータ 83 の下に配置) を使ったときの，ルータの対応率と False Negative の関係グラフを図 9 に示す．

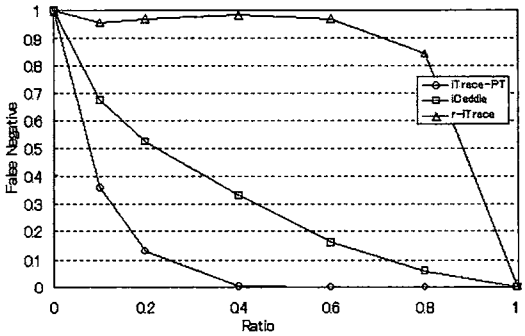

図 9 False Negative on SINET (One reflector)

図 9 は，ルータの対応率が 0.4 以下になると提案手法においても，攻撃元を特定できないケースがあることが示されている．これは，攻撃経路中に一つも対応ルータが存在しないケースがあることを意味している．しかし，対応率が 0.4 以上になると攻撃経路中に少なくとも一つは対応ルータが配置され，攻撃元を特定できている．

続いて，攻撃者が 3 つのリフレクタ (ルータ 83,22,42 の下に配置) を使ったときの結果を図 10 に示す．

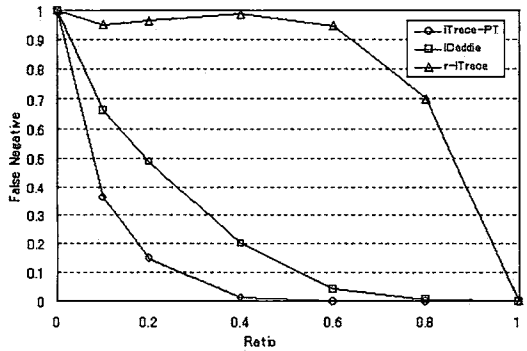

図 10 False Negative on SINET (Three reflectors)

図 10 より，提案手法は，攻撃者がリフレクタを 3 つ使っても，1 つの時と同じような結果を示しており，リフレクタの数に大きく依存しないことが示された．この場合も，提案手法は，ルータの対応率が 0.4 以上であれば攻撃元を特定できている．

7. ま と め

本稿では，iTrace-PT 手法を DRDoS 攻撃に適用し，リフレクタに新たな機能を持たせず，対応ルータの数が少ない場合でも比較的有効に機能する手法を提案した．提案手法は，攻撃者-リフレクタ間の経路情報を持った iTrace パケットを攻撃パケットと同様にリフレクタに反射させることにより，対応ルータの数が少ない場合でも，攻撃元を特定することが可能である．シミュレーションにより，提案手法は対応ルータの数が少ない場合でも比較的有効に機能することを示し，SINET においてルータの対応率が 0.4 以上であれば，攻撃元を特定できることを示した．

今後の課題としては以下のようなことが挙げられる．

- 低い対応率の時の False Positive 値の改良

対応ルータをランダムに配置するのではなく，最も有効に機能するような配置を行えば，低い対応率の時の False Positive 値は改良されるはずである．例えば，リンク数が多いルータに優先的に配置することにより，攻撃経路中に一つも対応ルータが存在しないケースを大きく減らすことができ，False Positive 値を改良できるはずである．

- さまざまなトポロジでのシミュレーション

どんなトポロジにおいても提案手法が有効に機能するかを調べるため，さまざまなトポロジにおけるシミュレーションが必要である．

文 献

[1] D. Song, A. Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback", Proc. IEEE INFOCOM, 2001.

[2] A.C. Snoeren et al, "Hash-Based IP Traceback", ACM SIGCOMM 2001, August 2001.

[3] S.M. Bellovin, "ICMP Traceback Messages", Internet draft: draft-vellovin-itrace-00.txt, March 2000.

[4] 高田友則，中山雅哉，"低レートの DoS 攻撃に対応する改良型 ICMP Traceback"，情報処理学会 DPS Workshop 2007 予稿集，2007/10/31-11/2. 掲載予定.

[5] V. Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", Computer Communication Review 31(3), July 2001.

[6] B. Wang, H. Schulzrinne, "An IP Traceback Mechanism for Reflective DoS Attacks", IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 901-904, May 2004.

[7] N. Nishio, N. Harashima, H. Tokuda, "Reflective Probabilistic Packet Marking Scheme for IP Traceback", IPSJ Journal, vol.44, no.8, pp.1848-1860, August 2003.

[8] S. Gibson, "Distributed Reflection Denial of Service", 2002. http://www.grc.com/dos/drdos.htm

[9] 警察庁, "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", July 2006.

[10] R. Braden, "Requirements for Internet Hosts - Communication Layers", October 1989. http://www.ietf.org/rfc/rfc1122.txt

[11] SINET3, "SINET3 (学術情報ネットワーク)". http://www.sinet.ad.jp/