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

2008－DPS－134 (11)
2008－CSEC－ 40 (11)
2008／3／6

DNS ログに注目した詐称 IP 探索

竹森 敬祐† 藤長 昌彦† 西垣正勝‡

†KDDI 研究所 〒356-8502 埼玉県ふじみ野市大原 2-1-15

‡静岡大学創造科学技術大学院 〒432-8011 静岡県浜松市中区城北 3-5-1

あらまし Source IP を詐称した攻撃対策として，ネットワークを通過する攻撃パケットを被害者側 (Destination) から加害者側 (Source) へと遡って追跡する IP トレースバックが注目されている．しかし，トレースバックに必要な機能を，通信経路上の多数のルータに組み込むこと，もしくは専用の装置を多数設置することが導入への障壁となっている．そこで本研究では，既存の DNS サーバのログ，もしくは，DNS 通信をキャプチャする装置だけで Source IP を探し出す，詐称 IP 探索方式を提案する．これは，攻撃の直前に被害者ホストの Fully Qualified Domain Name (FQDN)に該当する Destination IP を DNS サーバに問い合わせたログから，Source IP を探し出す手法である．また，Source IP が詐称されていることを，通信に関与しないドメインに漏洩しないように，Source IP と FQDN のハッシュ値を用いて確認する手法と，複数の DNS ログを照合することで探索結果の信頼性を向上させる手法についても検討する．本手法の有効性を確認するために，Bot から発信されるパケットを収集することで，DNS 検索型の攻撃割合を調査する．

キーワード 詐称 IP ，DNS ログ，FQDN

IP Traceback using DNS Log

Keisuke TAKEMORI†， Masahiko FUJINAGA† and Masakatsu NISHIGAKI‡

†KDDI R&D Laboratories Inc. 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502 Japan

‡Shizuoka University 3-5-1 Jyohoku, Naka-ku, Hamamatsu-shi, Shizuoka, 432-8011, Japan

Abstract An IP traceback system that tracks a spoofing packet from a victim (destination host) to an attacker (source host) has been active researched against IP spoofing attacks. However, it is hard to implement a tracking function or probe on many routers that connect the source host to the destination host on the Internet. In this research, we propose a simple IP traceback scheme that finds a victim FQDN event with attacker IP on DNS server or DNS probe logs. It assumes that most source hosts retrieve destination FQDN before spoofing attacks. The spoofing attacks are confirmed with a hash function calculated with the source IP and the victim FQDN to prevent leakage of communication record. We also consider that the reliability of traceback results can be gained to check multiple traceback results. Efficiency of our scheme is evaluated to investigate bot communication patterns that include DNS queries.

Keywords IP Spoofing, DNS Log, FQDN

1. はじめに

Source IP を詐称した多量の通信パケットを送りつける Denial of Service (DoS)攻撃に対する脅威が高まっている．詐称 IP 攻撃への対策として，ネットワークを通過する攻撃パケットを被害者側 (Destination) から加害者側 (Source) へと遡って追跡する IP トレースバックが注目されている[1]-[4]．しかし，トレースバックに必要な情報を収集するために，通信経路上の多数のルータに専用の機能を組み込むこと，もしくは，多数の専用装置を設置することが，導入への障壁となっている．特に，昨今注目されている Hash 方式の IP トレースバックでは，通過する全てのパケットの Hash 値を管理する必要があり，メモリやハードディスク容量の限界から，攻撃を検知してから Source IP の特定までを，短時間で完了しなければならない課題もある．

そこで本研究では，既存の DNS サーバのログ，もしくは，DNS 通信をキャプチャする装置だけで Source IP を探し出す，詐称 IP 探索方式を提

案する.これは,加害者ホストが攻撃の直前に,被害者ホストのFQDNに該当するDestination IPをDNSサーバに問い合わせた記録から,Source IPを探し出す手法である.また,Source IPが詐称されていることを,Source IPとDestination FQDNを組み合わせたハッシュ値を用いてSource DNSに確認することで,攻撃通信に関与しないドメインに通信記録を漏洩しないように詐称の有無を把握できる.さらに,複数のDNSログを照合することで探索結果の信頼性を向上させる手法についても検討する.本手法の有効性を確認するために,Botから発信されるパケットを収集して,DNS検索型の攻撃の割合を調査する.

尚,本研究では"探索"という用語で説明しているが,これは従来の一つずつ通信経路を遡りながら"追跡"する手法とは異なり,被害者側から加害者側のDNSログを照合するのみで,直接Source IPを特定することができることを意味している.また,探索の場合,中継回線に専用の機能や装置を設置する必要がなく,設置漏れによる失敗率を抑える効果がある.さらに,扱うデータ種別も限られることから,機能や装置のコストを抑えて実装することもできる.

2. 既存技術

2.1. IPトレースバック

ここでは詐称IPの追跡手法として注目されているHash方式,ICMP方式,パケットマーキング方式について概観する.

Hash方式は,通過するパケットのハッシュ値を保存しておき,被害者側に届いた攻撃パケットのHash値を検索しながら追跡する手法である[1][2].本方式は,通過するルータ上で全てのパケットのハッシュ値を管理しておくことで1パケット単位のトレースを行えるものの,ハッシュ管理の仕組みやルータ間連携の実装が複雑になること,経路上の全てのルータでトレースが成功しなければならない問題などがある.

ICMP方式は,ルータを通過するパケットをサンプリングして,パケット情報とルータ情報を,ICMPパケットに載せてDestination IPへ送付する手法である[3].本方式は,被害者側だけで情報を組み立てることができる簡易な手法であるが,トレース情報を通知するための通信負荷,多数のICMPパケットを収集すること,多数の専用装置を経路上に設置することが問題となる.

パケットマーキング方式は,ルータを通過するパケットをサンプリングして,ルーティングに影響のないヘッダ領域に,ルータ情報を書き込む手法である[4].本方式は,被害者側だけで情報を組み立てることができる簡易な手法であるが,書き込み情報が上書きされること,多数のヘッダ情報を収集することなどが問題である.

2.2. IPトレースバック間連携

ここでは,End-to-Endの追跡を支援する,ドメイン間連携の仕組みについて概観する.

その一つに,ドメイン内とドメイン間を,それぞれのトレース層に分けて処理することで,迅速に追跡できるInter Trackと呼ばれる手法が注目されている[5].これは,異なる種別のIPトレースバック方式を結合できる利点があるものの,End-to-Endの全てのトレース処理が成功しなければならない問題がある.

トレース途中で失敗した処理を復元する手法として,追跡処理を失敗したルータもしくはドメインからの報告を受け,周囲のルータもしくはドメインが処理を並行復元する,並列型トレースバック方式が提案されている[6].これは,ルータやドメイン毎のトレース過程をセンタ局が確認しながら追跡を調停するフレームワークであるが,やはり専用の機能や装置を多数の経路上に設置することを前提にしている.

3. DNSログに注目した詐称IP探索

ここでは,既存のDNSサーバのログ,もしくは,DNS通信パケットのログに注目した詐称IP探索方式を提案する.本研究で探索対象とするSource IPの詐称攻撃として,攻撃の直前にDNSサーバを利用してDestination IPを問い合わせるものとする.

3.1. DNS検索処理の復習

図1に,.kddilabs.jpドメイン内のSourceホストが,www.kddi.comに該当するDestination IPを検索する処理を例に,FQDNからDestination IPを名前解決する手順を説明する.DNS検索における基本として,Recursive(再帰)検索要求を受けたDNSサーバは,リゾルバとなって,FQDNを解決するまでドメインツリーをたどってDNS検索を行い,最終結果を問い合わせ元に返信する.場合によっては,Sourceホスト自身がリゾルバになることもある.Iterative(反復)検索を受けたDNSサーバは,自身が管理しているゾーン情報のみを返答し,他のDNSサーバへ問合せを行うことはない.

Ⅰ Sourceホストは，プライマリDNSサーバに対してFQDNに該当するDestination IPを再帰検索で問い合わせる．プライマリDNSサーバはリゾルバとなり，Sourceホストからの名前解決を代行する．

Ⅱ リゾルバは，最上位にあるRoot DNSサーバに対して，.comドメインを代表するDNSサーバのIPアドレスを問い合わせる．
リゾルバは，.comドメインのDNSサーバに対して，.kddi.comドメインを代表するDNSサーバのIPアドレスを問い合わせる．
リゾルバは，.kddi.comドメインのDNSサーバに対して，www.kddi.comに該当するDestination IPを問い合わせる．

Ⅲ Destination DNSサーバは，FQDNに該当するDestination IPをリゾルバに返信する．

Ⅳ リゾルバは，Sourceホストに対して，名前解決されたDestination IPを返信する．

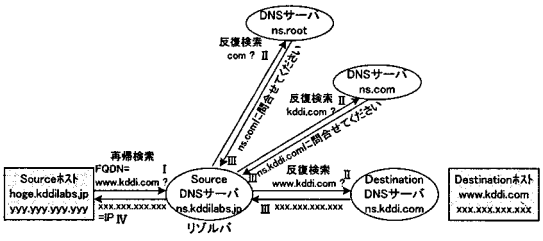

図1. DNS検索の例

図2にリゾルバDNSサーバから出力される再帰検索ログの一例を示す．ここにはSourceホストのIPとDestination FQDNの記録が残されている．リゾルバDNSサーバの通信回線に，DNSパケット監視用の装置を設置した場合でも，同様のログを取得できる．

時刻	Src-IP(問合せ元IP)	Dst-FQDN	Dst-IP
2007.08.20, 20:18;04	192.168.0.21	www.local.co.jp	192.168.0.234
2007.08.20, 20:18;06	192.168.28.229	mail.local.co.jp	192.168.23.21
2007.08.20, 20:18;10	yyy.yyy.yyy.yyy	www.kddi.com	xxx.xxx.xxx.xxx
2007.08.20, 20:18;12	192.168.100.57	www.local.jp	192.168.200.73
2007.08.20, 20:18;16	192.168.140.23	ns.local.go.jp	192.168.156.21
2007.08.20, 20:18;20	192.168.29.222	mail.local.com	192.168.19.10
	...		

図2. DNSログの一例

3.2. DNSサーバ連携型の詐称IP探索

図3に，Destination DNSとリゾルバDNSのログを用いてSourceホストのIPを探索する手法を提案する．ここで，記号ⅠからⅣの処理は，図1に説明した名前解決の処理であり，Root DNSと.comを代表するDNSへの問い合わせ処理を省略したものである．以下，詐称IP探索に関わる①から④の処理について説明する．

① 詐称IP攻撃を受けたDestinationホストは，自身について名前解決を行ったSource IPの探索を，攻撃のあった時刻情報を添えて，Destination DNSサーバに依頼する．

② Destination DNSサーバは，攻撃の時刻情報を基に自身のDNSログの中から，FQDNの反復検索を行ったSource DNSサーバを見つけ出す．そして，名前解決を行ったSource IPの探索を，攻撃の時刻情報を添えて，Source DNSサーバに依頼する．

③ Source DNSサーバは，攻撃の時刻情報を基に自身のDNSログの中から，FQDNの再帰検索を行ったSourceホストを見つけ出す．そして，Source IPの情報をDestination DNSサーバに返信する．

④ Destination DNSサーバは，Destinationホストに，探索されたSource IPを返信する．

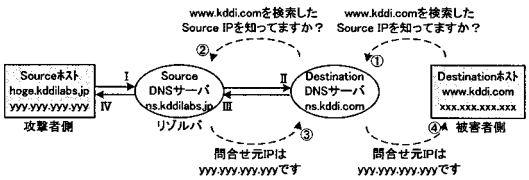

図3. DNSサーバ連携型の詐称IP探索

3.3. DNSログ管理センタ型の詐称IP探索

3.2節では，DNSサーバ同士が連携するモデルを提案した．これは，分散処理を実現できるものの，DDoS攻撃などの多数の詐称IPを探索するには適していない．

そこで，探索処理を制御するセンタを設けて，Destination DNSサーバはセンタに問い合わせるのみで，Source DNSサーバへの問い合わせをセンタ局が受け持つことで，DDoS攻撃を一括探索する仕組みについて提案する．この様子を図4に示す．

① 詐称IP攻撃を受けたDestinationホストは，自身について名前解決を行ったSource IPの探索を，攻撃のあった時刻とDestination DNS情報を添えて，センタに依頼する．

② センタは，Destination DNSサーバに攻撃の時刻とFQDN情報を添えて，Destination DNSサーバに問い合わせる．

③ Destination DNSサーバは，攻撃の時刻情

報を基に自身の DNS ログの中から，FQDN の反復検索を行った Source DNS サーバを見つけ出し，その情報をセンタに返信する．

④ センタは，Source DNS サーバに攻撃の時刻と FQDN を添えて，Destination DNS サーバに問い合わせる．

⑤ Source DNS サーバは，攻撃の時刻情報を基に自身の DNS ログの中から，FQDN の再帰検索を行った Source IP を見つけ出し，Destination DNS サーバに返信する．

⑥ センタは，Destination ホストに，探索された Source IP を返信する．

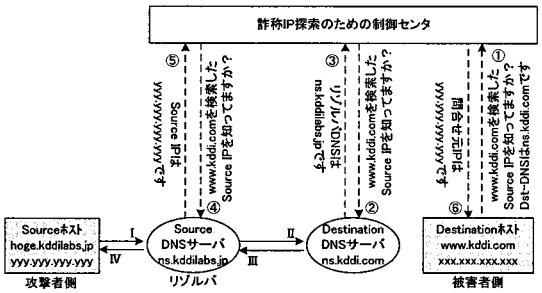

図 4. センタ制御型詐称 IP 探索

3.4. 探索結果の信頼性の向上

Destination ホストが人気のサイトで，同時刻に複数の Source ホストが FQDN の名前解決を行った場合，正規ホストと攻撃者ホストを見分けることができない．

そこで，複数の探索要求や探索結果を照合することで，共通して現れる Source IP を疑わしい Source ホストと考えることにする．このとき，Source DNS 側で複数の探索要求を照合する手法と，Destination DNS 側で複数の探索結果を照合する手法を提案する．

図 5 に，Source DNS 側で，異なる Destination DNS からの探索要求を受けて，重複する Source IP を抽出する照合モデルを示す．Source DNS サーバは，共通する Source IP を疑わしい Source ホストとして返信する．これは，攻撃者が短期間に複数の Destination ホストに対して詐称 IP 攻撃を行うことを想定したモデルである．

図 6 に，Destination DNS 側で，異なる Source DNS からの探索結果において，Source IP が重複するものを抽出する照合モデルを示す．Destination DNS サーバは，この共通する Source IP を，より疑わしい Source ホストとみなす．これは，攻撃者が複数の DNS サーバへ並列に Destination ホストを検索することを想定したモデルである．

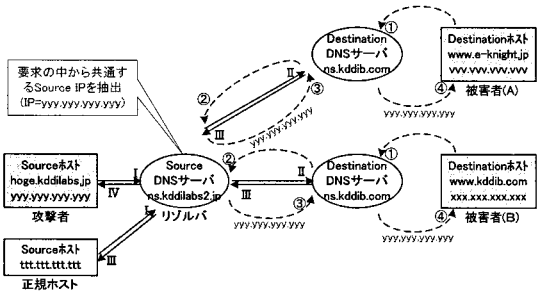

図 5. Source DNS 側での探索要求の照合

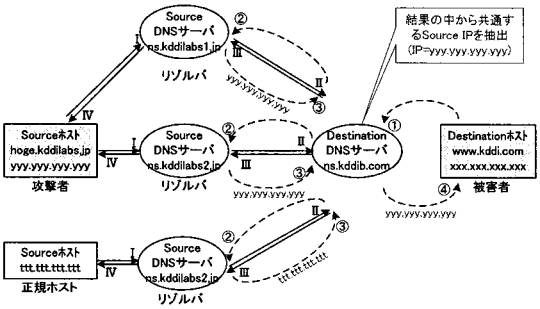

図 6. Destination DNS 側での探索結果の照合

3.5. 秘匿性を考慮した詐称 IP の確認

Source IP が詐称されていない場合に，これを探索すべきではない．

そこで，Source IP が詐称されていることを，通信に関与しないドメインに漏洩することなく確認する手法として，Destination 側に届いた攻撃パケットの Source IP と Destination FQDN の組み合わせのハッシュ値を，Source IP を管理するドメインの DNS サーバに問い合わせる手法を提案する．もし，Source DNS サーバに該当する Source IP と FQDN の記録が残っていれば，同じハッシュ値を容易に算出でき，その IP は詐称されていないものとみなせる．同じハッシュ値を算出できなければ，Source IP は詐称されており，探索処理に移行する．Source IP とアルファベットを含む Destination FQDN を組み合わせることで，ハッシュ前の文字列の組み合わせが膨大になるため，秘匿性を担保できる．以下，Source IP が詐称されていることを確認する手順について，図 7 を用いて説明する．

① Destination ホストは，攻撃パケットのヘッ

ダから Source IP を取り出し，自身の FQDN と時刻情報を添えて，Destination DNS サーバに，詐称の有無を問い合わせる．

② Destination DNS サーバは，Source IP を管理するドメインの DNS サーバに，Source IP と FQDN を組み合わせたハッシュ値 hash(Source IP + Destination FQDN)と時刻情報を添えて，同じハッシュ値の有無を問い合わせる．

③ Source DNS サーバは，自身の DNS ログの中から時刻情報を元に，Source IP と FQDN のハッシュ値を算出し，同じハッシュ値の有無を返信する．

④ Destination DNS サーバは，詐称の有無の結果を Destination ホストに返信する．

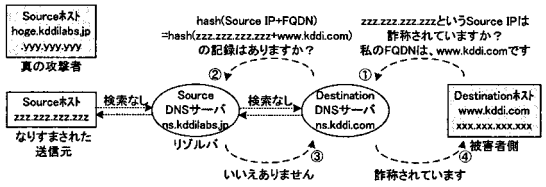

図 7. 秘匿性を考慮した詐称 IP の確認

4. 有効性確認のための調査

本手法の有効性を確認するために，DNS 検索型攻撃割合について，Bot 感染ホストから発信される攻撃を対象に調査する．また，そのときの DNS 通信パターンについても調査する．

4.1. DNS 検索型攻撃割合の調査

本手法の有効性を確認する一つの指標として，詐称 IP 攻撃のターゲット Destination IP について DNS 検索を行う攻撃の割合がある．そこで本研究では，詐称攻撃の踏み台に利用される Bot に注目して，Bot が外部ホストと通信する際の DNS 検索率について調査した．

Bot の検体を収集するために Nepenthes[7]ハニーポットを利用した．そして収集された Bot 検体を仮想マシンモニタ上の Windows OS ホストに感染させて，発信される通信をモニタした．表 1 に，Bot が指令を受け取る通信とその直前に DNS 検索した件数，ならびに，Bot からの攻撃通信とその直前に DNS 検索した件数を示す．指令サーバと通信する場合には，必ず DNS サーバから Destination IP を検索していた．攻撃については，単純な感染活動である IP スキャンを除いては，55%の確率でターゲットとなる Destination IP を DNS サーバで検索していた．

ところで，既存のハッシュ方式によるトレースバック[1][2]では，多数の経路上にプローブを設置する必要があり，プローブの設置率とトレース成功率について評価がなされてきた[6]．プローブの設置率を，ほぼ完全な状態とみなせる 90%としたときの，追跡ホップ数に対する既存のトレース成功率と，提案の探索成功率について，比較したものを図 8 に示す．提案方式は，全ての攻撃が DNS 検索を行う場合と、DNS 検索率=0.55 の場合を示しておく．提案方式は，Destination DNS から Source DNS へ直接問い合せて探索するため，ホップ数が 2 以上のとき成功率が一定となる．DNS 検索率=0.55 の場合でも，ホップ数が 8 以上において従来方式よりも探索成功率が高くなることがわかる．

表 1. Bot 感染ホストから発信される通信のうち DNS 検索を行う件数と割合

	全数	DNS 検索有
通信数(=感染数)	37 件	-
指令通信数	37 件	37 件(100%)
攻撃通信数	29 件	16 件(55%)

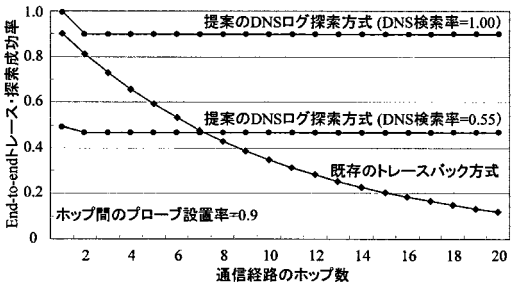

図 8. ホップ数に対する追跡成功率と探索成功率

4.2. DNS 通信パターンの調査

4.1 節で収集された Source ホストと DNS サーバ間の DNS 通信を Ethereal[8]で確認した様子を図 9，10 に示す．参考までに，図 10 については，通信パターンを視覚化するツール[9]を用いて表示した様子を図 11 にも示しておく．

図 9 では，1 つの Source ホストが，1 つの Source DNS に，複数の Destination FQDN の検索を行っており，図 5 で示した Source DNS での探索要求の照合を行えることがわかる．

図 10 では，1 つの Source ホストが複数の Source DNS に，共通した Destination FQDN の検索を行っており，図 6 で示した Destination DNS での探索結果の照合を行えることがわかる．

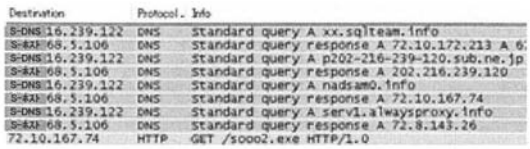

図 9. 1 Src DNS からの多 Dst ホストの検索通信

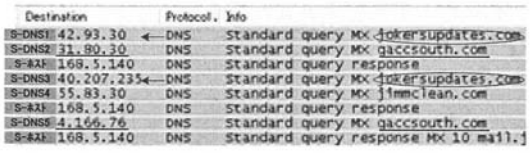

図 10. 1 Src ホストから多 Src DNS の検索通信

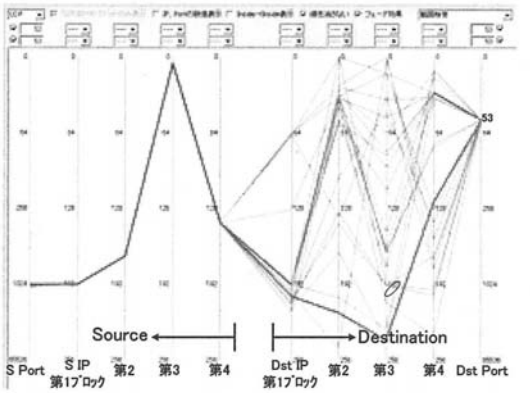

図 11. 図 10 の DNS 通信の視覚化（1 対多通信）

5. 有効に機能する条件についての考察

本手法は，攻撃者側が被害者の Destination IP を特定するときに DNS 検索を行うことを想定している．よって，直接 Destination IP を指定して送信元 IP の詐称攻撃を行う場合には，これを探索できない．昨今の Bot を利用した攻撃の場合，指令の中に Destination IP を直接指定することもできるため，本手法を容易に回避されることは否めない．その場合には，指令サーバを DNS 検索した通信を探索することで対応する．

本手法では，DNS サーバが相互連携する必要があり，DNS サーバ自身もしくは専用のプローブ装置を設置することになる．こうした機能を簡易に実装する手法について，今後課題とする．

6. おわりに

本研究では，詐称 IP 攻撃に対して，DNS サーバのログの中から，攻撃の直前に FQDN を検索した Source IP を探し出す手法を提案した．その際，Bot の中には，複数の DNS サーバに，複数の FQDN 検索を行う特徴があることが判明し，これら複数の探索要求や探索結果を照合することで，共通して現れる Source IP をより疑わしい発信元と判定する手法についても提案した．また，Source IP が詐称されていることを，攻撃パケットに含まれる Source IP と攻撃先の FQDN のハッシュ値を用いて問い合わせることで，秘匿性を担保した確認手法も検討した．

本手法は，既存の DNS サーバのログや，DNS 通信プローブのみで実現できることから，簡易な探索手法として普及が期待される．また，Destination DNS から Source DNS へ直接問い合せて探索するため，ホップ数に依存せず高い探索成功率も期待される．

謝辞

本研究は，独立行政法人情報通信研究機構(NICT)の委託研究「インターネットにおけるトレースバック技術に関する研究開発」の一環として行なわれた．ここに深謝します．

参考文献

[1] Strayer, W.T. Jones, C.E. Tchakountio, F. Snoeren, A.C. Schwartz, B. Clements, R.C. Condell, M. Partridge, C., “Traceback of single IP packets using SPIE，” DARPA Information Survivability Conference and Exposition, Proceedings, Vol. 2, pp. 266-270, April 2003.

[2] A.C. Snoeren, C. Partridge, L. A. Sanchez, C.E. Jones, F. Tchakountio, S.T. Kent, and W.T. Strayer “Hash-Based IP Traceback，” Proceeding or SIGCOMM ’01, August 2001.

[3] Steven Bellovin, and Marcus Leech, Tom Taylor, “ICMP Traceback Messages,” IETF, Internet Draft, draft-ietf-itrace-04.txt, Aug. 2003.

[4] D. Song and A Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback,” Proc. of IEEE Inforcom, April, 2001.

[5] Hiroaki Hazeyama, Youki Kadobayashi, Masafumi Oe, and Ryo Kaizaki, “Intertrack: A federation of IP traceback system across borders of network operation domains,” Proc. of Annual Computer Security Application Conference (ACSAC2005), Technology Blitz Session, Dec. 2005.

[6] Keisuke Takemori, Koji Nakao, “Performance Analysis of IP Traceback Systems with Serial and Parallel Control Schemes,” IEEE, PACRIM’07, T31-1 Session, August 2007.

[7] Nepenthes, http://nepenthes.mwcollect.org/

[8] Ethereal, http://www.ethereal.com/

[9] 竹森敬祐，三宅優，“Firewall ルールの作成に適した通信パターンの視覚化と攻撃パターン検知，” 信学，SCIS 2008, 2C1-4, 2008 年 1 月．