Vol.2010-DPS-142 No.14
Vol.2010-CSEC-48 No.14
2010/3/4

IP アドレスデータベースと確率的パケットマーキングを用いたパケットフィルタリング機構の設計

木内 忠司[†1] 堀 良彰[†1] 櫻井幸一[†1]

近年, インターネットの普及によってネットワークは広がり企業から家庭まであらゆる場所からインターネットへと接続することが可能なった．それに伴い様々な脅威も増大している．

その一つに DoS（Denial of Service：サービス不能）攻撃という脅威がある．これらの DoS や DDoS 攻撃に対処するため, 発信元を特定の技術である IP トレースバック技術やパケットが通過する際にその情報を元に疑わしいパケットの通信を遮断するフィルタリングなどが研究されている．本稿ではパケットフィルタリングについて注目する

本研究では Tao Peng らによる IP アドレスデータベースによるフィルタリングと Minho Sung らによる通信経路を攻撃者が通過した経路と通過してない経路の二つに分け, 遮断を行うフィルタリング手法を組み合わせたフィルタリングの提案を行う．

A Design of History Based Packet Filtering with Probabilistic Packet Marking

Tadashi Kiuchi ,[†1] Yoshiaki Hori [†1]
and Kouichi Sakurai [†1]

The network extended by the spread of the Internet, and the Internet became it from all places possible in recent years. Various threats increase along with it, too. There is a threat of DoS (Denial of Service: It is not possible to serve) attack in the one.

The sending origin is researched to deal with these DoS and DDoS attack and filtering etc. that intercept the communication of IP trace backing technology that is a specific technology and a doubtful packet are researched. The packet filtering is paid to attention in this announcement.

It proposes filtering by Tao Peng by the Internet Protocol address data base and filtering that divides into two (the route where the attacker passed the communication route by Minho Sung and the route that doesn't pass), and combines the intercepted filtering approaches in the present study.

1. はじめに

近年，インターネットの普及によってネットワークは広がり企業から家庭まであらゆる場所からインターネットへと接続することが可能なった．だがネットワークを介したさまざま脅威も存在する．その一つに DoS（Denial of Service：サービス不能）攻撃という脅威がある．DoS 攻撃とは図 1 に示したように大量のパケットを標的となるサーバに対して送信することで通信回線やサーバのリソースを過度に消費させることでそのサービスの提供を妨害する攻撃手法である．従来の単一箇所から発信される DoS 攻撃に加え複数地点から攻撃パケットが送信される DDoS（Distributed Denial of Service：分散型サービス不能）攻撃もまた大きな問題となっている[1)]．

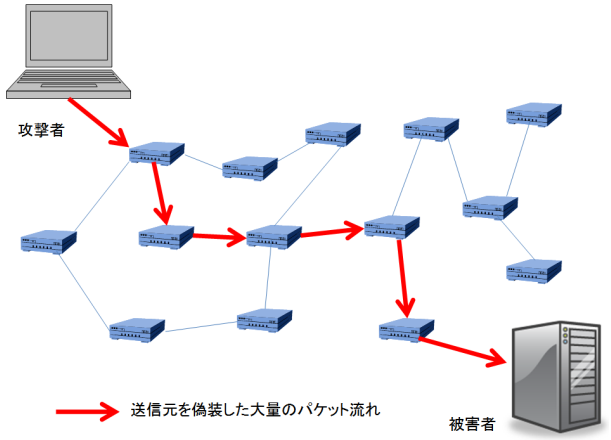

図 1 DoS 攻撃について

†1 九州大学大学院システム情報科学研究院
Graduate School of ISEE, Kyushu University

Vol.2010-DPS-142 No.14
Vol.2010-CSEC-48 No.14
2010/3/4

これらの DoS や DDoS 攻撃に対処するためには攻撃パケットの発信源をつきとめる必要があるが，DoS 攻撃に用いられる攻撃パケットは通常，送信元の IP アドレスが偽装されているため発信源をつきとめ攻撃者を特定することが困難なものとなっている．そこで発信元の IP アドレスが偽装されていたとしてもそのパケットの発信元を特定するための IP トレースバック技術や疑わしいパケットをルータを通過させずに遮断するパケットフィルタリングなどが研究されている[2]．

本稿ではまず DoS 攻撃の攻撃パケットを遮断するためのパケットフィルタリングに注目した二つの研究について紹介する．Tao Peng らによる手法では IP アドレスデータベースと呼ばれるものに, ルータを通過する IP パケットの送信元 IP アドレスとそれぞれの IP アドレスが何度現れたか記録していく．この記録を元にルータを通過する IP アドレスを頻繁に現れる IP アドレスとそうでないものに分け，普段あまり観測されない IP アドレスを優先的にフィルタリングすることで DoS 攻撃が行われている間，正常な通信を守ることができる．Minho Sung らによる手法では確率的パケットマーキングを用いて被害者から見て，パケットの送信経路を攻撃者によって影響を受けた経路を影響を受けてない経路に分け，，受信パケットの増加から攻撃を攻撃を検知すると攻撃者が利用した経路からの通信を遮断しその攻撃の大部分を回避する手法が提案されている．Tao Peng らによる手法では事前に攻撃者により攻撃パケットが適当な IP アドレスである程度通信を行っておくことでフィルタリングを避けることができる問題がある．

そこで，パラメータ設定は複雑になるが両方式の問題点を解決するものとして確率的パケットマーキングとルータでの送信元 IP アドレスの観測を利用したフィルタリング手法を提案する．この提案手法では伝送されるパケットを途中のルータで確率的パケットマーキングを利用しマークを行う．さらに被害者近傍のルータでは伝送されてくるパケットの送信元 IP アドレスを常に観測し頻繁に現れる送信元 IP アドレスを調べる．DoS 攻撃が始まるとマーク情報から攻撃経路を特定し，頻繁に現れる送信元 IP アドレスとマーク情報から攻撃パケットのフィルタリングを行う．これにより，攻撃者でない発信元から送られたパケットが攻撃経路上でマークされていた場合パケットがフィルタリングされることを減らすパケットフィルタリングを行う．

本稿の構成は以下のようになっている．2 節ではパケットフィルタリングについて概説，3 節では提案方式の元となる既存手法の紹介，4 節では提案手法について紹介，最後に 5 節で結びを述べる．

2. 背　　景

2.1 パケットフィルタリング

DoS 攻撃に対抗する手段の一つとして研究されているものの一つに入力フィルタ方式と呼ばれるものがある．この方法はネットワークの境界となるノードで不正な送信元と正しい送信元をもったパケットを区別しフィルタリングする手法のことである. すべてのネットワークにおいて送信元の IP アドレスを偽造できないように設定できれば IP トレースバック技術は必要ないが, ホストが接続されるすべてのインターフェースにおいて入力フィルタを設定しなければ IP アドレスの偽造を許してしまうため, 入力フィルタによる問題解決にはネットワーク管理者の手作業に委ねられる. ところがすべての作業を手作業で行うことは困難であるため自動化を行うため研究が行われている．

2.2 確率的パケットマーキング

ここでは IP トレースバックベースのフィルタリング方式[5] で用いられている確率的パケットマーキングについて説明する．経路復元のための情報を ICMP トレースバック法のように別のパケットにおさめて送るのではなく，その情報をルータを通過する IPv4 パケットのヘッダ内の未使用ビットを使って被害者へと伝えようとする方式で，ネットワークへの余計な負担をかけないですむ利点がある．この手法では IP パケットのフラグメントの際に用いられるヘッダ情報である図 2 に示した IP identiffication フィールドを流用して，ルータにおいてパケットが通過した際に一定の確率でそこにマークを行う．この設計はフラグメント化したパケットはインターネットを流れるトラフィックに対しわずかな量であるため，IP identiffication フィールドの流用に問題はないはずであるという前提に基づき行われている．一般にルータを識別するための IPv4 のアドレスは 32 ビットであるのに対し IP identiffication フィールドは 16 ビットであるため符号化アルゴリズムにおいて何らかの工夫が必要となる．また受け取ったマークからもパケットの発信源の特定のため，複合化アルゴリズムにおいて何らかの知識を必要としたり，膨大な計算を必要としたりする場合がある．

Savage らの発表した提案はマーキング方式に関する最初の論文で，R_s をマークを行うルータの IP アドレス，R_e を R_s へパケットを転送した 1 ホップ前のルータの IP アドレスとした時，隣接するルータの IP アドレスの組を (R_s, R_e) として各リンクを表現し，これを細分化して IP identiffication フィールドに埋め込み逆探知を実現しようとする方式である[3]．

アドレスの排他的論理和 $(R_s \oplus R_e)$ によって (R_s, R_e) を簡潔に表現し，これを edge-id

Vol.2010-DPS-142 No.14
Vol.2010-CSEC-48 No.14
2010/3/4

と呼ぶ．複数の edge-id からルータの IP アドレスを求めるにはそれぞれの edge-id が観測点からホップ数が既知であればよい．そこでホップ数 0 のルータの IP アドレス R_0 を元に隣接ルータのアドレス $\hat{R}$ は $\hat{R} = R_0 \oplus (R \oplus R_0)$ から求められる．よって，観測点からのポップ数を記録するため，マーク内の 5 ビットを割り当てさらに edge-id を 8 個の断片に分割し復元のため 3 ビットをオフセットとして割り当てる．

同一のポップ数に複数の edge-id が存在すると，復元の過程で異なる edge-id から生成された edge-id の断片と組み合わせてしまい IP アドレスを正しく復元できない危険性がある．そこで符号化の際に IP アドレスとそのアドレスのハッシュ値をビットインターリーブしこれを 8 個の断片にして分割し送信する．復元したアドレスが正しいかどうかはビット・インターリップから戻した値から検証できる．

3. 関 連 研 究

3.1 履歴情報によるフィルタリングを用いた DoS 攻撃防御に関する研究

まず Tao Peng らによる 手法[4] について説明する.DoS 攻撃でな通常のトラフィックの送信元 IP アドレスは過去の通信を一ヶ月観測するとその中に 5 回以上登場する IP アドレスが全体の 9 割ほどを占めるというデータに基づき提案されている．各エッジルータは IP アドレスデータベースと呼ばれるものを用意し, ルータを通過するパケットの送信元 IP アドレスを一定期間保管しておく. 攻撃を受けていない間にパケットに記されているそれぞれの IP アドレスごとに一定期間内に観測された頻度に応じて正規の IP アドレスのリスト・頻繁に現れる正規の IP アドレスリストに分け記録を行う. 特定の IP アドレスの出現頻度が増えてきたことが観測された場合, その IP アドレスがリストに載っているか調べる. 載っていない場合, そのパケットを攻撃パケットと判断し破棄する. それが正規の IP アドレスリスト・頻繁に現れる正規の IP アドレスリストに載っている場合はある程度の量の通信は許容しそれ以上の頻度でパケットを観測した場合, それを破棄する.Tao Peng らは実験により DDoS 攻撃の間, ８０～９０%の正規の通信が行えることが示された.

問題点としては, 攻撃者がこの方法でフィルタリングを行っていることを知っていた場合, あらかじめダミーの通信を送っておくことでフィルタリングをされにくくすることが可能であることが挙げられる.

3.2 IP トレースバックベースのパケットフィルタリングの研究

続いて Minho Sung らによる手法[5] について紹介する.

この手法は IP トレースバックの手法の一つである確率的パケットマーキングを用いて被害者から見て，パケットの送信経路を攻撃者によって影響を受けた経路を影響を受けてない経路に分け，攻撃経路を通過してきたパケットをフィルタリングすることで DoS 攻撃に対処するというものである．DoS 攻撃のパケットを遮断するため [3] の論文により DDoS 攻撃の際にはパケットは下図のようにして被害者へとパケットが届くことがわかっている. 上図は [2] の方式についてあらわしたものである. 被害者へと攻撃者または正規のクライアントから通信が行われるとき各ルータでは以下の動作を行う.

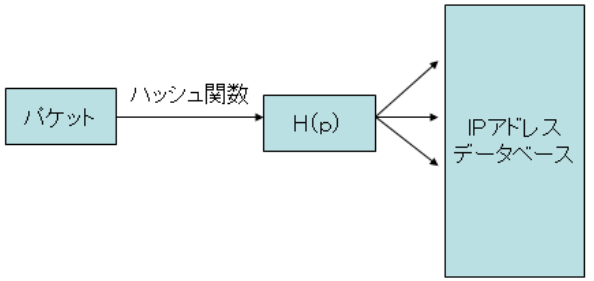

図 2 履歴情報によるフィルタリングにおいて IP アドレスデータベースへの記録の流れ

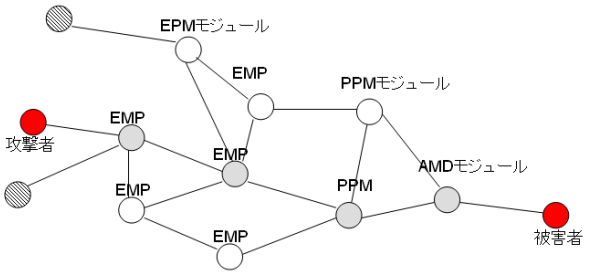

図 3 IP トレースバックベースのパケットフィルタリング　各モジュールの配置例

- EPM(Enhanced Probabilistic Marking) モジュール：確率的パケットマーキングと同様に一定の確率でアドレス情報をパケットの未使用領域へと書き込む働きをする.
- PPF(Preferential Packet Filtering) モジュール：攻撃の検出とフィルタリングを行う

Vol.2010-DPS-142 No.14
Vol.2010-CSEC-48 No.14
2010/3/4

かどうか AMD モジュールへ支持を行う働きを持つ.

- AMD(Attack Mitigation Decision-making) モジュール：攻撃経路を経由して送信されてきたパケットを遮断する働きを持つ.

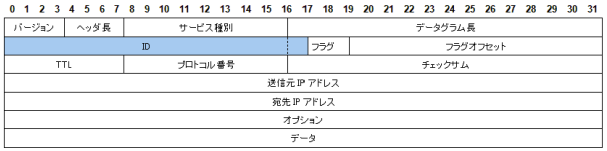

図 4 IP トレースバックベースのパケットフィルタリングでのマーキングに利用する領域

パケットが送信元からあて先まで転送されていくとまず途中でいくつかの EMP モジュールを経由して伝送される．このとき各ルータでは一定確率でルータのアドレスの情報が書き込まれ，送信先で攻撃を検知するとこの情報を元にパケットがどのルータを経由して伝送されてきたかを構築する．

EPM モジュールで書き込まれた情報を元に PPF で攻撃を検出すると,AMD モジュールにおいてパケットに書き込まれた情報を元にフィルタリングを行う.

ネットワーク上の経路を攻撃者により利用された部分とそうでない部分に分けフィルタリングを行うことで,DDoS 攻撃を受けていても何もしない場合の 3 倍から 7 倍のスループットを得ることができる. 問題点としては正当な通信も遮断されてしまうことが挙げられる.

4. 提 案 手 法

履歴ベースのフィルタリング手法では攻撃前にあらかじめダミーのデータを送られると弱く，また IP トレースバックベースのフィルタリング手法では正規の通信（攻撃パケットでないもの）を破棄する可能性がある．そこで，それぞれの手法を組み合わせることで両方式の問題点を解決するものとして確率的パケットマーキングとルータでの送信元 IP アドレスの観測を利用したフィルタリング手法を提案する.

4.1 各モジュールの役割

ここでは各ルータに持たせる働きについて説明する.

- **攻撃検知モジュール**
  フィルタリングにより守りたい被害者近傍に配置する．入力パケットを観測し，攻撃を受けているかどうかの判別を行う．攻撃を検知するとフィルタリングを開始するようにフィルタリングモジュールへと指示を出す
- **マーキングモジュール**
  通過するパケットに対し，一定確率 q でパケットの未使用領域に対し当該ルータの位置情報としてこのルータにパケットを伝送した隣接ルータとの IP アドレスの XOR を記録する.
- **フィルタリングモジュール**
  守りたいホスト近傍に配置する．攻撃を検知した場合，マーキングモジュールでマークされた情報から攻撃経路の特定を行う．特定した攻撃経路をもとに，この経路を通過して届いたパケットに対し下記のホワイトリストと照らし合わせ，過去にパケットの送信元 IP アドレスが現れた頻度に基づきフィルタリングする.
- **ホワイトリスト作成モジュール**
  平時は通過するパケットの IP アドレスを記録しホワイトリストの作成を行う．どこに配置するか，検討の余地があるが今回はフィルタリングモジュール内に配置する．リストを参照しホワイトリストに載っている送信元 IP アドレスを持つパケットについては過去の履歴情報に基づき通過させ，載っていないものに対しては遮断するフィルタリングを行う.

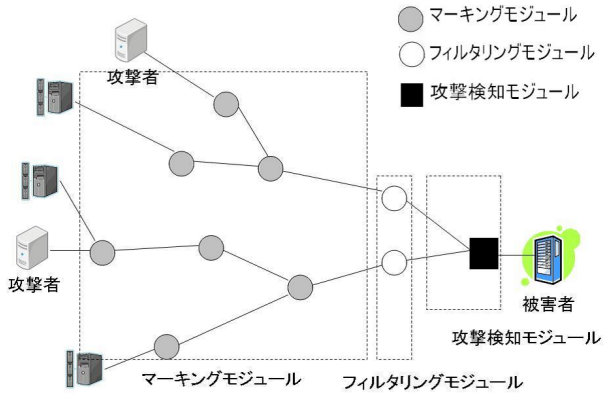

図 5 提案方式のモジュール配置例

Vol.2010-DPS-142 No.14
Vol.2010-CSEC-48 No.14
2010/3/4

4.2 提案方式の挙動

ここでは提案方式がどのように DoS 攻撃のパケットをフィルタリングするかの説明をする．図５は提案方式のモジュールの配置の一例を挙げたものである．

まず，DoS 攻撃が行われていない時，伝送されるパケットがどのように扱われるか説明する．送信元から宛て先までパケットが伝送されると，パケットはいくつかのマーキングモジュールを経由して伝送されることになる．パケットがマーキングモジュールを通過する際には一定確率 q でパケットの未使用領域に対しルータの位置情報として１ホップ前のルータとの IP アドレスの XOR を記録する．いくつかのマーキングモジュールを経由し，フィルタリングモジュールに伝送される．フィルタリングモジュールでは届いたパケットの IP アドレスをアドレスごとに何回通過したか記録していく．IP アドレスがどのくらいそのルータで観測されたかを記録することで，そのルータにおいてある送信元 IP アドレスを持ったパケットが頻繁に通過するかどうか知ることができる．フィルタリングモジュールを経由してパケットは攻撃検知モジュールへと伝送される．ここでは届くパケットを観測し DoS 攻撃を受けているかどうかの検知を行う．

次に DoS 攻撃が開始されたときの提案方式の挙動について説明する．マーキングモジュールでは DoS 攻撃中もパケットへ確率的マーキングを続ける．攻撃検知モジュールで DoS 攻撃を検知すると，ここからフィルタリングモジュールへ被害者の IP アドレス情報とともに DoS 攻撃を受けていることを知らせる．DoS 攻撃を受けていることを知らされたフィルタリングモジュールは，マーキングモジュールでパケット内にマークされた情報を元に DoS 攻撃のトラヒックがどの経路を経由して伝送されてきたのか調べる．攻撃経路を経由してこなかったパケットはフィルタリングせず伝送する．攻撃経路を経由してきたパケットに対しては，過去に作成したホワイトリストを用いて、ある IP アドレスが観測期間中何日以上現れたかを d，ある送信元 IP アドレスを持つパケットが何パケット以上現れたかを u とするとき，過去に d 日以上かつ u 個以上のパケットを伝送していた IP アドレス以外をフィルタリングする．

4.3 各モジュールの設計

この節では前節で述べた各モジュールの働きを実現するための，各モジュールの設計について述べる．

フィルタリングモジュールでは以下の操作を行う．

- **入力**
  攻撃パケット，非攻撃パケットの入力が行われると，送信元 IP アドレスごとにカウントし頻繁に現れる送信元 IP アドレスのリストを作成する．
  フィルタ実行の指示の入力を攻撃検知モジュールから受けるとフィルタを開始する．
- **出力**
  フィルタリングされなかったパケットの伝送を行う．
- **保持情報**
  ホワイトリスト：平常時（非攻撃時）に観測された送信元 IP アドレスとそれぞれの出現回数を記録．
  攻撃経路情報：攻撃検知後ルータに届くパケットにマークされた情報を元に攻撃経路を特定しフィルタリングに利用する．
- **パラメータ**
  d：ある送信元 IP アドレスが観測期間中何日以上観測されたか．攻撃経路上でマークされ，観測期間中 d 日以上観測されていないパケットをフィルタリングする．
  u：ある送信元 IP アドレスを持つパケットが観測期間中何パケット観測されたか．観測期間中 u 個以上観測されていないパケットをフィルタリングする．
- **フィルタリングについて**
  攻撃経路を通過し頻繁に現れないパケットをフィルタしていく．攻撃経路を経由してこなかったパケットはフィルタリングせず伝送し，攻撃経路を経由してきたパケットに対しては，ホワイトリストを参照し過去に d 日以上かつ u 個以上のパケットを伝送していた IP アドレス以外をフィルタリングする．

攻撃検知モジュールでは以下の操作を行う．

- **入力**
  攻撃パケット，非攻撃パケットの入力を受け内蔵の IDS により攻撃検知が行えると仮定する．
- **出力**
  入力パケットを伝送する．攻撃を検知するとフィルタリングモジュールに対しフィルタリングを開始するよう指示を送る．
- **保持情報**
  IDS に必要な情報を保存

Vol.2010-DPS-142 No.14
Vol.2010-CSEC-48 No.14
2010/3/4

マーキングモジュールでは以下の操作を行う.

- **入力**
  攻撃パケット，非攻撃パケットの入力を受け取ると一定確率 q で 1 ホップ前のルータとマークを行うルータの IP アドレスの XOR を未使用領域に書き込む.
- **出力**
  入力パケットを伝送，マークを行った場合，マークされたパケットを伝送.
- **パラメータ**
  q：パケットに対してマーキングを行う確率.

4.4 既存手法と提案手法との比較

この節では 4.2 節で述べた提案手法と 3.1 節で述べた履歴ベースのフィルタリング手法と 3.2 節で述べた IP トレースバックベースのフィルタリング手法について比較を行う.

表 1 はそれぞれの手法について攻撃パケットの遮断率、正規の通信の遮断率、攻撃前に攻撃に利用する偽装 IP アドレスを IP アドレスデータベースへ登録を行った後の攻撃に対する脆弱性、パケットの未使用領域への書換が必要かどうか、パラメータ数がいくつになるかについてまとめたものである．攻撃パケットの遮断率はトレースバックを用いた手法で 9 割強[5]、履歴ベースの手法では 8 割～9 割[4] ほどである．両手法の仕組みを利用した提案方式も同程度の結果が得られると思われる．正規の通信の遮断率はトレースバックを用いた手法では 2 割から 3 割、履歴ベースの手法では頻繁にあて先アドレスと通信をしていないため、IP アドレスデータベースに登録されていない IP アドレスを持つ通信者が 1 割ほどいる場合、それらの通信者は DoS 攻撃発生時フィルタリングされる．提案方式では IP アドレスデータベースを用いるほか、履歴ベースの手法では遮断されてしまう IP アドレスデータベースに登録されていないの IP アドレスを持つ通信社のパケットも届けることができるため、履歴ベースと同程度かそれ以下に遮断率に抑えられる．履歴ベースの手法はこの手法をとっていることが攻撃者にわかっているとすると、あらかじめ攻撃者によりいくつかの偽装アドレスを履歴へ何度か登録させた後攻撃を行われると弱いという欠点を持っている．IP トレースバックベースのフィルタリングにはこの攻撃は意味を成さない．提案手法では攻撃経路を通過したパケットに対し履歴情報を参照するため履歴ベースの方法よりは頻繁な IP アドレスとして登録されるのに必要パケットが多くなるため、履歴ベースの手法に比べると攻撃がしにくくなる．従来手法でパラメータが 1 つ、2 つであったのに対し提案手法では 3 つ設定する必要があるが確率的パケットマーキングのパラメータ設定とフィルタリングの閾値の設定のパラメータとで互いに独立したパラメータであるためパラメータ設定が煩雑化することはないと考えられる.

5. 結　　論

近年, ネットワークの普及とともに増加しているインターネットにおける脅威の一つである DoS 攻撃が問題となってきている．DoS 攻撃は大量の不正なパケットを攻撃対象に送信することで対象のサービスの提供を妨害する.DoS 攻撃に対処するにはまずその攻撃の発信元を特定しなければならないが，DoS 攻撃に用いられる攻撃パケットは通常, 送信元の IP アドレスが偽装されているため, その特定は困難である. そこで DoS 攻撃に用いられる IP パケットを途中のルータで遮断し攻撃からホストを守るパケットフィルタリングが研究されている

本稿では DoS 攻撃からホストを守るための手法として履歴ベースのパケットフィルタリングと，IP トレースバックベースのパケットフィルタリングの二つの手法について紹介し，それぞれの問題点について述べた．そこで，パラメータ設定は複雑になるが両方式の問題点を解決するものとして確率的パケットマーキングとルータでの送信元 IP アドレスの観測を利用したフィルタリング手法を提案し，それを実現するための設計と提案手法と既存手法の評価を行う枠組みを示した.

今後の目標としては，本稿で示した提案手法とその評価を実際に行い提案手法の有用性を示すことが挙げられる.

謝辞　本研究の一部は，独立行政法人科学技術振興機構 (JST) 戦略的国際科学技術協力推進事業（日印研究交流）による研究課題「数理科学的手法による暗号アルゴリズム解析とネットワークセキュリティ強化評価」の支援を受けている.

参　考　文　献

1) David R. Mirza Ahmad, “ハッキング対策マニュアル” ソフトバンククリエイティブ December 2003
2) 門林雄基，大江将史，“IP トレースバック技術”，情報処理，Volume 42，Number 12，December 2001
3) S Savage, D Wetherall, A Karlin, T Anderson “Network suport for IP traceback,” IEEE/ACM Transactions on Networking, Vol.9, No.3, pp.226-237,June 2001.
4) Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao “Protection from Distributed Denial of Service Attack Using History-based IP Filtering,” Proc . of the IEEE International Conference on Communications, p.p. 482-486 , May 2003
5) Minho Sung and Jun Xu, Member, IEEE “IP Traceback-Based Intelligent Packet

Vol.2010-DPS-142 No.14
Vol.2010-CSEC-48 No.14
2010/3/4

表 1 提案手法と既存手法比較

	攻撃パケットの遮断率	正規の通信の遮断率	IAD へ登録からの攻撃	パケット書換	パラメータ数
提案方式（4．1節）	良	少ない	やや弱い	必要	3
履歴ベースのフィルタリング（3．1節）	良	少ない	弱い	不要	2
IP トレースバックベースのフィルタリング（3．2節）	良	やや多い	受けない	必要	1

Filtering: A Novel Technique for Defending against Internet DDoS Attacks," IEEE Transactions on Parallel And Distributed Systems, VOL. 14, NO. 9, p.p. 861-872, September 2003