目次

目次 i
概要 ii
1. はじめに 1
2. 既存技術とその課題 2
2.1 マーキング方式 2
2.2 Hash-based 方式 2
3. MAC-based IP トレースバック 3
3.1 MAC 情報の利用方法 3
3.2 アドレス情報の記録 4
3.3 シグネチャリスト 5
3.4 システムの構成と追跡動作 6
4. 実装 7
5. 評価 8
5.1 性能測定 8
5.2 問合せ時間の測定 10
5.3 閾値の調査 10
5.3.1 実験 1 SYN Flood 攻撃 11
5.3.2 実験 2 ICMP Flood 攻撃 13
5.2.3 実験 3 HTTP GET Flood 攻撃 14
5.4 既存技術との比較 16
6. まとめ 17
謝辞 18
参考文献 19
研究業績 21
付録 22
DoS 攻撃の分類と概要 22
DoS 攻撃の分類 22
DoS 攻撃の概要 23

概要

インターネット利用人口の増大に伴い, 悪意ある利用者による DoS 攻撃が多発している. DoS 攻撃は正常なアクセスとの区別ができず，ファイヤーウォールの設置やルータのフィルタリングといった方法で防ぐことは難しい．また，送信元の IP アドレスが偽造されていることがほとんどで，攻撃者の特定は困難とされている．これまで様々な IP トレースバック技術が研究されているが，攻撃経路を正確に追跡できなかったり，ルータの処理負荷が大きくなる等の問題が指摘されている. そこで我々は偽造が困難なルータの MAC アドレスに着目した MAC-based IP トレースバックを提案する．MAC-based IP トレースバックはパケットの転送回数が閾値を超えた場合のみ DoS 攻撃の可能性があると判断し，攻撃経路の情報を生成する．また，様々な DoS 攻撃に対応するためシグネチャを利用して DoS 攻撃ごとに閾値を決定する．提案方式を実装し評価を行った結果，ルータに与える負荷は十分に小さく，様々な DoS 攻撃を検出できることを確認した.

1. はじめに

インターネット技術は情報交換手段における社会基盤のひとつとして定着し，現在では，電子商取引や有料コンテンツ配信など様々なサービスが展開されている．しかし，これらのサービスを妨害する攻撃が脅威となっている．中でもサービス不能攻撃（DoS 攻撃）は，ターゲットホストに対して大量の接続要求やデータを送りつけることによりホストを機能不全にしたり，ネットワークのトラヒックを増大させるなどしてネットワークの機能を麻痺させる攻撃であり，防御が極めて困難な攻撃として問題になっている．

DoS 攻撃は正当な通信との区別が困難なため，ファイヤーウォールの設置やルータのフィルタリングといった方法で防ぐことは難しい．ソフトウェアの脆弱性をついた攻撃においては，少量の攻撃パケットでホストが麻痺する場合もある．これに対してはセキュリティ更新プログラムをサーバに適応することで回避できるが，攻撃者はセキュリティホールの検出を続けるため，一時的な防御法にしかならない場合が多い．

DoS 攻撃を回避するには，攻撃ホストと接続されているルータを発見し，接続を切断したり，通信のトラフィックを制御する必要がある．しかし，送信元アドレスは偽造されている場合がほとんどであり，攻撃者を特定するのが難しいという特徴がある．そのため，ルータに残された情報をたよりに手作業で上流のルータをさかのぼる必要があり，人的労力が膨大になる．

このような DoS 攻撃に対して追跡過程の自動化を行い，身元が偽造されていても攻撃ホストを特定できる技術として，IP トレースバック技術[1]が盛んに研究されている．IP トレースバック技術は，主にルータに機能を追加し，攻撃パケットが通過した経路をさかのぼる．

既存の IP トレースバック技術には以下のようなものがある．ICMP パケットに追跡のための情報を送信する ICMP 方式[2]，パケット自体に追跡のための情報を埋め込むマーキング方式[3], 全てのパケットをログとして記憶する Hash-based 方式[4][5]が提案されている．多くの研究は IP レイヤの情報を利用するが，MAC(Media Access Control)の情報を利用する方式も一部に見られる[6].

最近では特定のネットワーク内でのトレースバックだけではなく，隣接するネットワーク間でのトレースバックを相互連携させるシステムが提案されている[7]．本稿では，ネットワーク間におけるトレースバックの相互連携よりも，ネットワーク内における途中経路の特定を行い，最終的に攻撃ホストが接続している隣接ルータまでの追跡を前提に話を進める．

本研究では攻撃者による偽造が困難なルータの MAC アドレスに注目し，かつ DoS 攻撃の可能性がある場合のみ必要な情報を記録する MAC-based IP トレースバックを提案する．DoS 攻撃パケットは特定の上位ルータから同じ宛先 IP アドレスで大量に送られる．このとき，上位ルータの MAC アドレスから上位ルータを確実に特定，記憶しておくことにより，攻撃の経路を推測する手がかりを得る．また，ルーティング処理時にパケットの転送回数

を計測し，一定の閾値を超えると攻撃と判断する．攻撃の種類によっては閾値が異なることがあるため，DoS 攻撃ごとにシグネチャを定義，DoS 攻撃の可能性があるかどうかを判断する．攻撃ごとに閾値を設けることで様々な DoS 攻撃に対応させることが可能である．

提案システムを実装した結果，攻撃ホストまでの経路を追跡できることを確認するとともに，ルータの性能劣化はほとんど無いことを確認した．

さらに，実際にサーバに DoS 攻撃を仕掛け，DoS 攻撃ごとに閾値を決定することを試みた．

2 章で既存技術と課題を述べ，3 章で MAC-based IP トレースバック，4 章で実装，5 章で評価を述べ．6 章でまとめを行う．

2. 既存技術とその課題

以下に代表的な IP トレースバック技術として，マーキング方式と Hash-based 方式について概要とその課題を述べる．

2.1 マーキング方式

マーキング方式は，ルータがパケット転送時に，ある一定の確率で攻撃経路の情報を生成する方式である．[3]では IP ヘッダの identification フィールドに中継ルータの IP アドレスを分割（フラグメント）して挿入し，被害ホストへ送り届ける．被害ホストはマーキングされたパケットを収集し，分割する前の IP アドレス情報を復元して攻撃経路を再構築する．新たに追跡のためのパケットを新たに発生しないことから，ネットワークに負荷をかけずに追跡を実行できる利点がある．しかし，攻撃流量が少ない場合，ルータはマーキングを行わないことや，経路構築の計算量が膨大になるという課題がある．

2.2 Hash-based 方式

Hash-based 方式は，ルータは転送する全てのパケットに対してログを記録する方式である．IP ヘッダの中でも，ルータを経由してもフィールド値が変化しない不変部分 20 バイトとペイロードの先頭 8 バイトを記録する．追跡においては，探査装置が被害ホストに隣接するすべてのルータに対して攻撃パケットのログが記録されているかどうかの判定を行う．該当するログ情報が記録されていれば，そのルータに隣接する上位ルータに対しても同様に判定を繰り返す．これにより，最終的に被害ホストまでの攻撃経路を構築する．攻撃パケットの情報が 1 つだけでも記録されていれば発信源を特定できるという利点があるが，パケットごとにハッシュ計算をするための高い処理能力がルータに求められる．随時パケットのログを記録し続けなければいけないため，ルータが保持する記憶容量によっては攻撃追跡のためのログ情報が失われる可能性があり，限られた時間で追跡を完了させる必要がある．[6]ではパケットのログを記録する際に，同時に MAC の情報も含める方式が提案されている．ログの記録と同時に攻撃パケットを転送した上位ルータの MAC の情報を記録

することにより，上位ルータの特定が容易になるという利点がある．

3. MAC-based IP トレースバック

MAC-based IP トレースバックは MAC の情報を利用して攻撃者の追跡を行う．MAC アドレスを利用することにより IP フィールドを偽造した攻撃に影響されないでトレースバックを行うことができる． DoS 攻撃の可能性のあるパケットから経路情報の記録を行う点に特徴がある．

3.1 MAC 情報の利用方法

攻撃ホストから被害ホストに DoS 攻撃が仕掛けられたときのパケットの MAC アドレスが変化する様子を図 1 に示す. 攻撃ホストから送信されたパケットの送信元 IP アドレスは一般に偽造されており，送信元 MAC アドレスも偽造されている可能性が大きい．攻撃パケットの内容は図 1 のように，IP アドレス“A IP”を持つ攻撃ホストが，IP アドレス“V IP”を持つ被害ホストに攻撃を仕掛けたとき, ルータを通過するごとに MAC アドレスが入れ替わっていく．このとき攻撃ホストが送信する攻撃パケットの送信元 IP アドレスは“A IP”から“F IP”に，MAC アドレスは“A MAC”から“F MAC”に偽造されているものとする．宛先 IP アドレスは被害ホストのアドレスであり，ルータを通過してもその内容は変わることがない．また，MAC アドレスは中継されるルータの MAC アドレスであり，この部分を偽造することはできない．つまり，攻撃パケットには被害ホストの IP アドレスと上位ルータの正しい送信元 MAC アドレスが必ず含まれている．

MAC-based IP トレースバックでは, ルータが攻撃経路の構築において攻撃パケットの送信元 MAC アドレスから上位のルータを特定して記録しておく. この情報をもとにトレースバックを行う．

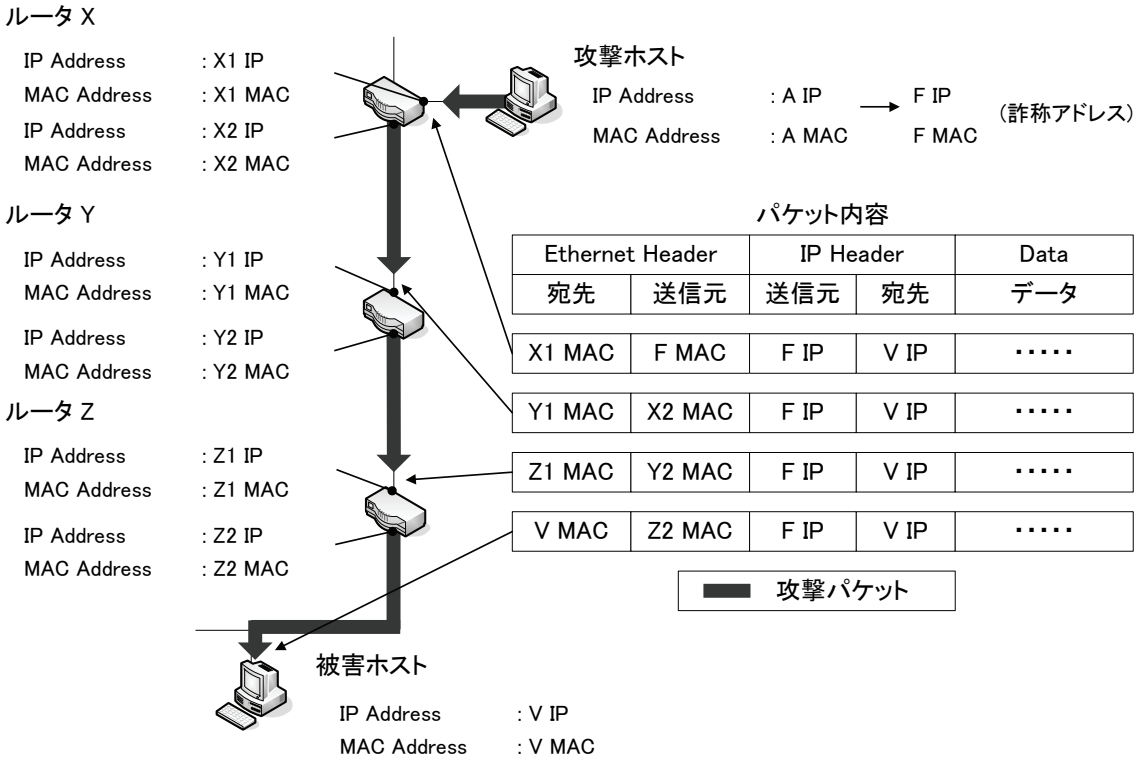

図 1. 攻撃パケットのアドレスが変化する様子

3.2 アドレス情報の記録

MAC-based IP トレースバックに対応したルータでは, 一般パケットと攻撃パケットの判別を行うために，単位時間あたりにおけるパケット転送回数をリアルタイムで計測する．ある宛先に対するパケットの転送回数が，設けられた閾値を超えると DoS 攻撃の可能性があると判断する．DoS 攻撃には様々な種類があるため，DoS 攻撃ごとにシグネチャを定義し，閾値を設定する．

ルータはシグネチャごとにパケット通過数を数える一時カウンタテーブル（TCT: Temporary Counter Table），及び経路構築時に参照するトレースバックテーブル（TBT: Trace Back Table）の 2 つを保持する（図 2）．パケット転送時にパケットの宛先 IP アドレスとシグネチャ, 転送回数を TCT に記録する．シグネチャには個々の DoS 攻撃を判別できるプロトコルタイプやポート番号等のフィールド名と値が記述される．TCT の内容は一秒程度の短い一定間隔で消去する．カウント値にはシグネチャごとに閾値が設けられており，カウント値が上記一定時間内に閾値を超えた場合，宛先 IP アドレスを攻撃対象とした DoS 攻撃が行われている可能性があると判断し，この時のパケットの送信元 MAC アドレスを利用して上位ルータを特定する．実際に TBT に記録する内容としては, ARP キャッシュテーブルから上位ルータの IP アドレスを取得し，この内容を記録する．TBT は攻撃の可能性があった場合のみ生成されるもので，数日単位の期間保持する．

このように上位ルータを特定するために MAC アドレスを利用するが, 上位ルータを TBT

に記憶するときは IP アドレスを用いる．これは，管理ホストからの追跡を行いやすくするためと，レイヤ 2 を抽象化するためである．プロバイダネットワークのレイヤ 2 は LAN とは限らず，ATM や専用線を利用しているところもある．このような場合においても TBT のフォーマットは変える必要はない．レイヤ 2 がイーサネットの場合は MAC アドレス，ATM の場合は VPI/VCI アドレスを入力値として ARP キャッシュテーブルを参照し，上位ルータの IP アドレスを取得する．一方，専用線の場合はインタフェース名を入力値としてルーティングテーブルを参照し IP アドレスを取得することができる．

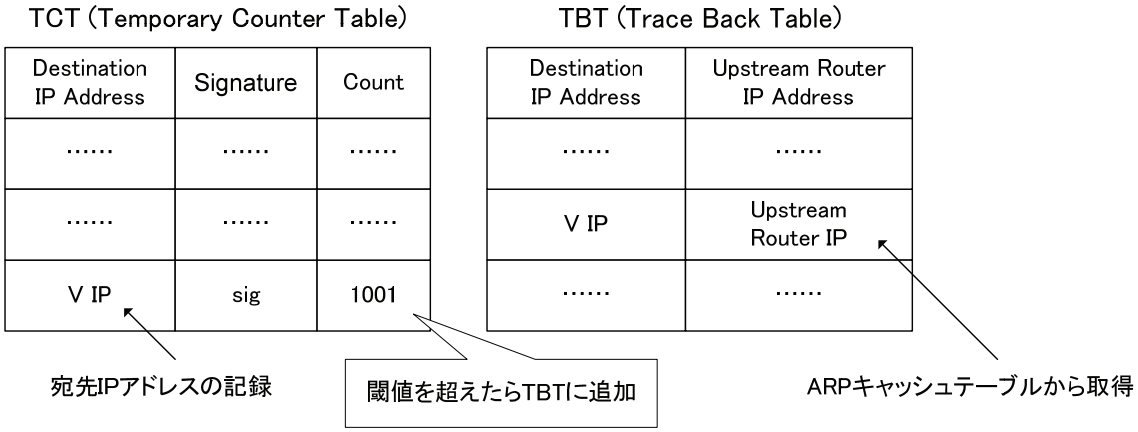

図 2．テーブル内容とアドレス情報の記録

3.3　シグネチャリスト

カウント値に設けられる閾値は，ルータの起動時にネットワークの管理者によって決定される．処理の重いプロトコルでは，少量のパケットでもシステムの機能を低下させ，OS の脆弱性をついた攻撃では単発のパケットを受信しても機能不全となる．あらゆる DoS 攻撃にも対応可能とするため，ルータは DoS 攻撃を判別するためのシグネチャリスト(signature list)を保持する．下記に，DoS 攻撃の中から代表的なものを 10 種類取り上げて定義を行った．それぞれの DoS 攻撃を判別するフィールドと値を表 1 に示す．表内，シグネチャ欄の括弧は実際の MAC-based システムで用いられる書式を記述した．シグネチャリストはプロトコルタイプごとにグループ分けできる．DoS 攻撃の判別においては，IP ヘッダのプロトコルタイプの値から対応するシグネチャグループを参照し，次にポート番号や TCP フラグといったフィールドを参照する．

表 1. DoS 攻撃の種類とシグネチャ

DoS攻撃名	プロトコルタイプ	攻撃タイプ	シグネチャ
SYN Flood	TCP	Flood系	プロトコルタイプ：TCP、TCPフラグ：SYN （ip_p = IPPROTO_TCP, th_flags_a = TH_SYN）
SYN Flood	TCP	Flood系	プロトコルタイプ：TCP、TCPフラグ：SYN （ip_p = IPPROTO_TCP, th_flags_a = TH_SYN）
Tear-Drop	TCP	脆弱性	プロトコルタイプ：TCP、 IPフラグメントオフセット：フラグメントオフセット＜受信したIPデータ長の合計 （ip_p = IPPROTO_ICMP, ip_flag_off < total_flag_len）
WinNuke	TCP	脆弱性	プロトコルタイプ：TCP、宛先ポート番号：139、TCPフラグ：URG （ip_p = IPPROTO_TCP, th_dport = 139, TH_URG = 1）
HTTP GET Flood	TCP	Flood系	プロトコルタイプ：TCP、宛先ポート番号：80、ペイロード：GET （ip_p = IPPROTO_TCP, th_dport = 80, data = GET）
Land-Attack	TCP	脆弱性	プロトコルタイプ：TCP、IPアドレス：宛先＝送信元、ポート番号：宛先＝送信元 （ip_p = IPPROTO_TCP, ip_src = ip_dst, th_sport = th_dport）
UDP Flood	UDP	Flood系	プロトコルタイプ：UDP （ip_p = IPPROTO_UDP）
IKE-DoS	UDP	脆弱性	プロトコルタイプ：UDP、宛先ポート番号：500 （ip_p = IPPROTO_UDP, th_dport = 500）
Ping-of-Death	ICMP	脆弱性	プロトコルタイプ：ICMP、IPフラグメント：IPオフセット*8+IPデータ長＞65535 （ip_p = IPPROTO_ICMP, ip_flag_off + ip_len > 65535）
ICMP Flood	ICMP	Flood系	プロトコルタイプ：ICMP、ICMPタイプ：要求 （ip_p = IPPROTO_ICMP, icmp_type = ICMP_ECHO）

3.4 システムの構成と追跡動作

MAC-based IP トレースバックは図 3 のようなネットワーク構成を想定する．攻撃ホストと被害ホストはプロバイダの外部ネットワークに存在し，プロバイダが提供するルータには本提案方式の機能が搭載されているものとする．プロバイダ内には管理ホストが存在し，DoS 攻撃が発生したときは管理ホストの指示に従いトレースバックを開始する．点線内がプロバイダに相当し，被害ホストは特殊な機能を持たない一般端末である．

被害ホストが DoS 攻撃を受けたことを知ると，被害者側のユーザはプロバイダに対して電話等により攻撃ホスト特定の依頼を行う．追跡時においては，管理ホストがルータに対して問合せを行い，ルータは TBT を参照し，順次返答することにより，攻撃経路を構築していく．

問合せを受けたルータは被害ホストの IP アドレスをキーに上位ルータの IP アドレスをすべて割り出して，管理ホストに返答する．管理ホストは返答結果から，次の上位ルータに問合せを行う．これらの操作を同様に行うことで，最終的に管理ホストは攻撃側の隣接ルータまでの IP アドレスを割り出し，攻撃経路を構築することができる．

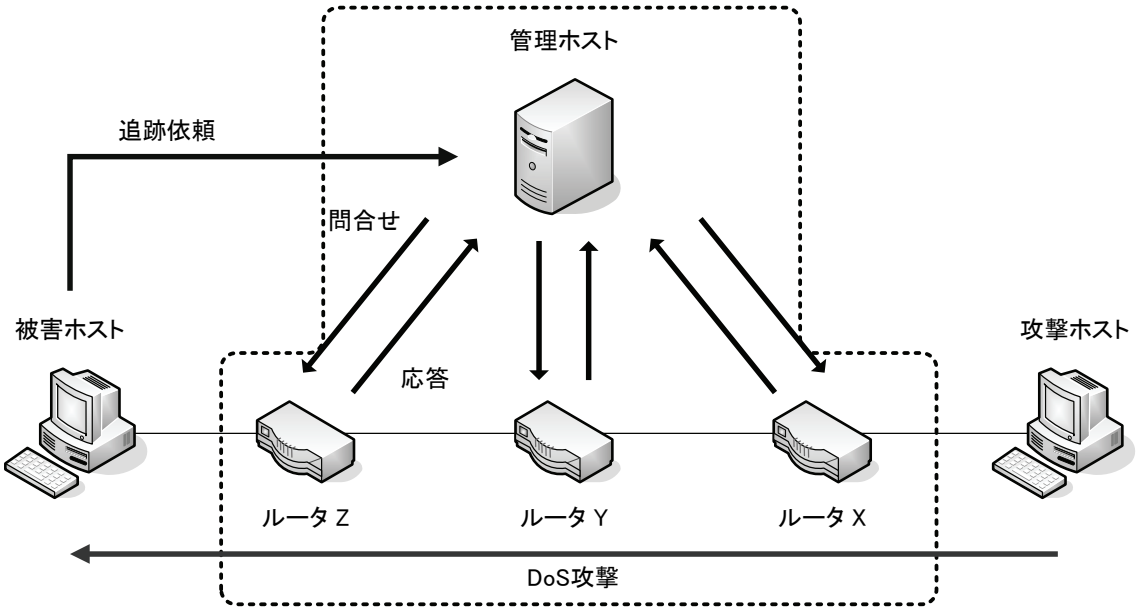

図 3. 想定するネットワーク構成

4. 実装

レイヤ 2 が LAN の場合を想定し，MAC-based IP トレースバックを実装し評価を行った．図 4 にルータのモジュール構成を示す．MAC-based IP トレースバックを実行するルータはカーネル内のデータリンク層において，追跡情報アドレスのためのテーブルを生成する．OS には FreeBSD 5.3-Release を選択した．

データリンク層の入力関数である ether_input()から MAC-based モジュールを呼び出し，入力パケットの内容を参照して TCT，TBT を更新する．処理されたパケットはデータリンク層の元の場所に戻すため，既存の通信処理には一切影響を与えない．

転送パケットを受け取ると，MAC-based モジュールが呼び出され，始めにシグネチャリストから DoS 攻撃の判別を行う．IP ヘッダのプロトコルタイプの値から対応するシグネチャグループを判別し，次にポート番号や TCP フラグといったフィールドを参照する．もし該当する DoS 攻撃のシグネチャと一致すれば TCT に宛先 IP アドレスとシグネチャを記述し，カウント値の増加を行う．カウント値の増加後にシグネチャの閾値を超えていれば TBT へ転記する．

管理ホストと通信を行う応答デーモンはアプリケーションで動作させている．管理ホストからの問合せがあった場合は MAC-based モジュールで生成した TBT をシステムコールで呼び出し，要求された宛先 IP アドレスと上位ルータの IP アドレスを抽出する．その後，Socket を利用して管理ホストと返答する．なお，管理ホスト側の処理は全てアプリケーション層にて実装した．

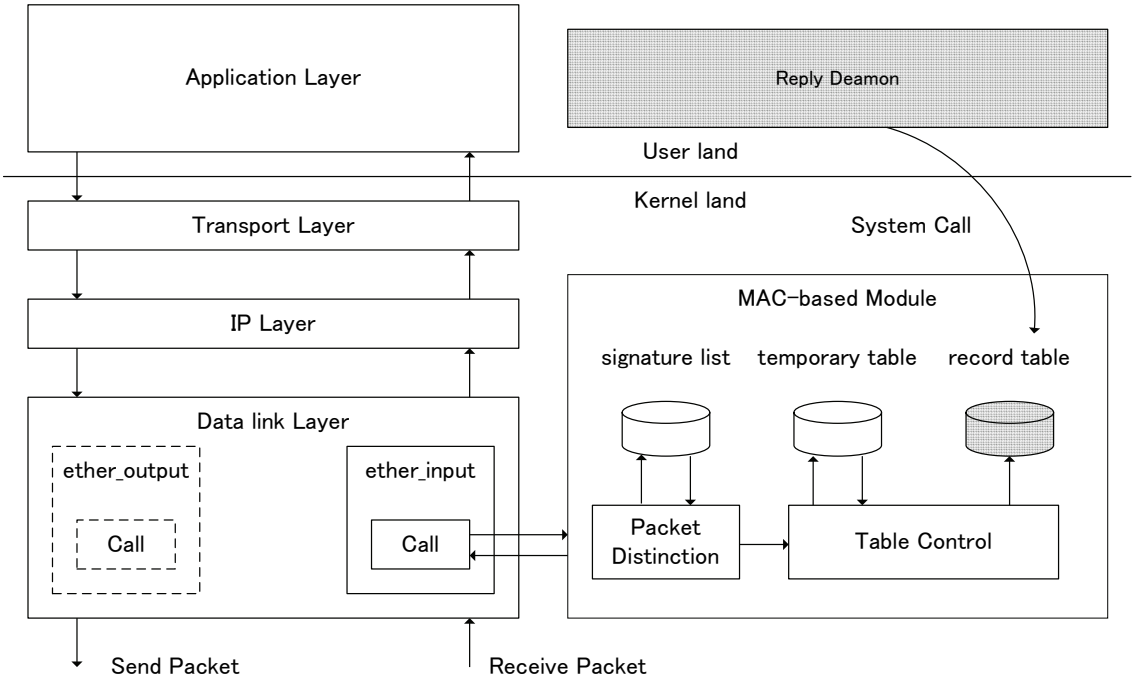

図 4. MAC-based IP トレースバックのモジュール構成

5. 評価

上記機能をルータ及び管理ホストに実装し，MAC-based 方式の性能測定として FTP によるスループット測定，パケット処理能力の測定を行い，提案方式を実装させた場合の処理低下を求めた．トレース実験を行った結果，正確な攻撃経路の構築が行えることを確認するとともに，管理ホストがルータに問合せを行ってから返答するまでの時間を測定した．シグネチャを定義するため DoS 攻撃種類と概要を調査し．実際にサーバに DoS 攻撃を仕掛け，サーバ負荷に基づいて閾値を求めた．ただし，ここで求めた閾値はサーバが停止，通信不能となる値であり，実際の設定ではある程度の余裕を持たせる必要がある．最後に既存技術と本方式の比較を行った．

5.1 性能測定

MAC-based システムを実装した場合に，ルータの中継処理に与える影響がどの程度あるのか，FTP を利用した実行スループット測定とパケット処理能力の測定を行った．実験機の環境は表 2 のとおりであり，LAN は 100BASE-TX で接続した．実装時の測定を行う場合には，ルータのシグネチャリストに 10 種類のシグネチャを保持しておいた．

表 2. 測定環境

	ルータ	サーバ	クライアント
CPU	Intel Pentium 4 2.4 GHz	Intel Pentium 4 3.2 Ghz	Intel Pentium 4 3.2 Ghz
メモリ	512 MB	1.0 GB	1.0 GB
OS	FreeBSD 5.3-Release	Windows XP Professional	Windows XP Professional

FTP スループット測定では，FTP サーバと FTP クライアントの間にルータを 1 段挟み，ルータに MAC-based モジュールを実装した場合と，そうでない場合を比較した．転送に用いるデータは 200,000,000 バイトの容量を持つバイナリデータとした．50 回測定を行った平均結果を表 3 に示す．MAC-based モジュールを実装した場合は，実装していない場合に比べスループット値の減少比は 0.0595% 程度となった．

表 3. FTP スループット測定結果

	実装なし	実装あり
スループット値［Mbps］	72.221	72.178

パケット処理能力では，ルータが 1 秒間に転送できるパケット数を求めるため，netperf を利用した．クライアントからサーバに対して UDP による一方向転送を行う．UDP のデータサイズを 18 バイトから 1,472 バイトまで変化させ，それぞれ 20 秒間の測定を 10 回行った結果を表 4 に示す．表から，実装後のパケット処理能力は，どのデータサイズでも減少比は 1%未満となった．データサイズが 18 バイトの減少比において，他の減少比より値が高いことに関しては， MAC-based モジュールの追加が若干影響していると思われる．パケットのデータサイズが小さい分，より多くのパケットを転送することになり，その分パケットの処理数が増え，モジュール追加によるオーバーヘッドが積み重なったものだと考えられる．

表 4. netperf によるパケット処理能力結果

データサイズ [byte]	18	512	1024	1472
実装なし［pps］	75,755	21,624	11,466	8,126
実装あり［pps］	75,109	21,623	11,463	8,120
減少比［%］	0.853	0.051	0.026	0.074

それぞれの実験において，実装時のルータはテーブルの更新とシグネチャの参照を行っていることを確認している．MAC-based モジュールの動作による処理負荷の増加は極めて低く．特に DoS 攻撃の判断においては，プロトコルタイプやポート番号の値がシグネチャと一致するかどうかをチェックするだけの動作を行っており，また，シグネチャはプロトコルタイプごとにグループ分けされているため，転送パケットに対してシグネチャリストの内容をすべてチェックする必要をなくしている．1 つの判別処理が単純であるため，処理時間も短く，シグネチャリストを今後増加させても処理速度はあまり低下しないと考えられる．測定結果から分かるように，ルータに MAC-based IP トレースバック機能を実装させてもパケット転送における影響はほとんどないと考えられる．

5.2 問合せ時間の測定

追跡時間を推定するため，管理ホストとルータ間における問合せ時間を測定した．事前に攻撃ホストは SYN Flood を利用した攻撃をターゲットに仕掛けおり，それぞれのルータが保持する記録テーブルには，被害ホストの IP アドレスと上位ルータの IP アドレスが記録されているものとし，管理ホストが問合せを行ってから，ルータからの応答が返るまでの時間を測定した．試行回数を 50 回としたときの平均値は 1.214[msec]となった．ルータ台数をｍとすると，それぞれの問合せに要する合計時間は 1.2*m[msec]となる．結果から，いくつかのルータホップをまたがった追跡でも短い時間で攻撃経路を構築することができる．

5.3 閾値の調査

MAC-based IP トレースバックにおいて DoS 攻撃ごとの閾値の決定が重要となる．実際にターゲットとなるサーバを構築し，DoS 攻撃ごとにサーバが使用不可となる閾値を調査した．本実験は提案方式と直接の関連はないが，閾値決定の目安を得るために参考となる．攻撃ツールとしては公開されている DoS 攻撃ソースコードを実験用に改造したものを用いた．代表的な DoS 攻撃として SYN Flood，ICMP Flood，HTTP GET Attack を選定した．

実験で用いたネットワーク構成を図 5 に示す．WEB クライアントが WEB サーバに対して繰り返し所定の HTTP 要求を行っている状態において，攻撃ホストから WEB サーバに DoS 攻撃を仕掛けた．実験構成は表 5 に示す．WEB サーバソフトウェアには Apache 1.6.2

を利用し，OS の設定を含め全てデフォルトとした．

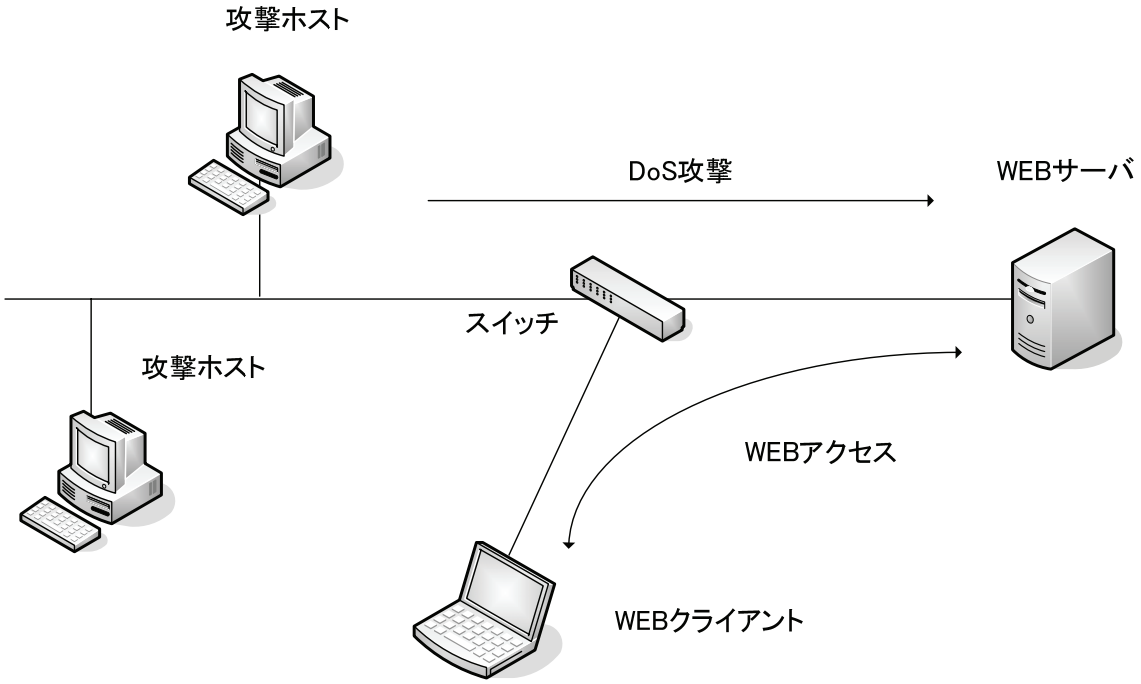

図 5．実験のネットワーク構成

表 5．実験機の構成

	攻撃ホスト	WEB サーバ	WEB クライアント
CPU	Intel Pentium 4 3.2 Ghz	Intel Celeron 2.66 Ghz	Mobile Intel Pentium 3 M 800Mhz
メモリ	1.0 GB	512 MB	256 MB
OS	Windows XP Professional	Fedora Core 4	Windows XP Professional

5.3.1 実験 1　SYN Flood 攻撃

攻撃ホストを 2 台使用し，ターゲットに対して同時に攻撃を仕掛けた．攻撃パケットレートを徐々に増加させたときのアクセス応答時間，同時に WEB サーバの CPU 負荷，プログラム完了時間を測定した．

プログラム完了時間として，サーバが平常時に 100[msec]要するプログラムを実行したとき，負荷をかけた状態での所要時間の増加を求める．実験で用いたプログラム内容の一部を以下に示す．if 文による空のループ処理を 14,000,000 回繰り返す処理が 100[msec]の所要時間を要することを確認している．

```
for( i = 0 ; i < 14000000 ; i++ ){}
```

図 6図 7からSYN Floodの攻撃パケットレートが6,500[pps]を境にアクセス応答時間，CPU 負荷ともに増加していることが確認できる．プログラム終了時間においては正常時より，20 倍の時間を要した．上記のパケットレート超えて送信した場合，WEB サーバからの応答が返らず，TCP コネクションのタイムアウトが敏感に発生した．攻撃パケットレートが 10,000[pps]の環境下ではプログラム終了時間は正常時より，100 倍の時間を要した．WEB サーバの OS には，デフォルトで SYN クッキーが設定されており，クッキーの計算が CPU 負荷を浪費させていると考えられる．結果から，実験環境と同等なネットワーク構成であれば，SYN Flood 攻撃に対する閾値はおおよそ 6,500[count/sec]となる．

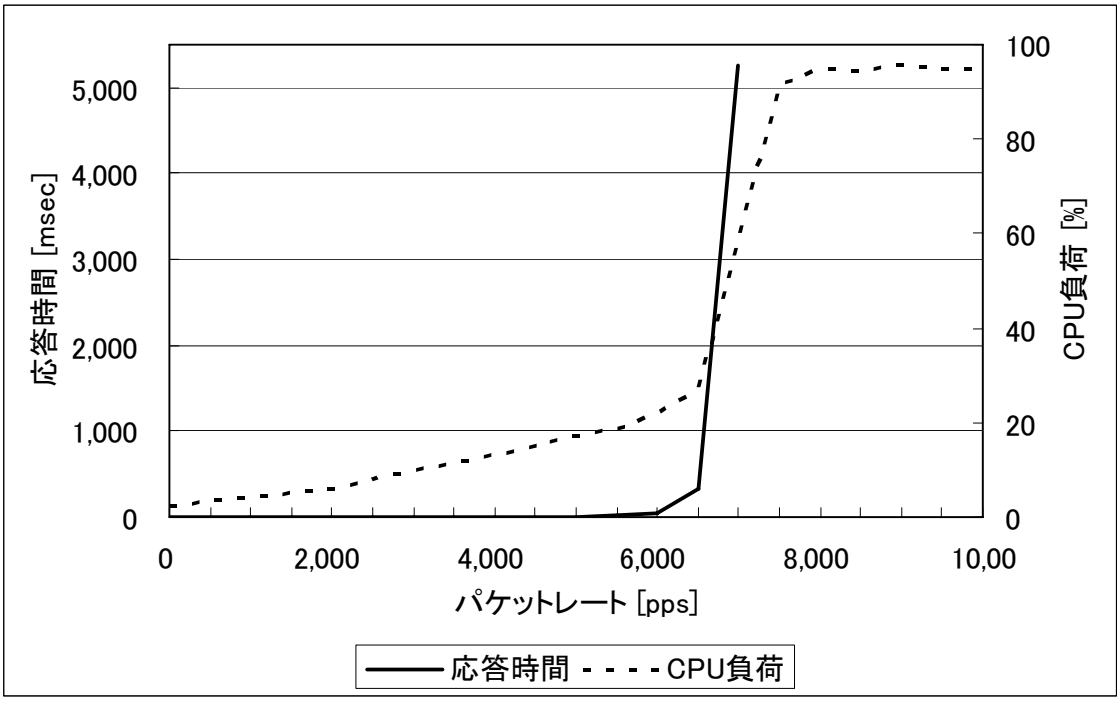

図 6. SYN Flood における応答時間と CPU 負荷

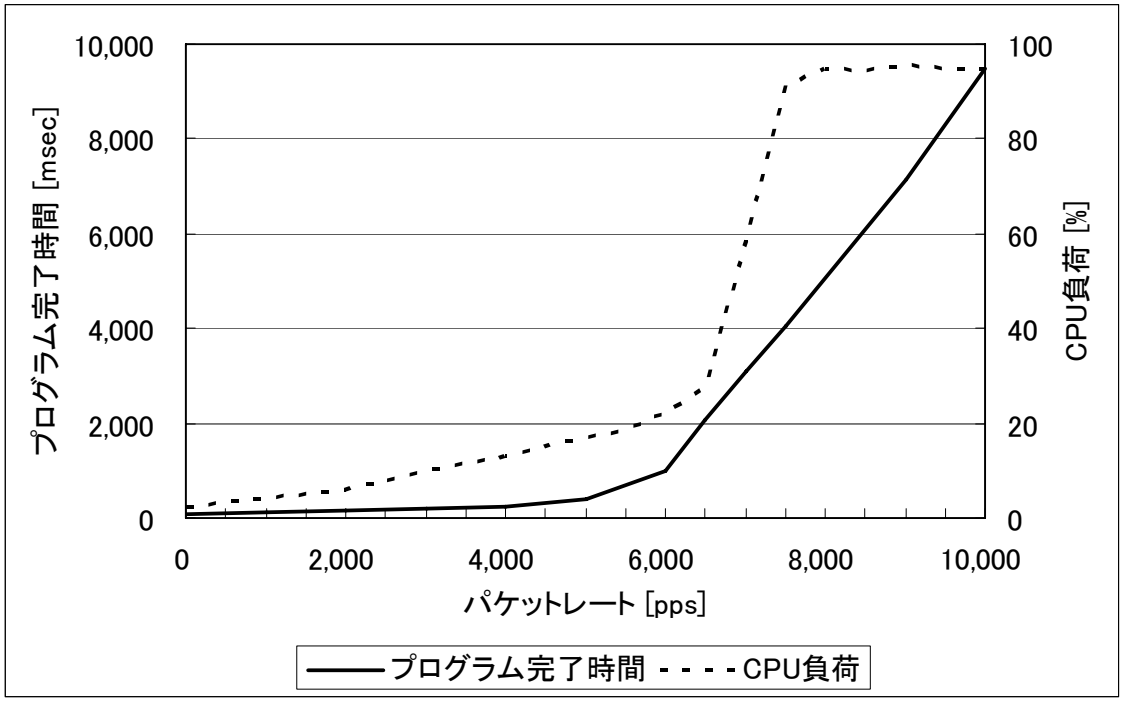

図 7. SYN Flood におけるプログラム完了時間と CPU 負荷

5.3.2 実験 2 ICMP Flood 攻撃

攻撃ホストを 2 台使用し，ターゲットに対して同時に攻撃を仕掛ける．攻撃パケットレートを徐々に増加させたときのアクセス応答時間，同時に転送パケットロス率を測定した．

ICMP Flood 攻撃のパケットデータサイズを 1,472 バイトとして設定させた．図 8 から攻撃パケットが，ルータ，スイッチが処理できる最大理論パケットレートの値である 8,127［pps］を超えてからパケットロス率が上昇し 40%となり，最終的に 100%へと到達することが予測できる.パケットロス率の増加に伴い TCP コネクションのタイムアウトが発生し，WEB アクセス応答時間が増加することに関しては，パケットロスによる再送制御が起因している．攻撃のパケットレートが 20,000[pps]を超えてから WEB サーバとの通信が不能状態になった．サーバの CPU 使用率を調べてみると，いずれのパケットレートにおいて 1%前後の値を示しており，ICMP Flood 攻撃はターゲットのシステムを低下させるのではなく，ネットワークの大域を浪費させる攻撃であることが分かる．結果から実験環境と同等なネットワーク構成であれば，ICMP Flood 攻撃に対する閾値はおおよそ 8,100[count/sec]となる．

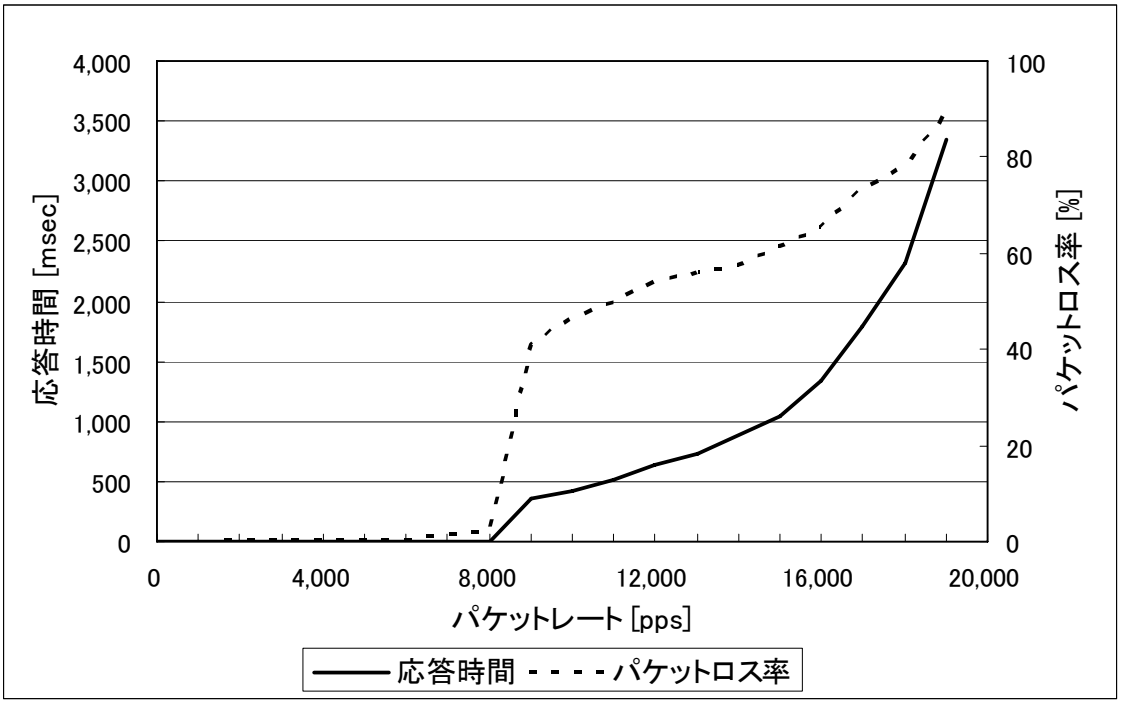

図 8. ICMP Flood における応答時間とパケットロス率

5.2.3 実験 3 HTTP GET Flood 攻撃

攻撃ホストを 10 台使用し，ターゲットに対して同時に攻撃を仕掛ける．攻撃パケットレートを徐々に増加させたときのアクセス応答時間，同時に WEB サーバの CPU 負荷，プログラム完了時間を測定した結果を図 9，図 10 示す．

攻撃ホストの HTTP リクエスト数を上げてターゲットに攻撃を仕掛けた結果，合計リクエスト数が 1,250[pps]を超えることはなかった．このことから，サーバが処理できる総リクエスト数は 1,250[pps]前後であると分かる．CPU 負荷においてはリクエスト数に比例して上昇し， プログラム完了時間においては，700[pps]の環境下で上昇し始め，1,250[pps]では正常時より，30 倍の時間を要した．このときの CPU 負荷は，ほぼ 100%である．結果から実験環境と同等なネットワーク構成であれば，HTTP GET Attack に対する閾値はおおよそ 1,250[count/sec]となる．

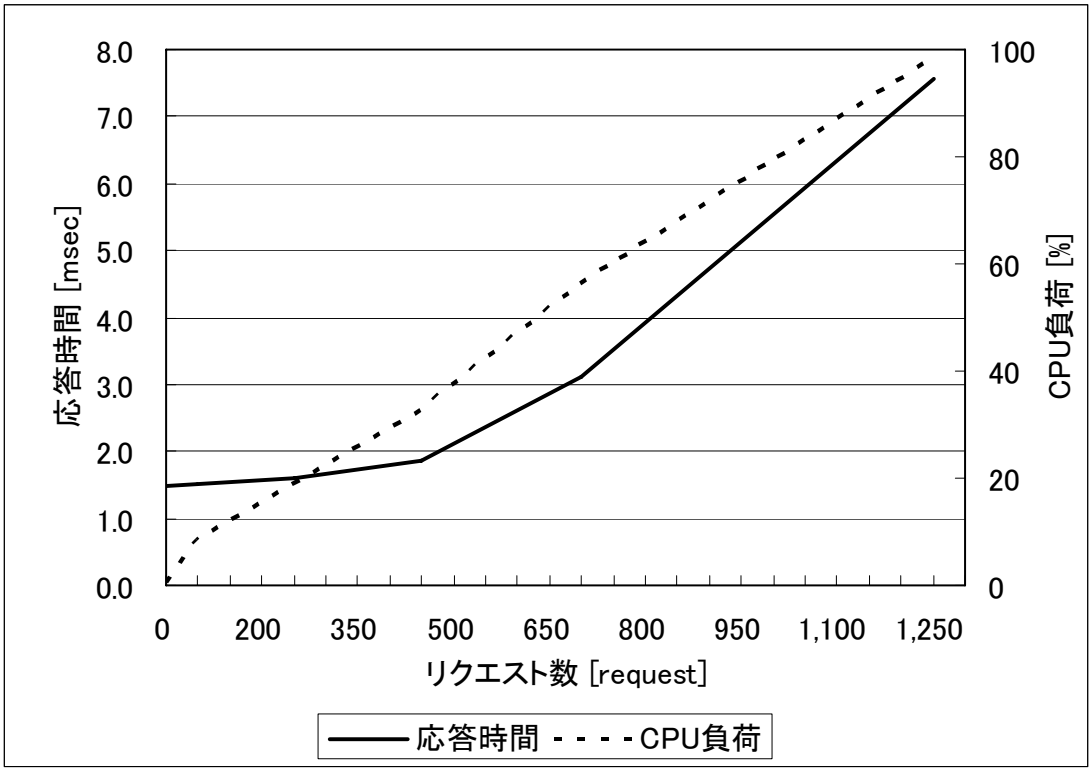

図 9. HTTP GET Flood における応答時間と CPU 負荷

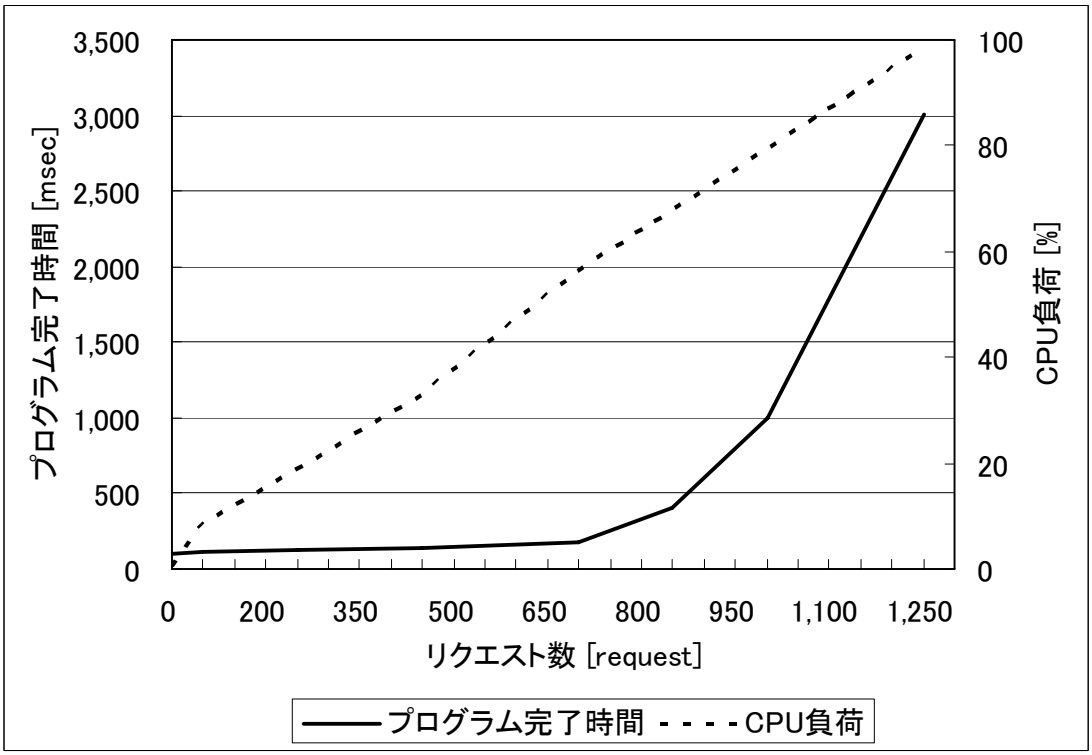

図 10. HTTP GET Flood におけるプログラム完了時間と CPU 負荷

実験 1，2，3 から得た閾値を表 6 にまとめる．また，Ping of Death 攻撃などの脆弱性を狙った攻撃は，OS のバージョンによっては 1 つのパケットを送りつけることでターゲットのシステムを停止させる．このような攻撃に対しての閾値は 1[count/sec]で TBT を更新する必要があると考え，表 7 のように定義した．定義を行った閾値を表 1 で示したシグネチャに関連付け，それぞれの攻撃をさらに試した結果，DoS 攻撃の判別と TBT への記録を確認した．脆弱性を狙った攻撃には，ターゲットとなるサーバの OS を Windows 95 に変更して実験を行った．

表 6．実験から得られた閾値

DoS 攻撃名	閾値[count/sec]
SYN Flood	6500
ICMP Flood	8100
HTTP GET Attack	1250

表 7．脆弱性を狙った攻撃に対する閾値

DoS 攻撃名	閾値[count/sec]
Ping of Death	1
WinNuke	1

5.4 既存技術との比較

既存方式と提案方式を比較した結果を表 8 に示す．ルータコストに関しては，Hash-based 方式は転送するすべてのパケットに対してハッシュ関数を適応させるのでルータにかかる負荷が大きく，処理能力の低いルータを用いるとパケット転送のスループットに影響を与える．MAC-based 方式は DoS 攻撃とみなされるパケットを転送した場合にのみ攻撃情報を記録し，ルータにかかる処理は極めて軽いため，ルータに必要なコストは小さい．

事後追跡に関しては，Hash-based 方式は十分な記憶容量を保持していなければ，ログの上書き等によって DoS 攻撃終了後に追跡情報が失われる可能性がある．限られた時間の間でルータに問合せをしなければ攻撃経路を構築できない．しかし，MAC-based 方式は DoS 攻撃と判断されるパケットから追跡のための情報を記録するため，経路情報が失われる可能性は低い．マーキング方式は DoS 攻撃の発生中に経路情報を被害ホストに通知するため，リアルタイムな追跡を行うことができる．

経路生成に関しては，Hash-based 方式はどのような攻撃流量に対しても追跡のための経路情報を記録することができる．一方，マーキング方式はパケット転送時に一定の確率で経路情報を生成するので，攻撃流量が少ない場合，また単発パケットの攻撃には攻撃者の追跡を行うことができない．MAC-based 方式はパケット転送回数の閾値によって経路情報を

記録するため，閾値の決定が特に重要となる．DDoS 攻撃のように攻撃者が複数の経路に分散している場合，攻撃ホストに近いルータほど攻撃パケットの流量は少なくなる．そのため閾値を小さく設定させると一般パケットが DoS 攻撃と誤って判断され，異なる経路情報を生成する．逆に，閾値が必要以上に大きい場合は経路情報を生成することができない可能性がある．

経路解析量に関しては，マーキング方式は膨大なマーキングパケットから攻撃経路の情報を再構築しなければならないことから，攻撃ホストの特定までに時間を要する．特に偽造されたマーキングデータを受け取った場合に計算量が増大する問題が挙げられている．Hash-based 方式は経路情報の構築にあたり，どの上位ルータが攻撃パケットを転送したのか分からないため，転送したと思われるすべての上位ルータに対して問合せを行う．その結果，問合せのために余分なトラフィックの発生を招いてしまう．MAC-based 方式は上位ルータの特定に MAC アドレスを利用している．

プロトコル定義に関しては，独自の追跡シーケンスを利用する Hash-based 方式と提案方式はエラーの発生を考慮した設計が必要であり，プロトコルを悪用した攻撃も重要視しなければならない．マーキング方式は，追跡を行う管理ホストとの通信を行わないため，プロトコル定義を必要としない．

表 8．既存技術と提案方式との比較

	ルータコスト	事後追跡	経路生成	経路解析	プロトコル定義
マーキング方式	○	○	×	×	○
Hash-based 方式	×	△	○	△	×
提案方式	○	○	△	○	×

6. まとめ

本研究では IP アドレスが偽造されても，パケットの MAC アドレスを利用することにより上位ノードを特定し，攻撃経路を構築できる MAC-based IP トレースバックについて検討した．MAC アドレスを利用することで上位ノードを安易に特定することが可能である．パケットの転送回数を計測し，設けられた閾値から攻撃経路の情報を記録するため，ルータに記録する容量が少ない．閾値を DoS 攻撃ごとに設定させるため，脆弱性をついた攻撃や処理負荷の高いプロトコルを利用した攻撃に対しても対応可能である．

MAC-based 方式を実装し，動作検証と性能測定を実施した．その結果，ルータにはほとんど負荷がかからないことを示した．

今後は，さまざまなネットワークトポロジ環境において，どの程度まで正確に攻撃経路をさかのぼることが可能か，実用性を確認するとともに，分散型 DoS 攻撃（DDoS 攻撃）に対しても正確に追跡できるように検討を行う予定である．

謝辞

本研究に関して，研究の方向や進め方など終始ご熱心なご指導とご教示を賜りました，名城大学理工学部情報工学科 渡邊晃教授に心より厚くお礼申し上げます.

本研究を進めるにあたり，研究内容に関して終始ご熱心なご指導とご教示を賜りました，名城大学理工学部情報工学科 小川明教授，高橋友一教授，宇佐見庄五講師に心より厚くお礼申し上げます.

最後に，本研究を行うにあたり，適切なご検討を頂いた，名城大学理工学部情報工学科渡邊研究室の皆様に心より感謝致します.

参考文献

[1] 門森雄基，大江将史“IP トレースバック技術”情報処理 Vol. 12，No. 42，Aug，2001.

[2] Steve Bellovin, et al,“ICMP Traceback Messages,” Internet-Draft, Expires Aug, 2003.

[3] S. Savage, D. Wetherall, A. Karlin, and T. Anderson,”Practical network support for IP traceback,” in Proceedings of ACM SIGCOMM’00, pp. 295.306, Aug. 2000.

[4] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent，and W. T. Strayer,“HashBased IP Traceback,” Proceedings of ACM SIGCOMM 2001，San Diego，CA，USA，Aug 2001.

[5] C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S.T. Kent and W. T. Strayer，“Single-Packet IP Traceback，” ACM/IEEE Transactions on Networking，vol.10，no.6，December 2002.

[6] Shigeyuki Matsuda，Tatsuya Baba，Akihiro Hayakawa，and Taichi Nakamura，“Design and Implementation of Unauthorized Access Tracing System,” in Proceedings of the 2002 Symposium on Applications and the Internet (SAINT 2002)，IEEE Computer Society，pp.74-81，January 2002.

[7] 大江将史，櫨山寛晃，門林雄基,”IP トレースバックシステムの相互接続アーキテクチャの提案”,”2004 年 IP トレースバックワーキンググループ報告書”, Feb. 2005.

[8] 岡崎直宣, 河村栄寿, 朴美娘, “サービス不能攻撃の追跡手法の効率化に関する検討”, 情報処理学会論文誌，Vol. 44，No. 12，Dec. 2003.

[9] BLOOM，B. H. Space/time trade-offs in hash coding with allowable errors. Communications of ACM 13，7 (July 1970)，422–426.

[10] D. X. Song and A. Perrig，“Advanced and authenticatedmarking schemes for IP traceback,” in Proceedings of IEEEINFOCOM 2001，Apr. 2001.

[11] K.-C. Lan，A. Hussain，and D. Dutta，“The Effect of Malicious Traffic on the Network,” USC/ISI.

[12] D. Moore，G.M. Voelker，and S. Savage，“Inferring internet denial-of-service activity,” In Proc. USENIXSecurity Symposium，Washington D.C，Aug. 2001.

[13] 鈴木彩子，大森圭祐，松嶋 竜，川端まり子，大室 学，甲斐俊文，西山 茂,“IP トレースバックシステムの数学モデルと実証実験”,情報通信研究機構季報, Vol.51, Nos.1/2，2005.

[14] 石橋勇人，山井成良，安部広多，大西克美，松浦敏雄,”IP アドレス/MAC アドレス義存に対応した情報コンセント不正アクセス防止方式”，情報処理学会論文誌，Vol.40，No.12，1999.

[15] S. Savage, D. Wetherall, A. Karlin, and T. Anderson，”Practical network support

for IP traceback,”in Proceedings of ACM SIGCOMM’00, pp.295.306, Aug. 2000.

[16] C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S.T. Kent and W. T. Strayer “ Single-Packet IP Traceback , ” ACM/IEEE Transactions on Networking, vol.10, no.6, December 2002.

[17] 伊藤大輔,泉裕, 齋藤彰一, 上原哲太郎, 國枝義敏,”TCP セッション管理による DoS 耐性の考察”, 情報処理学会研究報告, 2001-QAI-1, pp.183-190, 2001.11.

[18] H. Burch, B. Cheswick,”Tracing Anonymous Packets to Their Approximate Source , ” In Proceedings of the 14th USENIX Systems Administration Conference, pp.313−322, Dec.2000.

[19] T. Baba and S. Matsuda：“ Tracing Network Attacks to Their Sources,” IEEE InternetComputing, vol.6, no.3, pp.20-26, 2002.

[20] 池田竜朗, 山田竜也,“発信源追跡のためのハイブリッドトレースバック方式”東芝レビュー, Vol.58, No.8, 2003.

研究業績

1. 学術論文

なし

2. 国際会議

なし

3. 口頭発表

[1] 播磨宏和，渡辺晃，“MAC アドレスを用いた IP トレースバックの提案”，平成 16 年度電気関係学会東海支部連合大会，Sep.2004.

[2] 播磨宏和，渡辺晃，“MAC アドレスを用いた IP トレースバック技術の提案”，第 67 回情報処理学会全国大会，Mar.2005.

[3] 播磨宏和，渡辺晃，“MAC-Based トレースバック方式の実装”，平成 17 年度電気関係学会東海支部連合大会，Sep.2005.

[4] 播磨宏和，渡辺晃，“MAC アドレス情報に基づく IP トレースバック技術の提案 “，マルチメディア，分散，協調とモバイル（DICOMO2005）， Jul.2005.

[5] 播磨宏和，渡辺晃，“MAC-based トレースバック方式の提案”，マルチメディア，分散，協調とモバイル（DICOMO2006）， Jul.2006.

付録

DoS 攻撃の分類と概要

DoS 攻撃の分類

DoS 攻撃は 2 つに分類される.

・大量のパケットを送信する攻撃
|
├── コネクション型（正当通信）
|　　|
|　　└── Octopus, HTTP GET Flood, HTTP POST Flood
|
└── コネクションレス型（偽造通信）
　　|
　　└── SYN Flood, LAND,Smurf, UDP Flood, ICMP Flood

・TCP/IP モジュール実行におけるバグを利用する攻撃
|
├── ICMP プロトコルの脆弱性
|　　|
|　　└── Ping of Death, Jolt, Jolt2, SSPING, IceNUKE
|
├── フラグメント処理の脆弱性
|　　|
|　　└── Teardrop, Teardrop2, Bonk, Boink
|
└── NetBIOS プロトコルの脆弱性
　　|
　　└── WinNuke

DoS 攻撃の概要

DoS 攻撃の中でも特に代表的な攻撃を抜粋し概要を示す.

フラッド系の攻撃

SYN Flood

SYN Flood は TCP の 3 ウェイハンドシェイクを利用した攻撃である. 攻撃者は送信元 IP アドレスを偽造した大量の SYN パケットをターゲットに送信する. SYN パケットを受信したターゲットは偽造 IP アドレスへ向けて SYN/ACK パケットを返し, ACK 応答を待ち続ける. このときターゲットは TCP コネクションにおけるハーフオープン状態となり，ACK 応答を受信するためにハーフオープン状態をバッファに記録する. ACK 応答が返ってこないまま攻撃者からの新たな SYN パケットを受信し続ける結果, バッファが埋め尽くされシステム機能低下および通信不能状態に陥る.

UDP Flood

UDP Flood は非常に大きなデータサイズを持つパケットを送信または，小さなサイズを持つパケットを大量送信することで，ターゲットに負荷をかける攻撃である．ターゲットが UDP ポートを開いていない場合や UDP パケットを処理できない場合は ICMP Port Unreachable メッセージを偽造された送信元 IP アドレスに返す．ターゲットは UDP パケットの受信処理に追いつかずにシステム機能低下および通信不能状態に陥る．また，ICMP Port Unreachable メッセージの氾濫によってネットワーク大域全体が埋め尽くされ，トラフィックの速度が低下する.

ICMP Flood

IPCP Flood は Ping Flood とも呼ばれ，大量の ICMP 要求をターゲットに送信する攻撃である．ターゲットは ICMP 応答に処理が追いつかずにシステム機能低下および通信不能状態に陥る．ICMP 要求を受け取ったターゲットは偽造 IP アドレスに対して ICMP 応答を送信するため，UDP Flood と同様にネットワーク大域を埋め尽くす.

Smurf

Smurf は送信元アドレスにターゲットの IP アドレスを挿入した ICMP 要求をブロードキャスト送信する攻撃である．基本原理，効果は ICMP Flood と同じであるが，攻撃者が直接ターゲットに攻撃を仕掛けるものではなく，宛先として第 3 者のホストをパケットの増幅を行うリフレクタとしている．ネットワークに属するすべてのホストが攻撃者から送信された ICMP 要求を受け取ると，ターゲットを宛先として一斉に ICMP 応答パケットを送信することになる．攻撃者から送信された 1 つの ICMP 要求

はリフレクタにより増幅されるため，ICMP Flood よりも大きな効果をもたらす.

HTTP GET Flood

HTTP GET Flood は WEB サーバをターゲットにした攻撃であり， WEB ブラウザでターゲットとなる WEB ページを表示させ更新を何度も行う. 大勢の攻撃者から一斉に HTTP 要求を行うことでサーバに大きな処理負荷を与える．サーバの処理能力を超える負荷がかけられた場合，システム機能低下および WEB 機能停止に陥る．同時に TCP セッションを大量に確立するため，TCP コネクションのリソースを消費させる.

脆弱性をついた攻撃

Ping-of-Death

Ping-of-Death は IP パケットの最大サイズを超える ICMP 要求パケットを送信することで，受け取ったターゲットはシステム停止に陥る．IP パケットの最大サイズは 65,535 バイトである. 20 バイトの IP ヘッダ, 8 バイトの ICMP ヘッダを除くと, ICMP に格納できる最大データ長は 65,507 となる．OS の一部では ICMP の最大データ長を超えたサイズを指定することが可能である．攻撃者から送信されたパケットはルーティング過程で複数のフラグメントに分割されてターゲットに届く．ターゲットは収集したフラグメントパケットを TCP スタック内で構築するが，IP パケットのサイズが 65,535 バイトを超えてオーバーフローを起こす．その結果，ターゲットは通信不能状態に陥る.

WinNuke

WinNuke は NetBIOS の脆弱性をついた攻撃で，ポート番号 139 に TCP でコネクション接続を確立した後，URG フラグを立てたパケットを送信することでターゲットは通信不能状態に陥る.

Land-Attack

Land-Attack は送信元 IP アドレスと送信元ポート番号の値を，それぞれ宛先と同じ値に改変した SYN パケットを送信する攻撃である．パケットを受信したターゲットはコネクション確立を試みるが，自分自身に ACK 応答を送信することになる．結果的にこの処理は TCP アイドルタイムアウト時間が経過するまで行われ，システム機能低下およびシステム停止に陥る.

Tear-Drop

Tear-Drop はフラグメント重複における脆弱性をついた攻撃である. フラグメントパ

ケットの構築の際，データが重複されるようにフラグメントオフセットの値が設定されている．攻撃者は意図的に 2 つのフラグメントパケットをターゲットに送信する．2 つ目のフラグメントパケットのフラグメントオフセット値を，最初に送信した IP データのサイズより小さい値に設定させる．その結果，ターゲットは TCP スタック内でデータを上書きしてしまい，通信不能状態やシステム停止に陥る．

IKE-DoS

IKE-DoS は IPsec で用いられる鍵交換プロトコルの脆弱性をついた攻撃であり，IPsec サービスが起動しているターゲットの 500 番ポートに非常に大きなデータを持つ UDP パケットを送信し続けることで CPU 使用率を消費させる．