第 3 章 Realtime tracing とは

1. Realtime tracing とは

前章では、現在 Tracing を行う際に利用される一般的な技術に関して述べたが、これらの技術を利用するだけでは確実な攻撃元ホストの特定をリアルタイムに行うことは不可能であるのが現状である。

攻撃元ホストの特定は、まず、攻撃として検知されたパケットの内容を調査することから始まる。しかし、この調査において、確実性の点で問題となるものが送信元 IP アドレスである。攻撃として検知されたパケットに含まれる送信元 IP アドレスは、一見攻撃元ホストの IP アドレスともとれる。もちろん、送信元 IP アドレスが実際の攻撃元ホストの IP アドレスである場合もあるが、多くの場合、身元の隠蔽や使用する攻撃手法のため、その送信元 IP アドレスは全く関係のない IP アドレスであったり、攻撃に使用する第 3 のホストの IP アドレスであったりする。そのため、送信元 IP アドレスをそのまま攻撃元ホストの IP アドレスとして安易に判断することはできず、攻撃として検知されるパケットの送信元 IP アドレスは、常に偽造されている可能性があることを考慮しておく必要がある。

攻撃者による送信元 IP アドレスの偽造に惑わされることなく、実際の攻撃元ホストの IP アドレスを追及し、その結果に確実性を伴わせるためには、攻撃として検知されたパケットを元に、その経路を適切な順序で追跡する作業が要求される。このようなパケット経路をさかのぼり、その発信源を突き止める作業は一般的にトレースバックと言われるが、これらの追跡作業を既存の技術を用いて行う場合には、人間の手動処理による膨大なデータ記録やシステムログ等に対する精査が要求され、必然的に多大な時間とコストをかけることになる。

また、実作業以外にも、例えば、インターネット経由による攻撃を受けた場合、攻撃元ホストの特定のために重要な痕跡であるデータ記録やシステムログ等が、自分の管理するシステム、ドメイン以外に存在する場合がある。この場合、それらの収集と精査を行うためには、ISP や裁判所等の許可・協力が必要となる。これらの機関に許可・協力を求めるためには、多くの事務的処理が必要となる。これにより、攻撃元ホストの特定作業を行う以前の段階においてかなりの時間とコストをかけることとなり、結果的に調査全体の長期化に繋がる。長期化する調査活動では、攻撃元ホストの特定に対する本格的調査を始める以前の段階で、証拠となるデータ記録やシステムログ等が消失、あるいは攻撃者によりログを消去される可能性が存在する。これは「原本性」ということばに表わされる電子文書の証拠能力の問題や、攻撃者が自らの不正行為や違法行為を否定する「否認」の問題と深く関わってくるため重要である。

このように、現状のトレースバック技術やシステムのはらむさまざまな問題点の多く

が、Realtime tracing 技術の開発動機となっていると考えられる。

しかし、Realtime tracing が実現したと仮定したとしても、攻撃者が実際に使用したホストを自動的に特定することは困難であり、ましてや攻撃を故意に実行した人物の特定が自動的に行えるわけではない。少なくとも現段階での Realtime tracing 技術の研究・開発は、これまで手動で行っていた Tracing 作業のうちの一部分を自動化するための試みと言い換えてよいであろう。そのため、Realtime tracing により得られる情報は、攻撃として検知されたパケットがどのルータを経由してたどりついたものであるか、ということが基本となっており、攻撃元ホストの特定を行うというよりは、実質的に、攻撃パケット発信源ホストを特定するといった表現が正確である。そのホストが攻撃パケット発信源であることは確実性を持っているとはいえ、それが実際に攻撃を行った攻撃元ホストであることは保証されないということである。将来的に、例えば、攻撃元ホストが属するネットワークの特定が可能となるかもしれないが、その場合においても、攻撃手法の種類によっては Tracing の結果を保証することは難しいと言える。あくまで、Realtime tracing 技術において目指されているところのものは、リアルタイムという語に象徴されるようにインシデントレスポンスの即時性にあると言える。この迅速な Tracing によって、攻撃パケットがどこから発信され、どの経路をたどってきたかという情報の確実性を高めることにつながることが期待されている。

インシデントレスポンスの即時性ということから、現在の Tracing 技術と Realtime tracing との主な違いは、どの範囲まで作業の自動化が可能であるかという点にあると考えることができる。確かに、現在の Tracing 技術によっても、攻撃パケット発信源を割り出せないというわけではない。しかし、前述のように、現在の Tracing 技術ではその精度と時間に問題がある。

2. Realtime tracing の技術

(1) 攻撃元ホストの隠蔽

Realtime tracing は、自動的にトレースバックを行う技術であると言い換えることが可能である。しかし一般的に、攻撃者は様々な技術を用いて自らの身元が特定されないように不正行為や違法行為を行う。そのため、Realtime tracing 実現のためには、攻撃者による攻撃元の偽装工作に惑わされることなく、確実に攻撃元ホストの特定を行うことが可能な技術が求められるのである。

ここで、Realtime tracing の技術に触れる前に、まずは攻撃者がどのようにして身元を偽装するのかを解説する。

次に挙げるものは、攻撃者が自分の身元を偽るために使用するインターネット上の二

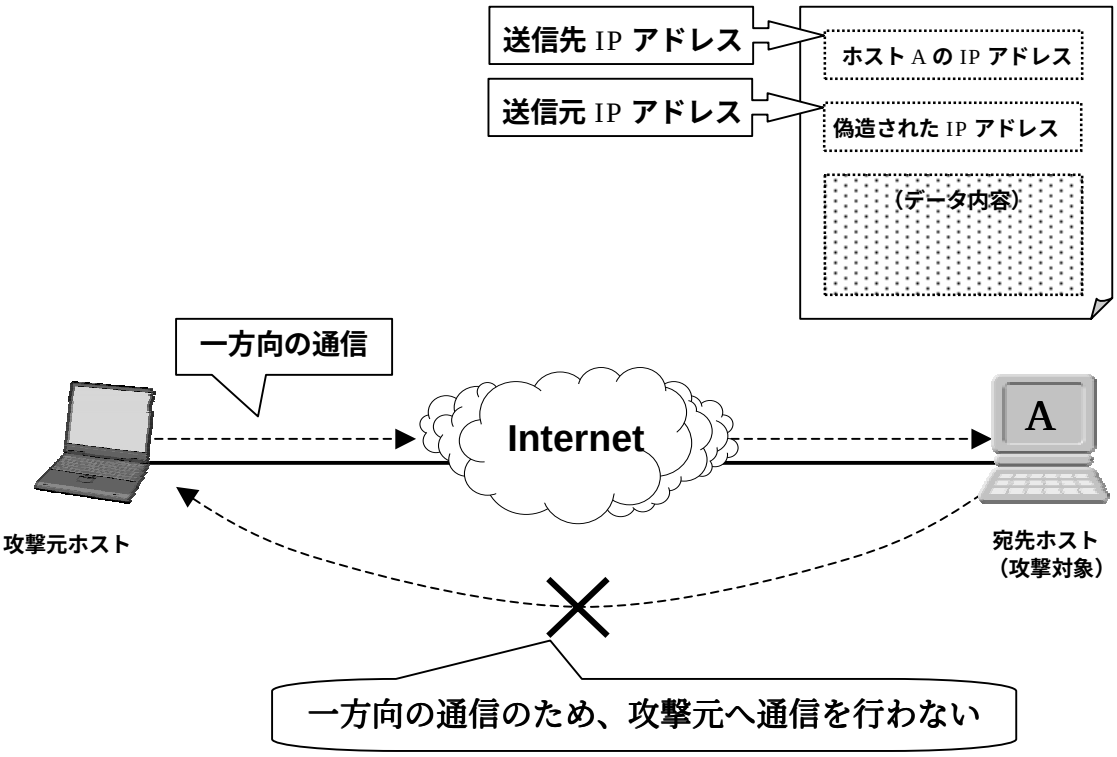
つのコンポーネントである。

[IP アドレス]

二つのコンポーネントのうち、一つ目は IP アドレスである。これは送信者により指定されたコンピュータへ確実にパケットが配送されるためには必要不可欠なものであり、インターネットソフトウェアが使用するネットワーク上の通信を行うための基本ユニットになる。各パケットには二つの IP アドレスが含まれており、それらは、パケットが到達する目的地（送信先 IP アドレス）とパケットの発信源（送信元 IP アドレス）になる。

IP 設計の根底には、「メッセージを送る人物は、必ず正しい返答を要求するはずである」という、ユーザに対する信頼性に依拠するところがある。そのため、パケットやメッセージの処理においては、パケットが目的地に到達するまでの間、特に送信元情報の正当性を確認することなどはなく、送信側から送られた情報のまま変更されることもない。攻撃者はこのことをうまく利用し、パケット送信時に送信元 IP アドレスを他のコンピュータや存在しないコンピュータのアドレスに偽造する。つまり、IP ルーティングは送信先アドレスにのみ依存して行われており、パケット内の送信元 IP アドレスがパケットの実際の送信元であるかどうかは関係なく、その確認もされないため、送信元情報が偽造されたパケットであっても目的地へ届いてしまうことになる。このように、インターネット上の一方向の通信における身元隠しは送信元を偽造することにより簡単に行われてしまう。(図 16 参照)

図 16



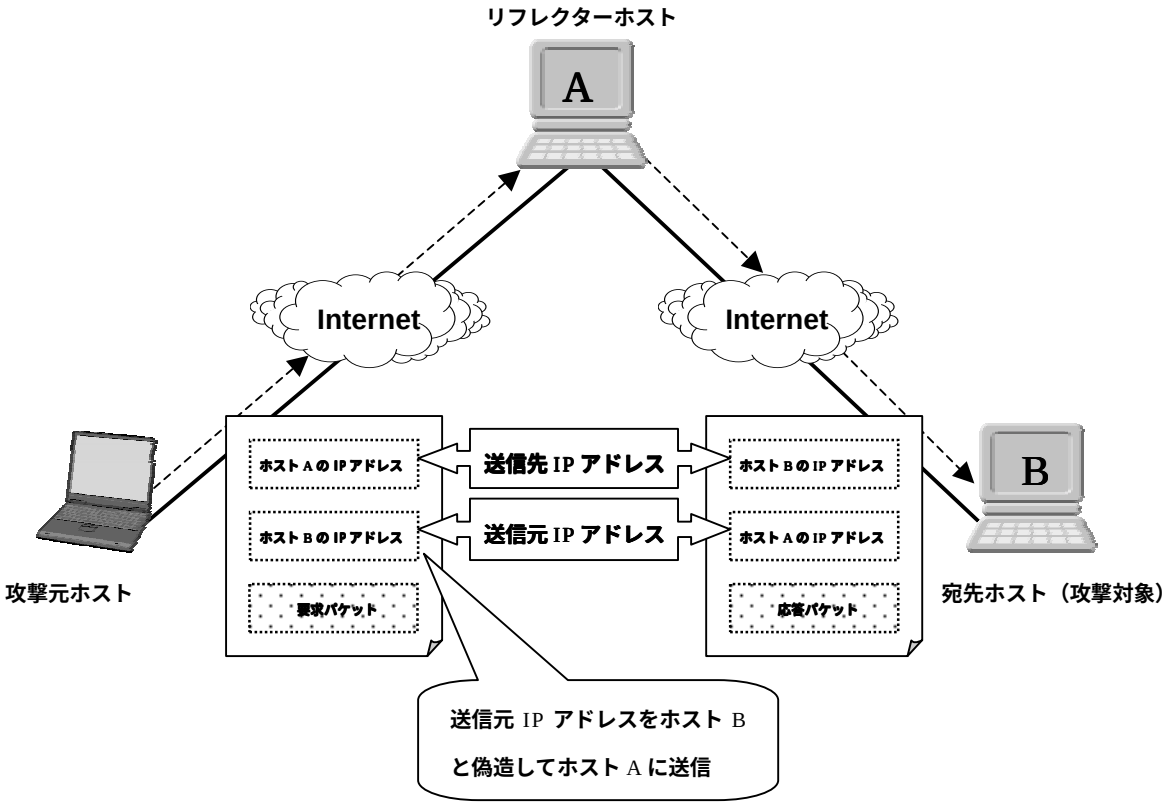
一方向の通信におけるアドレスの偽造は、送信元アドレスフィールドに対して、攻撃者により任意のアドレスを入れるだけの簡単なものである。しかし、双方向の通信の中で送信元を偽造することは、一方向における偽造よりも難しく、より技術を必要とする。理由としては、攻撃対象ホストは攻撃元ホストに対してではなく、偽造された送信元 IP アドレスに対してその応答を返すため、攻撃元ホストはその通信を直接受信することができず、その通信を確認することが原則的に不可能とされているからである。しかし、攻撃対象ホストが偽造送信元 IP アドレスに対して送るパケット内容を攻撃元ホストから確認することができなくとも、環境によっては攻撃者が攻撃対象ホストとの間で双方向の通信を実行することが可能な場合がある。その通信を実現するためには、攻撃者は攻撃対象ホストの応答パケット内にある TCP Sequence 番号[注1]を予測しなければならない。しかし、ある OS の実装では簡単に推測可能な TCP Sequence 番号を使用しているため、TCP Sequence 番号を予測した上で、その番号を含んだパケットを作成し、通信を乗っ取ることが可能となる。また、この攻撃はセッションハイジャック攻撃[注2]と呼ばれる。

[注1] TCP 層の通信において二つのホストが通信を行う際に、通信の信頼性を実現するためにデータのヘッダに付けられる番号のこと。

[注2] 二つのホスト間で行われている通信を第三者が割り込む形で奪う攻撃。具体的な手法としてはいくつかあるが、その一つとして TCP Sequence 番号を傍受あるいは推測することによって行われるものがある。

他にも攻撃者は攻撃対象ホストを攻撃するために、何の関係もない第 3 のホストを巧みに操るように偽造したパケットを作成する。攻撃元ホストはリフレクターホストと呼ばれる第 3 のホストへ応答を返すよう設計されたパケットを送信する。もしこの時に、攻撃者がパケットの送信元 IP アドレスとして攻撃対象ホストの IP アドレスを設定したとすると、図 17 のようにリフレクターホストは純粋にその応答を攻撃対象ホストに対して返すこととなる。つまり、この応答パケットがサービス不能攻撃として利用可能であることが理解できる。攻撃対象ホストにとっては、その攻撃がリフレクターホストから来たように見え、また、リフレクターホストにとっては最初のパケットが攻撃対象ホストから送信されたように見える。一方、攻撃者はその一連の通信には直接的に関わることはなく、その通信を外から傍観するだけである。

図 17



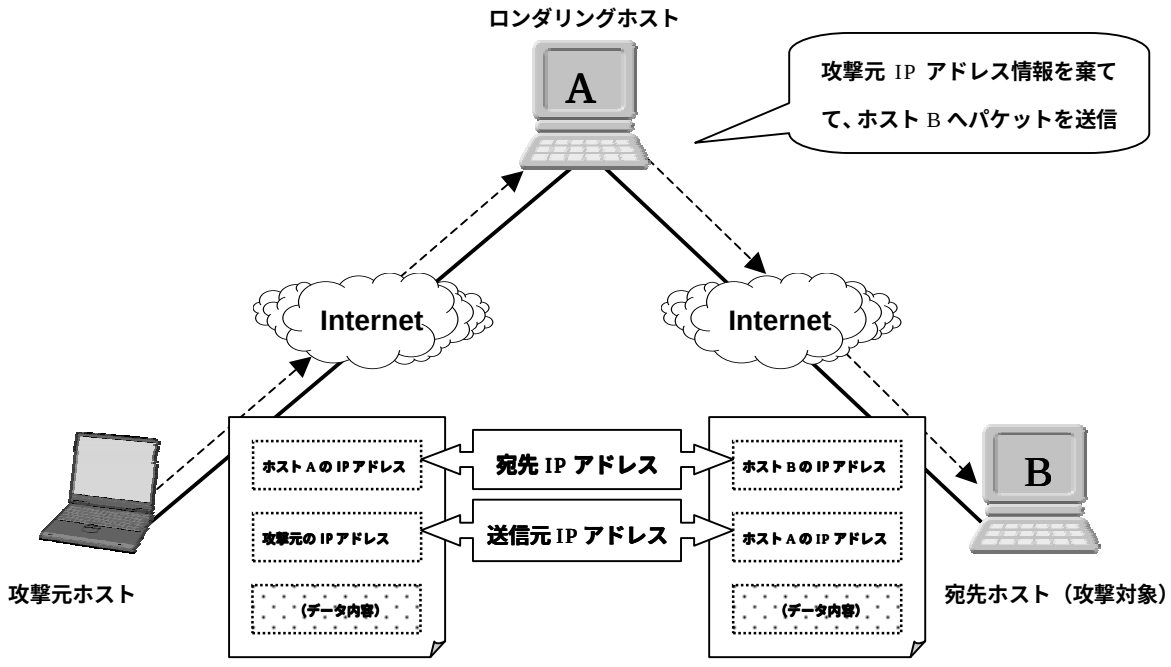
[ユーザアカウント]

二つ目のコンポーネントは、例えば電子メールやリモートアクセスなどで使用されるユーザアカウントである。一般的にアカウントとはユーザのために作成された名前やユ

ーザ ID とパスワードに見られるような認証を行うための符号から構成される。認証はシステムがユーザ ID を使用する人物が本当にそのアカウントに帰属する人物であるかどうかを確認するために行われる。しかし、実はその認証に妨げられることなく、第三者が本来使用権限のないマシンを利用可能にする方法が存在する。例えば、第三者のパスワードとユーザ ID を知ることができれば、不正行為や違法行為を行う間、攻撃者は他人になりすまして、あらゆることを実行することが可能である。また、脆弱性を持つシステムに対して Exploit コードを送り込み、その Exploit が成功した場合、攻撃者は管理者権限を取ることが可能となり、マシン上に新たなアカウントを作成することも可能である。

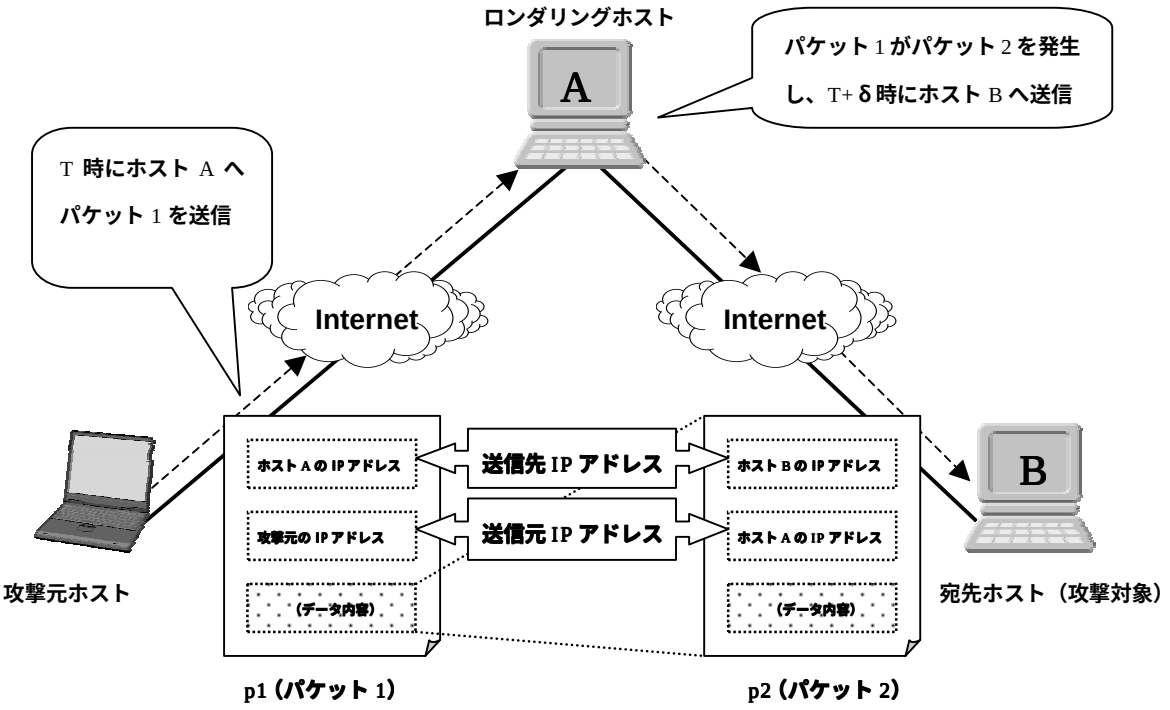
攻撃者はそのように盗んだ他人のアカウントや、攻撃者により新たに作成された本来は存在しないはずのアカウントを使用することで、攻撃対象ホストを攻撃する前に、パケットをロンダリング（Laundering)、すなわち洗浄しようとする。図 18 のように、ロンダリング発生時は、ロンダリングホストが攻撃対象ホストへ他のパケットを伝送するため、攻撃ホストのパケットをまず受け取り、その処理を行う。この処理により、送信元 IP アドレスをロンダリングホストの IP アドレスに変更することが可能になる。

図 18



また、ロンダリングホストを利用する場合、攻撃者が作成したオリジナルパケットのコンテンツやタイミングとは異なるコンテンツやタイミングを攻撃パケットに与えることが可能となる。（図 19 参照）

図 19



攻撃元ホストから、T 時にパケット 1(p1)が発生されるとする。そのパケットは、送信元アドレスに攻撃元ホスト、送信先アドレスにロンダリングホストが指定されている。ロンダリングホストは、p1 を受け取った後、p1 から p2 を発生する。そして、p2 における送信元アドレスは、ロンダリングホストになる。この変更により攻撃元ホストが偽造されることになる。また、攻撃元ホストが初めに送信したパケット内のデータ内容は、完全に別なものに形を変える可能性もある。攻撃者が T 時に攻撃元ホストからロンダリングホストへ送信したパケットは、ロンダリングホストにおいて、T＋δ時に攻撃対象ホストへ送信される。これらの、データ内容の変換や時間的遅延の大きさは、ささいなものである場合もあるし、そうでない場合もある。攻撃元ホストとロンダリングホスト間のコミュニケーション、ロンダリングホストと攻撃対象ホスト間のコミュニケーションは双方向であり、戻りのコミュニケーションが偽造されることはない。

データ内容が変換されることを説明するために、攻撃元ホストがロンダリングホストに Telnet をし、その後攻撃対象ホストに対して ssh のコミュニケーションを行う場合を考えてみる。攻撃者によるコマンドのプロセスは、攻撃者がロンダリングホストに接続している間、ロンダリングホスト上で実行される。そして、攻撃者が実行するコマンドにより、ロンダリングホストが攻撃対象ホストに対して接続を開始しようとする。この段階を考えてみると、ロンダリングホストは、攻撃元ホストから送られたコマンドを、

攻撃対象ホストへ TCP コネクションを接続するための攻撃パケットへ変換していると言える。一度ロンダリングホストと攻撃対象ホスト間にてコネクションが接続すると、攻撃者のパケット内には攻撃対象ホストに対するコマンドをコンテンツとして含ませることができる。ロンダリングホスト自体は、それらのコンテンツを変換する必要はなく、単にそのコンテンツを攻撃対象ホストに受け渡すだけでよい。

攻撃のタイミングは時間的遅延として表れる。時間的遅延は、システム処理の関係上、仕方なく生じる場合と攻撃者の関与を隠蔽するため攻撃者により意図的に生じさせられる場合がある。システム処理により生じる時間的遅延は、攻撃元ホストとロンダリングホスト間の通信とその後のロンダリングホストと攻撃対象ホスト間の通信の間におけるシステム処理の時間差により発生する。一方、攻撃者により意図的に生じさせられる時間的遅延は、例えば、攻撃者が未来のある時刻に実行されるようなスクリプトをロンダリングホスト上に埋め込むことや攻撃パケットの発生を遅らせるようにするプログラムをロンダリングホスト上にインストールすることにより発生する。

なお、攻撃者が使用するロンダリングホストには下記のように二つのタイプがある。

踏み台：

踏み台とは、攻撃元ホストから攻撃対象ホストへの通信を経由させる導管としての役割を果たす、攻撃者により乗っ取られたホストのことを言う。基本的には、攻撃者の通信が踏み台ホストによって変換されたり、遅延されたりすることはない。しかし、踏み台を通過する通信の流れは本質的には変化はしないにしろ、表面上では大きな変化をしている場合がある。例えば、コンテンツが暗号化されたり、通信を断続的に切断し、ランダムな時間的変化を発生させたりする。

具体的には、最初、攻撃者は攻撃元ホストと攻撃対象ホストの間に存在する中間ホストに対してログインを試みる。この中間ホストが「踏み台」と呼ばれるホストになる。この踏み台ホストにログインした攻撃者は、攻撃対象ホストに対して攻撃を開始する。その結果、どんなトレースバックも本来の攻撃元ホストを特定することは出来ずに、踏み台上に存在するユーザや、本来存在するはずもないユーザをトレースバックすることになる。

なお、攻撃者は典型的に複数の踏み台ホストを経由した古典的なペネトレーション攻撃を実行することが多い。

ゾンビ：

もう 1 つのタイプのロンダリングホストはゾンビと呼ばれるものである。ゾンビホストは、基本的には、攻撃者の通信が攻撃経路をたどる前にその通信を変換したり、遅延したりするために使用されるロンダリングホストである。

例えば、攻撃者は攻撃者からの接触後、数分、数日、数週間後に実行するように設定したトロイの木馬をゾンビホストにインストールする。そうすることで、攻撃者の使用する端末からの通信が、ゾンビホストから発生する通信と連続することはなくなり、時間的遅延と通信の変換を発生させることで攻撃者の特定を困難にさせる。また、あらかじめ複数のパケットを攻撃対象ホストに送るような攻撃スクリプトをゾンビホストに埋め込み、それらスクリプトを実行するための引き金として、攻撃者の使用する端末から単一のコマンド入力を含んだパケットを送信するようなこともある。このような分散型サービス不能攻撃(DDoS 攻撃)を行う場合には、一般的に多数のゾンビホストが使用されていることが多い。

このように、攻撃者は様々な方法を用いて、攻撃元ホストの隠蔽を図る。そのため、これらの隠蔽に対応可能である技術、すなわち、攻撃パケットの送信元 IP アドレスが偽造されていようと、ロンダリングホストが攻撃に使用されていようと、攻撃元ホストを確実にトレースバックできるような技術でなければ、Realtime tracing の実現は不可能であると言える。

(2) トレースバックの 3 要素

トレースバックの結果は次の 3 つのパラメータ、精度(precision)・正確性(accuracy)・適時性(timeliness)、により評価することが可能である。

精度はトレースバックの結果により特定される攻撃元ホストの範囲の基準となる。トレースバックにより特定される攻撃発信源は、唯一のホストとして明示される場合もあれば、数多くのホストがまとまる一つのグループとして明示される場合もある。グループとして明示される場合には、最終的な攻撃発信源として具体的なホストが示されることはなく、「特定の LAN 内に存在するホスト」や「特定の ISP 経由で接続されたホスト」、また、単に「ある特定の国に存在するホスト」として抽象的に示されることになる。また、あるトレースバック方法では、トレースバックにより導かれた手がかりと一致すること以外何ら固有の共通点を持たないホストのグループが攻撃元として特定されてしまうことや、トレースバック結果が環境に依存するため、トレースバックを行うたびに示される攻撃元ホストの範囲が異なるということもある。このように、トレースバック方法の違いにより、結果として表れる攻撃元ホストの範囲は大きく異なるため、精度とい

うパラメータを用いてトレースバックの性能を判断することが可能である。

正確性はトレースバック結果の信頼性の基準となる。つまり、トレースバックの結果として示される攻撃元がどれほど実際の攻撃元と近いかを意味する。あるトレースバック方法では、攻撃元として可能性があるホストは一つではないにも関わらず、たった一つのホストを特定してしまう。もし、トレースバックにより特定される攻撃元に誤りがあるようならば、攻撃元特定の正答率をもトレースバックと同時に算出する必要が生じることになるであろう。精度と正確性を用いることにより、トレースバックにおいてもっとも重要な機能とも言える、攻撃経路をどの程度まで正確にさかのぼることが可能であるかということを判断することができる。

適時性は、いつトレースバック結果を保持できるのかという基準となる。トレースバック方法によっては、攻撃最中にしかトレースバック結果を得られなかったり、攻撃後にしか入手することができないデータをトレースバックに必要とするため、攻撃後にしかトレースバック結果を得られなかったりと、結果を得られるまでの時間は様々である。また、ある方法では限定された存続期間を持つデータをトレースバックに必要とするため、結果がそれらデータの存在に依存することもある。つまり、適時性はトレースバックにより扱うデータの種類と取得時期により大きく影響を受けることになる。

トレースバックの基準としてこれら 3 つの要素が挙げられるわけだが、トレースバックを行う目的により、必要とされるパラメータは変化する。トレースバックを行う目的としては、攻撃対応・未来の攻撃に対する防御・責任追及などが挙げられる。

攻撃対応においては、進行中の攻撃を止めなければならないため、トレースバックには、リアルタイム性と高い正確性が必要とされる。当然のことのように、攻撃元特定の正確性がいかに効果的な対応を可能にするかということを決定することになる。もし攻撃元を正確に把握することができないならば、攻撃元に対して行う対策がその攻撃を止めることはありえない。しかし、攻撃を停止することに高い精度が要求されない場合もありうるであろう。例えば、もしルータや LAN、ドメイン上における特定インプットポートに対する進行中の攻撃を検知できたならば、攻撃効力を緩和するため、アクセス制御を行うことが可能である。もちろんトレースバックの精度や後のフィルタリング項目が、攻撃対応の効果を大きく左右することになる。

未来の攻撃に対する防御においては、次の攻撃をうける前に確実な防御策を立てられるのであれば、リアルタイム性は必要なく、相対的に高い精度が要求される。限られた時間内であれば、かなり大きなインターネットセグメントからのトラフィックをフィルタリングすることは受け入れられることもありうるが、当然そのようなアプローチは長期間受け入れられるものではない。しかし、もしトレースバックが高い精度で攻撃元を特定できるのであれば、より選択されたフィルタリングはもとより、攻撃者の特定が早まり、結果として攻撃を未然に防ぐことが可能になるかもしれない。例えば前述のようにはいかなくとも、ある一つの管理下にあるネットワークが発信源となっている攻撃を

トレースバックにより特定することができるならば、その情報に基づいて、その発信源のネットワークのシステム管理者に対して協力を申し入れ、攻撃元ホストの特定と攻撃の未然防止を行うことが可能になるであろう。

責任追求のためには、トレースバックによって得られた結果の証拠能力が重要であり、そのためには高い水準の適時性が求められる。この場合に関しては、高い精度は要求されない場合が多い。実際、責任追及のためには、トレースバックにより大企業のイントラネットや大規模な ISP などが特定できさえすれば十分であるとも言われている。

このようにトレースバックの目的とトレースバックの特徴を考察していくと Realtime tracing の実現に必要な要素が明らかになってくる。すなわち、精度・正確性・適時性すべてを持ち合わせたトレースバックでなければ、Realtime tracing を実現することはできないことは明白である。

(3) 自動トレースバックの種類

現状、Realtime tracing という名のもとに、新たな技術が研究されているわけではない。以下に紹介する技術は、一般的には自動トレースバックと呼ばれ、現在のトレース技術では解決や対応が困難とされている、偽造された IP アドレスを持つパケットに対する真の送信元を特定するため、また、踏み台ホストやゾンビホストを利用した DoS 攻撃の発信源を特定するために研究されているものである。しかし、これら自動トレースバックは人手を介した Tracing から飛躍的に向上した研究成果であり、今後の Realtime tracing システムを開発する上で必要不可欠なものであると同時に、確実にそのシステムの土台になるものであると言える。

これらの技術は、トレースバックを実行するタイミングによりプロアクティブトレーシング（Proactive tracing）とリアクティブトレーシング（Reactive tracing）と呼ばれる二つのタイプに分類される。

「プロアクティブトレーシング（Proactive tracing）」

プロアクティブトレーシングは、パケットが配送されている最中、同時にそのパケットに関わる Tracing 情報を収集しておくものである。万が一、あるパケットに対する Tracing を行う必要が生じた場合、攻撃対象ホストは予め収集されていた情報の中から Tracing 対象となるパケットの情報を検索・参照し、パケットの真の送信元を特定することとなる。つまり、攻撃があろうがなかろうが、常に Tracing のための準備を行っておくものになる。

「リアクティブトレーシング（Reactive tracing）」

リアクティブトレーシングは、攻撃検知後、Tracing を開始するものである。また、リアクティブトレーシングの多くは、パケットの真の送信元を特定するため、標的ホストからパケット発信源に向け、その攻撃経路をさかのぼっていく方法をとるものである。この Tracing を実現するためには、効果的なトレースバックアルゴリズムとパケットマッチング技術を開発しなければならず、様々な技術を用いてこの問題解決が試みられ、同時に多くの技術案が提案されている。

トレースバックは、その実行タイミングによる分類方法の他に、識別対象により以下のように分類することもできる。

≪パケット送信元の識別≫

受信したパケット（送信元 IP アドレスが偽造されている場合もありうる）における送信元ホストの特定は、ネットワークのスイッチ構造を通り、パケットの経路をさかのぼることにより実現可能であると言える。また、論理的には、宛先ホストに到達するまでにパケットが通過したルーティング機器を知ることができれば、パケット経路を把握することは可能である。例えば、世界中のルーティング機器を次のような機能を持つルーティング機器にリプレースすることは可能であるだろうか。

「隣接するホストからのパケット受信時に、受信パケット内部に存在するあるリストに各固有のルータ ID を入力していき、パケットがルーティング機器を通過する毎に、リスト上にルータ ID を追加していくような機能を持つルーティング機器。」

このような仕様のルーティング機器であれば、ホストは完全な経路を内部に含んだパケットを受け取ることが可能になる。

しかし、現実的な実現性を考えると、このようなルーティング機器を世界規模で導入するためには、ルーティングオーバーヘッドに加え、すべてのルーティングデバイス、ネットワークプロトコル、パケットの最小サイズ等の変更が必要とされる。つまり、実装上の問題として、実現不可能であることが分かる。そのため、現在のトレースバックにおける研究は、これら実装上の問題をどのように解決するかということに焦点が当てられている。各研究者らは次に挙げるような 3 つの異なるアプローチを展開している。

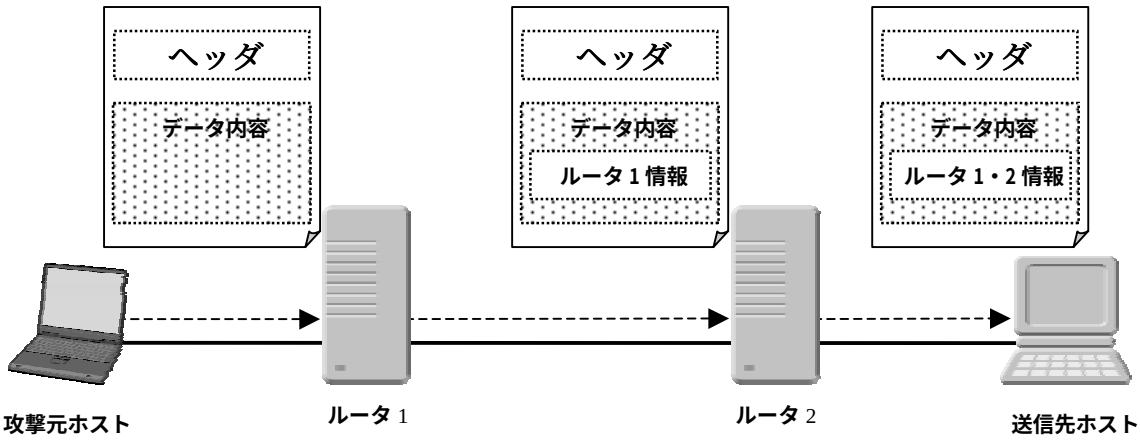
【OVERLOADING タイプ】

このタイプのアプローチは、Packet marking とも呼ばれ IP パケットヘッダ内のオプションフィールドや識別子フィールドと呼ばれる部分にルート識別要素を付加させるものである。このルート識別要素を分析することにより、パケット受信者はパケットが通過してきたルータ情報を得ることができるため、結果的にパケット発信源までの経路を

たどり、攻撃元ホストを特定することが可能になる。（図 20 参照）ただし、この技術を利用するためには、ルータが本来の役割であるパケット配送のための処理を低下させることなく、通過するパケットに対して、自らのルータ情報を付加させることが可能でなくてはならない。また、この方法では、ルータ情報を含むためのフィールドの大きさ(ビット数)に制限があるため、そのフィールド範囲内に大量のデバイスを通過して形成される固有ルートを符号化して入力する必要がある。さらに、その符号化は偽造不可能な安全な形で行われなければならない。制限されたフィールド内に入力可能な情報数には限界があるという問題に関しては、各ルータがほんの数台のルータとしか接続されていないという条件下であれば、問題は解決可能な範疇にある。仮に完全な固有ルートを特定することができなくとも、可能性があるパケット経路数はこのアプローチを用いることによりかなり切り詰められることになる。

Dawn Song 氏と Adrian Perring 氏により行われた研究では、ルーティング機器の IP アドレスを基にして作成された識別コードをパケット内部の IP 識別子フィールドに入力させる方法がとられた。また、この方法とあらかじめ作成された上流ルーティング機器の IP アドレスマップを用いることにより、パケットを受信したホストは効率良く、かつ高い精度で 32 デバイスまでの間であれば、パケット経路を再構築することが可能であることが報告された。

図 20



【TRACEPACKET タイプ】

このタイプのアプローチは、各パケットに対して、その送信元を特定するための補助的な役割を果たす追跡パケットを発信するルーティング機器を必要とする。送信先ホストでは、通常のパケット、及びそのパケットと関連性のある追跡パケットをすべて収集

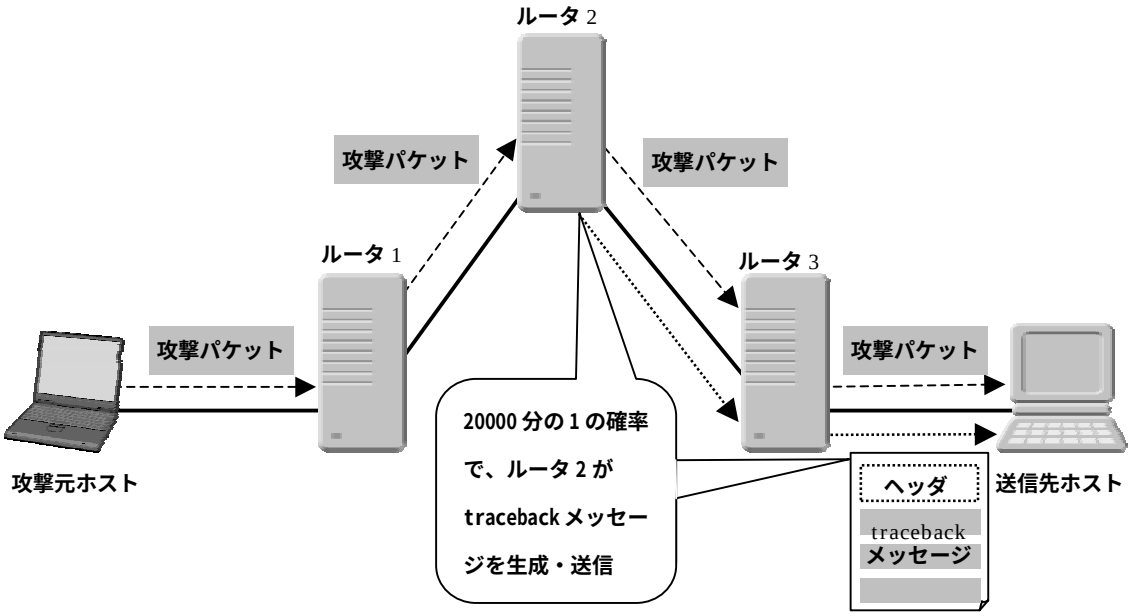
し、パケット経路を導き出すためにそれら追跡パケットの再構築と分析を行う。この方法の長所は、追跡パケットの発信元ルータを間違いなく識別できるような ID をその追跡パケット内に含ませることが可能になることである。明らかな欠点としては、もし全てのパケットに対して送信元を特定しようとする場合、追跡パケットの生成数も増加するため、ネットワークトラフィックの著しい増加が生じることが挙げられる。

このようなタイプの Tracing 技術は Messaging とも言われており、Steve Bellovin 氏を筆頭に IETF（the Internet Engineering Task Force）[注]により提案された ICMP Traceback Messaging（iTrace）という方法が有名である。この方法では、ICMP を利用することで、ルータがパケット配送時に通過するルーティング機器情報を含めたメッセージの作成と送信を行うことを実現している。（図 21 参照）ルータは IP パケットの通過場所の情報を含んだ ICMP トレースバックメッセージを作成し、パケットの送信先ホストへ向けてそのメッセージを送信する。つまり、結果的に送信先ホストはパケット本体と ICMP トレースバックメッセージを受け取ることになる。パケット経路の調査は、パケットの送信元 IP アドレスの確認とそのパケットに関連付けされた ICMP トレースバックメッセージを参照することにより行われる。なお、トラフィックの増加を最小限にするために、各ルータには ICMP トレースバックメッセージを 20000 分の 1 の確率で作成・送信するように、その機能を実装させている。そのため単一パケットを使用した攻撃においては、そのパケット経路を判断することは困難になる可能性が考えられる。しかし、攻撃者により大量のパケットが送信される Flood 系の攻撃[注]に対しては、攻撃対象ネットワークは攻撃経路を特定するに十分な ICMP トレースバックメッセージを収集することが可能になるため、その送信元をトレースすることが可能になる。

注 TCP/IP などのインターネットの標準を定める国際的な公開された団体。IETF が正式に発行する文書は RFC（Requests For Comment）として知られる。

注 DOS 攻撃の一種であり、TCP 層のコネクション確立の手順を利用する攻撃。代表的なものとして、SYN Flooding がある。

図 21



【QUERY タイプ】

このタイプのアプローチは、パケットを受信したホストが接続されたルーティング機器に対して即座に「このパケットが通過したか？」という質問内容を含むパケットを送信することにより実現される。また、ホストからの質問を受けたすべてのルーティング機器はこの質問に対して積極的な応答を行い、隣接するすべての上流ルータに対してもこの質問を繰り返し行っていく。その結果、ルーティング機器からの肯定的・否定的応答の結果がそのままパケット経路の特定につながることになる。この技術の使用もまた、ネットワークトラフィックを増加させる可能性はあるが、疑わしいパケットのみを追跡するのであれば、帯域のオーバーヘッドはある程度の範囲で抑えることは可能であると考えられている。

しかし、この方法を利用するためには他にも考慮しなければならない問題が存在する。ルーティング機器がホストからの質問に応答できるためには、通過する全てのパケット情報をある一定期間蓄積することが絶対条件となるが、使用するルーティング機器自体のデータ処理能力やメモリの限界を考慮すると、リアルタイムに近い状態でトレースバックを実現するためには、パケット情報を蓄積する期間をかなり短期間に設定せざるを得ない。また、異なるタイプのルーティング機器においても互換性をもつような質問応

答のためのプロトコルの存在が、このタイプのアプローチには必要と考えられている。

このようなプロトコルとしては Intrusion Detection and Isolation Protocol（IDIP）というものが、DARPA（Defence Advanced Research Projects Agency）[注]の支援により、Network Associates・Boeing Phantom Works・the Univ. of California at Davis・SiliconDefense の共同作業により開発はされているが、このような新規プロトコルの導入はそう簡単に行えるものではない。そこで、新規プロトコルを導入しなくても Query タイプのトレースバックを可能にするような技術案もいくつか提案されている。

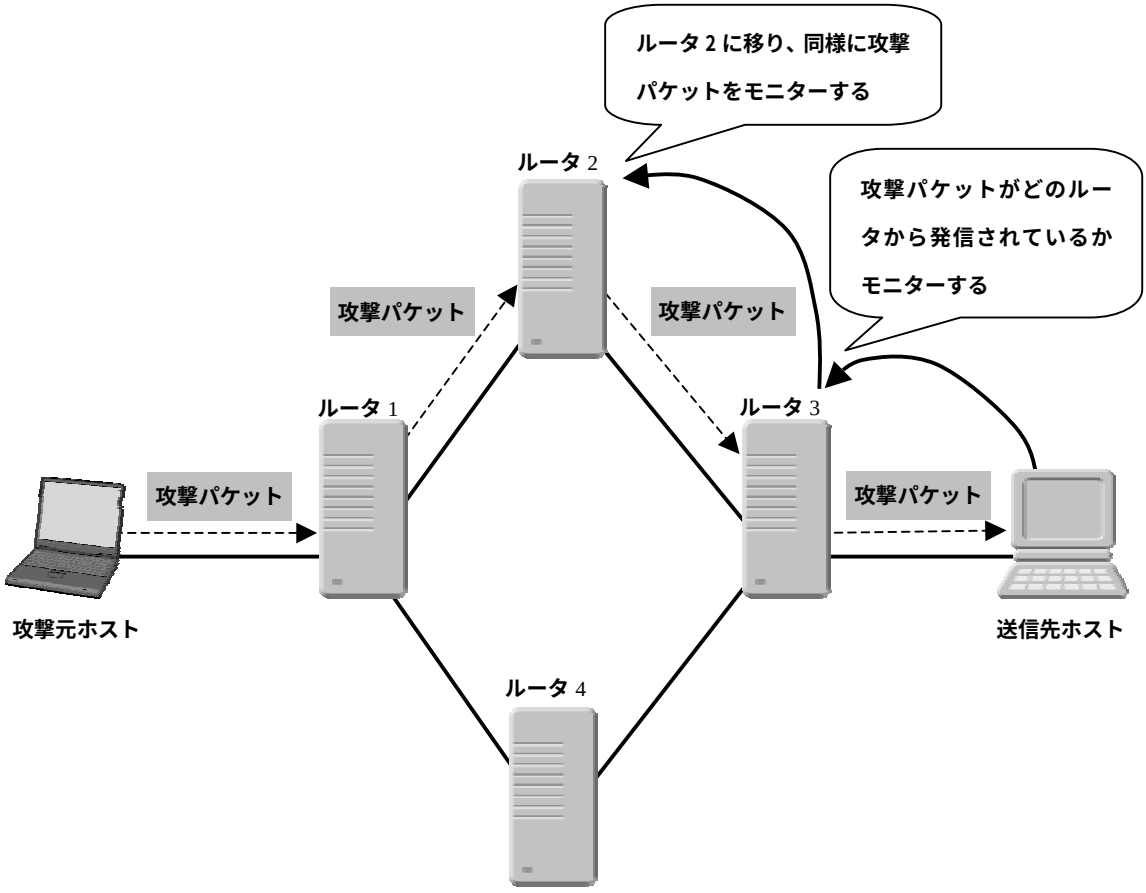
[Hop-by-Hop Tracing]

Hop-by-Hop Tracing と呼ばれる技術では、合併以前の MCI 社（米国）の DoSTracker のように、まず始めに、トレーシングプログラムが攻撃されているホストの一番近くに存在するルータにログインを行う。そこでは、送信元を特定しなければならない対象のパケットがモニターされ、ログインしたルータの上流に存在するどのルータからやって来るものなのかを特定する作業が行われる。そして、プログラムにより上流のルータが特定されると、次はそのパケットが送られて来るさらに上流のルータにログインし、パケットのモニターと上流ルータの特定を行う。この手順は、プログラムが攻撃の真の発信源を特定するまで、上流のルータに対して再帰的に繰り返される。（図 22 参照）

Hop-by-Hop Tracing では、ホップ数が多ければ多いほど、トレーシングを行うプロセス数が増加する傾向にある。その結果、トレースには時間がかかり、必要なトレース情報がトレース過程で消失してしまう可能性も出てくる。この欠点を克服するべく、Hop-by-Hop Tracing with overlay network と呼ばれる技術も提案されている。この技術を基にしたある方法では、エッジルータと特別に用意されたトラッキング専用ルータ間において IP トンネルを形成し、オーバーレイネットワークを構築する。そして、トンネル経由で IP パケットをトラッキングルータに配送することで、Hop-by-Hop Tracing を IP トンネルというオーバーレイネットワーク上で実行させる。これにより、トレースバックに必要となるホップ数（ルータ数）を減少させている。

[注]インターネット の生い立ちに深く関わった米国防総省高等研究局の略称。

図 22

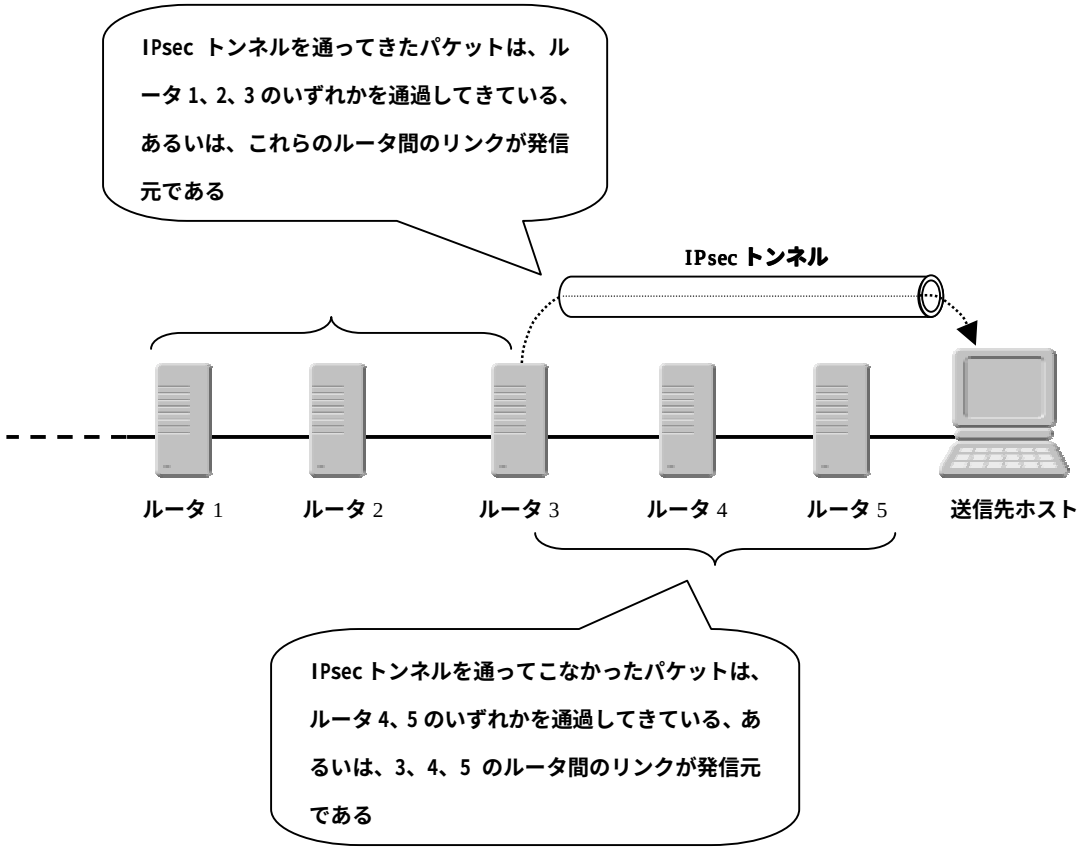


[IPsec authentication]

IPsec authentication と呼ばれる技術は、既存の IP セキュリティプロトコルに基づいた方法である。この方法では、IDS が攻撃を検知すると、Internet Key Exchange（IKE）プロトコルが IPsec セキュリティアソシエーション（SA）を攻撃対象ホストと管理ドメイン内にある数個のルータ（例えば、自律システム境界ルータ<autonomous system boundary router>）間に確立する。SA 終点のルータは、通過するパケットに対して、IPsec ヘッダとルータの IP アドレスを含むトンネル IP ヘッダを付加する。もし、攻撃が継続され、確立された SA において続いて起こる攻撃が確証されると、攻撃は対応するルータ（終点の SA）を越えたネットワークから発生していることになる。パケット受信者は攻撃パケットがどのルータを通過したかを調査するためにトンネル IP ヘッダの送信元 IP アドレスのチェックを行う。また、このプロセスは再帰的に繰り返されるため、パケット受信者は最終的に攻撃発信源を特定することになる。（図 23 参照）

この技術は、既存 IPsec と IKE プロトコルを使用するため、管理ドメイン内に対してトレースバックのための新しいプロトコルを導入する必要はない。しかし、管理ドメインを越えたトレースには、特別な協力のためのプロトコルが必要となる。なお、IETF 侵入検知ワーキンググループ(IDWG)では、そのようなプロトコルに関して議論がなされている。

図 23



前述にもあるように、パケットの送信元を識別するためには、ルーティング機器がトレースバック行為に対して補助的な役割を果たすことが必要となる。

しかし、すべてのルーティング機器が連携を取ることがトレースバックの成果をあげるために絶対的に必要であるかと言えば、必ずしもそうであるとは断言できない。そのような理由からも、トレースバックの研究者達の間では、トレースバック成功のために要求されるルーティング機器の補助的役割を果たすためのレベル、そのレベルによるトレースバック結果の正確性と精度の違い、またトレースバック方法やトレースバックアルゴリズムの違いが要求されている補助的役割を果たすためのレベルに与える影響はどのようなものであるのか、などが今後の研究課題とされている。

≪パケットストリームの識別≫

踏み台ホストやゾンビホストのようなロンダリングホストがパケットストリーム攻撃の攻撃元ホストとして判断されると、トレースバックでは「標的ホストに届くパケットストリームをどのホストが引き起こしたのか」という次の問題に直面する。そして、その問題を解決することが、真の攻撃元ホストの特定につながるのである。

踏み台ホストを使用した攻撃とゾンビホストを使用した攻撃を比較すると、踏み台ホストを使用した攻撃の方が攻撃元ホストを特定しやすいと言われている。その理由は、踏み台ホストは攻撃パケットの本質を変更してしまうホストではなく、単に攻撃元ホストから標的ホストへの通信を中継するための導管としての役割を担うだけであるため、すぐに踏み台ホストを経由する攻撃パケットを標的ホストが受け取ることが可能であるからである。そのため、踏み台ホストに出入りする二つの通信の流れを比較対照することにより、上流ホストを特定することが可能になる。つまり、踏み台ホスト越しの自動トレースバックとは、ネットワーク上の異なる場所で見られる二つのパケットストリームが本来同一のストリームであるかどうかを判断することであると言える。

一方、ゾンビホストの場合は攻撃元ホストとの因果関係を考えると、攻撃を導く真の攻撃元ホストの特定が容易でないことが理解できる。具体的には、攻撃を導く攻撃元ホストからゾンビホストへの通信内容が、実際の攻撃となるゾンビホストから標的ホストへの通信内容と類似性を持たず、発生時間の関連性も発見しづらいものであることが攻撃元ホストの特定において問題になる。そのため、攻撃の引き金となる通信と攻撃となる通信を自動トレースバックにより比較対照することは難しく、真の攻撃元ホストを特定するためには、ゾンビホスト上のアクセスログやプロセスなどを調査する必要が生じることになる。

これらパケットストリームを使用した攻撃の発信源を特定するためには、ストリームマッチングと呼ばれる技術が効果的であるとされている。この技術は比較対照を行う対象物の違いによりパケットコンテンツとインターパケットタイミングと呼ばれるタイプに分類することが可能である。また、パケットストリームの特徴を読み取る場所としては、ホストベース（各ホストが自身の入力と出力パケットストリームをマッチング）とネットワークベース（ネットワークトラフィックをスニッフィングすることによりパケットストリームをマッチング）といったような二つの選択肢が考えられる。

【Content Matching タイプ】

Content Matching タイプの Tracing 方法は、1990 年代半ば、カリフォルニア大学デービス校に在籍中の Stuart Staniford-Chen 氏 により開発された。サムプリンティング（Thumbprinting）と呼ばれるこの方法は、パケットストリームを離散的時間間隔に分け、間隔毎にパケットストリームのダイジェスト(hash)を作成し、それらダイジェストの

類似性をもとめることにより、二つのストリームを比較するものである。

この方法を研究中に Staniford-Chen 氏は、異なる 2 つのパケットストリームを比較した時よりも同様なパケットストリームを比較した時に、ダイジェストにより多くの類似性が見られることを発見した。つまり、ネットワーク上の異なる 2 地点で作成されたダイジェストに類似性が見られるならば、ダイジェストの作成元となったパケットストリームは同一のものである可能性があり、その 2 地点を同じパケットストリームが通過している可能性が考えられるのである。そこで、このダイジェストの比較を広範囲に行うことが可能であれば、パケットストリームの発生個所をも特定することが可能ではないかと言われている。しかし、この方法は、非暗号化のパケットストリームに対するトレースバックではかなりの効果が見込めるものの、暗号化されたパケットストリームに対しては有効的な方法ではないという欠点が存在する。

【Interpacket-timing matching タイプ】

Purdue 大学で進行中の研究において、ストリームの比較対照を行うにあたり、Interpacket-timing を使用することがいくつかの成果を収めている。ランダムなネットワーク遅延が存在するにも関わらず、ネットワークプロトコルの特徴と人間とコンピュータの相互関連がタイミングサムプリント（timing thumbprint）を生成する。このタイミングサムプリントを比較することによりストリームの同一性を確認するわけであるが、比較にあたりネットワークの輻輳が少なからず影響を与える可能性がある。しかし、ネットワーク内の異なる 2 地点で観測された同一パケットストリームのタイミングサムプリントを比較すると、関連性のないパケットストリームのタイミングサムプリントを比較した時よりも類似性を持つことが確認された。もちろん、タイミング（時間）は暗号化による影響を受けないため、この方法は、Content Matching よりも高い効果が期待できる。

他の研究者もまた、Interpacket-timing matching を使用する別のストリームマッチングの方法を提案している。この方法では、ネットワーク上のある地点でパケットストリームのタイミングを積極的に変化させ、別の地点でパケットストリームのタイミング変化率の比較を行う。しかし、この方法を採用しようとする場合、パケットストリームがタイミングの変化を受ける管理ドメインの外で発生した場合には法的な問題が生じる可能性も考えられる。

一つのホストに対する入出力のストリームを比較対照するホストベースのシステムには数多くの長所が存在する。ホストにおけるネットワークスタックが自動的に各パケットを結合し、分類するので、パケットの関連付け作業を実行する上で余計に必要となる処理はない。また、ホストに対して入出力されるトラフィックの量は制限されるので、

過度の負担をかけることなく、比較作業のための計算処理が実行可能になる。しかし、問題もある。一般的には考え難い状況ではあるが、ホストベースの強力なトレースバックシステムでは、攻撃経路上のすべてのホストに対してストリーム比較システムの導入と制御が必要となってしまう。

逆にネットワークベースのストリーム比較システムであれば、ネットワーク上にあるすべてのホストに対してネットワークソフトウェアをストリーム比較や制御のために変更するような必要はなく、常に、比較を行うパケットストリームが通過する攻撃経路となるネットワーク上の 2 拠点でスニッフィングをするだけでよい。しかし、ネットワークベースのシステムではホストベースのものよりも多量のネットワークトラフィックを調査しなければならない。また、トラフィックをストリームに分類し、各サムプリントを計算し、異なる地点で観測されたストリームがどれほど類似しているのかを計算する必要もある。そのため、ネットワークベースの方法では、ネットワークトラフィックに計算処理を間に合わせることが困難であるとされている。

もし、ストリームの比較がリアルタイムで実行されないようであるならば、さらに考慮しなければならない問題が生じる。攻撃直後にトレースバックを開始する場合には、ストリームを比較するためのシステムは、数多くのサムプリントや比較を行うストリームの識別子をどこかに蓄積している必要が出てくる。しかし、蓄積の量には制限があることが予想されるため、結果的には、ストリームの比較に要求される適時性に影響を及ぼすことになってしまう。

Packet Marking、Content matching、Interpacket-timing matching など、どのトレースバック技術を使用したとしても、現状では自動的にゾンビホストの上流に存在する真の攻撃元ホストを発見することは困難であるとされている。実際にそのような攻撃元ホストを特定するためには、自動トレースバックに加え、ゾンビホストにアクセスし、攻撃の原因を判断するための調査を行う必要があるからである。具体的には、アウトプットストリームの直接的な原因（トロイの木馬やスクリプトといった）を調査し、ゾンビホスト上のログを精査することにより攻撃発生のトリガ（リモートコマンドやクーロンジョブなど）を発見する作業が必要となる。トリガに関する情報がログ上に発見されると、その情報から真の攻撃元ホストがゾンビホストにアクセスしたであろう、おおよその時間帯を限定することが可能になる。攻撃元ホストは直接的な原因や攻撃発生のトリガに対して何らかの関わり合いがあるため、トリガが作用する以前にゾンビホストに対して少なくとも一つのリモート接続を確立しているはずである。それゆえ、限定された時間帯の間にリモート接続をしていたホストが真の攻撃元ホストである可能性が生じてくる。しかし、調査を行わなければならない時間帯が長いと、攻撃元ホストの可能性が考えられるホスト台数は増え、また、その可能性あるホストに関する情報を含んだログは、ログ保持期間の制限により既に消失していることも考えられるため、特定作業は

困難になることが予想される。これらのことからも分かるように、当面、ゾンビホストが使用された攻撃に対して自動トレースバックを行う際には、その可能性が制限されてしまうことが考えられる。

(4) Realtime tracing の効果

既存の Tracing とは異なり、Realtime tracing が現実のものとなれば、攻撃発信元の特定を正確に、そしてリアルタイムに行うことが可能になる。前項では、Realtime tracing 実現に希望を与える数種類の技術について言及した。それら技術は研究環境でのみその成果を示しているものであり、現実のネットワークにおいても使用、実装可能な技術でであるかは今だ開発途中の技術であるがために疑問が残るところである。また、Realtime tracing の実現に至っては、技術以外にも様々な問題、障害が存在すると言われている。しかし、仮にそれら全てを解決したとし、広大なインターネット上で Realtime tracing が現実のものとなるならば、以下のような効果が期待される。

(a). 偽造 IP アドレスを持つパケットを使用した攻撃や DoS 攻撃の発信源の特定が可能

既存の Tracing に使用される技術では、偽造された送信元 IP アドレスを持つ攻撃パケットや DoS 攻撃における真の攻撃パケット発信源を特定することは困難である。しかし、Realtime tracing では、前項で挙げた技術を用いることでその発信源の特定が可能になる。また、DDoS 攻撃においては現在の技術研究では正確にその発信源を特定することが困難であるが、今後 DDoS 攻撃に対する Tracing 技術がさらなる進歩を遂げていくと、Realtime tracing の効果の一つとして、DDoS 攻撃の発信源をも正確に特定することが可能になることが予想される。

(b). Tracing 作業の効率化

既存の Tracing 技術を用いた発信源特定作業においては、その作業すべてを自動プロセスにて行うことは不可能である。そのため、必然的に人間による手動プロセスの介入が必要となるが、現在の Tracing 作業では手動プロセスを要する部分も多く存在するのが現状である。しかし、Realtime tracing 技術を用いることにより、現在の Tracing 作業において、通常人間による手動プロセスが用いられる作業の一部分を自動化することが可能となる。Tracing 作業が自動化に近づけば、作業における人的負荷も軽減され、それに伴い、Tracing 作業におけるコストは格段に低下することが予想される。

(c). 攻撃パケット発信源の早期発見

Tracing 作業が自動化されることにより、攻撃パケット発信源の特定がリアルタイムで行うことが可能になる。実際は、ネットワークのある場所で攻撃が行われていることを IDS により判断されることが Tracing 作業のトリガになると考えられるため、攻撃と同時にその発信源を特定するとは言えないかもしれない。しかし、Tracing 作業のためには人間による手動プロセスが余儀なくされ、場合によっては Tracing に必要となる情報も時間の経過と共に消失してしまい、その結果発信源を特定することも不可能になる可能性が高い現在の状況を考えると、リアルタイムに近い形で発信源を特定することが可能になるのは間違いない。

(d). 早期対策

ここで言う早期対策とは、今進行中の攻撃に対する直接的な対策のことではない。直接的な対策であれば、Firewall や IDS のような既存の技術、標的となっているサーバに対する設定変更やパッチあて等の作業において十分対処可能である。

Realtime tracing では、攻撃パケット発信源の特定を行うため、そのパケットを受信した地点から攻撃パケットの経路をさかのぼるようにして発信源の特定を行う。つまり攻撃パケット発信源の特定と共に、攻撃経路も特定することが可能なのである。これは、自ネットワークを含む管理ドメインに攻撃パケットが届く以前に対策が可能であることを示している。例えば、パケットの発信源に近い経路途中の ISP が特定できたのならば、その ISP に対して何らかの対応を要求することが可能である。また、パケットの発信源が踏み台ホストからのものであると分かれば、そのホストの管理者に対して至急の対応を求めることも可能である。

さらに言うと、攻撃パケット発信源の特定が可能であれば、攻撃者の特定も早くなることは言うまでもない。もちろん簡単に攻撃者を特定できることは少ないが、既存の Tracing 技術を用いるよりも攻撃者特定までの早さとその確立は高くなるものと予想される。

(5) Realtime tracing の利用状況

トレースバックが抱える問題はいくつかの独立した部分を持つため、完全な解決方法となると、個々の問題を解決するための手法を統合する必要があり、また、必要時には各問題を解決するに相応しいツールの使用が常時可能である基盤設備（インフラストラクチャ）を形成する必要がある。これは、単に異なるトレースバック機能を実装したツールを開発すればよいのではなく、ツールが実装するトレースバック機能にはすべての時間枠（攻撃最中や攻撃後など）においてその機能を果たすことが考慮されている必要

があり、ツールの実行がいつでも可能である環境でもなくてはならない。しかし、現状、そのようなツールの存在や利用の報告はなく、完全なトレースバックが実施可能である基盤設備は存在していない。また、当面の間、トレースバックの実行面、特に管理障害や自動プロセスでは入手不可能な情報に対する面においては、絶対的な人間による補助的な手動プロセスを必要とするため、完全なトレースバックツールの誕生は今のところ期待できないのが現状と言える。

現在のトレースバックにおける状況や完全なトレースバックツールの誕生が期待できない今、Realtime tracing の実現が待たれるところであるが、その Realtime tracing 自体もまた研究段階の技術であるため、Realtime tracing においてもその利用報告は無い状況である。しかしながら、研究段階の Realtime tracing の中でも、より実現性の高いものは存在する。

技術的な統合の可能性を考えた場合、前述にもある IDIP がより実現性が高いと考えられる。IDIP アーキテクチャでは、疑わしいトラフィックを追跡するために質問応答プロトコルを実装するためネットワーク上の IDIP 使用可能な機器－侵入検知システムや Firewall など－を使用する。DARPA の Common Intrusion Detection Framework（CDIF）言語をこれら本質的に異なる機器間での通信の際に使用する。経路要求自体はその返答により制御されているが（肯定的な返答は経路要求の転送を行い、否定的な返答は経路要求の転送は行わない)、すべての報告は、Central Detection Coordinator と呼ばれる機器により受信される。もし、ホスト to ホストではないならば、この機器は幅広い見解を総合的に扱うために、複数の管理ドメインを経由するトレースバックを許可し情報の関連付けを行う。新たなトレースバックツールには、そのようなより強力なトレースバックとすばらしい分析力を考慮するためのアーキテクチャが組み込まれると考えられる。

また、IETF の ICMP Traceback Working Group では、第三章.2.(3)の「TRACEPACKET タイプ」で述べたように、ICMP の新たなメッセージとして traceback メッセージを定義し、そのメッセージ内にパケットが通過してきたルータなどの IP アドレスや MAC アドレスなどの経路情報をおさめる手法の標準化が提案されている。しかしながら、Realtime tracing 技術に関して、このように標準化の動きがあるものは稀であり、Realtime tracing 実現のためには今後新たなワーキンググループの設立による標準化への活発な動きが求められる。

第 4 章 Realtime tracing の将来

1. Realtime tracing の課題

(1) 物理的課題

攻撃に対するトレースバックの実効性は、様々な要因によって変化するが、これらの要因の一つにネットワーク環境が挙げられる。ネットワーク環境によっては、トレースバックシステムの実効性が確保されている場合もあれば、そうではない場合もある。トレースバックシステムの実効性が確保されている場合、そのネットワークは制御された環境にあると言える。例を挙げると、ネットワークやデスクトップコンピュータの設定が一人の管理者により管理されているようなネットワークがあるとすれば、それは制御された環境であると言える。このような環境であれば、トレースバック用ツール（例えば、改良されたルータ、特別なホストやネットワーク監視機器）の配置も可能であり、利用可能な送信元やネットワーク通信タイプのフィルタリングも可能である。また、完全に制御された環境下でのトレースバックであれば、高いセキュアネットワーク内において、内部攻撃の送信元を見つけることも容易であると考えられる。しかしながら、一般的なネットワーク環境では、ここまで徹底したネットワークの制御は現実問題として難しいと言える。例えば、管理者によりネットワークは制御されているものの、デスクトップコンピュータの設定に関しては一切管理されていないようなイントラネットでは、部分的にしか環境を制御していないと言える。また、今日のインターネットなどは、制御されていないネットワークの典型的な形であると言える。このようにネットワークが制御されていない状況においては、トレースバックの実効性は低い水準にとどまることは否めない。

別の要因としては、トレースバックに影響を与える攻撃の種類が挙げられる。攻撃特徴の主な識別要素は、トラフィック量と攻撃の時間幅である。

一般的に、攻撃はその攻撃経路に沿った形である量のトラフィックを生成し、ある一定時間継続する。長時間に渡り攻撃が続き、多くの情報が伝送されれば、その分トレースバックの実効性は高まると言える。しかしながら、極論として、攻撃元ホストから発生した攻撃がたった一つのパケットから構成されるものであるとした場合、一般的なトレースバックではこのケースに対して対処できない。「極論」とあるように、このような場合は現実的に稀な事象ではあるが、可能性が全くないとは断言できない。

(2) 社会的課題

前述の物理的課題に加えて懸念材料として挙げられるべきものは、トレースバックに対する社会的な障害である。インターネットを組織する政府や通信業者、企業の間には、いまだにネットワーク犯罪に対する足並みが揃っていないこと以前に、明確な国際的基準がないことからくる根強い不信感が存在する。この信頼性の欠如により、多くの組織が、トレースバックシステム実現のための情報共有や相互支援のための行動よりも、攻撃を受けた事実を公表しないことにより組織の信頼失墜を免れようと試みたり、個人情報保護の見地から情報開示に非協力的になるなどの行動をとりがちになっている。先に述べたように、トレースバックは付加的なインフラやネットワークを共有する組織間の協力を必要とする。

トレースバックへの協力を促進するためには、二つの次元で考えていくことができるであろう。

一つ目はある程度の協力を強制するような政府の規制を増すことである。しかし、政府による規制の強化に関しては、個人情報保護の観点から根強い反発がおこると考えられる。一例として、米国では、2001 年 9 月 11 日の同時多発テロ移行強化されてきたテロ対策の一環として、国防総省によって「全情報認知（TIA）」システムの構想が練られている。しかし、この TIA システムに対しては、クレジットカード、医療、教育、住居移動に関する膨大なデータを収集することになるため、各方面から批判の声があがっている。DARPA ではこの TIA システムを実現化するために、電子メールや Web 閲覧を行う際にもユーザに電子 DNA（eDNA）という認証タグによる身分証明を行わせるという eDNA 案と呼ばれる計画が考案されていたが、コンピュータおよびプライバシーの専門家からの激しい批判があったこともあり、この eDNA 案は断念されたという経緯がある。

二つ目は、特に企業などの利益団体において、ネットワーク上の犯罪による被害に対する経済的コストの増大を社会全体で押し上げていく流れを作ることである。現在においても、個人顧客情報が失われた場合には、顧客がプライバシー喪失のため企業を訴えることは当然想定してしかるべきであろう。電子商取引においては、DoS 攻撃の間に失うビジネスコストを回収するために ISP を訴えることもありうる。法的には、ビジネスは予期できない出来事から生じた害に対する責任を逃れることが可能な場合がある。通常、犯罪法ではこの予期できない範疇の場合、その効力はない。しかし今後は、ネットワーク攻撃は企業が予期すべきほど当たり前のことであると認知されてくる可能性がある。近い将来、企業側がこれらネットワークに対する攻撃をコストの一部として抱えていかなければならなくなった場合、一つの流れとして考えられるのは、攻撃による直接的なコストと攻撃に対する責任の脅威が、最終的に保険業界に対する要求となるということである。ネットワーク犯罪によるコストが保険システムの中に取り入れられることにより、企業側にとってはトレースバックシステムに対するインセンティブ（Incentive）

が生まれる可能性がある。インセンティブとは、広義には、人や組織に特定の行動を促す動機付け、誘引のことであるが、ここでは保険業界主導によって、企業においてトレースバックツールや技術の採用が自発的に実施される可能性が生まれるということである。

しかし、ネットワークへの攻撃に対して保険を適用するためには、保険会社はそれ相応のデータを持たなければならない。すなわち、多くの保険に関する情報と同様、ネットワーク上の犯罪に関する適切な基準の定義と、包括的なデータの収集が業務上の課題としてたちあらわれることは必然的となってくる。当然、このような大規模かつ複雑な作業のすべてを、保険業界という特定の団体のみに一任することはあまりに過重な負担である。

2. Realtime protection との関係

Realtime tracing の目的が、攻撃パケットの発信源をリアルタイムに特定することであるのに対して、Realtime protection では、悪意のある第三者からの攻撃をリアルタイムに防御することが目的となる。両者共リアルタイムとは付くものの、その目的とするところは大きく異なると言える。

両者の根本的な違いは、前述した目的の違いに他ならないが、Tracing に対する考え方を見てもその違いは明らかである。第 3 章の 2－(2).トレースバックの評価にもあるが、トレースバック技術の要素としては、精度・正確性・適時性が挙げられる。Realtime tracing においては、それらすべての要素が必要とされるのだが、Realtime protection では、適時性が最も重要視される。もちろん、Realtime protection に Realtime tracing において必要とされる精度や正確性が加わるのであれば、より効果的な防御や攻撃対策の手段をとることが可能になるかもしれない。しかし、Realtime protection において最も重要視されるものは、どこからどこへの攻撃パケットが自ネットワークに送り込まれているのかをリアルタイムに知ることである。Realtime protection の場合、「どこから」を示すものが、攻撃者自身の使用するマシンの IP アドレスであろうが、偽造された IP アドレスであろうが問題ではない。なぜなら、リアルタイムに攻撃を防御するために必要な材料は、守るべきネットワークに到達する攻撃パケットの保持する情報、つまりは、送信元 IP アドレスや送信先 IP アドレス、そして送信元ポート番号や送信先ポート番号といったものであるからである。そして、実際に攻撃を防御する際は、それらの情報を元にアクセス制御装置において攻撃パケットのフィルタリングを行なうことになる。このように、Realtime protection では、Tracing 技術というよりは、むしろ今進行中の攻撃を攻撃として正しく検知できること、つまり、IDS の技術（機能）が重要視されていると考えられる。

また、Realtime protection の機能を備えた製品は既に市場で販売されている。これらの製品は、以下のような方法で Realtime protection を実現している。

1．Reset パケットを送信して通信を切断する。
2．Firewall、ルータと連携して通信を切断する。
3．インラインでネットワークに設置して、攻撃と判断された通信を遮断する。

まず、１の方法であるが、攻撃として判断された通信の送信元・送信先アドレスに対して、Reset パケットを送信し、該当の通信を切断する。Reset パケットを使用するため、TCP の通信にしか利用できない。また、攻撃として判断されてから Reset パケットを送信するため、攻撃対象マシンに対する最初の攻撃を遮断することは不可能である。

２の方法であるが、攻撃として判断された通信に対して、その攻撃元の IP アドレスからの通信を一定期間遮断するような指示を Firewall やルータに送信し、一時的にルールを変更して、攻撃を遮断する。１の方法と同様に、攻撃として判断されてから Firewall やルータに通信を一定期間遮断するような指示に送信するため、攻撃対象マシンに対する最初の攻撃を遮断することは不可能である。

３の方法であるが、インラインで設置し、攻撃と判断された通信を遮断するため、１，２の方法とは異なり、攻撃対象マシンへの最初の攻撃をも遮断することが可能である。

１,２の方法では完全な意味での Realtime protection が実現できないため、Realtime protection の機能を謳う製品は、３の方法で実現されており、これらの製品は IDP（Intrusion Detection and Prevention）や IPS（Intrusion Prevention System）と呼ばれている。Realtime protection が防ぐものは攻撃自体であり、攻撃元を特定しているわけではない。そのため、あくまでもネットワークの入り口で攻撃を防ぐだけであり、攻撃元を突き止め、攻撃を止めさせるといった根本的な対処法にはならないことを注意しなければならない。しかし、悪意のある第三者からの攻撃を正確に判断できさえすれば、攻撃として判断された通信を遮断すればよいだけであり、通信の許可・不許可は Firewall のような既存の技術を利用することで実現可能であるため、Realtime protection の技術は Realtime tracing の技術より容易なものであるとは言える。

3. Realtime tracing の研究状況

(a) 国からの委託研究事業

平成 11 年度～平成 13 年度
“不正アクセス発信源追跡技術に関する研究開発”
株式会社 NTT データ
東日本電信電話株式会社
（通信・放送機構（TAO）からの委託）
平成 11 年から 13 年まで、以下の研究開発を実施。平成 13 年 3 月終了。
（１）パケット発信源追跡に関する研究開発
（２）次世代不正アクセス検知技術の研究開発
（３）発信源追跡技術の不正利用防止技術の研究開発

研究報告書及び要約に関しては、通信・放送機構（TAO）のサイトから入手可能。
http://www2.shiba.tao.go.jp/seika/

「平成 11 年度不正アクセス発信源追跡技術に関する研究開発報告書」(報告書･和文要約)
「平成 12 年度不正アクセス発信源追跡技術に関する研究開発報告書」(和文要約)

「平成 11 年度不正アクセス発信源追跡技術に関する研究開発報告書」では、研究開発目標として、以下の三点を挙げている。

1. パケット発信源追跡技術の研究開発
2. 次世代不正アクセス検知技術の研究開発
3. 発信源追跡技術の不正利用防止技術の研究開発

1 では､実際のインターネット環境を模した実験環境において､「隣接ノード追跡技術」､「追跡管理技術」の二つの技術を開発する。

「隣接ノード追跡技術」は、IP アドレス以外の識別子を利用し、隣接ノードを順順にたどることによって、パケットが通過してきた経路および発信源を特定する技術の研究開発である。

「追跡管理技術」は、「隣接ノード追跡技術」を利用した追跡において、追跡全体を管理する技術の研究開発である。

2 では、「未知不正アクセス検知技術」、「追跡不正アクセス抽出技術」の二つの技術をリアルタイムで実現するプロトタイプを開発する。

「未知不正アクセス検知技術」は、不正アクセスの情報ではなく、正常なアクセスの情報を登録しておく等の方法により、未知の手法を含む広範な種類の不正アクセスを検知する技術の研究開発である。

「追跡不正アクセス抽出技術」は、人工知能的アプローチを利用して、多くの検知結果の中から追跡すべきアクセスのみを抽出することにより、不要な追跡を発生させてネットワークに余分な負荷をかけないような判断を行う技術の研究開発である。

3 では、「不正利用対象データの隠蔽技術」、「不正利用対象データの原本性保証技術」、「システム不正アクセスの否認防止技術」に分かれている。

「不正利用対象データの隠蔽技術」は、追跡システムにおいて、追跡および監視を行うためのメッセージ転送を不正アクセス者に検知・解読されないための技術の研究開発である。

「不正利用対象データの原本性保証技術」は、追跡システムの追跡情報などの改竄防止技術、および改竄されていないことを証明する技術の研究開発である。

「システム不正アクセスの否認防止技術」は追跡情報やログの参照を要求した者の本人性確認を行い、不正アクセスの事実を証明する情報を保護することによって、不正アクセスの否認を防止する技術の研究開発である。

(b) NTT グループ

情報処理学会と IEEE の論文集に、NTT グループの研究グループから以下の論文が提出されている。これらは、通信・放送機構（TAO）からの委託研究である平成 11 年度～平成 13 年度「不正アクセス発信源追跡技術に関する研究開発」の一環として研究発表されたものである。

馬場達也、山岡正輝、小久保勝敏、松田栄之、"プロトコル仕様及びポリシー情報を利用した不正アクセス検知方式の検討"、情報処理学会第 60 回全国大会講演論文集(3)、pp.285-286、 2000 年 3 月

渡辺英俊、馬場達也、竹爪慎治、松田栄之、"不正アクセス発信源追跡のためのパケット識別情報の検討"、 情報処理学会第 60 回全国大会講演論文集（3)、 pp.289-290、2000 年 3 月

馬場達也、小久保勝敏、松田栄之、"不正アクセス検知のためのプロトコルチェック方式の検討"、 情報処理学会第 61 回全国大会講演論文集（3)、 pp.257-258、 2000 年 10 月

鴨田浩明、馬場達也、小久保勝敏、松田栄之、"ニューラルネットワークを利用した不正アクセス被害予想方式の検討"、 情報処理学会第 62 回全国大会講演論文集（3)、 pp.283-284、 2001 年 3 月

鴨田浩明、馬場達也、小久保勝敏、松田栄之、矢口博之、"ニューラルネットワークを用いた不正アクセス被害予測方式における予測精度の向上"、 情報処理学会第 63 回全国大会講演論文集（3)、 pp.489-490、 2001 年 9 月

早川晃弘、馬場達也、小久保勝敏、松田栄之、"不正アクセス発信源追跡システムの実装と検証"、 情報処理学会第 63 回全国大会講演論文集（3)、 pp.491-492、 2001 年 9 月

馬場達也、 鴨田浩明、 小久保勝敏、 松田栄之、 "プロトコル仕様及びポリシー情報を利用した不正アクセス検知システムの実装と評価"、 コンピュータセキュリティシンポジウム 2001（CSS2001）論文集、情報処理学会シンポジウムシリーズ Vol.2001、No.15、 pp.173-178、 2001 年 10 月

早川晃弘、馬場達也、小久保勝敏、松田栄之、"不正アクセス発信源追跡システムにおける追跡時間の評価"、情報処理学会第 64 回全国大会講演論文集（3)、pp.389-390、2002 年 3 月

馬場達也、 鴨田浩明、 小久保勝敏、 松田栄之、 "プロトコル仕様及びポリシー情報を利用した不正アクセス検知システムの実環境評価"、 情報処理学会研究報告、Vol.2002、 No.68、 2002-CSEC-18、 pp.33-38、 2002 年 7 月

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.

Tatsuya Baba and Shigeyuki Matsuda, "Tracing Network Attacks to Their Sources", IEEE Internet Computing, Vol. 6, No. 2, pp.20-26, March/April 2002.

(c) 東北大学大学院グループ

電気情報通信学会において、東北大学大学院情報科学研究科を中心にしたグループで以下の論文・レポートが提出されている。これらはいずれも、ネットワーク上でトラフィックを観測し、トラフィックパターンに基づく攻撃検知、追跡技術を提案している。

武井 洋介、太田 耕平、加藤 寧 他、” トラヒックパターンを用いた不正アクセス検出及び追跡方式”、電子情報通信学会技術研究報告 99 (通号 436)、pp.37-42、1999 年 11 月

坂口 薫、和泉 勇治、太田 耕平 他、” 2 次計画法を用いたトラヒックパターンの比較による DoS の追跡手法の提案 (特集テーマ IP サービスとそれを支えるネットワーク技術,一般)”、電子情報通信学会技術研究報告 101(356)、pp.15-22、2001 年 10 月

金丸 朗、太田 耕平、加藤 寧 他、” 解説 高速ネットワークに対応可能な DoS 攻撃の追跡技術--不正アクセスの抑制と根絶を目指して”、電子情報通信学会誌 84(10) (通号 929)、pp.727-729、2001 年 10 月

(d) 奈良先端科学技術大学院大学グループ

奈良先端科学技術大学院大学では、以下のトレースバックに関する研究が情報処理学会および情報処理学会各研究会に提出されている。DDoS 攻撃の対策としての、Hash 系のトレースバック技術に注目した研究や、逆探知パケット方式のモデル化を目指したものがある。

門林雄基, 大江将史, "IP トレースバック技術", 情報処理学会誌 Vol.42 No.12 - 006, 2001 年

櫨山 寛章, 大江 将史, 門林 雄基, "ＭＡＣトレースバック：Hash-Based IP トレースバック拡張方式の提案", 情報処理学会 高品質インターネット研究会(QAI) 研究報告「高品質インターネット」2002 年度 No.004 – 001

澤井 裕子, 大江 将史, 飯田 勝吉, "逆探知パケット型 IP トレースバックのトラフィック量とその攻撃経路再構成時間のモデル化とシミュレーションを用いた検証", 研究発表：電子情報通信学会 通信ソサイエティ, インターネットアーキテクチャ研究会, 第 2 回研究会, 2002 年 7 月 26 日
http://www.ieice.org/cs/ia/jpn/conference/200207/presentation/Sawai.pdf

第 5 章 総評

Tracing の最終的な目標は、攻撃の実行主体であるところの攻撃者の特定にある。しかし、今後の関連技術の発展を見込んだとしても、自動プロセスのみで攻撃者の特定を行うことは不可能であり、人間による手動プロセスの介入が必要とならざるを得ないと言えるであろう。

現状、Tracing を行う際に自動プロセスのみで判断可能なものは、パケットの送信元 IP アドレスに限られ、その他に関しては人間による手動プロセスが必要となる。しかし「送信元 IP アドレスが判断可能である」とは言え、それがそのまま「攻撃パケットの発信源 IP アドレス」であるとは限らない。なぜなら、攻撃者は自身の身元を隠蔽するため、送信元 IP アドレスを偽造するなどの方法を用いて実際の攻撃を行うからである。そのため、現状の Tracing では、攻撃パケットの真の発信源となるホストを自動プロセスのみで特定することは不可能であると言える。

しかし、Realtime Tracing が現実化すれば、自動プロセスのみで攻撃パケットの発信源までは特定することが可能になる。ここで言う発信源の意味は、攻撃パケットの送信元 IP アドレスが偽造されている場合も、また、踏み台ホストから攻撃を受ける場合も、問題なくその攻撃パケットの発信元ホストを特定することが可能であるということである。特定可能であるのはホストであり、依然、最終目標とされる攻撃者のリアルタイムでの特定は不可能であることに変わりはないが、Tracing に必要とされる手動プロセスは大幅に減少し、発信源の特定は攻撃の検知とほぼ同時に近い形で行うことが可能になる。発信源の早期特定は、防御面において効果的な対応策を取ることを可能にするだけではなく、結果として攻撃者を特定するための情報を早い段階で把握することが可能であるため、攻撃者の発見確率が高まることが期待される。

技術的な面では、Realtime tracing 実現に繋がる自動トレースバックの研究が、あらゆる場で行われている。それらの研究成果によると、偽造された送信元 IP アドレスを使用した攻撃や DoS 攻撃においても、その発信源を特定可能であるという報告がなされている。しかしながら、DDoS 攻撃に関しては、その攻撃手法や特徴からいって、発信源の特定は困難であるという報告がなされている。それゆえ今後は DDoS 攻撃における正確な発信源の特定が Realtime tracing 実現に向けての技術的課題になるであろう。また、上記研究は研究用に用意された実験ネットワーク環境においてその成果を示しているに過ぎない。実際のネットワークやインターネット上のトラフィックは複雑かつ膨大な量であるため、同様の結果が得られるかは疑問であり、今後は現実のネットワーク環境に近い環境での調査が必要とされてくる。

また、Realtime tracing 実現に向けては、技術的問題に留まらず、物理的問題、社会的問題もその障害になるとされている。

物理的問題に関しては、Realtime tracing を実行する上で必要となる専用機器の導入やプロトコルの使用が可能であるかどうかという問題が挙げられる。たとえ、自ドメインにおいてそれらの機器やプロトコルの導入、使用が可能であっても、攻撃パケットは世界中のあらゆるところからインターネットを介してやってくる。つまり、その攻撃パケットの発信源を特定するためには、世界中のネットワーク上の必要とされる場所に、それらの専用機器やプロトコルを配備する必要が生じることになる。

社会的問題に関しては、トレースバックという行為に対してすべての人々がその意義と重要性を理解し、社会的協力が得られなければ、完全なるトレースバックは実行不可能であることが挙げられる。

現実的な問題として、トレースバックの意義や重要性は、いまだ社会全体に認知されているとは言いがたい状況である。一般的に、人々が最も重要視するものは、現に進行中の攻撃をいかにして防御するか、また、将来的に被る可能性のある攻撃の影響を如何にして予防するかである。そのため、Firewall や IDS の存在は専門的な技術者以外にも広く知られるところとなり、多くのネットワークで導入が行われている。確かに、それらの機器導入は、攻撃の防御や予防などに対しては効果的であり、攻撃対策には必要不可欠なものである。しかしながら、攻撃が行われてしまった場合の事後対策に関しては比較的重要視されていないのが現状である。最近になり、ようやくインシデントレスポンスという言葉が世の中に普及し始めてきた。インシデントレスポンスとは「コンピュータ・セキュリティ・インシンデントに対応すること」を意味し、コンピュータ・セキュリティ・インシデントについては、JPCERT/CC の FAQ により「コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの（その疑いがある場合）を含む。例えば、リソースの不正使用、サービス妨害行為、データの破壊、意図しない情報の開示や、さらにそれらに至るための行為（事象）などがある」との説明がある。インシデントレスポンスでは、様々な対応策を行う上で、Tracing 作業が非常に重要な意味をもつ作業の一つであることが理解できる。しかし現状では、このことを認識していたとしても、様々な理由により、トレースバックシステムの導入には慎重を期している組織が少なからずあることも事実であろう。その理由の一つとしては、一般企業などにおいて、攻撃を受けたことを第三者に知られてしまうところの Tracing 行為は、顧客からの信頼失墜に繋がる恐れがあるとの懸念が、経営陣に根強くあるからであると思われる。短期的には、それは正しい選択であろう。しかし、攻撃に対する防御や予防を考慮すると、攻撃者の発見、そしてその逮捕こそが一番の効果的な対策となりうるのである。このことが、社会全体で認知されていかなければ、おそらく Realtime tracing の実現は遠い先のことになるであろう。ネットワークを形成しているすべての組織の協力体制により、犯罪者に対する包囲網を敷いていくことが今後一層求められるであろう。

第 6 章 付録

＜参考資料＞

第 2 章

[1]. W･R･スティーヴンス, 「詳解 TCP/IP〈Vol.1〉プロトコル」, 橘 康雄 訳, 井上 尚司 監訳, ピアソン・エデュケーション, 2002 年 4 月

[2]. 笠野 英松, 「ポイント図解式 インターネット RFC 事典」増補版, アスキー, 2002 年 4 月

[3]. Kevin Washburn, Jim Evans, 「TCP/IP バイブル」改訂新版, 株式会社オープンループ／海江田一詩 訳, アスキー, 1999 年 3 月

[4]. ステフェン･ノースカット, マット･フィルノウ, マーク･クーパー, カレン･フレデリック, 「ネットワーク侵入解析ガイド―侵入検知のためのトラフィック解析法」, クイープ 訳, 武田 圭史 監修, ピアソン･エデュケーション, 2001 年 12 月

[5]. 白井 雄一郎, 白濱 直哉, 又江原 恭彦, 柳岡 裕美, 「インターネットセキュリティ 不正アクセスの手法と防御」, 三輪信雄 監修, ソフトバンクパブリッシング, 2001 年 7 月

[6]. ラック SNS チーム, 「セキュリティ技術大系 2003　インターネット編」, 日経 BP 社, 2002 年 9 月

[7]. ラック SNS チーム, 「セキュリティ技術大系 2003　イントラネット編」, 日経 BP 社, 2002 年 9 月

[8]. 小林 林広, 好田 崇志, 山後 正孝, 大塚 慎太郎, 「技術者のための Windows2000 Server セキュリティ完全対策」, 吉永 昇 監修, 技術評論社, 2002 年 9 月

[9]. Chris Prosise, Kevin Mandia,「インシデントレスポンス　不正アクセスの検出と対策」, エクストランス訳, 坂井順行, 新井悠 監修, 翔泳社, 2002 年 7 月

第 3 章

[10]. Shigeyuki Matsuda, Tatsuya Baba, Akihiro Hayakawa, Taichi Nakamura, NTT Data Corporation, “Design and Implementation of Unauthorized Access Tracing System,” 2002 Symposium on Applications and the Internet (SAINT) January 28 - February 01, 2002
http://www.computer.org/proceedings/saint/1447/14470074abs.htm

[11]. H. jang and S.Kim, “An Intruder Tracing System based on a Shadowing Mechanism,”Proceedings of the IEEE symposium on Computers and Communications, pp. 904-909, Taormina/Giardini Naxos, Italy, July 1~4, 2002
http://computer.org/proceedings/iscc/1671/16710904abs.htm

[12]. Dan Sterne, Kelly Djahandari, Brett Wilson, Bill Babson, Dan Schnackenberg, Harley Holliday, and Travis Reid, “Autonomic Response to Distributed Denial of Service Attacks,” W.Lee, L.Me, and A.Wespi (Eds.):RAID 2001,LNCS 2212,pp.134 –149,2001.
http://www.cse.ogi.edu/~wuchang/cse581_winter2002/papers/22120134.pdf

[13]. BELLOVIN, S. M. ICMP traceback messages. Internet Draft,IETF, Oct. 2001. draft-ietf-itrace-02.txt
http://www.ietf.org/internet-drafts/draft-ietf-itrace-02.txt

[14]. Susan C. Lee and Clay Shields,“Technical,Legal,and Societal Challenges to Automated Attack Traceback,” 2002 IEEE
http://www.computer.org/itpro/it2002/f3012abs.htm

[15]. W. Lee and K. Park, “On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack”, Proceedings of the IEEE INFOCOM01, April 2001, Anchorage, Alaska
http://www.silicondefense.com/research/itrex/archive/tracing-papers/park01effectiveness_of_marking.pdf

[16]. S. Staniford-Chen and L.T. Heberlein, “Holding Intruders Accountable on the Internet.” Proc. IEEE Symposium on Security and Privacy, Oakland, CA, May 1995,pp. 39?49.
http://citeseer.nj.nec.com/staniford-chen94holding.html

[17]. H. Burch, B. Cheswick, “Tracing Anonymous Packets to Their Approximate Source,” Proc. USENIX LISA '00,December 2000.
http://www.usenix.org/publications/library/proceedings/lisa2000/burch/burch_html/
http://www.silicondefense.com/research/itrex/archive/tracing-papers/burch00tracing_approximate_source.pdf

[18]. Tatsuya Baba, Shigeyuki Matsuda, “Tracing Network Attacks to Their Sources,” 2002 IEEE
http://computer.org/internet/ic2002/w2020abs.htm

[19]. Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson , “Practical Network Support for IP Tracebac,”Proceedings of the 2000 ACM SIGCOMM Conference, pp. 295-306, Stockholm, Sweden, August 2000
http://www.cs.washington.edu/homes/savage/traceback.html

[20]. D. Song and A. Perrig. “ Advanced and authenticated marking schemes for IP traceback.Technical ”Report UCB/CSD-00-1107, University of California, Berkeley, June 2000.
http://www.perrig.net/~dawnsong/papers/iptrace.pdf

[21]. Drew Dean, Matt Franklin, and Adam Stubblefield. An Algebraic Approach to IP Traceback. In Proceedings of the 2001 Network and Distributed System Security Symposium, San Diego, CA, February 2001.
http://citeseer.nj.nec.com/dean01algebraic.html

[22]. Xinyuan Wang,Douglas S. Reeves,S. Felix Wu,Jim Yuill,“Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework,”North Carolina State University
http://www.cs.ucdavis.edu/~wu/publications/2001-03-watermark-ifipsec.pdf

[23]. S. Felix Wu, Lixia Zhang, Dan Massey, Allison Mankin, Intention-Driven ICMP Trace-Back. Internet Draft,IETF, Nov. 2001. draft-wu-itrace-intention-00.txt http://irl.cs.ucla.edu/papers/draft-ietf-itrace-intention-00.txt

[24]. S. Felix Wu, Lixia Zhang, Dan Massey, Allison Mankin, “On Design and Evaluation of “Intention-Driven” ICMP Traceback” http://irl.cs.ucla.edu/papers/Intention-iTrace.pdf

[25]. Glenn Mansfield, Kohei Ohta, Y. Takei, N. Kato, Y. Nemoto, "Towards trapping wily intruders in the large," Recent Advances in Intrusion Detection (1999). http://www.silicondefense.com/research/itrex/archive/tracing-papers/mansfield00wily_hacker.pdf

[26]. Kohei Ohta, Glenn Mansfield, Yohsuke Takei, Nei Kato, Yoshiaki Nemoto,"Detection, Defense, and Tracking of Internet-Wide Illegal Access in a Distributed Manner", Proceedings of the 10th Annual Internet Society Conference (INET 2000), July 2000. http://www.isoc.org/inet2000/cdproceedings/1f/1f_2.htm http://www.ipa.go.jp/security/fy12/contents/crack/idws/13INET2000.PDF

[27]. H.T.Jung, et. al.,”Caller Identification System in the Internet Environment,” Proceedings of USENIX Security, Symposium IV, 1993 http://www.silicondefense.com/research/itrex/archive/tracing-papers/jung93caller_identification_system.pdf

[28]. D. Schnackenberg, K. Djahandari, and D. Sterne, "Infrastructure for Intrusion Detection and Response", Proceedings of the DARPA Information Survivability Conference and Exposition(DISCEX), Hilton Head Island, SC, January 25-27, 2000. http://www.nai.com/common/media/nai/pdf/DISCEX-IDR-Infrastructure.pdf

[29]. D. Schnackenberg, K. Djahandari, and D. Strene, Harley Holiday, Randall Smith, "Cooperative Intrusion Traceback and Response Architecture

(CITRA)", Proceedings of the 2nd DARPA Information Survivability Conference and Exposition (DISCEXII), June 2001.
http://www.computer.org/proceedings/discex/1212/volume1/12120056abs.htm
ftp://ftp.tislabs.com/pub/IDIP/DISCEX_CITRA.pdf

[30]. R.Stone."CenterTrack:An IP Overlay Network for Tracking DoSFloods,"in Proceedings of the 9th USENIX Security Symposium pages 199 –212, http://www.silicondefense.com/research/itrex/archive/tracing-papers/stone00centertrack_new.pdf

[31]. Stuart Staniford-Chen, "Distributed Tracing of Intruders",Masters Thesis University of California Davis, 1995 http://www.silicondefense.com/research/itrex/archive/tracing-papers/staniford95distributed_tracing_of_intruders.pdf

[32]. H.Y. Chang, P. Chen, A. Hayatnagarkar, R. Narayan, P. Sheth, N. Vo, C. L. Wu, S.F. Wu, L. Zhang, X. Zhang, F. Gong, F. Jou, C. Sargor, X. Wu, "Design and Implementation of A Real-Time Decentralized Source Identification System for Untrusted IP Packets", Proceedings of the DARPA Information Survivability Conference & Exposition, January 2000. http://www.silicondefense.com/research/itrex/archive/tracing-papers/chang00design_and_implementation_of_realtime.pdf

[33]. Ho-Yen Chang, S.Felix Wu, C. Sargor, X. Wu, "Towards Tracing Hidden Attackers on Untrusted IP Networks", submitted for publication 2000 http://www.silicondefense.com/research/itrex/archive/tracing-papers/chang00towards_tracing_hidden_attackers.pdf

[34]. K. Yoda and H. Etoh, "Finding a Connection Chain for Tracing Intruders", In F. Guppens, Y. Deswarte, D. Gollamann, and M. Waidner, editors, 6th European Symposisum on Research in Computer Security - ESORICS 2000 LNCS -1985, Toulouse, France, Oct 2000 http://www.silicondefense.com/research/itrex/archive/tracing-papers/yoda00chaining.pdf

[35]. Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer, "Hash-Based IP Traceback",Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 2001. An earlier version appeared as BBN Technologies Technical Memo, BBN-TM-1284
http://nms.lcs.mit.edu/~snoeren/papers/spie-sigcomm.html
http://www.acm.org/sigcomm/sigcomm2001/p1-snoeren.pdf

[36]. Luis A. Sanchez, Walter C. Milliken, Alex C. Snoeren, Fabrice Tchakountio, Christine E. Jones, Stephen T. Kent, Craig Partrige, and W. Timothy Strayer, "Hardware Support for Hashed-Based IP Traceback", Proceedings of the 2nd DARPA Information Survivability Conference and Exposition (DISCEXII), June 2001.
http://www.ir.bbn.com/projects/SPIE/pubs/spie-discex01.pdf

[28]. M.Asaka, S.Okazawa, A.Taguchi, and S.Goto, "A Method of Tracing Intruders by Use of Mobile Agents", INET'99, June 1999.
http://www.silicondefense.com/research/itrex/archive/tracing-papers/asaka99local_attack_detection_and_tracing.pdf

[37]. M.Asaka, A.Taguchi, and S.Goto, "The Implementation of IDA: An Intrusion Detection Agent System", in Proceedings of the 11th FIRST Conference 1999, Brisbane, Australia, June 1999
http://citeseer.nj.nec.com/347867.html

[38]. M.Asaka, S.Okazawa, A.Taguchi, and S.Goto, "A Method of Tracing Intruders by Use of Mobile Agents", INET'99, June 1999
http://www.isoc.org/isoc/conferences/inet/99/proceedings/4k/4k_2.htm
http://citeseer.nj.nec.com/asaka99method.html

[39]. Heejin Jang and Sangwook Kim, "A Self Extension Monitoring for Security Management" 16th Annual Computer Security Applications Conference Dec. 2000, New Orleans, Louisiana.
http://www.silicondefense.com/research/itrex/archive/tracing-papers/jang00self-extension_monitoring.pdf

[40]. S. C. Lee and C. Shields,"Tracing the Source of Network Attack: A Technical, Legal and Societal Problem", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, June 2001. http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW1C1(09).pdf

[41]. Cisco Systems, "Characterizing and Tracing Packet Floods Using Cisco Routers", Aug 1999. http://www.cisco.com/warp/public/707/22.html

[42]. Brentano, Gihan V. Dias, Terrance L. Goan, L. Todd Heberlein, Che-Lin Ho, Karl N. Levitt, Biswanath Mukherjee, et al. "DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype", Proceedings of the 14th National Computer Security Conference, 1991. http://citeseer.nj.nec.com/snapp91dids.html

[43]. Steven R. Snapp, James Brentano, Gihan V. Dias, Terrance L. Goan, Tim Grance, L. Todd Heberlein, Che-Lin Ho, Karl N. Levitt, Biswanath Mukherjee, Douglass L. Mansur, Kenneth L. Pon, and Stephen E. Smaha,"A system for distributed intrusion detection", In COMPCOM Spring '91 Digest of Papers, pages 170-176, February/March 1991 http://seclab.cs.ucdavis.edu/papers/pdfs/ss-jb-91.pdf

[44]. Calvin Ko, Deborah A. Frincke, Terrence Goan, Jr., L. Todd Heberlein, Karl Levitt, Biswanath Mukherjee, Christopher Wee, "Analysis of an Algorithm for Distributed Recognition and Accountability", 1st ACM Conference on Computer and Communications Security http://citeseer.nj.nec.com/ko93analysis.html

[45]. S.M. Bellowin, "Security Problems in the TCP/IP Protocol suite", ACM Computer Communications Review 19/2 (1989), 32 - 48. http://www.deter.com/unix/papers/tcpip_problems_bellovin.pdf http://citeseer.nj.nec.com/bellovin89security.html

[46]. John Ioannidis, Steven M. Bellovin, "Pushback: Router-Based Defense Against DDoS Attacks", draft February 2001.
http://www.research.att.com/~smb/papers/pushback-impl.pdf

[47]. Sally Floyd,Steve Bellovin,John Ioannidis,Kireeti Kompella, Ratul Mahajan,Vern Paxson, "Pushback Messages for Controlling Aggregates in the Network", Internet Draft: draft-floyd-pushback-messages-00.txt, submission date Jul. 2001 , expiration date Jan. 2002.
http://citeseer.nj.nec.com/cache/papers/cs/26764/http:zSzzSzwww.research.att.comzSz~smbzSzpaperszSzpushback-CCR.pdf/mahajan01controlling.pdf
http://www.icir.org/pushback/

[48]. Buchholz, Thomas E. Daniels, Benjamin Kuperman, Clay Shields, "Packet Tracker Final Report", CERIAS Technical Report 2000-23, Purdue University, 2000.
https://www.cerias.purdue.edu/infosec/bibtex_archive//archive/2000-23.pdf

[49]. David Moore, Geoffrey Voelker, and Stefan Savage, "Inferring Internet Denial-of-Service Activity", To appear in the 2001 USENIX Security Symposium.
http://www.caida.org/outreach/papers/2001/BackScatter/usenixsecurity01.pdf

[50]. Y. Zhang and V. Paxson, "Detecting Stepping Stones", Proceedings of 9th USENIX Security Symposium, August 2000.
http://www.icir.org/vern/papers/stepping/
http://citeseer.nj.nec.com/294604.html

[51]. T. H. Ptacek and T. N. Newsham,"Insertion, evasion, and denial of service: Eluding network intrusion detection", Technical report, Secure Networks, Inc., January 1998.
http://secinf.net/info/ids/idspaper/idspaper.html
http://citeseer.nj.nec.com/ptacek98insertion.html

[52]. 経済産業省, サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」,平成 14 年 04 月
http://www.meti.go.jp/kohosys/press/0002626/

[53]. 櫨山寛章,「電話網とインターネットにおける追跡システムの比較」,奈良先端科学技術大学院大学計算機言語学講座
http://www.soi.wide.ad.jp/class/20010013/materials_for_student/09/hazeyama_1122.pdf

[54]. S.Ying,“IA0126 DDoS Automated Response Re-Run,”presentation given at DARPA Information Assurance Program Biweekly Meeting,September 29,2000
ftp://ftp.tislabs.com/pub/IDIP/Ying_briefing.ppt

[55]. CERT Coordination Center,"Denial of Service Attacks"
http://www.cert.org/tech_tips/denial_of_service.html

[56]. Dave Dittrich, “Distributed Denial of Service (DDoS) attacks/tools resource page,” 2002.
http://staff.washington.edu/dittrich/misc/ddos/

[57]. Network Associates Technology, Inc.
http://www.nai.com/research/nailabs/adaptive-network/aitr.asp

[58]. CERT, ``TCP SYN Flooding and IP Spoofing Attacks," CERT Advisory CA-96.21, Sept, 1996.
http://www.cert.org/advisories/CA-1996-21.html

第 4 章

[59]. Top Layer Networks, Inc.
http://www.toplayer.com/content/products/intrusion_detection/attack_mitigator.jsp

[60]. NetScreen Technologies,Inc.
http://www.netscreen.com/products/pdf/IDP100_ds6p.pdf

[61]. Symantec Corporation.
http://enterprisesecurity.symantec.com/Content/displaypdf.cfm?PDFID=295&EID=0

[62]. 夏井高人, 「ネットワーク社会の文化と法」, 日本評論社, 1997 年

[63]. 堀部政男, 「プライバシーと高度情報化社会」, 岩波新書, 1988 年

[64]. 上原孝之, 「図解 そこが知りたい！ネットワーク危機管理入門」, 翔泳社, 2000 年 7 月

[65]. サイバー刑事法研究会報告書
「欧州評議会サイバー犯罪条約と我が国の対応について」
http://www.meti.go.jp/policy/netsecurity/Cybercriminallawcom.htm

[66]. 武井 洋介、太田 耕平、加藤 寧 他、” トラヒックパターンを用いた不正アクセス検出及び追跡方式 ”、電子情報通信学会技術研究報告 99 (通号 436)、pp.37-42、1999 年 11 月

[67]. 坂口 薫、和泉 勇治、太田 耕平 他、” 2 次計画法を用いたトラヒックパターンの比較による DoS の追跡手法の提案 (特集テーマ IP サービスとそれを支えるネットワーク技術,一般) ”、電子情報通信学会技術研究報告 101(356)、pp.15-22、2001 年 10 月

[68]. 金丸 朗、太田 耕平、加藤 寧 他、” 解説 高速ネットワークに対応可能な DoS 攻撃の追跡技術--不正アクセスの抑制と根絶を目指して ”、電子情報通信学会誌 84(10) (通号 929)、pp.727-729、2001 年 10 月

[69]. 馬場達也、山岡正輝、小久保勝敏、松田栄之、"プロトコル仕様及びポリシー情報を利用した不正アクセス検知方式の検討"、 情報処理学会第 60 回全国大会講演論文集（3)、 pp.285-286、 2000 年 3 月

[70]. 渡辺英俊、馬場達也、竹爪慎治、松田栄之、"不正アクセス発信源追跡のためのパケット識別情報の検討"、情報処理学会第 60 回全国大会講演論文集(3)、pp.289-290、 2000 年 3 月

[71]. 馬場達也、小久保勝敏、松田栄之、"不正アクセス検知のためのプロトコルチェック方式の検討"、 情報処理学会第 61 回全国大会講演論文集（3)、pp.257-258、 2000 年 10 月

[72]. 鴨田浩明、馬場達也、小久保勝敏、松田栄之、"ニューラルネットワークを利用した不正アクセス被害予想方式の検討"、 情報処理学会第 62 回全国大会講演論文集（3)、 pp.283-284、 2001 年 3 月

[73]. 鴨田浩明、馬場達也、小久保勝敏、松田栄之、矢口博之、"ニューラルネットワークを用いた不正アクセス被害予測方式における予測精度の向上"、情報処理学会第 63 回全国大会講演論文集（3)、 pp.489-490、 2001 年 9 月

[74]. 早川晃弘、馬場達也、小久保勝敏、松田栄之、"不正アクセス発信源追跡システムの実装と検証"、 情報処理学会第 63 回全国大会講演論文集（3)、pp.491-492、 2001 年 9 月

[75]. 馬場達也、 鴨田浩明、 小久保勝敏、 松田栄之、 "プロトコル仕様及びポリシー情報を利用した不正アクセス検知システムの実装と評価"、コンピュータセキュリティシンポジウム 2001（CSS2001）論文集、 情報処理学会シンポジウムシリーズ Vol.2001、 No.15、 pp.173-178、 2001 年 10 月

[76]. 早川晃弘、馬場達也、小久保勝敏、松田栄之、"不正アクセス発信源追跡システムにおける追跡時間の評価"、情報処理学会第 64 回全国大会講演論文集(3)、pp.389-390、 2002 年 3 月

[77]. 馬場達也、 鴨田浩明、 小久保勝敏、 松田栄之、 "プロトコル仕様及びポリシー情報を利用した不正アクセス検知システムの実環境評価"、情報処理学会研究報告、 Vol.2002、 No.68、 2002-CSEC-18、 pp.33-38、 2002 年 7 月

[78]. 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.

[79]. Tatsuya Baba and Shigeyuki Matsuda, "Tracing Network Attacks to Their Sources", IEEE Internet Computing, Vol. 6, No. 2, pp.20-26, March/April 2002.

[80]. 門林雄基, 大江将史, "IP トレースバック技術", 情報処理学会誌 Vol.42 No.12 - 006, 2001 年

[81]. 櫨山 寛章, 大江 将史, 門林 雄基, "ＭＡＣトレースバック：Hash-Based IP トレースバック拡張方式の提案", 情報処理学会 高品質インターネット研究会(QAI) 研究報告「高品質インターネット」2002 年度 No.004 – 001

[82]. 澤井 裕子, 大江 将史, 飯田 勝吉, "逆探知パケット型 IP トレースバックのトラフィック量とその攻撃経路再構成時間のモデル化とシミュレーションを用いた検証", 研究発表：電子情報通信学会 通信ソサイエティ, インターネットアーキテクチャ研究会, 第 2 回研究会, 2002 年 7 月 26 日
http://www.ieice.org/cs/ia/jpn/conference/200207/presentation/Sawai.pdf

＜索引＞

A

ARP 10, 11, 12, 13, 14, 16

C

CDIF 49
Content Matching 44, 45

D

DARPA 41, 49
DDoS 攻撃 34, 47, 57, 58
DoS 攻撃 24, 36, 47, 51, 57, 58

F

Firewall 1, 3, 4, 24, 48, 49, 53, 59
FQDN 17, 19

H

Hop-by-Hop Tracing 41

I

ICMP 14, 15, 16, 19, 21, 61, 63
IDIP 49, 64, 68
IDP 53
IDS 1, 3, 4, 24, 25, 48, 52, 59
IDWG 43
IETF 39, 43, 49
Internet Key Exchange 42
IPS 53
IPsec 42, 43
IP アドレス 9, 10, 11, 12, 13, 16, 17, 19, 20, 24, 28, 29, 30, 31, 34, 47, 52, 53, 54, 58
ISO 4
ISP 34, 36, 48, 51

J

JPNIC 9, 10

M

MAC アドレス 7, 8, 9, 10, 11, 12, 13, 16

N

nslookup 17, 19

O

OSI 参照モデル 4, 5, 6
OVERLOADING 37

P

Packet marking 37
Packet Marking 46
Proactive tracing 36

Q

Query 41
QUERY 40

R

Reactive tracing 36
Realtime protection 52, 53
Reset パケット 53

T

TCP Sequence 番号 29
TCP/IP 2, 4, 5, 6, 9, 10, 60, 66
Thumbprinting 44
traceroute 19, 20
traceroute・tracert 20, 21
TTL 19, 20

W

whois 18

あ

アカウント 30, 31

い

インシデントレスポンス 1, 59, 60
インターネット層 6, 13

さ

サイバー犯罪条約 68, 69

せ

脆弱性 31
精度 4, 27, 34, 35, 36, 43, 52
セキュリティアソシエーション 42

そ

ソース IP アドレス 24
ゾンビ 34, 36, 44, 46

た

ターゲット IP アドレス 24
ダイジェスト 44

て

データグラム 9, 14, 16
データリンク層 6, 7, 8, 9, 12, 13, 14

と

ドメイン名 10, 17, 18
トランスポート層 5, 13, 16
トロイの木馬 34, 46
トンネル IP ヘッダ 42

ね

ネットワークインターフェース層 6
ネットワーク層 5, 9, 10, 12, 13, 14, 16

は

パケットマッチング 37

ふ

物理層 6
踏み台 33, 36, 44, 48, 58
プライベート IP アドレス 10
ブロードキャスト 10, 11

ほ

ポートスキャン 24

ゆ

ユニキャスト 11

り

リフレクターホスト 30

る

ルータ 12, 13, 14, 15, 19, 20, 35, 50, 53

ろ

ログ解析 1, 24, 25
ロンダリングホスト 31, 32, 33, 34