発信源追跡のための ハイブリッドトレースバック方式

Hybrid Traceback Scheme for Finding True Source of Packets

池田　竜朗　　山田　竜也
■IKEDA Tatsuro　■YAMADA Tatsuya

近年，インターネットにおけるDDoS（Distributed Denial of Service）攻撃や踏み台攻撃といった攻撃の対抗策として，IP（Internet Protocol）トレースバック技術が注目されている。IPトレースバック技術とは，IPアドレスの送信元が偽造されていたとしても，正確な発信源の特定を可能とする技術の総称である。東芝では，受動的と能動的といった性質の異なるIPトレースバック技術を組み合わせるハイブリッドトレースバック方式を提案し，試作システムを開発した。このシステムは，追跡者の意図を反映し，低負荷で詳細な発信源追跡を実現する。

Internet Protocol (IP) traceback has attracted attention as a technology for coping with denial of service, distributed denial of service, and connection laundering attacks.　IP traceback is the generic term for the technology, which determines the true source of attacking packets.　Toshiba has proposed a "hybrid traceback" system that combines two types of IP traceback schemes: active and passive. This system is able to reflect the tracer's intention and achieve detailed tracing with a lower load on the network than conventional schemes.

1　まえがき

近年の広域帯常時接続環境の普及により，ネットワークに対する攻撃手法も大規模化及び広域化している。特にDDoS攻撃（分散型サービス不能攻撃）は，攻撃対象であるサイトやホストに対するトラフィックを急激に増加させるため，攻撃対象のみならずネットワーク全体へ過大な負荷を掛けてしまう。また，個人の常時接続環境の普及に伴い，これらの端末に対する攻撃やその端末を利用した踏み台攻撃（DDoS攻撃などの攻撃パケット発信源として利用される）などの問題も生じてきている。このような攻撃は，ネットワークや機器やサービスに対する実被害が大きく，有効な対処手段を講じることが難しいため，深刻な問題となっている。

このような攻撃に対抗するセキュリティ対策の一つとして，攻撃パケットの発信源を特定し攻撃の元から断つという手段を取りうる。しかし，現在のインターネットでは，ファイアウォールによるネットワークの分断や，IPアドレスの送信元偽造の容易さなどにより，攻撃パケットの発信源を特定することが困難である場合が多い。また，特定できたとしても，本来の攻撃者ではないという状況が起こりうる。したがって，そのような場合においても正確な発信源特定を行える技術が必要となってくる。

ここでは，はじめに発信源特定技術の一つであるIPトレースバック技術の概要を述べ，次いで，東芝が提案するハイブリッドトレースバック方式について述べる。

2　IPトレースバック技術の概要

2.1　IPトレースバック技術

IPトレースバック技術とは，一般にIPパケットの送信元アドレスが詐称されたとしても，発信源を特定できる技術の総称である。IPトレースバック技術は基本的に，注目したトラフィックに対して，そのトラフィックを中継したルータがどのインタフェースからどのインタフェースに中継したかを報告する機構を用いる。これにより，発信源のIPアドレスが詐称されたとしても，攻撃経路のルータを順次たどることにより，原理的には発信源を突き止めることが可能である。IPトレースバック技術は，近年盛んに研究がなされており，様々な方式が提案されてきている。そこで当社は，IPトレースバック技術を以下のように分類した[(1)]（**図1**）。

⑴　受動的トレースバック方式（Passive Traceback）
　追跡者（Tracer）の意図に関係なく実施されるトレースバック方式で，ルータなどが自律的に，攻撃パケットのあて先アドレスに追跡情報を報告する。追跡者は，基本的に送信されてくる追跡情報を解析することで，攻撃経路や発信源の特定を行う。

⑵　能動的トレースバック方式（Active Traceback）
　追跡者から要求が出たときに初めて実施されるトレースバック方式（追跡者が主体となって行う方式）で，発信源追跡のためのコミュニケーションを行うことで，詳細で即時性のある発信源追跡を可能にする。

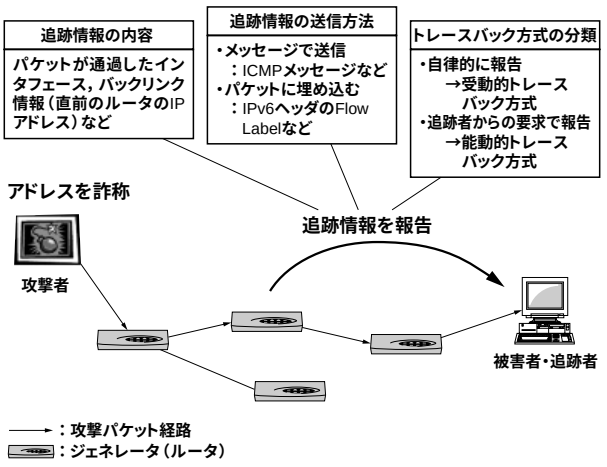

図1.IPトレースバック技術 ― 攻撃パケットの経路に存在するルータなどのネットワーク機器が追跡情報を報告する。
IP traceback technology

2.2 IPトレースバック技術の要求条件

IPトレースバック技術を実現しようとする場合，以下の要求条件を満たすことが望ましいと考える。特に，実際のネットワークにおいて発信源追跡を実施するためには，発信源追跡の処理によるネットワークへの負荷をいかに軽減できるかが重要である。

⑴ 有用性　継続中の攻撃を検知したとき，確実かつ効率的に攻撃の発信源を特定できること
⑵ 耐悪用性　IPトレースバック技術を悪用した攻撃を阻止できること
⑶ 既存ネットワークとの親和性　IPトレースバック技術を採用していない通信機器（ルータなど）が追跡経路中にあっても，追跡が継続して行えること
⑷ 低負荷性　ネットワークに過負荷を与えることなく，発信源追跡を実現できること
⑸ 経済性　発信源追跡環境の構築と運用において，管理コストが大きくならないこと
⑹ 運用性　発信源追跡実施時において，人間系による関与の度合いが少ないこと

2.3 ICMP Traceback Messages

受動的トレースバック方式において，追跡情報を送信する方式は大きく二通りある。通過する通常のパケットの未使用ヘッダ内に断片的に追跡情報を挿入するマーキング方式と，一つの追跡情報を通常のパケットとは別のパケットで送信するメッセージ方式である。

現在，受動的トレースバック方式におけるメッセージ方式の標準規格として，ICMP（Internet Control Message Protocol）[2] Traceback Messages[3]がある。この規格の仕様策定作業は，国際標準化団体であるIETF（The Internet Engineering Task Force）のICMP Traceback（以下，itraceと略記） Working Groupにおいて進められている。この方式（以下，itrace方式と言う）は，インターネット制御用プロトコルのICMPメッセージを利用して，パケットの経路上に位置するルータなどのネットワーク機器から追跡情報をパケットのあて先に送信するというものである。この追跡情報を生成するネットワーク機器は，ジェネレータ（Generator）と呼ばれる。ジェネレータは，通過パケットに対する追跡情報を，ある一定の確率に基づいて自律的に生成する。このため，追跡者が発信源を追跡したいときに追跡できないばかりか，追跡したいパケットの種類を明示的に指定することができないという問題がある。この問題は，受動的トレースバック方式全般に当てはまると言える。

当社では，これらの問題を解決するために，従来型のトレースバック技術に加えて，追跡者の意図を反映する手段（能動的トレースバック方式）を組み合わせたハイブリッドトレースバック方式[1, 4]を提案し，この方式を実現するためのコンポーネントを試作した。開発した試作システムは，侵入検知・防止（Intrusion Detection and Prevention）システムなどの上位アプリケーションが発信源追跡に利用可能な構成としている。

3 ハイブリッドトレースバック方式

3.1 ハイブリッドトレースバック方式の概要

itrace方式などに代表されるこれまでのトレースバック方式は，受動的トレースバック方式がほとんどであった。受動的トレースバック方式だけではその性質上，発信源追跡の正確性や運用管理面において問題があるため，当社では，この方式に加えて能動的トレースバック方式を組み合わせたハイブリッドトレースバック方式の概念モデルを提案し，試作システムを開発した。ハイブリッドトレースバック方式の概要を**図2**に示す。

能動的トレースバック方式は詳細な発信源追跡処理が可能であるが，本来の通信パケット以外に新たにパケットを集中的に生成してしまうため，ネットワーク負荷の原因となってしまう。そのため，当社は，実際の発信源追跡の処理自体は低負荷な受動型トレースバック方式を主体とする方法を用い，詳細な発信源追跡時には能動的トレースバック方式を実施することにした。これにより，低負荷で精度の高い発信源追跡を実現するものである。

ハイブリッドトレースバック方式を用いることにより，以下のような効果が期待できる。

⑴ 効率化　発信源追跡の開始地点を指定し，そこからの詳細な発信源追跡が可能となる。攻撃者に，より近い位置から発信源追跡を開始することができる。

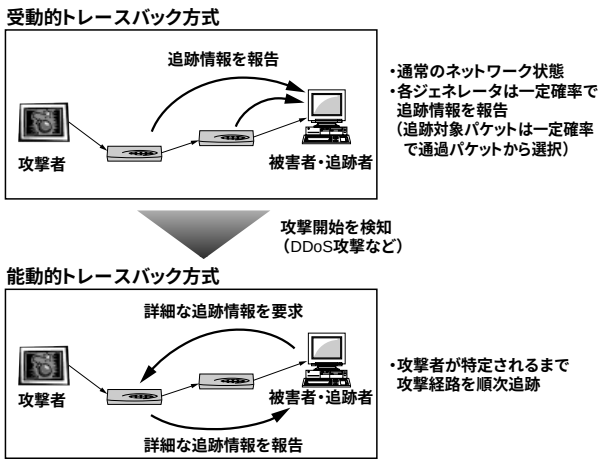

図2. ハイブリッドトレースバック方式 ― 通常時には受動的トレースバック方式を実行し，攻撃検出時には能動的トレースバック方式に切り替えて詳細な発信源追跡を行う。
Hybrid traceback scheme

⑵ 負荷軽減　発信源追跡の開始時期を追跡者が任意に設定することが可能となる。また，通常時に流通させなければならない受動的トレースバック方式によるトラフィック量を制御し，減少させることができる。

⑶ 経済性　発信源追跡自体は受動的トレースバック方式をそのまま利用することによって，実装と配置にかかるコストを削減することができる。

3.2 ハイブリッドトレースバックシステム

当社が開発したハイブリッドトレースバックシステムの構成を説明する。ネットワーク上には複数のジェネレータが配置される。各ジェネレータは，それぞれ能動的トレースバック方式（3.3節で説明するアクティブトレースバックプロトコル）と，受動的トレースバック方式（itrace方式など）を搭載する。追跡者は，実際に発信源追跡処理を実行するものであり，被害者（Victim：攻撃の対象となるもので，主に攻撃パケットのあて先アドレスの機器）が所属するネットワークに配置される。

ジェネレータが実装する受動的トレースバック方式は，任意の方式を採用してよく，また複数であってもよい。実際の発信源追跡に利用する方式の選択は，追跡者とジェネレータとの間で交渉を行い，決定する。このため，従来の受動的トレースバック方式を活用することが可能である。

また，追跡者は各自律システム（Autonomous System）に存在する。これら追跡者どうしは，相互に代理追跡処理を依頼することが可能である。これにより，追跡処理の分散処理やネットワーク的に到達できない箇所への発信源追跡処理が可能となる。

試作システムにおける具体的なトレースバック方式は，受動的トレースバック方式としてitrace方式を採用した。能動的トレースバック方式については，3.3節で記述するアクティブトレースバックプロトコルを開発した。

3.3 アクティブトレースバックプロトコル

アクティブトレースバックプロトコル（Active Traceback Protocol）[5]は，明示的に追跡情報の要求を送信する必要があることと，実装や配置によるコストを削減する意味から，既存の提案方式に沿うように考えて，ICMPを元にしたメッセージ方式のプロトコルとした。これは，試作システムが採用した受動的トレースバック方式であるitrace方式との親和性をも併せ考えたものである。

アクティブトレースバックプロトコルは，ICMPのメッセージフォーマットのMESSAGE BODYの中にTLV（Tag-Length-Value）形式でメッセージを格納する。アクティブトレースバックプロトコルで規定する主なメッセージを以下に示す。

⑴ 開始要求メッセージ（Begin Trace）　追跡者がジェネレータに対して能動的トレースバック処理の開始を要求するメッセージ。

⑵ 停止メッセージ（End Trace）　追跡者がジェネレータに対して開始要求メッセージにより開始された能動的トレースバック処理の停止を通知するメッセージ。

⑶ 拒否メッセージ（Deny Trace）　ジェネレータが追跡者から送信された開始要求メッセージを拒否するときに送信するメッセージ。

⑷ 能力調査要求メッセージ（Capability Query）　ジェネレータに実装されている受動的トレースバック方式を問い合わせるメッセージ。

⑸ 能力調査応答メッセージ（Capability Reply）　能力調査要求メッセージに対する応答を追跡者に送信するメッセージ。ジェネレータが実装している受動的トレースバック方式を送信する。

⑹ 代理追跡依頼メッセージ（Delegate Active Trace）　追跡者が，別の追跡者に対して代理の追跡を依頼するときに送信するメッセージ。依頼元の追跡者を依頼元追跡者（Original Tracer），依頼先の追跡者を代理追跡者（Proxy Tracer）と呼ぶ。

⑺ 代理追跡受諾メッセージ（Accept Delegation）　代理追跡者が代理追跡依頼メッセージを受諾するときに送信されるメッセージ。

⑻ 代理追跡拒否メッセージ（Deny Delegation）　代理追跡者が代理追跡依頼メッセージを拒否するときに送信されるメッセージ。

3.4 ハイブリッドトレースバック方式のプロセス

ハイブリッドトレースバック方式は，以下のプロセスを実施する。基本的には，監視プロセス後に要求・応答プロセスが複数回実施される。能力調査プロセスと代理追跡プロセスは，必要な場合に適宜実施される。なお，(1)，(2)のプロセスは受動的トレースバック方式，(2)，(3)，(4)のプロセ

スは能動的トレースバック方式(試作システムではアクティブトレースバックプロトコル)により実行される。

⑴　監視プロセス　　通常のネットワーク利用時に実施されるプロセスである。従来の受動的トレースバック方式により，追跡情報が送信される。追跡者はこの追跡情報を監視し，攻撃検知した場合に以降のプロセスへ移行する。

⑵　要求・応答プロセス　　ハイブリッドトレースバック方式の中心となるプロセスである。追跡者が特定のジェネレータに対して，詳細な情報の送信を要求するときに実施される。要求を受けたジェネレータは，より詳細な追跡情報を返信する(**図3**)。

試作システムでは，応答処理に受動的トレースバック方式であるitrace方式を利用している。開始メッセージとして，itrace方式の追跡情報生成確率の変更(追跡行為のパラメータを変更)依頼を通知することで，より詳細な情報の取得を可能としている。また，このプロセス開始時に選択されるジェネレータは，監視プロセス時に送信してきたジェネレータの中で，ネットワーク距離的にもっとも遠いジェネレータとする。これにより，能動的トレースバックを実施する回数を削減することが可能である。

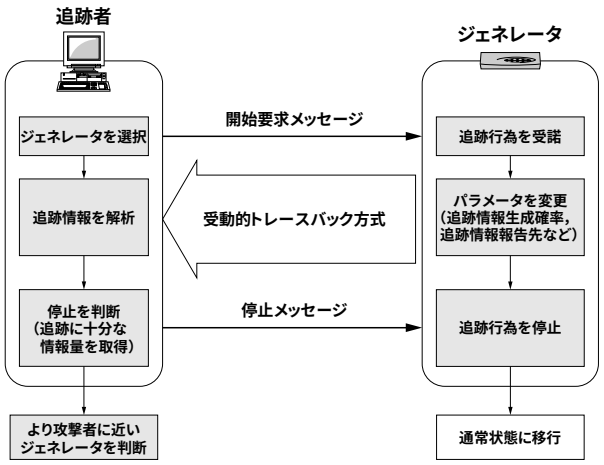

図3．要求・応答プロセス ― 追跡者が特定のジェネレータに対して，追跡情報の送信を要求する。

Request-response process

⑶　能力調査プロセス　　追跡者が，ジェネレータのトレースバック能力を調査するときに実施される。要求・応答プロセスを実施する前に，ジェネレータが実装している受動的トレースバック方式を調査し，追跡情報の送信手段を交渉することを目的とする。

⑷　代理依頼・応答プロセス　　追跡者からネットワーク的に到達できない場所(ファイアウォールやＮＡＴ(Network Address Translation)を越えたネットワークなど)に対して発信源追跡を継続して行うために，ネットワーク境界に位置している別の追跡者に対して代理追跡を依頼するときに実施される。

4　あとがき

ここでは，ハイブリッドトレースバック方式の概要について述べた。通常時はネットワーク負荷の少ない従来の受動的トレースバック方式を行い，攻撃時には能動的トレースバック方式により詳細な発信源追跡処理を行うことで，ネットワーク負荷軽減と効率性や正確性を両立させた発信源追跡手段を実現した。今後，試作システムの評価実験を行い，その有効性について検証していきたい。

謝　辞

この論文は，通信・放送機構が実施する2001年度及び2002年度 高度通信・放送研究に係る委託研究“ 個人ユーザ向けの常時接続端末におけるセキュリティ保護技術に関する研究開発 ”の委託を受け，当社が研究開発しているシステムに関するものである。

関係者各位のご支援に感謝する。

文　献

⑴　池田竜朗，ほか．“ ハイブリッドスキームを利用したIPトレースバック技術 ”．2002年暗号と情報セキュリティシンポジウム予稿集．電子情報通信学会情報セキュリティ研究専門委員会．2002，p. 958－990.

⑵　J. B. Postel．“ Internet Control Message Protocol ”，IETF RFC792，1981. <http://www.ietf.org/rfc/rfc0792.txt>，(accessed 2003-04-25).

⑶　S. Bellovin，et al．“ ICMP Traceback Messages ”，Internet-Draft. <http://www.ietf.org/internet-drafts/draft-ietf-itrace-04.txt>，(accessed 2003-04-25).

⑷　山田竜也，ほか．“ 発信源追跡のためのハイブリッドトレースバック方式の提案 ”．コンピュータセキュリティシンポジウム2002論文集．情報処理学会コンピュータセキュリティ研究会．2002，p.23－28.

⑸　Tatsuya YAMADA．“ Active Traceback Protocol ”．Internet-Draft. <http://www.ietf.org/internet-drafts/draft-yamada-active-trace-00.txt>，(accessed 2002-11-01，expires 2003-04).

池田　竜朗　IKEDA Tatsuro

e-ソリューション社 SI技術開発センター SI技術担当。
情報セキュリティ技術の研究・開発業務に従事。情報処理学会会員。
Systems Integration Technology Center

山田　竜也　YAMADA Tatsuya

e-ソリューション社 SI技術開発センター SI技術担当。
IPネットワーク技術の研究・開発業務に従事。
Systems Integration Technology Center