5H−04　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　〜IPトレースバックに関する一考察〜

大岸　伸之†, 山崎　博司†, 池田　竜朗††, 森尻　智昭††, 才所　敏明†
†東芝情報システム(株), ††(株)東芝 SI技術開発センター

1. はじめに

近年，インターネットを通して提供されるサービスに対して，DoS/DDoS(Distributed DoS)攻撃に代表される大規模かつ巧妙な攻撃による被害が増加している．

家庭などにおいても常時接続環境が普及しつつある現在，個人ユーザのマシンがDoS攻撃などにさらされることや，所有者の知らない間に攻撃の踏み台となるなどの可能性が高まってきている，このため，早急にこれらの攻撃に対する有効なセキュリティ対策が求められている．

2. IPトレースバック技術

DoS/DDoS攻撃に対処するためには，攻撃に利用されるIPパケットの発信源を特定することが一つの有効な対抗策として考えられている．しかしながら発信源を特定するための始点アドレスを詐称された場合，発信源を特定することは困難である．このような始点アドレスを詐称された場合においても，攻撃パケットの発信源を特定可能な技術がIPトレースバック技術である．

3. IPトレースバック技術体系[1]

IPトレースバック技術は，以下に示す観点から体系化を行うことが可能である．本稿ではこれらをIPトレースバックの技術コンポーネントと呼ぶこととする．IPトレースバック技術は，各コンポーネント(に属する基礎技術)の組み合わせにより構成される．

Security for Regular-Connected Personal Terminal - IP Tarceback -
Nobuyuki OHGISHI†, Hiroshi YAMAZAKI†,
Tatsuro IKEDA††, Tomoaki MORIJIRI††,
Toshiaki SAISHO†
†TOSHIBA Information Systems Co., 2-1, Nisshin-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa, JAPAN
††TOSHIBA Co., SI Technology Center, 3-22, kata-machi, Fuchu-shi, Tokyo, JAPAN

(1) トレースバックスキーム

トレースバックスキーム・コンポーネントは，トレースバック自体のスキーム形態であり，そのスキームとして主に**受動型トレースバック方式(Passive Traceback)**と**能動型トレースバック方式(Active Traceback)**がある．

受動型トレースバック方式は，パケット通過経路上に存在するジェネレータ(トレースバック機能を有したルータなどのネットワーク通信機器)が，通過する任意のパケットに対して自律的に追跡情報を生成する方式である．それに対して能動型トレースバック方式は，ジェネレータ以外のエンティティ(要求者:Requester)からトレースバックの要求を行う方式である．

(2) 追跡情報提示スキーム

追跡情報提示スキーム・コンポーネントは，トレースバックで利用する情報(追跡情報)を，トレースバックを行うエンティティに対して提示するスキーム形態である．その主な形態としては，**ログ保存方式**と**追跡情報提供方式**がある．

ログ保存方式では，ジェネレータは生成した追跡情報を，ログとして保存する．追跡者は，この追跡情報のログを解析することにより，攻撃パケットの通過経路を構築し，最終的に攻撃者を特定する．追跡情報提供方式は，生成した追跡情報をジェネレータが追跡者に適宜提示するものである．

(3) 追跡情報キャリア

追跡情報キャリア・コンポーネントは，追跡情報を送信する媒体の形態であり，現在のところ提案されている主なものとしては，ICMP(Internet Control Message Protocol)などを利用して別経路により送信する方法であるメッセージング方式[2]と，IPパケットそのものに追跡情報を付加する方法であるマーキング方式[3]がある．

(4) 追跡対象パケット識別

追跡対象パケット識別・コンポーネントは，トレースバックを行うときには，追跡対象パケットであることを識別する形態である．追跡対象パケットの一部を追跡情報キャリアに付随させるなどの方法がある．

4. ハイブリッドスキームを利用したIPトレースバック・モデル

前述の通り，IP トレースバック技術は各コンポーネントの組み合わせにより構成される．これらのコンポーネントや，これらのコンポーネントから構成される単体でのIPトレースバック技術は，実運用を考慮したとき，攻撃検出の可能性，既存ネットワークとの整合性，将来的なサービスとの競合といった面等でそれぞれに課題を有している．そこで，2種類のトレースバックスキーム(受動型／能動型トレースバック方式)を組み合わせることで，単体のトレースバック方式を利用するのに比べて，各々の方式を補完し，より効率的なトレースバックを行うことが可能となる．スキームの簡単な流れを以下に示す．

【フェーズ 1:トレースバック要求】

依頼者は，受動型トレースバック方式によって攻撃の兆候を検知した際，能動型トレースバック方式の始点となる初期ジェネレータを決定する．

【フェーズ 2:追跡情報通知】

初期ジェネレータは，依頼者から指定された攻撃発信元から送られてくる追跡対象パケットの直前エンティティの情報である直前リンク情報を依頼者に通知する．

【フェーズ 3:トレースバック】

依頼者は，追跡対象パケットの内容から攻撃パケットかどうかを判断する．攻撃パケットと判断した場合，初期ジェネレータから通知された直前リンク情報を元に攻撃者を特定する．

直前リンク情報が別のジェネレータを指している場合は，そのジェネレータを初期ジェネレータとして再度能動型トレースバック方式を行い，攻撃者を特定していく．

受動型トレースバック方式で攻撃を検知し，攻撃者のおよその位置を推測し，能動型トレースバック方式で詳細な情報を入手することで，通常時にネットワークを流れるトレースバックに関する通信パケットを最小限に抑えることが可能となる．また，受動型トレースバック方式単体に比べて，より詳細な追跡行為を行うことができる．

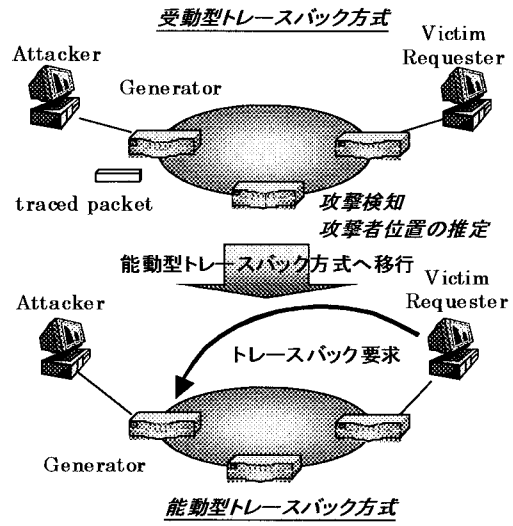

図 1：ハイブリッドスキーム・トレースバック

謝辞

本発表は，通信・放送機構が実施する平成 13 年度高度通信・放送研究に係る委託研究「個人ユーザ向け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．

参考文献

[1] 大岸，池田他，“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”,SCIS2002 予稿集，2002/1

[2] Steven M. Bellovin and Marcus D. Leech: ICMP Traceback Messages,Internet Draft , draft-ietf-itrace-00.txt(2000)

[3] 門林雄基，大江将史「IP トレースバック技術」情報処理 2001 年 12 月号