# 第 X 部

# IP トレースバック・システムの研究開発

# 第 10 部
# IP トレースバック・システムの研究開発

## 第 1 章　はじめに

Traceback ワーキンググループは IP Traceback などに代表されるトレースバック技術に関する基礎研究およびトレースバック技術の実用化に取り組むワーキンググループである。

今年度は、AS 内における sFlow を用いた AS 境界探査トレースバックシステムや、Forwarding Data Base 検索とハッシュベース IP トレースバックのハイブリッド型の発信源探査トレースバックシステム、また計測用の新たな Bloom Filter 方式の研究などを論文としてまとめ、研究会や国際会議などで発表を行った。また、トレースバック技術の標準化に向けて IETF への参加や JANOG、Internet Week などで発表を行った。さらには、WIDE バックボーン内での境界探査トレースバックシステムの実証実験に向けて順次各 NOC にトレースバックプローブを設置中である。

トレースバック相互接続システムの開発もほぼ終わり、NICT の委託研究で行っている「トレースバック技術の実用化に向けた研究」に携わっている協力会社のトレースバックシステムとの相互接続試験も無事成功した。

2008 年度にトレースバックシステム相互接続アーキテクチャである InterTrack の実装を公開を予定しており、現在リリースに向けてソースコードの整理を行っている。また、2008 年度は今まで日本語で記述してきた設計書やマニュアルなどを英語化し、ソースコードの公開と同時に公開する予定や、個人名ドラフトとしてインターネットドラフトの執筆も予定している。

## 第 2 章　2007 年度の研究発表

2007 年度に行った研究発表は次の通りである。

- JANOG 19 にて門林発表 [192]
- APAN 23 Manila にて櫨山発表 [54]
- WIT 2007 にて松本発表 [198]
- JWIS 2007 にて櫨山、Gregory 発表 [18, 55]
- Internet Week 2007 にて門林発表 [191]

次に、各研究発表の概要を掲載する。本文に関しては各参考文献を参照されたし。

### 2.1 IP トレースバックとその応用 JANOG 19

2007 年 1 月 25 日（木）、26 日（金）に沖縄県那覇市沖縄ハーバービューホテルで開催された JANOG 19 meeting にて門林雄基（奈良先端科学技術大学院大学）と許先明（株式会社ブロードバンドセキュリティ）によって発表が行われた。発表の詳細に関しては文献 [192] を参照されたし。以下、発表概要である。

#### 2.1.1 概要

ソースアドレスが詐称された攻撃の発信源を探査する技術「IP トレースバック」が実用化をむかえている。本発表では奈良先端大で開発した IP トレースバック技術を使った実証実験について報告する。さらに、オペレータからみた IP トレースバックの可能性、課題、法的側面からみた課題などについて、これまで明らかになっていることについて整理し、JANOG での議論の礎としたい。

### 2.2 A brief report of IP traceback experiment with Japan ISPs

2007 年 1 月 22 日（月）から 26 日（金）にフィリピン、マニラの Edsa-Shangri La Hotel で開催された 23rd APAN Meeting 内 Security Workshop にて櫨山寛章（奈良先端科学技術大学院大学）が発表を

行った。発表の詳細に関しては文献 [54] を参照されたし。以下、発表概要である。

#### 2.2.1 概要

IP traceback is a tracking technique the true forwarding path of packets/flows, even if the target packet is source-spoofed. Now we are trying to deploy a hash based IP traceback and an ineter-AS traceback exchange architecture in the real internet, with 3 Japan commercial ISPs and WIDE backbone. In this presentation, we breifly present our activity.

### 2.3 ネットワークトラフィック分析のための Iterative Bloom Filter の提案

2007 年 6 月 25 日（月）、26 日（火）に鳥取環境大学（鳥取県鳥取市）で開催された第 8 回インターネットテクノロジーワークショップ（WIT 2007）で松本義秀（奈良先端科学技術大学院大学）が発表を行った。発表の詳細に関しては文献 [198] を参照されたし。以下、発表概要である。

#### 2.3.1 概要

ネットワークトラフィック分析の利用例の 1 つである Hash-Based IP トレースバックにおいて、Bloom Filter（BF）を用いることで、入力パケットの Hash 値の重畳により記憶空間の節約と処理の高速化が可能である。しかし、BF に対し同一 Hash 値を複数登録した場合は重畳されるため、登録回数による分析は不可能になる。そこで、Hash 値の登録回数を記録できる Counting Bloom Filter（CBF）2）の利用が考えられるが、登録回数の記憶領域を事前に確保する必要があり、偏りのあるトラフィックに対しては記憶効率が悪く、結果的に false positive の確率が上がることになる。本論文は、BF のアルゴリズムを拡張した、Iterative Bloom Filter（IBF）を提案する。IBF の基本的な考え方は、入力 Hash 値が重複した場合には Hash 関数の個数を増加させることで、同じ BF の配列内に重複回数の情報を追加して埋め込むことにある。また、参照処理においては登録されている Hash 関数の個数から、重複数の推定値を算出する。IBF は、CBF に比べ正確な登録回数を算出できないが、登録回数の記憶領域の見積もりが不要であり、基本的にはカウンタのオーバフローが発生しないという特徴を持つ。本論文では、CBF、IBF の特性を比較し、IP トレースバックだけではなく、偏りのある入力値を持つアプリケーションにおいても適用が可能であることを示す

### 2.4 Message Forwarding Strategies for Inter-AS Packet Traceback Network

2007 年 8 月 6 日（月）、7 日（火）に早稲田大学で開催された 2nd Joint Workshop on Information Security（JWIS 2007）で櫨山寛章（奈良先端科学技術大学院大学）が発表を行った。発表の詳細に関しては文献 [55] を参照されたし。以下、発表概要である。

#### 2.4.1 概要

Inter-domain traceback techniques and architecture has been long wanted to locate the ingress point of a DDoS attack on the intradomain backbone network, to discover the source Autonomous Systems (ASes) of address spoofed packets, and/or to detect suspected nodes on local subnets. We have proposed an inter-domain traceback architecture, called InterTrack, which designed to meet the current routing/network operation manners and policies. In this paper, we try to explain out message forwarding strategies of our inter-domain traceback architecture with several pseudo codes, and we explore the ways of constructing an Internet-wide packet traceback network both in-band and out-band while considering deployment models of InterTrack.

### 2.5 Message Forwarding Strategies for Inter-AS Packet Traceback Network

2007 年 8 月 6 日（月）、7 日（火）に早稲田大学で開催された 2nd Joint Workshop on Information Security（JWIS 2007）で Blanc Gregory（奈良先端科学技術大学院大学、Ecole Supérieure d'Informatique Electronique Automatique）が発表を行った。発表の詳細に関しては文献 [18] を参照されたし。以下、発表概要である。

#### 2.5.1 概要

DDoS attacks have created a need for components that not only filter out these malicious flows

but also track these flows back to their source, even if spoofed. To track back over inter-domain, an Autonomous System (AS) has to determine the actual upstream ASes about the targeted flow. Usually, inferring the upstream AS of a flow requires collecting large amount of packets, classifying packets to unique flows and analyzing the upstream ASes of each flow. This method consumes too much storage and wastes much time. To reduce such costs, we propose a new method for inferring flow direction using flow sampling techniques. Through several experiments and improvements, we finally developed a Flow Direction Inferring (FDI) algorithm and an FDI system which allows an AS to determine the upstream AS and/or downstream AS of a single packet exported by sFlow on a Border Router (BR), without classifying packets to a flow.

### 2.6 IP トレースバックとその応用 JANOG 19

2007 年 11 月 19 日（月）から 22 日（木）まで秋葉原コンベンションホールで開催された Internet Week 2007 内の The Internet Operations Workshop にて門林雄基（奈良先端科学技術大学院大学）によって発表が行われた。発表の詳細に関しては文献 [191] を参照されたし。以下、発表概要である。

#### 2.6.1 概要

国内で IP トレースバックの技術開発を続けてきた結果、ドメイン内やドメイン間での障害対応に活用できる見通しが立ってきました。ここではオペレーションの視点から、IP トレースバックの現時点での活用方法を提案します。

## 第 3 章　おわりに

2007 年度の Traceback ワーキンググループの活動は IP トレースバック相互接続アーキテクチャを通した相互接続試験や単一ドメイン内で利用するトレースバックシステムの開発を行った。現状としては、DNS リフレクションやボットネットなどの踏み台攻撃への対応、パケットの秘匿性の確保や高速広帯域ネットワークへの対応、方式のコストパフォーマンスなど IP トレースバックの実用化に向けてはまだまだ研究として取り組むべき課題が残されている。

2008 年度の活動予定としては、NICT の委託研究で行う実証実験に向け、北陸リサーチセンター内シミュレーション設備を用いた環境でのデプロイメントシミュレーションや実証実験に向けた予備実験を行う予定である。