# 第 XI 部

# IP トレースバック・システムの研究開発

# 第 11 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。

今年度からは、昨年度までに開発した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 の実証実験を目的とし、NICT 委託研究「トレースバック技術の実用化に関する研究」で別途開発されている IP トレースバックシステムとの相互接続検証、Interop Tokyo 2008 での運用実験、WIDE バックボーンでの IP トレースバック実験の開始などを行っている。

また、2009 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 の実装をオープンソースとして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やドキュメントの英文化を行っている。

## 第 2 章　2008 年度の研究発表

2007 年 1 月から 2008 年 11 月までに行った研究発表は次のとおりである。

- Bloom Filter に関する研究発表
  - IEICE Transactions on Information and Systems, vol. E91-D, No. 5 に論文を投稿し、採録（5 月に出版）
  - APRICOT 2008 TAIPEI にて口頭発表（2 月）
  - コンピュータセキュリティシンポジウム 2008 にて発表（10 月）
- sFlow version 5 を用いたトレースバックシステムに関する研究発表
  - APRICOT 2008 TAIPEI にて口頭発表（2 月）
  - コンピュータセキュリティシンポジウム 2008 にて発表（10 月）
- 相互接続性検証と実証実験に向けた準備に関する研究発表
  - JFIRST ワークショップにて口頭発表（3 月）
  - 電子情報通信学会 IA 研究会 7 月研究会にて発表（7 月）
  - JAIPA ICT 沖縄フォーラムにて発表（7 月）
  - 26th APAN meeting Qweenstown にて発表（8 月）
  - 電子情報通信学会 IA 研究会 9 月研究会にて発表（9 月）

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。

## 第 3 章　ネットワークトラフィック計測に対して効果的な Bloom Filter の応用

インターネットで用いられているプロトコルやネットワークに影響を与えず導入可能なトレースバック技術としてハッシュダイジェスト型 IP トレースバックは数あるトレースバックの方式提案の中で実用化が見込まれている。ハッシュダイジェスト型 IP トレースバックではパケットのハッシュ値を Bloom Filter と呼ばれるメモリマップにパケットの通過記録をバイナリデータとして記録する。Bloom Filter は高い記憶容量と低い誤検知率を有するが、同一ハッシュ値をもつ同種のパケットがいくつ通過したかなどのカウンティング機能を有していない。Bloom Filter が使用するメモリ量を増加せずに高いカウンティング機能を持たせるため Adaptive Bloom Filter の研究開発を行った。本章では、IEICE Transactions on Information and Systems, vol. E91-D, No. 5 に採録された研究論文の概要を掲載する。

### 3.1 Adaptive Bloom Filter: Space Efficient Counting Algorithm for Unpredictable Network Traffic

IEICE Transactions on Information and Systems, vol. E91-D, No. 5 にトレースバックやトラフィック計測向けの Bloom Filter の応用アルゴリズムに関しての論文を投稿し、採録された。論文の詳細に関しては文献 [107] を参照されたし。以下、発表概要である。

#### 3.1.1 概要

The Bloom Filter (BF), a space-and-time efficient hash-coding method, is used as one of the fundamental modules in several network processing algorithms and applications such as route lookups, cache hits, packet classification, per-flow state management or network monitoring. BF is a simple space-efficient randomized data structure used to represent a data set in order to support membership queries. However, BF generates false positives, and cannot count the number of distinct elements. A counting Bloom Filter (CBF) can count the number of distinct elements, but CBF needs more space than BF. We propose an alternative data structure of CBF, and we called this structure an Adaptive Bloom Filter (ABF). Although ABF uses the same-sized bit-vector used in BF, the number of hash functions employed by ABF is dynamically changed to record the number of appearances of a each key element. Considering the hash collisions, the multiplicity of a each key element on ABF can be estimated from the number of hash functions used to decode the membership of the each key element. Although ABF can realize the same functionality as CBF, ABF requires the same memory size as BF. We describe the construction of ABF and IABF (Improved ABF), and provide a mathematical analysis and simulation using Zipf's distribution. Finally, we show that ABF can be used for an unpredictable data set such as real network traffic.

## 第 4 章　sFlow version 5 を用いたトレースバックシステムの研究開発

インターネットで用いられているプロトコルやネットワークに影響を与えず導入可能なトレースバック技術としてハッシュダイジェスト型 IP トレースバックは数あるトレースバックの方式提案の中で実用化が見込まれている。しかしながら、ハッシュダイジェスト型 IP トレースバックではポートミラーなどであるドメイン内部を通過するすべてのパケットの通過記録を取得することを前提としており、その高い追跡精度とのトレードオフとして導入コストおよび運用コストが高いことが懸念されている。Traceback ワーキンググループでは導入コストおよび運用コストの低減を目指し、sFlow version 5 を用いた AS 内部向けトレースバックシステムの研究開発を行った。本章では、各研究発表の概要を掲載する。

### 4.1 sFlow-based AS Border Traceback

2008 年 2 月 20 日から 29 日に台北にて APRICOT 2008 Taipei、Conference, Sequrity Service にて櫨山寛章（奈良先端科学技術大学院大学）が sFlow version 5 を用いた単一 AS 向けトレースバックシステムについて発表を行った。発表の詳細に関しては文献 [63] を参照されたし。以下、発表概要である。

#### 4.1.1 概要

単一 AS 内におけるトレースバック技術として、sFlow version 5 を用いたトレースバックシステムを開発した。開発を行う上で、単純に sFlow version 5 を収集するだけではサンプリングされたパケットの転送元 AS および転送先 AS を正確に判定できないことがわかり、研究の結果、送信元アドレス偽装されたパケットに関しても正確に転送元 AS および転送先 AS を特定できるアルゴリズムを開発した。この研究成果に関して APRICOT 2008 Taipei の Security Services トラックにて口頭発表を行い、環太平洋の ISP オペレータらから貴重な意見を得ることができた。

### 4.2 sFlow を用いた IP トレースバック手法の評価

2008 年 10 月 8 日から 10 月 10 日に沖縄コンベン

ションセンターで開催されたコンピュータセキュリティシンポジウムにて村越優喜（奈良先端科学技術大学院大学）が、sFlow を用いたトレースバックシステムを AS 内トレースバックシステムとして用いた場合の AS 間トレースバックの成功率に関する予備実験の結果について発表を行った。発表の詳細に関しては文献 [233] を参照されたし。以下、発表概要である。

#### 4.2.1 概要

DDoS 攻撃への対策手法の一つとして、送信元 IP 詐称パケットの攻撃元の特定も行える IP トレースバック技術があり、なかでもパケットのハッシュ値のみを記録するダイジェスト方式がその追跡精度と安全面の両面から実用的であると期待されている。しかし、ダイジェスト方式ではポートミラーなどで Autonomous System 内を通過するすべてのパケットを収集し記録することが期待されているため、大規模なネットワークでは設置コストが高い。そこで本論文では、パケットサンプリング技術である sFlow に着目し、sFlow を用いることにより、一定の追跡精度を維持したままダイジェスト方式を用いた IP トレースバックにとって効率的なパケット収集を構築できるか否かを検討する。本論文では、sFlow でサンプリングしたパケットを追跡用のパケットダイジェストとして用いるダイジェスト方式 IP トレースバックシステムを実装し、この実装のみを用いた場合の IP トレースバックの成功率及びシステムの負荷について実験を行った。

## 第 5 章　インタードメイン・トレースバックシステムの実証実験に向けた相互接続検証と運用実験

平成 21 年度に計画している ISP 環境におけるインタードメイン・トレースバックシステムの実証実験に向けて、相互接続性検証や北陸リサーチセンター内大規模検証施設（StarBED）を用いた実験、および国内 AS 網へのトレースバックシステム導入シナリオと導入シナリオ別の追跡率、メッセージ伝搬効率に関する研究発表を行っている。本章では、各研究発表の概要を掲載する。

### 5.1 インタードメイン・トレースバックシステムの概要

2008 年 3 月 25 日（火）〜26 日（水）に秋葉原 UDX 4 階 UDX Gallery で開催された日本シーサート協議会 Joint Workshop on Security 2008, Tokyo にて櫨山寛章（奈良先端科学技術大学院大学）がインタードメイン・トレースバックシステムの概要と最新の研究成果について口頭発表を行った。発表の詳細に関しては文献 [223] を参照されたし。以下、発表概要である。

#### 5.1.1 概要

トレースバックの実証実験を進めるべく、NICT 委託研究にて共同研究を行っているテレコムアイザックジャパンとともに、日本シーサート協議会 Joint Workshop on Security 2008, Tokyo にて口頭発表を行った。発表では、平成 17 年度より研究活動を推進してきたトレースバック研究は、平成 20 年度、21 年度に ISP 環境で実証実験を行う予定であることと、その準備として平成 19 年度に行ったトレースバックシステム間の相互接続試験や NICT 北陸リサーチセンター内大規模シミュレーション施設で行ったシミュレーション実験に内容について説明を行い、平成 20 年度、21 年度の実験概要を説明し、実験参加者を募った。

### 5.2 Telecom-ISAC Japan の御紹介：トレースバック研究のご紹介 A：大規模 Simulation

2008 年 7 月 11 日に健康文化村カルチャーリゾートフェストーネで開催された JAIPA 沖縄 ICT フォーラムで櫨山寛章（奈良先端科学技術大学院大学）が Telecom-ISAC Japan の紹介の中で、共同研究を行っている Telecom-ISAC Japan トレースバック分科会とともにトレースバック研究に関して口頭発表を行った。発表の詳細に関しては文献 [222] を参照されたし。以下、発表概要である。

### 5.3 実証実験に向けた IP トレースバックシステム導入シナリオに関する一考察

2008 年 7 月 9 日に品川インターシティで開催されたインターネットアーキテクチャ研究会第 2 回研究会にて櫨山寛章（奈良先端科学技術大学院大学）が、国内インターネット網へのトレースバックシステム

の導入シナリオ別の追跡可能性の変化について発表を行った。発表の詳細に関しては文献 [224] を参照されたし。以下、発表概要である。

#### 5.3.1 概要

我々の研究グループでは IP トレースバックの実用化に向けて平成 20 年度に日本国内の商用 ISP 5 社程度を交えた事前実験、および平成 21 年度に商用 ISP 20 社程度を交えた実証実験を計画している。事前実験および実証実験の準備を行うに至り、効果的な導入 ISP の配置や、何社に協力を仰げば日本国内全体を不完全ながらも網羅できるのかといった疑問が挙がっており、IP トレースバック導入による効果に関し予備調査を行う必要がある。本論文では CAIDA Project の eBGP 観測情報に基づいた国内外 AS 間の接続情報をもとに、国内 AS 網における IP トレースバックシステム導入の効果をシミュレーションにより調査した。調査した結果、国内 AS 上位 5 社に導入すると国内 AS 網に対し 70%以上の追跡可能性を実現でき、また小規模・中規模トランジット AS から IP-TB を導入した場合でも、13 AS に IP-TB が導入されれば国内 AS 網に対する追跡可能性は 50%以上になることが明らかとなった。

### 5.4 A trail of traceback system in Interop Tokyo 2008

2008 年 8 月 4 日から 8 日に Queenstown, Millennium Hotel で開催された APAN 26: Sustainable Networking で櫨山寛章（奈良先端科学技術大学院大学）が Interop Tokyo 2008 にて行った単一 AS 向け IP トレースバックシステムの相互接続検証と運用実験に関して口頭発表を行った。発表の詳細に関しては文献 [62] を参照されたし。以下、発表概要である。

#### 5.4.1 概要

We developed a Hash-based IP traceback system and we had a trial of IP traceback operation in Interop Tokyo 2008 from 11th June to 13th June, 2008. The IP traceback system audited all external links of Interop Tokyo 2008. Triggered by alerts from Intrusion Detection Systems settled in customer side, the IP traceback system traced the actual external path of attacks, even when a target packet was source IP spoofed packet.

### 5.5 Mesh of Trees トポロジにおけるトレースバックメッセージ伝達効率に関する一考察

2008 年 9 月 26 日に機械振興会館で開催されたインターネットアーキテクチャ研究会第 3 回研究会にて宮本大輔（奈良先端科学技術大学院大学）が、国内インターネット網へのトレースバックシステムの導入シナリオ別のメッセージ伝達効率の変化について発表を行った。発表の詳細に関しては文献 [230] を参照されたし。以下、発表概要である。

#### 5.5.1 概要

本論文では、現在のインターネットのトポロジとして知られる Mesh of Trees トポロジにおける、トレースバックにおける追跡メッセージの伝達効率に関する考察を行う。IP トレースバック方式の 1 つである InterTrack は逆探知を行うために送受信する追跡メッセージの数が、トポロジの複雑であればあるほど増加する。そこで、Mesh of Trees トポロジにおいてメッシュを構成するコア AS、ツリーを構成するリーフ AS、及びその中間にあたる中規模 AS にそれぞれトレースバック装置を配備した場合を想定する。その上で、CAIDA の提供する AS 隣接データセットを用い、各 AS 群にトレースバック装置を配備した際における、追跡メッセージ数と追跡可能性について調査を行い、メッセージ伝達効率を観察する。この観察結果に基づき、追跡メッセージの伝達効率が高い配備シナリオについても考察を行う。

## 第 6 章　おわりに

2008 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運用実験を行った。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。

2009 年度の活動予定としては、NICT の委託研究で行う実証実験と連携して WIDE バックボーンでの運用実験を行う予定である。