第 IX 部

IP トレースバック・システムの研究開発

第 9 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、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した。また、情報通信研究機構委託研究「トレースバック技術の実用化に関する研究」にて商用 ISP 15 社を交えて実施されたドメイン間 IP トレースバックの実証実験への協力や、WIDE バックボーンで AS 境界探査トレースバックシステムの運用実験を実施した。

第 2 章　2009 年度の活動

2008 年 12 月から 2009 年 11 月までに行った活動は次の通りである。

- 日中韓における AS 間トレースバック導入シナリオに関する研究発表
  - JWIS2009 にて発表（8 月）
- トレースバック相互接続システム（InterTrack）の研究開発
  - ThinkIT における解説記事（2 月）
  - InterTrack のソースコードの公開（7 月）
  - 商用 ISP 15 社を交えたトレースバック実証実験のプレスリリース（11 月）
  - WIDE バックボーンにおける AS 境界探査型トレースバックシステムの運用

次に、各研究発表の概要を掲載する。各研究発表の本文に関しては各参考文献を参照していただきたい。

第 3 章　日中韓における AS 間トレースバック導入シナリオに関する研究発表

国内での IP トレースバック実証実験（文献 [121]）を進めるにあたり、文献 [125] や文献 [132] において、国内インターネットにどのように AS 間トレースバックシステムを導入すべきかの導入シナリオ検討を昨年度実施した。今年度は、国によって AS 間トレースバックシステムの導入シナリオに違いが出てくるのかを検証するために日本、中国、韓国をケーススタディとして考察を行った。本章では、日本、中国、韓国における AS 間トレースバック導入シナリオを検討した文献 [69] の概要を記載する。論文の詳細に関しては文献 [69] を参照していただきたい。

A Comparative Evaluation of Traceability in CJK Internet

In this paper, we evaluate the traceability in IP traceback systems (IP-TBSs) by deployment simulation. In general, the traceability of attack sources or attack paths is expected to improve with the number of autonomous systems (ASes) participate in such systems. However, since there are various types of AS, such as core AS and leaf AS, the traceability would be affected by the types of network topology and/or the deployment scenario. Herein, we employ 3 types of emulated Internet topologies that resemble the inter-AS topology in China, Japan, and South Korea. We use 4 types of deployment scenarios to estimate the traceability of attack sources and attack paths. On the basis of the obtained results, we discuss the deployment scenario in each network region and demonstrate our scenario used in the field test conducted in the fiscal year 2009.

第 4 章　トレースバック相互接続システム（InterTrack）の研究開発

また、今年度は、WIDE プロジェクトなどでこれまで開発してきたトレースバック相互接続システムである InterTrack のソフトウェアリリースや、情報通信研究機構の委託研究「インターネットにおけるトレースバック技術の研究開発」にて実施された商用 ISP 環境における AS 間トレースバックの運用実験への協力、WIDE バックボーンにおける AS 間トレースバックシステムの運用実験を実施した。

4.1 ThinkIT におけるトレースバック技術の解説

2009 年 2 月に ThinkIT にてトレースバック技術や InterTrack に関する技術解説を行った。詳細は文献 [109] を参照していただきたい。

4.2 InterTrack のソースコードの公開

マニュアルなどの整備を行った後、2009 年 7 月に InterTrack のソースコードを `http://intertrack.naist.jp/` にて公開した。

4.3 商用 ISP 15 社を交えたトレースバック実証実験

2009 年 11 月 26 日に情報通信研究機構委託研究「トレースバック技術の実用化に関する研究」にて商用 ISP 15 社を交えて実施されたドメイン間 IP トレースバックの実証実験に関するプレスリリースが行われた（参考文献 [121]）。

この実証実験では InterTrack を含めたトレースバックシステムを商用 ISP 15 社のバックボーンに設置し、商用 ISP 運用者によるトレースバックシステムを用いたインシデント対応の運用実験が実施された（参考文献 [137]）。

Traceback ワーキンググループでは、この運用実験の一部として実施された「異なるトレースバックシステム間の運用連携」にて、商用 ISP 15 社の環境に設置されたトレースバックシステムと WIDE バックボーンで運用実験を行っている AS 境界探査型 IP トレースバックシステムとの運用連携実験に参加した。WIDE バックボーンで運用実験を行っている AS 境界探査型 IP トレースバックシステムに関しては 4.4 節にて説明する。

4.4 WIDE バックボーンにおける AS 境界探査型 IP トレースバックシステムの運用

本節では、WIDE バックボーンにおける AS 境界探査 IP トレースバックシステム（InterTrack）の運用実験に関して報告する。図 4.1 は WIDE バックボーン内に設置した InterTrack の設置概略図である。設置は、藤沢 NOC の AI3 に向けた対外線、NTT 大手町 NOC の Verio に向けた対外線、KDDI 大手町 NOC の Los Angelos NOC 行き（LAIX、PIAX 対外線）と DIX-IE に向けた対外線を監視する形で都

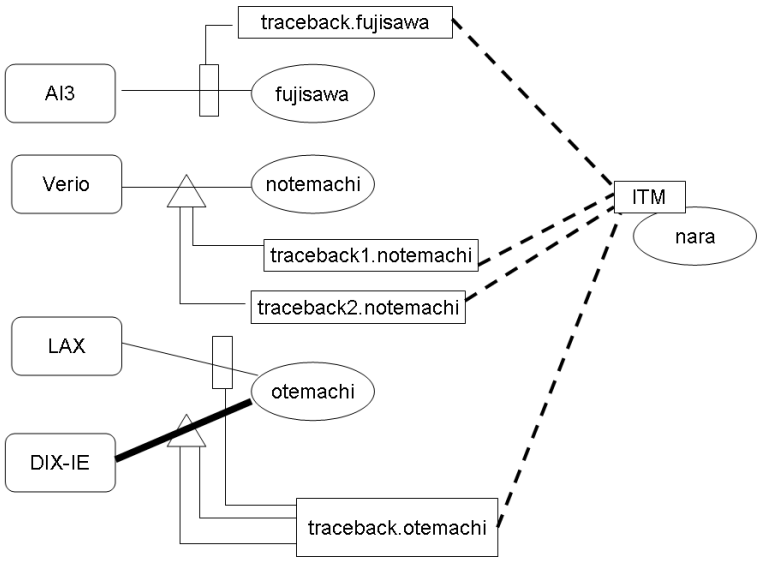

図 4.1.　WIDE バックボーンにおける境界探査型 IP トレースバックシステムの設置図

合 4 台の PC を設置し、奈良 NOC 内にコントロールサーバ用 PC を設置した。

4.4.1 対外線監視用 PC 設置

まず対外線監視用 PC の構成を説明する。AI3 対外線は NOC のレイヤ 2 スイッチから双方向ミラーでトラフィックを取得し、Proside 社 AmazeBlast 1 台（traceback.fujisawa）にて監視している。Verio 対外線は Finisar 社のシングルモードファイバー用光スプリッターを挟み込み、Intel 社の 1000Base-LX カードを挿した Proside 社 AmazeBlast 2 台（traceback1.notemachi、traceback2.notemachi）にて双方向トラフィックを監視している。DIX-IE 対外線は Finisar 社のシングルモードファイバー用光スプリッターを挟み込み、myri 社製の 10G-LR カードを 2 枚刺した JCS 社のサーバ（traceback.otemachi）で双方向のトラフィックを監視している。また、KDDI 大手町 NOC ではラックスペースの関係上、DIX-IE 対外線監視用 PC にて LAX 対外線のトラフィックをレイヤ 2 スイッチからのポートミラーによって取得し、監視している。

2007 月 2 月から WIDE バックボーンへの対外線監視用 PC 設置の調整および機材設置を開始した。設置作業ではポートミラー設定や対外線に光スプリッタの挟み込み、監視用 PC に取り付けるインターフェースカードの調整など、さまざまな個所で調整が必要となり、実際の機材設置は WIDE バックボーンの構成変更などに合わせて順次実施した。最終的に図 4.1 中の全ての監視ポイントでの監視体制が整ったのは 2009 年 5 月 15 日であった。

奈良 NOC 内に設置した AS 境界探査トレースバックシステムのコントロールサーバ用 PC（ITM サーバ）では、InterTrack のコントロールデーモンである ITM を動作させ、対外線監視 PC の制御やトレースバックのログ収集をおこなっている。ITM サーバと各対外線監視用 PC との間は Racoon の IPSec Transfer mode を使ってサーバ間の認証と暗号路の形成を行い、ITM サーバ以外からの対外線監視用 PC への遠隔ログインを禁止する形式で運用を実施した。

4.4.2 InterTrack の運用

ここでは、InterTrack の運用と利用方法に関して簡単な説明を行う。InterTrack 自体はまだ開発中でありバグも多いため、Munin を利用して図 4.2 に示すように起動 daemon の使用メモリ量を計測してメモリリークの解析を行い InterTrack のデバッグの実施に役立てている。また、図 4.3 に示すように各対外線監視用 PC で取得したトラフィック量などを計

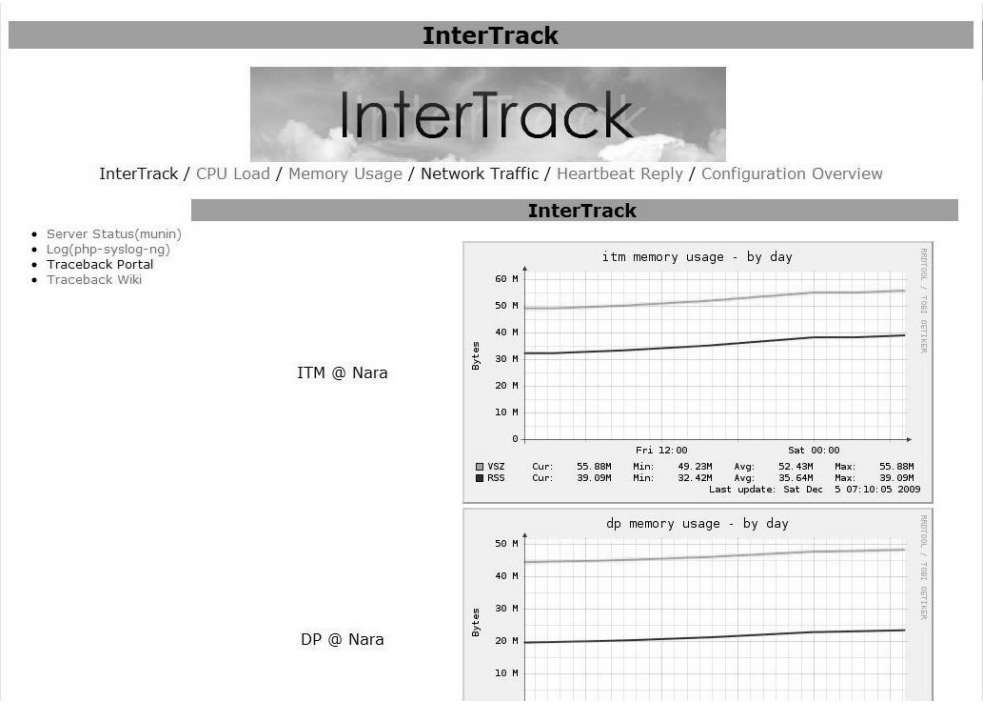

図 4.2. Munin によるメモリリーク解析

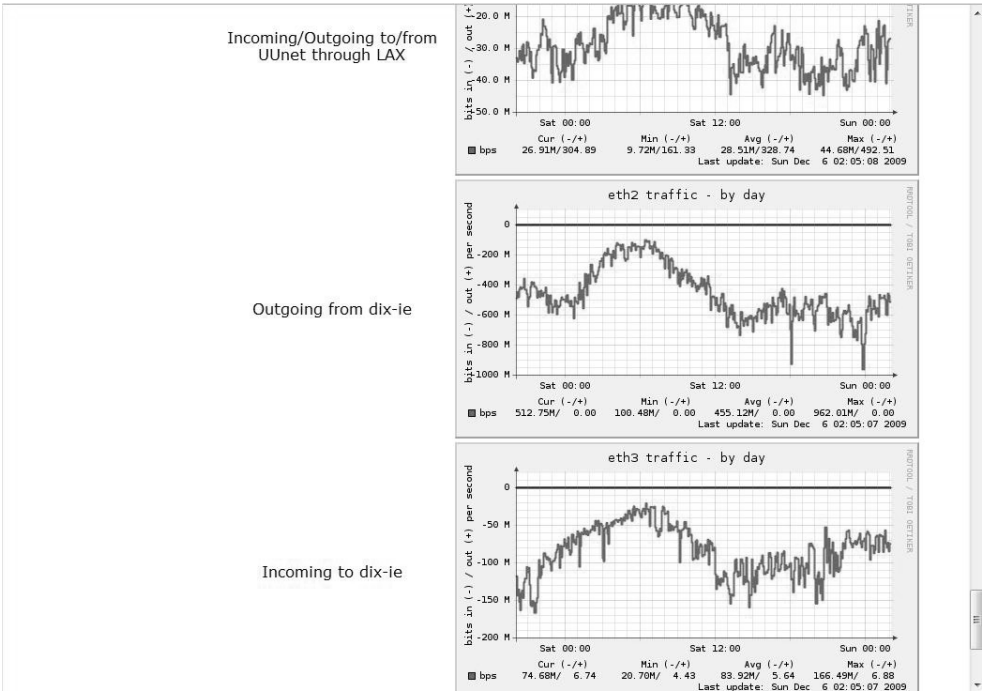

図 4.3.　Munin による取得トラフィック量の計測

測している。

WIDE バックボーン内における InterTrack の運用実験では、各対外線監視 PC から設定に応じてランダムサンプリングしたパケットを ITM を介して対外線監視 PC 上で動作しているハッシュダイジェスト方式 [88] のトレースバックプローブデーモン（BTM2）に XML ベースのメッセージによって問い合わせを行い、各対外線を通過したかどうかと、どの隣接 AS から流入したか、もしくはどの隣接 AS へ転送したかなどを調査する形式で運用した。各対外線監視 PC 上では BTM によって IP ヘッダ情報とハッシュダイジェスト方式のトレースバックで使用されるパケットヘッダのハッシュ値とペイロード先頭 8 バイトのハッシュ値（パケットダイジェスト）のみを一時的に保存し、問い合わせのあったパケットのみ、ログに出力する形式である。運用で用いているハッシュ関数は 4.3 節で説明したトレースバック実証実験との運用連携実験を実施するため、委託研究で研究開発されたハッシュ関数 [60] を用いて実施した。出力したログは sysylog によって ITM サーバに回収し、図 4.4 に示すように PHP Syslog-ng を利用して検索できるように設定して運用を行った。

図 4.5 はとあるパケットダイジェストを PHP Syslog-ng を介して検索した結果である。図 4.5 に示すタイムスタンプ（上から 1 行目と下から 1 行目の TC のログのタイムスタンプ）でわかるように 1 秒以内で追跡リクエストに対する調査と応答が終了していることが分かる。それぞれのログの内容を簡単に説明すると、まず notemachi1 で動作しているトレースバッククライアントデーモン（TC）で検索対象となったパケットダイジェスト（84585efe94e4e813）をキャプチャしパケットヘッダ情報およびイーサネットヘッダ情報をログに残している（上から 1 行目）。そしてパケットダイジェスト（84585efe94e4e813）に対する追跡リクエストを発行している（上から 2 行目）。TC の要求を受け取った ITM は各対外線監視 PC 上で動作している BTM2 に調査用リクエストを発行し、各監視ポイントでの結果が ITM に返されてログに出力されている（上から 3 行目から下から 2 行目まで）。そして最終的に ITM から TC に返された追跡結果がログに表示されている。下から 1 行目の結果からわかるように、TC には通過したか否かの情報（found/not found）のみが返される。

また、検索対象となったパケットダイジェストは notemachi1 のみに記録が残されていたことが分かる（上から 4 行目）。また、各監視ポイントで動作している BTM2 では BGP の Open パケットから AS 番号と BGP Open パケットの送信元 MAC アドレスを対

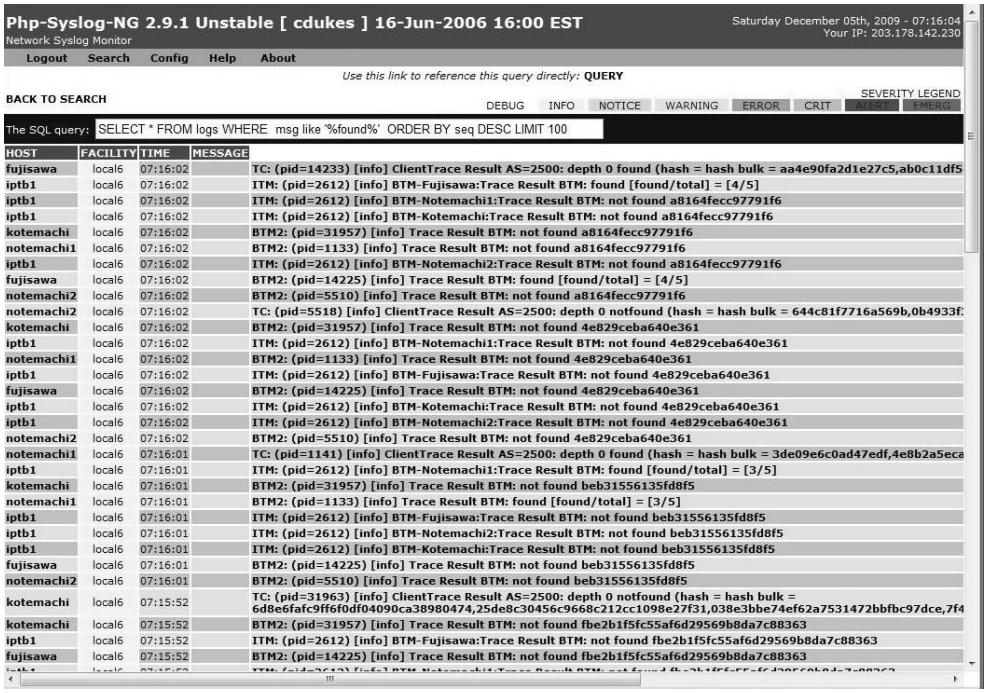

図 4.4. PHP Syslog-ng を用いた IP トレースバックログの閲覧ページ

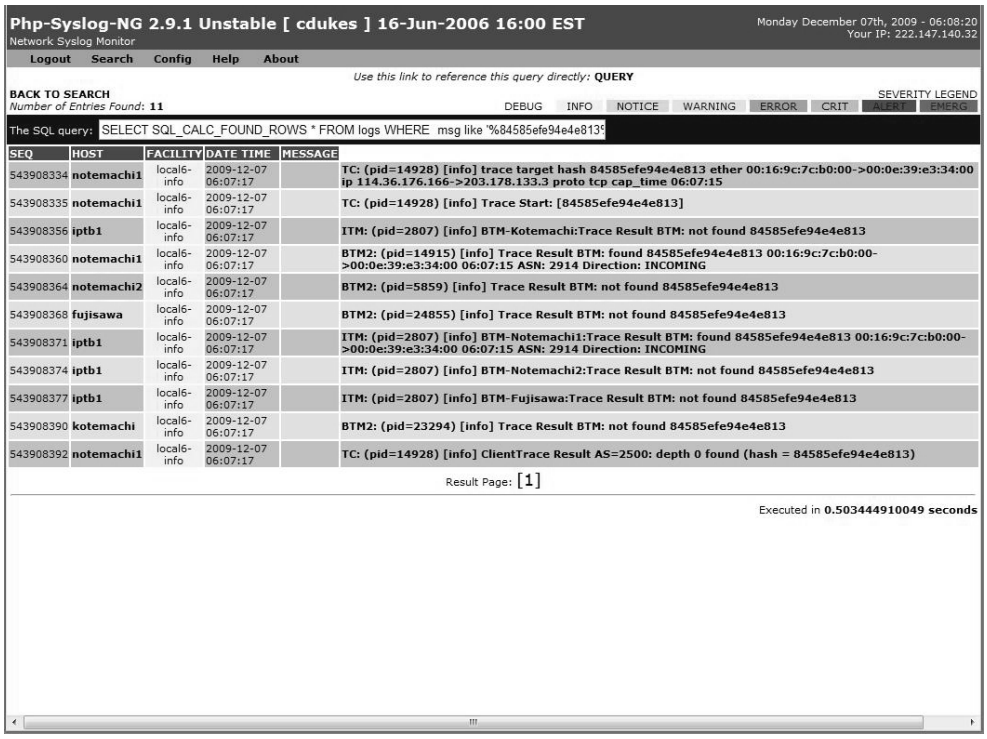

図 4.5. IP トレースバックログの閲覧ページでの検索結果

にしてパケットの流入・流出方向を推定する機能を備えている。図 4.5 の上から 4 行目の項目の内容を説明すると、検索対象パケットは AS 2914 から流入してきたパケット（INCOMING）であり、AS2914 側の対外接続ルータ（と思われるルータの）インターフェースの MAC アドレスは 00:16:9c:7c:b0:00 であり、WIDE 側の対外接続ルータのインターフェースは 00:0e:39:e3:34:00 であることが分かる。対向ルー

タの MAC アドレスや AS 番号がわかることは、インターネットエクスチェンジポイント（IX）など単一インターフェースから接続する隣接 AS が多い場合に、どの隣接 AS との間のパケットなのかを容易に判別できるため、障害切り分けに役立つと考えられる。

この運用実験では、TC を対外線監視 PC 上で動かしていたが、TC 単独を任意の場所に設置することができる。たとえば、DoS 攻撃を受けた場合に DoS 攻撃を受けているサーバの近くに TC を設置することで、どの境界からパケットが流入しているのかを判別できるため、フィルタを投入するルータの絞り込みに役立つ、という利用方法が考えられる。

第 5 章　おわりに

2009 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のソースコードの公開を行った。また、情報通信研究機構の委託研究である「インターネットにおけるトレースバック技術の研究」における商用 ISP 15 社を交えた実証実験と WIDE バックボーンで運用している AS 境界探査型トレースバックシステムの運用連携実験を実施し、11 月におこなわれた世界初のトレースバック実証実験の成功に寄与した。

トレースバック技術としては、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。

2010 年度の活動予定としては、引き続き WIDE バックボーンでの運用実験を通したトレースバック研究を行う予定である。