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 WG 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、2010 年 3 月 21 日から 3 月 27 日まで開催された 77th IETF において、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」における共同研究者とともにトレースバックに関する Bar BoF を開催した。また、2010 年 3 月末日にて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」も終了し、IP パケットに特化したトレースバック研究に区切りをつけることができた。そこで、発展的解消として Traceback WG を 2010 年 8 月 3 日に終了し、あらたに CYBEX WG を設立することとなった。今後、トレースバック技術をふくむインシデント情報交換フレームワークの標準化や実用化、および WIDE バックボーンでのトレースバックシステム稼働実験などは CYBEX WG にて引き続き行っていく。

本報告では、2009 年 12 月から 2010 年 8 月 3 日までの Traceback WG での活動をまず報告し、次に WG クローズ報告として、Traceback WG で実施した研究実績をまとめる。

第 2 章　2010 年度の活動

2009 年 12 月から 2010 年 8 月 3 日までに行った活動は次の通りである。

- トレースバック実証実験に関する発表
  - IEEE CCNC 2010 にて、情報通信研究機構委託研究の共同研究者らとともに 2009 年度に実施した商用 ISP 5 社を交えたトレースバック実証実験の事前実験に関して国際会議発表論文にまとめ、共著にて発表（1 月）
  - WAIS 2010 にて、情報通信研究機構委託研究の共同研究者らとともに 2010 年度に商用 ISP 15 社を交えて実施したトレースバック実証実験の本実験に関して国際会議発表論文にまとめ、共著にて発表（3 月）
  - 77th IETF meeting にて traceback Bar BoF を開催し、2010 年度に実施した実証実験と実用化における課題（標準化）について報告し、Bar BoF 参加者からの意見を収集（3 月）
- Interop Tokyo 2010 における情報通信研究機構トレーサブルネットワークグループの展示への技術協力（6 月）
- WG をクローズ。あらたに CYBEX WG を設立。（8 月）

第 3 章　トレースバック実証実験に関する発表

今年度は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」における共同研究者らと共に日本国内の ISP を交えて実施した実証実験に関する発表を国際会議（IEEE CCNC 2010）、国際会議併設ワークショップ（WAIS 2010）、IETF での Bar BoF にて発表した。以下、各発表の概要をまとめる。

3.1 Demonstration Experiments Towards Practical IP Traceback on the Internet

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」における共同研究者らと共に、2008 年 9 月から 2009 年 3 月まで実施した国内商用 ISP 5 社を交えた事前実験をまとめた論文である。発表は第一著者である若狭賢が発表した。詳細は文献 [186] を参照していただきたい。

Abstract　Recently, Distributed Denial of Service (DDoS) attacks have become a critical issue on the Internet. Theoretical approaches into traceback systems to counter these attacks have been actively researched. However, with no instances of actual application of traceback systems on the Internet, such a response has yet to achieve widespread adoption. This is because multiple autonomous systems (ASs) need to be linked to carry out end-to-end tracking, and this poses a number of issues, including (i) the operational and practical environmental constraints of installing equipment at a variety of Internet Exchange Points (IXPs), (ii) the need to establish operational procedures, and (iii) establishing the monitoring points needed to conduct the traceback. Given these factors, with the aim of achieving the widespread adoption of traceback systems on the Internet in Japan, in this paper we introduce the challenges posed by installing equipment at multiple ASs and report on tracking experiments conducted in response to simulated attacks. Specifically, in terms of (i) environmental constraints, this involved summarizing the size and access restrictions of installed equipment, and in terms of (ii) establishing operational procedures, this involved summarizing the role of operators from the outbreak of an incident to conducting traces and taking countermeasures. Additionally, we investigated the connection status of ASs in Japan to calculate (iii) the number of ASs in which equipment must be installed to satisfy the adoption rate required to carry out tracking.

3.2 Large Scale Demonstration Experiments Towards Achieving Practical Traceback on the Internet

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」における共同研究者らと共に、2009 年 4 月から 2009 年 10 月まで実施した国内商用 ISP 15 社を交えた実証実験をまとめた論文である。発表は第一著者である若狭賢が発表した。詳細は文献 [185] を参照していただきたい。

Abstract　Recently, attacks involving source IP spoofing have become a critical issue for Internet security and operation from the viewpoint of ISP. Research and development into traceback systems that trace an end victim host to an end spoofing host via multiple ISPs is progressing. However, many difficult issues, including those that can't be resolved by IT technology alone, have prevented traceback systems from achieving widespread adoption. We had been researching issues of widespread traceback adoption since 2005, and resolved many challenges on a step-by-step basis. In 2006 we developed an operational model that provided a solution to the three cornered deadlock affecting traceback, which consisted of interrelated operational, legal and technical issues. In 2007 we constructed a three-layer traceback system. In 2008 we conducted a first of demonstration experiments with five ISPs, and found an efficient traceback deployment scenario applicable to Japan. In this paper, we introduce the results of large scale demonstration experiments conducted in 2009, and consider issues about system performance, operational efficiency, the management system's validity, and system adaptability, all of which are necessary for our traceback system to achieve widespread adoption.

3.3 A Field Trial of Inter-Domain Traceback Operation in Japan

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」における共同研究者らと共に、事前実験、実証実験で構成したトレースバックシステムの概要を internet draft（informational）にまとめた。発表は 77th IETF 期間中に Bar BoF を開催し、共著者である櫨山、竹森、若狭それぞれが発表した。詳細は文献 [79] を参照していただきたい。また、77th IETF での発表資料はデータ通信協会のトレースバック研究ポータルサイト [88] から入手可能である。また、開発したトレースバック実装のうち公開可能なものは [137] にて公開している。

Bar BoF の開催時間と事前アナウンスが急だったため、77th IETF 参加者メーリングリストにて色々批判は出たが、Bar BoF に参加していただいた方か

らは好意的な意見をいただき、また、個別に ISP 事業者の研究部門の方からコンタクトも受けたため、潜在的にトレースバック技術の標準化に関心を持つ ISP 事業者や開発ベンダはそれなりに存在することが確かめられた。

Abstract We had a field trial of inter-domain IP traceback operation with fifteen ISPs in Japan with their real network environments, from May to the end of August in 2009. In this memo, we briefly report this field trial. The details of the evaluation results have been reported in [185].

第 4 章　Traceback WG の研究成果

ここでは、設立準備期間も含め 2001 年から 2010 年までの Traceback WG の活動を時系列にて簡単にまとめる。

- 2001 年度
  - 9 月 WIDE 研究会にて Traceback BoF を開催した。
  - IP トレースバック技術の解説論文 [208] を発表した。
- 2002 年度
  - 2002 年 9 月 WIDE 研究会にて横河電機開発の Hash-based IP Traceback システム、サイバーソリューション開発の Hash-based IP Traceback システムの実験を実施した。
  - 2002 年 10 月、Traceback WG が正式に設立した。横河電気、サイバーソリューション、奈良先端大が主なメンバとして参加した。
  - 論文誌掲載論文 1 本 [200]、国際会議発表論文 3 本 [76, 141, 158]、国内研究会発表論文 2 本 [212, 217] を発表した。
- 2003 年度
  - 論文誌掲載論文 2 本 [77, 199] を発表した。
  - トレースバックシステム連携アーキテクチャ InterTrack の設計を開始した。
  - FDB ベーストレースバックツール traceman を開発。2004 年 3 月 WIDE 合宿にて snort と連携した追跡実験を実施した。
- 2004 年度
  - 国内研究会発表論文 2 本 [201, 206] を発表した。
  - トレースバックシステム連携アーキテクチャ InterTrack のプロトタイプ版を開発した。
- 2005 年度
  - 国際会議発表論文 1 本（WIP）[73] を発表した。
- 2006 年度
  - 情報通信研究機構委託研究「インターネットにおけるトレースバック技術に関する研究開発」での実証実験に向け、トレースバックシステム連携アーキテクチャ InterTrack のリファクタリングを開始した。
  - 国際会議発表論文 1 本 [72]、国内研究会発表論文 1 本 [211] を発表した。また、実証実験に向けて、国内外のカンファレンス [69, 209] にて口頭発表を実施した。
- 2007 年度
  - 国際会議発表論文 3 本 [21, 74, 75]、国内研究会発表論文 1 本 [221, 226, 232] を発表した。また、実証実験に向けて、国内外のカンファレンス [71, 94, 205, 207] にて口頭発表を実施した。
  - WIDE バックボーンの対外線 4 か所に InterTrack と境界探査型トレースバックシステムを設置し、実証実験向け開発と運用実験を開始した。
- 2008 年度
  - Interop Tokyo 2008 ShowNet にて実証実験に向けたトレースバックシステムの予備検証を実施した。実施結果は APAN26 にて発表した [70]。
  - トレースバック連携システムとして InterTrack を利用した商用 ISP 5 社を交えた事前実験を情報通信研究機構委託研究にて実施した。また事前実験で明らかとなった不具合を WIDE バックボーンに設置した InterTrack 検証環境を利用し修正した。
  - 論文誌掲載論文 1 本 [121]、国内研究会発表論文 1 本 [219, 227, 229, 231] を発表した。また、実証実験に向けて、Web での解説記事 [210] を執筆した。
- 2009 年度
  - InterTrack を利用した ISP 間トレースバック連携システムの実証実験を情報通信研究機構

委託研究にて商用 ISP 15 社を交えた形式で実施し、共同研究者連名でプレスリリースを発行した [216]。実施結果や実用化における課題はインターネットドラフト [79] にまとめ、77th IETF meeting にて Bar BoF を開催し、発表した。

- 国際会議発表論文 3 本 [130, 185, 186]、国内研究会発表論文 1 本 [233] を発表した。
- トレースバック連携システム参照実装 InterTrack を公開した [137]。

• 2010 年度

- Interop Tokyo 2010 における情報通信研究機構トレーサブルネットワークグループの展示における技術協力（6 月）
- CYBEX WG の設立に伴い、2010 年 8 月 3 日に Traceback WG をクローズした。

第 5 章　おわりに

2002 年 10 月 31 日から 2010 年 8 月 3 日までの約 8 年間、トレースバック技術の研究開発とトレースバック技術の実用化の道筋を立てるべく Traceback WG では活動してきた。この 8 年間の間で、トレースバック技術はほぼまとまり、実証実験を実施することもでき、トレースバック技術の実用化に向け大きな寄与を果たすことができた。しかしながら、実証実験の結論として、トレースバック技術の実用化に関しては標準化が必要であり、トレースバック技術を使う運用企業とともに標準化を行う必要があることが明らかとなった。これを受け最終的には CYBEX で扱うような事業者間のインシデント情報交換フレームワークとともにトレースバック技術に関する標準化がなされることが望ましいと Traceback WG では考えた。そこで、発展的解消として Traceback WG をクローズし、新たに CYBEX WG を設立することとなった。トレースバックに関する研究開発や WIDE バックボーンにおける実験は引き続き CYBEX WG にて続けていく。