Vol.2009-CSEC-46 No.17
2009/7/2

インターネットにおけるトレースバック・システムの ISP 環境を利用した事前実験

若狭　賢[†]　木村　道弘[††]
甲斐　俊文・橋口　輝[†††]
藤長　昌彦・竹森　敬祐[††††]
門林　雄基・櫨山　寛章[†††††]

送信元を詐称した攻撃への対応は Internet 上の重要な課題である．そのために，様々なトレースバック手法が研究レベルで提案されているが，技術論以外の問題点の壁が厚く、実 Internet 環境上におけるトレースバックの実験例は皆無である．我々は 2008 年後半に実 Internet 環境で模擬攻撃を用いたトレースバック事前実験を実施し，実験結果を測定すると共に多数の ISP へトレースバック・システムを導入する際に発生する複数の問題点の確認と対応を行った．本論文では，事前実験結果を紹介し，次年度に計画する大規模な ISP 環境における実証実験への要求事項を取りまとめる．

Demonstration Experiments Toward the Practical IP Traceback on the Internet

Ken Wakasa[†]　Michihiro Kimura[††]
Toshifumi Kai, Akira Hashiguchi[†††]
Masahiko Fujinaga, Keisuke Takemori[††††]
Youki Kadobayashi, Hiroaki Hazeyama[†††††]

Recently, source IP spoofing attacks are critical issues for the Internet. Theoretical approaches into traceback systems have been actively researched. However, with no instances of the actual application of traceback systems on the Internet, this is yet to reach widespread adoption. This is because multiple autonomous systems (ASs) need to be linked to carry out endto-end tracking, and this poses a number of issues. Given these factors, with the aim of 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 conduct tracking experiments in response to simulated attacks.

1. はじめに *

スパムメールや DoS 攻撃など，ネット上にはさまざまな種類のインシデントが発生し，その手口は日々巧妙化している．時に攻撃者は自身の所在を隠すために，送信元 IP アドレスを詐称した攻撃を行う．現在，攻撃の踏み台となっているホストを特定して駆除するために，送信元 IP アドレスを詐称した攻撃者や攻撃の経路を追跡する技術として，トレースバックが注目されている[1][2].

筆者らは，インターネットにおけるトレースバック・システムの実環境への実装を目指したトレースバック・システムの開発と平行して，2005 年度・2006 年度に実環境でのトレースバック・システムの運用上の課題である、法的な要求事項（通信の秘密）、ISP が迅速に連携するための枠組み等の課題を法的側面と技術的側面から整理してきた[3].

そして，2007 年度は過去に洗い出した法的な要求事項に適合した、トレースバック装置・トレースバック管理機構・トレースバック・マネージメントシステム、の 3 階層からなるトレースバック・システムを構築した[4]．2008 年度前半は，ISP 環境におけるトレースバック機器の配置計画，および，模擬攻撃を使用した実験シナリオ案を策定し[5]，事前実験の準備を完了した．また，平行して我が国の ISP ネットワークの AS 接続環境を調査した上で，トレースバック導入シナリオのシミュレーションを行った[6].

本稿では，事前実験概要を紹介するとともに、トレースバック導入に係る問題点を考察して、具体的なトレースバック導入プランを提案する．

以下，2 章では事前実験に利用したシステムの概要と適法用件を紹介し，3 章では事前実験の結果を報告する．そして 4 章ではプローブを導入する ISP の選定シナリオ[6]を再検討した上で，5 章で事前実験から得られた知見を考察する．そして，6 章で次年度に計画する大規模な ISP 環境における実証実験への要件をとりまとめる．

* [†]財団法人日本データ通信協会
Japan Data Comunications Association
[††]日本電気株式会社
NEC Corporation
[†††]パナソニック電工株式会社
Panasonic Electric Works, , Ltd.
[††††]株式会社 KDDI 研究所
KDDI R&D Laboratories Inc.
[†††††]奈良先端大学院大学
Nara Institute of Science and Technology

2. 事前実験システムの概要

2.1 トレースバック・システム

本トレースバック・システムは，DoS 攻撃や DDoS 攻撃パケットの通過経路及び発信元 ISP を特定することを目指したシステムである. 通常, 攻撃パケットは複数の ISP を経由して，発信元の端末から被害サーバまで到達するため，各 ISP にトレースバックのための装置を配置し，それらを連係動作させる必要がある．この時，各 ISP の間で互いのネットワークの情報やトレースバック情報が見えてしまうことは通信の秘密において問題であるため，ISP 内部で閉じてトレースバックを行うシステムと，ISP 間でトレースバック情報を交換する仕組みとに分けてシステムを構成した．ISP 内でトレースバックを行う仕組みとして，隣接 ISP との間で通過パケットのハッシュ値を記録するハッシュ方式を採用した. ISP 間で IP トレースバック情報を交換する仕組みは，ISP 内トレースバックの結果に基づいてトレースバック・リクエストを適切な ISP に転送していく InterTrack [7]と名づけられた図 1 に示す方式を採用した．また，インシデント対応時に各 ISP 担当者とトレースバック管理センターが連携して攻撃の対処を行う ISP 連携のためのシステムとしてオペレーター連携支援システムを開発した.

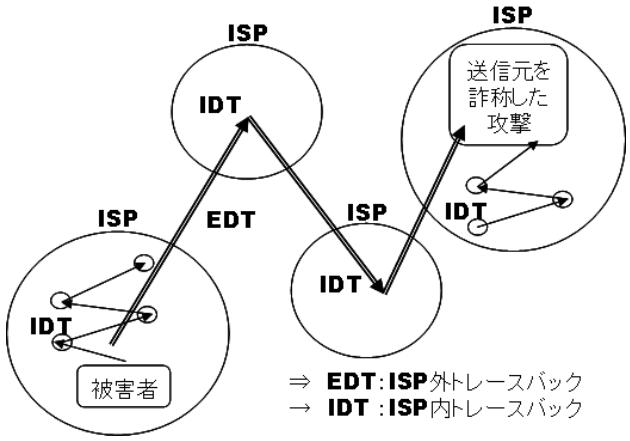

図 1　InterTrack の動作

2.2　適法要件

我々は，国内外の関連法案の調査と，国内 ISP への大規模アンケート調査を行ってきた. これらから制定されたトレースバック･システムへの適法要件を表 1 に示す[3].

表 1　トレースバック・システムへの適法要件

適法要件	対応手段
(1) データ破壊などが無いこと	タップ･ミラーの利用
(2) ハッシュ値のみの取得･交換	ハッシュ方式の採用
(3) 関連する情報交換の制約	アクセス･コントロール
(4) インシデント･レスポンス	ポリシー
(5)インシデント発生以前の対応禁止	ポリシー
(6) データ共有に係る守秘義務	守秘義務誓約書
(7)適切な方法による情報開示	情報公開
(8) 攻撃追跡に係る守秘義務	守秘義務誓約書
(9) セキュリティ･ポリシーと個人情報への	ISMS

2.3. ISP 内のトレースバック・システムの構成

運用コストの削減および機械的処理による通信の秘密の確保を目的として，ISP 内のトレースバックを，次の 4 つのモジュール（図 2）から構成した[4]).

①攻撃パケットを検知する IDS

②各 ISP の通信を記録するプローブ装置　（表 1-(1)(2)への対応）

ISPが他のISPと接続する境界部分を通過するパケットのヘッダ部分に対してハッシュ値を算出し[a]，これをメモリ上に一時的に記録する.

③攻撃パケットの通過を特定するコントローラ

攻撃パケットの通過が確認できた場合，InterTrack [7]により隣接 ISP のコントローラに対して再帰的にトレースバック実行をリクエストし，ISP ごとのトレースバック結果を DB に登録する.

④トレースバック結果を保存する DB　（表 1-(3)への対応）

オペレーター連携支援は専用の Web システムで提供される．例えば，被害側 ISP のからトレースバック管理センターへの被害報告がなされ管理センターから攻撃側 ISP へ攻撃事実の確認依頼がなされるが，こうしたやり取りを取り仕切る.

[a] 適法要件からハッシュ対象はデータ部分を除外した。

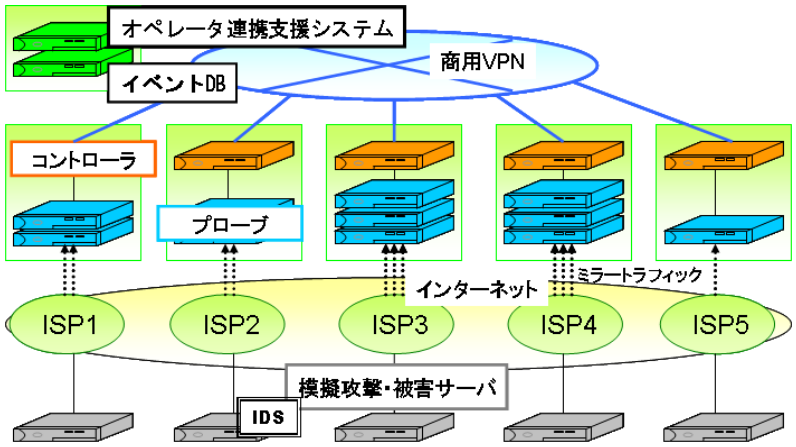

図 2　トレースバック・システム実装図

2.4. ISP 間トレースバックの自動化

運用コストの削減のために, ISP 間のトレースバックを取り仕切る InterTrack[7]を使用して自動化された処理フローを以下に述べる.

①IDS が攻撃パケットを検知し，コントローラにトレースバックをリクエストする.
②コントローラは攻撃パケットのハッシュ値を同じ ISP 内のプローブに問合せる.
③次に, InterTrack [5]は隣接 ISP のコントローラにトレースバックをリクエストする.
④隣接 ISP のコントローラで同様の処理を行う．これを再帰的に繰り返し，攻撃パケットが通過した全ての ISP にトレースバックがリクエストされる.
⑤トレースバック結果は，最初に IDS からリクエストを受け取った ISP のコントローラに集約された後，DB に登録される.

2.5.　オペレーター連携支援システム

ISP 間連携を用いて，被害側 ISP が攻撃を認知してから攻撃送信側 ISP で対処が行われるまでのシナリオを，トレースバック管理センターが中心となって取り仕切るオペレーター連携支援システムの処理フローを図 3 に示す.

①被害者が攻撃に気づき，ISP に対処を依頼する　（図 3-(1)）
②被害者側の ISP のオペレーターは，DB にアクセスして該当攻撃パケットに対応したトレースバックが自動実行済みを確認し（図 3-(2)），トレースバック管理センターにインシデント対応を依頼する（図 3-(3)）.
③トレースバック管理センターは，DB にアクセスして攻撃者側の ISP を特定し（図 3-(4)），その ISP に攻撃の対処を依頼する（図 3-(5)）.
④攻撃送信者側の ISP は，自社設備で攻撃送信者をつきとめ，適切に対処する．（図 3-(6)）

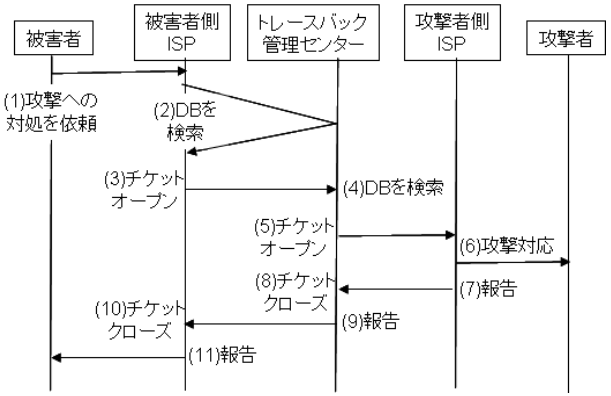

図 3　ISP 間連携を用いたオペレーター連携対応フロー

3.　事前実験の結果

我々は 2008 年度前半の実験の準備フェーズで，ISP へのトレースバック機器の適切な配置に係る検証を確認した[5]．本章では，その後に実施した実験結果を述べると共に，トレースバック・システムの実用化において大きな問題点の一つである，トレースバック・オペレーション手順の確立に係る仮説の検証結果を述べる.

3.1　模擬環境での実験結果

実験を始める前に，データセンター内に事前実験の模擬環境を構築し，図 2 に示したトレースバック・システムを用いて，基礎性能評価を行った．実験結果では，自動追跡は平均 0.3sec 以下で終了し，誤検知率は最悪のケースでも 0.3%であることが判明した.

3.2　実環境での実験の様子

我々は，ISP-5 社の協力を得て実験を行った．各 ISP にはコントローラ装置 1 台，プローブ装置複数台，DB アクセス用 PC 1 台，模擬攻撃用サーバ 1 台を設置した．各 ISP

は専用 PC から DB とオペレーター連携支援システムにアクセスする．模擬攻撃用サーバは模擬攻撃の送受信に使用する．DB とオペレーター連携支援システムは 1 台に集約しセキュリティ管理のあるデータセンターに設置し，トレースバック管理センターも設けた．プローブ装置は，トータルで 10 台，ソフト・プローブが 9 台，10G まで対応可能なハード・プローブが 1 台，ISP-5 社に設置された．ソフトウエア・プローブとコントローラーには，NEC Express5800-110RH-1（N8100-1268、Intel@Xenon3060 2.40G Dual Core processor、4GB memory、160GB SAS HDD）を使用した．

各ISPに設置したプローブ数は，ISPの隣接AS環境に準じて，1 台～3 台である．ハード・プローブは 2 段ハッシュ構成[ii]の 25 ビット・ブルームフィルタ[iii]を使用し，ソフト・プローブは 2 段ハッシュ構成の 26 ビット・ブルームフィルターを使用する．各プローブのブルームフィルターは2秒ごとに10個のフィルターが用意されているため，1 パケットのハッシュ情報は 20 秒間プローブのキャッシュ・メモリーに保持される．今回の実験環境では，プローブに流入されたISPトラフィックの最大量は 100Mbps であった．そして想定される流入パケット数は 297,620 パケット/秒なので，プローブの論理的な検知エラー率は 25 ビット・ブルームフィルターで 0.309%，26 ビット・ブルームフィルターで 0.078%となる．

トレースバック・システム用のネットワークとして VPN を用意し，DB／オペレーター連携支援システム，トレースバック管理センター，及び各 ISP のコントローラと DB を接続した．一方，各 ISP の模擬攻撃サーバはインターネットに接続され，トレースバック管理センターから遠隔制御した．各 ISP に設置されたコントローラーは，VPN 網を経由して，全コントローラーと情報交換を行う．今回の実験では，コントローラーは InterTrack の Flood モードを使用して情報交換を行った．大規模 Simulation 実験の検討結果を踏まえ[8]，Flood モードではコントローラーは関連する全てのコントローラーに問い合わせ要求を発信する．

実験開始前にトレースバック管理センターと実験参加の ISP-5 社で操作練習を実施した．そして，送信元アドレスを詐称した模擬攻撃を使用した，被害役 ISP-1 社と攻撃役 ISP-1 社によるシナリオに沿った実験を 6 回実施した後，複数 ISP から ISP-1 社への攻撃，シナリオの無い実験，などの応用実験を 3 回実施した．なお実験で用いた模擬攻撃は syn flood 攻撃を模擬した TCP80 番ポートへの syn パケットで，送信速度は 100[packet/sec], パケットサイズは 46Byte, である. ISP の実環境で実施されたため，ISP 顧客へのトラフィックに影響を及ぼさないように，通常の DoS 攻撃とは違い非常に小規模な攻撃で実施した．

[ii] ヘッダー部の複数個所から 2 種類のハッシュ値を生成し、この 2 種類のハッシュ値を演算して新たなハッシュ値を生成する。
[iii] トレースバックにおけるブルームフィルタとは、算出されたハッシュ値をメモリのアドレス番地に見立てて、そのビットを On/Off することで、ハッシュ値間のマッチング検索を高速化する手法である。

3.3 実環境での実験結果

実験は 2008 年 10 月から 12 月までの 3 ヶ月間で実施した．以下、実験結果をまとめたものである。

実験では、送信元アドレスを偽造した IP パケットをエンドエンドでトレースし，実 ISP 環境でトレースバック・システムが正常に機能することが確認できた．図 4 のレスポンスタイムは，プローブを設置した ISP-5 社で測定した結果である。各 ISP について 2000 回以上のクエリィーのレスポンスタイムを測定し、平均・最大・最低値をもとめた。各 ISP のトレースバック・システムの平均レスポンス・タイムは，データセンターにおける模擬実験における測定時間と同等の，0.3 秒以下である．最大の場合でも，トレースバック・システムの応答時間は 1.6 秒以下である．

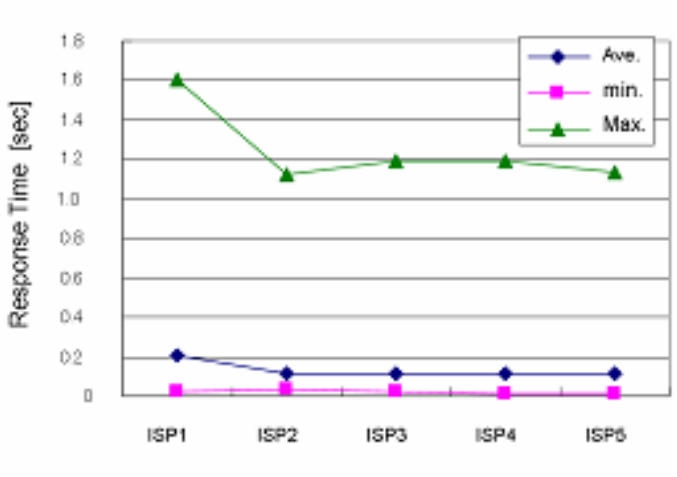

図 4　各 ISP におけるレスポンスタイム

図 6、図 7 に示すように、誤検知率は，最も誤検知が発生したプローブで 0.029%であり，想定される最悪の状況下での誤検知率である 0.3%の 1/10 以下を確認した．

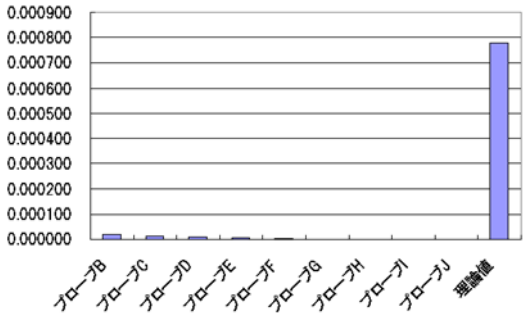

図 5 26 ビット・ブルームフィルターを使用したプローブの誤検知率

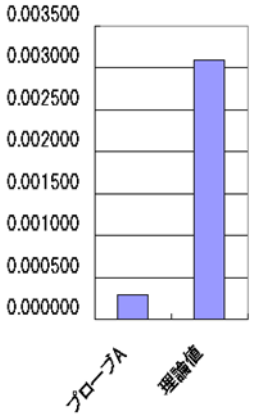

図 6 25 ビット・ブルームフィルターを使用したプローブの誤検知率

表 2　各シナリオの対応時間

実験日	総計	対応時間	結果
第一週	71分	56分	成功
第二週-1	88分	69分	成功
第二週-2	67分	59分	成功
第三週	67分	59分	失敗
第四週-1	60分	45分	成功
第四週-2	47分	36分	成功

表 3　各 ISP のインシデント対応時間

実験日	被害ISP	攻撃ISP	総計
第一週	28分	15分	43分
第二週-1	39分	15分	54分
第二週-2	14分	26分	40分
第三週		29分	
第四週-1	17分	12分	29分
第四週-2	7分	23分	30分

表 4　各 ISP の待ち時間

実験日	被害ISP	攻撃ISP
第一週	26分	36分
第二週-1	23分	41分
第二週-2	42分	14分
第三週		35分
第四週-1	25分	27分
第四週-2	27分	16分

インシデント対応シナリオに基づく各 ISP での基本オペレーションの実行も確認できた．各シナリオの対応時間を表 2 に示す，各実験は想定した時間内に終了したが、オペレーションに無駄時間が存在することを確認した．無駄時間は，ISP と TB 管理センターの双方のオペレーターが相手の返答を待つことで発生し，表 4 に示すとおり平均 30 分であった．最悪の場合は，表 2（第二週-1）で示すように対応時間はトータルで 88 分になった．また，ISP-1 社から ISP 複数社への攻撃による追加実験では，特に TB 管理センターのオペレーターで混乱が発生した．

3.4　トレースバック対応プロセスの検証結果

トレースバック・システムを使用し，想定したインシデント対応シナリオを実施する一連の作業手順を定めたものをトレースバック対応プロセスと呼ぶ．今回の実験では，以下の 7 項目のトレースバック対応プロセスの検証結果を得た．

１）トレースバック対応プロセスの流れの検証

作成した作業プロセスは，被害受付から対処までの一連の対応が実 ISP 環境で実施可能であることを確認した．また，作業のボトルネックになったポイントを確認した．

２）トレースバック対応プロセスにおける重要チェックポイントの抽出

判断に迷うポイントなどを抽出した．また手順のみならず，システムからの情報についてもチェックポイントとの連動が必要なポイントを抽出した．

３）トレースバック対応プロセスを ISP に実施してもらうためのサポート内容の検証

操作練習時に用意したドキュメントで，環境の異なる参加者が一定レベル以上の作業品質を保持可能なことを検証した．ただし，操作練習については，ある程度の時間が必要となることを確認した．

４）トレースバック対応プロセスの運用者側の対処ボリュームの検証

実験時間内に全ての手順が実行可能なことを確認した．なお，被害 ISP と攻撃 ISP に手順数の差はないが，対応時間に大きな時間があることが確認した．また，同時に複数の攻撃に対応するためには，要員の増員の必要性が認識した．

５）より大規模な実験を行うために必要な環境の検証

手順のチェック方法は，紙資料への記録からシステム化の対応が必要なことを確認した．また，参加 ISP が増加した場合のガバナンス維持に向けた手順やチェック内容の見なしの必要性を認識した．

６）開発されたシステムのユーザビリティの検証

判断を要するポイントで，システムのメッセージがわかりづらい点などを確認した．

７）手動対応プロセス，自動化プロセスの機能検証

システム間の連携において，人手による転記などを自動化する必要性を認識した．

4. トレースバック・システムの導入ISPを選定するシナリオ[6]の検討

2008 年に検討したトレースバック・システムを日本のインターネットへ導入する際の設置 ISP を選定するシナリオの 2 案を再検討すべく，事前に日本の AS トポロジの調査を行った．

4.1 日本のASトポロジの調査方法

日本の AS トポロジの調査のために，4 種類のトポロジ構成のデータセットを用意した．データセットには CAIDA Project による eBGRP 観測情報を元にした AS 間接続関係データ（以下，as-rel [9]） を元にし，日本国内の AS を抜き出すために日本ネットワークインフォメーションセンター（以下、JPNIC）で公開されている日本国内の AS 情報データを用い，文献[10]で示す Region Based Filter を用いて JPNIC 登録 AS ，および，JPNIC 登録 AS と隣接関係を持つ国外 AS との AS トポロジデータ as-rel.jpdomain を作成して, as-rel.jpdomain で作成される AS トポロジで調査を行った．

導入シナリオを作成するにあたり，as-rel のリンク情報を元に日本国内の AS を隣接 AS 数と接続関係を元に順位付けを行った．as-rel には AS 番号，隣接 AS 番号，2 つの AS 間のリンク情報の 3 要素が記載されており，隣接 AS との関係により -1，0，1，2，に定義されている． このリンク情報の値を元に本稿では，AS のランクポイント算出し，ランクポイントの大きい AS から順に上位 AS と定義する．

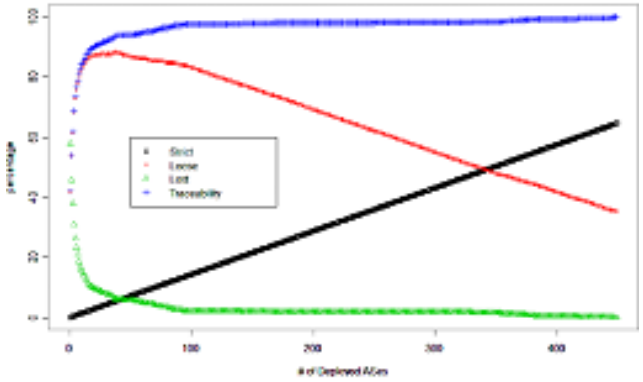

図 7 大規模 AS からの導入シナリオでの追跡成功率

4.2 トレースバック導入ISPの選定シナリオ 1

シナリオ 1 では，国内 AS のうち接続ポイントの多い最上位の AS から順にトレースバック・システムを導入した場合の追跡可能性の変化を調査する。

図 7 はシナリオ 1 でのシミュレーション結果をグラフにしたものである．シミュレーションの結果，国内上位 5AS に導入した段階で追跡可能性が約 73.63%を超え，国内上位 20AS に導入した場合に追跡可能性が 90%を超えることが確認された．

4.3 トレースバック導入ISPの選定シナリオ 2

シナリオ 2 では，国内 AS のうち小規模中規模 ISP をランダムに選択しで並べ，シナリオ 1 で導入効果の高かった上位 5AS を段階的に導入し，その後リーフ AS に導入するという，実験に参加可能な ISP を絞り込むための導入シナリオで実施した．ランク上位の AS は, 13 番目にランク 1 位, 32 番目にランク 2 位, 118 番目にランク 3 位, 120 番目にランク 4 位，340 番目にランク 5 位の AS がトレースバック・システムを導入するものとしてシナリオを作成した．シナリオ 2 では，12 番目の AS まで導入した場合は約 21.75%程度である．つまり，小中規模 ISP のみに導入しても一定の導入効果がうかがえることがわかる．13 番目の AS にランク 1 位の AS が加わることで追跡可能性は約 58,35%まで急激に上昇し，下位 32 番目の AS（ランク 2 位） まで導入した段階で追跡可能性は約 70.74%を超えることが明らかになった．この結果からやはり隣接 AS 数の多いランク上位の ISP がトレースバック・システムを導入すると飛躍的に導入効果が向上することが判明した．

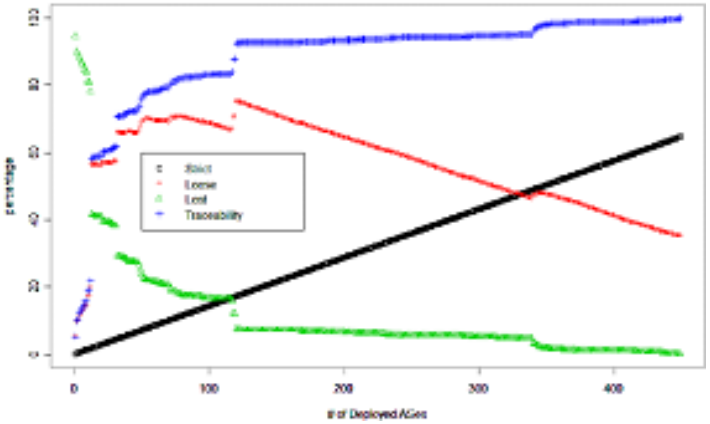

図 8 小中規模 AS からの段階的な導入シナリオでの追跡成功率

シナリオ 1 によるシミュレーションの結果，大規模トランジット AS に導入すると追跡可能性が著しく高くなることが確認できた．しかしながら，大規模 AS へのトレースバック・システムを導入費用は莫大なため，実証実験での導入は難しい．一方，シナリオ 2 のシミュレーション結果から，小中規模 AS からトレースバック・システムを導入しても 13AS 程度導入されれば追跡可能性が 25%以上になり，そこへ大規模 AS がひとつ加わることで 50%以上になることが明らかとなる．小中規模 AS で実施されある程度効果が認められてから大規模 AS やほかの小規模な AS に導入されていくというシナリオが，現実的なトレースバック導入シナリオだと考えられる．

5. 考察

実験で得られたいくつかの知見を元に、2009 年度に計画している ISP-15 社による実証実験の課題を考察する。

今回の実験に参加した ISP-5 社は隣接 AS 関係を持っておらず, InterTrack の隣接 AS 間でトレースバック・リクエストを順次転送する仕掛け[8]が生かせなかった．また，今回の実験では我々がトレースバック・システムの設定を実施したが、本来 ISP の接続情報は全て公開されず頻繁に変更されるため、ISP がトレースバック・システムの設定を行うことが望ましく，InterTrack の動作に関する知識が必要とされる．

実ネットワークを観測するプローブで発生した不具合の調査は，通信の秘密の制約のために観測する回線データの解析が出来ないため，困難を極めた．また，特定箇所に問題が発生したため，システム全体が作動しないケースがあった．トレースバック・システムの規模が大きくなると，全てが正常稼動していることを期待できない．トレースバック・システムを障害に強いシステムに改善すると共に，問題の発生箇所を速やかに発見する仕組みを開発する必要がある．

4 章のシナリオ 2 の再検討結果から、我が国の Internet 環境へのトレースバック・システムの導入は、大規模 AS より中小規模 AS、密な隣接 AS より全国に点在する AS へまず導入していくシナリオが現実的と判断できる。そして、初期にトレースバック・システムが導入される ISP は全国に点在すべきである。

6. まとめ

トレースバック・システムの実装を目指し，2005 年度より、トレースバック・システムの運用上の課題の整理[3]，法的な要求事項に適合した 3 階層トレースバック・システムの構築[4]，ISP 環境におけるトレースバック機器の配置計画，および，模擬攻撃実験シナリオ案の策定[5]を行い，平行して我が国へのトレースバック導入シナリオのシミュレーション[6]を行った．本稿では，ISP-5 社で実施した事前実験結果を報告すると共に，わが国へのトレースバック導入に係る問題点を考察して，具体的なトレースバック導入プランを提言した．2009 年度は ISP-15 社による実証実験を実施し，送信元 IP アドレスを詐称した攻撃の検知・追跡・対応に係る手順の確立を目指す．

謝辞 本研究は，独立行政法人情報通信研究機構の平成 17 年度からの研究案件「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」の一部である．

最後に，有用な意見を多数頂いた Telecom-ISAC Japan トレースバック WG メンバー，および，アンケート・ヒアリング調査に積極的にご協力を頂いた多数の ISP・ホスティング事業者様，そして実験への参加を決断された ISP-5 社様へ深く感謝します．

参考文献

[1] D. McPherson and C. Labovitz, “WorldWide Infrastructure Security Report,” Arbor Networks, Sep. 2008. [Online]. Available: http: //www.arbornetworks.com/sp security report.php

[2] P. Ferguson and D. Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing,” RFC 2827 (Best Current Practice), May 2000, updated by RFC 3704. [Online]. Available: http://www.ietf.org/rfc/rfc2827.txt

[3] 木村道弘，若狭賢，中谷浩茂，甲斐俊文，遠藤彰一，野村豊：インターネットにおけるトレースバック運用に係る ISP 間連携の取り決め事項の整理，コンピュータセキュリティシンポジウム 2006 (CSS2006)https://www.telecom-isac.jp/pmaterials/index.html

[4] 若狭賢，木村道弘，中谷浩茂，甲斐俊文，藤長昌彦，竹森敬祐，門林雄基，櫨山寛章：インターネットにおけるトレースバック・システムの実証実験に至る全体計画案の策定，コンピュータセキュリティシンポジウム 2007 (CSS2007)

[5] 若狭賢，木村道弘，中谷浩茂，甲斐俊文，藤長昌彦，竹森敬祐，門林雄基，櫨山寛章：インターネットにおけるトレースバック・システムの＊＊＊＊，コンピュータセキュリティシンポジウム 2008 (CSS2008)

[6] 櫨山寛章，若狭賢，門林雄喜：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，情報通信学会技術研究報告 IA2008-14 PP.25-30, July 2008

[7] Hiroaki Hazeyama, Youki Kadobayashi, Masafumi Oe and Ryo Kaizaki : InterTrack: A federation of IP traceback systems across borders of network operation domains,In Proceedings of 11th IEEE Symposium on Computers and Communications (ISCC '06), pp. 378-385 (2006).

[8] H. Hazeyama, Y. Matsumoto, and Y. Kadobayashi, “Message Forwarding Strategies for Inter-AS Packet Traceback Network,” in Proceedings of The 2nd Joint Workshop on Information security, August 2007.

[9] CAIDA Project, “AS Relationships.” [Online]. Available: http://www.caida.org/data/active/as-relationships/index.xml

[10] H. Hazeyama, M. Suzuki, S. Miwa, D. Miyamoto, and Y. Kadobayashi, “Outfitting an inter-AS topology to a network emulation testbed for realistic performance tests of DDoS countermeasures,” in Proceedings of the conference on Cyber security experimentation and test (CSET’08),Aug 2008, pp. 1–6