インターネットにおけるトレースバック・システムの ISP 実ネットワークにおける大規模実証実験の紹介

若狭　賢[†]　山形　昌也[¶]　大島　龍之介[!]
[†]財団法人日本データ通信協会　[¶]日本電気株式会社　[!]株式会社クルウィット
東京都港区　東京都港区　東京都三鷹市
甲斐　俊文・橋口　輝[『]　藤長　昌彦・竹森　敬祐[〃]　櫨山　寛章・門林　雄基[※]
[『]パナソニック電工株式会社　[〃]株式会社 KDDI 研究所　[※]奈良先端科学技術大学院大学
東京都港区　埼玉県ふじみの市　奈良県生駒市

あらまし　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2009年前半に大規模な実Internet環境で模擬攻撃，および，実インシデント対応のトレースバック実証実験を実施し，実験結果を測定した.本論文で本実証実験結果を紹介する．

Large Scale Demonstration Experiments Toward the Practical Traceback on the Internet

Ken Wakasa[†]　Masaya Yamagata[¶]　Ryunosuke Ohshima[!]
[†]Japan Data Communications Association　[¶]NEC Corporation　[!]clwit, Inc
Minato-ku, Tokyo　Minato-Ku, Tokyo　Mitaka-city, Tokyo
Toshifumi Kai, Akira Hashiguchi[『]　Masahiko Fujinaga, Keisuke Takemori[〃]
[『]Panasonic Electric Works,Ltd.　[〃]KDDI R&D Laboratories Inc.
Minato-ku, Tokyo　Fujimino-city, Saitama
Hiroaki Hazeyama, Youki Kadobayashi[※]
[※]Nara Institution of Science and Technology　Ikoma-city, Nara

Abstract Recently, source IP spoofing attacks and stepping stone 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 large scale ASs and conduct tracking experiments in response to simulated attacks and real attacks.

1　はじめに

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，ISP 連携の枠組み等を，法的側面と技術的側面から整理した[1]．2007 年度は

法的な要求事項に適合した，システム・管理機構・マネージメント，の 3 階層のトレースバック・プラットフォームを構築した[2]. 2008 年度は ISP 環境におけるトレースバック機器の配置計画，および，模擬攻撃実験シナリオ案を策定し[3]，ISP5 社による事前実験を実施した[4] . 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[5]. 本稿では，2009 年度前半に実施した大規模な実証実験を紹介する.

2 実証実験システムの概要

2.1 トレースバック・システム

トレースバック・システムへの適法要件に対応した 3 階層システムを図 1 に示す.

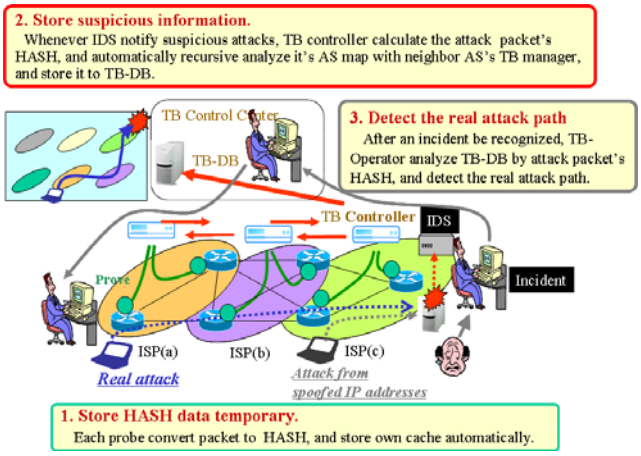

図 1 3 階層のトレースバック・システム

2.2 トレースバック・システムの構成

ISP 内のトレースバックを，次の4つのモジュールから構成した.

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
③攻撃パケットの通過を特定するコントローラ
④トレースバック結果を保存する DB

2.3 ISP間トレースバックの自動化

ISP 間のトレースバックを InterTrack[6]を使用して自動化し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 [6]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 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が DB に登録される

2.4 オペレーター間連携支援システム

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示す.

①被害者が攻撃に気づき，ISP に対処を依頼する.
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であることを確認し，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.
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，その ISP に攻撃の対処を依頼する.
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.

2.5 実証実験のISPと研究所

北海道・東北・北陸・首都圏・関西・中国・四国・九州・沖縄，に点在した ISP-15 社に実験に参加していただけた. また，実インシデント実験対応で研究機関-3 組織に協力していただき，各研究所には実験参加 ISP の Internet 回線を使用したハニーポットを設置していただいた.

3 実証実験の結果

3.1 事前実験の問題点の対応内容

事前実験の主要な問題点への対応は完了できた.

1)システムのバグ対応，および，ISP 環境における事前動作確認の拡充

2)ISP 間連携を補完する CHAT サービス等の導入
3)実験参加 ISP への事前トレーニングの拡充
4)トレースバック・管理センターの人員と設備の増強
5)実験記録用紙などの改定

3.2 実証実験の様子

我々は, ISP-15 社と研究所-3 組織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, 専用 PC1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. 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. そして, 実験開始前にトレースバック管理センターと ISP-15 社で操作練習を実施した.

最初に, a) ハッシュ・テーブル保持時間の最適値の調査, b)誤検知率の調査, c)プローブ性能の上限を超えるトラフィックの見逃し率調査, を実施した.

次に, 模擬攻撃を使用した実験を総計 6 回実施した. a)被害役 ISP-1 社と攻撃役 ISP-13 社, および, 被害役 ISP-14 社と攻撃役 ISP-1 社によるシナリオに沿った DDoS 攻撃対応. b)被害役 ISP-N 社と攻撃役 ISP-M 社による攻撃回数数回のシナリオに沿った DDoS 攻撃対応. c)攻撃役 ISP-N 社と被害役・中継役各 ISP-1 社によるシナリオに沿った DNS リフレクション攻撃対応. d)異なるトレースバック・システムによるシナリオに沿った DDoS 攻撃対応. e)シナリオのない DDoS 攻撃対応. f)障害発生時のシナリオのある DDoS 攻撃対応.

最後に, 実インシデント対応実験を 2 回実施した.

3.3 実証実験結果

2009 年 5 月から 9 月までの 5 ヶ月間で実施した.

1)性能測定

a)ハッシュ・テーブル保持時間の最適値調査

トレースバック処理時間を2パターンの構成で測定した. 1つ目のパターンは, 各 ISP のトレースバック・システムをフルメッシュで接続し, 攻撃パケットを検知した ISP からトレースバックリクエストを他のすべての ISP に向けて送信する. この構成で模擬攻撃の追跡を 20 回測定し, 全て 1.0 秒以下で処理が完了した.

2つ目のパターンは, 各 ISP のトレースバック・システムを直列に接続し, 攻撃パケットを検知した ISP からトレースバックリクエストを順番に伝達する. ISP を 13 ホップ直列に構成し, 模擬攻撃の追跡を 20 回測定し, 平均 3.0 秒で処理が完了した.

今回の実証実験環境では, ハッシュ・テーブルの保持時間は 4sec 程度が望ましいことが分かった.

b)誤検知率の調査

既知のハッシュ方式より誤検知率が少ない提案方式を考案し, 誤検知率の理論式も導出した. 提案方式の効果および理論式の検証ために, 2パターンの誤検知率の測定実験を行った.

1つ目のパターンは, 1台のプローブ上で, 既知方式と提案方式を切り替えて誤検知率を測定する試験である. 表 1 のように, 提案方式の方が誤検知率は小さいく, 理論値と実測値も一致した.

表 1 既知ハッシュ方式と提案方式の誤検知率比較

ﾌﾟﾛｰﾌﾞ	ﾄﾗﾌｨｯｸ	ﾋﾞｯﾄ幅	方式	誤検知率	
				測定値	論理値
H	890 Mbps	20 bit	既知	0.223	0.221
			提案	0.083	0.083

2つ目のパターンは, 15 の ISP 環境に設置した各ソフトウェアプローブにおいて誤検知率の実測値と理論値が一致するかどうかを確認する試験である. 表 2 のように, おおよそ理論式と誤検知が一致した.

表 2 各ﾌﾟﾛｰﾌﾞにおける誤検知率測定結果

ﾌﾟﾛｰﾌﾞ	ﾄﾗﾌｨｯｸ	ﾋﾞｯﾄ幅	方式	誤検知率(*10^{-6})	
				測定値	論理値
A	445	26 Bit	提案	5.78	3.65
B	440			3.46	3.57
C	320			3.07	1.89
D	180			0.40	0.60
E	105			0.31	0.20
F	105			0.25	0.20

c)トラフィック見逃し率の調査

プローブがパケットをダイジェストテーブルに記録する処理が追いつかない場合, 見逃しが発生する. 我々は専用ハードウェアのハードウェアプローブと,

Linux 上で動作するソフトプローブを開発した. なお, 事前のテストベッド試験で, ソフトウェアプローブは約 300Mbps まで, ハードウェアプローブは 10Gbps までのトラフィックを取りこぼさないことを確認していた.

実証実験の環境での性能を発揮できるかを確認するためにパケットの見逃し率を測定した. 表3のように. ソフトウェアプローブは実ネットワーク環境下でもテストベッド上と同程度の処理性能であった, ハードウェアプローブは実トラフィックでも見逃しは発生しなかった.

表 3　見逃し率測定結果

ﾌﾟﾛｰﾌﾞ	ﾄﾗﾌｨｯｸ	ﾌﾟﾛｰﾌﾞ	ﾋｯﾄ数/問合せ数	見逃し率
A	※445	ｿﾌﾄ	653/2040	0.680
B	440		1635/2040	0.198
C	320		1799/1800	0.001
D	180		1800/1800	0.000
E	105		1860/1860	0.000
F	105		2220/2220	0.000
H	890	ﾊｰﾄﾞ	2040/2040	0.000

※50%ｻﾝﾌﾟﾘﾝｸﾞされたﾄﾗﾌｨｯｸ

2) 模擬攻撃実験

2-1) DDoS 攻撃対応

トレースバック・オペレーションの課題検証を行うため, DDoS 模擬攻撃を用いて, 様々な実験を ISP-15 社と TB 管理センターで実施した. TB 管理センターには, 次の役割を有するメンバーを配置した.

・責任者:申告されたインシデントの追跡を判定
・オペレーター:オペレーションの実施
・記録:チェック内容の記録
・ISP サポート:ISP への連絡と問題発生時の対応
・進行管理:状況の管理とトラブル発生時の状況判断
・攻撃役:模擬攻撃サーバから模擬攻撃を実行
・被害役:模擬攻撃の検知と ISP への被害申告

a)1 対 13, 14 対 1

本実験では, 1ヶ所の ISP へ DDoS 攻撃が発生した場合に, トレースバック・システムにより攻撃元を探索可能でき、かつオペレーションを実行可能であるか検証した. また, 逆に同時に複数の攻撃を行っている利用者がいる ISP が攻撃対処のオペレーションができるかどうか検証した. なお, 攻撃を受ける ISP, 攻撃が発信される ISP は事前に確定済である.

実験全体を通しては, 想定時間内に全ての処理が収まっていることが確認できた.

a-1)攻撃役 ISP-1 社・被害役 ISP-13 社のケース

被害者から各 ISP へ被害が申告され, TB 管理センターに同時に 13 件の対処が依頼され, TB 管理センターと攻撃役 ISP に処理が集中する. 今回の実験においては, 処理の遅延や停止などのトラブルが発生することは無かった.

a-2)被害役 ISP14 社・攻撃役 ISP1社のケース

各 ISP とも特に問題はなく対応を行うことが確認できた. しかし, 被害役 ISP が複数回の確認依頼を被害者へ行う事態や, 一部の攻撃が探索できない事態が発生し, 攻撃元未発見時の対応処理を行うこととなったが, 問題なく処理を実行することができた.

b)N 対 M*L 回

複数の攻撃役 ISP と被害役 ISP をそれぞれ, 3つ, 5 つのグループに分けた. ここでは, どの ISP も同時に複数の攻撃対処(被害対応, 攻撃対応)オペレーションが実行できるか検証した.

・攻撃役 ISP 2 社, 被害役 ISP 1 社を 5 組
・攻撃役 ISP 1 社, 被害役 ISP 2 社を 3 組

本実験は, 被害役 ISP, 攻撃役 ISP が同時に複数の攻撃へ対処する, 現実に近い環境を想定した.

攻撃については, 被害者からの申告が検索できない等が発生したが, 処理手順に基づき対応できた.

TB 管理センターでは複数の攻撃が発生し受付を逐次で行うため, 時間がかかることが確認された.

c)シナリオの無い攻撃

実環境同様いつどのような事態が発生するか分からない中でオペレーションが実行できるかを検証した. 攻撃役からランダム, かつ時間差のある攻撃が行われた. 各 ISP のオペレーターは一連の手続きに従い処理を行っており, 自社の役割が事前に設定されていなくても適切な対応を行うことができることが確認できた. また, 各 ISP の対応は, 予め役割が決められている場合と同様に適切に対応することが可能であることも確認できた.

d)異なる TB 間連携

複数の異なるトレースバック・システム間連携の可能性について検証を行った. 攻撃者と被害者が異なるトレースバック・システムに属している環境において, トレースバック・システム間の連携による探索を行った. 我々のトレースバック・システムと別な研究機関が有

するトレースバック・システムを使用した．実験参加ISP は我々のトレースバック・システムに属するものとし，被害者をこの中に設定した．また，模擬攻撃は別な研究機関のトレースバック・システム内から発信されるよう役割設定とした．さらに，本環境においては，2 つの TB 管理センター間のシステムは直接には接続されておらず，トレースに必要な情報を，予め決められたルールによって，メールを用いて交換した．

一方のトレースバック・システム内からの模擬攻撃が，異なるトレースバック・システムの被害者で検出されたことをトリガーに，双方のトレースバック・システム間での連携実験を行うことができた．連携にあたっては，被害役 ISP から，連携先トレースバック・システムへトレースに必要な情報（時刻，ハッシュ値）を送信した．引き渡された後の情報については，システム上の差異もあり攻撃元の特定は行うことができなかった．

e)障害発生対応

本実験では，トレースバック・システム内のシステム障害や，オペレーション・ミスなどの問題によりトラブルが発生した際の，対応結果の変化について検証を行った．

2 つの障害として，「システムの故障」，「TB 管理センターのオペレーション・ミス」をシナリオに織り込み実行した．被害役 ISP -1 社，攻撃役 ISP-4 社，を割り当て，各社にはどのような問題が発生するかは伝えず，通常の DDoS 模擬攻撃対応を行ってもらうことで，実験を進めた．想定した問題は以下の通りとした．

ア）ある ISP ではコントローラが故障しており，ここからの攻撃は検出されない．

イ）ある ISP ではシステム障害により誤検知（攻撃が無いのにあったと検知）が発生．

ウ）TB 管理センターのオペレーション・ミスで，攻撃の出ていない ISP へ対応を依頼．

イ），ウ）は，ISP は自社からの攻撃が出ていないことを確認した上で，TB 管理センターへ攻撃の事実が確認できない旨を連絡できた．誤検知の場合でも，ISP 側と密な確認を行うことでその真偽を確認できることが検証できた．

ア）については，検出できていない箇所への攻撃確認依頼を行うことで，攻撃発信事実を確認し，攻撃の停止を行うことが可能となった．実験環境においては，常に各機器の動作監視を行っており，故障などのトラブルは事前に把握することも可能であるため，このような対応も可能であると考えられる．

2-2）DNS リフレクション攻撃

DNS リフレクション攻撃実験は，中継役 ISP-1 社に DNS リフレクション用コントローラ 1 台，DNS リフレクション用プローブ 1 台を追加で設置した．DNS リフレクション用コントローラ装置は，攻撃先の DNS reply パケットのハッシュ値を DNS リフレクション用プローブに問い合わせる．DNS リフレクション攻撃を検出すると，攻撃元の DNS query パケットのハッシュ値を結果として得られるので，このハッシュ値に対してトレースバックを繰り返し，最終的に集約された結果が DB に登録される．

トレースバック管理センターはパケットの変化が発生している情報を把握できるが，ISP 側からの情報の見え方やトレースバック手順が DDoS 実験と同様であった．

実験は，攻撃役 ISP-2 社と被害役・中継役各 ISP-1 社によるシナリオ A，および，攻撃役 ISP-5 社と被害役・中継役各 ISP-1 社によるシナリオ B を実施した．

シナリオ A では，問題無くシナリオ通りに DNS リフレクション攻撃に対処出来る事が確認できた．

シナリオ B では，対応した攻撃役 5 社のうち，4 社は問題無くシナリオ通りに対処できたが，攻撃役 1 社は攻撃元 DNS request パケットを確認できずに対処失敗となった．原因については，攻撃元 DNS request パケットが送信速度も低いため，IDS で検出されなかったためと考えられる．

また，攻撃役 ISP には攻撃先パケットのプロトコル，src アドレスとポート番号，dst アドレスとポート番号が伝えられるが，DNS リフレクション攻撃に対処するためには src アドレスと dst アドレスを入れ替えて考える必要があることを確認した．パケットが変化する攻撃に対処する場合には，今回の実験で ISP に伝えられる情報は不十分であった．

3）実インシデント実験

実インシデント実験は，実証実験に参加頂いた ISP のいずれかのネットワーク配下に，研究機関-3 組織のハニーポットやセンサーを設置し，ハニーポッドやセンサーでの検知結果を元にした調査依頼から，実攻撃元を追跡する実験である．この実験により，模擬攻撃ではなく実攻撃もプローブで検知できるのか，

攻撃元まで追跡ができるのか，を確認する．

2 回の実インシデント実験では，研究機関側で攻撃を検知し，それ基づいた追跡依頼で調査を行ったところ，被害者である研究機関の上位にあたる ISP のプローブで対象を検知していることが確認できた．しかし，攻撃元まで追跡するには至らなかった．理由は，追跡したパケットが日本以外からの送信されていること(攻撃元，および経路上にプローブが設置されていないこと)と言える．

実攻撃パケットであってもプローブで検出できることが確認された．トレースバック・システムの導入拡大で実攻撃を追跡出来る可能性が高いことを確認した．

4　実運用に向けた課題

今回の実験環境は全てのシステムや ISP 側の環境が一通り見渡せる状況にあった．今後，数多くの ISP へ本システムが導入された場合に本実験と同じレベルの管理を行うためには，より大規模な体制と管理システムが必要になると考えられる．

また，実際の運用では 24h7d の運用も検討することが必要になってくると考えられる．このような組織を維持するためには，更なるマネジメントルールの確立が必要とされる．特に，トレースバック・システムの障害やオペレーション・ミスによる問題の発生を防ぐために，監視機能の強化や冗長化などのシステム面の強化と，オペレーションの自動化などによる，ヒューマンエラーが発生しない仕組みの導入が必要であると考えられる．

同様の方式を持つ異なるトレースバック・システムとの連携実験も行ったが，事前に仕様の違いなどの調整を行わなかったため，精度の高いトレースは行えなかった．インターネットが様々な組織により運営されていることを考えると，日本国内だけでも複数のトレースバック・システムの方式が存在する可能性がある．探査精度を高めるためにも，システム間連携の仕組み，運用ルール・マネジメントルール等の整備が必要であると考えられる．

5　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[1]，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[2]，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[3]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[5]を行った．そして 2008 年に ISP-5 社で事前実験[4]を実施した．

本書では，2009 年に ISP-15 社と研究機関-3 組織で実施した実証実験の結果を報告し，若干の考察を行った．今後は，トレースバックの実導入に係る課題の詳細調査を行う予定である．

6　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．

参考文献

[1]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）

[2]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）

[3]若狭賢，木村道弘，中谷浩茂，甲斐俊文，橋口輝，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 ISP 環境への配置と事前実験シナリオの策定，コンピュータセキュリティシンポジウム 2008（CSS2008）

[4] 若狭賢，木村道弘，中谷浩茂，甲斐俊文，橋口輝，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 ISP 環境を利用した事前実験結果，第 46 回コンピュータセキュリティ研究発表会（CSEC46）

[5]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

[6]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.