成果概要書

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

（１）研究の目的

インターネットにおけるトレースバック技術に関しての実運用環境への実装を目指した研究開発を行う。

具体的には、基盤となる全体のアーキテクチャの設計、トレースバックアルゴリズムの開発、トレースバック用データ収集装置の開発、及び、それらを統合したトレースバックプラットフォームの開発を行い、更に、当該プラットフォームの実装及び運用体制について検討し、実運用環境への実装に向けた統合試験・検証を行う。

（２）研究期間

平成１７年度から平成２１年度（５年間）

（３）委託先企業

日本電気（株）＜幹事＞、国立大学法人奈良先端科学技術大学院大学
パナソニック電工（株）、（株）クルウィット
財団法人日本データ通信協会、（株）KDDI 研究所

（４）研究予算（百万円）

平成１７年度	３００（契約金額）
平成１８年度	３００（　〃　）
平成１９年度	２５３（　〃　）
平成２０年度	２１１（　〃　）
平成２１年度	１８７（　〃　）

（５）研究開発課題と担当

課題ア：全体アーキテクチャの設計

1. トレースバック機構を構築する上で考慮するべき事項の網羅
（国立大学法人奈良先端科学技術大学院大学）
2. 基本的なトレースバック方式の開発
（㈱ＫＤＤＩ研究所）
3. トレースバックシステムの相互接続アーキテクチャの開発
（国立大学法人奈良先端科学技術大学院大学）

課題イ：トレースバックアルゴリズムの開発

1. IP パケットトレースバックアルゴリズムの開発
（パナソニック電工㈱）
2. アプリケーショントレースバックアルゴリズムの開発
（㈱クルウィット）
3. 異なるレイヤ由来の情報からトレースバック能力を向上させるアルゴリズムの開発
（㈱クルウィット）

課題ウ：トレースバック用データ収集装置（プローブ装置）の開発

1. IP トレースバック用データ収集装置の開発
（㈱ＫＤＤＩ研究所）
2. アプリケーショントレースバック用データ収集装置の開発
（日本電気㈱）

課題エ：トレースバックプラットフォームの実証実験

1. 実装および運用体制の検討
（財団法人日本データ通信協会）
2. 攻撃パターンの想定
（財団法人日本データ通信協会）
3. 動作検証
（財団法人日本データ通信協会）

課題オ：テーマ全体管理
（日本電気㈱）

（６）これまでの主な研究成果

特許出願：国内出願　１９件　　外国出願　　１件
外部発表：研究論文　３９件　　その他研究発表　４３件
報道発表　　１件　　展示会　８件　　標準化提案　２件

具体的な成果

課題ア　全体アーキテクチャの設計・改修

ア－１　トレースバック機構を構築する上で考慮すべき事項の網羅

トレースバック技術に関する考慮すべき事項を網羅した文書を作成し、ＮＩＣＴセキュリティリサーチセンターとの協力の元 ITU-T にてトレースバック技術に関する標準化議論を開始した。

ア－２　基本的なトレースバック方式の開発

課題ア-3 の相互接続アーキテクチャの実装から通知されるトレー

ス結果を課題エの定める運用ポリシーに則って開示するイベントDBと、ISP オペレータ間での柔軟な情報共有を可能とするトラブルチケットシステムからなるオペレータ間連携支援システムを開発し、20 年度の事前実験の結果を踏まえて改良し、実証実験を完遂した。

ア－３　トレースバックシステムの相互接続アーキテクチャの開発

課題ア-2 のオペレータ間連携支援システム、課題イ-1 、ウ-1 のＩＰトレースバックシステム、課題イ-2、イ-3、ウ-2 のアプリケーショントレースバックシステム、またブラックホール方式やサンプリング方式などの基本方式と結合可能なトレースバックシステム相互接続アーキテクチャを開発し、平成 21 年度の実証実験やＮＩＣＴ北陸リサーチセンターでの大規模検証などで DNS をもちいた踏み台攻撃も追跡可能であることを確認した。

課題イ　トレースバックアルゴリズムの開発

イ－１　IP パケットトレースバックアルゴリズムの開発

IP パケットトレースバックアルゴリズムおよびそれを搭載したトレースバックシステムの開発を行った。

本システムには、次のような特徴を持たせている。

- 改良 Hash 方式を用い、高速・高精度検知の実現している。また、プライバシ保護、適法性を考慮している。
- データ収集装置の数（設置コスト）を最小限に押さえられるシステムとしている。
- 機器障害の検出、障害レベルに応じた自動復旧機能を有し、信頼性と安定性を向上させている（フェールセーフも確保している)。
- IPv6 環境での有効性も理論レベルで確認できている。
- 本システム単体で動作するトレースバック機能（流入口探査）に加え、InterTrack（課題アで開発の AS 間トレースバックシステム）との連携による発信 ISP 探査も可能となっている。
- アプリケーショントレースバック（課題イ-2）との連携による踏み台攻撃探査も可能となっている
- 本システムについて、実インターネットでの有効性、実用性の検証を行った。

イ－２　アプリケーショントレースバックアルゴリズムの開発

SMTP と DNS の 2 つのアプリケーションレベルの情報を用いて踏み台検出を行うアルゴリズムの開発を行った。実験・評価により、通踏み台検出アルゴリズムの有効性を確認した。収集した情報に対してハッシュ化機能を実装し、匿名化機能を有している事を確認した。インバウンド通信とアウトバウンド通信の時間差が、3 分以内の攻撃の検出ができる事を確認した。

イー３　異なるレイヤ由来の情報からトレースバック能力を向上させるアルゴリズムの開発

IP トレースバックとアプリケーショントレースを組み合わせることによって、より広範囲の追跡が行えるシステムの開発を行った。実験・評価を行い、組み合わせにより、より広範囲にトレースバックの結果が得られる事を確認した。また、解析時間が 5 分以内に収まることを確認した。日本の ISP の実ネットワーク上での実証実験においても、有効性を確認できた。

課題ウ　トレースバック用データ収集装置の開発

ウー１　IP トレースバック用データ収集装置の開発

10Gbit/s のトラヒックに対して、取りこぼし無く IP パケットを分類、情報収集可能なハードウェアプローブを開発した。また、同等の機能を安価に実現するソフトウェアプローブを開発し、ネットワークの最適箇所に設置することを可能とした。両者を用いて実証実験を完遂し、有用性、安定性を確認した。更に、IPv6 に対応した IP トレースバック用ソフトウェアプローブを実装、評価した。

ウー２　アプリケーショントレースバック用データ収集装置の開発

電子メールにおける踏み台攻撃及び DNS 攻撃における踏み台攻撃について、アプリケーショントレースバック用データ収集装置を開発し、トレース機能、パケット収集機能、匿名化機能について評価を実施し、実用的な時間で実行可能であること及び 10Gps トラフィック環境において実行可能であることを確認した。また、15-ISP による実証実験において模擬 DNS-Refrection 攻撃を、StarBED による仮想 ISP 環境実験においてインバンド通信とアウトバウンド通信の時間差が 3 分以上ある模擬電子メール踏み台攻撃を検知、トレースできることを確認した。

課題エ　トレースバックプラットフォームの実証実験

エー１　実装および運用体制の検討

19 年度に策定した各種文書案を、専門家による詳細の法的レビューの実施後に、平成 20 年 10 月からの事前実験に参加する ISP へ紹介し、意見・要望を集約し、対応した。策定された各種文書案をベースにしたマネージメント規約は ISP に高く評価され、平成 20 年 10 月から 5-ISP による事前実験、平成 21 年 6 月からの 15-ISP による実証実験、が無事遂行できた。

エー２　攻撃パターンの想定

19 年度に策定したトレースバックで対処すべき攻撃候補案を、平成 20 年 10 月からの事前実験に参加する ISP へ紹介し、意見・要望

を集約し、対応した。また、アンケート・ヒアリング調査で、幅広く ISP へ対処すべき攻撃候補案に係る意見と、最新の攻撃情報を収集した。そして、平成 21 年 6 月からの 15-ISP による実証実験では、ISP 現場で対応に苦慮している DDoS 攻撃、および、踏み台攻撃対応として DNS-Refrection 攻撃、に即した模擬攻撃実験を実施できた。

エー３　動作検証

21 年度の実証実験の課題抽出のため、平成 20 年 10 月から 5-ISP による事前実験を実施した。抽出された課題を解決し、平成 21 年度は 15-ISP による実証実験を実施した。実証実験では、１）大規模な ISP 環境におけるトレースバック・パフォーマンスの測定、２）2 種類の模擬攻撃を使用したシナリオ実験、３）3 研究機関の協力を得て、実インシデント実験、を実施した。この実験は国内外に認められ、IEEE の国際学会で 3 回発表した。

（７）研究開発イメージ図

「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」の開発成果について

1. 施策の目標

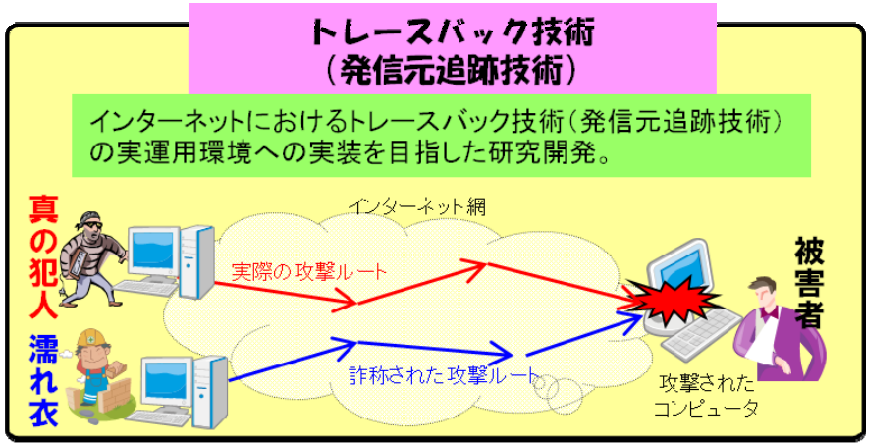
・悪意ある通信からネットワークを守る通信技術を実現し、安心・安全な通信インフラを実現する。具体的には、2013年までに、インターネットにおけるトレースバック技術を実用化する。

2. 研究開発の背景

・情報通信ネットワークは、もはや我が国の社会・生活基盤の一部であり、それを安心して安全に利用できる環境を確保することは不可欠。一方、対処すべき課題が時とともに変化していくことから、今後とも時宜に応じた研究開発を適切に実施していくことが必要。それらを一括して「情報セキュリティ技術」として扱い、社会・生活基盤の充実の観点から、我が国全体及び政府として重点的に取り組むべき研究開発課題とされている。

3. 研究開発の概要と期待される効果

・トレースバック技術とは送出機器のアドレスを詐称している通信であっても、本当の送出元ISPを探知しうる技術。具体的には，基盤となる全体のアーキテクチャ設計、トレースバックアルゴリズムの開発、トレースバック用データ収集装置の開発、及びそれらを統合したトレースバックプラットフォームの開発を行い、更に当該プラットフォームの実装及び運用体制について検討することで、実運用環境への実装を目指す。



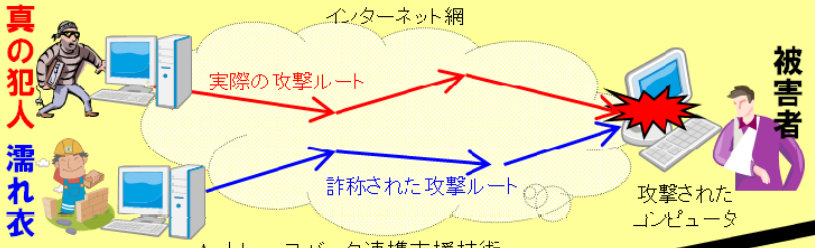
4. 研究開発の期間及び体制

平成17年度～平成21年度（5年間）
NICT委託研究（日本電気株式会社、国立大学法人奈良先端科学技術大学院大学、パナソニック電工株式会社、株式会社クルウィット、財団法人日本データ通信協会、株式会社KDDI研究所

トレースバック技術の主な成果

トレースバック技術（発信元追跡技術）

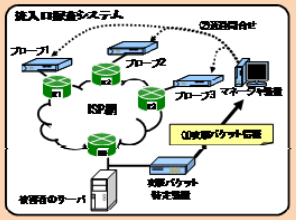
インターネットにおけるトレースバック技術（発信元追跡技術）の実運用環境への実装を目指した研究開発。



A トレースバック連携支援技術
B IPトレースバック技術
C アプリケーショントレースバック技術

IPトレースバック技術

●IPパケットを詐称した攻撃(特にDoS、DDos攻撃)に対する高性能かつ実用的なトレースバックアルゴリズムの開発が不可欠。
●本研究開発では、機能や性能などの技術的な部分に加え、実用性・効果・コスト・デプロイメント・適法性を考慮した方式を世界で初めて提案、開発。プローブ装置として10Gbpsを達成。
●15-ISP協力の下、実運用環境の実証実験により有効性を確認。



流入口探索システム

情報処理学会 DICOMO 2008において最優秀論文賞を受賞

トレースバック連携支援技術

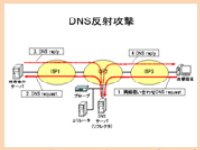
●トレースバック技術の選択は各ISP事業者に閉じており、また事業者間に跨るトレースバックはオペレータによるメールや電話を介して行われているため、システム的なサポートの実現が課題。
●本研究開発では、トレースバックシステム相互接続(右図)、オペレータ間連携(左図)を世界で初めて開発。
●15-ISP協力の下、実運用環境の実証実験により有効性を確認。

オペレータ支援システム

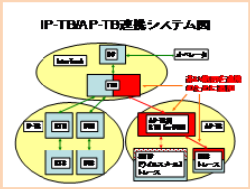

大規模シミュレーションにおけるトレースバック動作状況

アプリケーショントレースバック技術

●IPトレースバックでは検出できない踏み台攻撃(攻撃を受けたホストにおいてさらに他のホストに攻撃を行う手法)に対応するトレースバックアルゴリズムの開発が不可欠。
●ウイルスメールやDNS反射攻撃など多様なアプリケーションに対応可能な汎用的アプリケーショントレースバックフレームワーク、IPトレースバックと相補的に組み合わせることにより、単一のインターフェースからトレースバック結果が得られる方式を世界で初めて開発。
●15-ISP協力の下、実運用環境での実証実験により有効性を確認。



DNS反射攻撃の概念図



IP-TB/AP-TB連携システム構成

トレースバック技術の外部投稿成果、主な発表

1．特許出願および論文発表等

	特許出願	論文	研究発表	標準化提案	報道発表	展示会	その他
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	20	39	35	2	1	8	8

2．研究成果発表会等の開催について

（1）ワークショップを毎年主催し、トレーバック技術の周知と実証実験への参加を呼びかけ

2009年に実施のワークショップでは、総務省の担当官、NICT自ら研究チーム、NICT委託研究チーム、T-ISAC会員企業、ISP企業が一同に会し、最新の研究成果を紹介するとともに、実証実験実施に向けたトレースバック技術への期待や、抱える課題について議論。開催日は2009年3月5日で、42名が参加。
それ以前は、2008年3月5日、2007年3月5日（広域モニタリングシステムと合同開催）、2006年1月24日、の計4回を開催。

※写真は2009年3月5日の様子

（2）Interop ShowNetへ出展

Interopは、ネットワークコンピューティングに特化したテクノロジーとビジネスの最も権威のあるイベントで、世界5都市にて毎年開催されている展示会。2008年は6月11日～13日、2009年は6月10日～12日に、幕張メッセで開催。
2008年は、Interopにて構築される最先端のネットワーク環境であるShowNetに接続し、1つのISPにトレースバックシステムが導入された場合の構成を検討するために、ShowNetを1つのISPと仮定して、出展者側に設置した攻撃検知システムが検知した攻撃の追跡を実施。2009年は、実証実験に向けたこれまでの取り組みについての展示を実施。

トレースバック技術の成果展開・普及等について

- NICTセキュリティリサーチセンター・トレーサブルネットワークグループの協力の下、ITU-Tでのトレースバック技術の国際標準化議論を進めていく。
- 研究成果である各種論文、開発したソフトウェア、実証実験の成果等を公開し、大学や企業、研究機関等によるネットワークセキュリティの研究推進を支援する。
  - http://intertrack.naist.jp/
  - https://www.telecom-isac.jp/tb/