「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

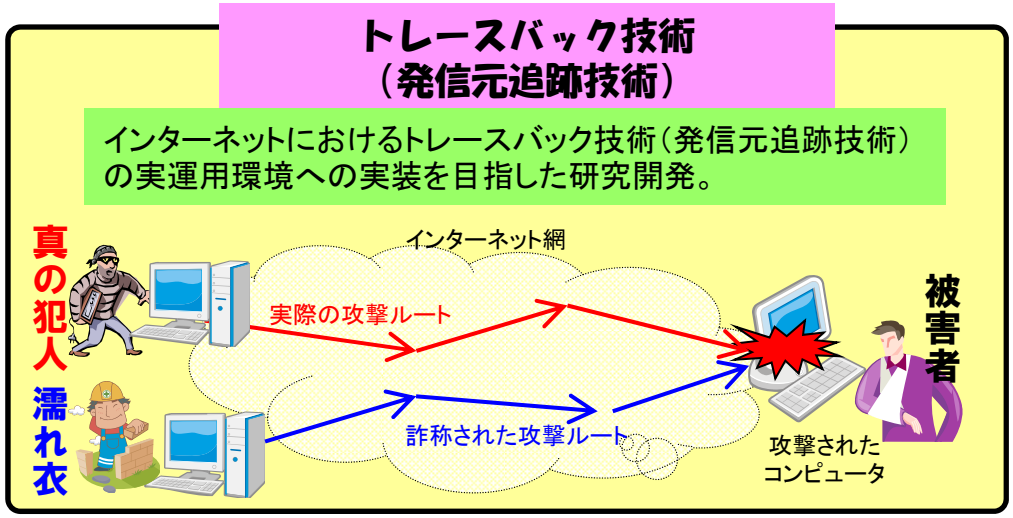
・悪意ある通信からネットワークを守る通信技術を実現し、安心・安全な通信インフラを実現する。具体的には、2013年までに、インターネットにおけるトレースバック技術を実用化する。

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。



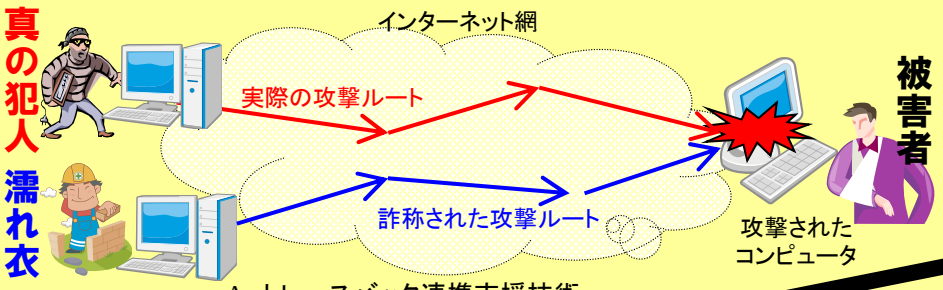
4. 研究開発の期間及び体制

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）

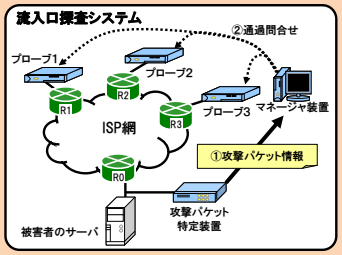
インターネットにおけるトレースバック技術（発信元追跡技術）の実運用環境への実装を目指した研究開発。



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。



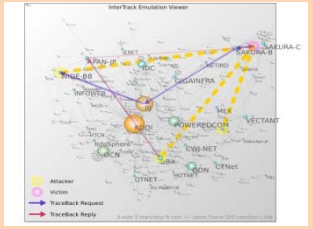
流入口探索システム

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。

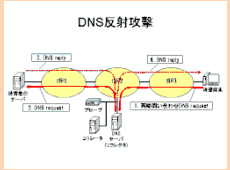
オペレータ支援システム



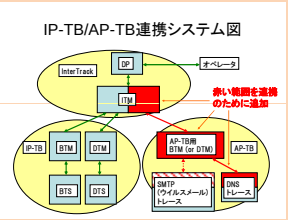
大規模シミュレーションにおけるトレースバック動作状況

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/