

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
松下電工(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(") |

(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
(株)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

(松下電工(株))

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

(株)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

(株)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

(株)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(株))

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(株))

(6) 主な研究成果

特許出願： 5 件 (累計 9 件)

外部発表： 2 3 件 (累計 4 1 件)

具体的な成果

(1) トレースバック連携支援技術を開発

複数 ISP に跨るトレースバックシステム連携、オペレータ間連携の実装を完了

(2) DoS/DDoS 攻撃対策技術を開発

攻撃流入口探査による IP トレースバックについて、基本的な連携動作の確認を実施。また、フィールド試験により、実運用環境での実証実験に向けた課題を抽出。

(3) 踏み台攻撃検知技術を開発

ウィルスメール、および、DNS を利用した踏み台攻撃検知によるアプリケーショントレースバックについて、方式を開発し、その実装を実施。

(4) ISP 事業者の合意形成の準備

実証実験のための契約書案、ポリシー案を作成し、かつ、実験案の作成を実施。

(7) 研究開発イメージ図

- ・課題ア-2 オペレータ間のトレースバック連携の支援、
- ・課題ア-3 異種トレースバックシステムの協調・連携
- ・課題イ IP,アプリケーショントレースバックシステムの提供
- ・課題ウ トレースバック用データ収集装置の開発
- ・課題エ-1 事業者間の合意形成
- ・課題エ-2 実攻撃パターンの策定
- ・課題エ-3 実環境での検証

