別紙３

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（　〃　）

（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）主な研究成果

特許出願：　　５件（累計１４件）
外部発表：　　２５件（累計６９件）

具体的な成果

(1) トレースバック連携支援技術を開発

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し、実証実験環境での複数ドメインに跨る評価検証に使用できるように強化。

(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、データセンタにおける Close 試験，ISP 環境を利用した事前実験を通じて、実運用環境での実証実験に向けた課題を抽出し、実装を実施。

(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、単一のインターフェースから IP トレースバックとアプリケーショントレースバックを実行するアルゴリズムの設計・開発を実施し，データセンタにおける Close 試験において動作検証を実施。

(4) ISP 事業者の合意形成の準備

平成 19 年度までに策定した実証実験のための契約書案、ポリシ案、実験案の作成を多くの ISP へ紹介し、事前実験及び実証実験へ参加する ISP の募集に成功。また、実際の ISP 環境を利用した事前実験を実施し、実証実験に向けて技術面及び運用面の課題を整理。

（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