資料９－３

トレースバック技術への取り組み

門林　雄基
奈良先端科学技術大学院大学
情報科学研究科

情報通信研究機構
情報通信セキュリティ研究センター

トレースバック技術の必要性

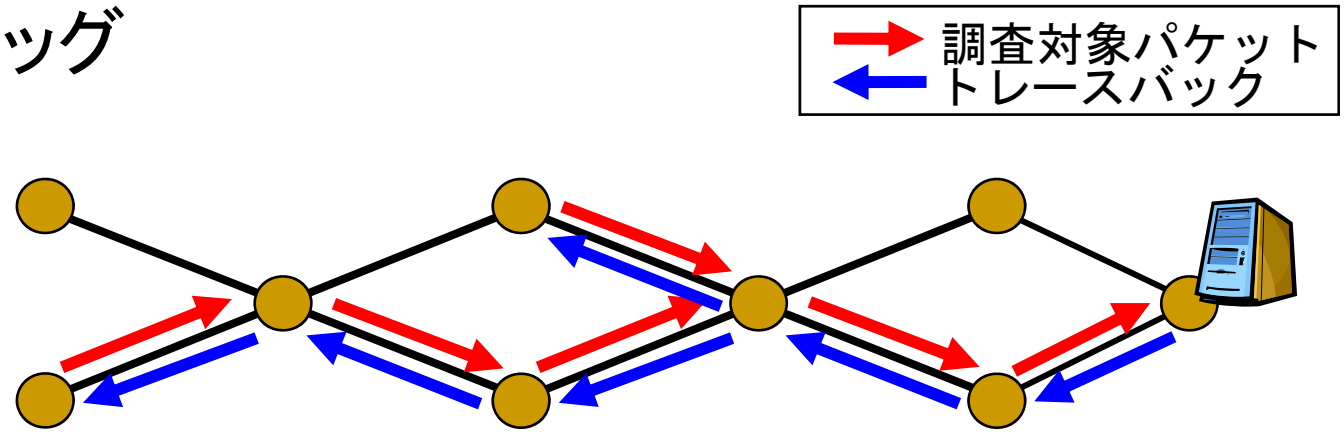
- 通信における責任の喪失
  - 始点アドレスの詐称
  - Webサイト, eメール等における本人確認の欠如

- 上記を悪用した攻撃の増加
  - 商用サイト、政府機関へのサービス妨害攻撃
  - 大量の迷惑メール送信

- トレースバック技術により発信源を特定し、事案解決を迅速化できるケースがある

IPトレースバックが提供する機能

- 「このパケットはどこから来たのか？」
- 流れた経路を復元
- 様々な用途：
  - サービス妨害攻撃や、迷惑メールの発信源を特定
  - 大口顧客の経路監視
  - 経路のデバッグ



現在の研究開発状況

- 2000: プロバイダ内のトレースバック方式研究
- 2004: プロバイダをまたがるトレースバックシステムの開発に着手 (InterTrack)
- 2005: NICT委託研究開始、8社コンソーシアム
- 2007: InterTrack システム稼働、各社センサ統合
  - KDDI, 沖電気, 松下電工によるセンサ
- 2008: プロバイダに設置し、実証実験を開始
- 2009: 大規模実験、技術移転、とりまとめ

活動概要 - 研究開発目標

本研究の最終目標

- トレースバックアルゴリズムの開発とトレースバックプラットフォームの実装、および運用体制の検討を経て、実ネットワークに近い環境を用いて、開発したトレースバックシステムの有効性の検証のために実証試験を実施する。
- これら活動を通し、攻撃がどこから実行されようとしているのかを探索する能動的な警戒手段としての実用的なトレースバックの技術確立を本研究の最終目的とする。

各課題の最終目標

課題　ア　「全体アーキテクチャの設計」

トレースバック技術に対する誤解や過度の期待を解消 。
攻撃フローが存続する間にトレースバックを容易に行う。
相互接続アーキテクチャを設計・実装 する。

課題　イ　「トレースバック・アルゴリズムの開発」

踏み台攻撃を検知することのできる実用的なトレースバックアルゴリズムを開発する。また、プライバシの保護についても既存方法についての検討を行い、盛り込むものとする。

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」

プローブ装置を利用する実用的なトレースバック用のソフトウェアを開発する。また、プライバシの保護機能も動作するものとする。

課題　エ　「トレースバックプラットフォームの実証実験」

課題ア、イ、ウで開発された成果についてトレースバックプラットフォームの実証実験を実施する。

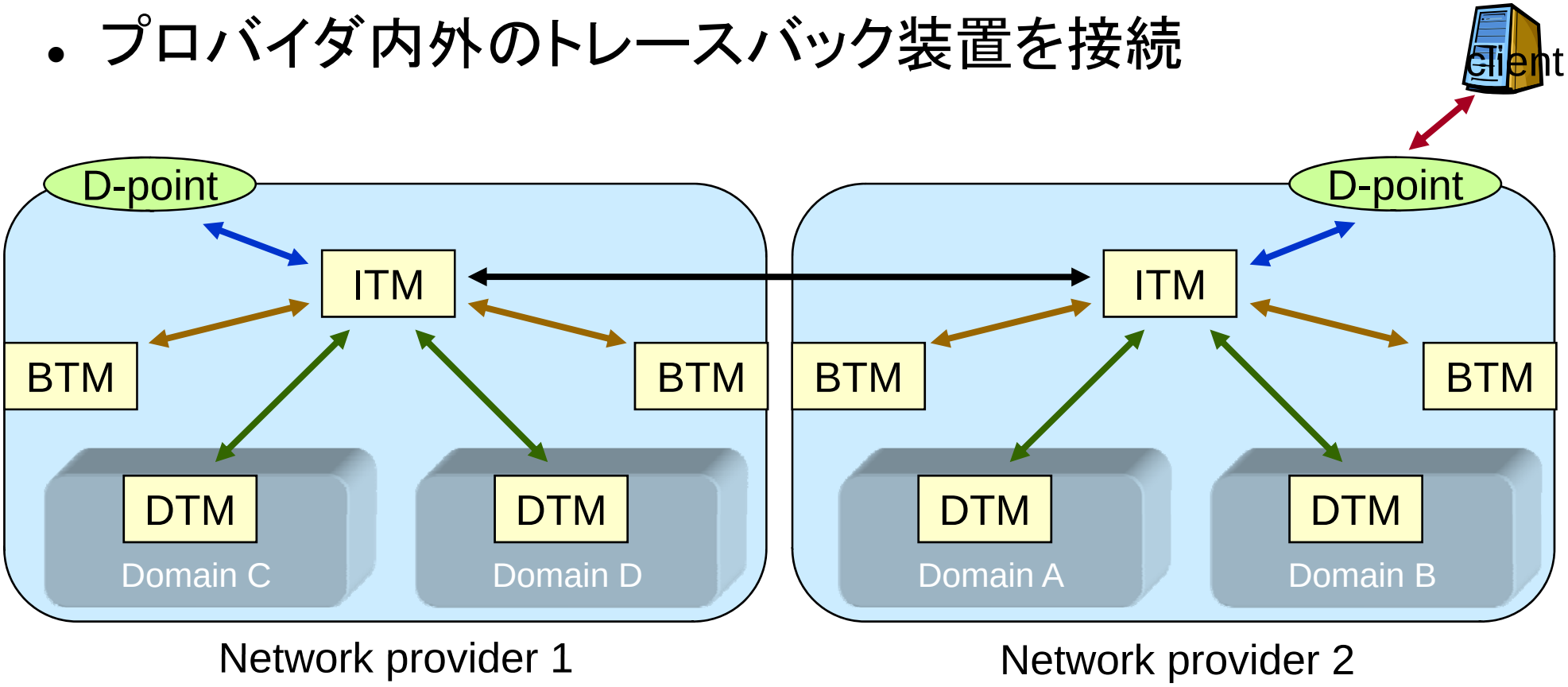
活動概要 - 体制

代表研究責任者　：日本電気株式会社

- **課題 ア　「全体アーキテクチャの設計」**
  - ア - 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）
  - ア - ２　基本的なトレースバック方式の開発　（株式会社ＫＤＤＩ研究所）
  - 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　（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」**
  - イ - １　ＩＰパケットトレースバックアルゴリズムの開発　（松下電工株式会社）
  - 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　（株式会社クルウィット）
  - イ - 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（株式会社クルウィット）
- **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」**
  - ウ - １　IPトレースバック用データ収集装置の開発　（株式会社ＫＤＤＩ研究所）
  - ウ - 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　（日本電気株式会社）
- **課題　エ　「トレースバックプラットフォームの実証実験**
  - エ - 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）
  - エ - ２　攻撃パターンの想定　（財団法人日本データ通信協会）
  - エ - 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」**　（日本電気株式会社）

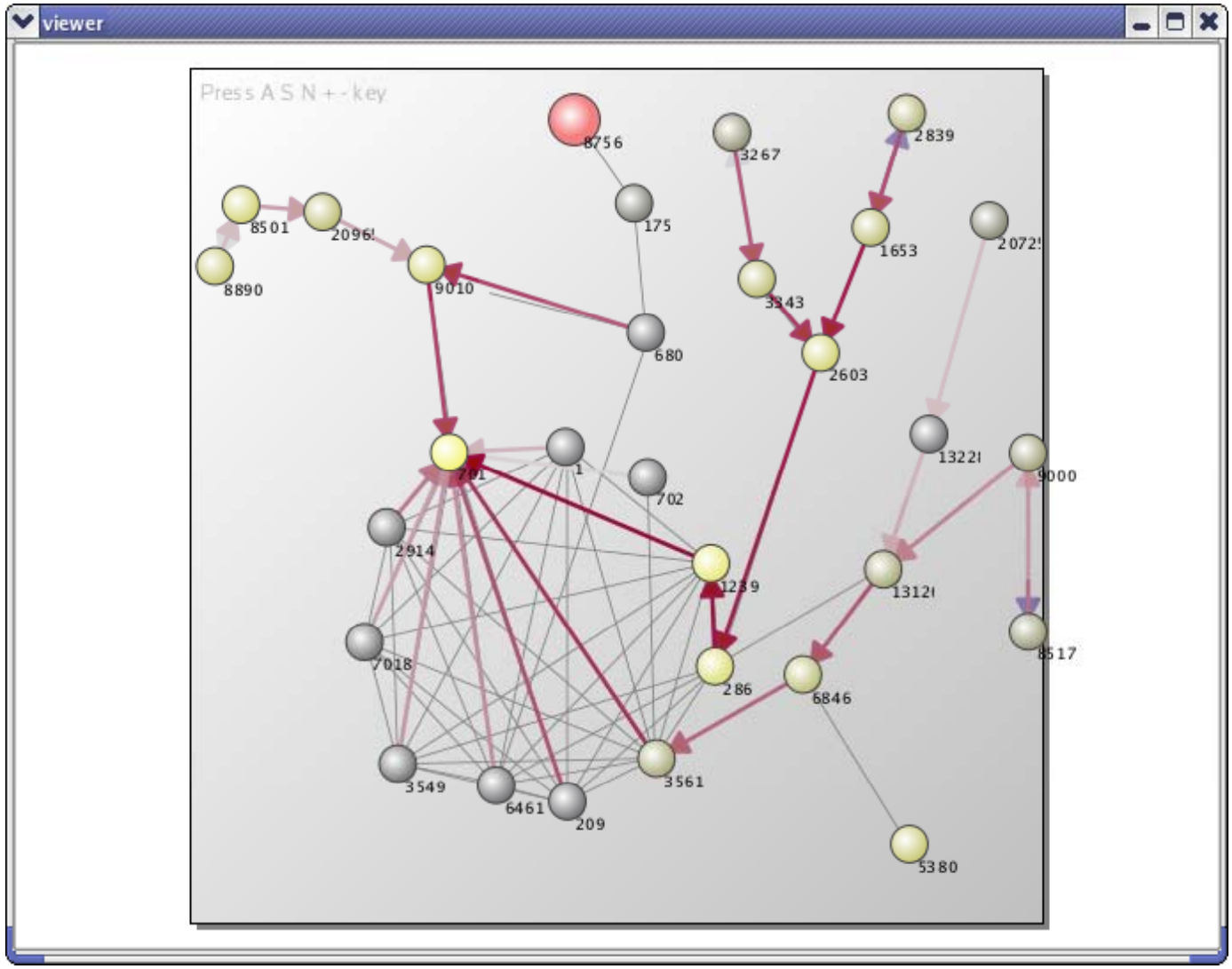
プロバイダをまたがるトレースバックシステム

- InterTrack システム
- プロバイダ内外のトレースバック装置を接続



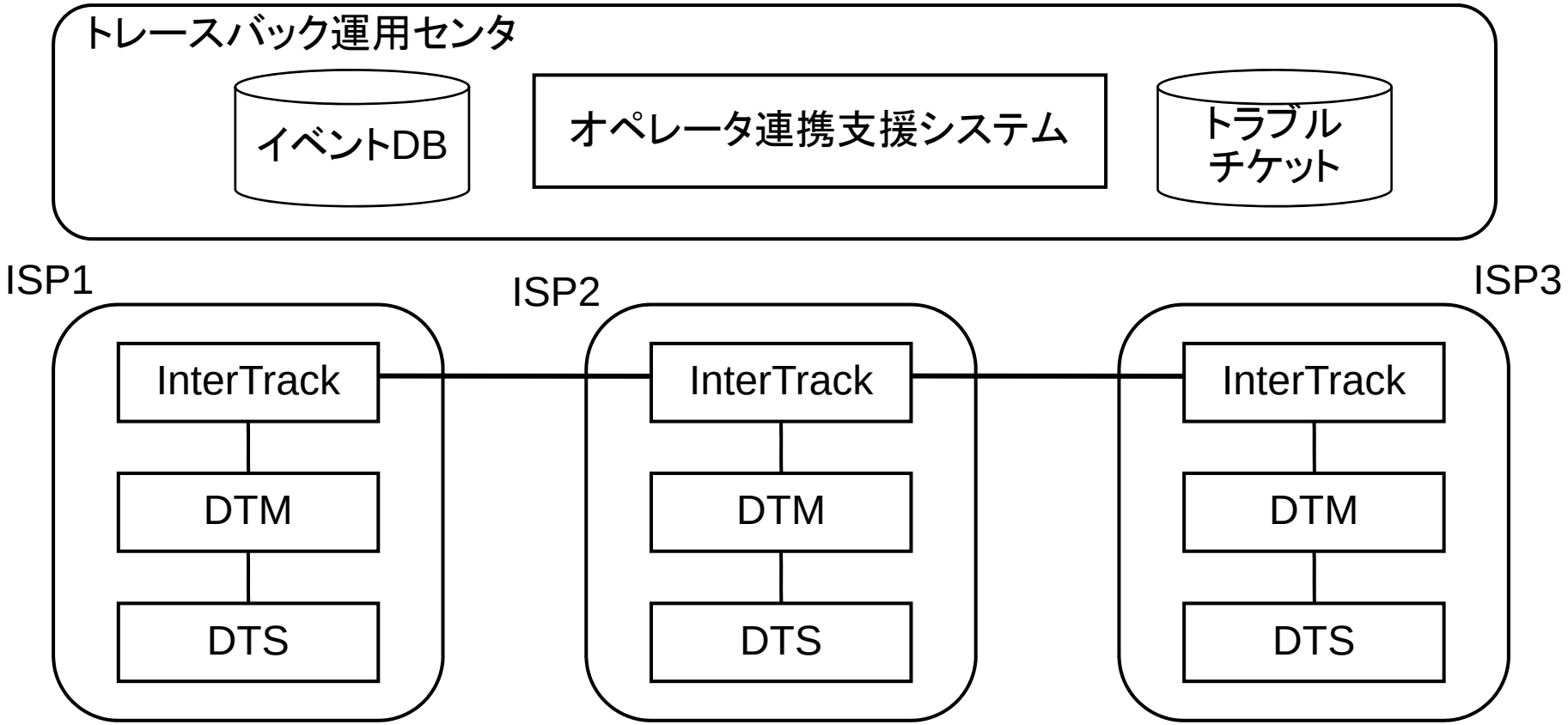
“An Autonomous Architecture for Inter-Domain Traceback across the Barriers of Network Operation”, IEEE ISCC 2006.

InterTrack によるトレースバックの様子



トレースバックから事案対応へ：オペレータ連携支援システム

- InterTrack により攻撃経路を特定
- 経由するネットワークの運用者が、事案ごとに情報共有し、追跡結果をもとに連携して事案対処する



CJKでの国際連携活動方針（私案）

- サイバーセキュリティ問題全般に関する見取り図を共有
  - 技術的 / 社会的 / 社会技術的
  - 研究機関、産業界、法曹界
  - 見取り図に、現在の活動をマッピング
- ギャップ分析
- 共通するギャップについては共同してあたる
  - トレースバック含む

ITUでの国際標準化活動（私案）

- 概念整理、用語整理
  - サイバーセキュリティ参照モデル
  - ネットワークにおけるOSI7階層モデルを手本として
  - 参照モデルにおけるトレースバックの位置づけ
- プロトコルの標準化 (IETF) vs モデルの標準化 (ITU)