

広域インシデント情報共有 および分析技術の開発

Cyber Solutions Inc.

本技術開発の位置づけと背景

- IPAの重視する提案の方向性との関係
 - セキュリティイベントを解析する機能の開発
 - セキュリティ関連標準への準拠性および相互運用性に関する技術開発
 - セキュリティ機能の実装
- 背景
 - インシデント情報の広域な流通による新しいセキュリティアプリケーションに対する期待と取り組み
 - IETF INCH (Extended Incident Handling) WGの活動の活発化

本技術開発の概要

□ 目的

- インシデント情報交換メッセージフォーマット (IODEF) を活用した新世代システムの開発、標準化の推進

□ 技術開発

- IODEF情報交換技術を活用した不正アクセス追跡システムの相互運用技術
- IODEF情報交換技術を活用した広域インシデントの分析技術

期待される効果

- 不正アクセス追跡システムの相互運用
 - 広域ネットワークでの不正アクセス発信元の特定
- 広域インシデントの分析技術
 - ウィルス感染等のインシデントの流行、影響範囲、出所の分析
- IODEF標準自体の普及と展開
 - 新しい広域連携セキュリティアプリケーション

IODEFの課題と本技術開発の位置づけ

□ 課題

- キラーアプリ不在
- 標準実装不在

□ 本技術開発の位置づけ

- 実用的なアプリケーションの開発
 - 相互運用の機運が高まっている追跡システム
 - 展開が期待されている定点観測システム
- 現在の標準案のフェージビリティ検証
 - INCH-IODEF
 - IHCH-RID (Real-Time Inter-Network Defense)
 - RID: アーキテクチャ提案

不正アクセス追跡システムの概要

- DoSに代表されるアドレス詐称攻撃の真の攻撃元を追跡するための技術
 - 複数種の多様な技術が実現
 - 複数の商品が市場に登場
 - 複数組織にまたがる広域協調追跡 **課題！**
 - 多種類の追跡システムの相互運用 **課題！**

INCH-RIDに基づく追跡情報交換

広域インシデント分析技術の概要

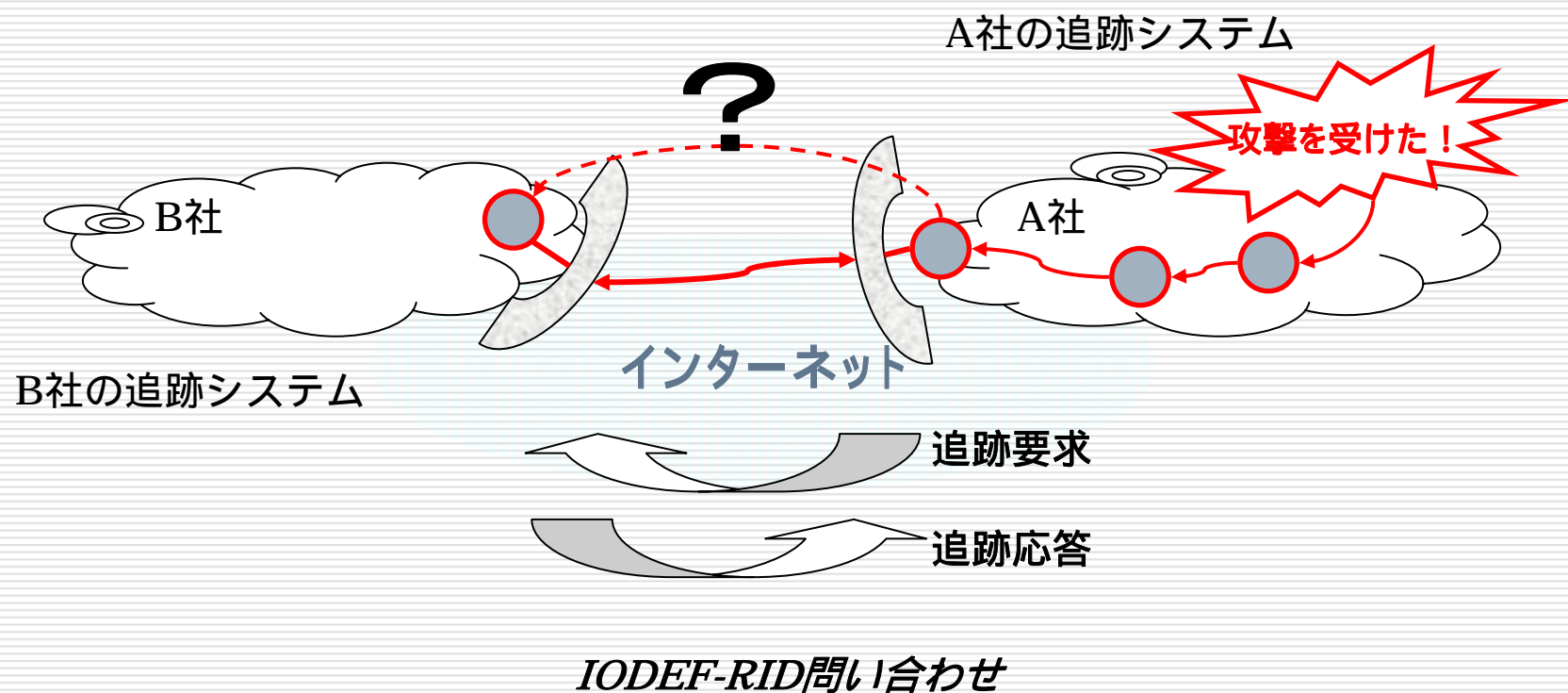
- ネットワーク中の広域多地点の観測結果からネットワーク全体のインシデント発生状況を分析する技術
 - 広域多地点の観測 実現
 - 標準技術による相互運用 **課題！**
 - 広域情報の分析 **課題！**

INCH-IODEFに基づく広域情報集約と分析

本技術開発のターゲット

- INCH-IODEF/RIDのAPI実装
 - インポート/エクスポート機能
 - 問い合わせ/通知機能
- IODEFを活用した相互運用可能な不正アクセス追跡システムの開発
- IODEFを活用した広域インシデント分析システムの開発

不正アクセス追跡システムの相互運用技術



広域シンシデントの分析技術

