トラフィックログをAI技術を用いて解析し攻撃性の高いトラフィックを検出する研究について StarBEDを用いて基礎研究を実施

研究テーマ

AI技術を活用したセキュリティ研究システムの開発研究

研究実施機関

信州大学 総合情報センター

研究の概要

インターネットサービスの普及に伴い、サービスやネットワークへの攻撃も増加している。特に近年の大規模DDoS攻撃は正規の通信を偽装するため、既存のセキュリティ装置では対策が不十分である。そこで本研究はトラフィックログをAI技術であるデータマイニングを行い、攻撃性の高いトラフィックの検出を試みる。

StarBED利用規模

物理ノード6台

各ノード上では様々なAI技術を用いて解析

- SOM
- デンドログラム
- 異常検知
- 多次元民度尺度法
- ●

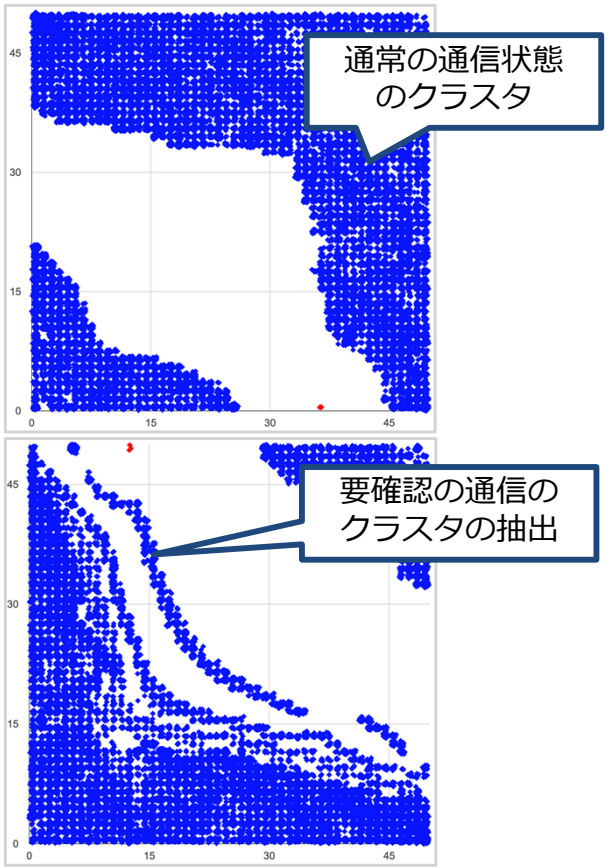
NICT総合テストベッドを活用した研究成果

インターネットを介して行われる攻撃について、低コストな装置での攻撃検知のために、StarBED上でトラフィックデータを、様々なAI　技術を用いて解析し可能性を検証

研究のポイント

1. 1日当たり数億件に上るトラフィックデータを継続的に取得
2. 現実的な脅威に基づいた攻撃を再現し実施
3. 通常のトラフィックに混入された攻撃的な通信を様々なAI技術を用いて検知
4. 適切な可視化による検知結果の定時システムの開発

SOM(自己組織化マップ :Self-Organizing Maps)を用いて不審な通信をクラスタリング



デンドログラムによるクラスタリングを用いて攻撃トラフィックをクラスタリング