

情報通信研究機構

# NICT 先端研究

(141)

近年サイバー攻撃はますます急増しつつあり、人的リソースが不足している。そのため、サイバー攻撃を効率的に解析する高度な自動化技術が必要となってきた。人工知能

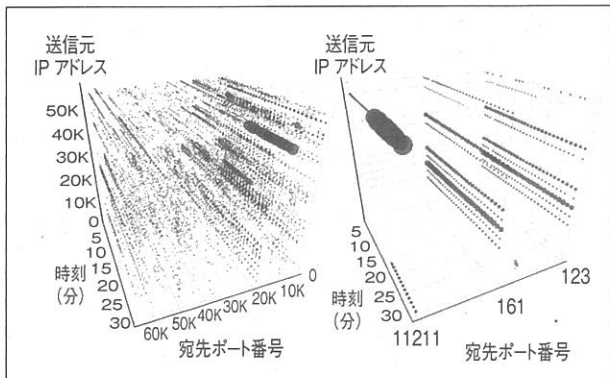
(AI)・機械学習は、研究室では、サイバー攻撃感染ホストの規模、通それを実現する有効な撃を大規模かつリアルタイムに観測する未使手段であり、積極的に用IPアドレス観測きた。我々は分析コスト削減および人的ミス(ダークネット)を削減しており、サイバの低減、そしてサイバの早期発見を最小化するためには、I攻撃の状況を迅速に把握する取り組みを迅速かつ正確に攻撃活把握する取り組みを要がある。NICTサ従来はダークネット分析する研究課題に取イバーセキュリティ研に届く通信量の変化やり組んできた。

我々は問題解決のたが見られると考えられ、ある一定時間で同の時間帯と比べて異常なパターンを示すホを複数検出したり、他の強いホストグループを自動的に見つけることができた。

## サイバー脅威 AIで発見

サイバーセキュリティ研究所・**韓燦洙** (ハン チャンスウ)

2018年九州大学大学院修士号(理学)修了後、同年にNICT入所。同時に九州大学博士後期課程在学中。機械学習を用いたマルウェアおよびネットワーク解析に関する研究に従事。



⑤ダークネットに届いたパケット通信を時刻、送信元IPアドレス、宛先ポート番号を軸に3Dプロット  
⑥同期性の強いホストグループを検出した結果。点の大きさはパケット数の大小関係を示す

定量的な実験の結果、本システムでサイバー攻撃の約97%を検知でき、専門家の分析負担軽減につながった。我々はこのようにAI・機械学習で新たなサイバー脅威・攻撃活動の発生を自動的に瞬時に検出し、それに関する情報を自動的に集約し提供する技術の研究開発を実施している。(火曜日に掲載)