情報通信研究機構

NICT 先端研究 ⑭①

サイバー脅威 AIで発見

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）・機械学習はそれを実現する有効な手段であり、積極的に導入する動きが高まってきている。

サイバー攻撃の被害を最小化するためには迅速かつ正確に攻撃活動の発生を把握する必要がある。NICTサイバーセキュリティ研究室では、サイバー攻撃を大規模かつリアルタイムに観測する未使用のIPアドレス観測網（ダークネット）を保有しており、サイバー攻撃の状況を迅速に把握する取り組みを実施している。

従来はダークネットに届く通信量の変化やり組んできた。感染ホストの規模、通信の特徴を見て専門家が手動で分析を行ってきた。我々は分析コスト削減および人的ミスの低減、そしてサイバー攻撃の早期発見を目標に、AI・機械学習手法を用いて自動的に分析する研究課題に取

サイバーセキュリティ研究所・サイバーセキュリティ研究室 研究員 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エアおよびネットワーク解析に関する研究に従事。

我々は問題解決のために、ダークネットに届く送信元ホストらが示す同期性に着目した。サイバー攻撃のほとんどは、多数の感染ホストを用いて、全インターネット空間に一斉にスキャン通信をバラまく傾向があり、その時ホストらに同期性が見られると考えられるためだ。

我々は複数の手法を用いて、多角的にホストらの同期性を推定する方法を考えた。例えば、ある一定時間で同様なパターンを示すホストをグループ分けし、その中で異常な同期性を示すホストグループを検出したり、他の時間帯と比べて異常に同期性の多い時間帯を検知するシステムを研究開発した。その結果、図のように同期性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。

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）

㊧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
㊨同期性の強いホストグループを検知した結果。点の大きさはパケット数の大小関係を示す