IoT が拓く未来
2021 年度採択研究者

2021 年度
年次報告書

白川 真一

横浜国立大学 大学院環境情報研究院
准教授

IoT セキュリティのための機械学習の自動カスタマイズ技術

§1. 研究成果の概要

本研究では、複数の IoT 機器のデータ連携によって、各 IoT 機器で実行される機械学習モデルを効率的に自動カスタマイズする技術を確立し、IoT におけるサイバー攻撃検知システムの検知性能や学習効率を向上させることを目指している。本年度は、まずターゲットとなる IoT セキュリティに関するデータの入手と整備、実データを用いた実証方法の検討を開始した。具体的には、IoT セキュリティのエキスパートや連携機関から提供された各種 IoT 機器の正常通信や IoT 機器がマルウェアに感染した際の異常通信のデータを用いて、通信データから攻撃を検知するタスクを検討した。また、これらの事前に収集したデータを活用することで、別の IoT ネットワークの機械学習モデルの性能を向上させるタスクを検討した。IoT 機器の異常通信データから基本的な特徴量を抽出し分析を行った結果、データの観測時期によって通信の特徴が変化していることが示唆された。このことから、サイバー攻撃検知を行う機械学習モデルも、通信データの変化に合わせてチューニングが必要であると考えられる。次に、そのような状況で効率的な学習やモデルのカスタマイズを実現すべく、複数の異なるデータソース（IoT ネットワーク）から得られるデータを効率的に学習に利用する方式を開発した。この方式は、別のデータソースから得られた各データを対象モデルの学習に利用するかを決定するものであり、データソース間の連携方法を自動カスタマイズする方式となっている。この方式をボット検知のデータセットに適用したところ、データ連携を最適化する提案方式によって検知性能が向上することを確認した。次年度以降は、引き続きデータソース間の連携方法の最適化方式や検知モデルの自動カスタマイズ方式を開発し、実際の IoT 機器の通信データを用いた実証を行っていく。