

研究背景：IoT環境への攻撃の増加

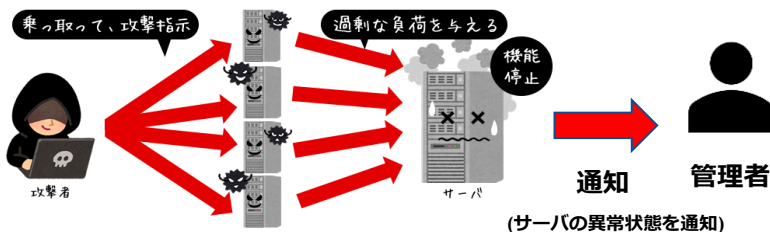
- IoT機器を標的としたマルウェア・攻撃は増加傾向
 - ✓ 1Gbpsの規模を超えるIoT機器を踏み台とするDDos攻撃は2016年と2018年を比べると**1.7倍**になった
 - ✓ IoTを標的とするマルウェアの数も2018年までに**121,588種類**にまで増加
- IoT機器のセキュリティの課題
 - ✓ 機器の性能がPCやスマホなどと比べるとかなり劣っていて**セキュリティ対策ソフトを導入するのが困難**
 - ✓ リアルタイムでの監視が困難で**異常を発見するのが遅くなる**



リアルタイムで監視する仕組みが必要

研究背景：IDS(侵入検知システム)

- IDS(Intrusion Detection System)の略称で不正侵入検知システム
 - ✓ システムやネットワークに対して外部からの不正なアクセスや兆候があった場合に異常を通知するシステム



提案手法：研究の概要

【IoT環境向けのIDSに求められること】

- ① 高精度・軽量
- ② 処理時間が速い(リアルタイム性)

【提案手法】

① **新たな特徴量選択法の考案**

- ✓ 特徴選択をすることで無駄なデータを削減し演算の軽量化と性能を向上に期待できる

② **リアルタイム性の検証**

- ✓ IoT機器を想定した機器上で分類時間を検証

まとめ

【特徴選択】

- ✓ 特徴選択をすることで分類器の性能を向上させるができた
- ✓ 特徴選択をすることで分類器の判断時間を短縮できることが確認できた
- ✓ 提案手法を用いることで、短い時間で精度が向上する特徴を選択することができた

【リアルタイム性の検証】

- ✓ IoT機器を想定したリソースの乏しい機器でも1つのデータに対する判断時間はリアルタイム性があることが確認できた