「つなぐだけ」で実現するIoT機器/NWのセキュリティ監視（大阪市立大学）

ネットワーク内に接続された IoT 機器を検出、自動で機器識別

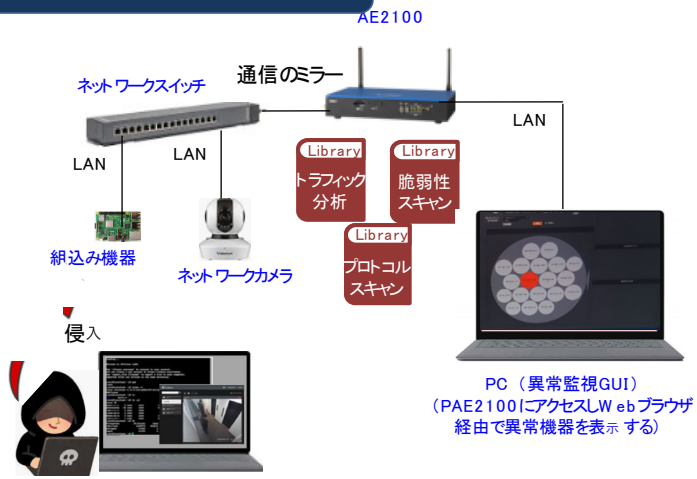
概要

IoT 機器の急速な増加に伴い、これらの機器を狙ったセキュリティ攻撃が深刻化しています。セキュリティ対策が十分に行えない IoT 機器に対してネットワーク側で適切に管理・運用することが求められています。本ソリューションは、AE2100 をネットワークに接続するだけで、ネットワーク内に接続された機器を検出し、それらの通信パターンから機器がどのような種別かを自動で識別できるシステムを提供します。

特徴

- ✓ 専門的な知識を必要としない簡単接続
- ✓ 「つなぐだけ」で自動で機器検出・識別
- ✓ 通信パターンの機械学習により高い精度を実現する識別エンジン
- ✓ 異常振る舞い検知機能
- ✓ ソフトウェア更新による機能拡張
- ✓ GUI によるリアルタイム表示

使用イメージとデモ環境



拠点を模擬したローカルNWのネットワークスイッチで通信を複製（ミラー）したものをAE2100に接続し、通信トラフィックのパターンに対して機械学習による分析を行うことで、その拠点のトラフィック異常や接続機器の脆弱性の有無をGUIで表示する。

① 無許可機器の接続検知と機器推定
　新規に機器が接続されたことを検出し、機器種別を推定した上でGUI上でアラートを出す。（パスワードの設定に不備がある場合など）
② 機器の異常な振る舞い検知
　パスワードの設定不備を突いて機器に不正接続し、拠点内NWをスキャンする。
　ネットワークカメラの脆弱性を突いて侵入し、内部の映像ファイルを不正取得する。
　→ トラフィック異常がGUI上で表示される。
③ 機器の脆弱性スキャン
　ネットワーク内の機器をスキャンすることにより、パスワードの設定不備や実装脆弱性を検知しGUI上でアラートを出す。