IoT が拓く未来
2019 年度採択研究者

2020 年度
年次報告書

山内 利宏

岡山大学 大学院自然科学研究科
准教授

IoT 機器の実行環境の隔離を実現する IoT 基盤ソフトウェアの構築

§1. 研究成果の概要

IoT 機器のファームウェアの解析手法を研究し，IoT 機器のファームウェアの大規模データセットを対象として，解析と分析を行った．解析対象を拡充するために，2020 年度はさらに大規模なファームウェアのデータセット(2000 年から 2019 年に公開された 5,712 ファームウェア)を対象とした．また，ファームウェアの中にはアンパックできずに解析できないものがあるため，分析対象のデータを増やすために，公開されている 2,379 GPL ソースコードを対象とした，ファームウェアと GPL ソースコードを合わせて，2000 年から 2019 年に公開された 13 ベンダの IoT 機器 1,510 種に関する分析を実施した．

今年度の研究では，IoT 機器のセキュリティ機構およびソフトウェアバージョンの体系的な調査方法を確立した．この調査方法を用いた実態調査によって，IoT 機器は既存のセキュリティ機能を十分に活用していないことを明らかにした．また，セキュリティ機能の適用率の変化については，NX bit は増加傾向，PIE は減少傾向にあることを明らかにした．さらに，IoT 機器ベンダへのインタビューによって，ソフトウェアの脆弱性はバージョンアップではなくパッチで対処されることがあることを確認した．よって，ソフトウェア内のバージョン番号文字列に基づいて脆弱性の有無を調査する方法は誤検知を生じる可能性があることを明らかにした．

IoT マルウェアの不正接続後の Telnet ログを分析し，IoT マルウェアがログイン後，マルウェアをダウンロードし，感染するためのコマンド実行手順や，シェルへのアクセスを獲得するために実行するコマンド実行順を明らかにした．

OS やアプリケーションを改変せずに seccomp 機能を IoT 機器で活用するアクセス制御機構の基本方式も検討し，実装により実現可能性を確認した．

【体表的な原著論文情報】

1) 白石 周碁，福本 淳文，吉元 亮太，塩治 榮太朗，秋山 満昭，山内 利宏，“ソフトウェア解析とベンダインタビューによる IoT 機器のセキュリティに関する大規模実態調査，”コンピュータセキュリティシンポジウム 2020 (CSS2020) 論文集，pp.875-882，(10，2020)

2) 山内 利宏，吉元 亮太，吉岡 克成，″IoT 機器への不正な Telnet 接続ログのコマンドに着目した分析，″ 情報処理学会第 83 回全国大会，情報処理学会第 83 回全国大会講演論文集，第 3 分冊，pp.393-394，(3，2021)．