IoT が拓く未来
2019 年度採択研究者

2019 年度
実績報告書

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

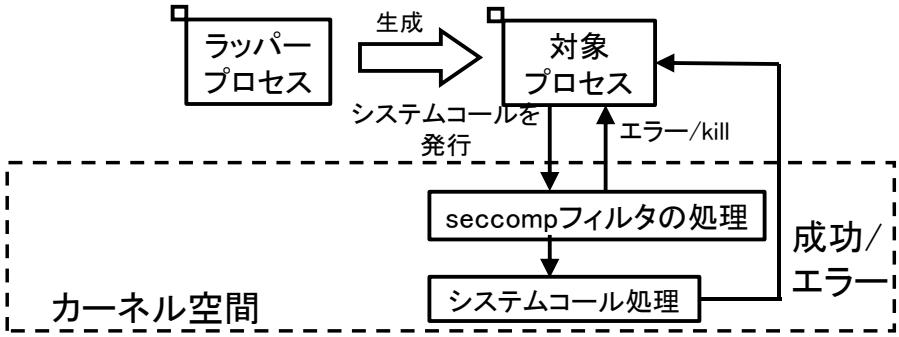
2019 年度は，IoT 機器の調査と各 IoT 機器におけるセキュリティ上の課題の明確化，及び Seccomp を利用したアクセス制御機構の基本機能について研究を進め，外部発表を行った．

1. IoT 機器の調査と各 IoT 機器におけるセキュリティ上の課題の明確化

IoT 機器がマルウェアに感染する仕組みや課題を明確化するために，IoT 機器のソフトウェア構成の調査を行った．国内外 10 ベンダから発売されている IoT 機器で使用される IoT 機器のファームウェアを対象として，ソフトウェア構成について分析を行った．分析内容としては，利用されているソフトウェア名とバージョン情報を抽出した．また，実行ファイルについては，セキュリティ機能の適用の有無について調査した．調査結果から，以下のことを明らかにした．2019 年度に新たに配布されたファームウェアでも，数年前～十数年前にリリースされたソフトウェアを利用していることがある．また，IoT 機器以外の計算機で広く利用されている Linux ディストリビューションと比べ，セキュリティ機能の適用率が低いことを明らかにした．ソフトウェアのバージョンをファームウェアの更新時に上げている IoT 機器は少ないため，今後，安全性のさらなる検証が必要である．

2. Seccomp を利用したアクセス制御機構の基本機能

マルウェアに侵入された IoT 機器が，攻撃者に自由に利用されることを防ぐため，Linux の標準のアクセス制御機構である Seccomp を利用したアクセス制御機構の基本方式ついて設計（下図）し，実装と評価した結果について報告した．実現における課題として，Seccomp のシステムコールフィルタの生成方法，およびフィルタをプロセスに適用する方法がある．フィルタの作成方法については，保護したいプログラムを実行し，そのシステムコール発行ログからフィルタを生成する手法を実現した．また，フィルタの適用方法として，ラッパープロセスを用いて，保護対象プロセスを起動し，seccomp フィルタを適用する方法を実現した．評価の結果，低オーバヘッドでシステムコールの発行を制限でき，利用するシステムコールが少ないプログラムの場合，多くのシステムコールの発行を制限できることを示した．


ラッパー
プロセス
生成
対象
プロセス
システムコールを
発行
エラー/kill
seccompフィルタの処理
システムコール処理
成功/
エラー
カーネル空間