

IoT が拓く未来
2019 年度採択研究者

2021 年度 年次報告書

山内 利宏

岡山大学 学術研究院自然科学学域
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

本研究では、IoT 機器に IoT マルウェアが侵入したとしても、攻撃を成功させず、IoT 機器を悪用させないソフトウェア構成法を目指している。2021 年度は、研究目的を達成するために、IoT マルウェアの攻撃手法の分析、IoT マルウェア検体の分類手法の検討、IoT 機器のファームウェアの大規模調査の継続、および IoT 機器の攻撃サーフェス削減手法とアクセス制御手法の研究を行った。

IoT マルウェアの攻撃手法の分析では、IoT マルウェアがリモートからログインした際に、どのようにして外部からプログラムやスクリプトをダウンロードして実行するのかという点に着目し、コマンドを分析し、攻撃手法を明らかにした。また、Linux カーネル内部でアクセス制御する場合に、システムコール単位でアクセス制御するために、コマンドのログと一緒に、コマンド実行に伴って発行されるシステムコールを取得する機構を開発し、ハニーポット環境で実際の IoT マルウェアの攻撃ログを取得し、分析した。

IoT マルウェアの分類手法として、マルウェアを実行せずに取得できる表層データと fussy hash を組み合わせて、深層学習を利用してマルウェアを分類する手法を実現し、高い精度で分類できることを示した。

IoT 機器ファームウェアの大規模調査では、5 つのベンダを加え、18 ベンダについて 2020 年のデータも追加して分析した。依然として、IoT 機器においてセキュリティ機能の利用があまり行われていないことを示し、ソフトウェアの脆弱性修正において、バージョンを上げずにプログラムを修正する暗黙的パッチが広く行われていることを分析により示した。また、セキュリティ機能の利用が進まない理由として、上流のサプライヤーの影響が大きく、セキュリティ機能の利用が進んでいないことを指摘した。

アクセス制御手法の研究として、Seccomp を用いた手法で実際の脆弱性への防御実験を行い、その特徴を示した。また、IoT 機器向けのアクセス制御手法検討のための調査を行った。

【代表的な原著論文情報】

- 1) Toshihiro Yamauchi, Ryota Yoshimoto, Takahiro Baba, Katsunari Yoshioka, Analysis of commands of Telnet logs illegally connected to IoT devices, 12th International Conference on E-Service and Knowledge Management (ESKM 2021), poster, Proceedings of 2021 10th International Congress on Advanced Applied Informatics (IIAI-AAI 2021), pp.913-915, (7, 2021).
- 2) Takahiro Baba, Kensuke Baba, Toshihiro Yamauchi, Malware Classification by Deep Learning Using Characteristics of Hash Functions, Proceedings of the 36th International Conference on Advanced Information Networking and Applications (AINA-2022), vol.2, pp.480-481 Springer Nature (2022.04). (発表予定)
- 3) 大迫 勇太郎, 山内 利宏, 吉岡 克成, 藤橋 卓也, 渡辺 尚, 猿渡 俊介, IoT マルウェアの分類方法に関する検討, コンピュータセキュリティシンポジウム 2021 (CSS2021) 論文集,

vol.2021, pp.697-704, (10, 2021).

- 4) 白石周碁, 吉元亮太, 塩治榮太朗, 秋山満昭, 山内利宏, ソフトウェア差分に着目した IoT 機器サプライチェーンセキュリティ上の課題発見と大規模実態調査, 電子情報通信学会 第 58 回情報通信システムセキュリティ研究会, 電子情報通信学会技術研究報告, vol.121, no.410, ICSS2021-76, pp.105-110 (2022.03).
- 5) 山内 利宏, 吉元 亮太, LKM を介した Seccomp フィルタの適用によるアクセス制御手法の提案と評価, 情報処理学会第 93 回 CSEC・第 53 回 IOT 合同研究発表会, 情報処理学会研究報告, vol.2021-CSEC-93, no.12, pp.1-6, (5, 2021).