研究課題別事後評価結果

１．研究課題名：　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

２．個人研究者名

山内　利宏（岡山大学大学院自然科学研究科　教授）

３．事後評価結果

IoT 機器のセキュリティ向上に向けた OS レベルでの攻撃検知、攻撃無効化技術の確立に挑戦する研究である。カーネル空間におけるメモリマッピングを考慮したアクセス制御機構や攻撃可能領域削減方式の実現と、実環境での効果検証により、IoT 機器の脆弱性課題を根本から解決することを目指した。

IoT マルウェアの攻撃を防止もしくはその影響を緩和可能な基盤ソフトウェアレベルのセキュリティ基盤技術構築に向け、IoT 機器のソフトウェア脆弱性の大規模分析、セキュリティ対策の実態調査と根本課題解析、マルウェア感染動作分析、システムコールレベルのアクセス制御メカニズム、パケットフィルタを用いたシステムコール発行制限メカニズムの構築に取組み、製品として実稼働する組込ソフトウェアの脆弱性を分析し、アクセス制御ソフトウェアのカーネル実装とその具体的な攻撃隔離効果を検証した点は評価できる。特にソフトウェア脆弱性の大規模分析では、IoT 機器ソフトウェアのセキュリティ対策レベルを自動的に分析するツールの開発に成功し、18 ベンダの１万個以上のファームウェア・ソースコードを分析した点は、脆弱性課題の根本原因究明に資するインパクトのある成果である。

IoT 機器のセキュリティ向上に向けて、ソースコード分析やベンダーインタビュー等の網羅的・現実的な研究開発を推進し、IoT 機器の開発工程やサプライチェーンまでを考慮した実用性の高い攻撃検知・攻撃無効化の研究成果により、IoT 産業界からも注目される研究者としての飛躍につながった。今後も多様化・進化し続けるサイバー攻撃にも対応可能とする提案手法の高度化・実用性実証と、経済安全保障を考慮した課題の明確化とビジョン構築等、国際コミュニティの最先端研究を牽引しうる研究成果の更なる発展と、著名かつ難関国際学会・論文誌への成果発信を期待する。