

2024 年度年次報告書

基礎理論とシステム基盤技術の融合による Society 5.0 のための基盤ソフトウェアの創出

2021 年度採択研究代表者

竹房 あつ子

情報・システム研究機構 国立情報学研究所
教授

形式検証とシステムソフトウェアの協働によるゼロトラスト IoT

主たる共同研究者:

五十嵐 淳 (京都大学 大学院情報学研究科 教授)

須崎 有康 (情報セキュリティ大学院大学 情報セキュリティ研究科 教授)

関山 太郎 (情報・システム研究機構 国立情報学研究所 准教授)

研究成果の概要

形式検証とシステムソフトウェアの融合により、ゼロトラストの概念を踏襲した安全な IoT システム (ZT-IoT) の実現を目指し、(課題 1) ZT-IoT システムのためのシステムソフトウェア、(課題 2) ZT-IoT システムのためのセキュリティポリシエンジンを、(課題 3) ZT-IoT システムを支える監視・介入技術、(課題 4) ZT-IoT サービス連携のためのセキュア・オブジェクトの研究を進めている。2024 年度は、要素技術に関する研究開発を進めるとともに、PoC Phase 1 で各ソフトウェアおよびアルゴリズムの評価を行い、最終 PoC に向けた改良点の抽出を行った。

(課題 1) では、実時間挙動トラッキング機構を改良し、IoT 機器の監視と実際の脆弱性検出を成功させた[1]。通信の監視では、eBPF で動的な固定小数点方式を用いた異常検出手法を開発した[2]。また、ソフトウェア認証機構と OTA フレームワークの統合試験を行う[3]とともに、IoT 機器用 CA で必要とされる機能を提案・実証を行った[4]。(課題 2) では、提案する IoT システムモデル記述言語 Rabbit を改良し、より現実的なシステム記述を可能にする[5][6]とともに、コードの公開を行った。(課題 3) では、ネットワークシミュレーション・エミュレーション環境によるシナリオベースのトラフィック生成フレームワークの設計・実装を行い[7]、コードを GitHub で公開するとともに、再帰型を用いたプログラムのスケーラビリティ評価技術に関する理論研究を進めた[8][9]。(課題 4) では、開発したリモートアテステーション機能が OP-TEE 本体に採録されるとともに、ハードウェア由来の鍵管理を実装し、ヨーロッパ最大のオープンソース会議 FOSDEM で発表した[10]。

【代表的な原著論文情報】

- [1] Jie Yin, Yutaka Ishikawa, Atsuko Takefusa, “A Lightweight Monitoring and Anomaly Detection Framework for IoT Devices,” IEEE COMPSAC’2025, Jul. 2025.
- [2] Atsuya Osaki, Manuel Poisson, Seiki Makino, Ryusei Shiiba, Kensuke Fukuda, Tadashi Okoshi, Jin Nakazawa, Dynamic Fixed-Point Values in eBPF: a Case for Fully in-kernel Anomaly Detection, Proc. AINTEC 2024, pp.46-54, 2024.
- [3] 青木信雄, 山下直希, 丹生智也, 坂根栄作, 合田憲人, 石川裕, 小野泰司, 竹房あつ子, DEMO-10: IoT ソフトウェアの信頼性とレジリエンスを高める ZT-OTA Update Framework のプロトタイプ実装, Computer Security Symposium, Oct. 2024.
- [4] Eisaku Sakane, Atsuko Takefusa, A Design of Automatic Certificate Management for a Zero Trust IoT System, International Symposium on Grids and Clouds (ISGC) 2025, Mar. 2025.
- [5] Terunobu Inaba, Yutaka Ishikawa, Atsushi Igarashi, Taro Sekiyama. Rabbit: A Language to Model and Verify Data Flow in Networked Systems, Proc. the 11th International Symposium on Networks, Computers and Communications (ISNCC'24), Oct. 2024.
- [6] Atsushi Igarashi, Yutaka Ishikawa, Sewon Park, Taro Sekiyama. Extending Rabbit towards verified networked systems with user-defined semantics for system calls. 第 27 回プログラミングおよびプログラミング言語ワークショップ(PPL 2025). ポスター発表. Mar. 2025.
- [7] M. Poisson, R. Carnier, K. Fukuda, Goth-X: a generator of customizable, legitimate and malicious IoT network traffic. The 17th Cyber Security Experimentation and Test Workshop (CSET), pp.65-73, Aug. 2024.

- [8] Taro Sekiyama, Hiroshi Unno. Algebraic Temporal Effects: Temporal Verification of Recursively Typed Higher-Order Programs. Proc. ACM Program. Lang. 9 (POPL), pp.2306-2336, 2025.
- [9] Taro Sekiyama, Hiroshi Unno. Higher-Order Model Checking of Effect-Handling Programs with Answer-Type Modification. Proc. ACM Program. Lang. 8 (OOPSLA2): 2662-2691, 2024.
- [10] Kuniyasu Suzuki, Remote Attestation on Arm TrustZone OP-TEE with VERAISON Verifier — current status and future plan —, FOSDEM 2025, Feb 2025.