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

2021 年度
年次報告書

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

§1. 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 (Internet of Things)システム(ZT-IoT)の実現を目指し、(研究課題1)ZT-IoT システムのためのシステムソフトウェア、(研究課題 2)ZT-IoT システムのためのセキュリティポリシエンジン、(研究課題 3) ZT-IoT システムを支える監視・介入技術、(研究課題 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実施する。2021 年度は、IoT システムアーキテクチャの概念設計を行うとともに、要素技術の研究に着手し、アルゴリズムまたはシステムの設計に向けた知見を得た。

(研究課題 1)では、実時間挙動トラッキング機構、認証ベース実行制御システム、データ完全性保証通信機構の設計を進めるとともに、ソフトウェア認証機構のシステムモデルの定義を行い、ソフトウェア設計の指針を得た。

(研究課題 2)では、IoT システムモデリング、セキュリティポリシ記述言語設計、セキュリティプロシージャの正当性保証に向けて、プロセス計算や多重集合書き換えによるセキュリティプロトコル検証、アクセス制御論理、ネットワーク検証、TEE や eBPF を対象とした検証を調査し、理論構築や言語設計のための知見を得た。

(研究課題 3)では、監視アルゴリズムの性能測定を含む IoT システム上での実装に向けた調査、通信データからモニタリング仕様学習に向けたサーベイ、柔軟な制御構造操作を伴うプログラムのスケーラビリティ検証技術に関する研究を行った。

(研究課題 4)では、IoT デバイスに信頼の基点を形成する方法を検討した。HSM と TEE が候補となるが、ハードウェア製造者以外に書き換え不能な HSM を設けるべきであるとの結論を得た。デバイス同士が互いに真正性を確認するためにプログラムコードを送り込んで検査する方法の検討を開始した。

§2. 研究実施体制

(1)竹房グループ

① 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)

② 研究項目

(1a) 実時間挙動トラッキング機構

(1b) 認証ベース実行制御システム

(1c) データ完全性保証通信機構

(1d) ソフトウェア認証機構

(2)五十嵐グループ

① 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)

② 研究項目

(2a) ZT-IoT システムのセキュリティポリシ及びセキュリティプロシージャの記述言語の設計

(2b) 形式検証によるセキュリティプロシージャの正当性保証

(3)関山グループ

① 主たる共同研究者:関山 太朗 (情報・システム研究機構 国立情報学研究所 助教)

② 研究項目

(3a) セキュリティ保証に必要な情報収集のための IoT システムモニタリングアルゴリズム

(3b) 脅威検知の仕様策定に向けた統計的・論理的アプローチの融合

(3c) セキュリティアクションの実施に必要なスケーラビリティ評価技術

(4)松井グループ

① 主たる共同研究者:松井 俊浩 (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)

② 研究項目

(4a) TEE による信頼のチェーン実装

(4b) セキュアオブジェクトの開発

(4c) IoT 機器間相互セキュリティポリシ強制

【代表的な原著論文情報】

1)"ZT-IoT: ゼロトラスト IoT のためのシステムソフトウェア構築に向けて", 竹房 あつ子, 五十嵐 淳, 関山 太郎, 松井 俊浩, 小野 泰司, 福田 健介, 蓮尾 一郎, 合田 憲人, 石川 裕, 情報処理学会研究報告 2022-OS-154(3), pp. 1-16, 2022 年 3 月.