2023 年度年次報告書
社会変革に向けた ICT 基盤強化
2021 年度採択研究代表者

塩谷 亮太

東京大学 大学院情報理工学系研究科
准教授

実用性と安全性を両立する秘密情報量に基づく情報漏洩防止基盤

研究成果の概要

2023 年度は，1.情報量に基づく動的情報フロー追跡と，2.情報量の追跡に基づくハードウェア設計の自動検証の研究を行った．また，これらの情報量の追跡の研究から派生した 3.ソフトウェアのファジングやトリアージの研究を開始した．以下ではこれらについて簡単にまとめる．

1. 動的情報フロー追跡においては，当初から研究を進めていた情報漏洩検出に加え，攻撃検出を行う新しい方式の研究を進めた．これらの研究では，これまで主に自己情報量やエントロピーに基づいて理論を構築してきたが，2023 年度に行った研究の結果，モデル・カウンティングに基づく新しい情報フロー追跡の方法を発案した．このモデル・カウンティングに基づく方法では，従来の研究にあった明示的フローや暗黙的フローが混じった場合の曖昧さや入力の確率分布に関わる問題を解決することができた．

2. ハードウェア設計の自動検証の研究では，研究当初は回路内のレジスタ間で伝搬される情報量を追跡する方針でバグや脆弱性を見つけることを目指していたが，これまでに行った研究により，追跡を行わずに相互情報量を使用する新しい方法を発案した．

3. 動的情報フロー追跡の考え方をソフトウェアのファジングやトリアージに応用する研究を新たに始めた．ファジングについては，プログラムに含まれる分岐と分岐の間の情報フローを考慮して内部状態を探索する方法を発案した．またトリアージについては，1. の攻撃検出の方法を応用し，バグを引き起こした変数がどのぐらいプログラム外から制御出来るかを定量化することで，バグの深刻度を測る方法を発案した．

上記のうち，1. と 3. においては，現在セキュリティやプログラミング言語における著名な国際会議に合計 3 本の論文を投稿中であり査読結果を待っている．また，2. については 2023 年度に投稿した論文が，回路設計や検証におけるトップ会議である IEEE/ACM International Conference on Computer-Aided Design (ICCAD) に採録された．

【代表的な原著論文情報】

1) Yuichi Sugiyama, Reoma Matsuo, and Ryota Shioya: “SurgeFuzz: Surge-Aware Directed Fuzzing for CPU Designs”, IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pp. 1-9 (2023). doi: 10.1109/ICCAD57390.2023.10323819