社会変革に向けた ICT 基盤強化　　2022 年度
2021 年度採択研究代表者　　年次報告書

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

2022 年度は、情報量に基づく動的情報フロー追跡と、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。

1. 情報量に基づく動的情報フロー追跡においては、これまで実装のベースとして使用していた言語処理系を Lua 言語のものから、より広く使われている JavaScript 言語のものへと実装を切り替えた。Lua 言語に比べると JavaScript 言語は仕様が巨大であり、これへの動的情報フロー追跡の実装にはかなりの時間と手間がかかったが、しかしこれにより広範囲のアプリケーションを評価可能となった。
2. 研究開始当初はシステム内から外部へ出力される秘密情報の量を追跡する方法を研究していたが、システム外から内部へ挿入される情報量を追跡して攻撃を検出する新しい方法を研究開始後に発案した。2022 年度はこの研究を進め、既存の情報追跡による攻撃検知と比べて良好な評価結果を得た。
3. ハードウェア設計の自動検証の研究では、研究開始当初は回路内のレジスタ間で伝搬される情報の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、2022 年度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。この研究により、オープンソースの CPU 設計から未知のバグを複数発見した。

上記の研究結果に基づき、いくつかの国際会議へ投稿を行ったが、いずれも採録にいたらなかった。ただし、ハードウェア設計に関する著名な会議である DAC への投稿では、不採録論文の中では高得点であったため、論文の出版には当たらないポスター採録となった。また、国内ワークショップで行った研究発表では、情報処理学会 CS 領域奨励賞を受賞した。同賞は、同学会の研究会で行われた各年度の発表のうち特に優秀な 1〜2 件に与えられるものである。現在の状況としては、セキュリティ分野やハードウェア検証分野の複数の著名な会議に論文を投稿中であり、採否結果が出るのを待っているところである。