社会変革に向けた ICT 基盤強化
2021 年度採択研究者

2021 年度
年次報告書

空閑洋平

東京大学　情報基盤センター
准教授

データセンタハードウェアへのソフトウェア脆弱試験の適応

§1. 研究成果の概要

本研究は、データセンタでの研究開発が進むアクセラレータのハードウェア通信に注目し、ハードウェア通信をソフトウェアから実行することで、ソフトウェアによる高度な脆弱性診断機能を、ハードウェアに対して適応することを目標としている。本研究の対象とするデータセンタハードウェアは、NIC や GPU、NVMe デバイスなどであり、これらのデバイスは PCI Express (PCIe)インタフェースを用いてホストと接続し、デバイス間通信する。そのため、本研究では、PCIe プロトコルをソフトウェアで実装することで、ハードウェア通信をソフトウェアから実施する環境の構築を目指している。

今年度の主な成果は、ハードウェアの脆弱性診断を実現するために、研究対象の PCIe デバイスとデータ通信を実現するため、QEMU の仮想 PCIe デバイスに PCIe プロトコルを対応するアーキテクチャを設計し、実験によって動作を確認した。QEMU には、すでに NVMe や NIC といった高度な DMA 通信する仮想 PCIe デバイス実装が存在しているが、QEMU には PCIe プロトコルが実装されていないため、これらの仮想デバイスと物理 PCIe デバイス間ではデータ通信ができない。そこで、QEMU の仮想環境と物理 PCIe リンクをブリッジすることで、データ通信するアーキテクチャの研究開発を実施した。また、様々なハードウェア通信に起因した脆弱性診断を試行錯誤できる環境として、特に NVMe プロトコルに関連した機能開発を継続して実施した。また、脆弱性診断機能のシンプルな自動試験通信生成機能の設計、開発を実施した。今年度の進捗では、研究項目の設計と初期実装を実施したが、完全な動作できるところまでは確認できなかったことから、引き続き問題の箇所の特定と開発を継続する予定である。