2024 年度年次報告書
社会変革に向けた ICT 基盤強化
2022 年度採択研究代表者

三輪 忍

電気通信大学 大学院情報理工学研究科
准教授

# HPC ユーザのための TEE 利用支援フレームワーク

## 研究成果の概要

TEE を利用した並列計算機システムのアーキテクチャ検討を行った. 具体的には, 並列計算機の脅威モデルを構築した上で, 想定される攻撃を防ぐために必要な要素技術を詳細に検討し, 集中型の鍵管理システムと暗号化通信ライブラリからなる TEE ベースの並列計算機システムを提案し, その成果を国内最大級のセキュリティ会議であるコンピュータセキュリティシンポジウム 2024 にてポスター発表した[1].

無修正の Linux バイナリを SGX 上で実行するフレームワークの 1 つである Gramine を用いて, 複数ノードの SGX 上でプログラムを実行した際の MPI 通信性能を評価した. 具体的には, SGX をサポートする CPU を搭載した 4 ノードの PC クラスタを構築し, NPB と Intel MPI ベンチマークから選択した 16 種類のプログラムを上記の PC クラスタ上で実行することで各プログラムの実行性能を評価した結果, Gramine+SGX の MPI 通信性能への影響は軽微であることを確認した. 以上の研究成果は, 高性能計算分野の著名な国際会議である IEEE Cluster にてポスター発表した[2].

さらに, 複数ノードの SGX 間で安全なデータ転送を行うため, 暗号化 MPI 通信ライブラリの開発を行った. この通信ライブラリは PMPI インターフェースを用いて実装されており, ユーザはリンクするライブラリを変更するだけでコードの改変なしに MPI 通信を暗号化できる. 評価の結果, 開発したライブラリにおける MPI 関数の性能オーバヘッドは実用上問題ないことを確認した. 以上の研究成果は, 情報処理学会第 198 回 HPC 研究会にて発表を行った[4].

また, NUMA 構成と Gramine バージョンが SGX の性能に与える影響の評価も行った. 評価の結果, 2CPU の NUMA 構成のマシンでは, Gramine と SGX を利用した際, 2 つの CPU と片方の CPU のローカルメモリしか使用していない可能性が高いことがわかった. また, Gramine バージョンがアプリケーション性能に与える影響については, 多くのワークロードで差は見られなかったものの, 一部のワークロードで約 15%の性能差が生じることを確認した. 以上の研究成果をまとめ, 情報処理学会第 198 回 HPC 研究会にて発表を行った[3].

【代表的な原著論文情報】


1) 下島 航太, 八巻 隼人, 本多 弘樹, 松尾 真一郎, 三輪 忍, 並列計算システムにおける情報漏洩を防止する TEE の利用方法の研究, コンピュータセキュリティシンポジウム 2024（ポスター）(2024)
2) K. Shimojima, S. Miwa, H. Yamaki, and H. Honda, Evaluating MPI Performance on SGX and Gramine, 2024 IEEE International Conference on Cluster Computing Workshops (CLUSTER Workshops) (poster presentation), pp. 172-173 (Sep 2024)
3) 佐野 拳紳, 下島 航太, 八巻 隼人, 本多 弘樹, 三輪 忍, NUMA 構成と Gramine バージョンが Intel SGX の性能に与える影響の評価, 情報処理学会研究報告 2025-HPC-198, No.51, pp.1-8 (2025)
4) 下島 航太, 八巻 隼人, 本多 弘樹, 松尾 真一郎, 三輪 忍, Intel SGX を用いた並列計算環境のための暗号化 MPI 通信ライブラリ, 情報処理学会研究報告 2025-HPC-198, No.48, pp.1-8 (2025)