基礎理論とシステム基盤技術の融合による Society5.0 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

廣津　登志夫

法政大学　情報科学部
教授

プライバシセントリック情報処理基盤

§1. 研究成果の概要

現在のソフトウェアアーキテクチャには、一定のプライバシレベルのデータの流れを複数のコンポーネントにわたって扱うための実行制御機構がない。本研究では、ネットワークを越えた複数のノードにわたる一つの実行環境にデータとその処理を閉じ込める『セキュアネットワークコンテナ』の考え方を導入する。そして、セキュアネットワークコンテナ間のデータ移送を制御する仕組みにより、コンテナ内外でのデータの扱いに対してシステムが関与し、情報のプライバシレベルに対する制御性を利用者に提供する『プライバシセントリック』な情報処理基盤の実現を目指している。

2021 年度は、これらの目標に向けて基本的なアーキテクチャや言語仕様の検討と個々の要素技術の研究を進めた。要素技術は大きく「処理・通信の監視・制御」と「蓄積・保存データの分離」に分けられる。

「処理・通信の監視・制御」については、TEE(Trusted Execution Environment)を用いた監視機構とその移送技術および、VMM レベルでサービスの実行を制御する技術を中心に研究を進めた。TEE を用いた監視機構としては、Intel SGX を対象として、仮想マシン(VM)の監視を行うシステムを高い可搬性と開発効率を持って TEE 内で稼働させる仕組みを開発し、VMM レベルでサービスを制御する技術については、TEE から VM 内のプロセスに疑似的にシグナルを送り制御する仕組みを開発した。

「蓄積・保存データの分離」については、クライアント側でのプライバシデータの保護や制御による分離をクラウド側まで適切なレベルで維持し続ける技術を中心に研究を進めた。ここでは、TEE で保護された環境で稼働するサーバが安全な通信路越しに受け取ったデータを、クラウド基盤からその中身を見られることなく、必要な保護レベルに応じて分離したままで管理することができるシステムを開発した。

§2. 研究実施体制

(1) 廣津グループ

① 研究代表者:廣津　登志夫 （法政大学　情報科学部　教授）

② 研究項目

・ノードコンテナのためのセキュアストレージ

・ネットワークコンテナのためのシグナリング技術

・セキュアネットワークコンテナの構成記述

(2) 光来グループ

① 主たる共同研究者:光来　健一 （九州工業大学　大学院情報工学研究院　教授）

② 研究項目

・ノードコンテナのデータ移送監視・制御技術

・セキュアネットワークコンテナの構成記述

【代表的な原著論文情報】

1) 河村拓実, 光来健一: SGX 向け実行環境 Occlum と SCONE を用いた VM の安全な監視手法, 第 154 回システムソフトウェアとオペレーティング・システム(OS)研究会, 2022-OS-154(7), pp.1-10, 2022.

2) Kenji Nakaima and Kenichi Kourai: MigSGX: A Migration Mechanism for Containers Including SGX Applications, 14th IEEE/ACM International Conference on Utility and Cloud Computing (UCC 2021), No.6, pp.1-10, 2021.

3) 木村健人, 光来健一: システム外部からの OS メモリの書き換えによるシステム障害からの復旧, 第 33 回コンピュータシステム・シンポジウム(ComSys 2021), pp.75-84, 2021. (優秀若手発表賞)

4) 小林惇, 廣津登志夫: Intel SGX を利用したクラウド環境から保護された暗号化共有ファイルシステム, 第 154 回システムソフトウェアとオペレーティング・システム(OS)研究会, 2022-OS-154(8), pp.1-8, 2022.

5) 山本憲正, 廣津登志夫: 安全なクラウド上の共有を支援するファイルシステム拡張, 第 84 回情報処理学会全国大会, 2022.