2024 年度年次報告書
基礎理論とシステム基盤技術の融合による Society 5.0 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

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

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）

研究成果の概要

本研究提案では、ネットワークを越えた複数のノードにわたる実行環境において、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。2024 年度は、PoC 環境の設計・構築に着手するのと並行して、「セキュアネットワークコンテナ実行基盤」や「処理・通信の監視・制御」といった安全・安心を支える各種要素技術の改良・開発に取り組んだ。

「セキュアネットワークコンテナ実行基盤」については、サービス展開の際に生じる入れ子状のコンテナ環境に対応した多層オーバレイファイルシステムについて、オーバレイの深さにより生じていた処理オーバヘッドを削減した。また、マイクロサービス環境における処理フローのモニタリングに必要となる高精度時刻同期について、汎用のネットワーク機器における同期精度を向上させる技術の研究に取り組んだ。コンテナ間ネットワークに関しては、キャリアネットワークとクラウド上のサービスを連携させて、安全な通信路を提供する技術の研究も進めた。さらに、データのレベルでの保護技術として、音声データを中心としたマルチメディアデータの仮名化技術の開発も進めた。

「処理・通信の監視・制御」については、AMD SEV で保護された VM 内で VM を安全に動作させる入れ子型 SEV を BitVisor ハイパーバイザにも完全対応させ、レジスタ保護とメモリ整合性保証を行えるようにした。また、リモートからクラウドサービスのシステム情報を取得して監視する際に、必要なメモリデータを効率良く取得する機構も開発した。さらにユーザ側に VM を移送する実行形態に向けて、クラウドとエッジサーバにまたがって一貫性を保ちながら高速に VM の状態の保存・復元を行う仕組みを開発した。また、セキュアネットワーク構成の際の通信環境のセットアップ（シグナリング）の基礎となる、安全な公開鍵共有の仕組みの開発も進めた。

【代表的な原著論文情報】

1) Aoi Ito and Katsunobu Itou: Speaker Pseudonymization for Japanese Speech Using Duration Embeddings, 26th International Symposium on Multimedia, 2024
2) Kazuki Takiguchi and Kenichi Kourai: Protecting Nested VMs with AMD SEV, 15th ACM SIGOPS Asia-Pacific Workshop on Systems (APSys 2024), poster, 2024.
3) Kanta Uesugi and Kenichi Kourai: Secure and Efficient Monitoring of Confidential VMs using eBPF, 15th ACM SIGOPS Asia-Pacific Workshop on Systems (APSys 2024), poster, 2024.
4) Tokito Murata and Kenichi Kourai: Parallel and Consistent Live Checkpointing and Restoration of Split-memory VMs, Future Generation Computer Systems, Volume 159, pages 432-443, 2024.
5) Shoma Takehara and Toshio Hirotsu: Design and Implementation of a Public Key Server Protected by Trusted Execution Environment, Asian Internet Engineering Conference (AINTECH 2024), poster, 2024.