2023 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。2023 年度は、ユーザによる自己情報コントロールを可能とするためのプライバシ保護メカニズムの設計と実装を進めると同時に、前年度に引き続き「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」といった要素技術の改良・開発を行った。

プライバシ保護メカニズムについては、保護対象となるデータに対して暗号学的仮名化により属性などに関する複数の情報開示レベルを織り込んだ暗号学的多重化仮名方式を用いて、許諾に応じて部分的な属性情報（例えば性別や年代など）だけを取り出すことを可能にしている。そして、クラウド環境においてこの仮名化情報保護を強制する仕組みとして、仮名化ブローカによりプライバシ保護に関わる制御性をサービスプロバイダから切り離す仕組みを提案し実装を進めている。「セキュアネットワークコンテナ実行基盤」については、サービスを展開の際に生じる入れ子状のコンテナ環境に対応したオーバレイファイルシステムについて、任意の深さの入れ子を可能にした。また、多数のマイクロサービス実行環境のモニタリングに必要となる高精度時刻同期のモジュール化実装を行った。「処理・通信の監視・制御」については、仮想マシン（VM）向け Trusted Execution Environment (TEE)である AMD SEV を対象に、クラウド環境上の TEE にユーザのハイパーバイザを送り込んで、SEV-ES (レジスタ状態暗号化)や SEV-SNP(メモリ整合性保護)の下で、安全にサービスを監視・制御する仕組みを実現した。また、プロセス向けの TEE である Intel SGX においても、システム監視モード(SMM)と組み合わせることで安全にクラウド上の VM を監視する仕組みの開発も進めた。

【代表的な原著論文情報】

1) 廣津登志夫, 光来健一, 尾花賢, 石黒健太. 自己情報コントロールのための仮名化サービスアーキテクチャの検討, 第 160 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, 2023-OS-160(8), pp.1-7, 2023.
2) Kazuto Kobori, Chung-han Lee, Toshio Hirotsu: Performance evaluation of portable time synchronization method using eBPF. Concurrency and Computation: Practice and Experience, Vol. 36, No.8, e7957, 2023. doi: 10.1002/cpe.7957
3) Yoshimichi Koga and Kenichi Kourai: SSdetector: Secure and Manageable Host-based IDS with SGX and SMM, 22nd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2023), pp.539-548, 2023.
4) Kento Kimura and Kenichi Kourai: Xfas: Fault Recovery by Externally Controlling OS Behavior, 16th IEEE/ACM International Conference on Utility and Cloud Computing (UCC 2023), pp.1-10, 2023.
5) Yuichi Ozaki, Sousuke Kanamoto, Hiroaki Yamamoto, and Kenichi Kourai: Reliable and Accurate Fault Detection with GPGPUs and LLVM, 16th IEEE International Conference on Cloud Computing (CLOUD 2023), pp.540-546, 2023.