

社会変革に向けた ICT 基盤強化
2021 年度採択研究代表者

2022 年度
年次報告書

山田 浩史

東京農工大学 工学研究院
准教授

細粒度のリカバリを可能にする高信頼 OS

研究成果の概要

本研究では、メモリ故障や OS 自身のバグ、OS を乗っ取る攻撃といった多様化かつ複雑化している信頼性の阻害要因による障害発生を前提として、デザインレベルで OS に対して柔軟なリカバリ機能を溶け込ませる。OS の構成要素であるメモリオブジェクトのセマンティクスに活用し、メモリオブジェクトレベルでの細粒度のリカバリを可能にする OS アーキテクチャを新規提案し、実際にソフトウェアとして実現してその有効性を示す。本研究では、1.障害によって破損したメモリオブジェクトのみを OS レベルで破棄・修正・復元、2.それで修復不可能な場合はセーフティネットとして仮想マシンモニタ(VMM)レベルでアプリケーション層のメモリオブジェクトを保持したまま OS 層のみを再構築、という 2 段階でのリカバリを達成する機構を開発する。第二年次は、OS-level でのメモリオブジェクト回復機構の設計および実装を行い、加えて VMM-level の回復機構の設計、実装を開始した。OS-level でのメモリオブジェクト回復機構については、xv6 上でのプロトタイプングを完了させた。また Linux のファイルシステムに対して回復機構の設計を開始した。VMM-level でのメモリオブジェクト回復機構に関しては、Linux-KVM を対象に設計および実装を進めている。具体的には次のとおりである。第一に、xv6 におけるメモリオブジェクト回復機構に関して、メモリ故障を想定し、ファイルシステムやメモリアロケータ、プロセススケジューラといった OS の機能ごとに作り込み、入念な動作検証を完了した。第二に、Linux については ext4 を対象としてメモリオブジェクトのリカバリハンドラの構築を行った。第三に、VMM-level における OS 回復機構の仕組みを Linux-KVM を対象に作り込み始めた。基本設計を完了させ、その正当性を検証しているところである。

【代表的な原著論文情報】

- 1) T.,Shimomura, and H.,Yamada: Hardening In-memory Key-value Stores against ECC-uncorrectable Memory Errors, Proc of the 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks(DSN'22), pp.509-521, 2022.
- 2) T.,Iguchi, and H.,Yamada: Graceful ECC-uncorrectable Error Handling in the Operating System Kernel, Proc. of the 33rd IEEE International Symposium on Software Reliability Engineering (ISSRE'22), pp.109-120, 2022.
- 3) 根津直也, 山田浩史: 耐メモリ故障性の強化を支援するフォールトインジェクタ, 第 155 回 システムソフトウェアとオペレーティング・システム研究会, 優秀若手発表賞
- 4) 和田健, 山田浩史: Reboot-based Recovery を指向する Unikernel, 第 158 回システムソフトウェアとオペレーティング・システム研究会, 最優秀若手発表賞