2024 年度年次報告書
AI 共生社会を拓くサイバーインフラストラクチャ
2024 年度採択研究代表者

葛野 弘樹

神戸大学 大学院工学研究科
准教授

攻撃耐性を備えたセキュアな基盤ソフトウェアの研究

研究成果の概要

2024 年 10 月から 2025 年 3 月の研究においては，研究課題の要素技術を明らかにし，特権昇格攻撃防止手法の研究を推進した．研究成果は国内研究会 1 件，国際会議論文 2 本である．

（2024 年 10 月～2025 年 3 月）脆弱性を利用した攻撃プログラムの実証と自動動作追跡

汎用 OS である Linux カーネルの脆弱性（特権昇格攻撃 258 件，DoS 攻撃 814 件）を利用した攻撃の実証として，研究開発環境を構築した．研究開発環境にて，研究提案者の研究開発した OS 動作追跡機構を拡張し，攻撃時の OS 処理の追跡かつ自動化解析を実施，特権昇格攻撃とDoS攻撃の OS 処理の自動動作追跡手法を検討した結果を国内研究会で報告した[1]．

（研究）脆弱性を介し権限情報改ざんを試みる特権昇格攻撃防止手法の確立

方針：システムコール単位での OS 処理の実行制御：OS への攻撃に対し，システムコール単位での OS 処理の効率的な実行制御実現が求められる．システムコール単位での OS 実行制御機構で利用するために，OS 処理の実行制御のシステムコールと関連する一連の関数コールフローを解析し，特権昇格攻撃および DoS 攻撃にて利用されるシステムコールと紐づく OS 関数の特定を進めた[1]．

方針：権限情報単位での保護制御：ユーザプロセスの権限情報に対して，攻撃時に権限情報のメモリ位置を特定し，改ざんする試みを失敗させる攻撃無効化が求められる．権限情報の保護として，権限情報への改ざん有無の遠隔監視機構[2]，ならびに権限情報のメモリ位置の前後に読書き制限を行う領域を設置する保護手法[3]，を提案し，国際会議で報告した．

【代表的な原著論文情報】

1) 葛野 弘樹，山内 利宏，システムコールと関係するカーネル関数の特定手法の提案，第 70 回情報通信システムセキュリティ研究会 (ICSS), Mar, 2025.
2) Hiroki Kuzuno, Toshihiro Yamauchi, kdMonitor: Kernel Data Monitor for Detecting Kernel Memory Corruption, The 2024 7th IEEE Conference on Dependable and Secure Computing (DSC 2024), (12, 2024).
3) Hiroki Kuzuno, Toshihiro Yamauchi, RKPM: Restricted Kernel Page Mechanism to Mitigate Privilege Escalation Attacks, The 18th International Conference on Network and System Security (NSS 2024). (11, 2024).