

論文審査の要旨および学識確認結果

報告番号	甲 第 号	氏 名	鈴木 慶汰
論文審査担当者：	主査	慶應義塾大学教授	博士(理学) 河野 健二
	副査	慶應義塾大学教授	博士(工学) 高田 眞吾
		INRIA Senior Research Scientist	Ph.D. Julia Laetitia Lawall
		Beihang University Associate Professor	Ph.D. Jia-Ju Bai
学士(工学)、修士(工学) 鈴木 慶汰君提出の学位請求論文は、「Improving Linux Kernel Reliability through Targeted Static Analysis (ターゲット特化型静的解析による Linux カーネルの信頼性向上)」と題し、全5章から構成されている。 現代のコンピューティングシステムの中核をなす Linux カーネルは、その規模の大きさと複雑さから多くのバグを含んでおり、システムの信頼性を損なう要因のひとつとなっている。ソースコードを実行せずにバグを検出する静的解析は、この問題に対処する上で不可欠な技術であるが、解析の速度と、精度・網羅性との間には根本的なトレードオフが存在する。特に、Linux カーネル開発ライフサイクルにおける二つの主要なフェーズである「日常的な開発フェーズ」と「包括的な統合フェーズ」では、静的解析ツールに求められる要件が大きく異なる。 本論文は、それぞれのフェーズごとに求められる要件を明確にし、これらの課題に対し、レスポンス重視の日常的な開発フェーズのためのフレームワークと、包括的な統合フェーズでしばしば見逃される困難なバグパターンを対象とした静的解析手法をそれぞれ提案・実装し、Linux カーネルの信頼性向上に貢献するものである。 第1章は序論であり、本研究の背景として Linux カーネルにおけるバグ検出の重要性と、既存の静的解析手法が抱える課題を述べている。特に、開発のフェーズごとに異なるツール要件に着目し、本論文が取り組む二つの主要な貢献の概要と論文全体の構成を示している。 第2章では、Linux カーネルにおけるバグ検出、特に静的解析に関する先行研究を概観している。日常的な開発ワークフローで利用される高速なツールと、統合フェーズで用いられる網羅的なメモリリーク検出ツールそれぞれの長所と限界を分析し、本論文で提案する手法の学術的な位置付けを明確にしている。 第3章では、日常的な開発フェーズ向けの高速なバグ検出手法を提案している。軽量の解析で検出可能な「Finger Traceable (FiT) bugs」というバグのクラスを定義し、これらを検出するためのフレームワーク「FiTx」の実装手法について述べている。FiTx は、関数の戻り値に応じて解析状態の伝播を制御する独自の手法を用いることで、解析速度を犠牲にすることなく高い精度を達成しており、実際に未知のバグを47件発見している。この成果は Linux コミュニティにもフィードバックし、Linux カーネルに取り込まれている。 第4章では、統合フェーズにおいて既存の網羅性に着目したツールが見逃しがちな「構造体のメンバに関連するメモリリーク」に特化した、新しいスケーラブルな静的解析手法を提案している。高コストなポインタ解析を回避しつつ、制御フローグラフ(CFG)上で直接フィールド単位の状態を追跡することにより、スケーラビリティと精度の両立を図っている。本手法により、平均5年以上も潜在していた未知のバグ12件を発見し、Linux コミュニティに報告し承認されていることを報告している。 第5章は結論であり、本研究で得られた成果を総括し、今後の研究の展望について述べている。 以上要するに、本論文は、Linux カーネル開発の異なるフェーズの特性に着目し、それぞれの課題に適したバグをターゲットとして、各々の要件を満たす静的解析手法を提案・実証したものであり、その成果はオペレーティングシステムの信頼性向上に大きく貢献するものである。 よって、本論文の著者は博士(工学)の学位を受ける資格があるものと認める。			
学識確認結果	学位請求論文を中心にして関連学術について上記審査会委員で試問を行い、当該学術に関し広く深い学識を有することを確認した。 また、語学(英語)についても十分な学力を有することを確認した。		