先端科学技術研究科　修士論文要旨

所属研究室 （主指導教員）	ソフトウェア設計学 （飯田　元　（教授））		
学籍番号	2411146	提出日	令和 8年 1月 16日
学生氏名	白井　達也		
論文題目	継続的Fuzzingの有効性に関する大規模実証分析		

要旨

近年，ソフトウェア開発においてオープンソースソフトウェア（OSS）の利用が不可欠となる一方で，深刻な脆弱性の増加が問題となっている．これに対し，CIプロセスに統合し，短時間かつ高頻度なテストを行う「継続的Fuzzing」が普及しつつある．しかし，その長期的な有効性や，従来のFuzzingに関する知見が適用可能かは十分に解明されていない．本研究では，継続的Fuzzingの長期的な有効性の推移を明らかにするため，OSS-Fuzzに参加する878プロジェクトにおける約112万回のセッションを対象に大規模な実証分析を行った．分析の結果，以下の知見を得た．(i) 継続的Fuzzingの導入時点で多くのバグが潜在しており，運用初期段階で高いバグ検出率を示すこと．(ii) 継続的Fuzzingの運用の進行に伴い，コードカバレッジは線形的に増加する傾向を示すこと．(iii) カバレッジの増加だけでなく，減少もバグ検出に寄与していること．(iv) 開発者が指定したシードコーパスは，長期的なバグ検出率の維持およびカバレッジ向上に有効であること．
本研究は，継続的Fuzzingの長期運用の有効性を実証し，今後の運用戦略やツール開発に重要な示唆を与えるものである．