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	2411076	提出日	令和 8年 1月 19日
学生氏名	加藤　陸		
論文題目	継続的ファジングにおける高リスク変更への追加ファジング実行フレームワーク		

要旨

オープンソースソフトウェア(OSS)の脆弱性検出において，継続的ファジングが広く利用されている．Google の OSS-Fuzz では，大規模な継続的ファジングが行われ，これまでに 10,000 件を超える脆弱性が発見されている．本研究では，脆弱性混入リスクが高い日を予測し，追加ファジングを実行する Just-In-Time(JIT) を用いたリスク考慮型重点的追加ファジング実行フレームワーク(RAISE)を提案する．RAISE は，特定の日に脆弱性が混入されたか否かを推定するために，日次粒度での二値分類を行う．OSV(OSS の脆弱性が記録されているデータベース)から得られる脆弱性混入コミットと，OSS-Fuzz から得られる日次のカバレッジおよび変更メトリクスを統合し，評価においては，15 件の C/C++ プロジェクトを対象にクロスプロジェクト検証を用いて RAISE の性能を検証するとともに，シミュレーションとして，追加ファジングセッションを割り当てるための 5 つの戦略を比較した．VCCFinder ベースの静的特徴量と動的なファジング特徴量を組み合わせた Random Forest によるモデルは，ROC-AUC 0.74 および PR-AUC 0.10 を達成し，ランダム予測を上回る性能を示した．特徴量重要度の分析では，カバレッジ関する特徴量，とりわけ PatchCoverage が最も高い重要度を示した．また，968 件の脆弱性を対象としたシミュレーションの結果，重回帰戦略 (Multi-Regression Strategy) は，比較した 5 つの戦略の中で最も高い効率を達成した．