

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)	サイバーレジリエンス構成学 (門林 雄基 (教授))		
学籍番号	2411002	提出日	令和 8年 1月 19日
学生氏名	青木 悠真		
論文題目	オープンソースプロジェクトにおけるセキュリティ評価指標の実証的分析		
要旨			
ソフトウェアサプライチェーンにおけるリスクが増大する中、オープンソースプロジェクトのセキュリティリスク評価に注目が集まっている。 OpenSSF Scorecardはオープンソースプロジェクトのセキュリティに対する態度を自動的に評価するツールとして期待されており、依存関係の選択において、実務者の意思決定を支援する可能性がある。 しかし、Scorecardが実際の脆弱性リスクを適切に評価できているかについて、その妥当性に関する研究は十分に行われていない。 本研究では、合計1,086,513件のリポジトリにおけるScorecardデータを収集し、Scorecardの有効性に関する実証的な分析を行った。 特に、既知の脆弱性情報が確認された4,856件のリポジトリと、脆弱性が報告されてない中から層別サンプリングを用いて抽出した同数のリポジトリを用いて、詳細な分析を行った。 本研究の結果は、実務者が依存関係を選定する際の判断基準としてのScorecardの有用性を明らかにするとともに、より安全な依存関係選択のための指標活用方法について示唆を与えるものである。			