論 文 内 容 の 要 旨

博士論文題目　Exploring Entire Software Ecosystems through Dependency Updates

氏　　名　　WATTANAKRIENGKRAI SUPATSARA

Third-party libraries provide a means for software teams to quickly build applications, avoiding the need to start from scratch. The widespread adoption of these libraries has led to the creation of large ecosystems with complex networks of interdependencies, where sustainability and security issues of a single library can have widespread network effects. Analyzing these critical issues across entire ecosystems has proven challenging without a structured framework. In this thesis, I propose a framework for comprehensive ecosystem analysis, derived from the findings of four empirical studies on contributions that are congruent with dependency updates and on unsafe dependency updates throughout the ecosystem. This framework includes a dashboard, a GitHub Action, and a set of guidelines. The dashboard presents the levels of contributions congruent with dependency updates, which are associated with the likelihood of a library becoming dormant. The GitHub Action is designed to automatically detect unsafe dependency updates in library repositories. Finally, the guidelines suggest that employing a combined qualitative and quantitative approach could yield actionable recommendations for all tiers of the ecosystem, underscoring the importance of sharing this data with comprehensive documentation for future research.

氏　名	WATTANAKRIENGKRAI SUPATSARA

（論文審査結果の要旨）

本論文は、ソフトウェア、および、汎用性の高い複数のソフトウェアを再利用可能な形でまとめたソフトウェアライブラリの間での依存関係の更新情報に基づき、それらの集合体であるソフトウェアエコシステム、さらには、ソフトウェアエコシステム群に波及する開発・保守リスクを探索的に分析するためのフレームワークを提案するものである。

今日、第三者が作成したソフトウェアライブラリ（サードパーティライブラリ）の活用は、オープンソースソフトウェアに限らず、広くアプリケーションソフトウェアの開発に浸透し、大規模なソフトウェアエコシステムを形成する原動力となっている。サードパーティライブラリの活用は、ソフトウェアの迅速な開発に大きく貢献するものであるが、同時に、ソフトウェアエコシステムを構成するソフトウェアやライブラリの間はもとより、ソフトウェアエコシステムの間にも、複雑で高い相互依存性をもたらしている。ある1つのソフトウェアやライブラリに持続可能性やセキュリティ等に関するリスク（開発・保守リスク）が生じただけで、そのリスクがエコシステム全体に波及し、他のソフトウェアエコシステムにとってもリスクとなる可能性がある。エコシステム全体やエコシステム群で波及するリスクの分析には、構造化されたフレームワークが不可欠であるとされている。

本論文で提案するフレームワークは、ソフトウェアやライブラリ間での依存関係の更新（依存関係更新）と当該更新における開発者の貢献（開発貢献）との関係、エコシステム全体にリスクが波及する「安全でない依存関係」とその更新等に関する4つの実証実験の結果から導出されたものである。具体的には、ダッシュボード、GitHubアクション、および、ガイドラインで構成される。ダッシュボードは、ライブラリが休眠状態になる可能性が高いことを示す依存関係更新と一致する開発貢献とそのレベルを提示する。GitHub Actionは、サードパーティライブラリが集積されているライブラリ・リポジトリを対象に、安全でない依存関係の更新を自動検知する。ガイドラインは、質的・量的分析法を組み合わせることで、ソフトウェアエコシステムの各層に対して、開発・保守リスク回避のための行動を推薦することができる。

以上の通り、本論文は、ソフトウェアやソフトウェアライブラリ間での依存関係の更新と当該更新に携わった開発者の貢献との関係性に着目することで、ソフトウェアエコシステム群に波及する開発・保守リスクを低減・回避するための、これまでにない具体的なフレームワークを実現した。開発・保守リスクの系統的な低減・回避につながる知見は、広くソフトウェア開発とソフトウェアエコシステムの高度化、そして、ソフトウェア工学研究の発展に大きく貢献することから、博士（工学）論文として価値あるものと認める。