大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

トップエスイー ソフトウェア開発実践演習

ソフトウェアの差分開発における Event-B適用の効果検証

キヤノン株式会社　原田真伍　harada.shingo@mail.canon

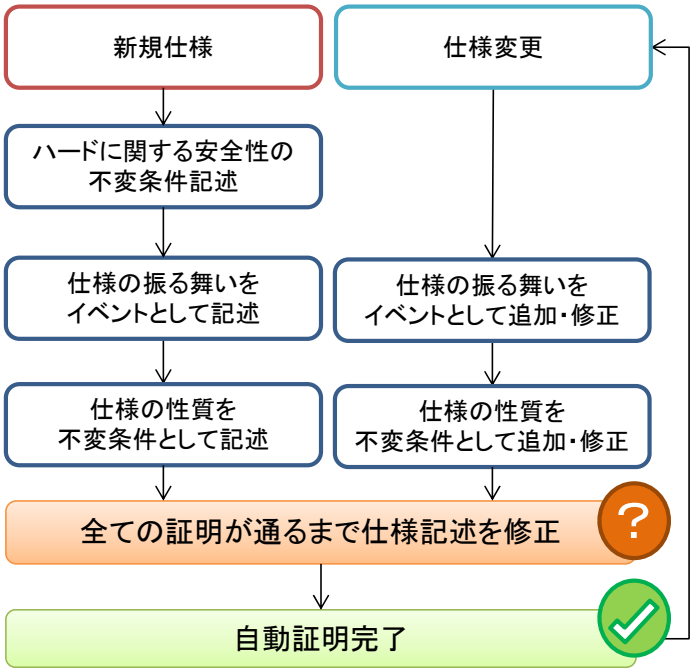
開発における問題点

ソフトウェアの差分開発において、インクリメンタルに追加される要求仕様に対し、ハードの安全性や要求仕様間の整合性の確保が出来ずソフトウェアに不具合として混入されることがある。開発下流や市場投入後に不具合が発覚する場合には、多くの手戻り工数が発生してしまう。

手法・ツールの適用による解決

Event-Bの自動証明ツール（Ateliear B Provers）を用いて、インクリメンタルに追加される要求仕様の仕様記述を行うことで、開発上流でソフトウェアの不具合混入を防ぐ。開発上流の要求仕様の段階でハードの安全性や仕様間の整合性の確保が可能かどうか、その効果検証を行う。

Event-B適用フロー



特徴

□ 特徴1
新規仕様時にハードに関する安全性の不変条件を記述し、ハードの安全性への影響を確認する土台を作る。

□ 特徴2
仕様変更時に証明完了済みの仕様記述をベースに追加・修正し、元仕様との整合性を確認する。

□ 特徴3
集合論理に基づく自動証明ツールにより、不変条件違反をテストファーストライクに抽出する。

効果確認

以下の指標から要求仕様の妥当性を評価した。
- 不変条件違反数
- イベント記述修正数

インクリメンタルに追加される要求仕様をEvent-Bで仕様記述することにより開発上流品質の確保が可能であることを確認することができた。

今後の展望

- 費用対効果の検証
  - ✓ 仕様記述工数は増加
  - ✓ バグ防止による手戻り工数は減少
- 導入に最適なスコープの選定
  - ✓ 守るべき安全性を有するモジュール
  - ✓ バグが混入されやすい複雑なモジュール