【基盤研究（S）】
総合・新領域系（総合領域）

研究課題名　証明スコア法に基づく革新的仕様検証システムの構築

北陸先端科学技術大学院大学・情報科学研究科・教授　二木（ふたつぎ）　厚吉（こうきち）

研　究　分　野：情報学-ソフトウェア
キ ー ワ ー ド：仕様記述・仕様検証、形式手法、問題仕様、CafeOBJ、証明スコア（proof score）

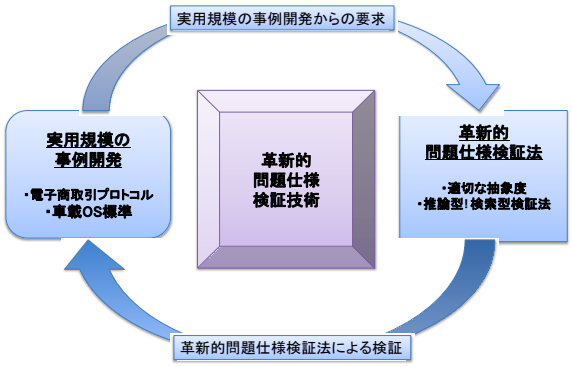
【研究の背景・目的】

問題仕様（問題領域や応用領域における組織、規則、活動、処理の仕様やモデル）の信頼性と安全性の確保は、21 世紀のソフトウェア科学技術の最重要課題の一つである。たとえば、現在多くの企業や行政組織は、客や住民の要求に迅速かつ的確に応えるべく、ネット上での新たなサービス提供に積極的に取り組んでおり、問題領域の要求を定式化した問題仕様の信頼性と安全性の確保が最重要の課題となっている。また、電気自動車への移行を想定した車載ソフトウェア分野では，操作システム(OS)などの基本ソフトウェアの機能やアーキテクチャを標準化し、多くのメーカーが柔軟に連携して高信頼で安全なソフトウェアを開発し得るオープンな体制の整備が急務であり、基本ソフトウェアの要件を定式化した標準（問題仕様）の信頼性と安全性の確保が最重要の課題である。

本研究は，信頼性や安全性を重要な要件として問題仕様を検証するための、**革新的な仕様検証技術**を研究開発する。具体的には、研究代表者二木と研究分担者緒方が研究開発してきた CafeOBJ 証明スコア法に基づく検証技術と、研究分担者青木が研究開発してきた車載 OS の検証技術の研究成果に基づき、実用的に重要な事例開発と仕様検証法の研究を相互補完的に展開することで、実用規模の問題仕様を系統的に作成しかつ検証し得る、革新的な問題仕様の検証システムを構築する。これにより、信頼性と安全性の確保が最重要の要件となる 21 世紀のソフトウェア科学技術に対する本質的かつ独創的な貢献を目指す。

【研究の方法】

現状の仕様検証技術を革新して実用的な問題仕様の検証を可能とするために、実用規模の事例に対し(1)**適切な抽象度**の問題仕様を作成し、それを(2)推論型と探索型をシームレスに融合した**推論型×探索型検証法**で検証することで、問題仕様の検証技術を確立する。具体的には、(a)**電子商取引プロトコル**と(b)**車載 OS 標準**の２つの事例を取り上げ、事例開発と仕様検証法研究の２つを相互補完的に展開することで、研究開発を推進する。これにより、実用規模の問題仕様の作成法と検証法を実証的に明らかにし、それらを **CafeOBJ に基づく問題仕様検証システム**として体系化し世界に広く発信する。



【期待される成果と意義】

(1) 適切な抽象度を持った問題仕様を作成し、それを推論型×検索型検証法で効率的に検証し得る、実用規模の問題仕様の検証システムが実現される。これにより、例えば、車載 OS 標準を曖昧性を排して客観的に形式化して記述し、(i)その標準を満たせばある性質が確保されることの検証（証明）、(ii)その標準で規定された内容だけではある性質は確保されない反例の提示（反証）、といった従来は不可能であった検証が可能となる。

(2) 電子商取引プロトコルと車載 OS 標準の厳密かつ検証可能な問題仕様が開発され公開される。これらの問題仕様は、当該分野のソフトウェアの信頼性と安全性の質的向上に資するだけでなく、より高い信頼性と安全性を達成し得る様々な革新的ソフトウェア開発技術の可能性を開く。

(3) より一般的には，様々な問題領域で，ソフトウェア開発の早期に、要求、仕様、設計などの証明や反証による検証が可能となり、信頼性や安全性が極めて重要な要件となる 21 世紀のソフトウェア科学技術への本質的かつ独創的な貢献となる。

【当該研究課題と関連の深い論文・著書】

Kokichi Futatsugi: Fostering Proof Scores in CafeOBJ, Proc. of 12th International Conference on Formal Engineering Methods (ICFEM 2010), LNCS 6447, Springer, pp.1-20, 2010. (invited keynote paper)

【研究期間と研究経費】

平成２３年度－２７年度
１３４，３００千円

【ホームページ等】

http://www.ldl.jaist.ac.jp/cafeobj/
futatsugi@jaist.ac.jp