科学研究費助成事業（基盤研究（Ｓ））公表用資料
〔平成２７年度研究進捗評価用〕

平成２４年度採択分
平成２７年３月１５日現在

アーキテクチャ指向形式手法に基づく高品質ソフトウェア開発法の提案と実用化

Architecture Oriented Formal Approaches to High Quality Software Development

課題番号：24220001
荒木　啓二郎（ARAKI KEIJIRO）
九州大学・大学院システム情報科学研究院・教授

研究の概要　本研究では、安心安全な社会を支える基盤としてのITシステムを高品質にかつ効率良く開発するために、形式手法に基づく開発法を提示して、その実用化を目指す。産学連携のもとに、形式手法適用事例研究を行い、大規模複雑なシステムを、アーキテクチャ指向の概念に基づき系統的に記述し分析・検証するための適用性の高い方法を確立する。本研究の成果を具現化する開発支援ツール群を開発して、一般の利用に供する。

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、ソフトウェア工学、アーキテクチャ、ソフトウェアライフサイクル

１．研究開始当初の背景

最近、IT システムの障害が大きな社会問題に発展する事故や事件を報道などでしばしば目にする。システムそのものに存在する不具合が原因である場合もあれば、運用操作上のミスが原因である場合もある。システムの大規模複雑化によってシステムの品質を保証することが困難になるとともに、ネットワークによって多種多様なシステムが相互に接続されることによって、一つのシステム障害による影響が波及する範囲と速さが人知の及ばぬ状況になってきた。人間の日常社会生活における社会基盤を支える IT システムが果たす役割は、今後ますます大きくなる。それに伴って、IT システムの品質に対する要求は、機能や効率のみならず、安心安全という面でも、より大きく、より高くなってきている。

IT システムの重要な構成要素であるソフトウェアの機能や安全性を保証する方法として、近年、形式手法 (formal methods) に対する関心と期待が高まっている。本研究は、アーキテクチャ指向の概念に基づいて、多様な形式手法を適材適所でソフトウェアライフサイクルの各段階において有機的に活用する方法を提案するもので、ソフトウェア・リスク分析への応用も視野に入れたより広範で高度なソフトウェア開発方法論の確立を目指す。

２．研究の目的

本研究は、アーキテクチャという観点を取り入れることにより、多様な形式手法を適材適所でソフトウェアライフサイクルの各段階において活用する方法を提案し、実行環境や操作も含めたモデル化と分析・検証にも活用できるよう形式手法の適用性を高めることによって、ソフトウェア・リスク分析への応用も視野に入れたより広範で高度な研究である。形式手法における種々の要素技術、形式手法の実用化および普及活動の実績、品質保証法、アーキテクチャ指向システム開発などに関する研究代表者および分担者のこれまでの成果に基づいて、運用・保守の段階も含むソフトウェアライフサイクル全般に亘って、アーキテクチャ指向形式手法に基づくソフトウェアの品質特性の確認と検証に有効な方法を提案し、その実用化を目指す。

３．研究の方法

本研究では、研究代表者および分担者の形式手法における種々の要素技術、形式手法の実用化および普及活動の実績、品質保証法、アーキテクチャ指向システム開発などに関する従来の研究成果に基づいて、運用・保守の段階も含むソフトウェアライフサイクル全般に亘って、アーキテクチャ指向形式手法に基づくソフトウェアの品質特性の確認と検証に有効な方法を提案し、その実用化を図る。産学連携のもとに実践的

に研究を推進することにより、開発現場における従来からの開発プロセスにおいても形式手法を組入れて有効に活用する事例を蓄積して再利用可能とし、併せて、開発支援ツールを開発し公開する。

このために以下の四つの課題に取組む。(1) 形式手法を適用したソフトウェア開発のための要素技術の提案ならびに開発事例研究、(2) 形式手法を組入れた開発プロセス参照モデルの提示と活用、(3) アーキテクチャ指向形式手法の提案、(4) 開発支援ツールの開発。

４．これまでの成果

(1) 形式的システムモデル構築法

研究を進めるにつれて、数学的背景を持つ厳密に記述された形式的なシステムモデルの有用性に対する認識がより高まった。形式的システムモデル構築方法を、予備形式化（Preformal）という新たな概念に基づいて系統的に提示できるという見通しを得た。本研究において開発中のツール群も、この予備形式化という概念で、それらの機能や利用法をうまく説明できる。

(2)開発プロセス

ソフトウェア開発の品質や効率の向上には要素技術だけでなく、ソフトウェア開発のプロセスも重要である。要素技術として形式手法に着目した場合の、その導入とプロセス改善に関する研究を行った。形式手法導入の阻害要因の一つとして、実際の開発に形式手法を導入する際に必要なプロセスのテーラリングの問題があるため、プロセス改善のモデルを用いた形式手法導入時のプロセスのテーラリングに関して検討を行った。

(3) 支援ツール開発

本研究の成果をツールの形で具現化して公開することを目的に掲げている。現在、非形式な開発文書から形式的システムモデルの構築を支援するための用語辞書に関するツール、開発の上流工程でアイデアの提示やブレーンストーミングやレビューなどを、形式仕様記述との紐付けのもとに行うことを支援する会話型のツール三種 LivelyWalkThrough、WeblyWalkThrough、CloudyWalkThrough と、形式仕様記述言語 VDM-SL による記述のための対話型ツール (VDMPad) の開発を行い、公開して一部は利用に供している。

５．今後の計画

(1)開発プロセスへの形式手法の組入れ

具体的ソフトウェアの開発事例に基づいて、種々の形式手法の中から、個別の手法をソフトウェアの開発現場で効果的に適用する方法を提示する。形式手法適用のためのプロセス参照モデルを提示して現場の開発プロセスへのマッピングを行う方法を示す。特に、テストと開発文書に着目して、ソフトウェアの品質と開発効率を向上させる実効的な方法を提案する。

(2)アーキテクチャ指向によるシステム記述と分析・検証

アーキテクチャ指向の概念に基づいて、ソフトウェアライフサイクル全般において有効な形式手法の適用方法を提示する。特に、運用や保守などの段階で、システムの実行環境や操作を考慮したシステムの機能および安全性などの品質特性の分析や検証を支援する方法を提案する。

(3)支援ツールの実用化

現在開発中のツールの完成度と実用性を高める。また、ソフトウェア開発事例を蓄積・再利用するための事例ベースを構築して、アーキテクチャ指向形式手法によるソフトウェア開発法の教育および普及のために活用する。

６．これまでの発表論文等（受賞等も含む）

[1] T. Oda, P. G. Larsen, and K. Araki: VDMPad: a Lightweight IDE for Exploratory VDM-SL Specification, Proc. 3rd FME Workshop on Formal Methods in Software Engineering, Florence, Italy, (to appear) (16-24 May 2015).

[2] S. Kusakabe, H.-H. Lin, Y. Omori, and K. Araki: Generating Supportive Hypotheses in Introducing Formal Methods using a Software Processes Improvement Model, Proc. 2nd FME Workshop on Formal Methods in Software Engineering, Hyderabad, India, (June 2014).

[3] Y. Omori and K. Araki: A Distributed Agile Formal Specification Environment, Proc. International Conference on Advanced Software Engineering and Information Systems 2013, CD-ROM, Jakarta, Indonesia, (Nov. 2013).

[4] S. Kusakabe, Y. Omori, and K. Araki: A Combination of a Formal Method and PSP for Improving Software Process, Proc. TSP Symposium 2012, http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=298101, St. Petersburg, USA, (Sept. 2012).

本研究のホームページ：
http://aofa.csce.kyushu-u.ac.jp/index.php

VDMPad ツール：
http://sourceforge.net/projects/vdmpad/
http://vdmpad.csce.kyushu-u.ac.jp/