様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年５月２３日現在

機関番号：１７１０２
研究種目：基盤研究（B）
研究期間：2009～2011
課題番号：2130009
研究課題名（和文）　ソフトウェア開発の現場で使えるフォーマルメソッドに関する研究

研究課題名（英文）　Study on Formal Methods Applicable to Practical Software Development

研究代表者
荒木　啓二郎（ARAKI KEIJIRO）
九州大学・システム情報科学研究院・教授
研究者番号：40117057

研究成果の概要（和文）：

本研究では、ソフトウェアの開発現場、特に、日本の企業において、フォーマルメソッドの導入と有効な適用を支援することを目指して、以下のような実用的な研究成果をあげた。

フォーマルメソッドを実際のソフトウェア開発に適用する際には、フォーマルメソッドの特質を理解し、自らの開発対象ならびに開発プロセスを十分認識した上で、フォーマルメソッド適用の目的を明確にして、自らの開発プロセスの中にうまく取り入れる必要がある。本研究では、産学連携のもとに実際のソフトウェア開発へフォーマルメソッドを適用した経験および知見をまとめ、ソフトウェア開発にフォーマルメソッドを適用する際の具体的な指針を提示した。また、産学連携に基づいて、学生チームによる PBL（Project Based Learning）においてフォーマルメソッドに基づくソフトウェア開発の実践を通して、フォーマルメソッドの関する知識と適用経験を企業に移転する事例研究を行うことによって、フォーマルメソッド導入の一つの有効な仕組みを提示した。

ソフトウェア開発プロセスにフォーマルメソッドを有効に向き入れるために、PSP（Personal Software Process）および TSP（Team Software Process）に準拠した開発プロセスにおいてフォーマルメソッドを適用したものを開発プロセス参照モデルとして提示した。また、VDM による開発対象の厳密な記述に関して、記述し分析する立場と、それらの記述に基づいてソフトウェアの設計ならびに実現を行う立場との両方に配慮した記述の枠組みを提示した。

フォーマルメソッド適用を支援するツールの一つとして、ソフトウェア開発の当初に提示される自然言語による記述を基にして、徐々に形式的なシステム記述を構築する課程を支援するツールを試作した。

研究成果の概要（英文）：

We present practically applicable guidelines to introduce formal methods to software development at Japanese companies through Industry-Academia collaboration in applying formal methods to real system development. Especially, we made trials to perform PBL (Project Based Learning) courses to adopt formal methods to the upper stages of system development process with technical supports on domain knowledge and project management from company engineers, and then we showed the effectiveness of PBL under Industry-Academia collaboration to transfer technology on formal methods to system development projects at Japanese companies.

We also adopted formal methods in system development processes based on PSP (Personal Software Process) and TSP (Team Software Process), and show the reference models to introduce formal methods into traditional system development processes in system development projects. We present a framework to describe formal system models in VDM both for system analysis/validation and system implementation.

We developed a prototype tool which supports system developers to describe formal system models from initial informal documents on system requirement, specification

and/or design written in a natural language (Japanese language in our case).

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	4,200,000	1,260,000	5,460,000
２０１０年度	3,400,000	1,020,000	4,420,000
２０１１年度	3,200,000	960,000	4,160,000
総　計	10,800,000	3,240,000	14,040,000

研究分野： 総合領域
科研費の分科・細目： 情報学・ソフトウェア
キーワード： ソフトウェア工学、フォーメルメソッド適用、ソフトウェア開発プロセス、形式仕様記述、産学連携、開発文書品質向上

１．研究開始当初の背景

近年、我国では、証券取引システム、銀行オンラインシステム、航空管制システム、鉄道システム、通信システムなどにおける障害により日常社会生活に大きな支障をきたし、システムの復旧や改善などに莫大な時間と人手と費用をついやす場合が少なからず発生している。ソフトウェアの大規模複雑化に加えて、ネットワークを介した相互接続による複雑な連携、ならびに、安全性や頑健性や性能などに関する高度で厳しい要求に対して、ソフトウェア開発が十分に対応できていない状況である。これらに対する有効な手段の一つとして、フォーマルメソッド（formal methods）に基づくソフトウェア開発への関心と期待が高まってきている。しかしながら、形式手法を導入して効果を上げている企業も一部にあるものの、我が国のソフトウェア開発の現場におけるフォーマルメソッドの普及は、まだ十分には進んでいない。

フォーマルメソッドの特質や効用、および、実際のソフトウェア開発プロセスとの関連などが十分に認識されていないことも、その要因の一つであると考えられる。このため、特に、我国のソフトウェア開発の現場において、フォーマルメソッドが導入され効果的に適用されることを促進するための、適用性の高いフォーマルメソッドの実用的な研究を行う必要性がある。

２．研究の目的

本研究では、我々がこれまで国内で蓄積してきた形式手法に基づくシステム開発に関する研究成果ならびにシステム開発事例、および、産学連携によるモバイル FeliCa チップ開発への形式手法適用の成功事例などの経験、さらに、研究代表者自身の国内における SEA SIG-FM や VDM 研究会などによる啓発普及活動、IPA/SEC における高信頼性システム開発法に関する委員会などにおける調査研究や産学交流、また Integrated Formal Methods 1999 や Formal Methods 2003 などのプログラム委員長や International Conference on Formal Engineering Methods 2008 の大会委員長などの国際的なフォーマルメソッドのコミュニティ活動の経験と実績に基づいて、我が国におけるフォーマルメソッドに基づく信頼性の高いソフトウェアシステムの効率的な開発を支援する方法の提案および支開発現場への導入と普及を促進することを目的とする

３．研究の方法

従来から取扱ってきた具体の実用システムを対象として、形式仕様記述言語 VDM++を用いたシステムの抽象モデルの記述を行い、そのモデルをベースとして、システムの機能、振舞い、性能、安全性など各種のシステム特性の記述と分析を有限状態機械モデル、時相論理、フィードバック制御、スケジューリングなどの理論に基づいて記述分析を行う。具体の事例としては、非接触型 IC チップ、通信制御システムなどを対象とする。それぞれ記述や分析の目的や観点が異なるので、多種多様なシステム開発における経験・ノウハウの再利用に向いている。

これらの適用事例を基に、システム開発現場においてフォーマルメソッドの導入に対する障壁を明らかにして、それを軽減して導入普及を促進するための方法をツールとして具現化して提示する。それらの有用性を評価するとともに、具体事例の蓄積とツールの改良を行う。

４．研究成果

本研究では、ソフトウェアの開発現場、特に、日本の企業において、フォーマルメソッドの導入と有効な適用を支援することを目指

して、産学官連携のもとに実際のシステム開発の事例を通して得られた経験知見に基づいて、開発現場へのフォーマルメソッド導入の問題点の分析、フォーマルメソッドの特性の考察、具体的な技術要素の提案、導入の指針の提示、導入のための教材やプロセスの提案、フォーマルメソッド適用支援ツールの開発に関する成果を得た。
(1) フォーマルメソッドに限ることではないが、新たな技術を導入し、実際のソフトウェア開発に適用する際には、フォーマルメソッドの特質を理解し、自らの開発対象ならびに開発プロセスを十分認識した上で、フォーマルメソッド適用の目的を明確にして、自らの開発プロセスの中にうまく取り入れる必要がある。本研究では、産学連携のもとに実際のソフトウェア開発へフォーマルメソッドを適用した経験および知見をまとめた。実用システム開発にフォーマルメソッドを適用した経験および知見に基づいて、ソフトウェア開発にフォーマルメソッドを適用する際の具体的な指針を提示した。
(2) フォーマルメソッドを適用する際の有効な道具建てとしての形式仕様記述言語 VDM++ を対象として、ソフトウェア開発の現場に導入することを念頭において入門解説を行い、併せて、ソフトウェア開発プロセス全体を俯瞰して、開発対象の VDM 記述に関して、記述し分析する立場と、それらの記述に基づいてソフトウェアの設計ならびに実現を行う立場との両方に配慮した記述の枠組みを提示した。さらに、仕様と実現の間の首尾一貫生を確認する手法として、map-reduce の概念に基づいて大規模テストを実施する手法を提案した。
(3) 本研究では、特に、実際の開発現場での個々の開発プロセスへフォーマルメソッドを有効に取り込む際に有用となることを目指して、PSP (Personal Software Process) や TSP (Team Software Process) に準拠した開発プロセスにおいてフォーマルメソッドを適用する事例に基づいて、フォーマルメソッドを適用したソフトウェア開発プロセスの参照モデルとして提示した。また、アジャイル開発プロセスとフォーマルメソッドとの関連に関する考察に基づいて、VDM++ をアジャイル開発においてフォーマルメソッドを有効に適用する基盤として利用する方法を提案した。また、産学連携に基づいて、学生チームによる PBL (Project Based Learning) においてフォーマルメソッドに基づくソフトウェア開発の実践を通して、フォーマルメソッドの関する知識と適用経験を企業に移転する事例研究を行うことによって、フォーマルメソッドに関心はあるものの、具体的な導入に踏み出すことができない企業に対して、フォーマルメソッド導入の一つの有効な仕組みを提示した。
(4) フォーマルメソッド適用の際には、ツールによる支援が求められる。本研究では、開発ソフトウェア開発の当初に提示される自然言語による記述を基にして、徐々に形式的なシステム記述を構築する課程を支援するツールを開発した。今後は、このツールの完成度を高めて、ソフトウェア開発の現場で使えるフォーマルメソッドを具現化したプロセスならびに支援ツールとして提供することを目指す。
(5) 本研究では、産学官連携のもとにフォーマルメソッドの入門講習会や教育セミナーへの協力も数多く行ってきた。独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センター形式手法人材育成部会との連携のもとにフォーマルメソッドのセミナーや形式手法導入パイロット教育コースなどに協力したほか、地域の産官学連携活動でのフォーマルメソッドの普及や個別の企業にける社内教育セミナーへの協力などを行った。これにより、開発現場の技術者との直接交流を通して、フォーマルメソッド導入や適用に関する問題点を認識することができ、本研究を発展させることに繋がった。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 6 件）
(1) Yusuke Wada and Shigeru Kusakabe: Performance Evaluation of A Testing Framework using QuickCheck and Hadoop, 情報処理学会論文誌, 査読有, 53 巻 2 号, pp.557-565, 2012 年 2 月.
(2) 荒木啓二郎：形式手法導入のための産学連携 PBL の活用, SEC journal, Vol.7, No.4, pp. 177-182, 2012 年 1 月.
(3) 大森洋一, 荒木啓二郎：自然言語による仕様記述の形式モデルへの変換を利用した品質向上に向けて, 情報処理学会論文誌 プログラミング, 査読有, Vol.3, No.5, pp.18-28, 2010 年 12 月.
(4) 荒木啓二郎：ソフトウェア開発現場への形式手法導入 － 形式手法適用の実経験から得られた知見 －, SEC journal, Vol.6, No.2, pp.104-107, 2010 年 6 月.
(5) 中津川泰正, 栗田太郎, 荒木啓二郎：実行可能性と可読性を考慮した形式仕様記述スタイル, コンピュータソフトウェア, 査読有, Vol.27, No.2, pp.130-135, 2010 年 5 月.
(6) 栗田太郎, 荒木啓二郎：モデル規範型形式手法 VDM と仕様記述言語 VDM++ －高信頼性システムの開発に向けて－, 日本信頼性学会誌「信頼性」, 査読有, Vol.31, No.6, pp.394-403, 2009 年 9 月.

〔学会発表〕（計 28 件）

(1) 井上心太：ツールを使用した形式仕様作成の事例研究，第 175 回情報処理学会ソフトウェア工学研究会，2012 年 3 月，東京都.
(2) Keijiro Araki: Formal Approaches to Software Development – Practice and Experience –, Software Engineering Seminar, POSTECH, Pohang Korea, December 2011, Pohang Korea.
(3) 宮下怜：VDM 記述からの Promela 記述生成における変換手法の提案，第 174 回情報処理学会ソフトウェア工学研究会，2011 年 11 月，奈良市.
(4) Yusuke Wada: Performance Evaluation of A Testing Framework using QuickCheck and Hadoop，ソフトウェアエンジニアリングシンポジウム 2011 論文集，CD-ROM，2011 年 9 月，東京都.
(5) Shinya Yamada: An Introduction of a Formal Method in PBL: A Case Report, Joint Workshop on Software Science and Engineering, IEICE-SS2011-3, pp.11-16, June 2011, Seoul Korea.
(6) 日下部茂：規律を重視したソフトウェア開発プロセストレーニングコースを利用した個人レベルでの形式手法導入の試み，ソフトウェア・シンポジウム 2011 論文集，2011 年 6 月，長崎市.
(7) 荒木啓二郎：産学連携によるフォーマルメソッド導入事例 ― 仕様の品質向上を目指して ―，ソフトウェア・シンポジウム 2011，2011 年 6 月，長崎市.
(8) Hiroshi Mochio: VDM++ as a Basis of Scalable Agile Formal Software Development, Proc. 9th Overture Workshop, CD-ROM, June 2011, Limerick Ireland.
(9) Shigeru Kusakabe: Facilitating consistency check between specification and implementation with map-reduce framework, Proc. 9th Overture Workshop, June 2011, Limerick Ireland.
(10) 荒木啓二郎：ソフトウェア検証分野における産学連携への要請，第 1 回 ソフトウェア工学の若手研究者の育成に関するワークショップ，北陸先端科学技術大学院大学，2011 年 4 月，能美市.
(11) 園田貴大：ドメイン知識を用いた検証に向けた状態遷移図の抽象化方法に関する考察，第 170 回情報処理学会ソフトウェア工学研究会，2010 年 11 月，大阪市.
(12) Yasumasa Nakatsugawa: A Framework for Formal Specification Considering Review and Specification-Based Testing, Proc. IEEE Region 10 Conference (TENCON2010), CD-ROM, T7-9.P2, November 2010, Fukuoka Japan.
(13) Yoichi Omori: Tool Support for Domain Analysis of the Software Specification in Natural Language, Proc. IEEE Region 10 Conference (TENCON2010), CD-ROM, T17-3.3, November 2010, Fukuoka Japan.
(14) Shinya Yamada: Validation of Stepwise Refinement with Test Cases Generated from Formal Specification, Proc. IEEE Region 10 Conference (TENCON2010), CD-ROM, T17-10.P2, November 2010, Fukuoka Japan.
(15) 荒木啓二郎：ドキュメントの品質と開発プロセスにおけるコミュニケーションでのフォーマルメソッドの有用性，「次世代型オフショアのあり方」ワークショップ，ソフトウェア技術者協会，2010 年 7 月，中国無錫市.
(16) 和田祐介：JUnit 向け単体テストを対象とした MapReduce 型並列分散実行フレームワークの提案，第 168 回情報処理学会ソフトウェア工学研究会，2010 年 6 月，横浜市.
(17) 大森洋一：自然言語による仕様記述の形式モデルへの変換を利用した品質向上手法，第 170 回情報処理学会プログラミング研究会， 2010 年 6 月，東京都.
(18) 荒木啓二郎：システム開発の現場でのフォーマルメソッド適用に向けての課題と方策，ソフトウェア・シンポジウム 2010，2010 年 6 月，横浜市.（招待講演）
(19) 日下部茂：大学での科学・工学的アプローチ例，ソフトウェア・シンポジウム 2010，ワーキング・グループ「ソフトウェアプロセス改善 次の 10 年」，2010 年 6 月，横浜市.
(20) 生田裕樹：QuickCheck を用いるモデルベーステスト実行のための MapReduce 型テストフレームワークの提案，先進的計算基盤システムシンポジウム SACSIS2010 論文集，pp.193-200，2010 年 5 月，東京都.
(21) 荒木啓二郎：Formal Methods の課題と今後の展開，ソフトウェア技術者協会 形式手法分科会 (SIG-FM)，2010 年 3 月，横浜市.
(22) Keijiro Araki: Formal Approaches to System Development – Practice and Experience –, ICT Seminar, Hanyang University, March 2010, Seoul Korea. (invited speech)
(23) Keijiro Araki: Application of Formal Methods to Practical System Development – Ten Commandments of Formal Methods Revisited –, International Workshop on Future Software Technologies, December 2009, Macau.
(24) 栗田太郎：形式手法適用の実際と教訓 –「形式手法の十戒」に照らし合わせて–，ソフトウェア工学の基礎ワークショップ (FOSE2009) 論文集，近代科学社，pp.25-35，2009 年 11 月，箱根.
(25) 中津川泰正：FeliCa IC チップ開発における仕様記述フレームワークの構築，ソフトウェア工学の基礎ワークショップ

(FOSE2009) 論文集, 近代科学社, pp.13-24, 2009年11月, 箱根.
(26) Shigeru Kusakabe: Leveraging Light-Weight Formal Methods with Functional Programming Approach on Cloud, Proc. 4th International Conference on Software and Data Technologies, Vol.1, pp264-268, July 2009, Sofia Bulgaria.
(27) 荒木啓二郎：形式手法の開発現場への導入について, SEA上海 Software Forum「最新のソフトウェアの課題とその方策」, 2009年7月, 中国上海市.
(28) 大森洋一：分散ストレージの安全性検証, 第 14 回情報処理学会組込みシステム研究会, 2009年7月, 名古屋市.

〔図書〕(計 3 件)
(1) 荒木啓二郎（監修）, 石川冬樹（著）: VDM++ による形式仕様記述, 近代科学社, 2011年7月.
(2) Tatsuo Okada, Keijiro Araki and Hiroaki Nishino（共編）: Proceedings of 2010 IEEE Region 10 Conference, November 2010. (CD-ROM)
(3) 山本修一郎, 藤枝純教, 岩崎新一, 荒木啓二郎, 塚本英昭（分担執筆）: 高信頼性システム開発技術の動向 ～ 形式手法を中心として ～, 独立行政法人 情報処理推進機構 ソフトウェア・エンジニアリング・センター 高信頼性システム技術作業部会, 2010年3月. (web出版)

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
特になし

６．研究組織

(1)研究代表者
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
研究者番号：40117057

(2)研究分担者
日下部 茂（KUSKABE SHIGERU）
九州大学・大学院システム情報科学研究院・准教授
研究者番号：70234416
持尾 弘司（MOCHIO HIROSHI）
筑紫女学園大学・文学部・准教授
研究者番号：70234416
大森 洋一（OMORI YOICHI）
九州大学・大学院システム情報科学研究院・助教
研究者番号：20309727

(3)連携研究者
なし