様式 C-19

# 科学研究費補助金研究成果報告書

平成２３年　３月３１日現在

機関番号：３２６８９
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号： 20500031
研究課題名（和文）設計モデルと検証モデルの体系化のためのアスペクト指向モデリング技術の研究

研究課題名（英文）Aspect-Oriented Modeling for Design and Verification Modeling

研究代表者
岸　知二（KISHI TOMOJI）
早稲田大学・理工学術院・教授
研究者番号：30422661

研究成果の概要（和文）：
設計検証にモデル検査技術を適用する際に構築される設計モデルや検証モデルのためのモデリング技術について研究を行った。ソフトウェアの設計モデルとそれを抽象化した検証モデルとは横断的な関係を持つことが多いため、シナリオベースならびに状態遷移ベースの二種類のアスペクト指向モデリングメカニズムを定義し設計検証の評価を行った。さらに検証モデル作成のリファレンスとしての想定モデルについても検討した。

研究成果の概要（英文）：
Design verifications utilizing model checking techniques require development of design model and verification model, and we have studied modeling techniques for these models. As software design model and verification model could have cross cutting relations, we have developed two aspect-oriented modeling mechanisms one is scenario based and the other is state transition based. We also developed assumption model that is used as a reference model for developing verification model.

交付決定額

（金額単位：円）

| | 直接経費 | 間接経費 | 合　計 |
|---|---|---|---|
| 2008 年度 | 900,000 | 270,000 | 1,170,000 |
| 2009 年度 | 1,300,000 | 390,000 | 1,690,000 |
| 2010 年度 | 1,300,000 | 390,000 | 1,690,000 |
| 年度 | | | |
| 年度 | | | |
| 総　計 | 3,500,000 | 1,050,000 | 4,550,000 |

研究分野：ソフトウェア工学
科研費の分科・細目：情報学・ソフトウェア
キーワード：ソフトウェア検証、モデル検査技術、アスペクト指向モデリング

## １．研究開始当初の背景

近年、組込みソフトウェアの大規模化、複雑化、短納期化の中で、いかにして高信頼なソフトウェアを実現するかが大きな問題となっており、そのための重要課題のひとつとして設計品質の向上が指摘されている。そうした中、設計検証に対して形式検証技術(特にモデル検査技術)を適用する取り組みが産業界でも進められており、ソフトウェア開発の中でどのように形式検証技術を有効に活用するかの研究が求められている。

モデル検査技術をソフトウェアの設計検証へ適用するためには、検証の基礎となる理論や検証エンジンの研究とともに、実際のソフトウェア開発の中で形式検証技術をどのように位置づけ活用するかという視点から

の研究が必要となる。ソフトウェア設計の研究はモデリング技術を基礎に進められており、設計モデルと検証モデルとをどのように体系化するかといったモデリング技術面からの研究が重要となる。

２．研究の目的

本研究の目的は、ソフトウェアの設計結果としての設計モデルと、それを形式検証する際に必要となる検証モデルとを体系付けるためのモデリング技術を提案、評価することである。

我々は、組込みソフトウェアを主対象として、モデル検査技術による設計検証の研究を進めており、最終的には設計と検証とを有機的に関連付けた検証指向のソフトウェア設計技術の確立を目指している。そのためには、設計作業と、形式検証技術による設計検証作業とをソフトウェア工学的な視点から適切に関連づける必要がある。本研究はこうした設計作業と検証作業との体系化の基盤となるモデリング技術の確立を目指すものである。

モデリング技術の観点から考えると、検証モデルは、検証する性質に必要な側面に注目して設計モデルを抽象化したものと捉えることができる。両モデルは一般に横断的な関連を持つため、アスペクト指向技術を活用したモデリング技術がそれらの体系化に適していると考えられる。アスペクト指向モデリングは AspectJ などの構造を UML 上で表現したものが多いが、シナリオを考慮したアスペクト指向モデリング等も有効と考えられる。本研究はこれらの既存研究をベースに、それをさらに発展させるものである。

３．研究の方法

本研究では、まず設計検証の事例を調査することでモデリングメカニズムに対する要件を整理する。次にそれに基づいてモデリングメカニズムの基本部分を定義し、設計検証に適用して評価をする。以降インクリメンタルに評価を繰り返し、メカニズムを拡張あるいはリファインする手法をとる。

４．研究成果

(1) 概要

設計検証の事例検討に基づき、検証モデル構築における問題点や、その構築に適したモデリングメカニズムへの在り方を検討した。一般に要求はシナリオ的に与えられることが多いとの観測から、要求やそれに関わる性質をシナリオ的に与え、それをステートマシン図で表現される検証モデルにウィーブするモデリングメカニズムの活用を検討した。具体的には、シーケンスポイントカットの考え方に基づいたアスペクト指向の検証モデルを定義し、それに基づいた設計検証を試行・評価した。

一方、ステートマシン図等で記述された検証モデル上に横断する性質に関する検証などについては、状態遷移をベースにしたアスペクト指向モデルが有効であると判断されたため、状態遷移ベースのアスペクト指向モデルを定義し、その設計検証への応用についても検討、評価した。

また、事例検討によって、設計検証では通常は設計モデルとして明示的に定義されない各種の想定事項が存在し、それらを検証モデルにどう反映するかが検証結果に大きな影響を及ぼすことが分かった。そこでそうした想定事項のモデル化を支援するために想定モデルを提案し、それを踏まえた設計検証の手法について提案し評価した。

検証モデルの構築には様々な方法があり、現状では代表的な構築手法というものが存在しない。検証モデルの検討においては、設計の中で検証をどう位置付け、どのようにモデル検査による設計検証を行うことを想定しているのか、前提とする手法の提示が必要と考えられる。そこで本研究の想定する設計検証の手法を大きな枠組みとして整理した。

以下、シナリオベースのアスペクト指向技術によるモデル、状態遷移ベースのアスペクト指向技術によるモデル、想定モデル、および検証手法について説明するとともに、本研究を通じた考察を行う。

(2) シナリオベースのモデル

モデル検査においては、検証モデルは状態モデルとして与えられることが一般的である。一方、要求などソフトウェア開発の上流ではシナリオを活用してソフトウェアのふるまいを理解することが多い。したがって設計検証においても、どういう状況でどのような性質が成り立つかをシナリオ的に定義し、それを検証するために必要な表明や処理を状態モデルにウィーブすることが適切ではないかと考えシーケンスポイントカットを用いたアスペクト指向モデルを定義した。

シーケンスポイントカットはシーケンス図などで表現されるシナリオ上でパターンとしてポイントカット（対象モデル上の修正個所の集合）を指定するとともに、対象モデル上でそのパターンに合致するふるまいに相当する部分に、アドバイス（新たな振る舞いを付け加えたり削除したりする指定）を与える。本研究では対象モデルとして、検証モデルのステートマシン図を設定し、要求などから導出される性質記述を検証する assertion などをシーケンスポイントカットで指定して、対象モデルに埋め込むことで検証を行うために利用した。

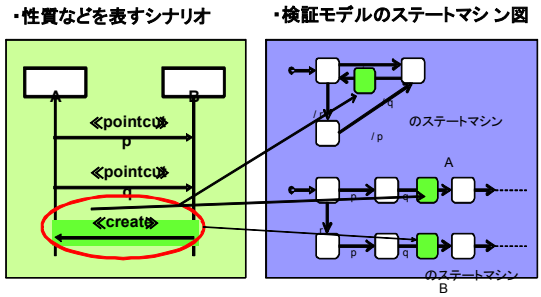


図 1　シーケンスポイントカットの例

図 1 はシーケンスポイントカットのイメージを示したもので、シーケンス図でパターンを示し、それに該当するステートマシン図の部分に、指定した処理が挿入される例を示している。

本方式の有効性を確認するために、モデル検査ツールである SPIN の仕様記述言語 Promela を対象に、シーケンスポイントカットを用いて性質検証に必要な記述を埋め込むツールを試作し、検証実験を行った。具体的にはセキュリティに関わる性質の検証を行い、一定の有効性を確認した。一方、性質記述においてシーケンスポイントカットの表現が妥当なものと妥当でないものがあること、またシーケンスポイントカットの埋め込み方式には、いくつかの技術的課題があることなどもあわせて確認された。

(3)状態遷移ベースのモデル

シーケンスポイントカットでは、検証モデルに横断するモデル要素を表現するためにシナリオを用いるが、アスペクト指向モデリングでは、より直接的にステートマシン図上の概念でそれを指定する方法がより一般的であるため、そうした手法についても評価した。

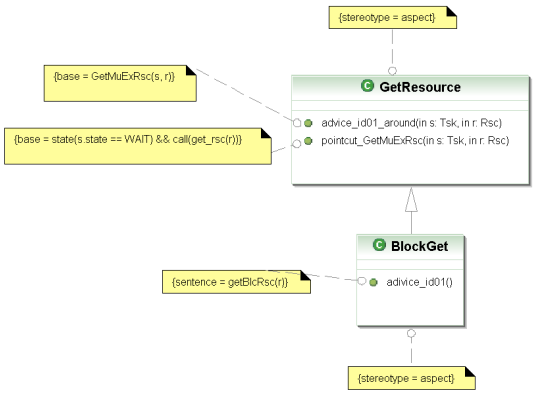


図 2　アスペクト定義の例

具体的には Stein などの提唱する UML 記法のアスペクト拡張などを参考として、ステートマシン図上にジョインポイントを定義し、それに基づいてポイントカットを指定し、検証に必要なモデル変更定義をアドバイスとして埋め込む手法を利用して、検証を行う方法を評価した。

図 2 は本モデルでのアスペクト定義の例で、GetResource というクラス記号がアスペクトを表しており、プロパティの部分にアドバイスとポイントカットが定義されている。我々は Promela 言語に対するアスペクト指向拡張言語(Aspect-Promela)を開発しており、内部的にこの機能を利用することで支援環境を試作し、設計検証に対して適用した。

外部仕様段階で、ふるまいに対する振る舞いモデルを意識するような場合（例えば電話機の外見えのふるまいを状態モデルとして理解する場合など）には、こうした状態遷移ベースのモデルを利用した性質の定義が有効であると考えられる。評価実験では RTOS のサービスコールの利用方法などを切り替えて検証する際などに、状態遷移ベースのアスペクト指向モデルが有用であることが確認された。またウィーブに関する技術的課題はシナリオベースの場合に比べ少ない。シナリオベースのモデルと状態遷移ベースのモデルとは、どちらが設計検証のモデリングに適しているというよりは、目的に応じた使い分けが重要と考える。

(4)想定モデル

上述したように、シナリオベースであっても、状態遷移ベースであっても、アスペクト指向技術を活用したモデルはソフトウェアに対して期待する振る舞いや性質の記述に一定の有用性がある。しかしながら検証はそうしたモデルで明示的に定義される情報だけでなく、例えば RTOS の設定、外部環境の想定、システムの仕様化の前提など多様な情報に強く依存する。こうした情報は多くの場合、体系だって与えられなかったり明示化されず暗黙的な想定となったりすることが多い。モデル検査においては検証に必要な情報はすべて明示的に検証モデル中に定義する必要があるため、こうした情報を整理してどういう情報をモデルに反映するかを検討するための枠組みが望まれる。

想定モデルはそうした情報を検証モデルにどう反映するかを検討する際のリファレンスとなるものである。具体的にはプロダクトライン開発で使われるフィーチャモデルの記法を応用して、検証の際に検討すべき情報をテンプレート的に整理したものである。検証においてはこのテンプレートを参照しながら、そのときの検証に必要な情報を取捨選択し、検証モデルに反映させる。

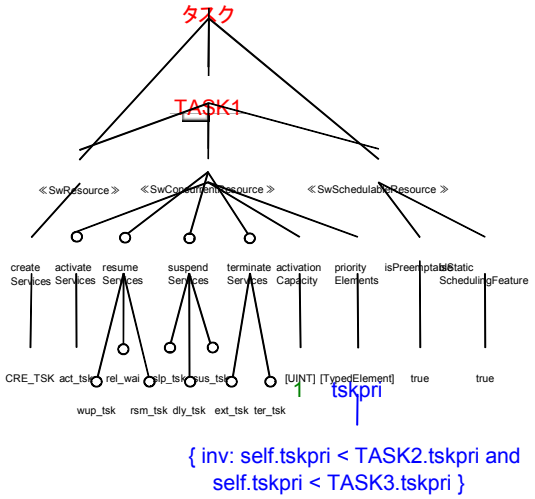


**図 3　想定モデルの例**

図 3 は RTOS の利用方法に関わる想定事項を想定モデルで記述した例である。検証に必要な具体的な情報が OCL を応用した記法で記述されており、これらを検証モデルに反映させることを意図している。またこうした想定モデルをどのように Promela への検証モデル定義に反映させるかについての一手順もあわせて検討した。

(5)検証手法

どのように設計検証を行うのかという方法や考え方によって、モデリング技術の使われ方やそれに対する要件が変わる。そこで今回の研究において想定する検証の典型的な手順を示し、その中でどのように設計モデルや検証モデルあるいは想定モデルが構築されるのかを整理した。

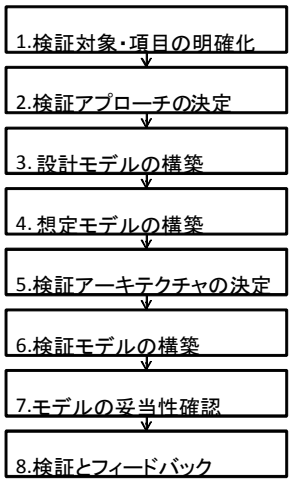


**図 4　設計検証の手順**

図 4 は我々の検討した設計検証の手順の概要を示すものであり、設計検証においてどのような事項をどのような順序で決定し、それを踏まえてどういうモデルを構築するかを示している。

(6)考察

本研究では当初設計モデルや検証モデルの構築に適した特定のモデリングメカニズムを定義することを意図していたが、上述したように目的に応じて適切なモデリングメカニズムは異なる。また想定する設計や検証の手順によって、モデルの利用方法や、モデルに求められる要件も異なることが分かった。従って目的に応じた使い分けが重要と考えられる。

またモデルは検証対象となるソフトウェアを抽象化するものであるが、モデル検査技術などを利用するためには、検証に必要な側面を正確かつ必要十分な詳細度で定義する必要があり、スケーラビリティの問題が出てくる。我々はスケーラブルなモデリングに関する国際ワークショップ(SCALE)を 2 回主催し、モデルのスケーラビリティに関する議論を重ねてきた。検証モデルの構築においてもこうしたスケーラビリティの考慮は不可欠であり、今後はスケールの観点を踏まえて、モデリングメカニズムと、その運用方法についてさらに検討を深めていきたい。

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）

〔学会発表〕（計 5 件）

① 岸知二, モデル検査のための設計モデル構築手法に関する考察, 情報処理学会ソフトウェア工学研究会, Vol2010-SE-168, No.9, pp1-6, 2010 (査読無し).
② 岸知二, ソフトウェア設計・検証手法に関する考察～モデリンの観点より～, 情報処理学会ソフトウェア工学研究会, Vol.2009-SE-165, No.5, pp1-5, 2009 (査読無).
③ 朝倉功太, 岸知二: 想定モデリングに基づくソフトウェアプロダクトラインのコア資産検証手法, 情報処理学会 組込みシステムシンポジウム 2009 (ESS2009), pp169-177, 2009. (査読有り).
④ 金井勇人, 岸知二: モデル検査のためのアスペクト指向メカニズム切替方式の提案, 情報処理学会、SIGSE vol.2008, no93, pp49-56, 2008, 情報処理学会 CS 領域奨励賞受賞, (査読無し).
⑤ 岸知二, 高橋弘, 徳田寛和, モデル検査技術を活用したソフトウェア設計・検証

手法に関する考察，情報処理学会ソフトウェア工学研究会，Vol.2008 No.55, pp95-100, 2008 （査読無し）.

〔その他〕
ワークショップ開催

① Natsuko Noda and Tomoji Kishi, New Challenge of Scalable Modeling, 2nd Workshop on Scalable Modeling Techniques for Software Product Lines (SCALE 2010), the second proc. of SPLC2010, pp191-192, 2010.
② Tomoji Kishi and Kyo-Chul Kang: Scalable Modeling Techniques for Software Product Lines (SCALE 2009), proceedings of SPLC2009, p299, 2009.

６．研究組織
(1)研究代表者
岸　知二（KISHI TOMOJI）
早稲田大学・理工学術院・教授
研究者番号：30422661