2B-01

# 複数のユースケース記述に対する モデル検査を用いた要求検証プロセスの提案

松原 潤弥† 井原 博之†† 齋藤 芳明†††

株式会社デンソークリエイト† 株式会社デンソー†† 株式会社小松製作所†††

## 1. はじめに

近年，車両制御システムに求められる機能の高度化によって要求が複雑化している．しかしながら，要求の複雑化により，レビューによる欠陥検出は限界に近付いている．

レビューに替わる欠陥検出手法として，要求を表現したユースケース記述を状態遷移モデル化し，モデル検査で検証する試みがなされている[1][2]．しかし，車両制御システム開発の要求検証において，モデル検査を用いた実用的な要求検証プロセスが確立されているとは言い難いのが現状である．

そこで要求を表現した複数のユースケース記述に対し，モデル検査を用いて各ユースケース記述の検証・複数のユースケース記述間の検証と，ボトムアップ的に検証を繰り返すことで欠陥検出を試みた．本稿は，この試みによる要求検証プロセスについて述べる．

## 2. ユースケース記述・モデル検査の特徴

### 2.1.ユースケース記述の特徴

一般的に要求定義で利用されるユースケース記述を用いることで，車両制御システムに求められる機能的な振る舞いが明らかにできる[3]．

### 2.2.モデル検査の特徴

モデル検査は，状態遷移モデルに表現した検証対象が，性質と呼ばれる検証内容を満たすことを検証する[4]．

レビューによる要求検証は，レビューアのスキルに依存するため，欠陥を見落とす可能性がある．しかし，モデル検査は状態遷移モデルが取りうる状態を網羅的に探索するため，検証内容に対する欠陥の見落としを防ぐ効果が期待できる．

A Study of Requirements Verification Process to multiple UML Use Cases using Symbolic Model Checker

†Junya Matsubara, ††Hiroyuki Ihara, †††Yoshiaki Saito

†DENSO CREATE INC., ††DENSO CORPORATION, †††Komatsu Ltd.

## 3. 提案手法

要求を表現した複数のユースケース記述を状態遷移モデルに変換して一度に検証するのではなく，まず要求を小さく分割した各ユースケース記述の単位で検証する．これにより要求の複雑さを低減するとともに，モデル検査を用いた検証のミスを防止する．次に複数のユースケース記述を連結することで要求全体の正しさを検証する．このとき欠陥はユースケース間にのみ存在するため，複数のユースケースで記述された要求であっても欠陥の特定が容易になる効果が期待できる．

本アプローチによる要求検証プロセスを図 1 に示す．

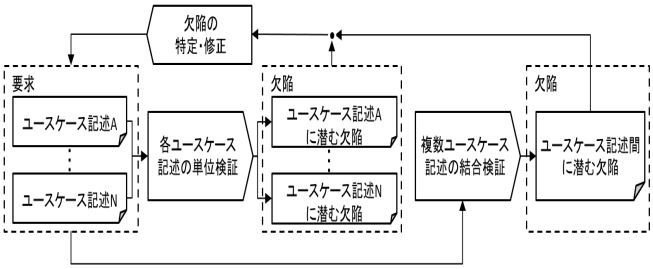


図 1. 要求検証プロセス

### 3.1.要求検証実現に向けたユースケース記述

一般的なユースケース記述[3]は，機能的な振る舞いとして，システムとアクタの間のやり取りを主系列，代替系列，または例外系列(以降，系列)に記載する．またユースケースの開始前に満たすべき条件を事前条件，ユースケースの終了後に満たすべき条件を事後条件に記載する．

これらの情報が記載されたユースケース記述をモデル検査で検証するには，ユースケース記述から状態遷移モデルおよび検証内容とする情報を決定しなければいけない．過去研究は，ユースケース記述におけるシステムとアクタの間のやり取りから状態を抽出し状態遷移モデルとしている．しかし，検証内容に関する情報は，ユースケース記述内に散在している．その結果，検証内容を決める際に，ユースケース記述を分析しなければならない．要求検証プロセスとして，規則的な検証を実現するには，これらの情

報を定型的に記述する必要があると考えた．そこで本アプローチ実現のために，次の 2 項目を新たに定義する．

まず，ユースケース記述に項目「期待する振る舞い」を設ける．「期待する振る舞い」は，ユースケース記述内に散在する検証内容となる情報であり，入力，その入力に対する出力を以下の形式で記載する．

・入力が「ある入力値」ならば，
　出力は「ある出力値」とする

次に，同様の形式で車載制御システム全体への要求項目「システムに期待する振る舞い」を設ける．要求定義時には「システムに期待する振る舞い」に対して，各ユースケース記述の系列および「期待する振る舞い」が等価になるよう各ユースケース記述を定義する(図 2)．

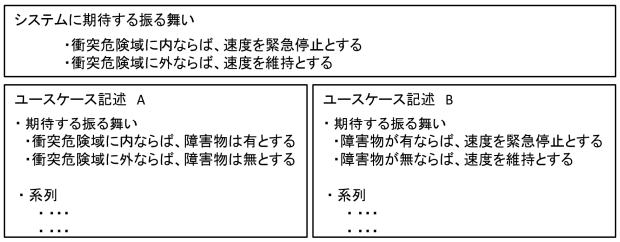


図 2.　新たに設けた項目の例

### 3.2.ユースケース記述の単体検証・結合検証

ユースケース記述の単体検証は，各ユースケース記述の系列に潜む欠陥検出を目的とする．ユースケース記述から状態遷移モデルを作成し，検証内容である「期待する振る舞い」を満たすことをモデル検査で検証する(図 3)．

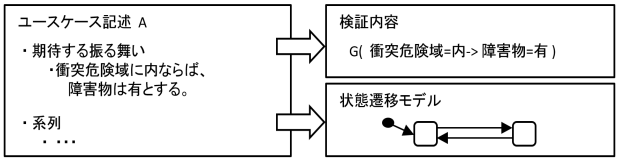


図 3.　単体検証の例

ユースケース記述の結合検証は，ユースケース記述間に潜む欠陥検出を目的とする．複数のユースケース記述を統合した状態遷移モデルを作成し，検証内容である「システムに期待する振る舞い」を満たすことをモデル検査で検証する(図 4)．

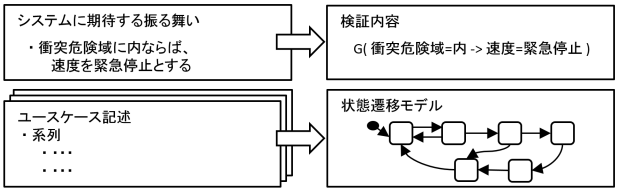


図 4. 結合検証の例

### 4.評価実験と考察

検討した要求検証プロセスの有効性を確認するために，車両制御システムの要求に見立てた 8 個のユースケース記述を用意し評価した．

実験の結果，各ユースケース記述の系列や，複数のユースケース記述間に潜む欠陥が検出できると判り，要求検証プロセスの有効性が確認できた．

本要求検証プロセスにより，複数のユースケース記述に対するモデル検査を用いた要求検証を目途付けることができたと言える．

## 謝辞

本研究は JMAAB[1]要求開発ワークショップの活動として実施した．本研究に対してご助言を戴いた関係者に感謝の意を表する．

## 参考文献

[1] 中村遼太郎，林晋平，佐伯元司，“ユースケース記述の規則への整合性検査に向けて“，ソフトウェアエンジニアリングシンポジウム 2014

[2] 高久陽平，林晋平，佐伯元司，“ユースケース記述からの状態遷移モデル生成”，情報処理学会研究報告

[3] Larman，“実践 UML-オブジェクト指向分析設計と反復型開発入門”，ピアソン・エデュケーション

[4] Alessandro Cimatti, NUSMV: A New Symbolic Model Verifier, Lecture Notes in Computer Science volume 1633

[1] Japan MBD Automotive Advisory Board の略．