5H-06

形式手法と保証ケースによるコンポーネントの妥当性確認方式の提案

山本　椋太†　　山本　修一郎†

名古屋大学大学院情報科学研究科†

1. はじめに

金融，医療，および交通システムなどの高い信頼性が要求されるシステムに対して，そのシステムが高信頼であることを適切に確認するための証拠が必要である．このため，「システムが高信頼である」という主張を証拠によって説明可能である保証ケース[1]による，システムの高信頼性保証のための方法が注目されている．

筆者らは保証ケースの適用法について検討しており[2]，エンタープライズアーキテクチャ（EA）の高信頼化を目的として O-DA (Open Dependability through Assuredness)標準を The Open Group に提案した．

O-DA では，主張が成立することを説明する証拠の信頼性を強化するために，形式手法の有用性を指摘している．しかし，形式手法を用いた証拠の作成方法については，O-DA では具体化されていなかった．

本稿では，コンポーネントから構成されるシステム開発への O-DA の適用ついて，形式手法を用いて証拠を作成する取り組みについて述べる．

2. O-DA と ABACE

O-DA 標準の目的は高保証アーキテクチャを開発するためのフレームワークとガイドラインを定義することである[3-5]．大規模で複雑なシステムのディペンダビリティを達成するために，O-DA 標準では高保証性（Assuredness）という概念を導入している．

高保証性があるとは，アーキテクチャの実装が保証すべき要求に適合していることを確信するために，満足できる水準の証拠が提供されていることをステークホルダが合意している状態をいう．アーキテクチャが高保証性を持つことを確認することが保証である．保証するための議論構造を記録する成果物が保証ケースである．アーキテクチャ指向保証ケース開発法 ABACE(Architecture Based Assurance Case Engineering)においては，保証したい対象を構成する要素とその関係に基づき，保証ケースを，以下の手順に従って系統的に作成できる[6-7]．

【手順 1】アーキテクチャを構成する 3 要素である対象システムの構成要素と関係ならびに，対象システムが満たすべき品質特性を定義する．
【手順 2】アーキテクチャに基づいて，最上位主張「システムが品質特性を満たす」を作成する．
【手順 3】最上位の主張を，構成要素とその関係に基づいて，2 つの下位の主張「構成要素は品質特性を満たす」と「構成要素関係は品質特性を満たす」に分解する．
【手順 4】この 2 つの主張を，それぞれ，構成要素と構成要素関係の実体ごとに下位の主張に分解していく．
【手順 5】最終的に，すべての構成要素と構成要素関係の実体が品質特性を満たすという主張に分解したことを確認する．

最下位の主張が成立することの確認のためには，2 つの方法がある．すなわち，主張が成立する上でのリスクを識別して対策していることを確認する方法と，形式手法による主張の正当性を証明する方法である．形式手法による主張の正当性を証明するため，形式的証拠を作成する．

3. 形式的証拠の作成法

検証すべき形式的証拠（TBV, To Be Verified）には以下の 4 種類がある[8]．[TBV 1]コンポーネントの入出力の検証，[TBV 2]コンポーネントの事前条件と事後条件の検証，[TBV 3]コンポーネント間の相互作用の検証，[TBV 4]コンポーネント間の一貫性の検証．

TBV1 について，入力の検証とは，入口のコンポーネントに入力される可能性のある値を網羅できているかの検証を指し，出力の検証とは，出口のコンポーネントが出力する可能性のある値を網羅できているかの検証を指す．

また，TBV2 について，事前条件とは入力引数が満たすべき条件であり，事後条件とは入力引数と出力引数が，満たすべき条件である．

したがって，TBV の種類に応じて，B, Event-B, VDM などの形式手法を適切に選択することになる．

4. 形式的証拠の作成法

IC カードを用いたドア制御システムを考える．図 1 にドア制御システムの構成を示す．図 1 に示

†Ryota YAMAMOTO　†Shuichiro YAMAMOTO
†Graduate School of Information Science, Nagoya University

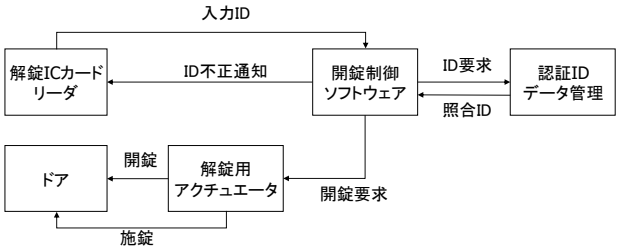

図 1　ドア制御システムの構成

したドア制御システムの信頼性を保証するためには，コンポーネントが信頼できることと，コンポーネント間の相互作用関係が信頼できることを説明する必要がある．システムが信頼できることを説明するために作成した保証ケースを図 2 に示す．

図 2 の最下位の主張に対して形式手法で証拠を作成する方法について説明する．

形式的証拠の作成について，本稿においては表 1 に示すとおりの形式手法を用いて実施した．

以下，3 において示した 4 つの形式的証拠について，その具体的な記述方法を説明する．

TBV1 について説明する．TBV1 の作成のため，各コンポーネントが入力される値および，出力される値の検証を行う．入力が正常な場合・異常な場合の双方を検証し，いずれの場合でも出力が定義域外とならないように検証を行う．

出力に関しては，返り値を格納する変数の不変条件によって検証する．定義した不変条件に対して，型検証エラーや証明できない証明責務がなければ，出力についても矛盾はない．

TBV2 は，コンポーネントの事前条件・事後条件の検証が目的である．コンポーネント自身の入出力変数の定義から逸脱していなければよい．

この検証は型検証の段階で実施されている．事後条件については，対応する不変条件を逸脱していないことから問題はないこととしている．TBV3 では，コンポーネント間の相互作用の検証が必要である．これについては，各コンポーネントに状態を表す変数(以後，状態変数と呼ぶ)によって検証する．つまり，あるコンポーネントの動作によって，他方のコンポーネントが正常な状態値ならば，コンポーネント間の相互作用に問題はない．

TBV4 のために，コンポーネント間の一貫性の検証を行う．Event-B の記述では，システムを構成する各コンポーネントの内部パラメータは，すべて 1 つのモデル内に存在する．その内部パラメータを表す変数の制約条件が満たされているかの検証と，ガード条件により内部状態の定義を厳しくすることで，一貫性を保っている．

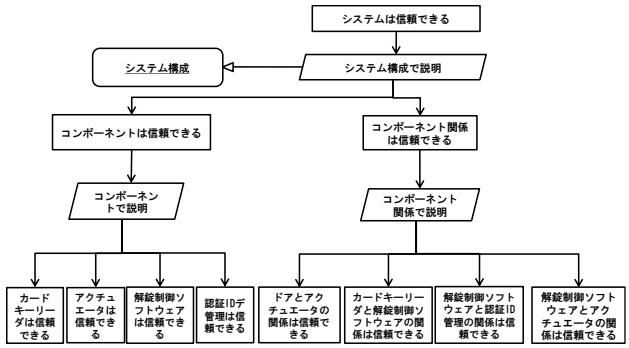

図 2　ドア制御システムに対する保証ケース

表 1　形式手法の選択例

TBV	形式手法	理由
TBV1	B	コンポーネント毎に検証でき，変数の不変条件を利用して事後条件を表現できる．
TBV2		
TBV3	Event-B	システム全体を 1 つのモデルに記述するため全体の検証に向く．
TBV4		

5. まとめ

本稿では，保証ケースと形式手法を融合する方法を提案した．これまでの O-DA では，ABACE によってアーキテクチャに基づく系統的な保証ケースの作成について具体化してきたが，保証ケースで重要となる客観的な証拠の作成については具体化していなかった．本提案では，証拠の種類を分類しておき，分類ごとに適切な形式手法の選択によって，形式手法を用いた証拠の作成法を具体化した．

今後，提案手法をより多くの例に適用して評価していく予定である．

謝辞

本研究は，科研費 JP24220001 の助成を受けたものです．

参考文献

[1] T. Kelly, A Six-Step Method for the Development of Goal Structures, York Software Engineering, 1997.
[2] 山本修一郎, 要求工学第 58 回アシュアランスケースと GSN, ビジネスコミュニケーション vol.46, No.8, pp.68-71, 2009.
[3] Open Group Standard, Real-Time and Embedded Systems:, Dependability through Assuredness™ (O-DA) Framework, 2013
[4] 山本修一郎, 連載-57 O-DA を用いたアーキテクチャ品質保証サービスの構築例, WebComputerReport, 日本経営科学研究所, pp19-28, 2016
[5] 山本修一郎, O-DA における高保証アーキテクチャ開発手法の現状と課題, KBSE 研究会, 2017.1 月
[6] 山本修一郎,森崎修司,渥美紀寿,正田稔,モデルに基づく統一的保証ケース作成手法の提案, AI 学会, KSN 研究会, 2015.
[7] 国立大学法人名古屋大学, 2015 年度ソフトウェア工学分野の先導的研究支援事業「保証ケース作成支援方式の研究」成果報告書, 2016
[8] 山本椋太, 山本修一郎, コンポーネントベース開発に対する O-DA による形式的妥当性確認手法 , KBSE 研究会, 2017.1 月