様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　　７　日現在

機関番号：　１４６０３
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００１００

研究課題名（和文）議論学を応用したソフトウェアインテグリティレベルの提案

研究課題名（英文）Defining software integrity levels using argumentation theory

研究代表者
高井　利憲（Takai, Toshinori）

奈良先端科学技術大学院大学・情報科学研究科・客員准教授

研究者番号：１０４２５７３８

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：反論も記述可能なアシュアランスケースの枠組みとして，双極木議論フレームワークを提案した．その意味を与えるため，抽象対話議論の部分クラスとして，証拠に基づく双極抽象対話議論を定義し，双極木議論フレームワーク上においても，数理議論学で基礎となる無衝突性や選好拡張を定義できることを示した．さらに双極木議論フレームワークに基づき，アシュアランスケースの合成手続きを提案した．具体的には，アシュアランスケースの合成が満たすべき性質を提案し，それらを満たす撤回可能ゴール構造条件の十分条件を一つ示した．この結果は，ソフトウェアインテグリティレベルの分配手法を与える上で基礎となるものである．

研究成果の概要（英文）：We proposed a bipolar multirelational evidence-based argumentation framework for describing assurance cases with explicit counter-arguments. For the semantics of the framework, we also propose a subclass of abstract dialectical framework, called an evidence-based abstract dialectical framework and showed that conflict-freeness and the preferred-extension can be defined for that framework. Moreover, we also proposed a modular construction for assurance cases. Precisely, we proposed criteria for modular constructions among assurance cases and we showed a sufficient condition of a subclass of defeasible goal structuring notations for that criteria. This result can be the basis for defining decomposition of software integrity levels.

研究分野：　情報科学

キーワード：　アシュアランスケース　論証　議論　ゴール構造化表記法　抽象対話議論

１．研究開始当初の背景

航空機や自動車などの安全性を求められるシステムにおいては，保証する安全性の程度を表す指標であるインテグリティレベル(integrity level)を求められることが一般的である．例えば，自動車のパワーウィンドウの制御ソフトウェアとブレーキシステムのそれとでは，ともに安全性に関係はするが，必要な保証の程度は異なる．このように，リスクの程度について関係者間で共通の理解を得るための指標がインテグリティレベルであり，産業分野毎に国際標準規格が存在する．一般に，その根拠となっているのは，ハードウェア分野の信頼性工学の知見であり，例えば，機能安全規格 IEC61508 では，安全機能の故障率によりインテグリティレベルを規定している．ソフトウェアに対するインテグリティレベルもその必要性は古くから認識されており，1998 年には，ソフトウェア一般のインテグリティレベルを扱う ISO/IEC15026 (JIS X 0134:1999)が発行されている．しかし，波及した分野規格も含めて，その定義は経験に基づく基準しか与えられていないのが現状である．

一方で，ソフトウェアのリスクに関する性質の保証手段として，近年アシュアランスケースが普及しつつある．アシュアランスケースは，安全性に限らずセキュリティやディペンダビリティなどの性質に関する主張を記述する文書である．従来の仕様書と違い，その主張を支える証拠に基づいた議論(argument)による論証を含むことが特徴である．

２．研究の目的

本研究では，議論学の技術を応用することにより，理論的な裏付けのあるソフトウェアインテグリティレベルを提案する．具体的には，アシュアランスケースに対して，議論学の知見を応用した評価法を提案する．従来，評価の難しかったソフトウェアのリスクに対して，理論的裏付けのある評価法を与えることにより，ソフトウェアの安全性や信頼性，セキュリティなどの保証技術の向上に貢献できると期待する．

３．研究の方法

まず上述した課題の解決のための基礎として，議論学を応用することにより，反論を記述できるアシュアランスケースの表現形式に対する意味論を与える． 次に，この意味論に基づくアシュアランスケースの合成を表す演算を提案する．

次に，これらの手法を具体的な事例に対して適用するケーススタディを実施する．ケーススタディは，安全性や信頼性，セキュリティなどの性質の保証が必要なシステムを想定し，システム保証の活動を仮想的に実施することを想定する．

最後に，アシュアランスケース集合の意味論に基づくソフトウェアインテグリティレベルを提案することを目指す．

４．研究成果

議論学を応用したインテグリティレベルを提案するにあたり，以下の研究成果を得た．

(1) 反論などを記述可能なアシュアランスケースの表記法として提案している撤回可能ゴール構造表現の意味を記述可能な枠組みとして，双極木議論フレームワークを提案した．これは，Dung の議論フレームワークに対して，反証と支持の両関係をもち，複数の意見が存在してはじめて成立する反証と支持，それらの関係に対する異議申し立てなどを同時に表現できる枠組みである．

(2) 上述双極木議論フレームワークに基づき，撤回可能ゴール構造表現で記述されたアシュアランスケースの合成手続きを提案した（図 1）．まず，アシュアランスケースの合成が満たすべき性質を提案し，それらを満たす撤回可能ゴール構造条件の十分条件を一つ示した．これは，異なる視点から導かれる複数の合理的な解決策の集合を提示する手法とみなすことができる．以上(1)及び(2)の結果は，議論学に基づいたソフトウェアインテグリティレベルを提案するにあたり，インテグリティレベルの分配手法を与える上で基礎となるべき結果である．

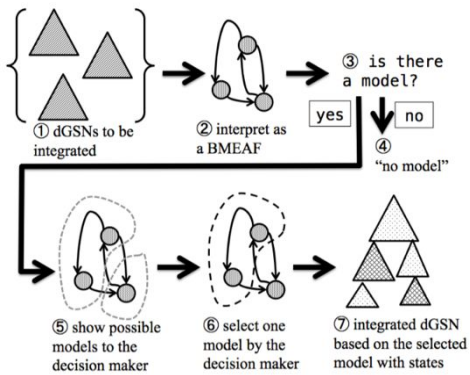

図 1 アシュアランスケースの合成手続きの概要

(3) 消費者向け製品のための効果的なリスク共有手法にむけた取り組みについて発表した．従来産業界でリスク共有のために使用されているアシュアランスケースに対して，構造化された表現が消費者に馴染みがないこと，及び記述が巨大になりうること，とい

った問題点を解決することにより，消費者に対してもリスク共有が可能となるような手法の提案を目指す研究である．本研究においても，議論学を応用して記述された議論の記述を含むアシュアランスケースから，議論の情報を用いて消費者に提示する情報を抽出するものである．

(4) インテグリティレベルを適用する分野のケーススタディを進めた．具体的には，自動車の自動運転における運転操作システム，ドローンを用いることを想定した宅配システム，介護施設における介護ロボットについて，インテグリティレベルを定義するための基礎となるシステム定義やリスク分析，安全性論証などの成果物を作成した．

(5) 議論学を応用したソフトウェアの受け入れテストの効率化手法を提案した．本提案は，議論学に基づくアシュアランスケースの，既存のソフトウェア開発プロセスの効率化に関する応用研究である．本成果については，安全性に係わるソフトウェアの開発手法などを発表する場であるクリティカルソフトウェア ワークショップにおいて発表し，一般講演の部の最優秀賞を受賞した．

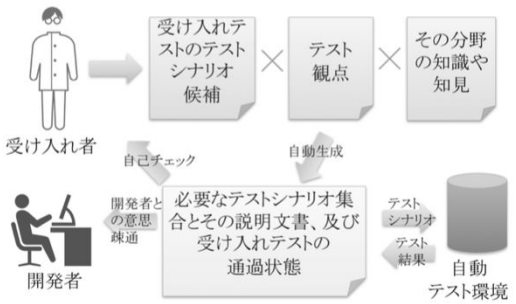

図 2 議論学を応用したソフトウェア受け入れテストの効率化手法の全体像

(6) 抽象対話議論の部分クラスとして，証拠に基づく双極抽象対話議論を定義し，いくつかの証明基準に基づく論破関係と擁護関係を与えた．それらに基づいて，無衝突な論証集合や選好拡張を定義した．これは，(1)で提案した双極木議論フレームワークにおいても，数理議論学で基礎となる無衝突性や各種拡張が定義できることを示す結果である．

(7) ゴール構造化表記法のストラテジノードに対して，数理議論学の知見を用いた分類を試みた．具体的には，数理議論学における議論スキーマを用いて，ストラテジノードの特徴付けを試みた．また，関連する講義の演習で得られたゴール構造化表記法の記述例を用いてストラテジノードの分析することにより，分類の妥当性を検討した．本成果であるストラテジノードの分類に基づき，より精密なインテグリティレベルの提案に繋がると期待される．

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 8 件）

① Toshinori Takai: Modeling evidence-based arguments by abstract dialectical framework, 3rd International Workshop on Argument for Agreement and Assurance (AAA 2017)(国際学会), 2017 年.

② 高井利憲: 議論スキーマからみた GSN/D-Case のストラテジに対する考察, D-Case 研究会, 2017 年.

③ 宮村純真, 高井利憲: 介護施設における移動介護ロボットのシステムアシュアランス, 第 12 回 D-Case 研究会, 2017 年.

④ 長村佳歩, 高井利憲: 自動運転システムにおける運転指示ソフトウェアのシステムアシュアランス, 第 12 回 D-Case 研究会, 2017 年.

⑤ 高井利憲: ソフトウェアの受け入れテストに対するゴール構造化表記法を用いた効率化の取り組み, 第 14 回クリティカルソフトウェアワークショップ, 2016 年.

⑥ 八木英光・高井利憲・飯田元: 消費者向け製品のための効果的なリスク共有手法の提案, 知能ソフトウェア工学研究会(SIG-KBSE), 2016 年.

⑦ 高井利憲: ペルソナに基づく D-Case の記述, 第 8 回 D-Case 研究会, 2015 年 05 月

⑧ Toshinori Takai, Hiroyuki Kido, and Yutaka Matsuno: Modular construction of assurance cases written in defeasible goal structuring notation, 2nd International Workshop on Argument for Agreement and Assurance (AAA 2015)(国際学会), 2015 年.

６．研究組織

(1) 研究代表者
高井 利憲（TAKAI, Toshinori）
奈良先端科学技術大学院大学・情報科学研究科・客員准教授
研究者番号：10425738

(2) 研究分担者
高橋 和子（TAKAHASHI, Kazuko）
関西学院大学・理工学部・教授
研究者番号： 30330400

木藤 浩之（KIDO, Hiroyuki）
電気通信大学・情報学専攻・客員研究員
研究者番号：　90705287

松野 裕（MATSUNO, Yutaka）
日本大学・理工学部応用情報工学科・
准教授
研究者番号：　70534220

(3) 連携研究者
古澤 仁（FURUSAWA, Hitoshi）
鹿児島大学・理工学域理学系・教授
研究者番号：　00357930