

科学研究費助成事業 研究成果報告書

平成 27 年 6 月 9 日現在

機関番号：14603

研究種目：若手研究(B)

研究期間：2013～2014

課題番号：25730044

研究課題名(和文) レビュー結果を利用したアシュアランスケースの効率的な構築保守手法の開発

研究課題名(英文) An effective development method of an assurance case from software review results

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・特任准教授

研究者番号：10425738

交付決定額(研究期間全体)：(直接経費) 1,500,000円

研究成果の概要(和文)：近年産業界でも用いられているアシュアランスケースの構造的な表現方法の一つであるGSNに対して、反論を記述する方法を導入し、撤回可能GSNとして提案した。反論の記述は、ソフトウェアレビュー結果を構造的に記録する際に必要となるものである。また、データマイニング分野の技術を応用することにより、レビュー記録などを含む大量の成果物から、アシュアランスケース構築に必要な情報を抽出する手続きを提案するとともに、提案した手続きを評価するためのアシュアランスケースの品質指標を定義した。以上の提案手続きや品質指標などを用いて評価実験を実施し、従来手法に対して提案手続きに優位性が存在する可能性を示した。

研究成果の概要(英文)：We propose a defeasible GSN (dGSN) by introducing some supplemental notation and semantics in order to express rebuttals for existing arguments and to show the status of the arguments. Rebuttals in arguments can be used to record the results of software review activities in a structural and effective way. We also propose procedures for retrieving information used for constructing an assurance case by applying some data-mining techniques and in order to evaluate the proposed procedures, we consider some quality metrics of assurance cases written in GSN. The experiments we conducted to evaluate the proposed procedure, based on the proposed quality metrics, showed there are capabilities that our procedures have some advantages in comparison with the traditional construction of assurance cases.

研究分野：ソフトウェア工学

キーワード：アシュアランスケース セーフティケース ソフトウェアレビュー ディペンダビリティ 撤回可能性
議論 説明責任

1. 研究開始当初の背景

航空機や発電所など高い安全性を求められるシステムにおいては、証拠に基づく安全性に関する「議論」、およびそれらに支えられた安全性に関する「主張」を記述する文書である安全ケース (safety case) を作成することが一般に浸透している。近年では、自動車の車載組込みソフトウェアや医療関連ソフトウェアなど身近なシステムのソフトウェアに対しても、国際標準規格などで安全ケースを要求されることが多くなってきている。航空機や発電所など、安全性に多くのコストがかけられるシステムに関しては、膨大な記述量になりうる安全ケースを作成・管理する要員を確保することが可能であったが、厳しいコスト制約のある消費者向けの組込みソフトウェアなどに関しては、その記述と管理が大きな課題になっている。

一方、既存のソフトウェア開発における代表的な活動の一つに、インスペクションやウォークスルー、設計レビューなどを含むソフトウェアレビューがある。レビューはソフトウェア技術者のもっとも知的な活動の一つであるため、その成果物には価値の高い情報が含まれているといえる。しかしその表現は、一般には、発見された誤りやレビュー会議中に議論された懸案などを順に列挙した「表形式」で記録されるだけである。より構造化して記録すれば、レビューで得られた知見の再利用などより有効活用できると予想される。また、レビュー記録をシステム保証の視点からみると、(1) 開発者間の議論を通じた対象の誤りの原因についての考察、(2) その対応策などの妥当性に関する考察、なども含まれる。これら (1) および (2) は、アシュアランスケースの記述に必要な情報の重要な部分を構成していると考えられる。

2. 研究の目的

そこで、まずはソフトウェアレビュー記録をアシュアランスケースとして記述することにより、レビューによって得られた情報の構造化とそれによる再利性の向上を目指す。これは、レビューという通常のソフトウェア開発でも実施している活動の記録から、アシュアランスケースに関する情報が得られるというだけでなく、レビュープロセス自体の効率化にも繋がるのが期待される。

さらに、レビュー記録が単純な目視によっては把握できないほど大量にあることを想定し、そのような情報に対してトピックモデリングや形式概念分析の技法を応用して、アシュアランスケースの議論の構造や議論で使用するべき証拠の候補などの情報を抽出することを目指す。抽出された情報を利用して、

ソフトウェア開発におけるアシュアランス担当者 (アシュアランスケースを構築・管理する者) の支援を行う。具体的には、従来、ソフトウェア開発時に生成される膨大な量の成果物について、アシュアランス担当者が注意深くその証拠能力を確かめ、バージョンなどの整合性を管理していたものを、ある程度自動的にどのような議論に関係するのかの情報を提供することにより支援することを目的とする。

一方、現在産業界でも利用が始まっている、アシュアランスケースの構造的な表現形式である GSN (goal structuring notation) には、一般の意味での議論における反論や、却下された対案とその却下理由を書く方法が規定されていない。これらは、意思決定や合意形成という役割を担うアシュアランスケースには必須であると思われるにもかかわらず、である。ソフトウェアレビューの記録を GSN 形式で記述することを目的に、現状の GSN と矛盾しない形でそれら反論や却下理由の表現方法を提案する。

3. 研究の方法

大量のデータを扱うための手法であるトピックモデリングおよび形式概念分析を応用することにより、アシュアランスケース記述に必要な情報の抽出手続きを構築する。次に、いくつかのオープンソースソフトウェアのプロジェクトを対象とした評価実験を行う。ここでは、プロジェクトの課題管理システムなどで公開されているバグ報告票をレビュープロセスの成果物と見立てる。また、実験を通じた提案手法の評価を目的として、GSN で記述されたアシュアランスケースの評価指標を提案する。一般に、アシュアランスケースは、リスクに関するコミュニケーションの媒体として期待されているものであり、定量的な評価基準などはあまり利用されないが、本研究ではアシュアランスケースの構築手法間の相対的な比較のための指標を導入する。

これと並行して、議論学 (argumentation theory) の知見を応用することにより、現在アシュアランスケースの構造的記述に産業界でも利用され始めている GSN をベースとした、反論などを記述可能なアシュアランスケースの構造的な表記法を提案する。

4. 研究成果

(1) レビュー記録からアシュアランスケースに必要な情報を抽出する手法として、トピックモデリングや形式概念分析など、データマイニング分野の技術を応用した手続きをいくつか提案した。現状では、アシュアランスケースの構造的議論の自

動構築までは至っていないが、その端緒を開くことができた(発表論文 , ,) .

- (2) 上述提案手法を評価するにあたり、現在産業界でも用いられているアシュアランスケースの構造的な表現形式の一つである GSN で記述されたアシュアランスケースの品質指標をいくつか提案した(発表論文).これは、主に提案手法間や提案手法と従来手法とを比較するために導入したものである .
- (3) さらに、それら抽出した情報からアシュアランスケースを構築するために、議論学で用いられる Carneades モデルを応用した GSN 記述手続きを提案した(発表論文).これはアイデアを提示した段階であり、今後実証研究が必要である .
- (4) 以上の提案手続きや品質指標などを用いて評価実験を実施し、提案手続きにおいて、従来手法に対して優位性が存在する可能性を示した(発表論文).実験は、オープンソースの教育支援システムである Moodle の課題管理システム(issue tracking system)に含まれるチケットの集合を対象とし、そこからトピックモデリングなどの技術を応用して、アシュアランスケースに必要な情報の抽出を試みた .また、アシュアランスケースの議論構造の抽出も目指して、形式概念分析による抽出した情報の構造化も試みた .実験では、マニュアル(目視)による抽出と比較して、効率よく情報抽出が可能になることを示すことができた .
- (5) GSN に対して、ソフトウェアレビューに含まれる情報を構造的かつ効果的に記録する際に必要となる反論を記述する方法を導入し、撤回可能 GSN (defeasible GSN, dGSN)として提案した(発表論文).本提案は、上述評価実験で得られた知見をベースとしている .撤回可能 GSN は、GSN の記法を大幅に変更することなく、議論学における反論や撤回可能性を表現可能であり、現在、ツール開発ベンダーとツール化を進めている .
- (6) 撤回可能 GSN で記述されたアシュアランスケースに基づくシステムのリスク抑制のための完全性水準(integrity level)を定義するための枠組みを提案した(発表論文).これはアイデアを提示した段階であり、今後実証研究が必要である .
- (7) 提案した撤回可能を用いて、今後アシュアランスケースの効率的な構築に必要なと予想される、アシュアランスケースにおける議論の合成手続きを提案し、整合的な議論が得られるための十分条件を一つ示した(発表論文).これはアイデアを提示した段階であり、今後実証研究が必要である .
- (8) その他、アシュアランスケースの効率的な構築方法の一つとして、ソフトウェア

要求分析などで利用されるペルソナを応用した手法を提案した(発表論文).これはアイデアを提示した段階であり、今後実証研究が必要である .

- (9) また、ソフトウェアライフサイクルにおいて、アシュアランスケースを効率的に保守するために必要となる、既存成果物とアシュアランスケースとのトレーサビリティに関するモデルを提案している(発表論文).

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 1件)

Khana Chindamaikul, Toshinori Takai, Daniel Port, and Hajimu Iida: "Automatic Approach to Prepare Information for Constructing an Assurance Case," NAIST Technical Report, NAIST-IS-TR2014002, Nara Institute of Science and Technology Graduate School of Information Science, December 2014.

[学会発表](計 8件)

泉川大樹, 高井利憲: "ペルソナに基づく撤回可能付き GSN 構築手法の提案 --システムアシュアランス導入に関するリスクケースを題材として--, "' 電子情報通信学会技術報告, 知能ソフトウェア工学研究会(KBSE), pp. 55-58, 2015年3月6日, 電気通信大学(東京, 調布市).

高井利憲, 木藤浩之, 松野裕: "アシュアランスケース構築のための議論合成法," 電子情報通信学会技術報告, 知能ソフトウェア工学研究会(KBSE), pp. 59-64, 2015年3月6日, 電気通信大学(東京, 調布市).

Toshinori Takai and Hiroyuki Kido: "A Supplemental Notation of GSN Aiming for Dealing with Changes of Assurance Cases," In IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), The Fourth Workshop on Open Systems Dependability (WOSD2014), pp. 461-466, November 4, 2014, Naples (Italy).

Khana Chindamaikul, Toshinori Takai, and Hajimu Iida: "Retrieving Information from a Document Repository for Constructing Assurance Cases," In IEEE International Symposium on Software Reliability Engineering Workshops

(ISSREW), The 2nd International Workshop on Assurance Cases for Software-intensive Systems (ASSURE 2014), pp. 191-203, November 5, 2014, Naples (Italy).

Kenji Taguchi, Souma Daisuke, Hideaki Nishihara, and Toshinori Takai: "Linking Traceability with GSN," In IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), The 2nd International Workshop on Assurance Cases for Software-intensive Systems (ASSURE 2014), pp. 192-197, November 5, 2014, Naples (Italy).

Toshinori Takai and Hiroyuki Kido: "A Framework for Defining Degree of Confidence for Assurance Cases," Proc. of the 53rd Annual Conference of the Instrument and Control Engineers of Japan (SICE 2014), Organized Session Position Paper, September 10, 2014, Hokkaido University (Hokkaido, Sapporo).

Khana Chindamaikul, Toshinori Takai, and Hajimu Iida: Constructing assurance case using information from an issue tracking system, ソフトウェアエンジニアリングシンポジウム (SES2013), 2013年9月9日, 東洋大学 (東京, 文京区).

高井利憲: アシュアランスケース入門と最近の動向, ソフトウェアエンジニアリングシンポジウム (SES2013), 招待講演, 東京, 2013年9月9日, 東洋大学 (東京, 文京区).

〔図書〕(計 0件)

〔産業財産権〕

出願状況(計 0件)

取得状況(計 0件)

〔その他〕

ホームページ等

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・特任准教授

研究者番号: 10425738