車載システム開発におけるディペンダビリティ保証の現状

Present status of assuring dependability on automotive system development

小林 展英[1,2]　林 香織[1]　山本 修一郎[2]

Nobuhide Kobayashi[1,2], Kaori Hayashi[1], and Shuichiro Yamamoto[2]

[1]株式会社デンソークリエイト

[1]DENSO CREATE Inc.

[2]名古屋大学大学院情報科学研究科

[2] Graduate School of Information Science, Nagoya University

概要

今後の車載システムは，IoT 機器との接続，機械学習されたシステムとの連携など運用開始後の変化を前提とした開発が不可欠となる．本稿では，このような状況下で車載システムのディペンダビリティを保証する際の課題を明らかにし，その解決に有効な手法について紹介する．

Abstract:

In near future, automotive system will be connected to IoT devices, and machine learning system. These are continuously updating after operation starts, therefore automotive system engineers will have to consider the characteristic. This paper introduces issues of assuring dependability on the above circumstances, and the effective methods for each issue.

1. はじめに

従来の自動車業界では, 運用後の振る舞いが固定化できることを前提とした自動車単体で実現されるシステムを中心に品質保証に取り組んできた．しかしながら，今後の自動車業界は，様々な機器が有する情報を連携させることで，自動運転をはじめとする高度なシステムの実用化を目指している．この分野におけるシステムの障害は，ユーザの生命に対する危険，およびユーザの個人情報の流出をもたらし，大きな社会問題を招く．また，このようなシステムの多くは，自動車単体で実現されるのではなく，図 1-1 に示すように, 自動車が置かれた状況に合わせて動的に着脱される他車, IoT 機器, 社会インフラのような他システム群，実世界の状況に合わせて常に進化する知識群，さらにそれら膨大な情報群を効率的に扱う人工知能, などと連携することで実現される．これらのシステムは運用開始後も進化することに価値があり，従来の自動車業界が品質保証の前提としてきたシステム特性とは大きく異なっている．このように，今後の自動車業界では，品質に対する価値観が互いに異なるシステムが相互に連携して一つのシステムを実現していくこととなり，こうした状況は，前述した問題の解決をさらに難しくしている．

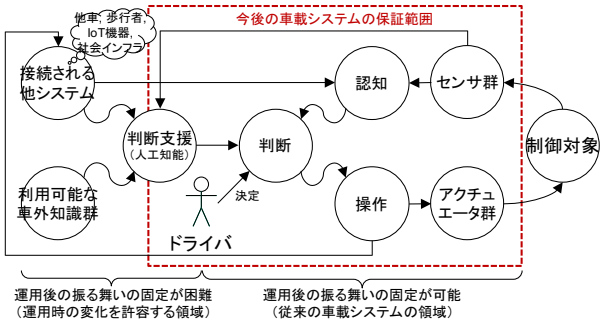

図 1-1 今後の車載システムの構成

このような状況下で, システムのディペンダビリティを保証する手段として O-DA (Open Dependability through Assuredness)[1]が注目されている．O-DA は，The Open Group で標準化されたオープンシステムに対するディペンダビリティ品質保証フレームワークであり，開発活動は TOGAF (The Open Group Architecture Framework)[2]に基づいている．O-DA の特徴は, TOGAF に基づいて作成した設計成果の品質状況をアシュアランスケースを用いて確認し，その結果を関係者と常に合意形成できている点にある．アシュアランスケースは，議論の前提条件を明らかにし，その前提条件に基づいて議論を構造的に分解

して記述できる文書である．システムのディペンダビリティに関する議論にアシュアランスケースを使用することで，異なる価値観を有したステークホルダ間の前提条件を揃え，議論内容を正しく共有することが可能となる．

しかしながら，車載システム開発における従来のアシュアランスケースの研究には，図 1-2 に示す 5 つの課題が存在している．次章でそれぞれの課題について説明する．

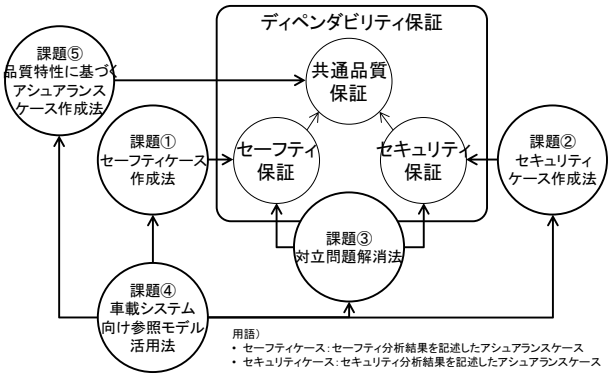

図 1-2 アシュアランスケース作成における課題

2. アシュアランスケースの課題

2.1. 課題①セーフティケース作成法

現在，車載システム開発では，HAZOP（Hazard and Operability Studies）[3]，FTA（Fault Tree Analysis）[4]といった分析手法を用いて安全性を分析し，その結果に基づいて車載ソフトウェアの開発を進めている．ISO26262 の本格導入を想定すると，これに加えて開発した車載システムの安全性を第三者に納得してもらうためのアシュアランスケースの作成が必要になる．アシュアランスケースの作成には，記述品質の安定化を図るために，GSN(Goal Structuring Notation)[5]，D-Case[6]などの図式言語の採用が期待されるが，従来のアシュアランスケース作成法では，HAZOP，FTA の分析結果を証拠として用いる，という分析過程が反映されない単純で間接的なガイドラインしか存在していなかった．このため，開発現場では具体的なセーフティ分析結果に基づいた説明が間接的になるという問題があった．この問題を解決するためには，HAZOP，FTA と D-Case を対応づけるとともに，その手順を提示する必要がある．

2.2. 課題②セキュリティケース作成法

モバイルサービスを保証対象としたセキュリティケースの効果的な作成法は考案されているが[7]，その手法を車載システム開発に適用した際の有効性について議論していない．このため，車載システムを題材とした有効性評価が必要である．

なお，本課題に関する取り組みは現在検討中であり，本稿で紹介する取り組み状況の範囲外とする．

2.3. 課題③対立問題解消法

ディペンダビリティは，セーフティ，セキュリティのように品質特性の異なる要求で構成されるため，それらの要求間で対立問題が発生する可能性を含んでいる．この問題を解消するためには，それらに対する達成度を定量的に評価できる手法が必要となる．

2.4. 課題④車載システム向け参照モデル活用法

車載システム開発において必要とされる知識は，車載ソフトウェアの大規模，複雑化に従って大幅に増加している．このため，一人のエンジニアが独力で開発全体の知識を備えることは非常に困難な状況となっている．このため，熟練者の知識を参照モデルとして資産化し，様々な分析においてそれらを活用する手法が必要となる．

2.5. 課題⑤品質特性に基づくアシュアランスケース作成法

O-DA を運用するためには，セーフティ要求，セキュリティ要求と同様に，ディペンダビリティを構成する様々な品質特性の要求に対して，アシュアランスケースを作成できる必要がある．

3. 関連研究

本章では，2 節で述べた課題の関連研究を紹介する．

3.1. セーフティケース作成法

HAZOP，FTA は，様々な分析に適用可能な手法として有効性が確認されているが，分析結果が対策されたことの証拠との対応づけは定義していない．HAZOP，FTA との組み合わせに関する研究としては，文献[8], [9]がある．これらの文献ではセーフティ分析における HAZOP，FTA の位置付けと他手法との組み合わせについて述べているが，D-Case との関係については述べていない．一方，D-Case との組み合わせについては，文献[10]で HAZOP との関係を述べている．しかしながら，FTA との関係については考慮していないので，システムのアーキテクチャに対する内部リスクを考慮できていない点と対策の網羅性についての確認が十分でない点に課題がある．文献[11], [12]で FTA を証拠に用いた D-Case の構造が示されているが，具体的な FTA の分析結果との組み合わせについては述べられていない．さらに，文献

[13]では規格化されている知識モデル群との組み合わせ，文献[14]では SysML をはじめとする設計手法との組み合わせが述べられているが，HAZOP，FTA との関係については述べていない．

セーフティ分析結果に基づいて D-Case を作成する手法に関する研究としては，説明構造[15]-[17]や説明の分解[18]に焦点を当てたパターンについて研究されているが，D-Case の作成方法については述べられていない．文献[19], [20]では D-Case の作成手順に関して述べているが，HAZOP，FTA との関係は述べていない．また，文献[21]においてモデル情報に基づいた D-Case の統一的な作成方法が提案されているが，HAZOP，FTA の分析結果を事例とした適用評価は行われていない．

3.2. 対立問題解消法に関連する研究

ゴール指向要求定義手法を拡張して，定量的な属性を付与した手法はいくつか存在している．

QA-NFR(Quantitative Assessment using NFR approach) [22]は， SIG (Soft goal Interdependency Graph)を用いて定量的にソフトゴールを評価する．しかしながら，ソフトゴールの分解時に下位のソフトゴール間の定量的な関係について考慮していない．AGORA (Attributed Goal-Oriented Requirements Analysis) は，ステークホルダ間の要求の衝突を明らかにするために，ゴールに対する属性として優先度と貢献度を定義する[23]. また，評価値を計算する属性の計算式が提供されている．FBCM (Fact Based Collaboration Modelling) [24]は，KPI 値に基づいてゴール間の相関係数を統計的に分析することによって目標となるゴールツリーを見直す方法を提案している．FBCM はゴール分割に対して統計的な証拠を提供することができる．IGEPM (Incremental Goal Evolution Process Methodology) [25]は，ビジネス環境の変化に基づいてゴールグラフを継続的に改善する方法を提案している．GQM [26]はゴールの達成度を評価する指標を特定する方法である．GQM はゴール層，クエスチョン層，メトリクス層から構成されるが，ソフトゴールの分割を考慮していないため，ゴール間で依存関係のある属性を扱うことができない．

3.3. 車載システム向け参照モデル活用法に関連する研究

自動車業界では，車載システム開発活動で作成される開発成果の記述言語として EAST-ADL[27]，AUTOSAR[28]が標準化されている．これらの標準規格は，主に欧州企業で実際の開発プロジェクトに適用されている．EAST-ADL は車載システム開発活動における全ての設計要素とその関係を標準化している．一方，AUTOSAR は，全ての車載ソフトウェアが必要とする共通機能を提供するソフトウェアプラットフォーム，製品依存の要求を実現するソフトウェアコンポーネントの規格，およびそれらを利用した開発を支えるプロセスとツールチェーンに関して標準化を進めている．しかしながら，標準化された仕様書は膨大な数が存在し，記述内容も複雑である．これらの仕様書から熟練者の知識を抽出し，様々な分析時に活用することは困難である．

3.4. 品質特性に基づくアシュアランスケース作成法に関連する研究

GSN はアシュアランスケースの記述に適しており[5]，その記述に用いる標準的なパターンが提案されている[15], [29], [30]．しかしながら，それらはアシュアランスケースの記述に要求される具体的な手順を説明していない．また，メタモデルを用いてアシュアランスケースの記述品質を制御する手法[31], [32]や設計成果からアシュアランスケースへ変換する手法[33], [34]が提案されている．しかしながら，メタモデルの定義方法までは議論していない．

4. 現状の取り組み

本章では，2 章で示した課題の取り組み状況について述べる．

4.1. D-Case を用いたセーフティ分析結果の説明手法の提案

課題①に対する取り組みとして，文献[35]では車載システム開発において従来から用いられているセーフティ分析手法と，D-Case と呼ばれるアシュアランスケースの記述法との統合手法を提案している．セーフティ分析に関する従来の研究では，個々の「分析技術」の応用やその組合せ方法について考慮しているが，第三者に対する客観的な「説明技術」との組合せまでは考慮していない．

本手法では，HAZOP，FTA を用いたセーフティ分析の結果を D-Case を介して論理的に統合する手法を考案している．提案手法では，システムの安全性を主張した最上位のゴールを，HAZOP，FTA を用いたリスク分析結果に基づいて，最小単位になるまで下位のゴールに分割する．さらに，最下位のゴールにはそのゴールの合格基準として FTA を用いて抽出したリスク原因の対策を紐付け，その基準を達成できる証拠を関連付けることで D-Case を完成させる．

さらに，エンジニア 10 名を対象として，HAZOP, FTA を個別に用いた従来形式の分析結果と上述した提案手法を用いて作成した D-Case の比較実験を行った．本実験では，それぞれの分析結果に対して同

一の質問を行い，正答率に関しては本手法が 90%前後，従来形式が 50%程度であり，回答時間に関しては本手法が約 4 分，従来形式が約 9 分という結果であった．この結果から，本手法を用いて作成した D-Case が従来形式の分析結果より優れることを確認できた. なお, 実際の車載ソフトウェア開発現場では，製品品質を保証する際に確認内容の網羅性の担保が重要となる．D-Case は，ゴールの分割根拠を明確に示すことができる記法であり，開発現場のマネージャが上記視点で製品品質を判断する際の有効なビューとなる可能性が高い.

4.2. 非機能要求の定量評価手法の提案

課題③に対する取り組みとして，文献[36], [37]では，異なる特性を有した非機能要求の衝突問題を解決するために，非機能要求の満足度を定量的に評価する手法が提案されている．非機能要求を満足する最適なアーキテクチャを導き出すためには，衝突する非機能要求に対してトレードオフの判断が必要となる．しかしながら，NFR フレームワークをはじめとする従来の研究では，非機能の分解は考慮しているが，子ノード間の重み関係を考慮していない.

提案手法では, NFR フレームワークを拡張して，分解に関する重み付けをソフトゴールの属性として持たせる記法を考案し，子ノードの間のトレードオフ関係を評価できるようにしている．これにより，熟練者の有する非機能要求に関する知識の体系化と重み付けによる設計方針の満足度の定量化が可能となった．また，上記内容をテーブル形式で表現し，定量化の計算を容易にするための変換則を考案している．IoT 機器との接続が一般的となる今後の車載システム開発では，従来重視されてきたセーフティ要求に加えて，セキュリティ要求の考慮も不可欠となる．提案手法は，相反するセーフティ要求，セキュリティ要求のトレードオフ関係を定量的に評価できる有用な手法になると予想される.

4.3. 7 人の侍フレームワークを用いた標準ソフトウェア資産の評価知識

課題④に対する取り組みとして，文献[38]では，ゴール指向分析手法におけるゴールの分解根拠に利用可能な車載ソフトウェア開発活動メタモデルを提案している。さらに，このメタモデルを利用して，プロダクトラインを適切に運用する際に重要となる標準ソフトウェア資産のアーキテクチャ評価手法を提案している. アーキテクチャ評価に用いる NFR フレームワークの SIG を作成するためには，プロダクトラインで扱う対象に応じて可変要素を想定し，その内容を構造化したソフトゴールとして定義する必要がある．しかしながら，開発経験の浅いエンジニアが開発活動全体を把握することは困難であり，その状況下で可変要素を抽出して構造的にソフトゴールを定義することは難しい．提案手法では，熟練者が有する開発活動に関する知識を 7 人の侍フレームワークに基づいて整理した車載ソフトウェア開発活動メタモデルの構造に従い，ソフトゴールを段階的に分解する手法を提案している.

4.4. 品質特性に基づくアシュアランスケース作成手法の提案

課題⑤に対する取り組みとして，文献[39]では，SPRME[21]を用いた統一的なアシュアランスケース作成法を考案し, さらにその有効性を確認している. SPRME は, アシュアランスケースの保証対象を 5 つの観点（Subject : 保証対象の構造，Property : 保証対象に期待される特性, Risk : 特性の達成を阻害するリスク，Measure : リスクを解消する対策，Evidence : 対策が備わっている証拠）で整理できるメタモデルを提供している．提案手法では，このメタモデルとアシュアランスケースの構成要素の対応関係を定義することで，アシュアランスケースを統一的に生成する変換則を明らかにした．また，提案手法を用いて作成したアシュアランスケースの有効性を確認するために，ソフトウェアレビューを対象とした従来手法との比較実験を行っている．本実験の事例とした従来のレビュー手法は，レビューアの能力に依存して実施しており，網羅性の観点で抜け漏れが発生していた．一方，提案手法では，確認すべき事項と対象の組み合わせがゴールツリー形式で提示されるため，網羅性の観点で従来手法よりも高い欠陥検出能力を有していることが確認できた．さらに，レビュー記録についても，従来のレビュー記録の形式には欠陥に関する指摘は記録できるが，レビューアが問題ないと判断した範囲に関する記録を残すことができない．このため，マネージャが最終的な品質を判断する際に，レビューアの確認した範囲を踏まえて判断することが難しい状況となっていた．一方，提案手法では，確認した範囲がアシュアランスケースとして漏れなく提示されるため，マネージャがレビューアの確認範囲を踏まえて品質を判断することが可能となる.

上述の結果から、SPRME を用いて作成したアシュアランスケースは、セーフティ、セキュリティを保証する際だけでなく、その他の品質特性を保証する際においても有用であることが確認されている。

5. 結論

本稿が対象とした車載システム開発分野は，従来，運用開始後の振る舞いが変化しない前提でセーフティ要求を中心に品質保証する特性を有していた．一方，自動走行などを想定した今後の車載システム開発では，運用開始後も常に進化することに価値がある人工知能のようなシステムとの連携が一般的になるため，セーフティ要求に加えてセキュリティ要求にも対応する必要がある．

上記の背景に対して，本稿では，セーフティ要求，セキュリティ要求といった相反する可能性のある要求群で構成されたディペンダビリティ要求の保証技術に関する研究を紹介した．運用開始後の進化を前提としたディペンダビリティ保証フレームワークとしては，The Open Group が提唱する O-DA が存在しており，その運用には想定されるシステムのリスクを網羅的に確認し，その結果を関係者と正しく合意形成した記録が不可欠となる．アシュアランスケースは，関係者との議論の前提を明文化した上で，議論内容を構造化して記録する文書であり，自然言語だけでなく，GSN などのモデリング言語を用いて記述することが可能である．しかしながら，従来のアシュアランスケースに関する研究では，2 章で示した課題が存在していた．本稿では，これらの課題に対応する技術として，D-Case を用いたセーフティ分析結果の説明手法の提案（課題①），非機能要求の定量的評価手法の提案（課題③），7 人の侍フレームワークを用いた標準ソフトウェア資産の評価知識（課題④），品質特性に基づくアシュアランスケース作成手法の提案（課題⑤），を紹介した．

参考文献

[1] The Open Group, *Dependability through Assuredness (O-DA) Framework*. 2013, pp. 1–69.

[2] A. Josey, *TOGAF® Version 9.1-A Pocket Guide*. Van Haren Publishing, 2011.

[3] J. Dunjó, V. Fthenakis, J. A. Vílchez, and J. Arnaldos, “Hazard and operability (HAZOP) analysis. A literature review,” presented at the Journal of hazardous materials, 2010.

[4] R. de Queiroz Souza and A. J. Álvares, “FMEA and FTA analysis for application of the reliability-centered maintenance methodology: case study on hydraulic turbines,” presented at the ABCM Symposium Series in Mechatronics, 2008.

[5] T. Kelly and R. Weaver, “The goal structuring notation–a safety argument notation,” presented at the Proceedings of the dependable systems and networks 2004 workshop on assurance cases, 2004.

[6] M. Tokoro, *Open Systems Dependability*. CRC Press, 2015.

[7] S. Yamamoto and N. Kobayashi, “Mobile Security Assurance through ArchiMate,” *IT CoNvergence PRActice (INPRA)*, vol. 4, no. 3, pp. pp. 1–8, Sep. 2016.

[8] K. Allenby and T. Kelly, “Deriving safety requirements using scenarios,” presented at the Fifth IEEE International Symposium on Requirements Engineering, 2001, pp. 228–235.

[9] P. Fenelon and B. Hebbron, “Applying HAZOP to software engineering models,” presented at the Risk Management And Critical Protective Systems: Proceedings of SARSS, 1994.

[10] F. Ding, S. Yamamoto, and N. Abrahim, “The Method of D-Case Development Using HAZOP Analysis on UML Models,” in *Knowledge-Based Software Engineering*, vol. 466, no. 54, Cham: Springer, Cham, 2014, pp. 617–629.

[11] Y. Matsuno and K. Taguchi, “Parameterised Argument Structure for GSN Patterns,” presented at the 2011 11th International Conference on Quality Software (QSIC), 2011, pp. 96–101.

[12] Y. Matsuno, J. Nakazawa, M. Takeyama, M. Sugaya, and Y. Ishikawa, “Towards a Language for Communication among Stakeholders,” presented at the 2010 IEEE 16th Pacific Rim International Symposium on Dependable Computing (PRDC), 2013, pp. 93–100.

[13] S. Yamamoto, “A Knowledge Integration Approach of Safety-critical Software Development and Operation based on the Method Architecture,” presented at the Procedia - Procedia Computer Science, 2014, vol. 35, pp. 1718–1727.

[14] I. Habli, I. Ibarra, R. S. Rivett, and T. Kelly, “Model-Based Assurance for Justifying Automotive Functional Safety,” presented at the Proc. 2010 SAE World Congress, 2010, vol. 1.

[15] R. Hawkins and T. Kelly, “A software safety argument pattern catalogue,” presented at the The University of York, 2013.

[16] T. Kelly and J. A. McDermid, “Safety Case Construction and Reuse Using Patterns,” in *Safe Comp 97*, no. 5, London: Springer London, 1997, pp. 55–69.

[17] T. Kelly, “Arguing safety: a systematic approach to managing safety cases,” University of York, 1999.
[18] R. Bloomfield and P. Bishop, “Safety and Assurance Cases: Past, Present and Possible Future – an Adelard Perspective,” in *Making Systems Safer*, no. 4, C. Dale and T. Anderson, Eds. London: Springer London, 2010, pp. 51–67.
[19] R. Palin and I. Habli, “Assurance of automotive safety–A safety case approach,” *International Conference on Computer Safety, Reliability, and Security*, 2010.
[20] V. Patu and S. Yamamoto, “How to develop Security Case by combining real life security experiences (evidence) with D-Case,” presented at the Procedia Computer Science, 2013, vol. 22, pp. 954–959.
[21] S. Yamamoto, S. Morisaki, and N. Atsumi, “A unified approach on assurance case development method based on models ,” presented at the SIG-KSN, 2015.
[22] N. Subramanian and J. Zalewski, “Quantitative Assessment of Safety and Security of System Architectures for Cyberphysical Systems Using the NFR Approach,” vol. PP, no. 99, pp. 1–13, 2014.
[23] H. Kaiya, H. Horai, and M. Saeki, “AGORA: Attributed goal-oriented requirements analysis method,” presented at the Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on, 2002, pp. 13–22.
[24] A. Kokune, M. Mizuno, K. Kadoya, and S. Yamamoto, “FBCM: Strategy modeling method for the validation of software requirements,” vol. 80, no. 3, pp. 314–327, 2007.
[25] S. Saito and S. Yamamoto, “The Incremental Goal Evolution Process Methodology.,” vol. proc. of workshops and doctoral consortium, pp. 254–261, 2006.
[26] V. R. Basili and D. M. Weiss, “A Methodology for Collecting Valid Software Engineering Data,” vol. 10, no. 6, pp. 728–738, 1984.
[27] EAST-ADL Association, *EAST-ADL Domain Model Specification Version V2.1.12*. 2013, pp. 1–244.
[28] S. Fürst, J. Mössinger, S. Bunzel, and T. Weber, “AUTOSAR–A Worldwide Standard is on the Road,” *14th International VDI Congress Electronic Systems for Vehicles*, 2009.
[29] Y. Matsuno and S. Yamamoto, “An evaluation of argument patterns to reduce pitfalls of applying assurance case,” presented at the Assurance Cases for Software-Intensive Systems (ASSURE), 2013 1st International Workshop on, 2013, pp. 12–17.
[30] N. Kobayashi and S. Yamamoto, “The Effectiveness of D-Case Application Knowledge on a Safety Process,” *Procedia Computer Science*, vol. 60, pp. 908–917, 2015.
[31] K. Attwood and T. Kelly, “Controlled expression for assurance case development,” presented at the Proceedings of the 23rd Safety-Critical Systems Symposium on Engineering Systems for Safety, 2015.
[32] K. Attwood, P. Conmy, and T. Kelly, “The Use of Controlled Vocabularies and Structured Expressions in the Assurance of CPS,” *ADA USER*, 2014.
[33] R. Hawkins, I. Habli, and T. Kelly, “The Need for a Weaving Model in Assurance Case Automation,” *www-users.cs.york.ac.uk*, 2015.
[34] R. Hawkins, I. Habli, D. Kolovos, R. Paige, and T. Kelly, “Weaving an Assurance Case from Design: A Model-Based Approach,” presented at the 2015 IEEE 16th International Symposium on High Assurance Systems Engineering (HASE), 2014, pp. 110–117.
[35] 小林 展英, 森崎 修司, 山本 修一郎, “D-Caseを用いた安全分析結果の説明手法の提案,” *情報処理学会論文誌*, vol. 58, no. 2, pp. 521–530, Feb. 2017.
[36] S. Yamamoto, “An Approach for Evaluating Softgoals Using Weight,” presented at the The Asian Conference on Availability, Reliability, and Security, AsiaARES, 2015, vol. 9357, pp. 203–212.
[37] N. Kobayashi, S. Morisaki, N. Atsumi, and S. Yamamoto, “Quantitative Non Functional Requirements evaluation using softgoal weight,” *Journal of Internet Services and Information Security (JISIS)*, vol. 6, pp. 37–46, 2016.
[38] N. Kobayashi, H. Yamada, and H. Utsunomiya, “The Evaluation Knowledge of Standard Software Asset using The Seven Samurai Framework,” *Procedia Computer …*, vol. 96, pp. 782–790, 2016.
[39] N. Kobayashi, “Assurance case development method using SPRME for software reviews.,” *ER2016*.