一般社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
KBSE2012-42 (2012-11)

ディペンダビリティ・コンテクストの推定手法の提案

高間 翔太† 松野 裕‡ 山本 修一郎‡

†名古屋大学大学院情報科学研究科 〒464-8601 愛知県名古屋市千種区不老町
‡名古屋大学情報連携統括本部情報戦略室 〒464-8601 愛知県名古屋市千種区不老町
E-mail: †takama.shota@f.mbox.nagoya-u.ac.jp, ‡{matsu, yamamotosui}@icts.nagoya-u.ac.jp

あらまし

近年、システムのディペンダビリティを保証するための研究が進められており、様々なシステムを対象にしたアシュアランスケースの作成が進められている。しかし、それらの記述されたアシュアランスケースが妥当であるかどうかを確認することは、未だ解決すべきことが多い。

そこで、本稿では与えられたアシュアランスケースからコンテクストを推定する手法を提案する。

具体的には、現在記述を進めている、スーパーコンピュータの運用手順に対するアシュアランスケースに対してコンテクストを推定する。本稿では、その初期の結果を報告する。

キーワード ディペンダビリティ, コンテクスト, アシュアランスケース, 推定手法

A Proposal on Inference Method for Dependability Context

Shota TAKAMA† Yutaka MATSUNO‡ and Shuichiro YAMAMOTO‡

† Graduate School of Information Science, Nagoya University Furo-cho, Chikusa-ku, Nagoya, Aichi, 464-8601 Japan
‡ Strategy Office of Information and Commnications Headquarters, Nagoya University Furo-cho, Chikusa-ku, Nagoya, Aichi, 464-8601 Japan
E-mail: †takama.shota@ f.mbox.nagoya-u.ac.jp, ‡{matsu, yamamotosui}@icts.nagoya-u.ac.jp

Abstract

System assurance has become of great importance in many areas, and assurance cases have been used for assuring dependability of various systems. However, it is difficult to validate the adequacy of assurance case. In this paper, we propose a method to infer contexts of an assurance case. We show a preliminary result on applying the method to an assurance case of the operation manual for the supercomputer of Nagoya University.

Keyword Dependability, Context, Assurance Case, Inference Method

1. はじめに

近年、システムのディペンダビリティを保証するための研究が進められており、様々なシステムを対象にしたアシュアランスケースの作成が進められている。しかし、それらの記述されたアシュアランスケースが妥当であるかどうかを確認することは、未だ解決すべきことが多い。

そこで、本稿では与えられたアシュアランスケース

からコンテクストを推定する手法を提案する。

具体的には、現在記述を進めている、スーパーコンピュータの運用手順に対するアシュアランスケースに対してコンテクストを推定する。本稿では、その初期の結果を報告する。

本論文の構成は次の通りである。

2 章において、本稿で用いるアシュアランスケースに関連する研究について、その表現方法である GSN の例を用いて説明する。

3 章において、本稿で提案する手法について説明する。アシュアランスケースの記述に用いられる要素のうち、コンテクストについて詳しく説明した後、コンテクストを推定するために必要な問題の定義、および定義された推定問題に対する解決策について説明する。

4 章において、本稿で提案する手法を適用する対象について説明し、適用対象に対して提案規則を適用した例を説明する。本稿では、名古屋大学のスーパーコンピュータの運用手順などについてまとめられた、運用要件定義表を利用して記述されたアシュアランスケースに対して、コンテクストの推定を試みる。

5 章において考察を述べる。与えられたアシュアランスケースからコンテクストの推定を行うことで、記述されたアシュアランスケースの構造を明確にできた点等を説明する。

最後に、本稿において発生した疑問点や、今後の展望について述べる。

2. 関連研究

2.1. アシュアランスケース

アシュアランスケース[1][2]は、システムの品質（安全性だけでなく、信頼性やセキュリティを含む）が確保されていることを示すための方法であり、セーフティケース[3][4][5][6][7][8]を一般化した方法である。セーフティケースは、想定する環境下において、システムが安全に動作することを体系立てて保証するための方法である。セーフティケースは欧州を中心として、防衛や航空、鉄道などの分野で発達してきた。そのため、セーフティケースやディペンダビリティケースはアシュアランスケースの中に含まれる概念となっており、システムの安全性が確保されていることを示すためにはセーフティケースを、システムのディペンダビリティが確保されていることを示すためにはディペンダビリティケースを記述するという位置づけである。

アシュアランスケースの表記法としては様々な方法が提案されている。その一つに、GSN (Goal Structure Notation) [5][9]という表現法が存在する。GSN とは、要求される品質（安全性や信頼性など）を、木構造に分解することで体系立てて議論を進める方法であり、Tim Kelly らが提唱した。図 1 に、GSN の例を示す。

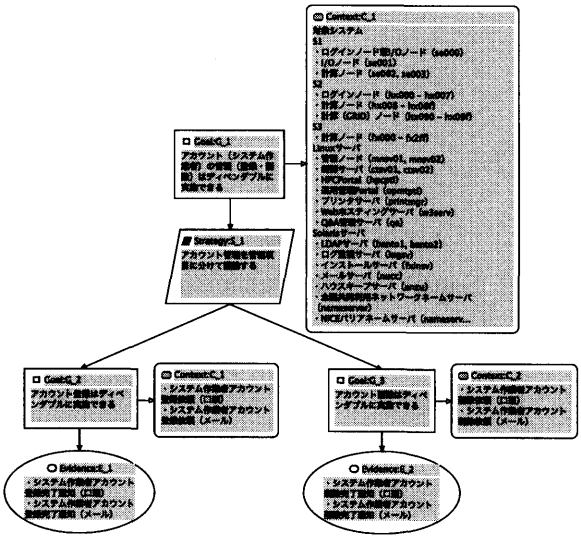


図 1：GSN（例）

GSN では、要求される品質をトップゴール（命題）に定める。また、トップゴールに対し、動作環境や制約などをコンテクスト（制約・条件）として付加する。さらに、ストラテジー（観点・考え方）によってゴールを分解し、分解されたゴールはストラテジーの下の階層でサブゴールとして記述される。ストラテジーによって、トップゴールとサブゴールとの間の依存関係を明確化することができる。そして、エビデンス（証跡）を最下層のサブゴールの直下に付加することで、最下層のサブゴールを保証することができる。これらの表現法を用いて、最下層まで分解されたサブゴールをエビデンスで保証することで、抽象的に表現される品質（トップゴール）を保証することができる。

2.2. 従来の記述方法の問題点

従来の GSN の表現方法では、適用対象の複雑化に伴って GSN の構造が複雑になり、最下層のゴールが達成されることをエビデンスで保証しても、命題で要求される品質が満たされるようになったかどうかを判断しづらくなってしまう。また、GSN の記述方法に対する明確なガイドラインが存在しないため、記述者によって結果が異なるということが発生した。先行研究[10]では、GSN に対する行列の解釈に基づいたレビュー手法が提案されている。

3. 提案手法

3.1. コンテクスト

本節では、2.1 で紹介したアシュアランスケースの表記法である GSN の要素のうち、コンテクストについ

て詳しく説明する。

コンテクストとは、システムの環境やディペンダビリティ要求、トップゴールやコンテクストに現れる語彙の定義や、その他必要な情報を記述するために付加される要素のことを示す。コンテクストの役割としては、前述のシステムの環境やディペンダビリティ要求、語彙の定義の他、ストラテジーによる場合分けの理由となる情報の説明や、最下位ノードに記述されたエビデンスの前提条件を示すことなどが挙げられる。さらに、それぞれの役割によってコンテクストを付加する位置が異なる。例としては、コンテクストの内容がシステムの環境や語彙の定義等である場合は、トップゴールの横にコンテクストを付加する。また、コンテクストの内容がストラテジーによる場合分けの理由である場合は、コンテクストはストラテジーの横に付加され、コンテクストの内容がエビデンスの前提条件である場合は、コンテクストはエビデンスに最も近いゴールの横に付加される。

3.2. コンテクストの推定問題

以下の2項目について推定問題を定義する。これらの定義をもとに、記述されたアシュアランスケースに対してコンテクストの推定を試みることとする。

問題 1. コンテクストの内容を適切に推定できるか

コンテクストの内容が適切でない場合、そのコンテクストがどのような用途で付加されているかがわからないだけでなく、記述されたアシュアランスケースの信頼性に影響を及ぼしてしまう恐れがある。そのため、コンテクストを推定する際には、コンテクストの内容が適切であるかどうかを考慮する必要がある。

問題 2. コンテクストの接続位置を適切に推定できるか

コンテクストを適切でない位置に付加すると、コンテクストが余計な情報をカバーしてしまう恐れがある。例えば、ストラテジーによる場合分け後の要素の一つに対応するコンテクストを、ストラテジーの前に付加した場合、場合分け後に関係しない要素にまで付加したコンテクストの内容が影響を及ぼしてしまう。そのため、コンテクストを推定する際には、コンテクストの接続位置が適切であるかどうかを考慮する必要がある。

3.3. 基本方針

本節では、上記の推定問題に対する解決策として、以下の2規則を用いることで、与えられたアシュアランスケースからコンテクストを推定する方法を提案する。

規則 1. コンテクストとすべき最小の情報を、記述されたアシュアランスケースの要素（ゴール、ストラテジー、エビデンス、それらの相互関係など）から抽出する。

規則 2. 抽出した情報から記述されるべきコンテクストを推定する。

4. 適用結果

4.1. 適用対象

本稿では、名古屋大学のスーパーコンピュータにおける運用要件定義表[11][12]の AsIs 版を利用した。図 2 に、本稿で利用したスーパーコンピュータにおける運用要件定義表の例を示す。

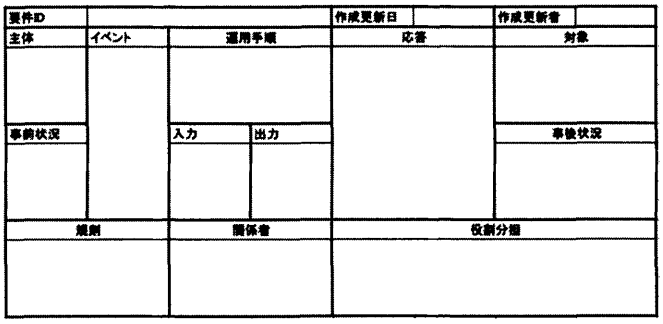


図 2：運用要件定義表（例）

本稿では全 58 項目ある運用要件のうち、9 項目の運用要件について記述したアシュアランスケースを用いて、コンテクストの推定を試みた。実際にエビデンスを推定した運用要件の例としては、運用要件定義項目番号 28 番「システムログ監視・報告」、同番号 39 番「ハード障害監視」、同番号 41 番「障害切分け」、同番号 57 番「アカウント（利用者）管理（登録・変更・削除）」などが存在する。

4.2. 適用例

上記の名古屋大学のスーパーコンピュータの運用要件定義表のうち、9 項目の運用要件におけるアシュアランスケースのコンテクストを、4 章で提案した 2 規則を用いて推定した。また、アシュアランスケースの記述や編集には D-Case Editor[13]を用いた。その結果、上述の 2 規則を用いてアシュアランスケースのコンテクストを推定できることを確認した。以下では規則の適用方法を明らかにする。

図 3 に、運用要件定義項目番号 57 番「アカウント（利用者）管理（登録・変更・削除）」について記述したアシュアランスケースのうち、「アカウント登録はデ

ィペンダブルに実行できる」というサブゴールとストラテジー、その場合分け後のサブゴール、そして、場合分けのためのストラテジーから推定したコンテクストを示す。

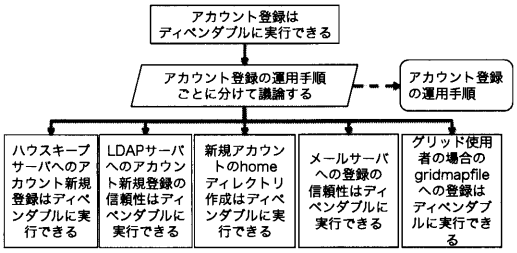


図 3：運用要件定義項目番号 57 番
について記述したアシュアランスケース
（ストラテジーから推定したコンテクスト）

「アカウント登録はディペンダブルに実行できる」というサブゴールを場合分けするためのストラテジーと場合分け後のサブゴールから、コンテクストとなりうる情報を抽出し、コンテクストの推定を行った。図 3 において、ストラテジーから場合分けを行う理由を、また、場合分け後のサブゴールからその理由の詳細情報を抽出した。続いて、抽出した情報からコンテクストを推定し、ストラテジーの横に付加することで、「アカウント登録の信頼性を保証する」というサブゴールに対して場合分けを行った理由と、その理由である運用手順の情報を説明するコンテクストを示すことができていることがわかる。

また、図 4 に、図 3 で示したアシュアランスケースのうち、「ハウスキープサーバへのアカウント新規登録はディペンダブルに実行できる」というサブゴールと、対応するエビデンス、そのエビデンスから推定したコンテクストを示す。

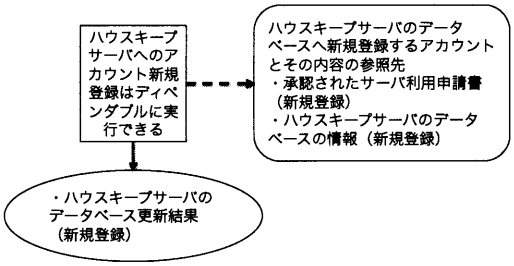


図 4：運用要件定義項目番号 57 番
について記述したアシュアランスケース
（エビデンスから推定したコンテクスト）

図 3 で場合分け後に記述された「ハウスキープサーバへのアカウント新規登録はディペンダブルに実行できる」というサブゴールに対応するエビデンスからコンテクストとなりうる情報を抽出し、コンテクストの推定を行った。図 4 において、サブゴールの出力となるエビデンスから、入力となるコンテクストの情報を抽出した。続いて、抽出した情報からコンテクストを推定し、このサブゴールの横に付加することで、「ハウスキープサーバへのアカウント新規登録はディペンダブルに実行できる」というサブゴールに対して入力となる情報を説明するコンテクストを示すことができていることがわかる。

さらに、図 5 に、図 3 で示したアシュアランスケースのうち、「ハウスキープサーバへのアカウント新規登録はディペンダブルに実行できる」というサブゴールについて、推定前に記述されていたコンテクストとエビデンスを示す。

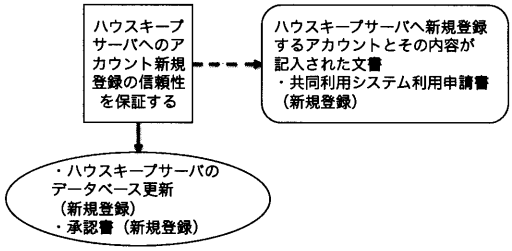


図 5：運用要件定義項目番号 57 番
についてコンテクストの推定前に記述されていた
アシュアランスケース

図 4 と図 5 とを比較すると、図 5 ではコンテクストにシステムの利用申請書が記載されており、エビデンスにハウスキープサーバのデータベース更新（結果）と申請書が混在して記述されており、コンテクストにハウスキープサーバのデータベースの入力情報が記述されていない。アカウントの新規登録を行う際には、承認済みの状態である利用申請書を入力とする必要がある。また、エビデンスとしてハウスキープサーバのデータベースの更新結果を出力するために、コンテクストにハウスキープサーバのデータベースの入力情報が必要である。そのため、アカウントの新規登録を行う際の入出力としてエビデンスとコンテクストが望ましくない状態であることがわかる。一方、図 4 では、エビデンスに記述されたハウスキープサーバのデータベースの更新結果という出力から情報を抽出し、承認されたサーバの利用申請書とハウスキープサーバのデータベース情報という 2 つの入力情報を、サブゴールが満たされるための入力コンテクストとして推定した結果が示されている。この結果より、アカウント新規登録に必要な入力と出力を、それぞれコンテクストとエビデンスに適切な状態で記述することができたことがわかる。

5. 考察

記述されたアシュアランスケースの要素からコンテクストとなりうる情報を抽出し、その情報からコンテクストを推定することにより、アシュアランスケースの構造を明確化できた。例としては、ストラテジーに対するコンテクストを推定することにより、ストラテジーによる場合分けの理由を詳細化でき、場合分けの理由をより明確化できた。また、記述されたアシュアランスケースの曖昧な点や不十分な点を発見することができ、アシュアランスケースに対する改善点の提案が可能であると考えられる。

さらに、提案した手法を用いることで、運用要件定義表に記載されていない内容でも、アシュアランスケースを作成する際に必要と考えられるコンテクストに用いるための情報を抽出できると考えられる。例としては、次のサブゴールの前提条件となるコンテクストを、前のサブゴールのエビデンスから推定する際に、エビデンスとして記述される情報が運用要件定義表に記載されていない内容でも、次のサブゴールのコンテクストとして記述できる点が挙げられる。

また、コンテクストの推定を行う際に、既にコンテクストが記述されている場合があった。例としては、5章の適用例に示すように、図5が挙げられる。その場合にも本稿で紹介したコンテクストの推定手法を用いてコンテクストを推定し、既に記述されたコンテクストと比較することで、既に記述されているコンテクストの内容のレビューを行うことができると考えられる。例えば、5章の適用例における、図4と図5の比較により、既に記述されているコンテクストの内容を、推定したコンテクストを用いてレビューできている点が挙げられる。

最後に、スーパーコンピュータの運用手順に対するアシュアランスケースの作成手法に対して、本稿で提案したコンテクストの推定手法を追加することにより、アシュアランスケースの作成段階でコンテクストの抜け漏れを防ぐことができるのではないかと考えられる。

6. おわりに

本稿では、実際に運用されているシステムの運用要件に対するアシュアランスケースに対してコンテクストを推定することで、以下の課題を抽出した。

(1) 与えられたアシュアランスケースに対して、すべてのコンテクストを推定することは困難である。

例えば、運用要件定義項目番号 57 番「アカウント（利用者）管理（登録・変更・削除)」において、「アカウント（利用者）管理（登録・変更・削除）はディペンダブルに実行できる」というトップゴールに記述される環境条件などのコンテクストは、運用要件定義表に記載されているものを参考に記述しているため、与えられたアシュアランスケースのみでは、これらのコンテクストの推定に十分な情報を得ることはできないと考えられる。

(2) 今回の適用事例では、2規則を用いることで与えられたアシュアランスケースに記述されるべきコンテクストを推定できた。しかし、提案した手法の規則の十分性や、提案した手法によって推定したコンテクストの結果の妥当性については、今後も他の運用手順について記述されたアシュアランスケースに適用することで評価していく必要がある。

また、本稿で提案したアシュアランスケースに対するコンテクストの推定規則を、スーパーコンピュータの運用手順についてのアシュアランスケースだけでなく、他のシステムについて記述されたアシュアランスケースにも適用することで、本稿の手法を、アシュアランスケースのコンテクストをレビューする一般的な手法に発展させることができるのではないかと考える。

最後に、エビデンスに書かれた内容を参照することで、エビデンスから推定可能なコンテクストに必要な情報をパターン化できるのではないかと考える。

7. 謝辞

本研究は、JST-CREST「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」研究領域（DEOS プロジェクト）の支援を受けた。

参　考　文　献

[1] Peter Bishop, Robin Bloomfield, Sofia Guerra, The future of goal-based assurance cases, DSN, 2004

[2] R. Bloomfield and P. Bishop, Safety and assurance cases: Past, present and possible future – an Adelard perspective, in Proc. 18th Safety-Critical Sys. Symp., Feb. 2010

[3] Tim Kelly, John A McDermid, Safety Case Construction and Reuse using Patterns, 16th SAFECOMP, 1997

[4] Peter Bishop, Robin Bloomfield, A Methodology for Safety Case Development, the Sixth Safety critical Systems Symposium, 1998

[5] Tim Kelly and Rob Weaver, The Goal Structuring Notation – A Safety Argument Notation, Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, July 2004

[6] Tim Kelly, Arguing Safety – A Systematic Approach to Managing Safety Case, Ph.D. Thesis, University of York, 1998

[7] GSN Community Standard Version1, Origin Consulting(York) Limited, on behalf of the Contributors, November 2011

[8] Jane Fenn, Richard Hawkins, Tim Kelly, P Williams, Safety Case Compositon Using Contracts – Refinements based on Feedback from an Industrial

Case Study, SSS, 2007

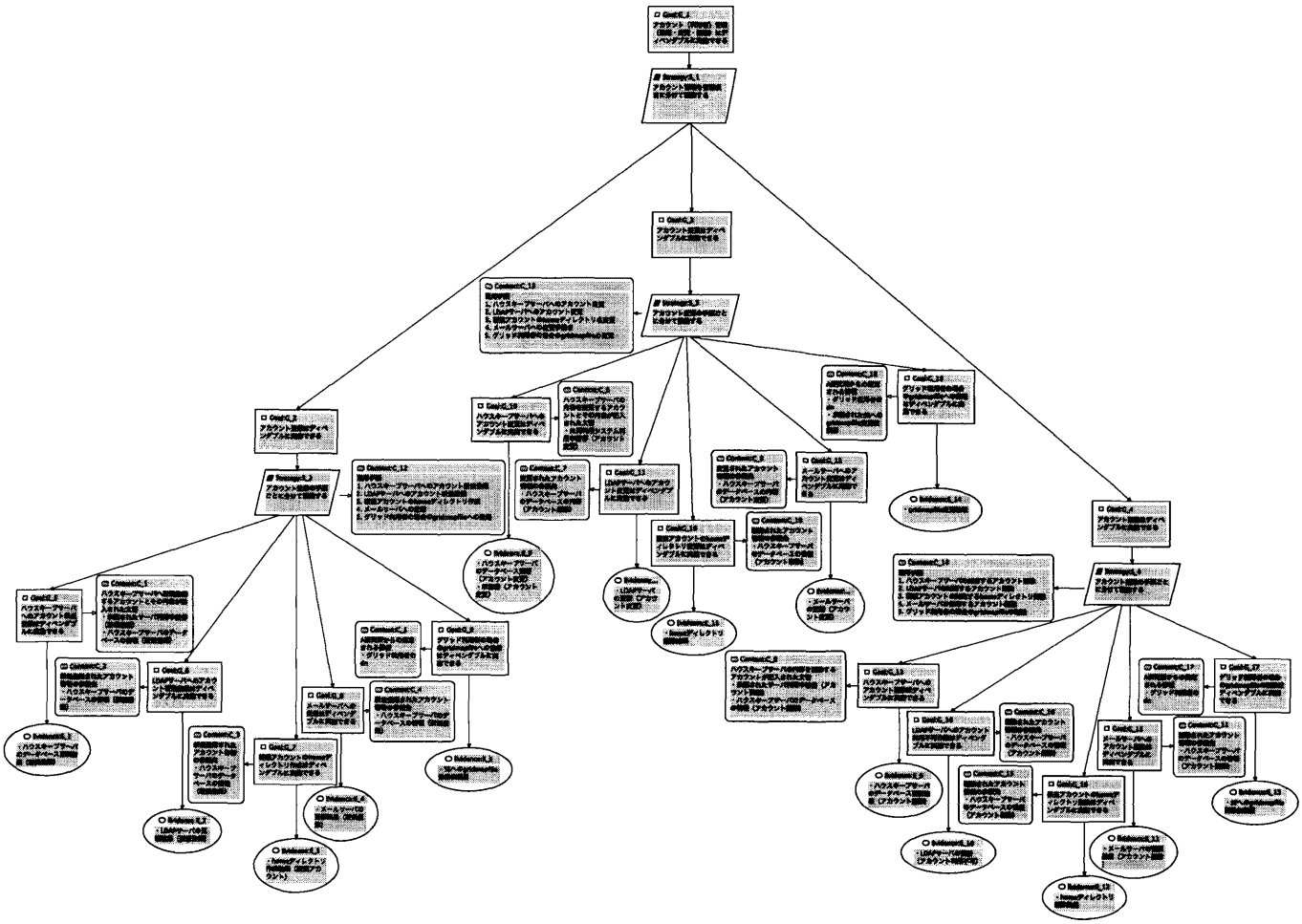
[9] 山本修一郎, “要求工学基礎知識”, 32 章, pp.235-240, Feb.2012

[10] Shuichiro Yamamoto, Yutaka Matsuno, A review method based on a matrix interpretation of GSN, 10th Joint Conference on Knowledge-Based Software Engineering 2012, 2012

[11] 山本修一郎, “要求工学基礎知識”, 19 章, pp.107-114, Feb.2012

[12] Shuichiro Yamamoto, A Service Operation Management Method based on a Human Behavior Model: A Case Study of Japanese University, 2012

[13] Yutaka Matsuno, Hiroki Takamura, Yutaka Ishikawa, A Dependability Case Editor with Pattern Library, IEEE 12th HASE2010, 2010



付録：運用要件定義項目番号 57 番「アカウント（利用者）管理（登録・変更・削除）」について記述し、コンテクストを推定したアシュアランスケース（全体図）