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
SS2012-16 KBSE2012-18 (2012-7)

スーパーコンピュータ運用手順に対する ディペンダビリティの確認手法の提案

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、複雑化した情報システムをディペンダブルに運用し、確認することが困難になってきている。
そこで、本稿ではアシュアランスケースを用いた情報システムの運用手順に対するディペンダビリティの確認手法を提案する。
具体的には、名古屋大学のスーパーコンピュータの運用手順に対してアシュアランスケースを用いることによって、運用手順の妥当性、抜け漏れなどがないか確認した初期の結果を報告する。

キーワード スーパーコンピュータ, ディペンダビリティ, アシュアランスケース, 運用手順

A Proposal on a Method for Reviewing Operation Manuals of Supercomputer

Shota TAKAMA† Yutaka MATSUNO‡ and Shuichiro YAMAMOTO‡

† Graduate School of Information Sciences, Nagoya University Huro-cho, Chikusa-ku, Nagoya, Aichi, 464-8601 Japan
‡ Strategy Office of Information and Commnications Headquarters, Nagoya University Huro-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
The more information systems become complex, the more difficult it is to operate dependably. In this paper, we propose a method for reviewing operation manuals of information systems based on assurance case to verify the dependability of information systems. We also show an early result on applying the method to the operation manual for the supercomputer of Nagoya University.

Keyword Supercomputer, Dependability, Assurance Case, Operation Manual

1. はじめに

近年、複雑化した情報システムをディペンダブルに運用し、確認することが困難になってきている。
そこで、本稿ではアシュアランスケースを用いた情報システムの運用手順に対するディペンダビリティの確認手法を提案する。
具体的には、名古屋大学のスーパーコンピュータの運用手順に対してアシュアランスケースを用いることによって、運用手順の妥当性、抜け漏れなどがないか確認した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、本稿に用いる技術の関連研究につい

て説明する。本稿で用いるアシュアランスケースについての関連研究について、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を適用する対象について説明する。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記述された運用要件定義表を利用して、実際に利用されているシステムにおける運用手順のディペンダビリティの確認を試みた。

4 章において、本稿で提案する手法について、基本方針と発生した課題、また、その改善策について説明する。アシュアランスケースを記述する際に用いる規則の基本方針やその規則の適用上で生じた課題、そしてその課題に対する改善策について説明する。

5 章において、3 章で説明した適用対象に対して、4 章で説明した規則を適用した例を説明し、適用方法を明らかにする。本章を通して、4 章で説明した規則を用いてアシュアランスケースを記述できることを確認した。

6 章において、5 章で示した結果についての考察を述べる。アシュアランスケースを用いて実際に利用されているシステムにおける運用手順のディペンダビリティを確認することで、運用手順が記載されたドキュメントの構造を明確にすることを確認できた。

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]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][8]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[9]を示す。

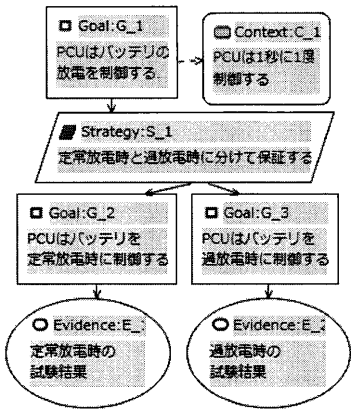


図 1：GSN（例）

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）として付加される。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、抽象的に表現される品質（トップゴール）を、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。

3. 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[10]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。

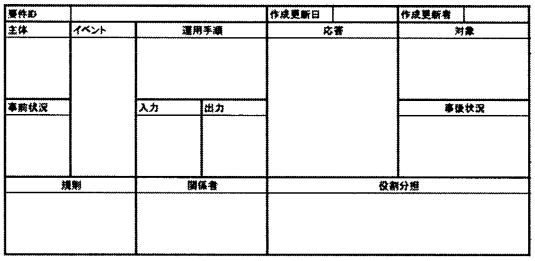


図 2：運用要件定義表（例）

本稿では全 58 項目ある運用要件のうち、4 項目の運用要件について、アシュアランスケースを用いて記述を試みた。実際にアシュアランスケースを記述した運用要件は、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 29 番「システムログ監視結果判断」、同番号 57 番「アカウント（利用者）管理（登録・変更・削除）」、同番号 58 番「アカウント（システム作業者）の管理（登録・削除）」の 4 項目である。

4. 提案手法

4.1. 基本方針

本稿におけるアシュアランスケースの記述方法の基本方針として、以下のような規則によってアシュアランスケースによる運用要件の記述を試みた。

規則 1. トップゴールに運用要件定義表の定義項目を使用する。

規則 2. 入出力や運用手順、目的などをコンテクストとして、トップゴールの横に記述する。

規則 3. 運用要件が細分化できる場合は、トップゴールの直下で場合分けを行って細分化する。

規則 4. コンテクストの項目ごとに場合分けを行う。

4.2. 適用上の課題

4.1 で提案した手法を用いて、運用要件定義項目番号 28 番「システムログ監視・報告」についてアシュアランスケースの作成を試みた。このアシュアランスケースを作成する上で、トップゴールを「システムログ監視・報告の信頼性を保証する」と設定し、入出力や運用手順、目的をコンテクストとして、トップゴールの横に記述した。

また、トップゴールをシステムログの監視とシステムログ監視結果の報告という 2 つの運用要件に細分化できるととらえ、運用要件の場合分けを行った。

さらに、システムログの監視の信頼性を保証するというサブゴールを検証するために、トップゴールの横に記述した入出力や運用手順、目的をコンテクストに記述し、コンテクストの項目ごとに場合分けを行おうと試みた。

しかし、この方法で場合分けを行う際に、いくつかの課題が発生した。一つ目は、コンテクストの項目の数だけ同一階層におけるストラテジーの数が増加してしまった。その結果、場合分け後のノードが横に大きく拡大するという結果になり、それぞれのノードと場合分け理由との対応の理解が困難となった。

二つ目は、コンテクストの項目ごとに場合分けを行った後の下位ノードの詳細を見ていくと、検証項目が重複してしまう可能性があり、トップゴールに対して正しい場合分けを実行できない可能性が懸念された。

4.3. 解決策

本稿においては、上記の課題に対する解決策として以下の 7 規則を用いて、アシュアランスケースを記述する方法を提案する。なお、この規則は 4.1 で述べた 4 規則を再整理したものである。

規則 1. トップゴールに運用要件定義表の定義項目を使用する。

規則 2. 運用要件が細分化できる場合は、トップゴールの直下で場合分けを行って細分化する。

規則 3.運用手順が時系列になっている場合は、運用手順ごとに場合分けを行う。そうでない場合は、運用手順に対する目的ごとに場合分けを行う。

規則 4. 入力はコンテクストに、出力はエビデンスに記述する。

規則 5. 入出力 X に含まれる各項目 a については、入出力先の詳細な項目として X（a）のように括弧書きで記述する。

規則 6. コンテクストはエビデンスに最も近いゴールの横で記述する。

規則 7. 記述されたエビデンスが別のサブゴールの前提条件となる場合は、エビデンスの内容を対応するゴールのコンテクストとして記述する。

5. 適用例

3 章で紹介した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、4 項目の運用要件におけるアシュアランスケースを、上述した 7 規則を用いて記述した。アシュアランスケースの記述には D-Case Editor[11]を用いた。この結果、7 個の規則だけでアシュアランスケースを記述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、トップゴールとその場合分け後のサブゴールを示す。

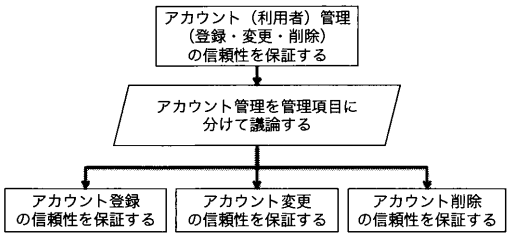


図 3：運用要件定義項目番号 57 番
について記述したアシュアランスケース
（トップゴールとその場合分け後のサブゴール）

トップゴールにおいて運用要件定義表の定義項目を使用し、運用要件を細分化するために場合分けを行った。図 3 において、トップゴールに対する場合分けを行い、それぞれ「アカウント登録」、「アカウント変更」、「アカウント削除」の信頼性を保証するという 3 項目のサブゴールに分割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、「アカウント登録の信頼性を保証する」というサブゴールとその場合分け後のサブゴールを示す。

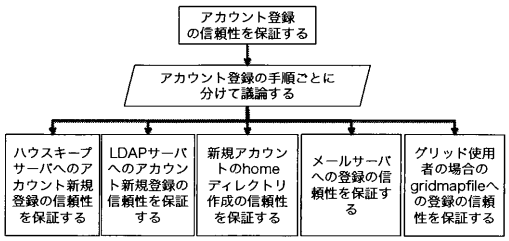


図 4：運用要件定義項目番号 57 番
について記述したアシュアランスケース
（アカウント登録の信頼性の保証についての詳細）

図 3 で作成したサブゴールに対して、アカウント登録の運用手順を用いて場合分けを行った。図 4 において、「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運用手順ごとに場合分けを行い、それぞれの運用手順項目の信頼性を保証するという 5 項目のサブゴールに分割できていることがわかる。

さらに、図 5 に、図 4 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の信頼性を保証する」というサブゴールと、対応するコンテクスト、エビデンスを示す。

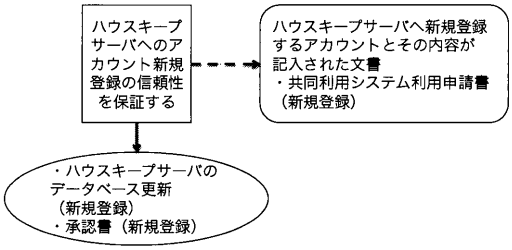


図 5：運用要件定義項目番号 57 番
について記述したアシュアランスケース
（最下層のゴールとコンテクスト・エビデンス）

図 4 で作成した「ハウスキープサーバへのアカウント新規登録の信頼性を保証する」というサブゴールサブゴールに対して、右側に対応する入力をコンテクストに、出力をエビデンスに記述した。また、各入出力 X の項目 a は、コンテクストやエビデンスの詳細な項目として X(a) のように括弧書きで記述した。さらに、コンテクストはエビデンスに最も近いゴールの横で記述した。図 5 において、「ハウスキープサーバへのアカウント新規登録の信頼性を保証する」というサブゴールに対応する入力がコンテクストに、出力がエビデンスに記述され、各入出力項目はそれぞれの入出力に対して括弧書きで記述されていることがわかる。また、コンテクストが対応するエビデンスに最も近いゴールの横で記述されていることがわかる。

続いて、図 6 に、図 4 で示したアシュアランスケースのうち、「LDAP サーバへのアカウント新規登録の信頼性を保証する」というサブゴールと、対応するコンテクスト、エビデンスを示す。

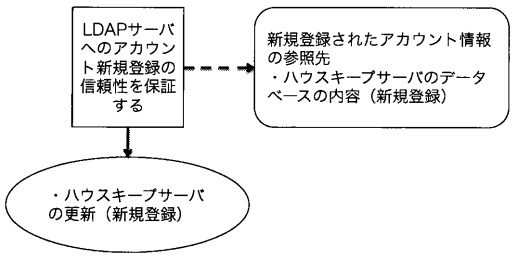


図 6：運用要件定義項目番号 57 番
について記述したアシュアランスケース
（別の最下層のゴールとコンテクスト・エビデンス）

一方のサブゴールで記述されたエビデンスが、もう一方のサブゴールの前提条件となっている場合に、一方のサブゴールのエビデンスの内容をもう一方のサブゴールのコンテクストとして記述した。図 6 において、図 5 で示した「ハウスキープサーバへのアカウント新規登録の信頼性を保証する」というサブゴールに対応するエビデンスが、次のサブゴール「LDAP サーバへ

のアカウント新規登録の信頼性を保証する」のサブゴールの前提条件になっているため、図5で示したエビデンスの内容が図6のサブゴールにおけるコンテクストとして記述されていることがわかる。

最後に、図7に、運用要件定義項目番号28番「システムログ監視・報告」について記述したアシュアランスケースのうち、トップゴールを細分化した後、「システムログ監視の信頼性を保証する」というサブゴールとその場合分け後のサブゴールを示す。トップゴールの細分化は、図3で細分化を適用した場合と同様に行い、「システムログ監視の信頼性を保証する」というサブゴールと、「システムログ報告の信頼性を保証する」というサブゴールに細分化した。

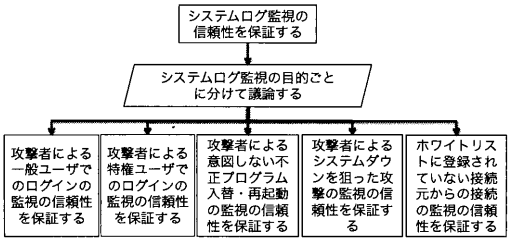


図7：運用要件定義項目番号28番
について記述したアシュアランスケース
（システムログ監視の信頼性の保証についての詳細）

トップゴールにおいて運用要件定義表の定義項目を使用し、運用要件を細分化するために場合分けを行った後、システムログ監視の運用手順を用いて場合分けを試みた。しかし、システムログ監視の運用手順は時系列になっていないため、運用手順に対する目的ごとに場合分けを行った。図7において、「システムログ監視の信頼性を保証する」というサブゴールに対して運用手順の目的ごとに場合分けを行い、それぞれの運用手順項目の信頼性を保証するという5項目のサブゴールに分割できていることがわかる。

6. 考察

運用要件定義表に対してアシュアランスケースを記述することにより、ドキュメントの構造を明確にすることができた。これにより、ドキュメントの曖昧な点や不十分な点を発見することができ、ドキュメントに対して妥当性の確認とともに、改善点の提案が可能になると考えられる。

例えば、運用要件定義項目番号28番「システムログ監視・報告」において、監視したシステムログの報告タイミングの曖昧さを検出することができる。すなわち、ドキュメントに対して不十分な点や曖昧な点があることを、アシュアランスケースを記述することによって検出することができる。

また、同番号29番「システムログ監視結果判断」において、同番号28番と要件定義項目を統合できるのではないかと考えられる。これは、同番号29番についてアシュアランスケースを記述する中で、「システムログ監視結果判断」で用いるシステムログ結果は、同番号28番で得られるエビデンスを用いてコンテクストとして記述する必要があったことに由来する。

さらに、同番号58番「アカウント（システム作業者）の管理（登録・削除）」の運用要件定義表において、曖昧な点や不十分な点があるのではないかと考えられる。同番号58番についてのアシュアランスケースを作成する中で、運用要件定義表内の入出力において、メールや口頭でアカウント管理の依頼が行われていることがわかり、依頼における明確な文書がない点がわかった。

最後に、4章で提案した記述手法について、発生した課題に対する改善策の7規則を適用することで、場合分けによる下位ノードの項目の重複を避けることができる。また、コンテクストを対応するエビデンスに最も近いサブゴールの横に記述することで、それまでの場合分けの理由が明確になり、対応関係が取りやすくなったと考えられる。

7. 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を作成することで、以下の課題を抽出した。

(1) 一方のノードで記述したエビデンスと、コンテクストとのリンク方法を明確化する必要がある。

例えば、運用要件定義項目番号28番「システムログ監視・報告」において、「システムログ監視の信頼性を保証する」というノードで記述したエビデンスを、「システムログ報告の信頼性を保証する」というノードで前提条件として用いるため、コンテクストとして記述する必要がある。このとき、上述の同番号57番について記述したアシュアランスケースと比較すると、一方で記述されたエビデンスと、そのエビデンスが前提条件となるコンテクストとの位置が近い場合（上述の同番号57番）と、位置が遠い場合（同番号28番）があることがわかる。そのため、エビデンスとコンテクストとの対応関係を明確にするために、両者のリンク方法の明確化が必要であると考えられる。

(2) 今回の適用事例では7規則でアシュアランスケースを記述できた。しかし、規則の十分性については今後も他の運用項目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の記述

規則を用いて、アシュアランスケースの記述を半自動化できるようにすることで、アシュアランスケースの記述を効率化できると考えられる。しかし、アシュアランスケース記述の半自動化に際しては、ゴールやコンテクストなどの定義や、ストラテジーによる場合分けなどにおいて、適切な日本語を生成できるかどうか検証する必要がある。

8. 謝辞

本稿の作成にあたり、研究資料を提供してくださった、慶應義塾大学大学院の田中康平氏に感謝の意を表する。

また本研究は、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] T. Scott Ankrum, Alfred H. Kromholtz, Structured Assurance Cases: Three Common Standards, IEEE International Symposium on High – Assurance Systems Engineering, 2005

[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, DSN Workshop on Assurance Cases, 2004

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

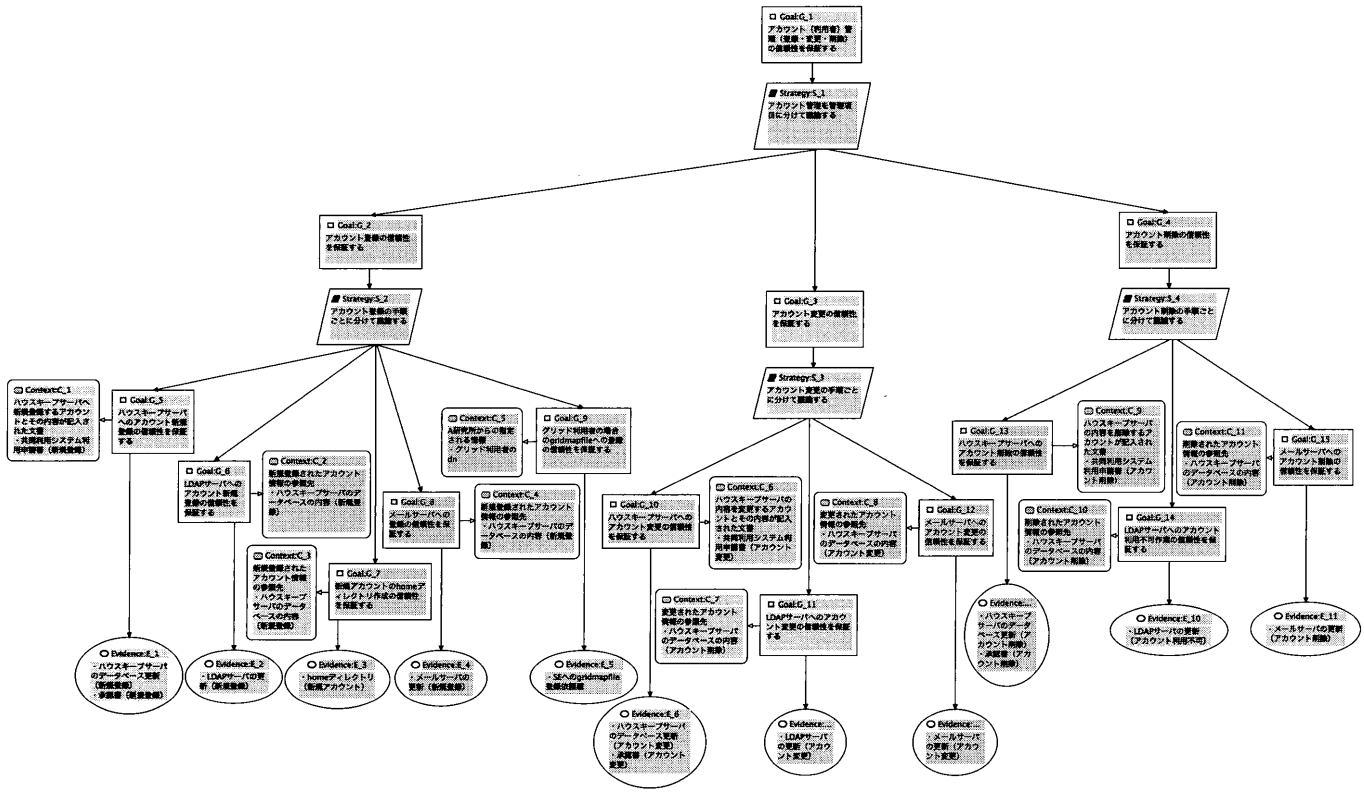
[7] Jane Fenn, Richard Hawkins, Tim Kelly, P Williams, Safety Case Compositon Using Contracts – Refinements based on Feedback from an Industrial Case Study, SSS, 2007

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

[9] 田中康平, 松野裕, 中坊嘉宏, 白坂成功, 中須賀真一, “アシュアランスケースを用いた小型人工衛星の品質保証”,日本信頼性学会 第 20 回春期信頼性シンポジウム, 2012

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

[11] 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）」について記述したアシュアランスケース（全体図）