Institute of Electronics, Information, and Communication Engineers

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
KBSE2012-40 (2012-11)

アシュアランスケース構築法の提案

松野　裕† 　高井　利憲†† 　ヴァイセパトゥー† 　山本修一郎†

† 名古屋大学
†† 奈良先端科学技術大学院大学

あらまし　アシュアランスケースがシステムのディペンダビリティを保証する手法として注目を集めている。しかし一般の技術者にわかりやすいアシュアランスケースの構築法は特に日本ではあまり知られていない。本稿では、一般の技術者および大学生などを対象としたアシュアランスケースの構築法を提案する。またその有効性を学生への模擬実習において評価を行う。

キーワード　アシュアランスケース、講義、演習、メトリクス

A Writing Method for Assurance Cases

Yutaka MATSUNO†, Toshinori TAKAI††, Vaise PATU†, and Shuichiro YAMAMOTO†

† Nagoya University
†† National Advanced Institute of Science and Technology

Abstract　Assurance Cases have been recognized as a promising method for dependability assurance. However, there has not been a writing method which is easy to understand for ordinary engineers, specially in Japan. In this paper, we propose a writing method targeting ordinary engineers and university students. The method is accompanied with lectures and exercises. We did preliminary experimental lectures and exercises for 17 engineers. We show the preliminary results.

Key words　Assurance Cases, Lectures, Exercises, Metrics

1. はじめに

システムの安全性やディペンダビリティの保証の必要性が高まっている。アシュアランスケース (assurance case, 保証ケース) [2] はそのための有力な手法として欧米を中心として関心が高まっている。しかしながら特に日本ではまだ新しい手法であるため、実際にどうやって書けばよいのか、どのように有用であるか、実例はどのようなものであるのか、わからない場合が多い。

1.1 D-Case 実証評価研究会

D-Case [7] は、欧米で近年高い安全性が要求されるシステムの開発運用において、提出が義務付けられるまでに普及している安全性ケース (Safety Case) [4] をもとに研究を開始した。安全性ケースとは、テスト結果や検証結果をエビデンスとしてそれらを根拠にシステムの安全性を議論し、システム認証者や利用者などに保証する、あるいは確信させる (assure) ためのドキュメントである。近年、安全性だけでなくセキュリティやディペンダビリティなども対象として使われ始めている。その場合、セキュリティケースや、ディペンダビリティケースと呼ばれる。これらを総称してアシュアランスケースと呼ばれる。D-Case では、従来のアシュアランスケースに加えて、対象システムのモニタリング機能との連携などの拡張を行なっている [8]。現在の安全性ケースでは、システム供給者、第 3 者コンサルティグ会社、システム利用者（国防省など）の間のコミュニーケーションなどに使われるが、主には認証のために提出されるドキュメントとして使われてきた。しかしながらいまだ専門家によって記述がおこなわれるのみであり、特に日本では広く使われるにはいたっていない。そこで我々は以下にフォーカスをおいて研究している。

（1） 一般の企業の方にとってわかりやすい入門書や講習の開発

安全性ケースはこれまで高い安全性が求められるシステムに対して、高度な専門知識を持つコンサルタントなどによって書かれてきたため、安全性ケースのガイドブックなどは、安全性分析など高い専門知識を前提とされたものがあるだけだった。わかりやすい入門書や講習が必要であると考えた。

（2） 一般の企業の方にとって使いやすい、ニーズに即したツールの開発

安全性ケースが普及し始めてまだ日が浅いこともあってか、

This article is a technical report without peer review, and its polished and/or extended version may be published elsewhere.
Copyright ©2012 by IEICE
NII-Electronic Library Service

ツールはイギリス Adelard 社の ASCE ツール(注1)などいくつかあるだけである。また ASCE ツールなどは、主に認証ドキュメントを作成するためのツールであり、他の開発ツールとの連携が容易ではなく企業のニーズに即したツールが必要であると考えた。

（3） 記述、応用例の充実

安全性ケースの問題の一つは、企業の重要な情報を含むことから、なかなか実際の例が表に出てこない点がある。しかしそれでは一般の、特に日本企業の方に具体的なイメージを持っていただくことは困難である。わかりやすく、具体的な記述例や応用例が必要であると考えた。

我々はこれまでの基礎研究・開発に加えて、上記 3 点に着眼し、広く企業の方に使っていただけるための活動を本格化している。その一環として、2012 年 9 月 14 日に、名古屋で第 1 回 D-Case 実証評価研究会を開催した。30 名以上の企業の方にご参加いただき、活発な議論ができた (図 1 がその様子である)。ご興味のある方は、ぜひご参加いただきたい。D-Case 実証評価研究会のホームページ(注2)をご覧いただきたい。

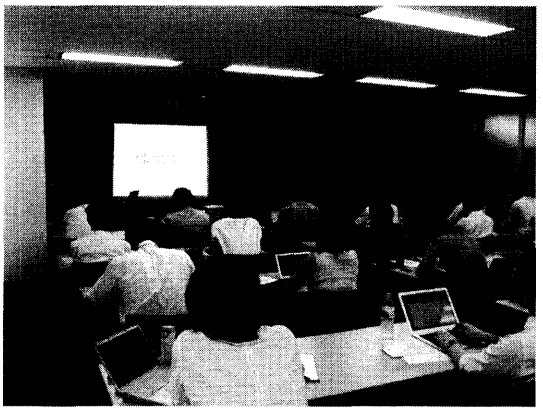

図 1 D-Case 実証評価研究会の様子

本論文の構成は以下の通りである。2 節において開発中のアシュアランスケース構築法を紹介する。構築法は D-Case 入門 [10] としてまとめている。3 節において、構築法をもとにした、一般企業のエンジニアの方を対象とした模擬講義および演習の内容を紹介する。4 節において、模擬講義と演習の結果をもとにしたアシュアランスケースの評価法に関する考察を示す。5 節においてまとめる。

2. D-Case 入門

一般の企業の方向けのアシュアランスケースの入門書を開発中である。その初版を出版した [10]。その中で我々が開発中のアシュアランスケースの構築法を紹介している [9]。本節では [10] の内容を簡単に紹介する。

これまでのアシュアランスケースの構築法 [1], [3] などをもとに、より具体的で分かりやすい構築法を開発中である [9]。以下に概要を示す。詳細は D-Case 入門 [10] を参照されたい。

(注1)：http://www.adelard.com/asce/choosing-asce/index.html
(注2)：http://www.dependable-os.net/osddeos/event/dcase.html

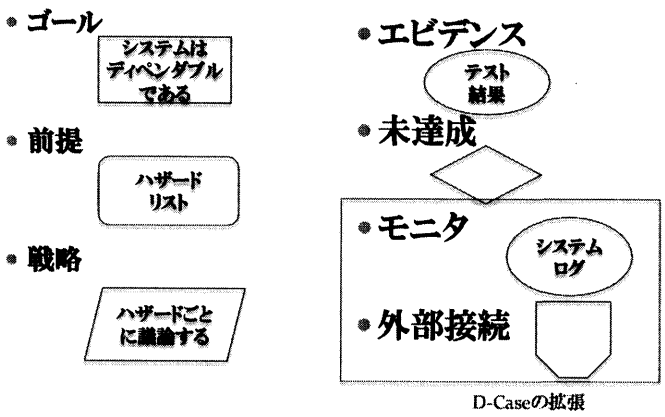

図 2 D-Case の主なノード

2.1 D-Case/GSN の規則

D-Case はアシュアランスケースの代表的な表記法である GSN(Goal Structuring Notation) [6] を拡張した表記法によって記述する。D-Case は主に以下のノードにより構成される (図 2)。このうち、モニタと外部接続は D-Case の GSN からの拡張である。

（1） ゴール (Goal)

対象システムに対して、議論すべき命題である。例えば「システムはディペンダブルである」とか「システムは適切な安全性をみたす」などである。

（2） 戦略 (Strategy)

ゴールが満たされることを、サブゴールに分割して詳細化するときの議論の仕方である。例えば、「システムは安全である」というゴールに対して、現時点で識別されているハザードに対処できていることによって議論したいとき、戦略ノードとして「識別されたハザードごとに場合分け」を用いると、例えばひとつのサブゴールは「システムはハザード X に対処できる」となる。

（3） 前提 (Context)

ゴールや戦略を議論するとき、その前提となる情報である。例えば、運用環境や、システムのスコープ、あるいは「識別されたハザードのリスト」などである。

（4） エビデンス (Evidence)

詳細化されたゴールを最終的に保証するものである。例えばテストや形式手法による検証結果などである。

（5） 未達成 (Undeveloped)

ゴールを保証するための十分な議論もしくはエビデンスがないことを表す。

（6） モニタ (Monitor)

運用中のシステムより取得可能なエビデンスである。たとえばインターネットのアクセスログなどです。D-Case ツールはシステムと連携し、モニタリングを用いながらディペンダビリティの保証を支援する。

（7） 外部接続 (External)

他のシステムの D-Case へのリンクである。システムは単一でディペンダビリティを保つことはなく、助けあいながら保つ。

NII-Electronic Library Service

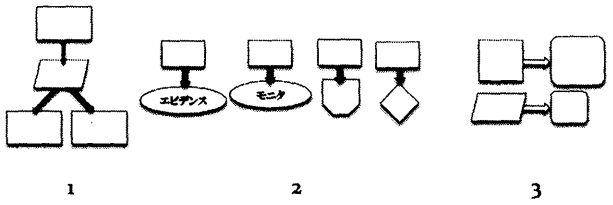

図 3　ノードのつなげ方

ノードのつなげ方、矢印は以下のとおりである (図 3)。

（1） ゴールは戦略を通して分解される。

（2） D-Case の葉は、エビデンス、モニタ、外部接続、未達成のいずれかである。

（3） 前提は、ゴール、もしくは戦略につなげられる。

（4） 矢印は 2 種類ある。

- ゴールから戦略、戦略からゴール、ゴールからエビデンス、モニタ、外部接続、未達成
- ゴールから前提、戦略から前提 (白抜きの矢印)

2.2 D-Case 構築法

（1） システムライフサイクルを整理し、それぞれのフェーズの入力、出力ドキュメントをまとめる

（2） 入力、出力ドキュメントを分類する

（3） トップゴールを置く: 「システムはディペンダブルである」

（4） ディペンダビリティ要求、環境情報、語彙定義を前提としてトップゴールにおく

（5） 大まかに D-Case の構造を考える

（6） 必要なドキュメントを前提として置く

（7） ドキュメントから D-Case のサブツリーを作る

（8） サブツリーができていない部分を典型的な議論構造を使って作る

（9） 上記を必要なだけ繰り返す

3. 実験結果と評価

D-Case 入門 [10] の内容を用いて、社会人を対象として模擬講義および演習を 10 月 19 日に行った。参加した社会人は 17 名で、組込みシステム企業、コンサルティング会社などから来ていただいた。模擬講義及び演習の内容は以下の通りであった。

（1） ディペンダビリティの講義 (40 分)

（2） アシュアランスケースと GSN の講義 (40 分)

（3） GSN の基本演習 (60 分)

（4） D-Case 構築法の講義 (40 分)

（5） D-Case 作成演習 (60 分)

GSN の基本演習では構文やノードに書く内容に関する基本的な演習を行った。D-Case 作成演習では、あるシステムに関するドキュメントを与え、それをもとに A4 の用紙 1 枚程度の空欄に GSN を書いてもらう演習を行った。例えば、以下のような問題を出題した。

問題 図 4 のようなコースで行うロボットレースがあるとします。与えられたドキュメントをもとに (次スライド以下) 適切なトップゴールを設定して、D-Case を書いてください (エビデンスまで書いてください。「他のサブゴールと同様」などの省略は用いてよい)

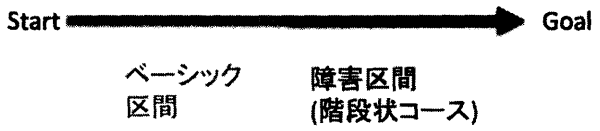

図 4　コ　ー　ス

与えられたドキュメント

- ロボットレース競技規約
  - ベーシック区間は４０秒以内にクリアすること
  - 障害区間では、与えられた条件をクリアすること
- レースコース仕様書
  - ベーシック区間
  - 障害区間と与えられた条件
- ロボット仕様書
- ロボットの設計およびレビュー結果
  - 通信、ライントレース、階段を登る機能の設計およびレビュー結果
- ロボットコンポーネントのユニットテスト結果
  - 通信、ライントレース、階段を登る機能のユニットテスト結果
- ベーシック区間、障害区間走行テスト結果
  - 通信、ライントレース、階段を登る機能の走行テストログ
- リスク分析結果
  - ベーシック区間でのリスク分析結果
    - 通信障害によりスタートできない
    - ライントレースに時間が掛かる
  - 障害区間でのリスク分析結果
    - 階段を登る衝撃でロボットが転倒する

現在、受講していただいた方へのアンケートと答案を解析している途中であり、その結果は別稿にて示したい。ここでは、アンケートの結果のみを示す (図 5)。アンケートでは基本的な

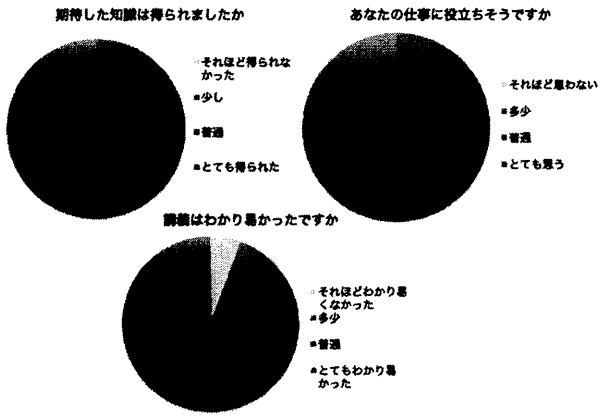

図 5　アンケート結果

質問として、講義によって、

NII-Electronic Library Service

Institute of Electronics, Information, and Communication Engineers

- 期待した知識は得られたか
- 仕事に役立ちそうか、講義は
- わかり易かったか

、を書いてもらった。図5を見ると、アシュアランスケースは今後の仕事に役立ちそうだと期待してもらうことに、今回の講習は成功したといえる。しかし、講義のわかり易さについては、まだ準備不足が目立ち、今後改善していく必要があると考える。

今回は、日本では初めてに近い本格的なアシュアランスケースの講習及び演習であった。また欧米でのアシュアランスケースの講習内容などは、公開されておらず、解析なども我々が知る限り行われていない。

今回の講義・演習に加え、学生などへの講義・演習を行なっている。それらの結果や解析なども今後論文として公開していく予定である。

4. メトリクス

本研究では，提案した構築手法を評価するために，アシュアランスケースの評価方法についても検討した．アシュアランスケースの評価については，Kelly の既存研究 [5] がある．そこでは，次の 6 つの評価軸が提案されている．

（1） 網羅性 (coverage)
（2） 独立性 (dependency)
（3） 限定性 (definition)
（4） 直接性 (directness)
（5） 関連性 (relevance)
（6） 頑健性 (robustness)

ここでは，GSN で記述されたアシュアランスケースに適用可能な，それぞれの軸に対して定量的に評価するための評価尺度を導入する．

4.1 網 羅 性

アシュアランスケースに記述されている議論やエビデンスの，最終的な結論である主張に対する網羅性であり，次の二つの合計で評価する．

（1） GSN の全ての葉に対するエビデンスである葉の割合
（2） GSN の各戦略に対する網羅性の評価

GSN の葉は，エビデンスか未定 (undefined) であるので，1. 実際にエビデンスが用意された割合を表す．2. の方は，例えば，親ゴールから子ゴールへの分割に関する網羅性の定義が戦略の中に含まれているかどうかや，含まれていた場合にその定義に従って実際にすべての子ゴールが用意されているかどうかを評価する．また，一般に戦略はトップゴールに近いほどトップゴールに対する影響が大きいといえるため，木構造における深さによって戦略間に重みをつけてもよい．

4.2 独 立 性

エビデンス間の依存関係である．依存しあう複数のエビデンスからなる議論は説得力に欠けるための評価軸である．これは，全エビデンス数に対する，独立しているものの数によって評価する．例えば，GSN に 4 つの葉があり，すべてエビデンスだった場合を考える．このうち一つのエビデンスが他のエビデンスに依存している，または，同じものを参照している場合などは，これらは一つと数え，3/4 と評価するなどである．

4.3 限 定 性

想定されるシステムの目的を，ゴールの記述が十分反映しているかどうかや，想定動作環境が十分現実を反映しているかどうかを評価する軸である．つまり，ゴールの記述そのものの妥当性である．これは，妥当性確認 (validity) に相当するため，客観的な評価は難しいが，今回は，全ゴールの中で．そのゴールの主張が成り立つための想定動作環境の記述が文脈などによって記述されているかどうかなどによる尺度を考えている．

4.4 直 接 性

次の関連性とともに，戦略やエビデンスの質に関する評価軸である．間接的な議論やエビデンスは説得力が欠けることを表す．定量的な尺度としては，全戦略数に対する直接的な戦略の数と，全エビデンス数に対する直接的なエビデンスの数との二つによるものを考えた．間接的な戦略は例えば，開発プロセスによる議論，また，間接的なエビデンスは，類似製品の過去の実績やテスト結果などを想定している．

4.5 関 連 性

前の直接性とともに，戦略やエビデンスの質に関する評価軸である．直接性と似ているが，直接性は、間接的ではあるが、間違ってはいない戦略やエビデンスを問題とするが，これは、そもそも適切ではないものを問題視するものである．具体的には，エビデンスの場合は，その上のゴールとの関連が適切か否か，戦略の場合は，その直上のゴール（親ゴール）と直下のゴール群（子ゴール群）との関連が適切か否かをみる．網羅性とも関係するが，こちらは網羅していることではなく，網羅性の定義や枠組みそのものの妥当性を評価する．定量的な尺度は前の直接性と同様とする．

4.6 頑 健 性

システムや環境の変化にどの程度アシュアランスケースが耐えられるか否かを評価する軸である．定量的な尺度としては，全ての戦略の中で，親ゴールにたいしてその子ゴールの集まりが，必要条件ではない十分条件になっているものの割合を考える．つまり，必要十分条件の場合は，システムや環境の変化に対して，アシュアランスケースの変更の必要性が生じる可能性が高いが，十分条件であれば，ある程度は変更無しで対応できる可能性があるからである．

5. ま と め

本論文では、アシュアランスケースの構築手法を講義するための入門書および講義を開発し、社会人に対して行った。アシュアランスケースは日本においてはまだ馴染みがなく、そのための講義や演習なども広くは行われていない。今後、模擬講義などを通して、講義や演習の改善を行なっていく予定である。現在、答案などを解析中である。解析結果などを今後まとめていきたい。

文 献

[1] http://www.adelard.com/web/hnav/ASCE.
[2] *Workshop on Assurance Cases: Best Practices,Possible Obstacles, and Future Opportunities, DSN 2004*, 2004.

NII-Electronic Library Service

Institute of Electronics, Information, and Communication Engineers

[3] GSN contributors. GSN community standard version 1.0, 2011.

[4] J.R. Inge. The safety case, its development and use in the United Kingdom. In *Proc. of ISSC25*, 2007.

[5] T.P̃. Kelly. Reviewing assurance arguments – a step-by-step approach. 2007.

[6] Tim Kelly and Rob Weaver. The goal structuring notation - a safety argument notation. In *Proc. of the Dependable Systems and Networks 2004, Workshop on Assurance Cases*, 2004.

[7] Yutaka Matsuno, Jin Nakazawa, Makoto Takeyama, Midori Sugaya, and Yutaka Ishikawa. Toward a language for communication among stakeholders. In *Proc. of the 16th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'10)*, pages 93–100, 2010.

[8] Yutaka Matsuno and Shuichiro Yamamoto. Toward dynamic assurance cases. In *Proc. JCKBSE 2012*, pages 154–160. IOS Press, 2012.

[9] Yutaka Matsuno and Shuichiro Yamamoto. A new method for writing assurance cases. *International Journal of Secure Software Engineering (IJSSE)*, Special Issue on Cybersecurity Scientific Validation, January 2013. Accepted for Publication.

[10] 松野裕、高井利憲、 山本修一郎. *D-Case* **入門 ～ディペンダビリティ・ケースを書いてみよう!～**. 株式会社ダイテックホールディング, 2012. ISBN: 978-4-86293-079-8.

NII-Electronic Library Service