人工知能学会
第18回知識流通ネットワーク研究会
SIG-KSN-018-02

保証ケースの先端研修教材の試作と評価

山本修一郎*，森崎修司**，渥美紀寿*

*)名古屋大学　情報連携統括本部　情報戦略室
**）名古屋大学大学院情報科学研究科
***)名古屋大学工学部
愛知県名古屋市千種区不老町

Advanced teaching material development on assurance case and its evaluation

Shuichiro Yamamoto, Shuji Morisaki, Noritoshi Atsumi

Nagoya University
Furo-cho, Chikusa-ku, Nagoya Aichi Japan

概要

保証ケースを教育する基礎的な教材が報告されている．しかし，保証ケースをパターンに基づいて統一的に作成する手法や，保証ケースのレビュ手法を教育する高度な内容の教材は報告されていない．また、今後多くの手法が開発されることになれば、研修教材を効率的に開発する手法も必要になる。

このため，本稿では、手法研修教材の開発手法を提案するとともに、それに基づく保証ケースについての高度な研修教材の開発事例について報告する。

Several teaching materials are proposed to learn assurance cases. However, it is not sufficient to educate advanced assurance case methods. The teaching material development method is also necessary to develop many different kinds of materials for teaching advanced assurance case methods.

In this paper, a method to develop teaching materials on methods is proposed. Case studies for developing advanced teaching materials on the assurance case are also described.

1. はじめに

高い安全性が要求される複雑なシステムを実現するために、保証ケースの作成が必要とされるようになっている[1]。たとえば、自動車分野で導入が必要とされる IS026262 機能安全規格などで、安全性に対する保証ケースである安全性ケースの作成が開発プロダクトだけでなく開発プロセスに対しても義務付けられている。このため、多様なモデルに対する統一的な保証ケースの作成手法の研究、既存コンポーネントに対する保証ケースの作成手法の研究、保証ケースの客観的なレビュ手法の研究が必要である。

このため、筆者らは，独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センターが実施した「2015 年度ソフトウェア工学分野の先導的研究支援事業」の支援を受け、以下の各項目について研究を実施した。

a) 多様なモデルに対する統一的な保証ケースの作成手法の研究
　ソフトウェア開発・システム開発における多様なモデル図に対する保証ケースの実践的な作成法について研究する。
b) コンポーネントに対する保証ケース作成手法の研究
　ソフトウェア開発・システム開発における既存コンポーネントに対する保証ケースの実践的な作成法について研究する。
c) 保証ケースの客観的なレビュ手法の研究
　ソフトウェア開発・システム開発における保証ケースの実践的なレビュ手法について研究する。
d) 実践的保証ケース研修教材の試作
　ソフトウェア開発・システム開発における開発

技術者に対する保証ケースの実践的な研修教材について研究し、教材を試作する。

e) 保証ケース手法の実践的適用評価の研究

ソフトウェア開発・システム開発において必要とされる実践的な保証ケース手法について研究する。

研究項目 a)については、[7-9]で報告した。[7]では、委託研究で採用したモデルに基づく保証ケース作成法によって保証ケースのゴールを定量的に評価する手法を提案した。[8]では、モデルに基づく保証ケース作成法をエンタープライズアーキテクチャのモデリング言語 ArchiMate に対して適用評価を実施した。[9]では保証ケースが対象とする成果物や品質特性，リスクなどのモデル情報に基づき，保証ケースを統一的に作成する手法を提案した。

研究項目 b)については、[11]で報告した。[11]ではコードに対する保証方式について、オープン SSL の仕様書に基づく保証ケースを用いて、オープン SSL コードの脆弱性を確認することにより有効性を評価した。

研究項目 c)については、[10,12]で保証ケースが対象とする成果物や品質特性，リスクなどの構成情報に基づくシステミグラムによって，保証ケースをレビュする手法を提案した。

研究項目 e)については、[13]で保証ケースの導入準備能力を客観的に評価する手法について提案した。

本稿では、研究項目 d)「実践的保証ケース研修教材の試作」について報告する。

以下ではまず，2 節で，本研究の目的について述べる．3 節で，手法研修教材の開発手法を提案する．4 節では，保証ケース作成手法に対する提案手法の適用事例を説明する．5 節では，手法研修教材開発手法ならびに、試作した研修の有効性，妥当性について議論する．6 節で関連研究について述べ、7 節で結論を述べる．

2. 研究の目的

統一的保証ケース作成手法や保証ケースレビュ手法について教育する研修教材がないことから、多様なモデルに対する統一的な保証ケース作成手法ならびに、保証ケースの客観的なレビュ手法に関して ISD（Instructional System Design）原則に基づいて試作した研修教材を提供する必要がある。

もし、新たに考案した保証ケースの手法を教育するための教材がなければ、手法を効率的に展開できない。また、教材の有効性を確認するためには、教材の試行評価が必要になる。この理由は、有効性が確認されてない教材を活用することが困難になるためである。

3. 手法研修教材の開発手法

複数の手法に対する研修教材を開発する場合、あらかじめ手法研修の開発手順を共通化して定義しておくことにより、研修教材開発を効率化できる。

すなわち、図 1 に示す 4 段階からなる手法研修の開発手順を定義した。

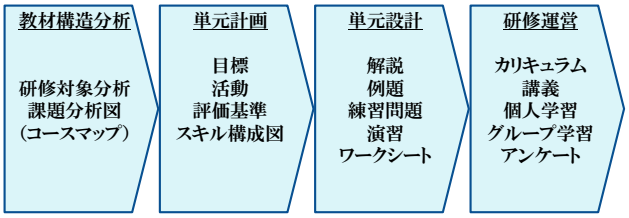


図 1　手法研修の開発手順

【段階 1】教材構造分析

研修対象分析では、研修対象とする手法を分析することにより、手法を実施する上で必要な活動とそのための知識を抽出する。

課題分析図（コースマップ）の作成では、抽出した活動と知識に基づいて、学習要素（単元）とその依存関係を明らかにする。

【段階 2】単元計画

まず、研修全体の目標をスキル構成図で定義する。次に、課題分析図で定義された単元について、研修する順に番号付ける。また、単元ごとに、学習活動の概要を記述する。さらに、単元を習得したことを確認するための評価基準を定義する。単元計画の内容をコース単元一覧表にまとめる。

【段階 3】単元設計

研修単元ごとに、基本概念の解説と、基本概念を具体的に説明する例題ならびに、基本概念を学習したことを練習できる確認問題を作成する。
また、演習で用いるワークシートを作成する。

【段階 4】研修運営

研修単元の時間配分を決め、カリキュラム構成を定義する。

カリキュラムに基づき、講義、個人学習、グループ学習からなる研修を運営する。

受講生へのアンケートを実施し研修内容を評価する。

4. 保証ケース教材の作成

a) 多様なモデル図に適応する統一的な保証ケース作成手法、c) 保証ケースレビュ手法に基づく先端的な保証ケース研修教材を試作するために、前述した手法教材開発手順を適用した結果について述べる。

この試作では、3 時間程度の研修で使用するための説明、確認問題、演習ワークシートなどからなるテキスト形式の実践的な保証ケース研修教材を開発する。

この試作で想定される問題として、研修教材の内容が難解・複雑で実践的でないと十分な教育効果が得られないことと、教材量が多すぎると学習者が理解できないことがある。このため、前述した手法研修教材開発手法を適用して、コース単元とその関係をコースマップによって明確化することにより、学習目標と学習内容としての知識を構造化するとともに、重要性に従って単元を選択できるように設計することが必要である。

4.1 統一的保証ケース作成手法の研修教材

保証ケースの基本知識を持つ受講者が少ないことを考慮する必要がある。

コースマップを作成することにより、研修教材を設計した。統一的保証ケース作成手法のコースマップでは、以下の 13 単元とその関係を定義した。

①保証ケース対象成果物の構造を理解している
②システムのリスクを分析できる
③保証ケースで説明するシステムの特性を理解している
④保証ケースの表記法を理解している
⑤保証ケースのコンテクストと分解を理解している
⑥リスク対策の証拠を定義できる
⑦モデルを定義できる
⑧保証ケースの説明パターンを理解している
⑨説明パターンを組合せることができる
⑩分析の網羅性を理解している
⑪説明対象の優先順位を評価できる
⑫統一的な保証ケースを作成できる
⑬保証ケースをグループで統一的に作成できる

統一的保証ケース作成手法についてのコースマップを付図 1 に示す。統一的保証ケース作成手法コースの各単元内容について、付表 1 に示す。

とくに、ルートゴール、モデル図の構成要素・関係層、構成要素・関係分類層、構成要素と関係の実体層、リスク対策層に基づく階層に従って、モデル図の構成要素と関係に基づく統一的な保証ケースの作成手順を具体化する能力は、⑫⑬で保証ケースを統一的に作成することで学習することができる。

ここで、①は、そのために必要な基礎知識を習得するために用意している。②③④⑤⑥は基礎知識を応用して統一的作成法を習得するための応用知識を習得するために用意している。⑦は成果物の構成を定義するための知識を習得するために必要である。⑧は上述したように応用知識を統一的作成法に結び付けて習得するための知識を習得するために必要である。⑨⑩⑪では統一的作成法によって作成した保証ケースが適切であることを確認するために必要な知識を習得することができる。

統一的保証ケース作成手法についての研修教材の試作では、対象システムの構成モデル、保証すべき品質特性、保証対象を構成する要素のリスクなどの主張（Claim）の前提（Context）ならびにそれらの重要性を表す重みに基づいて、保証ケースの主張を階層的に分解するスキルを学習する統一的保証ケース作成手法の教材を実現した。

この対象とする学習目標は、付図 2 に示す構成の保証ケースのスキルを本教材で習得することである。なお、「保証ケースの表記法を理解している」は、基本的な知識である。それに基づいて、統一的な保証ケースを作成する上で必要となる知識「保証ケースのコンテクストと分解を理解している」「保証ケースの説明パターンを理解している」「分析の網羅性を理解している」「リスク対策の証拠を定義できる」については基本的な知識を応用する能力を学習させるものである。

この研修の受講対象者のスキルレベルはソフトウェア開発経験者とした。統一的保証ケース研修カリキュラムの例を表 1 に示す。研修はこのカリキュラムに従って実施した。

表 1　統一的保証ケース研修カリキュラム例

時間	カリキュラム
13:30～14:50	第1章　保証ケースの統一的作成基礎知識 1.1　システムの構成 1.2　システムのリスク 1.3　システムの特性 1.4　保証ケースの表記法 1.5　主張の分解 1.6　リスク対策の証拠
15:00～16:20	第 2 章　保証ケースの統一作成手法の知識 2.1　モデルの定義 2.2　主張の分解 2.3　主張の階層的分解 2.4　分解の網羅性 2.5　主張の優先順位 2.6　統一的な保証ケース
16:30～17:30	第 3 章　保証ケースによる合意形成 3.1　議論の合意形成 アンケート

4.2 保証ケースレビュ手法の研修教材

保証ケースレビュ手法のコースマップでは、以下の 13 単元とその関係を定義した。

①保証ケースの対象成果物の構造を理解している
②システムのリスクを分析できる
③保証ケースで説明するシステムの特性を理解している
④保証ケースの表記法を理解している
⑤保証ケースのコンテクストと分解を理解している
⑥リスク対策の証拠を定義できる

⑦モデルを定義できる
⑧保証ケースの説明パターンを理解している
⑨説明パターンを組合せることができる
⑩分析の網羅性を理解している
⑪説明対象の優先順位を評価できる
⑫統一的な保証ケースを作成できる
⑬保証ケースをグループで統一的に作成できる

とくに、システミグラムに従って、保証ケースの構成要素と関係に基づく客観的な保証ケースのレビュ手順を具体化する能力は、⑫⑬で保証ケースをレビュすることで学習することができる。

ここで、①～⑤は、そのために必要な保証ケースレビュの基礎知識を習得するために用意している。⑥～⑩は基礎知識を応用してレビュ対象の見える化手法を習得するための応用知識を習得するために用意している。⑪では保証ケースから作成したシステミグラムに基づいて保証ケースのレビュ指標を客観的に定義するために必要な知識を習得することができる。

4.3 研修教材の規模

試作した研修教材のスライド数を表 2 に示す。

表 2 研修教材の概要

項目	統一的保証ケース作成法研修教材	保証ケースレビュ手法研修教材
教材	114	82
例題	12	8
演習問題	6	7

4.4 研修実施結果

保証ケース統一作成手法の研修教材と運営方法の妥当性を確認するために、2 回に分けて研修を実施した。第 1 回研修では、座学を中心として最後にグループ演習を実施した。第 2 回研修では、基礎知識の習得段階からグループ演習を実施した。研修参加者と 2 回の研修のアンケート回答者数に基づいて比較した結果を表 3 に示す。

表 3　保証ケース統一的作成法の研修結果

項目	第 1 回	第 2 回
研修参加者(経験者数)	24 名(3)	22 名(0)
満足度（注１）	95.8%	95.5%
理解度（注１）	100%	81.8%
活用度（注１）	95.8%	86.4%
研修時間十分性（注２）	100%	57.9%
難易度（注３）	100%	72.2%
演習満足度（注１）	72.7%	81.8%
演習時間十分性（注２）	95%	73.7%
教材充足性（注１）	88.2%	77.8%

ここで、表 3 の注の意味は次のとおりである。
注 1：まあまあそう思う、そう思う、非常にそう思うと回答した参加者の比率
注 2：長い、ちょうどよいと回答した参加者の比率
注 3：易しい、ちょうどよいと回答した参加者の比率

第 2 回研修では演習中心としたことから演習満足度が向上している。しかし、演習時間十分性については、逆に、研修時間だけでなく演習時間ももっと必要だという結果になった。

各章の理解度について、よく理解できた章と理解が難しかった章について、2 回の研修参加者からの回答結果を図 2 と図 3 にまとめる。なお、これらの図では、よく理解できた章を「容易」と理解が難しかった章を「困難」とした。

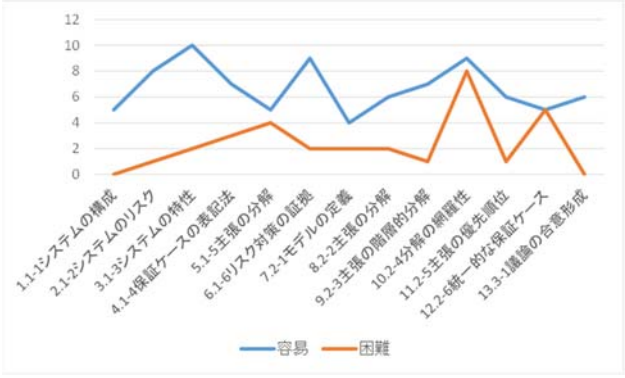


図 2　第 1 回研修の理解度

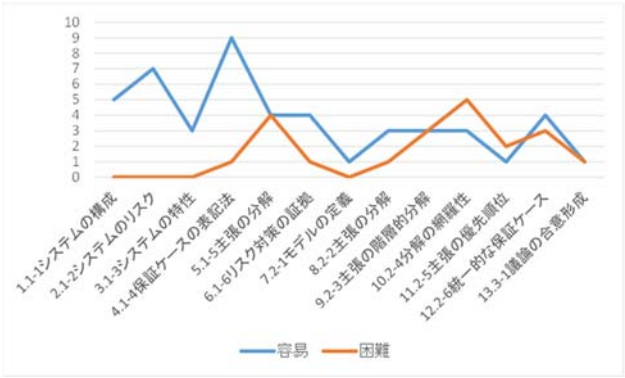


図 3　第 2 回研修の理解度

保証ケース統一作成手法の研修実験の評価結果について主な結果をまとめると、次のとおりである。

・2 回の研修実験を実施することにより、保証ケース統一作成手法研修が有効であることを確認した。

・2 回の研修参加者による研修の評価点数は、すべて 3.5 以上であった。

・半日研修の場合、講義中心の研修のほうが演習中心の研修よりも、研修満足度が高い。

・教材内容の難易度について、大半の参加者が容易に理解できると回答したことから教材は適切である。

・研修時間を半日から、1 日に拡大することで、参加者の満足度を向上できる可能性がある。

なお、保証ケースレビュ手法についての研修内容の詳細ならびに実施結果については紙幅の関係で省略する。

5. 考察

5.1 手法研修教材開発手法の有効性

保証ケースについての先端研修教材 2 件をそれぞれ、2 か月で無理なく試作できたこと、また試作した教材を実際に使用した研修での理解度も高かったことから、手法研修教材開発手法の有効性を確認した。

5.2 研修教材の外部評価

企業の有識者から、本研修教材について以下のような肯定的な意見を得た。

レビュ手法の研修教材をぜひ提供してほしいので、成果の適用について議論したい。

研修教材を DEOS 協会[20]で認証を受けるには、まずシラバスを用意する必要になるので、開発した教材に基づいてシラバスをぜひ作成してほしい。

今回開発されたような発展的な保証ケースの応用教材が継続して提供されるのはいいことだ。

5.3 限界

本稿では，開発した 2 件の研修教材について各 2 件の研修を実施し教材の有効性を確認した．提案教材の有効性を立証するためにはさらに多くの研修例に対して評価する必要がある．

6. 関連研究

DEOS 協会がディペンダビリティ技術の普及に役立つ教育コンテンツを認証している[20]。認証された D-Case 教材として、D-Case トレーニング構造編がある。この教材は、D-Case 教育シラバス構造編[21]に基づいて認証されている。この教材は保証ケースの一種である D-Case の構造について基礎知識を教育するための教材であり、本稿で示した先端的な保証ケース手法の教材ではない。

稲垣と鈴木は、授業設計マニュアル[22]を提案している。一般的な授業を設計するための教材構造分析と単元計画の手順を提示している。しかし、保証ケースのようなシステム開発手法についての教材設計法ではない。また、単元設計や研修運営については具体的に記述していない。

7. おわりに

本稿では、手法研修開発手法を提案するとともに，この手法に基づいて「統一的保証ケース作成手法」と「保証ケースレビュ手法」に関する研修教材 2 件を 4 か月で作成できることを示した．また，実際にこれらの教材を用いた研修を実演することで、教材を使用した研修事例による評価結果を示した．この適用事例から，提案手法の有効性を確認した．

今後の研究課題として，提案手法を用いた新たな保証ケース手法に対する研修教材の開発、保証ケース手法以外の手法に対する研修教材開発への適用評価ならびに、研修教材開発効率の評価などがある．

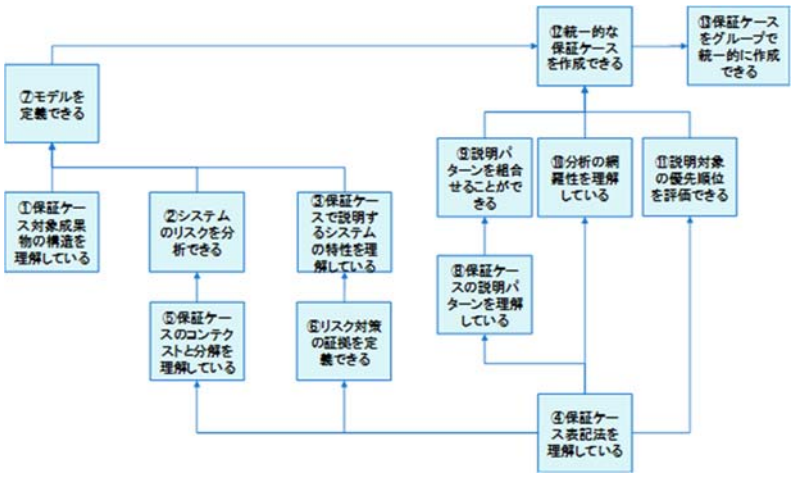
謝辞

本研究は，独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター（SEC: Software Reliability Enhancement Center）が実施した「2015 年度ソフトウェア工学分野の先導的研究支援事業」の支援を受けたものです．

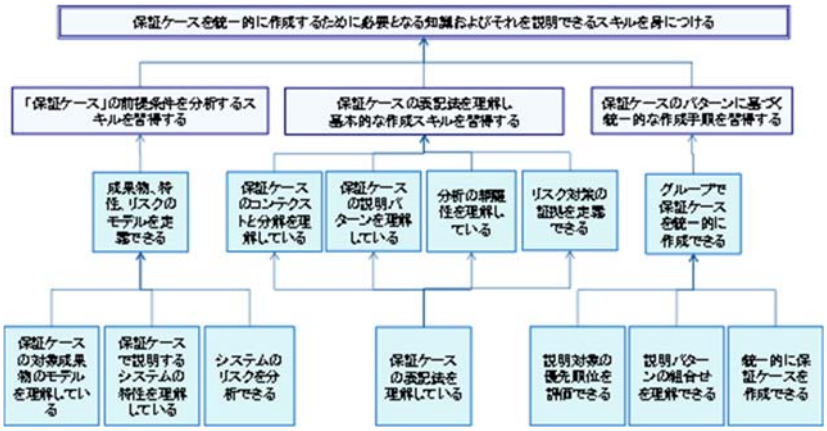
参考文献

[1] Kelly, T., McDermid, J., Safety Case Construction and Reuse using Patterns, University of York (1997)
[2] Kelly, T., Arguing Safety, a Systematic Approach to Managing Safety Cases, PhD Thesis, Department of Computer Science, University of York (1998)
[3] McDermid. J., Software safety: where's the evidence?, in SCS '01: Proceedings of the Sixth Australian workshop on Safety critical systems and Computer Society, Inc. (2001)
[4] Kelly, T., and Weaver, R., “The Goal Structuring Notation – A Safety Argument Notation,” Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases (2004)
[5] Bloomfield, R., and Bishop, P., Safety and Assurance Cases: Past, Present and Possible Future, Safety Critical Systems Symposium, Bristol, UK, 9-11 (2010)
[6] 情報処理推進機構, RISE, http://www.ipa.go.jp/sec/rise/index.html
[7] Shuichiro Yamamoto, Assuring Security through Attribute GSN, ICITCS 2015, pp.1-5, 2015
[8] Shuichiro Yamamoto, An approach to assure Dependability through ArchiMate, Assure 2015, pp. 50-61
[9] 山本修一郎,森崎修司、渥美紀寿、正田稔、モデルに基づく統一的保証ケース作成手法の提案、AI 学会、KSN 研究会、2015. 10
[10] 山本 修一郎,森崎修司、渥美紀寿、構成情報に基づく保証ケースレビュ手法の提案、AI 学会、KSN 研究会、2015. 10
[11] 宮林 凌太, 渥美 紀寿, 森崎 修司, 山本 修一郎、入力分析に基づくコード保証方法の提案、KBSE 研究会、Vol.115, No.281, KBSE2015-39, pp.17-22, 2015
[12] Shuichiro Yamamoto, An assurance case review method using Systemigram, AAA2015
[13] 山本修一郎,森崎修司、渥美紀寿、保証ケース導入準備能力評価指標の提案, KBSE研究会、2016.3.4.
[14] 松野裕，山本修一郎，高井利憲， D-Case入門，～ディペンダビリティ・ケースを書いてみよう！～, ダイテックホールディング, 2012，ISBN 978-4-86293-079-8
[15] 山本修一郎, 保証ケース作成上の落とし穴, [Kindle 版], Amazon Services International, Inc. , 2013
[16] 山本修一郎，システムとソフトウェアの保証ケースの動向, [Kindle版], Amazon Services International, Inc., 2013
[17] 山本修一郎，保証ケース議論分解パターン, [Kindle版], Amazon Services International, Inc. , 2013
[18]山本修一郎，主張と証拠: アシュアランスケースへの招待，アセットマネジメント, ISBN 4862930956, 9784862930958, 2013
[19] 山本修一郎，議論パターンポケットガイド，2014

[20] DEOS 協会, DEOS 認証制度について, http://deos.or.jp/certification/index-j.html
[21]D-Case 教育シラバス構造編, http://deos.or.jp/link/obj/pdf/D-Case_syllabus_v1.11.pdf
[22] 稲垣忠, 鈴木克明, 授業設計マニュアル-教師のためのインストラクショナルデザイン, 北大路書房, 2011
[23] Real-Time and Embedded Systems, “Dependability through Assuredness™ (O-DA) Framework,” Open Group Standard (2013)



付図 1　統一的保証ケース作成手法コースマップ



付図2　統一的保証ケース作成手法のスキル構成

付表1　統一的保証ケース作成手法コースの単元内容

コース単元	説明
①保証ケースの対象成果物の構造を理解している	保証ケースで保証しようとする対象システムの成果物の構成内容を理解して説明できるスキルを習得する。
②システムのリスクを分析できる	保証しようとするシステムが持つリスクを成果物の構成に従って分析できるスキルを習得する
③保証ケースで説明するシステムの特性を理解している	保証ケースで説明すべき、安全性やセキュリティなどのシステムが持つべき品質特性を理解できるスキルを習得する。
④保証ケース表記法を理解している	主張、コンテクスト、説明分解、証拠からなる保証ケース表記法についてのスキルを習得する。
⑤保証ケースのコンテクストと分解を理解している	保証ケースの主張をコンテクストの内容に従って、下位の主張に分解するスキルを習得する。
⑥リスク対策の証拠を定義できる	リスク対策できていることを証拠によって保証するためのスキルを習得する。
⑦モデルを定義できる	成果物、特性、リスクの構成とその実体によって、モデル化するスキルを習得する。
⑧保証ケースの説明パターンを理解している	主張をコンテクストの内容に従って下位の主張に分解するスキルを習得する。とくに、成果物の構成に基づく分解、リスクに基づく分解、品質特性に基づく分解について習得する。
⑨説明パターンを組合せることができる	主張を階層的に分解するために、成果物分解、特性分解、リスク分解の３パターンの組合せ方に関するスキルを習得する。
⑩分析の網羅性を理解している	コンテクストの内容に従って主張を下位の主張に分解する際の下位の主張の網羅性を確認するスキルを習得する。
⑪説明対象の優先順位を評価できる	上位の主張に対する下位の主張間の優先順位を定義するスキルを習得する。
⑫統一的な保証ケースを作成できる	最上位の主張から、成果物分解、特性分解、リスク分解に従って階層的に保証ケースを作成するスキルを習得する。
⑬保証ケースをグループで統一的に作成できる	統一的な保証ケースを複数人で議論することにより合意形成できるスキルを習得する。