独立行政法人情報処理推進機構 委託

2015 年度ソフトウェア工学分野の先導的研究支援事業

「保証ケース作成支援方式の研究」

成果報告書

平成 28 年 2 月

国立大学法人名古屋大学

本報告書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」の公募による採択を受け名古屋大学情報連携統括本部（研究責任者　山本修一郎）が実施した研究の成果をとりまとめたものである.

目次

研究成果概要

保証ケースは，開発対象システムが安全性や高信頼性をもつことを論理的に保証するために用いられる構造的な文書である．保証ケースは，①システムが特性を持つことについての主張と，②上位の主張を下位の主張で説明するための分解，③説明のための前提，④主張の根拠となる証拠から構成される．

保証対象とするシステムの状況を考えると，現行のシステム開発では，モデルが定義されている場合と，明確なモデルが定義されていない場合がある．モデルに基づくシステム開発では，多様なモデルに対して保証ケースを作成する必要がある．このため，保証ケース作成支援方式の研究では，モデルに基づく保証ケースの統一的作成法ならびに，モデルがないコンポーネントコードに対する保証ケース作成法について研究することとした．

また，保証ケースの導入に積極的な開発組織では保証ケースがすでに作成されている場合がある．このため，既存の保証ケースについて，保証ケースの客観的なレビュ手法について研究することとした．

さらに，システム開発組織に対して，新たに開発する保証ケース作成支援方式の知識を教育するために，実践的保証ケース教材の試作について研究する．また，保証ケース手法を導入する上で，開発組織が必要な準備能力を備えていることを確認するために，保証ケース手法の実践的導入適合性についての研究を実施することとした．以下では，これらの研究項目と主な成果について概説する．

上述したことから，保証ケース作成支援方式の研究では，モデルに基づく保証ケースの統一的作成法，コンポーネントに対する保証ケース作成法，保証ケースの客観的なレビュ手法，実践的保証ケース教材の試作，保証ケース手法の実践的導入適合性について研究することとした（図 1）．

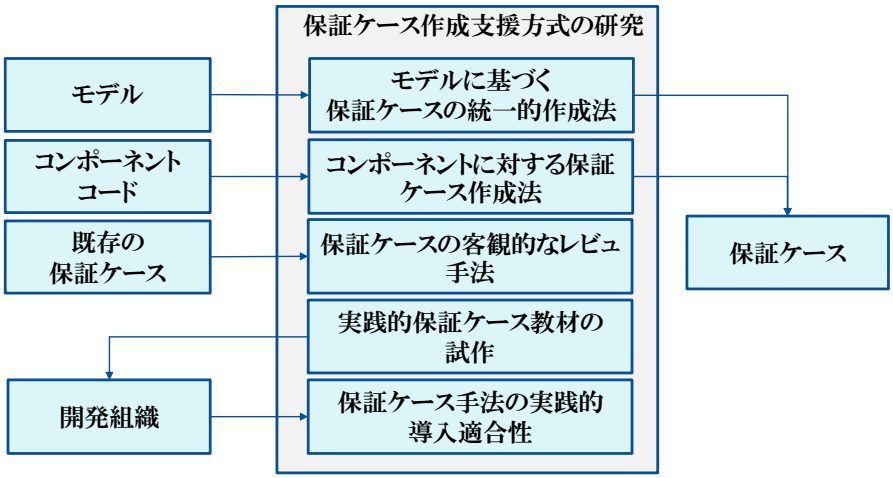


図 1　保証ケース作成支援方式の研究の位置づけ

以下では，各研究成果についてまとめる．

研究課題１「モデルに基づく保証ケースの統一的作成法」

【目的】

多様なモデルに対する保証ケースの作成を容易化するために，任意のモデルに対して適用できる保証ケースの統一的な作成法を確立する．

【課題】

これまで，モデルごとに保証ケースの分解パターンを用意していた．しかし，多様なモデルに対して個別に分解パターンを用意するのは限界があった．

【手法】

どのようなモデルも，必ずモデル要素と要素関係によって定義されている．したがって，モデルを保証する場合，モデル要素と要素関係に基づいて，保証ケースを一般的に分解することができる（モデル構成に基づく分解であることからこの分解をアーキテクチャ分解と呼ぶ）．また，モデル要素とその関係が期待される品質特性をもつことについて，品質特性の下位特性ごとに分解して保証することができる（品質特性の構成に基づく分解であることから，この分解を品質特性分解と呼ぶ）．さらに，モデル要素とその関係が必要な品質特性を持つうえでのリスクとその対策が実施されていることに対して分解することができる．（リスク対策についての分解であることから，この分解をリスク分解と呼ぶ）このように，対象とするモデルが品質特性を持つことを，アーキテクチャ分解，品質特性分解，リスク対策分解にしたがって統一的に保証ケースを作成できる．

モデルに基づく保証ケースの統一的作成法の概要を図２に示す．

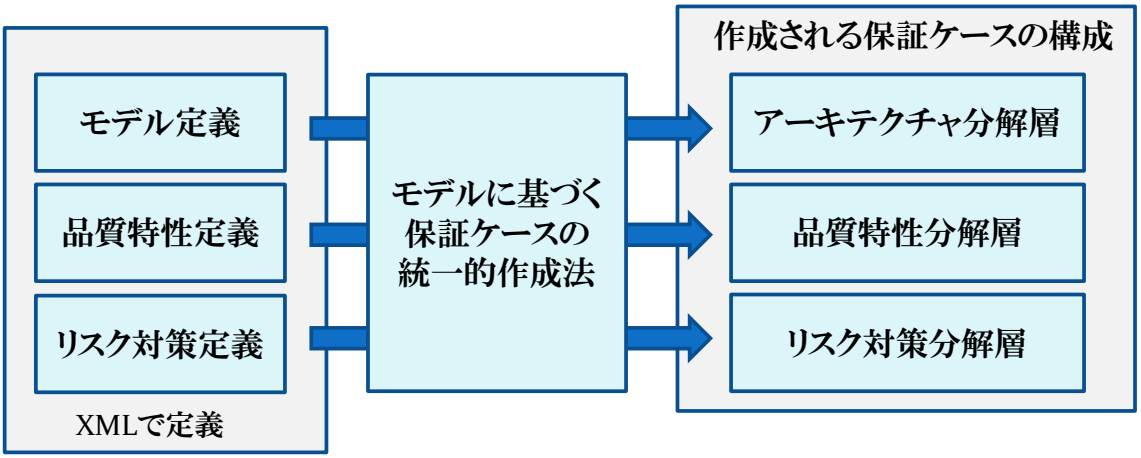


図２ モデルに基づく保証ケースの統一的作成法の概要

【成果】

１）モデルに基づく保証ケースの統一的作成法をアルゴリズムで定式化した．このアルゴリズムでは，要素と要素関係をもつ任意のモデルから統一的に保証ケースを作成できる．

２）アルゴリズムに基づいて保証ケース作成支援ツールを試作した．保証ケース作成支援ツールでは，XML により，モデル，品質特性，リスク対策を定義しておくことにより，保証ケース情報を半自動的に生成できる．生成された保証ケース情報を保証ケースエディタに入力することで保証ケースを作成できる．

３）統一的作成法の適用実験で評価した結果，手動でモデルから保証ケースを作成する場合に比べて，ツールを用いることにより，作成時間を約 5.6 倍に向上できることを明らかにした．

【提供成果】

１）統一的保証ケース作成手法（研修教材として提供）

２）統一的保証ケース作成支援ツール

【有識者による本研究成果の評価】

１）統一的保証ケースの評価で，保証ケース作成支援ツールのシステム構成図に対して自己適用した点が評価できる．

２）有識者のテスト知識を獲得する上で，テスト対象，品質リスクを明確に記述できていないという問題があった．不具合を発見するテスト有識者の経験を展開していく場合，テスト対象の構成と品質リスクを定義してデータベース化することが重要になるので，統一的保証ケース作成方式で考案された保証構造図，品質特性定義，そのリスク定義を活用できる．

３）対象物の見方を整理する方法が客観的ではないだけでなく，有識者ごとに個別的だった．統一的保証ケースを用いれば，論理的に説明できる．

４）テストサービスを提供しているが，これまでテストの統一的基準がないため，客観的な評価ができないという問題があった．保証ケースレビュ方式で定式化している内容である①対象物，②品質特性，③リスク，④対策ができていることの確認テストテストという関係を考慮すると，テストの観点を統一的に分類する仕組みを作ることができそうだ．

５）あらかじめ特性分解パターンを用意しておき，分析者が適切な品質特性を選択して分解することができるので，現在実施している「アーキテクチャチェックサービス」の中で，受託研究で開発されたたツールを試行適用できそうだ．

研究課題 2「コンポーネントに対する保証ケース作成法」

【目的】

リポジトリに格納される静的情報と保証ケースの構成要素との関係の明確化と，それに基づく既存コンポーネントに対する保証ケース作成手法の具体化を実施する．

【課題】

モデルに対する保証ケースの作成では，これまでパターン分解による手法があった．しかし，コードに対する保証ケースの作成法はなかった．また，既存システムを保証する場合，モデルが定義されていないことが多いという問題もあった．

【手法】

コンポーネントコードに対する保証ケースの作成では，コンポーネントへの入力と出力に着目する．コンポーネントの入出力仕様に対して，対応するコードでは指定された入力に対する処理によって出力を作成する必要がある．

この点に着目して，コンポーネントコードに対する保証ケースでは，図 3 に示すように，入出力分解層で必要な入出力に対する主張を分解することにより，対応するコードについて具体化すべき証拠層を用意する．次いで，コードを探索して対応するコードがあれば，証拠として明記する．もし対応するコードがなければ，証拠がないことになり，仕様を実現す

るコードが抜けていることを検出できる．この考え方を，証拠に基づく欠陥摘出原理（Defect Detection by Evidence，DDBE）と呼ぶ．

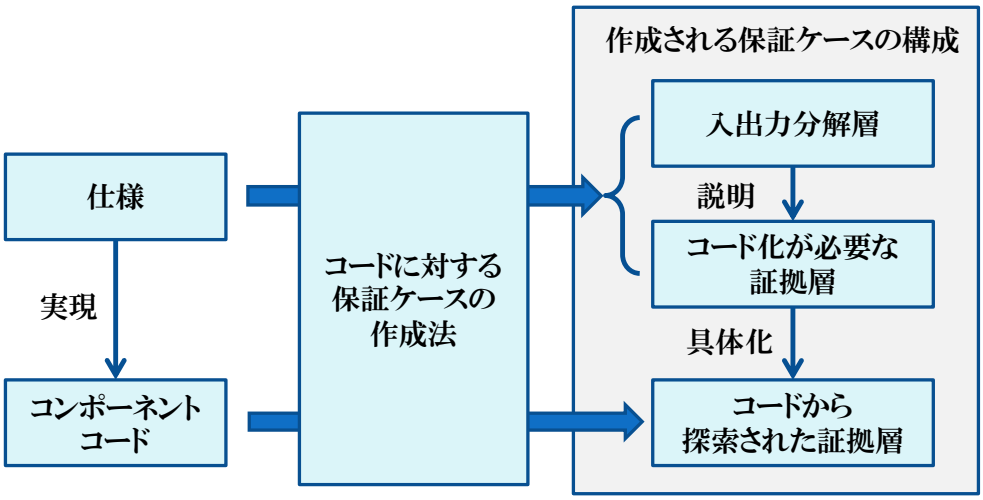


図 3　コンポーネントに対する保証ケース作成法

【成果】

1）コンポーネントコードに対する保証ケース作成手法 DDBE を定式化した．

2）考案した手法をオープン SSL に適用して，12 個の具体化すべき証拠に対して，11 個のコードが対応したが，対応するコードがない 1 個が脆弱性の欠陥であることを摘出した．

3）保証ケースと対応するリポジトリのメタモデルを，前提，主張，具体化すべき証拠，証拠，識別子，式，ブロックによって具体化した．

【提供成果】

1）コンポーネントコードに対する保証ケース作成手法 DDBE

2）保証ケースと対応するリポジトリのメタモデル

【有識者による本研究成果の評価】

1）これまでのコードレビュの根拠は有識者の経験か論理しかなかった．しかし有識者の経験の観点やその活用は個別的だ．設計書のレビュでは，「てにをは」レベルの指摘が多いと開発者の士気が低下する．提案手法では，本質的な機能の存在を問うレビュができる点がよい．

2）オープンソースの評価にも適用できそうだ．企業が OSS を使う場合，目的があり，それに適合する OSS 製品が複数あることが多い．このとき，OSS 製品には個人が作成したものや企業が整備したものもある．本手法を応用して，ライセンスの有無やサポート体制を条件として複数の OSS 製品の目的適合性検査手法を考案できそうだ．

3）クラウドのサービスレベルを保証する方法に応用できそうである．たとえば，自社クラウドと外部クラウドの連携では，サービスレベルの保証方法や，異常時の対応策の十分性などを保証する必要があるので，今回の成果を応用できそうである．

4）オープンソースコードのセキュリティチェックが重要になっており，今回の成果が適用できると考えている．

5）必要な要素がそろっていることを主張としておき，そうなっているコードの部分を証拠として提示すればミドルウェアの API を利用するコードの適切性を保証する方法として，受託研究成果を活用できるだろう．

6）コードの静的チェックツールでは，あらかじめ定義してある一般的な規則に基づいてチェックする．これに対して，本手法では，コードに対する確認すべき内容を保証ケースで明確にして，対応する証拠としてコードの断片を人手で探索するため，与えられた仕様に対して具体的に探索できる点がよい．

7）コード保証ケースの メタモデルでは SACM よりも単純で，コードもそれに対応するように，式，識別子，ブロックだけに限定した点がよい．

8）コード保証ではどれくらいの規模のコードを対象にするのか/規模は制限していない．大きな規模のコードだと，保証ケースが大きくなる可能性はある．実際には，日々のコーディングには限界がある．IPO（Input Process Output）に対応させた小さなコード部分ごとに，1 ページ程度に収まる保証ケースを作成して確認できる点がよい．

9）オープンソースをビジネスで使おうとするがリスクが怖い．そこで，何を確認すべきかが分かれば，提案手法では，それに基づいて確実にオープンソースのコードを保証できる点がよい．

研究課題 3「保証ケースの客観的なレビュ手法」

【目的】

保証ケースレビュ観点の分類，観点に応じたレビュプロセスの定式化を実施する．

【課題】

既存の保証ケースをレビュする場合，客観的なレビュ手法が明確ではないため，属人的なレビュになりやすいという問題があった．とくに，保証ケースの主張では，「システムが安全である」などのように，日本語文を用いるため，用語関係があいまいになりやすいという問題があった．

【手法】

保証ケースのレビュプロセスを，理解，問題識別，原因分析，欠陥修正から構成し，理解段階で，保証ケースからシステミグラムを作成することにより，システミグラム上で問題識別，原因分析，を客観的に実施できるようにする（図 4）．また，この結果に基づいて，保証ケースの欠陥修正を容易化できる．

ここで，システミグラムは，名詞をノードとし，動詞をノード関係で表現する単純な図式である．システミグラムを用いて，保証ケースを構成する主張を理解することができる．

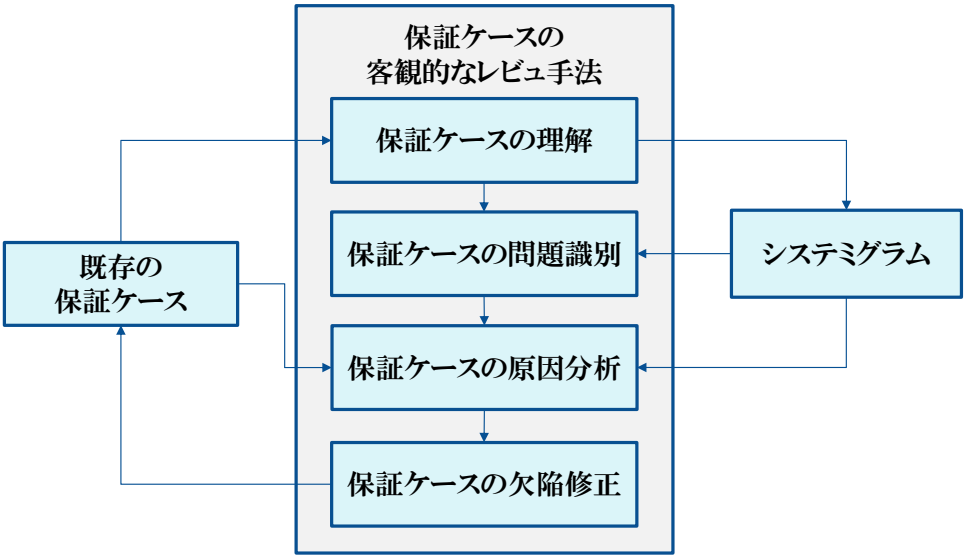


図 4　保証ケースレビュ作成法

【成果】

1）保証ケースに基づくシステミグラムの作成法

2）システミグラムを用いた保証ケースのレビュ指標として，完全性，明確性，適切性，追跡性を定義した．

3）保証ケースのレビュプロセスの指標として，理解率，問題件数，原因分析率，欠陥修正率を定義した．ここで，問題件数は，完全性，明確性，適切性，追跡性の指摘件数の総和である．

【提供成果】

1）保証ケースレビュ手法　（研修教材）

2）保証ケースレビュ指標

3）保証ケースレビュプロセスの指標

【有識者による本研究成果の評価】

1）保証ケースの作成では辞書が必要になることは認識していた．しかし，保証ケースを作成する前にオントロジーを作成しようとすると，プロジェクトごとに必要となるオントロジーの作成自体に手間がかかりすぎてしまい，これまでうまくいかなかった．これに対して，本手法では保証ケースからシステミグラムを用いてオントロジーを作成できる点が効率的でよい．

2）保証ケースとシステミグラムを対応付けるためにシステミグラムの書き方を SPRME（主体 Subject，性質 Property，リスク Risk，対策 Measure，証拠 Evidence）に合わせて限定している点がよい．

3）システミグラムを用いたレビュでは，保証ケースに対するシステミグラムの作成に属人性が出るので，システミグラムへの変換手順を具体化した点がよい．

4）保証ケースだけでは意味的内容をレビュするのが難しいので，システミグラムを活用する点がよい．

研究課題 4「実践的保証ケース教材の試作」

【目的】

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，保証ケースレビュ手法のそれぞれに対する高度な保証ケース研修教材について，ISD 原則に基づいて，教材を試作する．ここで，分析，設計，開発，実施，評価からなるプロセスにより，効果的な教材を設計する手法が ISD（Instructional Systems Design）である．

【課題】

保証ケースに対する統一的な保証ケース作成手法，保証ケースレビュ手法などの先進的な手法については，研修教材がないという問題がある．また，研修教材を開発担当者に対して試行適用することにより，研修の有効性を評価しておく必要がある．

【手法】

研修教材を効率的に開発するため，ISD 原則に基づいて系統的に研修単元を構成するとともに，コースマップを用いて単元間の依存関係を無駄のないように設計した．

教材と，コースマップ，単元の関係を図 5 に示す．各単元では，基本概念，例題，確認問題を用意した．またコース全体の理解を深めるために，グループで議論できるように演習問題を用意した．

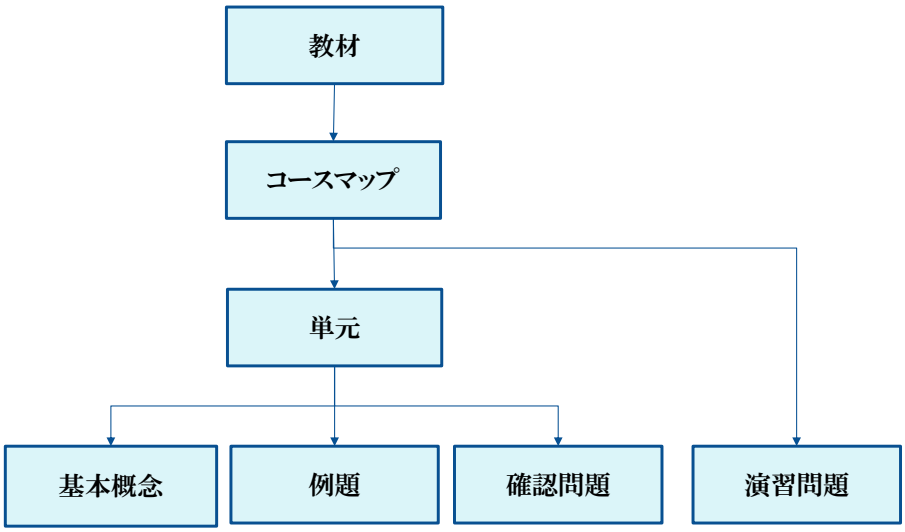


図 5　保証ケース手法研修教材の構成

【成果】

1）統一的保証ケース作成手法の研修教材（114 スライド）を試作した．

2）平均システム開発経験約 7 年の参加者に対して，統一的保証ケース作成手法の研修（4 時間）を実施することにより有効性を確認した．研修参加者の満足度の平均は，95.7%であった．

3）保証ケースレビュ手法の研修教材（82 スライド）を試作した．

4）平均システム開発経験約 7 年の参加者に対して，保証ケースレビュ手法の研修（4 時間）を実施することにより有効性を確認した．研修参加者の満足度の平均は，95.7%であった．

【提供成果】

1）統一的保証ケース作成手法　研修教材

第 1 章	保証ケースを統一的に作成するための基礎知識
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
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
第 3 章	保証ケースによる合意形成
3.1	議論の合意形成

2）保証ケースレビュ手法　研修教材

第 1 章	保証ケースをレビュするための基礎知識
1.1	システム要素の相互関係
1.2	保証ケースの表記法
1.3	主張の問題点
1.4	分解の問題点
1.5	網羅的なレビュ
第 2 章	保証ケースをレビュするための知識・スキル
2.1	システミグラムの表記法
2.2	システミグラムで主張
2.3	システミグラムで分解
2.4	システミグラムで証拠を表現
2.5	保証ケースのレビュ
2.6	保証ケースのレビュ指標
2.7	個人レビュ
第 3 章	保証ケースによる合意形成
3.1	グループレビュ

【有識者による本研究成果の評価】

1）レビュ手法の研修教材をぜひ提供してほしい.

２）今回開発された発展的な保証ケースの応用教材がたくさん出てくるのはいいことだ.

研究課題５　「保証ケース手法の実践的導入適合性」

【目的】

保証ケースの導入を計画している企業担当者へのヒヤリングを実施することにより，研究課題 1，2，3 で研究した保証ケースの効率的な作成手法について，現場ニーズとの適合性を評価する.

【手法】

保証ケース手法を導入する上で，開発組織が必要な準備能力を備えていることを確認するために，IT ケイパビリティの評価指標を参考にして，活用ビジョン，活用コミュニケーション，プロダクトデザイン，プロセスデザイン，投資適正，人材開発について 37 項目を 2 段階（あり：１，なし：０）で評価できる定性評価指標（定性評価 37 項目版）を作成した．また，研究課題１から研究課題 5 について，研究の必要性を 4 段階（大いに必要:3，必要:2，疑問:1，不要:0）で回答するようにアンケートを設計した.

さらに，客観的に導入準備能力を評価するために，以下の 5 段階で各項目を評価できる保証ケース導入準備能力評価指標（客観評価 50 項目版）を作成した.

0：作業として実施する必要があるが，実際には実施していない
1：指示書はなく，口頭で指示して作業を実施している
2：指示を受けて作業を実施している．メモで指示している
3：部門標準の作業マニュアルを整備して，作業を実施している
4：全社標準の作業マニュアルを整備して，作業を実施している
5：作業の変化に応じて，マニュアル類を適切に改善している

【成果】

１）18 組織に対してメールで実施したアンケート結果から，研究の必要性について，統一的保証ケース作成法が 2.67，コード保証ケース作成手法が 2.39，保証ケースレビュ手法が 2.67，保証ケース研修教材が 2.61，保証ケース導入準備能力評価指標が 2.5 となった．この結果，すべての研究課題が必要以上の値であったことから，本受託研究課題には実践的導入適合性があると判断できた.

２）18 組織に対してメールで実施したアンケート結果から，開発組織の保証ケース導入準備能力評価指標（2 段階評価）は図 6 に示すように，平均 22.2% となった．このことから現状では，国内の開発組織への保証ケースの導入は容易ではないことが判明した.

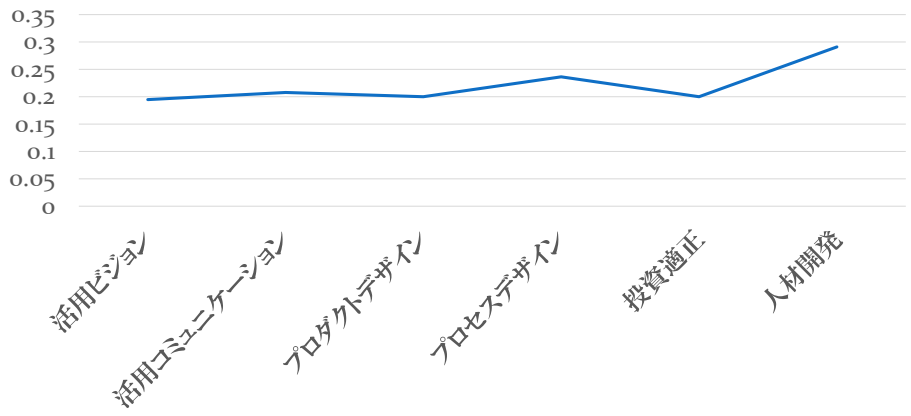


図 6　保証ケース導入能力準備指標（定性評価 37 項目版）の評価結果

3）客観的に導入準備能力を評価するために，保証ケースの導入に積極的な企業 3 社について面談で客観評価 50 項目版を用いて評価した結果，活用ビジョン能力，活用コミュニケーション能力，プロセスデザイン能力，投資的成果能力，保証人材開発能力では，各社間で差があることが判明した．したがって，保証ケースの導入を推進する上で，客観的な指標を用いて導入準備能力を評価することにより，弱点がどこにあるかを明確化できるので，適切な対策を段階的に実施できる可能性があることが明らかになった．

4）保証ケース導入準備能力評価指標として策定した評価指標を，新技術の組織への導入準備能力を測定するために適用できるように，新技術導入準備能力評価指標として一般化した．

【提供成果】

1）保証ケース導入準備能力評価指標（定性評価 37 項目版，客観評価 50 項目版）

2）新技術導入準備能力評価指標（客観評価 50 項目版）

【有識者による本研究成果の評価】

1）保証ケースの導入準備能力指標値を企業横断的に客観評価できるようにした点がよい．

2）開発した導入準備能力を応用して研修効果を測定する能力評価指標もできる可能性がある．

3）現在，ソフトウェア開発人材能力育成プログラムを策定しようとしている．保証ケース導入準備能力評価指標を開発人材育成指標に展開できると考えているので，ぜひ参考にしたい．

研究成果の産業界への展開

研究成果が誰に対してどのような場面で役立つかについてまとめると，以下のようになる．

（1）モデルに基づく保証ケースの統一的作成法

保証ケース作成支援ツールを用いた統一的作成法は，アーキテクチャ品質評価サービスなどに展開できる．具体的には，システム開発者に対して，開発対象システムのアーキテクチャ品質を評価しようとする場面で，保証ケースを開発対象システムのモデルから作成することにより，システムが所望の品質を満たすことを保証する作業に役立つ．

（2）コードに基づく保証ケース作成法

コードに基づく保証ケース作成法は，コードレビュ手法などに展開できる．具体的には，システム開発者に対して，開発対象システムのコードの品質を評価しようとする場面で，コードが実現すべき仕様から保証ケースを作成することにより，コードが所望の機能目標を満たすことを確認するレビュ作業の効率化に役立つ．

（3）保証ケースレビュ手法

保証ケースレビュ手法は SPRME（対象，特性，リスク，対策，証拠）分析に基づく保証ケース作成法（SPRME 法），統一的作成法との統合化手法，保証ケースの全体理解法に展開できる．具体的には，システム分析評価者に対して，開発対象システムの品質を評価しようとする場面で，対象，特性，リスク，対策，証拠を対応付けて明確化することにより，評価すべきシステムに対する保証ケースを系統的に作成することができるので，対象システムが所望の特性を満たすことを保証する作業の効率化に役立つ．

（4）開発技術者向け教育研修教材を作成

開発技術者向け保証ケースの教育研修教材は，第三者機関（DEOS 協会）で認証された教材として展開できる．具体的には，第三者機関で認証された保証ケースの発展教材を求めている担当者に対して，保証ケースの基礎知識を持つ学習者により高度な保証ケースの知識を提供しようとする場面で，統一的保証ケース作成法ならびに保証ケースレビュ手法の教材を用いて，保証ケースの発展知識についての研修教材開発の効率化に役立つ．

（5）保証ケース導入準備能力評価指標

保証ケース導入準備能力評価指標は，指標を用いた保証ケース導入法，形式手法などの新技術の組織への導入能力評価手法，アーキテクチャ品質評価サービスの設計法として展開できる．具体的には，保証ケースを導入しようとしている場面で，その組織の保証ケース導入担当者が，保証ケースの組織への導入を，必要な能力には何があり，どの能力を向上させることで，導入を成功させることができるかを知る上で役立つ．

1 研究の目的・背景と期待される効果

1.1 研究目的とその背景

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．たとえば，自動車分野で導入が必要とされる ISO26262 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．産業界における具体的な課題と関連する研究の動向について，また，それらの中で研究責任者の現時点での貢献状況について，以下に述べる．

(1) 多様なモデルに対する統一的な保証ケース作成手法の必要性

航空宇宙，自動車や医療機器などの高い安全性が要求されるシステムの安全性を保証するために，保証ケースの作成が求められている．システムの安全性を保証するためには，システムを構成するソフトウェアのモデルだけでなく，システムの利用モデルや構造モデルを明らかにすることにより，これらのモデルの安全性を保証ケースで確認する必要がある．これらのモデルには，BPMN(Business Process Modeling Notation)，UML(Unified Modeling Language)や SysML(Systems Modeling Language)など多様なモデルがある．BPMN は業務プロセスをモデル化できるのでシステムの利用・運用プロセスを定義できる．現代のソフトウェア開発で広く普及している UML には，ユースケース図やクラス図，シーケンス図，状態図，アクティビティ図などが含まれる．要求図などにより UML を拡張した SysML は組込みシステム向けに普及してきている．これらの多様なモデルに対して保証ケース作成手法を用意できないと，産業界への保証ケースの適用は進展しない．

保証ケースの作成を容易化するために，アーキテクチャやプロセス構造に基づく保証ケースパターンが報告されている．しかし，多様なモデルに対する統一的な保証ケースの作成手法については明らかになっていない．

これらに対して，研究責任者はネットワーク装置監視システムの保証ケース作成へのアーキテクチャパターン適用評価について研究を進め，国際会議論文を執筆して採録されている．また，保証ケースパターンを，対象分解(15)，参照モデル分解(10)，条件分解(7)，推論分解(4)，証拠分解(11)，再分解(2)に分類して，合計 49 個のパターンを整理した議論分解パターンポケットガイドとして公開している．

(2) 既存コンポーネントに対する保証ケース作成手法の必要性

ソフトウェアコンポーネントを再利用することで，ソフトウェア開発を効率化するだけでなく，開発されたソフトウェアの品質を向上できる可能性がある．この場合，再利用対象コンポーネントの安全性を保証する必要があるため，コンポーネントに対する保証ケースの作成手法が必要である．既存コンポーネントの安全性を保証するには，上述したようなコンポーネントのモデルに対する保証ケースだけでなく，コンポーネントのコードに対する保証ケースが必要である．

現状では，コードに対する保証ケース作成手法は確立されていない．一方，コードの静的解析技術は成熟しており，コンポーネント情報を格納するリポジトリが構築されている．しかし，コード情報に基づいて保証ケースを作成する手法は確立されていない．

これらに対して，研究責任者はプログラムコードに対する静的解析情報の表現方法に関する研究を進めてきた．

(3) 保証ケースの客観的なレビュ手法の必要性

作成された保証ケースの妥当性を確認するためには，保証ケースを適切にレビュする必要がある．保証ケースの具体的なレビュ手法については，保証ケースが正しい構成規則を用いて記述されていることや成果物と保証ケースとの追跡性ならびに網羅性を確認する手法が報告されている．また，主張，証拠などの不完全性や依存性についての定義がある．しかし，保証ケースを構成する主張を記述する用語の適切性や一貫性，主張を下位の主張に分解する際の網羅性，主張に対する証拠の十分性などの観点から，保証ケースの妥当性を内容に踏み込んで客観的に確認するためのレビュ手法は確立されていない．

これらに対して，研究責任者は保証ケースで使用される用語間の関係に基づいて用語関係図を作成する手法ならびに，保証ケースを構成するコンテクストノードと証拠ノードの関係から保証ケースをレビュする手法について研究を進め，国際会議論文も採録されている．

1.2 期待される効果

産業界の課題に対する，設定した研究の期待効果は以下の通りである．

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

多様なモデル図を用いている開発現場に対して統一的な保証ケース作成法を提供できる．

たとえば，ソフトウェア開発・システム開発で作成したモデル図に対して，安全性や妥当性を確認するために保証ケースを作成する場面で，成果を適用することができる．モデル図との一貫性・追跡性が満たされた保証ケースの作成を効率化でき，信頼性や安全性などの品質保証コストを削減できる．

b) コンポーネントに対する保証ケース作成手法の研究

コードとして蓄積された膨大な既存資産に対して保証ケースを作成することができるため，保証ケースによる安全性の保証を効率化できる．

たとえば，ソフトウェア開発・システム開発で作成されたコンポーネントコードを再利用する際に，コンポーネントの安全性や妥当性を確認するために保証ケースを作成する場面で成果を適用することにより，再利用コンポーネントの欠陥検出，信頼性・安全性保証活動を効率化できる．また再利用コンポーネントの信頼性を保証できる．既存リポジトリから獲得した情報に基づいて保証ケースの作成を効率化できる．

c) 保証ケースの客観的なレビュ手法の研究

客観的なレビュ観点とプロセスにより，現場技術者が保証ケースを適切にレビュできるようになることが期待される．

たとえば，完全性，明確性，適切性，追跡性などのレビュ観点に基づいて保証ケースをレビュする場面や，証拠の充足度合いに基づいて保証ケースの充足度合いをレビュする場面で，成果を適用することができる．保証ケースの品質を客観的に確認することができるので，レビュ品質と効率を向上できる．

d) 実践的保証ケース研修教材の試作

国内企業に保証ケース技術を普及させるための，わかりやすく，より実践的な研修教材を提供できる．

たとえば，保証ケースの基礎知識を持つ技術者に対して，多様なモデルに対する統一的な保証ケースの作成手法，コンポーネントに対する保証ケース作成手法ならびに，客観的なレビュ手法を企業が教育しようとする場面で，成果を適用することができる．多様なモデルならびにコンポーネントに対する保証ケースの作成・レビュ知識の習得を効率化できる．

e) 保証ケース手法の実践的適用評価の研究

業界で必要とされる保証ケース手法へのニーズを解明できる．

たとえば，保証ケース手法・研修教材を企業が導入しようとする場面で，保証ケースへのニーズと導入準備能力指標を測定することにより，適切な保証ケース手法と研修教材を選択して活用できる．保証ケースの導入準備能力と保証ケース手法・教材へのニーズとの関係が明確化でき，保証ケースの導入を推進できるようになる．また，保証ケース手法・教材の導入効果が向上する．

2 実施内容

2.1 研究アプローチ

2.1.1 研究の全体像

本研究は，保証ケース作成支援方式に関する研究である（表 2-1）.

具体的には，モデルに基づく保証ケースの統一的作成法，コンポーネントに対する保証ケース作成法，保証ケースの客観的なレビュ手法，実践的保証ケース教材の試作，保証ケース手法の実践的導入適合性について研究する.

本研究により，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，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，保証ケースの実践的なレビュ手法，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，保証ケース手法の実践的適用評価手法の提供を目指すものである.

表 2-1 保証ケース作成支援方式の研究の概要

	研究課題	内容，目標
a	モデルに基づく保証ケースの統一的作成法	モデル図の構造情報に基づいて保証ケースに関する活動プロセスを定式化し，支援ツールを試作することにより，自動化範囲と自動化による改善効果を明確化
b	コードに基づく保証ケース作成法	コードの静的解析情報に基づく，コードに対する保証ケースの作成手法を定式化
c	保証ケースレビュ手法	保証ケースの構成情報に基づき，レビュプロセスを定式化
d	開発技術者向け教育研修教材を作成	定式化した保証ケース作成・レビュ手法に基づき，開発技術者向け研修教材作成・研修実施・有効性確認
e	保証ケース導入準備能力評価指標	保証ケースの導入計画企業担当者へのヒヤリングを実施，保証ケースの導入可能性を評価

2.1.2 関連するこれまでの研究について

保証ケースの研究動向について述べ，その後，設定した各研究目標に関連する研究分野について述べる．なお，以下で説明する研究のうち，研究責任者が当該委託研究以前に実施していた研究は，保証ケースの分解パターンについての研究と，前提と証拠の関係から GSN を作成する研究，GSN から用語関係図を作成する研究，システミグラムから安全性ケースを作成する研究である．これらは当該委託研究とは直接関係しない.

保証ケースの研究動向をまとめると以下のようである．システムの安全性を確認するために，安全性ケース(Safety case)，保証ケース（Assurance case，アシュアランスケース）やディペンダビリティケース（Dependability case）が注目されている．このため GSN(Goal Structuring Notation)[1][2][3]を用いてこれらを記述する方法が提案されている.

しかし，実際のシステム開発プロジェクトの担当者による保証ケースの作成を容易化するためには，エディタを提供するだけでは不十分である．システム開発プロセスやシステム開発文書に即して，より具体的な保証ケース作成手順を提供する必要がある.

重要システムの実行中に優先順位の高い要求を満足することを確認するために，ディペンダビリティケースが必要とされている[4].

保証ケースでは，ゴール（主張），戦略，前提（コンテクスト），根拠（証跡，ソリューション）によって，システムのディペンダビリティに関する議論を構造化して確認することができる．このため，保証ケースの関連研究として，安全性ケースやディペンダビリティケースについて以下のような手法が研究開発されている．

GSN を作成するために，①ゴールを識別する，②ゴールを記述するための基礎を定義する，③ゴールを満足させるための戦略を識別する，④戦略を記述するための基礎を定義する，⑤戦略を吟味する，⑥基本的な証跡を識別するという 6 段階の手法を Kelly が提案している[1][2].

European Organisation for the Safety of Air Navigation が制定している安全性ケース開発マニュアル[5]では，安全性ケースのコンテクストを定義することが重要であると指摘している．また安全性ケースをレビュするためのチェックリストを提案している．

複数のシステムから構成されるシステム（System of Systems）の開発過程で，システム分析，ゴール要求抽出，代替設計案の識別，矛盾点の解消からなる保証ケースを構造化して作成する手法が提案されている[6].

保証ケースを作成する際に必要となる議論分解の観点として，システム構成や機能構成，属性構成などが整理されている[7].

DEOS プロジェクトではディペンダビリティケースに基づいてオープンシステムの障害対応サイクルと変化対応サイクルを支援する研究を推進している[8]．このためディペンダビリティケースを編集できる D-Case エディタが開発された[9].

2012 年 6 月にボストンで開催されたディペンダブルシステムとネットワーク国際会議(Dependable Systems and Networks DSN2012)では，概念文書，設計書，運用手順書，準備ハザードリストに基づいて安全性ケースを作成する手法が提案されている[10].

これらの手法では，多様な適用分野や開発工程を対象として保証ケースの作成法が個別的に提案されている．しかし，保証ケースを用いて実際のシステムがディペンダブルであることを確認するためには，システム開発プロセスや工程生産物との具体的な対応関係や利用手順が一貫した形で明確になっている必要がある．しかし，具体的な工程生産物に基づく保証ケースの作成法は提示されてはいない．

上述したことから，システム開発運用工程生産物を用いた保証ケースの作成手順の具体化が必要である．この理由は，上述したように，保証ケースの作成手順が，断片的な取り組みにとどまっており，システム開発プロセスや工程生産物を利用する系統的な手順が明確になっていなかったからである．

また故障解析（FTA）や FMEA 分析，Hazard 分析などのリスク分析技術がある．前述したように逸脱分析を用いて保証ケースを作成する手法[11][12]も提案されている．しかし，開発運用プロセス全体を通じた保証ケースとリスク分析の具体的な適用関係は必ずしも明確になってはいない．

したがって対象となるシステムに対する統一的な分析手法として確立されてはいないという問題があった．また，保証ケースが前提とする「証跡に基づく論理的な議論による妥当性の論証」という考え方は，日本の文化にはなじまないところがある．この理由は，このよ

うな論証の基礎的な訓練が日本では不足しているからである．これは，これまで数年にわたってGSNを技術者に教育してきた筆者らの経験に基づく仮説である．逆にいえば，論証についての知識とスキルがあれば，保証ケースを作成することは難しいことではないともいえる．

このため保証ケースを開発者が作成しようとすると，なにを論証すべきか，どのように論証すべきか，なにが証跡なのか分からず初心者が躓くことになる．たとえば，Kellyによる6段階作成法[13]の最初でゴールを識別するところから悩むことになる．

したがって保証ケースを記述するためにGSNの構文を教えただけでは，論証に慣れていない日本の現場における技術者が保証ケースを作成することは困難である．このため，欧米で開発されてきた保証ケースの作成手法よりも具体的な適用対象に特化した，より実践的な手法が日本の開発現場では必要になる[14]．

主張を戦略によって分解する際の観点や，分解の順序についての指針が明確に整理されていなかったために，どのように論証を展開すべきかが分からないという問題があった．このため，前述したように議論分解の観点として，システム構成(Architecture)，機能構成(functional)，属性構成(set of attributes)，帰納分解(infinite set)，要求やリスクの完全集合(complete)，単調分解(monotonic)，具体化(concretion)が示されている[7]．しかし，Bloomfieldの観点では，具体的な分析・設計モデルに基づく保証ケースの議論分解が考慮されていない．

保証ケースと多様なシステム開発モデルの関係では，モデルとコンテクストや証跡との対応付けが具体的ではないため，複数のモデルと複数の保証ケースが集合レベルで対応しているとされているだけであった．このため，要素単位での具体的な関係が不明確だった．したがってシステム開発モデルにある貴重な情報が十分活用できないという問題があった．

もし，このような既存の開発モデル情報を活用できれば保証ケース作成効率と品質を向上できる．一方，この過程で保証ケースを適切に作成できなければ開発モデル情報の品質が低いことになるので，システムや開発モデルの品質もまた向上できない．システムに対するディペンダビリティを確認するためには，開発モデルと保証ケースを適切に連携させた手法を開発することが望ましい．このような手法を用いることにより保証ケースの作成を容易化できるだけでなくシステム開発モデルの品質を向上でき，最終的にはシステム自体の品質を向上できる．

Kellyは，4段階の保証ケースレビュ手法を提案している[15]．保証ケースレビュでは，まず，①議論構造を理解し，次いで②議論構造について構造面から問題がないことを確認する．さらに，③議論状況について十分性とともに，議論の完全性を確認する．最後に，④議論の批評と反論を確認する．このKellyの段階的レビュ手法では，十分性と完全性の段階だけが反復するプロセスになっている．

また，Kellyは網羅性，独立性，限定性，直接性，関連性，頑健性という6特性を議論が持つ必要があるとしている．

GSNのコンテクストと証拠の関係を行列（context evidence matrix，CEM）で表現することにより，GSNをレビュする手法が提案されている[16]．この手法では，GSNからCEMを作成することにより，異なるGSN間の等価性や包含関係を確認することができる．

松村ら[17]は，GSN の一種である D-Case から用語関係図(word relationship diagram, WRD)を導出する手法を提案した．WRD では，D-Case の主張，戦略，前提，証拠から用語とその関係を抽出する規則を提案している．これにより，D-Case の用語を明確化できることを明らかにした．

また，松村ら[18]は GSN の前提条件の依存関係を記述できる行列(Context Dependency Matrix, CDM) に基づいて,GSN のノード名と構造を系統的に作成する手法を提案している．

Boadman は，システムモデル図が自然言語表現と対応しやすいことに着目して，より明確に自然言語による文章と対応する図式として，システミグラムを提案した[19][20][21][22]．システミグラムでは名詞句をノードとし，名詞句間の関係を示す動詞句によりノード間の関係を定義する．

システミグラムの起源は，Checkland によるソフトシステム方法論 (SSM) [23]で用いられたシステムモデル図にある.複雑な人間活動を分析するために考案された方法論が SSM である．

システミグラムは複雑なシステムを記述する手法として広く適用されている．たとえば，システム工学で注目されている 7 人の侍モデル[24]をシステミグラムで自然に表現できる[25]．

またシステミグラムを編集するツールも公開されている[26]．

システム安全性の状況をシステミグラムで分析した結果に基づいて，対象システムに対する安全性ケースを作成する方法が提案されている[27]．

保証ケースの議論分解構造をパターン化しておくことで，保証ケースの適用を容易化できる．たとえば，システム構成，品質特性の構成，リスクの構成などに基づいて，上位の主張を下位の主張に分解することができる．このとき，分解の網羅性を説明するために，これらの構成情報を分解の前提として記述する．

2.1.3 研究目標と研究課題

(1) 研究目標

本研究では，多様なモデルに対する統一的な保証ケース作成手法，既存コンポーネントに対する保証ケース作成手法，保証ケースの客観的なレビュ手法をそれぞれ研究目標に設定するとともに，これらの手法を適切に開発技術者に教育するための研修教材等の研究と，これらの手法および教材が現場ニーズに適合していることについても研究する．

以下に設定する研究目標とその概要について述べる．

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

対象ソフトウェアのモデル記述に基づく保証ケース作成プロセスの定式化，ツール試作による評価を実施する．

【目標設定理由】

多様なモデルごとに，対応する保証ケースの分解パターンを用意するのは効率的ではないから．

【産業界の課題と研究目標との関係】

多様なモデル図を用いている開発現場に対して統一的な保証ケース作成法を提供できる．

b) コンポーネントに対する保証ケース作成手法の研究

リポジトリに格納される静的情報と保証ケースの構成要素との関係の明確化と，それに基づく既存コンポーネントに対する保証ケース作成手法の具体化を実施する．

【目標設定理由】

既存システムの場合，対応するモデルが存在しない場合がある．この場合，モデルに対して保証ケースを作成する手法だけでは，このような多くの場合に対応できないから．

【産業界の課題と研究目標との関係】

コードとして蓄積された膨大な既存資産に対して保証ケースを作成することができるため，保証ケースによる安全性の保証を効率化できる．

c) 保証ケースの客観的なレビュ手法の研究

レビュ観点の分類，観点に応じたレビュプロセスの定式化を実施する．

【目標設定理由】

保証ケースの導入初期段階では，保証ケースに習熟していない技術者が保証ケースを書くことが多くなる．このため，適切な保証ケースのレビュ手法が必要であるから．

【産業界の課題と研究目標との関係】

客観的なレビュ観点とプロセスにより，現場技術者が保証ケースを適切にレビュできるようになることが期待される．

d) 実践的保証ケース研修教材の試作

上記 a)に係る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，b)に係る既存コンポーネント情報に基づく保証ケース作成手法，c)に係る保証ケースレビュ手法のそれぞれに対する高度な保証ケース研修教材について研究し，教材を試作する．

【目標設定理由】

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から．

【産業界の課題と研究目標との関係】

国内企業に保証ケース技術を普及させるための，わかりやすく，より実践的な研修教材を提供できる．

e) 保証ケース手法の実践的適用評価の研究

保証ケースの導入を計画している企業担当者へのヒヤリングを実施することにより，a)ならびに b)，c)で研究した保証ケースの効率的な作成・レビュ手法・研修教材について，現場ニーズとの適合性を評価する．

【目標設定理由】

保証ケースの導入にあたって，どのような知識が組織に具備されているかが，導入を成功させる上で重要になると考えられるから．

【産業界の課題と研究目標との関係】

業界で必要とされる保証ケース手法へのニーズを解明できる．

(2) 研究目標に向けた研究課題の設定

本研究の成果の具体的な内容について，まず，研究のアプローチ方法を述べ，次いで研究目標毎に述べる．

【研究のアプローチ方法】

［手法の定式化］

保証ケースに関する活動プロセスを，モデル図の構造情報やコンポーネントの静的解析情報などに基づいて保証ケースの作成手法を定式化する．また，保証ケースのレビュについては，保証ケースの構成情報に基づいて，レビュプロセスを定式化する．また，これらの手法に基づいて支援ツールを試作することにより，自動化範囲と自動化による改善効果を明確化する．

［教材試作］

定式化した保証ケース作成・レビュ手法に基づいて，開発技術者向けに教育研修教材を試作するとともに，試作教材を使用した手法研修を実施し，手法の有効性を確認するとともに，教材や研修の改善点を識別する．

［実証評価］

保証ケースの導入を計画している企業担当者へのヒヤリングを実施することにより，保証ケースの効率的な作成・レビュ手法・研修教材について，実践的な例題に基づいて手法・教材の利用効果を説明することにより，現場ニーズとの適合性を評価する．とくに，保証ケース導入についてのヒヤリング企業の成熟度を指標化することにより，客観的な適合性評価を実施する．

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・システム開発で使用するモデル図の種類ごとに構成要素とその関係の構造を定義しておくことにより，与えられた具体的なモデル図の構成要素と関係から，モデル図に対応する保証ケースを統一的に作成する手法を提供し，その支援ツールを開発する．

【課題設定理由】

任意のモデルが，構成要素とその関係に基づいて定義されることから，このモデル定義に対して保証ケースを作成する方法とその支援ツールを実現することにより，任意のモデルに対する保証ケースを統一的に生成できるから．また，これにより，モデルごとに保証ケースのパターンを開発する作業を不要にできるから．

b) コンポーネントに対する保証ケース作成手法の研究

リポジトリ情報に対応する保証ケースのメタモデルを定義しておくことにより，ソフトウェア開発・システム開発でプログラムコードとして実装されるコンポーネントを解析してリポジトリに格納される制御フローやデータフローなどの情報から，コンポーネントに対する保証ケースを効率的に作成する手法を提供する．

【課題設定理由】

コンポーネントのコードに対する保証手法の有効性を明らかにするためには，保証方法を定式化することと，コードの情報と対応付けて保証ケースの情報を管理するためのメタモデルが必要であること，ならびに，考案した手法の有効性を確認するためには実証実験が必要になるから．

c) 保証ケースの客観的なレビュ手法の研究

保証ケースの構成要素と用語関係に基づいて，定式化された完全性，明確性，適切性，追跡性などのレビュ観点と，それを確認するためのレビュ規則・手順からなるレビュ手法を提供する．

【課題設定理由】

保証ケースのレビュ手法を明らかにするためには，レビュ手法を定式化することと，レビュ手法の有効性を確認する評価実験が必要になるから．

d) 実践的保証ケース研修教材の試作

多様なモデルに対する統一的な保証ケース作成手法，保証ケースの客観的なレビュ手法に関して ISD 原則（Instructional System Design Principle，教育システム設計原則）に基づいて試作した研修教材を提供する．

【課題設定理由】

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から．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から．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だから．

e) 保証ケース手法の実践的適用評価の研究

保証ケースを企業へ導入するための技術面と管理面からなる準備能力を評価する指標を提示する．ヒヤリングによる保証ケース作成手法および実践的保証ケース研修教材に対するニーズを提示する．保証ケース作成手法および実践的保証ケース研修教材の適合性を客観的に評価する手法を提供する．

【課題設定理由】

組織の技術的な成熟度が高くなければ，保証ケースのような新技術を組織に導入することは困難だから，組織の成熟度を評価する指標の開発が必要である．また，開発した評価指標を適用評価しなければ指標の有効性が判断できないから．さらに，保証ケースを導入しようとする企業の受託研究テーマに対するニーズを明らかにする必要があるから．

2.2 研究の活動実績・経緯

本研究の活動実績および経緯について述べる．表 2-2 に研究実施実績を示す．

表 2-2 研究実施実績

作業項目		6月	7月	8月	9月	10月	11月	12月	1月	2月	進捗状況
a①保証ケース統一作成手順の定式化	予	→	→								完了
	実	→	→								
a②保証ケース作成支援ツールの試作	予			→	→	→	→	→			完了
	実			→	→	→	→	→			
a③ツールに基づく保証ケース作成実験	予							→	→		完了
	実							→	→		
b①コード保証ケース作成手順の定式化	予	→	→	→							完了
	実	→	→	→							
b②保証ケースメタモデルの具体化	予				→	→	→				完了
	実				→	→	→				
b③コンポーネント保証ケース作成実験	予							→	→		完了
	実						→	→			
c①レビュ観点・規則・手順の定式化	予	→	→	→							完了
	実	→	→	→							
c②保証ケースレビュ指標の定式化	予				→	→	→				完了
	実				→	→	→				
c③保証ケースレビュ実験	予							→	→		完了
	実							→	→		
d①ISD原則に基づく研修教材設計	予			→	→	→					完了
	実		→	→	→						
d②研修教材開発	予				→	→	→	→			完了
	実				→	→	→	→			
d③教材に基づく研修実験	予							→	→		完了
	実							→	→		
e①導入準備能力指標設計	予	→	→	→							完了
	実	→	→	→							
e②ヒヤリング項目設計	予				→	→	→				完了
	実				→	→	→				
e③ヒヤリング評価実施	予							→	→		完了
	実							→	→		
f①保証ケース統一作成ツール試作	予				→	→	→	→			完了
	実				→	→	→	→			
f②保証ケース研修教材試作	予				→	→	→	→	→		完了
	実				→	→	→	→	→		
f③保証ケース研修印刷	予					→			→		完了
	実					→			→		

作業グループごとに研究を実施し，約 2 週間ごとに開催した進捗会議で，研究状況を管理した．以下に，月ごとの主な研究活動実績を整理する．

【6 月】

（1）モデル M を構成要素の集合 E とその関係 R に基づいて，ゴールをアーキテクチャ分解することにより保証ケースを統一的に作成する手順の定式化に着手した．

（2）コードに基づいて保証ケースを作成する手順としてコードの入力に着目する方法を着想した．また，SSL のハンドシェイクを例題として保証ケースを検討した．

（3）レビュ観点・規則・手順の定式化では，保証ケースレビュを①構造の確認，②証拠の完全性の確認，③主張分解の完全性の確認から構成するとともに，保証ケースレビュのための保証ケースを作成した．

（４）ISD 原則に基づく研修教材設計の検討に 8 月から着手するため，ISD 原則に基づく教材作成法を調査した.

（５）導入準備能力指標の設計では，カロンによる問題識別,関係構築,展開戦略,継続管理という技術受容プロセスを用いて，導入準備能力と組み合わせることで能力プロセスマトリクスを考案し，SS2015 の D-Case WG で有効性について意見交換した．導入準備能力指標に基づく，ヒヤリング調査票の作成に着手した.

【７月】

（１）保証ケース統一作成手順の定式化

対象成果物モデルに基づく保証ケース作成手順を明確化し，論文「Assuredness through ArchiMate」を投稿した．また，外注仕様書の作成に着手した．まず，モデル定義言語の仕様を検討し，XML による構文案を作成した．また，試作システムの構成を定義した.

（２）コード作成手順の定式化

OpenSSL の既知の脆弱性として，ハードブリードの原因であるハートビートの処理（メッセージ長 1000 の指定によって内部記憶を抜き取る）保証ケースを検討した.

（３）レビュ観点・規則・手順の定式化

保証ケースレビュを①構造の確認，②証拠の完全性の確認，③主張分解の完全性の確認から構成するとともに，保証ケースレビュのための保証ケースを作成した．また用語関係を図式化するワードグラム（システミグラムを保証ケース表現できるようにカスタマイズした図式）を考案し，電気ポット問題に対して保証ケースと対応するワードグラムを作成した.

（４）ISD 原則に基づく研修教材設計

統一的保証ケース作成手法の研修項目を定義し，コースマップの設計に着手した.

（５）導入準備能力指標設計

IT ケイパビリティについてのチェックリストを参考にして，1)保証ケース構築基礎能力，2)リスク分析能力，3)保証ケース活用ビジョン構築能力，4)保証ケース活用コミュニケーション能力，5)プロダクトデザイン能力，6)プロセスデザイン能力，7)保証ケース投資適正能力，8)システム保証人材開発能力からなる 8 個の次元に基づく導入準備能力指標を設計した.

（６）有識者からのアドバイス

企業有識者 3 名，大学有識者 3 名を訪問し，受託研究に対するアドバイス会議 5 件を実施した.

【８月】

（１）保証ケース統一作成手順とツールの試作

保証ケース統一作成手順の定式化を完了した．研究会論文「モデルに基づく統一的保証ケース作成手法の提案」を執筆して投稿した.

保証ケース統一作成ツールの外注仕様書を作成して，3 社見積もりを完了するとともに外注先を決定し，発注手続きを実施した.

（２）コード保証ケース作成手順の定式化

入出力仕様に基づき，所望の入出力条件に対応するコードが存在することを確認するという方針に基づく保証ケース作成手順を定式化した．

また，メタモデルを作成するために，SACM のリポジトリを調査した

（３）レビュ観点・規則・手順の定式化

論文「Argument Situation Analysis by Systemigram」を作成し，AAA2015 に投稿した．また，研究会論文「構成情報に基づく保証ケースレビュ手法の提案」を執筆し，投稿した．

（４）ISD 原則に基づく研修教材設計

統一的保証ケース教材の外注仕様書を作成した．

（５）導入準備能力指標設計

導入準備能力指標 8 次元に基づき，合計 50 項目からなる指標を策定した．また，この 50 項目からヒヤリング項目（37 個）を作成した．さらにヒヤリング候補リストを作成し，メールによるヒヤリングを開始した．

（６）有識者からのアドバイス

企業有識者 1 名，大学有識者 1 名を訪問し，受託研究に対するアドバイス会議 2 件を実施した．

【９月】

（１）保証ケース作成支援ツールの試作

保証ケース統一作成ツールの試作に着手し，要件定義ならびに基本設計，詳細設計を完了した．

（２）保証ケースメタモデルの具体化

KBSE 研究会論文「入力分析に基づくコード保証方法の提案」の申込み，執筆を完了した．

（３）保証ケースレビュ指標の定式化

保証ケースレビュ実験データ準備として，被験者 2 名により 14 件の GSN のレビュを個別に実施した．この結果，レビュ指標として，表現，分解，前提，未定義からなる指標を考案した．

（４）ISD 原則に基づく研修教材設計

外注仕様書に対する SEC コメントを反映して，3 社見積もりすることにより，外注先を決定し契約手続きを完了した．また，13 項目からなる教材単位の構成を確認した．

（５）ヒヤリング項目設計・実施

導入準備能力評価指標のヒヤリング対象者からの回答を集計した．

【１０月】

（１）保証ケース作成支援ツールの試作

保証ケース統一作成ツールの製造と試験を完了し V0.5 のプロジェクト作成機能，主張分解機能，重み編集機能を確認した．

（２）コード保証ケースメタモデルの具体化

KBSE 研究会論文「入力分析に基づくコード保証方法の提案」の発表を完了した．また，保証ケースリポジトリのメタモデルを具体化するため，SACM のリポジトリを調査した．

（３）保証ケースレビュ指標の定式化

保証ケースレビュ実験データ準備として，被験者 2 名により 14 件の GSN の個別レビュ結果についてレビュ指標を計測することにより，共通点と差異点の分析に着手した．

（４）ISD 原則に基づく研修教材設計

外注仕様書に基づき，13 項目からなる教材単位について研修教材の外注を実施するとともに，内容を確認した．

（５）ヒヤリング項目設計・実施

導入準備能力評価指標のヒヤリング対象者からの回答をパターン分類することとした．

【１１月】

（１）保証ケース作成支援ツールの試作

保証ケース統一作成ツール V0.9 の製造と試験を完了し，プロジェクト保存機能と XMI 出力機能を確認した．

（２）コード保証ケースメタモデルの具体化

主張，前提，証拠，要説明証拠ならびに，コードの静的解析で抽出できる識別子，式，ブロックからなる，コード保証ケースのためのメタモデルを定義した．

SSL に対するオープンソースのコードの脆弱性を確認するための保証ケース作成実験の結果をまとめた．

（３）保証ケースレビュ指標の定式化

保証ケースのレビュ指摘結果で得られた項目を，表記誤り，前提誤り，分解誤り，前提表現誤り，証拠表現誤り，主張表現誤り，未定義用語に分類し，レビュ担当者の差異の影響を分析した．

（４）ISD 原則に基づく研修教材設計

統一的保証ケース教材についての研修 2 回（11/6,13）を実施した．

（５）ヒヤリング項目設計・実施

導入準備能力評価指標のヒヤリング対象者からの回答集計結果の類型を成熟型，発展型，特化型，萌芽型，未熟型に分類した．

【１２月】

（１）保証ケース作成支援ツールの試作

保証ケース統一作成ツール V1.0 の製造と試験を完了し，納品を確認した．また，ツールを用いた評価実験を実施した．

（２）コード保証ケースの拡張法の検討

コンポーネント保証ケース作成実験の結果を整理することにより，入力条件だけでなく，入出力条件に対して提案手法が拡張できる見通しを得た．

（３）保証ケースレビュ実験

システミグラムを用いて保証ケースをレビュする実験を実施した．これにより，保証ケースからシステミグラムを作成する手順を明らかにした．

（４）ISD 原則に基づく研修教材設計

保証ケースレビュ手法の研修項目を定義し，コースマップの設計を完了するとともに，保証ケースレビュ手法教材の外注仕様書を作成した．外注仕様書に対する SEC コメントを反

映して，3 社見積もりすることにより，外注先を決定し契約手続きを完了した．さらに，13 項目からなる教材単位の構成を確認した．

（５）ヒヤリング項目設計・実施

導入準備能力評価指標 50 項目について，5 段階評価手法に基づいて，対面ヒヤリング(2 回)を実施し，5 段階評価手法の妥当性を確認した．

（６）有識者からのアドバイス

企業有識者 3 名，大学有識者 1 名を訪問し，受託研究に対するアドバイス会議 4 件を実施した．

【１月】

（１）ツールに基づく保証ケース作成実験

ツールを用いた評価実験の結果を整理した．これにより，ツール利用によって保証ケース作成作業を 5 倍以上効率化できることを明らかにした．

（２）保証ケースレビュ実験

システミグラムを用いて保証ケースをレビュする実験結果を分析することにより，完全性，明確性，適切性，追跡性に関する指摘を抽出できることを明らかにした．

（３）ISD 原則に基づく研修運営実施

保証ケースレビュ手法の研修 2 回（1/18,22）を実施した．これにより，研修内容の妥当性を確認した．

（４）ヒヤリング項目設計・実施

導入準備能力評価指標 50 項目について，5 段階評価手法に基づいて，対面ヒヤリング(1 回)を実施し，5 段階評価手法の妥当性を確認した．

（５）最終報告

本受託研究について，IPA SEC で最終報告を実施した．

（６）有識者からのアドバイス

企業有識者 1 名，大学有識者 2 名を訪問し，受託研究に対するアドバイス会議 3 件を実施した．

◆学会参加状況

研究期間を通じて，国内外で開催されたシンポジウムや国際会議に積極的に参加し，研究動向調査や技術動向調査を実施した．以下では参加した学会と時期について述べる．

【会議名：ソフトウェア・シンポジウム2013(SS2013)】
期間：2015年6月15-17日

【会議名：TOG(The Open Group)国際会議　ボルチモア】
期間 2015.7.20-22

【会議名：ICITCS国際会議(5th International Conference on IT Convergence and Security)】

期間 2015.8.23-27

【会議名：ESEC/FSE2015(Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering)】
期間 2015.8.31-9/3

【会議名：SafeComp2015】
期間 2015.9.22-24

【会議名：TOG(The Open Group)国際会議　ボルチモア】
期間 2015.10.19-21

【会議名：AAA2015(2nd International Workshop on Argument for Agreement and Assurance)】
期間　2015 年 11 月 17 日

公表した研究成果について以下に列挙する.

[1] Shuichiro Yamamoto, A Generic Assurance case development method, TOG Baltimore 2015
【発表内容】委託研究で採用した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に対して適用評価した.

[2] Shuichiro Yamamoto, Assuring Security through Attribute GSN, ICITCS 2015, pp.1-5, 2015
【発表内容】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.

[3] Shuichiro Yamamoto, An approach to assure Dependability through ArchiMate, Assure 2015, pp. 50-61
【発表内容】委託研究で採用した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.

[4] Shuichiro Yamamoto, A Capability Index for introducing Assurance case, TOG Edinburgh 2015
【発表内容】委託研究で採用した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.

[5] 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
【発表内容】委託研究で採用した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.

[6] 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

【発表内容】委託研究で採用した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．

[7] 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

【発表内容】委託研究で考案した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．

[8] 山本修一郎，要求リスクコミュニケーション， KBSE 研究会，KBSE2015-37，pp.7-12，2015

【発表内容】委託研究で採用した要求リスクを，要求ならびに要求間の関係の抜け・誤りととらえることで，要求リスクを識別して，それを解消する対策を確認する保証ケースによりリスク対策できていることを説明するレビュ手法の有効性を評価した．

[9] Shuichiro Yamamoto，An assurance case review method using Systemigram，AAA2015

【発表内容】委託研究で採用した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評価した．

2.3 研究実施体制

研究実施体制を図 2-1 に示す．また，研究責任者のプロフィールを表 2-3 に示す．

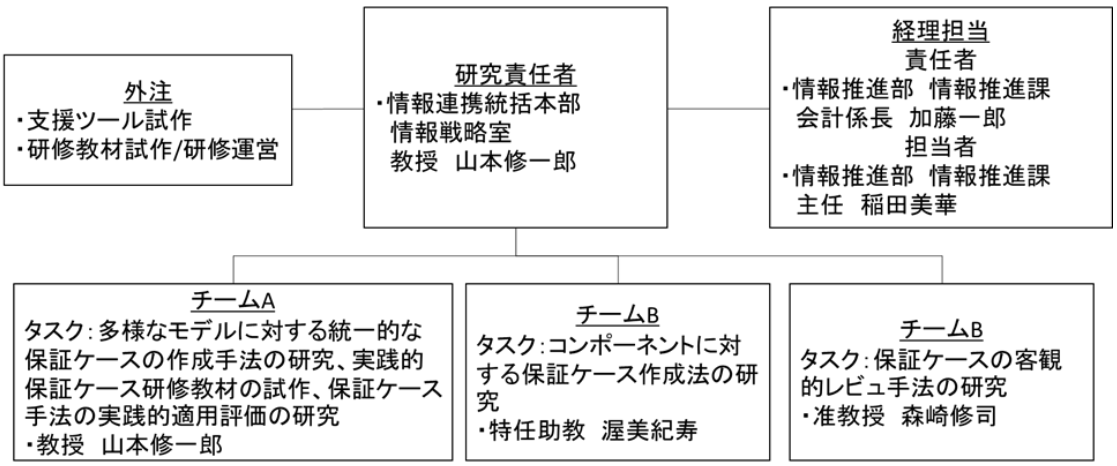


図 2-1　研究実施体制

研究者メンバーのプロフィールは，森崎修司　准教授（保証ケースレビュ方式担当），渥美紀寿　特任助教（コード保証ケース作成方式担当）である．

学生アルバイト 4 名の内訳は，モデルに基づく保証ケース作成方式の評価実験　1 名，コードに基づく保証ケース作成評価実験　1 名，保証ケースの客観的レビュ方式の評価実験 2 名である．

保証ケース作成支援ツールならびに，研修教材の開発と運営について外注を実施した．

保証ケース作成支援ツールの外注では，基本・詳細設計および設計書の作成，ツールの実装，テストおよびテスト報告書ならびに，操作説明書を作成した．

研修教材の開発と運営では，統一的保証ケース作成法と保証ケースレビュ手法について教材を開発するとともに，各 2 回の研修の運営を実施した．

外注先と担当内容は以下のようである．

統一的保証ケース作成支援ツール試作　株式会社　チェンジビジョン

保証ケース研修教材の試作と研修運営　株式会社　NTT データユニバーシティ

表 2-3　研究責任者のプロフィール

（ふりがな） 氏　名	やまもと しゅういちろう 山本　修一郎
生年月日	1954 年　5　月　29　日
所属機関	国立大学法人名古屋大学
所属（部署名）	情報連携統括本部 情報戦略室
役　職	教授
住　所	〒464-8601 愛知県名古屋市千種区不老町 1 番
TEL	052 747 6532
E-mail	yamamotosui@icts.nagoya-u.ac.jp

【学歴（大学卒業以降）】	【職歴】
1977.3.31 名古屋工業大学情報工学科卒業 1979.3.31 名古屋大学大学院工学研究科情報工学専攻修了 2000.10.18 名古屋大学 博士（工学）	1979 日本電信電話公社入社 2002 NTT データ技術開発本部副本部長 2007 NTT データシステム科学研究所所長 2009 名古屋大学 情報連携統括本部 教授

【研究実績】

NTT ソフトウェア研究所において分散型開発支援環境 SoftDA を実用化し NTT ソフトウェアによって商用化された．また SoftDA によるソフトウェア開発手法の研修教材を作成し，ソフトウェア開発プロジェクトへの普及を推進した．さらに，クライアントサーバシステム構築技術の研究・開発に取り組み，トランザクション処理モニタ VGUIDE を実用化した．VGUIDE は，1000 以上のクライアントを収容する通信サービス支援システムや NTT 全国約 200 支店 3000 端末で同時利用されるヘルプデスクサービスなど，高性能が要求される 25 以上の NTT 社内システムに導入された．さらに，Web ブラウザをクライアントとして VGUIDE の TP モニタと連携できる高性能 Web データベース連携ミドルウェア WebBASE を 1995 年に世界で初めて実用化した（情処学会業績賞）．WebBASE は，1996 年当時日本で最大級の検索エンジン NTT Directory の実用化に貢献するとともに国内の多数のイントラネット構築で活用された．さらに，IC カード用多目的 AP 管理 OS を開発しオンデマンドで IC カード AP をセキュアにダウンロードできる運用管理システム NICE を実用化した（信学会業績賞）．

NTT データで，IC カードによる VPN 実現方式[1]や要求工学について研究した[2,3]．

名古屋大学で，Assurance Case によるシステム保証技術の研究を実施した[4-6]．

【主な論文・著書】

[1] オンデマンド VPN システムの実装と評価，情処論誌，Vol.47, No.8, pp.2371-2383, 2006
[2] ゴールマネジメントフレームワークの提案と考察，情処論誌，Vol.49 No.8, pp.2843-2850,2008
[3] Proposal for Requirement Validation Criteria and Method based on Actor Interaction, IEICE TRANSACTIONS on Information and Systems, Vol.E93-D, No.4, pp.679-692, 2010.12
[4] An Evaluation of Assuring Test Case Sufficiency using A D-Case Pattern, WOSD2014
[5] Argument Algebra: A Formalization of Assurance Case Development, JCKBSE2014
[6] An Evaluation of Argument Patterns to Reduce Pitfalls of Applying Assurance Case, Assure 2013

3 研究成果

3.1 研究課題１「モデルに基づく保証ケースの統一的作成法」

3.1.1 当初の想定

(1) 研究内容

異なるモデルに対して統一的な保証ケースの作成法を考案するとともに，この作成法に基づき保証ケース作成支援ツールを試作する．保証ケース作成支援ツールでは，保証ケース編集機能を持ち，指定されたモデルの構造に基づき，対応する保証ケースを半自動的に生成する．また，試作ツールを用いた保証ケース作成実験により，有効性を評価する．

(2) 想定問題と対応策

想定される問題点としては，多様なモデル図を統一的に表現する方法を考案することがある．このため，BPMN や UML，SysML などの多様なモデル図に対して，統一的な方法で保証ケースを作成する手法を明らかにする．モデル図の一般構造は，構成要素と構成要素間の関係である．このため，モデル図の構成要素と構成要素間関係の型とそのインスタンスについて網羅的に安全性やセキュリティを保証するための階層的な保証ケースを作成する手順（「統一手順」と呼ぶ）を具体化することができる．このように，モデル図ごとに，構成要素と構成要素間関係の型を定義しておくことにより，具体的なモデル図に対して保証ケースを自動的に作成できる．本研究課題に対する問題設定と解決策の妥当性について大学ならびに企業の有識者からのアドバイス評価を実施する．

3.1.2 研究プロセスと成果

(1) 研究プロセス

①保証ケース統一作成手順の定式化

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５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．

②保証ケース作成支援ツールの試作

モデル図ごとに，上述した階層情報を登録することによって保証ケースを作成する支援ツールを試作する．なお，ツールの試作は外注により実施した．

③試作ツールに基づく保証ケース作成実験

試作したツールを用いて，複数のモデル図から保証ケースを作成する実験を実施する．これにより試作ツールの有効性の評価結果を整理する．

(2) 具体的な研究成果の内容

①保証ケース統一作成手順の定式化

ここではルートゴール，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５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．

まず，統一作成手順で利用する保証ケースの基本パターンとして，アーキテクチャ分解パターン，特性分解パターン，リスク分解パターンを説明する．

1）アーキテクチャ分解パターン

保証ケースのアーキテクチャ分解パターンでは，システムが特性を満たすことを，アーキテクチャとして定義されるシステム構成に基づいて保証する．システム構成では，システムの構成要素とその関係が定義されるので，図 3-1 のように，「システムが特性を満たしている」という主張を「システムの構成要素が特性を満たしている」ことと「システムの構成要素間の関係が特性を満たしている」という２つの下位の主張に分解することによって，保証ケースを作成できる．この２つの下位の主張はさらに，構成要素と関係要素によって分解される．

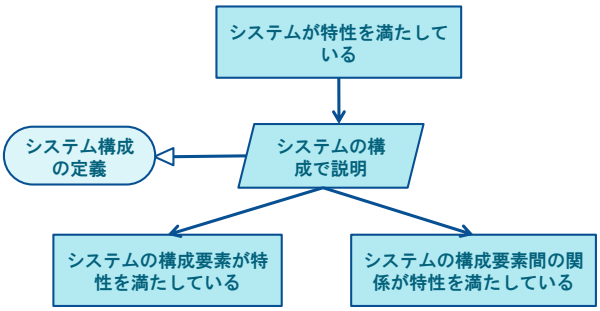


図 3-1　アーキテクチャ分解パターン

2）特性分解パターン

特性分解パターンでは，「システムが特性を満たしている」という主張を特性の構成要素に従って分解する．たとえば，ディペンダビリティ特性には，可用性，信頼性，安全性，一貫性，機密性，保守性がある．したがって，「システムがディペンダビリティ特性を満たしている」という主張を図 3-2 のように，6 個の下位の主張に分解できる．ここで，ディペンダビリティ特性には，可用性，信頼性，安全性，一貫性，機密性，保守性がある[19]．

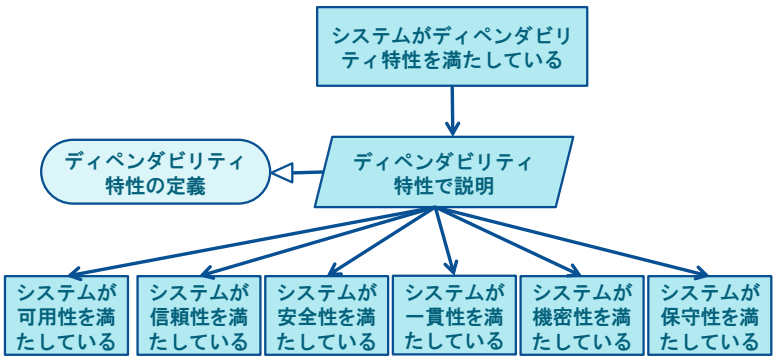


図 3-2　特性分解パターンの例

3）リスク分解パターン

安全性やセキュリティなどの特性については，対象がこれらの特性を満たすことを直接説明することは難しい．この場合，「対象が特性を満たしている」という主張を，特性リスクの定義に基づいて，「対象が特性リスクに対策している」という下位の主張に分解することで説明できる（図 3-3）．ここで，特性リスクが複数ある場合には，特性リスクごとに下位の主張を作成する．

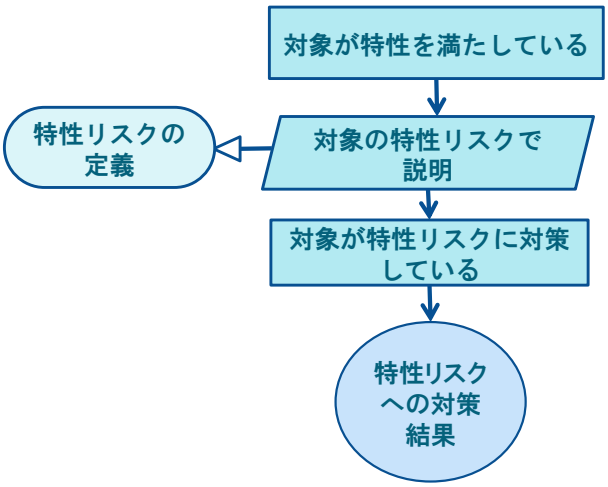


図 3-3　リスク対策分解パターン

4）分解パターンの合成

上述した，アーキテクチャ分解パターン，特性分解パターン，リスク対策分解パターンを組み合わせることができる．すなわち，まず「システム」に着目して「システムが特性を満たす」という主張をアーキテクチャ分解パターンで構成要素とその関係に分解する．次に，「特性」に着目して，下位特性に分解できる場合は，特性分解パターンで下位特性に分解する．最後に，下位特性に着目して，下位特性のリスクに基づいて，リスク分解パターンで分解することにより，リスク対策の証拠を明らかにすることができる．

モデルは，構成要素とその関係によって定義される．たとえば，ユースケース図の場合，アクタとユースケースがモデルの構成要素，アクタとユースケースの相互作用がモデルの関係である．同様にオープングループのアーキテクチャフレームワークである TOGAF[20]のアーキテクチャ記述言語 ArchiMate[21]のモデルも同様に，構成要素とその関係で定義できる．たとえば，ビジネスアーキテクチャ（BA）モデルには，ビジネスイベント，ビジネスプロセス，ビジネス対象，ビジネス情報形式などの構成要素と，トリガ関係，利用関係，実現関係などがある．

したがって，図 3-4 に示すように，モデルに対して統一的なモデル分解パターンを構成できる．まず，モデルの構成に基づいて，モデルの構成要素とその関係で主張を分解する．次に，構成要素の種類ならびに，構成要素関係の種類で主張を分解する．さらに，構成要素と構成要素関係の実体に基づいて主張を分解する．

この統一的モデル分解パターンは任意のモデルに対しても適用できる．この保証ケースパターンの階層構成を表 3-1 にまとめる．

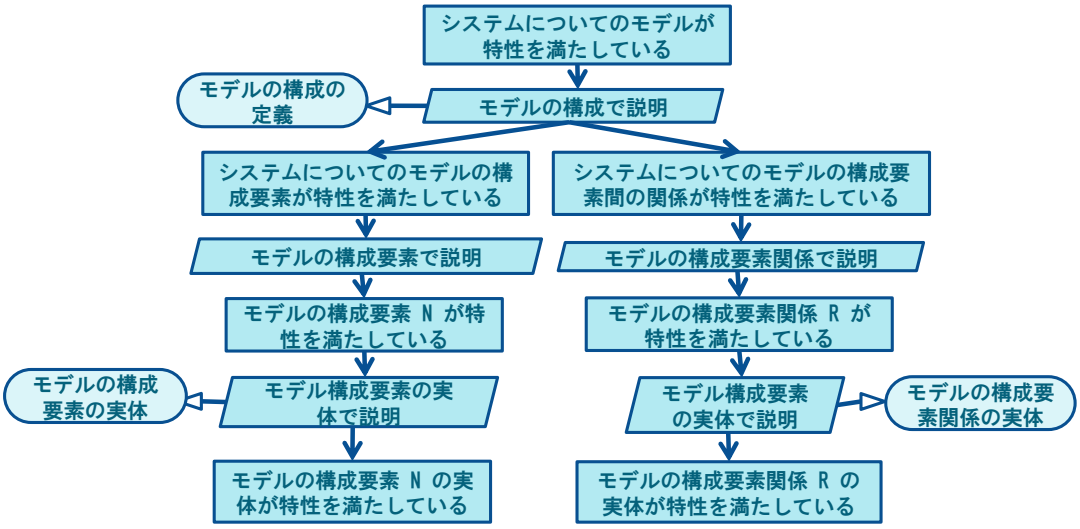


図 3-4　統一的モデル分解パターン

表 3-1　統一的保証ケースパターンの階層

階層	主張
ルート層	ルートゴールでは，モデルが特性を満たすことを主張する
要素と関係の分類層	ルートゴールをモデルの要素分類と関係分類に基づいて解することにより，それらが特性を満たすことを主張する
要素と関係の種類層	モデルの要素分類と関係分類に属する実体ごとに分解することにより，それらが特性を満たすことを主張する
実体リスクの対策層	実体に対するリスクによって分解し，リスクを軽減できることを主張する
エビデンス層	リスク対策ができている証拠を提示する

以下では，運転診断サービスという現実的なビジネスアプリケーションを対象として，保証ケースパターンの有効性を評価する．

【例】運転診断サービス

ガソリン販売会社は，ガソリンステーションを使用した車の運転情報の分析安全運転をサポートする運転診断サービスをクラウドサービスで提供する．車上デバイスでは，減速，アイドリング時間，噴射量の値のようなすべての情報を集める．車がガソリンスタンドに入り，エンジンを停止した場合，ワイヤレスネットワークを用いて，最後の燃料補給後から車上のデバイスで記録された運転情報をガソリンスタンドの接続デバイスに送信する．運転情報がクラウドサーバにガソリンスタンドの接続デバイスのネットワークを通して送られる場合，運転情報を分析し，スマートフォンを通して運転者に運転レポートを運転診断サービスが提示する．

運転診断サービスはドライバーの運転技術の水準を正確に判断できる．ガソリン販売会社は，保険会社と協力することによって，運転技術水準に従って，請求を変更する車両保険を提供する．

ArchiMate ビジネスアーキテクチャで記述した DDS(運転診断サービス)のビジネスプロセスを図 3-5 に示す．

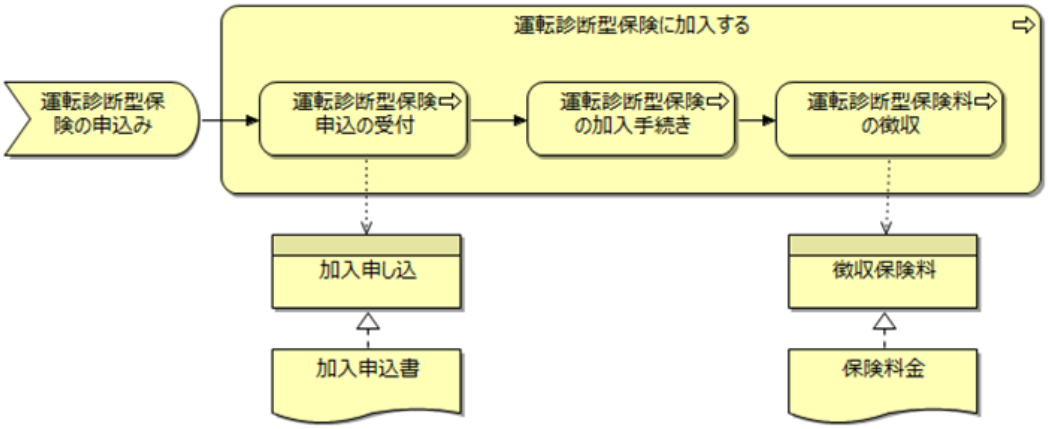


図 3-5　運転診断サービスのビジネスプロセスの例

図 3-5 に出現するモデルの構成要素は，ビジネスイベントとビジネスプロセス，ビジネスオブジェクト，ビジネス情報形式である．

「運転診断型保険の申込み」がビジネスイベントである．「運転診断型保険申込みの受付」「運転診断型保険の加入手続き」「運転診断型保険料の徴収」がビジネスプロセスである．

「加入申し込」「徴収保険料」がビジネスオブジェクトである．「加入申込書」「保険料金」がビジネス情報形式である．

図 3-5 に出現するモデルの関係要素は，トリガ関係，操作関係，実現関係である．

トリガ関係は，「運転診断型保険の申込み」から，「運転診断型保険申込みの受付」「運転診断型保険の加入手続き」「運転診断型保険料の徴収」への関係である．

操作関係は，「運転診断型保険申込みの受付」と「加入申し込み」，「運転診断型保険料の徴収」と「加入申込書」の関係である．

実現関係は，「加入申し込み」と「加入申込書」，「徴収保険料」と「保険料金」の関係である．

上述した保証ケースパターンを用いて図 3-5 の BA に対して作成した保証ケースを，図 3-6，図 3-7，図 3-8 に示す．

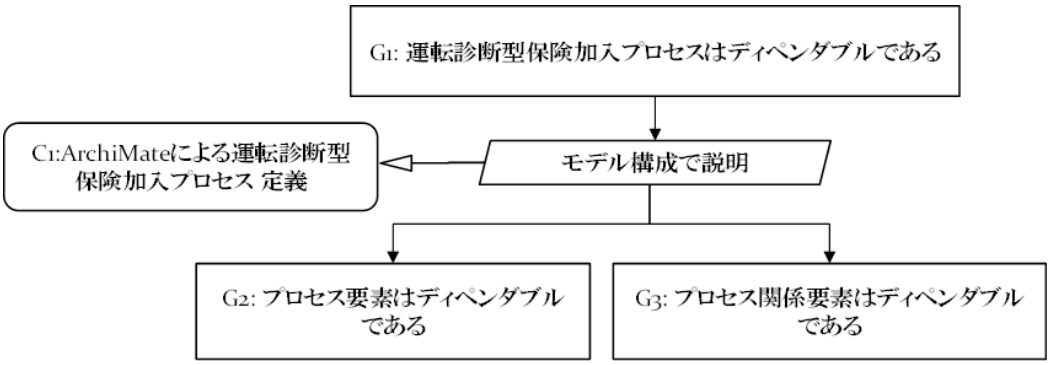


図3-6　運転診断型保険加入プロセスに対する最上位の保証ケース

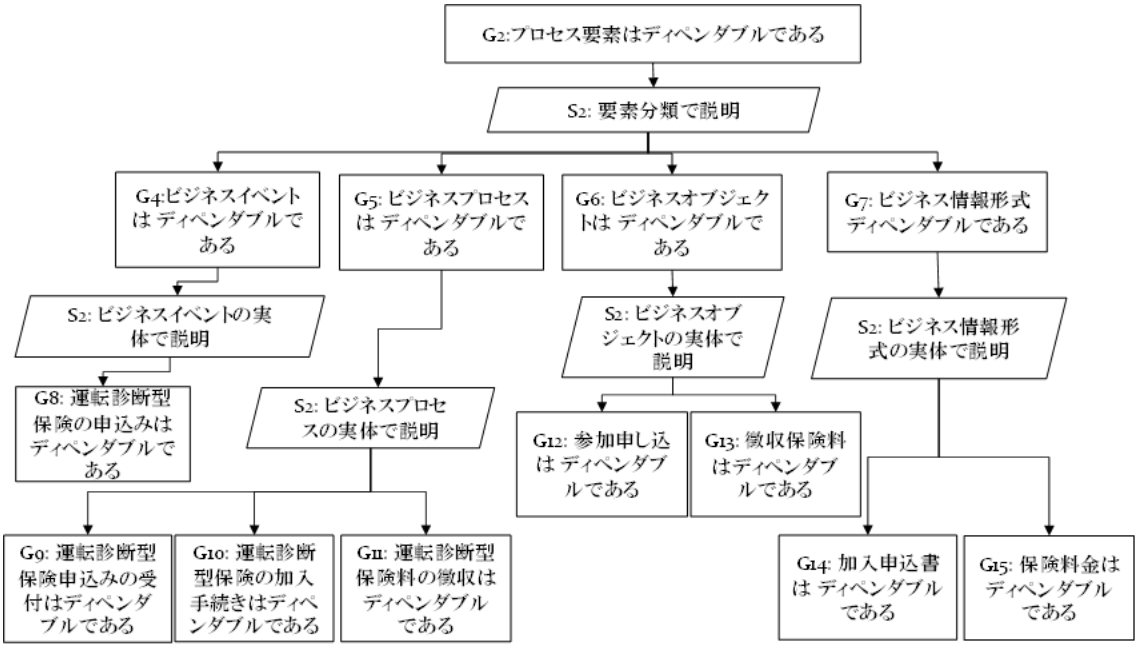


図3-7　G2に対する保証ケース

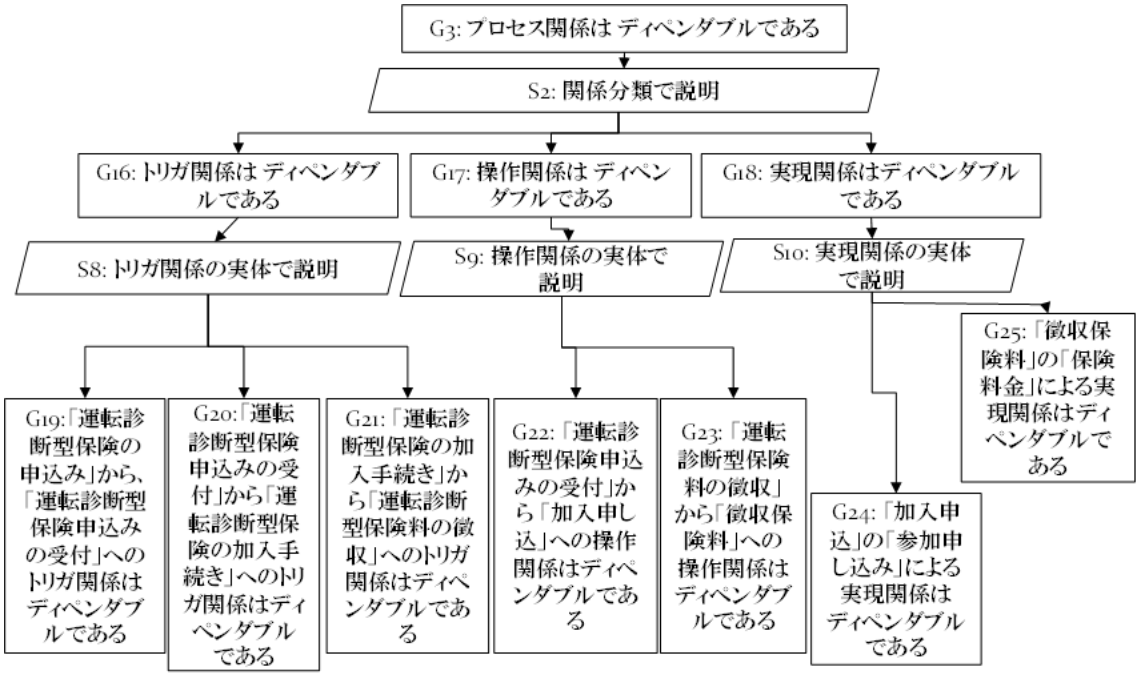


図 3-8　G3 に対する保証ケース

上述した運転診断サービスの事例の結果から，ArchiMate における運転診断サービスのための BA から保証ケースを容易に作成できることが明確になった．この結果から，提案手法の有効性が示された．この事例では，BA だけを対象としたが，アプリケーションアーキテクチャとテクノロジーアーキテクチャにおいても同じ結果が得られることは明らかである．

②保証ケース作成支援ツールの試作

ここではモデル図ごとに，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情報を登録することによって保証ケースを作成する支援ツールを試作する．試作では，外注仕様書を作成することにより，ツールの試作は外注により実施した．

受託研究で試作した保証ケース作成支援ツール UC2CT(Unified Context to Claim Tool)では，図 3-9 に示すように，モデルを用いて作成されるシステム開発工程成果物を入力として，保証ケース情報を生成することができる．出力された保証ケース情報を保証ケースエディタに入力することにより，モデルに基づく保証ケースを確認することができるようになる．このツールによって任意のモデルに対して保証ケースを半自動的に作成できるようになる．なお，保証ケース生成アルゴリズムを以下に示す．

【定義】　保証ケース生成アルゴリズム

For each model A=<Concept Set, Relationship Set>, where ConceptSet={<Name, Cc >|Cc is a Concept category of the model}
RelationshipSet={<Name, Cr >|Cr is a Relationship category of ArchiMate}
the following sets are calculated.

ConceptCategory(A)={ C | <x, C> is in ConceptSet of A }
RelationshipCategory(A)={ C | <r, C> is in RelationshipSet of A}
ConceptInstance(C, A)={ x| <x, C> is in ConceptSet of A}
RelationshipInstance(C, A)={ r| <r, C> is in RelationshipSet of A}
Based on the above sets, GSN model D is derived by the following steps.
The root goal can simply be developed such that the model A satisfies dependability principles.
Second level goals are derived by Concept and Relationship
Third level goals are derived by using
ConceptCategory(A) and RelationshipCategory(A)
Fourth level goals are derived by using
ConceptInstance(C, A) and RelationshipInstance(C, A)
Fifth level goals are derived by analyzing instance risks. The derivation shall be conducted by eliciting risks for each instance element of A.

【アルゴリズム終わり】

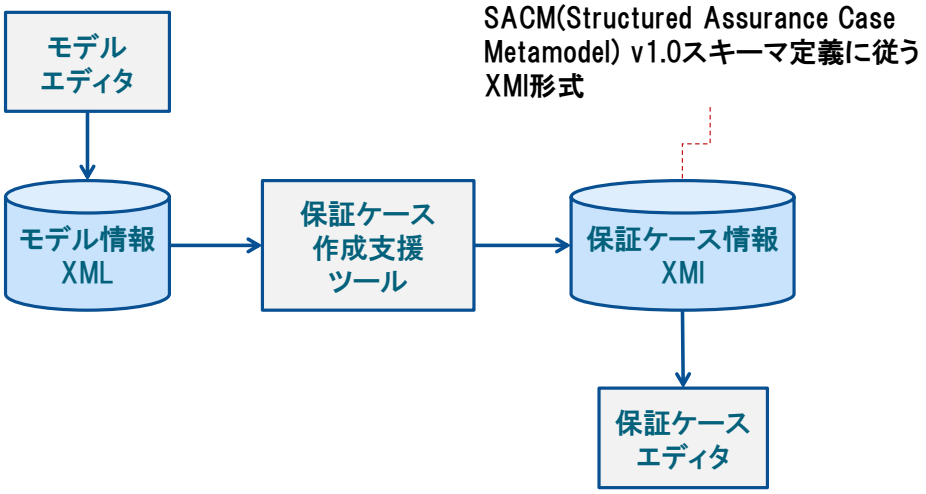


図 3-9　保証ケース作成支援ツールの概要

■モデルの定義例

UC2CT(Unified Context to Claim Tool)ツールのシステム構成を図 3-10 に示す．また，このシステム構成図もまた，構成要素とその関係を記述しているので，モデルであると考えられる．図 3-11 に，図 3-10 のモデルを XML で定義した結果を示す．

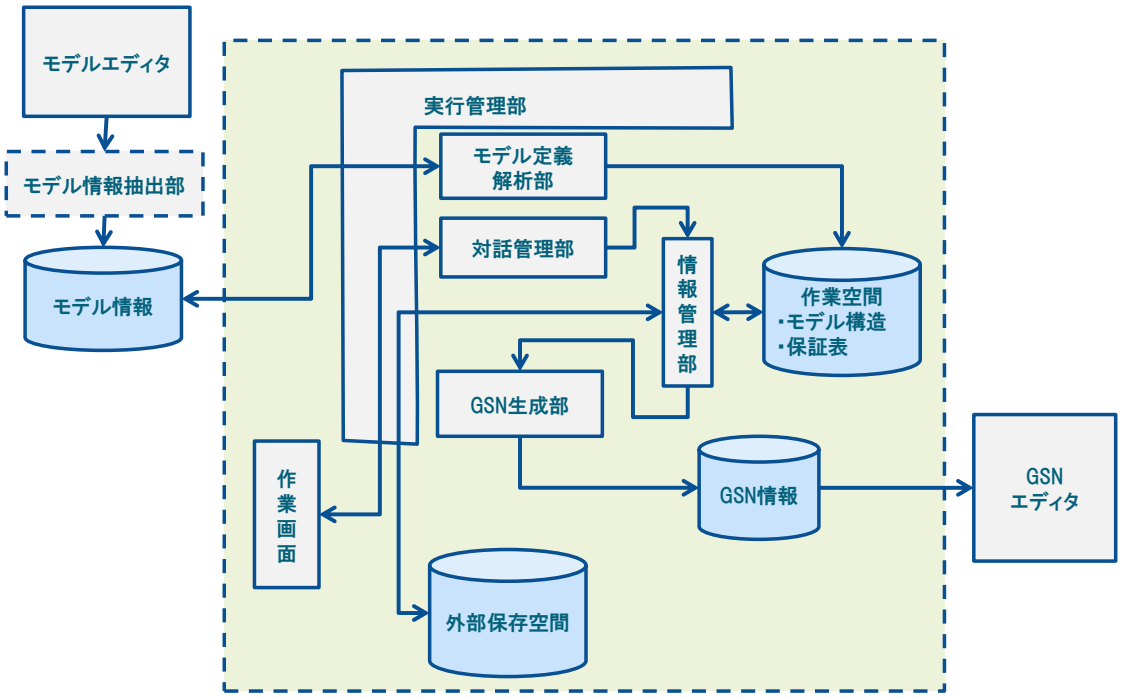


図 3-10　保証ケース作成支援ツールのシステム構成

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <modelDefinition>
  - <model name="保証ケース統合作成支援ツール">
    - <types>
      - <nodes>
          <node>Module</node>
          <node>Data</node>
        </nodes>
      - <relations>
          <relation>Module_Module</relation>
          <relation>Module_Data</relation>
        </relations>
      </types>
    - <instances>
      - <nodes>
          <node id="in-001" type="Module">実行管理部</node>
          <node id="in-002" type="Module">モデル定義解析部</node>
          <node id="in-003" type="Module">対話管理部</node>
          <node id="in-004" type="Module">GSN生成部</node>
          <node id="in-005" type="Module">情報管理部</node>
          <node id="in-006" type="Module">作業画面</node>
          <node id="in-007" type="Data">モデル情報</node>
          <node id="in-008" type="Data">作業空間</node>
          <node id="in-009" type="Data">外部保存空間</node>
          <node id="in-010" type="Data">GSN情報</node>
        </nodes>
      - <relations>
          <relation id="ir-011" type="Module_Module" target="in-005" source="in-003"/>
          <relation id="ir-012" type="Module_Module" target="in-003" source="in-006"/>
          <relation id="ir-013" type="Module_Module" target="in-004" source="in-005"/>
          <relation id="ir-014" type="Module_Data" target="in-002" source="in-007"/>
          <relation id="ir-015" type="Module_Data" target="in-006" source="in-002"/>
          <relation id="ir-016" type="Module_Data" target="in-006" source="in-005"/>
          <relation id="ir-017" type="Module_Data" target="in-010" source="in-004"/>
          <relation id="ir-018" type="Module_Data" target="in-009" source="in-005"/>
        </relations>
      </instances>
    </model>
</modelDefinition>
```

図 3-11　モデル定義例

また，図 3-12，図 3-13 にそれぞれ，品質特性とリスクの定義例を示した．

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<qualityDefinition>
  - <attribute name="ディペンダビリティ" root="true">
      - <struct>
            <attribute-ref>可用性</attribute-ref>
            <attribute-ref>信頼性</attribute-ref>
            <attribute-ref>安全性</attribute-ref>
            <attribute-ref>機密性</attribute-ref>
            <attribute-ref>一貫性</attribute-ref>
            <attribute-ref>保守性</attribute-ref>
        </struct>
    </attribute>
    <attribute name="可用性"/>
    <attribute name="信頼性"/>
  - <attribute name="安全性">
      - <criteria name="システム安全管理原則">
          - <list>
                <item>システムの仕様や運用方法を明確に文書化している</item>
                <item>システムの仕様や運用方法が当初の方針の通りに機能しているかどうかを定期的に監査している</item>
                <item>システムの監査結果をあいまいさのない形で文書化している</item>
                <item>システムの監査の結果に問題があった場合は、真摯に対応している</item>
                <item>問題対応の記録を文書化し、第三者が検証可能な状況にしている</item>
            </list>
        </criteria>
    </attribute>
    <attribute name="機密性"/>
    <attribute name="一貫性"/>
    <attribute name="保守性"/>
</qualityDefinition>
```

図 3-12　品質特性の定義例

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <riskDefinition>
  - <risks>
    - <risk name="通信コンポーネントリスク">
      - <struct>
            <deviation-ref>Exceptionリスク</deviation-ref>
            <deviation-ref>Delayリスク</deviation-ref>
            <deviation-ref>Omissionリスク</deviation-ref>
            <deviation-ref>Duplicationリスク</deviation-ref>
        </struct>
      </risk>

  - <deviations>
    - <deviation name="Exceptionリスク">
      - <list>
            <item>入力例外</item>
            <item>処理例外</item>
            <item>出力例外</item>
        </list>
      </deviation>

    </deviations>
</riskDefinition>
```

図 3-13　リスク定義例

UC2CT はエクセルのマクロで実現している．図 3-11，図 3-12，図 3-13 の XML 定義を UC2CT に入力すると，図 3-14 のように，エクセルで保証ケースの内容を編集できるようになる．UC2CT で XMI 出力メニュを指定すると，保証ケース情報が XMI 形式で出力できる．この結果を Asth GSN に入力した結果を図 3-15 に示す．この XMI 形式は SACM(Structured Assurance

Case Metamodel) v1.0 スキーマ定義に従っているので，この規格に準拠した GSN エディタであれば，UC2CT の結果に基づいて GSN を編集できる．

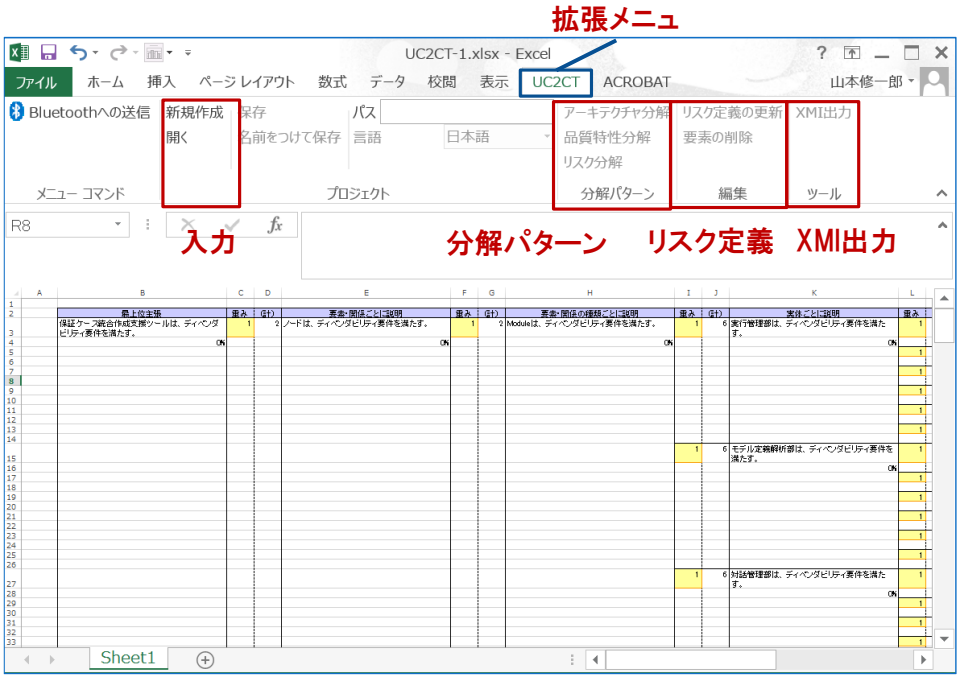


図 3-14　UC2CT(Unified Context to Claim Tool)ツール画面例

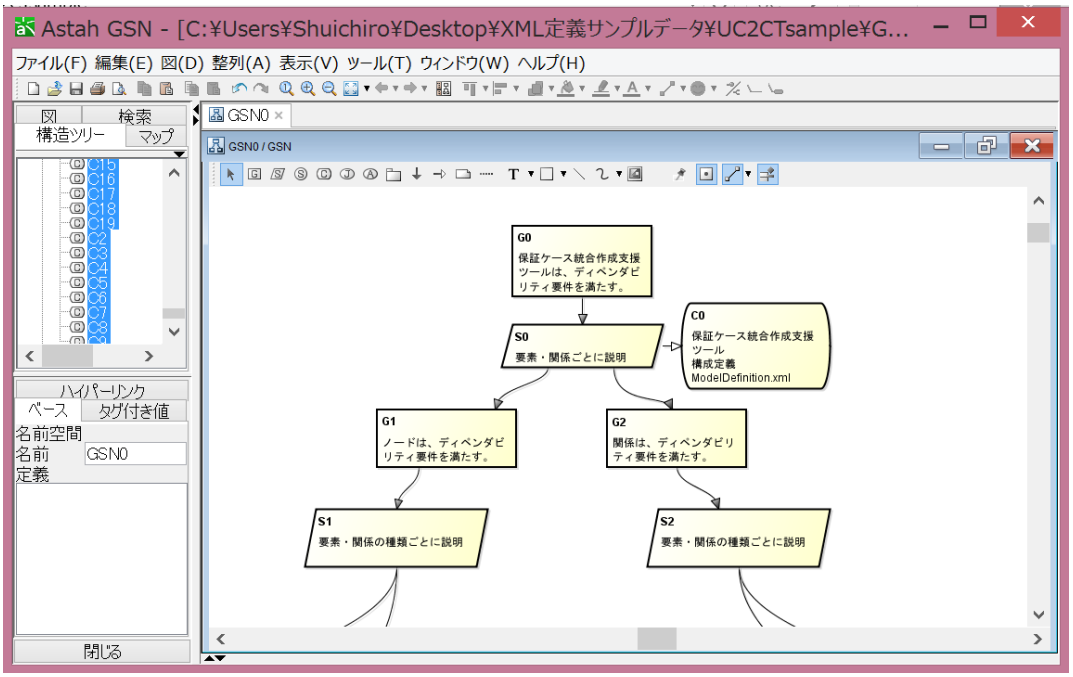


図 3-15　生成された保証ケースの編集画面例

③試作ツールに基づく保証ケース作成実験

ここでは試作したツールを用いて，複数のモデル図から保証ケースを作成する実験を実施する．これにより試作ツールの有効性の評価結果を整理する．

試作ツールを用いた保証ケース作成実験の結果を図 3-16 に示す．

実験対象としたモデルは，図 3-10 に示した保証ケース作成支援ツール UC2TC のシステム構成図である．このシステム構成図に対する保証ケースの規模は，主張 218 個，戦略 53 個，前提 47 個，証拠 165 個となった．

ツールを使わずに保証ケースを作成した時間は 275 分であった．これに対してツールを使用して保証ケースを作成した時間は 47 分であった．この結果，ツールの利用により，保証ケース作成時間を約 5.6 倍（約 82%削減）に向上できることが判明した．

また，後者の作成時間には XML 定義時間 28 分を含むことから，今後モデルから XML 定義を自動抽出できれば，保証ケース作成時間が約 14.5 倍になることも判明した．この結果を図示すると，図 3-16 のようになる．

なお，この 19 分の内訳は，ツールへの XML 入力，アーキテクチャ分解，品質特性分解，リスク対策分解，GSN エディタ変換を含むことを注意しておく．

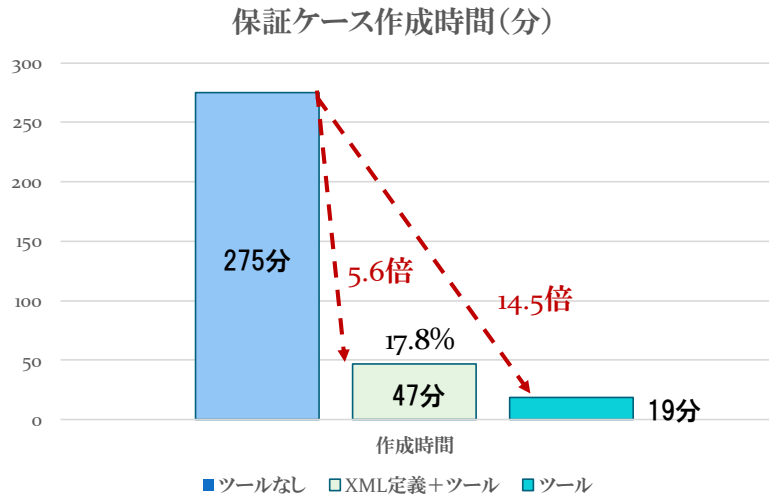


図 3-16　保証ケース作成実験の結果

3.1.3 発生した問題および今後の展望

(1) 発生した問題

欠陥のあるモデルへの対応については，モデルの要素と要素関係に誤りがある場合，生成された保証ケースで確認することができる．モデル要素と要素関係に抜けがある場合，ツールでは対応するモデル要素と要素関係も生成できない．この場合，「モデル要素に抜けがない」「モデル要素関係に抜けがない」という 2 個の主張を作成しておき，その妥当性を議論することで，議論参加者の合意によって保証することになる/複数の参加者による多面的な議論によって抜けを保証するしかない．つまり欠陥は，ノードと関係についてのそれ自体の欠陥（誤り）と，それらが抜けている欠陥（漏れ）がある．したがって，保証ケースで誤りがないことを確認することと漏れがないことを確認する主張を用意すればよい．

(2) 今後の展望

上述した内容に基づいて，保証ケースを用いたモデルの欠陥摘出手法を整理することができる.

3.2 研究課題 2「コンポーネントに対する保証ケース作成法」

3.2.1 当初の想定

(1) 研究内容

コンポーネントに対するソフトウェアコードに基づき，保証ケースを作成する手法を考案する．具体的には，保証ケースの作成手順を形式化し，メタモデルを定義するとともにそれぞれの妥当性を保証ケース作成実験にて確認する．

(2) 想定問題と対応策

コンポーネントについての制御フローやデータフローなどのコード情報に基づいて，保証ケースを作成するために，コード情報と保証ケースの構成要素との一貫性のある対応関係を明らかにする必要がある．したがって，具体的なコンポーネントコードを対象として，制御フローとデータフローに基づいて，入出力データに対する安全性やセキュリティなどの特性を保証する机上実験を実施することにより，コンポーネントの保証ケースを作成する手順を定式化する．次いで，これらの情報に対するリポジトリ情報と保証ケースの一貫性のあるメタモデルを定義することにより，リポジトリとの連携実験を実施する．なおリポジトリは名古屋大学でこれまで開発してきた XML に基づくソフトウェアリポジトリを用いる．ここで，コンポーネントに対するプログラムコード情報に関する保証ケースのメタモデルをリポジトリに格納する．

本研究課題に対する問題設定と解決策の妥当性について大学ならびに企業の有識者からのアドバイス評価を実施する．この実施内容については，「4.1.4 外部の客観的評価」【コードに対する保証ケース作成法】で述べる．

3.2.2 研究プロセスと成果

(1) 研究プロセス

①コンポーネントコード保証ケース作成手順の定式化

コンポーネントコードの定義情報に基づいて，保証ケースの構成要素を定義するための主張，前提を抽出することにより，保証ケースの作成手順を定式化する．

②保証ケースリポジトリメタモデルの具体化

概念クラス図を用いて，定式化したコンポーネントコードに対する保証ケースをリポジトリに格納するためのメタモデルを定義する．

③コンポーネント保証ケース作成実験

コンポーネントコードに対する保証ケース作成手順ならびにメタモデルの妥当性を確認するために，具体的なコンポーネントコードを作成するとともに，それを対象として保証ケースを作成する実験を実施する．

(2) 具体的な研究成果の内容

①コンポーネントコード保証ケース作成手順の定式化

ここではコンポーネントコードの定義情報に基づいて，保証ケースの構成要素を定義するための主張，前提を抽出することにより，保証ケースの作成手順を定式化する．

保証ケースに基づくコード保証手順は以下のようになる．

【手順 1】入出力仕様に基づき入出力制約を作成
【手順 2】入出力制約に基づき，証拠が未定義になっている保証ケースを作成
【手順 3】対応するコード断片を証拠に用いて，保証ケースを説明
【手順 4】保証ケースの主張を説明するコード断片がない場合，コードの欠陥として指摘

保証ケースの証拠を上述した手順に従って説明できない場合，コードには欠陥があることになる．つまり，この手順はコードの欠陥を摘出する具体的な方法を与えている．このため，保証ケースに基づいて欠陥を摘出する考え方を，証拠による欠陥摘出（DDBE，Defect Detection By Evidence）原理と呼ぶことができる．

この基本的な考え方を図示すると，図 3-17 のようになる．この保証ケースでは，「コードが安全である」という主張を最上位ゴールとする保証ケースを入出力引数の関係仕様を前提として分解している．

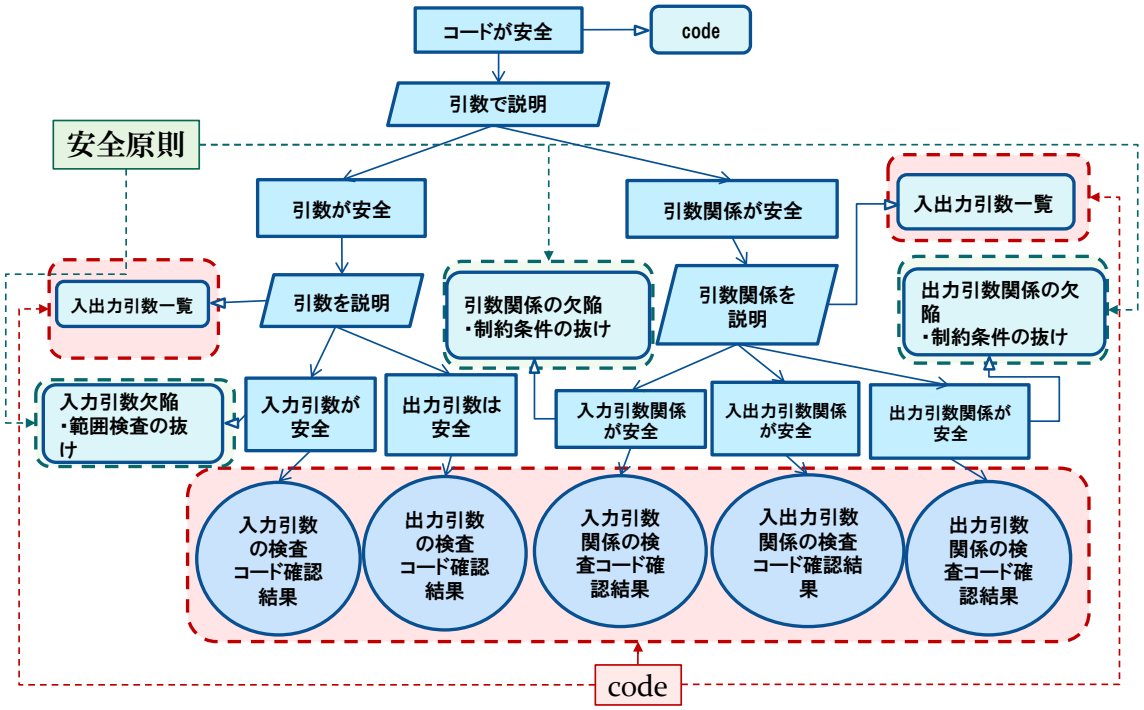


図 3-17　コードに対する保証ケースの考え方

最下位の証拠が，入力引数，出力引数，入出力引数の関係についての安全性を確認するために必要なコードを確認した結果に対応している．

この考え方を具体的に説明するため，割り算プログラムに対する入力保証ケースの作成例を図 3-18 に示す．この入力保証ケースでは，証拠の部分が TBE（To Be Explained）として未定義になっている．このように，対象とするプログラムコードに対する入力引数の関係に応じて最上位の主張を分解して，複数の TBE を明確化できる．次に，この例では 4 個の TBE に対して，割り算プログラムのコードを読むことで，図 3-19 に示すように，4 個の証拠

を具体化している．このように，必要な証拠がすべて定義できれば，割り算プログラムのコードが適切であることを保証できる．

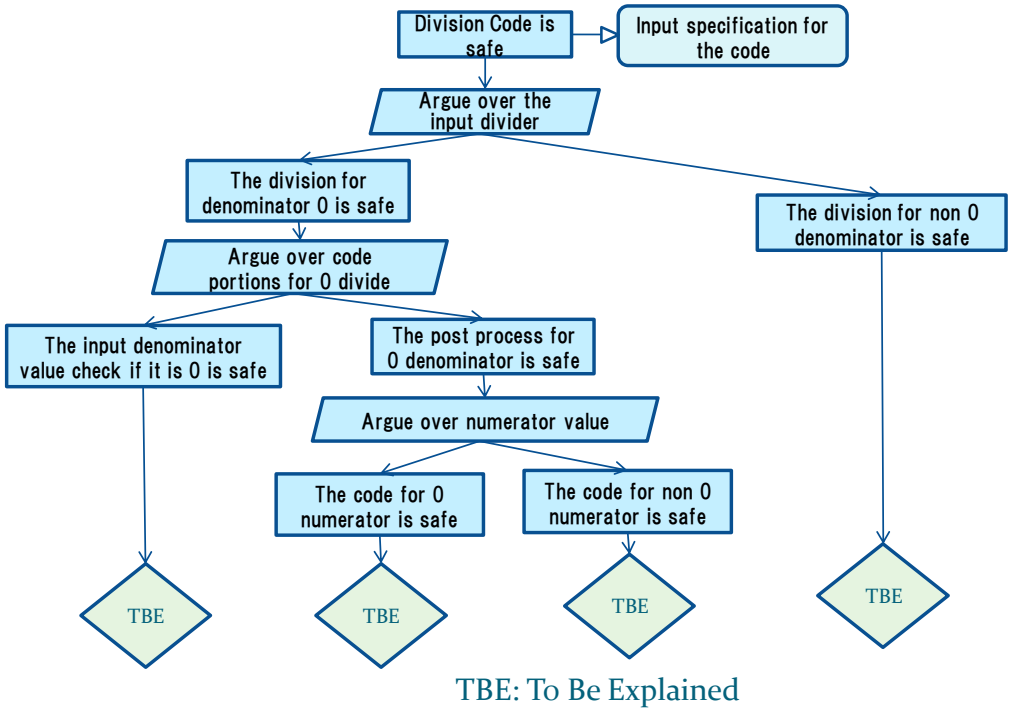


図 3-18　割り算に対する入力保証ケース

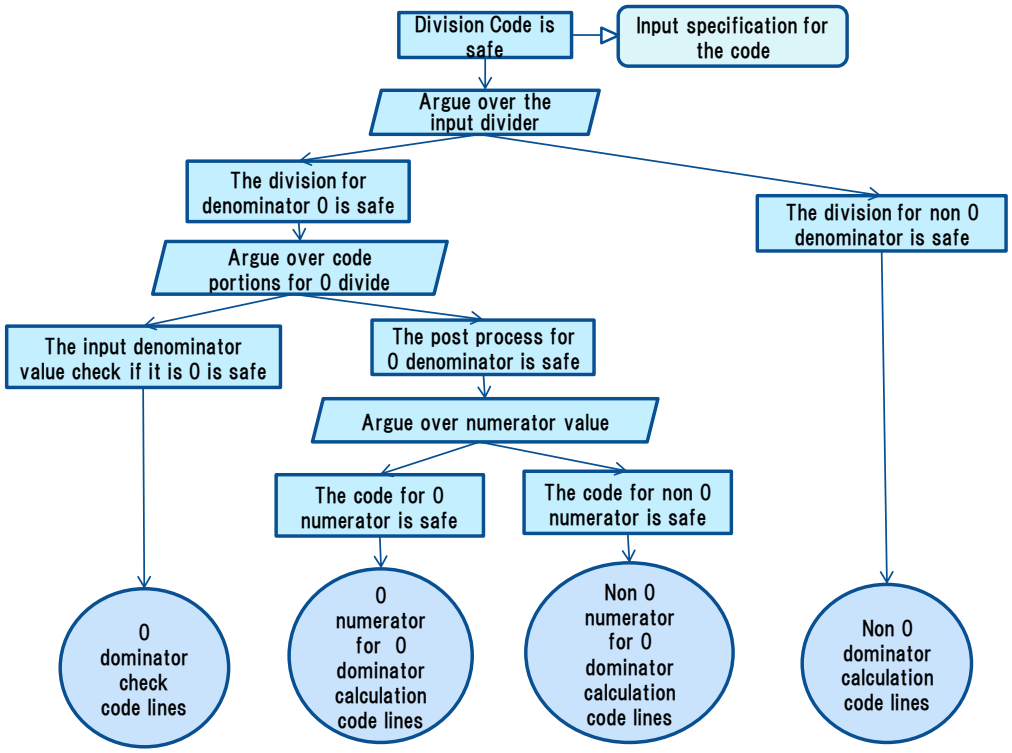


図 3-19　証拠を具体化した割り算に対する入力保証ケース

②保証ケースリポジトリメタモデルの具体化

ここでは概念クラス図を用いて，定式化したコンポーネントコードに対する保証ケースをリポジトリに格納するためのメタモデルを定義する．

コード保証ケースのリポジトリに対するメタモデルを図 3-20 のように定義した．このメタモデルでは，保証ケースに対して，前提（Context），主張（Claim），証拠（Evidence）と証拠に対する未定義（TBE）を抽出している．これに対して，コードに対するメタモデルでは，識別子（Identifier），式（Expression），コード断片（Block）を抽出している．

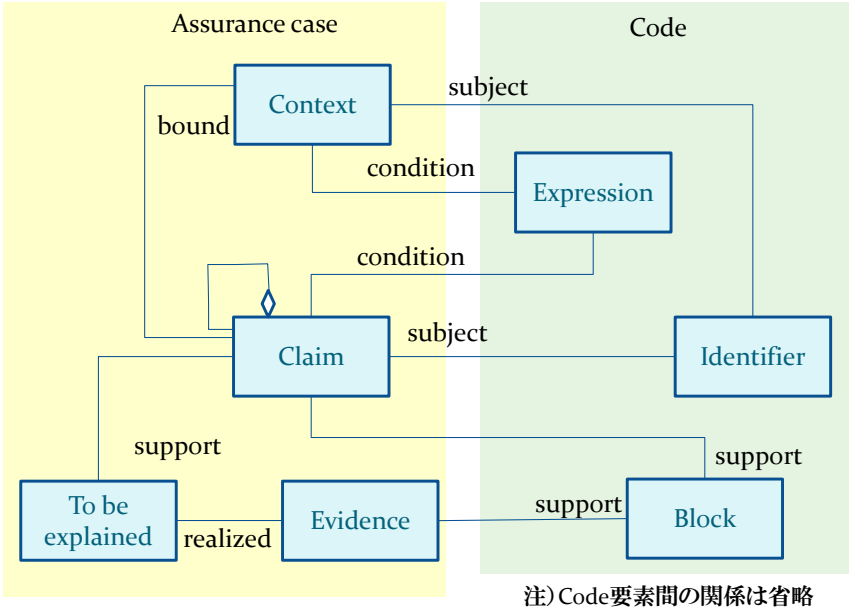


図 3-20 コード保証ケースのメタモデル

このメタモデルは，DDBE 原理に基づいて保証ケースを作成するために，余分な要素は排除することで必要最小限の要素だけを採用している．

③コンポーネント保証ケース作成実験

ここではコンポーネントコードに対する保証ケース作成手順ならびにメタモデルの妥当性を確認するために，具体的なコンポーネントコードを作成するとともに，それを対象として保証ケースを作成する実験を実施する．

上述したコードに対する保証ケース作成法の有効性を確認するために，具体的なコードを対象として保証ケースを作成する実験を実施した．

実験対象の概要は，次のようである．

対象とする入力仕様は，SSL/TLS Protocol V 1.0 で，3584 行からなる文章である．

対象とするコードは，オープンソースの OpenSSL 1.0.1j s3_clnt.c である．コード行数は，3469 であった．

被験者は，名古屋大学の学生（学部 4 年生）が 1 名である．

入力仕様分析によって，11 個の TBE を摘出した．この入力仕様分析に要した時間は 10 時間だった．入力仕様に基づく保証ケースの作成時間は 5 時間だった．

次いで，Open SSL のコードを探索して 10 件の TBE に対する証拠として対応するコードの断片を具体化したが，のこり 1 件の TBE については，対応するコードがなかった．この 1 件の具体化できなかった TBE に対応する保証ケースの部分を図 3-21 に示す．この図では，「セッション ID が空であるか，クライアントが送信した値と一致しない場合は安全である」という主張を説明しようとしている．この場合，対応するコードで鍵の入力条件を確認して，「暗号スィートの方式が，入力鍵を有効としない場合の処理は安全である」ことを説明する必要がある．このため，鍵の入力条件が不適切であるから，「エラー処理を中断していることを説明」する必要がある．この理由は，「不適切な入力処理の続行を禁止」する必要があるからである．したがって，主張「暗号スィートの方式が，入力鍵を有効としない場合に処理を中断している」に対応する証拠となるコードがなくてはならない．ところが，この TBE に対応するコードが確認できなかった．この TBE が具体化できなかった部分が実際に Open SSL の脆弱性に対応していた．

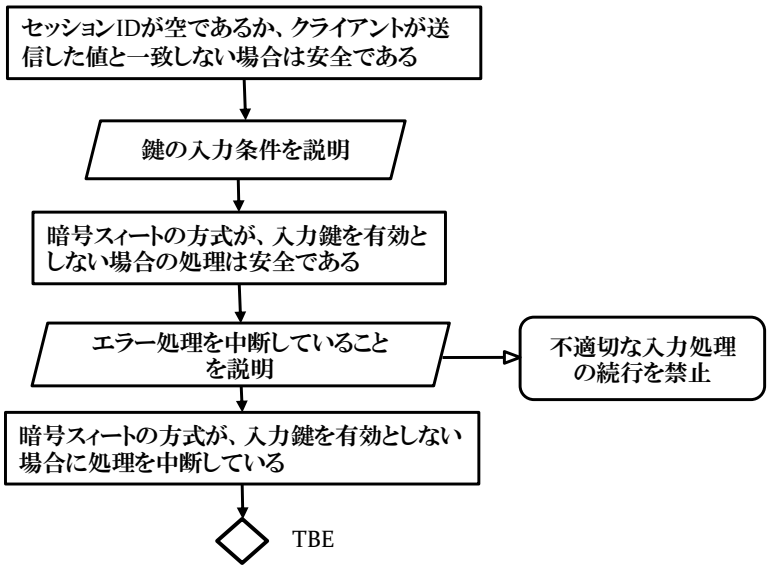


図 3-21　オープン SSL の欠陥を検出した保証ケースの部分

このコードに基づく保証ケースの説明時間は 8 時間であった．作業時間の内訳を示すと，図 3-22 のようになる．

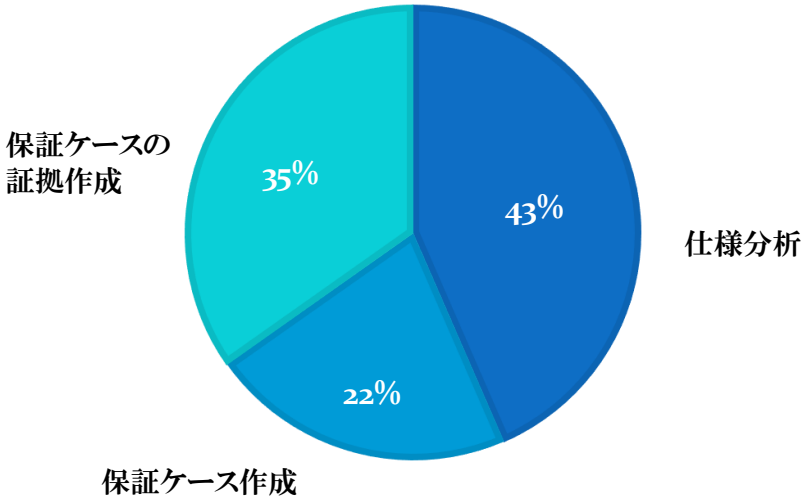


図 3-22　コードに基づく保証ケース作成時間の内訳

3.2.3 発生した問題および今後の展望

(1) 発生した問題

入出力仕様から作成した保証ケースに基づいて，保証ケースの証拠に対応するコード断片の探索活動が，担当者の能力に依存する．このため，担当者の能力によってはコード断片の見落としや摘出誤りが発生する可能性がある．

(2) 今後の展望

コード断片の見落としや摘出誤りの発生を防止する方法について，コードの静的解析を用いた研究を進める必要がある．

3.3 研究課題３「保証ケースの客観的なレビュ手法」

3.3.1 当初の想定

(1) 研究内容

作成された保証ケースをレビュするための客観的なレビュ手法を考案する．具体的には，レビュ規則とレビュ手順を定式化するとともに，レビュ指標を定義する．また，保証ケースのレビュ手順を定式化し，レビュ実験によって保証ケースのレビュ内容の妥当性を確認する．

(2) 想定問題と対応策

保証ケースをレビュする場合，担当者ごとに，レビュの観点や重要性の判断方針が異なるという問題がある．また，単純なレビュ規則を適用した場合，レビュにおける指摘誤りと誤りの指摘漏れが発生するという問題がある．このため，保証ケースを構成する主張（ゴール），前提（コンテクスト），議論（ストラテジ），証拠（エビデンス）を構成する用語関係に基づいて，完全性，明確性，適切性，追跡性などのレビュ観点を定式化するとともに，用語関係を考慮したレビュ規則により指摘誤りならびに，誤りの指摘漏れの削減を図る．また，主張と証拠の充足性に関する定量的な指標を導入することにより，重要性の対立を解消する方式を考案する．本研究課題に対する問題設定と解決策の妥当性について大学ならびに企業の有識者からのアドバイス評価を実施する．

3.3.2 研究プロセスと成果

(1) 研究プロセス

①レビュ観点・規則・手順の定式化

レビュ対象となる保証ケースの（イ）内容理解，（ロ）問題識別，（ハ）原因究明，（ニ）修正，からなるレビュプロセスの４観点に基づいて，レビュ規則とレビュ手順を定式化する．

②保証ケースレビュ指標の定式化

レビュの４観点ごとに実施すべき活動を抽出するとともに，その完了基準に基づいてレビュ指標を定義する．

③保証ケースレビュ実験

同一の保証ケース事例を対象として，定式化したレビュ手順を用いる被験者と，用いない被験者に分けて保証ケースレビュ実験を実施することにより，保証ケースレビュ手順の妥当性を確認する．

(2) 具体的な研究成果の内容

保証ケースのレビュ手法については，保証ケースが正しい構成規則を用いて記述されていることや成果物と保証ケースとの追跡性ならびに網羅性を確認する手法が報告されている．しかし，保証ケースの妥当性を保証対象の内容に踏み込んで客観的に確認するためのレビュ手法は確立されていない．

このため，システミグラムを用いて保証ケースが対象とする構成情報を図式化することにより，保証ケースの内容に基づくレビュ手法を提案した．また，完全性，明確性，適切性，追跡性からなるレビュ観点に基づき，レビュ規則を具体化する．さらに，本手法を列車運行

の安全性に対する保証ケースに適用することにより，保証ケース上で曖昧な箇所を摘出できることを確認した.

①レビュ観点・規則・手順の定式化

ここではレビュ対象となる保証ケースの（イ）内容理解,（ロ）問題識別,（ハ）原因究明,（ニ）修正，からなるレビュプロセスの４観点に基づいて，レビュ規則とレビュ手順を定式化する.

レビュの４観点とレビュ手順および規則との関係は以下のとおりである.

［観点］内容理解
［レビュ手順］システミグラムを作成することにより，内容を理解する
［レビュ規則］システミグラムの作成が完了した保証ケースノードの割合を計測

［観点］問題識別
［レビュ手順］システミグラム上の欠陥により，問題を識別する
［レビュ規則］完全性，明確性，適切性，追跡性についてのシステミグラムの欠陥数を計測

［観点］原因究明
［レビュ手順］対応項目の欠落・誤りを原因であると推定する
［レビュ規則］システミグラムの欠陥に対する保証ケース上の欠落・誤りの特定数を計測

［観点］修正
［レビュ手順］原因究明された問題について，欠落・誤り項目を補完・訂正する
［レビュ規則］問題項目数に対する修正数を計測

まず，システミグラムについて説明する．システミグラムは，ノードとその関係からなる(図 3-23)．関係には，ノードの包含関係とリンク関係がある．ノードは，人工物,エージェント,重要属性を表す．ノードリンクは，ノード間の関係を表す．ノードの包含関係では,ノードの内部ノードで，下位ノードやノード属性を表す.

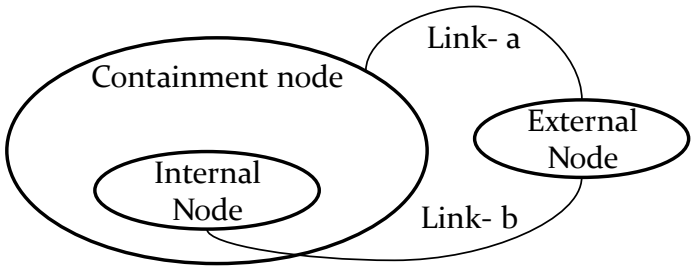


図 3-23 システミグラムの例

システミグラムを用いた保証ケースのレビュ手法では，レビュする保証ケースの主張を，以下の 2 種類に分類する．

［特性主張］ 〈対象〉が〈特性〉を満足している
［対策主張］ 〈対策〉によって〈リスク〉に対応している

特性主張は対象と特性の構成要素に従って，下位の特性主張に分解される．また，特性主張と対策主張には，上位の特性主張を下位の対策主張が説明するという関係がある．このとき，分解で指定される前提はリスクの構成要素である．

対策主張は証拠によって説明される．すなわち，対策主張は最下位の主張である．

特性主張を構成する対象と特性に対して，図 3-24 のシステミグラムを対応付ける．すなわち，対象の内部状態として，「特性を満足している」ことを表現する．

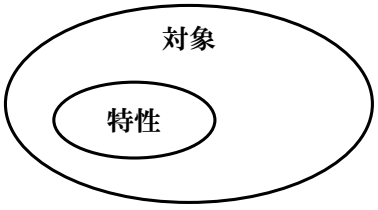


図 3-24　特性と対象

対象が複数の構成要素から構成される場合，システミグラムでは，上位の構成要素の内部に，下位の構成要素を記述する．

たとえば，A と B が対象に含まれる場合は，図 3-25 のようになる．

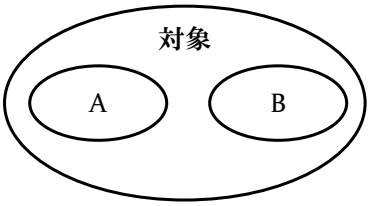


図 3-25　構成要素と対象

対策主張の場合，「対象が特性を満足する」という上位の主張を実現するために，「対策によってリスクに対応している」という主張が必要になる．この場合，図 3-26 のようなシステミグラムになる．

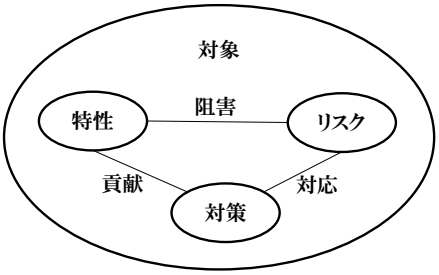


図 3-26　リスク対策による特性の満足化

また，証拠が対策を説明するシステミグラムは図 3-27 のようになる．

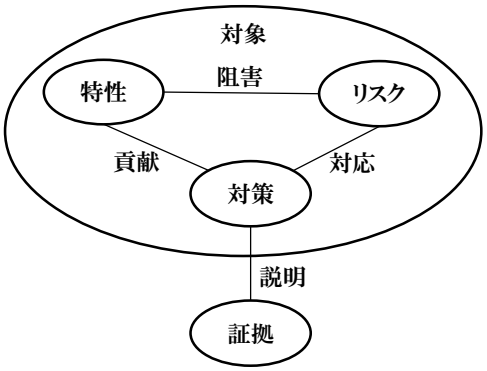


図 3-27　証拠による対策を説明するシステミグラム

システミグラムを用いて，保証ケースのレビュ手順を，①内容理解，②問題識別，③原因究明，④修正から構成する．

［内容理解］

保証ケースに対するシステミグラムを上述の方法で作成する

［問題識別］

システミグラムのレビュ規則に基づき，用語関係，特性関係を分析して，問題を識別する

［原因究明］

対応項目の欠落・誤りを検出するによって，問題原因を特定する

［修正］

原因究明された問題について，欠落・誤り項目を補完・訂正する

以下では，前述した構成情報に基づくレビュ手法の適用例を示す．まず，列車の運行に対する安全性について，図 3-28 の保証ケースがあるとする．

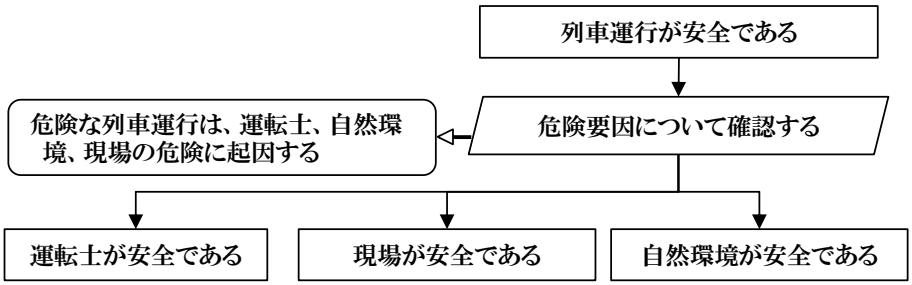


図 3-28　列車運行の安全性に対する保証ケース

この保証ケースから，図 3-29 に示すシステミグラムを作成できる．

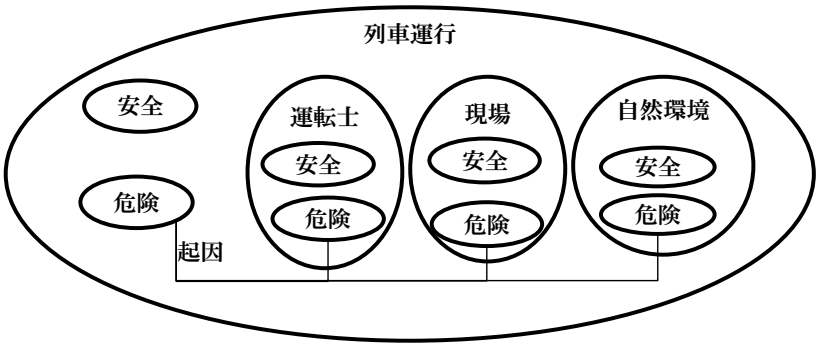


図 3-29 図 3-28 に対するシステミグラム

このシステミグラムは，レビュ規則の完全性①～④をみたしている．証拠については，図 5 の保証ケースではまだ記述していないので，完全性規則⑤は適用しない．

明確性規則②について，同名の異なるノードとして，安全と危険が出現している．しかし，これらは構成要素の状態名であり，相互に識別できるので問題にはならない．

次に，図 3-28 の「運転士が安全である」を具体化した図 3-30 について考える．

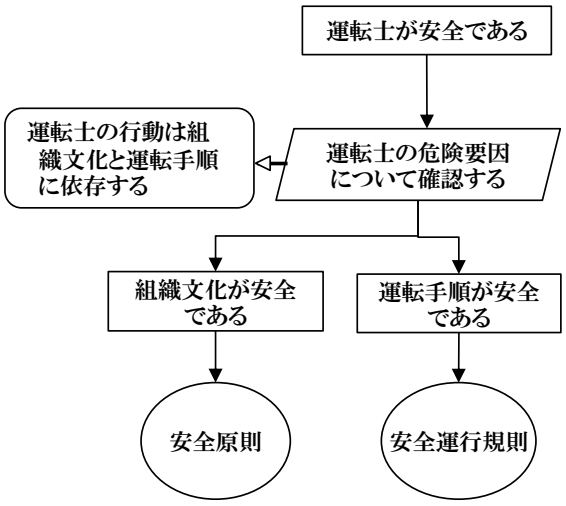


図 3-30　保証ケース「運転士が安全である」

この図 3-30 に対するシステミグラムを図 3-31 に示す.

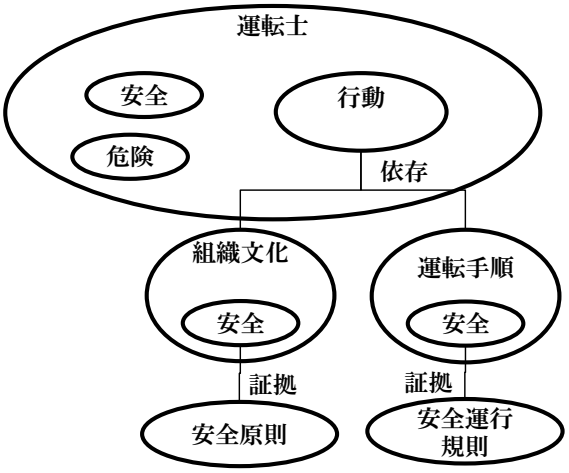


図 3-31　図 3-30 に対するシステミグラム

図 3-30 の保証ケースでは分解の前提「運転士の行動は組織文化と運転手順に依存する」で，安全に触れていないため，運転士の行動の状態として「安全」が欠落している．このため，運転士の安全と行動の安全との関係も曖昧になった．また，組織文化と運転手順の安全との関係も曖昧である．

さらに，組織文化と運転手順には，危険状態が欠落していることが分かる．したがって，組織文化が危険な状態であることと運転手順が危険であることをより明確にする必要がある．

さらに，保証ケース「現場が安全である」を図 3-32 に示す．そのシステミグラムを図 3-33 に示した.

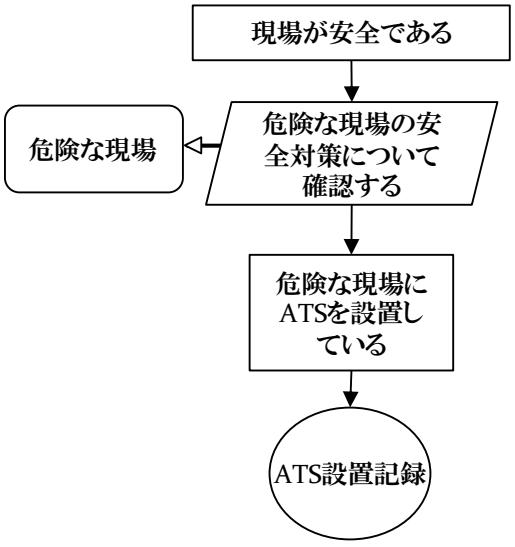


図 3-32　保証ケース「現場が安全である」

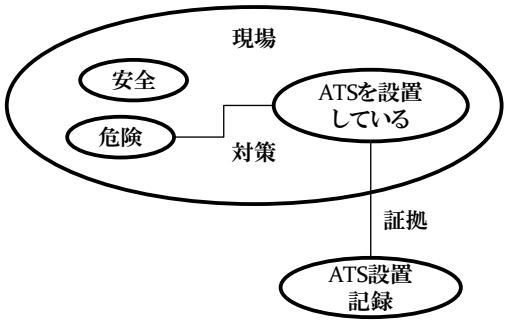


図 3-33 図 3-32 に対するシステミグラム

図 3-33 のシステミグラムでは，危険に対する対策として「ATS（Automatic Train Stop,自動列車停止装置）が設置されている」が明確になっており，証拠「ATS 設置記録」が対応付けられている．これは，図 3-27 で示した「特性，リスク，対策」の関係に対応している．

図 3-28 の保証ケースの「自然環境が安全である」を具体化した図 3-34 について考える．

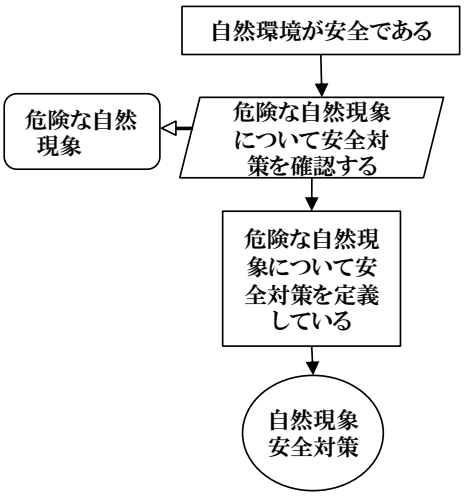


図 3-34　保証ケース「自然環境が安全である」

この図 3-34 に対するシステミグラムを図 3-35 に示す.

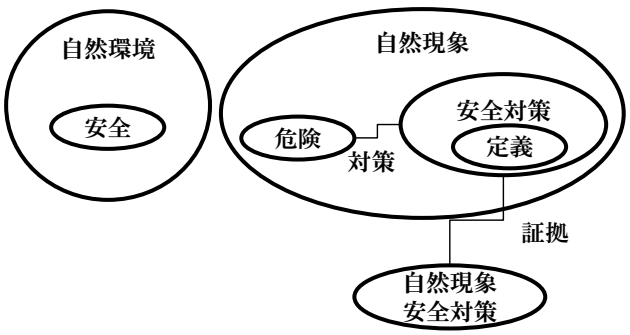


図 3-35　図 3-34 に対するシステミグラム

この図から分かるように，自然環境ではなく，自然現象に対して安全対策を定義していることが明確になった．したがって，自然環境と自然現象を統一するか，相互関係を明確にする必要がある．

上述した，保証ケースとシステミグラムの関係をまとめると，図 3-36 のようになる．

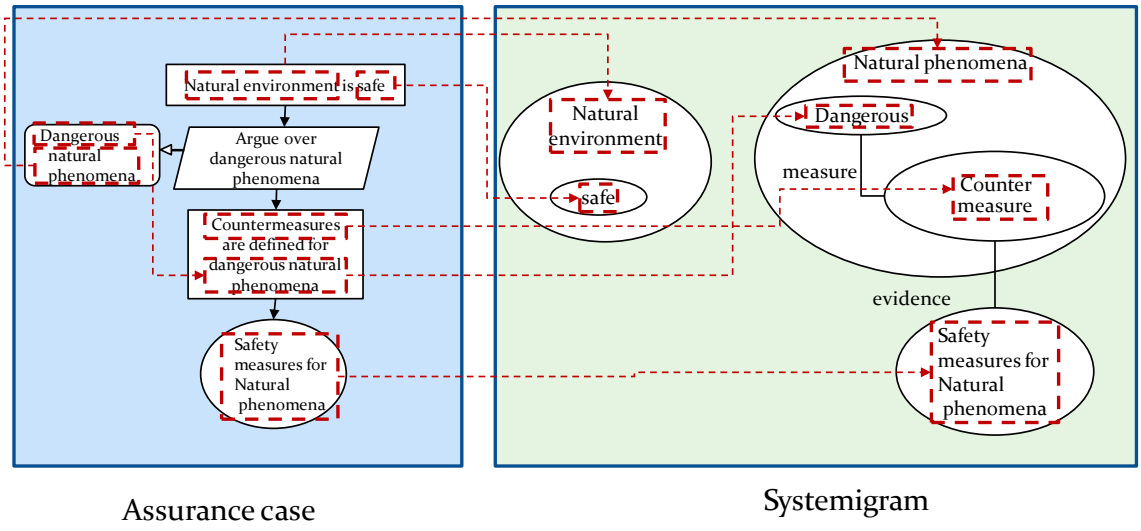


図 3-36　保証ケース(Assurance case)とシステミグラム(systemigram)の対応例

このように，保証ケースが対象とするシステムの成果物や品質特性，リスクなどの構成情報に基づいて，システミグラムを作成することで，より詳細で客観的なレビュができることを，具体例で明らかにした．とくに，具体例で使用した保証ケースは必ずしも問題があるとは思えない例である．このような例としたのは，「自然現象（Natural phenomena)」と「自然環境（Natural environment)」とを人間の設計者は同じものである認識しやすいことから，概念の食い違いが発生する可能性を見落としやすいためである．このような保証ケース上の用語の差異に起因する問題に対して具体的に問題点を指摘できた点で，本手法の効果を示していると考える．

②保証ケースレビュ指標の定式化

ここではレビュの４観点（内容理解，問題識別，原因究明，修正）ごとに実施すべき活動を抽出するとともに，その完了基準に基づいてレビュ指標を定義する．

レビュの４観点ごとに，活動と完了基準をまとめると次のようになる．

1）観点：内容理解

［活動］

対象とする保証ケースのノードに基づいてシステミグラムを作成する．

［完了基準］

保証ケースのすべてのノードについて，システミグラムを作成していること

［完了指標］

保証ケースのノードに対するシステミグラムの作成完了率

2）観点：問題識別

［活動］

システミグラムのノードに対して，表 3−2 に示したレビュ指標に基づいて，完全性，明確性，適切性，追跡性を確認する．この指標の根拠は，必要な項目が含まれていること「完全性」，あいまいさがないこと「明確性」，不必要な項目が含まれていないこと「適切性」，根拠が明確であること「追跡性」である．ここで，追跡性の観点における「関係の推移的閉包」とは，上位の特性が下位の特性に対応付けられていることと，その特性が満足されることが証拠によって確認できることを指す．

［完了基準］

システミグラムのすべてのノードについて，完全性，明確性，適切性，追跡性を確認して摘出したすべての問題を識別していること

［完了指標］

保証ケースのノードに対する問題確認の完了率

3）観点：原因究明

［活動］

識別した問題について，原因を究明する

［完了基準］

識別したすべての問題の原因を究明していること

［完了指標］

保証ケースの問題に対する原因究明の完了率

4）観点：修正

［活動］

原因が究明された問題ごとに，保証ケースを修正する

［完了基準］

すべての問題について，保証ケースを修正していること

［完了指標］

保証ケースの問題に対するシステミグラムの修正完了率

表 3-2　保証ケースレビュ指標

観点	定義	欠陥	欠陥例	指標
完全性	必要な項目が含まれていること	特性（安全），リスク（危険），対策の抜け，対策に対する証拠の抜け	必要な項目が含まれていない	不足項目数
明確性	曖昧さがないこと	同一名を持つ異なるノードがある	同名の異なるノードがある 未定義用語がある	不明項目数
適切性	不必要な項目が含まれていないこと	関係のつかない孤立ノードがある	項目の内容に誤りがある 不必要な項目が含まれている	孤立項目数
追跡性	根拠が明確であること	上位ノードから辿れないノードがある	証拠が明確でない関係の推移的閉包に抜けがある	追跡不能項目数

③保証ケースレビュ実験

ここでは同一の保証ケース事例を対象として，定式化したレビュ手順を用いる被験者と，用いない被験者に分けて保証ケースレビュ実験を実施することにより，保証ケースレビュ手順の妥当性を確認する．

実験対象システムは，図 3-37 に示す電気ポットの加熱制御システムである．このシステムに対して，「加熱が安全である」という主張に対する保証ケースを 14 名の被験者（大学院学生）が作成した．

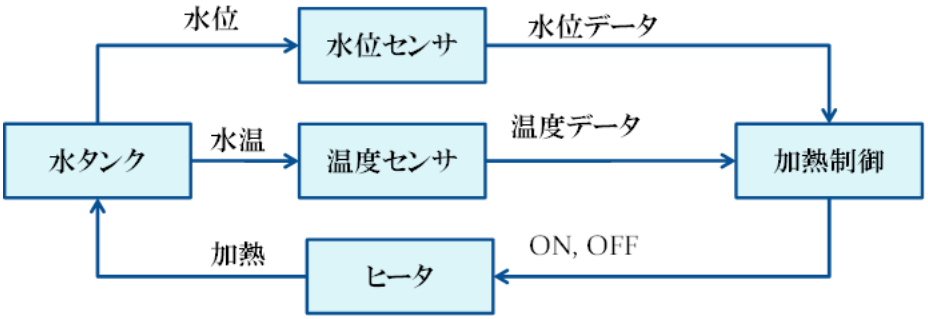


図 3-37　電気ポットの加熱制御システム

作成された 14 件の保証ケースを，保証ケースについて経験を持つ 2 名の大学院学生が次のようにしてレビュした．まず，上述したシステミグラムを用いた保証ケースのレビュ手法を適用せずにレビュした．次いで，システミグラムを用いた保証ケースレビュ手法を適用してレビュした．

レビュ手法を適用しないレビュの結果は表 3-3 のようになった．

表 3-3　指摘種別による比較

指摘種別	指摘総数	共通(%)	差異(%)
GSN の表記法が不適切	14	35.7	64.3
前提ノードの不足	21	85.7	14.3
前提の表現が不適切	11	45.5	54.5
主張の表現が不適切	13	23.1	76.9
証拠の表現が不適切	6	0	100
分解パターンが不適切	32	28.1	71.9
未定義の用語	18	0	100

指摘項目数の内訳をみると，図 3-38 のように，表記法が不適切と分解パターンが不適切に対する指摘項目数が 40%となった．未定義用語と前提の不足を加えると 74%となる．また，適切でない表現に対する指摘項目が 26%となり，約 4 分の 1 であった．

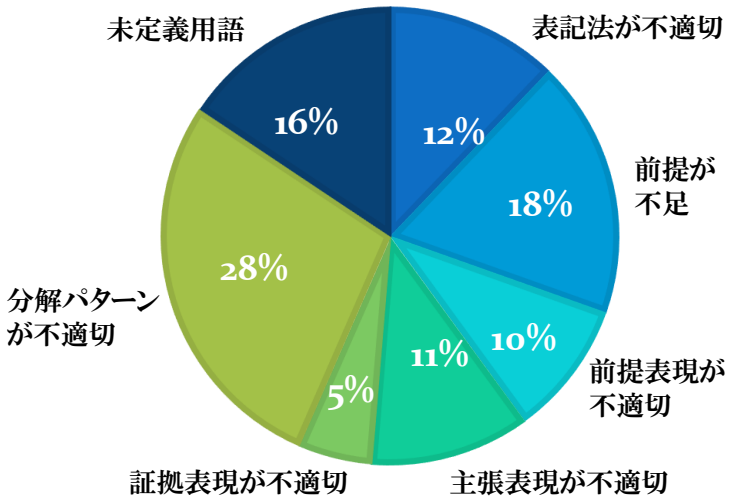


図 3-38　保証ケース指摘項目数の内訳

指摘項目数の平均は 8.2 件（最小 3 件，最大 17 件），共通指摘項目数の平均は 2.9 件（最小 0 件，最大 8 件），非共通指摘項目数の平均は 5.3 件となった．共通指摘項目数と非共通詩的項目数の比率は，34.8%対 65.2%となり，1 件の共通指摘項目に対して，2 件の非共通指摘項目が存在するという結果になった．

この結果から，レビュ手法の適用がない場合，保証ケースレビュにレビュアの属人性があることを確認した．

また，14 件の保証ケースに対する指摘項目数の分布を示すと図 3-39 のようになった．この図から，同じシステムに対して異なる担当者が保証ケースを作成すると，多様な保証ケースが作成されることが分かる．この結果は，統一的保証ケースの必要性を根拠づけている．

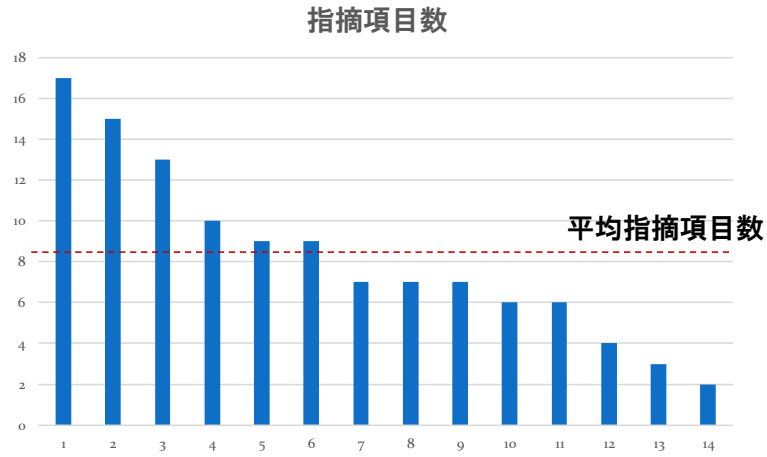


図 3-39　指摘項目数の分布

システミグラムを用いた保証ケースレビュ手法を適用したレビュでは，
a)保証ケースからシステミグラムを作成する手順を定義しておき，
b)この手順に従って被験者の作成した保証ケースからシステミグラムを作成して，
c)作成されたシステミグラムに対して，レビュ基準を用いて指摘項目を作成した．

保証ケースからシステミグラムを作成する手順を以下に示す．

【手順】保証ケースからシステミグラムを作成する手順
保証ケースの一つの証拠ノードに注目し，タイプ１の主張（G1 とする）が見つかるまでノードを上方に探索する．
G1 を見つけたら，G1 がタイプ１の主張であるから「システムが特性を持つ」ことが記述されているので，システミグラムのシステムに対応するノードとその特性ノードを作成する．
次に，G1 のすべての下位主張（G2 とする）に対して， 以下を反復する．
下位主張が存在する場合，G2 から「リスクノード」を作成する．
下位主張が存在しない場合（証拠ノードが接続されている場合），前提ノードにリスクの記述があるかどうか確認する．
リスクの記述がある場合，前提からシステミグラムの「リスクノード」を作成する．また，主張からシステミグラムの「対策ノード」を作成し，接続されている証拠ノードをシステミグラムの「証拠ノード」として作成する．
リスクの記述がない場合，主張からシステミグラムの「対策ノード」，接続されている証拠ノードからシステミグラムの「証拠ノード」を作成し，システミグラムではこれらを孤立ノードとする．
G2 のすべての下位主張 G3 に対して，以下を実行する．
G3 からシステミグラムの「対策ノード」を作成する．
G3 に下位主張がある場合，下位主張から，システミグラムの「対策ノード」の要素を作成する．

G3 または G3 の下位主張に接続されている証拠ノードから，システミグラムの「証拠ノード」を作成する．

全ての証拠ノードに対して，システミグラムの「証拠ノード」を作成し終えるまで，上記の手順を繰り返す．

【手順おわり】

14 件の保証ケースに対してシステミグラムを用いてレビュした結果を表 3-4 と図 3-40 に示した．適切性と追跡性の件数が一致しているのは，孤立ノードについては，上位ノードとの関係が追跡できなくなるためである．

表 3-4

項目	平均指摘項目数
完全性	2.57
明確性	4.07
適切性	5.50
追跡性	5.50
合計	17.64

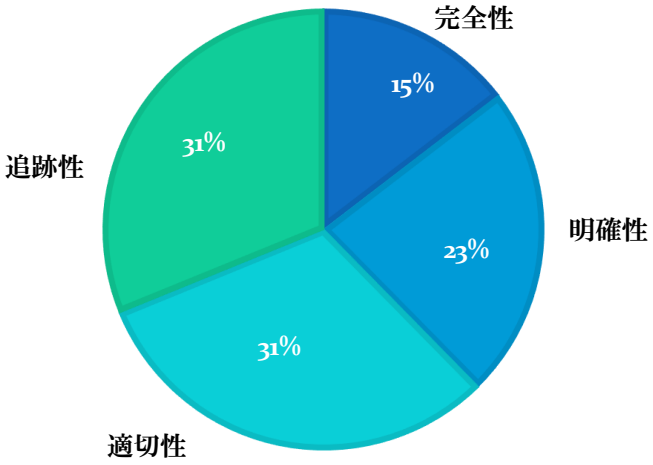


図 3-40　指摘項目数の内訳

図 3-41 の保証ケースについて，レビュ事例を比較すると以下のようになる．

保証ケースだけのレビュでの指摘件数は 6 件であった．保証ケースだけのレビュでは，ほとんどが前提に関する指摘で，表記法の誤りや主張内容の不適切さなどが指摘できていないというレビュ結果となった．

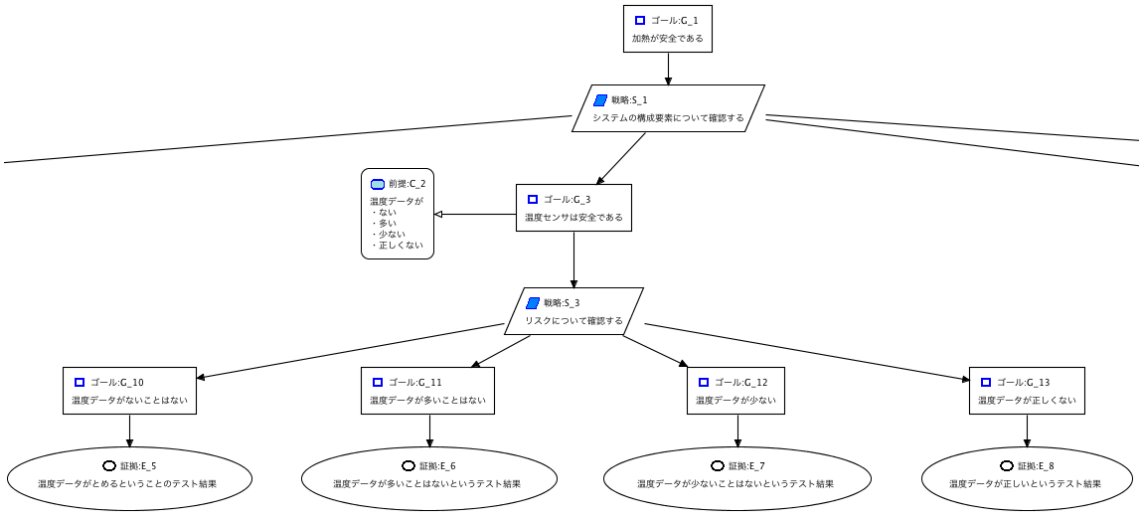


図 3-41　保証ケースの例（一部）

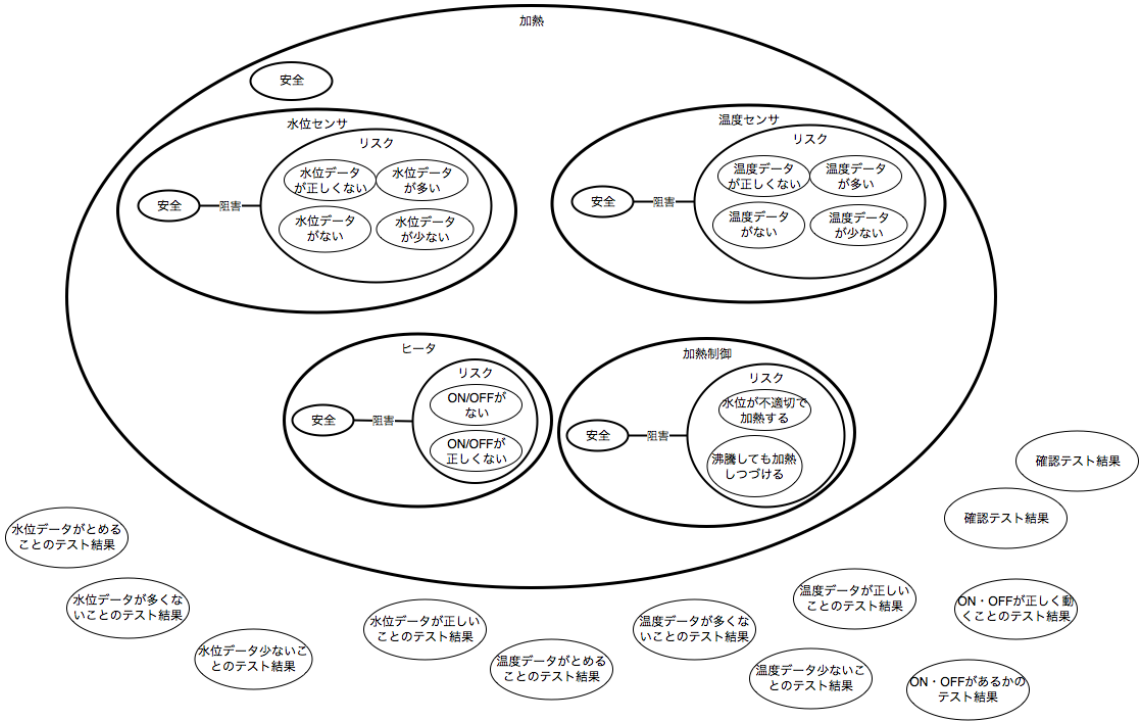


図 3-42　図 3-41 の保証ケースから作成したシステミグラムの例

これに対して，図 3-41 から作成したシステミグラムは図 3-42 のようになる．このシステミグラムを用いたレビュでの指摘件数は 30 件であった．システミグラムを用いたレビュでは，対象として保証ケースで多くのリスクが挙げられているものの，リスクに対する対策が一つも挙げられていないことが判明した．また，対策が挙げられていないため，保証ケースの証拠ノードで示された様々なテスト結果が，不必要な証拠として指摘された．この結果，レビュ指摘件数が多くなった．

3.3.3 発生した問題および今後の展望

(1) 発生した問題

保証ケースをレビュする場合，ゴール構文を２種類に限定して，システミグラムを作成する方法を用いた．この場合，この２種類で十分ではない可能性がある．このため，より多くの保証ケースをレビュすることで，ゴール構文の十分性を評価する必要がある．もし，十分でない場合については，保証ケースのゴール構文を追加して対応するシステミグラムに変換する方法を用意することで対処できる．

(2) 今後の展望

保証ケースのゴール構文の十分性について評価することにより，もし不十分であれば対応するシステミグラムへの変換規則を追加することができる．

3.4 研究課題 4「実践的保証ケース研修教材の試作」

3.4.1 当初の想定

(1) 研究内容

統一的な保証ケース作成手法と保証ケースレビュ手法について，研修教材を試作して実験評価する．なお，コード情報に基づく保証ケース作成手法については，教材設計までの実施とする．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試作する．

(2) 想定問題と対応策

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．また教材量が多すぎると学習者が理解できないという問題がある．このため，ISD 原則に従い，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．本研究課題に対する問題設定と解決策の妥当性について大学ならびに企業の有識者からのアドバイス評価を実施する．

3.4.2 研究プロセスと成果

(1) 研究プロセス

①研修教材の設計

ISD 原則に基づき，統一的保証ケース作成手法と保証ケースレビュ手法についての研修教材を設計する．保証ケースレビュ手法の教材では，レビュ指標に関する内容は，高度な研究要素を含むことから実践的な教材に含めるのは時期尚早であることから割愛する．

②研修教材の試作

統一的保証ケース作成手法と保証ケースレビュ手法について，研修教材を試作する．本研修教材の試作は外注により，実施した．

③研修教材の実験評価

試作した研修教材による研修を実施し，研修教材の有効性を評価する．研修は座学による個人演習,研修教材ごとに計２回実施する.対象者は社会人で各研修 40 名程度を想定する．本研修は外注により，実施した．

(2) 具体的な研究成果の内容

①研修教材の設計

ここでは ISD 原則に基づき，統一的保証ケース作成手法と保証ケースレビュ手法についての研修教材を設計する．ここで，ISD（Instructional System Design）原則とは，教育をシステムとしてとらえることにより，教育システムを設計する原則である．

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

統一的保証ケース作成手法についてのコースマップを図 3-43 に示す.

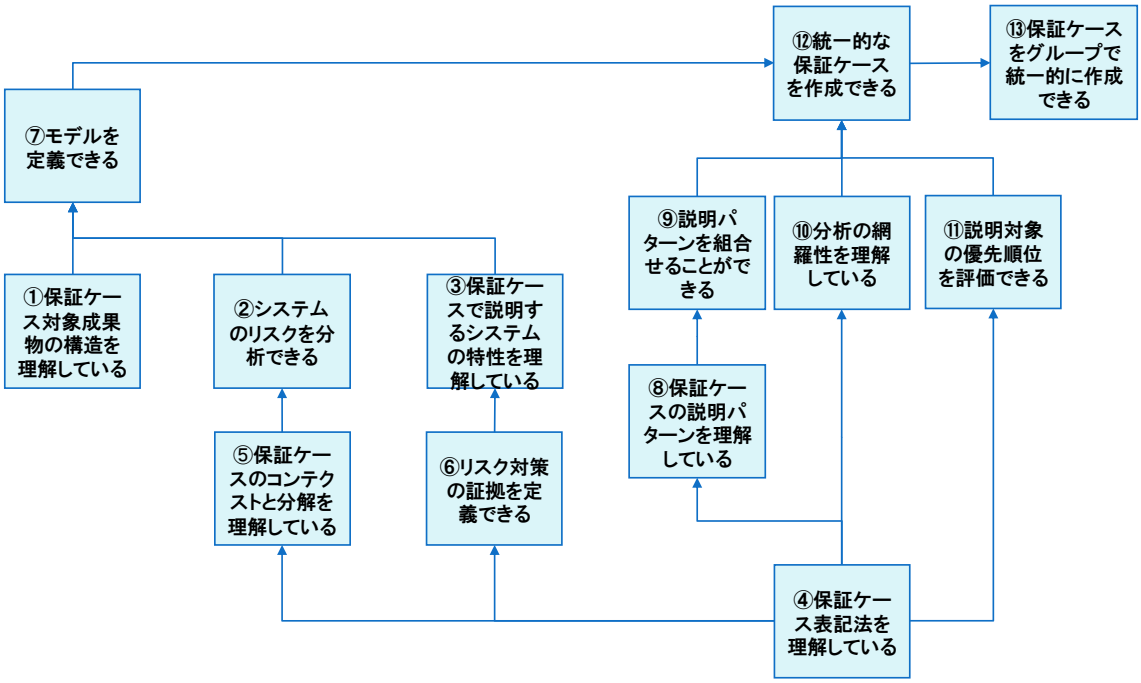


図 3-43　統一的保証ケース作成手法コースマップ

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，表 3-5 に示す.

表 3-5　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保証ケースの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の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.

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．

また，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

保証ケースレビュ手法コースマップを図 3-44 に示す．また，コース単元の内容を表 3-6 に示す．

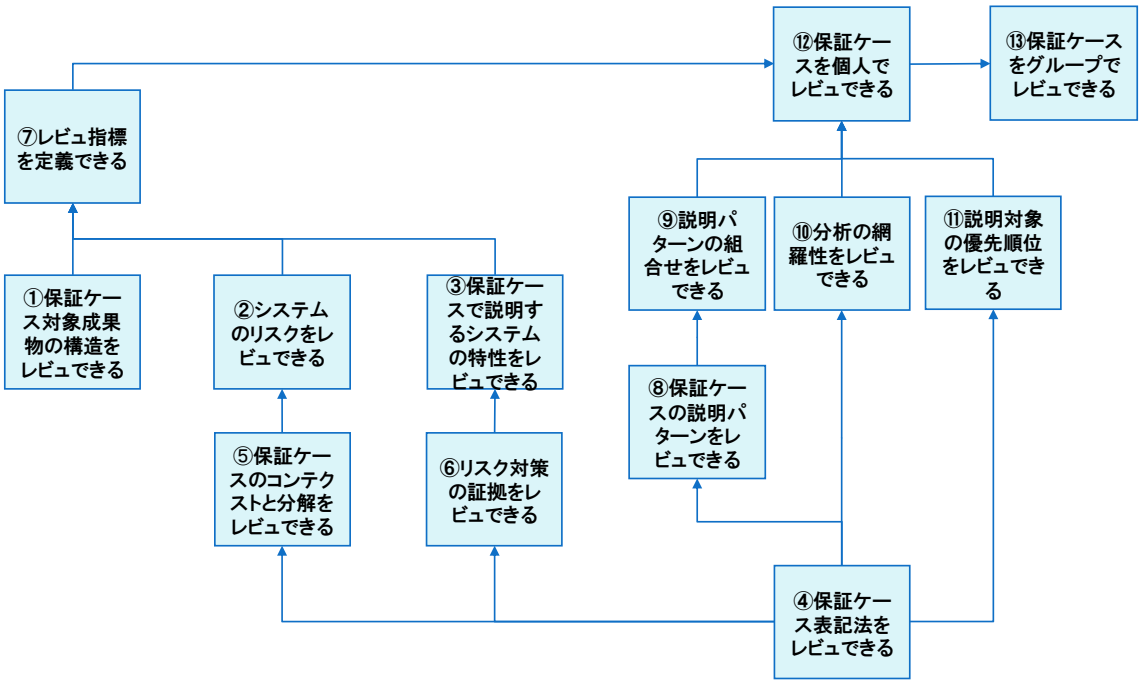


図 3-44　保証ケースレビュ手法コースマップ

表 3-6　保証ケースレビュ手法コースの単元

コース単元	説明
① 品質特性，リスク，対策の関係を理解できる	保証ケースで扱う概念要素の相互関係を理解して説明できるスキルを習得する.
② 保証ケースの表記法を理解できる	主張，コンテクスト，説明分解，証拠からなる保証ケースの表記法についてのスキルを習得する.
③ 保証ケースの主張の問題点を指摘できる	保証ケースで記述すべき主張の構文特性を理解できるスキルを習得する.
④ 保証ケースの分解の問題点を指摘できる	保証ケースで主張を分解する際の構文特性などの前提条件を理解できるスキルを習得する.
⑤ 保証ケースを網羅的にレビュできる	保証ケースの内容に従って，上位の主張から段階的に下位の主張と証拠をレビュするスキルを習得する.
⑥ システミグラムの表記法を理解できる	システミグラムの構成要素と関係を理解するためのスキルを習得する.
⑦ システミグラムで主張を表現できる	システミグラムによって，保証ケースの主張を構成する単語関係を見える化するスキルを習得する.
⑧ システミグラムで分解を表現できる	システミグラムによって，保証ケースの分解を構成する単語関係を見える化するスキルを習得する.
⑨ システミグラムで証拠を表現できる	システミグラムによって，保証ケースの主張とその証拠との説明関係を見える化するスキルを習得する.
⑩ システミグラムで保証ケースをレビュできる	システミグラムによって，保証ケース全体をレビュするスキルを習得する.
⑪ 保証ケースのレビュ指標を作成できる	保証ケースのレビュ指標をシステミグラムに基づいて定量的に定義するスキルを習得する.
⑫ 保証ケースを個人でレビュできる	最上位の主張から，分解構造に従って証拠にいたるまで階層的に保証ケースをレビュするスキルを習得する.
⑬ 保証ケースをグループでレビュできる	保証ケースを複数人でレビュすることにより客観的に合意形成できるスキルを習得する.

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.

②研修教材の試作

ここでは統一的保証ケース作成手法と保証ケースレビュ手法について，研修教材を試作する．

試作した研修教材の概要を表 3-7 に示す．

表 3-7 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

以下では，2 つの研修教材の試作内容を説明する．

1) 統一的保証ケース作成手法の研修教材

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，図 3-45 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．

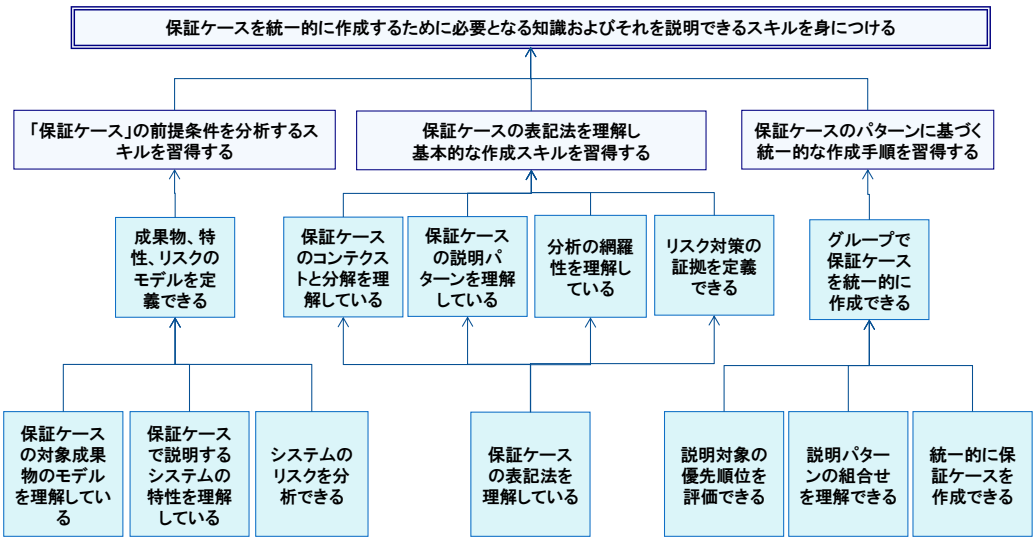


図 3-45　保証ケースのスキル構成概要

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．学習効果は図3-45のスキル構成で示した内容を習得することで，モデルに基づいて統一的に保証ケースが作成できることである．

13項目の教材本体・確認問題・演習ワークシート（回答・回答例を含む）をパワーポイントのスライド形式で作成する．本教材では表2に示した13単元を作成することとした．

なお，システムのリスク分析では，システムの構成要素と構成要素間の相互作用についての逸脱を分析する．逸脱分析の範囲については，逸脱を示唆するガイドワード「ない」「早い」「遅い」「過剰」「過少」などによって限定する知識を提示することとした．

各研修単元を，表3-8に示すように，基本概念，例，練習から構成した．

表3-8　研修単元の基本構成

種類	説明
基本概念	単元が対象とするスキルが必要とする知識を説明する
例	基本概念を分かりやすく説明する具体例を提示する
確認問題	基本概念を習得したことを確認する練習問題を提示する

また，研修単元ごとに作成する教材スライドの基本概念では，学習内容を説明することとした．図3-45に示した13項目のスキルを学習する時間と配分について，以下の表3-9に示すカリキュラムで決定した．

表3-9　統一的保証ケース研修カリキュラムの構成

時間	カリキュラム
13:30～14:50	第1章　保証ケースを統一的に作成するための基礎知識 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

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についての研修教材の試作では,「保証ケース」を分析するスキル,保証ケースの問題点を見える化するスキル，保証ケースの問題点を客観的にレビュするスキルに基づいて，保証ケースを客観的にレビュするために必要となる知識およびそれを説明でき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.

この研修教材が対象とする学習目標は，図 3-46 に示す構成により，保証ケースのレビュスキルを本教材で習得することである.

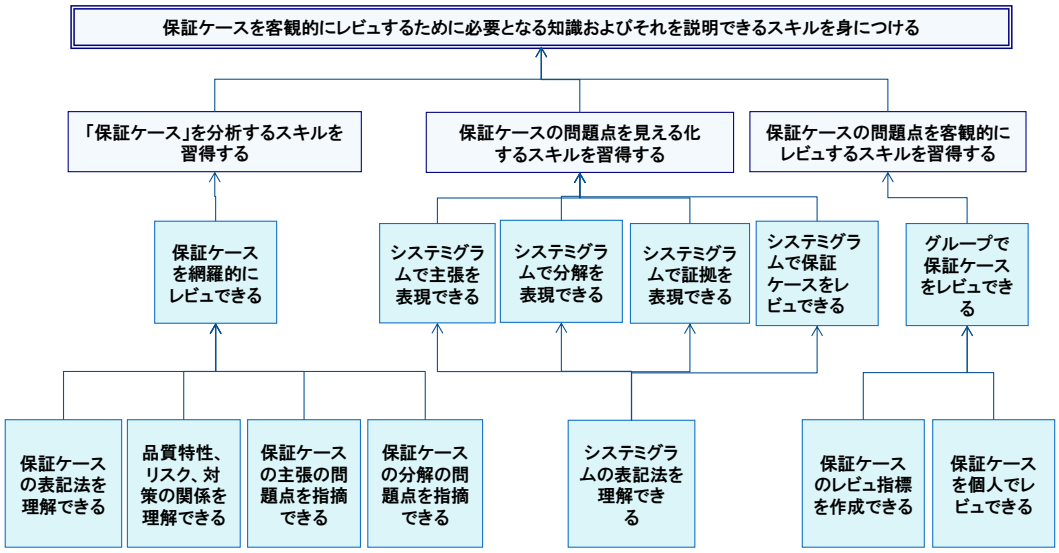


図 3-46　保証ケースレビュのスキル構成概要

本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．図 3-46 のスキル構成で示した内容を習得することで，システミグラムに基づいて客観的に保証ケースがレビュできることが本研修の学習効果である.

図 3-46 に示した 13 項目のスキルを学習する時間と配分について，以下の表 3-10 に示すカリキュラムで決定した.

表 3-10　保証ケースレビュ手法　研修カリキュラムの構成

時間	カリキュラム
13:30～14:50	第 1 章　　保証ケースをレビュするための基礎知識 1.1　　システム要素の相互関係 1.2　　保証ケースの表記法 1.3　　主張の問題点 1.4　　分解の問題点 1.5　　網羅的なレビュ
15:00～16:20	第 2 章　　保証ケースをレビュするための知識・スキル 2.1　　システミグラムの表記法 2.2　　システミグラムで主張 2.3　　システミグラムで分解 2.4　　システミグラムで証拠を表現 2.5　　保証ケースのレビュ 2.6　　保証ケースのレビュ指標 2.7　　個人レビュ
16:30～17:30	第 3 章　　保証ケースによる合意形成 3.1　　グループレビュ アンケート

③研修教材の実験評価

ここでは試作した研修教材による研修を実施し，研修教材の有効性を評価する．

保証ケース統一作成手法の研修教材と運営方法の有効性を確認するために，2 回に分けて研修を実施した．第 1 回研修を 11 月 6 日に，第 2 回研修を 11 月 13 日に，それぞれ実施した．第 1 回研修では，表 3-9 に基づき，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，表 3-9 の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 3-11 に示す．

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．

次に，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 3-47 と図 3-48 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．

表 3-11　保証ケース統一的作成法の研修結果

	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%

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

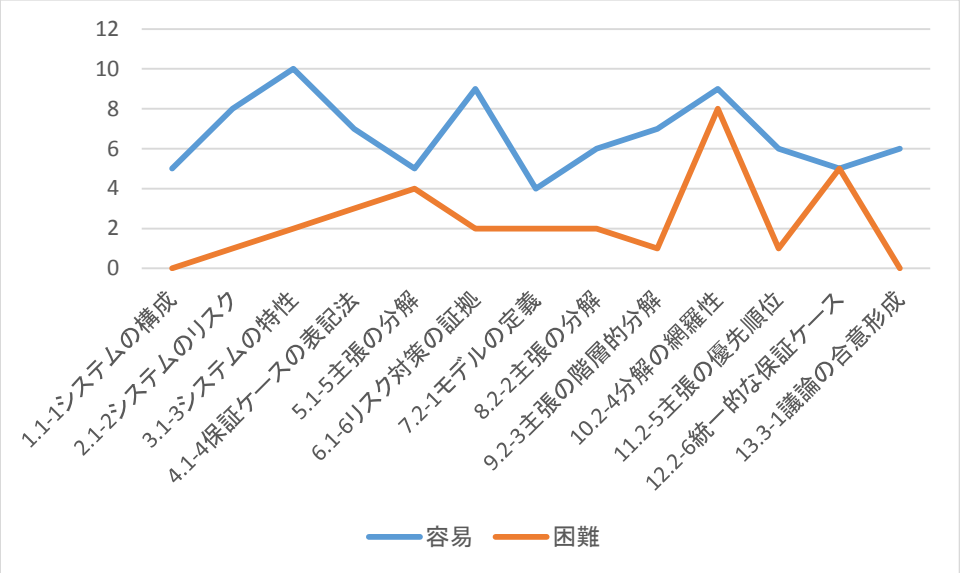


図 3-47　第 1 回研修の理解度

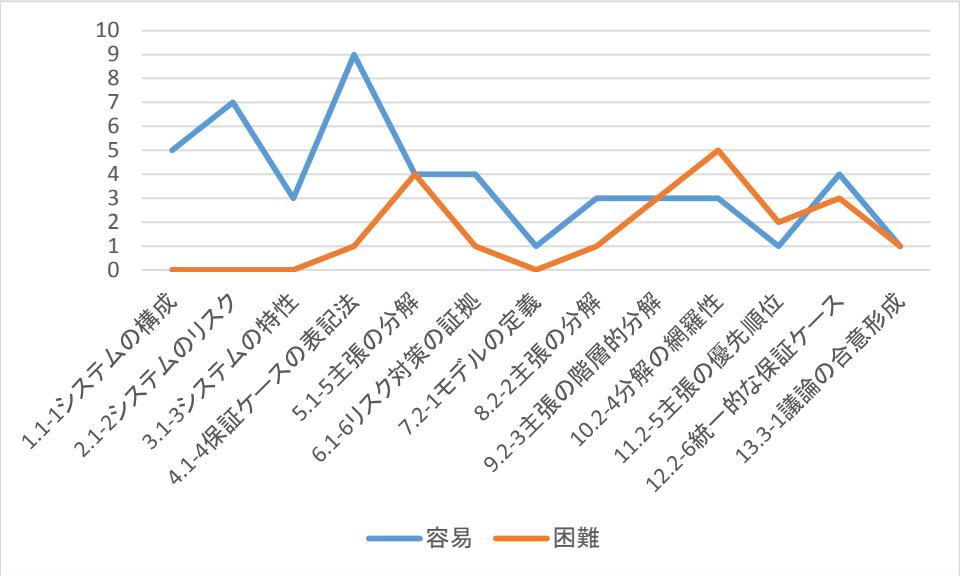


図 3-48　第 2 回研修の理解度

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，以下のとおりである．

- 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，理解が容易だと回答した参加者が多かったことから，教材内容は適切である．
- 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．

次に，保証ケースレビュ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 回研修を 1 月 18 日に，第 2 回研修を 1 月 22 日に，それぞれ実施した．第 1 回研修では，表 3-10 に基づき，座学で保証ケースの基礎知識を説明した後，保証ケースのレビュを個人並びにグループで実施して保証ケースのレビュが属人的になることを体感してもらった．その後に，レビュ手法を説明して保証ケースをグループでレビュする演習を実施した．第 2 回研修でも，第 1 回と同じ構成で研修を実施した．2 回の研修の参加者とアンケート回答者数に基づいて比較した結果を表 3-12 に示す．

第 2 回研修では演習時間十分性と教材充足性が低下した．しかし，それ以外については第 1 回研修よりも評価が向上している結果になった．時間について不足しているという結果となったが，半日研修としたためで，1 日で研修を実施することでこれらの項目についての評価も改善できると思われる．

表 3-12　保証ケースレビュ手法の研修結果

	第 1 回	第 2 回
研修参加者(経験者数)	24 名(2)	23 名(2)
満足度（注１）	95.7%	95.7%
理解度（注１）	100%	100%
活用度（注１）	95.7%	100%
研修時間十分性（注２）	59.1%	76.2%
難易度（注３）	77.3%	85.0%
演習満足度（注１）	76.9%	92.9%
演習時間十分性（注２）	72.7%	68.4%
教材充足性（注１）	100%	92.3%

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 回研修では演習時間を長めに設定したとしたことから演習満足度が向上している．しかし，演習時間が長い分，内容について深堀することができたため，逆に演習時間十分性については時間がもっと必要だという結果になった．

次に，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 3-49 と図 3-50 にまとめる．なお，図 3-49 と図 3-50 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．

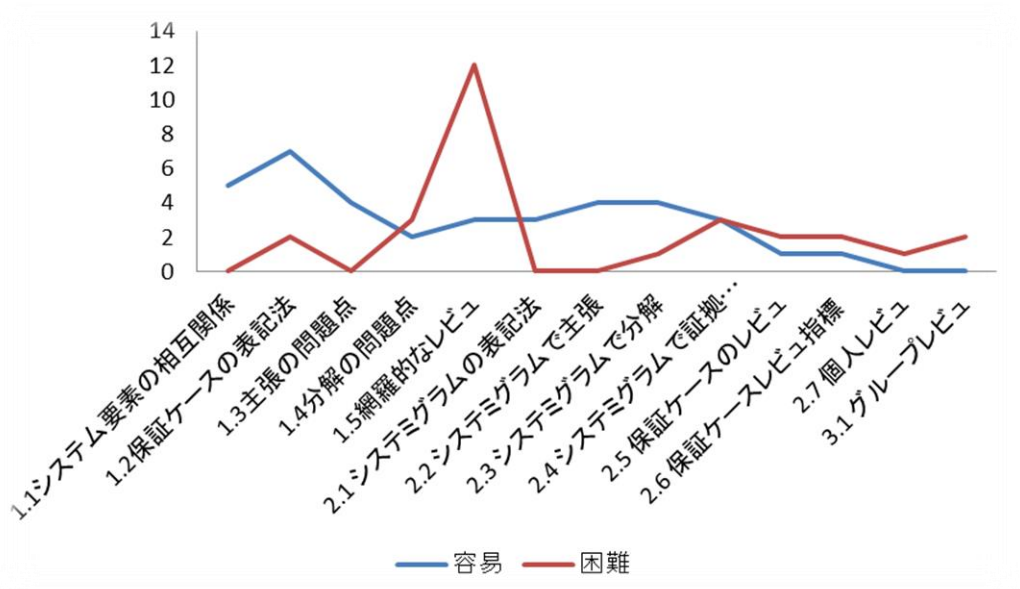


図 3-49　第 1 回研修の理解度

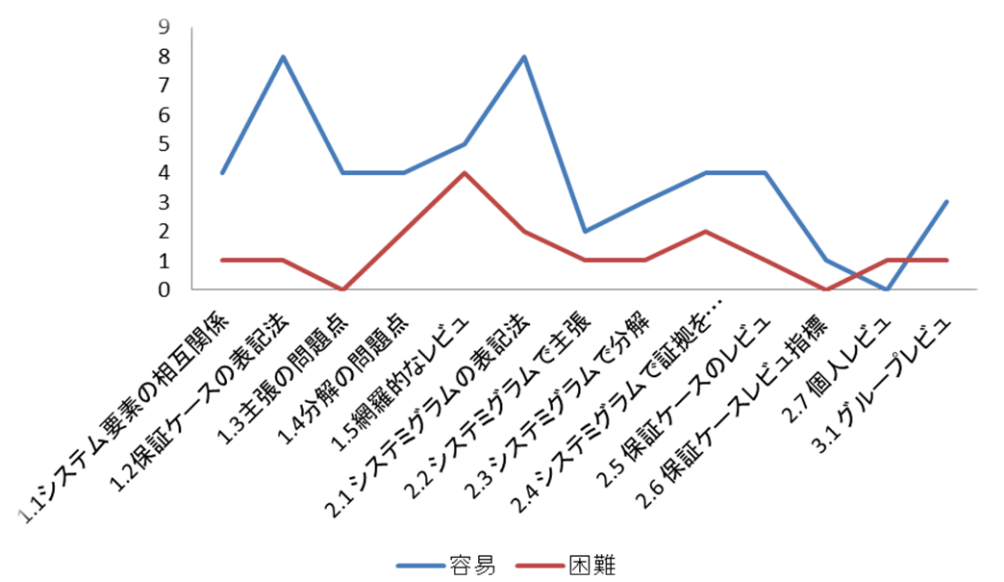


図 3-50　第 2 回研修の理解度

図 3-49 と図 3-50 の結果から，第 1 回研修では「分解の問題点」「網羅的なレビュ」「保証ケースのレビュ」「保証ケースのレビュ指標」「個人レビュ」「グループレビュ」など半数近くの章において困難という意見が容易という意見を上回った．

第 2 回研修では講義は基本的な説明を増やし，演習は時間を長めに設けたことから「個人レビュ」以外の章においては容易という意見が困難という意見を上回った．「個人レビュ」はいずれの回においても困難という意見が多く，保証ケースの経験がない受講者では個人レビュが難しいことがわかった．

3.4.3 発生した問題および今後の展望

(1) 発生した問題

研修参加者の目標人数を 40 としたが，実際にはどの研修でも 20 名から 24 名の参加となった．一方，2 回の研修参加者を合計すると 40 名を超えること，また参加者の平均経験年数が 7 年を超えること，参加者の満足度が 97.7%であったことから，研修教材の妥当性を確認するという目標を達成できたと考えられる．

(2) 今後の展望

目標人数には届かなかったが，新技術についての企業向けの研修で，20 名以上の参加者を確保できた点では，満足できると考えられる．

3.5 研究課題 5「保証ケース手法の実践的導入適合性」

3.5.1 当初の想定

(1) 研究内容

保証ケース手法の開発現場への実践的な導入可能性を判断するための適合性指標を考案する．また，適合性指標に基づくヒヤリングを企業に対して行い，保証ケース作成法の必要性と試作した研修教材作成の妥当性を明らかにする．

(2) 想定問題と対応策

技術面・管理面で，保証ケースを導入できるだけの準備が整っている企業の適切な担当者でないと，保証ケース手法・教材を適切に評価できないという問題がある．

このため，保証ケースのヒヤリング項目の設計では，技術面と管理面での導入準備能力を評価できる確認項目を定義・測定することにより，保証ケースの作成・レビュ手法・研修教材についての現場ニーズとの適合性ならびに，企業の導入準備能力との関係を客観的に評価する手法（具体的には「保証ケース手法の開発現場への実践的な導入可能性を判断するための適合性指標」のこと）を開発する．手法の開発は作業項目①と②で実施する．

3.5.2 研究プロセスと成果

(1) 研究プロセス

①導入準備能力指標設計

保証ケース手法の開発現場への実践的な導入可能性を判断するための適合性指標を開発する．

②ヒヤリング項目設計

ヒヤリング項目の設計では，（イ）ヒヤリング対象組織の状況に対する質問項目，（ロ）適合性指標に対応する質問項目，（ハ）本研究項目のニーズについての質問項目を具体化する．

③ヒヤリング評価実施

ヒヤリング項目に基づいて，企業に対するヒヤリングを実施する．収集したヒヤリング情報に基づいて（イ）（ロ）（ハ）の項目間の依存関係を評価することにより，保証ケース作成法の必要性と研修教材作成の妥当性を明らかにする．

(2) 具体的な研究成果の内容

①導入準備能力指標設計

ここでは保証ケース手法の開発現場への実践的な導入可能性を判断するための導入準備能力指標（適合性指標）を開発する．

保証ケース導入準備能力を，IT ケイパビリティの 5 次元（IT 活用ビジョン，IT 活用コミュニケーション，IT 活用プロセス，IT 投資適正化，IT 人材開発）[28]に基づいて，①保証ケース構築能力，②リスク分析能力，③保証ケース活用ビジョン構築能力，④保証ケース活用コミュニケーション，⑤保証ケース活用プロダクトデザイン，⑥保証ケース活用プロセスデザイン，⑦保証ケース投資適正化，⑧システム保証人材開発に分類した．ここで，保証ケースに関する能力次元を測定するために，保証ケース構築能力，リスク分析能力，保証ケー

ス活用プロダクトデザイン能力を追加した．この保証ケース導入準備能力分類ごとに，設定した評価指標の個数を，表 3-13 に示す．

表 3-13　保証ケース導入準備能力の分類と評価指標項目数

	能力分類	評価指標項目数
1	保証ケース構築	7
2	リスク分析	8
3	保証ケース活用ビジョン構築	7
4	保証ケース活用コミュニケーション	7
5	保証ケース活用プロダクトデザイン	5
6	保証ケース活用プロセスデザイン	5
7	保証ケース投資適正化	6
8	システム保証人材開発	5

具体的な評価指標の内容を表 3-14 に示す．なお，表中の AC(Assurance Case)は保証ケースのことである．

表 3-14　保証ケース導入準備能力評価指標 50

能力	評価指標
保証ケース構築（7）	①保証原則の定義 ②保証の根拠証拠の管理 ③保証対象の明確な定義 ④保証すべき主張の明確な定義 ⑤主張間の優先順位が明確 ⑥説明責任部門が明確 ⑦コンプライアンス課題の認識
リスク分析（8）	①保証の欠落がもたらす開発業務への影響を識別 ②リスク管理原則を定義 ③リスク管理計画を定義 ④リスク管理手順を定義 ⑤リスク管理情報を共有 ⑥リスクを評価 ⑦問題情報を共有 ⑧リスク対応手段を定義
保証ケース 活用ビジョン構築 (7)	①自社戦略目標と AC の役割が明確 ②AC が役割を果たすための組織を制度化 ③AC 投資を重点化 ④開発での AC の活用方針を明確化 ⑤AC 部門の役割が明確 ⑥AC 部門と開発部門の役割が明確 ⑦AC に基づく開発部門の結果責任が明確
保証ケース活用 コミュニケーション (7)	①AC の役割を社員が共有 ②AC の活用方針を社員が共有 ③AC 導入目的を開発部門が理解 ④AC 導入後の業務変化を開発部門が理解 ⑤部門間で AC による問題解決プロセスが定義 ⑥AC 活用事例を社内で共有する仕組みを定義 ⑦経営層，AC 部門，開発部門の３部門間で，AC の投資対効果を共有
プロダクト デザイン(5)	①成果物に対する保証品質を定義 ②成果物に対するあるべき AC 条件を定義 ③成果物に対する AC の活用方策を標準化 ④社内外の開発業務連携の観点で成果物に対する AC を標準化 ⑤成果物に対する重複のない AC を定義
プロセス デザイン（5）	①開発プロセスの保証計画を定義 ②AC による開発プロセスを定義 ③開発プロセスの AC 活用方策を標準化 ④社内外の業務連携プロセスを AC で標準化 ⑤AC の重複のない開発プロセスを実現
保証ケース 投資適正化(6)	①AC 資産の構築経費を配分 ②AC 部門の独立性を考慮 ③AC 導入経費対効果を事前に検証 ④AC 導入時に全社最適への適合性を検討 ⑤AC 導入後に活用状況・効果を測定 ⑥AC 活用問題を AC 導入検討時に解決
システム保証 人材開発（5）	①AC を活用した開発プロセス改革の提案人材を育成 ②経営層の身近に開発と AC の双方に精通した人材を配置 ③AC 人材が経営に関する知識を習得する機会を提供 ④AC 人材が現場の開発プロセスを理解する機会を提供 ⑤開発人材に AC の活用スキル研修を提供

②ヒヤリング項目設計

ここでは，国内の企業がどの程度まで，保証ケースの導入に向けた準備能力と本研究課題のニーズならびに，両者の相関関係を明らかにすることを目的とした．

保証ケースヒヤリング項目の設計では，上述した保証ケース導入準備能力評価指標 50 項目を表 3-15 に示すように 37 項目に削減して，回答しやすいようにした．変更点は以下の 3 点である．

・保証ケース構築能力を保証ケース基礎とし，7 項目から 3 項目に集約した
・保証ケース投資適正化を 6 項目から 5 項目とした
・リスク分析知識についての項目をすべて削除した．リスク分析知識については，十分な経験のある回答者を対象としたことから担当業務の中で実践していると思われることと，ヒヤリング項目数を削減してできるだけ，多忙な回答者の負担を軽減しようとしたことから，ヒヤリングしなくてもよいと判断したためである．

表 3-15　保証ケースヒヤリング項目 37

能力	評価指標
保証ケース基礎（3）	①保証ケースの基礎 ②保証ケースの必要性③保証ケースの効果
保証ケース 活用ビジョン構築 (7)	①自社戦略目標と AC の役割が明確 ②AC が役割を果たすための組織を制度化 ③AC 投資を重点化 ④開発での AC の活用方針を明確化⑤AC 部門の役割が明確 ⑥AC 部門と開発部門の役割が明確 ⑦AC に基づく開発部門の結果責任が明確
保証ケース活用 コミュニケーション (7)	①AC の役割を社員が共有 ②AC の活用方針を社員が共有 ③AC 導入目的を開発部門が理解 ④AC 導入後の業務変化を開発部門が理解 ⑤部門間で AC による問題解決プロセスが定義 ⑥AC 活用事例を社内で共有する仕組みを定義 ⑦経営層，AC 部門，開発部門の３部門間で，AC の投資対効果を共有
プロダクト デザイン(5)	①成果物に対する保証品質を定義 ②成果物に対するあるべき AC 条件を定義 ③成果物に対する AC の活用方策を標準化 ④社内外の開発業務連携の観点で成果物に対する AC を標準化 ⑤成果物に対する重複のない AC を定義
プロセス デザイン（5）	①開発プロセスの保証計画を定義 ②AC による開発プロセスを定義 ③開発プロセスの AC 活用方策を標準化 ④社内外の業務連携プロセスを AC で標準化 ⑤AC の重複のない開発プロセスを実現
保証ケース 投資適正化(5)	①AC 資産の構築経費を配分 ②AC 導入経費対効果を事前に検証③AC 導入時に全社最適への適合性を検討　④AC 導入後に活用状況・効果を測定 ⑤AC 活用問題を AC 導入検討時に解決
システム保証 人材開発（5）	①AC を活用した開発プロセス改革の提案人材を育成 ②経営層の身近に開発と AC の双方に精通した人材を配置 ③AC 人材が経営に関する知識を習得する機会を提供 ④AC 人材が現場の開発プロセスを理解する機会を提供 ⑤開発人材に AC の活用スキル研修を提供

ヒヤリングでは，回答しやすいように，「はい」「いいえ」として「保証ケース技術導入準備・アンケート調査票」を作成した．この 37 項目の質問は適合性指標に対応しており，ヒヤリング対象組織の状況を明らかにすることができる．なお，適合性指標に対してヒヤリング対象組織がどのような状況であるかを質問するため，ヒヤリング対象組織の状況に対する質問項目と，適合性指標に対応する質問項目を区別していない．また，各研究課題の必要性についても対応した 5 項目を設けることとした．この質問では，①大いに必要である，②必要である，③疑問がある，④不要であるという 4 個の中から 1 つを選択して回答することとした．この 5 項目の質問によって，本研究項目のニーズを明らかにすることができる．

3) ヒヤリング評価実施

ヒヤリング項目に基づいて，企業に対するヒヤリングを実施する．収集したヒヤリング情報に基づいて，ヒヤリング対象組織の状況に対する質問項目，適合性指標に対応する質問項目，本研究項目のニーズの項目間の依存関係を評価することにより，保証ケース作成法の必要性と研修教材作成の妥当性を明らかにする．研究の必要性については，①統一的保証ケース作成手法，②コード保証ケース作成手法，③保証ケースレビュ手法，④保証ケース研修教材，⑤保証ケース導入準備能力評価指標からなる 5 項目で回答してもらうようにした．

a. ヒヤリングの実施

保証ケースについて経験のある企業および大学の担当者 30 名に対して，メールでヒヤリング調査への協力を依頼したところ，18 名からの回答があった．組織規模の内訳は，従業員数 1 万名以上が 6，1 万名未満千名以上が 2，千名未満 100 名以上が 5，100 名未満が 5 となった．18 名の所属の内わけは，システム開発企業 7，メーカ 6，ツール開発，検証，IT 教育，コンサル，大学が各 1 であった．なお，担当業務の内訳は，技術開発 6，SE 4，研究開発 3，品質保証 2，教育 2，コンサル 1 であった．また，保証ケースの導入に具体的に取り組んでいる先導的な企業に対して対面でヒヤリングを実施した．

b. ヒヤリング結果

図 3-51 に，回答結果に基づいて，本受託研究の必要性と導入準備能力評価指標の値の関係を示した．ここで，研究の必要性については，5 つの研究項目ごとに 3 点満点として，大いに必要がある，必要がある，研究に疑問がある，研究する必要はない，のいずれかを選択してもらった．回答の数値化では，「大いに必要がある」を 3，「必要がある」を 2，「研究に疑問がある」を 1，「研究する必要はない」を 0 として数値化した．

この結果から保証ケース導入準備能力の平均が 0.22，研究の必要性の平均値が 2.75 となった．研究課題単位で平均を示すと，統一的保証ケース作成法が 2.67，コード保証ケース作成手法が 2.39，保証ケースレビュ手法が 2.67，保証ケース研修教材が 2.61，保証ケース導入準備能力評価指標が 2.5 となった．

ヒヤリング対象組織のうち，システム開発とメーカについて各研究の必要性を示すと次のようである．システム開発企業では，統一的保証ケース作成法が 2.71，コード保証ケース作成手法が 2.29，保証ケースレビュ手法が 2.71，保証ケース研修教材が 2.57，保証ケース導入準備能力指標が 2.71 となった．また，メーカ企業では，統一的保証ケース作成

法が 2.5，コード保証ケース作成手法が 2.12，保証ケースレビュ手法が 2.5，保証ケース研修教材が 2.5，保証ケース導入準備能力指標が 2.33 となった．

したがって，本受託研究は，すべての研究課題について企業担当者から，「研究する必要がある」以上で「大いに研究する必要がある」に近い高評価が得られた．一方で，導入準備能力評価指標の平均は，0.22 となり，37 項目中 8（<37×0.22=8.14）項目しか「はい」がないことになり，導入準備能力が十分であるとは言えない結果となった．

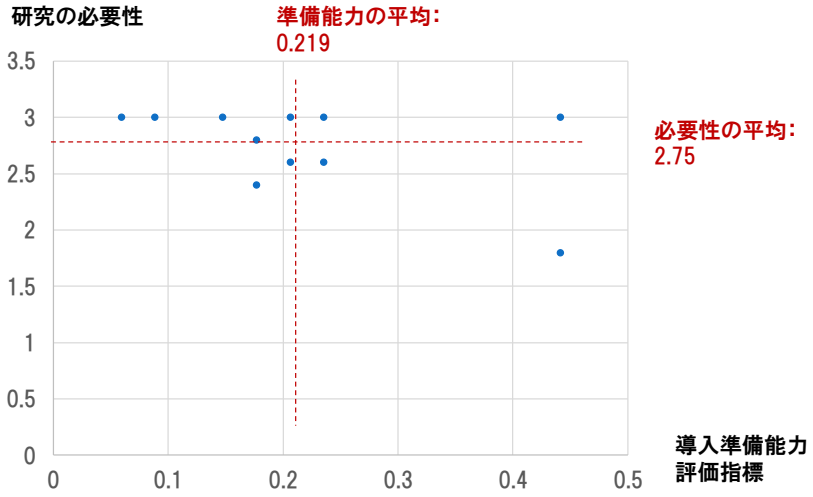


図 3-51　導入準備能力評価指標と研究の必要性の評価例

また，回答者ごとに回答結果に基づいて，ヒヤリング分類ごとに指標の達成度を比較すると，表 3-16 に示すように，各項目の指標値が 3 より小さい未熟型，指標値が 3 となる項目が 1 つある萌芽型，指標値が 4 より大きい項目が 1 つある特化型，2 より大きい指標値の項目が複数ある発展型，複数項目で指標値が 3 より大きい成熟型に分類された．

表 3-16　組織準備能力の類型

類型	説明	件数
未熟型	各項目の指標値＜3	10
萌芽型	2＜指標値＜4 の項目が 1 つある	2
特化型	4＜指標値となる項目が 1 つある	3
発展型	2＜指標値の項目が複数ある	2
成熟型	複数項目で指標値＞3	1
合計		18

図 3-52 に，各分類の件数をグラフ化した結果を示した．このように，保証ケースの知識を持つ担当者が所属する組織であっても，半数以上の組織では導入準備能力が未熟であることが分かった．

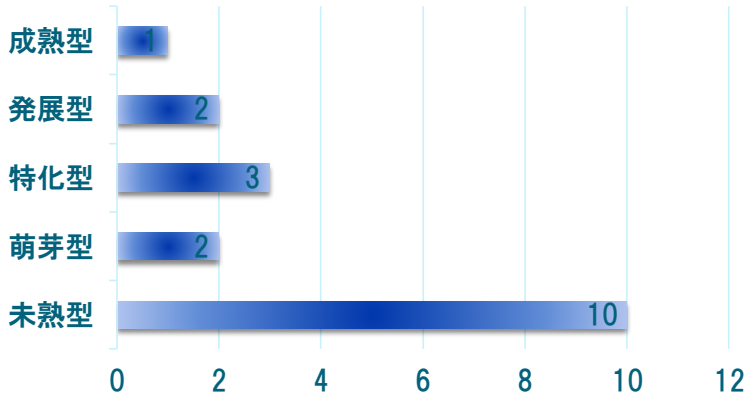


図 3-52　導入準備能力アンケート結果の類型

ただし，このヒヤリングは自己採点で，「はい」と「いいえ」を回答してもらったために，結果が回答者の主観に左右されている可能性がある．

このため，表 3-17 のように，客観的な項目の評価指標を定義した．この表では，証拠となる文書の有無によって客観的に水準が決定できるので，確認結果が主観に左右される可能性を排除できる．

表 3-17　評価指標の水準

段階	確認項目	観点
対象外	対象外	作業範囲外である
0	いいえ	作業として実施する必要があるが，実際には実施していない
1	口頭	指示書はなく，口頭で指示して作業を実施している．
2	メモ	指示を受けて作業を実施している．メモで指示している．
3	部門文書	部門標準の作業マニュアルを整備して，作業を実施している
4	全社文書	全社標準の作業マニュアルを整備して，作業を実施している
5	改善	作業の変化に応じて，マニュアル類を適切に改善している

この評価水準を用いて，保証ケースの導入に積極的な企業 3 社に対して，詳細な対面ヒヤリングを実施した．このヒヤリングでは，保証ケース導入準備能力評価指標 50 を用いた．3 社に対するヒヤリング結果を 8 次元の水準値でグラフ化すると，図 3-53 のようになった．

各社とも，リスク分析能力はあるけれども，プロダクトデザイン能力は高くないことが分かる．これに対して，保証ケース活用ビジョン能力，活用コミュニケーション能力，プロセスデザイン能力，投資的成果能力，保証人材開発能力では，各社間で差があることもわかる．したがって，保証ケースの導入を推進する上で，客観的な指標を用いて導入準備能力を評価することにより，弱点がどこにあるかを明確化できるので，適切な対策を段階的に実施できる可能性があることが分かる．

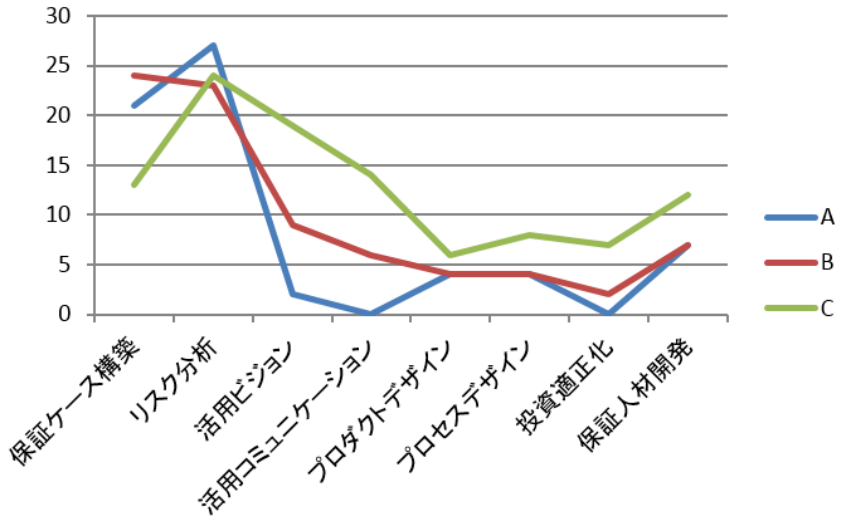


図 3-53　客観的導入準備能力評価例

3.5.3 発生した問題および今後の展望

(1) 発生した問題

項目間の依存関係に顕著な特性がみられなかった．この理由は，すべての研究項目へのニーズがヒヤリング企業でいずれも高かったためである．すべての研究項目のニーズが高いことは肯定的な結果であることから，項目間の依存関係がないことに対する対策は必要がないと判断した．

保証ケース導入準備能力を評価したところ，半数以上の企業で低かった．このため，多くの企業では，導入準備能力評価指標による組織能力の評価が有効に活用できない可能性が判明した．

(2) 今後の展望

上述したように，保証ケース導入準備能力が低い企業にも保証ケースの価値を受容できる仕組みが必要である．このため，導入準備能力評価指標で明確化した活動内容に基づいて，「システム品質保証サービス」を設計することにより，保証ケース導入準備能力が低い企業でも，保証ケースを活用したサービスを利用できる手法について研究する．

4 考察

4.1 研究による効果や問題点等

以下では，設定した研究目標に対する成果について，研究項目ごとに述べる．

4.1.1 研究目標の達成と残された課題

表 4-1 に示すように設定した研究目標をすべて達成した．設定した研究目標について達成していない課題はない．

表 4-1 研究目標の達成状況

	研究成果	設定した研究目標	達成状況
1	モデルに基づく保証ケースの統一的作成法	保証ケース作成手順の定式化 保証ケース作成支援ツールの試作 試作ツールによる保証ケース作成実験	達成
2	コードに基づく保証ケース作成法	コードに対する保証ケースの作成手法を定式化 リポジトリメタモデルの具体化 コードに対する保証ケース作成実験	達成
3	保証ケースレビュ手法	レビュ観点・規則・手順を定式化 保証ケースレビュ指標の定式化 保証ケースレビュ実験	達成
4	開発技術者向け教育研修教材作成	研修教材の設計 研修教材の試作 研修教材の実験評価	達成
5	保証ケース導入準備能力評価指標	導入準備能力指標設計 ヒヤリング項目設計 ヒヤリング評価の実施	達成

4.1.2 新たな研究課題

研究成果に対して，前述した「発生した問題および今後の課題」をまとめると以下のようになる．

1. モデルに基づく保証ケースの統一的作成法の課題
   保証ケースで誤りがないことを確認することと漏れがないことを確認する主張を用意することにより，保証ケースを用いたモデルの欠陥摘出手法を具体化できる．
2. コードに基づく保証ケース作成法の課題
   コード断片の見落としや摘出誤りの発生を防止する方法について，コードの静的解析を用いた研究に，保証ケースを適用できる．
3. 保証ケースレビュ手法
   保証ケースのゴール構文の十分性について評価することにより，もし不十分であれば対応するシステミグラムへの変換規則を追加することができる．
4. 開発技術者向け教育研修教材作成

多くの研修参加者を獲得するためには，募集期間を延伸することや教材の公開が必要になる．

5. 保証ケース導入準備能力評価指標

「システム品質保証サービス」を設計することにより，保証ケース導入準備能力が低い企業でも，保証ケースを活用したサービスを利用できる手法について研究する．

後述する有識者からのアドバイス（4.1.4 外部の客観的評価）に基づいて，顕在化した新たな研究課題を表 4-2 に示す．

表 4-2 新たな研究課題

	研究成果	新たな研究課題
1	モデルに基づく保証ケースの統一的作成法	アーキテクチャ品質評価サービスの研究・標準化 PMO，STAMP への適用，ビジネス IT 整合性保証サービス 表形式によるモデル入力，既存ツール連携（ArchiMate） 支援ツールを用いた品質特性・リスク対策知識の標準化
2	コードに基づく保証ケース作成法	設計レビュ手法，コードレビュ手法，形式手法との統合， サービス保証手法
3	保証ケースレビュ手法	SPREM に基づく保証ケース作成法，保証ケースの全体理解手法
4	開発技術者向け教育研修教材作成	保証ケースの応用教材として認証取得 研修教材に基づくガイドラインの開発
5	保証ケース導入準備能力評価指標	新技術の導入準備能力評価指標への拡張と適用評価 指標に基づく導入準備能力の開発法

以降に新たな研究課題に対する研究成果の適用イメージを記す．

STAMP への「モデルに基づく保証ケースの統一的作成法」の適用イメージを図 4-1 に示す．また，表形式によるモデル入力と既存ツール連携（ArchiMate）によって，保証ケース作成支援ツールを拡張した利用イメージを図 4-2 に示す．なお，紙幅の都合から，PMO，ビジネス IT 整合性保証サービスへの「モデルに基づく保証ケースの統一的作成法」については割愛した．

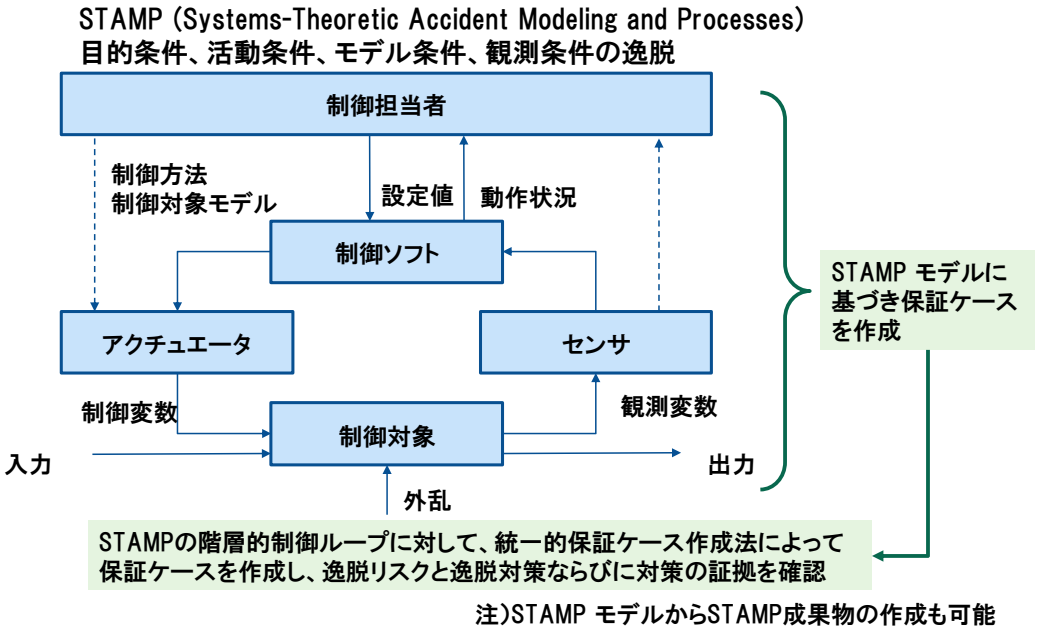


図 4-1　階層的制御ループの逸脱対策に基づく保証対象の例

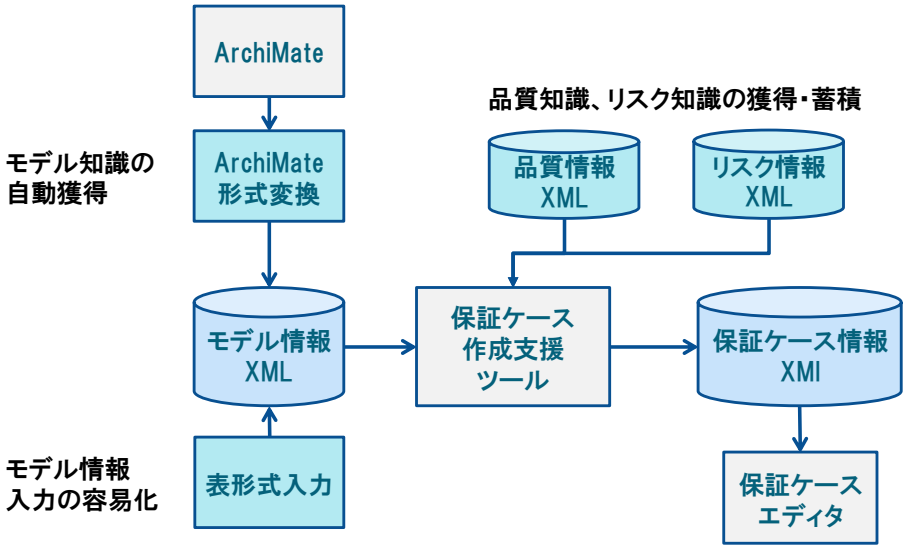
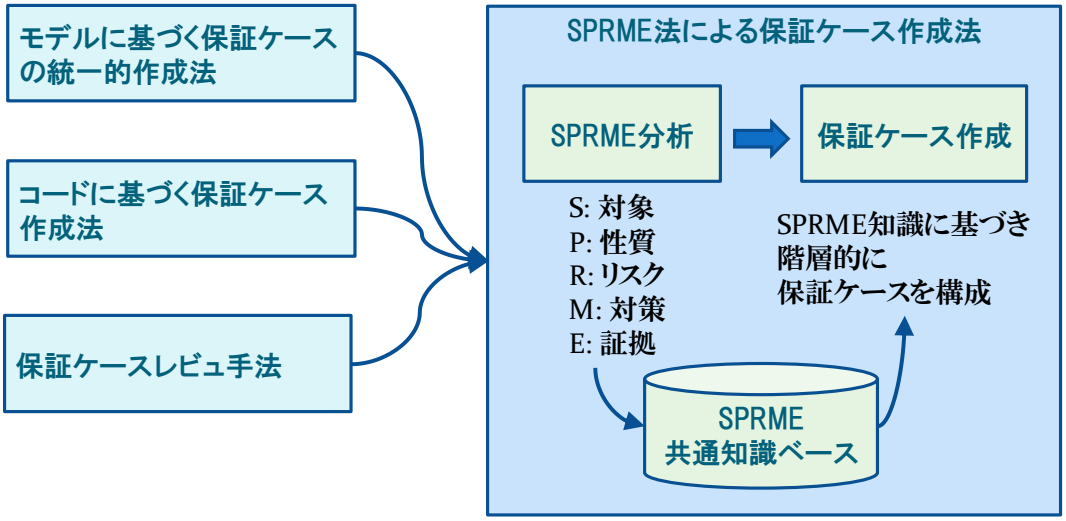


図 4-2　保証ケース作成支援システムの拡張例



注1:SPRME法に基づき、GSNとSTAMPなど関連手法を統合できる可能性がある
注2:SPRME共通知識ベースにより、断片的な知識を獲得・統合・再利用できる可能性がある

図 4-3　SPRME 法による保証ケース作成法の統合

保証ケースレビュ手法の研究で明らかになった SPREM に基づく保証ケース作成法の統合例を図 4−3 に示す．このよう図に示したように，SPRME 法に基づき，保証ケースと STAMP など関連手法を統合できる可能性がある．また，SPRME 共通知識ベースにより，断片的な知識を獲得・統合・再利用できる可能性がある．

また，保証ケース作成知識を導入準備能力評価指標に基づいて参照パッケージ化しておくことで，適用分野ごとに保証ケースの活用を容易化できる．たとえば，図 4-4 では，保証ケースによる品質保証サービス工学の考え方を示している．

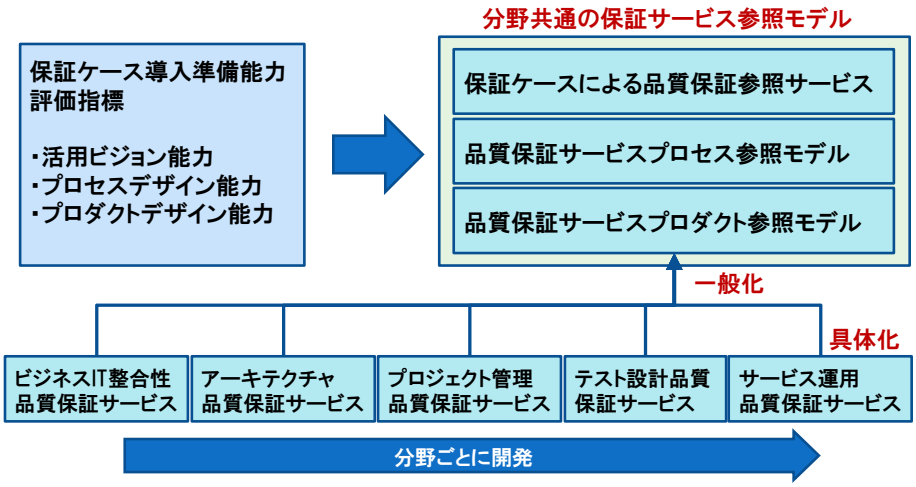


図 4-4　保証ケースによる品質保証サービス工学

保証ケース導入準備能力評価指標で必要とされる能力に対して，それを満たす典型的な例を保証ケースによる品質保証参照サービスとして定義するわけである．同様にして，プロ

セスデザイン能力とプロセスデザイン能力で求められる能力に対する参照サービスプロダクトと参照プロセスを定義できる．このような分野共通の品質保証サービス参照モデルに基づいて，ビジネス IT 整合性分野，アーキテクチャ品質保証分野，プロジェクト管理品質保証分野，テスト設計品質保証分野，サービス運用品質保証分野などの応用分野ごとに，品質保証サービスを具体化するのである．

典型的な品質保証サービスの例を図 4-5 に示す．この例ではアーキテクチャ品質保証サービスを示している．このように，参照サービスを具体化することで，適切な保証ケースの活用法を効率的に実現できる．

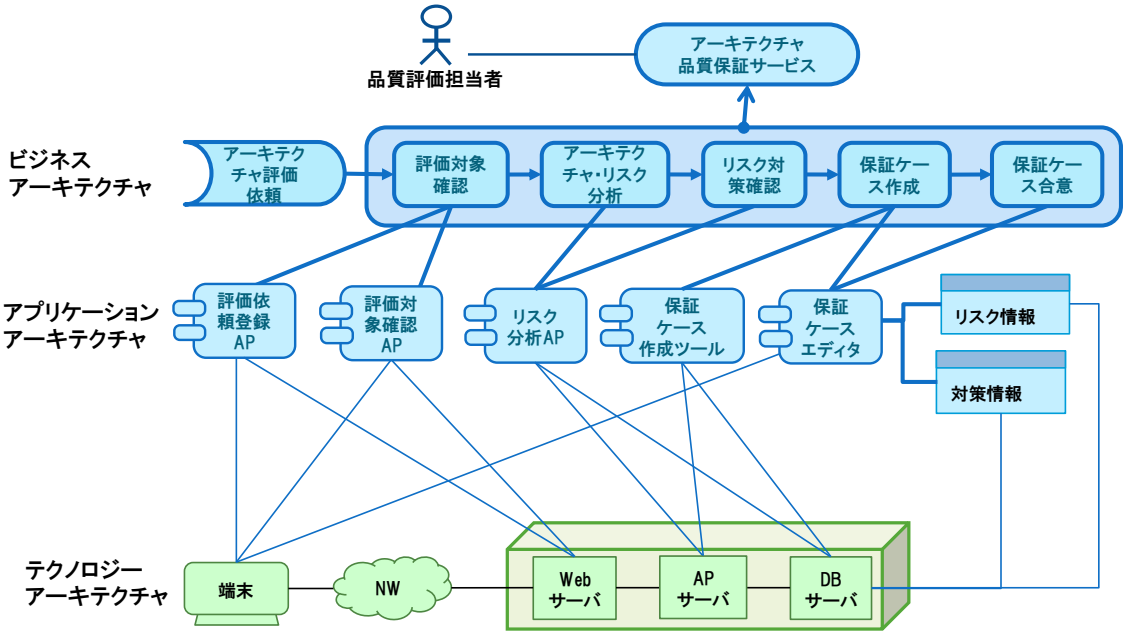


図 4-5　アーキテクチャ品質保証サービスの例

4.1.3 類似研究に対する優位性

本研究成果に対する類似研究の有無と，本研究成果の優位性をまとめると表 4-3 に示すようになる．

表 4-3 類似研究に対する本研究成果の優位性

	研究成果	類似研究	優位性
1	モデルに基づく保証ケースの統一的作成法	分解パターンに基づく保証ケース作成手法 任意のモデルに適用可能な手法はない	任意のモデルに適用できる点 品質特性・リスク対策を XML で定式化している点 ツール支援
2	コードに基づく保証ケース作成法	なし	証拠に基づく欠陥摘出法
3	保証ケースレビュ手法	定性的な保証ケースレビュプロセス	システミグラムによる客観的評価
4	開発技術者向け教育研修教材作成	保証ケースの基礎的な入門教材	統一的保証ケース作成法・システミグラムによる保証ケースレビュ手法の実践的な教材
5	保証ケース導入準備能力評価指標	保証ケース導入に対する定性的・定量的な評価指標はない	8 次元 50 指標を具体化 適用評価を実施

4.1.4 外部の客観的評価

客観的評価のため，産学の外部有識者に受託研究成果を説明することにより，有益なアドバイスを入手した．以下では，これらのアドバイスを，統一的保証ケース作成法，コードに対する保証ケース作成法，保証ケースレビュ手法，保証ケース研修教材，保証ケース導入準備能力評価指標，成果の統合化ごとにまとめて列挙する．

なお，アドバイス提供者は，大学関係者４名，企業関係者７名である．

【統一的保証ケース作成法】

1)統一的保証ケースの評価で，保証ケース作成支援ツールのシステム構成図に対して自己適用した点が評価できる．

2)有識者のテスト知識を獲得する上で，テスト対象，品質リスクを明確に記述できていないという問題があった．不具合を発見するテスト有識者の経験を展開していく場合，テスト対象の構成と品質リスクを定義してデータベース化することが重要になるので，統一的保証ケース作成方式で考案された保証構造図，品質特性定義，そのリスク定義を活用できる．

3)対象物の見方を整理する方法が客観的ではないだけでなく，有識者ごとに個別的だった．統一的保証ケースを用いて，論理的に説明したい．

4)テストサービスを提供しているが，これまでテストの統一的基準がないため，客観的な評価ができないという問題があった．保証ケースレビュ方式で定式化している内容である

①対象物，②品質特性，③リスク，④対策ができていることの確認テストテストという関係を考慮すると，テストの観点を統一的に分類する仕組みを作ることができそうだ．

5)あらかじめ特性分解パターンを用意しておき，分析者が適切な品質特性を選択して分解することができるので，現在実施している「アーキテクチャチェックサービス」の中で，受託研究で開発されたたツールを試行適用できそうだ．

【コードに対する保証ケース作成法】

6)これまでのコードレビュの根拠は有識者の経験か論理しかなかった．しかし有識者の経験の観点やその活用は個別的だ．設計書のレビュでは，「てにをは」レベルの指摘が多いと開発者の士気が低下する．提案手法では，本質的な機能の存在を問うレビュができる点がよい．

7)STAMP では個別的な観点から詳細な指摘が多発することがある．これに対してリスク対策をできるだけまとめるようにしていた場合，全体的には対応できることも対応できていないとして指摘されることがある．SPRME ではシステム全体のリスクと部分要素のリスクを紐づけることができるので，逸脱の粒度を制御できる可能性がある点がよい．

8)コード保証の例は興味深い．コード保証ケースの証拠作成はテストでやることを明示化していると考えられる．現状はコードの断片を証拠としているようだが，テスト結果を考慮するように，拡張できるだろう．引数条件をテストした結果を証拠にしてはどうか．

9)オープンソースの評価にも適用できそうだ．企業が OSS を使う場合，目的があり，それに適合する OSS 製品が複数あることが多い．このとき，OSS 製品には個人が作成したものや企業が整備したものもある．本手法を応用して，ライセンスの有無やサポート体制を条件として複数の OSS 製品の目的適合性検査手法を考案できそうだ．

10)クラウドのサービスレベルを保証する方法に応用できそうである．たとえば，自社クラウドと外部クラウドの連携では，サービスレベルの保証方法や，異常時の対応策の十分性などを保証する必要があるので，今回の成果を応用できそうである．

11)今回の研究ではコードの入力に基づいて内容を保証する方法が成果になっている．クラウドサービスの利用では，出力条件が満たされるかどうかが重要になることから，出力条件についてコードを保証する方法に拡張してほしい．異種クラウドサービス連携の保証方法について，今回の研究成果の適用を検討したい．

12)オープンソースコードのセキュリティチェックが重要になっており，今回の成果が適用できると考えている．

13)必要な要素がそろっていることを主張としておき，そうなっているコードの部分を証拠として提示すればミドルウェアの API を利用するコードの適切性を保証する方法として，受託研究成果を活用できるだろう．

14)コードの静的チェックツールでは，あらかじめ定義してある一般的な規則に基づいてチェックする．これに対して，本手法では，コードに対する確認すべき内容を保証ケースで明確にして，対応する証拠としてコードの断片を人手で探索するため，与えられた仕様に対して具体的に探索できる点がよい．

15)コード保証ケースの メタモデルでは SACM よりも単純で，コードもそれに対応するように，式，識別子，ブロックだけに限定した点がよい．

16)コード保証ではどれくらいの規模のコードを対象にするのか/規模は制限していない．大きな規模のコードだと，保証ケースが大きくなる可能性はある．実際には，日々のコーディングには限界がある．IPO（Input Process Output）に対応させた小さなコード部分ごとに，1ページ程度に収まる保証ケースを作成して確認できる点がよい．

【保証ケースレビュ手法】

17)保証ケースの作成では辞書が必要になることは認識していた．しかし，保証ケースを作成する前にオントロジーを作成しようとすると，プロジェクトごとに必要となるオントロジーの作成自体に手間がかかりすぎてしまい，これまでうまくいかなかった．これに対して，本手法では保証ケースからシステミグラムを用いてオントロジーを作成できる点が効率的でよい．

18)保証ケースとシステミグラムを対応付けるためにシステミグラムの書き方をSPRMEに合わせて限定している点がよい．そうしないとシステミグラムの表記法が多様化してしまうという問題がある．

19)システミグラムを用いたレビュでは，保証ケースに対するシステミグラムの作成に属人性が出るので，システミグラムへの変換手順を具体化した点がよい．

20)保証ケースのレビュ自動化に向けて，保証ケースの代数的定式化を進め，システミグラムを保証ケースから自動生成するツールを実現してほしい．

21)保証ケースだけでは意味的内容をレビュするのが難しいのでシステミグラムを活用する点がよい．

【保証ケース研修教材開発】

22)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．

23)研修教材をDEOS協会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．

24)今回開発された発展的な保証ケースの応用教材がたくさん出てくるのはいいことだ．

【保証ケース導入準備能力評価指標】

25)リスク分析能力が保証ケース構築能力に優先するなど，導入準備能力評価指標の次元間に順序があるかについても調査してほしい．

26)保証ケースの導入準備能力指標値を企業横断的に客観評価できるようにした点がよい．

27)開発した導入準備能力を応用して研修効果を測定する能力評価指標もできる可能性がある．

28)保証ケースの導入準備能力を個別に高くするのは限界がある．しかし保証ケースで経験者が設計内容を記述して説明すると分かりやすいと評価されることが多いので，保証ケースをコンサルサービスとして提供できるような仕組みを具体化すべきだ．

29)現在，ソフトウェア開発人材能力育成プログラムを策定しようとしている．保証ケース導入準備能力評価指標を開発人材育成指標に展開できると考えているので，ぜひ参考にしたい．

【成果の統合化】

30)SPRME (Subject, Property, Risk, Measure, Evidence) で保証ケース作成手法を整理・統合する試みは妥当である.

31)SPRME は特別な知識を必要としないのでだれでも分かる. 各項目を聞くだけでよいから, 保証ケースや STAMP のような手法概念を学習する必要がない点がいい. SPRME は知識獲得の仕組みになっている.

32)最近の開発は, クラウドでもサービスでも特別な固有技術を使わないので, SPRME でリスクと対策が整理できればオープンに利用できるようになるだろう.

33)オープンソースをビジネスで使おうとするがリスクが怖い. そこで, 何を確認すべきかが分かれば, 提案手法では, それに基づいて確実にオープンソースのコードを保証できる点がよい.

34)一連の受託研究成果は保証ケースが普及する土台を構築した点で評価できる. とくに, SPRME として保証ケースの研究を統合する考え方に賛成だ.

35)保証ケースを前提にすることなく, 保証ケースの内容を獲得できる点が興味深い. 保証ケースでは, コンテクストと無関係に分解できるので, なぜそうなったかが明示されないという問題がある. しかし, SPRME ではコンテクスト情報を獲得して保証ケースを作成できるから, 保証ケースの限界を解消している.

36)SPRME を用いて, 保証ケースから SPRME 情報を獲得しておき, 必要な要素だけ SPRME 情報を検索して提示する保証ケースの理解支援に向けた新たな研究を立ち上げられると思われる.

37)保証ケースの統一的作成法, コード保証方法, 保証ケースのレビュ方法には何かしらの関係があると思われる. 今後の課題として, 今回の研究成果を用いて, これらの関係が整理できることを期待している.

38)統一的保証ケース作成法と保証ケースレビュ方法を組み合わせることによりテスト設計の妥当性を客観的に評価する仕組みを考案できそうだ. 今後, テスト設計の妥当性を客観的に評価する仕組みについて議論したい.

39)SPRME は安全分野に特化した方法で興味深い. ISO26262 でも, 安全性ケースを安全性ゴール, ハザード, 対策に限定している. SPRME でもシステミグラムを限定している点がよい.

40)SPRME は書き方を決めているので, 保証ケースの記法についても整理すべきだろう. 制限したシステミグラムで書くと, 保証ケースの問題が明確になる.

上述した 40 件のアドバイスを分類すると, 以下のようになる.

好意的な評価(19 件)

1)6)7)14)15)16)17)18)19)21)24)26)30)31)33)34)35)39)40)

活用法の提案・期待 (14 件)

2)3)4)5)9)10)12)13)27)28)29)32)36)37)

要望(7 件)

8)11)20)22)23)25)38)

好意的な評価については，本成果の利点としてまとめて公開していく予定である．活用法の提案・期待については，本成果の適用事例の中で具体化していく予定である．要望については，発展的な内容を含むことから，本受託研究とは別に，新たな研究計画を策定して対応していく予定である．

4.2 産業界への展開と今後の研究の進め方

研究成果を産業界に展開するための取組みについて説明する．本研究では，予め産業界に研究成果を展開するため，次の項目についても，研究した．

(1) 保証ケース作成支援手法を導入しようとする組織の技術能力を評価する導入準備能力指標
(2) 保証ケース作成支援手法を教育するための研修教材
(3) 保証ケース作成支援手法の導入を自動化するためのツール開発

これらの成果によって，保証ケース作成支援手法を産業界に展開していくことができる．以下では，主な展開シナリオについて説明する．

4.2.1 研究成果の産業界への展開

保証ケース導入準備能力評価指標を用いて，試行的に産業界の準備能力を評価した結果から，現在の日本の産業界には，保証ケースの導入準備能力が不足していることが明らかになった．このことは，保証ケース手法を単独で日本の産業界に展開するのは容易ではないことを示している．

したがって，研究成果を産業界に展開するために，保証ケースを用いた品質保証サービスを具体化することにより，保証ケースの現場展開を容易化する必要があると考える．

以下では，研究成果が誰に対してどのような場面で役立つかについて詳しく記述する．

(1) モデルに基づく保証ケースの統一的作成法

保証ケース作成支援ツールを用いた統一的作成法は，①アーキテクチャ品質評価サービス，②プロジェクト品質評価サービス，③STAMP の品質評価サービス，④ビジネス IT 整合性保証サービスに展開できる．また，表形式ならびに，ArchiMate などのモデル編集ツールからのモデル入力機能を保証ケース作成支援ツールに追加できる．さらに，保証ケース作成支援ツールを用いた統一的作成法は，TOG(The Open Group，オープングループ)の O-DA(Open Dependability Through Assuredness)標準に展開できる．

以下では，それぞれについて，説明する．

保証ケース作成支援ツールを用いた統一的作成法に基づくアーキテクチャ品質評価サービスは，システム開発者に対して，開発対象システムのアーキテクチャ品質を評価しようとする場面で，保証ケースを開発対象システムのモデルから作成することにより，システムが所望の品質を満たすことを保証する作業に役立つ．

保証ケース作成支援ツールを用いた統一的作成法に基づくプロジェクト品質評価サービスは，プロジェクト管理者に対して，開発プロジェクトのプロセスおよびプロダクトの品質を PMO などで評価しようとする場面で，保証ケースを開発プロジェクトのプロセスモデル

ならびにプロダクトモデルから作成することにより，プロジェクトが所望の QCD 特性を満たすことを保証する作業に役立つ.

保証ケース作成支援ツールを用いた統一的作成法に基づく STAMP (Systems-Theoretic Accident Modeling and Processes)品質評価サービスは，システムの故障分析者に対して，分析対象システムの故障モデルと分析プロセスの品質を評価しようとする場面で，保証ケースを対象システムの故障モデルとプロセスから作成することにより，故障モデルとプロセスが所望の品質を満たすことを保証する作業に役立つ.

保証ケース作成支援ツールを用いた統一的作成法に基づくビジネス IT 整合性保証サービスは，IT を用いたビジネス企画・開発・運用者に対して，IT システムのビジネス整合性を評価しようとする場面で，保証ケースをビジネスプロセスモデルならびに IT システムモデル，ビジネスと IT の相互関係から作成することにより，ビジネスプロセスと IT システムが所望の整合性を満たすことを保証する作業に役立つ.

表形式によるモデル入力は，保証ケースで保証しようとする対象モデルを定義する作業の担当者に対して，保証ケースを作成しようとする場面で，対象モデルの構成要素の一覧表と，構成要素関係の表から，XML 定義情報を自動作成することにより，保証ケース作成支援ツールの入力情報定義作業の効率化に役立つ.

ArchiMate などのモデル編集ツールが生成したモデル定義情報を格納した外部ファイルに基づいて，保証ケース作成支援ツールのための XML 定義情報ファイルを作成する既存ツール連携機能は，保証ケースで保証しようとする対象モデルを定義する作業の担当者に対して，保証ケースを作成しようとする場面で，対象モデルの編集ツールの定義ファイルから，XML 定義情報を自動作成することにより，保証ケース作成支援ツールの入力情報定義作業の効率化に役立つ.

保証ケース作成支援ツールでは，品質特性ならびにリスク対策を XML で定義できる．したがって，対象分野の品質特性ならびにリスク対策知識の獲得・標準化をしようとする担当者に対して，品質特性ならびにリスク対策知識を定義する場面で，上述した XML 定義手法を用いることにより，これらの知識の獲得・標準化に役立つ.

保証ケース作成支援ツールを用いた保証ケース作成手法は，保証ケースを前提とする O-DA 標準化担当者に対して，O-DA の活用シナリオを作成する場面で，保証ケースの組織的な導入法を具体化することにより，標準化作業の効率化に役立つ.

(2) コードに基づく保証ケース作成法

コードに基づく保証ケース作成法は，コードレビュ手法，設計レビュ手法，形式手法（event-B）との統合化，クラウド連携サービスなどの連携サービス品質保証方法，オープンソースソフトウェアの品質保証方法に展開できる.

以下では，それぞれについて，説明する.

コードに基づく保証ケース作成法を活用したコードレビュ手法は，システム開発者に対して，開発対象システムのコードの品質を評価しようとする場面で，コードが実現すべき仕様から保証ケースを作成することにより，コードが所望の機能目標を満たすことを確認するレビュ作業の効率化に役立つ.

設計情報に基づく保証ケース作成法を活用したレビュ手法は，システム開発者に対して，開発対象システムの設計書の品質を評価しようとする場面で，設計書が実現すべき仕様から保証ケースを作成することにより，設計書が所望の目標を満たすことを確認するレビュ作業の効率化に役立つ.

コードに基づく保証ケース作成法を活用した形式手法と保証ケースの統合化手法は，システム開発者に対して，開発対象システムの仕様書を検証しようとする場面で，仕様書が実現すべき仕様から作成した保証ケースの最下位の主張についての入出力引数の関係を形式仕様記述しておき，対応するコード断片がこの形式仕様記述を満たすことを形式手法で検証する作業に役立つ.

コードに基づく保証ケース作成法を活用したクラウド連携サービス品質保証方法は，システム開発者に対して，クラウドサービスを活用して開発対象システムの品質を評価しようとする場面で，活用すべきクラウドサービスの入出力仕様から保証ケースを作成することにより，クラウドサービスが所望の目標品質を満たすことを保証する作業の効率化に役立つ.

コードに基づく保証ケース作成法を活用したオープンソースソフトウェア品質保証方法は，システム開発者に対して，オープンソースを活用した開発対象システムの品質を評価しようとする場面で，活用すべきオープンソースの入出力仕様から保証ケースを作成することにより，オープンソースソフトウェアが所望の目標品質を満たすことを保証する作業の効率化に役立つ.

(3) 保証ケースレビュ手法

保証ケースレビュ手法はSPRME（対象，特性，リスク，対策，証拠）分析に基づく保証ケース作成法（SPRME法），統一的作成法との統合化手法，保証ケースの全体理解法に展開できる.

SPRME（対象Subject，特性Property，リスクRisk，対策Measure，証拠Evidence）分析に基づく保証ケース作成法（SPRME法）は，システム分析評価者に対して，開発対象システムの品質を評価しようとする場面で，対象，特性，リスク，対策，証拠を対応付けて明確化することにより，評価すべきシステムに対する保証ケースを系統的に作成することができるので，対象システムが所望の特性を満たすことを保証する作業の効率化に役立つ.

SPRME 法と統一的作成法との統合化手法では，図 4-3 で示したように，まず SPRME 分析を実施した結果としての情報を XML 形式で表現することで，保証ケース作成支援ツールを用いて階層的保証ケースを効率的に作成することができる．

保証ケースの全体理解法では，作成された保証ケースを用いて合意形成しようとする担当者に対して，保証ケースの内容を理解しようとする場面で，対象，特性，リスク，対策，証拠を対応付けて明確化することにより，合意すべき保証ケースの内容を系統的に理解することができるので，対象とする保証ケースの意味を SPRME 項目とその関係で理解し合意形成する作業の効率化に役立つ．

(4) 開発技術者向け教育研修教材を作成

開発技術者向け保証ケースの教育研修教材は，第三者機関（DEOS 協会）で認証された教材として展開できる．以下では，これについて，説明する．

第三者機関で認証された保証ケースの発展教材を求めている担当者に対して，保証ケースの基礎知識を持つ学習者により高度な保証ケースの知識を提供しようとする場面で，統一的保証ケース作成法ならびに保証ケースレビュ手法の教材を用いて，保証ケースの発展知識についての研修教材開発の効率化に役立つ．

(5) 保証ケース導入準備能力評価指標

保証ケース導入準備能力評価指標は，指標を用いた保証ケース導入法，形式手法などの新技術の組織への導入能力評価手法，アーキテクチャ品質評価サービスの設計法として展開できる．以下では，これらについて，説明する．

指標を用いた保証ケース導入法は，図 3-48　客観的導入準備能力評価例で示したように，保証ケースを導入しようとしている場面で，その組織の保証ケース導入担当者が，保証ケースの組織への導入を，必要な能力には何があり，どの能力を向上させることで，導入を成功させることができるかを知る上で役立つ．

保証ケース導入準備能力評価指標を一般化して定義した新技術の組織への導入能力評価手法の例を表 4-4 に示す．この新技術導入能力評価指標は，組織に新技術を導入しようとしている担当者に対して，新技術の組織への導入を推進しようとしている場面で，組織の新技術導入準備能力を客観的に測定して，新技術の円滑な導入を促進する上で，具体的な改善すべき能力を明らかにできる点で役立つ．たとえば，形式手法などについて，企業ヒヤリングを実施することで国内企業の形式手法導入準備能力を横断的に評価することができるだろう．

アーキテクチャ品質評価サービスの設計への保証ケース導入準備能力評価指標の展開では，図 4-4 と図 4-5 で示したように，アーキテクチャ品質保証サービスの参照モデルを用いて，組織内で実践されているアーキテクチャ品質評価を効率化しようとする場面で，有識者の経験に依存している評価知識を見える化して再利用できるようにすることによって，アーキテクチャ品質評価作業の効率化に役立つ．

表 4-4　新技術導入能力評価指標

能力	評価指標
技術知識(5)	①適用対象の定義 ②技術の適用根拠の管理 ③技術適用限界の認識 ④適用対象間の優先順位が明確⑤ 適用部門が明確
課題分析 (8)	①新技術の不適用がもたらす業務への影響を識別 ②課題管理原則を定義 ③課題管理計画を定義 ④課題管理手順を定義 ⑤課題管理情報を共有 ⑥課題の影響度を評価 ⑦課題情報を共有 ⑧課題対応手段を定義
技術活用 ビジョン構築 (7)	①自社戦略目標と新技術の役割が明確 ②新技術が役割を果たすための組織を制度化 ③新技術投資を重点化 ④開発での新技術の活用方針を明確化 ⑤新技術提供部門の役割が明確 ⑥新技術提供部門と開発部門の役割が明確 ⑦新技術に基づく開発部門の結果責任が明確
技術活用 コミュニケーション (7)	①新技術の役割を社員が共有 ②新技術の活用方針を社員が共有 ③新技術導入目的を開発部門が理解 ④新技術導入後の業務変化を開発部門が理解 ⑤部門間で新技術による問題解決プロセスが定義 ⑥新技術活用事例を社内で共有する仕組みを定義 ⑦経営層，新技術部門，開発部門の３部門間で，新技術の投資対効果を共有
プロダクト デザイン(5)	①成果物に対する品質を定義 ②成果物に対するあるべき新技術の適用条件を定義 ③成果物に対する新技術の活用方策を標準化 ④社内外の開発業務連携の観点で成果物に対する新技術を標準化 ⑤成果物に対する重複のない新技術の適用を定義
プロセス デザイン (5)	①開発プロセスへの新技術導入計画を定義 ②新技術による開発プロセスを定義 ③開発プロセスの新技術活用方策を標準化 ④社内外の業務連携プロセスを新技術で標準化 ⑤新技術の重複のない開発プロセスを実現
技術投資適正化(6)	①新技術資産の構築経費を配分 ②新技術部門の独立性を考慮 ③新技術導入経費対効果を事前に検証 ④新技術導入時に全社最適への適合性を検討 ⑤新技術導入後に活用状況・効果を測定 ⑥新技術活用問題を新技術導入検討時に解決
技術人材開発 (5)	①新技術を活用した開発プロセス改革の提案人材を育成 ②経営層の身近に開発と新技術の双方に精通した人材を配置 ③新技術人材が経営に関する知識を習得する機会を提供 ④新技術人材が現場の開発プロセスを理解する機会を提供 ⑤開発人材に新技術の活用スキル研修を提供

4.2.2 今後の研究の進め方

今後の研究の進め方としては，①本年度の各研究成果の実証評価，論文化②統一的保証ケース作成法，コード保証手法，レビュ手法の統合化，③品質保証サービス工学などがある（表4-5）．

表 4-5　今後の研究の進め方

	研究成果	研究の進め方
1	モデルに基づく保証ケースの統一的作成法	①支援ツールを用いた，アーキテクチャ品質評価サービス ②PMO，STAMP への適用，ビジネス IT 整合性保証サービス ③表形式によるモデル入力，既存ツール連携（ArchiMate） ④品質特性・リスク対策知識の獲得・標準化 ⑤O-DA 拡張として標準化（TOG） ⑥論文化・ツールの公開 ここで，①～④は表 4－2 新たな研究課題の再掲．⑤は国際標準化に向けた新たな取り組み．⑥は成果の公開の取り組み．
2	コードに基づく保証ケース作成法	①設計・コードレビュ手法，②形式手法（event-B）との統合化，③連携サービス品質保証方法（例：クラウド連携サービス），④論文化 ここで，①～③は表 4－2 新たな研究課題の再掲．④は成果の公開の取り組み．
3	保証ケースレビュ手法	①SPRME（対象，特性，リスク，対策，証拠）に基づく保証ケース作成法（SPRME 法）の一般化，②保証ケースの全体理解，③統一的作成法との統合・ツール化，④論文化 ここで，①②は表 4－2 新たな研究課題の再掲．③は成果の統合に向けた新たな取り組み．④は成果の公開の取り組み．
4	開発技術者向け教育研修教材を作成	①保証ケース活用教材として認証（DEOS 協会），②研修教材に基づくガイドラインの開発，③論文化・教材の公開 ここで，①②は表 4－2 新たな研究課題の再掲．③は成果の公開の取り組み．
5	保証ケース導入準備能力評価指標	①形式手法などの導入能力評価手法への展開 ②指標を用いた保証ケース導入法 ③アーキテクチャ品質評価サービスの設計 ④論文化，指標の公開 ここで，①②③は表 4－2 新たな研究課題の再掲．④は成果の公開の取り組み．

保証ケースが現場に浸透していないことへの対策

我が国の産業界において，保証ケース単独での現場導入は時期尚早であることが，保証ケース導入準備能力評価指標に基づく調査結果から明らかになった．このため，

① 保証ケースの活用ビジョン，活用プロセス，活用プロダクトを考慮して，
② 適切な保証ケースの活用法を品質保証サービスの内部で隠蔽するように，
③「品質保証サービス工学」を具体化することにより，
④ 多様な現場へ，「品質保証サービス」を提供・活用する
必要がある．

「品質保証サービス工学」は，図 4-6 に示すように，分野共通の保証サービス参照モデルとして，一般化された品質保証サービスと品質保証サービスプロセスならびに品質保証サービスプロダクトから構成される．保証サービス参照モデルを，アーキテクチャ品質保証分野，プロジェクト品質保証分野などの現場で必要な個別の品質保証サービスに具体化することができる．

本受託研究では，組織ごとに保証ケース技術を導入して，その中で保証ケースの活用法を具体化することにより，個別的にシステムの品質を保証しようとしてきた．しかし，保証サービス参照モデルを用意しておき，それを組織ごとに具体化する方が効率的であると思われる．保証サービス参照モデルは，保証ケースのパターンではなく，保証ケースの活用法についてのパターンを，保証ケース活用ビジョン，保証ケース活用プロセス，保証ケース活用プロダクトを総合した統合パターンになっている点が重要である．

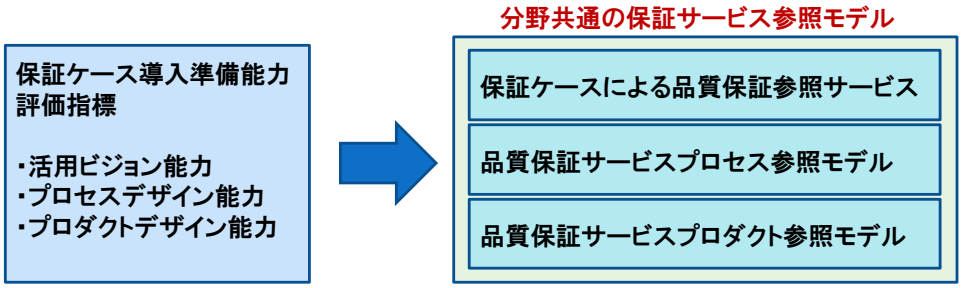


図 4-6　保証サービス参照モデルの研究

本受託研究で当初想定した研究方針と，本受託研究の成果から判明した今後の研究方針を比較して，表 4-6 にまとめる．

表 4-6　研究方針の比較

項目	当初の研究方針	今後の研究方針
活用形態	専門家が保証ケースを組織内で個別に活用	非専門家がオープンな保証サービスを活用
教育	組織ごとに保証ケース知識を担当者に総合的に教育	専門家向けの深い知識の教育と，保証サービスを利用する非専門家向けの基礎知識の教育に層別化
対象知識	成果物としての保証ケース	保証ケースの内容（SPRME）
知識流通	組織内で個別に流通	組織横断的に流通

4.2.3 産業界への要望

リスク分析知識，リスク対策知識については，機密性が高いことから，業界横断的に体系化することは難しい．しかし，コンポーネント再利用や，オープンソースの利用，クラウドサービスの活用が進展している．これらのオープンなコンポーネントやサービスの利用法についてのリスク分析知識については，業界横断的に共通化できる可能性がある．

本研究成果によって，現状では個別化したリスク分析・対策知識を蓄積活用するための標準的な記述法の実現性が明らかになった．この手法を用いて，リスク分析対策知識を産業界で標準化していく取り組みが必要である．たとえば，表 4-7 に示すような SPRME 分析表でこれらの知識を系統的に収集展開できる．SPRME 分析表は，保証ケースのような特別なグラフ構造を知らなくても使えるので，4.1.4 外部の客観的評価の項でも紹介した有識者からの意見にあったように，産業界に展開しやすいと思われる．

表 4-7　SPRME 分析表

S：対象	P：特性	R：リスク	M：対策	E：証拠

たとえば，図 4-7 に示す簡単な Web システムを SPRME 法で分析すると，表 4-8 のようになる．

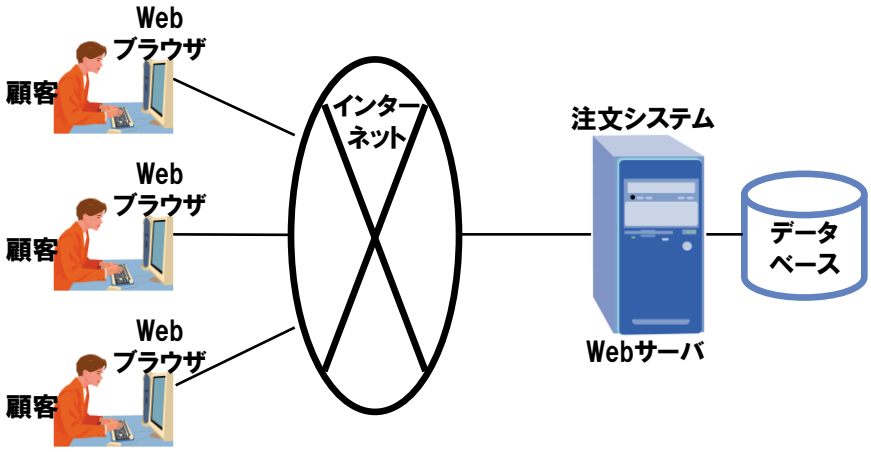


図 4-7　システム構成図の例

表 4-8 では，システムの構成要素ごとに，顧客，Web ブラウザ，インターネット，Web サーバ，データベースがあるので，これらを対象として，抽出する．次に，対象ごとに，特性として，セキュリティ，継続性，性能を識別している．これらの対象と特性の組に対して，リスクを識別する．

表 4-8　SPRME 分析表

S：対象	P：特性	R：リスク	M：対策	E：証拠
顧客	セキュリティ	不正な顧客	ユーザ認証システムの導入	ユーザ認証テスト結果
Web ブラウザ	セキュリティ	ウィルス感染	ウィルス対策ソフトの導入	ウィルス対策テスト結果
インターネット接続	継続性	回線断	回線断時の運用手順の定義	運用手順確認結果
Web サーバ	性能	サーバダウン	サーバ冗長化	システム構成確認結果
		スループット低下	ルータ，ロードバランサの導入	システム構成確認結果
データベース	セキュリティ	DB 情報の持出	DB アクセス認証の導入	DB アクセス認証テスト結果
	性能	アクセス速度の低下	性能チューニング	アクセス速度テスト結果

リスクには，不正顧客，ウィルス感染，回線断，サーバダウン，スループット低下，DB 情報持ち出し，などがある．これらのリスクに対する対策には，ユーザ認証システムの導入，ウィルス対策ソフトの導入，回線断時の運用手順の定義，サーバ冗長化，ルータ，ロードバランサの導入，DB アクセス認証の導入，性能チューニングがある．さらに，これらの対策に対して，ユーザ認証テスト結果，ウィルス対策テスト結果，運用手順確認結果，システム構成確認結果，DB アクセス認証テスト結果，アクセス速度テスト結果が示されている．

この SPRME 分析表で抽出された対策を付加したシステム構成図を図 4-8 に示す．このように，SPRME 分析によって対象システムが持つ特性リスクを解消する構成要素をシステムに追加できる．また，SPRME 分析表では特性，リスク，対策，証拠が明記されているから保証ケースを作成することも容易である．

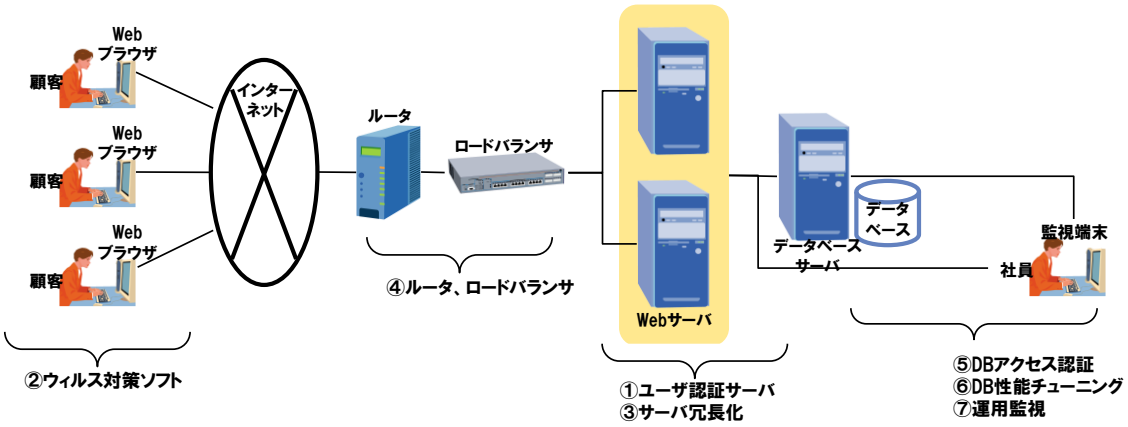


図 4-8　SPRME 分析によって改善されたシステム構成例

また，図 3-53　客観的導入準備能力評価例で示したように，現状では保証ケースの知識はあっても，それを活用するビジョンや，プロダクトならびにプロセスを変革するための能力が十分ではない．このため，上述したように，アーキテクチャ品質保証サービスとして，保証ケースの典型的な活用の仕方を提供することで，産業界に保証ケース作成支援技術ｎ導入を容易化できる．しかし，そのためにはアーキテクチャ品質保証サービスをどのように，企業内に展開していくかについての分かりやすい事例が必要である．そこで，以下に示すような，「O-DA を用いたアーキテクチャ品質保証サービスの構築シナリオ」をまとめている．このシナリオでは，架空の企業 A 社が保証ケースを導入して新たなアーキテクチャ品質評価サービスを構築する手順を具体化した．

実際にある企業では，このシナリオに基づいて，現在実施しているアーキテクチャ品質評価業務を，保証ケースを用いたアーキテクチャ品質保証サービスに向けて高度化するプロジェクトが進んでいる．ぜひ，このシナリオを活用していただきたい．なお，このシナリオは，アーキテクチャ品質保証について，まとめたが，プロジェクト品質保証やテスト設計品質保証についても，同様のシナリオを作成できることを注意しておく．

【O-DA を用いたアーキテクチャ品質保証サービスの構築シナリオ】

概要

A 社では，各担当者がばらばらに行っていた IT アーキテクチャの評価業務を標準化するとともに，TOG(The Open Group)で標準化された O-DA (Open Dependability through Assuredness)を用いた「アーキテクチャ品質保証サービス」を構築することにより，保証ケースとその支援ツールを導入した．従来，品質評価の現場ではリスク評価を担当者ごとに実施していたが，それを保証ケースで客観的に管理して利用できるようになり，大幅な業務の効率化を実現した．リスク分析結果や過去データの閲覧も可能になり，IT アーキテクチャ品質保証業務の品質が向上するとともに，IT アーキテクチャのリスク分析の効率化が可能になった．以下では，O-DA を用いた「アーキテクチャ品質保証サービス」の構築事例について述べる．

問題状況

A 社品質保証部の主な業務は，IT システムのアーキテクチャ品質保証である．同部門が担当する業務は，システムのアーキテクチャ設計に関する品質の点検業務である．IT 業界では，オープン化の流れにより競争にさらされ，コスト面の競争力が求められている．とはいえ，IT は A 社の顧客企業にとって必須の事業基盤であり，高品質の IT システムの提供が最も優先される．そのため，ミドルウェアや既存のアプリケーションをできるだけ再利用するとともに，リスクを確実に把握して対策ができていることを保証できる効率的な品質保証サービスが必要とされていた．

また，ミドルウェアは本社側で用意していたものの，IT アーキテクチャの品質評価業務の手法は担当者に任せており，有識者のリスク分析知識を可視化できておらず，共有できていなかった．これでは全体の効率化は難しいうえ，有識者が人事異動で抜ければ，また最初からリスク分析手順を未経験者に教育する必要がある．しかし，教育するためにはリスク分析知識が可視化できていなくてはならない．

このような問題を解決するため，全社レベルでのリスク分析知識の標準化も課題だった．さらに担当者に情報武装をさせることで，アーキテクチャ品質評価業務の質を向上させる必要もあった．有識者であれば，アーキテクチャを見てある程度状況を把握できるが，非熟練者には，アーキテクチャ上のリスクの発見が難しい．もしアーキテクチャの要素と要素関係について，この場合には危険だといった観点を参照できれば，経験が少なくてもリスクの発見を容易化できる．

そこで，アーキテクチャの品質保証を支援する「アーキテクチャ品質保証サービス」を再構築するプロジェクトが発足した．この課題状況をまとめると，表 4-9 に示すようになる．

表 4-9　課題分析表

関心事	問題状況	原因分析	あるべき姿	解決策
アーキテクチャ評価	システム構成が複雑化している．特に新技術導入が急増している． アーキテクチャの妥当性に不安のある開発が急激に増えている． アーキテクチャ評価技術の差異化が難しい．	必要時に，いつでも，アーキテクチャを適切に評価できない． アーキテクチャ評価の強みが不明確．	アーキテクチャの「高信頼性保証」	保証ケースで培ったノウハウを活用したアーキテクチャ評価と妥当性保証を一体化した，「アーキテクチャ評価サービス」を提供する

アーキテクチャビジョン

保証ケースを利用した「アーキテクチャ品質保証サービス」によって，業務効率と評価品質の向上を達成する．アーキテクチャ品質を客観的に保証できるだけでなく，品質保証結果の再利用が可能になることは大きい．担当者によってリスク分析のスキルが異なるとしても，担当者ごとに大幅な評価作業時間を短縮できる．また，保証ケースによって客観的にリスク対策ができていることを説明できるので，コミュニケーションミスを防ぐこともできる．さらに，IT アーキテクチャリスク分析の観点をアーキテクチャメタモデルと非機能要

求グレードに基づき標準化して，過去の傾向やどこが危険かといったことを登録することにより，経験が少ない担当者でもリスクを適切に検知することが可能になる．

アーキテクチャモデルから保証ケースを作成する新しい支援ツールを利用することで，保証ケース作成を効率化できただけでなく，従来各自が個別作成していた評価報告書類も自動的に作成できるようになる．これにより，アーキテクチャリスク保証の実施可能件数も向上する．

ビジネスシナリオ

アプリケーション開発部門が，アーキテクチャの評価をアーキテクチャ品質評価部門にアーキテクチャ評価を依頼する．

次いでアーキテクチャ評価部門が，以下のようにしてアーキテクチャを評価する．まず「指定された品質特性をアーキテクチャが達成していること」に対するリスクを分析する．次いで，アーキテクチャ評価部門がアーキテクチャ開発部門に，識別したリスクへの対策内容の提示を依頼する．アーキテクチャ開発部門がリスク対策内容をアーキテクチャ評価部門に提示する．アーキテクチャ評価部門がリスク対策によって，品質特性に対するアーキテクチャのリスクが解消できることを確認する．アーキテクチャ評価部門がすべてのアーキテクチャリスクが解消できることを説明する保証ケースを作成する．

アーキテクチャ評価部門が，保証ケースを用いてアーキテクチャが品質特性を達成していることをアーキテクチャ開発部門に説明する．

最後に，アーキテクチャ開発部門がアーキテクチャ評価部門から提示された保証ケースについて合意する．

上述したアーキテクチャ品質保証サービスのビジネスシナリオを図 4-9 のビジネスアーキテクチャで示した．この図ではアーキテクチャ評価依頼を契機として評価対象確認，アーキテクチャリスク分析，リスク対策確認，保証ケース作成，保証ケース合意という活動があることをビジネスアーキテクチャで明示している．このビジネスアーキテクチャで利用されるアプリケーションコンポーネントとテクノロジーコンポーネントが，それぞれ，アプリケーションアーキテクチャと，テクノロジーアーキテクチャで記述されている．

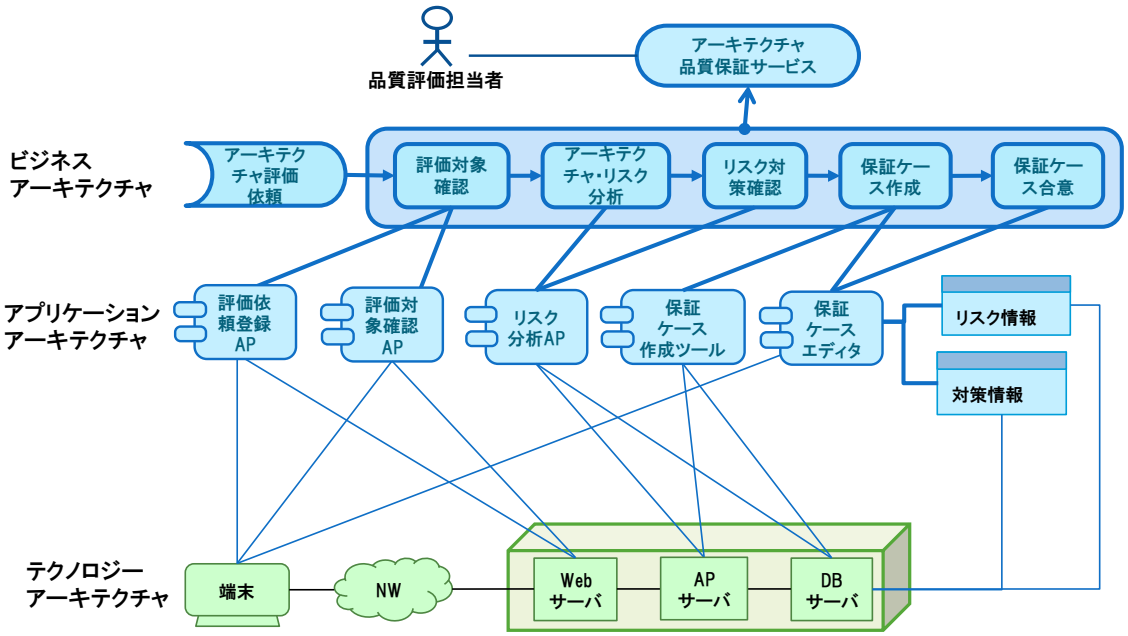


図 4-9　アーキテクチャ品質保証サービスの導入ビュウポイント

ビジネスアーキテクチャ

アーキテクチャ品質評価部門が「アーキテクチャ品質評価サービス」をビジネスサービスとして提供する．このビジネスサービスに対するビジネスアーキテクチャは以下のようになる．（2）から（6）はビジネスプロセスである．

（1）アーキテクチャ評価依頼イベント
（2）アーキテクチャと品質特性の確認
（3）品質特性に対するアーキテクチャリスク分析
（4）アーキテクチャリスクへの対策の確認
（5）保証ケースによるアーキテクチャリスク対策の妥当性の説明
（6）保証ケースによる合意形成

このとき，ビジネスオブジェクトとして，アーキテクチャ，品質特性，リスク，リスク対策，保証ケースを用いる．

O-DA フレームワーク（Open Dependability through Assuredness Framework）には，目的変化対応プロセスと，障害対応プロセスがある．O-DA フレームワークでは，アーキテクチャ開発部門とアーキテクチャ品質評価部門を分けることを考慮していない．このため，アーキテクチャ品質評価部門の役割を以下のようにした．

（1）目的変化対応サイクル（Change Accommodation Cycle）に対して，アーキテクチャの品質要求に対するリスク分析を担当する．
（2）障害対応サイクル（Failure Response Cycle）ではアーキテクチャの問題検知，未然回避，障害への迅速対応が必要となる．このため，アーキテクチャに対する運用上のリスクとして，問題検知リスク，未然回避リスク，障害への迅速対応リスクを明確にするとともに，それらのリスクへの対策の確認を担当する．

すなわち，アーキテクチャ品質評価におけるアーキテクチャリスク分析の内容には，アーキテクチャ自体のリスクだけでなく，アーキテクチャを運用する場合のリスク分析も含まれている．

現行ビジネスアーキテクチャ(Baseline Business Architecture)と目標ビジネスアーキテクチャ(Target Business Architecture)をまとめると表 4-10 のようになる．

表 4-10　現行アーキテクチャと目標アーキテクチャの比較

Baseline Business Architecture	Target Business Architecture
アーキテクチャ開発部門からのアーキテクチャ品質評価依頼・結果を統一的に管理していない 有識者がアーキテクチャ品質を個別に評価 アーキテクチャ評価の観点を整理しているがリスク識別基準は属人的 標準的なアーキテクチャ品質保証基準はない	アーキテクチャ開発部門からのアーキテクチャ品質評価依頼・結果を統一的に管理 アーキテクチャ品質評価プロセスを標準化 アーキテクチャ評価観点に基づくリスク識別基準を標準化 アーキテクチャ品質保証基準を保証ケースで標準化

アプリケーションアーキテクチャ

アーキテクチャ品質評価部門が利用するアプリケーションアーキテクチャでは，以下のようなアプリケーションサービス，アプリケーションコンポーネント，データオブジェクトを利用する．

（1）品質保証アプリケーションサービス

品質保証アプリケーションコンポーネントと品質保証データベースを用いて，品質保証部門によるアーキテクチャ品質評価のためのビジネスプロセスを実現する．

（2）品質保証アプリケーションコンポーネント

品質保証依頼管理アプリケーションを用いて，アーキテクチャ開発部門から受付けた評価依頼を登録して，アーキテクチャ評価を開始する．次に，アーキテクチャ情報と期待される品質特性情報に基づいて，アーキテクチャリスク分析アプリケーションを用いて，アーキテクチャリスクを抽出する．ここで，アーキテクチャリスク分析アプリケーションでは，有識者がアーキテクチャ構成要素に対する品質特性上のリスクを提示したアーキテクチャリスク情報を参照する．識別されたアーキテクチャリスクごとに，アーキテクチャ開発部門からアーキテクチャ対策を入手すると，このリスク対策情報を登録する．

保証ケース生成アプリケーションを用いて，①アーキテクチャ構成要素，②アーキテクチャが満たすべき品質特性，③アーキテクチャ構成要素が品質特性を満たす上でのリスク，④リスクへの対策を入力することにより，保証ケース情報を生成する．生成された保証ケース情報に基づいて，保証ケースエディタを用いて保証ケースを作成する．保証ケースをアーキテクチャ開発部門に提示することにより，アーキテクチャが期待される品質特性を持つことについて合意する．最後に，品質保証依頼管理アプリケーションを用いて，指定されたア

ーキテクチャ品質保証依頼について，品質保証が完了して依頼元から了承されたことを登録する．

（3）品質保証データオブジェクト

品質保証データベースでは，①品質保証依頼，②品質特性情報，③品質保証対象であるアーキテクチャ情報，④アーキテクチャリスク情報，⑤アーキテクチャリスク対策情報，⑥アーキテクチャ品質保証ケース情報を管理する．

現行アプリケーションアーキテクチャ(Baseline Application Architecture)と目標アプリケーションアーキテクチャ(Target Application Architecture)をまとめると表 4-11 のようになる．

表 4-11　現行アーキテクチャと目標アーキテクチャの比較

Baseline Application Architecture	Target Application Architecture
アーキテクチャ開発部門からのアーキテクチャ品質評価依頼・結果の管理が情報化されていない アーキテクチャリスク分析が情報化されていない アーキテクチャリスク対策知識が情報化されていない アーキテクチャ品質保証が情報化されていない	アーキテクチャ開発部門からのアーキテクチャ品質評価依頼・結果の管理を情報化 アーキテクチャ品質評価プロセスを情報化 アーキテクチャ評価観点に基づくリスク識別基準を情報化 アーキテクチャ品質保証基準を保証ケースで情報化

テクノロジーアーキテクチャ

Web クライアントから，社内ネットワークを介してアーキテクチャ品質保証サービスの Web サーバにアーキテクチャ評価担当者がアクセスする．Web サーバでは，アプリケーションサーバ上のアーキテクチャ評価依頼管理機能，アーキテクチャリスク分析機能，アーキテクチャ評価結果登録機能を提供する．

データベースサーバでは，アーキテクチャ評価依頼情報，アーキテクチャ情報，品質特性情報，アーキテクチャリスク情報，リスク対策情報，アーキテクチャ品質保証ケース情報を管理する．

現行テクノロジーアーキテクチャ(Baseline Technology Architecture)と目標テクノロジーアーキテクチャ(Target Technology Architecture)をまとめると，表 4-12 のようになる．

表 4-12　現行アーキテクチャと目標アーキテクチャの比較

Baseline Technology Architecture	Target Technology Architecture
担当者の PC でアーキテクチャ品質評価依頼とアーキテクチャ評価結果を作成して保存 アーキテクチャ品質評価の観点をワープロで文書化	アーキテクチャ開発部門からのアーキテクチャ品質評価依頼から結果登録までを Web サーバで管理 アーキテクチャリスク分析サーバ 保証ケース生成支援ツール 保証ケースエディタ データベースサーバでアーキテクチャ品質保証情報を管理

アクタ

（1）人間アクタ

アーキテクチャ評価依頼者とアーキテクチャ評価担当者が人間アクタである.

（2）計算機アクタ

アーキテクチャ評価依頼管理, アーキテクチャリスク分析, アーキテクチャリスク対策管理, アーキテクチャ品質評価情報管理が計算機アクタである.

移行アーキテクチャ

表 4-13 に示す保証ケース導入期, 品質リスク管理期, 統合的品質保証期からなるアーキテクチャロードマップによって, 現行アーキテクチャから段階的に移行アーキテクチャを構築する.

表 4-13 アーキテクチャロードマップ

段階	保証ケース導入期	品質リスク管理期	統合的品質保証期
BA	アーキテクチャ品質保証プロセス	アーキテクチャのリスク分析プロセス アーキテクチャ品質保証プロセス	統合的アーキテクチャ品質保証プロセス アーキテクチャのリスク分析プロセス アーキテクチャ品質保証プロセス
AA	保証ケースエディタ	リスク分析アプリケーション 保証ケースエディタ	アーキテクチャ品質情報管理アプリケーション アーキテクチャリスク分析アプリケーション 保証ケースエディタ
TA	PC	PC, Web サーバ AP サーバ DB サーバ	PC, Web サーバ AP サーバ DB サーバ

移行計画

移行アーキテクチャに対する投資効果とリスク分析結果を表 4-14 にまとめる.

表 4-14　移行アーキテクチャの投資効果とリスク分析

移行アーキテクチャ	投資効果	リスク分析
保証ケース導入期	アーキテクチャ品質保証文書の標準化効果	保証ケースの教育リスクと活用リスク
品質リスク管理期	アーキテクチャリスク分析知識の標準化効果	アーキテクチャリスク分析知識の獲得リスクと管理リスク
統合的品質保証期	アーキテクチャ品質保証プロセスと知識の標準化効果	情報化されたアーキテクチャ品質保証サービスの構築リスクと運用リスク

本シナリオで紹介した O-DA の適用結果を表 4-15 にまとめる．ただし，G.実装監督については参考のため，追加した.

表 4-15　O-DA の適用結果（まとめ）

記号	工程	実施内容
A	アーキテクチャビジョン	スコープ，制約，期待，ステークホルダを定義．事業環境を確認．保証ケースの位置付けを明確化
B	ビジネスアーキテクチャ	ビジネスの現行と目標アーキテクチャを定義，差異を分析．保証ケースに基づくアーキテクチャ品質保証プロセスを定義
C	情報システムアーキテクチャ	情報システムの現行と目標アーキテクチャを定義，差異を分析．保証ケースに基づくアーキテクチャリスク対策サービスの機能と情報を明確化
D	技術アーキテクチャ	技術の現行と目標アーキテクチャを定義，差異を分析．保証ケースに基づくアーキテクチャリスク対策サービスの情報基盤環境を明確化
E	ソリューション	アーキテクチャロードマップに基づく実施計画を定義し移行アーキテクチャを構築
F	移行計画	費用対効果分析，リスク分析に基づき移行実施計画を詳細化
G	実装監督	アーキテクチャ移行計画を管理．実装結果を確認

参考文献

[1] Kelly, T. P, A Six-Step Method for the Development of Goal Structures, York Software Engineering, 1997

[2] T. Kelly. “Arguing Safety, a Systematic Approach to Managing Safety Cases”. PhD Thesis, Department of Computer Science, University of York, 1998

[3] 山本修一郎, 要求工学第58回アシュアランスケースとGSN, http://bcm.co.jp

[4] Jackson, D. et al, Software for dependable systems- sufficient evidence?, NATIONAL RESEARCH COUNCIL, 2008

[5] European Organisation for the Safety of Air Navigation, Safety Case Development Manual, 2nd ed., EUROCONTROL, Oct. 2006.

[6] G. Despotou, T. Kelly, Design and Development of Dependability Case Architecture during System Development, . In proceedings of the 25th International System Safety Conference (ISSC), Baltimore, MD USA. Proceedings by the System Safety Society, 2007

[7] 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.

[8] DEOSプロジェクト, http://www.crest-os.jst.go.jp

[9] D-Caseエディタ, http://www.dependable-os.net/tech/D-CaseEditor/

[10] Ewen Denney and Ganesh Pai, Ibrahim Habli, Perspectives on Software Safety Case Development for Unmanned Aircraft, DSN2012

[11] Despotou G., Kelly T., Extending the Concept of Safety Cases to Address Dependability. In proceedings of the 22nd International System Safety Conference (ISSC), Providence, RI USA, proceedings by System Safety Society 2004.

[12] G. Despotou, T. Kelly, EXTENDING SAFETY DEVIATION ANALYSIS TECHNIQUES TO ELICIT FLEXIBLE DEPENDABILITY REQUIREMENTS, In proceedings of the 1st IET (Former IEE) International Conference on System Safety Engineering (ICSS), London, UK, June 2006.

[13] Kelly, T.: A Six-Step Method for the Development of Goal Structures, York Software Engineering (1997)

[14] 山本修一郎, 要求工学連載第90回サービス保証ケース手法, http://bcm.co.jp

[15] Kelly, T., Reviewing Assurance Arguments - A Step-By-Step Approach: http://www-users.cs.york.ac.uk/~tpk/dsnworkshop07.pdf, DSN workshop 2007.

[16] Yamamoto, S., and Matsuno, Y.: A review method based on a matrix interpretation of GSN. In Proc. JCKBSE 2012, pages 36-42. IOS Press, 2012.

[17] Matsumura, M., Patu, V., Matsuno, Y., Takama, S., Tokuno, T., Yamamoto, S.: A Method to Share Word Knowledge of Dependability Case. KES 2013: pp.10-19, 2013
[18] 松村昌典, 森崎修司, 渥美紀寿, 山本修一郎, コンテクスト依存表 (CDM) に基づく D-Case 作成法の提案, KSN 研究会, 9.26, 2014.
[19] Clegg. B. and Boardman, J.: A Systems Approach to Process Improvement in Design and Manufacture, Systems Approach to Manufacturing, IEE Colloquium on a (Digest No.: 1996/171), pp. 3/1 - 3/9, 11 Nov 1997
[20] Boardman, J and Sauser, B.: 2008. *Systems Thinking: Coping with 21St Century Problems.* Boca Raton, FL: Taylor & Francis / CRC Press.
[21] World of Systems, http://www.boardmansauser.com/
[22] Systemigrams, http://www.boardmansauser.com/thoughts/systemigrams.html
[23] Checkland, P.: Systems Thinking, Systems Practice, John Wiley & Sons Ltd., 1990.
[24] Martin, J.: The Seven Samurai of Systems Engineering, INCOSE International Conference, 2004
[25] 山本修一郎, 連載アーキテクチャ論　第 41 回　システミグラムと 7 人の侍フレームワーク, Computer report 54(9), 18-25, 2014-9, 日本経営科学研究所
[26] Systemitool, http://www.boardmansauser.com/thoughts/system_itool.html
[27] 山本修一郎, システミグラムと安全分析, 連載要求工学, 第127回, Vol.52, No.5, 2015
[28] 国領二郎監修, NTTデータ著, ITケイパビリティ―今すぐ始めるIT活用力―診断と処方箋, 日経BP, 2004