名古屋大学

D-Case研究会
2016.4.22

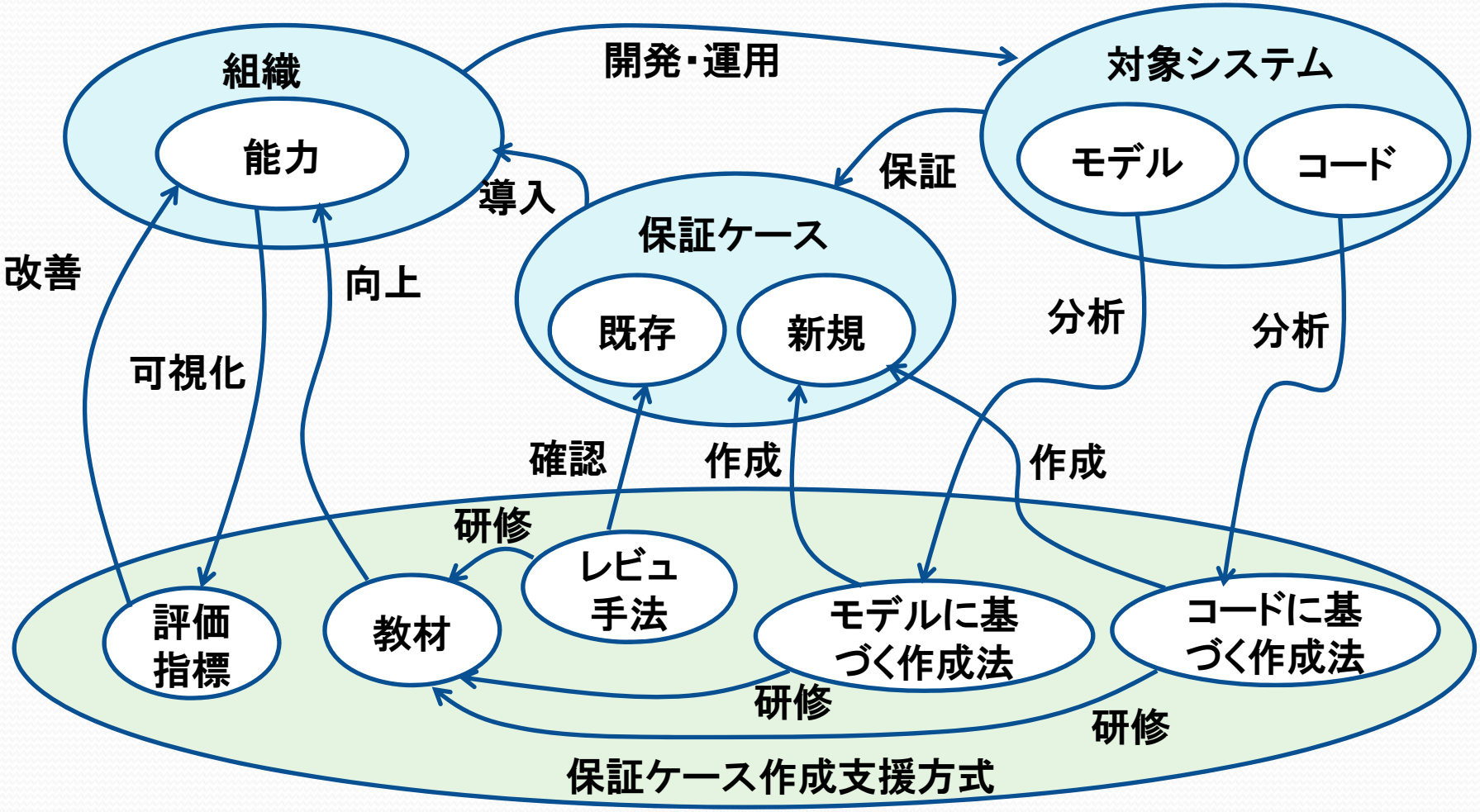
保証ケース作成のフロンティア

- 保証ケース作成支援方式の研究
- 目的
- 研究概要
- 考察
- 今後の課題

名古屋大学　大学院　情報科学研究科　情報システム学専攻
教授　山本修一郎

保証ケース作成支援方式の位置づけ

～システミグラム(*1,2)による説明～



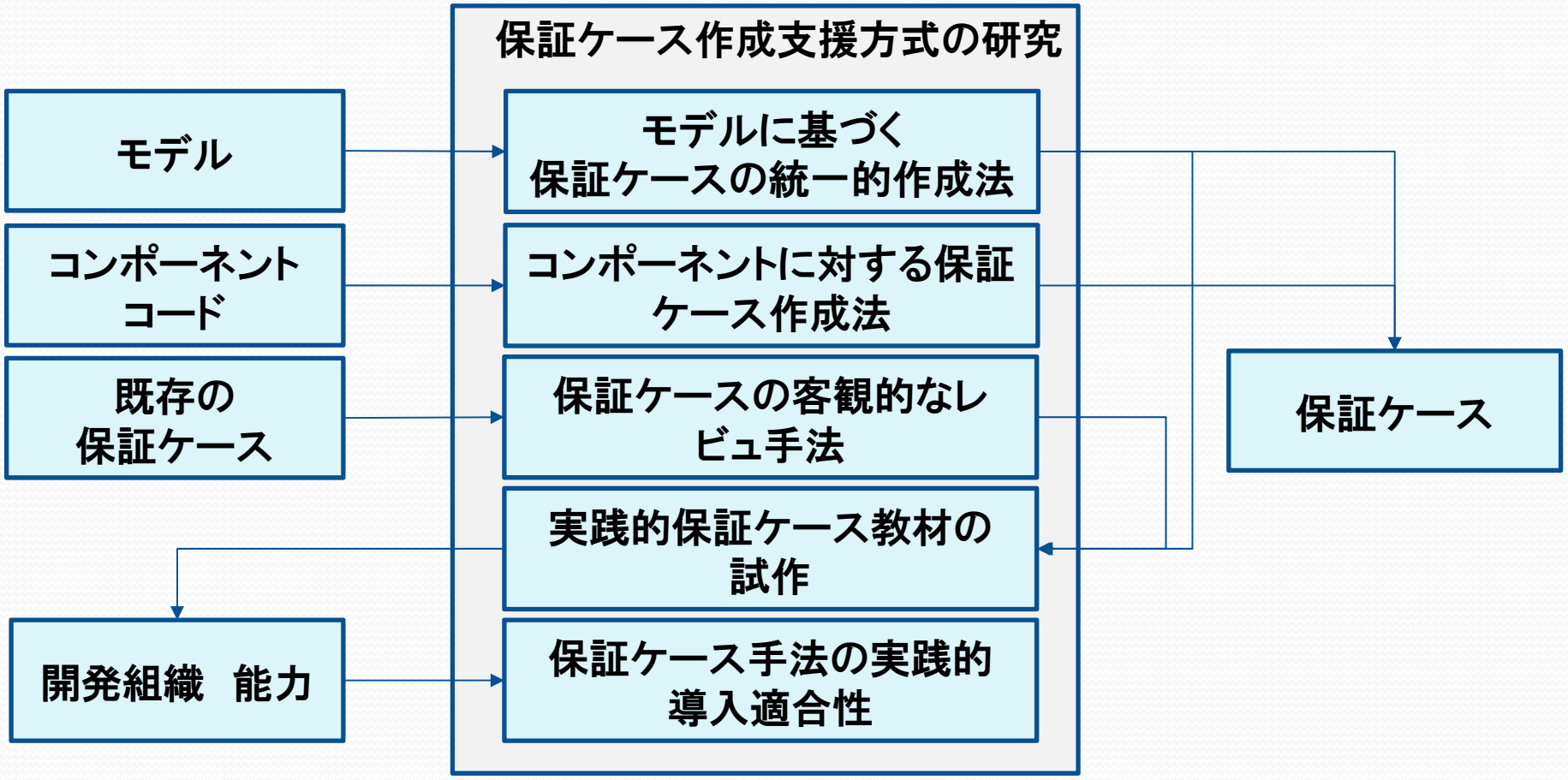
[*1] Boardman, J. and Sauser. B., *Systems Thinking: Coping with 21St Century Problems,* Boca Raton, FL: Taylor & Francis / CRC Press, 2008
[*2] 山本修一郎, アーキテクチャ論 18 システミグラム, 日本経営科学研究所, 2013

「保証ケース作成支援方式の研究」の概要

2015年度RISEの公募テーマ(B)ソフトウェア開発現場への適用を目的としたソフトウェア工学の成果・手法を詳細化・具体化・実用化する研究

	研究課題	内容、目標
1	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
2	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
3	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
4	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
5	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

研究項目の関係



名古屋大学

研究項目と実施期間

作業項目		2015 6月	7月	8月	9月	10月	11月	12月	2016 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						→		→		

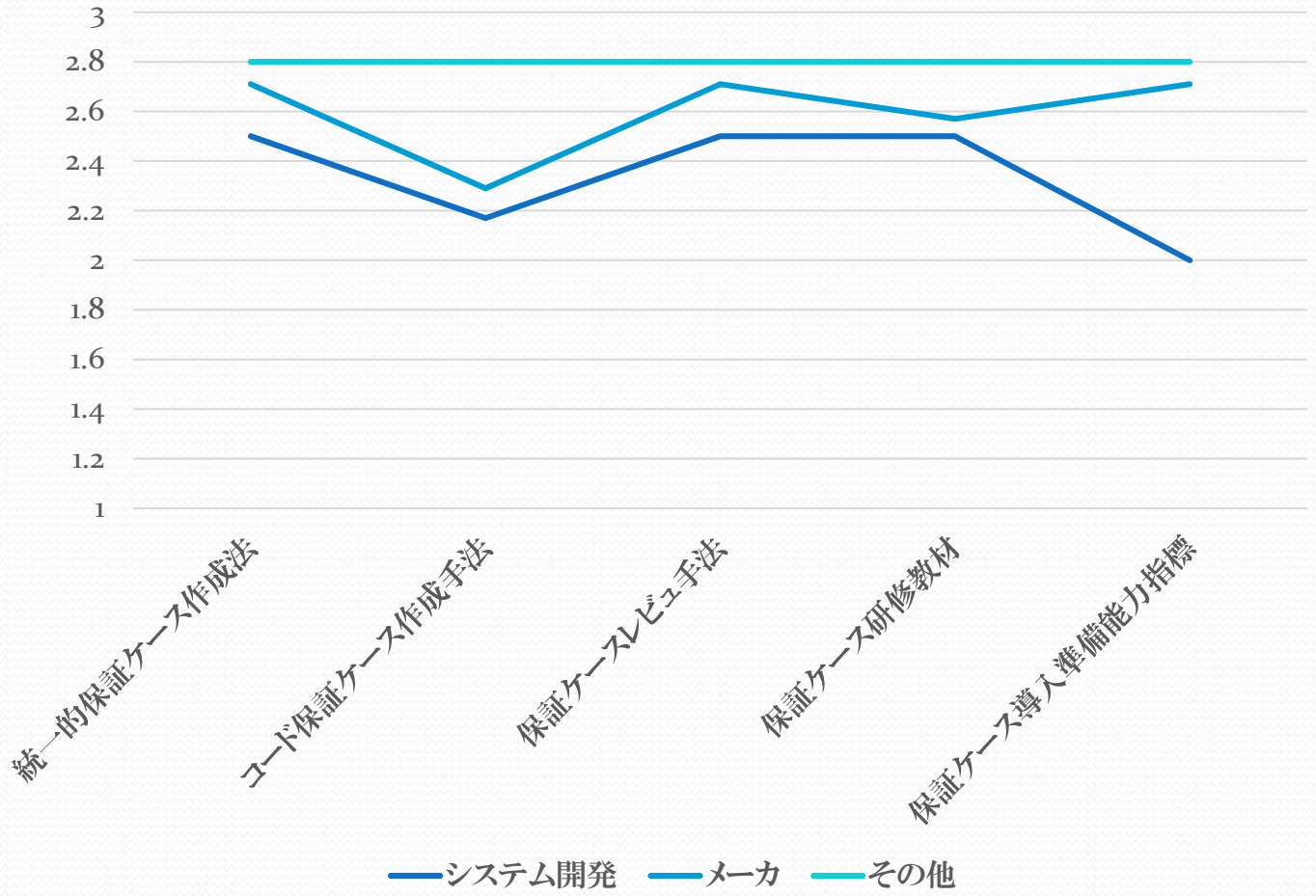
→ 計画
→ 実績

必要性の調査

- 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
  - メール　18組織

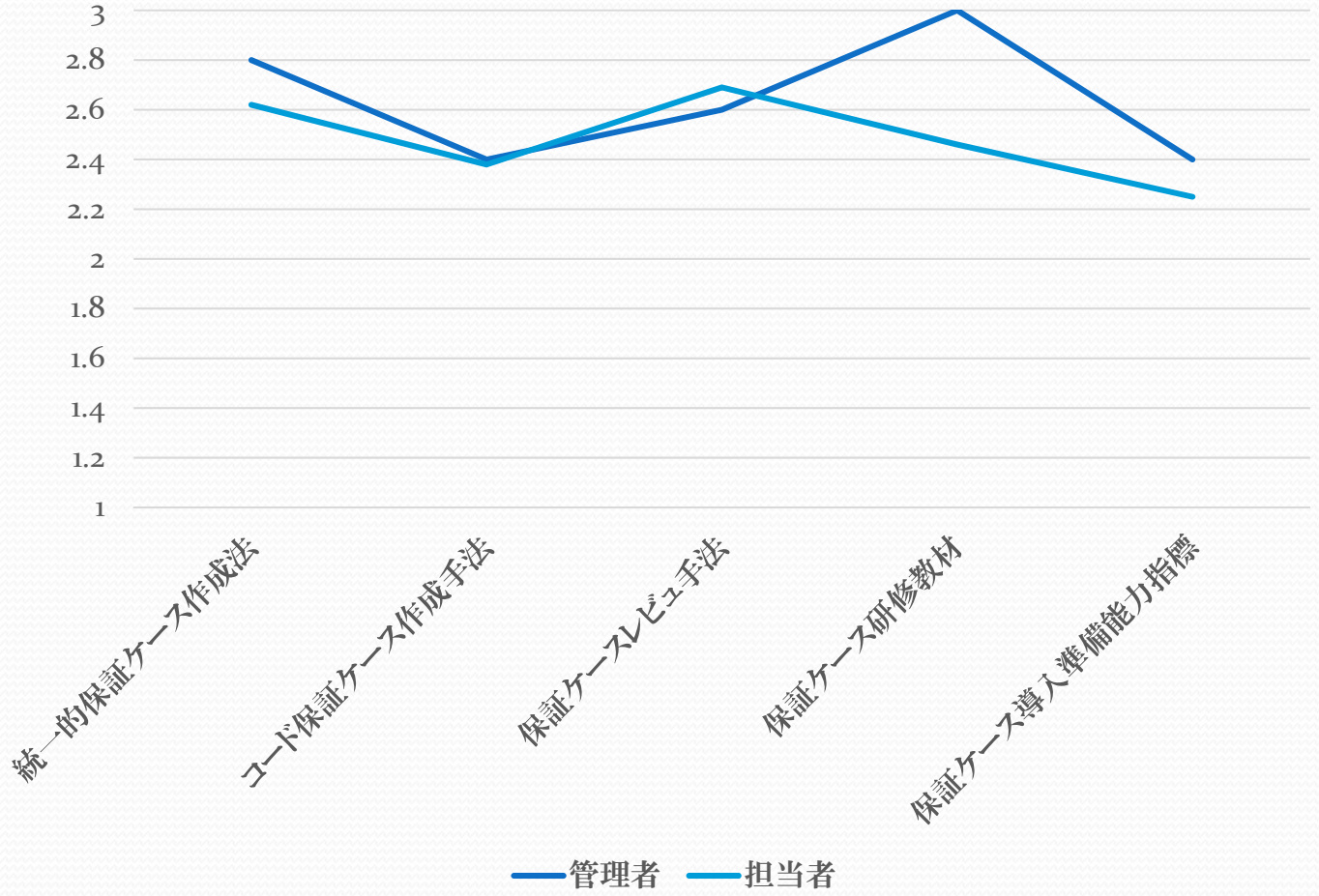
研究の必要性　業種別

回答数：18



研究の必要性　職責別

回答数：18



研究成果の概要

	研究課題	成果
1	モデルに基づく保証ケースの統一的作成法	a)モデルに基づく統一的保証ケース作成法 b)支援ツール(UC2CT) c)手法とツールの適用評価
2	コードに基づく保証ケース作成法	a)入力仕様に基づくコード保証ケース作成法 b)OpenSSLの脆弱性評価に基づき、有効性を確認 c)コード保証ケースのメタモデル
3	保証ケースレビュ手法	a)対象、特性、リスク、対策によるシステミグラム作成法 b)システミグラムによる保証ケースの定量的レビュ手法 c)実験による有効性の定量評価
4	開発技術者向け教育研修教材を作成	a)モデルに基づく統一的保証ケース作成法研修教材 b)システミグラムによる保証ケースレビュ法研修教材 c)開発技術者向け研修の実施評価
5	保証ケース導入準備能力評価指標	a)保証ケース導入準備能力評価指標(50) b)保証ケース導入準備能力パターン c)新技術導入準備能力評価指標

研究成果の発表、投稿状況

1. S. Yamamoto, A Generic Assurance case development method, TOG Baltimore 2015
2. S. Yamamoto, Assuring Security through Attribute GSN, ICITCS 2015
3. S. Yamamoto, An approach to assure Dependability through ArchiMate, Assure 2015
4. S. Yamamoto, A Capability Index for introducing Assurance case, TOG Edinburgh 2015
5. S. Yamamoto, An assurance case review method using Systemigram, AAA2015
6. 山本他, モデルに基づく統一的保証ケース作成手法の提案、KSN研究会、2015. 10
7. 山本他、構成情報に基づく保証ケースレビュ手法の提案、KSN研究会、2015. 10
8. 山本他、入力分析に基づくコード保証方法の提案、KBSE研究会、2015.10
9. 山本、要求リスクコミュニケーション、KBSE研究会、2015.10
10. 山本、RISE保証ケース作成支援方式の研究、D-Case研究会、2015.10
11. 山本、保証ケース導入準備能力評価指標の提案、KBSE研究会、2016.3
12. 山本、保証ケースの先端研修教材の試作と評価、KSN研究会、2016.3
13. 山本他、GSNレビュ実験と評価について、KSN研究会、2016.3
14. 山本、保証ケース作成のフロンティア、D-Case研究会、2016.4

名古屋大学

モデルに基づく保証ケースの統一的作成法

研究の目的と課題

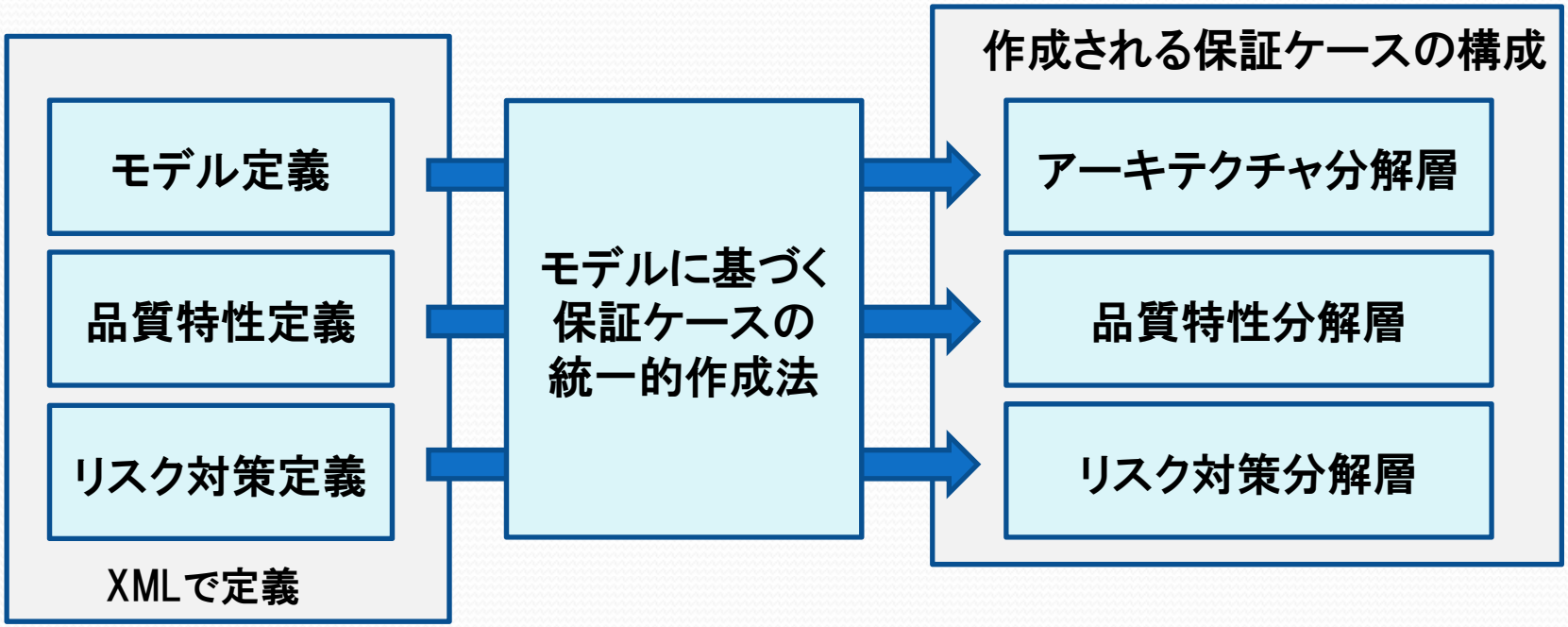
【目的】

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。

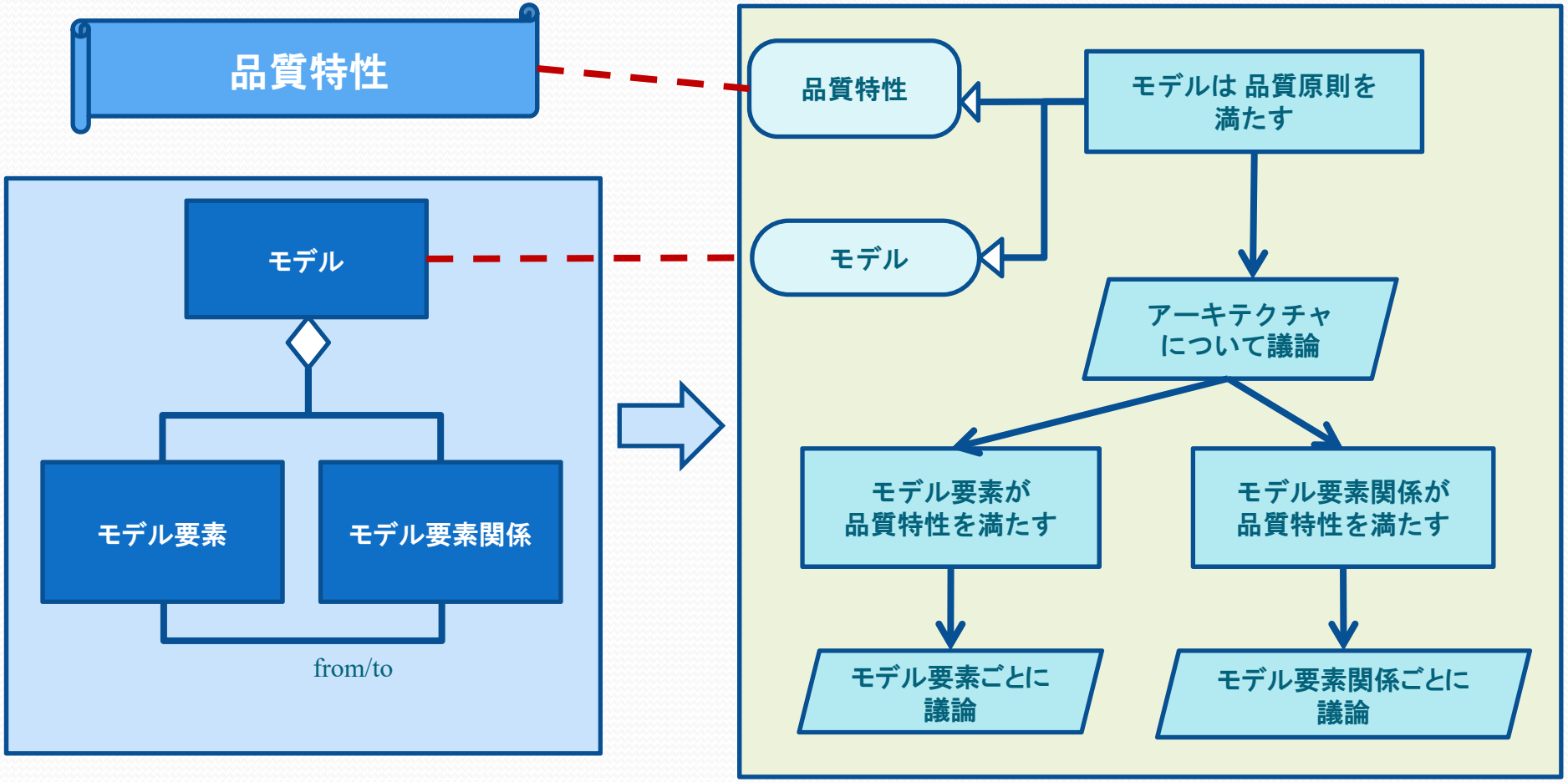
【課題】

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。

モデルに基づく保証ケースの統一的作成法



モデルに基づく保証ケース作成方式



Generic model configuration

Assurance case derived from the model

保証ケース生成アルゴリズム

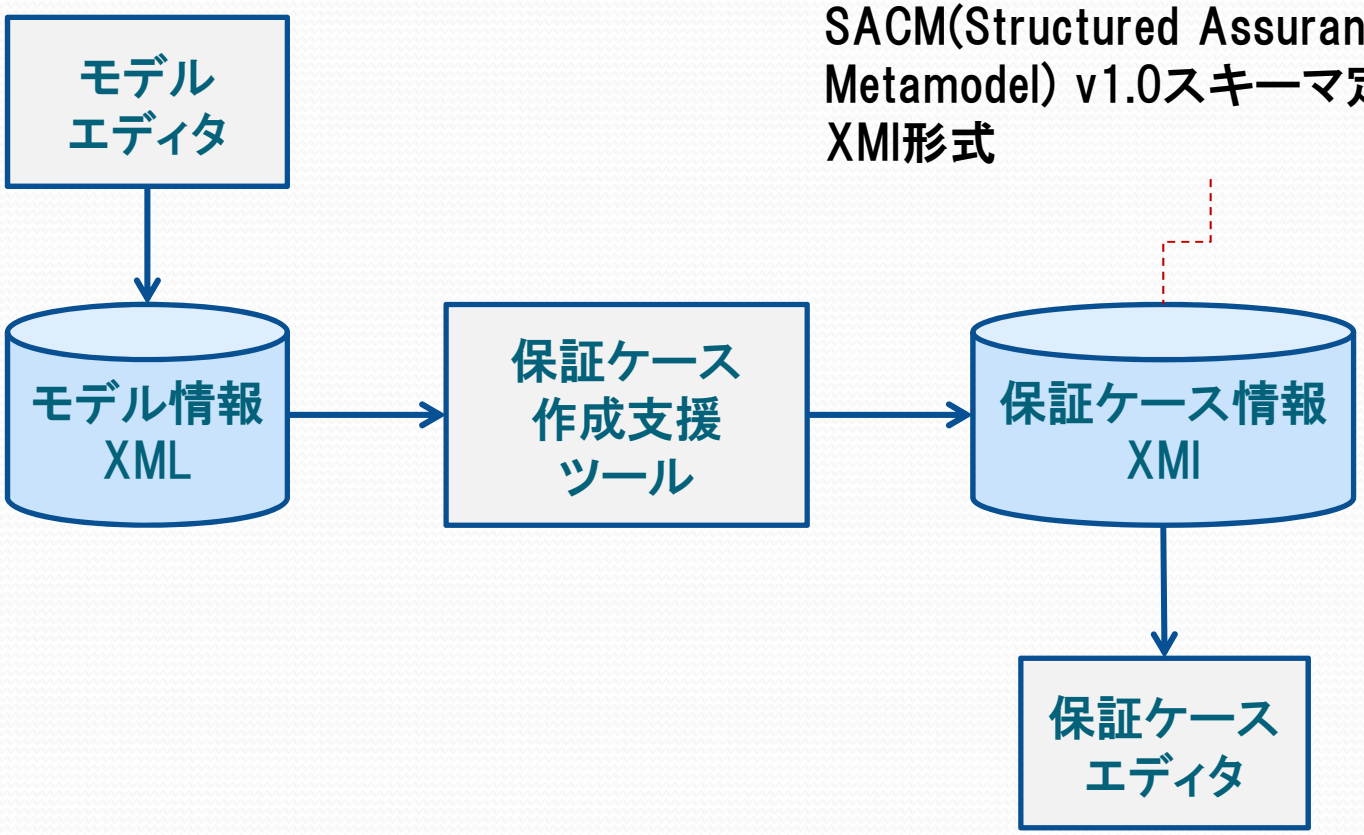
For each model A=<Concept Set, Relationship Set>,
where ConceptSet={<Name, Cc >|Cc is a Concept category of the model}
RelationshipSet={<Name, Cr >|Cr is a Relationship category of ArchiMate}
the following sets are calculated.

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.

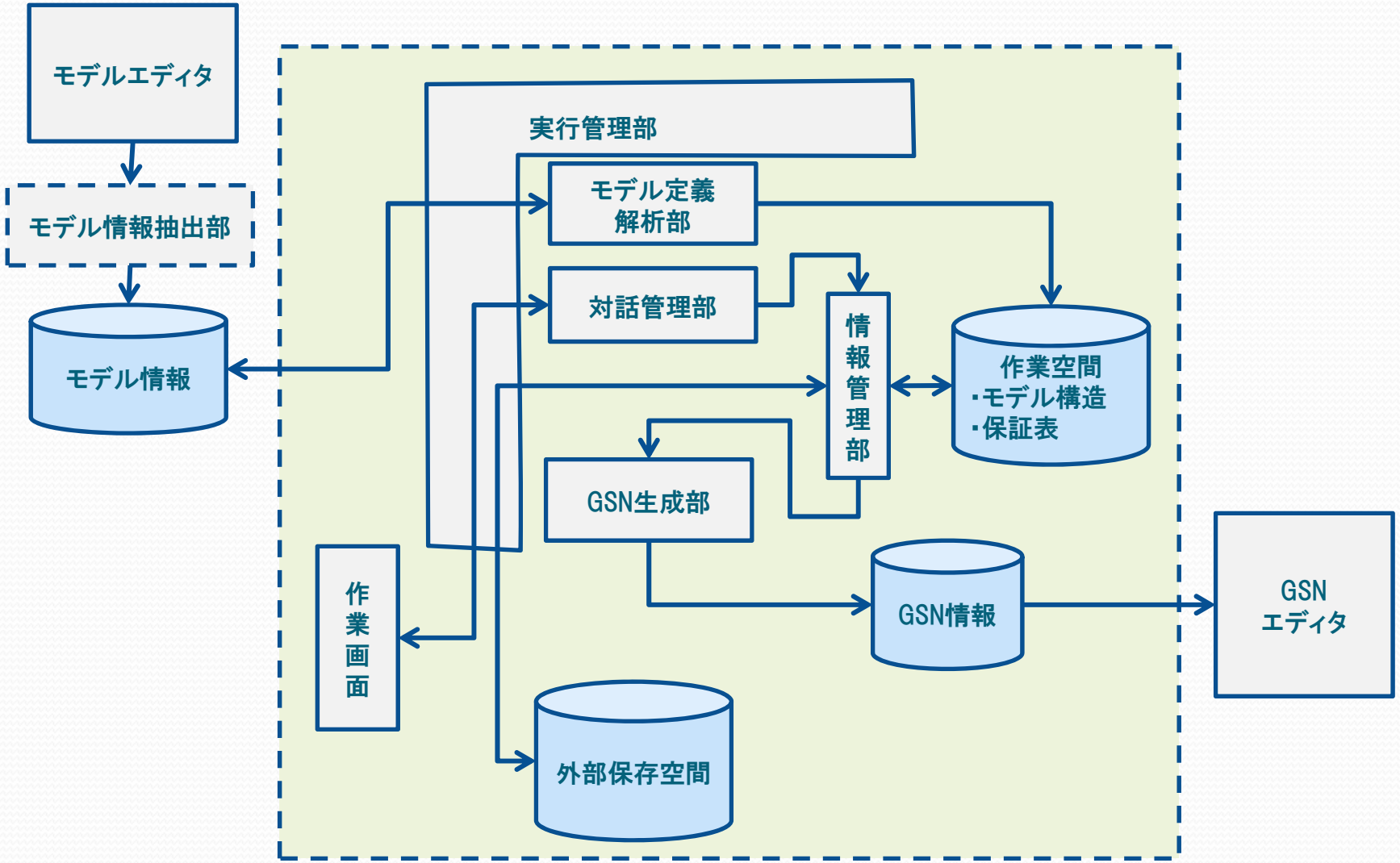
The root goal can simply be developed such that
the model A satisfies dependability principles.
Second level goals are derived by Concept and Relationship
Third level goals are derived by using
ConceptCategory(A) and RelationshipCategory(A)
Fourth level goals are derived by using
ConceptInstance(C, A) 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.

保証ケース作成支援システムの概要



UC2CT: Unified Context to Claim Tool

統一的保証ケース作成支援システムの構成



モデル定義例

```
<?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>
```

特性定義例

```
<?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>
```

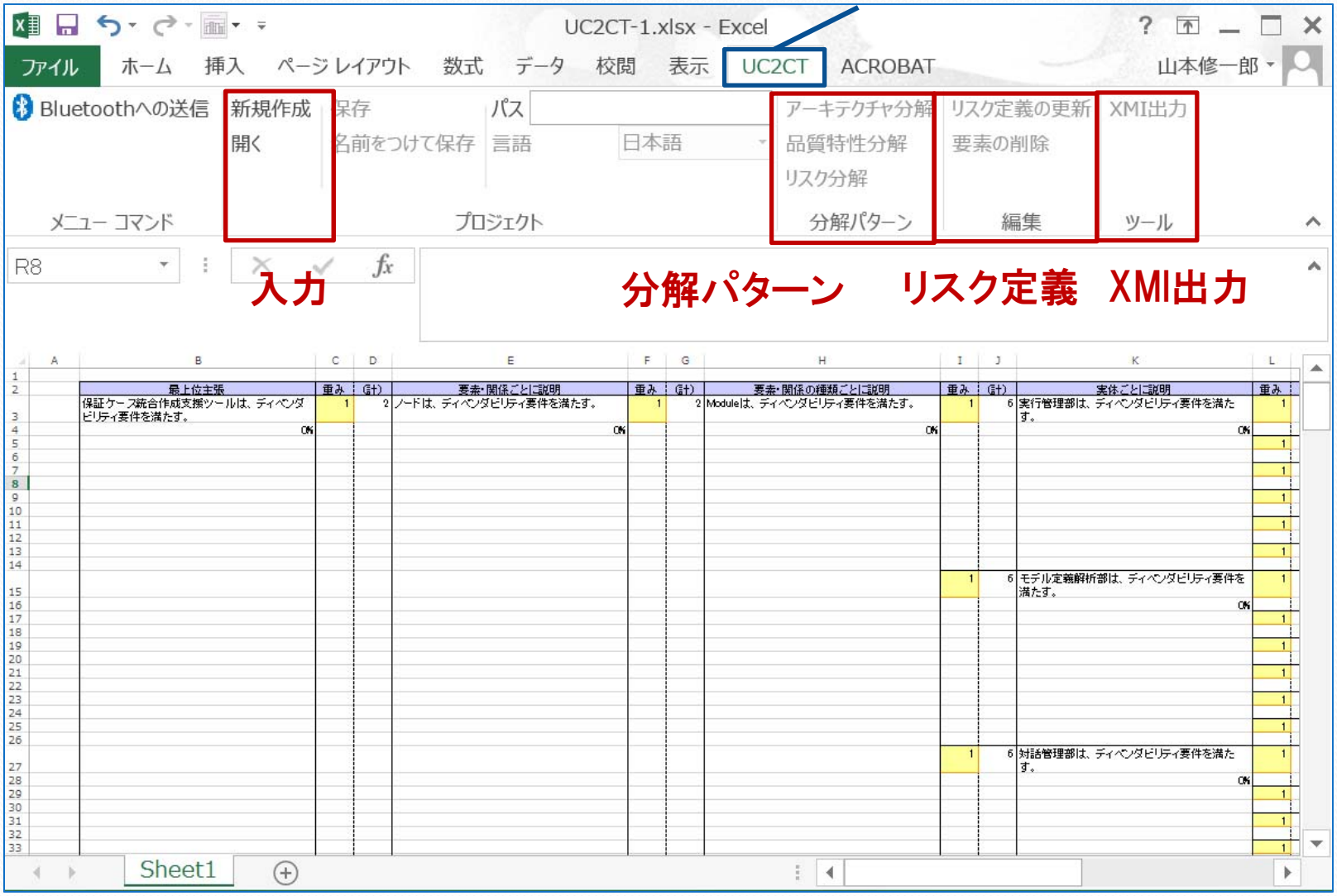
リスク定義例

```
<?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>
```

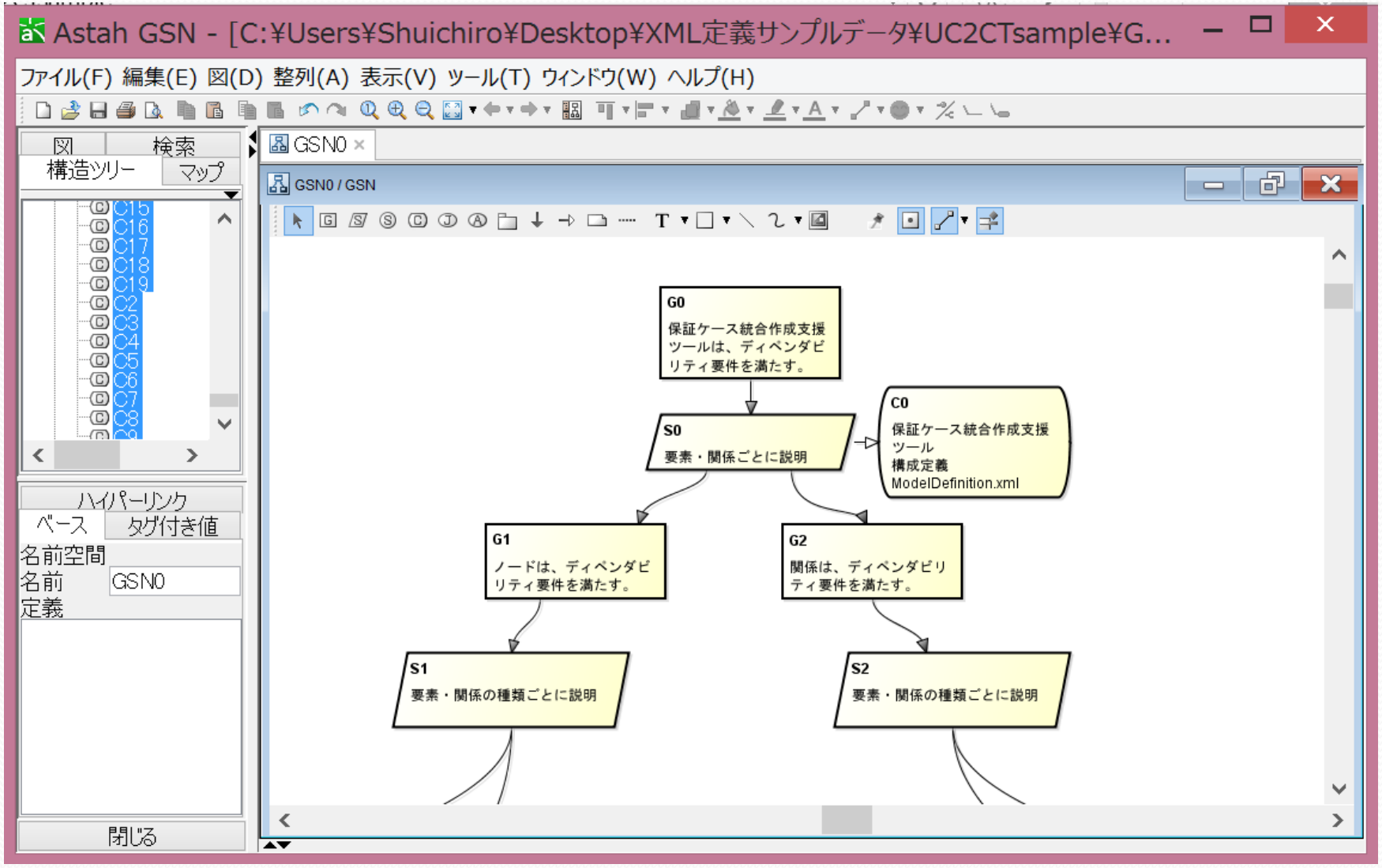
```
- <deviations>
  - <deviation name="Exceptionリスク">
    - <list>
        <item>入力例外</item>
        <item>処理例外</item>
        <item>出力例外</item>
      </list>
    </deviation>
```

```
  </deviations>
</riskDefinition>
```

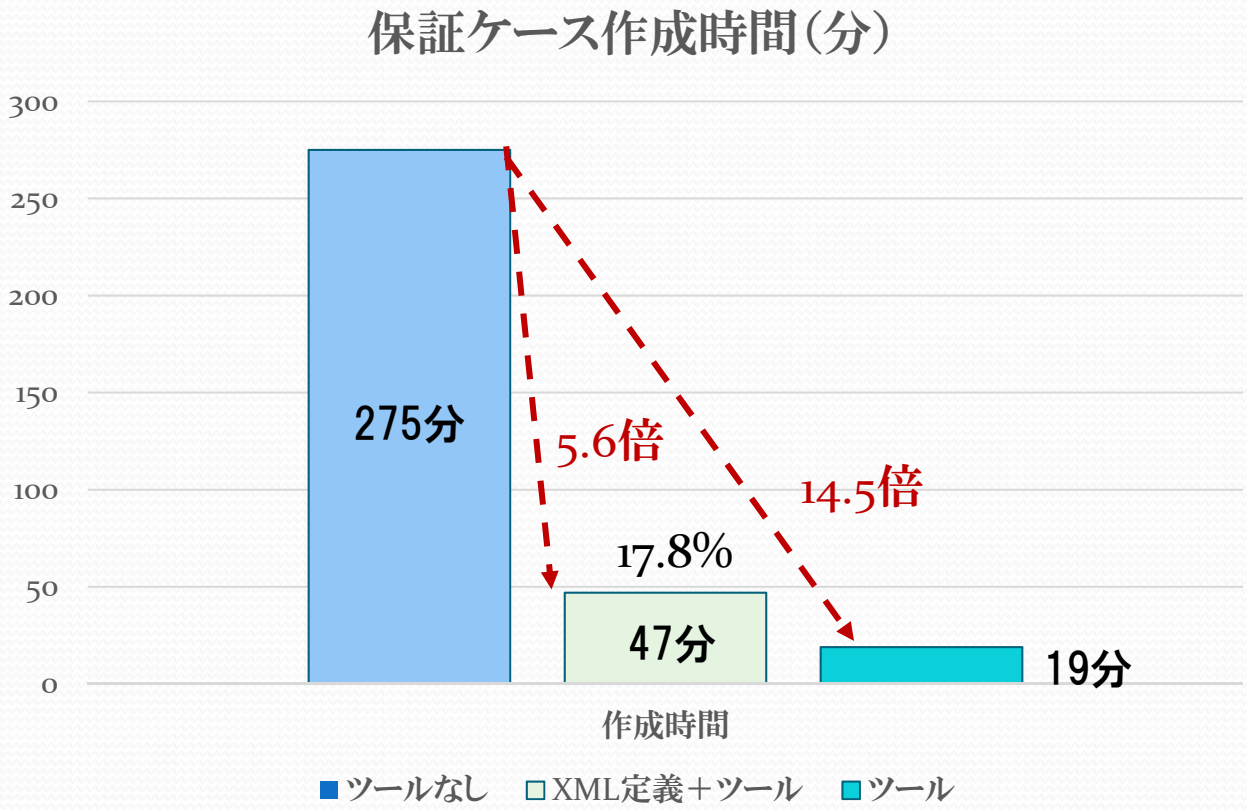
UC2CT(Unified Context to Claim Tool)ツール画面例



UC2CT による保証ケース作成例



保証ケース作成効果



保証ケースのノード数

主張	218
戦略	53
前提	47
証拠	165

*)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

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。

名古屋大学

コンポーネントに対する保証ケース作成法

研究の目的と課題

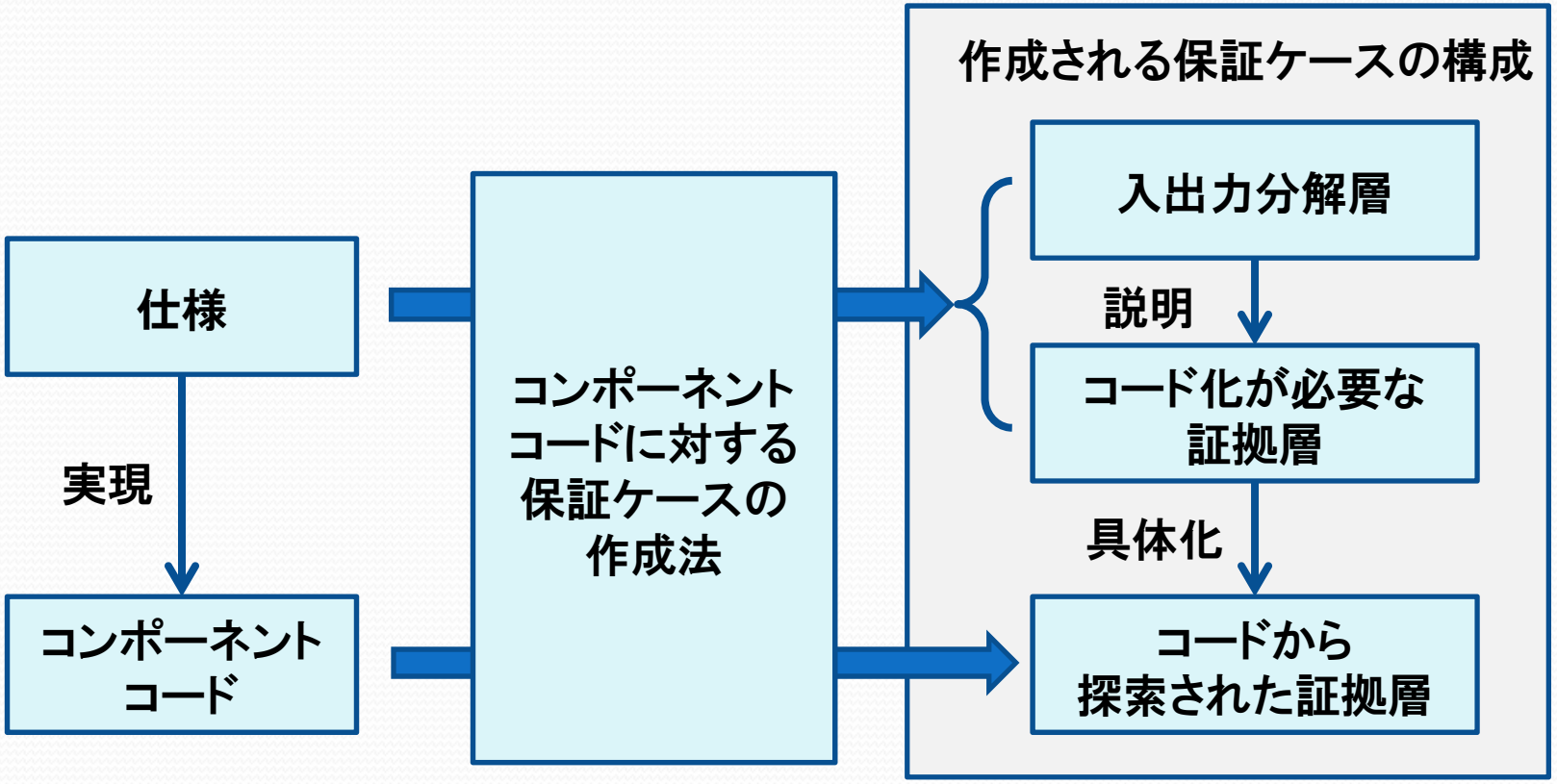
【目的】

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。

コンポーネントに対する保証ケース作成法



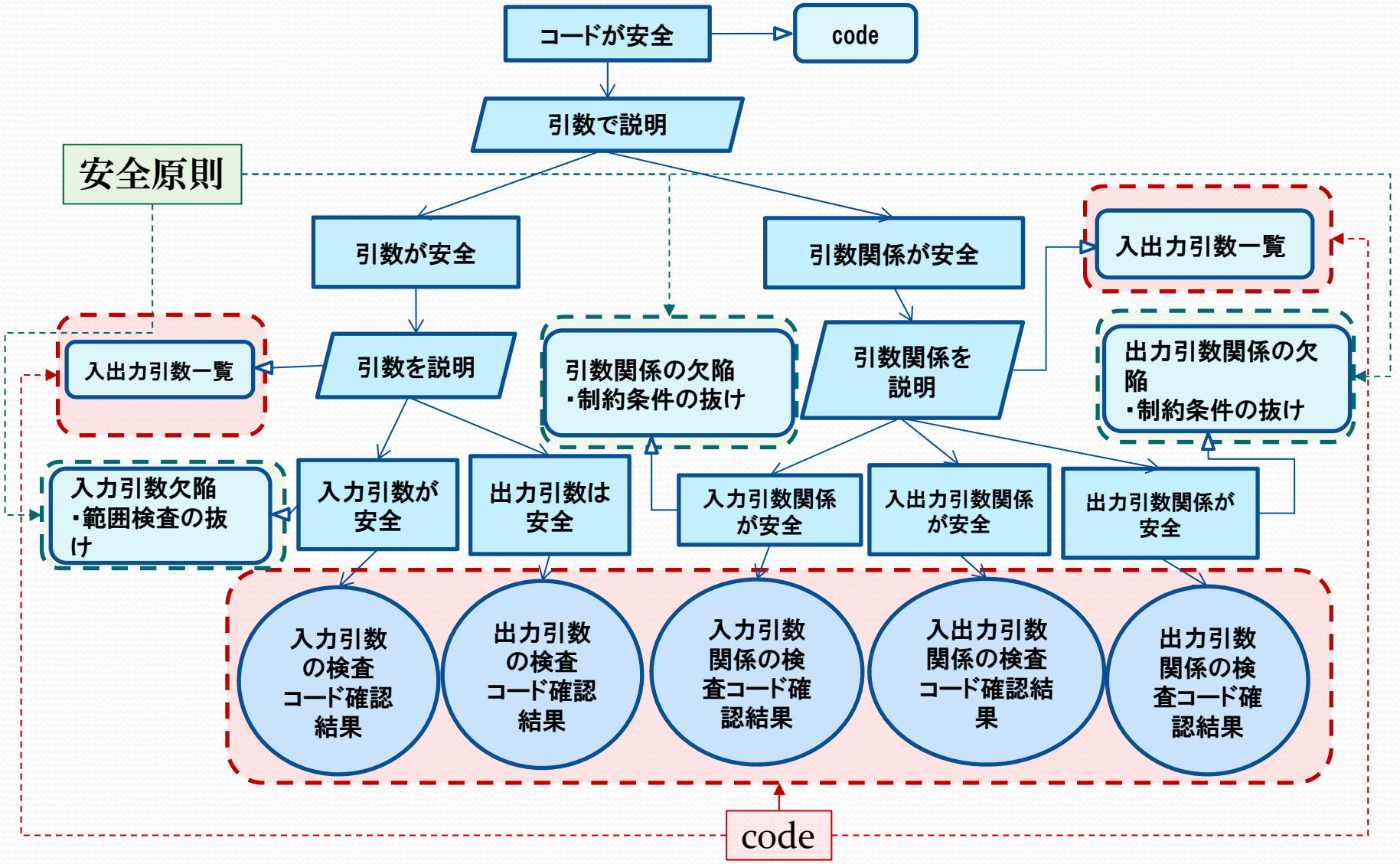
保証ケースに基づく欠陥コード摘出手順

- 入力仕様に基づき入力制約を作成
- 入力制約に基づき、保証ケースを作成
- 対応するコード断片を証拠に用いて、保証ケースを説明
- 保証ケースの主張を説明するコード断片がないことによって、コードの欠陥を摘出

【説明による欠陥摘出原理　DDBE】

Defect Detection By Evidence

Assurance case development for codes

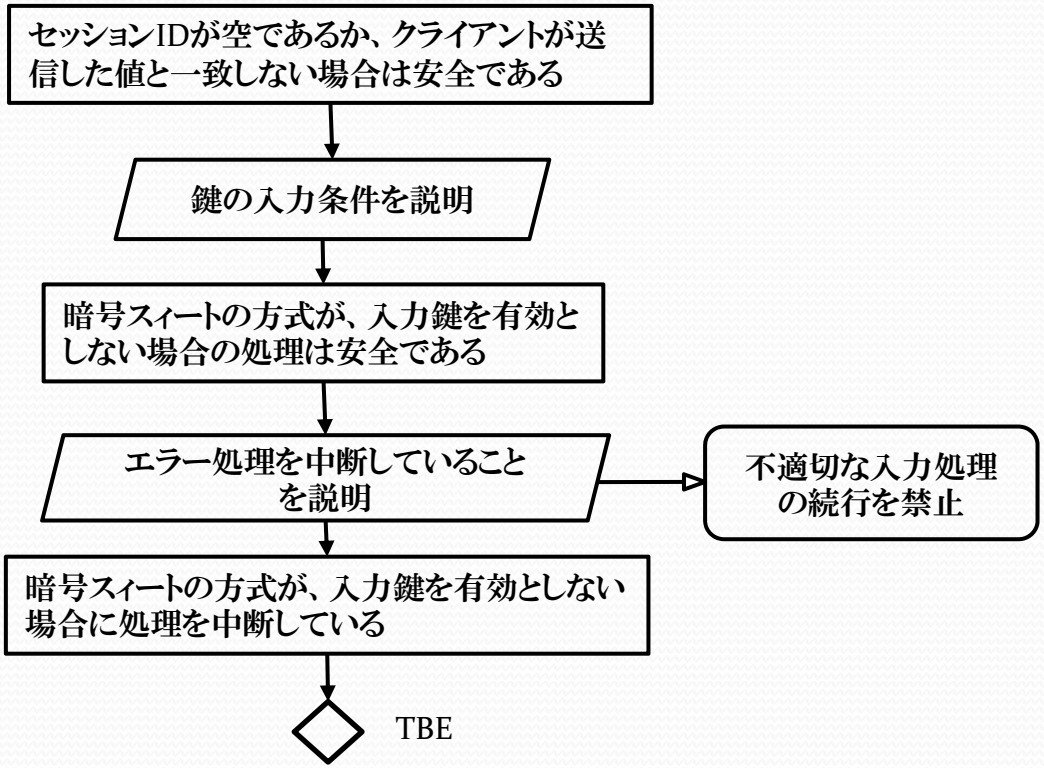


評価実験の概要

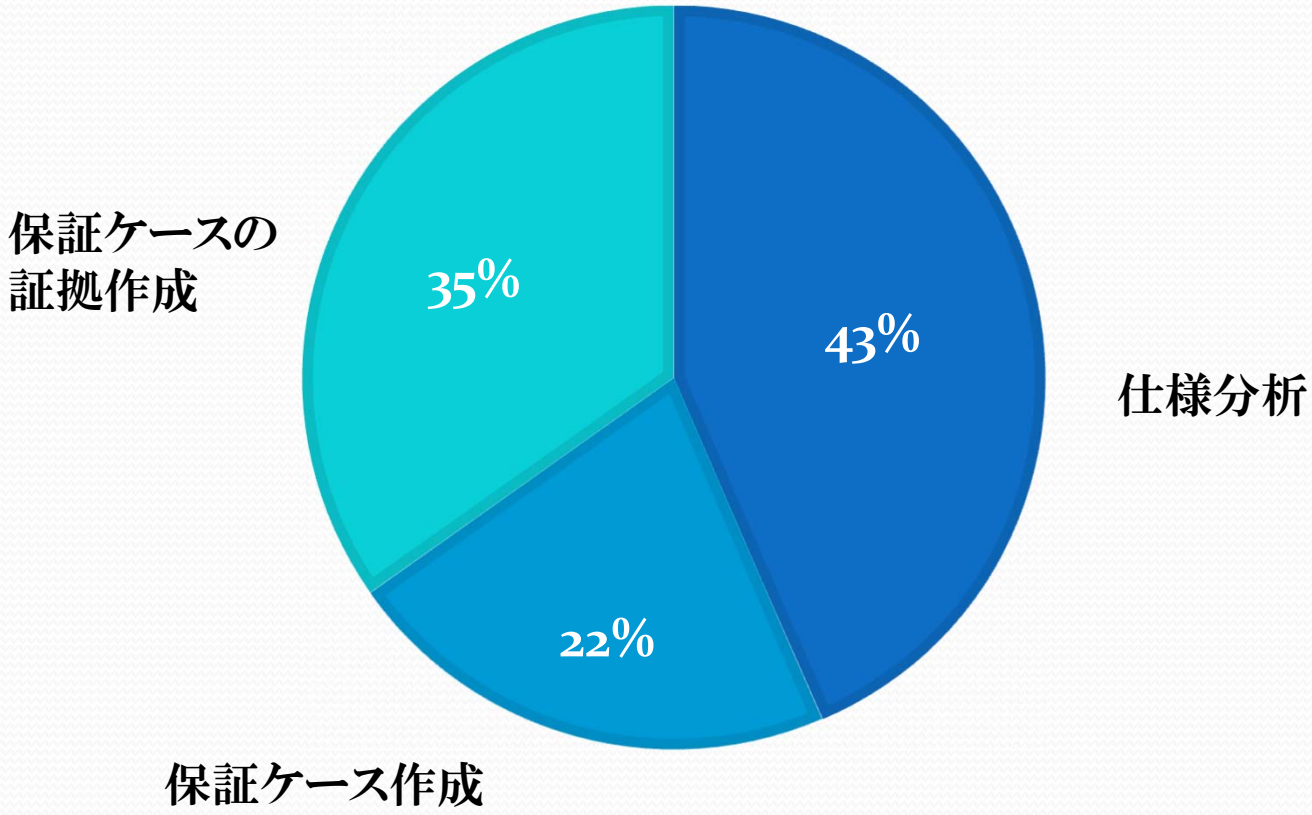
- 実験対象
  - SSL/TLS Protocol V 1.0, 3584 Lines 入力仕様
  - OpenSSL 1.0.1j s3_clnt.c , 3469 LOC 保証対象コード
- 入力仕様分析 10H
- 保証ケース作成 5H
- コードに基づく保証ケースの説明 8H
- 11 TBEを摘出
  - 10件を具体化
  - 1件が具体化不能 => Open SSL の脆弱性

- 被験者 名古屋大学 B4 1名

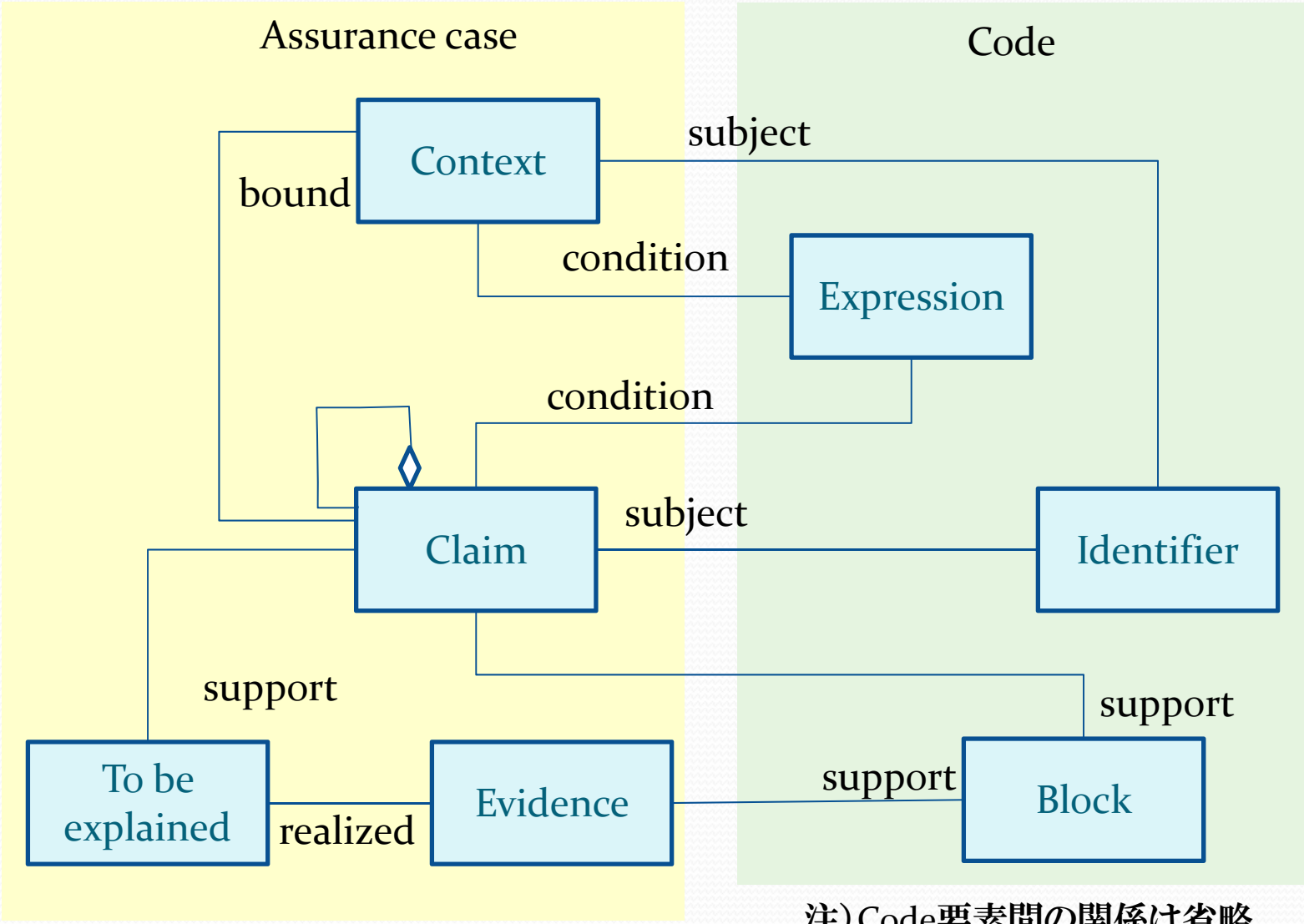
欠陥の検出と特定


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
鍵の入力条件を説明
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
エラー処理を中断していることを説明
不適切な入力処理の続行を禁止
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
TBE

コードに基づく保証ケース作成時間の内訳



Meta model



注）Code要素間の関係は省略

有識者による本研究成果の評価(1)

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。

有識者による本研究成果の評価(2)

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。

名古屋大学

保証ケースレビュ手法

研究の目的と課題

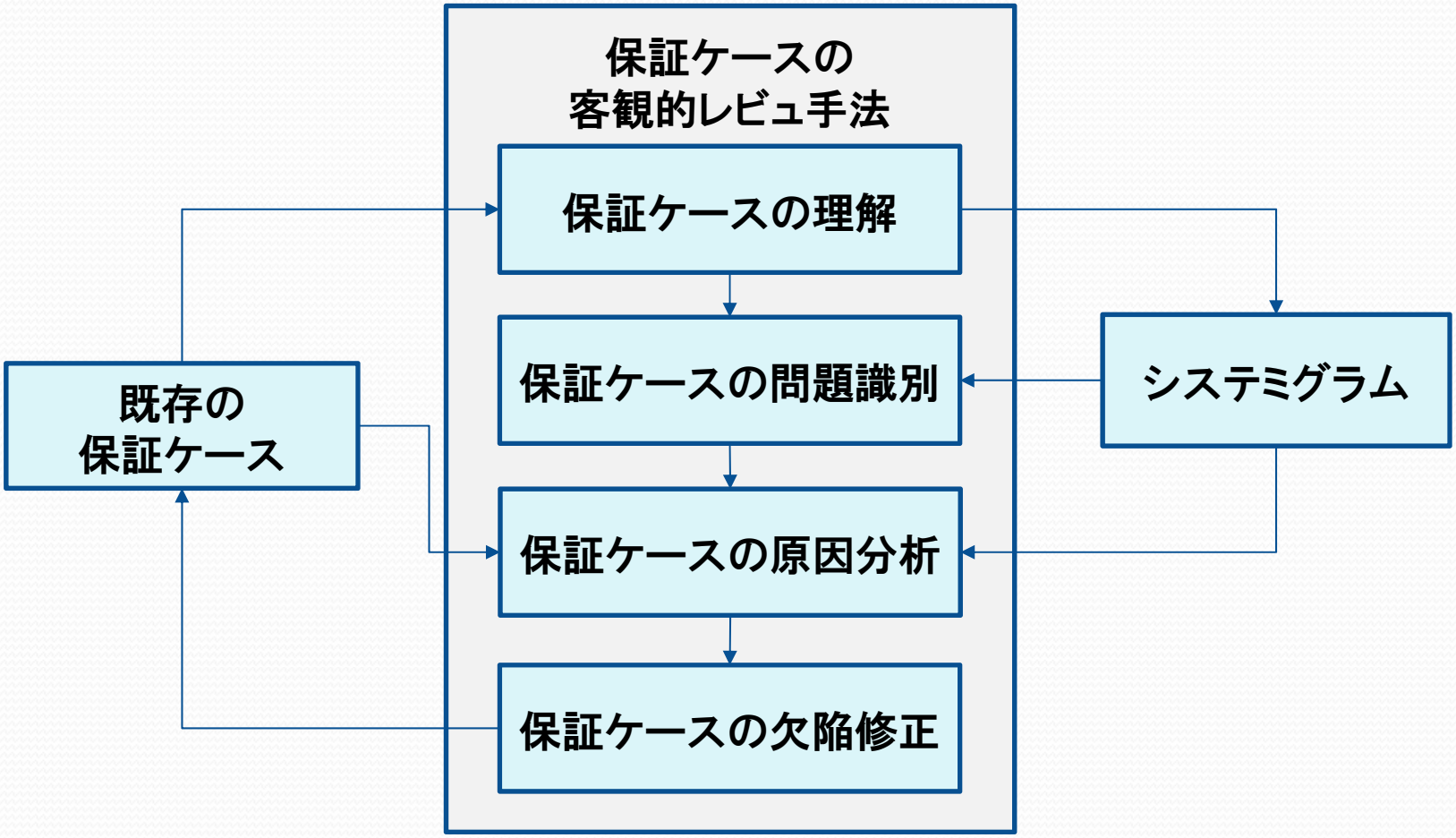
【目的】

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。

保証ケースの客観的レビュ手法

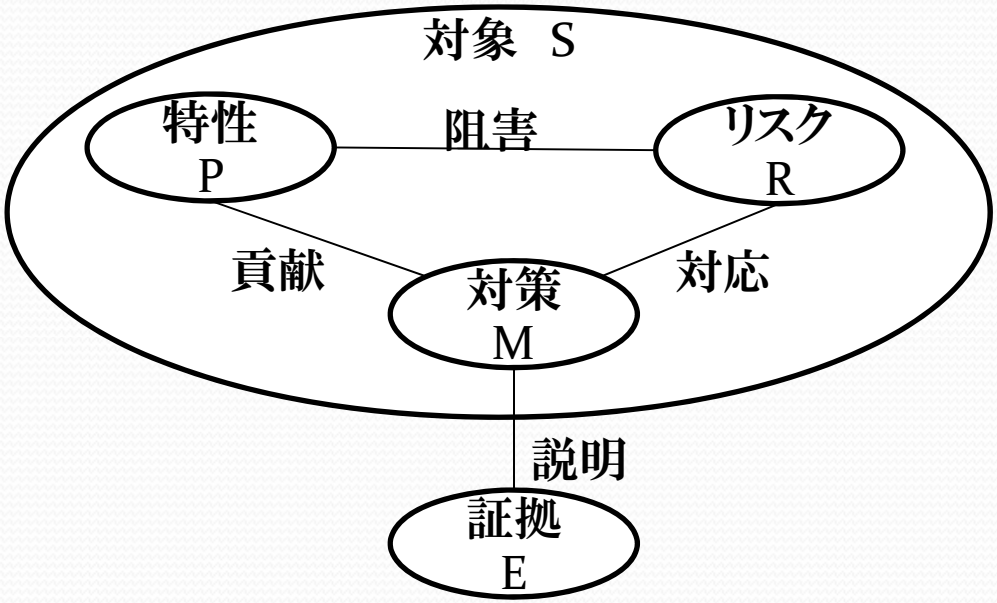


SPRMEに対するシステミグラムの例

- SPRME法(対象　S、特性　P、リスク　R、対策　M、証拠　E)

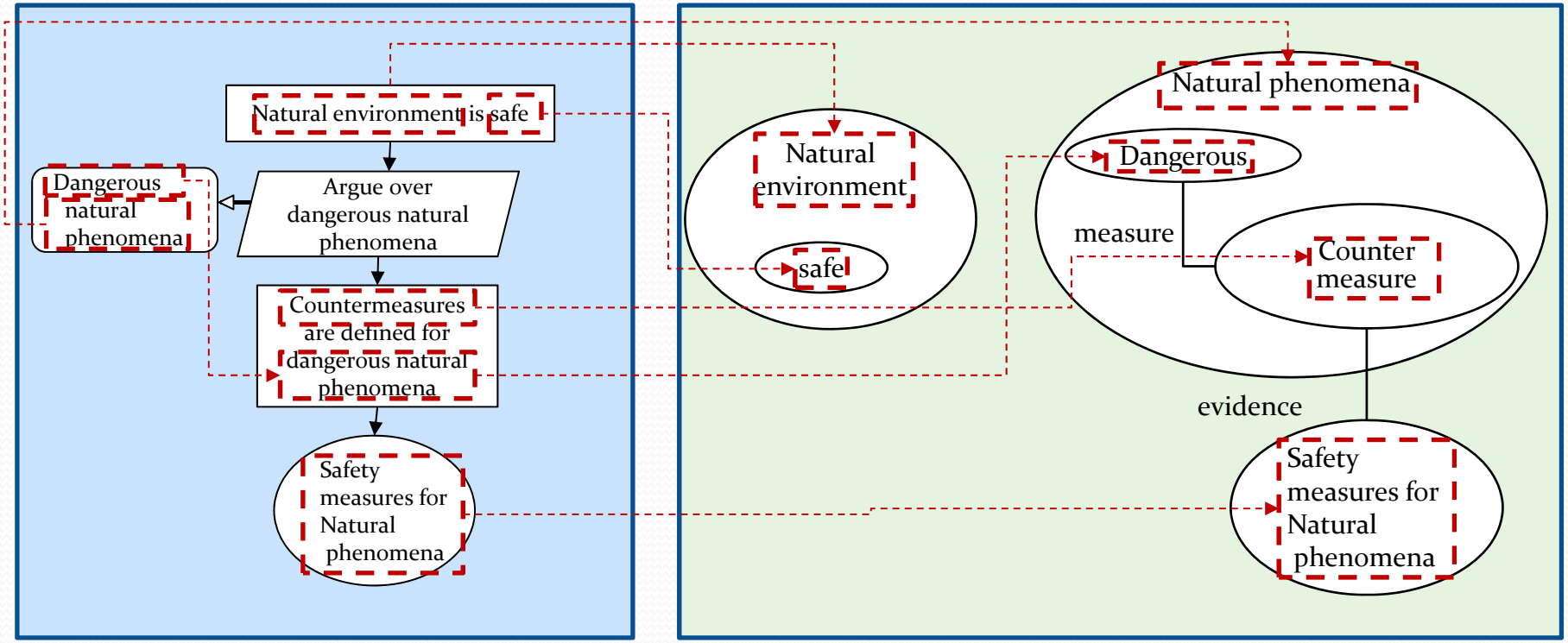
- 対象Sが特性Pを持つための条件

[条件1]対象Sが特性Pを持つことに対するリスクRを識別している
[条件2] Rへの対策Mとその証拠Eを確認している



保証ケースとsystemigramの対応付け

Systemigramを作成することで、自然環境の安全性を、自然現象のリスク対策で保証しようとしていることが明確になる。「自然環境」と「自然現象」の同一性を吟味する必要がある。



Assurance case

Systemigram

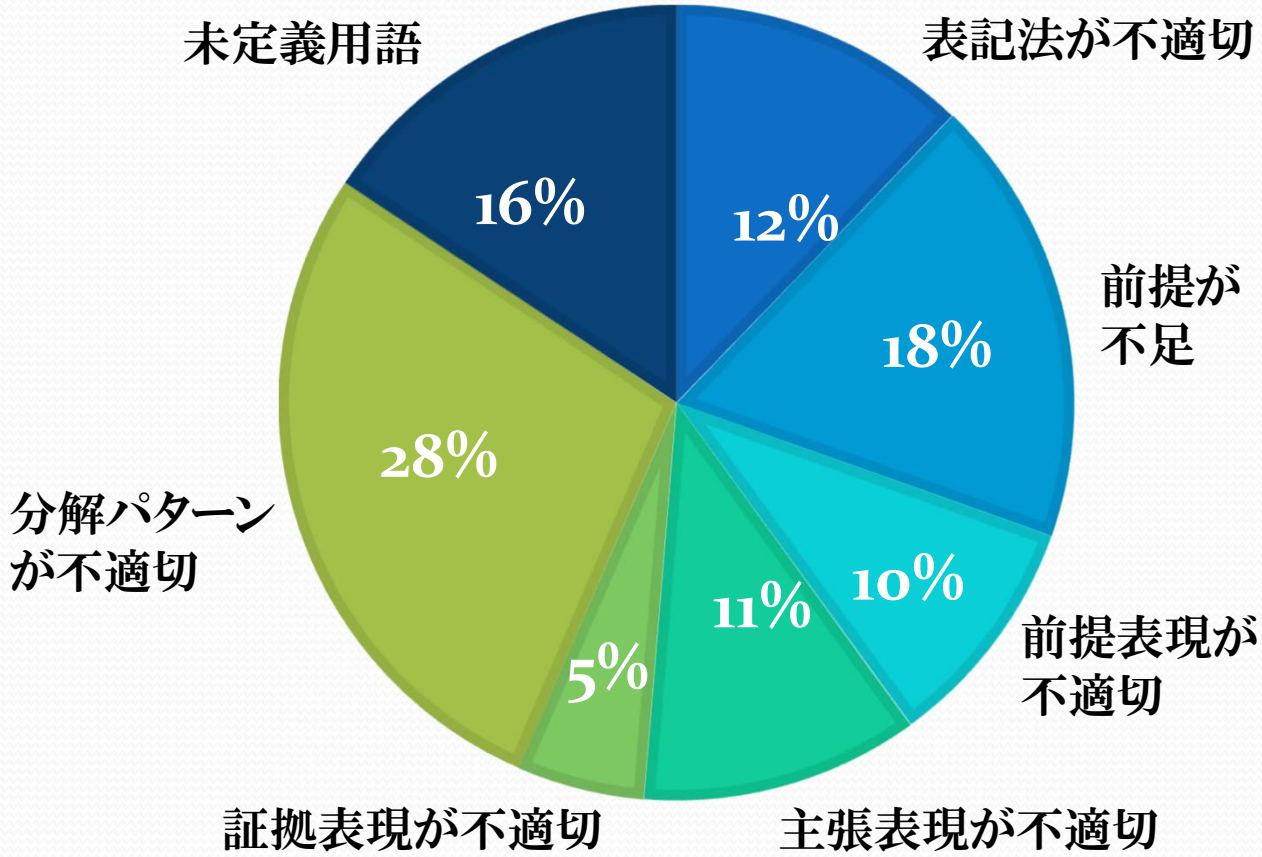
保証ケースレビュ比較実験の概要

- レビュ対象の保証ケース　　14名（X大　M, GSN経験なし）
- レビュ担当者　　2名（名大　M, GSN経験あり）
- 保証ケースレビュ
  - 手法適用なし　　「保証ケースレビュの属人性を確認」
    - 指摘項目数　　平均3.1件　（最小0件、最大7件）
    - 共通指摘項目数　　平均0.7件　（最小0件、最大4件）　：22.6%
    - 非共通指摘項目数　　平均2.4件　：77.4%
  - 手法適用あり
    - 指摘項目数　　平均9.8件　（最小0件、最大18件）
    - 共通指摘項目数　　平均5.4件　（最小0件、最大14件）：55.5%
    - 非共通指摘項目数　　平均4.4件　：44.5%

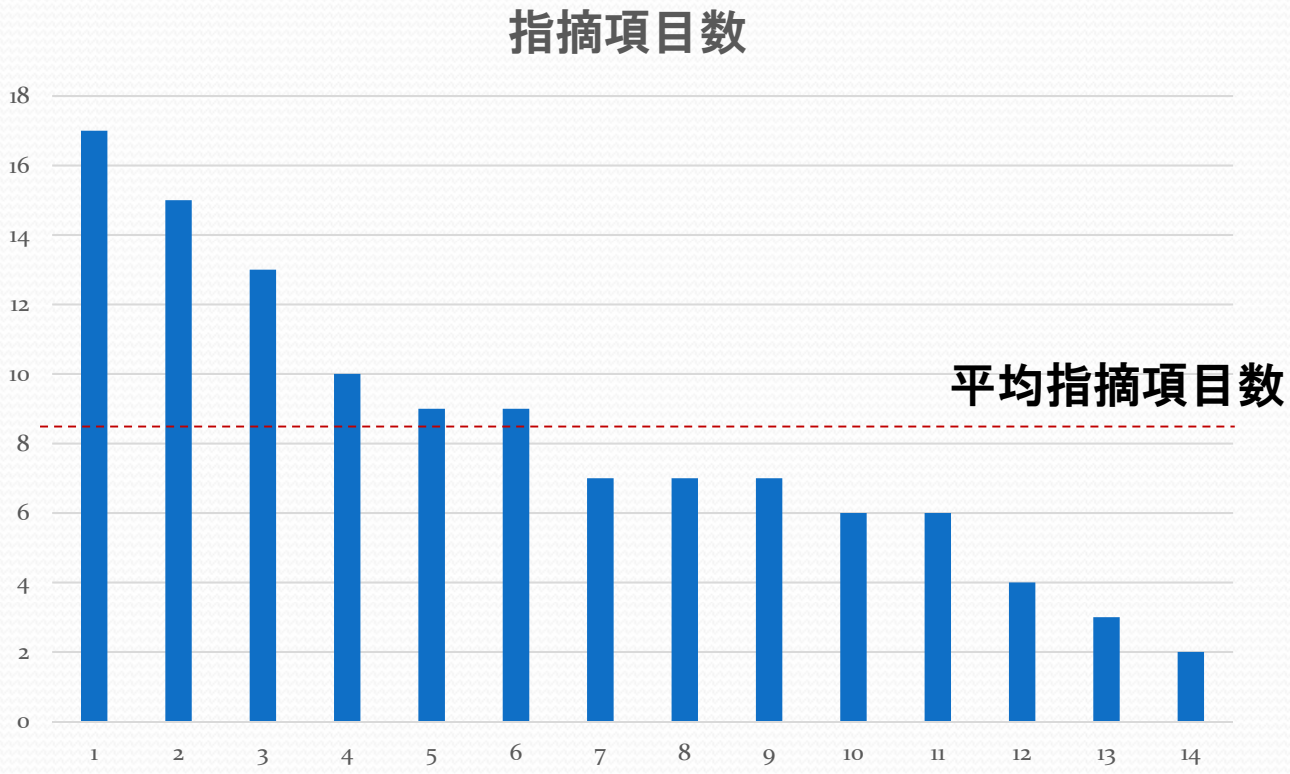
指摘種別による比較

指摘種別	共通(%)	差異(%)
GSNの表記法が不適切	35.7	64.3
前提ノードの不足	85.7	14.3
前提の表現が不適切	45.5	54.5
ゴールの表現が不適切	23.1	76.9
証拠の表現が不適切	0	100
分解パターンが不適切	28.1	71.9
未定義の用語	0	100

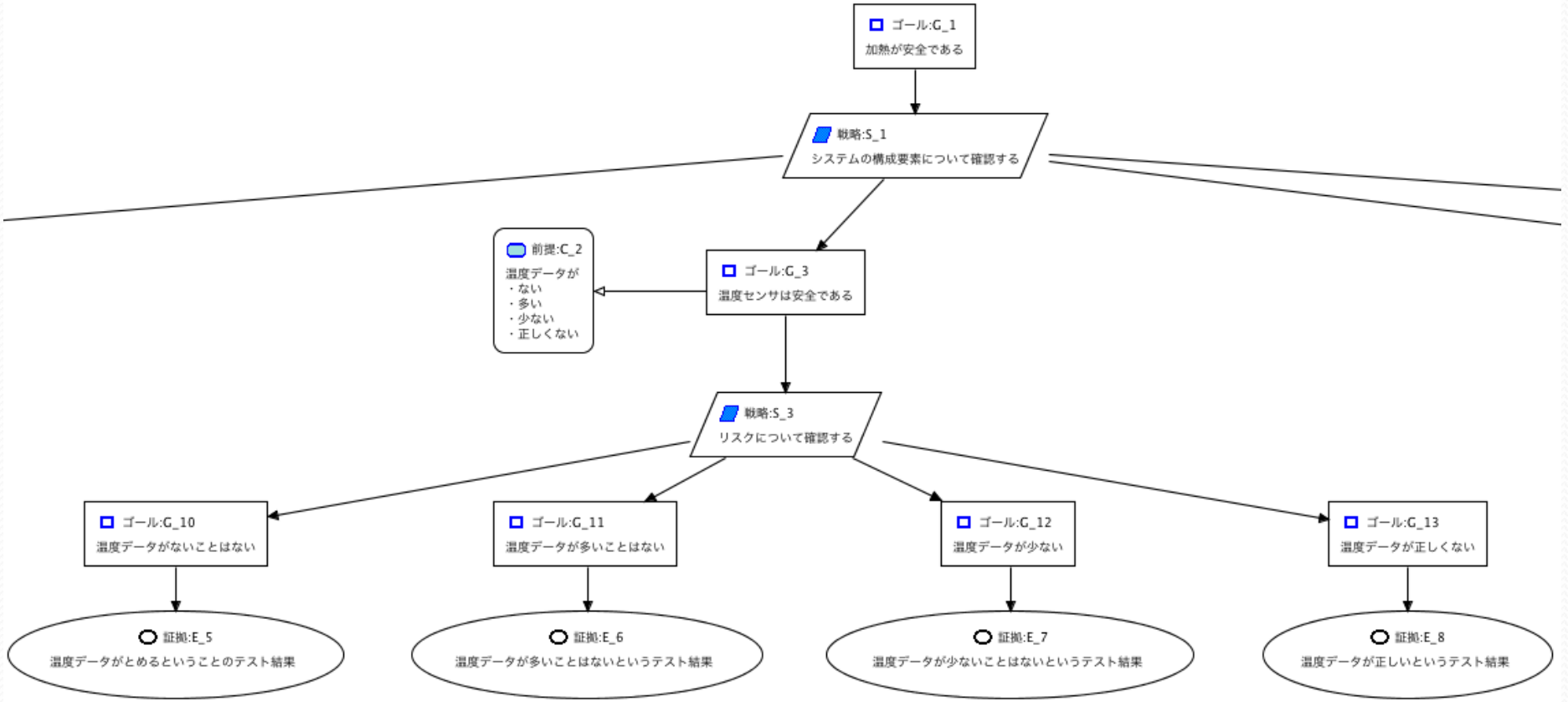
保証ケースの指摘項目数の内訳



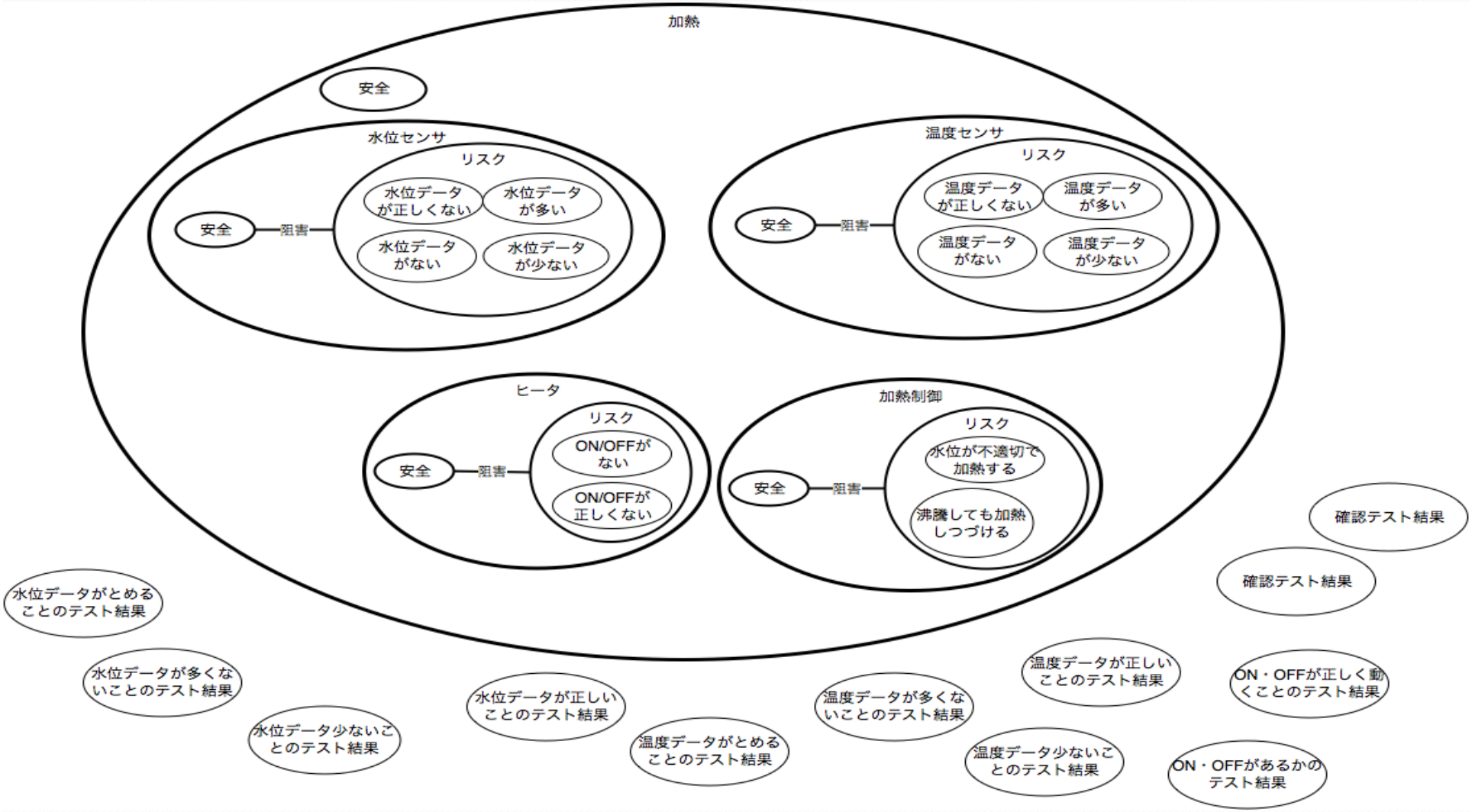
指摘項目数の分布



被験者が作成した保証ケースの例(一部)



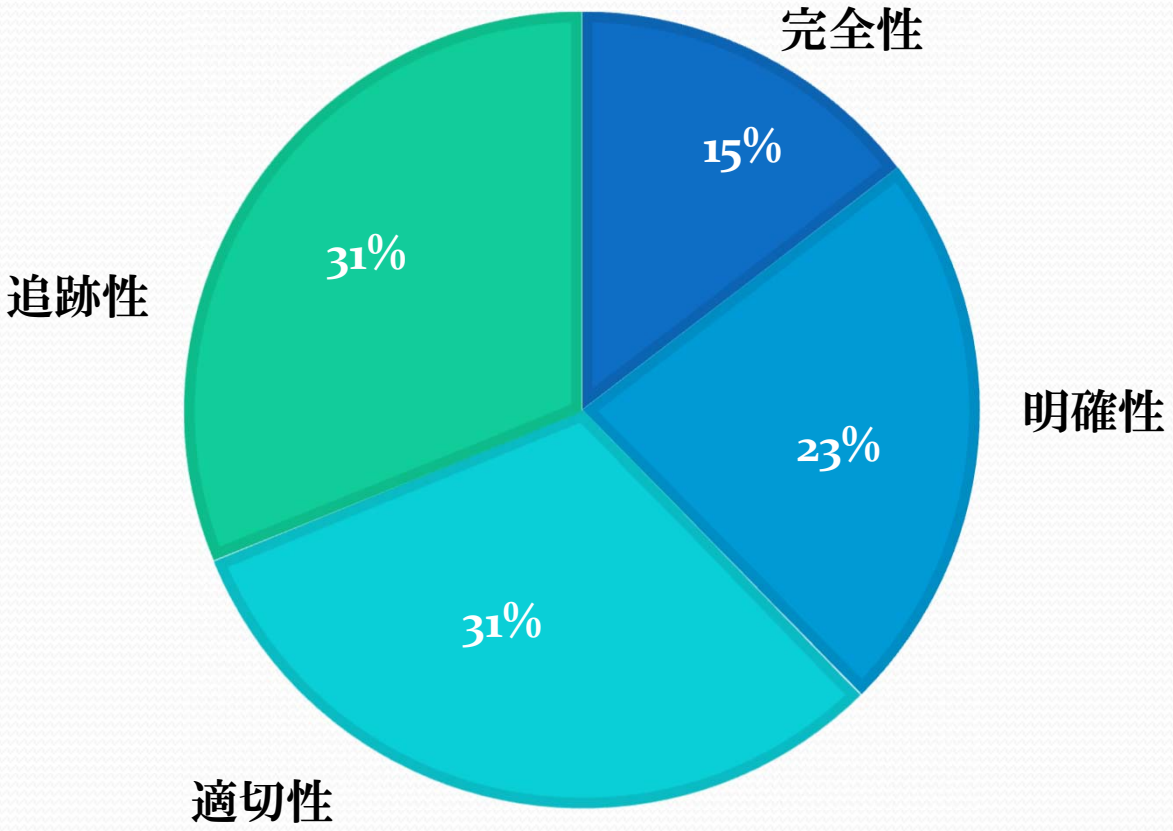
保証ケースから作成したシステミグラムの例



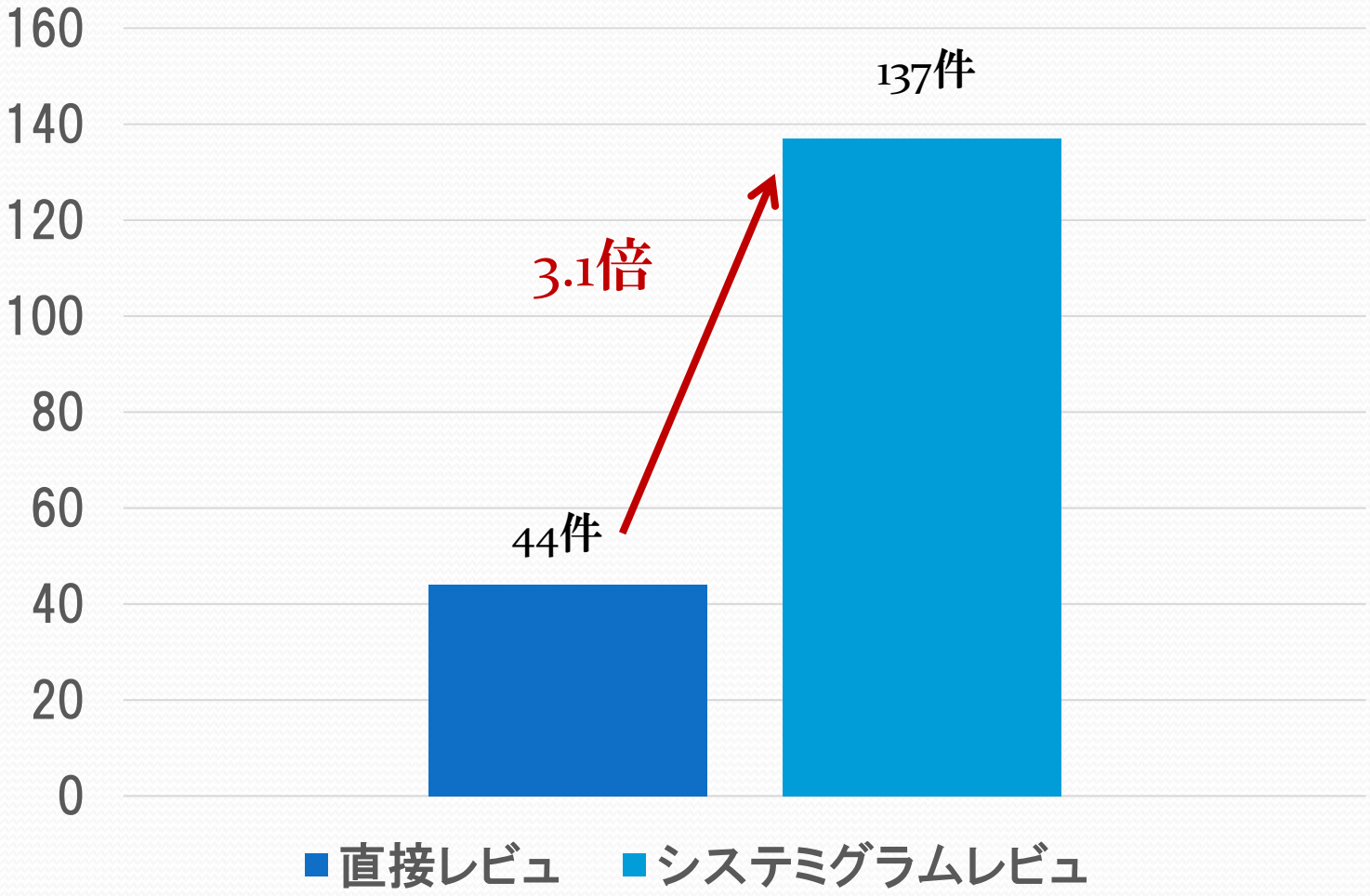
保証ケースレビュ指標

観点	定義	欠陥	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	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	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	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	追跡不能項目数

システミグラムに基づく指摘項目数の内訳

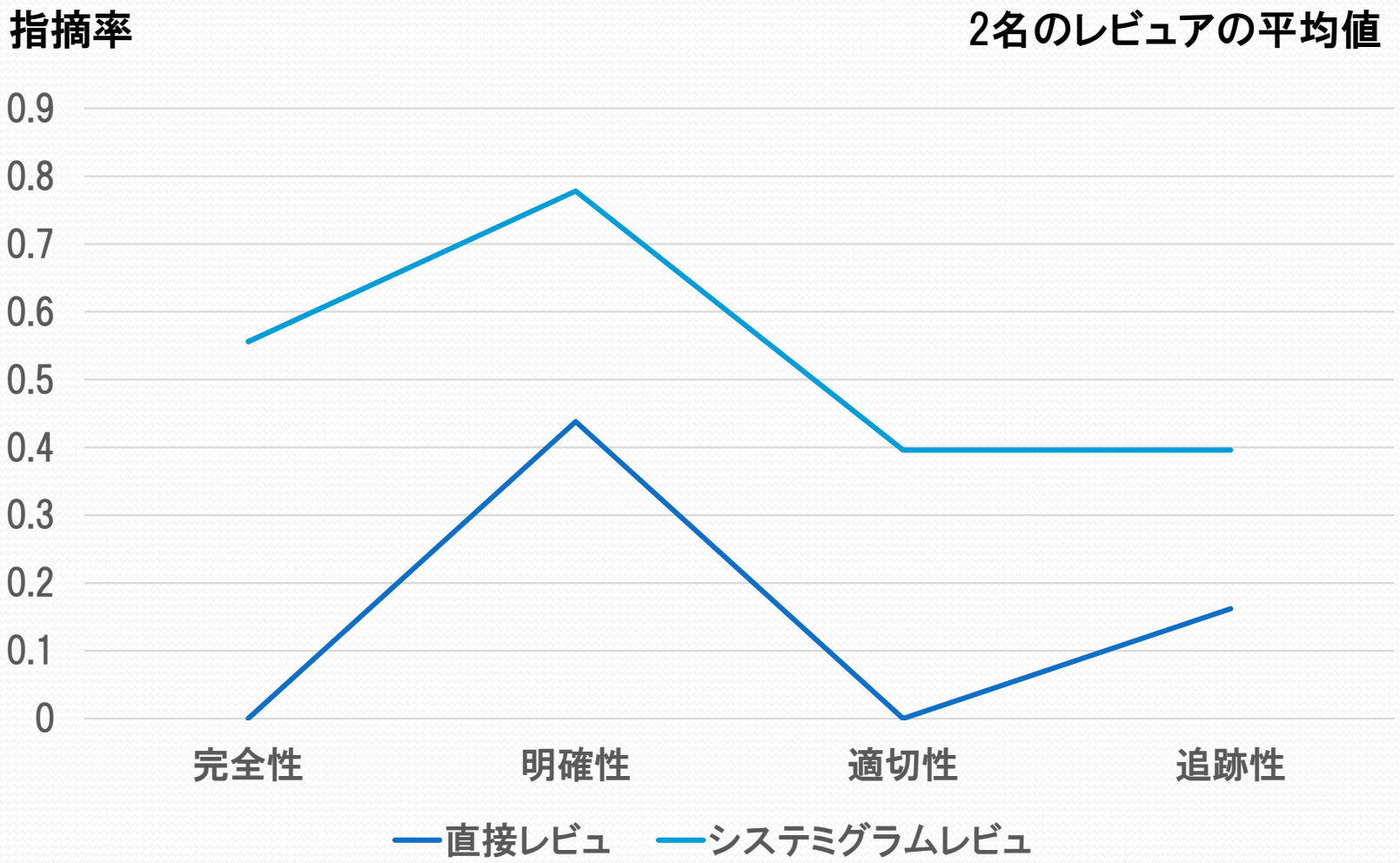


指摘件数の比較

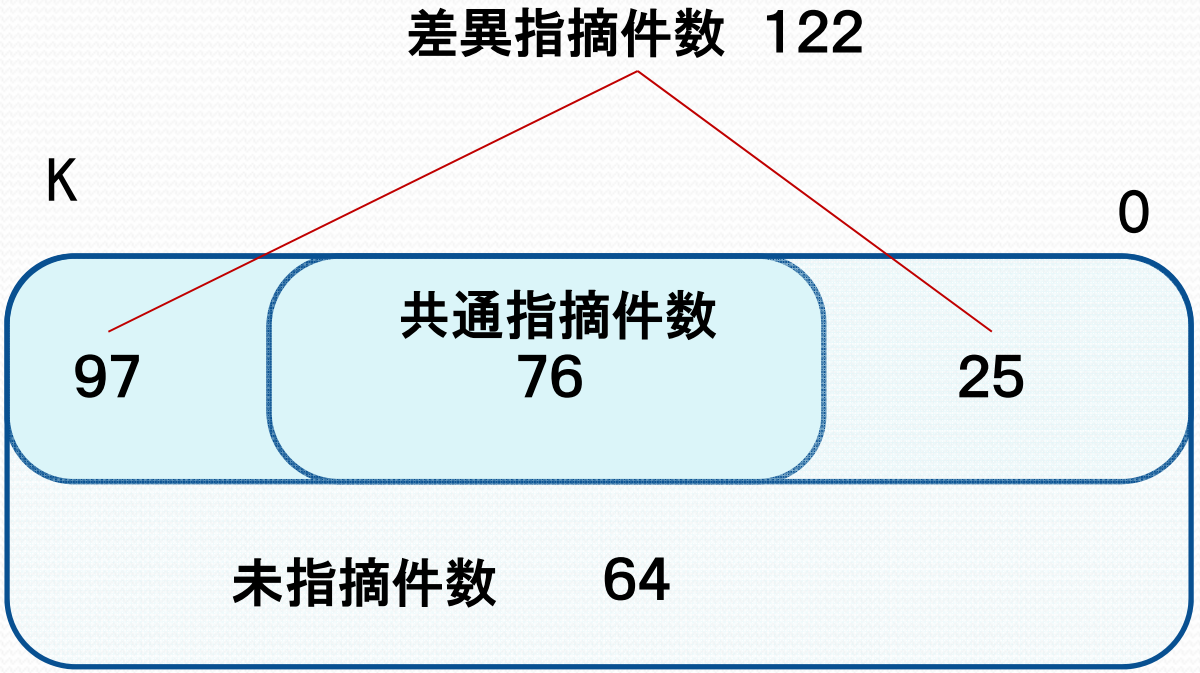


名古屋大学

レビュ能力の比較



システミグラムによるレビュ件数



【今後の課題】システミグラムの作成基準の統一が必要

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。

名古屋大学

開発技術者向け教育研修教材の作成

- 統一的保証ケース作成手法コースマップ
- 保証ケースレビュ手法

研究の目的と課題

【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。

ISD(Instructional Systems Design)

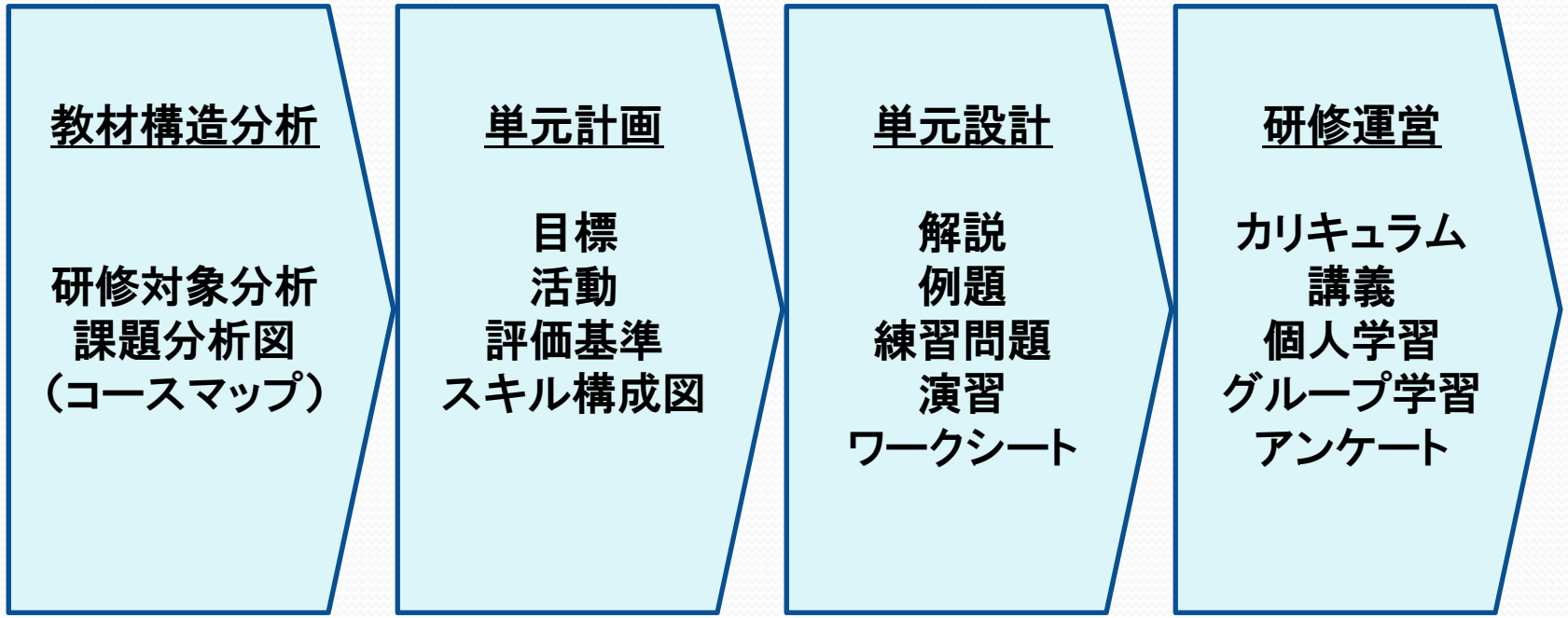
分析、設計、開発、実施、評価からなるプロセスにより、効果的な教材を設計する手法

【課題】

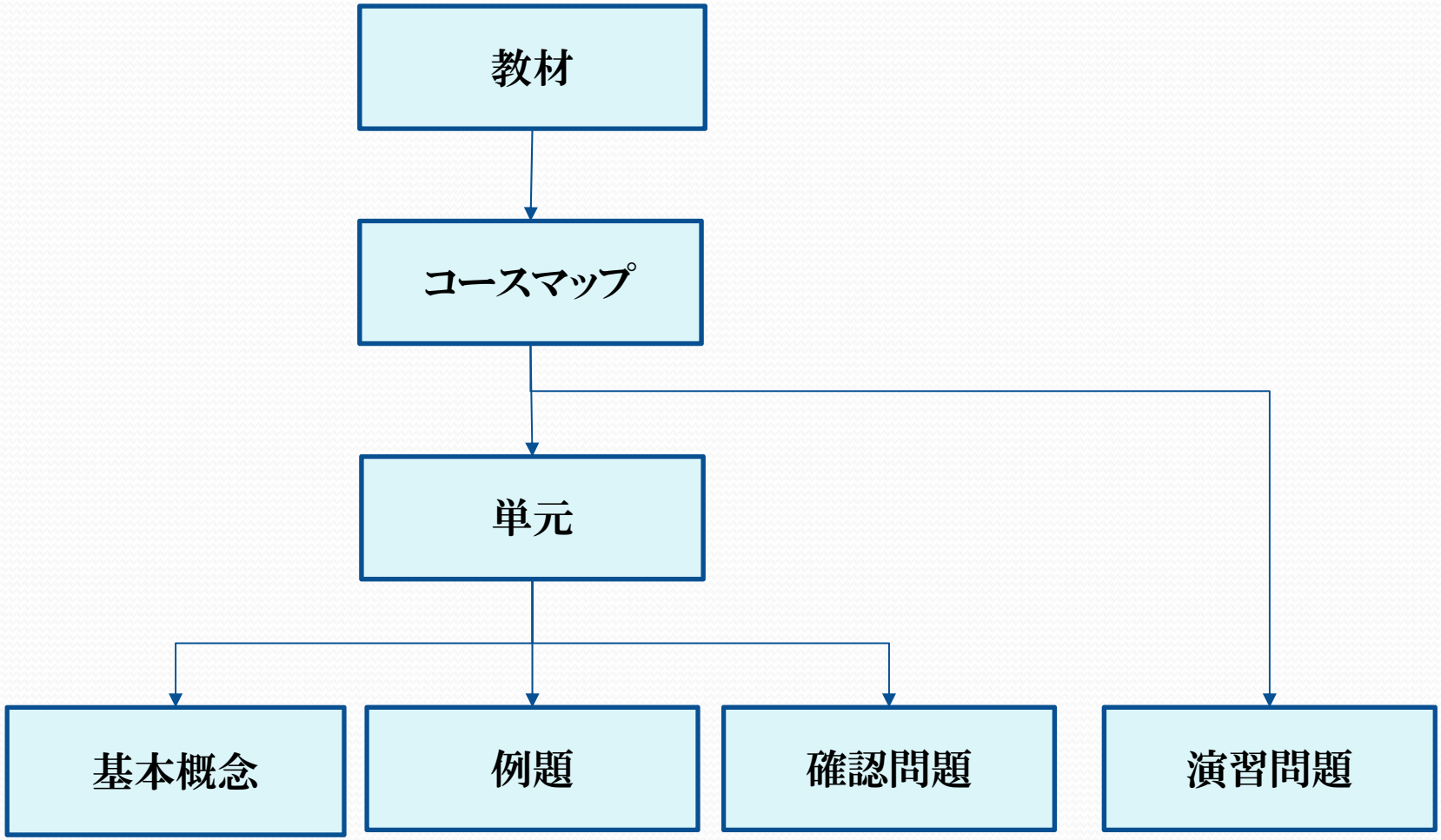
保証ケースに対する統一的な保証ケース作成手法、保証ケースレビュ手法などの先進的な手法については、研修教材がない

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

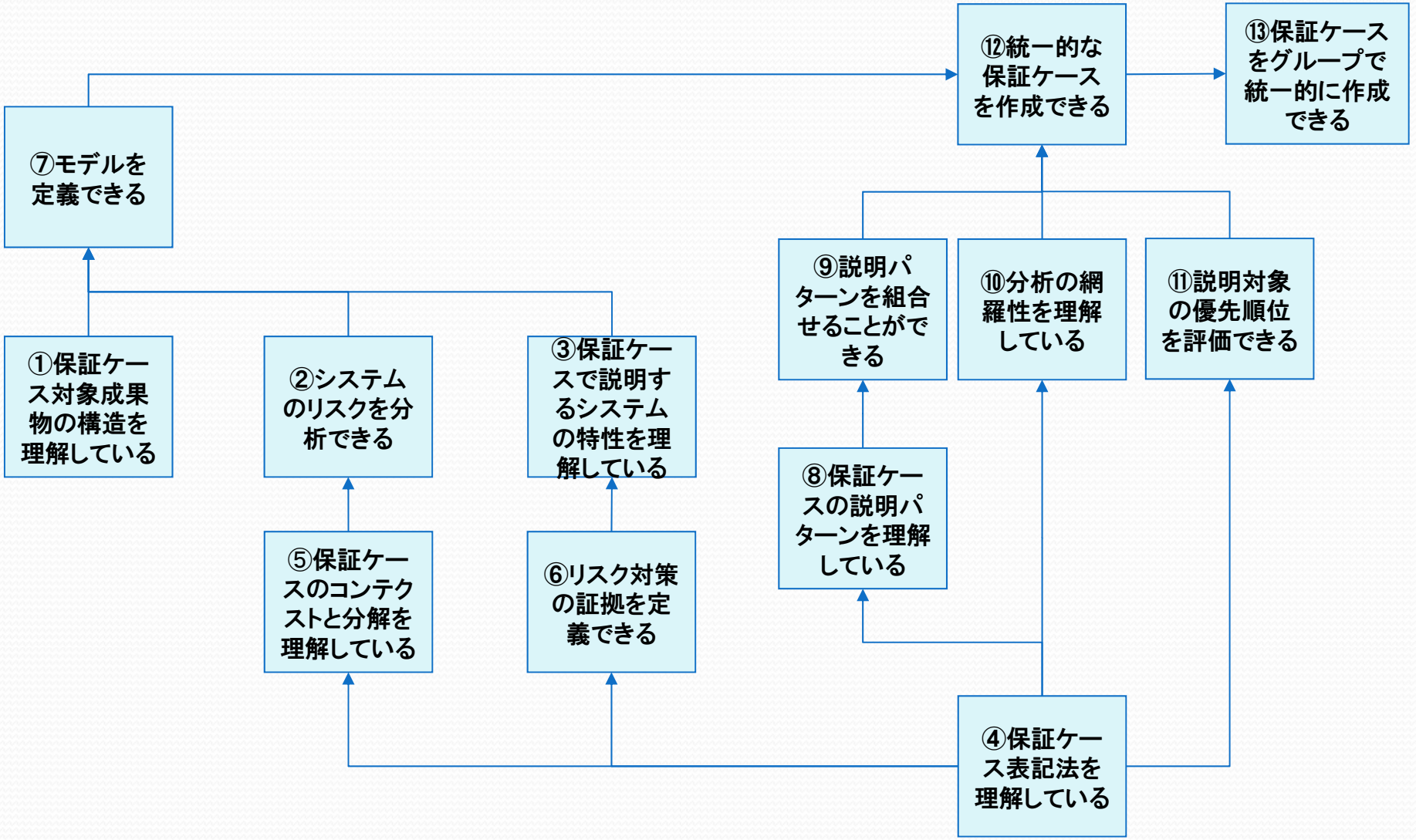
手法研修の開発手順



研修教材の構成



統一的保証ケース作成手法コースマップ



保証ケース統一的作成法カリキュラム

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

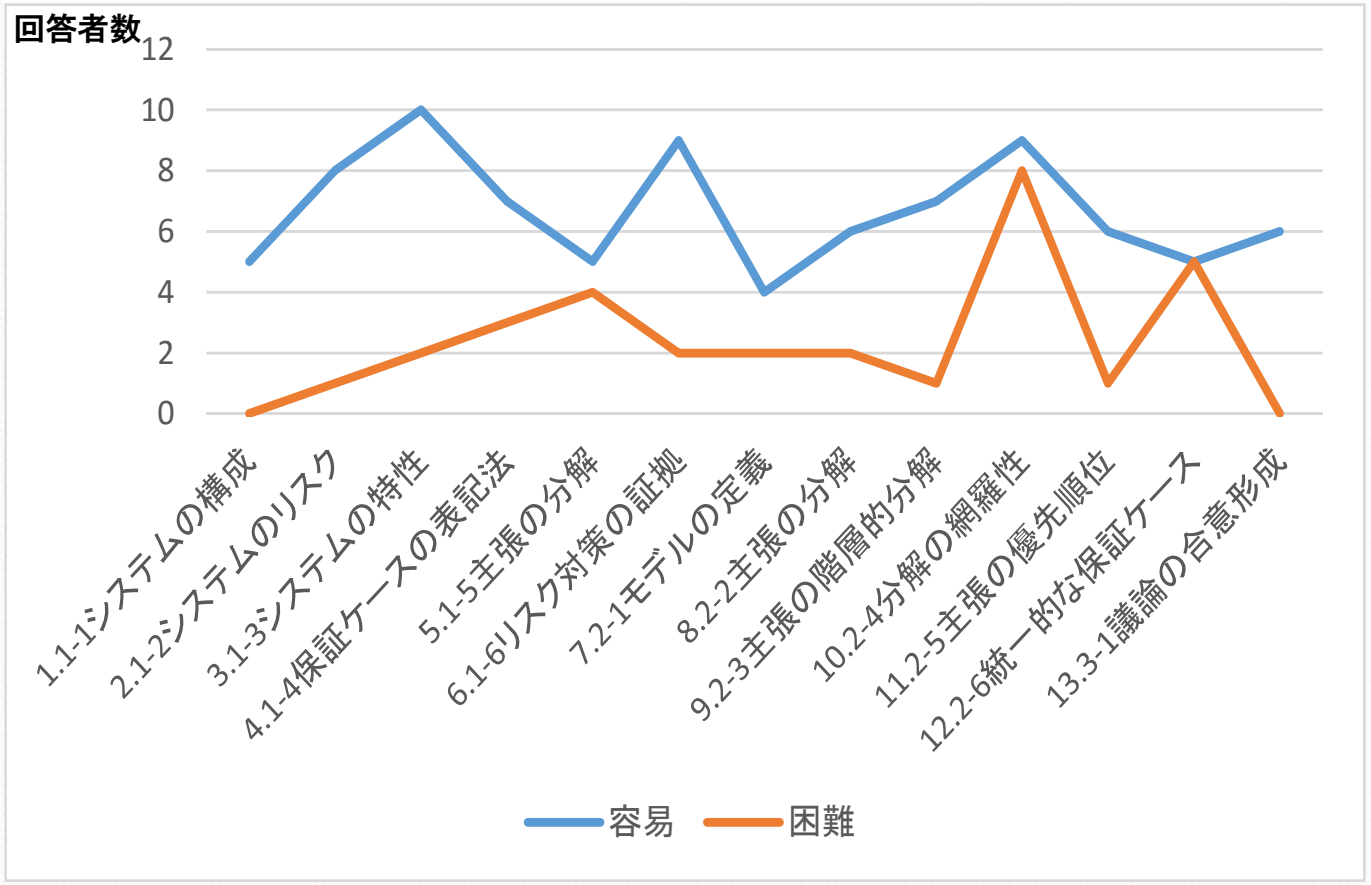
教材スライド：114枚

統一的作成法教材　研修結果

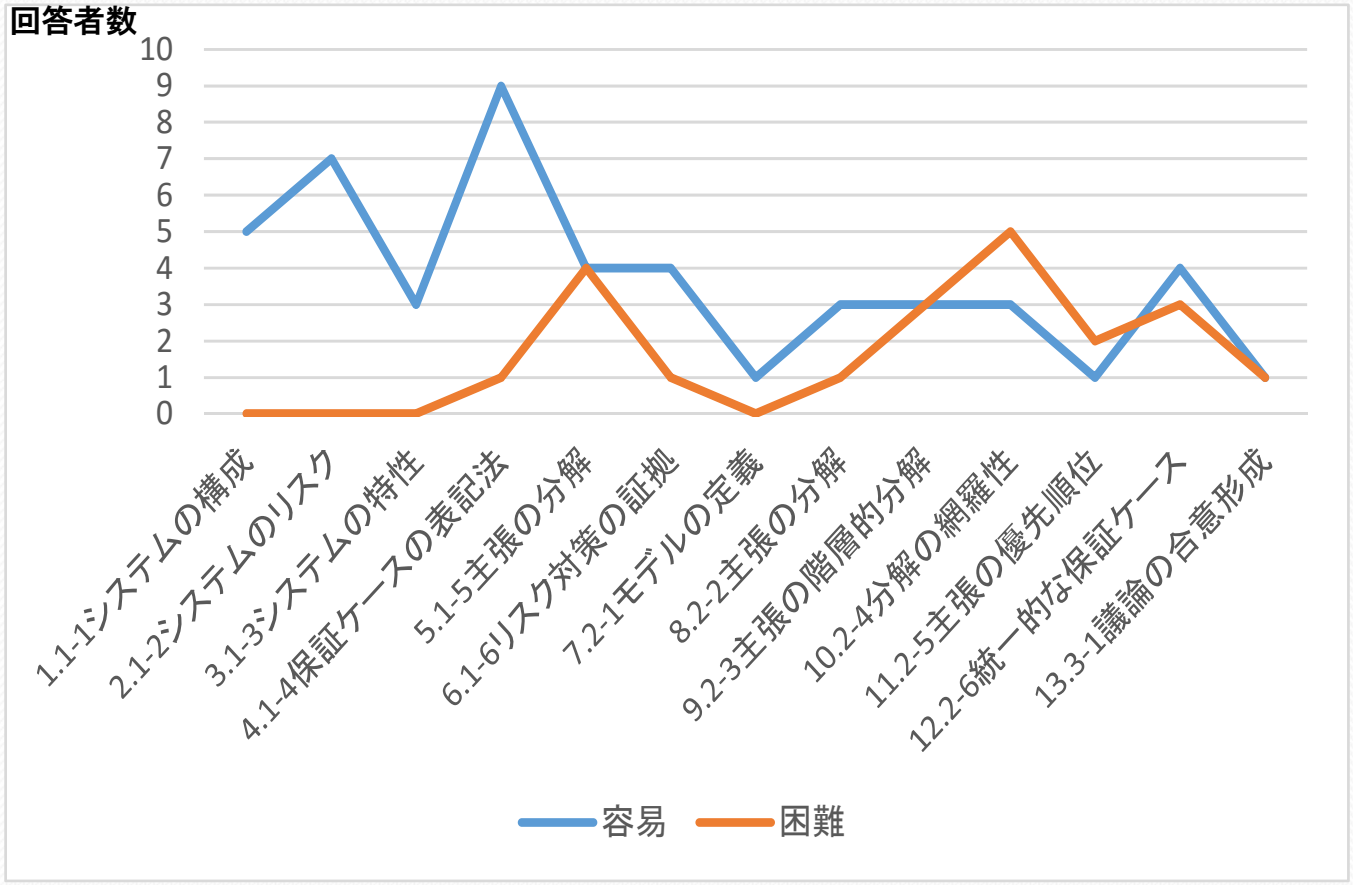
	第1回	第2回
研修参加者(経験者数)	24名(3)	22名(0)
満足度(注1)	95.8%	95.5%
理解度(注1)	100%	81.8%
活用度(注1)	95.8%	86.4%
研修時間十分性(注2)	100%	57.9%
難易度(注3)	100%	72.2%
演習満足度(注1)	72.7%	81.8%
演習時間十分性(注2)	95%	73.7%
教材充足性(注1)	88.2%	77.8%

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

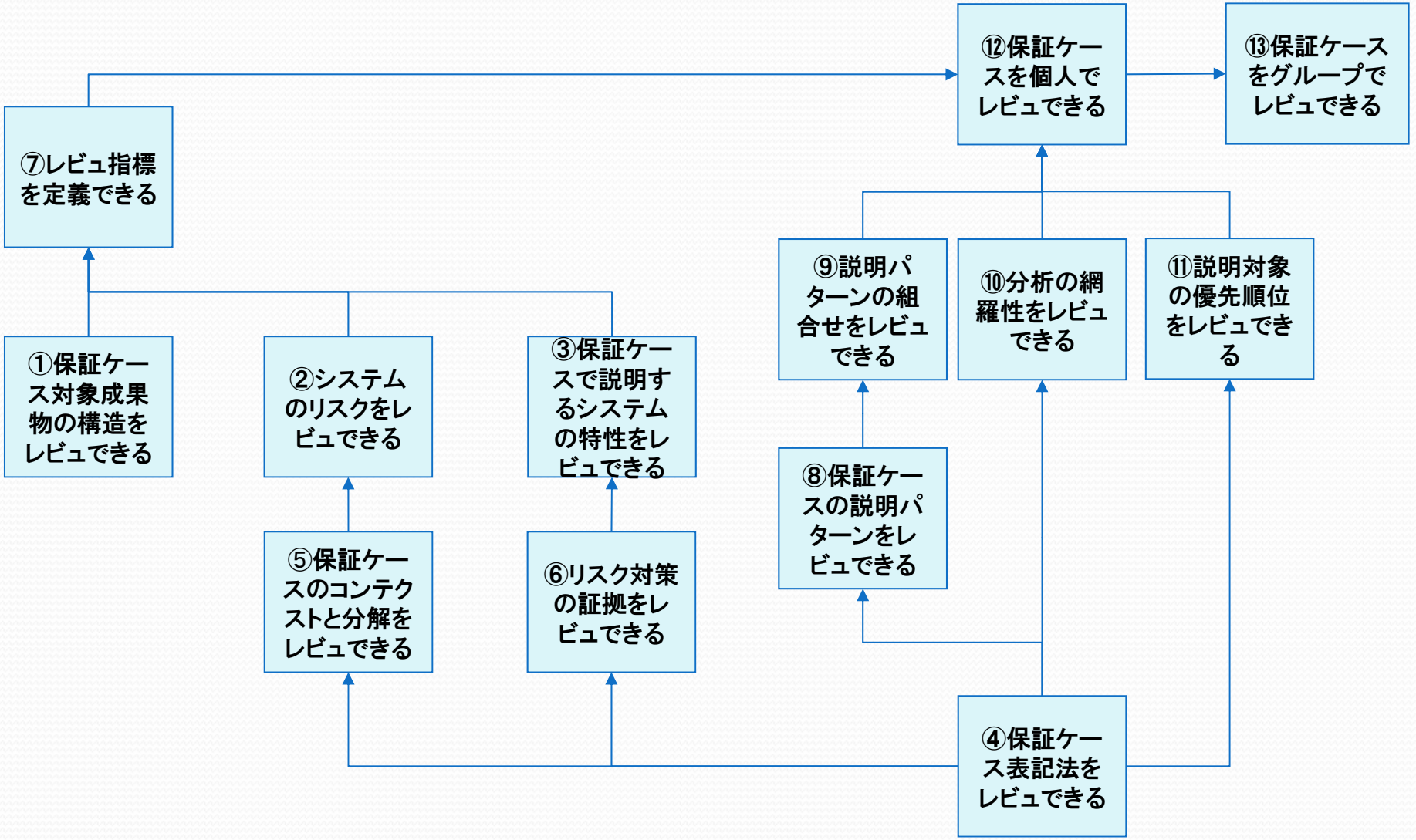
第1回統一的作成法研修の理解度



第2回統一的作成法研修の理解度



保証ケースレビュ手法コースマップ



保証ケースレビュ手法カリキュラム

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

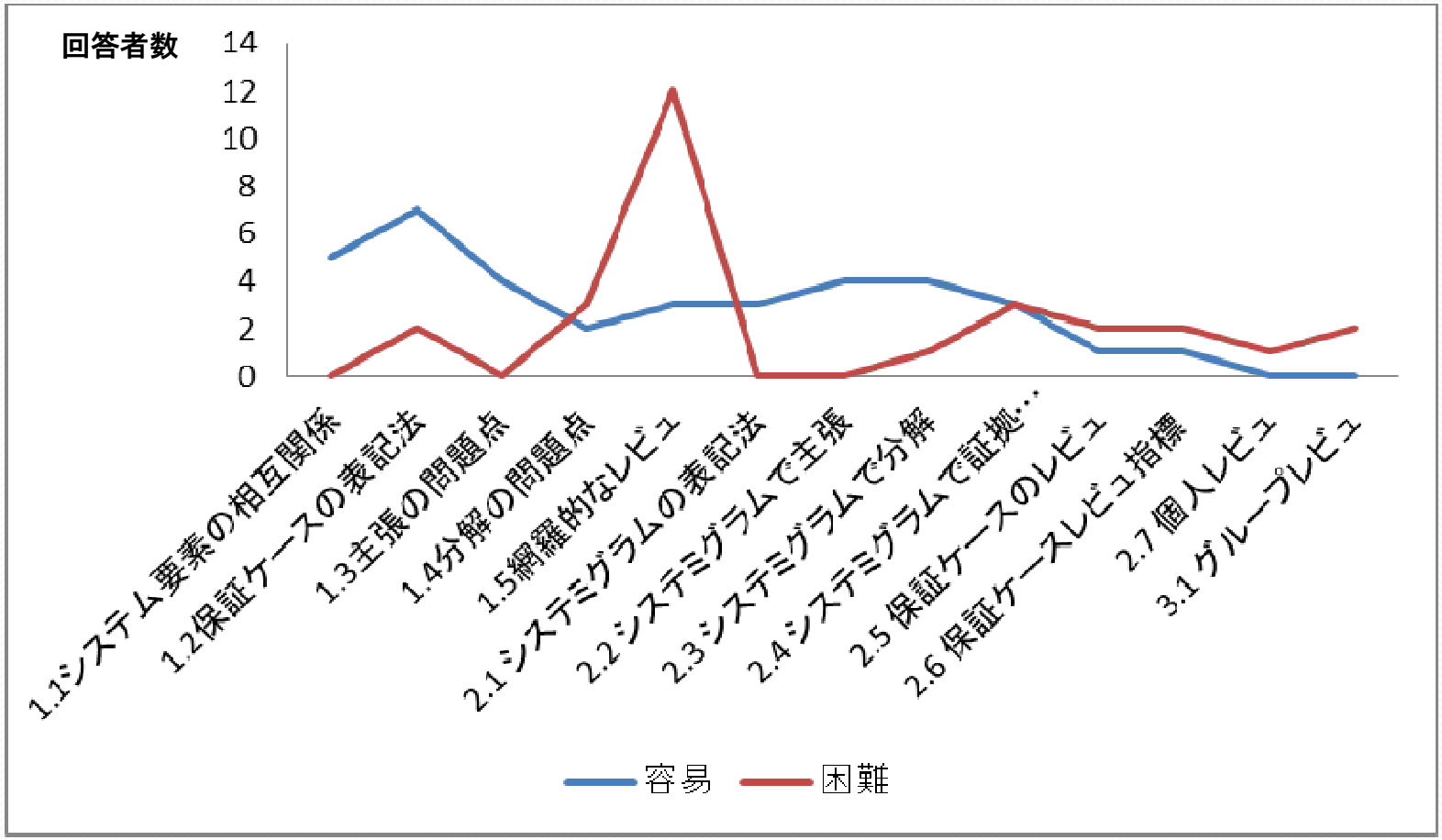
教材スライド：82枚

レビュ手法教材　研修結果

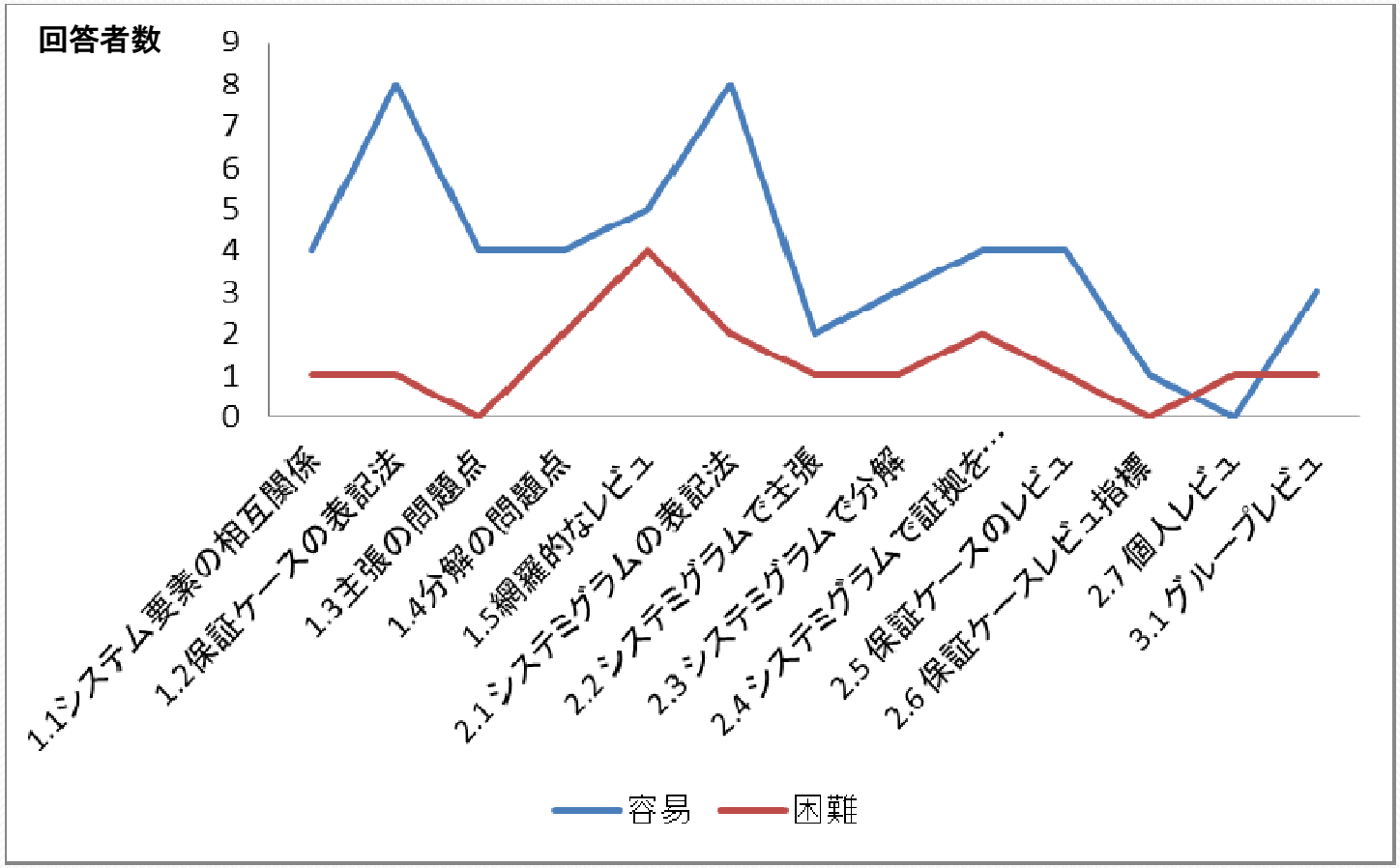
	第1回	第2回
研修参加者(経験者数)	24名(2)	22名(0)
満足度(注1)	95.7%	95.5%
理解度(注1)	100%	81.8%
活用度(注1)	95.7%	86.4%
研修時間十分性(注2)	59.1%	57.9%
難易度(注3)	77.3%	72.2%
演習満足度(注1)	76.9%	81.8%
演習時間十分性(注2)	72.7%	73.7%
教材充足性(注1)	100%	77.8%

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

第1回レビュ手法研修の理解度



第2回レビュ手法研修の理解度



研修教材の規模

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

注）スライド数

研修参加者の経験人年数

- 参加者数　合計　93名
- 平均経験年数　　7.2年

- 総経験人年数　668.9　経験人年

- 経験1年の160名が研修に参加した場合　160経験人年
- 経験4年の160名が研修に参加した場合　640経験人年

- 十分な経験人年数によって、研修教材の適切性が評価できた(668.9>640)

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。

名古屋大学

保証ケース導入準備能力評価指標

研究の目的と課題

【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とその導入について、現場ニーズとの適合性を評価する。

【課題】

現場組織に保証ケースを導入する場合、客観的な組織能力の評価指標が明確ではないため、属人的な能力評価になりやすいという問題があった。

また、保証ケースに関する組織能力の構成次元が明確ではないという問題があった。

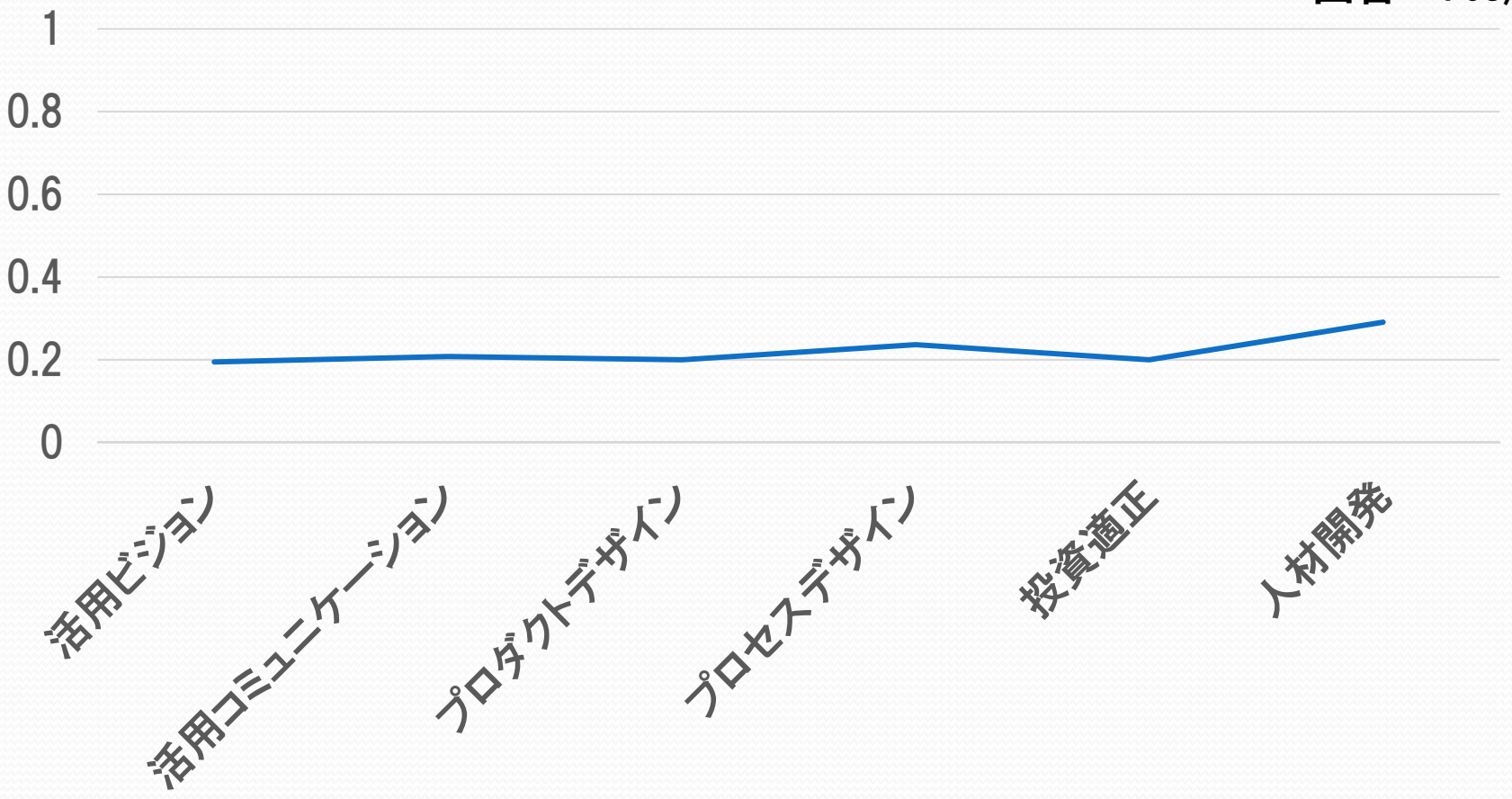
名古屋大学

保証ケース導入準備能力評価指標37

能力	評価指標
保証ケース構築 (3)	①保証ケースの基礎 ②保証ケースの必要性 ③保証の効果
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ケースを定義 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開発プロセスを可視化 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資産の経費を把握 ②AC導入経費対効果を事前検証 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

導入能力準備評価指標の測定例(平均)

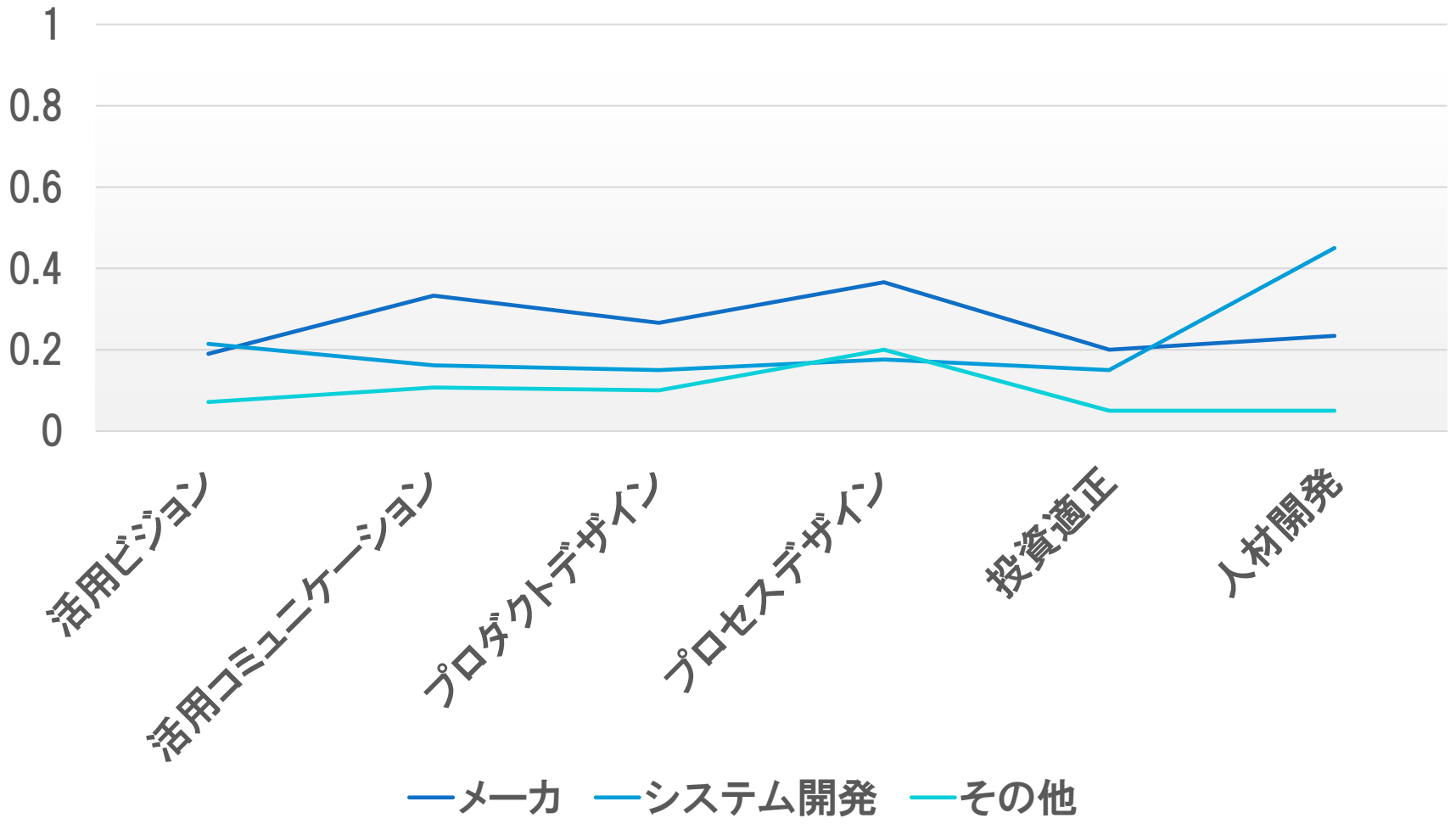
回答数:18
回答: Yes/No



名古屋大学

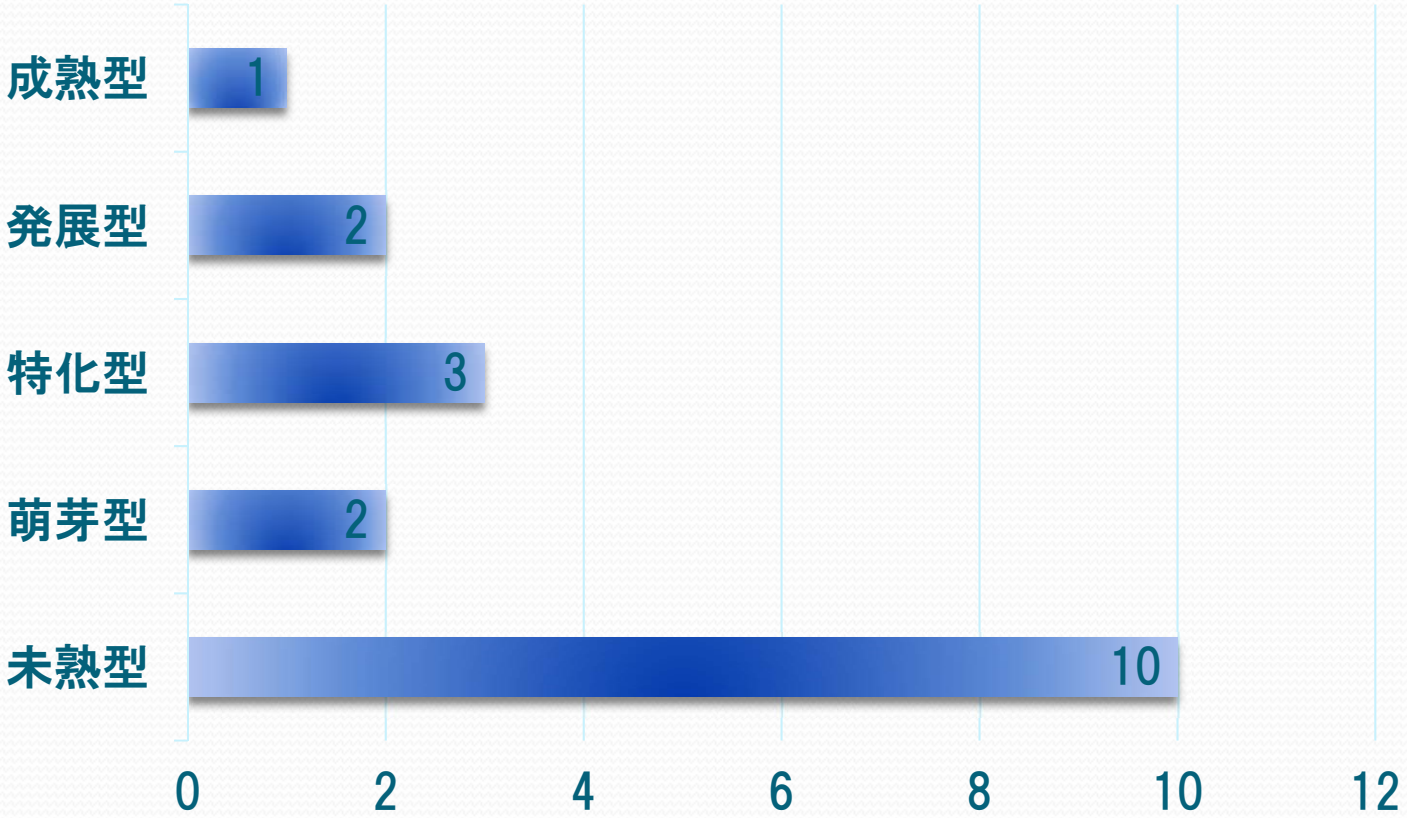
導入能力準備評価指標の業種別測定例

回答数:18
回答: Yes/No



評価結果の類型

回答数:18



評価結果の類型

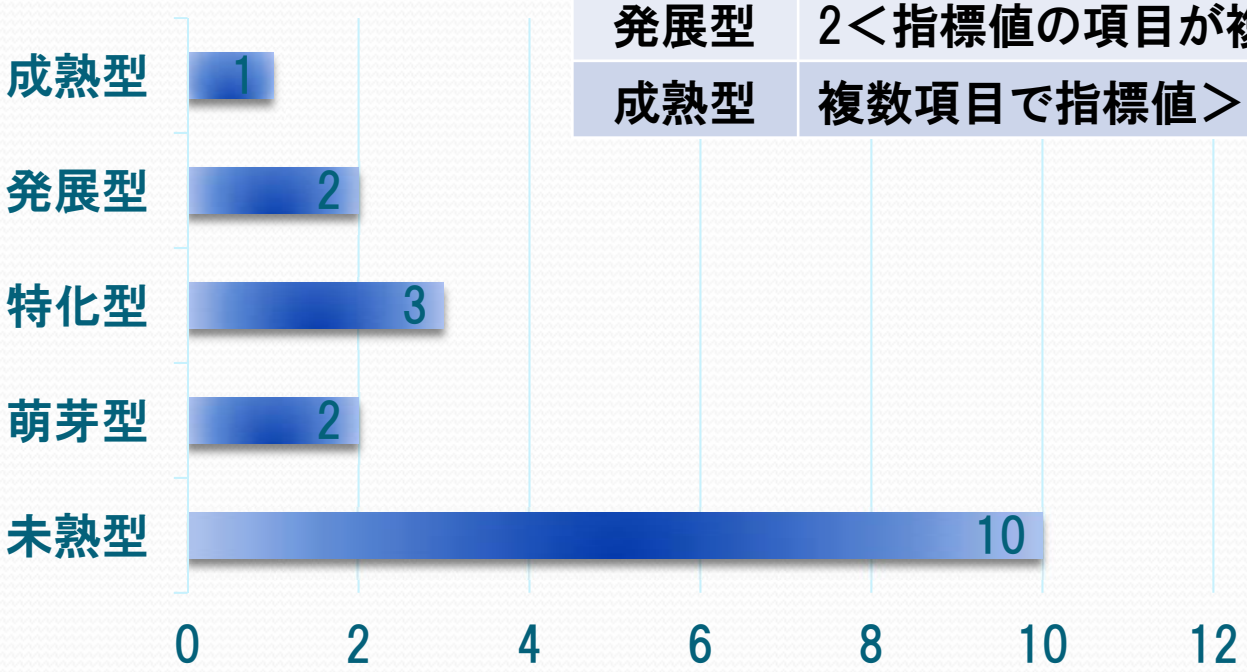
類型	説明	件数
未熟型	各項目の指標値＜3	10
萌芽型	2＜指標値＜4の項目が1つある	2
特化型	4＜指標値となる項目が1つある	3
発展型	2＜指標値の項目が複数ある	2
成熟型	複数項目で指標値＞3	1

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

評価結果の類型

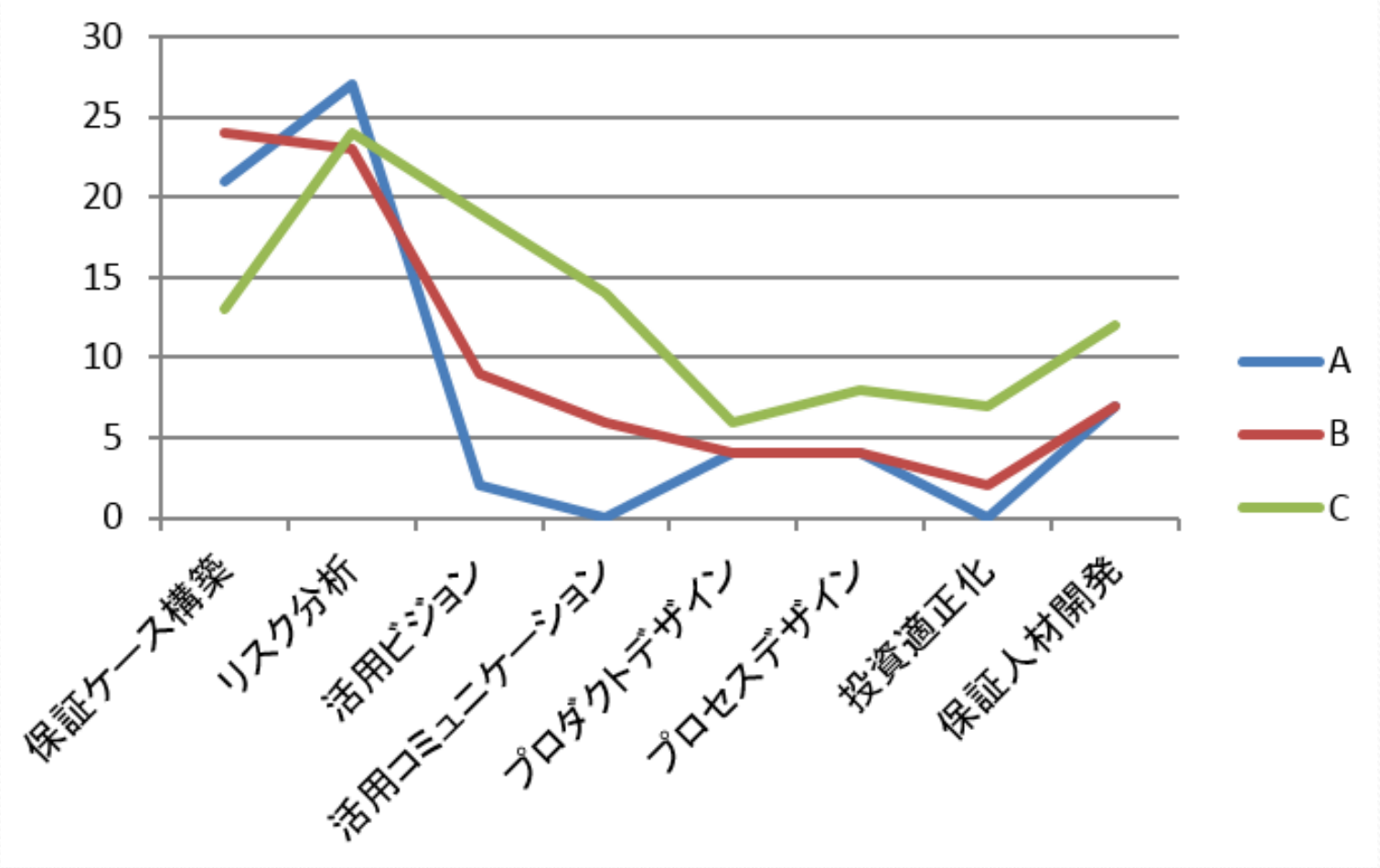
類型	説明	件数
未熟型	各項目の指標値＜3	10
萌芽型	2＜指標値＜4の項目が1つある	2
特化型	4＜指標値となる項目が1つある	3
発展型	2＜指標値の項目が複数ある	2
成熟型	複数項目で指標値＞3	1



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

客観的能力評価例



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。

名古屋大学

研究成果の活用

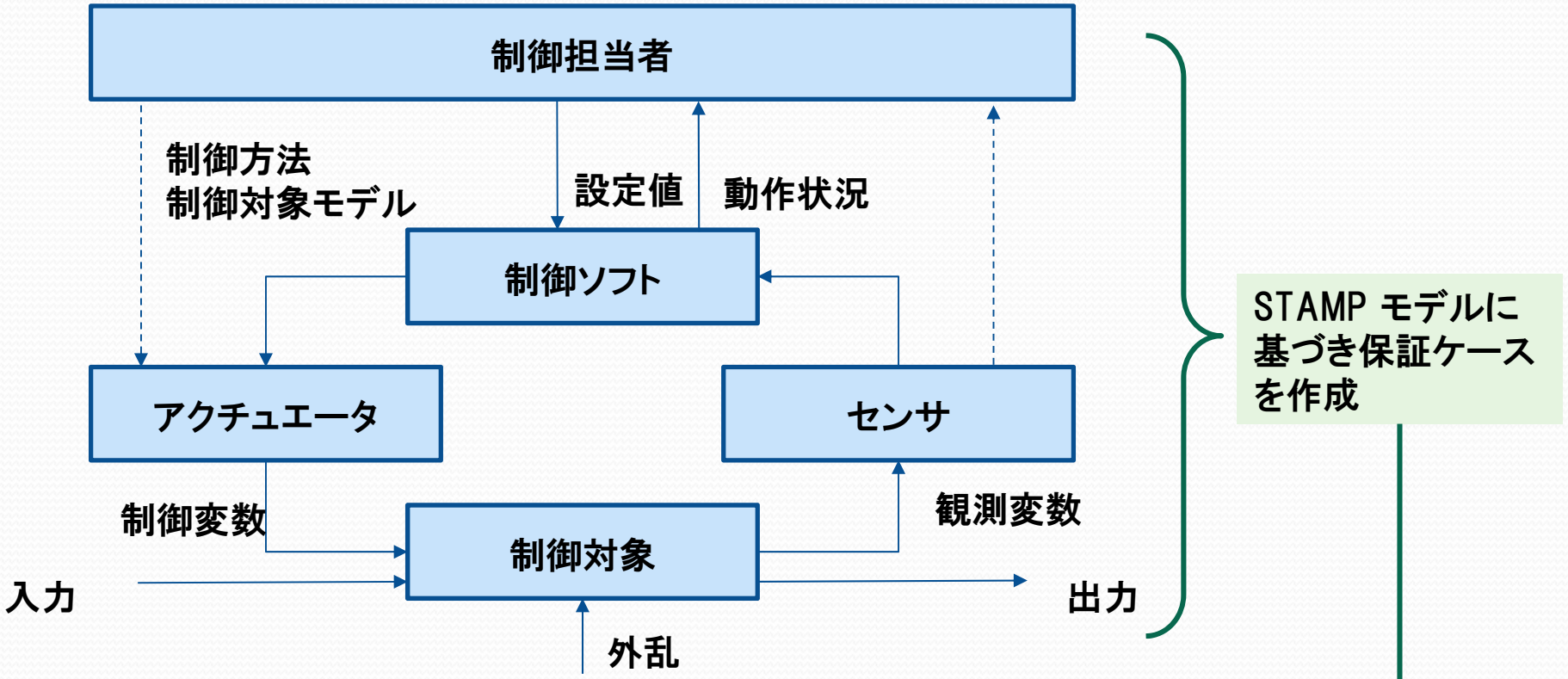
3. 研究成果の活用見込み

	研究成果	成果の活用見込み
1	モデルに基づく保証ケースの統一的作成法	支援ツールを用いた、アーキテクチャ品質評価サービス 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) 品質特性・リスク対策知識の獲得・標準化 O-DA拡張として標準化(TOG) 論文化・ツールの公開
2	コードに基づく保証ケース作成法	系統的コードレビュ手法、設計レビュ手法 形式手法(event-B)との統合化 連携サービス品質保証方法(例:クラウド連携サービス) 論文化
3	保証ケースレビュ手法	SPRME(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、統一的作成法との統合、ツール化、保証ケースの全体理解手法、論文化
4	開発技術者向け教育研修教材を作成	保証ケース活用教材として認証(DEOS協会) 論文化・教材の公開
5	保証ケース導入準備能力評価指標	指標を用いた保証ケース導入法 形式手法、要求工学などの導入能力評価手法への展開 アーキテクチャ品質評価サービスの設計 論文化、指標の公開

注)下線部分:活用組織が決定

階層的制御ループの逸脱対策に基づく保証対象例

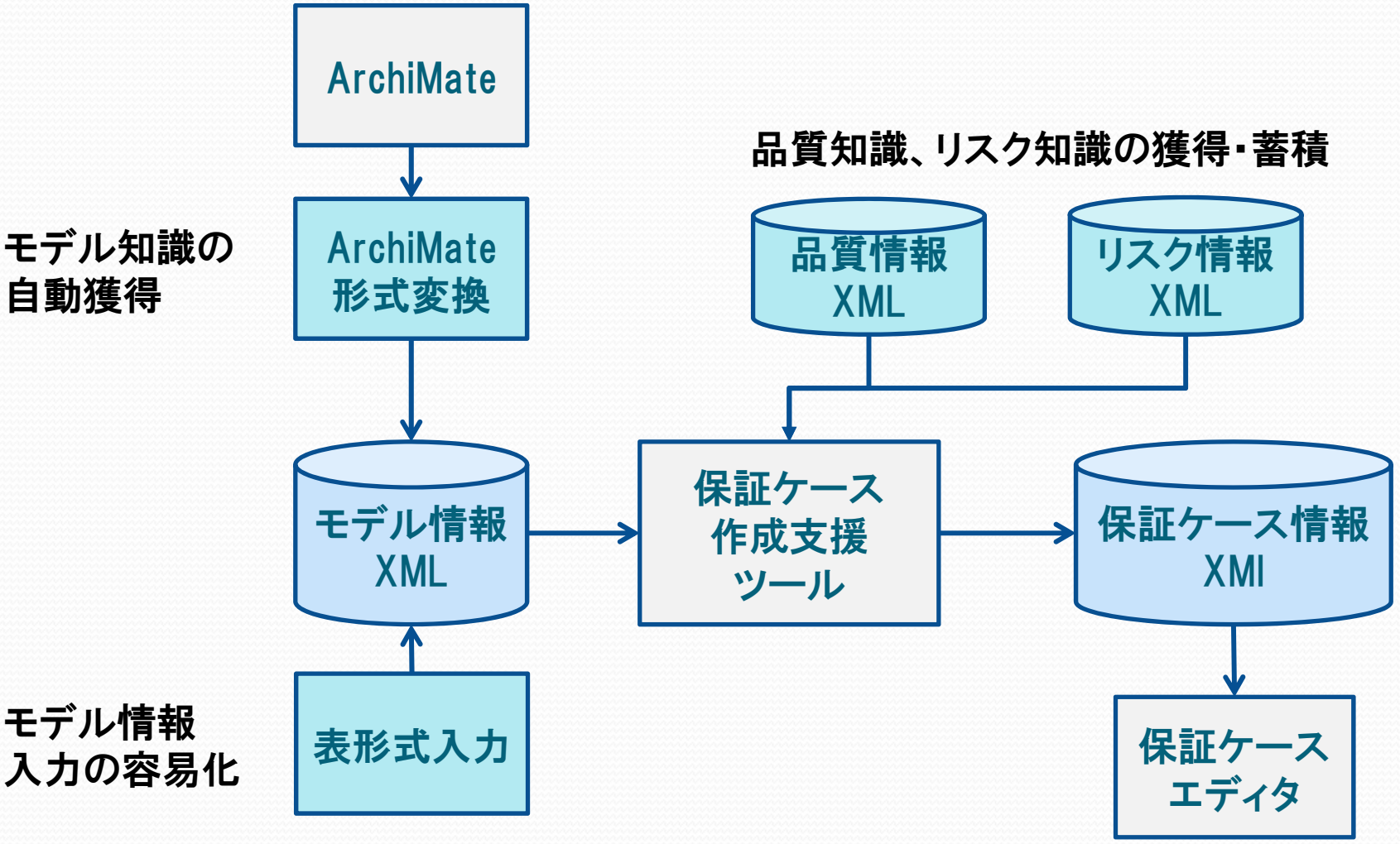
STAMP (Systems-Theoretic Accident Modeling and Processes)
目的条件、活動条件、モデル条件、観測条件の逸脱



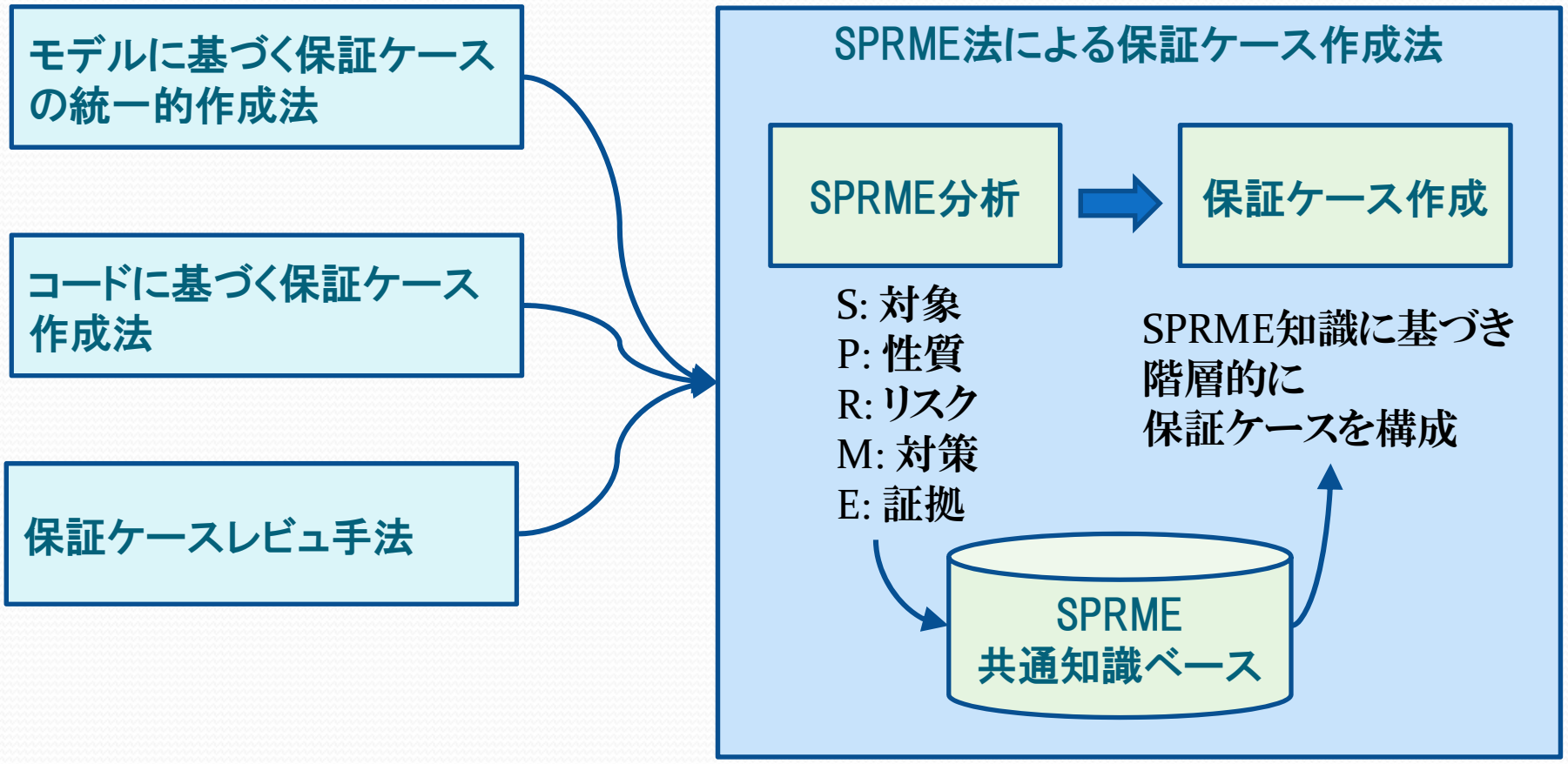
STAMPの階層的制御ループに対して、統一的保証ケース作成法によって保証ケースを作成し、逸脱リスクと逸脱対策ならびに対策の証拠を確認

注)STAMP モデルからSTAMP成果物の作成も可能

保証ケース作成支援システムの拡張



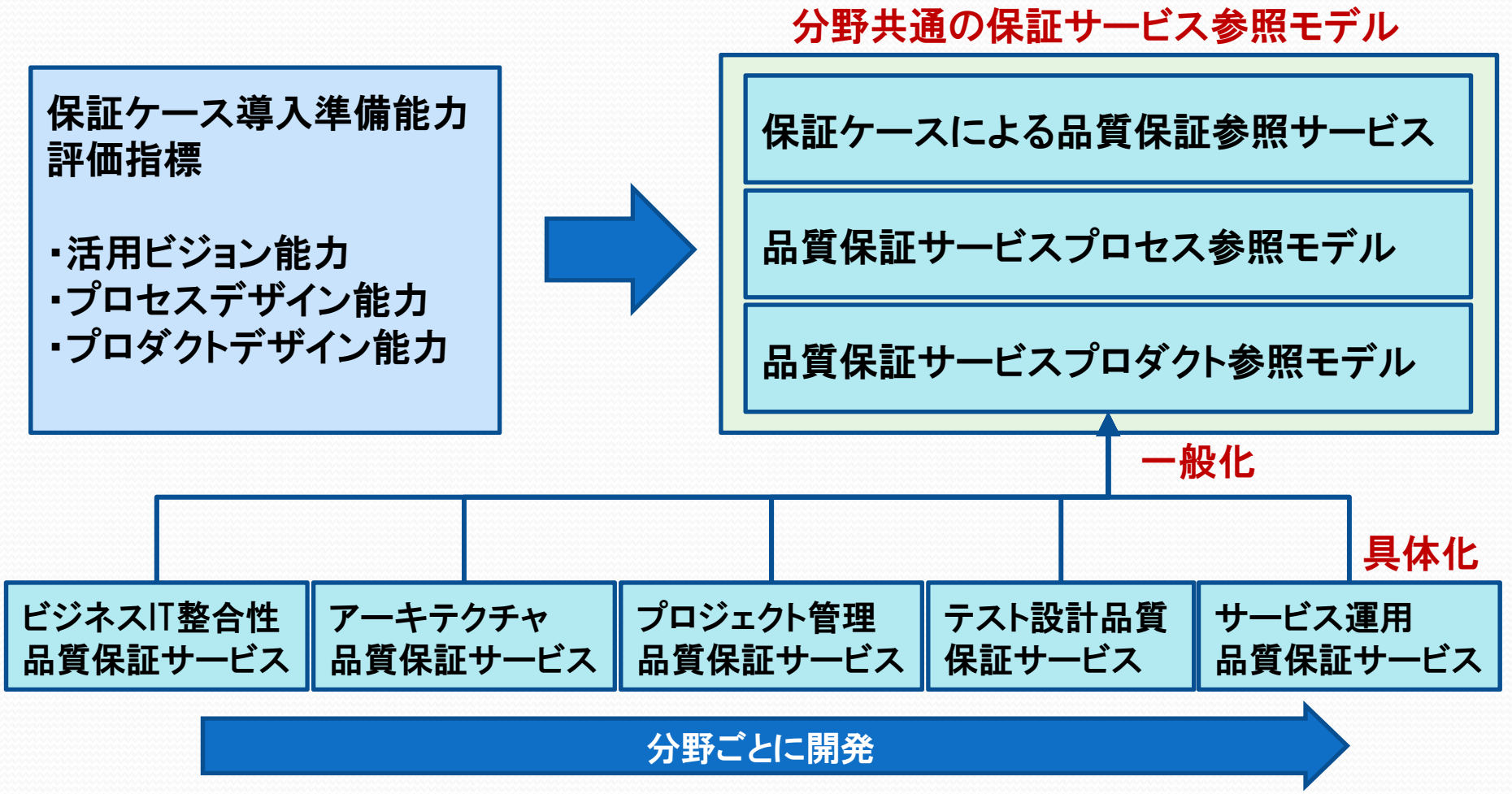
SPRME法による保証ケース作成法の統合



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

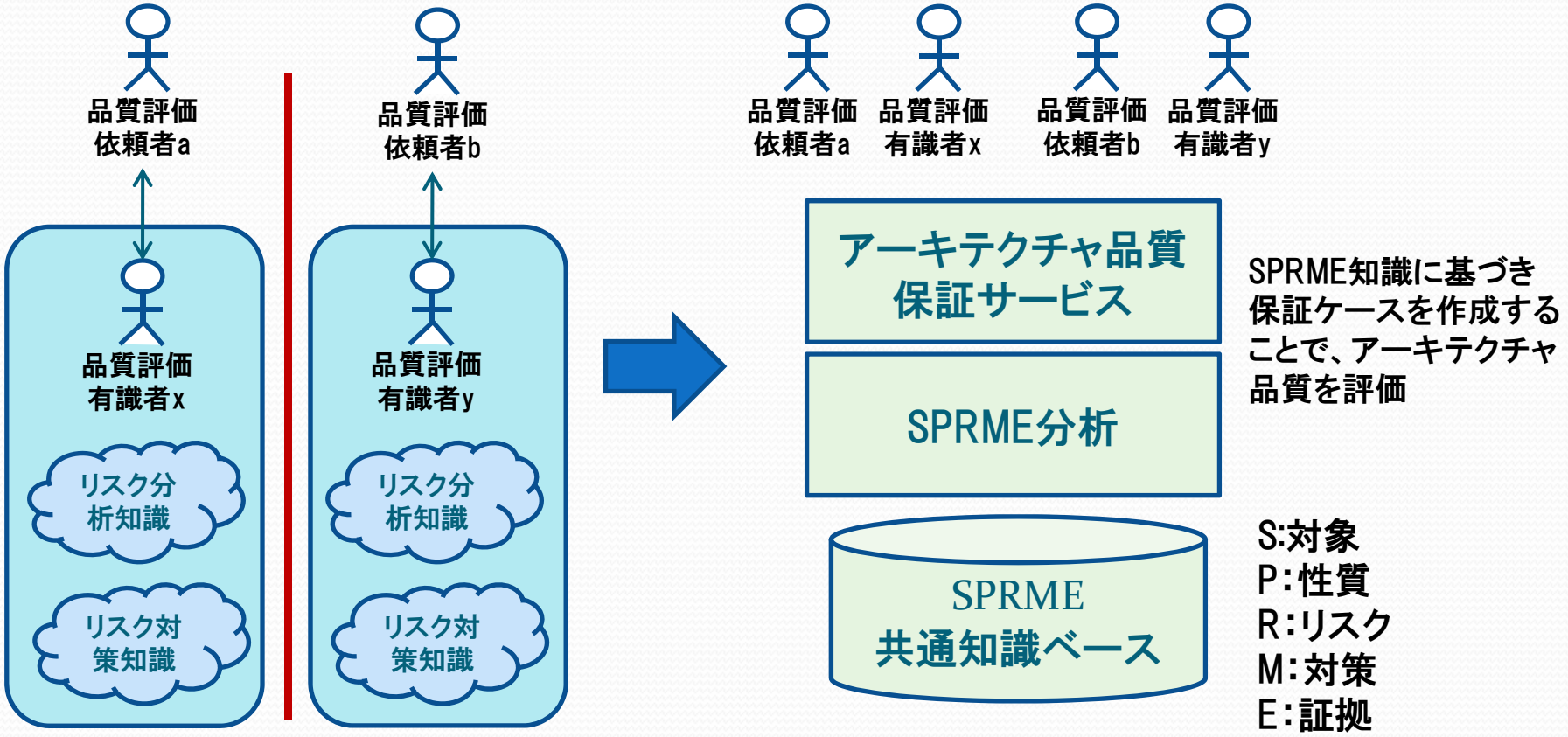
保証ケースによる品質保証サービス工学

評価指標に基づいて参照パッケージ化しておき、適用分野ごとに保証ケースの活用を容易化



アーキテクチャ品質保証サービス

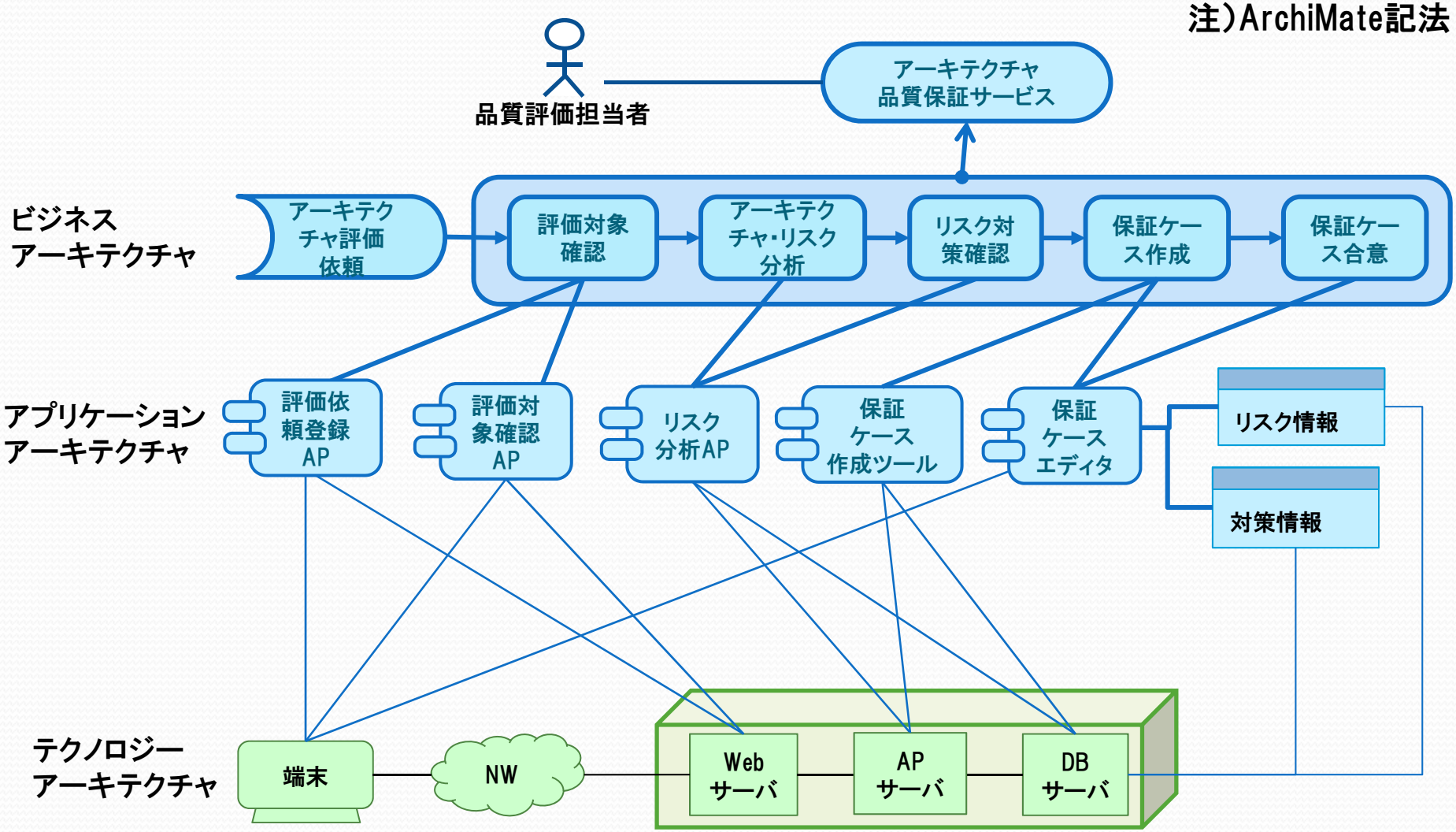
アーキテクチャ品質保証サービスにより、断片的個別的な評価知識を獲得・統合・再利用



有識者ごとに異なる断片的個別的な評価　　アーキテクチャ評価知識を統合再利用

アーキテクチャ品質保証サービスの例

注）ArchiMate記法



技術導入準備能力評価指標への展開例

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

名古屋大学

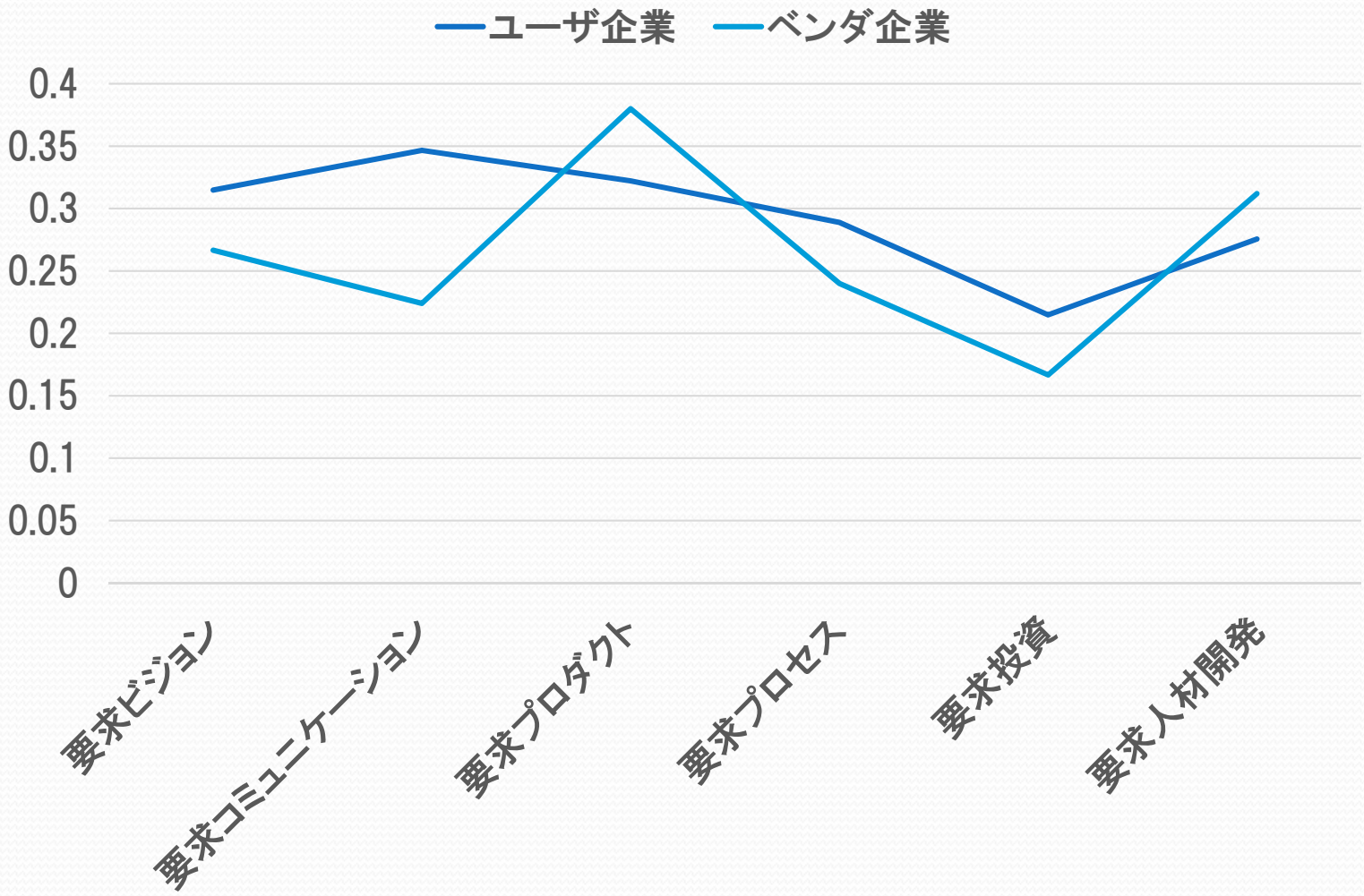
「形式手法」導入準備能力評価指標への展開例

能力	評価指標
形式手法知識(5)	①適用対象の定義 ②形式手法の適用根拠の管理 ③形式手法適用限界の認識 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形式手法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
形式手法活用ビジョン構築 (7)	①自社戦略目標と形式手法の役割が明確 ②形式手法が役割を果たすための組織を制度化 ③形式手法投資を重点化 ④開発での形式手法の活用方針を明確化 ⑤形式手法提供部門の役割が明確 ⑥形式手法提供部門と開発部門の役割が明確 ⑦形式手法に基づく開発部門の結果責任が明確
形式手法活用コミュニケーション (7)	①形式手法の役割を社員が共有 ②形式手法の活用方針を社員が共有 ③形式手法導入目的を開発部門が理解 ④形式手法導入後の業務変化を開発部門が理解 ⑤部門間で形式手法による問題解決プロセスが定義 ⑥形式手法活用事例を社内で共有する仕組みを定義 ⑦経営層、形式手法部門、開発部門の3部門間で、形式手法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形式手法の適用条件を定義 ③成果物に対する形式手法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形式手法を標準化 ⑤成果物に対する重複のない形式手法の適用を定義
プロセスデザイン (5)	①開発プロセスへの形式手法導入計画を定義 ②形式手法による開発プロセスを定義 ③開発プロセスの形式手法活用方策を標準化 ④社内外の業務連携プロセスを形式手法で標準化 ⑤形式手法の重複のない開発プロセスを実現
形式手法投資適正化 (6)	①形式手法資産の構築経費を配分 ②形式手法部門の独立性を考慮 ③形式手法導入経費対効果を事前に検証 ④形式手法導入時に全社最適への適合性を検討 ⑤形式手法導入後に活用状況・効果を測定 ⑥形式手法活用問題を形式手法導入検討時に解決
形式手法人材開発 (5)	①形式手法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形式手法の双方に精通した人材を配置 ③形式手法人材が経営に関する知識を習得する機会を提供 ④形式手法人材が現場の開発プロセスを理解する機会を提供 ⑤開発人材に形式手法の活用スキル研修を提供

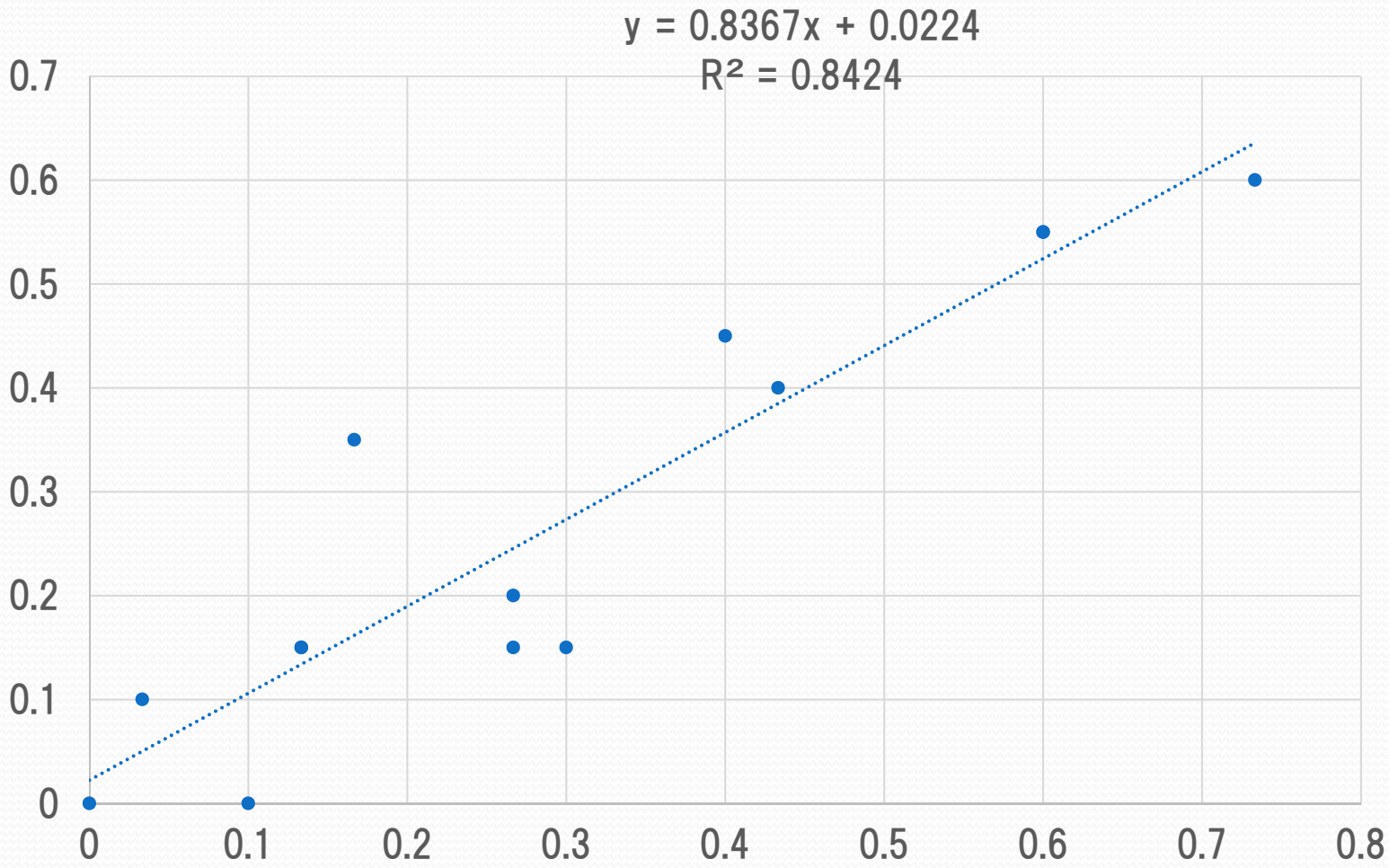
要求仕様化能力評価指標30

能力	評価指標
要求ビジョン構築 (6)	①自社戦略目標と要求定義の役割が明確 ②要求定義が役割を果たすための組織を構築 ③要求投資を重点化 ④開発での要求の活用方針を明確化 ⑤要求定義部門の役割が明確 ⑥要求に基づく開発部門の結果責任が明確
要求コミュニケーション (6)	①要求定義の役割を社員が共有 ②要求定義の目的を開発部門が理解 ③要求による問題解決プロセスを部門横断的に定義 ④要求定義事例を社内共有する仕組みを定義 ⑤経営層、要求定義部門、開発部門間で、要求の投資対効果を共有
要求プロダクト　デザイン(4)	①要求成果物に対する目標品質を定義 ②要求成果物の活用方策を標準化 ③社内外開発連携観点で要求成果物を標準化 ④要求成果物の重複のない記述項目を定義
要求プロセス　デザイン (4)	①要求開発プロセスを定義 ②開発プロセスの要求活用方策を標準化 ③社内外の要求業務連携プロセスを標準化 ④重複のない要求開発プロセスを実現
要求投資適正化(6)	①要求資産の構築経費を配分 ②要求部門の独立性を考慮 ③要求定義の経費対効果を事前に検証 ④要求定義時に全社最適への適合性を検討 ⑤要求定義後に活用状況・効果を測定 ⑥要求活用問題を要求検討時に解決
要求人材開発 (5)	①要求開発プロセス改革の提案人材を育成 ②経営層に開発と要求に精通した人材を配置 ③要求人材が経営知識を習得する機会を提供 ④要求人材が開発プロセスの理解機会を提供 ⑤開発人材に要求の活用スキル研修を提供

要求仕様化能力の評価例



要求ビジョンと要求プロセス



名古屋大学

得られた知見

当初の想定成果、活用方法、活用分野との相違

当初想定

個別的活用
専門的活用
成果物の保証
知識の保証系

今後の研究の進め方

横断的活用
非専門的活用
保証成果物の要件定義
保証知識の流通系

- 表形式による保証ケース情報の定式化
- SPRME知識の標準化
- SPRME法による統一作成法、コード保証法、レビュ手法の統合
- 保証ケース導入準備能力評価指標のサービス化
- 品質保証サービスエンジニアリング

今後の課題

- これまで、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
- 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統合したパターンになっている

提言

- 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。
- 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、保証ケースを活用した典型的な「システム品質保証サービス」を設計する
- これにより、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の研究が必要
- このようなサービスを利用すれば、多くの企業では、自ら保証ケースについて高度な導入準備能力を獲得することなく、保証ケースの価値を享受できる可能性がある。

名古屋大学

まとめ

- 保証ケース作成支援方式
- 主な研究成果
- 有効性
- 保証ケース作成のサービス化に向けた提言

名古屋大学

謝辞

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