統一的保証ケース

～ 保証ケースを使った合意形成について ～

研修の目的

目的

保証ケースを統一的に作成するために必要となる知識
及び それを説明できるスキルを身につける。
演習を通じて、受講者同士でディスカッションし、情報共有する。

◆ 習得するスキル

- 保証ケースの前提条件を分析するスキルを習得する。
- 保証ケースの表記法を理解し、基本的な作成スキルを習得する。
- 保証ケースのパターンに基づく統一的な作成手順を習得する。

研修カリキュラム

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

目次

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

1.1 システムの構成

目的

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。

◆ **習得するスキル**

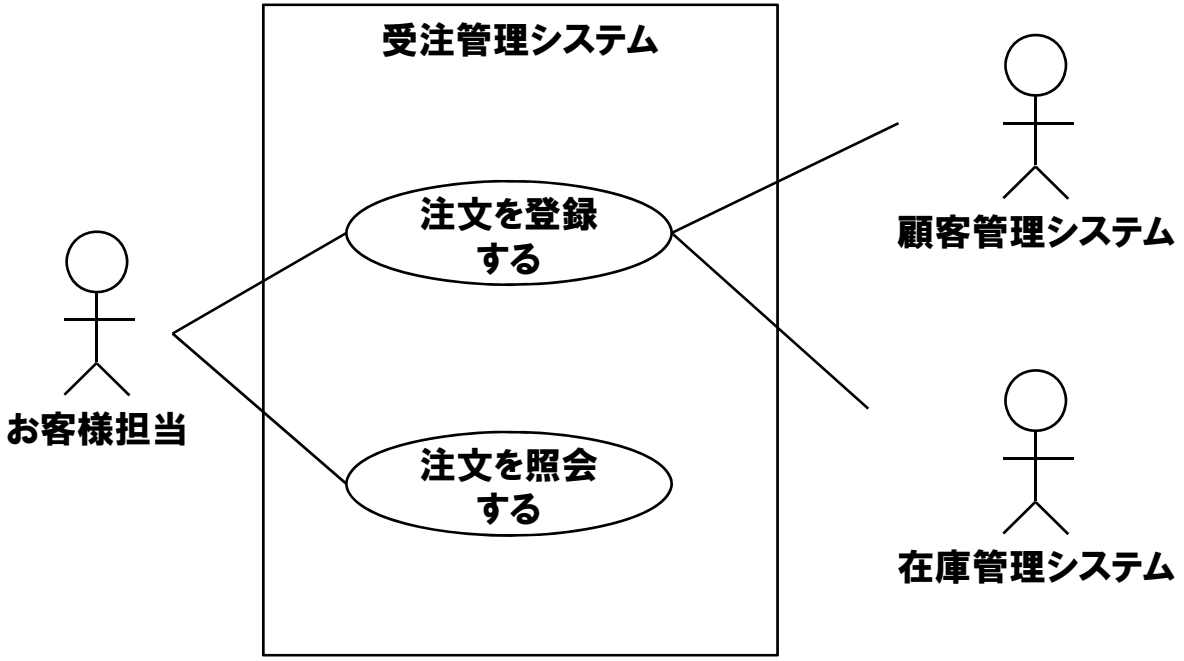
- **システムの構成としてユースケース図の構成について理解する。**

1.1　システムの構成

保証ケースで保証しようとする対象システムの構成として、本研修ではユースケース図について説明します。

ユースケース図とはUMLで定義されている図のうちの1つで、システムで実現する機能を明確にします。またシステムを使用するユーザや外部システムについても記述します。

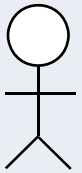
図1　ユースケース図の記述例



1.1　システムの構成

ユースケース図の要素としては、「アクター」と「ユースケース」があり、それらを結ぶ「関連」があります。保証ケースを作成する場合にはこういった要素と関連を使って定義することとなります。

表1　表記方法

No.	名称	記述例	内容
1	アクター	 お客様担当	システムの利用者や外部システムなどの要素をアクターとして定義します。
2	ユースケース	 注文を登録する	アクターに提供するシステムの機能をユースケースとして定義します。
3	関連		アクターとユースケースの関係を関連として定義します。

1.1 システムの構成

【例題】 問題文を読み、ユースケース図を作成してください。

ホテルYは日本全国でビジネスホテルを中心に設立、運営している会社です。

ホテルYでは宿泊情報を管理している宿泊管理システムがあります。このシステムを利用するにはホテルYの会員である必要があります。

会員である顧客はインターネットから宿泊を登録することができ、登録後は内容を確認することができます。なお、予約・変更・取消についても宿泊当日までインターネットで行うことができますが、当日の宿泊の取消はキャンセル料が100%かかってしまいます。

【記入欄】

【解答例】 1.1　システムの構成

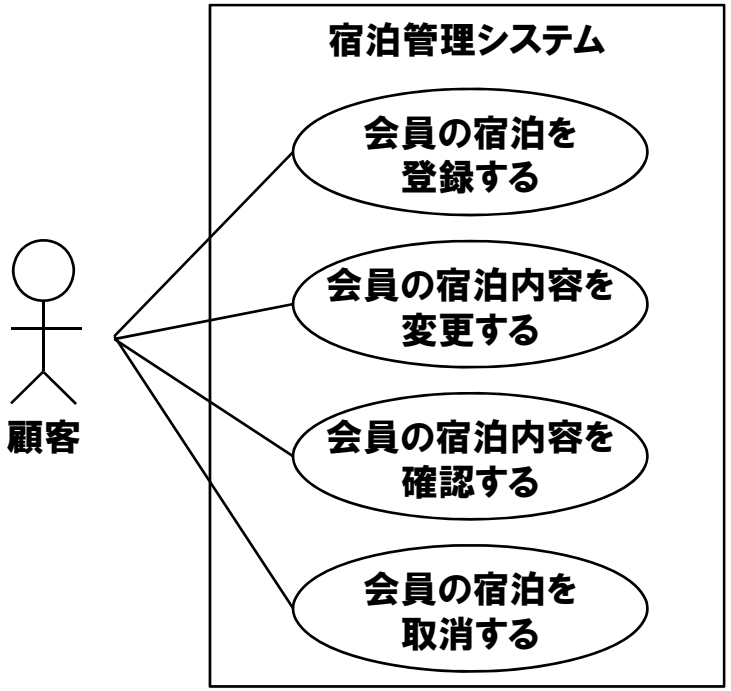
【例題】 問題文を読み、ユースケース図を作成してください。

ホテルYは日本全国でビジネスホテルを中心に設立、運営している会社です。

ホテルYでは宿泊情報を管理している宿泊管理システムがあります。このシステムを利用するにはホテルYの会員である必要があります。

会員である顧客はインターネットから宿泊を登録することができ、登録後は内容を確認することができます。なお、予約・変更・取消についても宿泊当日までインターネットで行うことができますが、当日の宿泊の取消はキャンセル料が100%かかってしまいます。

～解答例～



1.1 システムの構成

【演習】 問題文を読み、ユースケース図を作成してください。

ホテルYは日本全国でビジネスホテルを中心に設立、運営している会社です。

ホテルYでは会員情報を管理している会員管理システムがあります。このシステムは顧客自身がインターネットを利用して会員登録をすることができます。

会員登録をした後は、インターネットから自身の登録した内容の変更や確認を行うことができますが、会員を退会したい場合にはホテルYのオペレータに電話をし、退会したい旨を依頼しないと退会することができません。

また、インターネットを利用できない顧客は、ホテルYのオペレータに電話をすれば自身の代わりに、会員登録、内容の変更や確認を依頼することができます。

【記入欄】

memo

1.2 システムのリスク

目的

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。

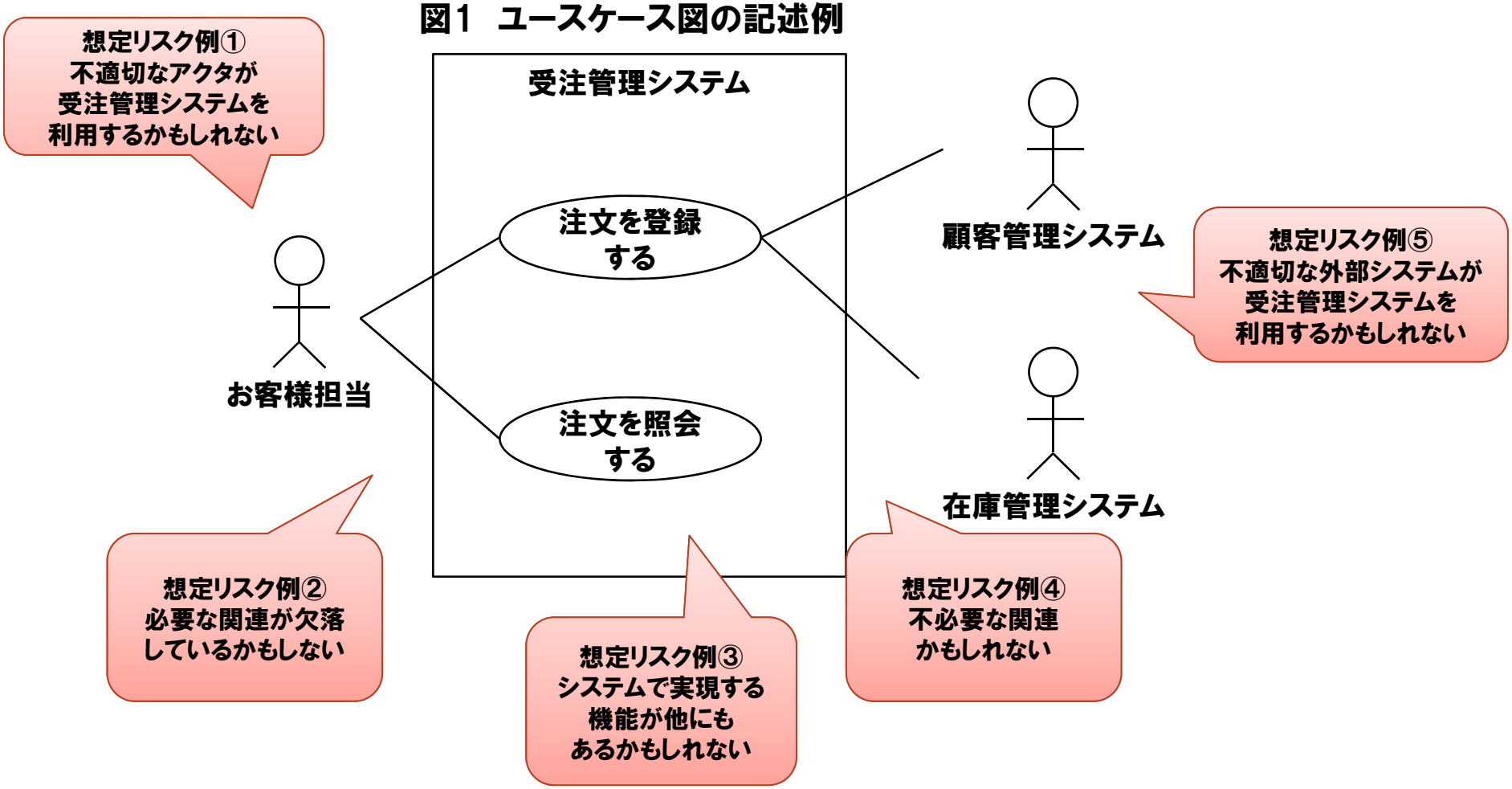
◆ **習得するスキル**

- **成果物として作成したユースケース図のリスクについて分析できるスキルを身につける。**

1.2 システムのリスク

ここではユースケース図を使い、どんなリスクが考えられるかについて考えてみましょう。
まずアクター、外部システム、関連に注目すると・・・以下のようなリスクが想定されます。

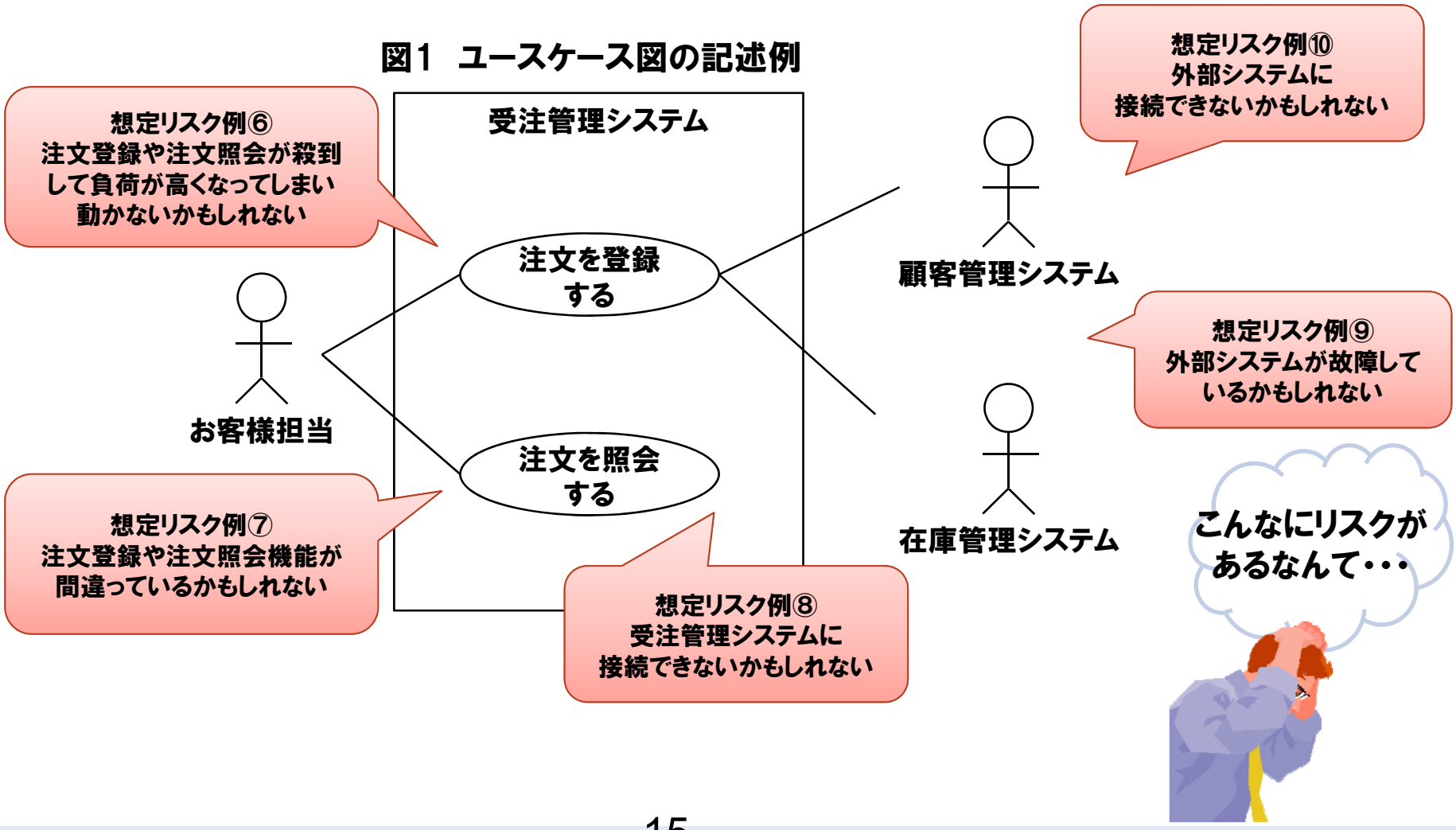
図1 ユースケース図の記述例



1.2 システムのリスク

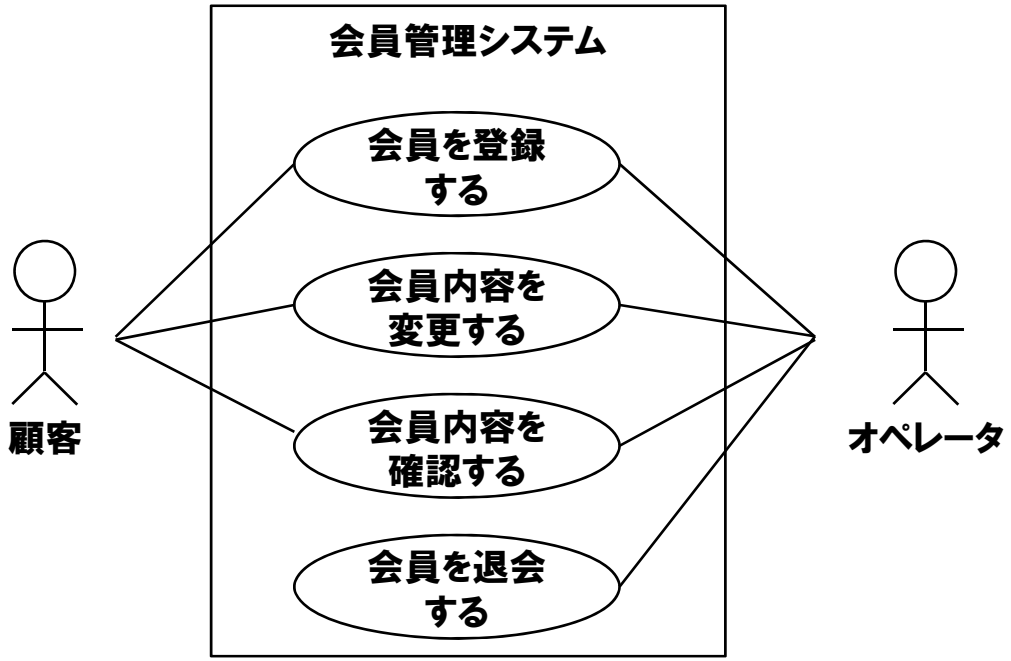
他にも以下のようなリスクが想定されます。
システムのリスク分析は「あらゆる逸脱（前提条件の逸脱、例外条件の逸脱等）」を考える必要があります。

図1 ユースケース図の記述例



1.2 システムのリスク

【例題】
1.1章 演習のユースケース図を例にどんなリスク(逸脱)が考えられるかを考えてみましょう。

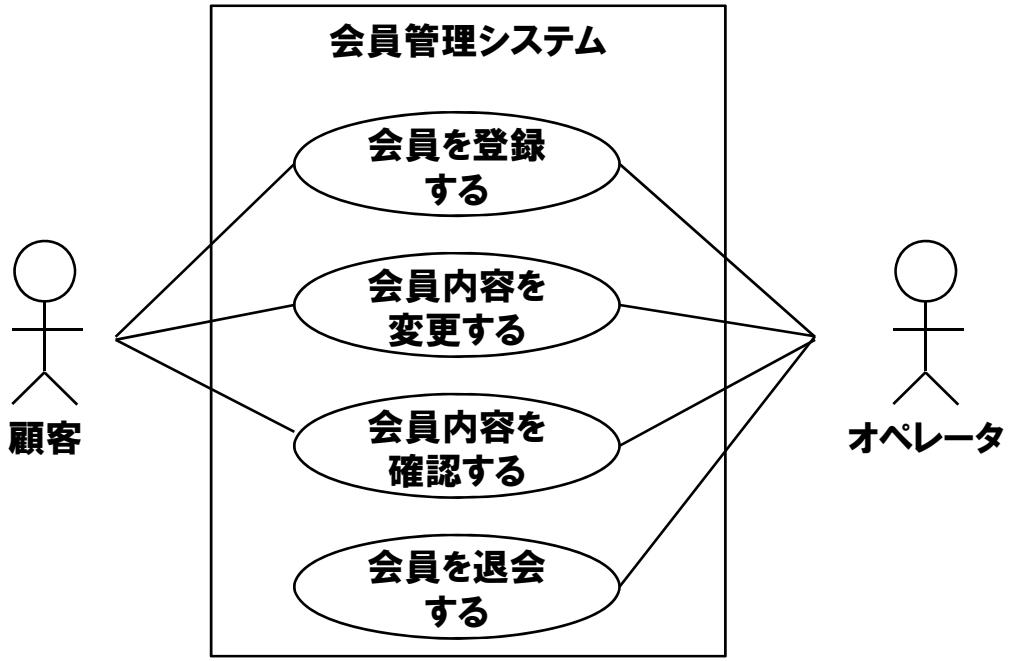


【想定リスク】

【解答例】 1.2 システムのリスク

【例題】
1.1章 演習のユースケース図を例にどんなリスク(逸脱)が考えられるかを考えてみましょう。

～解答例～



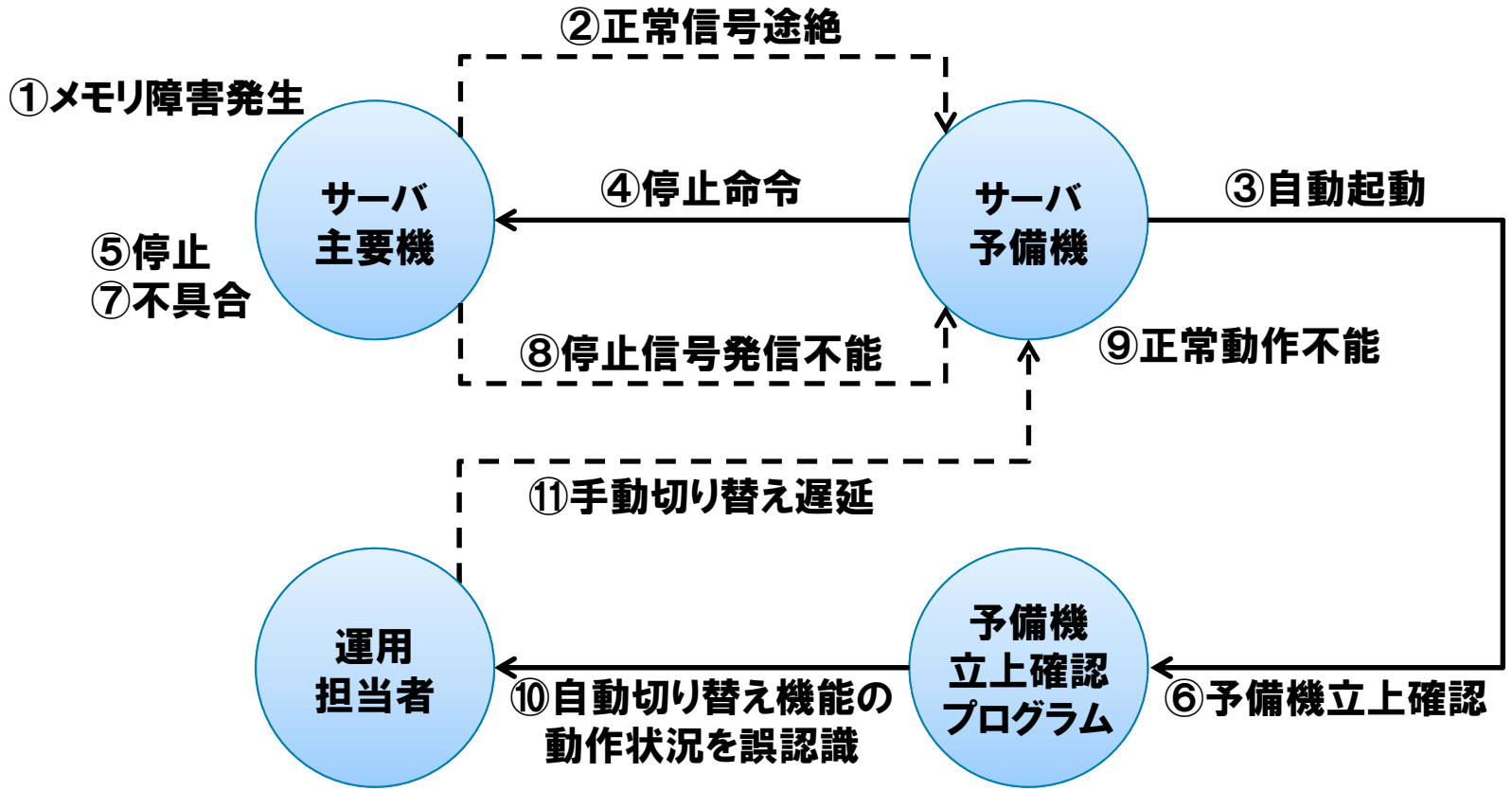
【想定リスク】

- 不適切なアクタが会員管理システムを利用するかもしれない
- 必要な関連が欠落しているかもしない
- システムで実現する機能が他にもあるかもしれない
- 不必要な関連かもしれない
- 不適切な外部システムが会員管理システムを利用するかもしれない
- 会員登録などの機能が殺到して負荷が高くなってしまい動かないかもしれない
- 会員登録機能等が間違っているかもしれない
- 会員管理システムに接続できないかもしれない
- 外部システムが故障しているかもしれない
- 外部システムに接続できないかもしれない

1.2 システムのリスク

【演習】東証のシステム障害を読み、どんなリスク(逸脱)が起こったのかを考えてみましょう。

サーバ主要機が障害を起こした場合、サーバ予備機に切り替わる仕組みとなっていたが、適切に切り替えが行われなかった。また、運用担当者はサーバ主要機の診断レポートを適切に解読できず適切に切り替えが行われなかったことに気が付かなかった。



参考:
日経新聞電子版,
2012/2/10 2:00

memo

memo

1.3 システムの特性

目的

**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。**

◆ **習得するスキル**

- **システムがディペンダブルであるために求められる特性について理解する。**
- **システムの品質特性と副特性について理解する。**

1.3 システムの特性

システムの品質特性としては以下の5つが挙げられます。
これはシステムがディペンダブルであると説明するときに使用する特性となっています。

ディペンダビリティとは、「アベイラビリティ（可用性）性能及びこれに影響を与える要因、すなわち信頼性性能、保全性性能及び保全支援能力を記述するために用いられる包括的な用語である」と、JIS Z8115（2000）で定義されています。

表2 システムの品質特性

No.	特性	説明
1	可用性	正しいサービスを提供できること
2	信頼性	正しいサービスを持続できること
3	安全性	ユーザと環境に破滅的な事態を生じさせないこと
4	一貫性	不適切な変更がないこと
5	保守性	修理・修正できる能力

1.3 システムの特性

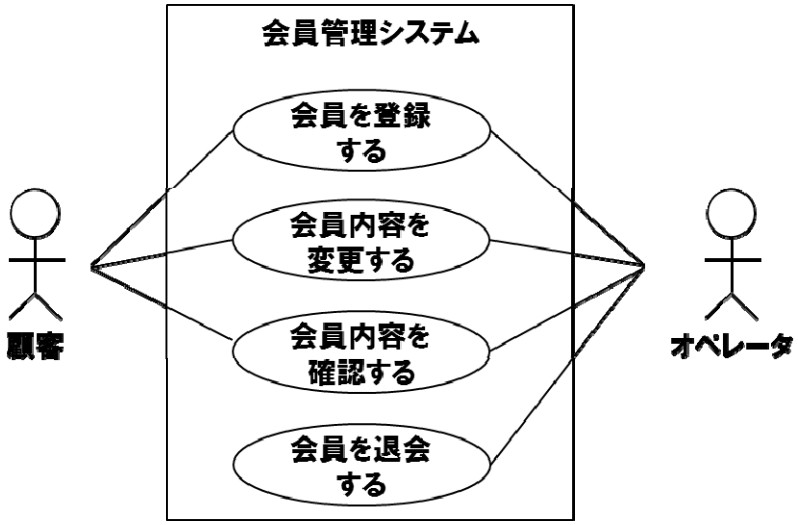
システムに求められる非機能要件に着目して考えてみましょう。
システム基盤の発注者要求を見える化する非機能要求グレード検討会では、非機能要件およびその要求項目を以下の通り定義しています。

表3 品質特性と副特性

No.	品質特性	副特性
1	可用性	運用時間(通常), 業務継続性, 目標復旧水準(通常), 目標復旧水準(大規模災害時), 稼働率, 耐障害性, 災害対策, 回復性
2	性能・拡張性	通常時の業務量, 業務量増大度, 保管期間性能目標値 バッチ、オンランスループット, バッチスループット
3	運用・保守性	計画停止, 運用負荷削減, 運用保守, 復旧作業, 異常検知対応, 運用時間, バックアップ, 運用監視, 交換用部材の確保, 運用環境, 運用管理方針
4	移行性	スケジュール、データ、リハーサル, 移行トラブル
5	セキュリティ	コンプライアンス, セキュリティリスク分析, セキュリティ診断, セキュリティリスク管理, アクセス・利用制限, データの秘匿, 不正監視, ネットワーク対策, マルウェア対策, Web対策
6	環境・エコロジー	制約条件, システム特性, 環境マネージメント

1.3 システムの特性

【例題】
会員管理システムが可用性を満たしていることを説明する手順について考えてみましょう。
手順１：機能に分解する
手順２：機能ごとに可用性を満たしていることを説明するため、副特性に分解する
手順３：副特性が求められる指標を満たすことを説明する

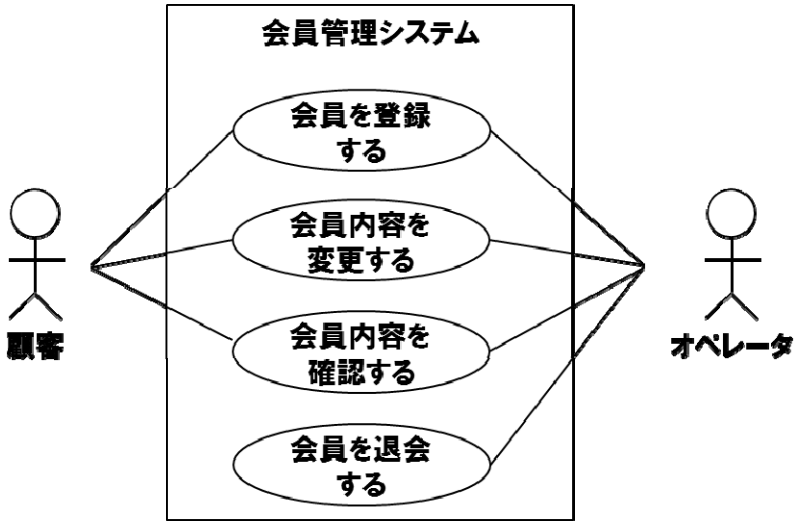


【記入欄】

【解答例】 1.3 システムの特性

【例題】
会員管理システムが可用性を満たしていることを説明する手順について考えてみましょう。
手順１：機能に分解する
手順２：機能ごとに可用性を満たしていることを説明するため、副特性に分解する
手順３：副特性が求められる指標を満たすことを説明する

～解答例～



「会員登録機能は可用性を満たしている」

↓

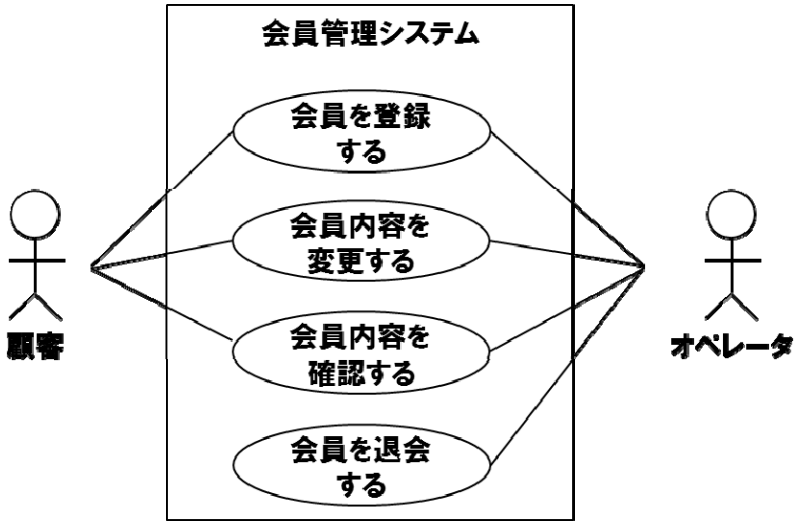
・会員登録機能は「運用時間（通常）」を満たしている
　→24時間稼働している
　　→証拠資料
　→計画的な停止はある
　　→証拠資料

・会員登録機能は「稼働率」を満たしている
　→稼働率99％
　　→証拠資料

※上記は可用性の一部の副特性です。

1.3 システムの特性

【演習】
会員管理システムがセキュリティを満たしていることを説明する手順について考えてみましょう。
手順１：機能に分解する
手順２：機能ごとにセキュリティを満たしていることを説明するため、副特性に分解する
手順３：副特性が求められる指標を満たすことを説明する



【記入欄】

memo

memo

1.4 保証ケースの表記法

目的

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。

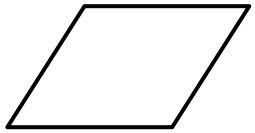
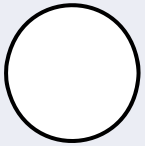
◆ **習得するスキル**

- **保証ケースを表記するときに使用する構成要素について理解する。**
- **保証ケースの表記法の基本ルールについて理解する。**

1.4　保証ケースの表記法

保証ケースを表記するときに使用する構成要素は5つあります。

表4　保証ケースの構成要素

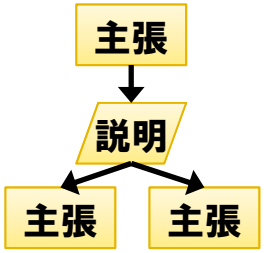
名称	図式要素	説明
主張（ゴール）		システムが達成すべき状態（性質）を示す。 下位の主張や説明に分解される。 なお、最上位の主張は複数あってもいい。 （例）システムは安全である
説明 （戦略）		主張の達成を導くために必要となる説明を示す。 下位の主張や説明に分解される。 （例）～による論証
前提 （コンテクスト）		主張の説明が必要となる理由としての外部情報を示す。 （例）想定するリスク
未定義 要素		まだ具体化できていない主張や説明であることを示す。 （アンデベロップドなどと表記する。）
証拠 （ソリューション）		主張や説明が達成できることを示す証拠（証跡）。 （例）テスト結果

1.4 保証ケースの表記法

保証ケースを表記するときに基本ルールを説明します。

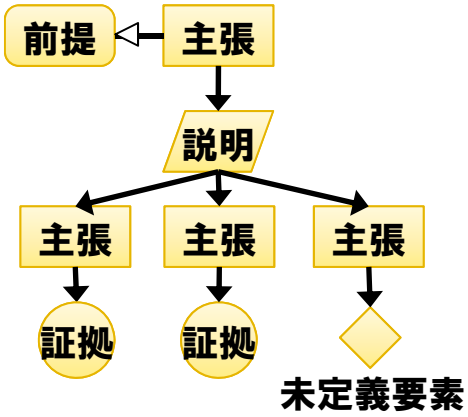
☑ 「主張」は「説明」を用いて、下位の「主張」に展開することができます。

（例）



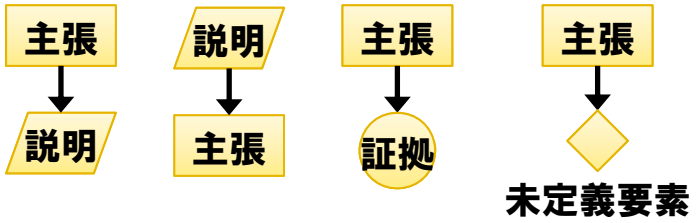
☑ 木構造を用いてシステムが満たすべき「主張」が最下位の「証拠」と「前提」によって成立することを確認します。なお、最下位が「未定義要素」となるときもあります。

（例）



☑ 矢印は「⇦」と「←」の2種類あります。

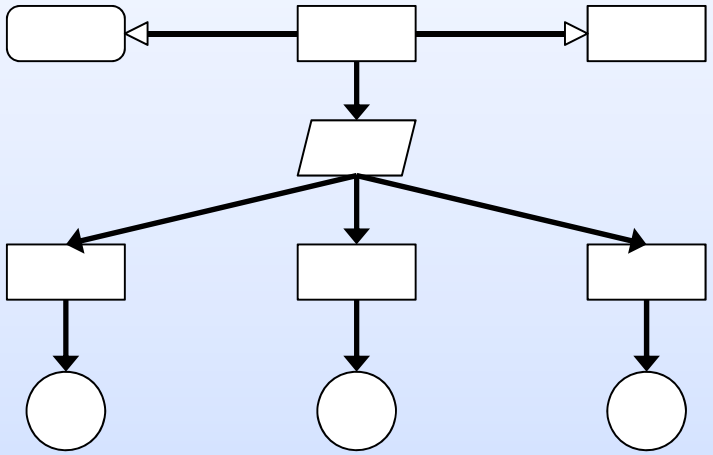
（例）



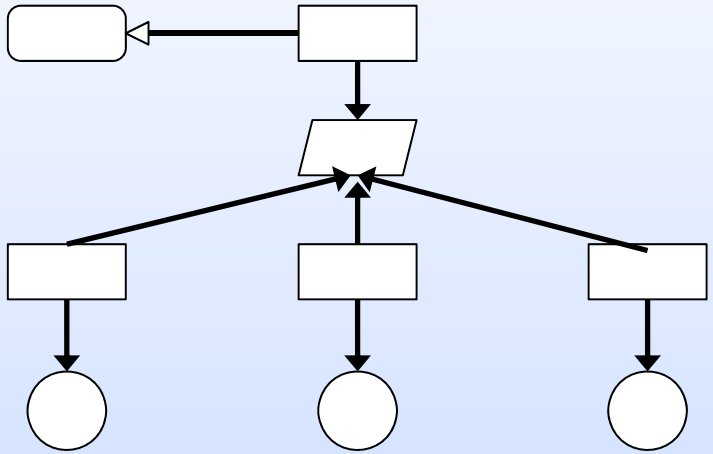
1.4 保証ケースの表記法

【例題】間違った表記について指摘してください。

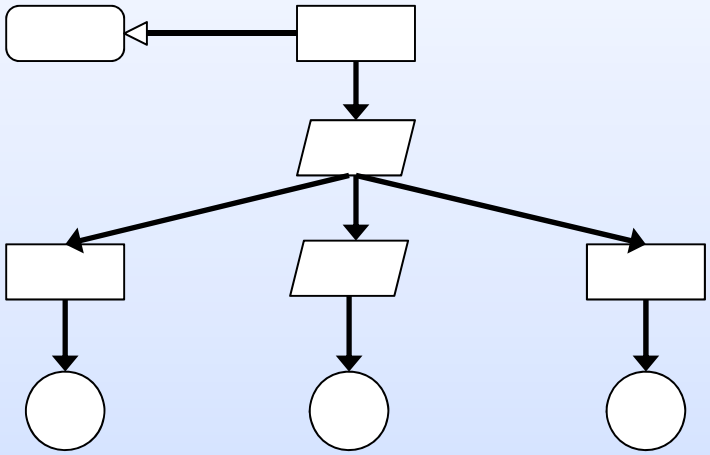
【問1】



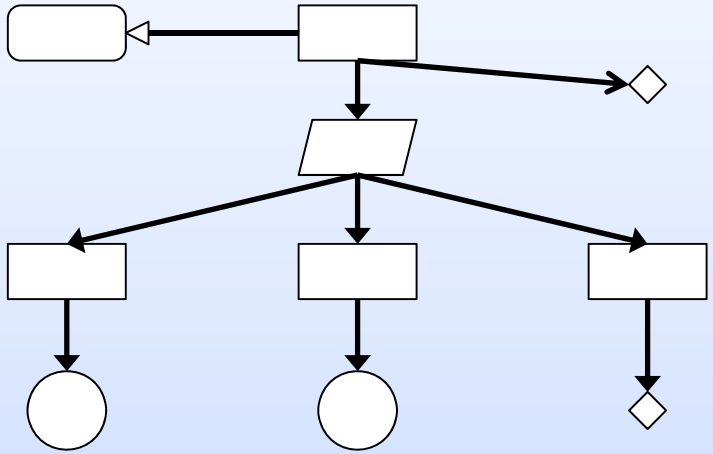
【問2】



【問3】



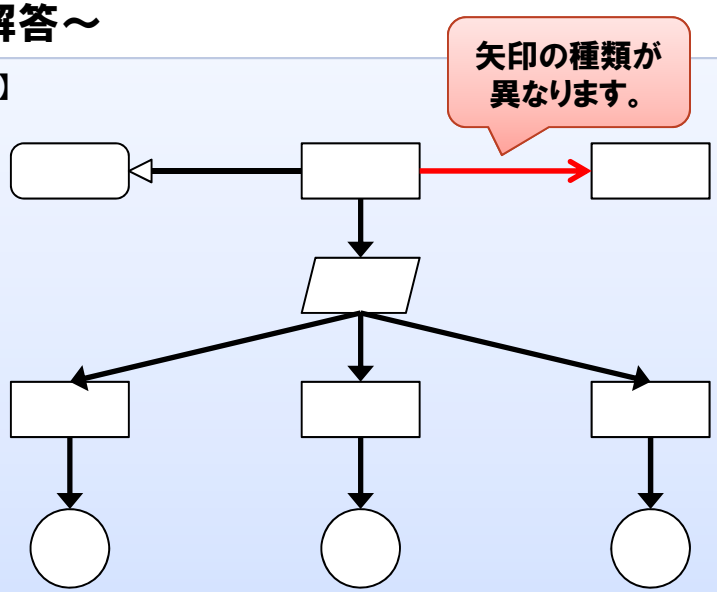
【問4】



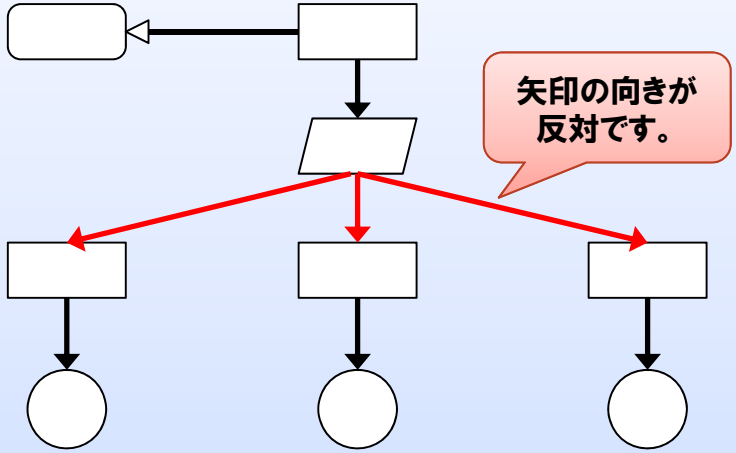
【解答例】 1.4 保証ケースの表記法

～解答～

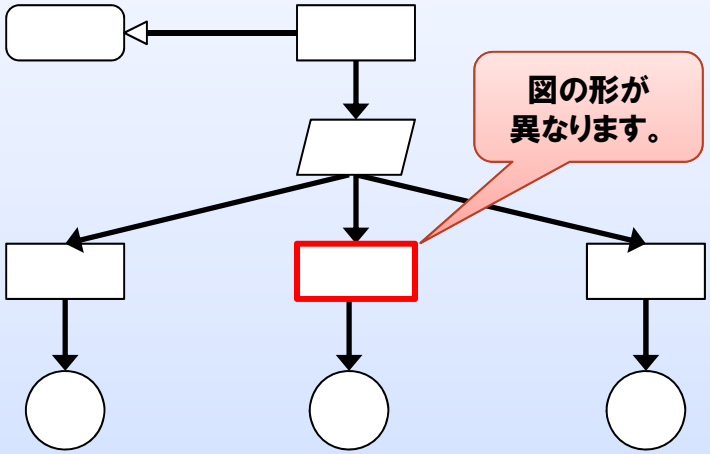
【問1】



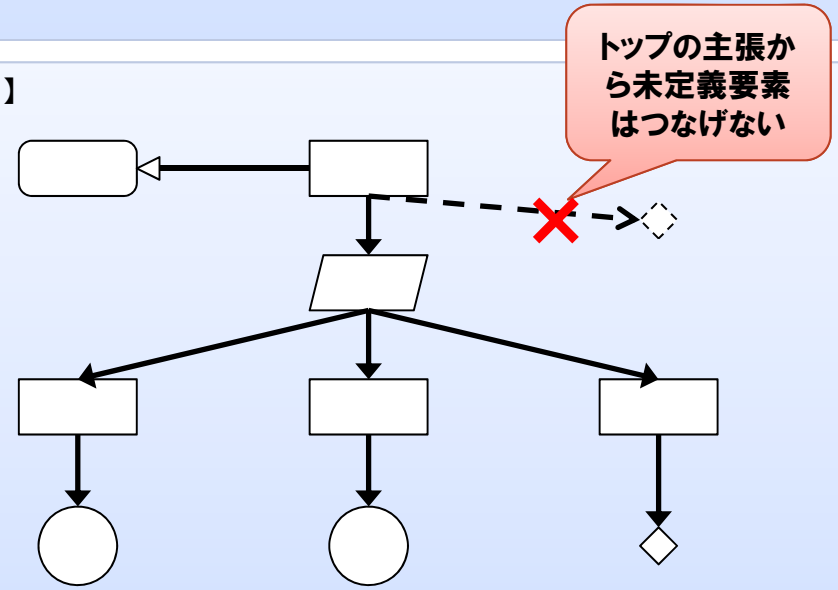
【問2】



【問3】



【問4】



1.4 保証ケースの表記法

【演習】
会員管理システムがセキュリティを満たすことを示す保証ケースを作成してください。

【記入欄】

memo

memo

1.5 主張の分解

目的

**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。**

◆ **習得するスキル**

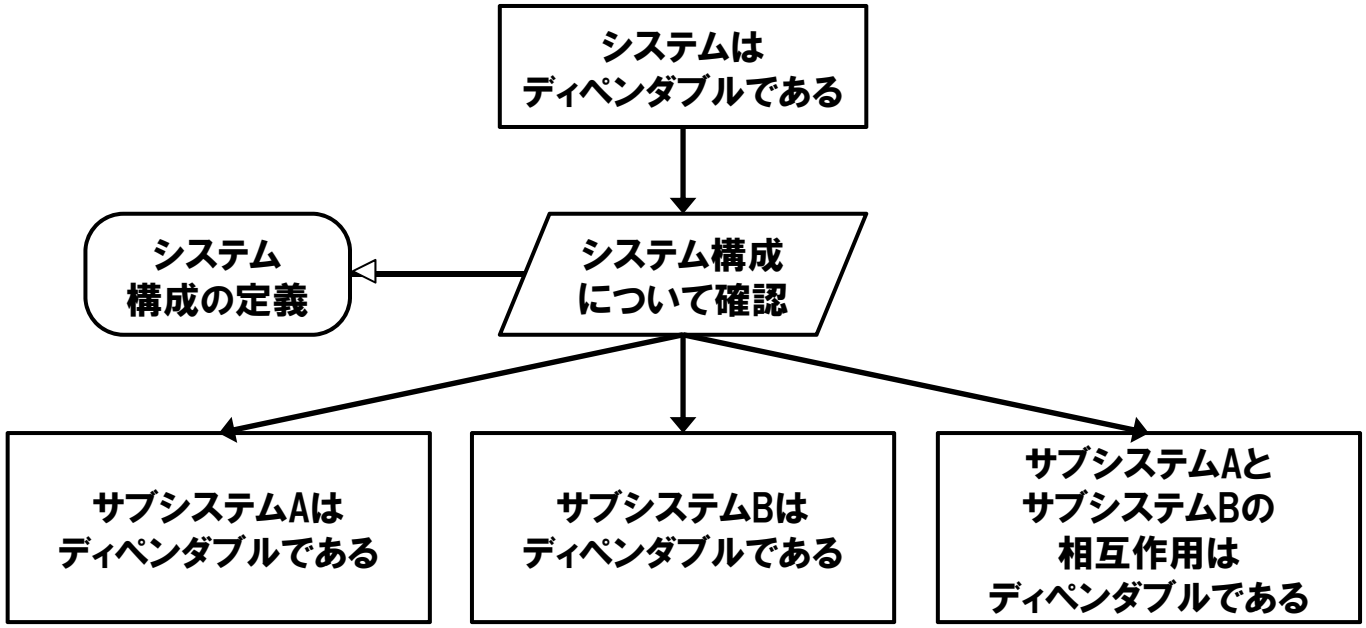
- **保証ケースの分解パターンとして、「成果物分解パターン」「特性分解パターン」「リスク分解パターン」について理解する。**

1.5 主張の分解

保証ケースの基本パターンには「成果物分解パターン」「特性分解パターン」「リスク分解パターン」の3種類があります。まず、成果物分解パターンについて説明します。

成果物分解パターン

システムが特性を満たすことをシステム構成に基づいて分解します。
ここでは、対象となるシステムがサブシステムAとBとで構成されるとしています。

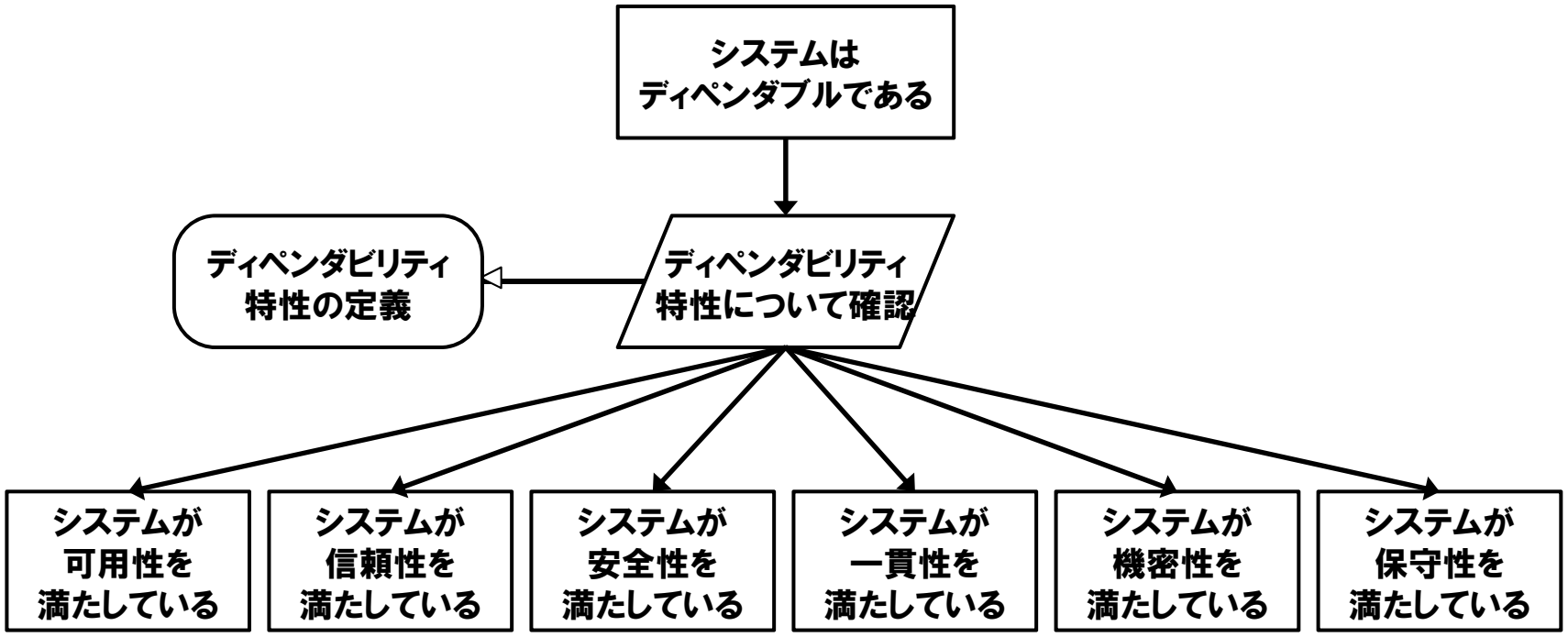


1.5 主張の分解

次に、特性分解パターンについて説明します。

特性分解パターン

システムが特性を満たすことを特性の構成要素に従って分解します。
ここでは、可用性、信頼性、安全性、一貫性、機密性、保守性があるとしています。

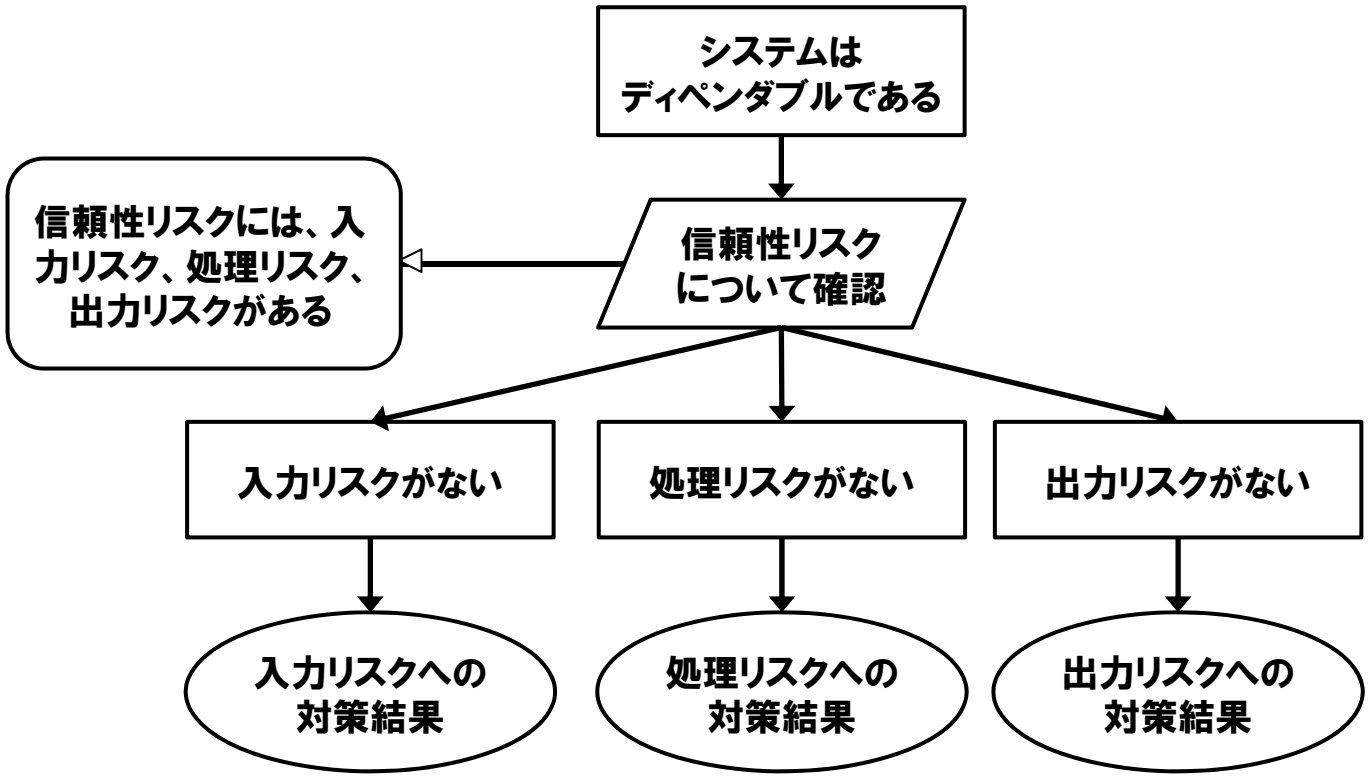


1.5 主張の分解

最後に、リスク分解パターンについて説明します。

リスク分解パターン

システムが特性を満たすことを特性リスクの定義に基づいて分解します。
ここでは、信頼性リスクには、入力リスク、処理リスク、出力力リスクがあるとしています。



1.5 主張の分解

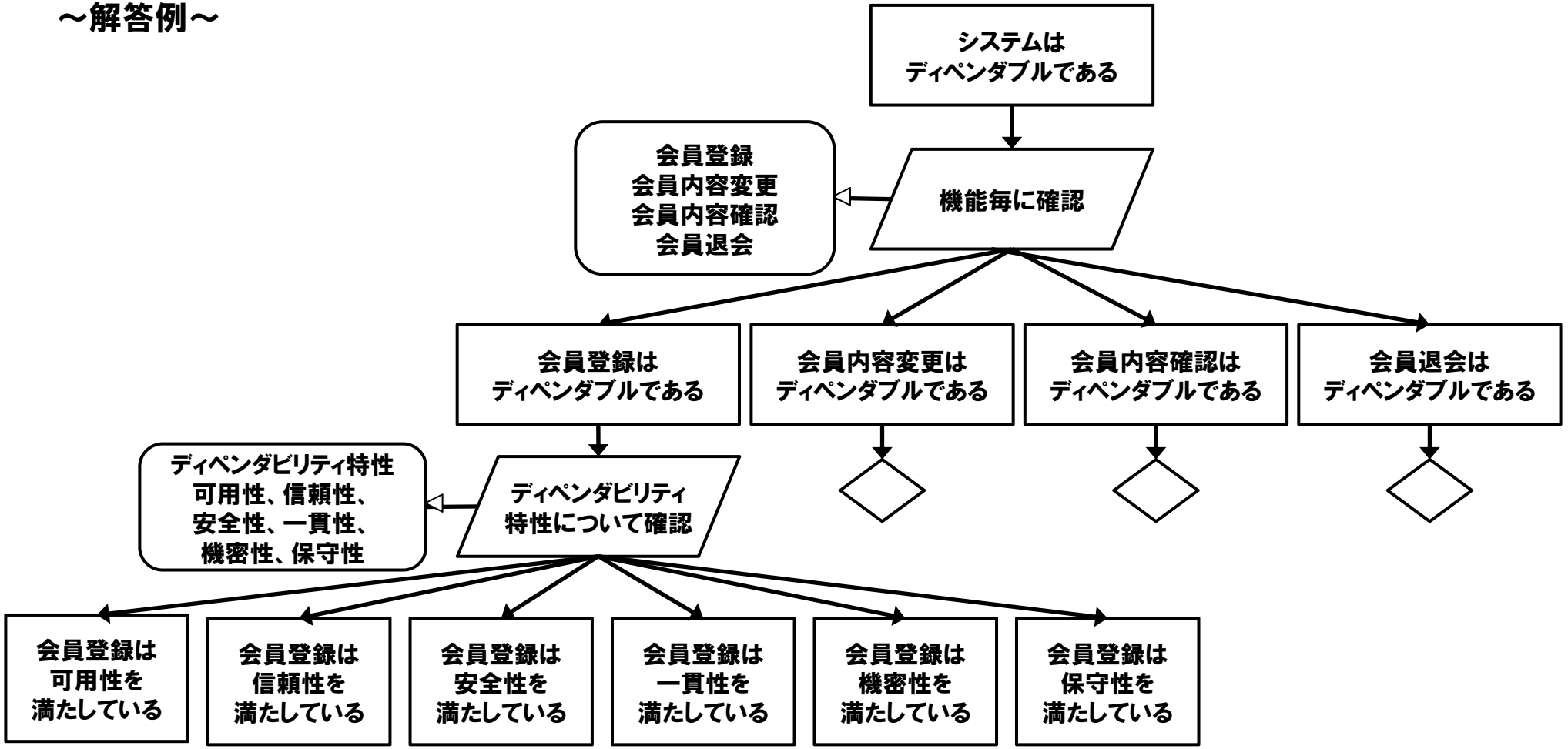
【例題】
会員管理システムの保証ケースを機能ごとに分解し、特性分解して作成してください。

【記入欄】

【解答例】 1.5 主張の分解

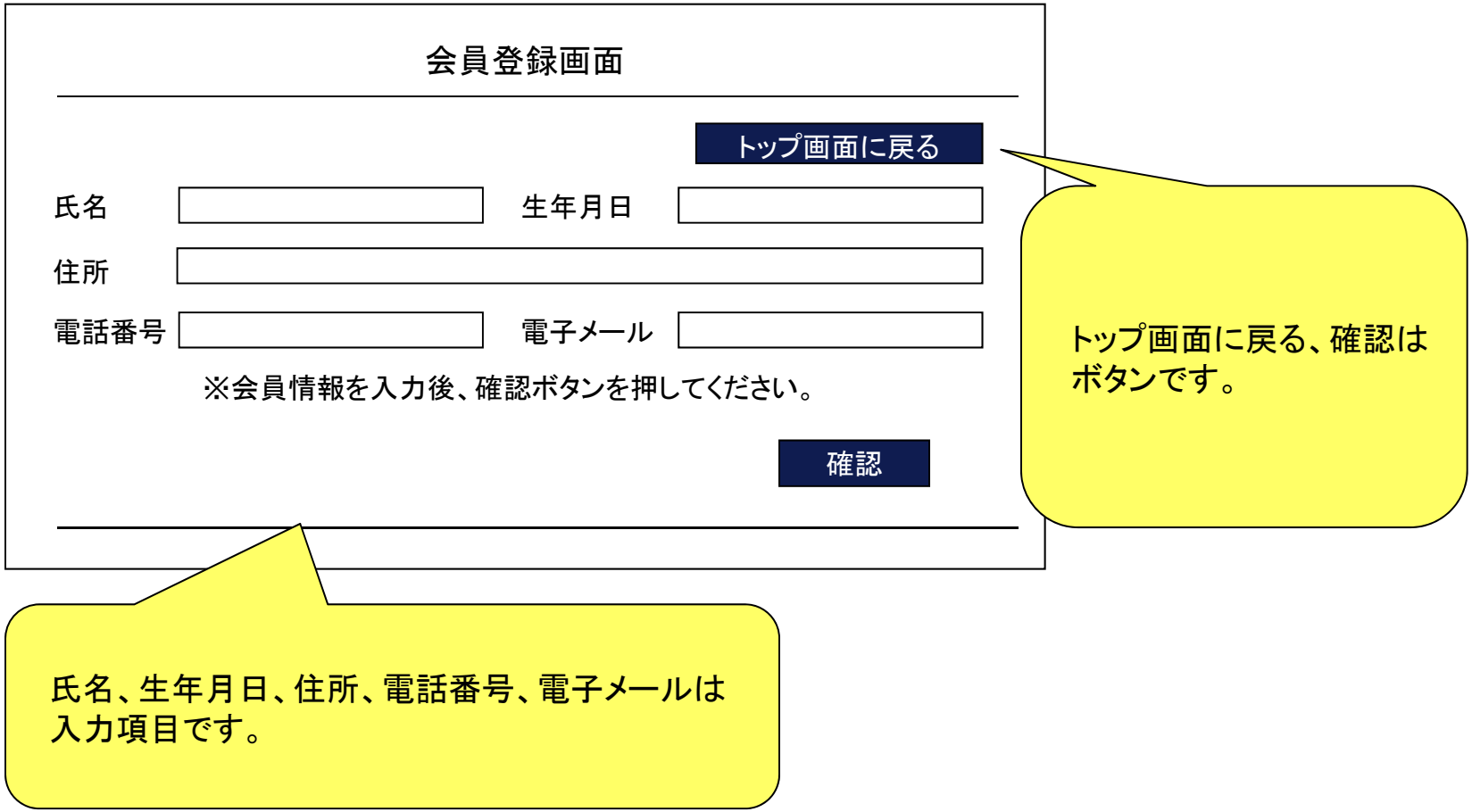
【例題】
会員管理システムの保証ケースを機能ごとに分解し、特性分解して作成してください。

～解答例～



1.5 主張の分解

【演習】
会員管理システムの会員登録の信頼性リスクについて保証ケースをリスク分解パターンで作成してください。



1.5 主張の分解

【演習】
会員管理システムの会員登録の信頼性リスクについて保証ケースをリスク分解パターンで作成してください。

【記入欄】

memo

memo

1.6 リスク対策の証拠

目的

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

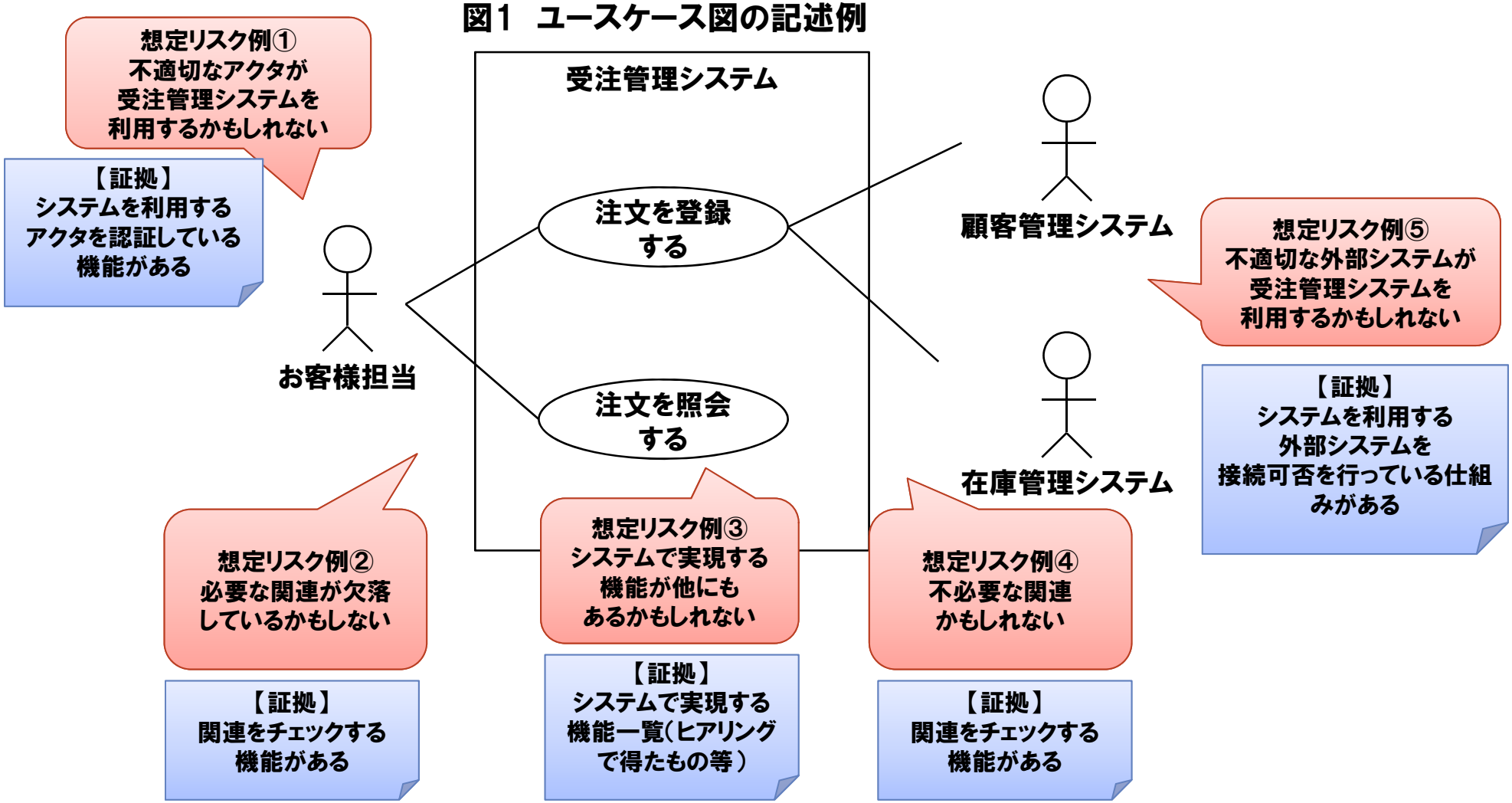
◆ **習得するスキル**

- **リスク対策としてどのようなものがあるかについて理解する。**

1.6 リスク対策の証拠

保証ケースを使ってリスク対策ができている証拠を示すことができます
下記のユースケース図のリスクについてどんな対策(＝その証拠)が考えられるかを説明します。

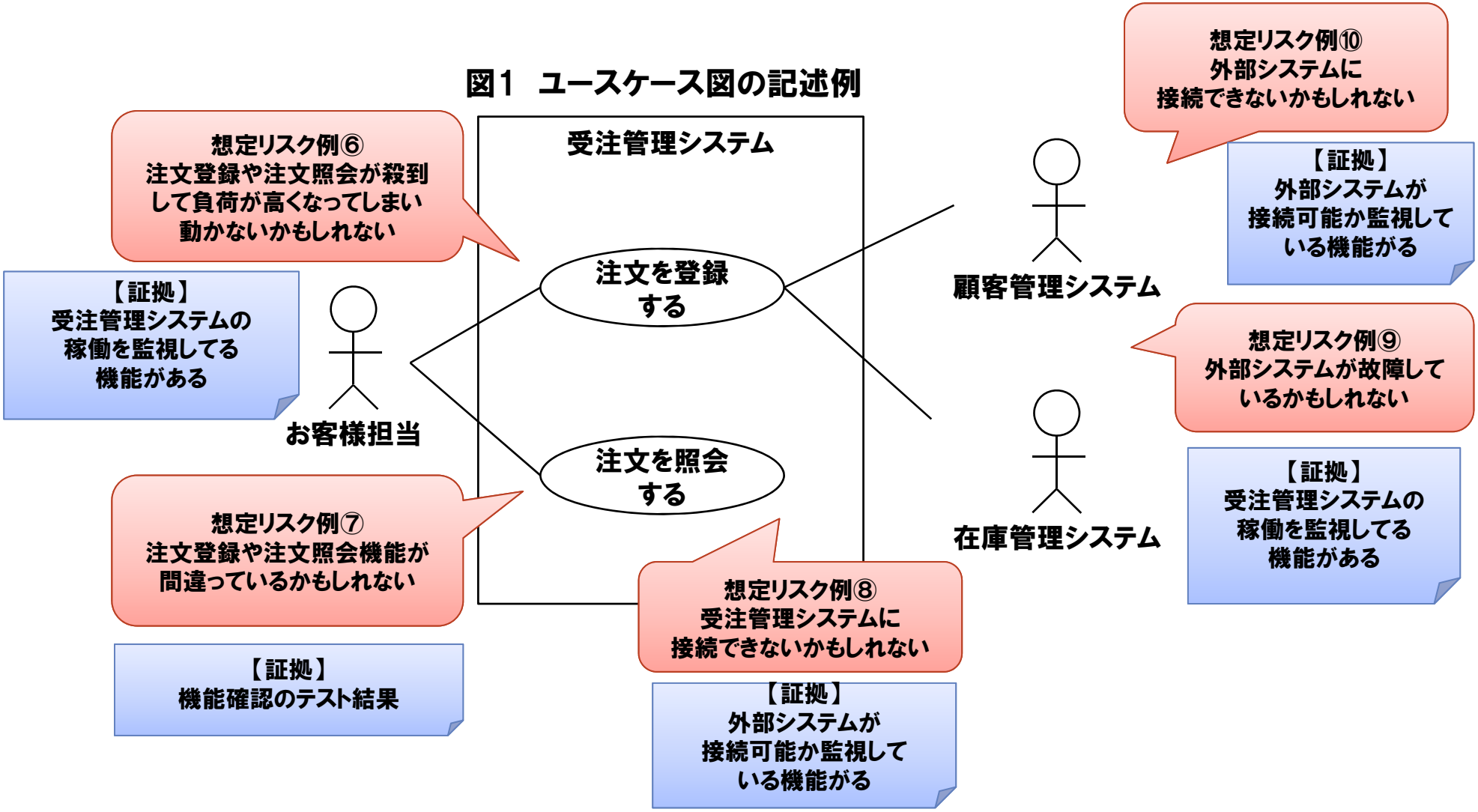
図1 ユースケース図の記述例



1.6 リスク対策の証拠

全頁に続き、ユースケース図のリスクについてどんな対策(＝その証拠)が考えられるかを説明します。

図1 ユースケース図の記述例



1.6 リスク対策の証拠

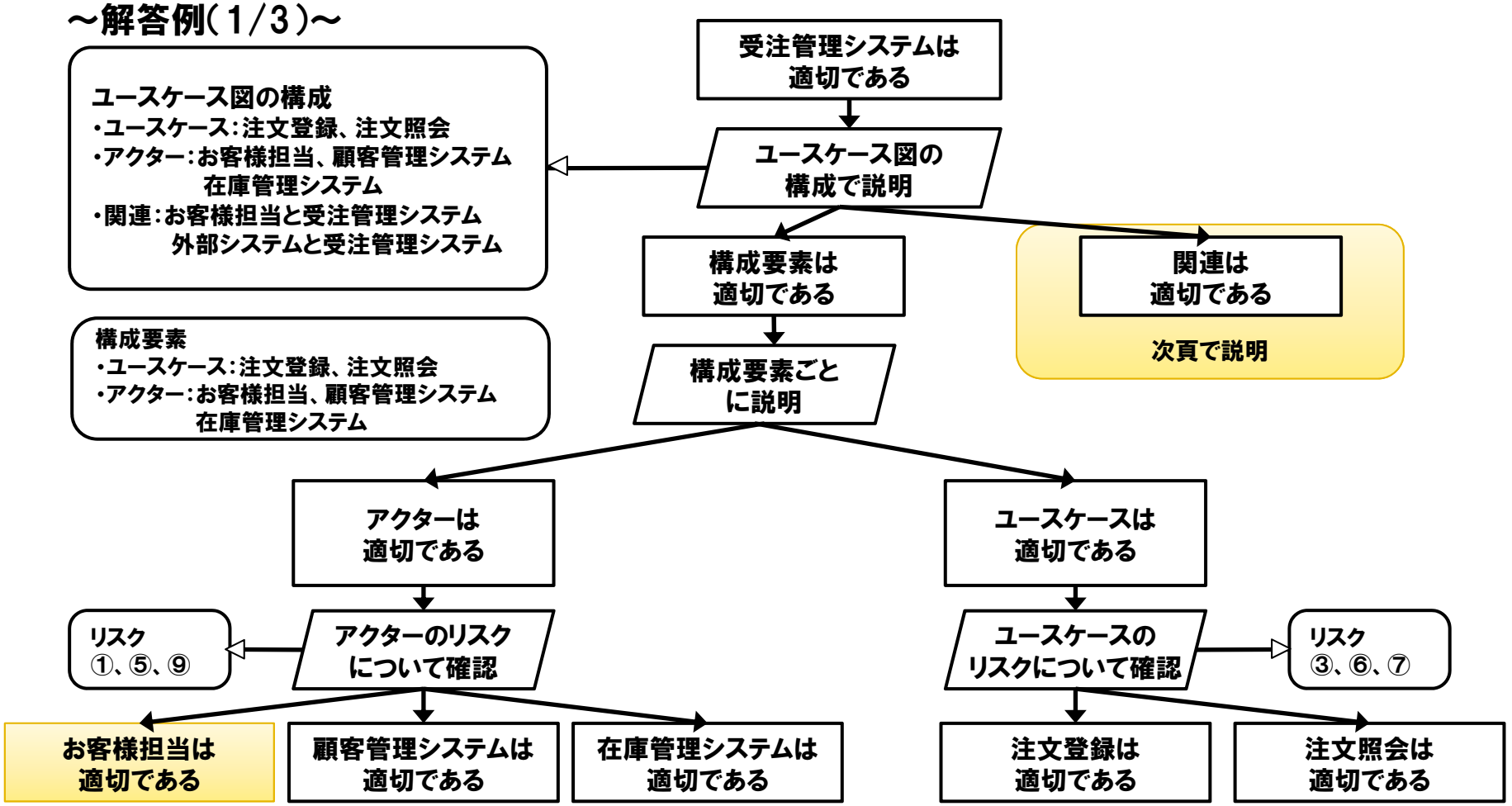
【例題】ユースケース図（受注管理システム）について保証ケースを作成してください。

【記入欄】

1.6 リスク対策の証拠

【例題】ユースケース図（受注管理システム）について保証ケースを作成してください。

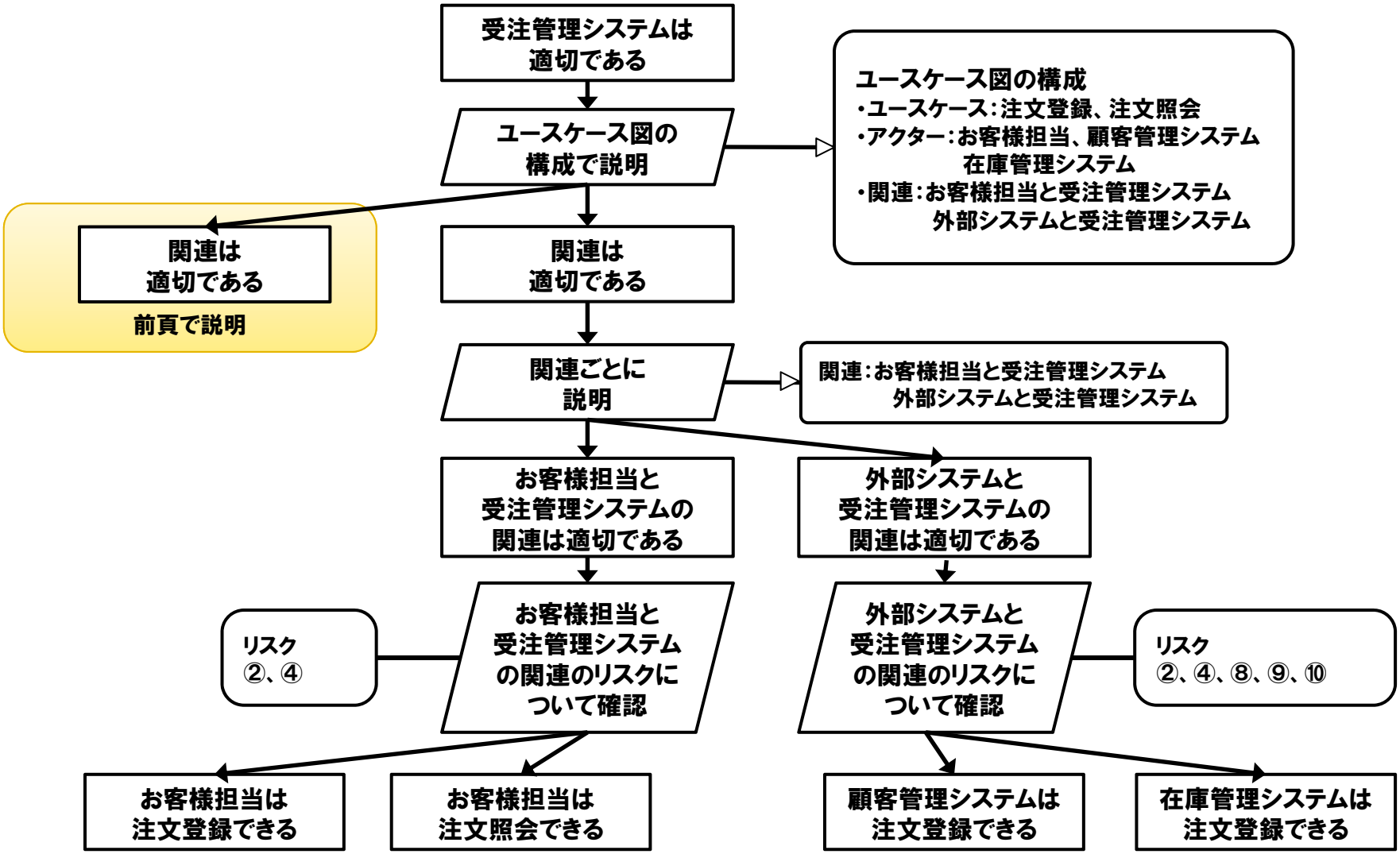
～解答例（1/3）～



※「お客様担当は適切である」について分解して説明します（解答例（3/3）を参照）。

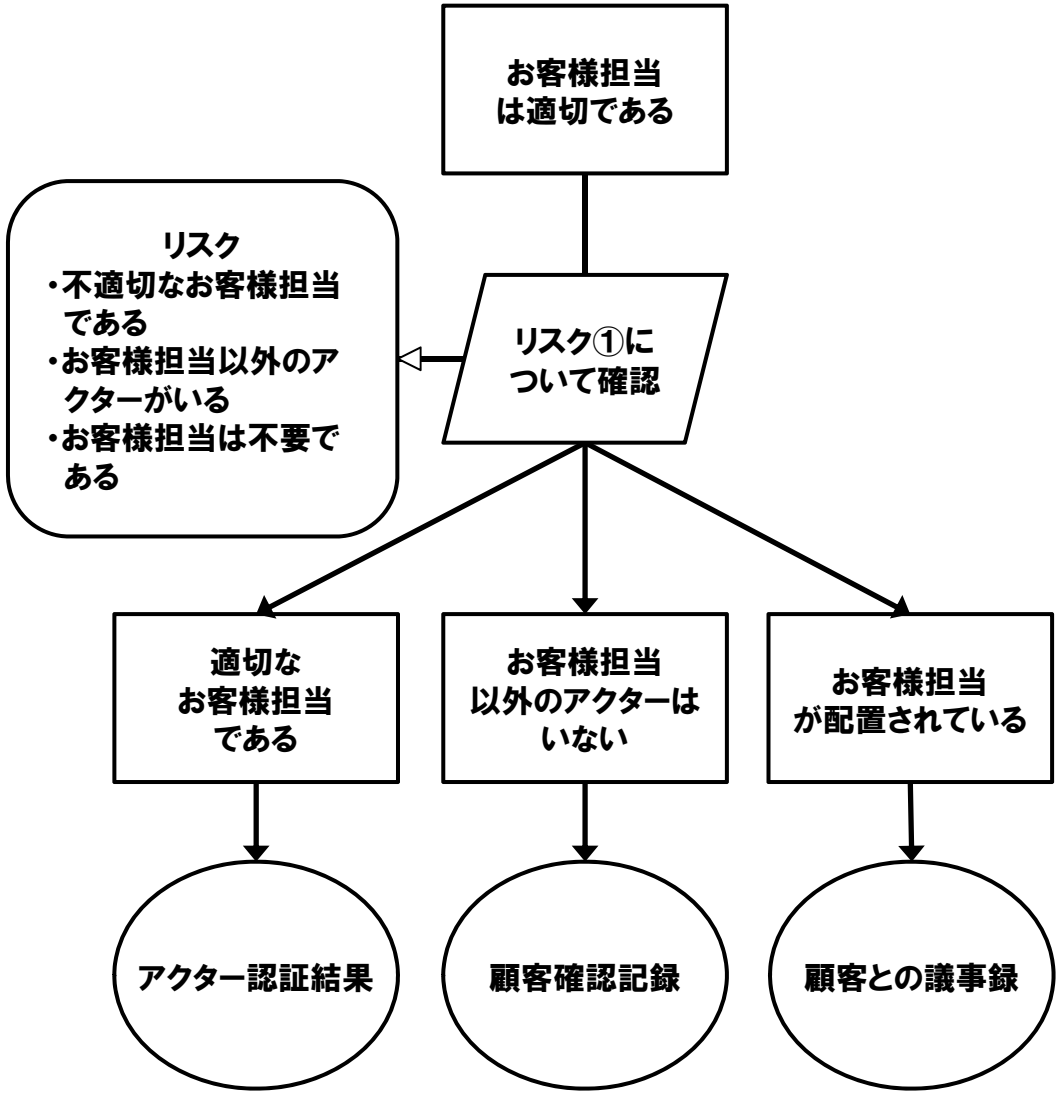
1.6 リスク対策の証拠

～解答例(2/3)～



1.6 リスク対策の証拠

～解答例(3/3)～

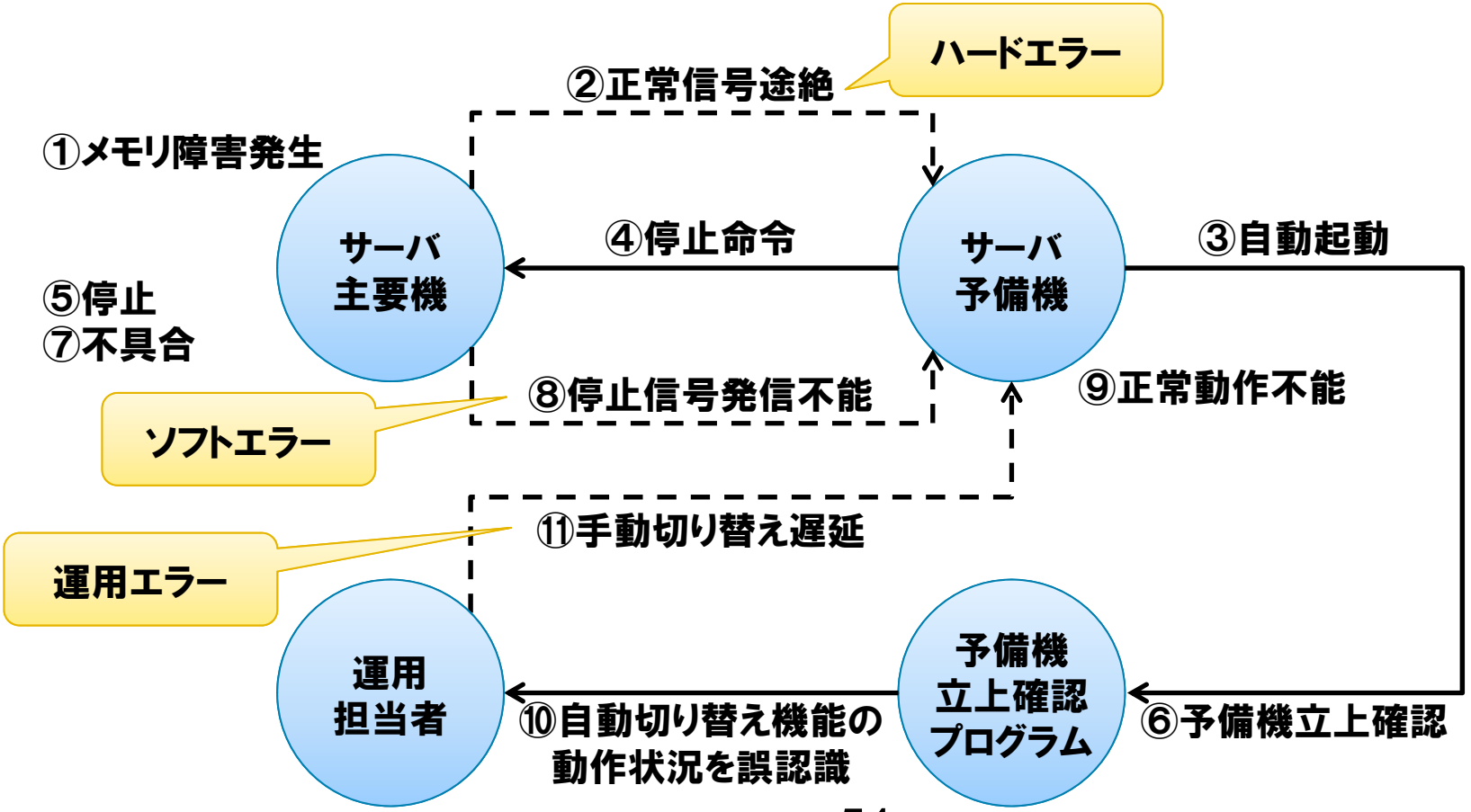


1.6 リスク対策の証拠

【演習】東証のシステム障害を踏まえ、どんなリスク対策が必要か考えてみましょう。

～1.2章 演習 再掲～

サーバ主要機が障害を起こした場合、サーバ予備機に切り替わる仕組みとなっていたが、適切に切り替えが行われなかった。また、運用担当者はサーバ主要機の診断レポートを適切に解読できず適切に切り替えが行われなかったことに気が付かなかった。



1.6 リスク対策の証拠

【演習】東証のシステム障害について、少し掘り下げて説明します。

～株式売買システムの障害（2012年2月2日）～

【障害概要】

情報配信ゲートウェイサーバでハード障害が発生し、監視端末上に異常メッセージが表示され、異常メッセージへの対応を完了したが、株式売買システムの一部銘柄で相場情報が配信できない事象が発生。その後、ハード障害を契機とした予備系への切り替え処理が正常に完了していないことが原因であると判明。当取引所の241銘柄及び他の券取引所を含む74銘柄の売買を停止。システム障害の復旧作業を完了し、取引を開始。

【再発防止措置】

①株式売買システムの障害発生に関する再発防止措置策等
- ・障害対応の体制面での改善及び強化
- ・確認手順及び確認項目の明確化
- ・速やかな復旧に向けた取り組み
- ・自動切替え発生時の動作確認

②本システムにおける切替え試験の実施
- ・類似障害再現により切替え機能及び対応フローの確認
- ・全サーバの切替え機能の確認

③再発防止策の他システムへの展開

出展：科学技術振興機構　DEOSの最新動向とD-Case事例紹介

1.6 リスク対策の証拠

【演習】東証のシステム障害について、少し掘り下げて説明します(続き)。

～デリバティブ売買システムの障害(2012年8月7日)～

【障害概要】

デリバティブ売買システムのネットワーク機器である業務L3スイッチの本番系(1号機)においてハードウェア障害が発生。ただちに障害対策本部を立ち上げ、障害の特定・復旧に向けた対応に着手したが、全派生商品の取引を停止。その後、システムの復旧作業を完了し注文受付・取引を再開。

【障害原因と対策】

本番系(1号機)のハード障害に伴い、待機系(2号機)事態は本番系への状態変更する自動切替え処理を正常に動作させたが、1号機内部の部分的なハード障害検知の異常により、1号機、2号機の両方が、本番系の状態となった。その結果、これらスイッチに接続されている装置が送信先を特定することが不可能となり、通信ができなくなった。本不具合に係る製品内臓プログラムの改修版のシステムへの取組みは、テスト環境での十分な検証を経た後に行う。なお、同様の事態に備える対策を既に講じた。

出展:科学技術振興機構　DEOSの最新動向とD-Case事例紹介

1.6 リスク対策の証拠

【演習】東証のシステム障害について、少し掘り下げて説明します(続き)。

～金融庁より業務改善命令を受け、再発防止策を発表～

【未然防止の観点での施策(業務継続の観点から万一の場合を想定)】

- ・取引停止につながる可能性の観点から機器の洗出し、切替えの仕組みや設計値の妥当性等確認(業務継続の観点)
- ・切替えが正常に機能しない場合の対応策等について確認し、総点検を踏まえた改善施策の検討・対応の実施計画を策定
- ・市販品の選定基準を策定

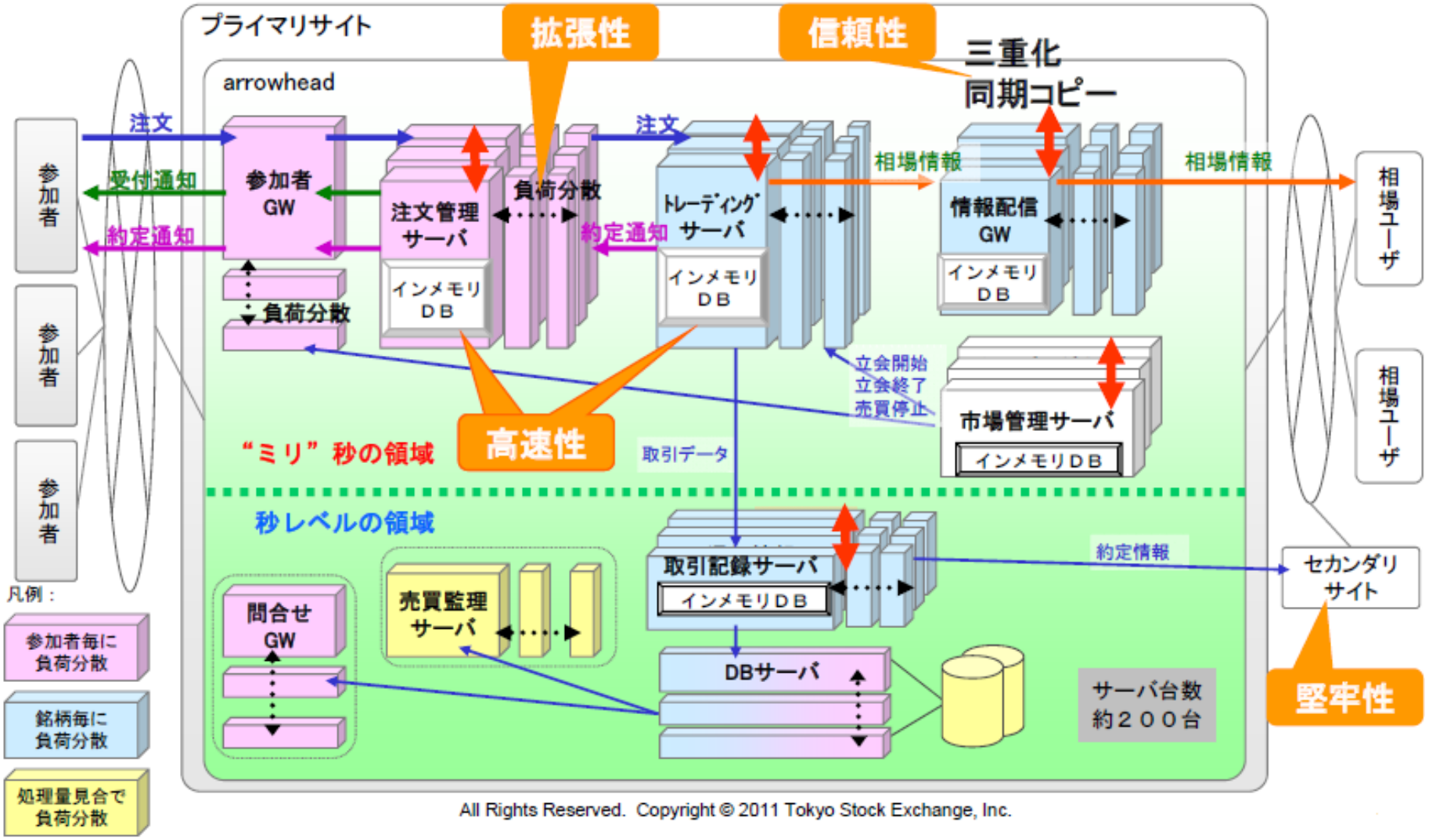
【障害発生時の業務影響を極小化するための施策】

- ・障害発生時の初動体制の整備や障害テスト等を通じた担当者の教育及び訓練
- ・復旧作業を短縮し業務影響を極小化するため、障害発生時に対外影響のある、7システムを対象に障害時運用プロセスの再点検を実施

出展:科学技術振興機構　DEOSの最新動向とD-Case事例紹介

1.6 リスク対策の証拠

東証の売買システムの概要です。



出展：ET2011講演資料より（東証売買システム（arrowhead）のディペンダビリティ実現のための方式および機能）

1.6 リスク対策の証拠

【記入欄】

memo

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

2.1　モデルの定義

目的

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。

◆　**習得するスキル**

- **成果物（ユースケース図）のモデル定義を理解する。**

2.1 モデルの定義

保証ケース統合作成支援ツールUC2CTでは、作成されたモデル定義言語からモデル図を自動作成します。ここではモデル定義言語の作成方法について説明します。

以下の図2 モデル定義言語によるユースケース図の定義は、図3 ユースケース図をモデル定義言語で記述した例です。

図2 ユースケース図

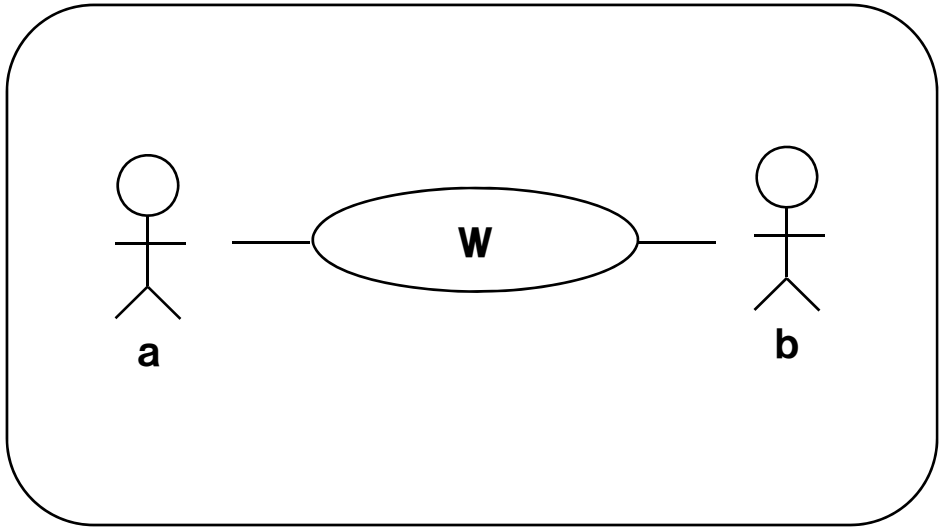


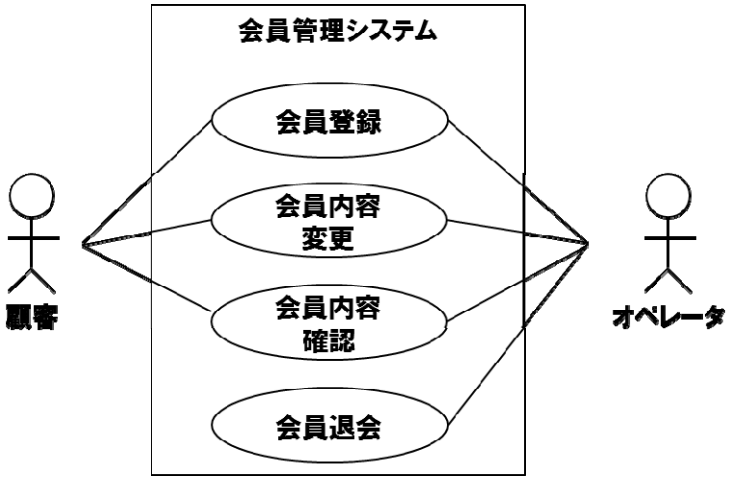
図3 モデル定義言語による
ユースケース図の定義

```
Model  usecase_diagram
type
  actor, usecase : Node;
  interaction : Relation;
  end type;
instance usecase-1: usecase_diagram;
  a, b: actor;
  w: usecase;
 (a, w) : interaction;
 (b, w) : interaction;
end instance;
```

Model, type, Node, Relation, end, instance は予約語である
type 節でモデルのメタモデルを定義する
instance 節でメタモデルで作成したモデルの実体の構成を記述

2.1 モデルの定義

【例題】
以下のユースケース図 usecase-1 についてモデル定義言語を作成してください。

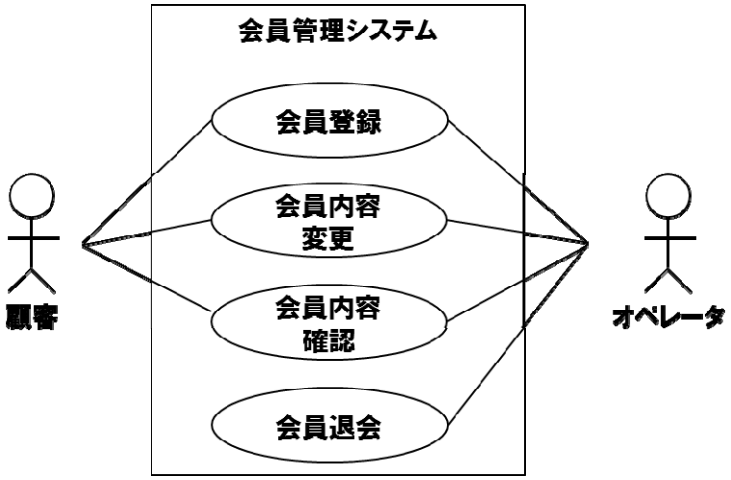


【記入欄】

【解答例】 2.1 モデルの定義

【例題】
以下のユースケース図 usecase-1 についてモデル定義言語を作成してください。

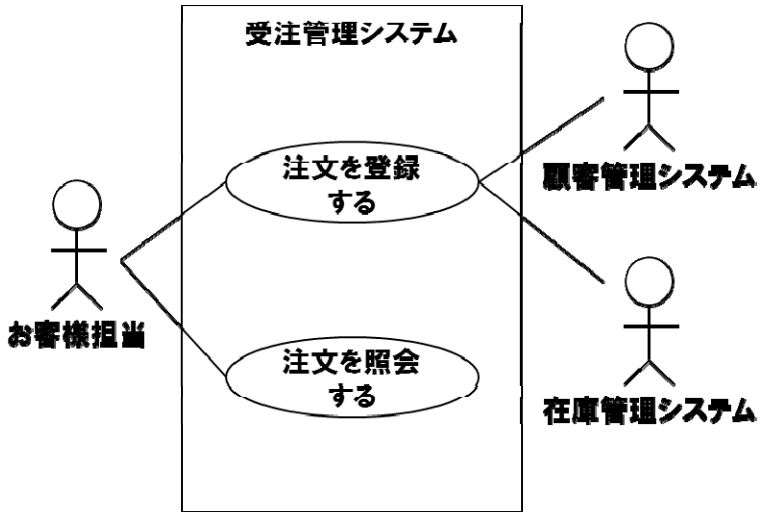
～解答例～




```
Model  usecase_diagram
type
  actor, usecase : Node;
  interaction : Relation;
  end type;
instance usecase-1: usecase_diagram;
  顧客, オペレータ: actor;
  会員登録, 会員内容変更, 会員内容確認, 会員退会: usecase;
 (顧客, 会員登録) : interaction;
 (顧客, 会員内容変更) : interaction;
 (顧客, 会員内容確認) : interaction;
 (会員登録, オペレータ) : interaction;
 (会員内容変更, オペレータ) : interaction;
 (会員内容確認, オペレータ) : interaction;
 (会員退会, オペレータ) : interaction;
end instance;
```

2.1 モデルの定義

【演習】
以下のユースケース図 usecase-1 についてモデル定義言語を作成してください。



【記入欄】

memo

memo

2.2 主張の分解(復習)

目的

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。

◆ **習得するスキル**

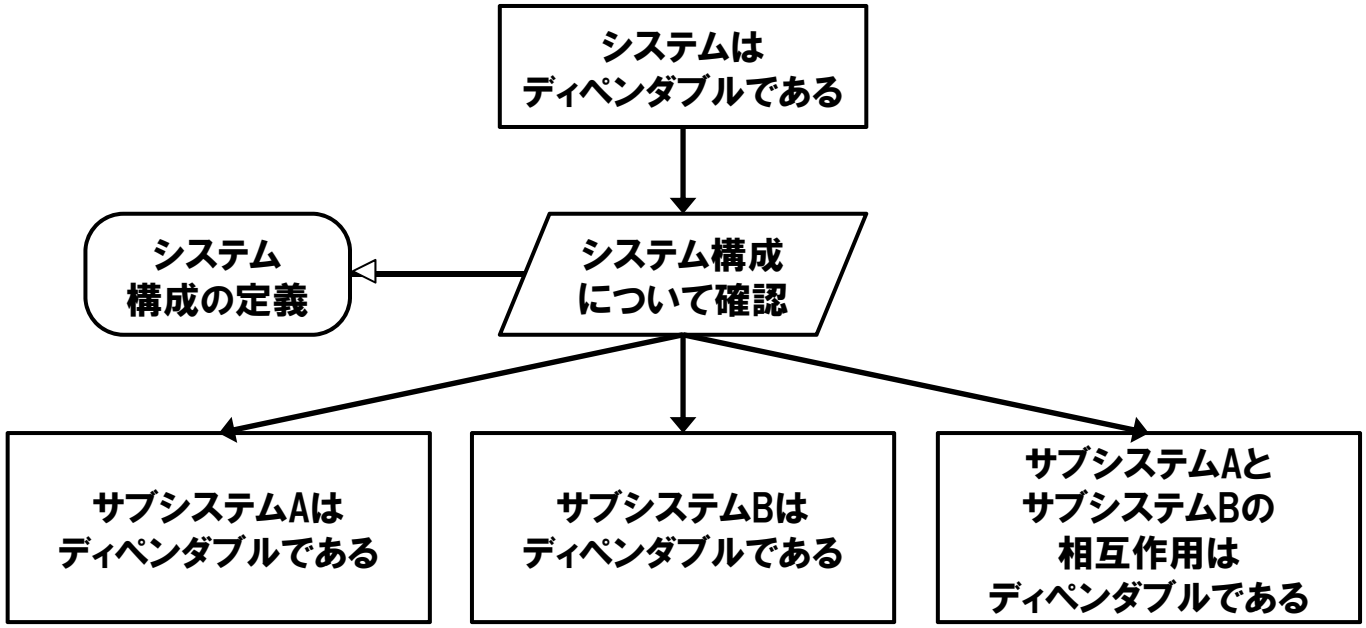
- **保証ケースの分解パターンとして、「成果物分解パターン」「特性分解パターン」「リスク分解パターン」について理解する。**

2.2 主張の分解 ～再掲～

保証ケースの基本パターンには「成果物分解パターン」「特性分解パターン」「リスク分解パターン」の3種類があります。まず、成果物分解パターンについて説明します。

成果物分解パターン

システムが特性を満たすことをシステム構成に基づいて分解します。
ここでは、対象となるシステムが2つのサブシステムAとBで構成されるとしています。

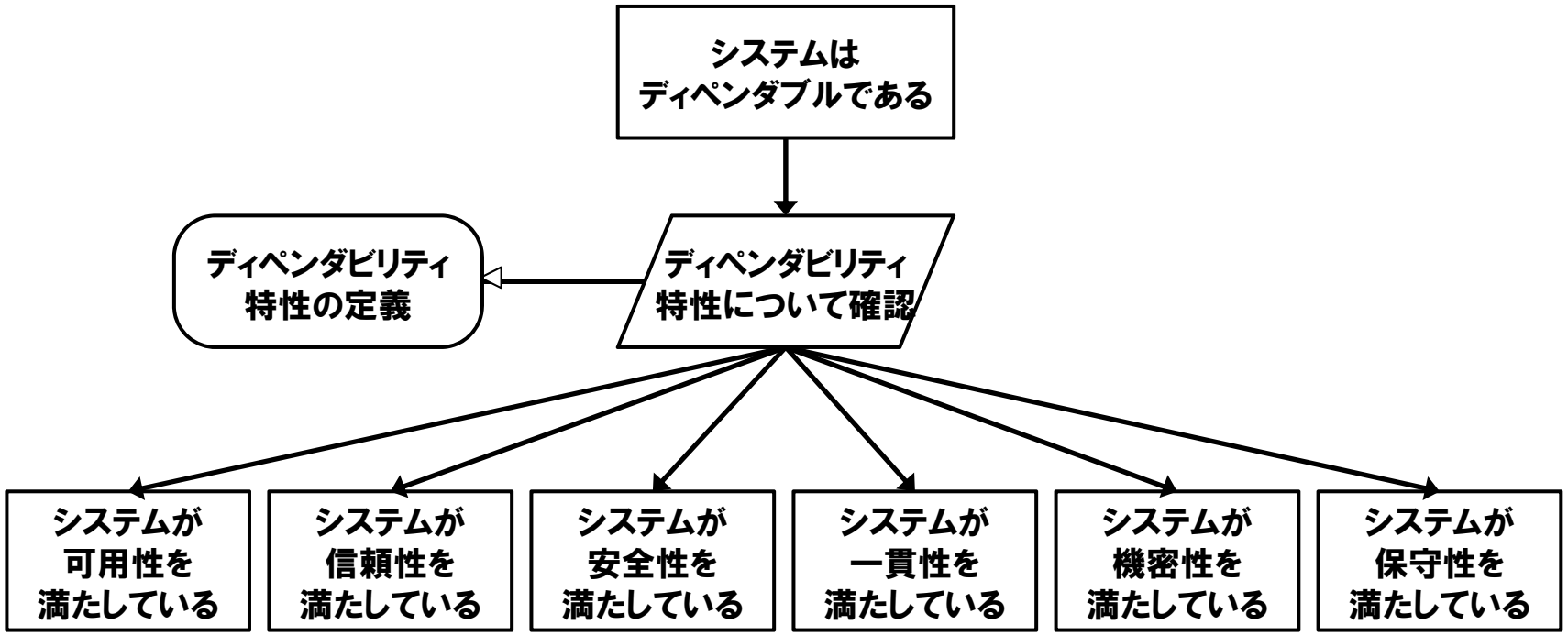


2.2 主張の分解 ～再掲～

次に、特性分解パターンについて説明します。

特性分解パターン

システムが特性を満たすことを特性の構成要素に従って分解します。
ここでは、可用性、信頼性、安全性、一貫性、機密性、保守性があるとしています。

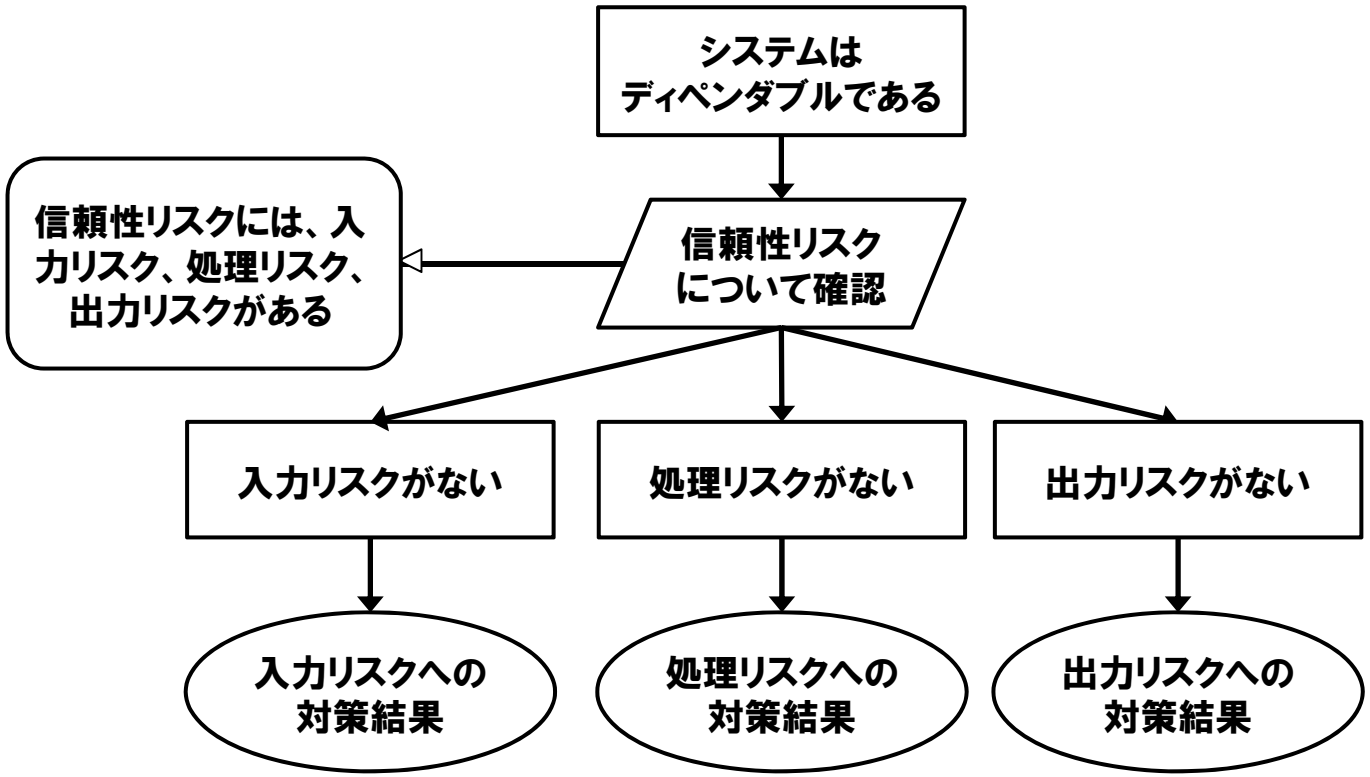


2.2 主張の分解 ～再掲～

最後に、リスク分解パターンについて説明します。

リスク分解パターン

システムが特性を満たすことを特性リスクの定義に基づいて分解します。
ここでは、信頼性リスクには、入力リスク、処理リスク、出力力リスクがあるとしています。



2.2 主張の分解 ～再掲～

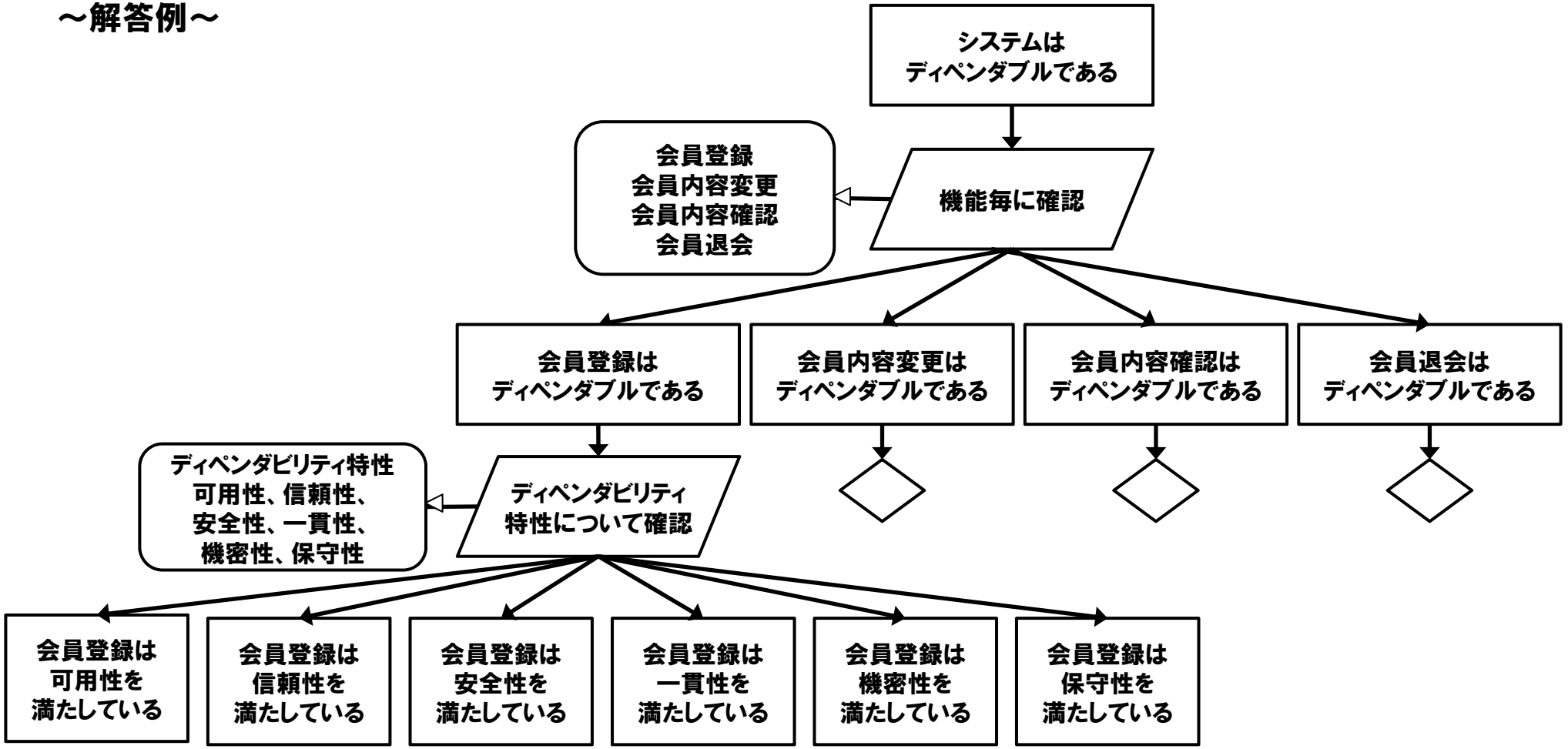
【例題】
会員管理システムの保証ケースを機能ごとに分解し、特性分解して作成してください。

【記入欄】

【解答例】 2.2 主張の分解 ～再掲～

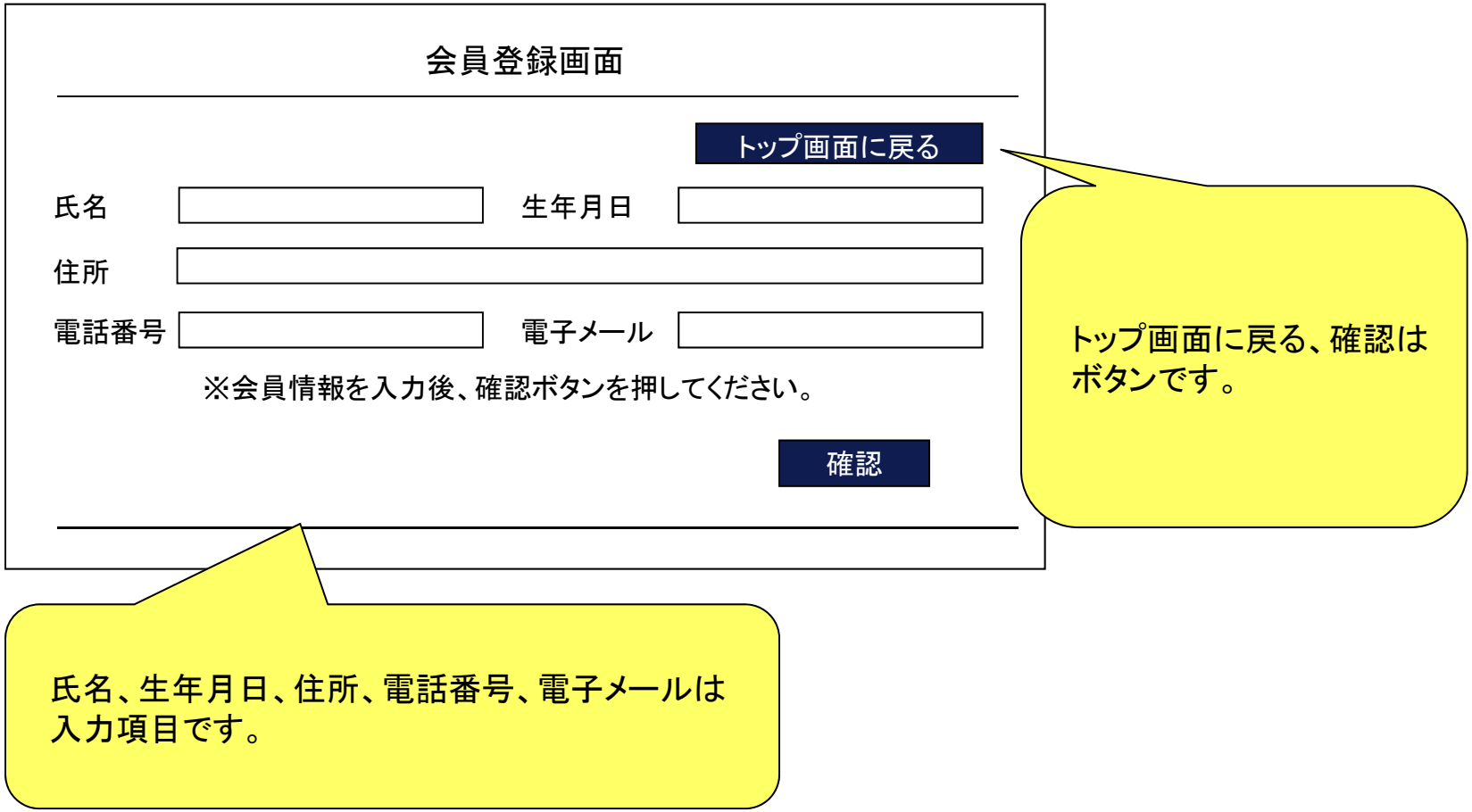
【例題】
会員管理システムの保証ケースを機能ごとに分解し、特性分解して作成してください。

～解答例～



2.2 主張の分解 ～再掲～

【演習】
会員管理システムの会員登録の信頼性リスクについて保証ケースをリスク分解パターンで作成してください。



2.2 主張の分解 ～再掲～

【演習】
会員管理システムの会員登録の信頼性リスクについて保証ケースをリスク分解パターンで作成してください。

【記入欄】

memo

memo

2.3 主張の階層的分解

目的

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。

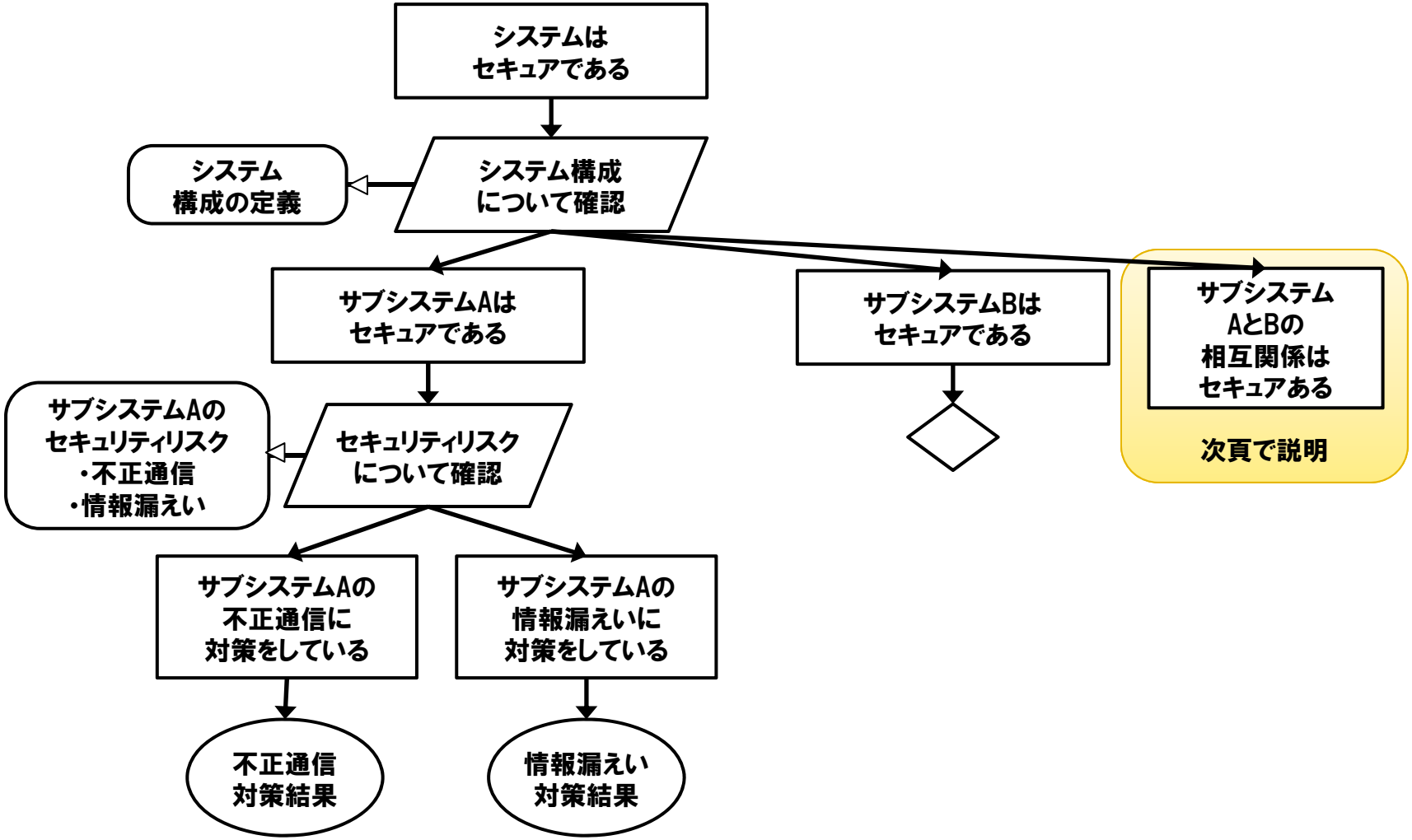
◆ **習得するスキル**

- **分解パターン（成果物分解、特性分解、リスク分解）を組み合わせた階層的分解について理解する。**

2.3 主張の階層的分解

保証ケースの分解パターンの「成果物分解パターン」、「特性分解パターン」、「リスク分解パターン」は組み合わせて利用することができます。システム構成について分解し、特性で分解し、更にリスクで分解しています。

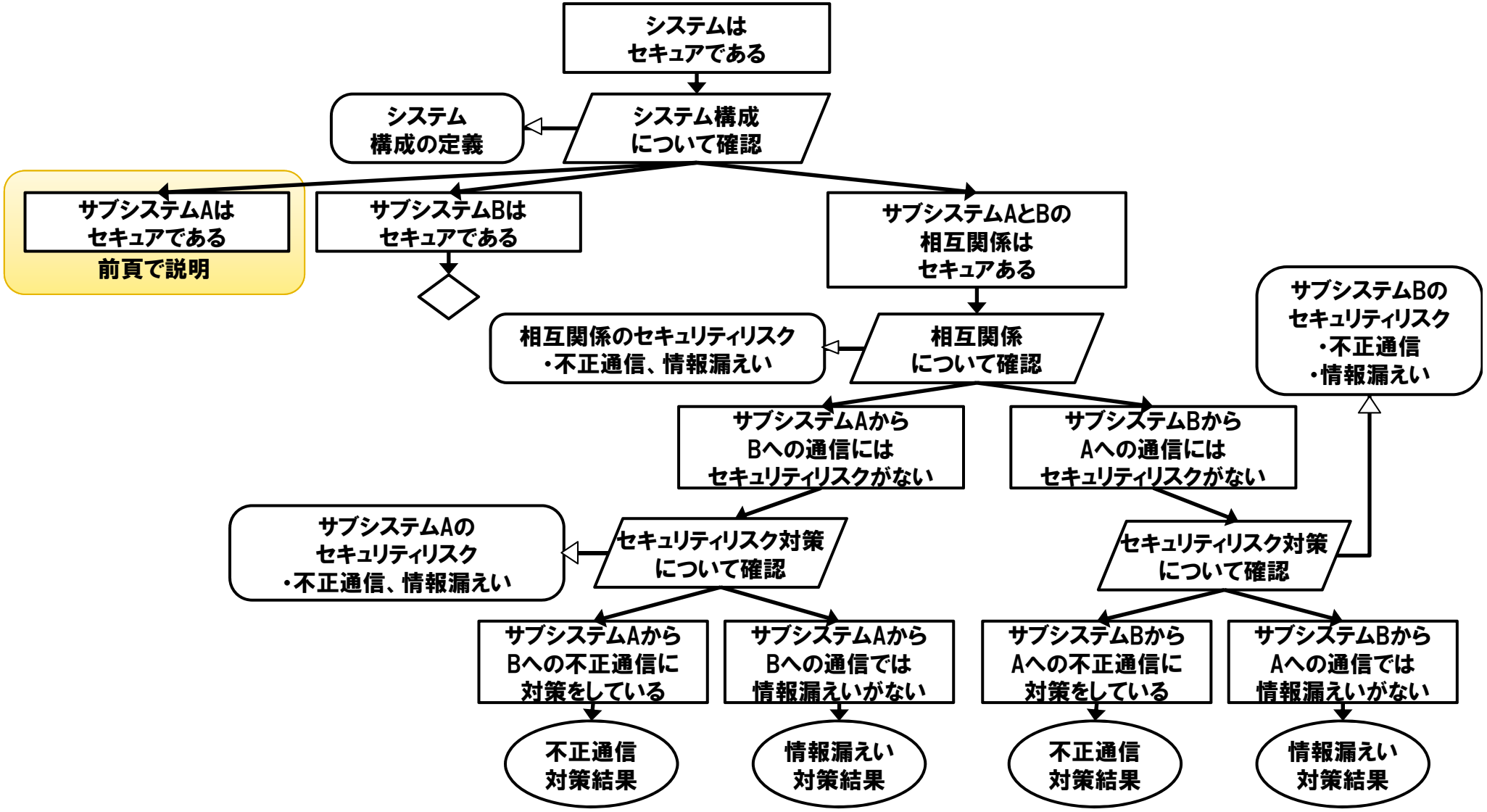
図5 分解パターンの組み合わせ



2.3 主張の階層的分解

サブシステム間の相互関係を分解した図が以下の通りです。

図5 分解パターンの組み合わせ



2.3 主張の階層的分解

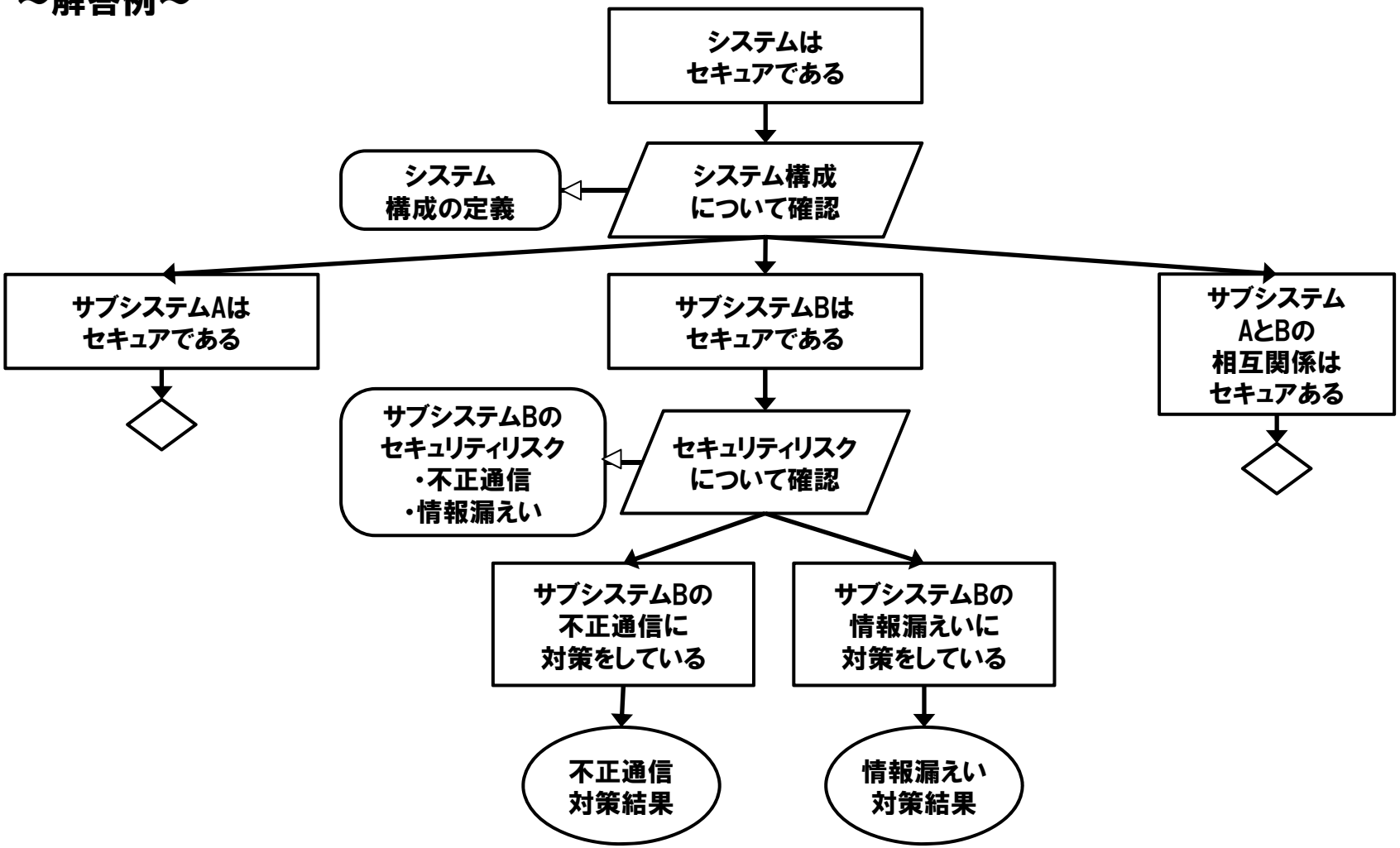
【例題】
サブシステムBがセキュアであることをシステム構成ごとに確認してください。

【記入欄】

【解答例】 2.3　主張の階層的分解

【例題】
サブシステムBがセキュアであることをシステム構成ごとに確認してください。

～解答例～



2.3 主張の階層的分解

【演習】
会員管理システムがセキュアであることを機能ごとに確認してください。

【記入欄】

memo

memo

2.4 分解の網羅性

目的

**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。**

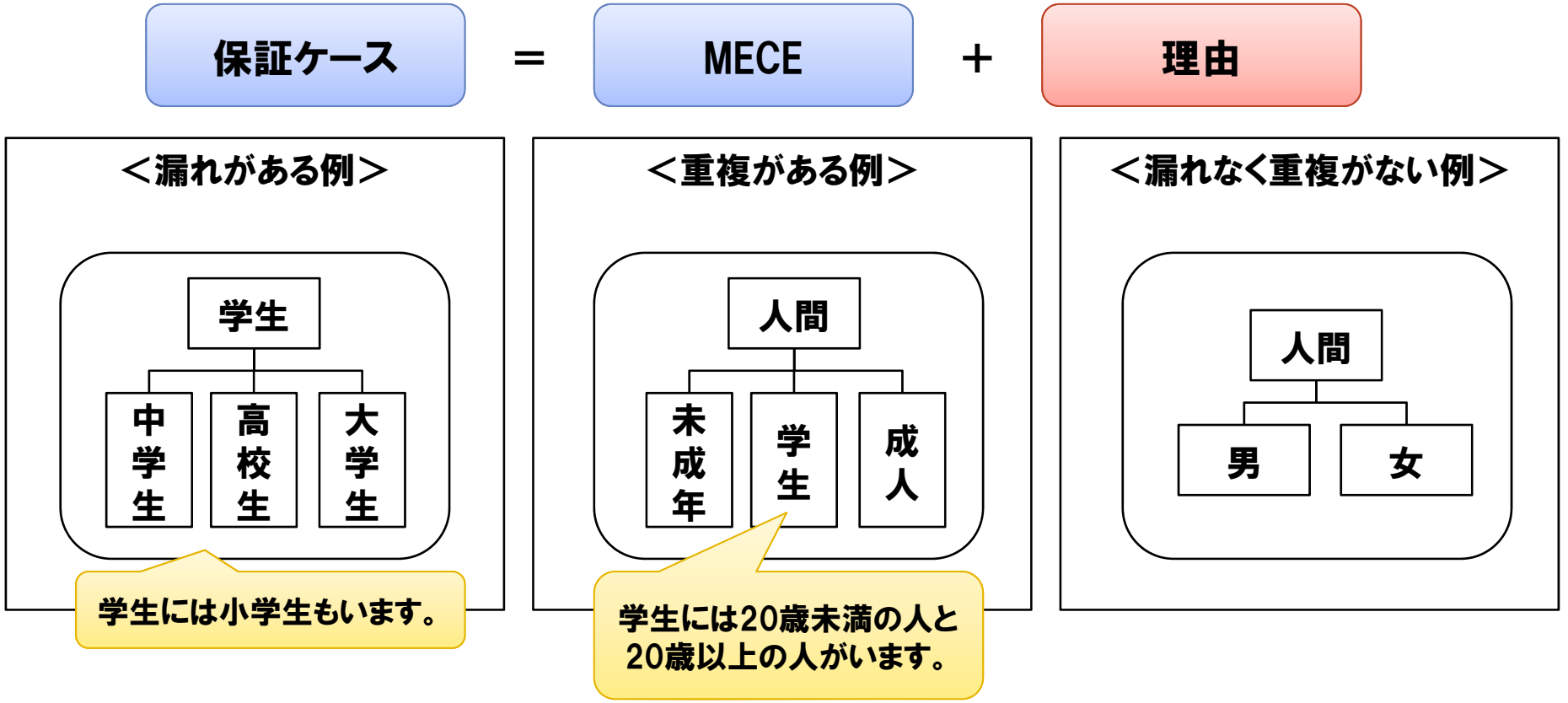
◆ **習得するスキル**

- **主張の分解の網羅性（完全性）とその理由を示す方法について理解する。**

2.4　分解の網羅性

保証ケースで主張を分解した場合、分解の網羅性(＝完全性)をコンテクストで保証します。また、網羅性(＝完全性)の理由もコンテクストで示します。この考え方は、MECEに理由を足したものとイメージしてください。

MECEとはロジカルシンキングで用いられる考え方です。Mutually Exclusive、Collecticely Exhaustiveの略で「全体として漏れがなく、重複もない漏れがなく、ダブりもない」という意味です。
これは保証ケースの網羅性(完全性)と同じ考えです。MECEにはその理由を明示的に示すことはないのですが、保証ケースでは理由を示すことが重要となっています。



2.4 分解の網羅性

【例題】
MECEとして正しい分解を考えてみましょう。

【問題】　　【記入欄】

①季節を分解してくだい。　[　　]
②日本の紙幣と貨幣を分解してください。　[　　]
③世界を分解してください。　[　　]
④通学手段を分解してください。　[　　]
⑤大学を分解してください。　[　　]
⑥以下の文章を読み、MECEとして正しいか否かを答えてください。
　正しくないと答えた場合には、ほかに考えられるシステムリスクについて書いてください。

システムのリスクは「前提条件が成立したリスク」と「想定した例外が発生したリスク」とがある。
［　正しい　・　正しくない　］
＜理由＞

【解答例】2.4　分解の網羅性

【例題】
MECEとして正しい分解を考えてみましょう。

【問題】　　【解答例】

①季節を分解してくだい。　　[春、夏、秋、冬]
②日本の紙幣と貨幣を分解してください。　　[1円,5円,10円,100円,500円,1000円,5000円,10000円]
③世界を分解してください。　　[ヨーロッパ、アジア、アメリカ、アフリカ、オセアニア]
④通学手段を分解してください。　　[自転車、徒歩、公共機関、車]
⑤大学を分解してください。　　[国立大学、公立大学、私立大学]
⑥以下の文章を読み、MECEとして正しいか否かを答えてください。
　正しくないと答えた場合には、ほかに考えられるシステムリスクについて書いてください。

システムのリスクは「前提条件が成立したリスク」と「想定した例外が発生したリスク」とがある。
[　正しい　・　正しくない　]
＜理由＞
他に、前提条件に対する想定外の逸脱が発生した場合のリスクがあります。

2.4 分解の網羅性

【演習】
あなたが出張を実施したことを適切に保証ケースで示してください。

【記入欄】

memo

2.5 主張の優先順位

目的

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。

◆ **習得するスキル**

- **主張の優先順位のつけ方について理解する。**

2.5　主張の優先順位

これまで主張の説明方法、その分解等について学習してきました。

しかし、2.4章 分解の網羅性で学んだように、主張を網羅的に分解すると膨大なリスクが出てきます。それら全てに対して対策をとることはもちろん重要ですが、システムを構築する場合にはコストに限りがあるため、全ての対策を行うことは難しいです。

その場合にはどのように対策するリスクを選択するのでしょうか？

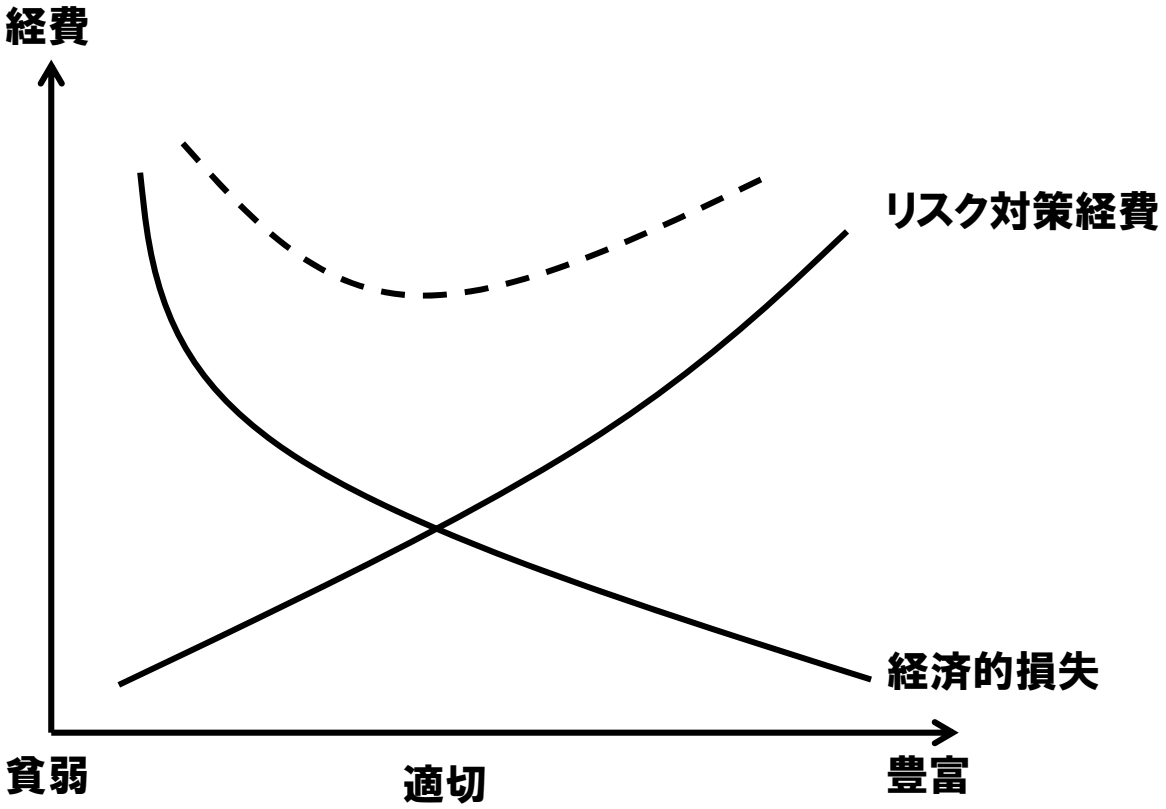
【優先順位のつけ方】

- 顧客要望やプロジェクトの状況に応じて決める
- リスクの影響が大きいものについて対応する
- リスクが起こる確率が大きいものについて対応する

そして、、、最後は自分で決めるのです！！

2.5 主張の優先順位

【例題】
以下はリスク対策の経済効果を図にしたものです。適切なリスク対策はどこなのか考えてみましょう。

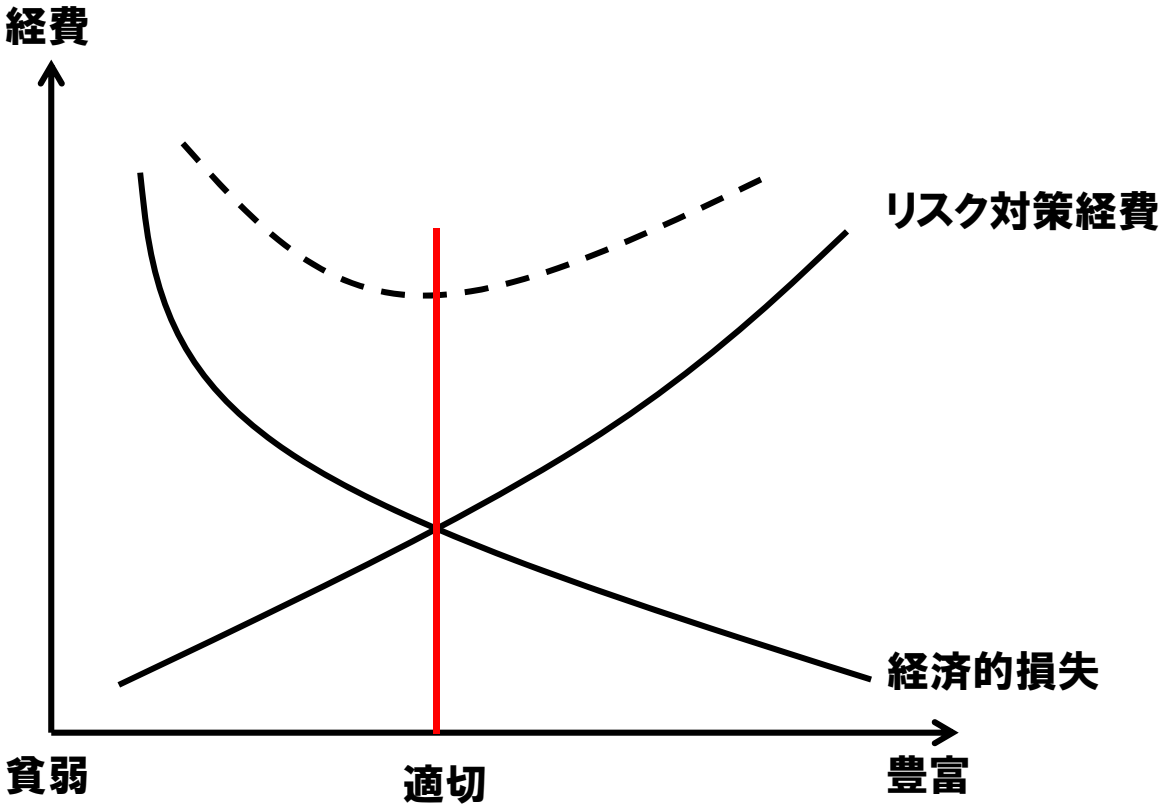


【適切なリスク対策について】

【解答例】 2.5　主張の優先順位

【例題】
以下はリスク対策の経済効果を図にしたものです。適切なリスク対策はどこなのか考えてみましょう。

～解答例～



【適切なリスク対策について】
リスク対策を行うには経費が必要です。貧弱な対策より豊富な対策のほうがより多くの経費がかかります。一方リスク対策を軽視すると経済的に大きな損失が発生してしまいます。適切なリスク対策を選択するためには、リスクを識別して、膨大な被害をもたらす可能性があるリスクに対して対策を用意したことを確認する必要があります。

2.5 主張の優先順位

【演習】
問題文を読み、あなたはどちらを優先させるかとその理由について考えてみましょう。

ホテルYは日本全国でビジネスホテルを中心に設立、運営している会社です。

ホテルYでは宿泊予約システムや会員管理システムを導入してから数年が経っているため、システムの見直しを行うことにしました。

（あなたはシステム開発の依頼を受けている会社の社員で、この案件のプロジェクトのリーダを任されました。そこで、どのようなシステムにするか検討するため、依頼元のホテルYの経理部の部長と実際にシステムを利用しているオペレータにヒアリングしました。）

経理部の部長：

「先日、競合ホテルの東京ホテルグループの会員システムがハッキングされ個人情報が盗まれるという話があった。うちは元々セキュリティにはお金をかけているが、東京ホテルグループのように狙われる可能性があるので、もっとセキュリティ機能を強化したい。」

オペレータ：

「システムはどれもスピードが遅くて困っている。先日も、電話で操作をお願いされているときに待たせてしまい怒らせてしまい、結局、別のホテルに宿泊すると断られてしまった。ビジネスチャンスを逃さないためにももっと性能を上げて欲しい。」

memo

2.6 統一的な保証ケース

目的

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。

◆ **習得するスキル**

- **これまで1章、2章で学んだことを復習する。**

2.6 統一的な保証ケース

これまでの学習したことをまとめます。

章	目的	概要
1.1 システムの構成	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。
1.2 システムのリスク	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。
1.3 システムの特性	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。
1.4 保証ケースの表記法	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。
1.5 主張の分解	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。
1.6 リスク対策の証拠	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

2.6 統一的な保証ケース

これまでの学習したことをまとめます。

章	目的	概要
2.1 モデルの定義	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。
2.2 主張の分解	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。
2.3 主張の階層的分解	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。
2.4 分解の網羅性	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
2.5 主張の優先順位	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

2.6 統一的な保証ケース

【例題】
年金機構の情報漏えいについて読み、どんなリスク対策が必要かを考えてみましょう。

特集：年金の個人情報流出

今回の攻撃は5月8日に始まった。職員がパソコンに届いた電子メールに添付されたファイルを開くと、パソコンがウィルスに感染して外部に個人情報を送り始めた。政府機関への不正アクセスを検知する「内閣サイバーセキュリティセンター（NISC）」が、この日のうちに不正アクセスと気づき、機構や厚生労働省に知らせた。

機構などによると、不正アクセスで流出したとみられるのは「情報系システム」に入っていた基礎年金番号、氏名、生年月日、住所の4種類の個人情報。このシステムは年金記録を管理する「社会保険オンラインシステム」とは分離され、年金受給者や加入者に年金関係の通知を郵送するときに使われていた。

職員のパソコンとはLAN（ローカルエリア・ネットワーク）で結ばれ、アクセス権限を持つ職員が見ることができる。作業がやりやすいように、情報をパソコンにダウンロードしてファイルで保存することも認められている。ファイルに保存する場合には原則としてパスワードをかける内規があるが、今回流出した約125万件のうち、4割強にあたる約55万件はパスワードがかかっていなかった。

出典：年金情報、ダウンロードした職員PCから流出か、朝日新聞、2015.6.3

2.6 統一的な保証ケース

【例題】
年金機構の情報漏えいについて読み、どんなリスク対策が必要かを考えてみましょう（続き）。

特集：年金の個人情報流出

情報セキュリティー会社「S&J」の三輪信雄社長は「インターネットに接続された端末で個人情報を扱うなど論外だ。基幹システムをネットワークから切り離した意味がなく、大事な情報を取り扱う公的機関としてはまったく不十分だ」と指摘する。

日本年金機構は今回の問題を受けて専用の電話窓口「0120-818211」を設けた。受け付けは、14日までの午前8時半～午後9時。ほかに全国に312カ所ある年金事務所でも自分の情報が漏れたかどうか確認できるという。

出典：年金情報、ダウンロードした職員PCから流出か、朝日新聞、2015.6.3

2.6 統一的な保証ケース

【例題】
年金機構の情報漏えいについて読み、どんなリスク対策が必要かを考えてみましょう(続き)。

特集:年金機構防御訓練せず　標的型メール、防御意識低く、

職員への標的型メールで約125万件もの年金加入者情報が流出した日本年金機構が、2010年の発足以来、標的型メールを想定した職員の模擬訓練を一度も実施していなかったことが機構関係者への取材で分かった。また、サーバー攻撃にたいする機構の防御意識の低さが年金加入者情報の流出を招いた可能性が高まった。【岸　達也】

◇マニュアル12年のまま

政府機関へのサイバー攻撃対応の司令塔「内閣サイバーセキュリティセンター(NISC)」によると、11年に衆参両議院や防御大手、三菱重工業を狙った標的型メール攻撃が相次いで発覚したため、NISCは11～13年度にそれぞれ、中央省庁や省庁が参加要請した特殊法人の職員らを対象に模擬訓練を実施した。標的型メールについて説明したうえで、無害なメールを実際に職員に送りつけ、開封するか否かをテスト。開封した職員には不審なメールを開封しないよう求めた。

11年度に6万人だった参加者は12年度に12万人、13年度に18万人と増え、13年度はほとんどの主要官庁を含む18府省庁が参加した。そのあと多くの省庁は独自訓練しているという。

出典:岸達也、年金機構防御訓練せず　標的型メール、防御意識低く、毎日新聞、2015.6.17

2.6 統一的な保証ケース

【例題】
年金機構の情報漏えいについて読み、どんなリスク対策が必要かを考えてみましょう(続き)。

特集:年金機構防御訓練せず　標的型メール、防御意識低く、

関係者によると、厚生労働省はNISCの訓練に参加したが、日本年金機構には参加を求めなかった。厚労省は訓練を巡る毎日新聞の取材に応じておらず、理由は不明だ。　機構幹部は独自の訓練を含め一度も訓練をしていないことを認めている。

また、機構によると、機構の年金事業は厚労省の委託のため、サイバー攻撃を受けた際のマニュアル「情報セキュリティポリシー」も厚労省のマニュアルに準拠している。機構は13年8月にマニュアルを改訂したが、これは厚労省の12年時点のマニュアルを反映させたものという。

機構は「マニュアルの内容は秘密だが標的型メールを想定した内容もあった。今回もマニュアルに沿った措置をとった」としている。しかし、実際には大量の情報が流出した。進化し続けている標的型メールを使ったサイバー攻撃に対し、機構のマニュアルが対応してなかった可能性が」ある。

情報セキュリティー会社「ラック」の西本逸郎・最高技術責任者は「模擬訓練を繰り返してもウィルス感染を100%防ぐことはできないが、職員の意識は確実に向上する。大量の個人情報を扱っている機構は訓練すべきだった。機構の対応は後手に回って被害が深刻化しており、マニュアルは検証が必要だ。政府主導で特殊法人を含めてサイバーセキュリティーを再チェックすべきだ」と話している。

出典:岸達也、年金機構防御訓練せず　標的型メール、防御意識低く、毎日新聞、2015.6.17

memo

2.6 統一的な保証ケース

【演習】年金機構の情報漏えい対策の適切性について保証ケースを作成してください。

【記入欄】

memo

第3章　保証ケースの合意形成

3.1　議論の合意形成

3.1　議論の合意形成

目的

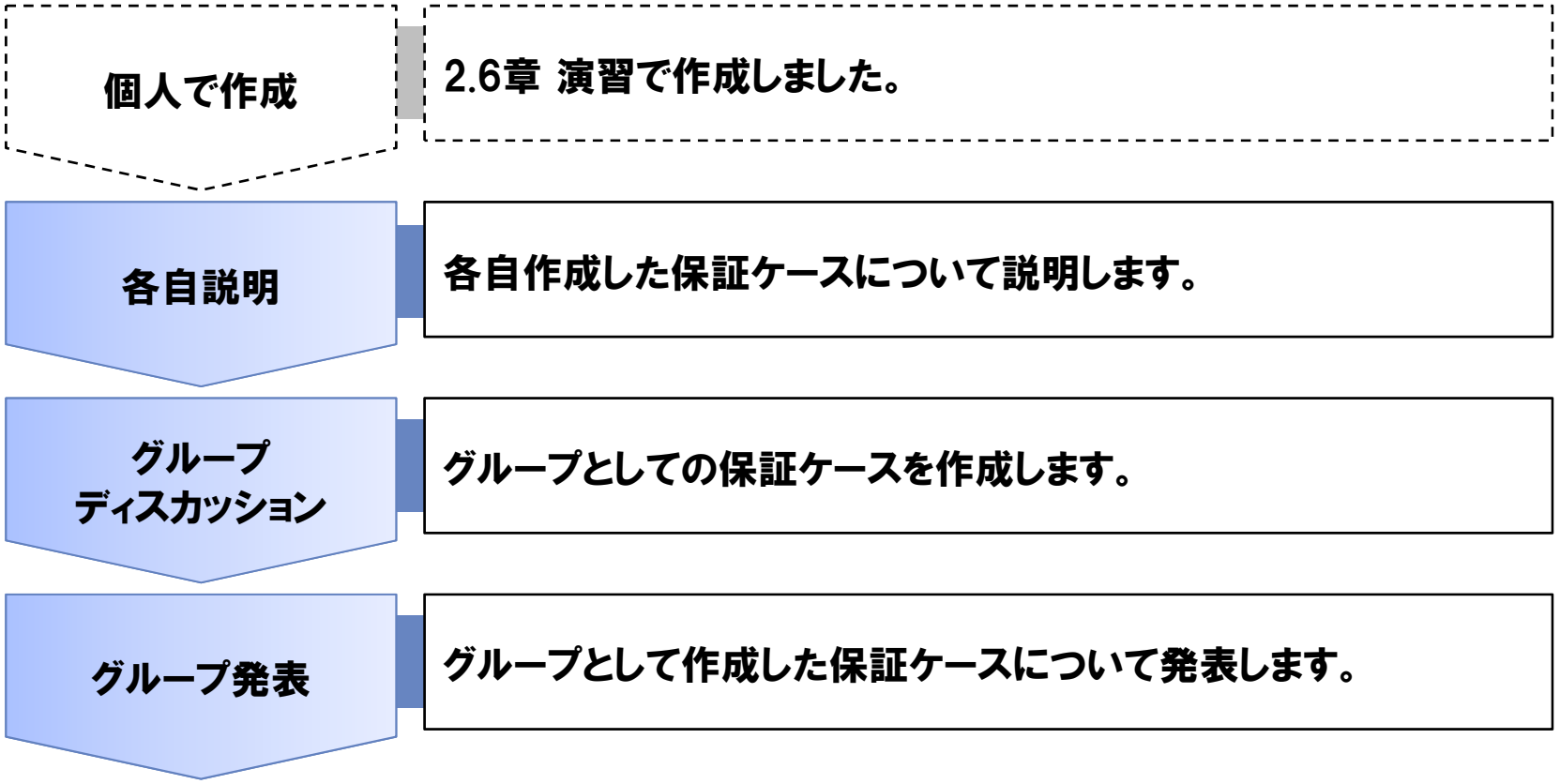
**統一的な保証ケースを複数人で議論することにより
合意形成できるスキルを習得する。**

◆　**習得するスキル**

- **グループで保証ケースを作成するスキルについて身につける。**

3.1 議論の合意形成

2.6 演習についてグループでディスカッションし、グループとしての保証ケースを作成してください。
進め方は以下の通りです。



3.1 議論の合意形成

【演習】年金機構の情報漏えい対策の適切性について保証ケースを作成してください。

【記入欄】

memo

memo