発表資料

システム可用性を考慮した ハザード対策検討手法の提案

国立研究開発法人　宇宙航空研究開発機構

発表者：髙附翔馬

共著者：梅田浩貴　佐々木貴広　植田泰士

e-mail：takatsuki.shohma@jaxa.jp

本発表のターゲット

- ハザード対策の検討方法に関心がある方
- 搭載機器の増加（機器冗長化等）が不可なシステム（※）の可用性向上の取り組みに関心がある方

  ※小型のため最小限の機器しか搭載不可なシステム等

  例：無人の深海探査機
- 宇宙機システムの開発で起きた課題への取り組み事例に関心がある方

本発表の概要

課題

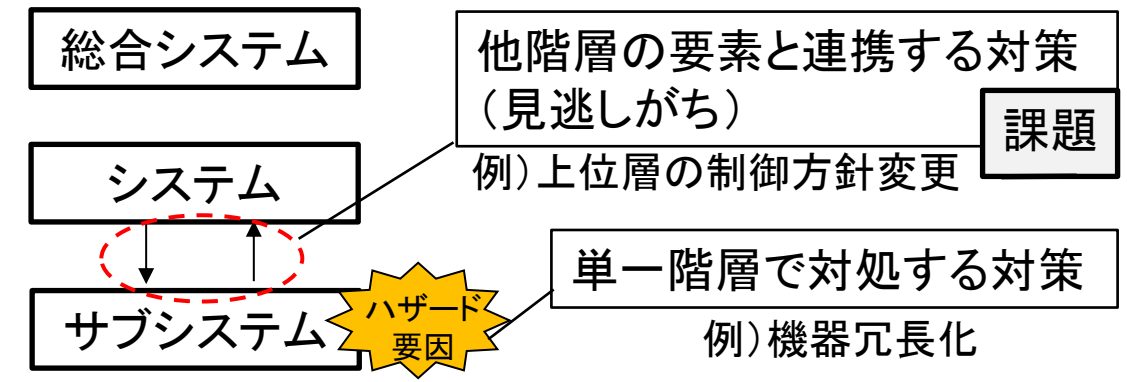
ハザード要因発生後に、ミッション継続可能にする対策において、他階層の要素と連携する対策を見逃しがち

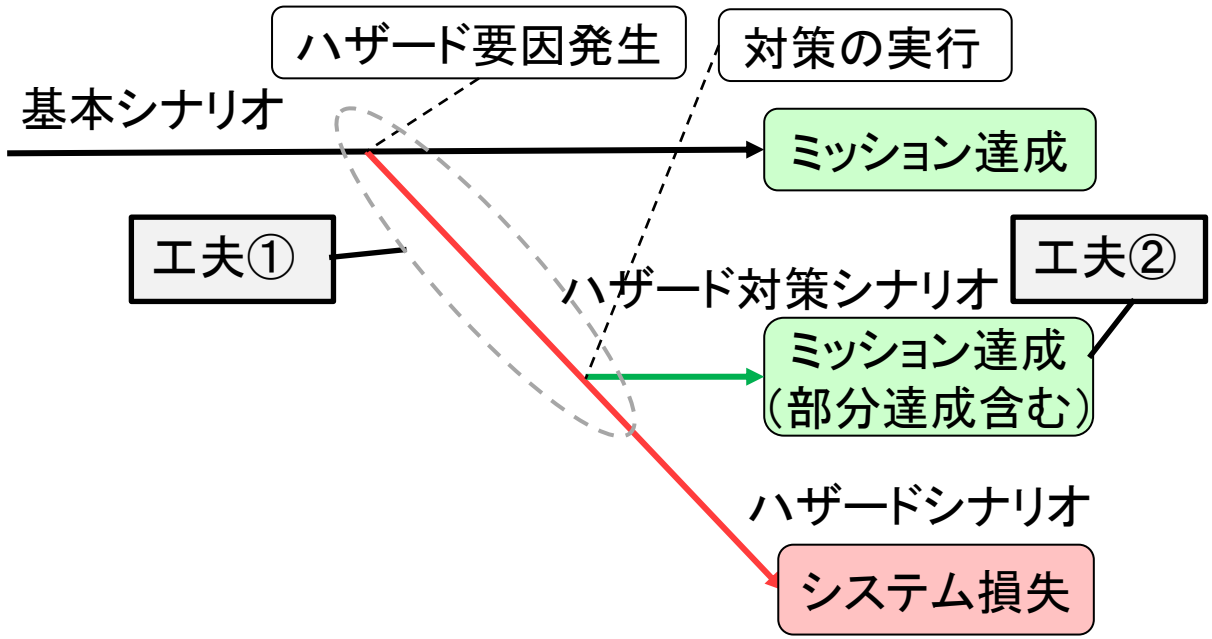
工夫

ハザード対策の検討時に
①対策時の前提を明確化
②ミッションを分割し部分達成条件を明確化

効果

実際のシステムのミッション達成度を向上する検討へ貢献





目次

- 背景（前提知識等）
  - 宇宙機システムの特徴とソフトウェアの品質
  - 一般的な安全解析手法
  - 安全解析手法を用いたハザード対策の検討方法
  - 宇宙機システムにおけるハザード対策の検討の特徴
  - 取り扱うシステムの特性
  - 課題
- 提案手法の説明
- 提案手法の有効性確認
  - 方法
  - 結果
  - 得られた効果
- まとめ

宇宙機システムの特徴とソフトウェアに求められる品質

宇宙機システムの特徴

- システム故障時の損失：大
  - 環境や人命の喪失の可能性あり
  - 損失するコスト：大
- システム故障の対応や復帰の難易度：高
  - 地球との通信は限られた期間のみ
  - 部品交換不可
- システム故障の対策の難易度：高
  - 想定外が発生しやすい
    - 動作環境が過酷（放射線によるメモリ化け発生等）
    - 過去の知見：少
      - 5年以上の長い開発期間
      - 少量多品種（研究実証向け）
  - 想定内でも実環境の試験不可

ソフトウェアに求められる品質：非常に高い

システム特性に応じた安全解析による
設計検証や試験が重要

宇宙機システムの例

人工衛星

宇宙ステーション

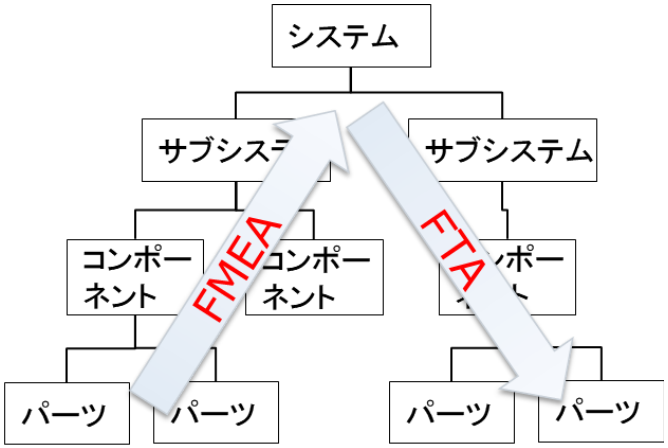
ロケット

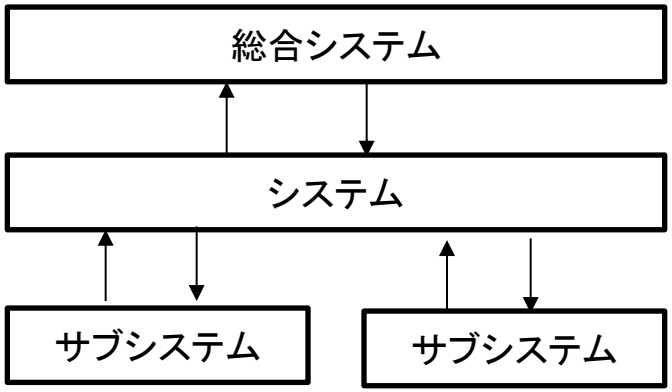
地上管制局

一般的な安全解析手法

主にハードウェア自体の故障をシステム故障の要因として分析するFTAやFMEA
ソフトウェアや人を含むコントローラの相互作用を要因として分析するSTAMP/STPA

手法	FTA、FMEA	STAMP/STPA
システム故障の要因	システム構成要素の故障	システム構成要素の相互作用（認識の齟齬など）
故障要因としてモデル化可能な構成要素	ハードウェア	ハードウェア、ソフトウェア、人など





・トップダウンアプローチ
FTA（事象から原因推定）

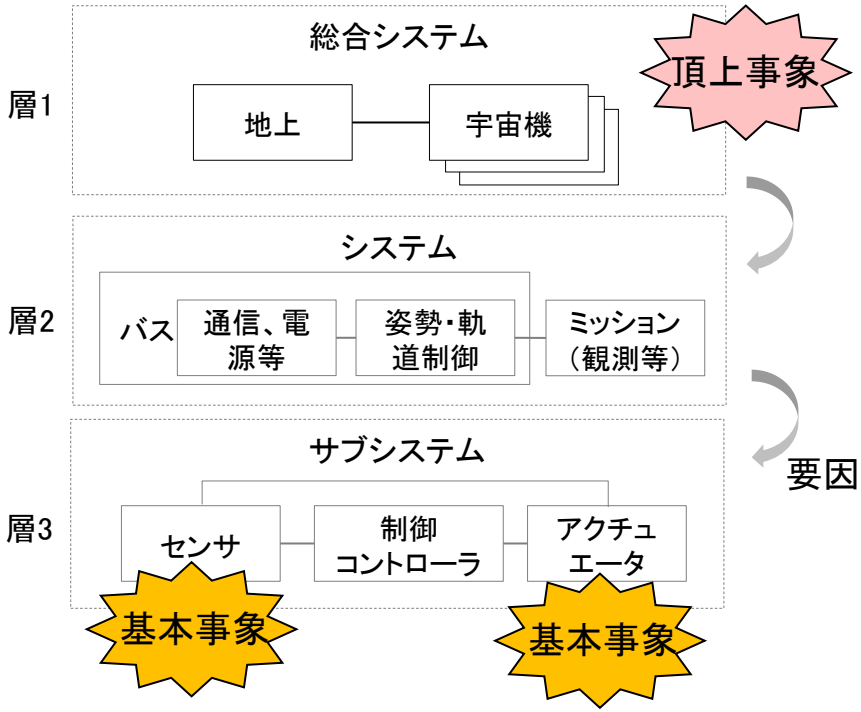
・ボトムアップアプローチ
FMEA（構成要素の状態から影響分析）

耐故障対策（ハザード対策）の検討方法：FTA

頂上事象を 時系列 や アーキテクチャ階層 で分解して
機器レベルの異常や故障として基本事象を導出し、対策を検討

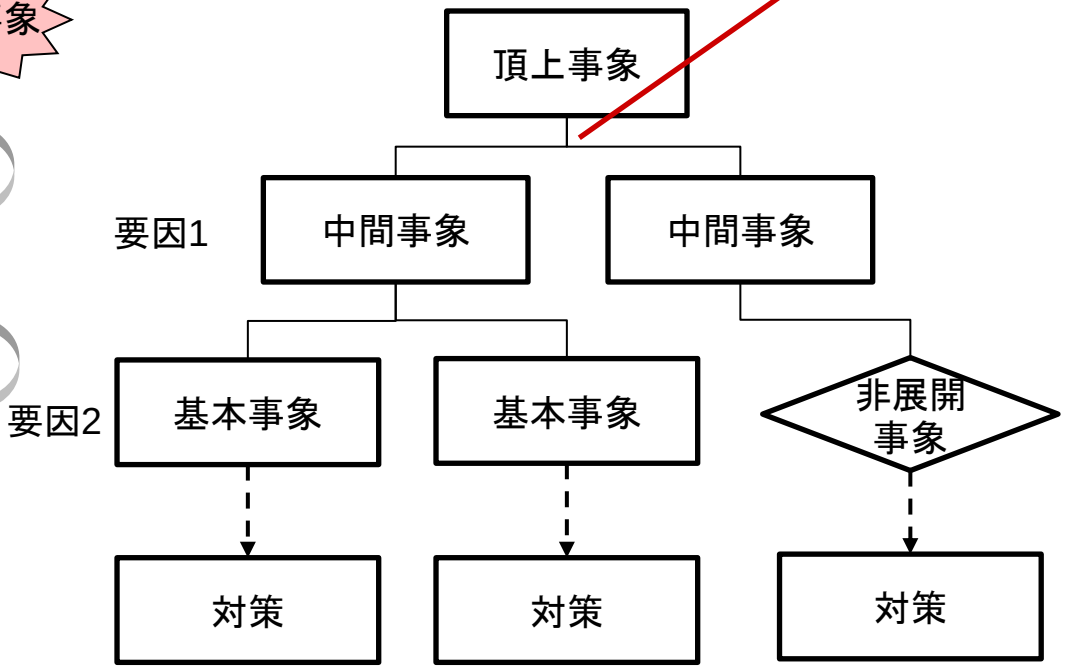
ハザードシナリオ

システム階層と分析の流れ



原因の展開パターン
①：時系列（順序）の分解
②：アーキテクチャ（構成要素＝名詞）や状態（形容詞）による分解

故障木解析（FTA）

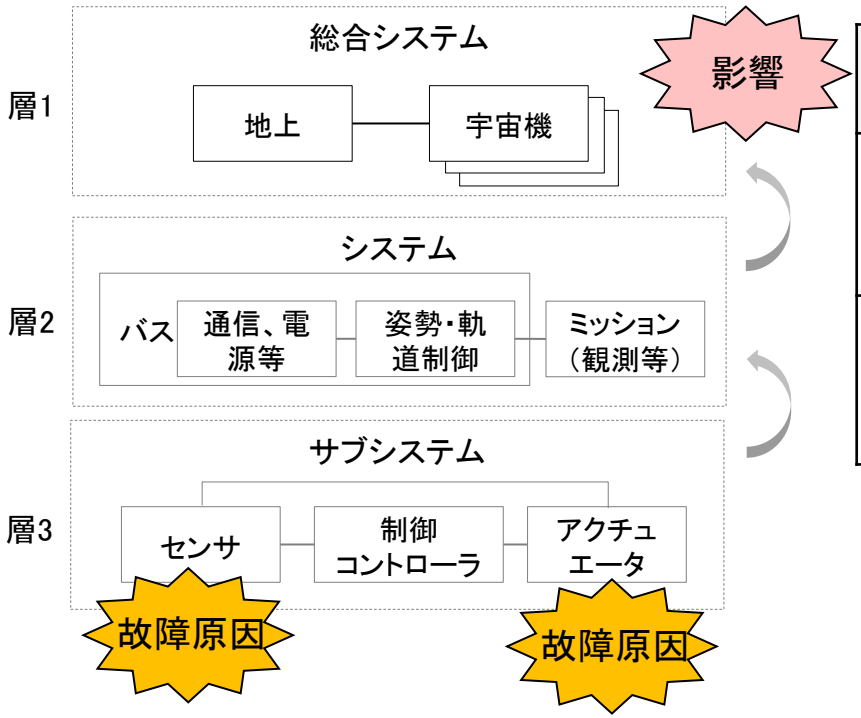


耐故障対策（ハザード対策）の検討方法：FMEA

システム構成要素の異常パターン（故障モード）がどんな原因で起こり
上位システムへ影響するか分析し、対策を検討

ハザードシナリオ

システム階層と分析の流れ



故障の影響解析（FMEA）

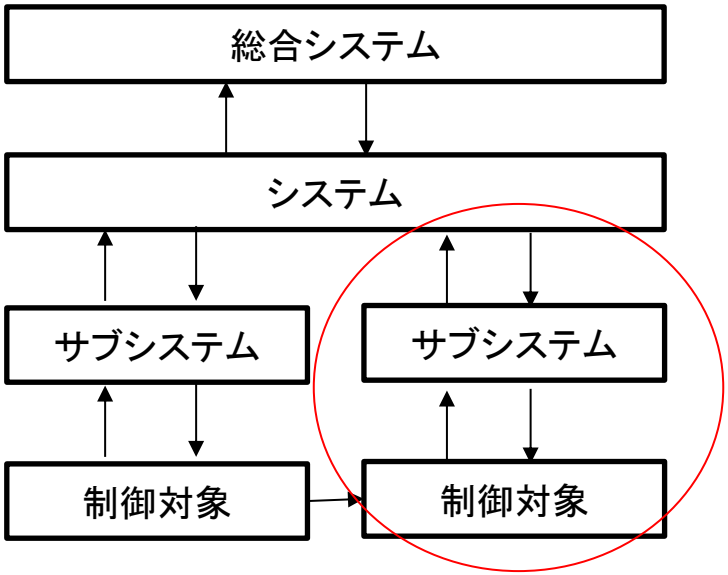
構成要素	故障モード	故障原因	影響	対策
観測機器	出力異常	太陽の視野干渉	データ取得不可	別角度の機器を設置（冗長化）
スラスタ	推力が出ない	バルブが閉故障	観測姿勢になれない	機器の信頼性向上

耐故障対策（ハザード対策）の検討方法：STAMP/STPA

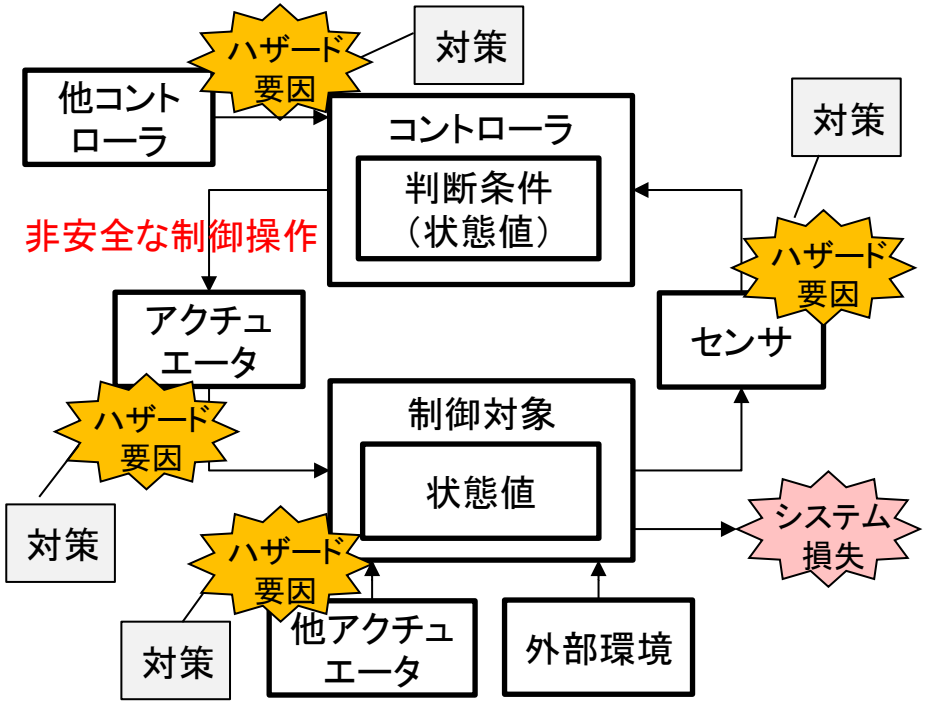
システム構成要素間の相互作用に着目し、
「コントローラがシステムの状態値を誤認し、非安全な制御操作を行う」
要因（ハザード要因）を制御ループを遡って特定し、対策を検討

ハザードシナリオ

制御構造のイメージ



制御ループによるハザード要因解析（STPA）



宇宙機システムにおける耐故障対策（ハザード対策）の検討の特徴

安全確保とミッション継続が確実な空間冗長（機器冗長、機能冗長等）を第一に考えるが、資金やシステムリソース（電力、質量等）の制約から対策範囲に限界あり。
それらの制約のもと、システム全体として可用性（ミッション継続性）を向上するためには、空間冗長以外の対策も手段の候補として設計検討することが重要！

ハザード要因に対する対策の検討例

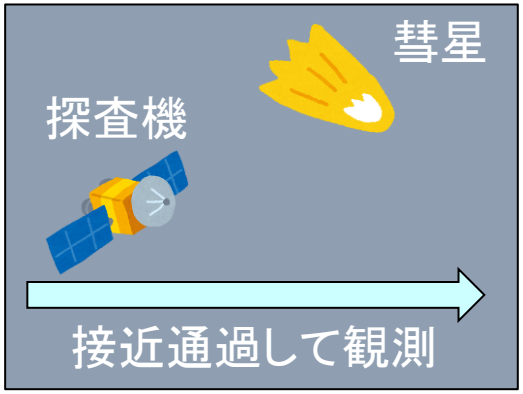
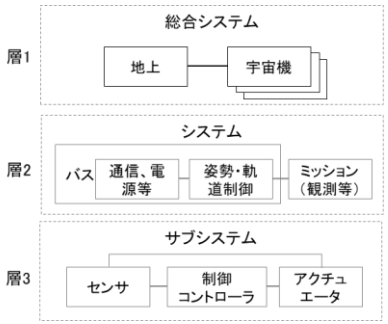
<システムリソース制約>
重量制限から空間冗長は1か所のみ

No	ハザード要因	システム構成要素	対策種別	空間冗長のみ検討		空間冗長以外も検討	
				採用する対策	ミッション継続可否	採用する対策	ミッション継続可否
1	機器Aの故障	機器A	空間冗長	○	○	○	○
			非空間冗長	N/A		×	
2	機器Bの故障	機器B	空間冗長	×	×	×	○
			非空間冗長	N/A		○	

ハザード要因発生時の個々の文脈を考慮することで、「他階層の要素と連携して対処する」等の非空間冗長の対策も検討することにより、システム可用性（ミッション継続性）が向上する場合がある

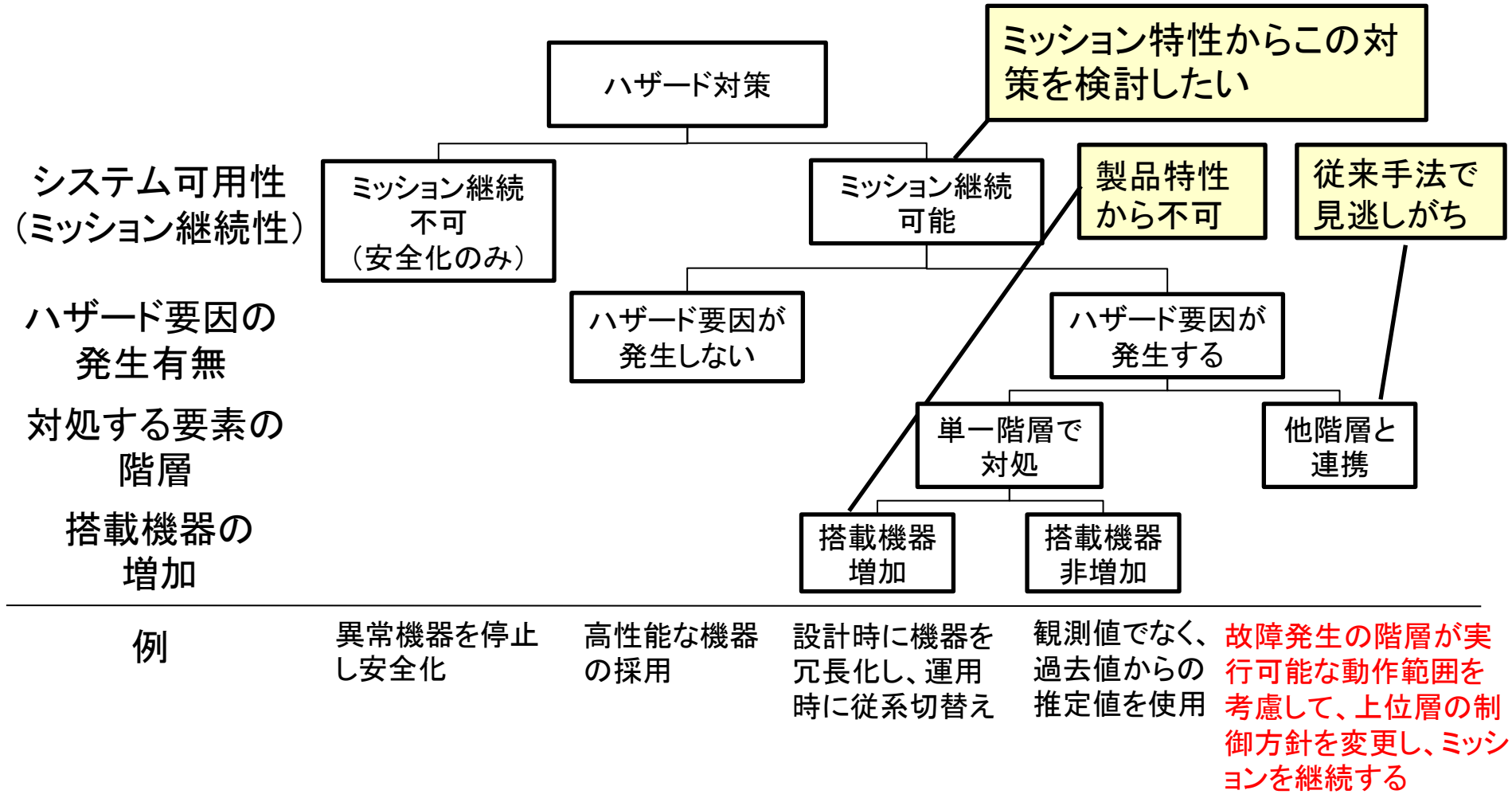
取り扱うシステムの特性

リトライ不可な 複数のミッションを同時に行う システム構造が階層化された
小型の 探査機システム（例：彗星探査機システム）
->搭載機器が増加しない手段でシステム可用性（ミッション継続性）を高めたい

分類	イメージ	特性	システム要求/制約
ミッション特性		チャンスは1度だけ（リトライ不可） 複数のミッションを同時実行	システム可用性（ミッション継続性）を可能な限り高めたい 姿勢制御の要求が厳しい 電力に余裕がない
製品特性		小型機	搭載機器は最小限（搭載機器増加を伴う空間冗長化の余裕なし）
アーキテクチャ特性		システム構造が階層化	目的（ミッションや安全）に対して構成要素の最適な役割分担を決定したい

発生した課題

従来実施していた安全解析手法を用いたハザード対策の検討方法では
ハザード要因の発生後に、他階層の要素と連携して
ミッションを継続可能にする対策の導出が難しい



どうして課題が発生したか？

従来のハザード対策の検討で用いた安全解析手法は、
システム故障の原因探索や機器故障の影響分析を目的とした手法であるため、
システム可用性を高める検討が難しい（単一階層内の冗長化になりがち）

【課題】
ハザード要因の発生後に
他階層の要素と連携して
ミッションを継続可能にする
対策の検討が難しい

手段：対策時の状況（環境条件や他要素の状態等）を特定することが難しい（何ができるかがわらない）

目的：ミッションの部分達成の定義が難しい（どんな状態にすればよいかわからない）

・FTAとSTAMP/STPA
システム故障の原因を探索する手法のため
・FMEA
異常発生の影響を分析する手法のため

提案手法のアイデア

対策検討の前提（文脈） と ミッションの部分達成条件 を明確化することで
課題解決を狙う

【課題】
ハザード要因の発生後に
他階層の要素と連携して
ミッションを継続可能にする
対策の検討が難しい

手段
対策時の状況（環境条件や他要素の状態等）を特定することが難しい
（何ができるかがわらない）

【解決策①】
対策検討の前提（文脈）を明確化

目的
ミッションの部分達成の定義が難しい
（どんな状態にすればよいかわからない）

【解決策②】
ミッションの部分達成条件を明確化

・FTAとSTAMP/STPA
システム故障の原因を探索する手法のため
・FMEA
異常発生の影響を分析する手法のため

提案手法の概要

運用目的や外部要素による制約（性能低下含む）の観点でシナリオを分割
　->対策検討の前提（文脈）を明確化
ガイドワードによってミッション達成状態を分割
　->ミッションの部分達成条件を明確化

解決策と工夫

【解決策①】
対策検討の前提（文脈）を明確化

【工夫①】
運用目的や外部要素による制約（性能低下含む）の観点でシナリオを分割

【解決策②】
ミッションの部分達成条件を明確化

【工夫②】
ガイドワードによってミッション達成状態を分割

手法工程

ミッション、システム構成要素、基本シナリオを定義

↓

コンポーネントやシステム間の制約（性能低下含む）を定義

↓

各制約発生がシステム損失に影響するか検討
（ハザードシナリオの定義）

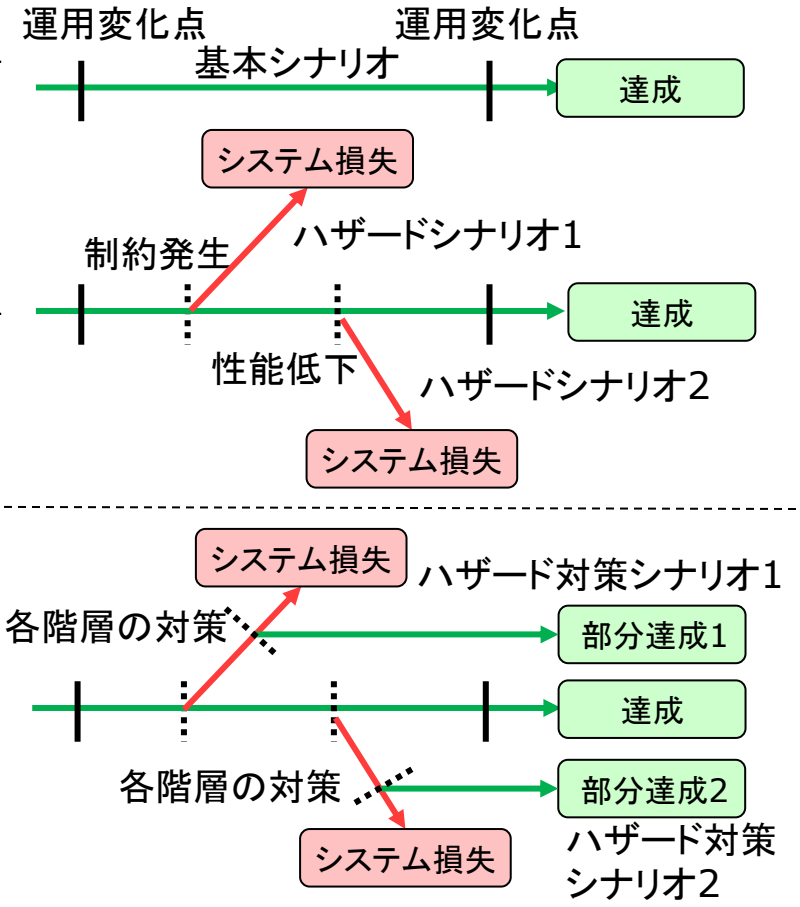
↓

ミッション達成状態を分割し、部分達成条件を抽出

↓

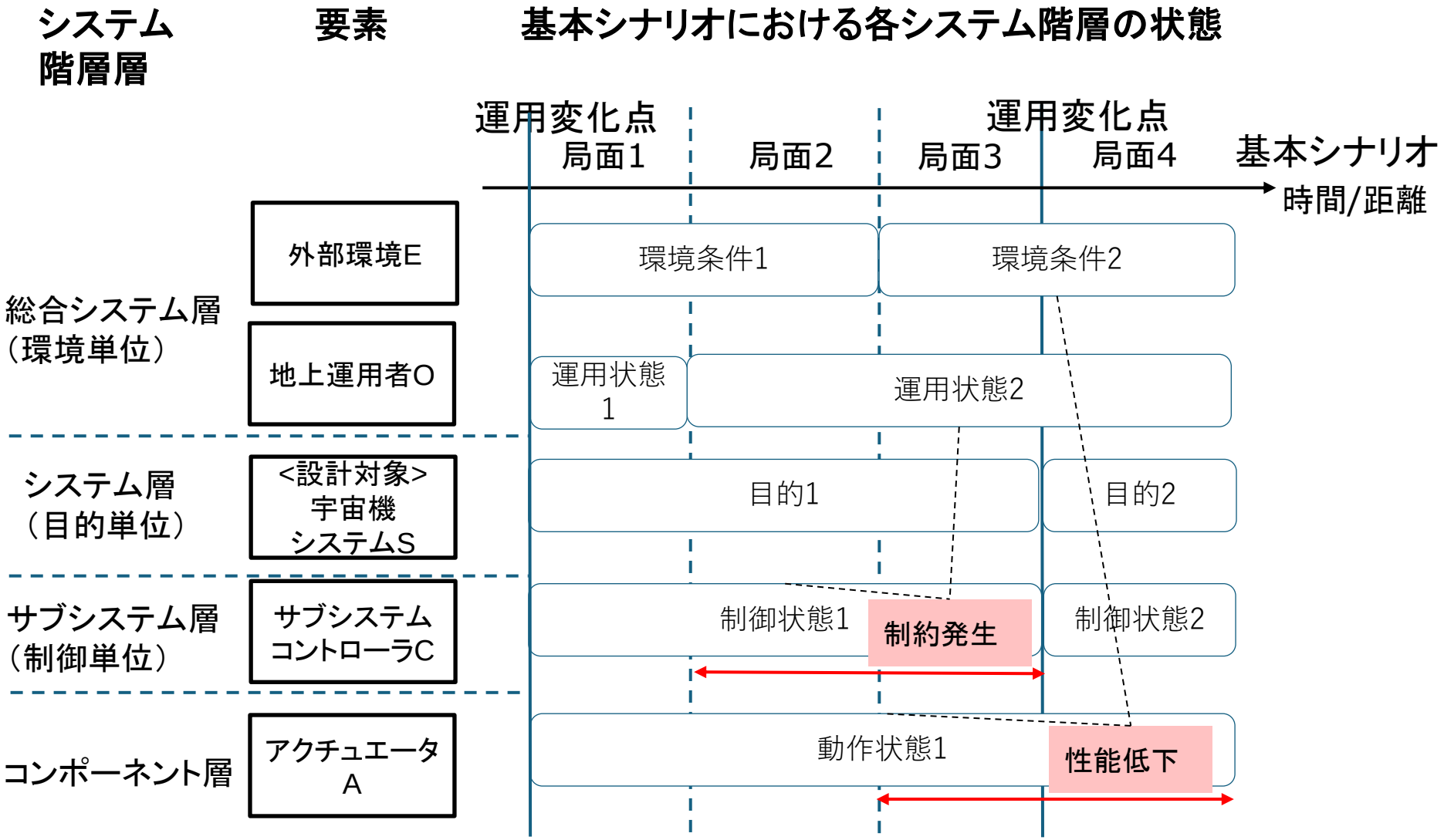
各システム階層でミッション達成（部分達成含む）を可能にする対策を検討
（ハザード対策シナリオの導出）

ハザード対策シナリオの導出イメージ



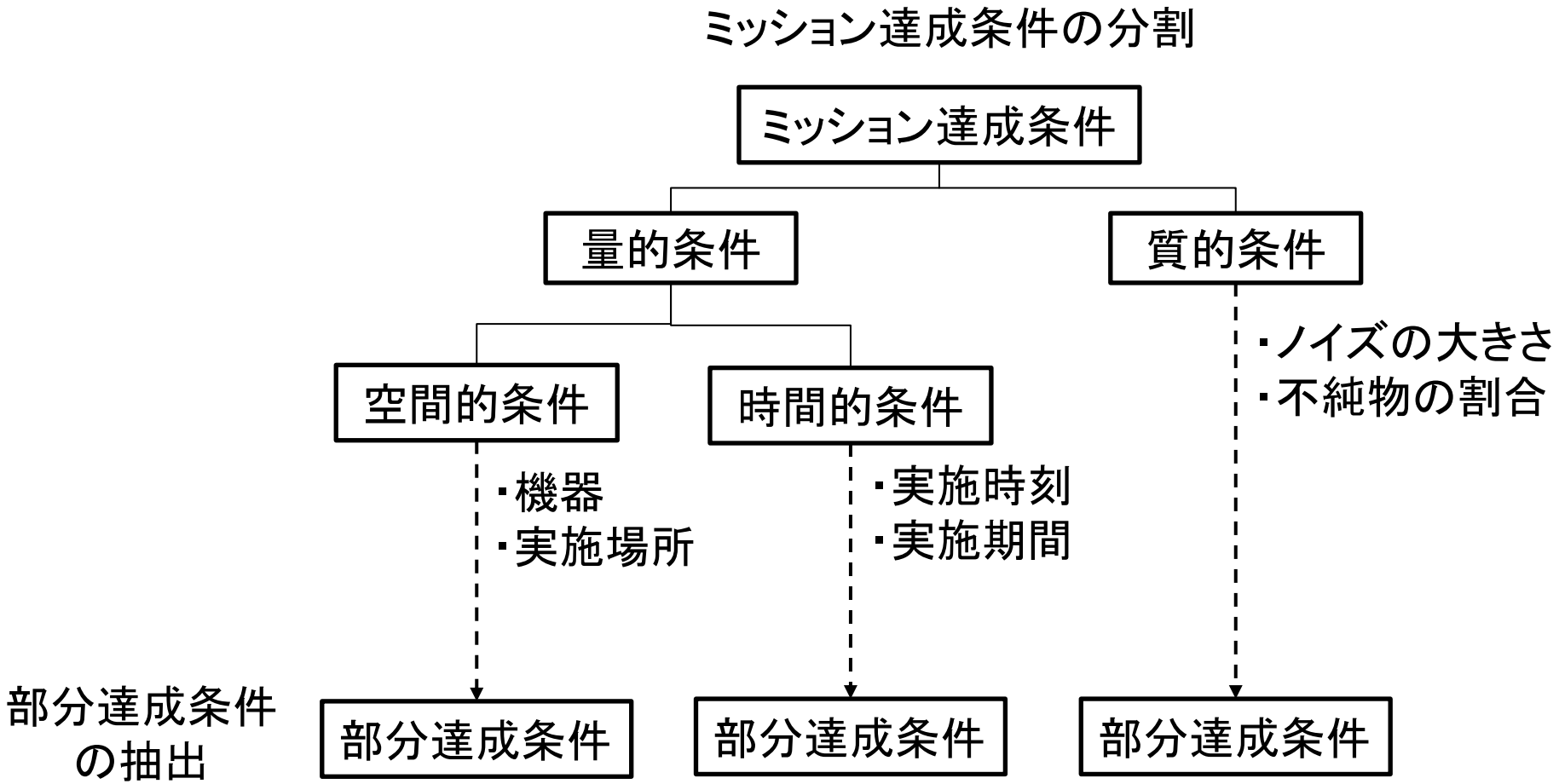
提案手法の詳細(1/3)

運用目的や外部要素による制約(性能低下含む)の観点でシナリオを分割
->対策検討の前提(文脈)を明確化



提案手法の詳細(2/3)

ガイドワードによってミッション達成状態を分割することで
ミッションの部分達成条件を明確化

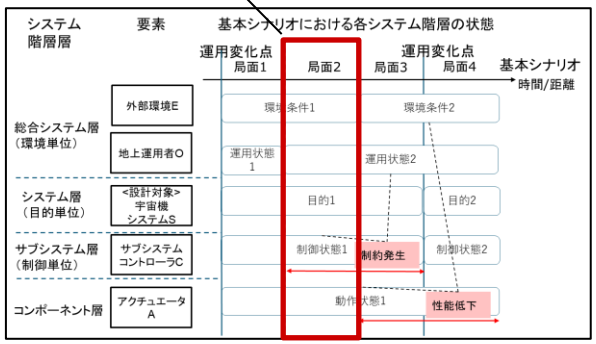


提案手法の詳細(3/3)

シナリオ分割して定義した局面と従来の安全解析手法の成果物から
定義したハザードシナリオに対して
システム階層別にミッションの部分達成条件を満たす
対策(ハザード対策シナリオ)を検討する

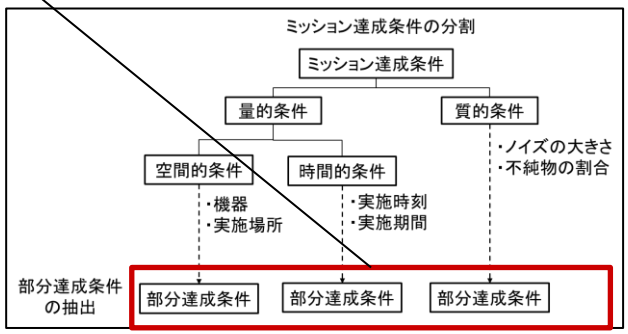
ハザード対策シナリオの導出

ハザードシナリオ			システム階層別対策		
局面	ハザード要因	システムへの影響	上位対策	同位対策	下位対策
			対策と達成する部分達成条件		



シナリオ分割して定義した局面

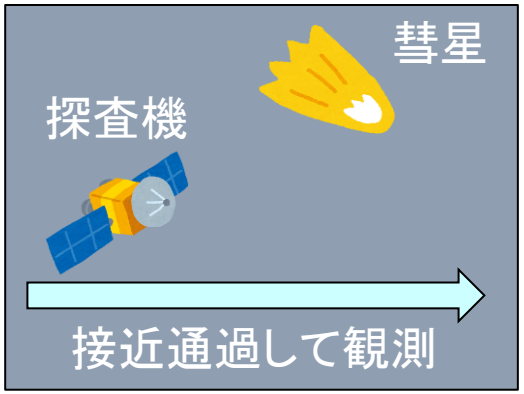
従来の安全解析手法の成果物



ミッションの部分達成条件

有効性確認の方法：適用対象と課題の整理

提案手法の有効性を確認するため、搭載機器が増加しない手段で
システム可用性（ミッション継続性）を高めたい システム
である 彗星探査機システム の 接近通過観測フェーズ に手法を適用

分類	イメージ	特性	システム要求/制約
ミッション特性		チャンスは1度だけ（リトライ不可）	システム可用性（ミッション継続性）を可能な限り高めたい
		複数のミッションを同時実行	姿勢制御の要求が厳しい 電力に余裕がない
製品特性		小型機	搭載機器は最小限 （搭載機器増加を伴う空間冗長化の余裕なし）
アーキテクチャ特性		システム構造が階層化	目的（ミッションや安全）に対して構成要素の最適な役割分担を決定したい

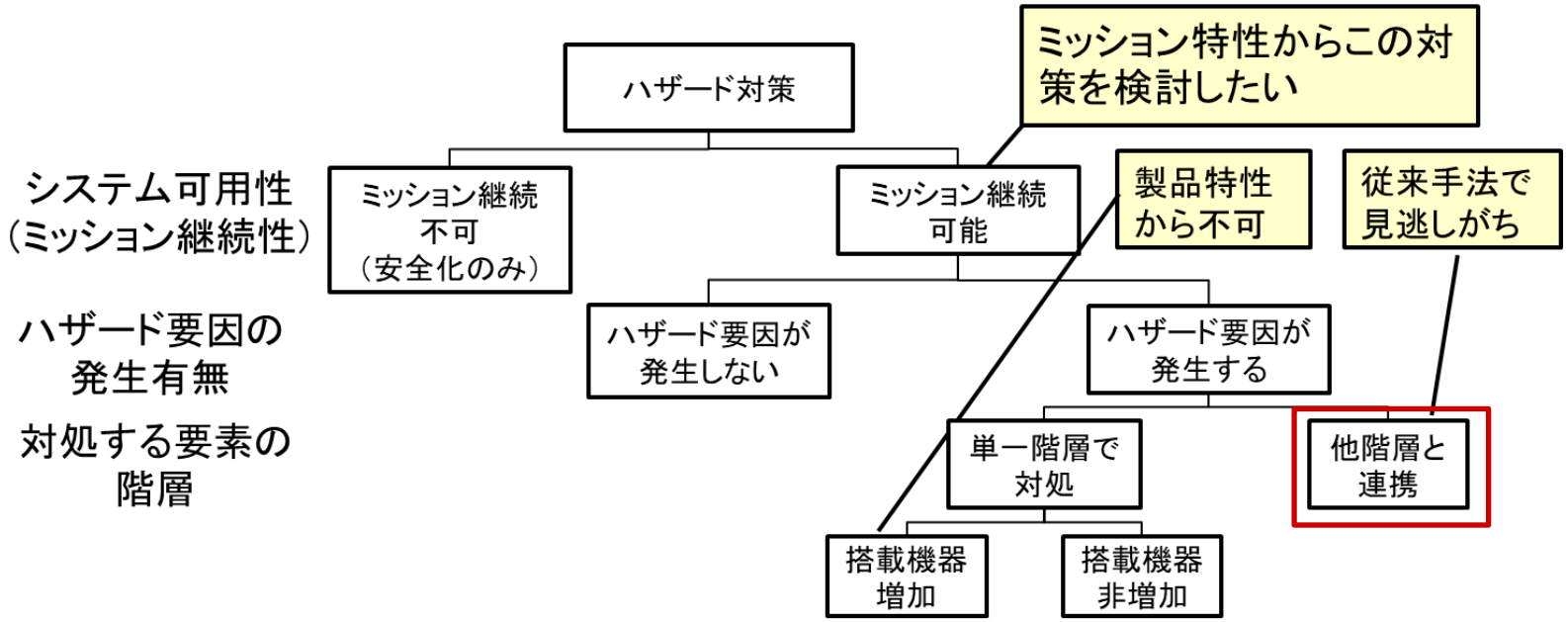
従来のハザード対策の
検討方法（従来手法）では

【課題】
ハザード要因の発生後に、他階層の要素と連携して
ミッションを継続可能にする対策の検討が難しい

有効性確認の方法：課題に対する有効性

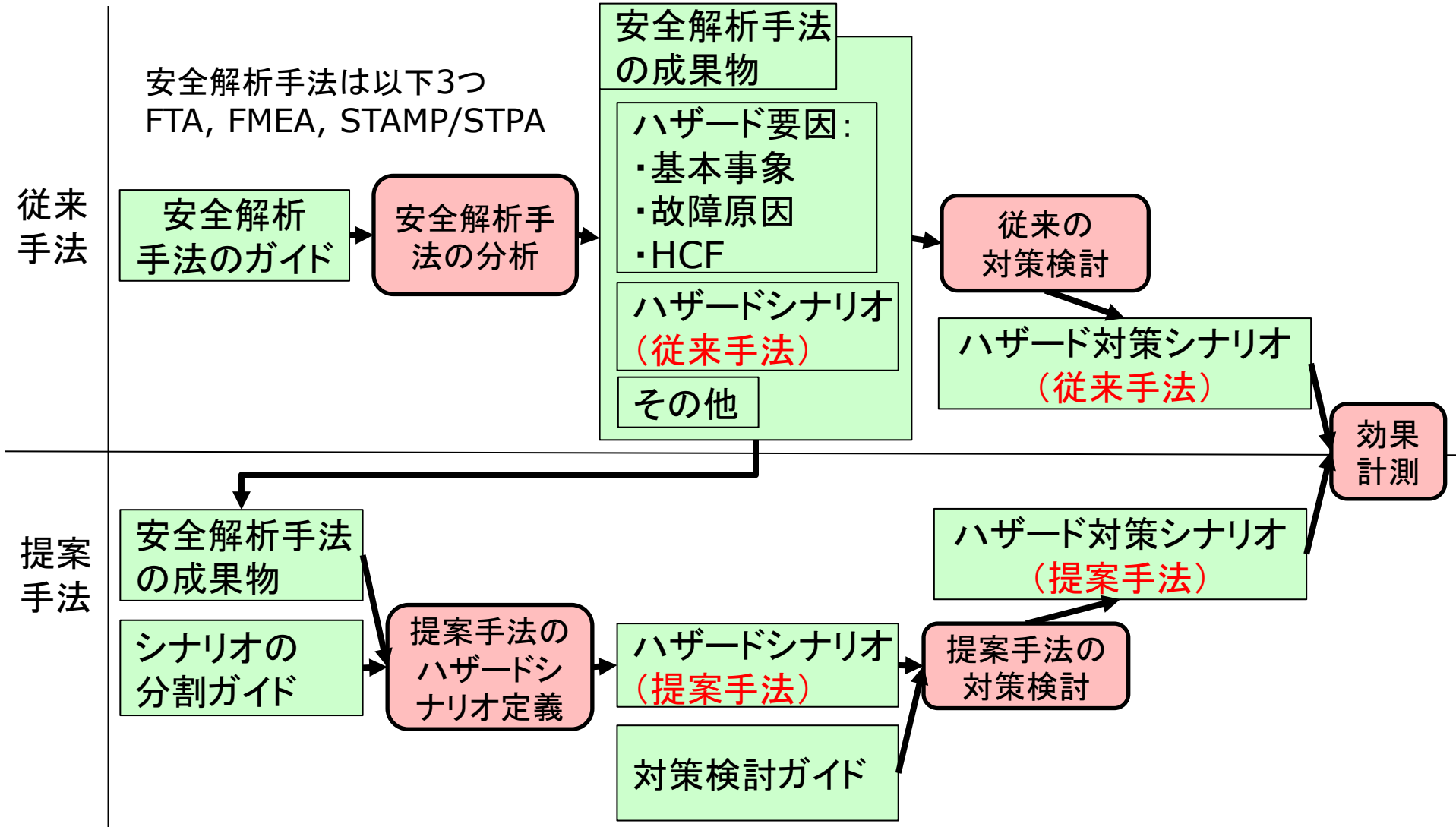
提案手法の課題に対する有効性の評価として
「従来手法で見逃しがちな対策を提案手法は導出できるか？」を評価する

記号	評価項目	何を評価するか？
A	課題に対する有効性	従来手法で見逃しがちな対策（※）を 提案手法は導出できるか？ ※ハザード要因の発生後に、 他階層の要素と連携して、 ミッションを継続可能にする対策



有効性確認の方法：流れ

ハザード対策の検討において、従来手法と提案手法でハザードシナリオと
その対策シナリオ（ハザード対策シナリオ）を導出し、効果を計測



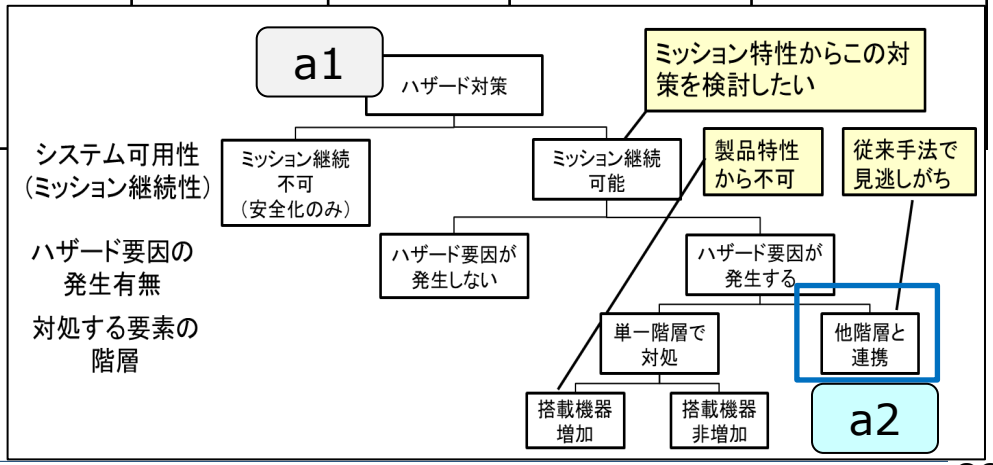
有効性確認の結果：評価項目A（課題に対する有効性）

提案手法は、従来手法が見逃しがちなハザード対策シナリオを導出できている
また、導出したハザード対策シナリオに占める割合は71%であった
（導出した対策の7割程度が狙いどおり）
->提案手法の課題に対して有効性が示唆

記号	【評価項目A　：課題に対する有効性】 従来手法が見逃しがちな（※）対策を 提案手法は導出できるか？	従来手法			提案手法
		FTA	FMEA	STAMP/ STPA	
a1	ハザード対策シナリオ数	33	40	18	38
a2	従来手法が見逃しがちな（※） ハザード対策シナリオ数	0	0	4	27
a3	導出したハザード対策シナリオに占める 従来手法が見逃しがちな（※） ハザード対策シナリオ数の割合 （a2/a1）	0%	0%	22%	71%

※ 従来手法が見逃しがちな

＝ハザード要因の発生後に、
他階層の要素と連携して、
ミッションを継続可能にする

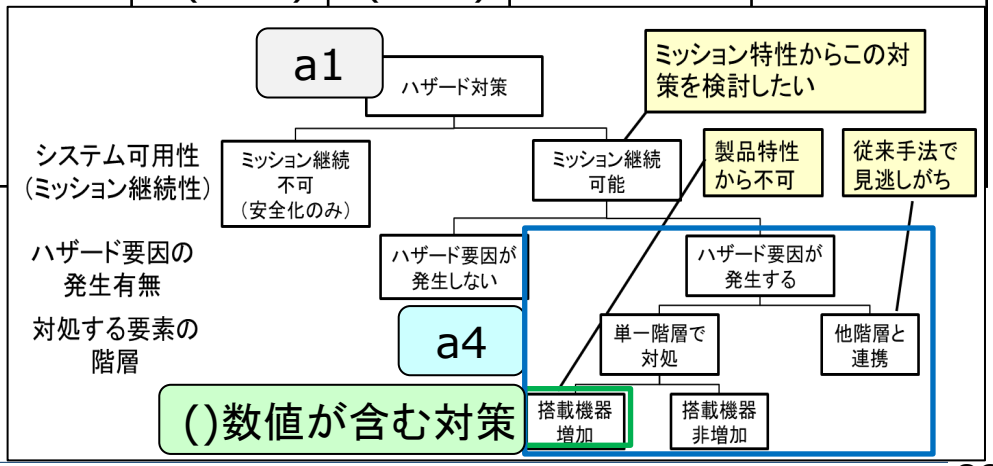


（参考）有効性確認の結果：ミッションの継続可能性のみの評価

提案手法は、導出したハザード対策シナリオの97%が
ハザード要因の発生後に、ミッションを継続可能なハザード対策シナリオである

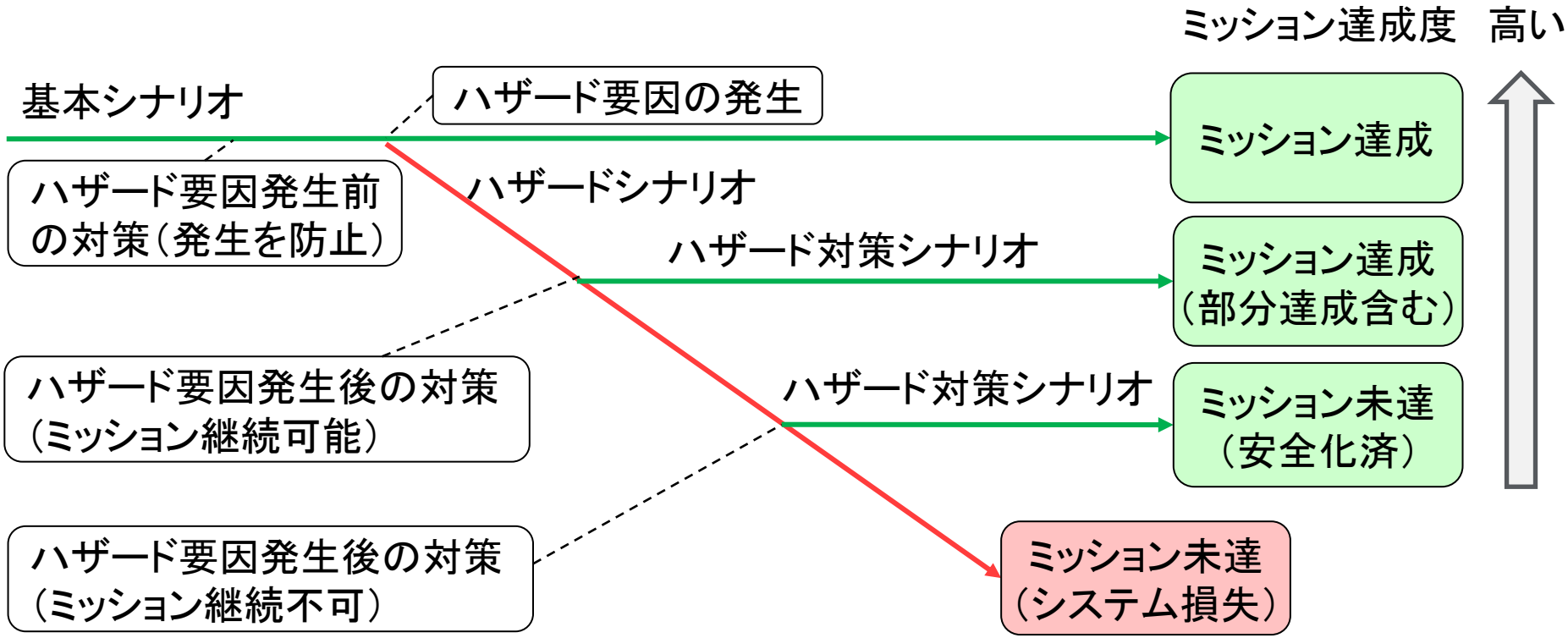
記号	【評価項目A　：課題に対する有効性】 従来手法が見逃しがちな（※）対策を 提案手法は導出できるか？	従来手法			提案手法
		FTA	FMEA	STAMP/ STPA	
a1	ハザード対策シナリオ数	33 (70)	40 (80)	18	38
a4	ハザード要因の発生後に、 ミッションを継続可能な ハザード対策シナリオ数	12 (49)	26 (66)	10	37
a5	導出したハザード対策シナリオに占める ハザード要因の発生後に、 ミッションを継続可能な ハザード対策シナリオ数の割合 （a4/a1）	36% (70%)	65% (83%)	56%	97%

※（）内の数値は搭載機器の増加
（右図の緑枠：機器冗長等）が
可能な場合の値



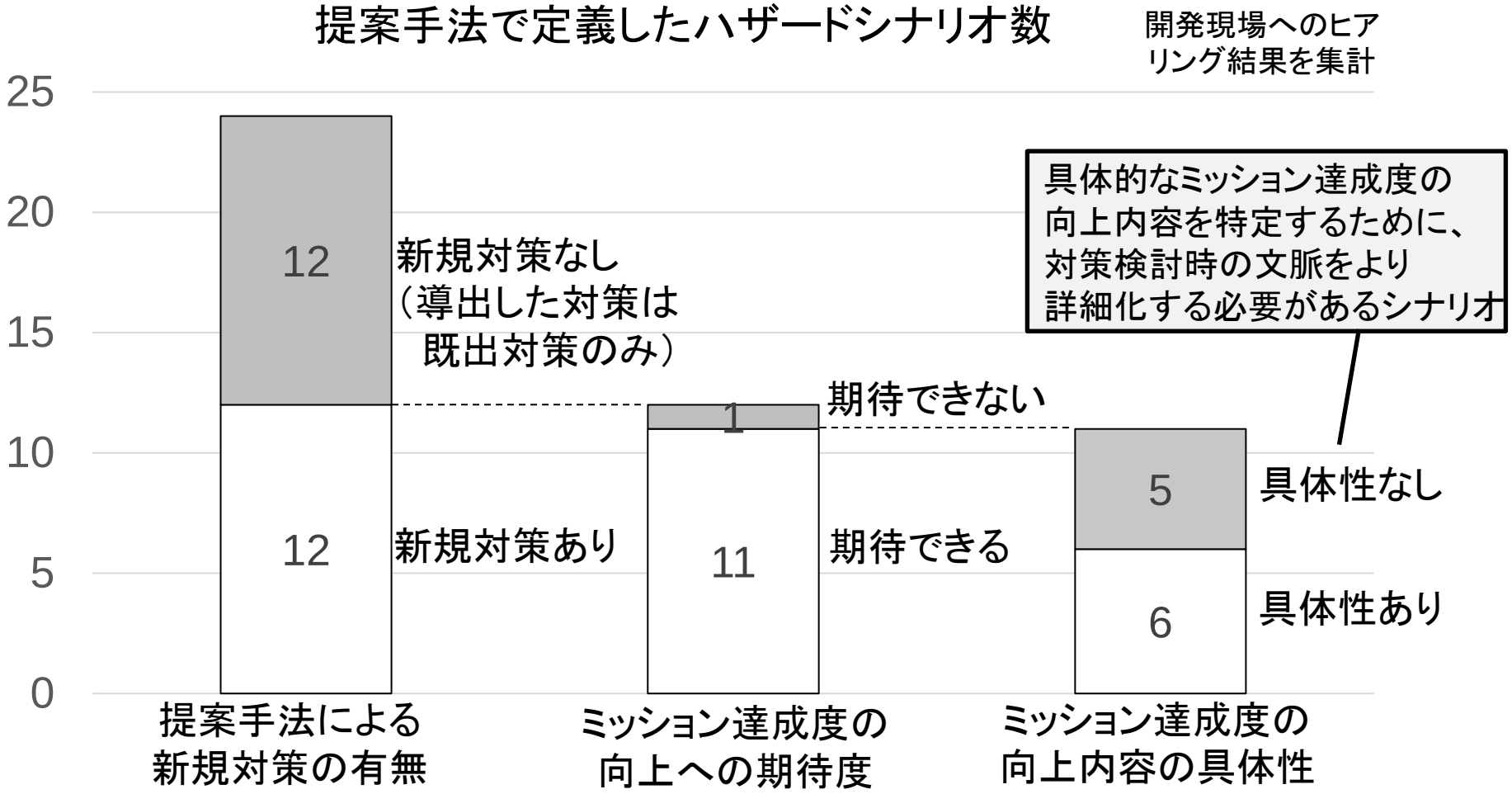
得られた効果：計測

提案手法の成果物によって
「既存の設計検討のミッション達成度が向上するか？」



得られた効果：結果

既存の設計検討に対して
ミッション達成度の向上が期待できるハザードシナリオを識別し
ミッション達成度を向上する検討へ貢献



まとめ

- 結論
  - 以下に対して提案手法の有効性が示唆

    「リトライ不可な 複数のミッションを同時に行う システム構造が階層化しているシステム」のハザード対策の検討において、「ハザード要因発生後に、他階層の要素と連携してミッションを継続可能にする対策」の導出
  - 提案手法は、既存の設計検討に対して、ミッション達成度を向上する検討へ貢献
- 提案手法の限界
  - 提案手法は、システム構成要素やそれらの相互作用に対してハザード要因を網羅的に導出できない

    ->従来の安全解析手法でハザード要因とその対策を導出した後、

    さらなるシステム可用性（ミッション継続性）向上のための利用を推奨
- 今後の展開
  - 異なる特性のシステムへの適用

    特に、ミッション特性（リトライ可能 や ミッション機器は1つ等）
  - 作業者の属人性評価

ご清聴　ありがとうございました