資料8-1-2
（ NC版　資料7-1-2 ）

国際宇宙ステーション(ISS)に提供するISS構成要素及び搭載物に係る安全性確認の現状について

平成26年1月28日（A改訂）
平成26年1月14日

独立行政法人
宇宙航空研究開発機構

A改訂内容
①ハザードの考え方を明記（p.5）

説明者
有人宇宙ミッション本部 有人システム安全・ミッション保証室
室長　上森　規光

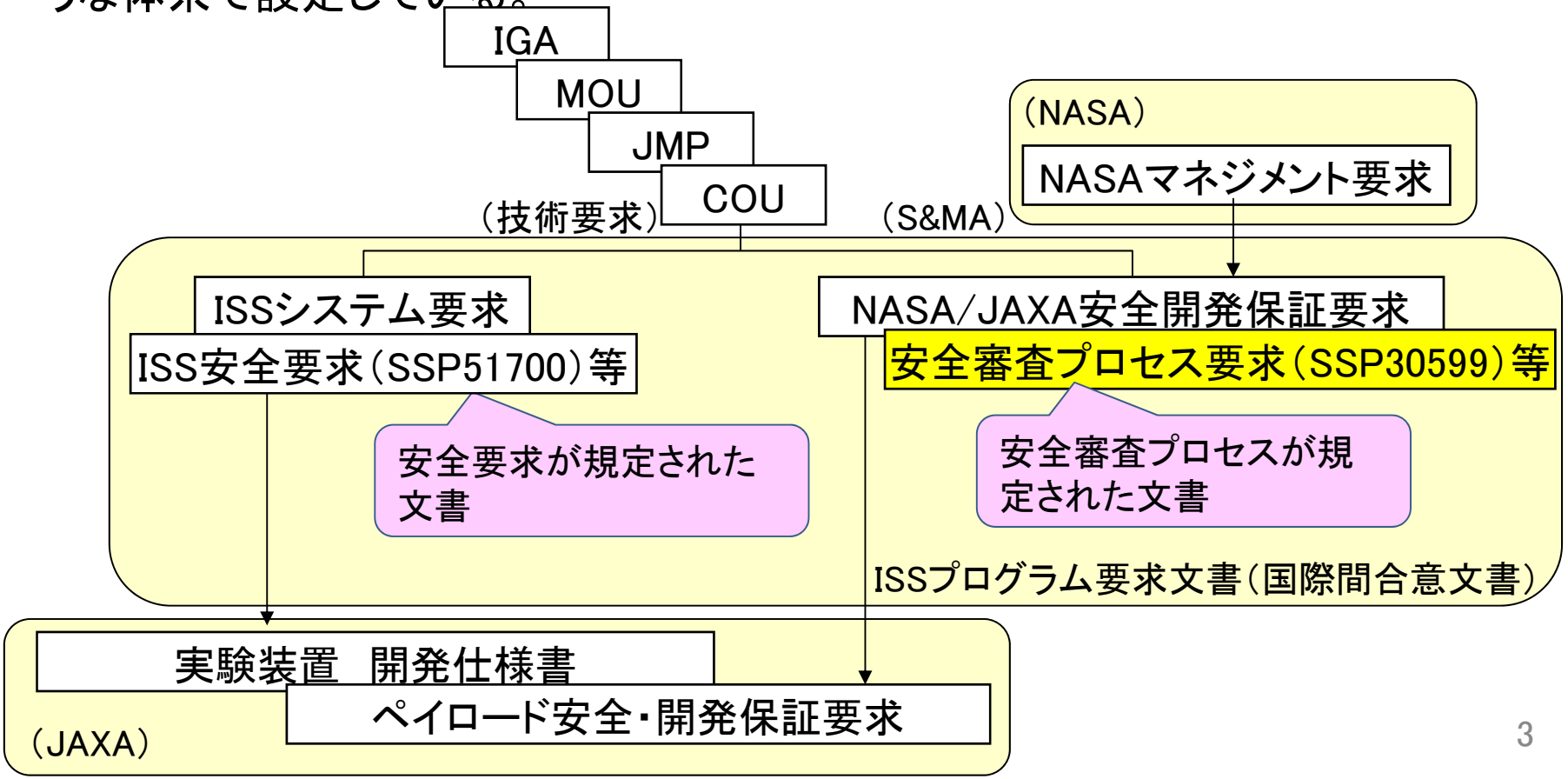
目次

1．目的

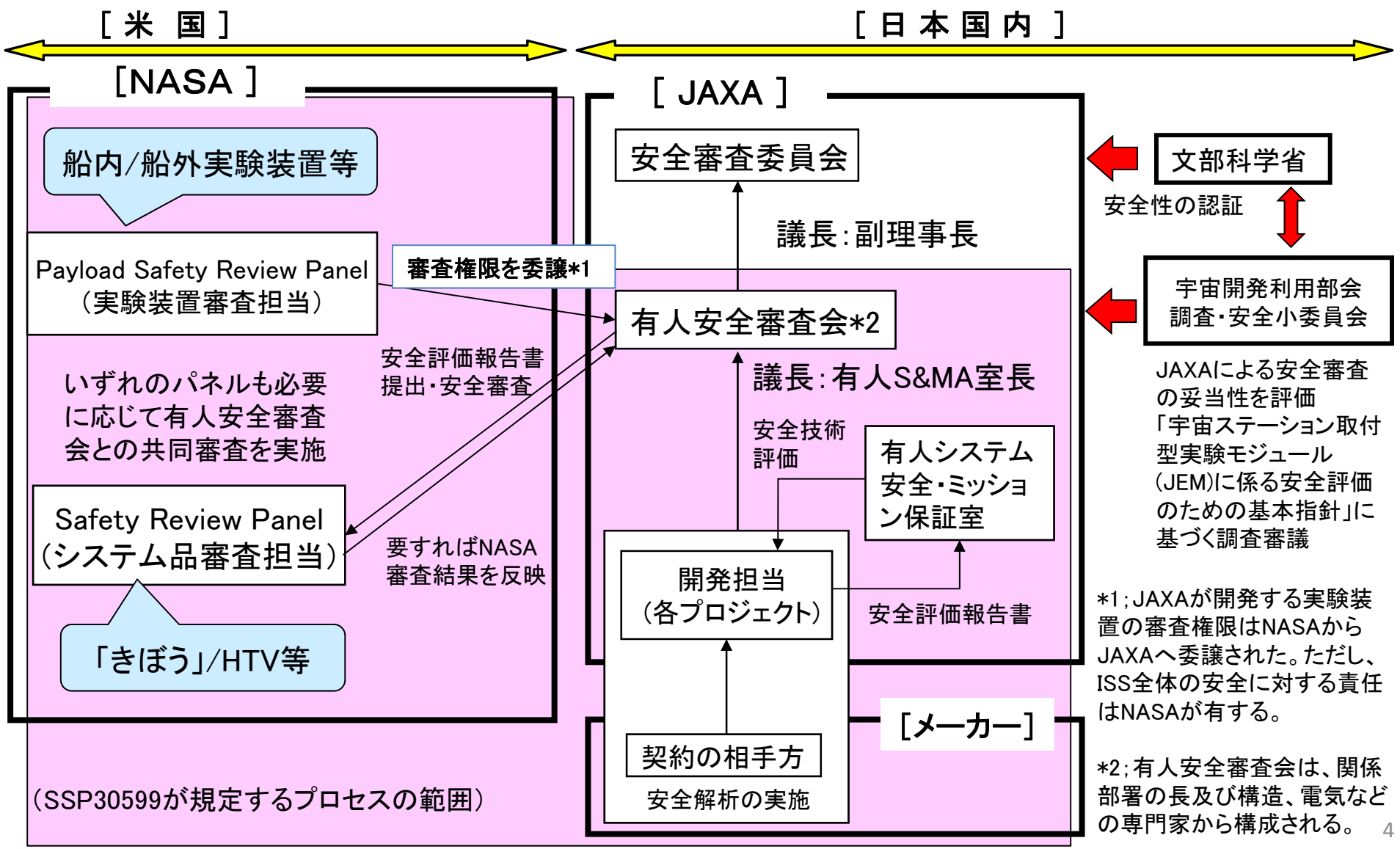
日本が国際宇宙ステーション（ISS）に提供する実験装置の安全性確認について、宇宙航空研究開発機構（JAXA）が実施している実際のプロセス等を概説する。

2. 要求の体系

- JAXAは、文部科学省を支援する実施機関として、NASAと共同管理計画（JMP;Joint Management Plan）や運用・利用方針（COU; Concept of Operation and Utilization）を設定している。
- JAXAは、安全・ミッション保証（S&MA）に係るプロセスや技術要求を以下のような体系で設定している。



3. ISSに係る安全審査体制



*1；JAXAが開発する実験装置の審査権限はNASAからJAXAへ委譲された。ただし、ISS全体の安全に対する責任はNASAが有する。

*2；有人安全審査会は、関係部署の長及び構造、電気などの専門家から構成される。

4.1. 安全確保の基本的な考え方
安全設計・審査の基本方針

「きぼう」の安全確保のため、以下の基本的な考え方に従って十分な安全対策を講じ、ハザードを管理することによって、リスクを可能な限り小さくする。
＊ハザードとは、「事故をもたらす要因が顕在又は潜在する状態」を言う。

(1)安全確保の対象
国際宇宙ステーションは、人間をその構成要素として含むシステムであり、搭乗員の死傷を未然に防止するため、安全確保を図る。

(2)安全確保の方法
「きぼう」の開発及び運用においては、すべてのハザードを識別し、以下の優先順位に従ってハザードを制御し、残存ハザードのリスクを評価する。

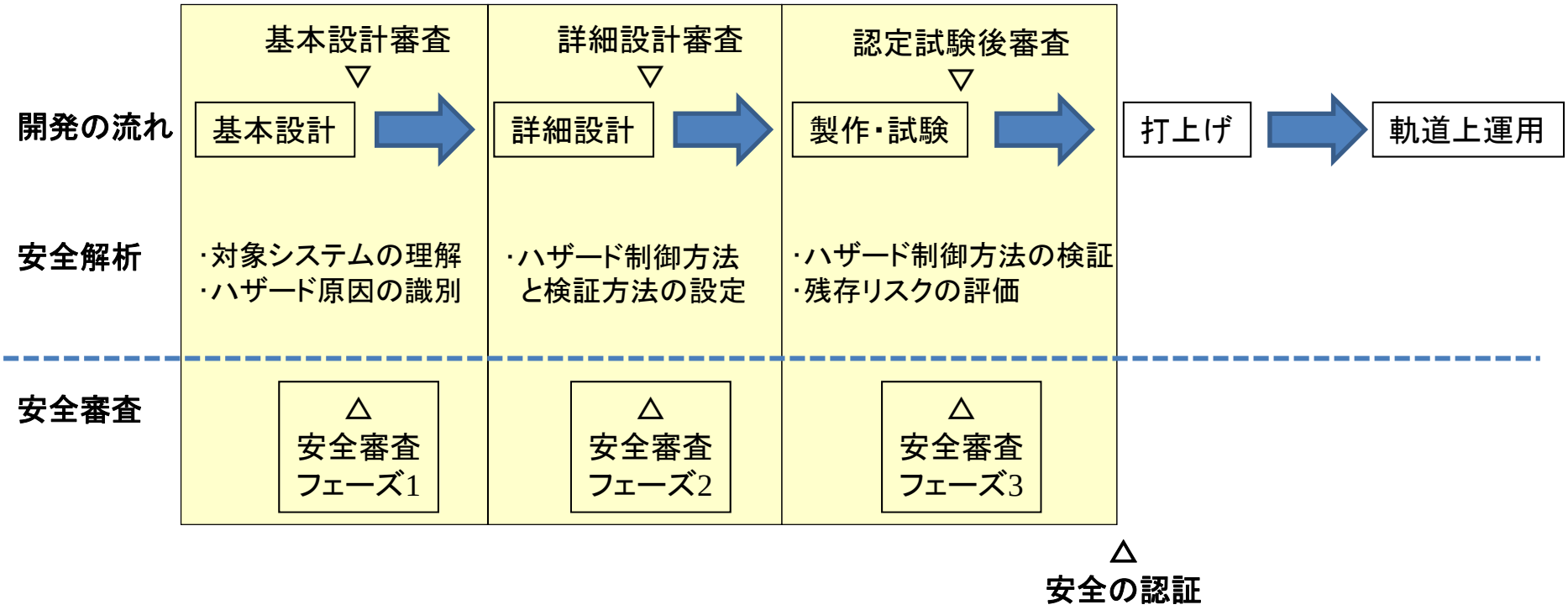
a. ハザードの除去
b. リスクの最小化設計(故障許容設計など)
c. 安全装置
d. 警報・非常設備等
e. 運用手段
f. 保全

(3)有人活動の特殊性への配慮
「きぼう」は、自然環境及び誘導環境から搭乗員及び安全に関わる機器を保護するために、十分な構造上の強度、寿命等を有するとともに、安全に関わるシステムの故障(誤操作を含む)に対する適切な許容度の確保、容易な保全等ができるようにする。また、火災、爆発、危険物等による異常の発生の防止並びに外傷、火傷、感電等の傷害及び疾病の発生の防止を図るとともに、緊急対策に十分配慮する。

4.1. 安全確保の基本的な考え方
安全設計・審査のプロセス

（1）ハザード管理

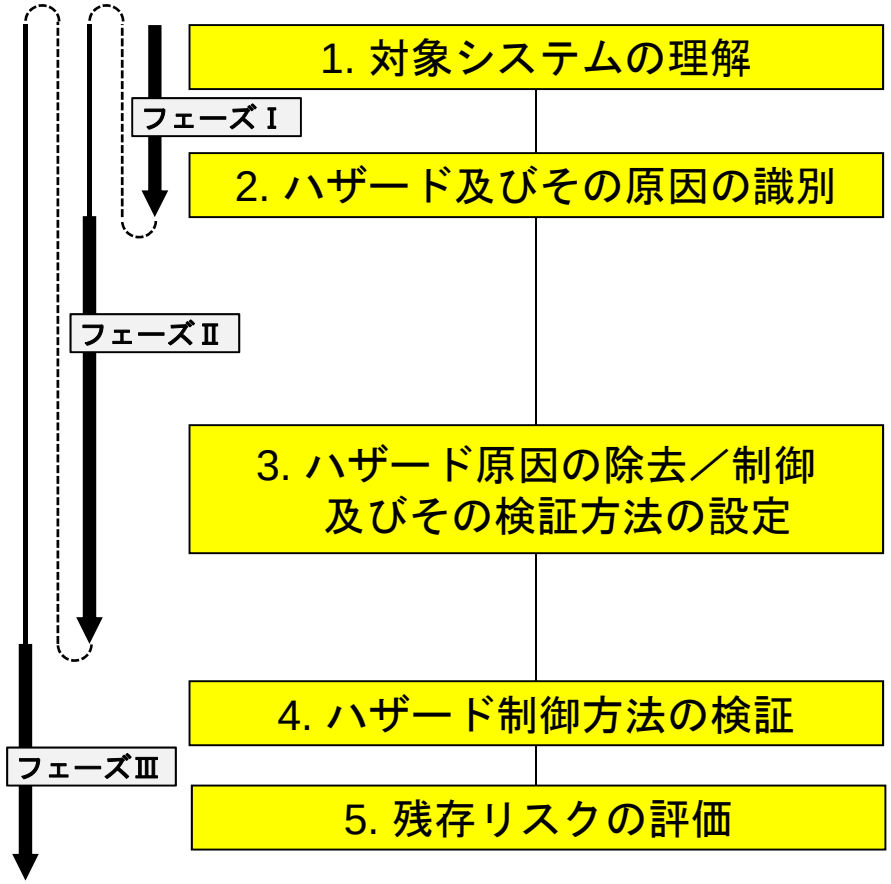
搭乗員の死傷等を未然に防止するために、直接搭乗員に被害を与えるハザード、あるいは安全に関わるシステムに被害を与えることにより間接的に搭乗員に被害を与えるハザード等を設計の早い段階から識別し、常に管理下に置きながら、設計活動の中で安全なシステムの開発をはかる。



（2）独立組織による評価／審査体制

開発部門とは独立に設置された、専門家チームによる評価と、審査部門による審査を実施する。

4.1. 安全確保の基本的な考え方
安全解析の手順



・対象とするシステムの機能・性能、その運用方法、そのシステムが遭遇する環境条件、他のシステムとのインタフェース等、を十分理解する。

・対象となるシステム及びその運用に掛かる予測可能な全てのハザードを、FTA、FMEA、標準ハザードによるチェック等の手法によって、被害の度合い*1を含めて識別する。また、識別したハザードの原因を識別する。これらは、対象とするハードウエア、ソフトウエア、運用、誤操作等のヒューマンエラー、インタフェース、環境条件等を考慮して、体系的かつ論理的に解析する。
FTA：Fault Tree Analysis
FMEA：Failure Mode and Effect Analysis

・ハザード原因については可能な限り除去する。除去できないものについては、制御*2する。
また、ハザード制御の検証方法*3を併せて設定する

・試験、解析、検査、デモンストレーションのいずれか、あるいは組み合わせによって確認する。

・ハザードの制御方法の検証結果を評価して、ハザードの残存リスクが十分低いレベルに制御されていることを確認する。

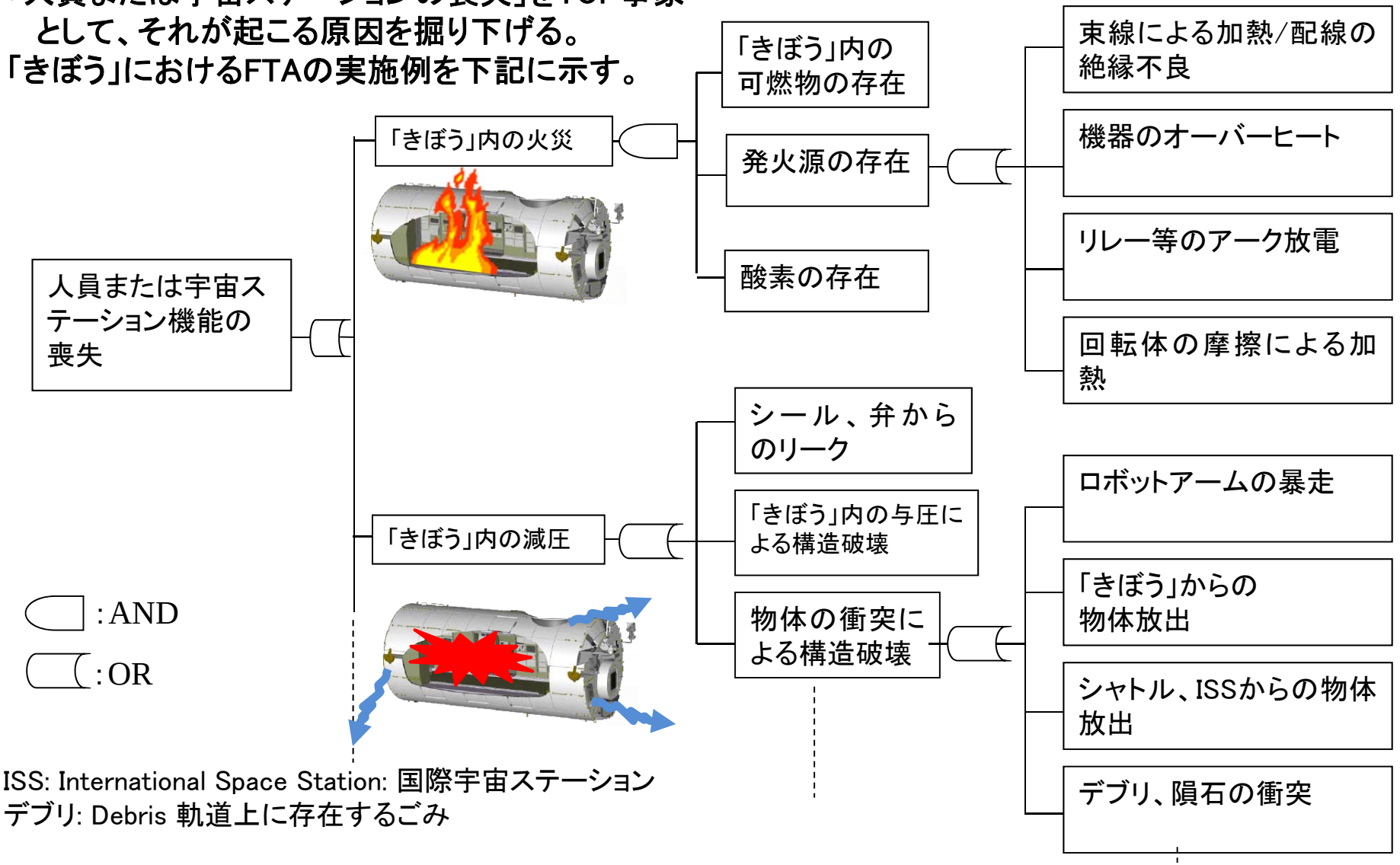
*1；被害の度合い
カタストロフィック（2故障許容設計相当）
打上げ機／ISSの喪失、致命的な人員の傷害となり得る状態。
クリティカル（1故障許容設計相当）
打上げ機／ISS機器の損傷や人員の傷害となり得る状態。

*2；制御
ハザードの影響の発現の可能性を下げる設計あるいは運用の仕組み。

*3；検証方法
その仕組みが有効に機能することを試験、解析、検査、デモンストレーションなどにより確認すること。

4.2. ハザードの識別
(1) FTA (Fault Tree Analysis)

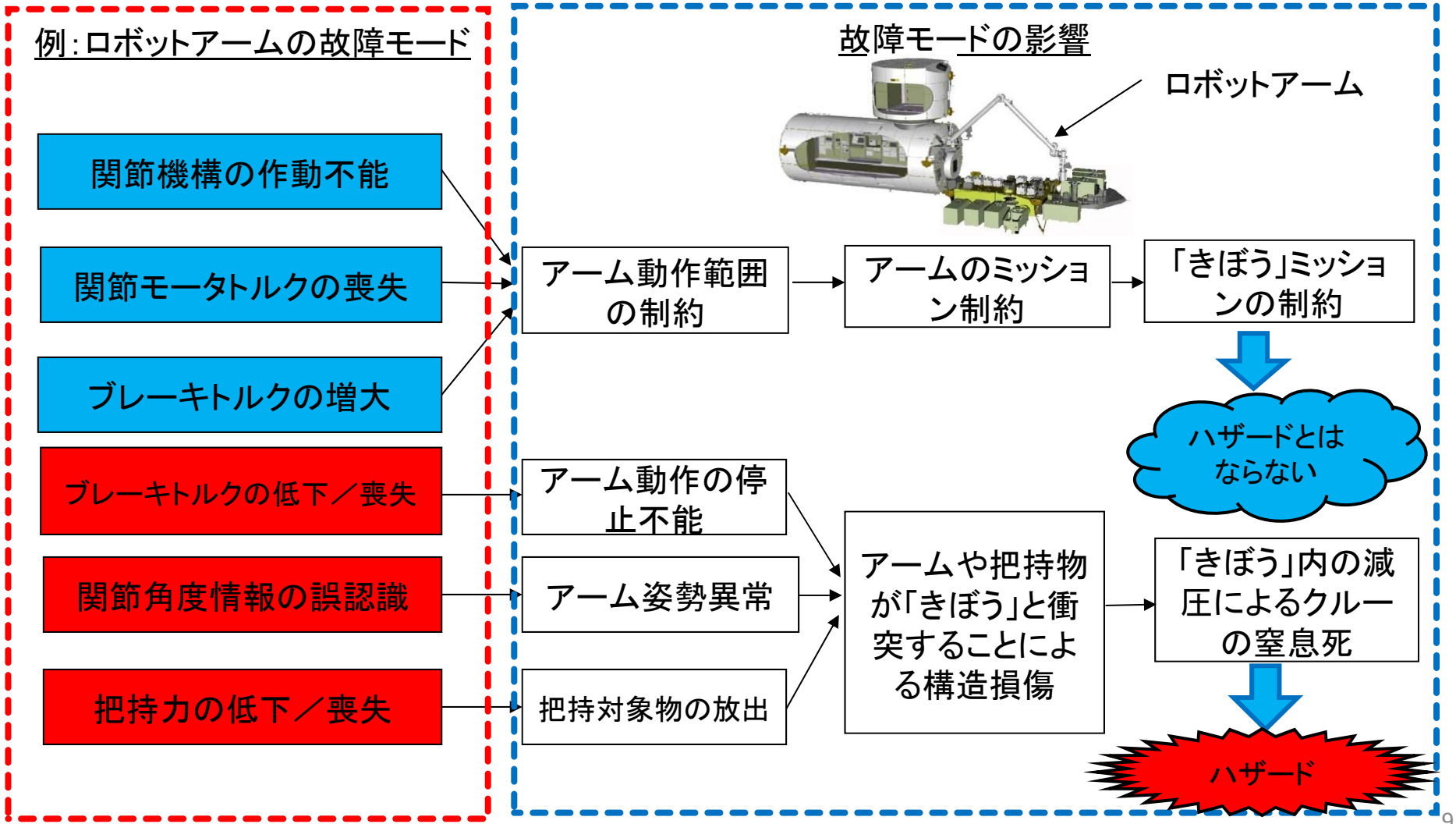
「人員または宇宙ステーションの喪失」をTOP事象
として、それが起こる原因を掘り下げる。
「きぼう」におけるFTAの実施例を下記に示す。



ISS: International Space Station: 国際宇宙ステーション
デブリ: Debris 軌道上に存在するごみ

4.2. ハザードの識別
(2) FMEA (Failure Mode and Effect Analysis)

個々の機器の故障が、システムにどのような影響を及ぼすかを調べる。
ロボットアームのFMEAの実施例を下記に示す。



4.2. ハザードの識別
(3) 標準ハザード

- ✓ ISSでは16種別の標準ハザードが定義されている。
- ✓ FTA、FMEA等の手法で識別されたハザードが標準ハザードに該当する場合は、標準化された方法で制御・検証する。
- ✓ 標準ハザードで対応できず、製品に特徴的な制御が必要な場合は、ユニークハザードとして識別する。

標準ハザード番号	標準ハザード (SSP 30599 Safety Review Processによる)
1	打上げ荷重による構造破壊
2	シールを有する圧力機器の破損
3	ベントポートを有する機器の破損
4	鋭利端部への接触、挟み込み
5	ガラス破損
6	火災(可燃性物質の使用)
7	船内空気の汚染(使用材料からのオフガス)
8	電磁適合性
9	電池の破裂/漏えい
10	高/低温部への接触
11	電力系の損傷
12	発火源の有無(シャトル打ち上げの場合)
13	回転機器(循環ポンプ、ファン)の破損
14	電力コネクタ着脱時の感電
15	クルー退避時の障害
16	水銀による船内空気の汚染

4.3 ハザードの除去/制御(1/4)

（1） ハザードの除去

一番優先すべき対応は、ハザード原因を設計により根源的に取り除くこと。

例えば、ガラス等、割れた際にけがの原因となるような材料は使用しない

（2） ハザードの制御

ハザードを除去できない場合に、潜在する人的・物的損失を低減できる最大の効果の有る設計などによる対策を講じること。

（NASA SSP30599 Safety Review Processより）

ハザードの制御により、発生頻度と被害の程度を許容可能なレベルに低減させる

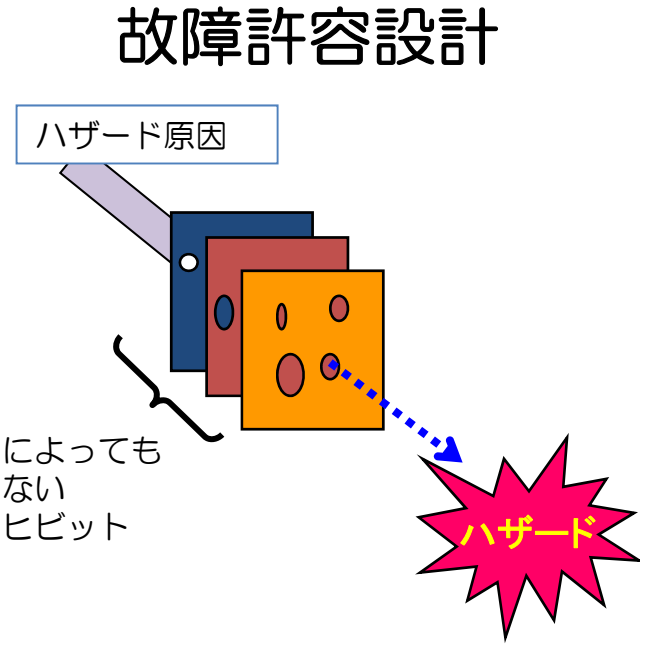
4.3. ハザードの除去／制御(2/4)

以下に優先順位の高い順にハザード制御方法を示す。

（1）故障許容設計

- 独立したハザード防御機能を設ける設計手法
  （万が一壊れても安全上の問題を発生させないような設計）
- 故障により意図しない動作が予想される場合、エネルギー遮断装置(インヒビット)を設置

  例：コネクタ脱着する電力ラインにスイッチを設け、
  感電を防止する等



- 故障許容数は、被害の度合いによって、異なる

  ➢破局ハザード（Catastrophic Hazard)の場合
  2つの故障、2つの誤操作、または1つの故障と1つの誤操作が同時発生した場合でも事故（打上げ機／ISSの喪失、致命的な人員の傷害等）に至らないような対策が必要

  ➢重要ハザード（Critical Hazard)の場合
  1つの故障または1つの誤操作により、事故（打上げ機／ISS機器の損傷や人員の傷害）に至らないような対策が必要

4.3. ハザードの除去／制御(3/4)

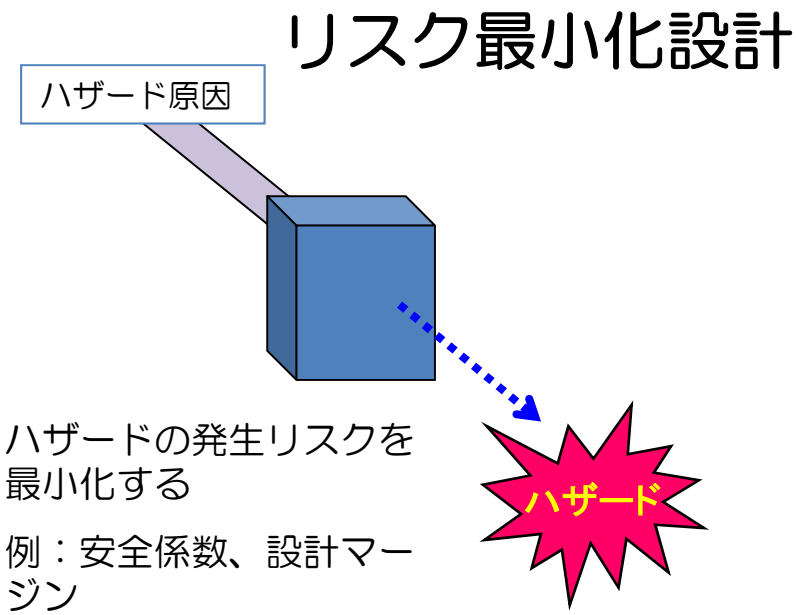
（2）リスク最小化設計

- 故障許容設計が適用できない場合、
- 適切な設計マージンの確保により、ハザードの発生リスクを最小化する設計手法（壊れないような設計）

例：十分な設計マージン持った圧力容器（圧力系破壊対応）、等

＜リスク最小化設計が適用される分野＞

- 構造
- 圧力容器
- 圧力配管および継ぎ手
- 火工品
- 安全上重要なメカニズム（機構）
- 材料の適合性
- 可燃性



4.3. ハザードの除去／制御(4/4)

(3)安全装置

➢ 万が一異常が発生した場合でも、被害の影響を最小にするための措置

例: 圧力容器に対して、破壊する前にリークする設計

(4)警報・非常設備装置

➢ 危険な状態を正しく、タイムリーに検知し、搭乗員あるいは地上作業員に知らせ、検知後の適切な緊急手順を準備する。

例: 火災検知システム、消火器、携帯酸素マスク等の設置

(5)運用手順

➢ 設計では対処しきれない場合に、操作手順により危険な状況を避ける。

例:電気コネクタ着脱前に上流電源スイッチを切り、感電を避ける

- 運用によるハザード制御を設定する際には、その運用制御の実現性について、運用の担当者と調整の上、設定する。
- 運用によるハザード制御は、運用制御合意文書*1にまとめて管理する。

*1;運用制御内容を装置開発担当部門から手順書を作成する運用部門に申し送るための文書

(6)保全

➢装置・部品の寿命がくる前に新品に交換し、ハザードの発生頻度を低減する。

4.4. ハザード制御の検証

（1）検証手段

安全設計が意図したとおり働く(機能する)ことを、以下の何れか、あるいはその組合わせによって確認する。

① 試験 :製品や運用が、代表的な環境条件の下で、要求仕様を満たしていることの確認
② 解析 :計算、シミュレーション等による推定
③ 検査 :目視観察、計測により即座に判定できる確認
④ デモンストレーション（実証）:実用に供せることの確認

（2）安全検証追跡ログによる管理

検証は、システム等が工場から出荷される前に完了させることを基本とするが、種子島宇宙センターなどの射場で打上げ直前に最終検証を行うものは、安全検証追跡ログ（SVTL：Safety Verification Tracking Log）に識別し、管理する。

4.5. 安全審査(1/5)
役割分担

【開発部門】

- 対象品の安全解析を実施し、安全評価報告書（ハザードレポートを含む）にまとめる。
- 最終的に全対象ハザードに対する制御方法の妥当性、成立性及び検証に対する責任を有する。

【安全審査部門】

- 開発部門とは独立に設置された安全審査パネル／安全評価部門（有人システム・安全ミッション保証室）は、安全要求とその解釈、並びにリアルタイム運用からフィードバックされる事例等を統合的に管理し、適宜開発・運用担当者に指針として展開する。
- 第三者的な観点で、開発部門が実施した安全解析結果の審査を行う。
- 個々の技術に係る専門家チームが、安全審査活動に対して、適宜支援を行う。
- 専門家チームは、要素及びシステム双方の観点で事前評価を行い、安全審査パネルに必要な助言を行う。

4.5. 安全審査(2/5)
安全審査のフェーズ分け

適切なタイミングで安全審査を実施し、安全解析の妥当性を確認している。

安全審査	安全審査のタイミング	安全審査の目的
フェーズ0 （要すれば）	概念設計終了時	1. ハザード識別法、識別結果の確認 2. 適用すべき安全要求の識別結果の確認
フェーズ I	基本設計終了時	1. 基本設計における全ハザード及びハザード原因の識別結果の確認 2. ハザード制御方法の妥当性の評価 3. 検証方法の確立が妥当かの評価
フェーズII	詳細設計終了時	1. 詳細設計における全ハザード及びハザード原因の識別結果の確認 2. ハザード制御方法が設計上実現されていることの確認 3. 検証方法の詳細が設定されていることの確認
フェーズIII	認定試験終了時	1. 製品が全ての安全要求に合致していることの確認 2. 検証が終了したことの確認 3. アクションアイテムが全てクローズしていることの確認

4.5. 安全審査(3/5)
安全評価報告書

安全評価報告書の構成（主要な項目を抜粋）

1. イントロダクション
2. 安全解析方法
3. システムの説明
4. 打上げコンフィギュレーション
5. 運用
6. 安全解析結果

添付
A. ハザードレポート
  ・標準ハザード
  ・ユニークハザード
B. 不適合報告書(NCR; Non Compliance Report)*1
C. 運用制御マトリクス(OCM; Operational Control Matrix)
D. 安全検証追跡ログ(SVTL; Safety Verification Tracking Log)

*1：安全要求には適合しないが、その安全要求の意図は満足しているなどの理由により、受入可能と判断する仕組み。

4.5. 安全審査(4/5)

安全審査の種類

審査対象物のハザード制御の特殊性や新規性、実績の有無などの観点から、安全審査を以下の3種類に分類して実施している。

	安全審査の種類	審査の区分及び実施方法	審査対象物の例
1	パネル審査	✓ 審査員、事務局及び開発部門による対話方式で審議を行う。	・ExHAM ・静電浮遊炉
2	文書審査	✓ 過去にフライト実績がある場合等。 ✓ 審査員による文書レビューによる審査を行う。	・通信ケーブル ・実験供試体
3	議長承認	✓ 安全上クリティカルでない、または過去に承認された内容から変更がない場合等。 ✓ 議長が承認／非承認を判断する。	・クルー線量計 ・Tシャツ

4.5. 安全審査(5/5)
NASAからの安全審査権限の委譲

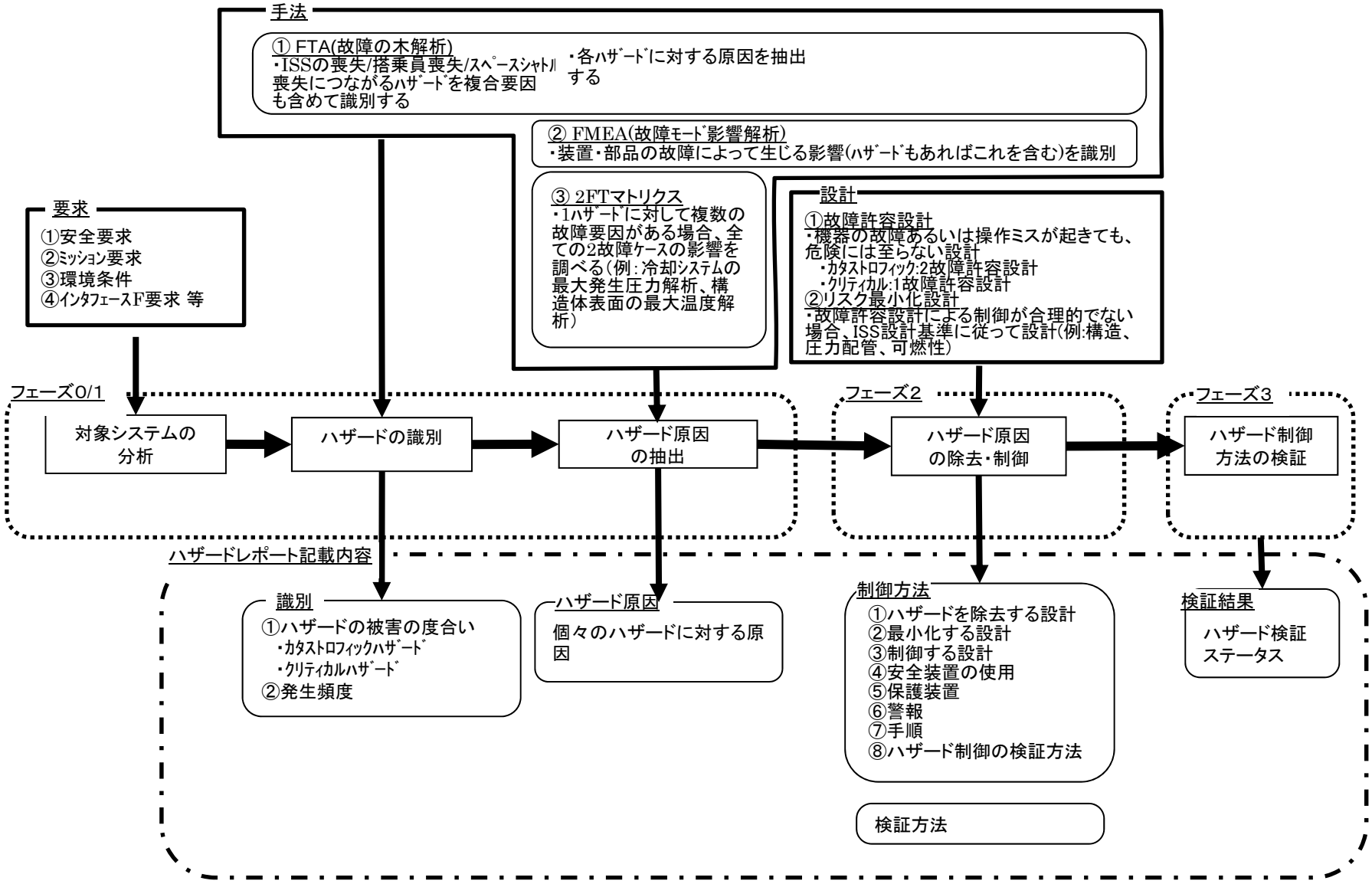
- ✓ JAXAの有人安全審査能力がNASA審査レベルと同等であることがNASAに認められ、平成22年 9月24日に、日本が開発する実験装置の審査権限についてNASA ISSプログラムからJAXAに権限委譲（フランチャイズ化）がなされた。
- ✓ ただし、実験装置の有するハザードの内容により、一部NASAとの調整を要する（下表参照）。
- ✓ 実験装置に加え、「きぼう」システム品についても、安全審査権限を委譲する方向でNASAと調整中。

	NASAの関与	実験装置／ハザードの分類の例
1	なし	a. 標準ハザードのみ b. シリーズ品／再飛行品 c. 毒性が低い(毒性レベル1)
2	事前調整	a. 毒性が中程度(毒性レベル2) b. 保全やトラブルシュートに関連するハザード c. 以前のフライトで生じた不具合に関連するハザード
3	該当するハザードレポートの審査	a. 毒性が高い(毒性レベル3,4) b. 不適合報告書(NCR)を含む c. 船外活動(EVA)に関連するハザード

添付

添付1　;安全設計の流れ

添付1　;安全設計の流れ


手法
① FTA(故障の木解析)
・ISSの喪失/搭乗員喪失/ｽﾍﾟｰｽｼｬﾄﾙ喪失につながるﾊｻﾞｰﾄﾞを複合要因も含めて識別する
・各ﾊｻﾞｰﾄﾞに対する原因を抽出する
② FMEA(故障ﾓｰﾄﾞ影響解析)
・装置・部品の故障によって生じる影響(ﾊｻﾞｰﾄﾞもあればこれを含む)を識別
③ 2FTマトリクス
・1ﾊｻﾞｰﾄﾞに対して複数の故障要因がある場合、全ての2故障ｹｰｽの影響を調べる(例：冷却ｼｽﾃﾑの最大発生圧力解析、構造体表面の最大温度解析)
設計
①故障許容設計
・機器の故障あるいは操作ミスが起きても、危険には至らない設計
・ｶﾀｽﾄﾛﾌｨｯｸ:2故障許容設計
・ｸﾘﾃｨｶﾙ:1故障許容設計
②リスク最小化設計
・故障許容設計による制御が合理的でない場合、ISS設計基準に従って設計(例:構造、圧力配管、可燃性)
要求
①安全要求
②ﾐｯｼｮﾝ要求
③環境条件
④ｲﾝﾀﾌｪｰｽF要求 等
フェーズ0/1
対象システムの分析
ハザードの識別
ハザード原因の抽出
フェーズ2
ハザード原因の除去・制御
フェーズ3
ハザード制御方法の検証
ハザードレポート記載内容
識別
①ハザードの被害の度合い
・ｶﾀｽﾄﾛﾌｨｯｸﾊｻﾞｰﾄﾞ
・ｸﾘﾃｨｶﾙﾊｻﾞｰﾄﾞ
②発生頻度
ハザード原因
個々のハザードに対する原因
制御方法
①ハザードを除去する設計
②最小化する設計
③制御する設計
④安全装置の使用
⑤保護装置
⑥警報
⑦手順
⑧ハザード制御の検証方法
検証結果
ハザード検証ステータス
検証方法