参考資料60-1-2
科学技術・学術審議会
研究計画・評価分科会
宇宙開発利用部会
調査・安全小委員会
(第60 回) R8.2.25

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の安全確認に係る JAXAの安全性確認の現状について

平成31年1月11日

国立研究開発法人
宇宙航空研究開発機構

説明者
有人宇宙技術部門 有人システム安全・ミッション保証室
室長　白井 達也

目次

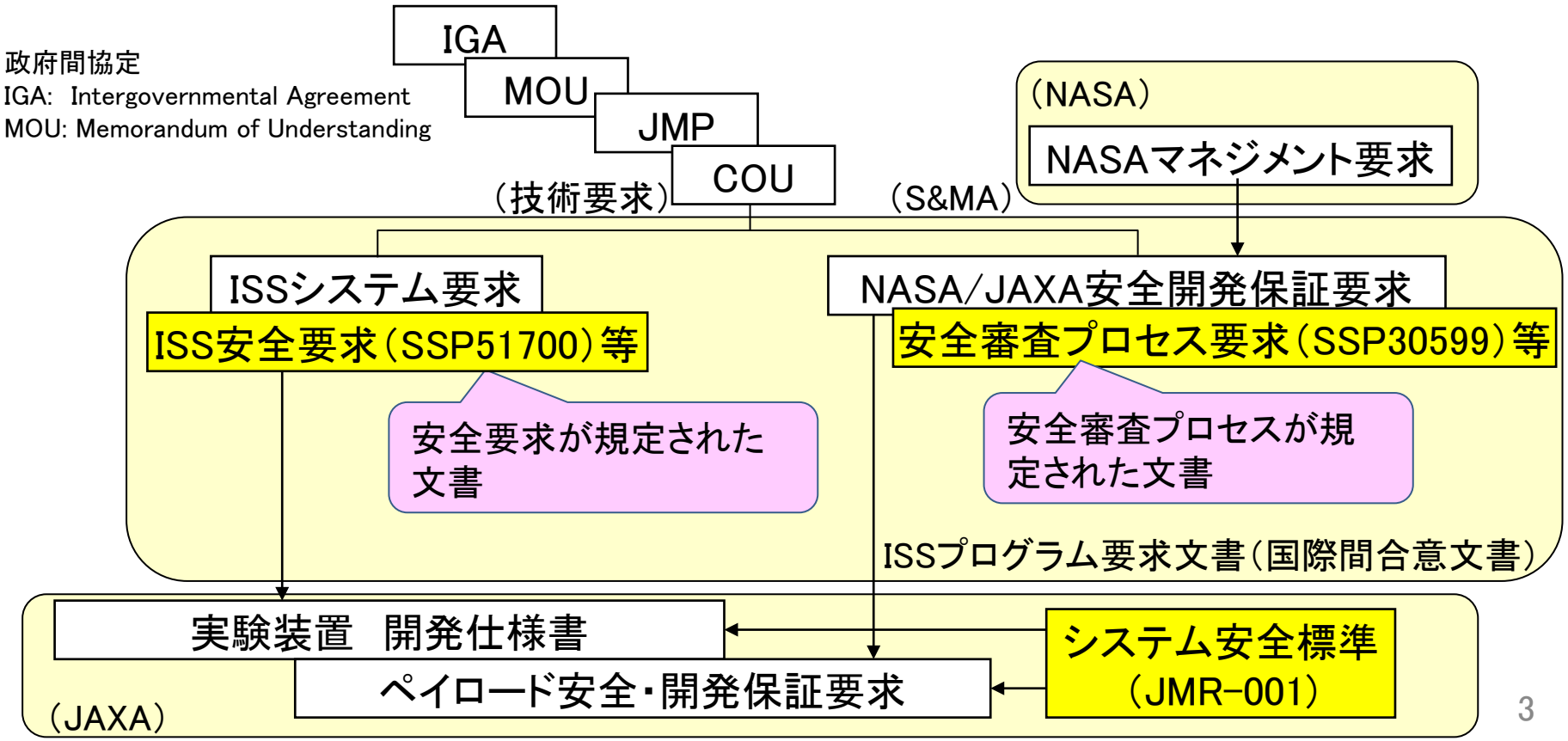
1. 目的

国際宇宙ステーション（ISS）に物資等を輸送する宇宙ステーション補給機「こうのとり」あるいはJAXAが開発するISS実験装置等に対し、JAXAが実施している安全性確認の現状として、安全確保の基本的な考え方や安全設計・審査のプロセスについて概説する。

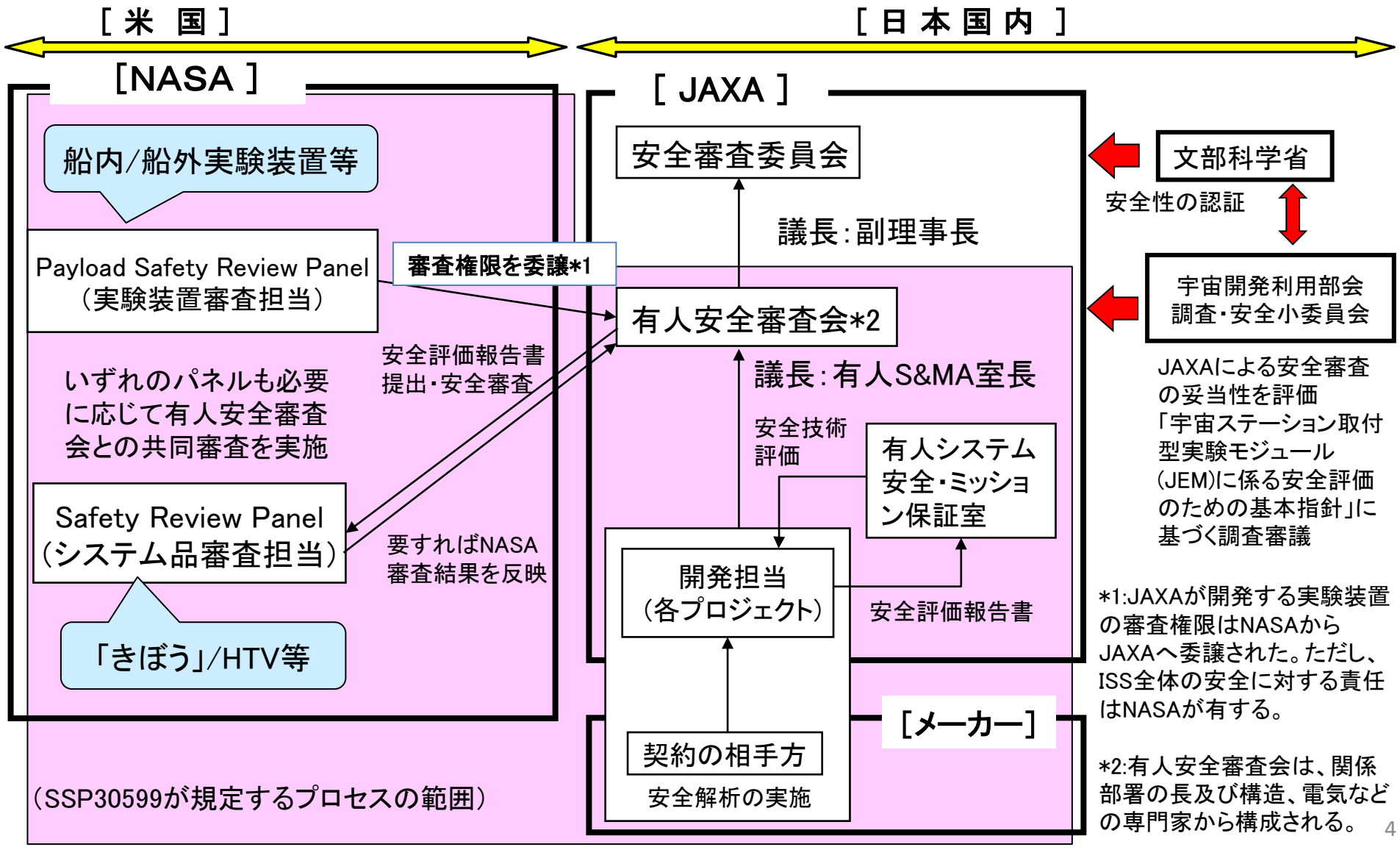
ISSの安全性は、ISS搭乗員の命を守ることを最優先事項としている。そのために必要なISS機能の維持について安全審査で技術的な評価を行っている。

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(1/4)

(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」の安全確保のため、システム安全標準(JMR-001)および安全審査プロセス要求(SSP30599)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。

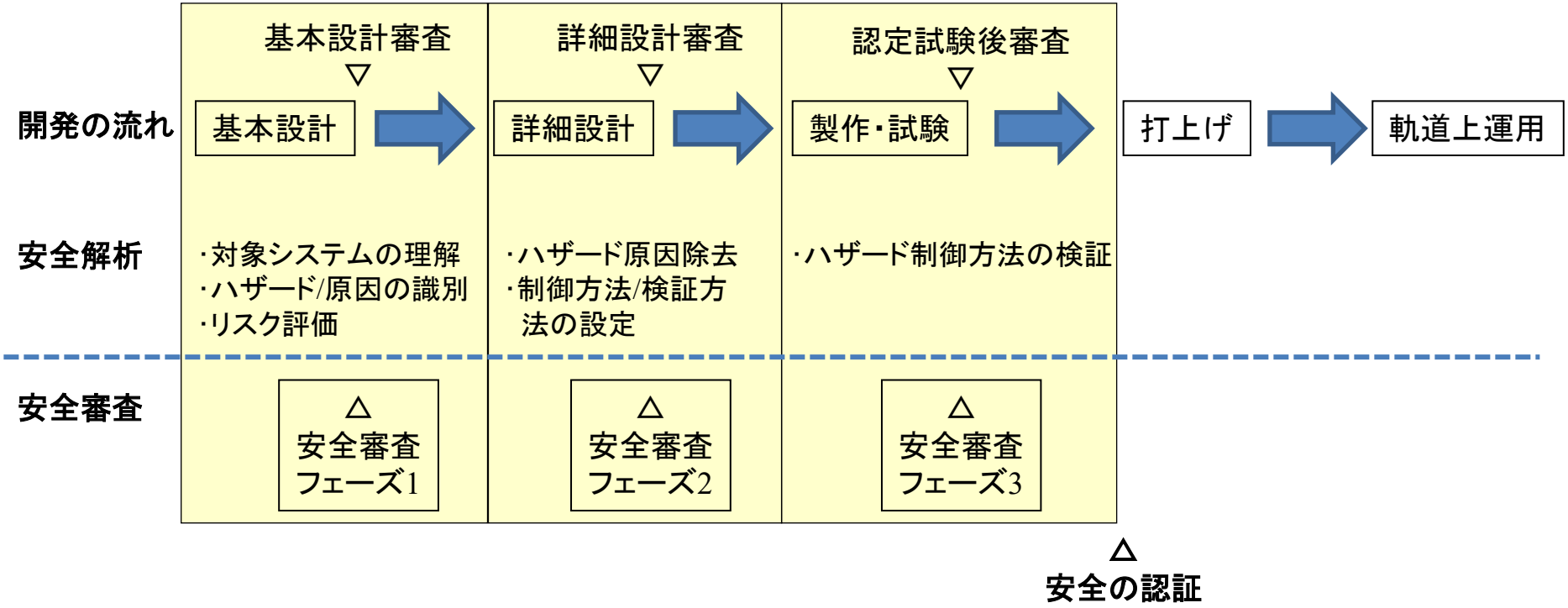
(3)有人活動の特殊性への配慮

「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(2/4)

(5)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。



(6)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(3/4)
ハザードの除去

発生の可能性をなくす →

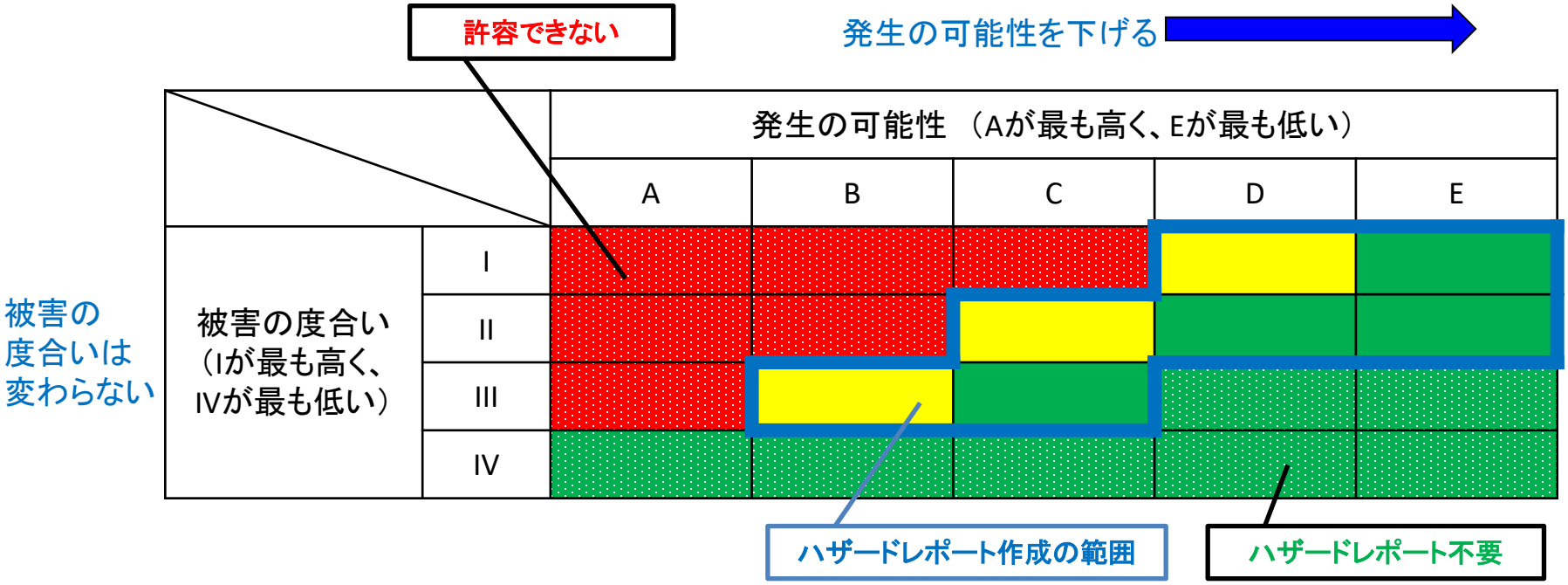
被害を生じさせない ↓

被害の度合い（Iが最も高く、IVが最も低い）	発生の可能性 （Aが最も高く、Eが最も低い）				
	A	B	C	D	E
I					
II					
III					
IV					

- 赤は許容できないもの、黄色は許容可否判断を必要とするもの、緑は許容可能なものと区別する。
- 「ハザードの除去」は、ハザード原因を設計により根源的に取り除くことにより、被害の発生あるいは発生の可能性をなくすことを目的とする。

被害の度合い	用語	説明
I	破局 (Catastrophic)	ISS搭乗員の死亡 ISSの喪失
II	重大 (Critical)	ISS搭乗員の重度な被害 ISSの重大な損傷
III	限界・局所的 (Marginal)	ISS搭乗員の軽度な被害 ISSの軽度な損傷
IV	無視可能 (Negligible)	ISS搭乗員に影響をもたらさない被害 ISSに影響をもたらさない損傷

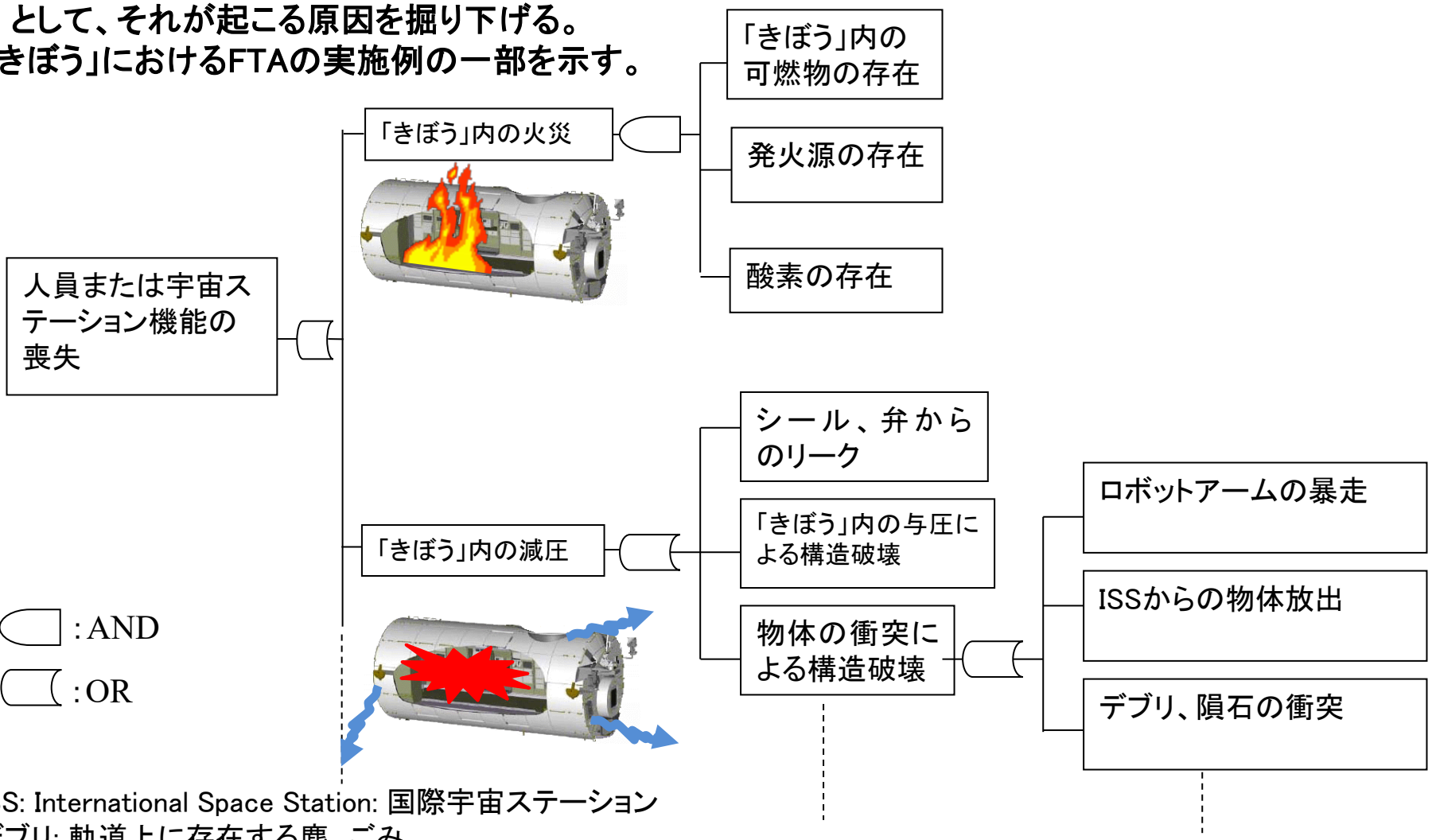
4.1. 安全確保の基本的な考え方(4/4)
ハザード制御



- 「ハザード除去」が出来なかったものを「ハザード制御」の対象とする。
- 「ハザード制御」は、発生の可能性を下げることを目的とし、最大の効果が有る手法により対策を講じる。
- ハザードの制御方法は検証可能なものとし、「ハザードレポート」を用いてハザード制御の有効性を判断する。

4.2. ハザード及びその原因の識別(1/3)
FTA (Fault Tree Analysis)

「人員または宇宙ステーションの喪失」をトップ事象
　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の実施例の一部を示す。



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

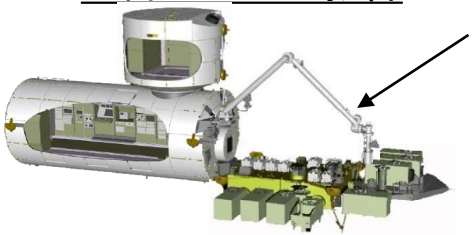
4.2. ハザード及びその原因の識別(2/3)
FMEA (Failure Mode and Effect Analysis)

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。

例：ロボットアームの故障モード

- 関節機構の作動不能
- 関節モータトルクの喪失
- ブレーキトルクの増大
- ブレーキトルクの低下／喪失
- 関節角度情報の誤認識
- 把持力の低下／喪失

故障モードの影響



アーム動作範囲の制約 → アームのミッション制約 → 「きぼう」ミッションの制約 → ハザードとはならない

アーム動作の停止不能
アーム姿勢異常
把持対象物の放出
→ アームや把持物が「きぼう」と衝突することによる構造損傷 → 「きぼう」内の減圧によるクルーの窒息死 → ハザード

4.2. ハザード及びその原因の識別(3/3)
標準ハザード

- ✓ ハザードレポートは「標準ハザード」と「ユニークハザード」の2種類にわけて起草する。
- ✓ 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、「標準ハザードレポート」を起草する。
- ✓ 「標準ハザードレポート」は過去の経験をもとに標準化されたハザードの制御・検証がひな形にされたものをもとに起草する。
- ✓ 現在、ISSでは14種別の標準ハザードレポートが用意されており、効率的な安全評価を実施するために活用されている。
- ✓ 標準化された方法以外で制御・検証するハザードは「ユニークハザード」を起草する。

番号	標準ハザード
1	可燃性材料の発火
2	船内環境の汚染（使用材料からのオフガス）
3	毒性物質、バイオハザードの漏洩
4	ガラス破片等の飛散
5	メカニカルハザードとクルー退避時の障害
6	高/低温部接触
7	クルーへのレーザあるいは電磁波の照射
8	騒音
9	不適切な接地による損傷
10	電力系の損傷
11	電力コネクタ着脱時の感電
12	非電離放射線
13	回転機器による損傷
14	シールを有する圧力容器による損傷

4.3. ハザード原因の除去/制御(1/5)

（1） ハザード原因の除去

一番優先すべきことは、ハザード原因を設計により根源的に取り除くこと。

例：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

ハザード原因を除去できないものについては、安全設計により対策を講じる。安全設計においては、基本的に故障許容設計によること。ただし、適切に設計し検証データを示すことができる場合は、設計マージンをとるといったリスク最小化設計によることができる。

（JMR-001システム安全標準より）

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. ハザード原因の除去/制御(2/5)

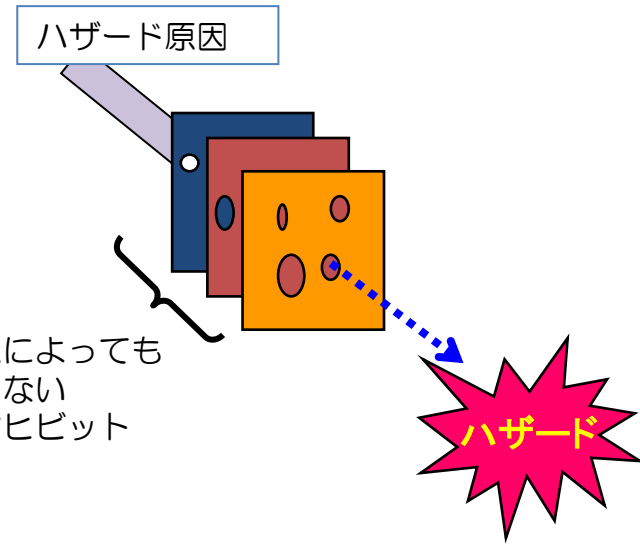
以下に優先順位の高い順にハザード制御方法を示す。

(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

故障許容設計



- 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. ハザード原因の除去/制御(3/5)

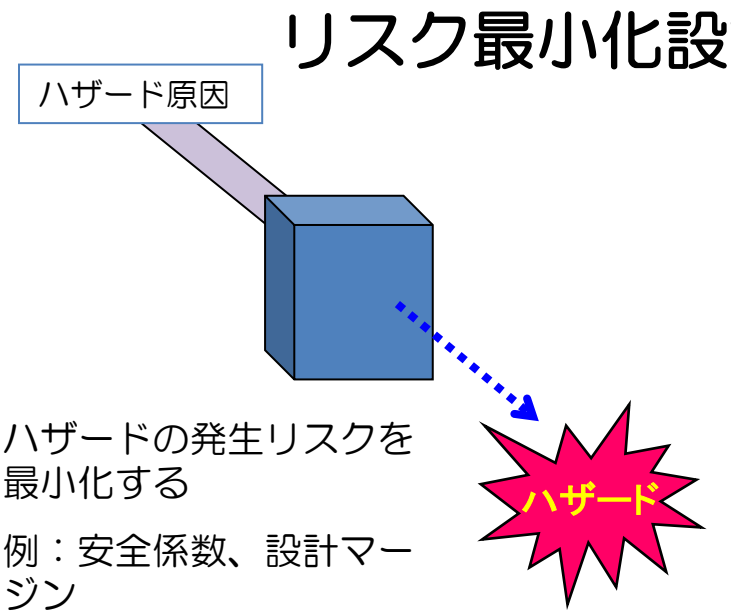
(2)リスク最小化設計

- 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. ハザード原因の除去/制御(4/5)

(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、合意文書*1でまとめて管理する。

*1:装置開発担当部門から運用手順書を作成する運用部門に申し送るための合意文書

4.3. ハザード原因の除去/制御(5/5)
ハザード発生時の対応

ハザードは、「人員または宇宙ステーション機能の喪失」をトップ事象としており、それが起こる原因を掘り下げて安全評価を行っている。人員とは、宇宙ステーションに搭乗している宇宙飛行士のことであり、宇宙ステーション機能が喪失した時の影響として一番先に考えることは宇宙飛行士の人命を守ることである。

宇宙飛行士の命に関わるハザードとして重要視しているのは、火災・減圧・汚染の3つである。ハザード発生時の対応の一例として、火災発生時の対応について以下に示す。

- 火災検知システム等の警報装置により監視し、二酸化炭素消火器による消火をする手順などが用意されている。
- 火を消し止められない場合、ハッチを閉めて安全なモジュールへ避難する。そして火災の発生したモジュール内を減圧し、消火する。
- 火災により、宇宙ステーションから避難する必要が生じた場合は、宇宙船(現在はソユーズ)に搭乗し、地球に緊急帰還する。
- 上記の緊急時への対応について、宇宙飛行士は地上での訓練に加え、宇宙ステーション到着直後に訓練を行っている。

これらのハザード発生時の対応は共通的に適応できるものであるため、全ての搭載品に対して個別に対応を用意することはせず、すでに確立されている共通的な方法を使うこととしている。

4.4. ハザード制御方法の検証(1/2)

（1）検証手段

ハザード制御方法が設計したとおり働く(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、検証完了まで管理する。

4.4 ハザード制御方法の検証(2/2)
ハザード制御後の発生確率

ISSの安全設計において、ハザード制御は発生の可能性を下げることを目的とし、最大の効果が有る手法により対策を講じている。よって、ハザード制御後のハザード発生確率は下がると言える。

ハザード被害の度合いが「I.破局(Catastrophic)」と「II.重大（Critical）」なものに対しては、発生確率によらず全てハザードレポートを起草し、ハザードの制御および検証が適切に行われてることを「見える化」している。

なお、「III.限界・局所的(Marginal)」で発生確率の判断で迷うものに対しては、原則としてハザードレポートを起草することとし、安全審査で技術評価を行っている。

ISSの安全審査では、ハザードレポートを用いて安全設計の妥当性や検証方法が最適なものになっているかの技術評価に時間をかけて審議し、ハザード発生確率の低減を確実に行っている。

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

安全審査のフェーズは0/I/II/IIIに分けている。

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、リスク評価 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。	・こうのとり(HTV) ・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

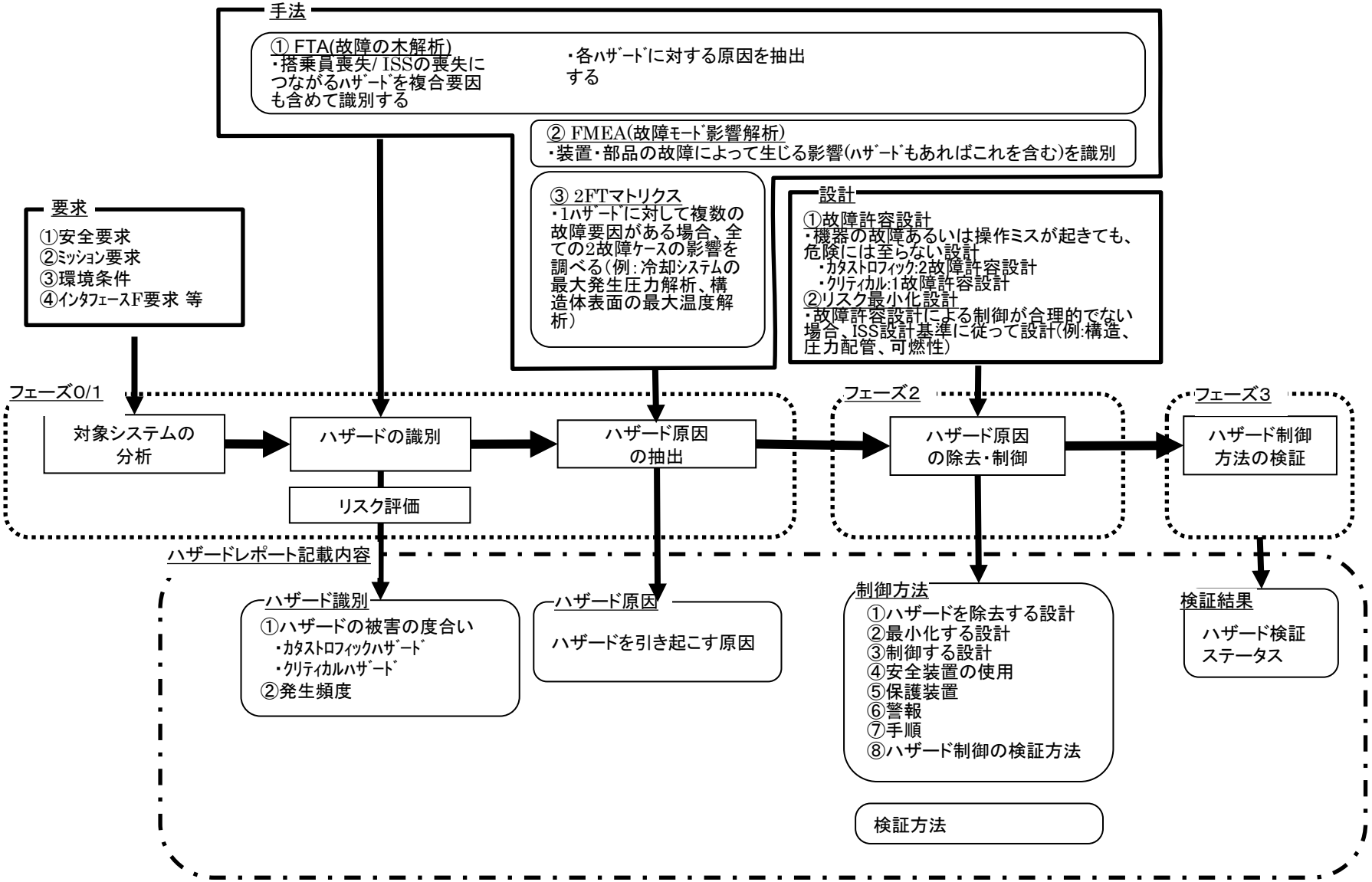
4.5. 安全審査(5/5)
NASAからの安全審査権限の委譲

- ✓ 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）。
- ✓ 近年、打上げ機数が増加している超小型衛星に対してはJAXAの権限委譲の調整を進めた結果、約半数はJAXAのみで安全評価を完結することができるようになり、新規参入者の敷居を下げることに貢献している。

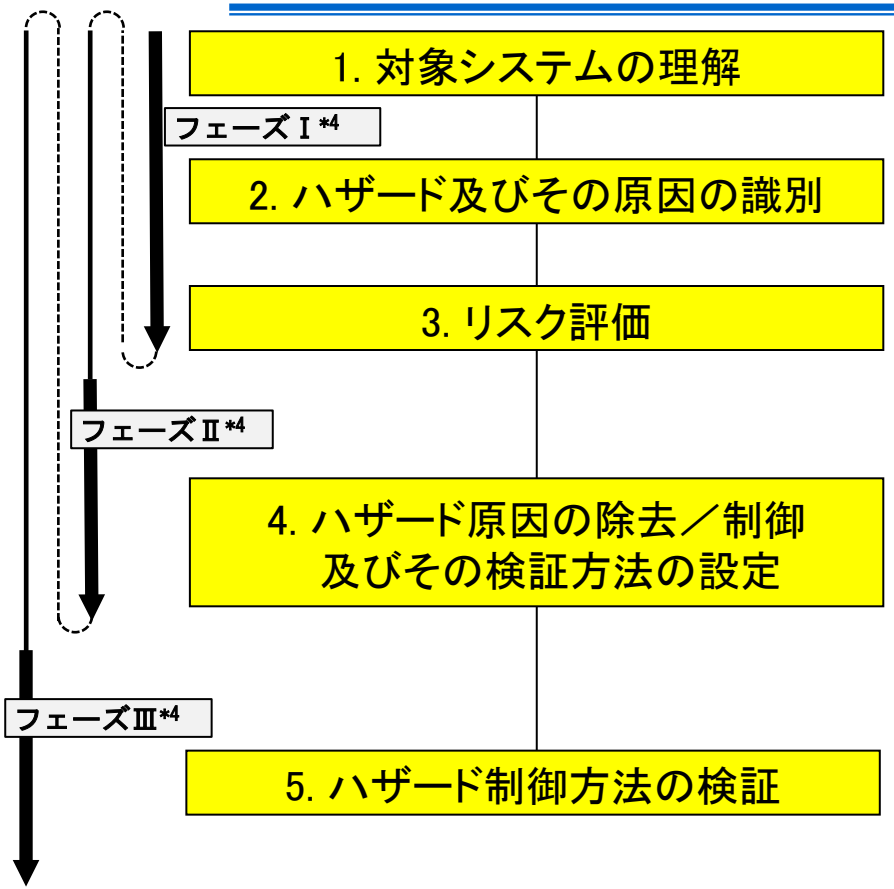
	NASAの関与	実験装置／ハザードの分類の例
1	なし	a. 標準ハザードのみ b. シリーズ品／再飛行品 c. 毒性が低い(毒性レベル1) d. 超小型衛星(特殊なハザード原因がないもの)
2	事前調整	a. 毒性が中程度(毒性レベル2) b. 保全やトラブルシュートに関連するハザード c. 以前のフライトで生じた不具合に関連するハザード
3	該当するハザードレポートの審査	a. 毒性が高い(毒性レベル3,4) b. 不適合報告書(NCR)を含む c. 船外活動(EVA)に関連するハザード

添付資料

添付1　安全設計の流れ


手法
① FTA(故障の木解析)
・搭乗員喪失/ ISSの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
リスク評価
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
ハザード識別
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
ハザードを引き起こす原因
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

添付2　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識別する。また、識別したハザードの原因を識別する。

・被害の度合い*1と発生の可能性の組み合わせでリスクを評価する。

・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

・ハザード制御方法を検証し、設定したハザード制御の有効性を確認する。

*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:フェーズI, II, III
フェーズI ：基本設計終了時
フェーズII：詳細設計終了時
フェーズIII：認定試験終了時

FTA：Fault Tree Analysis
FMEA：Failure Mode and Effect Analysis