資料4－1－3

宇宙ステーション補給機「こうのとり」4号機（HTV4）の接近・係留・離脱フェーズに係る安全検証結果について

平成25年6月20日

独立行政法人
宇宙航空研究開発機構

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 小沢　正幸

HTV: H-Ⅱ Transfer Vehicle

目　次

1. 概要

■ JAXAは、国際宇宙ステーション(ISS)協力の枠組みに則して、HTV4号機のISSへの接近・係留・離脱フェーズの安全性について確認・審査を行った。主な審査結果は以下のとおり。

- JAXA有人安全審査会　4月26日

  【結論】JAXAとしてはHTV4号機の安全性を確認した(全ハザードレポート(検証結果含む)の承認を完了した)

- NASA SRP　5月23日

  【結論】ISS全体の安全認証に責任を有する立場からNASAは、HTV4号機の安全性を確認した(全ハザードレポート(検証結果含む)の承認を完了した)

- JAXA安全審査委員会　5月28日

  【結論】JAXAとしてHTV4号機に係る有人安全審査会(及びNASA SRP)の審議結果を了承した

■ JAXAによる安全審査の妥当性について、評価をお願いする。

- 安全性確認の考え方、手法、プロセス
- 安全性確認結果の「宇宙ステーション補給機「こうのとり」(HTV)に係る安全対策の評価のための基本指針」※(平成24年9月6日 宇宙開発利用部会)への適合性

※以下、「基本指針」という。

2. HTVに対する安全性確認結果の概要

【HTV1～HTV3号機まで】

以下のステップで安全性を確認した。それぞれの確認結果については、宇宙開発委員会(平成24年7月に廃止)に報告し、妥当性の了解を得た。

(1) HTVによって起こりうるハザードをFTAを基に抽出し、個々のハザードに対して、原因の抽出、制御方法の設定と検証を行った。JAXA/NASAの安全審査会により、ハザードの識別、制御及び検証の妥当性を確認した。HTVのFTA概要をそれぞれ付図-1に示す。

(2) 上記で識別したハザードに対して基本指針項目への対応を整理した。結果を4.1項に示す。

(3) HTV1号機に対し、基本指針に対する設計・検証結果を網羅的に確認した。

(4) HTV2号機及びHTV3号機について、号機固有の変更事項を考慮してもHTV1号機と同様の安全性確保の方法が基本指針へ適合していることを確認のうえ、安全性が確保されていることを確認した。

【HTV4号機(今回)】

✓HTV4号機固有の変更事項を考慮してもHTV1号機と同様の安全性確保の方法が基本指針の定める要件を逸脱しないことを重点的に評価した。

✓また、HTV3号機までの運用実績等を踏まえ、HTV4号機に反映すべき対策等が適切に取り込まれていることを確認した。

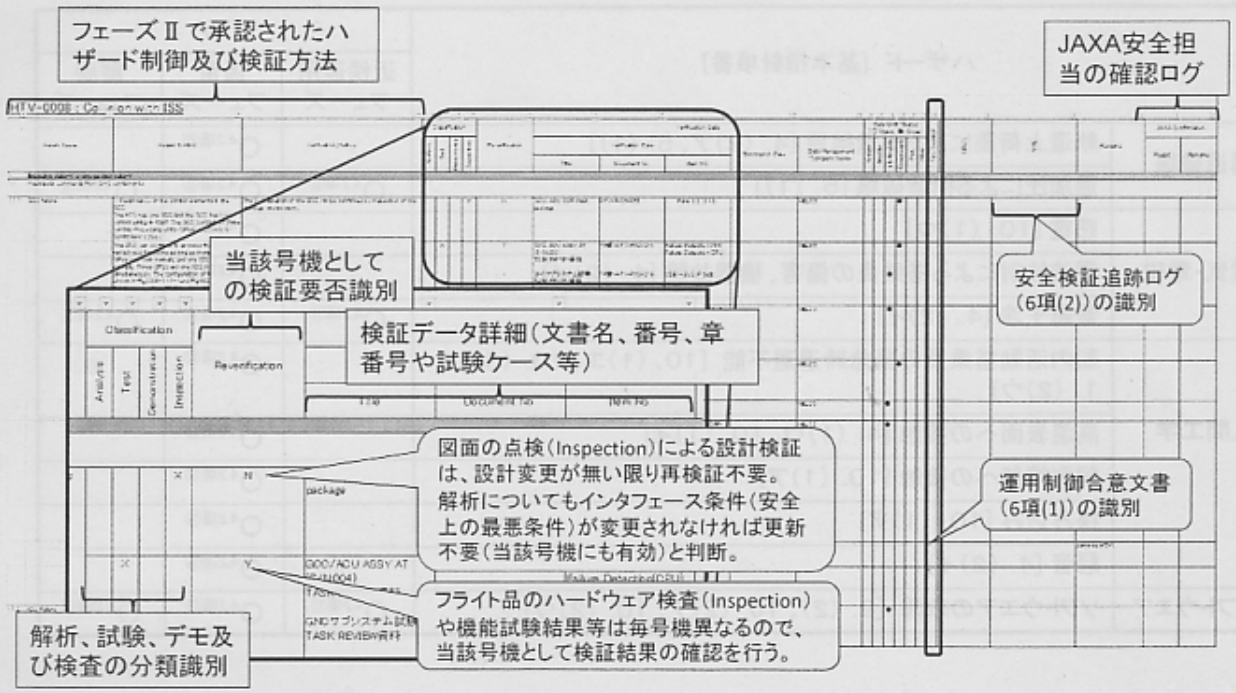
3. HTVの安全検証結果の確認方法

HTV1号機における安全性確認の結果を踏まえて、HTV2号機以降の安全制御及び検証については以下のような考え方で審査している。

- 設計や解析条件に変更がなく、後続号機にそのまま適用できる検証結果については後続号機の検証としても有効と判断。
- 設計変更、あるいは号機固有の設計がある場合には、従来機との差異がシステム全体のハザード制御に及ぼす影響を評価し、評価結果に応じてハザード原因の見直しや追加を行う。
- 号機固有の事項を含め、当該号機として検証が必要な項目については、全て識別し網羅的な検証結果確認を行う。

実際に検証結果確認に用いているフォームを次ページに示す。

3. HTVの安全検証結果の確認方法



4. HTV4号機の安全設計・検証結果

4.1 HTVに関するハザード及び対象フェーズ識別一覧(1/2)

ハザード［基本指針項番］		HTV		
		近傍運用フェーズ	係留フェーズ	離脱フェーズ
火災	火災［5.（2）、10.（3）、11.（1）、11(2)］		○4.2項①	
減圧	減圧［4.（1）ウ、11.（1）イ］		○4.2項②	
汚染	推進薬の船外搭乗員への付着による船内の汚染［4.（3）、6.（1）］		●4.3項(1)	
	船内空気汚染［4.（2）イ、5.（2）ア］		○4.2項③	
	ガラス破片飛散による搭乗員の傷害［10.（1）］		○4.2項④	
衝突	HTVのISSへの衝突［6、7、8、10.（4）］	●4.3項(2)		●4.3項(2)
	浮遊物のISSへの衝突［4.（3）］		○4.2項⑤	
	隕石／デブリの衝突(注1)［4.（1）ア、5.（2）イ］		○4.2項⑥	
	回転体の搭乗員への衝突［10.（1）］		○4.2項⑦	
爆発	推進薬システムの爆発［5.（1）、5.（2）ウ、6.（1）］	●4.3項(3)	●4.3項(3)	●4.3項(3)
	電池セルの破裂［8］	●4.3項(4)	●4.3項(4)	●4.3項(4)

注1：HTVは、打上げあるいは離脱時、隕石／デブリに衝突しない飛行経路を予め決定し飛行させるとともに、単独飛行中ISSに到着するまでは、必要により衝突回避のための軌道変更を行う。

○：「きぼう」と同様のハザード制御を設定しているもの
●：HTV特有のハザード制御を設定しているもの

4. HTV4号機の安全設計・検証結果

4.1 HTVに関するハザード及び対象フェーズ識別一覧(2/2)

ハザード［基本指針項番］		HTV		
		近傍運用フェーズ	係留フェーズ	離脱フェーズ
構造破壊	軌道上荷重による構造破壊［4.（2）ア、5.（1）］		○4.2項⑧	
	過加圧による構造破壊［5.（1）］	○4.2項⑧	○4.2項⑧	○4.2項⑧
電気・電磁	感電［10.（1）ウ］		○4.2項⑨	
	電波放射による搭乗員の傷害、機器故障［4.（2）イ］		○4.2項⑩	
	電磁干渉［4.（2）イ］	○4.2項⑪	○4.2項⑪	○4.2項⑪
人間工学	船内活動搭乗員の緊急時退避不能［10.（1）エ、10.（3）、11.（2）ウ］		○4.2項⑫	
	高温表面への接触［4.（1）ウ、10.（1）イ］		○4.2項⑬	
	鋭利端部への接触［10.（1）ア］		○4.2項⑭	
	挟み込み［10.（1）ア］		○4.2項⑮	
	騒音［4.（2）イ］		○4.2項⑯	
ソフトウエア	ソフトウエアの故障［9.（2）、10.（2）ア、10.（2）ウ］	○4.2項⑰	○4.2項⑰	○4.2項⑰

○：「きぼう」と同様のハザード制御を設定しているもの
●：HTV特有のハザード制御を設定しているもの

4. HTV4号機の安全設計・検証結果
4.2「きぼう」と同様なハザード制御の検証結果

－「きぼう」と同様な制御方法により対応した事項を以下に示す。いずれも検証作業が適切に行われたことを確認した。

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応（検証については下線を付す）	HTV4号機の対応及び検証結果	指針の対応項目
火災	I（カタストロフィック）	①非金属材料の燃焼により火災が発生し、船内活動搭乗員の死傷に至る。	【リスク最小化設計】 ・非金属材料に難燃性の材料を選定し、結果を使用材料リスト（MIUL）で確認した。 ・ヒータまたは電子機器の温度をモニタし、異常時に電力を遮断することで過熱を防止する設計となっていることを解析や試験で確認した。	・HTV4号機で更新された使用材料リスト（MIUL）を再確認し、追加された材料が難燃性の要求を満足することを確認した。 ・電力遮断に係るシステム設計解析（熱解析含む）についてはHTV1から変更なし。温度モニタや遮断機能に係るHTV4号機のハードウェアが健全であることを試験で検証した。	5.（2） 10.（3） 11.（1） 11（2）
減圧	I（カタストロフィック）	②HTVと船内と船外の間のシール部、または排気弁からの空気の漏洩により、船内が減圧し、船内活動搭乗員の死傷に至る。	【2故障許容設計】 ・シール部は2重とし、排気弁の意図しない開放を防止するため、2つのスイッチを設けた。それぞれ検査や試験で確認した。 ・万が一漏洩したとしても、搭乗員が退避する時間が確保できる設計であることを解析で確認した。	・モジュール隔壁部のコネクタやフランジシールの設計に変更はなく、HTV4号機としては実際に使用されるシールや排気弁のスイッチが健全であることを試験で確認した。 ・万が一漏えいした場合の退避シナリオはフライトルールとして確立しており、HTV4号機として検証は不要。	4.（1）ウ 11.（1）イ
汚染（推進薬による汚染を除く） ・船内汚染 ・ガラス・他	II（クリティカル）	③非金属材料からのオフガスにより船内空気が汚染され、搭乗員の健康を阻害する。	【リスク最小化設計】 ・構造・内装・搭載機器等に使用される非金属材料は、オフガス発生量の少ない材料を選定し、機器・ラック及びモジュールレベルの試験で許容範囲内であることを確認した。	・HTV4号機で更新された使用材料リスト（MIUL）を再確認し、追加された材料がオフガス発生量の要求を満足することを確認した。 ・打上げ前の形態でモジュールレベルの試験を行い、オフガス濃度が許容範囲内であることを確認する予定。（6項4番）	4.（2）イ 5.（2）ア
		④ガラスの破片、地上での組み立て時に船内残留する金属片による搭乗員の目・肺への障害に至る。	【リスク最小化設計】 ・ガラス機器は、破片が飛散しないように封入設計となっていることを検査で確認した。また初入室時にはゴーグルを装着する手順であることを確認した。	・船内で使用する照明装置が設計とおり（封入対応）であることを受け入れ検査で確認した。 ・軌道上で入室する際の手順（ゴーグル着用）は既にフライトルールとして確立しており、HTV4号機として検証は不要。	10.（1）

4. HTV4号機の安全設計・検証結果
4.2「きぼう」と同様なハザード制御の検証結果

「きぼう」と同様な制御方法を用い、その有効性を検証した事項（つづき）

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応（検証については下線を付す）	HTV4号機の対応及び検証結果	指針の対応項目
衝突（HTVのISSへの衝突を除く） ・浮遊 ・デブリ ・回転体	I（カタストロフィック）	⑤HTVの分離機構の意図しない動作により機器が放出し、他のISS機器へ衝突し、居住モジュールの破損による搭乗員の死傷にいたる。	【2故障許容設計】 ・分離機構のアクチュエータに3つのスイッチを設け、意図しないタイミングに機構が動作するのを防止する設計とした。機能試験や射場での組み立て時にスイッチが正常であることを確認した。	・HTV4号機のフライトハードウェアが健全であることや、システムとして適切に機能することについて受け入れ検査、機能試験で確認した。また、射場での組み立て時にスイッチが正常であることを確認する。（6項2番）	4.（3）
		⑥隕石・スペースデブリがHTV与圧キャリアへ衝突すると船内活動搭乗員への致命的な事象にいたる。またHTV圧力容器への衝突は、容器破裂による破片またはHTV自体のISSへの衝突にいたる。	【リスク最小化設計】 ・直径1cm以下のデブリは、スタッフィング入りバンパによる貫通防御対策を行う。バンパの有効性については要素試験で検証し、実機にバンパが適切に取り付けられていることを検査で確認した。 ・直径10cm以上のデブリに対しては、ISSの軌道制御により衝突回避する手順となっていることを、手順書（フライトルール）にて確認した。 ・直径1～10cmのデブリに対しては、衝突により与圧モジュールをデブリが貫通した場合、搭乗員は安全なモジュールへ退避する手順を手順書（フライトルール）にて確認した。。	・バンパが検証済みの設計とおりに製作されていることを検査で確認した。また、全てのバンパが所定の場所に取り付けられることを射場で確認する予定。（6項4番） ・直径10cm以上のデブリを回避する運用については、フライトルールに基づき適切に実施されており、HTV4号機固有の事項はない。なお、衝突リスクに応じて回避行動以外に搭乗員の（帰還機への）避難対応も追加されている。 ・万が一デブリが衝突した場合の対応手順についても確立しており、HTV4号機固有の事項はない。	4.（1）ア 5.（2）イ
		⑦HTVキャビンファンの破損により生じた破片が飛散し、他のISS機器へ衝突による居住モジュールの破損または直接搭乗員へ衝突するこにより死傷に至る。	【リスク最小化設計】 ・ファンは、ハウジング等により、破片の飛散が防止されていることを検査にて確認した。	・HTV4号機で使用するフライトハードウェアが設計とおりであることを検査で確認した。	10.（1）

4. HTV4号機の安全設計・検証結果
4.2「きぼう」と同様なハザード制御の検証結果

「きぼう」と同様な制御方法を用い、その有効性を検証した事項（つづき）

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応（検証については下線を付す）	HTV4号機の対応及び検証結果	指針の対応項目
構造破壊 ・軌道上荷重 ・過加圧	I（カタストロフィック）	⑧軌道上荷重（リブーストによる荷重、圧力荷重等）により構体の破損や把持構造の損傷によりISSを損傷し搭乗員に致命的な影響を与える。	【リスク最小化設計】 ・打上げ・軌道上・帰還・着陸等の定常運用における全ての荷重モードに対し十分な剛性・静強度・疲労強度を持つよう設計し解析で検証した。なお、構造解析に使用した構造数学モデルは、試験を実施し、ハードウェアとの相関性を確認した。また構造部材は疲労解析を行い十分な疲労寿命を有することを確認した。 ・運用中の最大荷重またはH-IIBとの共振を防止するため、規定の剛性・強度を持つよう設計し、PFMモデルを用いた静荷重試験で確認した。 ・耐熱性・耐食性・耐応力腐食性・耐電食性等を考慮し、過去の実績のある構造材料を選定したこと材料識別使用リスト(MIUL)、及び材料使用合意書(MUA)で確認した。 ・与圧構造の許容圧力を超えないように、適切な熱制御を行うことで、最悪条件でも許容圧力を超えないことを解析で検証した。	・従来から設定されている構造部材に対する破壊管理計画を適用し、HTV4号機のフライト品主構造が適切に製造されたことを破壊管理報告書（各種検査記録等を取りまとめた文書）で確認した。 ・曝露パレットについてはHTV4号機固有の搭載構造となるため、構造解析（解析検証の不確定係数を加算）にて、十分な強度を有していることを確認した。 ・HTV4号機で更新された使用材料リスト（MIUL）を再確認し、HTV4号機で更新された使用材料リスト（MIUL）を再確認し、HTV4号機で追加された部材等については、過去の実績のある適切な構造材料が選定されたことを確認した。なお、構造材料に係る材料使用合意書（MUA）の更新はない。 ・許容圧力に係る解析についてはHTV1号機から変更はなく、解析の前提となる熱制御や圧力リリーフ機能の健全性についてはHTV4号機を用いた試験等で確認した。なお、圧力リリーフ機能の最終確認は射場で行われる予定。（6項4番）	4.（2）ア 5.（1）

4. HTV4号機の安全設計・検証結果
4.2「きぼう」と同様なハザード制御の検証結果

「きぼう」と同様な制御方法を用い、その有効性を検証した事項（つづき）

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応（検証については下線を付す）	HTV4号機の対応及び検証結果	指針の対応項目
感電・電磁放射 ・感電 ・電波放射 ・EMI	I（カタストロフィック）	⑨搭乗員が高電圧表面に触れることにより感電し、搭乗員の死傷にいたる。	【リスク最小化設計】 ・高電圧露出表面のないこと、また適切に接地されていることを検査で確認した。	・HTV4号機の機器等が適切に接地されたことを検査で確認した。なお、HTVの構成要素間の接地等については射場で確認する。（6項3番）	10.（1）ウ
		⑩HTVからの意図しない電波放射により船外活動用宇宙服の誤動作に至る。	【リスク最小化設計】 ・HTVアンテナから放射される電波が、想定される船外活動実施場所で十分要求値内まで低減することを電磁干渉試験（放射・伝導雑音試験及び放射・伝導感受性試験で確認した。 ・また、HTVアンテナ周囲の危険範囲識別の為に、解析結果に基づくキープアウトゾーンが設定されてることを（フライトルールにて）確認した。	・HTV4号機に搭載するアンテナが要求仕様を満足していることを受け入れ試験で確認し、HTV1号機で設定したキープアウトゾーンがHTV4号機に対しても有効であることを確認した。。	4.（2）イ
		⑪ISSからの電磁波による電磁干渉により、安全上の機器が誤動作する。またHTVから発せられる電磁波により、ISS或いは他装置の安全上重要な機器が誤動作する。	【リスク最小化設計】 ・ISS或いは他装置の放射・伝導電磁環境にマージンを加えた環境に対し、HTVの機器が誤動作しないよう設計した。また、HTVが発生する放射・伝導による電磁波が、ISS或いは他装置が許容できる電磁環境レベルより十分に低くなるよう設計した。これらの設計の妥当性についてはEMC試験で確認した。また、最終的に射場でボンディング抵抗を計測し、電磁干渉評価の前提条件が確立していることを確認した。	・曝露パレットを除きEMCに影響する設計に変更はない。 ・曝露パレットについてはHTV4号機の仕様として電磁干渉の問題がないことを解析で確認した。 ・フライトハードウェアが適切にボンディング／グラウンディングされていることを検査で確認した。最終的にHTVの構成要素間の接地等については射場で確認する。（6項3番）	

4. HTV4号機の安全設計・検証結果
4.2「きぼう」と同様なハザード制御の検証結果

「きぼう」と同様な制御方法を用い、その有効性を検証した事項（つづき）

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応（検証については下線を付す）	HTV4号機の対応及び検証結果	指針の対応項目
不適切な人間工学設計（船内搭乗員退避不能、鋭利な端部、突起物、騒音） ・退避不能 ・エッジ ・挟み込み	I（カタストロフィック）	⑫減圧、火災等の発生時に船内搭乗員の退避路、HTVの隔離ができず、搭乗員の死傷に至る。	【リスク最小化設計】 ・搭乗員の退避に必要な経路は、ISS共通基準に基づく設計とし、適切な通路幅等が確保できること等を検査で確認した。また隣接モジュールの警告・警報音がHTV内でも認識できることを解析で確認した。	・船内のレイアウト（キャビン空間）についてはHTV1同様でありHTV4号機としての確認事項はない。 ・緊急退避経路が識別されていることについて、フライトハードウェアの検査で確認した。 ・ファンの騒音が十分小さいことを試験で確認した。	10.（1）エ 10.（3） 11.（2）ウ
		⑭船内搭乗員：装置の鋭利端部・突起物により、船内活動搭乗員の皮膚の裂傷に至る。 船外搭乗員：装置の鋭利端部・突起物により、船外活動中の搭乗員の手袋、衣服に穴が開き、搭乗員の死傷に至る。	【リスク最小化設計】 ・ISS共通の安全標準に基づき、装置は許容できない鋭利端部・突起物或いは隙間がない設計となっていることを検査で確認した。	・フライトハードウェアに鋭利な部位や突起が残っていないことを検査で確認した。 ・太陽電池パネル等、機能上鋭利な部位を除去できないものについて、キープアウトゾーンが設定されていることを手順書で確認した。	10.（1）ア
		⑮船内搭乗員：装置の隙間に搭乗員が挟み込まれ、指等の障害に至る。 船外搭乗員：装置の隙間、または可動機構に搭乗員が挟み込まれ、船内へに帰還できず、死傷に至る。	【リスク最小化設計】 ・機器の隙間は、ISS共通基準に基づく大きさとなっていることを検査で確認した。また、搭乗員が巻き込まれる恐れがある可動機構に対し、キープアウトゾーンが手順書に規定されていることを確認した。	・フライトハードウェアに挟み込みの懸念がある部位がないことを検査で確認した。 ・HTV4号機ではキープアウトが必要となる可動機構はない。	

4. HTV4号機の安全設計・検証結果
4.2「きぼう」と同様なハザード制御の検証結果

「きぼう」と同様な制御方法を用い、その有効性を検証した事項（つづき）

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応（検証については下線を付す）	HTV4号機の対応及び検証結果	指針の対応項目
不適切な人間工学設計（高温/低温部への接触） ・騒音 ・高温		⑯船内の過度の騒音により、搭乗員の難聴に至る。	【リスク最小化設計】 ・船内の騒音レベルは、ISS共通基準に基づく許容レベル以下となるよう設計し、これを試験で確認した。	・HTV4号機のファンから出る騒音が許容値内であることを試験で確認した。	4.（2）イ
	II（クリティカル）	⑬装置の高温部または低温部に搭乗員が触れ、火傷または凍傷を負う。 ※船外活動員に対する許容外表面温度：-117～112℃ ※船内活動員に対する許容外表面温度：-18～49℃	【1故障許容設計】 ・外部環境の最悪条件下において、実験装置内のいかなる機器の1故障（ヒータオン故障が最悪ケースと想定された）によっても、搭乗員が許容できる外表面温度となっていることを解析で確認した。なお、熱解析モデルは熱試験にてコリレーションしたものを用いた。	・解析条件の前提としてヒータシステムが適切に機能することをフライト品の機能試験で確認した。 ・曝露パレットについてはHTV4号機の仕様として問題となる高温／低温部がないことを解析で確認した。	4.（1）ウ 10.（1）イ
ソフトウェア	I（カタストロフィック）	⑰飛行管制、分離機構等のHTVの安全上重要なソフトウエア機能の誤動作により、HTVのISSへの衝突、機器の意図しない分離により他のISS機器へ衝突し、居住モジュールの破損による搭乗員の死傷にいたる。	【故障許容またはリスク最小化設計】 ISS共通のソフトウェア安全要求を適用した。 ・機能喪失がハザードとなる場合、独立した複数機能を搭載する。 ・不意起動がハザードとなる場合、危険な機能の起動に対する3重インヒビットを設ける。 ソフトウェアの検証として以下を実施した。 ・ソースコードの審査 ・ソフトウエア単体試験 ・シミュレータ試験 ・独立部門による独立評価（IV&V） ・ハードウェア搭載後のシステム試験	・ソフトウェアの更新部（影響範囲）に対し、以下の試験を実施し変更の妥当性を確認した。 ・ソースコードの審査 ・ソフトウエア単体試験 ・シミュレータ試験 ・フライトハードウェア搭載後のシステム試験	9.（2） 10.（2）ア 10.（2）ウ

4. HTV4号機の安全設計・検証結果
4.3 HTVに特有なハザード制御の検証結果

(1) 推進薬の船外クルーへの付着による船内の汚染

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応（検証については下線を付す）	HTV4号機の対応及び検証結果	指針の対応項目
推進薬の船外クルーへの付着による船内の汚染	I（カタストロフィック）	HTVの推進薬燃料（モノメチルヒドラジン：MMH）、酸化剤（四酸化二窒素：NTO）共に人体には有害であるため、宇宙飛行士の推進薬への接触は、推進系を有するHTV固有のハザードとなる。即ち、HTVから大量に推進薬が漏洩した場合、一部が宇宙服に付着し、船内に持ち込まれる可能性がある。	【2故障許容設計】 a. 前方スラスタ設置近辺は船外活動が想定されるため、バルブを3重に設置し、大量漏洩を避けられるような設計となっていることを検査で確認した。また、バルブや配管等に漏れが無いことを漏洩性能試験で確認した。 b. 船外活動中に不意のスラスタ開放指令を出さないよう、制御系を停止させる手順とした。	a. HTV4号機も同様の設計となっており、スラスタ弁が漏えいしても上流の遮断弁を閉じることで大量漏洩に至らないような処置が可能である。なお、HTV2号機までは船外活動時に無条件で上流の遮断弁も閉じていたが、HTV3号機運用時のNASA船外活動責任者の判断を踏まえ、HTV4号機では軌道上で行うスラスタ弁のリークチェックが要求を満足すれば、遮断弁は開いたままで運用してもよいこととなった。遮断弁の機能（シール性や耐圧性）及びシステムの動作の妥当性について単体の検査及び機能試験で確認した。また、射場で設定する締手が漏えいしないことや、システムがバルブを適切に制御できることについて射場で最終確認する予定。（6項1番） b. スラスタ弁が開かないように制御系を停止させる運用はHTV4号機でも変更ない。制御系が適切に停止できることについては機能試験で確認した。	4.（3） 6.（1）

4. HTV4号機の安全設計・検証結果
4.3 HTVに特有なハザード制御の検証結果

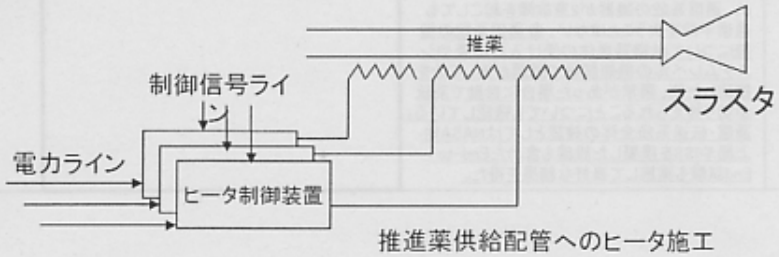
(2) HTVのISSへの衝突 (1/4)

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応（検証については下線を付す）	HTV4号機の対応及び検証結果	指針の対応項目
HTVのISSへの衝突	I（カタストロフィック）	誘導制御系の故障によりHTVが正しく制御できなくなりISSに衝突してしまう。	【2故障許容設計】 a. 誘導制御計算機は3つのCPUを有し、それぞれが同時に入出力コントローラに計算結果を出力し、入出力コントローラが3つのCPUからの出力を多数決で比較する設計とした。このため、CPUの1台が故障しても飛行を継続できる。また、入出力コントローラは2系あり、1台が故障しても、他系が処置を行える設計とした。上記計算機やコントローラの機能性能についてはソフトウェアを組み合わせた試験で検証を実施した。 b. 誘導制御計算機内で2故障が発生した際に、自動で緊急離脱系へ切り替わることについて試験で確認した。	a. HTV4号機のフライトハードウェアが所定の機能を提供できることについて、機器単体及びソフトウェアを組み合わせた試験で確認した。 b. HTV4号機の誘導制御計算機及び緊急離脱装置間のインタフェース試験において、自動で緊急離脱系へ切り替わることを試験で確認した。	7 10.（4）
		センサ系の異常によりHTVが正しく制御できなくなりISSに衝突してしまう。	【2故障許容設計】 a. 誘導制御に必要なセンサは、すべて2個以上設置し、計測値の比較等も踏まえて1故障許容設計とした。センサの機能性能等については購入時の製品検査や機能試験で確認した。 b. センサが2故障した場合、すなわちセンサの出力値が信頼できないような場合は、誘導制御計算機から緊急離脱制御装置に切り替わり、緊急離脱できることを試験で検証した。	a. 誘導制御に使用されるセンサの構成について、HTV1号機から変更はない。HTV4号機のフライト品センサについて、機能性能に問題が無いことを製品検査及び機能試験で確認した。 b. センサ異常に対応する処理ロジックは誘導制御計算機に搭載されソフトウェアに組み込まれているが、該当する処理ロジックに変更はない。	7 10.（4）

4. HTV4号機の安全設計・検証結果
4.3 HTVに特有なハザード制御の検証結果

(2) HTVのISSへの衝突 (2/4)

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応 (検証については下線を付す)	HTV4号機の対応及び検証結果	指針の対応項目
HTVのISSへの衝突	I (カタストロフィック)	推進系の故障でHTVが正しく制御できなくなりISSに衝突してしまう。	【2故障許容設計】 a. 姿勢制御系統を構成するバルブ・推進系の圧力、温度センサ等の機能部品が故障した場合、別系統に切り替えることで1故障許容とできる設計とした。各系統の機能や系統切り替えが問題無くできることについて試験で確認した。 b. 2故障時は、自動で緊急離脱系へ切り替わることについて試験で確認した。	a. 推進系のバルブ・圧力、温度センサ等の故障に対応する処理ロジックは誘導制御計算機に搭載されソフトウェアに組み込まれているが、該当する処理ロジックに変更はない。 b. HTV4号機の誘導制御計算機及び緊急離脱装置間のインタフェース試験において、自動で緊急離脱系へ切り替わることを確認した。	6. (2) 10. (4)
		推進系配管の凍結、破損後の漏洩により、HTVが正しく制御できなくなりISSに衝突してしまう。	【2故障許容設計】 姿勢制御系統、メインエンジン系統が繋がっている主要な配管／バルブ／推進薬タンクへのヒータ3重化の施工により、2故障許容設計とした。熱解析の結果、ヒータ1系統だけでも凍結が防止できることを確認した。また、ヒータシステムの機能性能についてはシステム試験等で問題無いことを確認した。	ヒータ故障時の凍結防止に係る温度解析については、環境条件や熱設計に変更がないため従来の解析が有効である。熱解析の前提条件ともなっているヒータシステムの機能については、機能試験で問題ないことを確認した。	6

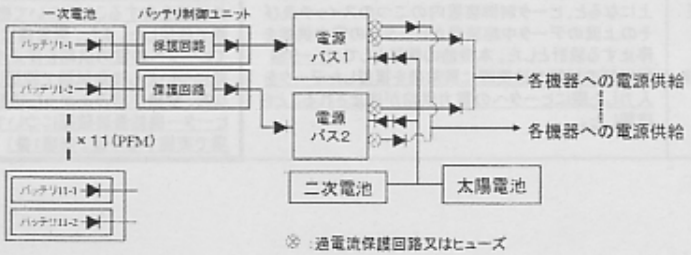


推進薬供給配管へのヒータ施工

4. HTV4号機の安全設計・検証結果
4.3 HTVに特有なハザード制御の検証結果

(2) HTVのISSへの衝突 (3/4)

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応 (検証については下線を付す)	HTV4号機の対応及び検証結果	指針の対応項目
HTVのISSへの衝突	I (カタストロフィック)	電源系の異常によりHTVが機能喪失してISSに衝突してしまう。	【2故障許容設計】 単独飛行中は、太陽電池及び二次電池並びに一次電池からの供給電力で飛行する。一次電池の個数は、運用上必要な容量を解析評価した上で2故障時の最悪シナリオを賄える個数のセルを搭載した。バッテリ及びその周辺回路がISS共通の要求に適合していることについては検査及び試験で確認した。	HTV1号機は一次電池を11台搭載していたが、実際の運用で一次電池がほとんど消費されなかった(太陽電池と二次電池だけでほとんど賄えた)ため、運用実績を踏まえてHTV2号機からマージンを見直した。この結果、一次電池の台数はHTV2号機から7台に変更され、HTV4号機でも7台搭載している。 HTV4号機に搭載されるバッテリ及びその周辺回路がISS共通の要求に適合していることについて、検査及び試験で確認した。 なお、打上げ前にバッテリが適切に充電されることについては射場で確認する予定。(6項4番)	8



※：過電流保護回路又はヒューズ

4. HTV4号機の安全設計・検証結果
4.3 HTVに特有なハザード制御の検証結果

(4) 電池セルの破裂

ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応 （検証については下線を付す）	HTV4号機の対応及び検証結果	指針の対応項目
電池セルの破裂	1 （カタストロフィック）	短絡で大電流が流れた場合の電池温度上昇によって、内圧が上昇しセルが破裂してしまう。	【リスク最小化設計】 個々の電池セル内に、過大な電流が流れたときに溶断して電流を遮断するヒューズが設けられていることを製品検査で確認した。 一次電池の放電を行うバッテリ制御ユニットの保護回路（過電流を検出して電流を遮断する）が適切に作動することを機能試験で確認した。	電池セルにヒューズが設けられていることを製品検査で確認した。また、過電流を検出して電流を遮断する機能が動作することを機能試験で確認した。	8
		逆電圧や過充電等、不適切な電圧制御により電池セルが損傷して破裂に至る。	【２故障許容設計】 一次電池に対しては、多段の逆流防止回路により逆電圧を防止できる設計になっていることを製品検査で確認した。 二次電池については、充電回路やバス電圧監視機能が冗長化され、適切に機能することを機能試験で確認した。	一次電池に対し、多段の逆流防止回路が周辺回路に組み込まれていることを検査で確認した。 二次電池に対し、冗長化された充電回路やバス電圧監視機能が適切に機能することを機能試験で確認した。	8
		電池の容器が十分な耐圧強度を有していない、あるいは圧力リーフができずに破裂してしまう。	【リスク最小化設計】 電池容器が使用圧力に対して適切な安全率を確保していることについて製品検査で確認した。 また、万が一の内圧上昇時に圧力リリーフを行うためのラプチャ（破断）機構が適切に機能することを実証試験で確認した。	HTV4号機に搭載される電池セルが要求仕様に適合していることを製品検査で確認した。また、電池セルにHTV1号機と同一仕様のラプチャ（破断）機構があることも製品検査で確認した。	8

5. HTV3号機ミッションからの反映／変更事項への対応

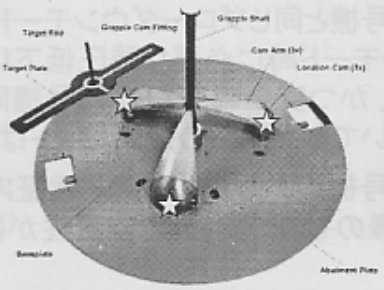
(1) 衝突回避マヌーバ（アボート）が実行されたことへの対応

平成24年第4回宇宙開発利用部会で報告の通り、HTV3号機がISSから離脱する際、ISSのロボットアーム（SSRMS）から意図しない初速が与えられ、設定された安全領域を越えてISSに接近する可能性が検知されたために衝突回避マヌーバ（アボート）が実行された。

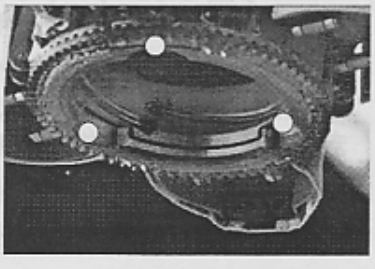
【初速が与えられた推定原因】

SSRMSがHTVを放した後、矢印方向に移動（Back Away）させる際、SSRMS把持機構側のポケット（〇印）とHTV側把持構造のカム部（☆印）で示した3か所の接触部の摩擦によってHTVが引っ張られてしまった。

HTV離脱時のSSRMS移動方向（矢印）



HTV側の把持構造



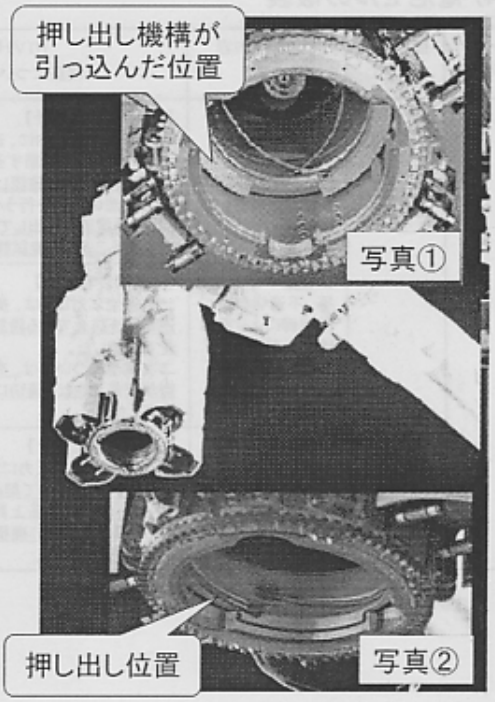
SSRMSの把持機構

5. HTV3号機ミッションからの反映／変更事項への対応

【HTV4号機以降の対策】
HTV4号機以降に同事象が再発することを防止するため、NASA及びカナダと共同でHTVの離脱方式について技術検討をすすめた結果、以下のような運用を行うこととなった。

- 従来は写真①のようにSSRMSの把持機構内部の押し出し機構を使わずに（引っ込んだまま）SSRMSをHTVから引き離していた。
- HTV4号機からは、写真②のように押し出し機構を駆動してHTVとSSRMSを強制的に分離し、その後SSRMSを移動する運用とする。

本変更はISSへの衝突ハザード制御に影響するため、新たに設けられたインタフェース条件（押し出しによる外乱）を加味してHTVの姿勢制御等への影響を追加検証（解析）した。その結果、従来どおりの制御方法をそのまま適用しても安全が確保できることを確認した。



5. HTV3号機ミッションからの反映／変更事項への対応

(2) HTV2号機と同じ海外調達スラスタを適用することの影響評価

- HTV2号機までは海外調達スラスタを使用したが、HTV3号機では国産スラスタを使用し、推進系の運用モードをブローダウンモード（加圧源を遮断しタンク残圧のみで飛行する）から調圧モード（ヘリウムガスで継続的にタンクの圧力調整を行う）に変更した。
- このため、HTV3号機では国産スラスタ及び推進系運用モードの変更によって新規に識別すべき、あるいは影響を受けるハザードの有無を確認し、更に原因事象や制御内容の見直しの必要性について評価した。結果、一部ハザードについて制御及び検証方法の見直しを審議・承認し、検証結果については従来通りの制御・検証を行うものを含めて妥当であることを確認した。
- HTV4号機ではスラスタがHTV2号機で使用した海外調達品に戻るため、推進系の運用モードについてもHTV2号機と同じブローダウンモードに戻すか検討した。結果、調圧モードではブローダウンモード時に必要な残圧低下に対する補加圧が不要になる等運用上のメリットがあり、かつ安全制御もHTV3号機同様に対応できることが確認できたため、HTV4号機についても推進系の運用モードは調圧モードにすることとした。
- 従って、本件に係るHTV4号機のハザード制御／検証内容は（スラスタ固有の検証事項を除き）HTV3号機と同様のもので実施し、安全性が確保されていることを確認した。

5. HTV3号機ミッションからの反映／変更事項への対応

(3) 号機固有の曝露パレット搭載品によるハザード制御の影響評価

・曝露パレットにペイロード(P/L)を搭載して打ち上げる場合、ペイロードに応じてJAXAが開発した結合機構(HCAM)またはNASAが開発した結合機構(FRAM)を選択することとなる。

・各号機への搭載実績

HTV1号機・・・HCAM P/L×2式

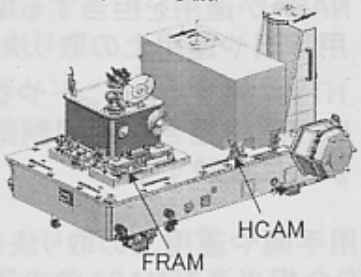
HTV2号機・・・FRAM P/L×2式

HTV3号機・・・HCAM P/L×1式

FRAM P/L×1式

HTV4号機・・・FRAM P/L×3式

(HTV3号機)



・HTV4号機では形態が類似しているHTV2号機(FRAM P/L搭載時)のハザード制御をベースとした安全性確保の方法によって、制御の妥当性について確認した。

5. HTV3号機ミッションからの反映／変更事項への対応

その他のHTV3号機からの変更事項

	項目	内容	安全上の影響評価
(4)	スタンドオフCTBコンテナの搭載	HTV2号機で搭載したCTB搭載構造(HTV3号機では搭載せず)を2式搭載する。	HTV2号機のハザード制御と同様の安全性確保の方法により、一般的な構造としての安全性(強度やシャープエッジ等が問題ないこと)が確認されているため問題なし。
(5)	NASA開発品の水バッグ搭載	HTV2号機で搭載したNASAが設計、製造及び検証した飲料水コンテナ(HTV3号機では搭載せず)を24式搭載する。	バッグ本体が漏れないこと等についてはNASAが責任を有する。JAXAは打上げ環境条件の保証及びNASAが設定した手順に従って充填や梱包が実施できたことを確認しNASAの了解を得ている。
(6)	表面電位センサの設置	太陽電池パネルを1枚取り外し、表面電位センサを取り付ける。	太陽電気パネルを1枚外しても発電容量が十分であることを、運用実績を加味した解析により確認済みである。また、表面電位センサは必要な構造強度を有しており、脱落等によりISSに衝突する懸念がないことを確認した。また、シャープエッジ等については、設置場所が船外活動搭乗員のアクセス可能な場所でないため評価不要と判断した(なお、本体は断熱材で覆われており露出していない)。
(7)	ソフトウェアの更新	主に以下のような事項を改善した ・(HTV3号機で発生したアボート等)オフノミナルからの復帰手順の最適化 ・運用負荷の低減	通常運用及びハザード制御に直接影響するロジックの変更はなく、また変更後のソフトウェアが安全上必要な機能を従来通り提供できることの検証が適切に行われており問題なし。

CTB: Cargo Transfer Bag

6. 運用への準備等 (1/2)

(1) 運用制御合意文書の運用への反映

以下のプロセスはこれまでのミッションで確立しており、HTV4号機も同様である。

- ハザード制御手段として、地上要員あるいは搭乗員の操作(運用)を用いる場合には、運用制御合意文書にその制御手段を記載して管理する。
  - NASAが運用を担当する場合にはNASAが運用制御合意文書に基づいて、運用手順や運用上の取り決めに反映する。
  - HTVに対するコマンドや状態監視を制御手段としている場合には、JAXAのHTV運用担当が運用制御合意文書に基づいて、運用手順や運用上の取り決めに反映する。

- 運用手順や運用上の取り決めについては、運用実施部門とは独立したJAXA運用安全担当及びNASA内の運用安全担当が、運用開始前までにその妥当性を評価する。

(2) 安全検証追跡ログによる管理

- 種子島宇宙センターにおいてフライト品について安全を確認すべき項目を安全検証追跡ログ(SVTL:Safety Verification Tracking Log)に整理した。HTV4号機の安全検証追跡ログを次ページに示す。

6. 運用への準備等 (1/2)

射場で確認するHTV4号機の安全検証追跡ログ

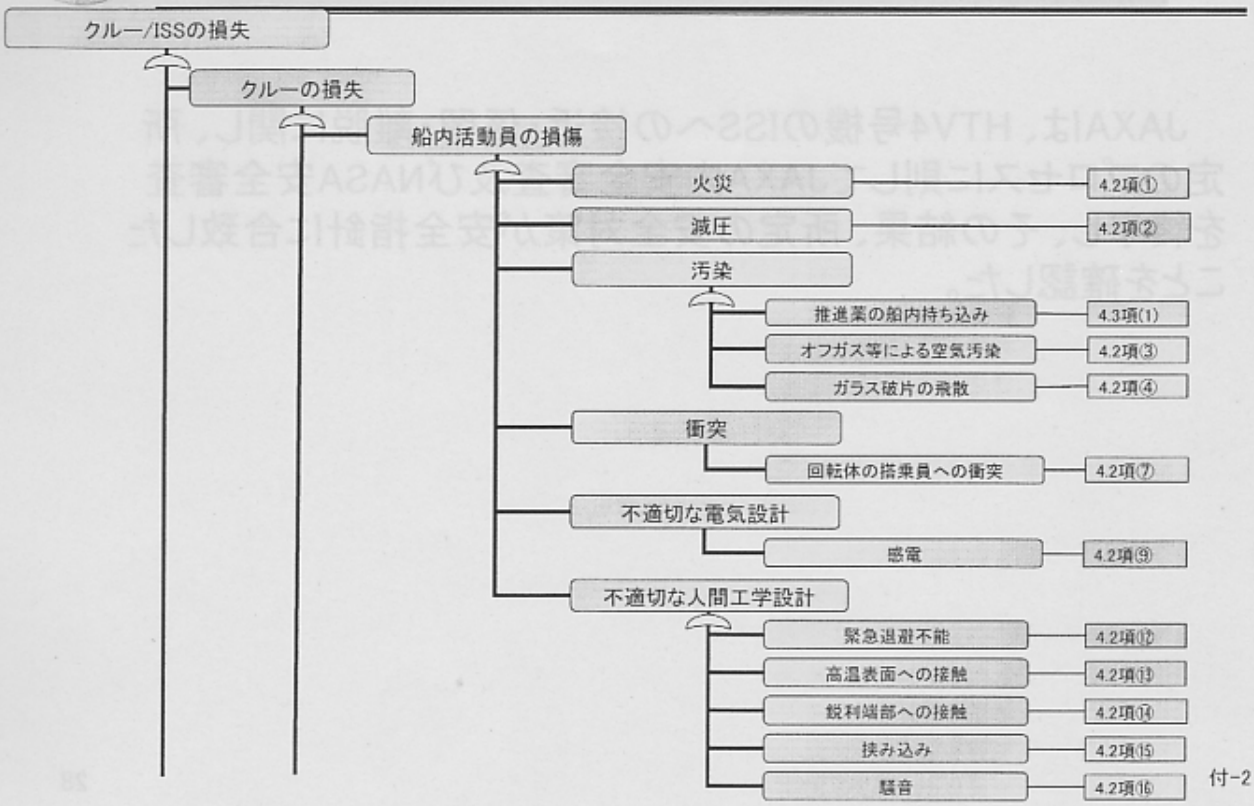
	検証項目	内容	参考
1	推進系の点検	打上げ前に射場において、安全制御に関する以下の項目の有効性を再確認する。 ・推進系ラッチバルブが正常に動作すること。 ・継手部にリークがないこと。 ・ヒータ制御が正常に機能すること。	 4.3(1) 4.3(1) 4.3(3)
2	機構系動作確認	分離機構のアクチュエータにある3つのスイッチが、正常に作動することを射場で確認する。	4.2⑤
3	ボンディング・グランディング計測	HTVの構成要素間の接地が適切であることを射場で確認する。	4.2⑨ 4.2⑪
4	その他、最終コンフィギュレーション設定に係る確認事項	HTV4号機打ち上げ前の最終コンフィギュレーション設定が適切であることを確認するため、以下の事項を射場で確認する。 ・モジュール内のオフガス量が許容値内であること。 ・全てのデブリバンパが取付が完了していること。 ・打ち上げ形態で圧力リーフ機能が適切に動作すること。 ・バッテリの充電が適切に行われたこと。	 4.2③ 4.2⑥ 4.2⑧ 4.3(2)

7. 結　論

JAXAは、HTV4号機のISSへの接近・係留・離脱に関し、所定のプロセスに則してJAXA内安全審査及びNASA安全審査を終了し、その結果、所定の安全対策が安全指針に合致したことを確認した。

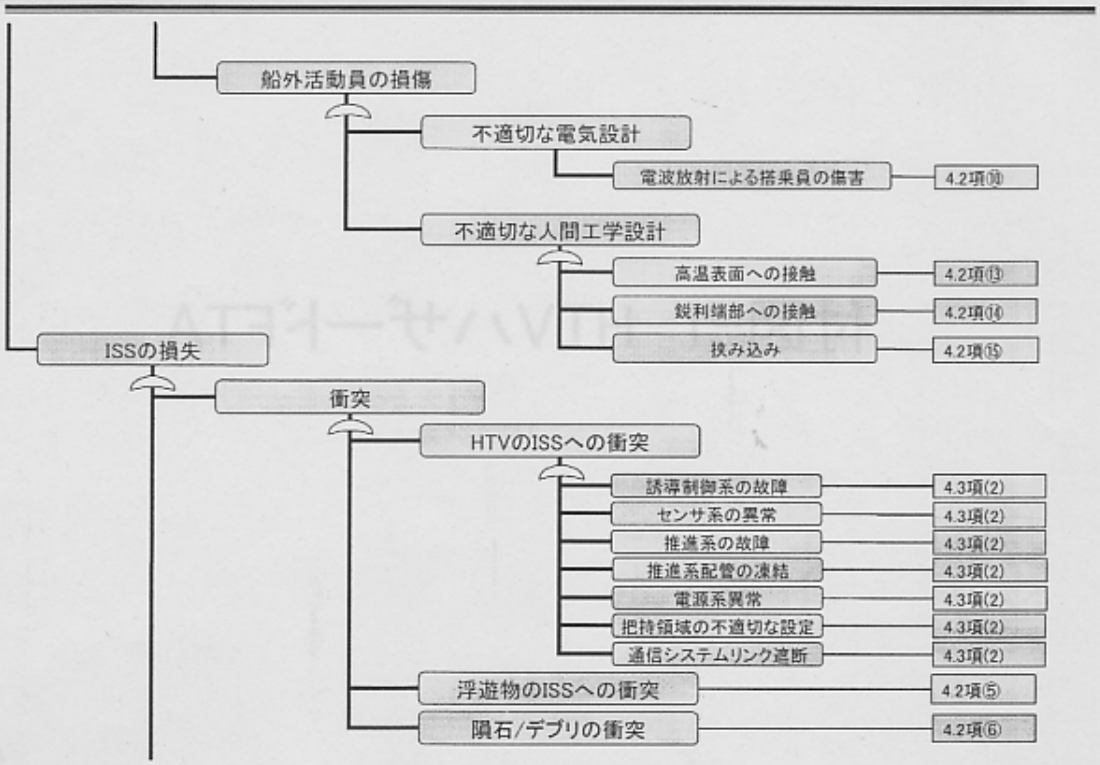
付図-1　HTVハザードFTA

付図-1　HTVハザード FTA　(1/3)



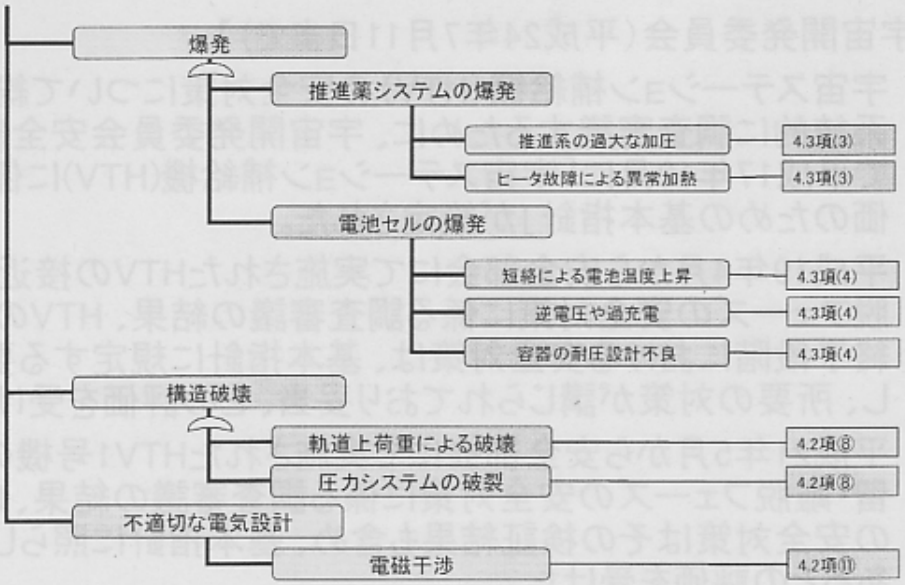
付-2

付図-1　HTVハザード FTA　(2/3)



付-3

付図-1　HTVハザード FTA　(3/3)



Backup Chart

HTV接近・係留・離脱フェーズの安全対策に係る調査審議の経緯

【宇宙開発委員会（平成24年7月11日まで）】

- 宇宙ステーション補給機（HTV）の安全対策について総合的かつ系統的に調査審議するために、宇宙開発委員会安全部会において平成17年10月に「宇宙ステーション補給機(HTV)に係る安全評価のための基本指針」が策定された。
- 平成19年4月から安全部会にて実施されたHTVの接近・係留・離脱フェーズの安全対策に係る調査審議の結果、HTVの詳細設計終了段階における安全対策は、基本指針に規定する要件を満たし、所要の対策が講じられており妥当、との評価を受けた。
- 平成21年5月から安全部会にて実施されたHTV1号機の接近・係留・離脱フェーズの安全対策に係る調査審議の結果、HTV1号機の安全対策はその検証結果も含め、基本指針に照らして妥当であるとの評価を受けた。
- HTV2号機及びHTV3号機については、再突入に係る調査審議の中で、接近・係留・離脱フェーズの基本指針への適合性が維持されていることについても確認を受けた。

安全解析の方法（1/2）

- 安全解析は、直接あるいは間接的に搭乗員に被害を与えるハザードを考慮し、対策をとることで、搭乗員の死傷を未然に防止する手法である。
- 安全解析では、FTA（Fault Tree Analysis：故障の木解析）等を用いてハザードを網羅的に識別し、それらの原因を抽出して、それぞれに制御方法を設定し、制御方法の妥当性を検証する。

  - 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いう。
  - ハザードの被害の度合いは、以下のようなカテゴリーに分類している。

【被害の度合い】

Ⅰ カタストロフィック
　能力の喪失に至る傷害又は致命的な人員の喪失となり得る状態

Ⅱ クリティカル
　重度な人員の傷害・疾病をもたらす状態

Ⅲ マージナル
　軽度な人員の傷害・疾病をもたらす状態

安全解析の方法 (2/2)

JAXAはハザードを網羅的に識別し、その制御方法を設定し、判断の妥当性を検証する一連の作業を行っている。

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	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. A/Iがすべてクローズしていることの確認