宇宙ステーション補給機（HTV）の
詳細設計終了段階における安全対策について
（案）

平成19年5月14日
宇宙開発委員会　安全部会

はじめに

宇宙ステーション補給機（HTV）はH-ⅡBロケット（H-ⅡA能力向上型）により打ち上げられ、国際宇宙ステーション（ISS）を共通運用するために必要な物資を補給することを目的としている。物資補給後は、大気圏への再突入により廃棄される。

宇宙開発委員会安全部会は、我が国がHTVの安全を認証するに当たって判断の基を提供するとの役割に基づき、HTVの安全評価を実施している。

平成17年9月には、HTVの安全確保を図るため、「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」（以下「基本指針」という。）をとりまとめた。

今般、独立行政法人宇宙航空研究開発機構（JAXA）においては、HTVの詳細設計終了段階における安全審査を終了したところであり、安全部会は、その安全の確保について、「基本指針」に基づく調査審議を実施した。[1]本調査審議においては、平成19年4月から5月にかけて計4回の会合を開催するとともに、JAXA筑波宇宙センターにおいて、HTVの熱構造モデル（STM）の視察を行った。本報告書は、HTVの詳細設計段階における安全対策の妥当性について調査審議を行った結果をとりまとめたものである。

---

[1] 「基本指針」は、当時の安全部会メンバーが作ったもので、現在のメンバーも多数入っている。しかし、審議は「基本指針」に基づいて行われたようには感じられなかった。また、「基本指針」の出来具合にも依存するが、もっと効果的な審議の方法があると思った。

目次

[2] 付録は添付されていないが、安全部会で配布されたものである。

1. 評価の対象範囲

HTVは、主に与圧キャリア、非与圧キャリア/曝露パレット、電気モジュール、推進モジュールから構成され、最大6トンの物資をISSに輸送する能力を有している。

HTVの運用は、打上げ、接近、係留、離脱、再突入の各段階に分けられる。

HTVは、H-ⅡBロケットによる打上げの後、自律飛行によりISSに接近し、ISSのロボットアームにより把持・係留される。物資を補給した後は、ISSから離脱し、自律飛行により大気圏に再突入して廃棄される。

今回の安全評価は、HTVの詳細設計段階における安全対策を評価の対象とした。評価は、「基本指針」に基づきISSへの接近・係留・離脱の各段階について実施した。

打上げ及び再突入に係る安全の確保については、「ロケットによる人工衛星等の打上げに係る安全評価基準」に基づき安全評価を実施することとし、今回の評価の対象範囲外とした。

なお、HTVにより輸送・補給される搭載物の安全については、搭載物の内容に応じて、必要があれば、別途調査審議を行うこととする[3]。

[3] この部分は「基本指針」に従っており、その文面を反復している。前半は、情報公開のために、HTV を知らない読者に向かって HTV を概説しているものと思われる。

2. 安全確保の基本的な考え方[4]

HTVの安全確保の対象は搭乗員の安全であり、搭乗員の死傷が未然に防止されなくてはならない。HTVの安全確保の体制と方法については、JAXAにおいて以下のような対策がとられている。

⑴ 安全確保の体制

ISS計画におけるHTVの接近・係留・離脱に係る安全確保の枠組みは、日本国政府及び米国航空宇宙局（NASA）の了解覚書（MOU）に規定されている。これに基づき、JAXAは、文部科学省の援助機関としてHTVを開発し、NASAと技術調整を実施してHTVの詳細な安全要求を設定するとともに、安全審査を実施している。

JAXAにおけるHTVの安全審査体制は、以下に示すように、複数の階層の下に実施されており、開発及び運用の担当部門から独立した部門においても、安全に関わる活動が行われている。

- HTVの開発担当部門であるHTVプロジェクトチームによって、安全解析が実施され、ハザードレポートを中心とした安全評価報告書にまとめられている。
- 開発及び運用の担当部門から独立した有人システム安全・ミッション保証室が、安全に関する方針及び要求を設定し、安全評価報告書の内容を評価するとともに、開発過程においても安全に関する技術評価を実施している。
- 有人システム安全・ミッション保証室長を議長とする有人安全審査会において、ハザードに関する安全設計結果及び検証手法の妥当性を個々に審査し、安全上の問題についての必要な勧告が行われている。
- 副理事長を議長とする安全審査委員会においてJAXAとして包括的に安全審査を実施している。

なお、安全上の問題は優先度が高いことが認識され、あらゆる安全上の問題について開発・運用の責任者まで報告・検討される体制が確立されている。

開発に当たっては、ISS全体の安全確保に責任を有するNASAとの技術的な調整が実施されており、MOUに基づく明確な役割分担と連携の下に、HTVの安全確保の対策が講じられている。

⑵ 安全確保の方法

HTVの安全確保のプロセスは、主にハザード解析の進捗に応じて複数のフェーズに分けられ、ハザードの識別・ハザードの除去制御や残存ハザードのリスク評価等が実施されている。

ここで、ハザードとは事故をもたらす原因が顕在又は潜在する

---

[4] 「基本指針」には書かれていない部分である。しかし、実際にはこれが「安全部会による審議の基本指針」になるのではないかと考える。安全部会の特別委員が、10時間足らずの審議で、HTVの安全について細かな点検を出来るとは思えない。青島刑事が「事件は現場で起こっているのだ。」と叫ぶように、安全対策はJAXA、NASA、製造メーカが日常の作業の中でやってきている。従って、体制や仕組みを調べ、解析手法や実証試験などの仕事の進め方を調べ、小数のサンプリングで技術的な詳細を点検すればいいのではないか。「基本指針」がそのように作られておらず、とても10時間では消化できない審議要求を出しているため、守られないのではないだろうか。但し、「基本指針」はJAXAが安全設計を進める上での、優れた指針にはなっていると思う。

なお、此処に書かれたことはJAXAが説明したのであるが、安全部会の審議の中で、その評価が行われたとは思えない。

状態をいい、ハザード解析とはハザードを網羅的に識別し、その制御方法を設定し、制御の有効性を検証する一連の作業をいう。なお、ハザード解析にあたっては、トップ事象に幅の広い事象を置き、抜けが無いように解析を実施している。

ハザード解析は以下のフェーズに従って実施される[5]。

- フェーズ0：対象システムの理解
  対象システム、運用、ミッション、環境条件、他のシステムとのインターフェース等を十分理解する。
- フェーズⅠ：ハザードの識別
  対象となるシステム及びその運用について、ハードウェア、ソフトウェア、運用、誤動作等のヒューマンエラー、インターフェース、環境条件等を考慮して、予測可能なすべてのハザード及びその原因を体系的かつ論理的に抽出する。
- フェーズⅡ：ハザードの除去・制御
  ハザードは可能な限り除去されるが、困難な場合には、①ハザードを最小とする設計、②安全装置、③警報装置・非常設備等、④運用手順、⑤保全の優先順位でハザードの制御を行う。
- フェーズⅢ：ハザード制御方法の検証
  設定されたハザード制御の有効性は、開発工程の適時適切な段階で、①試験、②解析、③検査、④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検証する。

残存ハザードのリスクは、ハザードの被害の度合い及びハザードの発生頻度のマトリクスで評価され、十分低いレベルに制御することとしている。残存ハザードのリスク評価に当たっては、ハザードの被害の度合い及び発生頻度を以下の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（致命的）ハザード
　人員の能力の喪失に至る傷害又は人員の致命的な傷害となり得る状態

Ⅱ：クリティカル（重大）ハザード
　人員の重度な傷害・疾病をもたらす状態

Ⅲ：マージナル（軽微）ハザード
　人員の軽度な傷害・疾病をもたらす状態

＜発生頻度＞

A: Probable（時々）
　プログラム中に発生する

B: Infrequent（偶に）
　プログラム中に発生する可能性がある

C: Remote（希に）
　プログラム中に発生する可能性があるが、ほとんど発生しない。

D: Improbable（微少）
　プログラム中に発生する可能性はほとんどない。

---

[5] 「ハザード解析」を説明しているが、「詳細設計終了段階」がどのフェーズに相当するかの説明が欠けている。従って、本文書で「対策が適切に行なわれている。」と報告するのであるが、「ハザードが制御されるような設計が行われた。」のであって、「ハザード制御の有効性が検証された。」のではないことは、読者が推測するしかない。

3. 安全設計結果[6]

HTVでは、火災、減圧、汚染、衝突、爆発、構造破壊、電気･電磁、人間工学、ソフトウェアの各項目に対応したハザードが識別された。これら、HTVのハザードは「きぼう」と共通のハザードとHTV特有の機器に起因するハザードに分別された。

識別されたハザードに基づくHTVの安全設計結果は「基本指針」の各項目に対応してJAXAから示された。

各々のハザードへの対応から抽出された事項を以下に示す。

⑴ 「きぼう」と共通のハザードへの対応から抽出された事項

HTVでは、「きぼう」の開発経験を踏まえ、「きぼう」と同様の考え方で安全設計がなされている部分が多く、宇宙環境対策、構造及び材料、安全･開発保証、人間･機械系設計、緊急対策については、「きぼう」と同等の安全設計が採用されている。

単一故障点と冗長系の独立性については、JAXAにおいて、信頼性確保の観点から次のような取組みを行っている。単一故障点についてはクリティカルアイテムとして識別し、妥当性解析を実施している。また、信頼性審査を実施し単一故障点の対処等を審査している。冗長系の独立性については、電気系のみならず、機械的、熱的にも配慮し、ワイヤーハーネスや配管の空間的な分離、コネクタの分離、ワイヤーハーネスの熱設計、帯電、電磁干渉等を考慮することで、共通故障原因を排除して冗長系の独立性を確保するように設計している。

デブリ、雰囲気空気、軌道上環境の保全、保全性については、HTVの設計に応じた対策が講じられており、その安全設計の有効性を確認するための検証方針についても明確化されている。また、ソフトウェアの安全設計、検証方針についても適切に対策が講じられている。

以下に、HTVの設計に応じた対策を示す。

ア デブリ

デブリについては、打上げ又は離脱時、デブリに衝突しない飛行経路を予め設定して飛行させるとともに、ISSへの接近中は必要に応じ衝突回避のための軌道変更を行うことで10 cm以上のデブリ等を回避する設計となっている。また、デブリと衝突した場合でも、10 cm未満の全てのデブリに対して、解析の結果からデブリがHTVを貫通する可能性は十分に小さいと評価されている。

イ 雰囲気空気

HTVの与圧キャリア内の空気組成は、打上げ直前に適切な組成であることを確認することとしている。また、ISSに係留される前に、HTV与圧キャリア内の気圧が既定値内であることを確認することとしている。係留時の与圧キャリア内の温度･湿度は、ISSの制御機能に依存している。

ウ 軌道上環境の保全

HTVは軌道上で放出しなければならない固形の廃棄物を持たず、故障時に漏洩する可能性のある推進薬は短期間に気化するものであり、軌道上環境の保全に対して特に問題はない。

エ 保全性

HTVの場合1機当たりの運用期間が45日程度であることから、

---

[6] 此処での記述はJAXAの説明に基づいている。その幾つかについては特別委員から質問を受け、「付録５　質問に対する回答」に示されている。しかし、はっきりと「納得した。」と云う返答を確認していない。また、全ての項目が質疑応答に掛かってはいない。

保全作業は考慮されていないが、JEMに搭載されている近傍域通信システムはユニット単位で交換可能な設計を採用しており、危険防止に対し配慮している。

オ　ソフトウェア

ソフトウェア機能の喪失がカタストロフィックハザードとなる場合については、独立した複数の機能を独立した複数の制御装置に搭載し、一つのソフトウェアの故障により、全ての安全機能を失うことの無いようにしている。一方、機能の不意の起動がカタストロフィックハザードとなる場合については、3重の指令により初めて装置が機能するシステム設計となっている。

また、接近、係留の各段階に使用するソフトフェアについては独立検証の対象とし、確実なFDIR（故障検知・分離・回復機能　Fault Detection and Isolation and Recovery）の動作を保証するためにソフトウェア試験を実施している。

⑵　HTV特有のハザードへの対応から抽出された事項

HTVは、ISSへの接近・係留・離脱を行うために必要な推進系、誘導制御系、電源系を有している点で「きぼう」とは異なっている。JAXAにおいては、これらの機能に起因するHTV特有のハザードとして、ISSへの衝突、推進薬による汚染、推進薬システムの爆発、電池セルの破裂を識別している。

以下にそれぞれHTV特有のハザードの制御として、推進系、誘導制御系、電力系等における安全設計及び検証方針について評価結果を示す。

A. HTVのISSへの衝突のハザードへの対応

ISS近傍において、ISSに衝突する軌道に入った場合や、推進系の不意な噴射・停止が発生した場合に、HTVがISSへ衝突し、ISSを損傷することで、搭乗員の死傷に至る可能性がある。

このため、以下の要因について機能の多重化や適切な設計余裕の確保により、衝突を回避する設計になっている。

①　誘導制御系の故障

誘導制御計算機は3つのCPU（中央処理装置）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ている。入出力コントローラは3つのCPUからの出力を多数決で比較するため、CPUの1台が故障しても飛行を継続できる設計となっている。また、2台の入出力コントローラのうち1台が故障しても他系が処理を行える設計となっている。誘導制御計算機内で更に故障が発生した場合（2故障時）には緊急離脱制御装置に切り替わり緊急離脱する設計となっている。故障検知は、ソフトウェア/ハードウェアによる自己故障診断機能、CPUと入出力コントローラ間の相互状態監視、入出力コントローラとの通信状態監視等により実施している。

これらの機能は、個々のコンポーネントの品質検査、誘導制御計算機における故障検知機能確認試験、誘導計算機・緊急離脱制御装置・センサを組み合わせた状態で故障を模擬して切り替えが行われることを確認する試験により、検証する方針である。

②　センサ系の異常

誘導制御に必要なセンサは全て2個以上設置される設計となっており、1故障許容設計である。ランデブーセンサ1故障時には近傍域通信システムを用いたISSに対する相対的な位置測定や、ISSからカメラを用いて測定した距離データとの比較等を用いて運用が継続できる設計となっている。2故障時に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

設計となっている。故障検知は、各センサ単体に対して誘導制御計算機が周期的に実施している。さらに誘導制御計算機は、同一種類のセンサ同士の比較、異なる種類のセンサ同士の比較、予測値と実測値の比較、規定値と実測値の比較等を実施することにより、故障したセンサを特定する機能を有している。

これらの機能は、センサの品質検査、1故障模擬で誘導制御機能が継続できることの確認試験、センサ故障時の切り替え機能の作動確認により検証する方針である。

③ 推進系の故障

推進系を構成する姿勢制御機器や圧力・温度センサ等の機能部品は2系統となっており、1故障許容設計である。2故障時にはメインエンジン系に切り替え、緊急離脱を実施する2故障許容設計となっている。故障検知は、誘導計算機が、規定の増速量、あるいは飛行経路の範囲を逸脱しているか否かを、予測値と実績値との比較、規定値と実績値との比較をすることにより実施している。

これらの機能は、バルブ・センサの品質検査、誘導制御計算機の試験における系統切り替え試験にて検証する方針である。

④ 推進系配管の凍結による破損を原因とする漏洩

推進系の主要配管・バルブ・推進薬タンクのヒータ制御の3重化設計により、2故障許容設計となっている。

これらの機能は、1系統で凍結を十分に防止できることを解析、品質保証、性能確認試験により検証する方針である。

⑤ 電源系異常

HTVは、単独飛行中も単一の故障により、安全に関わるシステムへの電力供給が停止しないように、複数の1次電池を並列に搭載し、電源バスを並列化するとともに、太陽電池及び2次電池からも電力を供給する設計となっている。

これらの機能は、バッテリーの品質検査と機能試験、電源バスの機能試験、通信・誘導制御機器と組み合わせたシステム試験による系統的な性能試験を実施するとともに、電池容量について必要なマージンを有することを解析し、検証する方針である。

⑥ ISSロボットアーム把持領域の不適切な設定

姿勢やセンサの誤差を考慮した把持領域を設定し、この設定領域からはずれる場合は、ISSの搭乗員又は地上要員がHTVの制御機能を起動してHTVが独自に姿勢制御を実施できるように設計されている。

この機能は、NASA、カナダと協力した妥当性解析、個々の部品の品質検査、性能検査により検証する方針である。

⑦ HTV近傍通信域通信システムとのリンク遮断

HTVはISS近傍運用段階となるとJEMとの間で近傍域通信システムによる通信を実施しながら接近する。この近傍域通信システムは冗長設計となっており、1故障許容設計となっている。またバックアップとして衛星間通信衛星とのリンクを確保しており、2重故障を起こした場合でも通信手段を失わないように設計されている。HTV側で2故障を検知した場合は、自動で接近を中止し、緊急離脱を行う2故障許容設計となっている。

これらの機能は個々のコンポーネントの品質検査、機能試験により性能保証を実施するとともに、最終的には通信系統の全体の確認として、NASAの地上局やISS側の通信装置を模擬した設備を用いて、全体的な系統試験を実施し、検証する方針である。

なお、今回の評価においては、故障が発生しても、リスクが最小となるように運用手順や関連するデータを整備するように提

案された。

B. 汚染

HTVの推進薬は燃料･酸化剤ともに人体には有害であるため、宇宙飛行士の船外活動中にHTVから大量に推進薬が漏洩した場合、宇宙服に付着し、船内に持ち込まれ宇宙飛行士が死傷する可能性がある。

このハザードを制御するため、船外活動領域に近い前方スラスタ設置近傍はバルブを3重にし、漏洩を避ける設計となっている。また、船外活動中は、不慮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運用としている。

これらの機能は、バルブ単品および配管系統の漏洩性能試験により検証する方針である。

C. 推進薬の爆発

推進薬が爆発した場合、ISSへの構造破壊を引き起こし、宇宙飛行士が死傷する可能性がある。

このハザードを制御するため、推進系の過大な加圧を防ぐように、ヘリウムガスの燃料･酸化剤タンクへの供給配管までに2直列の調圧弁を持ち、更に遮断弁を2重に配置することで、2故障許容設計となっている。またヒータ系統の異常加熱を防ぐように、温度センサーが規定の温度以上になった場合にヒータの電力供給を停止する設計となっている。

これらの機能は、単体での品質検査、性能試験、ヒータ制御装置の機能試験における模擬異常試験により検証する方針である。

D. 電池の破裂ハザード

電池の破裂によりHTVの構造破壊を引き起こし、船外活動中の宇宙飛行士の宇宙服を破損することで、死傷する可能性がある。

このハザードを制御するため、短絡時のヒューズ機能や保護回路による温度上昇防止、逆流防止回路による逆電圧防止やバス電圧監視機能による過充電の防止、容器の適切な設計を実施している。

これらの機能は個々の電池セルにおける品質検査、機能試験により検証する方針である。

4. 総合評価

以上のとおり、HTVの詳細設計終了段階における各ハザードの識別、制御について、JAXAが実施している安全対策は、「宇宙ステーション補給機（HTV）に係わる安全評価のための基本指針」に規定する要件を満たし、所要の対策が講じられており、妥当と評価する。

（参考1）

宇宙ステーション補給機（HTV）に係る
安全の確保に関する調査審議について

平成19年3月28日
宇宙開発委員会

1. 調査審議の趣旨

宇宙開発委員会においては、宇宙ステーション補給機（HTV）の安全確保を図るため、平成17年9月に「宇宙ステーション輸送機（HTV）に係る安全評価のための基本指針」（以下「基本指針」という。）をとりまとめた。

独立行政法人宇宙航空研究開発機構（JAXA）においては、HTVの詳細設計終了段階における安全審査を終了したところであり、その安全の確保について、「基本指針」に基づく調査審議が必要である。このため、安全部会において次のとおり調査審議を行う。

2. 調査審議の対象

HTVの詳細設計終了段階における安全対策

3. 調査審議の観点

「基本指針」に照らして、以下の観点から、安全対策の妥当性について調査審議を行う。

⑴ 安全評価対象に対するJAXAの安全確保の考え方、安全審査プロセス、課題抽出の手法等が妥当であるか。

⑵ 上記の観点に基づき、JAXAが実施した安全審査プロセスの中で抽出された課題の対処の方向性が妥当であるか。

4. 日程

調査審議の結果は、5月中を目途に宇宙開発委員会に報告するものとする。

5. 安全部会の構成員

本調査審議に係る安全部会の構成員は、別紙のとおり。

6. その他

「（会議の公開）第13条　本委員会及び部会の議事、会議資料及び議事録は、公開する。ただし、特段の事情がある場合においては、事前に理由を公表した上で非公開とすることができる。」（宇宙開発委員会の運営等について　平成13年1月10日宇宙開発委員会決定）に従い、安全部会は、原則として公開とし、特段の事情がある場合には非公開とすることとする。

別紙

宇宙開発委員会安全部会構成員

(委員)

部会長	池上徹彦	宇宙開発委員会委員
部会長代理	青江　茂	宇宙開発委員会委員
	森尾　稔	宇宙開発委員会委員(非常勤)

(特別委員)

工藤　勲	北海道大学名誉教授
熊谷　博	独立行政法人情報通信研究機構電磁波計測研究センターセンター長
栗林忠男	慶應義塾大学名誉教授
河野通方	国立大学法人東京大学大学院工学系研究科教授
佐藤吉信	国立大学法人東京海洋大学海洋工学部教授
下平勝幸	前日本大学理工学部非常勤講師
竹ケ原春貴	公立大学法人首都大学東京大学院システムデザイン研究科教授
中村　順	警察庁科学警察研究所爆発研究室室長
花田俊也	国立大学法人九州大学大学院工学研究院助教授
雛田元紀	宇宙科学研究所名誉教授
藤原修三	独立行政法人産業技術総合研究所爆発安全研究コア研究顧問
馬嶋秀行	国立大学法人鹿児島大学大学院医歯学総合研究科教授
松尾亜紀子	慶應義塾大学理工学部助教授
宮沢与和	国立大学法人九州大学大学院工学研究院教授
宮本　晃	日本大学大学院総合社会情報研究科教授

(平成19年5月14日現在)

(参考2)

宇宙ステーション補給機(HTV)に係る安全の評価に関する安全部会の開催状況

【第2回安全部会】
日時:平成19年4月5日(木)13:30～14:30
場所:宇宙航空研究開発機構　筑波宇宙センター総合開発試験棟
議題:(1)宇宙ステーション補給機(HTV)に係る安全評価について
(2)その他
※会議後にHTV熱構造モデルの視察を実施

【第3回安全部会】
日時:平成19年4月13日(金)14:00～16:00
場所:三田共用会議所　第3特別会議室
議題:(1)宇宙ステーション補給機(HTV)に係る安全評価について
(2)その他

【第4回安全部会】
日時:平成19年4月27日(金)14:00～16:00
場所:三田共用会議所　第3特別会議室
議題:(1)宇宙ステーション補給機(HTV)に係る安全評価について
(2)宇宙ステーション補給機(HTV)に係る安全対策について
(3)その他

【第5回安全部会】
日時:平成19年5月14日(月)14:00～16:00
場所:三田共用会議所　第3特別会議室
議題:(1)宇宙ステーション補給機(HTV)に係る安全評価について
(2)宇宙ステーション補給機(HTV)に係る安全対策について
(3)その他