文科省の瀬下参事官補佐が資料 5-2 (報告書案) を説明した後、活発な質疑応答があった。「安全対策案」は部会長一任で修文された後、定例会議に報告することが承認された。

佐藤：前回、前々回を休んでしまったので、前に議論されたのかもしれないが、4 ページのソフトウェアとか、5 ページの制御系に関し、2 重系、3 重系とか、2 アウト・オブ 3 とか、色々あるが、例えば、3 つの CPU から入出力コントローラに出力されるわけだが、比較というのが多分冗長系が出来ないのではないかと思う。比較器がもし故障した場合は、先程、「単一故障については云々」というのがあったが、これに入るのかと思う。その外、通信系に 2 重とか 3 重とか色々ありますが、切替器とかが必要になってきて、その切替器が多重になっているでしょうか。其れまで考えず、常識の範囲で通信のシステムが 2 重ということになっているのか。

また、7 ページの推進薬の爆発であるが、調節弁が 2 直列とか、…ええと、…直列だから良いのか。遮断弁を 2 重? これは、ああ、加圧を防ぐためのものなので、逆に言うと今度、加圧を防ぐために多分開くということだと思うが、閉じなくなってしまった場合、…これは、閉じる方ですか？ 閉じるか開くかどちらかに関し、多分、2 重になっていると思うが、制御のときにどちらかが故障すると、今度は、燃料を送らなければいけない時に燃料が送れないように思うが、その辺りの考えはもう議論されているのでしょうか。

池上：これは JAXA から答えていただくことであろう。

JAXA 深津：幾つかご質問いただいた中を順にお答えしたい。例えば、誘導制御系であれば、故障許容するためにシステムに 3 つの手段を持っている。コンピュータの中での比較は冗長ソフトウェアを使っているが、その後の緊急離脱機能に関しては基本的に独立したコンポーネント、ソフトウェアを使っている。これに関してソフトウェアの同時性による故障は無い。

切替機能について、専用の箱を作ってはいないが、制御装置の中に独立して持たせており、この切り替え機能が単一故障点になることは無いように配慮した回路設計をしている。

推進系は、過大な圧力になるところは閉めることで押さえたり、または、ラプチャーディスクを経由して圧力をリリーフすることを考えたりしている。圧力が過大で閉めてしまっても、残圧の部分で十分スラスターの反応に必要な圧力は供給できるという解析が行われている。遮断弁を閉じても、直ちにミッション機能喪失になることは無いとの解析結果が出ている。

池上：何か他にございますでしょうか。

河野：雑談風の話[1]をさせていただくことになると思う。これは HTV の話であるが、全般的に故障というものは思いも拠らない処で起こると認識している。2 重 3 重というものが、今まで役

[1] 「雑談」などという軽い話ではない。経験の少ない分野に踏み込んでいく、技術者の姿勢を評価する、大変重要な切り口であろう。「想いが至らない」領域を如何に減らすのかが課題であろう。

に立ったことがあるのだろうか。あと、7 ページに推進薬の爆発というのがサラッと書いてあるが、此れは異常なことが起きないと起こるわけが無い。何かが起きてこのようになる、一連の過程の中でのこういうことだと思えたりする。此処でやったように、系統立ててやることの意味、HTV だけでなく、今までの実績、衛星の不具合を見ると、そういうもの (連鎖?) が絡んできて考えている。それから複合的に何かが起きたときに次々と連鎖反応[2]のようなものが起きていくようなこともあるのではないか。どれか一つのことを起こさないようにしておいても、他で事故が起きたものが連鎖するようになったらどう考えるのか。最近衛星の不具合が起きているようなこともあるので、考えてみたが如何か。今日の議論にはあまり関係ないみたいであるが。

池上：ミッション保証室で、今まで実績などがありましたらどうぞ。

JAXA 武内：それでは、最初のところで、実際に何処までできるかという話になるが、先ず、思いも拠らない処で起こるというのは、正にその通りで、其れに対してどうするかというと、最初にやることは、「思いもよらないことではあるが、兎に角思い当たるところ」を如何に増やすかというところである。そのためには FMEA とか FTA とかハザード解析とか、今回やってきたが、結局或るものを如何に網羅するかが課題[3]であり、そこに如何に魂の入った情報網を作るかが重要だと思う。その際、衛星の失敗などを調査し、失敗の轍を踏まないようになっているか、仲間の経験が活きているかとか、安全に関する生の声を言える人を呼んで、今ある知恵を如何に持ってきて、それを外挿して、対象とするシステムの解析に役立てるかが、願っているところである。挿入っても思い当たらないところが出てくるので、前回にも少しお話したが、色々手順を踏んで、最後に、そうは言っても思い当たらないことに対して、如何に手元に情報を用意しておいて対応する[4]とか、また、対応する人たちが忙しい場面も出てくるので、私たちのように少し離れた者がまた別の目で見て、いざというときに対処するようにする。

池上：今まで、予備系に切り替わった実績はあるのか。

JAXA 深津：衛星の運用に支障が起きて予備系統に切り替わることは起きている。幾つか報告させていただいている。

河野：一連のものが起きたときの複合的な事故と、思いもよらないということは、今お話を伺うといろんな人にお考えを聞いて

---

2 「単独の故障だけではなく、連鎖とか、複合とか、広く可能性を推定したのか?」と、思いを馳せた範囲を聞いているのだと思うが、実際の FTA では、それらも想定されているのであろう。しかし、質問冒頭の「故障は思いも拠らない処で起こる」との言葉が強烈で、武内室長は其れにばかり反応していたようである。

3 「或るもの」と書いたが、「有るもの」と言ったのかもしれない。不具合原因を「気付かなかったので見落とした」のであれば、「気付け」と言ったところで改善されるわけが無い。「気付きやすい仕組み」を用意するしかないのであろう。つまり、過去の開発を通じて蓄積した不具合、不具合原因分析などの情報を、データベース化して目に付き易くすることは有効であろう。

4 この部分は「運用」の話であって、「安全」の話ではないと思う。

いるということであるから、やはり、思いもよらないということは避けられないと言っているような気がしている[5]。やはり、思いもよらないことを全部潰していくというようなことは、人間が考えるからしょうがないと言えばしょうが無いかもしれないが、まあ、機械に考えさせるというのもあるかもしれないが、そのようなことはやっておられるのか、不可能だと思っておられるのか。

JAXA 武内[6]：機械にやらせるのに近いところは、解っていることはシステマチックなアプローチとして、例えば「ハザードはこのようなものがある。」と云うのはどんどん増えてきて、「其れに対する制御はこうやります。」と云うのはどんどん出ている。其れが、今知っている範囲の網羅性は確保していて対応する。ただし、新たに解ってきたものも逐次、できるだけ追加していくアプローチも行なう。

JAXA 虎野[7]：補足したい。ご指摘の中の連鎖事象については、今回、HTV の点検チームを組織し、JAXA 内外から過去にプロジェクトや開発で経験してきた方々を集め、その中で連鎖事象なども検討してきた。現在、設計段階のレビューは終わり、今のところ連鎖事象に関する設計への反映はない。今後、製造段階や試験段階で、現物の配置を確認するときに、反映が出る可能性はあるが、設計段階では問題が無いという結論が出ている。

河野：この報告ではそのことが書かれていないようだが、其れは当然の常識だということか[8]。

JAXA 虎野：ええ、私どもはそう考えております。

池上：「はやぶさ」を見ると、最初から全身創痍[9]で飛んでいる訳ですよね。これは人の活動を前提にやっているが、私から言うのもおかしいが、過剰品質になっているのではないか。[10] やたらに高いものを作っている、NASA の方がもう少し賢くやっているというようなことは無いのか。実際に予備系統をおいた場合、其れを実際に使われる例が、頻繁にあるということであればそれはそうかもしれない。今まで全然なく、

---

5 何かが起こったときには、「思いもよらない経過で故障 (事故) が発生した。」と云うことが多い。JAXA 武内室長の発言に有るように、「思い当たるところを如何に増やすか」と云う努力だけが頼りで、全部を潰すことは出来ない。少しでも広く潰そうとした JAXA の努力の程度を安全部会の委員が評価すれば良いと思う。

6 「過去の不具合のデータベースを利用する」と云うことか。

7 JAXA 内外の経験者による「点検チーム」と云うこと。上記武内室長の発言も併せても、NASA との共同点検が抜けている。但し、安全部会の報告書案に記載が有るように、今までに説明済みのものだから省略したのであろう。

8 「これこそ報告して貰いたい事であるし、それを審議するのが我々の役目だと思う。」と言って頂きたかった。

9 満身創痍

10 特別委員のときであれば、このような野次馬発言も許されるであろうが、安全部会長の発言としては不適切である。わが国が初めて有人系の自律飛翔システムを手掛けているとき、危険予知に万全を尽くし、有人システムの設計手法を理解しようとしている者に向かい、水を差すようなことを言って良いのか。

違うところで故障が起きている[11]という話なのか、その辺りのことは如何か。

JAXA 深津：日本ではないが、スペースシャトルでは、3 重冗長にしていたものが、2 重までダウンし、残りの 1 系統で飛びきったという事例があると聞いている。その意味で、多重システムの有効性はあると思う。コストに関してはいろいろの議論があり、難しいとは思うが、過去の例と NASA の経験を考えると、多重システムの有効性は有ると思っているし、HTV という初めてのシステムに関し、我々もいろいろと協議してやっているので、高いか安いかの話は別にして、この位やっておかないと、安全面でこの設計がある程度必要なのかと判断している。

佐藤：5 ページのところの誘導制御系の故障について、真ん中の辺りに、「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、…により実施している。」とあるが、自己故障診断機能とは冗長系と言うより、故障が起きたら中断し、ミッションは果たせないが、安全側に「離脱する」とかいう思想だと思うが、自己診断と冗長系がバランスの取れた安全対策が、コストの問題も考えてミッションも効果的で安全性も向上できるということであろう。ところで、自己故障診断機能の診断率、診断できる故障率、その辺りの概略の値を把握されているのか。

JAXA 深津：故障率とは、ソフトウェアの故障率のことか。

佐藤：此処には、「ソフトウェア/ハードウェアによる自己故障診断機能」とある。故障を診断するわけなので、普通はハードウェアの故障を診断すると思うが、必ず誌の 100%故障が診断できるわけではないと思うので、何%の故障まで診断するのかということ。難しいと思うので、もし解っていれば。

JAXA 深津：故障率という解析はしていないが、故障診断機能としては想定しうる故障ケースとして、数十万ケース[12]をソフトウェア上で解析し、其れが実際ソフトウェア上で切り替わるというシミュレーション試験を行っている。そこで想定したケースは今確認試験中で、その試験が終わった段階でもし出来ないものがあれば、率という形で説明できると思う。ハードウェアについては回路の信頼度計算をやっており、その故障率は公表している。

佐藤：解りました[13]。ありがとうございます。

松尾：さっきの 3 重で 2 重まで行った話。良く解らないが、「3 重にしておいて良かった。」と思うのか、部品それぞれの信頼性は相当高くなければいけないのに、「二つも行っちゃって良いのか。」と思う、両側面が有ると思う。その辺は中々難しいところのような気がする。先程の河野先生の仰ったこと

---

11 そのような説明は JAXA から一切行われておらず、逆に、予備系に切り替わった実績があることは先の質問への回答で JAXA が述べている。「安全」を審議する場で、全く違うものの例を引いたり、机上で想像しただけの質問に、具体的な回答を出すことは大変であろう。

12 佐藤委員が考え直し、質問をし直せば、これが回答であろう。簡単な質疑応答で済む処が、やたら時間を消費している。

13 理解できたようには見えないが、質疑を終える必要があった？

と関係するが、同じもので冗長をとってもしょうがないというが、切り替えたときにそういう系でも役に立ったことがある。そうすると、偶発というものがそんなにしょっちゅう起こって良いものかということも有って、中々考え方が難しいわけです。3 重で 2 重まで踏み込まれたなどというのは、どう考えれば良いでしょうね。ここで議論をしていても、「3 重になっている。2 重になっている。」と云うことで評価が終わっているところも有るが、それぞれの硬さが十分なのかも考える必要があろう。はっきりした質問ではないが[14]、何となく其処は判然としないというところがある。

池上：複合的なことが起きたので二つまで行ったというようなことなのか。単独だと普通考えられない[15]ですね。

JAXA 深津：JAXA で起きた事象ではないので、技術的に正確なところは申し上げられない。JAXA でそのようなことが起きた場合には、その設計が良かったということではなく、起きてしまえば其れを切る判定をした上で、次号機以降必要な改善を行い、いくら 3 重システムがあるといってもメインのシステムがきちんと動いて信頼性を確保するのが原則と考えている。あくまでも 3 重というのは異常事態の対処機能という位置付けと思っている。先程は、そういう事が起きてももったので、3 重システムの有効性を説明しただけで、其れが起きたらそれで善しとすることではない[16]。

森尾：今、3 重の 2 重までというのがどういうケースか知らないが、例えば GPS のポジショニングを 3 重にするというのも有りましたが、共通の原因でおかしくなるのでは余り意味が無いわけで、恐らく違う手法によるポジショニングを組み合わせることしかないと思う。嘗ての飛行機の INS では、同じものを 3 つ積んでいた。[17]同じものだから、同じ原因で狂うことがある。だから、難しい。先程仰ったのは、結局思いも拠らない処で事故を起こすということは、我々がいくら考えても解らない[18]ので、より確かな方法としては、過去の事故の事例を

---

14 この一言が加わっているので、俎上に載せる価値が産まれる。単なる野次馬発言ではなくなる。

15 コメントの意味が解らない。「普通考えられない」と云う表現はかなり強いもので、「常識外の使われ方をしたので壊れた。」と言っているようなものであろう。猫の体を洗い、其れを乾かすのに電子レンジを使用し、猫の血を沸騰させて殺してしまった飼い主が、そのことがコーション・ラベルに書いてなかったことで、裁判に勝訴したことがあったそうである。勝訴したのであるから、「電子レンジで猫の毛を乾かそうとする」のは、普通考えられることなのか。3 重冗長の第 1 予備系まで壊れることは、「電子レンジの猫」よりも考えられないことなのか。

16 観念的に過ぎた回答ではないか。信頼度を積算すると目標信頼度を達成できず、冗長系を追加して目標値まで上げるのではないか。また、目標信頼度は、コストや技術的難易度、経験の深さなどを考慮し、総合的に決めたものではないか。

17 JAXA の説明には無かったが、今回の JAXA 内での作業で、過去の事例として参照しているものであろう。

18 「我々が」は何を指すのか？「部会メンバーが」なら分からぬでもないが、「JAXA が」であって貰ったら困る。

総浚いして[19]、どういう原因でどういう事故が起こったのかを幅広く調べ、少なくとも同じ理由で二度と同じ事故を起こさないということが、我々全知を尽くして出来ることではないかと思います。JAXA ではそういう、衛星やロケット、或いは飛行機の事故例の分析とか、データバンクなどはやっていますか。

JAXA 深津：其れについては当然[20]取り組んでおります。過去の事故は分析した上でデータベース化し、直近の事故は各本部で共通の横通しをし、当然、各事故の横通しをするための信頼性担当セクションがあり、其処で連携を取って、プロジェクトに展開されるようになっている。また、ISS プログラムにおいては、NASA からの反映、ISS で起きている実際の故障の反映、シャトルでの事故からの教訓というのも受けられるので、その反映に努力している。中々、それで全部消えきっていないという現実は別にしても、努力は続けている。

森尾：もう一つ。大きな事故は皆が知ることが出来るので、データが集めやすくなる。事故になり掛かったが大きな事故にはならなかったこと、アクシデントまで行かないインシデント、或いはヒヤッとしたということ、事故まで至らなかったものの情報を集めるのが難しい。飛行機業界がやっているのは本人の責任は追及しないとか、職の○○は守るとか、全く別な情報集めの仕組みを持っているが、例えば JAXA でも安全保障室などにそういう仕組みで、幅広く集める仕組みがあるのか。

JAXA 武内：はい、今、JAXA のシステムの一つに「ヒヤリ、ハッと」のシステムがあり、各部で出たものを一箇所に集めることをやっている。

河野：今の、思いも拠らないというのが気に掛かっているが、良く知っているかということ、よく練習する、試験をしてみると言うことであろう。だから、ある意味ではこの HTV というものは、一種の試験問題で、これで上手いこと行かせることで技術が確立するのではないかと思っている[21]。あとは、思いも拠らないところを思わせること、一度思わせた後でどうするかというと、プロジェクトマネージャにきちんと論功行賞をやって、失敗したら島送りかなんかで、成功したら給料 3 倍とか、此れは冗談であるが、そういう風にして一所懸命考えている人を作ることが大事だと思う。

馬嶋：これだけ議論すると面白いというか、かなり深いところまで議論が出来たと思うが、文章的なことであるが、3 ページの 3. 安全設計結果に「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。」とあり、その次に、「各々のハザードの対応か

---

19 既に、今回の質疑応答の冒頭で、そのような回答をしているように思える。

20 説明済みのことを質問され、「当然」の一言が付け加えられたと考えるのは、考え過ぎであろうか。

21 正にそのような一面があるだろう。許された予算の中で、出来るだけ広範囲に「宇宙を利用するための技術を開発する。」ことは、我が国の宇宙活動の目的の重要な 1 項目であろう。

ら抽出された事項を以下に示す。」と続き、以下 8 ページまであるが、実際にはこれは一部である。これだけ見ると、ここだけのことが抽出された事項であって、全部が語られていると言うのでは不十分ではないか。5-1-2 とか 4-1-3 に書いてあること全てに関して、安全評価が部会で議論されたということにならないと、安全対策の全てだと言うことは出来ないのではないかと思う。

池上：其れは前にも指摘があって、初めてお聞きになる人は、「これしかやらなかったのですか。[22]」と、こういう話になる。これは、文章的にそういう事が無いようにもう一度練っていただくということで宜しいでしょうか。

馬島：はい。

花田：細かいことだが、6 ページの「デブリ」の最後の 2 行（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。）について、「デブリと衝突した場合でも」とあるので、HTV の対デブリ防護能力が 10 cm と理解できる。本当でしょうか。花田の理解は、1 センチは大丈夫だけれども、1 センチから 10 センチ未満は小さいので、頻度も小さくなって、結果的に 10 センチ未満のものは大丈夫だということになるのだと思う。「デブリと衝突した場合でも」と云うのを削除した方が良いと思う[23]。如何でしょうか。

池上：JAXA 側で何かコメントありません。

JAXA 深津：この文章のベースとなったのは、委員ご指摘のご理解でありますが、基本的には被貫通確率を表現しようとしたのに過ぎないので、確かに 10 センチのデブリが当たっても大丈夫ということではない。解析の結果、10 センチ以下のデブリが貫通する可能性が小さいと評価しているだけである。当たって、穴とか亀裂が開くかもしれないが、そのときには避難することで、安全上の問題は有りません。ただ、被貫通確率という、確率計算の表現を受けて書いたものに過ぎません。そういう意味では、誤解を招くところがあるなら、修文が必要かと思う。

池上：修文する。どういう風に修文すれば嘘でないことになるか。

JAXA 深津：JAXA としては委員ご指摘の提案で良いと思います。

池上：なるほど、これを削除して。削除することを前提に、レビューしましょう。

青江：良く解らないが、削除することは意味を持ってはいるが、要

---

22 何故このような言葉が選ばれるのか解らない。 ①全ての項目のチェックをしたいと考えているのか。②全てをチェックしたと報告したいのか。③全ての項目をチェックするだけの能力と時間があると思っているのか。
2 日後の定例会議で修正された報告書を見ると、②に想定した、「全てをチェックした。」ことになってしまっている。JAXA は全てを事細かに報告していないし、報告した全てを特別委員が承認していない。「質問が無かったのは承認したこと。」になっている。

23 上手く表現できていないことは合意できるが、この対処法に賛同しきれない。傍聴時には資料が見られず、解らなかったが、3 種類（1 センチ以下、10 センチ未満、10 センチ以上）に別ければ書けるのであろう。

は何かあっても逃げられる、搭乗員の死傷は無いということではないか。そういう評価でしょう。其れが一番重要なことなのではないですか。

JAXA 深津：はい。

青江：其れを書いておく必要があるということではないのですか。人が死傷をするかどうか、解析をしたわけでしょう。だから、「人の死傷はありません」と云うことが結論として書いておくと、端的にして解り易いのではないかと言っているだけである。

JAXA 深津：はい、其れはおっしゃるとおりだと思います。

青江：ただ単に、言われるように此処を取るだけでも、それはそれなりの意味があるけれど、と言っているだけなのですよ。

JAXA 武内：頂いた指針との対応でも、今ご指摘のところが入れてありますので、その分をこちらに、報告書の方に入れていただけるのが良いかと思います。

事務局 瀬下：此処にある文言については、メーンテーブルにお配りしています安全 4-1-3 で、3/15 に示されている内容を具体化しました。事務局としては、1 センチ以上のものについては此処に書いてあるような形で大丈夫とし、それ以外のものについては①②③の下に、「デブリ等が HTV を貫通しない確率については、10 センチ以下の全てのデブリに対して 0.9977 である」ということなので、これを記載することで確率が小さいものであることが示されるという判断の下に、修文させていただきたい。そういう意味では青江先生が仰っているように、たとえ衝突しても死傷する確率が小さいということがここで示されているということになると思う。JAXA のご提案はどういうことになりますか。

JAXA 武内：はい、私どもの説明の問題であったかもしれませんが、3/15 の③の下で、「万一デブリ等が衝突して、HTV の与圧壁を貫通した場合に、ISS が圧力減少を検知して、搭乗員は緊急避難機に避難していく」と云うところを、青江委員がご指摘になったのだと思いますので、その分を追加してくださると良いと思う。

確率自体が十分に小さく、万一の場合にも、搭乗員は逃げることが出来る。こういう論法で如何かと思う。

池上：この文章を活かす形でやるわけね。

松尾：どっちにしても確率は十分小さいという話は吹っ飛んでしまうかな。

池上：では、そういう風に 3/15… (途中で口を止める)

事務局 瀬下：先程、「衝突した場合」を削除したらとのご提案ですが、そういう形で対応したいと思います。改訂の趣旨としては、3/15 ページの内容ということで宜しいでしょうか。

花田：はい。

事務局 瀬下：では、JAXA とも調整した上で、「衝突した場合」を削除したいと思います。

池上：「万一」と云う言葉があれば、少しは、ロジカルになるのではないか。

池上：それでは大体ご意見を伺ったと思いますので、今の部分の改定を含みまして、(終了)