JEM 開発における安全保証について

原　宣一

まえがき

「JEM の安全保証とは誰が誰に安全を保証するのか。」先日、ある方からこのような御質問を受けた。突然のことであったとは言え、職責上、私の答えが正確であったか、また納得していただけたか気になっている。「保証は英語の Assurance からきており、Sure にする、つまり確実にするという意味であって、補償（Compensation）の意味ではありません。従って、JEM の開発にあたって、JEM が確実に安全な物となるように活動することなのです。」とお答えしたように思う。もう少しご説明したかった安全保証の要点と是正すべきと感じている事項を｛つぶやき｝ながら述べる。

JEM（Japanese Experiment Module:宇宙ステーション取付け型実験モジュール）

1．安全保証の目的について

宇宙機の安全が確実なものであるようにするためには何をすればよいのであろうか。まずその宇宙機の設計を確かなものとする必要がある。設計がおろそかであっては安全な物となり得ないのである。つまり宇宙機の開発にあたって信頼性保証が必要であるということだ。同様に製造がおろそかであってはならないから品質保証も必要である。宇宙開発事業団（以下、NASDA）においては、その創立から間もなく取られた技術導入路線によって、ロケットや衛星の開発に信頼性保証と品質保証が必要であるという意識は定着している。ここでも保証は Assurance であり確実なものとするという意味である。

但し、NASDA においては昔から安全管理業務はもっぱら地上の人や設備に対する保護であって、ロケットや衛星を守ることは安全管理業務の目的に入っていなかったと言って良い。ロケットの飛行安全とはロケットが異常な飛行を始めたらロケットを破壊して地上に被害が及ばないようにすることなのである。無人システムでは当たり前のことであった。当初、信頼性安全管理部であった部門が信頼性管理部と安全管理部に分けられた理由は、組織が大きくなったこともあるが安全管理は独立した立場で実施すべしとの思想が根強かったからでもあろう。そしてロケットや衛星自体のミッションを守るという観点は安全管理部の所掌外とみなされてきた。NASDA においては組織規程で安全管理部の項に明記されているように安全を図る目的は「人」と「財産」を守ることであって、原子力のように「人」だけではないのである。原子力では安全の対象は「作業員」及び「近隣の住民」を守ることであり、ミッション又は財産

であるべき原子炉自体を守るとは言っていない。「原子力の安全性」(*1)

NASAにおける安全の考え方は1700.1B「NASA安全方針」(*2)に記載されている。これによると安全の目的は以下のことを避けることである。NASAの場合、「人」だけでなく「財産」や「ミッション」も安全の対象として明記していることは確かである。

①人命の喪失
②人の負傷
③設備、財産の損傷や喪失
④ミッション喪失や試験の失敗
⑤大衆の不興を引き起こす事象

[1] {⑤は蛇足であるように思われる。①～④で読めないことで⑤は何かを考えると、広い解釈が出来そうな文言ではある。(注：A版では文書名も「安全マニュアル」(*3)であったが、⑤は“不当なリスク”となっていた。)実際には、安全の対象が「人」だけであろうと「ミッション」であろうと守るべき対象は守らねばならないのだから、この違いはどうでも良いことのように思われかもしれない。ただ、担当部門の所掌範囲が違ってくるのである。ミッションを守ることは信頼性管理部の所掌であって、安全管理部ではなさそうである。また、「財産」を守るとなると「人の悪意による妨害行為」(Sabotage)に対する安全保障(これはSecurity)まで入ってくる(*4)。安全保障は日本では一般に総務部の所掌であり、技術屋の領分を越えている。悪徳総会屋から会社を守ることも総務部の業務らしい。}

日本では安全というと、NASDAの規定にも拘わらず、「人」に対してだけの意識が強いことは宇宙基地特別部会報告(*5)にも「宇宙ステーションは、人間をその要素として含むシステムであるので、その安全性は何よりも優先されなければならず…」との表現が出てくることからも読み取れる。NASAの安全方針でも、「人」を守るためには「ミッション」や「財産」を捨ててよいのか、という究極の選択を迫られた時の回答に困る筈である。このように安全確保の対象はわかりきっているようでいてすっきりしない一面がある。

[2] {①から⑤の順序づけが優先順位を示していると解釈できようが、負傷ぐらいを覚悟してもミッションを守ることが優先されることもありそうである。

安全と安全性は両方の言葉が同義で広く使われている。「性」は性質を表す時に使う接尾語であるのに安全はもともと性質を表している言葉である。従っ

て、NASDA が最近改訂した STD-12A「システム安全性標準」(*6)の定義のように区別して使うことはもはや無理であろう。}

安全を確保することは本来「価値」を守ることであると認識することが正しいように思われる。では、価値判断は誰もが同じかというとそんなことはない。しかし、同じ民族なら同じ価値判断を持つ、同じ自由圏の人ならば同じ価値判断を持つ、延いては人類は共通の情報を持って同じ環境下におかれれば、同じ価値判断を持つ、とせざるを得ないのである。これは世界平和の達成に必要な原理でもある。

2．JEM の安全保証について

安全の対象を「価値」を守ることと考えれば、事業団におけるプログラムにおいて有人も無人も区別無く「ミッション」を守るために安全保証が必要であったことになる。一方、NASA においては特にチャレンジャー事故の後、信頼性保証や品質保証と安全保証は密接に関連しているので統合してこれらの活動を行うことが適切であるとし、用語も従来の Safety, Reliability, Maintainability and Quality Assurance と言っていたものを Safety and Product Assurance とまとめた表現にした。NASDA はこの訳語として「安全・開発保証」の用語を作っている。なお、ESA は Product Assurance and Safety と称し、NASA はさらに Safety and Mission Assurance に変えてしまった。

JEM の開発において NASA と同等の安全保証をしなければならないことは IGA(*7)（ステーション計画の多国政府間取り決め文書）および MOU(*8)（ステーション計画の日本政府と NASA との了解覚え）で規定されている。そこで、NASDA では JEM の開発を担当する各社に対して諸々の管理活動を要求する文書として 1088D「JEM 安全・開発保証要求書」(*9)を定めた。1088D はステーション計画がフリードムという名前で呼ばれていた時代の最初の頃に上記の主旨で NASA が国際パートナの意見を取り入れて策定した計画定義要求文書 PDRD(*10) の第 9 章安全・開発保証要求を基にして、既存文書となっていた宇宙開発事業団の 1177A「信頼性プログラム共通仕様書」(*11)及び 558「品質プログラム共通仕様書」(*12)の内容を加味して制定されたものである。この文書は JEM を開発する契約相手会社に対し、840G「JEM システム仕様書」(*13)と共に調達仕様書で呼び出し、契約により義務づけることにより契約相手会社の管理活動を商法で担保するものである。JEM の設計に取り入れるべき安全技術要求事項は 840G「JEM システム仕様書」に盛り込まれ、安全管理要求事項は 1088D「JEM 安全・開発保証要求書」に記載されている。

[3]｛安全・開発保証活動は誰が行うべきかについて 1088D には次のように書かれていることを紹介したい。「本 JEM プログラムに従事するものは、すべて安全・開発保証活動を行っているとの認識の下に活動しなければならない。」そして、「安全・開発保証の管理を実施するに当たっては、設計、開発、運用及び利用等の各組織とは機能的に独立した体制で実施すること。」との記述もある。安全・開発保証はその管理は独立した部門にさせることが要求されているが、忙しい設計部門は安全・開発保証はそれを専門にする部門で分担して欲しいと思いがちであろうし、実質をやるなら管理も自分のところでやりたいと思うのが常である。｝

NASDA の技術系職員の主な業務の一つは開発仕様書と管理要求書を上手に作って契約し、契約が正しく履行されるように契約相手会社を監督することである。この他、開発計画を作成したり予算獲得等あることは言うまでもない。宇宙開発においては契約に当たって、技術要求を記した開発仕様書だけでなく、諸管理活動を規定した管理要求書をも示して契約している。つまり、「いい物が出来れば良いのでしょう、作り方はまかして下さい。あれこれ言わずに。」と契約相手方は言うかもしれないが、発注者は「あれこれ」言うのである。例えば「規定の形式の文書で不具合記録を記載すること」とか、「各フェーズの設計終了時点で設計審査をすること」等である。このために費用が多少増えようとも、これら信頼性保証、品質保証の活動を組み入れて開発した方が結局、マクロに見て費用効果が高いという判断があるからである。

さて、安全保証のため 1088D「JEM 安全・開発保証要求書」で規定している安全管理活動としてはは 4 項目ある。この内 2 つ典型的なものは安全管理（安全審査を含む）とシステム安全である。他の 2 項目は試験安全と産業安全でこれらはどちらかといえば常識的な要求である。

3．システム安全について

システム安全を要求するとは JEM のシステムが安全であることを要求するという意味ではない。結果的には JEM のシステムが安全なものになるのであるが、システム安全（System Safety）とは、システムのライフサイクルを通じて管理工学的手法を駆使して、運用効率や費用、スケジュールの制約の基に最適の安全確保を図りなさいという要求である。NASA の定義では、

"The optimum degree of risk management within the constraints of operational effectiveness, time and cost attained through the application of management and engineering principles throughout all phases of a program." NHB 5300.4 (1D-2)(*14)

この要求は「費用を厭わず安全確保を図る」と言っているのではなく各種の制約を考えて最適なリスク管理を図りなさいという要求である。理解がある要求のようであるが、この包括的な表現であるが故に意味するところは広い。主要なことは、次の3項目であり、そのための方法まで規定されている。

1）安全解析を実施してハザードを識別すること。
2）識別されたハザードに対して最適な設計をすること。
3）残存リスクの評価をすること。

[4] {NASDAはSTD-12A「システム安全性標準」のA改訂時に多くの用語を適切な定義に直した。ただし、このシステム安全の定義も元のＮＡＳＡの定義から単なる「システムの安全」の意味に変更してしまった。これならば敢えて定義に載せる必要も無い。「システム安全」は技術用語として長年使われてきた元の定義を残すべきであった。}

4．安全審査について

安全管理要求の中で最も典型的なものが安全審査を実施しなさいという要求である。システム安全の見地から、開発のフェーズに合わせて3～4回実施しなければならない。最終的に安全が確認されれば最終段階で1回行えば良さそうであるが、万一設計変更を余儀なくされることがあれば、手戻りが大変なものになってしまうことと、最終段階では審査出来ないことも有り得るからである。実際には詳細設計を終了した直後に行うフェーズⅡ安全審査が最も重要である。安全審査も審査をする対象は設計であるが、設計審査と独立に行なうことが暗黙のうちに要求されている。逆に、コンポーネント・レベル以下の単位では安全審査は設計審査に含まれていると解釈し、独立に行うことは希である。

安全審査を設計審査と独立に行わなければならない理由は二つ考えられる。

（1）安易な妥協の排除

通常、設計とは妥協の産物とも言われるように性能、スケジュール、コストのバランスで決められるものであるが、安全面だけは一旦、スケジュールとコストの制約を外して安全技術要求（性能の一部）が満たされているかを点検する。そして最終的に妥協が必要であれば、よりマクロな上位の立場の判断で決めるようにする。従って、安全審査の審査委員長は設計から独立した人でなければ独立に行う意味がない。

NASAの安全審査はパネルによる審査であり、形の上ではSSCB（スペース・ステーション・コントロール・ボード）が決定権限を持っているのであるが、

設計に対する実際上の拒否権限を安全審査委員長が持っていると言ってよい。設計審査も審査委員に他のプログラムの人や品質保証部等他の部の人を審査委員に加えるが、通常審査委員長は設計の責任者が行うものである。他のプログラムの人を加える意味は、担当設計者が陥りがちな思い込みや広い分野での経験不足を補うものである。

[5]{設計審査と同じ審査員が安全技術要求に関する事項だけを審査するのは設計審査第2部に過ぎない。契約により各社が社内で主催する安全審査レベルであっても設計審査と独立に行う意義を理解しないと安全審査の名に値しない。}

（2）安全の専門家による審査

安全を専門とする人達（審査パネル）により、設計から独立した審査委員により完全な独立審査の形を取るものである。

NASAはスペース・シャトル・プログラムにおける審査のためにJSC（ジョンソン宇宙センター）にPSRP（Payload Safety Review Panel）とKSC（ケネデイ宇宙センター）にGSRP（Ground Safety Review Panel）を設けている。JSCではステーション・プログラムのためにSRP(Safety Review Panel)も設けている。NASAはこれら審査のやり方を次の文書で決めている。

1）スペース・シャトルのペイロードに対して：

NSTS 13830B(*15)「NSTSペイロードのシステム安全のための実施手順」

2）ステーションの各エレメントに対して：

SSP 30599A(*16)「安全審査手順、国際宇宙ステーションアルファ計画」

日本では宇宙開発委員会安全分科会における安全審査の審査委員は設計部門から完全に独立しているが、安全審査だけを専業にしている人で構成するというわけには行かない。宇宙開発委員会の安全評価部会はJEMの安全審査のために「安全評価のための基本指針」(*17)を定めている。但し、JEMの開発フェーズとの関係で見れば後追いであったこともあり、本指針自体は定性的な要求に留められている。

JEMについては契約で義務づけた契約者主催のもの以外にも、NASDA主催のもの、及び、宇宙開発委員会安全分科会レベルのものがある。これらに加えて国際取り決めにより、NASAによる安全審査も受ける必要がある。但し、IGAやMOUの記述はNASAが行うステーション全体の安全審査に協力するという形の表現ではある。

[6]｛設計が完全であれば審査は簡単でも結果は良いはずである。審査資料作成とその説明に労力を取られすぎて設計自体がおろそかになったりすると逆効果になりかねない。設計者はくたびれて安全審査さえ通れば良いという傾向になりがちである。審査で指摘されて設計変更を余儀なくさせられるようなことは設計者として恥ずべきことである。指摘を待って設計を変えているのでは設計者が設計しているのか審査員が設計しているのかわからない。安全審査を通っても、失敗すれば第一責任は設計者にあるのである。成功すれば栄誉は設計者側に行くのであって審査員が誉められるわけではないのだから。審査員の指摘能力は、いかに安全審査を専門にしているNASAの審査員であったとしても、設計者の書いた審査資料に対してせいぜい同意を与えるぐらいが関の山であると考えるべきであり、審査資料に記載されない設計の細部まで目が届くと期待するのは良くない。NASAの審査員は設計が安全技術要求を満たしているかどうかを判断するだけであって、どうすべきだとは言わないように注意している。従って、設計者自身が安全であることを確信する設計を行うことが肝要である。決して安全審査員の審査をパスしたことによってのみ安全を確信してはならない。｝

[7]｛JEMの安全審査体系は構成が複雑すぎて、設計審査をパスさせなければならない設計者に審査のための負担をかけすぎるきらいがあると懸念される。下のレベルの審査の審査員が上のレベルの審査の説明員となる形式を取れば設計者の負担は軽くなるが、上位のレベルの審査がより大まかな審査でないと成立し得ない。設計者に代わって詳細を説明する必要に迫られると想像で答えざるを得ない局面になるからである。もし、審査での説明が間違っていれば反って安全を阻害する要因になる。｝

[8]｛日本では何か事故が起きると必ずマスコミは設計審査や安全審査が十分行われたかという取り上げかたをする。人間にミスは付き物なのに何故審査で見つけられなかったのかとの発想である。この結果、審査の強化ばかりが対策として加えられることになる。事故が起きた原因が設計時の考慮不足であったのであれば、まず強化すべきは設計陣である。審査体制の強化は間接的で費用効果が悪いことが多い。つまりシステム安全でいう最適な安全から外れる怖れがある。最初から設計者に十分調査し考える時間、勉強する時間を与えることが重要なことである。｝

5．安全技術要求について

前述のようにNASAは安全審査パネルが安全審査を行うが、そのための基準

となる文書を定めている。設計が安全でないという判定を下す時には、何故かを言わなければならないからである。安全技術要求第何項を満たしていないという説明が必要である。このためにPSRP、SRP及びGSRPが使う文書は次のものである。

1）シャトルのペイロードに対して：

NSTS 1700.7B (*18)「スペースシャトルを使うペイロードの安全方針と要求事項」

2）ステーションの各エレメントに対して：

NSTS 1700.7B ISS ADDENDUM (*19)「国際宇宙ステーションを使うペイロードの安全方針と要求事項」

SSP 50021(*20)「安全要求文書　国際宇宙ステーション」

ソフトウエアについては50021の子文書の形で次の文書が制定されている。

SSP 50038B(*21)「コンピュータ制御システムの安全要求 国際宇宙ステーション計画」

3) 射場安全に対して：

KHB 1700.7B (*22)「スペース・シャトル・ペイロード地上安全ハンドブック」

これらはいわばトップ文書であって、これらの文書で引用されている文書も多くある。

安全技術要求の本質的で代表的な安全要求に次のものがある。

① キャタストロフィックなハザードに対しては2 FT

そのハザードが人間の死やミッションの失敗に至る場合、つまり破局的な事象が生じる場合には、二つの故障が同時に起こっても、又は二つの操作ミスが重なっても、あるいは故障と操作ミスが重なってもそのような事象が発生しないように対処した設計にしなければならない。

② クリティカルなハザードに対しては1 FT

そのハザードが人に対し重大なる負傷を与えたり、かなりの財産の損失になるような場合、つまり重大な被害をもたらす事象が生じる場合は、一つの故障又は一つの操作ミスがあってもそのような事象が発生しないように対処した設計にしなければならない。

FTとはFault Tolerantの意味で故障許容と訳されている。Failure（故障）とFault(欠陥)を使い分けるなら、Failure Tolerantであるが、この使い分けはNASA文書においても混乱している。ソフトウエアの分野ではFailureより軽い概念がFaultであって、FaultはFailureに至る欠陥の意味で両方が使いわけられている。

絶対的に2 FTや1FTを要求されているわけではなく、冗長系を無理矢理つ

くると成立しないもの、反って安全でなくなるものは除かれている。例えば、ステーションの与圧壁は２重３重にする必要はない。２重３重にすれば重くなって成立し得ないであろう。何が除かれるべきかは技術の現状（state-of-the-art）で個々に違って来るもので、実際の設計を基にNASAと議論することはNASAの経験を受け継ぐ機会として非常に有効である。

③ インヒビットの設置要求

上記①に対応して、逆に意図せぬ時に作動してしまうとキャタストロフィックな事象が起きたことになるような物に対しては、作動のためのエネルギー源とその対象物との間に物理的な独立した３個以上の遮断スイッチ類を設置しなければならない。

④ シャープエッジの除去

有人プログラムで特有な要求であるが、宇宙飛行士が触れる怖れのある所には一切角張っている装置は設置できない。角はすべて丸めておかねばならない。

船外活動では宇宙服が破れたらキャタストロフィックな事態になるのでステーションの船外の装置はより厳しく審査される。

[9]｛図面の描きやすさと工程の簡略化からきているのであろうが日本の技術者はとかく角張った装置を設計しがちである。この点に関しては医学機器の分野の方が進んでいると思う。病院では患者が触れそうな機器はすべて角が丸くなっているのを見習う必要がある。｝

⑤ ソフトウエアに対する要求

安全の見地から、必ず作動しなければならない時は上記のFT要求が課されるが、不用意に作動することがあってはならない機能に関してはそのFaultが広がらないように設計しなければならない。また複数あるインヒビットの制御は完全に分離されていなければならない。

6．安全解析の手法について

新たに開発するものが安全であることはいかなる方法で示したら良いのであろうか。すべてのハザードを識別して、これに対する安全技術要求はどの文書の何項に記載されたどのようなものかを確認し、その要求を満たすような設計を行い、設計の意図通りのものが製造されたことを確認すれば良いのである。

NASAはステーション計画でSSP-30309E(*23)「安全解析とリスク評価の要求書」を定めている。まず、ハザードを識別し、それがどの程度のものか評価して、分類する作業であるハザード解析を行う。ハザードを識別するためには

FTA (Fault Tree Analysis:故障の木解析)や FMEA (Failure Mode Effect Analysis: 故障モード影響解析) 等の各種の解析手法を駆使して漏れがないようにする必要がある。 FMEA から作成される CIL(Critical Item List: 重要品目表)はクロスチェック用に使うこと等が記載されている。次に、その識別されたハザードが実際に事故となる可能性の度合い (Likelihood of Occurrence) と事故が起こった場合に推定される被害の程度 (Severity) との二つの観点からそのハザードを分類する。30309E では前者に対し 4 分類、後者に対して 3 分類としている。

カテゴリ Ⅰ : 破局的な被害 (Catastrophic)
カテゴリ Ⅱ : 重大な被害 (Critical)
カテゴリ Ⅲ : 少しの被害 (Marginal)
カテゴリ A : 起こりうる (Probable)
カテゴリ B : 起きる可能性がある (Infrequent)
カテゴリ C : 起きるかも知れない (Remote)
カテゴリ D : まず起きる可能性が無い (Improbable)

[10] {米国の他の文書ではもっと細分したものもあり、また、数値を与えたものもあったが、30309E では定性的な表現のみで定義されている。また Likelihood of Occurrence は Frequency of Occurrence と記載されているのもある。この混乱は確率(Probability)に対する工学分野における解釈の歴史的混乱から生じている。詳細は拙論(*24)「信頼度の意味するもの」宇宙先端、を参照して頂きたい。実世界の確率の定義として確信の度合い (degree of belief) を採用すれば解消することである。被害の度合いも確率も合理的な推定に基づく「主観」でよいのである。}

2 種類のカテゴリの組み合わせを NASA はリスク・インデックスと称している。設計の結果が IA であってはならないのである。また、これらを縦軸と横軸にしたマトリックスを作り、個々に識別したハザードの要因ごとのリスクをプロットすると、何が最も対策を講じる対象であるかが一目で判る。

NASA はハザードとハザード要因 (Hazard Cause) を区別している。ハザードとして大きく識別し、その要因を細かく識別してハザード要因ごとに対策が取られているかを見るわけである。すると、考えれば考えるほどハザード要因は増え、無限にあるようにも見える。しかし、この状況は構造物の強度解析における強度計算と似ている。ある大きさのある構造物に対して無限に細かく強度を当たらなければならないかというとそんなことはない。知識と経験により、どの部位が標定個所となっているかが分かってくるからである。安全解析も慣れてくれば、解析すべき部位が分かってくる。

安全解析とは被害の程度とその発生確率を決める作業である。即ち、ハザード及びハザード要因が識別され、これらがどの程度のリスクであるかを示すことである。30309E ではこのための書式を決めており、ハザード・レポートと称している。安全審査の時の審査資料は SAR（Safety Assessment Report）であるが、その主要な内容としてハザードレポートが含まれる。

[11] {安全の反対語としての危険という言葉を使って危険解析と言ったり、英語のハザード解析の訳として、危険解析とされていることもある。しかし、これらはハザード解析とする方がより適切である。ハザードは識別した段階では安全とも危険とも言えないものである。}

7．ハザードとリスク概念について

安全解析で重要な最も概念はハザードとリスクである。ハザード（Hazard）の定義は、前述の 30309E では、"The presence of a potential risk situation caused by an unsafe act or condition"、一方、［NASA 安全方針］では、"Existing or potential condition that can result in or contribute to a mishap"、となっている。NASDA では「安全開発保証要求書」に「事故の起きる要因が潜在又は顕在する状態をいう」と定義している。この定義は「 NASA 安全方針」の定義に由来することは明らかである。米国の他の文書においては他の違う表現で定義されたものもあるがいずれも本質的な違いはない。

空を飛ぶ飛行機には墜落というハザードがある。昔の飛行機はかなり危険であったが技術の進歩の結果、非常に安全な乗り物になった。しかし、依然として墜落というハザードが除かれたわけではない。

[12] {ハザードは日本語にはなかった概念であるのに危険とか危険要因と訳されていることが多かった。そしてこのことが誤解を生む要因であった。近い意味の用語を使って新しく意味を広げて使うよりも思い切ってカタカナのままにしておいた方が良い例の一つである。 コンフィギュレーション（形態）、ベースライン（基本線）、インタフェース（界面）はもはやカタカナでしか使われない。かって NASDA においてこれら漢字の訳が使われたことがある。一般に火口品を作動させることは Hazardous Operation であるがこれが「危険な運用」なら、そのような運用はすべきでないのであって、ハザードな運用でも安全な運用であることを確信できる時にのみ実行するのである。}

リスクは広く一般に使われているので、殆ど自明であると考えられるが正確

にはかなり違っている。「NASA 安全方針」では"As applies to safety, exposure to the chance of loss of injury or loss. It is a function of the possible frequency of occurrence of an undesirable event, of the potential severity of the resulting consequences, and of the uncertainties associated with the frequency and severity."

また、NHB5300.4(1D-2)では"The chance (qualitative) of loss of personal capability, loss of system, or damage to or loss of equipment or property."であった。

30309D では 1700.1B「安全方針」と殆ど同じであった。これに対し、少なくとも最後の一行は削除すべきという意見を出したら、これは届いたようだ。30309E では"Exposure to the chance of injury or loss. It is a function of the possible frequency of occurrence of an undesirable event and the potential severity of the resulting consequences."

1088D では「人間の喪失、システムの喪失、装置の損傷もしくは喪失、または財産の損傷もしくは喪失を招く（定性的な）可能性。」となっており、NASA の古い定義に由来する。

宇宙開発に限らず、一般には二つの量を掛け合わせてその値をリスクというのである。その一般化として発生確率を確率密度関数で表した時の確率論で定義している期待値をリスクとするのが最も適切である。NASA がこのように定義出来なかった理由は、やはり前述の実世界における確率の解釈の混乱によるものであろう。なお、リスクは価値の次元を持つことも指摘しておきたい。

[13] {NASA のリスクの定義で、従って 1088D の定義でも、欠けていることは、リスクはその大小を比べることに意義があるという認識である。二次元量はそのままでは比べられないことは、例えば、「二つの長方形が与えてこれを比べよ。」と言われても比べるものが面積なのか周囲の長さかによって答えが違ってくる。つまり二次元量を一次元量に変換する式（評価式）が必要なのである。NASA の定義では a function との言葉までは出てくるがその定義が示されていない。}

[14] {被害の期待値という言葉に関し、「被害を期待するとは不謹慎」というご指摘を頂いたことがある。数学用語の「期待値」は Expectation であるが、英語の expect には、「嵐が来ることを expect する」という使い方があり、数学用語の「期待値」も「予期値」であればより適切であった。確かにミッションの成果等、「得べかりし利益」に「期待値」を使うことがあってもリスクとは言わない。、リスクという用語は専ら望ましくない被害についてのみ使う習慣は定着しているから、リスクの定義は被害の「覚悟値」である。}

さて、最後に全く自明であると思われる安全（Safety）の定義を見てみると、やはり文書によって多少の違いがある。

NHB5300.4(1D-2)では、"Freedom from chance of injury or loss of personnel, equipment or property." そして、この訳として 1088D では「人間の死傷または装置・財産の損傷・喪失のおそれのないこと。」

NHB 1700.1 (V1-B)では Safety の定義はないが、Safety Assurance の定義が "The attainment of acceptable risk for the safety of personnel, equipment, facilities, and the public during and from the performance of operations."

広辞苑では、「【安全】 (1)安らかで危険のないこと。平穏無事。(2)物事が損傷したり、危害を受けたりするおそれのないこと。」であり、一方「【危険】危ないこと。危害または損失の生ずるおそれがあること。」となっており、安全は危険の反対の概念である。

私は安全の定義は「リスクが許容できる程小さい状態を言う。」とすることが最も適切であると思う。そして危険は安全の反対の概念として「リスクが許容できないほど大きい状態を言う。」となる。許容できるかどうかはその時々の社会的背景によっても違ってくるが、安全と危険の中間領域というのは存在し得ない。特に、有人宇宙プログラムでは常に安全との判断のもとに進めるものであって、危険を冒して宇宙に行くのではない。

あとがき

まえがきで紹介した御質問の 「誰が誰に保証するのか」に対する回答は、「IGA や MOU の規定により、日本国が米国、他に対して保証するのです。」または「納税者である国民に対して、その税金を使う立場である NASDA の代表として理事長が保証することです。」という回答も正解であったように思えるのである。

[15] {安全保証を実施するに当たって用語の定義が重要であると痛感させられる。理論的に用語の完全な定義体系を作れないことは簡単に証明できることではある。しかし、出来るだけ合理的に用語の定義を決めることが必要であり、基本的な重要な用語に関しては影響力の大きい NASA 文書に表れる定義から見直す必要がある。NASA は各センターの独立性が強いこともあるが、基本的な用語だけでも定義の統一を図るべきだと言いたい。 }

[16] {宇宙開発における保証活動の要求は NASA のアポロ計画の遺産と言えるものであるが、最近はコンカーレント・エンジニアリングだ、低コスト開発

だ、との掛け声の下に家元のNASAからくずれてきている。確かに、パソコンやネットワーク技術の発達を踏まえて、見直し又は修正の時期に来ているのかもしれない。その前に必要なのは用語の統一である。}

参考資料

1) 「原子力の安全性」、近藤俊介、同文書院

2) NHB 1700.1B NASA Safety Policy and Requirements Document, June 1993

3) NHB 1700.1A Basic Safety Manual, 1984

4) 宇宙先端 第7巻第6号「『安全』を考える」渡辺 貢成、1991年11月

5) 宇宙基地特別部会報告「宇宙ステーションの開発利用の本格化に向けて」昭和62年7月

6) NASDA-STD-12A「システム安全性標準」、平成7年10月

7) AGREEMENT AMONG THE GOVERNMENT OF THE UNITED STSTES OF AMERICA, GOVERNMENTS OF MEMBER STATES OF THE EUROPEAN SPACE AGENCY, THE GOVERNMENT OF JAPAN, AND THE GOVERNMENT OF CANADA ON COOPERATION IN THE DETAILED DESIGN, DEVELOPMENT, OPERATION, AND UTILIZATION OF THE PERMANENTLY MANNED CIVIL SPACE STATION
常時有人の民生用宇宙基地の詳細設計、開発、運用、及び利用における協力に関するアメリカ合衆国政府、欧州宇宙機関の加盟国政府、日本国政府及びカナダ政府の間の協定　　（ＩＧＡ）

8) Memorandum of Understanding Between the Government of Japan and the United States National Aeronautics and Space Administration on Cooperation in the Detailed Design, Development, Operation and Utilization of the Permanently Manned Civil Space Station
常時有人の民生用宇宙基地の詳細設計、開発、運用及び利用における協力に関する日本国政府と合衆国航空宇宙局との間の了解覚書　　（ＭＯＵ）

9) NASDA-ESPC-1088D 「宇宙ステーション取付型実験モジュール(JEM) 安全・開発保証要求書」平成7年10月18日Ｄ改訂

10) SSP 30000 "Program Definition and Requirements Document", (PDRD)
Section 9 Safety and Product Assurance Requirement

11) NASDA-SPC-1177A「信頼性プログラム共通仕様書」

12) NASDA-SPC-558「品質プログラム共通仕様書」

13) NASDA-ESPC-840G「システム仕様書 宇宙ステーション取付型実験モジュール(JEM)」平成9年3月14日Ｇ改訂

14) NHB 5300.4 (1D-2) "Safety, Reliability, Maintainability and Quality Provisions for

the Space Shuttle Program", October 1979
15) NSTS 13830B "Implementation Procedure for NSTS Payloads System Safety Requirements", November 1989
16) SSP 30599A "Safety Review Process International Space Station Alpha Program" January 11, 1995
17) 「宇宙ステーション取付け型実験モジュール（JEM）に係る安全評価のための基本指針」宇宙開発委員会、平成8年4月24日
18) NSTS 1700.7B "Safety Policy and Requirements For Payloads Using the Space Transportation System", January 1989
19) NSTS 1700.7B ADDENDUM "Safety Policy and Requirements For Payloads Using the International Space Station", December 1995
20) SSP 50021 "Safety Requirements Document International Space Station", December 12, 1995 (3/26/96)
21) SSP 50038B "Computer-Based Control System Safety Requirements International Space Station Program", November 17, 1995
22) KHB 1700.7B "Space Shuttle Payload Ground Safety Handbook", September 1, 1992
23) SSP-30309E "Safety Analysis and Risk Assessment Requirements Document International Space Station Alpha Program", October 28, 1994
24) 宇宙先端 第11巻第1号「信頼度の意味するもの」原 宣一、1995年1月