JEMの安全・開発保証

原 宣一

大宮市で開催された第21回宇宙技術および科学の国際シンポジウムでJEMの安全・開発保証について紹介する機会を頂いた。確実にミッションを達成するために、どのようにしなければならないかを規定する文書が安全・開発保証要求書である。一般にはなじみの薄い安全・開発保証の内容を少しでも多くの人に理解して貰おうと意気込み、また、ちゃっかりと含めた1、2の提案について賛同者が出てくることを期待していたものの、あいにく本セッションの参加者は少なかった。以下は、提出した原稿の元にした和文草稿である。

アブストラクト

日本が宇宙ステーション・フリードム計画に JEM（宇宙ステーション取付け型実験モジュール）計画で参画することを決めて以来、その開発と運用を担当する NASDA（宇宙開発事業団）では有人宇宙プログラムに対し、S&PA（安全・開発保証）活動を行ってきた。本稿は JEM 開発における S&PA 活動について紹介すると共に、より S&PA の基盤を固めるための一つの提案を行っている。

1. 序文

安全・開発保証活動は、確実にミッションが達成されるために行うべき一連の行動である。確実にミッションが達成されるためには、ミッション計画者の意図どおりに対象物を開発し運用することである。意図どおりに開発するためには、確実にそれが設計されて、確実にそれが製造されることである。確実な設計のために信頼性保証活動が必要であり、確実な製造のために品質保証活動が必要である。有人宇宙プログラムとしては、安全保証活動が強調される。さらに、コンピュータ・ソフトウエアの開発にはその特殊性を考慮したハードとは違った観点のソフトウエア開発保証(SPA)が必要とされる。これら4種類の保証活動は相互背反ではなくお互いに関連しあっていることから、調和の取れた活動にすべきである。換言すると、これまで個別に行われてきた管理業務を共通の視点をおいて相互に点検し要求の無駄をなくすことが新しく生まれた用語である安全・開発保証から期待される最大の利点である。

2. JEM 安全・開発保証の目的

JEMプログラムにおける安全･開発保証の目的はプログラムで規定された目的を安全に達成することである。この故にJEMプログラムのもとでの全ての活動は安全・開発保証の一部を構成する活動であると言える。従って、JEMプログラムに係る全ての人が安全・開発保証の役割を果たしているとの認識のもとに自己の責任を果たさなければならない。しかし、一つのプログラムに必要な作業を二つの区分、不可欠の作業と保証作業、に分けることが出来よう。不可欠の作業とは設計、強度計算、作図、製造、試験、運用、その他である。保証作業とは審査、点検、故障解析、その他でミッションを成功させるために必要な作業である。ミッションの成功はどうでもよければ不要かもしれない作業である。これら二つの区分に明確な境界ははないのであるが、後者が狭い意味での安全開発保証活動と呼ばれる作業である。保証作業の概念を Fig. 1 に示す。

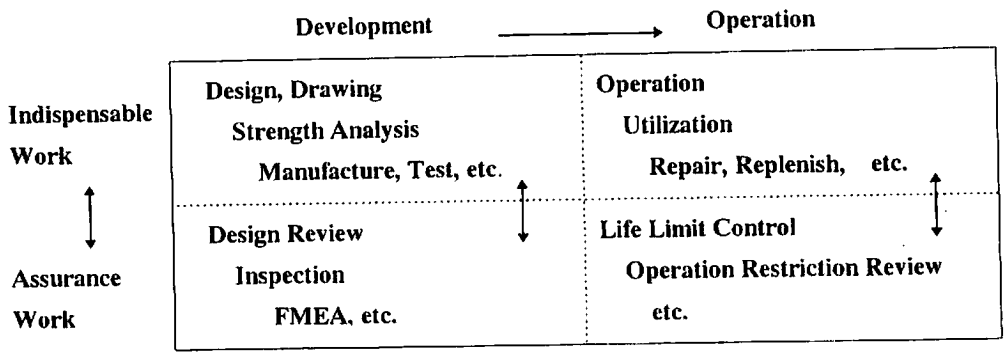

Fig.1 Concept of the Assurance Work

3. JEM 安全・開発保証の組織

安全・開発保証は開発や運用の組織が自己の判断のみで遺漏なく行うことは難しい程広範囲に及ぶ活動なので、その管理については開発や運用の組織から独立した組織で担当すべきとされている。もし、彼らは忙しかったり資金が充分でないと安全・開発保証活動のいくつかを省略してしまいがちとなろう。JEM開発のためのNASDAの組織としては、宇宙ステーションの開発及び運用を担当している宇宙環境利用システム本部から独立している信頼性管理部の下に宇宙ステーション信頼性管理室をおき、この室がJEMに係るS&PAの管理業務を担当

している。JEMの契約各社においては概して設計部門から独立した品質保証部の下でS&PA管理業務が担当されてきた。Fig. 2はNASDAにおけるJEM安全・開発保証の組織を示す。

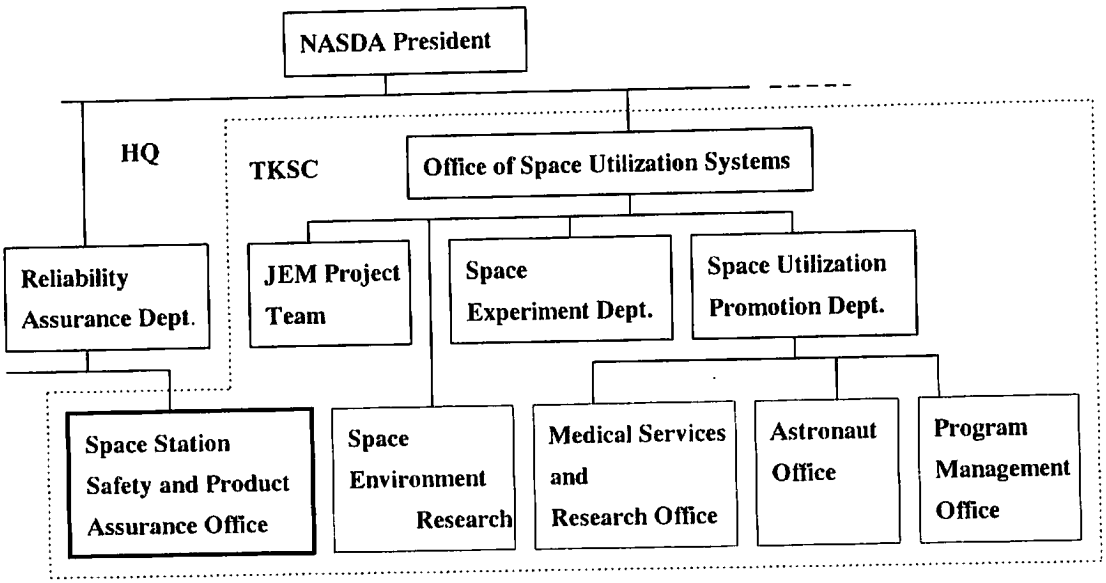

Fig.2 Organization for JEM S&PA in NASDA

4. JEM 安全・開発保証の根拠

多くのNASA文書がNASDAの宇宙開発にとって教科書の役割を果たしてきた。NASDAはNASA文書の規定を出来るだけ正しく解釈し、出来るだけ忠実に従ってきた。国際宇宙ステーション（ISS）計画では、可能な限り各国がNASAと同じ基準で、また同じ価値観の下に進めることが望ましい。一方、NASAにおいてもステーション全体の安全に対する計画及び要求を設定するにあたって、国際パートナ（IP）達の意見を取り入れている。

他国間政府協定(IGA)や二国間覚え書き(MOU)のような国際取り決めに基づき、NASAが定めたSSP 30000 プログラム定義要求文書(PDRD)に合致するか越えるものとしてNASDAは各種の国内文書を制定した。NASDAはPDRDの第９章「開発保証要求」に対応する文書としてまず、平成元年に NASDA-ESPC-1088「JEM安全・開発保証要求書」を制定し、少し遅れてCR-99302「JEM安全・開発保証計画」を定めた。NASDA自身の安全・開発保証活動に加えて、NASDAは契約各社における安全・開発保証活動を義務づけるため、NASDA-ESPC-1088をJEMを構成するハードウエア及びソフトウエアの契約者との契約に用いてきた。

NASDA-ESPC-1088はステーション計画がフリードムからISSへの変遷の時期においてもNASAとのmeet or exceed交渉を通じて維持改訂が行われてきた。現在最新のものはD版である。ISSに変わった後のNASAとNASDAの2国間の最上位の文書としてSSP 50030が定められた。NASAはすべてのPDRDを廃止したのでPDRD9章の代わりにNASAとNASDAの2国間文書であるSSP 50145を準備した。NASDAは新しいSSP 50145とNASDA-ESPC-1088が適合するように多くのコメントや意見をNASAに提出した。結局、NASAとNASAは相互にこの文書に記載された事項を実行することが国際宇宙ステーションにJEMを効果的かつ安全に組み込むために必要なことであることを同意した。これらの文書体系を Fig.3 に示す。

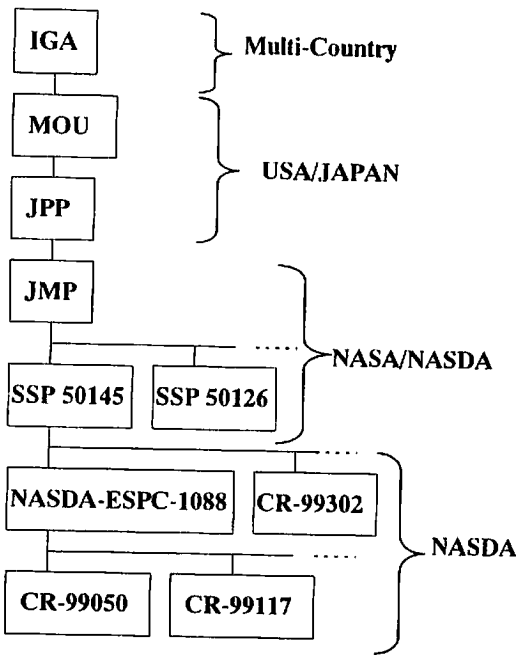

Fig.3 Document Tree Related JEM S&PA

5. JEM 安全・開発保証の内容

NASDA-ESPC-1088 は NASDA がこれまで無人プログラムに適用してきた NASDA-SPC-1177A「信頼性プログラム要求」と NASDA-SPC-558「品質保証プログラム要求」に加えて SSP 30000 の 9 章を加味して作成されたものである。NASDA-SPC-1177A と NASDA-SPC-558 は現在、NASDA-STD-17 と NASDA-STD-16 に置き換えられている。この文書は、安全保証要求、信頼性保証要求、品質保証要求、にソフトウエア開発保証要求から構成されている。 次の 3 要求

はこれら4種の保証に共通であると言えよう。
1）組織を明確にすること
2）活動は計画を立てること
3）文書に基づくこと
これらの要求は敢えて記載するまでもなく当然のことと思われるかもしれない。NASDA-ESPC-1088に規定された多くの他の要求も見方を変えれば、即ち安全・開発保証の観点から見れば、すべて当たり前のことなのである。

NASDAはもう一つ別の安全・開発保証要求文書NASDA-ESPC-1681を制定した。これはJEMに組み込まれる実験装置のようなJEMペイロードの開発のためにNASDA-ESPC-1088を簡素化したものである。SPAの要求事項はNASDA-ESPC-1681には規定されていない。

JEMの運用を成功裏に行うためになすべきことについての規定はまだNASDA-ESPC-1088にも記載されていない。これらは現在検討が続けられており、近いうちにNASAとの協議の後、NASDA-ESPC-1088に含められるか「JEM運用安全・開発保証要求書」制定されるであろう。

NASDA-ESPC-1088の内容を紹介することが必然的にJEM安全・開発保証活動の説明になる。以下5.1～5.5項は一部著者のコメントを含んだ、この文書のやや詳細な抜書きである。

5.1 安全・開発保証一般要求

一般要求は安全・開発保証活動方針と安全・開発保証共通要求から構成されている。JEMプログラムの遂行にあたって安全・開発保証管理を実行しなければならない。

1）安全・開発保証活動方針

安全・開発保証活動の考え方と活動の根拠が述べられている。安全・開発保証活動はこの章に記載された方針に従って行われなければならない。

2）安全・開発保証の共通要求事項

ここには次の事項が安全・開発保証の共通要求として規定されている。

・ 管理対象、内容、方法、スケジュールを明確にしなければならない。
・ 安全・開発保証プログラム計画書を作成して履行しなければならない。
・ 検証計画書等、付録にリストアップした文書を作成しなければならない。
・ **安全・開発保証管理を実施する部門は、設計、開発、運用及び利用等の各組織から独立していること。**
・ マイルストーン審査に安全・開発保証部門を参加させること。
・ 供給業者に対しても安全・開発保証管理活動を行うこと。

・ 安全・開発保証管理文書とデータを整備して迅速な検索が出来るようにすること。
・ 安全・開発保証活動について定期的に報告すること。
・ 安全・開発保証活動が契約に合致していることを社内監査で確認すること。
・ 安全・開発保証管理責任者は十分な識見、経験を有する者であること。
・ 事業団の代理者を受け入れなければならない。
・ 安全・開発保証の観点から評価を受けた検証計画を作成しなければならない。
・ 事業団及び国際パートナ支給品(NFE/IGFE)は規定どうり管理しなければならない。
・ ソフトウエアについても同様に安全・開発保証要求を適用する。さらに、ソフトウエアの特質に起因する要求をSPAとして後の章で規定している。
・ デビエーション及びウエーバーはNASDA-STD-1によること。

5.2 安全保証

安全保証としては、安全管理、システム安全、産業安全、及び試験安全についての要求事項が規定されている。

1）安全管理

安全管理に対する要求事項の要点はハザードを識別し、そのリスクを評価することである。このための有効な方法を確立する必要がある。即ち、安全管理のための組織を明らかにし、安全管理の計画を立てて安全審査の実施を計らなければならない。この他、事故の場合の調査と報告に関すること、安全管理組織の人の訓練に関すること等が規定されている。

2）システム安全

JEM の設計から運用を通してのライフサイクルにおけるリスクを最小化するため、NHB 1700.1(V1-B) に従ってシステム安全が実行されなければならない。言い換えると、

① まず、ハザードを識別すること。
② 次に適切な設計および性能要求を設定し、これを文書化し実行すること。
③ そして、安全解析を実施して総合的なリスクを評価することが必要である。

ハザードを識別するためには故障の木解析（FTA: Fault Tree Analysis)や故障モード影響解析（FMEA: Failure Mode Effect Analysis）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べきである。

適切な設計のために安全技術要求がある。識別されたハザードの制御のための設計要求が安全技術要求である。 NASDA-ESPC-1088 では JEM のシステム安全技術要求として NASDA-ESPC-840、KHB-1700.7B、SSP 5005 を呼び出すことにより規定している。

現在のところ、NASA の PSRP、SRP 及び GSRP の各審査パネルが安全審査の時の判定基準として使う文書として以下の文書がある。

① シャトルのペイロードに対して PSRP の基準文書：NSTS 1700.7B

② ステーションの各エレメントに対して SRP の基準文書：
NSTS 1700.7B ISS ADDENDUM、SSP 50021、及び SSP 50038B

③ 射場安全に対して GSRP の基準文書：KHB 1700.7B

JEM 開発はのために日本は NASA の安全技術要求に合わせる方針を採ってきた。しかし、国のレベルで JEM の安全を審査するための基準文書が 1996 年 4 月に宇宙開発委員会により定められた。幸いなことに、この文書と NASA の安全技術要求とは両立する内容である。民間航空機の世界では連邦航空局（FAA）によって定められた連邦航空規制(FAR)が航空機の開発及び運行のための安全技術要求としての事実上の世界標準である。**宇宙の分野でも FAR に対応する世界標準となる１つの文書が存在することが望ましい。**

安全解析とは当該ハザードが対象とする事故が起きた場合の被害の大きさとその事故が発生する確率を求める作業である。安全技術要求は識別されたハザードの制御のための設計要求である。安全解析は SSP 30309 に従って実施されなければならない。ハザードな状態、要因、影響、制御及び検証方法は CRS-94013 に従って識別され文書化されなければならない。安全解析結果、即ち、識別されたハザード要因がどの程度のリスクであるかを示す文書がハザード・レポートと称され、この書式も 30309E に決められている。安全審査の時の審査資料は安全評価報告書（SAR: Safety Assessment Report）であるが、ハザードレポートはその主要な内容として含まれる。

加えて、ハザードの除去及び制御、ハザード・レポート完了の基準、人間工学、仕様書および手順書審査、地上支援装置安全、変更審査、飛行および地上ハードウエア故障、地上および飛行試験の評価、そしてミッション運用活動の評価について規定されている。

３）産業安全

国内法規を遵守して、地上運用の安全を図らねばならない。

４）試験安全

試験時の安全余裕の評価をすること、及び試験施設等の審査が必要である。

5.3 信頼性・保全性保証

信頼性・保全性 (R&M) 保証の要求は主として設計部門が設計作業を行う時の作業要求である。本要求の多くはNASDA-SPC-1177A「信頼性プログラム共通仕様書」に由来するものである。ここで、一般要求、R&M保証管理、信頼性工学及び保全性工学に関する要求、と材料・工程及び部品の管理に対する要求が規定されている。

1）一般要求

Ｒ＆M保証活動は不可欠なものと認識しなければならない。

・Ｒ＆Mの作業を定義すること。
・Ｒ＆M要求の効果的な実行を図りこと。
・解析や審査を通じてR&M特性の評価を行うこと。
・そして、最適なトレードオフを行うこと。

2）R&M 保証管理

・ R&Mプログラム計画を作成し、維持しなければならない。
・ 下請負契約についてもR&Mプログラムが必要と識別した品目についてはその供給業者にもR&M保証要求を課すこと。
・既開発品を使用する場合は、性能等の必要な情報を提出しなければならない。
・R&Mに関して検証要求が設定され実行されなければならない。
・設計の確認のため認定試験を行いR&Mの評価を行わなければならない。

3）信頼性・保全性工学

信頼性工学と保全性工学は密接な関係があるが本来異なる分野である。

a）信頼性工学

信頼性設計基準、設計仕様書、信頼性故障許容保証、信頼性解析／トレード・スタデイ、信頼度予測、部品ストレス解析、ワーストケース解析(WCA)、トレンド解析、特別解析、故障モード及び影響解析（FMEA）、クリテイカル・アイテム・リスト(CIL)管理、信頼性及び保全性データ、有効寿命品目（LLI）、設計過誤を含む人為故障の除去、設計審査計画、異常／故障報告と是正処置、設計の標準化、ソフトウエア・インタフェース保証、クリテイカリテイ・カテゴリについて規定されている。具体的には、以下の要求がある。

・信頼度予測他の解析のためブロック・ダイアグラムを作成すること。
・部品ストレス解析を実施すること。

・ワースト・ケース解析を行うこと。
・トレンド解析を実施すること。
・スニーク解析等は必要に応じ、特別解析として別契約で行うこと。
・SSP30234 に従った FMEA を行うこと。細部については CR-99144 によること。
・クリテイカル・カテゴリは SSP30234 により、CIL 管理を行うこと。
・信頼性・保全性データを CR-99146 に従って作成し維持すること。
・有効寿命品目は CR-99145 や CRS-94020 に従って管理すること。
・設計過誤の防止及び除去に対する手段を講じること。
・契約の相手方は設計審査をしなければならないこと。供給業者の設計審査に参加すること。
技術変更管理を行うこと。
・異常／故障報告と是正処置に対する要求。
・設計の標準化を図るべきこと。
・ソフトウエアとのインタフェースを管理すること。

b）保全性工学

保全構想、保全計画、保全性設計基準、保全性解析／トレード・スタデイ、ツールの要求、ORU 配置、問題報告と是正処置、保全性解析、保全性評定・実証及び保全性データの作成、についての要求事項が規定されている。具体的には次の要求がある。
・ORU 保全活動を基礎とする場合は EVA や IVA による保全性設計基準を守るべきこと。
・保全性解析をやるべきこと。
・最適な ORU 形態を策定し、保全性解析／トレード・スタデイを行うこと。
・保全用ツールについて確認すること。
・ORU 配置とアクセス性についての考慮を払うべきこと。
・問題報告及び是正処置にも保全性の配慮をすること。
・保全性予測データを CR-99147 に従って作成し、維持すること。
・システムのダウンタイムを最小にするために予防保全解析を行うこと。
・緊急予防保全解析を行うべきこと。
・保全構想に一致する補用品要求解析を実施すること。
・保全性評価、実証及び保全性データの収集を行うこと。
・保全性実証要求：ORU を取り外して交換が出来ること。
・ORU でない部分の修理が出来ること。
・ORU レベルの保全性情報が CR-99146 に従って、用意、提出、そして維持されること。

4）材料・工程及び部品の管理

材料及び工程は CR-99117 に従って、選定され、適用され、そして管理されなければならない。材料・工程プログラム計画が用意され承認されなければならない。もし、材料または工程が CR-99117 に適合しない場合には材料使用協定書（MUA）が承認されなければならない。材料及び工程スペックは管理され、重要なものは NASDA に審査のため提出されねばならない。また、材料・工程の認定、材料識別及び使用リスト、そして非破壊検査計画について規定されている。

EEE 部品は CR-99050 に従って、安全・開発保証活動がなされなければならない。機構部品は CRS-94010 に従って管理されなければならない。

材料・工程及び部品に関する具体的な要求は次の通りである。

・MSL に無い材料の使用にあたっては材料使用合意書（MUA）を提出し、審査を受けること。
・材料及び工程の仕様書を管理すること。
・材料及び工程の認定をすること。
・材料識別及び使用リストを作成すること。
・非破壊検査計画書を作成すること

ＥＥＥ部品の具体的な管理要求としては次の通りである。

・EEE 部品の選定に際しての一般的な要求があることに加え、クリテイカリテイ３以外はグレード１の部品を使わねばならない。
・クリテイカリテイ３についてはグレード１または２の部品を使用すること。
・CR-99051 や SSP 30423 に記載されていない非標準 EEE 部品については CR-99050 に従って、JEM 非標準部品承認申請(JNSPAR)を提出すること。
・EEE 部品の放射線感受性データについての放射線試験の方法は、SSP 30513 に従わなければならない。
・静電気放電の影響を受けやすい部品については CR-99287 に従って取扱い管理計画書が作成され実行されなければならない。
・EEE 部品は EEE 部品仕様書で管理しなければならない。
・EEE 部品の認定データが無い場合には、その部品を EEE 部品レベルで認定しなければならない。
・EEE 部品の調達にあたっては、発注決定前調査計画、発注決定前調査報告、分解解析(DPA)計画、及び分解解析(DPA)報告を作成すること。また、源泉検査を行うこと。
・EEE 部品リストとして設計時部品リスト(ADPL)と製造時部品リスト（ABPL）を作成すること。
・ＥＥＥ部品適用性審査を行わなければならず、CR-99291 に基づきデイレーテ

イングが行われているか、放射線データの有効性等を審査すること。
・EEE 部品の不具合については所定の管理を行うこと。
・EEE 部品にはトレーサビリティのためのデータを付与すること。
・不適合部品はウエーバー又はデビエーションの処置を取ること。
・機構部品は CRS-94010 に従って管理すること。

5.4 品質保証

品質保証要求事項はもともと NASDA-SPC-558 に由来するもので、ISO9001 のように広い意味の品質保証概念であるため設計管理まで含んでいる。しかし、安全・開発保証の一部としての品質保証要求事項は製造に関する要求が主体となる。一般的な要求以外の主要な要求事項は識別及び検索、購買管理、製造管理、検査及び試験、不具合管理、物品の記録、計測管理、スタンプ管理、取扱い・保管・防錆・マーキング・ラベリング・包装・梱包及び出荷、統計的手法の利用、財産管理である。これらのより具体的な要求は次の通りである。

1）品質保証プログラム管理及び計画
品質保証活動の概念、品質保証プログラム計画、品質情報、教育訓練、各種審査会における品質保証部門の確認事項が規定されている。

2）識別及び検索
物品等の購買、製造、検査、試験等の記録の相互関係を明らかにするため、識別のためのシステムを設定しまけれればならない。このため、識別法、文書化、識別管理及びトレーサビリテイ、識別リスト、記録の保管、及び、記録の検索についての細部要求事項が規定されている。

3）購買管理
購買するすべての物品等の品質に責任を持たなければならない。このため、供給業者の選定における評価、購買文書、供給業者に対する品質保証活動、事業団の下請負監督、受入検査、受入記録、供給業者格付けシステム、監査、検査試験との整合性、及び、不具合情報の通知に関しての細部要求事項が規定されている。

4）製造管理
物品等が技術仕様書等の要求に合致していることを保証するため製造工程を管理し、製造時に得られたデータを含む製造作業の記録を残さなければならな

い。このため、物品等の管理、清浄度管理、特殊工程の管理、ワークマンシップの標準、仮組み付け品の管理についての細部要求事項が規定されている。

5）検査及び試験の管理

物品が契約、図面及び仕様書の要求事項に合致していることを実証するために必要な検査及び試験（以下「検査等」という。）を計画し、実施しなければならない。このため、検査等の計画、試験仕様書、検査等の手順書、品質保証業務の代理人指定、検査等の実施、検査等の記録、及び、試験の実施における品質保証部門の役割についての細部要求事項が規定されている。

6）不具合管理

物品等が適用図面、仕様書等の要求に適合しない場合及び機能的に疑わしい現象を示した場合には、その物品等を不具合品として識別、分離し、適切な処分及び是正処置（以下「処分等」という。）を行う文書化された不具合処理システムを確立し、維持しなければならない。このため、不具合品の識別及び分離、不具合の文書化、原因調査と解析、初審、再審委員会、処分実施の確認、事業団への申請、処分実施の確認、是正処置、供給業者のＭＲＢ、不具合の統計的解析、及び、NASDA データベースの利用についての細部規定がある。

7）物品の記録

継続的な物品の履歴の管理のために、納入するサブシステム及びシステムを含む品目ごとに記録を作成、維持し、最新の状態に保たなければならない。

8）計測管理

品質が合致していることの客観性を保証する一環として、計測管理システムを確立し、計器、測定器、標準器(以下「計測器等」という。)を、以下の要求事項に合致するよう管理し、利用しなければならない。このため、計測器等の受け入れ、特殊な計測器等の評価、計測の精度、較正の精度、校正管理、環境条件、取扱い保管及び運搬、修正措置、及び、検査に用いる製造用治工具についての細部規定がある。

9）スタンプ管理

すべての物品等に検査状態又は工程中の状態等が分かるように表示をしなければならない。このため、物品等の状態の表示、及び、スタンプ管理システムについての細部が規定されている。

１０）取扱い・保管・防錆・マーキング・ラベリング・包装・梱包及び出荷

物品等の取扱い、保管、包装及び出荷等の手順を確立し文書化しなければならない。また、対象となる物品等の特性に応じて、必要な静電気放電対策や振動対策等を施さなければならない。このため、取扱い、保管、防錆、マーキング及びラベリング、包装、梱包、及び、出荷についての細部が規定されている。

１１）統計的手法の利用

製造と検査の作業の管理をするために、統計的工程管理が効果的な場合には、これを使用しなければならない。このため、統計的工程管理、及び、抜取検査については既存の MIL 規格 (MIL-STD-105D, MIL-STD-414)を使用すべき等の細部の規定がある。

１２）財産管理

事業団及び国際パートナから与えられたすべての事業団及び国際パートナの財産に責任を持たなければならない。このため、契約の相手方の責任、及び、不適切な事業団及びＩＰの財産に関しての細部規定がある。

5.5 ソフトウエア開発保証

ソフトウェア固有の特質に起因する要求を記述している。これらは、管理、ソフトウエア QA、ソフトウエア・コンフィギュレーション管理、ソフトウエア故障解析(SFA)、ソウトウエアの統合管理、ソフトウエア不具合管理、検証及び有効性確認(V&V)、独立検証及び有効性確認(IV&V)、ソフトウエア安全、等が規定されている。

１）管理

ソフトウエアの管理として、組織、SPA 計画、審査、供給業者に対する要求及び審査、既開発ソフトウエア、事業団及び国際パートナ支給品、進捗状況報告、委員会参加、運用とメンテナンス、訓練、ソフトウェアツール、ＳＰＡ記録に関する細部要求事項が規定されている。

２）品質保証要求

ソフトウエアの品質保証要求として監査、ツール、技法、方法論、ソフトウェア文書、ソース・コード評価、ソフトウェア試験に関して細部要求事項が規定されている。

3）コンフィギュレーション管理
ソフトウエアのコンフィギュレーション管理として、コンフィギュレーション識別、状態記録、検証、コンフィギュレーション変更管理、ソフトウェア納入、ソフトウェア・ライブラリ、デビエーション及びウエーバに関する事項が規定されている。

4）不具合管理
ソフトウエアの不具合管理のため、不具合報告、及び、JEM 問題報告及び是正処置についての細部規定がある。

5）ソフトウェアフォールト解析
クリティカリティ・カテゴリ３を除く品目の機能を支援するソフトウェアに対してソフトウェアフォールト解析を実施しなければならない。

6）ソフトウェア安全
SSP 30309 に従って、ソフトウェア安全解析を実施しなければならない。

7）標準
ソフトウェア開発標準を確立し履行しなければならない。

8）トレード・スタデイ
SPA 担当は適宜トレード・スタディに参加して全ての管理要求が適切に考慮されて実施されていることを確実なものとしなければならない。

9）インテグレーション保証
ハードウェア対ソフトウェア、ソフトウェア対ソフトウェア、人間対ソフトウェアインタフェースの評価と統合のプロセスを設定しなければならない。これらのプロセスは、インタフェース文書及び SSP 30459 で規定された要求を満足すること。

１０）検証及び有効性確認（V&V）
ソフトウェアが、承認されたプロセスに従って開発され、維持されたことが検証されていること。未処置の不具合が存在しないことの検証がなされていること。すべての適用要求を充足することの確認がなされていること。

１１）独立検証及び有効性確認（IV&V）

IV&Vの意図を満たす、これと同等な活動を実施しなければならない。

１２）セキュリティ保証

セキュリティ管理計画書を作成し、管理しなければならない。

6. JEM安全・開発保証のデータベース

フリードム時代からステーション計画は大型コンピュータに対する多数の端末機という構成であった技術管理情報システム（TMIS）を活用することが行われてきた。安全・開発保証の分野ではJEMに関しても特にNASAで既存の３種類の情報システム（PRACA、EPIMS、MAPTIS）に細部仕様を合わせてNASAとの情報交換が容易になるように取り決めて作った。このシステムは数年前に完成したが使い勝手の点で極めて不満の多いものであった。この頃、インターネットにモザイクのブラウザ・ソフトが使われ始めたのを見て、急遽システムを変更するところとなった。特にソフトを開発する必要がなく、世の中の流通ソフトを上手く利用するだけで済むので、全世界的に自然の流れであった。

NASDAはインターネット技術を利用して新たに構築したこの情報システムを安全・開発保証の補完的な活動の一つとして、S&PAデータ交換(SPADE)システムと名づけた。これはNASAを含むJEM関係者がJEMのS&PA関連データを必要とするときに簡単に閲覧できるようにしたものである。但し、NASDAから前もってパスワードを交付してもらう必要がある。現時点、SPADEの中のデータの種類はT-MIS時代と同じであるが、データの蓄積量は日増しに増えている。

現時点でSPADEに取り込まれているデータの種類は以下のものである。

１）J-PRACA： JEMの問題報告及び是正措置

これはJEM開発におけるPFM以降の不具合に関する情報である。

２） J-MAPTIS

これは材料及び工程に関する情報で次のものから成る。

MUA：材料使用協定

MIUL：材料識別及び使用リスト

JEM-MSL：JEM材料選定リスト

可燃性、臭気、オフガス試験

３） J-EPIMS

これは部品情報に関するデータベースで以下のデータを集積している。

JEM-APL：JEMの承認部品リスト

JNSPAR：JEMの非標準部品承認申請

ADPL：設計時部品リスト

この他、JEM FMEA/CIL、JEM ORU、JEM HAZARD REPORT、JEM PAYLOAD、JEM LLI、JRAM、JEM EPAS、S&PA Vocabularyも加えた。将来JEMの運用時代にもこのシステムが有効に使われるために、蓄積すべきデータ種類の見直しと事実上の標準となりつつあるAcrobatのPDFの採用等、日進月歩のコンピュータ技術の有効利用が常時検討されている。

7. 安全・開発保証に用いられる基本的な用語の定義

5項で紹介したようにS&PA活動の内容は少し複雑であり、S&PA要求の簡素化が望まれていると思われる。複雑である原因の一つには4種類の保証の統合がまだ完全でないことであろう。この観点で見ると最初に取り掛かれることは、S&PAで使われる「ハザード」、「リスク」、「安全」、「クリテイカリテイ」、「故障」、「欠陥」のような**基本的な用語を統一された定義にすることである。**これらの語のいくつかはNASA文書の中だけでもバージョンが存在する。例としてこのうちのいくつかを示す。

1）ハザードの定義

米国の文書においてはいくつかの表現で定義されているがいずれも本質的な違いはないが1700.1BのNASA安全方針で統一すべきであろう。

NHB-1700.1B：“Existing or potential condition that can result in or contribute to a mishap”

SSP 30309E：“The presence of a potential risk situation caused by an unsafe act or condition”

NASDAでは「安全・開発保証要求書」に「NASA安全方針」と同じ定義を採用している。

2）リスクの定義

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」：“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.”

NHB5300.4(1D-2)：“The chance (qualitative) of loss of personal capability, loss of system, or damage to or loss of equipment or property.”であった。

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."

NASDA では 1088D に NHB5300.4(1D-2)と同じ定義を採用している。

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。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。

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使って、**被害の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。

3）安全の定義

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)："Freedom from chance of injury or loss of personnel, equipment or property."

NHB 1700.1 (V1-B)：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."

NASDA では NHB5300.4(1D-2)の定義を採用している。

著者の考えでは**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。そして非安全（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、**意思決定者にとって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あってはならない。**

8. 実世界における確率の定義

数学的な定義は明らかなことであるが、工学で用いる「確率」の定義を見直すことが最も重要である。最近、宇宙開発に対する緊縮な環境下において確率論的リスク・アセスメント（PRA）が効果的な管理手段として再び注目されてきているからでもある。

確率理論の応用として、実世界の事象に対して確率モデルを作ってその確率モデルにより事象の発生が高い低いの議論をしても意思決定には直接役立つわけではない。その確率モデルがどの程度実世界の事象を表しているかの不確かさが生まれるからである。ネイマン・ピアソンによる仮説・検定論の応用からモデルの確かさを信頼水準で表現する方法は論理の展開としては誤ってはいないが、信頼水準の取り方に何の根拠もないことから本質的な解決にはなっていない。

本質的な解決は、**確率の定義として確信の度合いとする**ことにより得られる。確信の度合いは知り得た情報から数値を割り当てることで決められる。情報に基づき数値を割り当てる際にはベイズの定理が支配的な役割を果たす。つまりベイズ流統計学から確率を決めることが最も合理的である。

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。

文献

1) 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、 (IGA) 、1988

2) 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、 (MOU)、1989

3) SSP 30000 "Program Definition and Requirements Document", (PDRD) Section 9 Safety and

Product Assurance Requirement

4) SSP 30309E "Safety Analysis and Risk Assessment Requirements Document International Space Station Alpha Program", October 28, 1994

5) SSP 30234 "Instructions for Preparations of Failure Modes and Effects Analysis and Critical Items List for Space Station"

6) SSP 30459 "International Space Station Interface Control Plan"

7) SSP 30513 "Space Station Ionizing Radiation Environment Effects Test and Analysis Techniques"

8) SSP 50005 "International Space Station Flight Crew Integration Standards"

9) SSP 50021 "Safety Requirements Document International Space Station", December 12, 1995

10) SSP 50030 "NASA/NASDA Joint Management Plan", March 25, 1994

11) SSP 50038B "Computer-Based Control System Safety Requirements International Space Station Program", November 17, 1995

12) SSP 50126 "NASA/NASDA Bilateral Data Exchange Agreement (BDEA), Lists and Schedules"

13) SSP 50145 "NASA/NASDA Bilateral Safety and Product Assurance Requirements", August 7, 1995

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

15) KHB 1700.7B "Space Shuttle Payload Ground Safety Handbook", September 1, 1992

16) NSTS 1700.7B "Safety Policy and Requirements For Payloads Using the Space Transportation System", January 1989

17) NSTS 1700.7B ADDENDUM "Safety Policy and Requirements For Payloads Using the International Space Station", December 1995

18) MIL-STD-105D "Sampling Procedures and Tables for Inspection by Attributes"

19) MIL-STD-414 "Sampling Procedures and Tables for Inspection by Variables for Percent Defective"

20) ISO 9001 "Quality Systems-Model for Quality, Assurance in Design/Development, Production, Installation and Servicing"

21) IAA-97-IAA.6.2.06 "Risk as a Resource", M. Greenfield, October 6-10, 1997

22) "Space Shuttle Probabilistic Risk Assessment", Joseph R. Fragola, ESREL'96 - PSAM-III, June 24-28 1996, Crete, Greece

23) "Introduction To Probability and Statistics from a Bayesian Viewpoint", D.V.Lindley, 1965

24) "Probability, Statistics, and Truth", Von Mises, R., Dover, New York, 1957.

25) Title 14 of the U.S. Code of Federal Regulations Federal Aviation Regulations

NASDA Documents: (Japanese)

1) NASDA-STD-1B "Configuration Management Provision", October 6, 1997

2) NASDA-STD-16 "Quality Assurance Program Provision", July 21, 1994

3) NASDA-STD-17 "Reliability Program Provision", March 18, 1997
4) NASDA-SPC-558 "Quality Assurance Program Provisions" (disuse)
5) NASDA-SPC-1177A "Reliability Program Provisions" (disuse)
6) NASDA-ESPC-840G "JEM System Specification"
7) NASDA-ESPC-1088D "Safety and Product Assurance Requirements for Japanese Experiment Module (JEM) Attached to the Space Station" October 18, 1995
8) NASDA-ESPC-1681 "Japanese Experiment Module (JEM) Payload Safety and Product Assurance Requirements", June 21, 1995
9) CR-99117 "JEM Material and Process Requirements"
10) CR-99144 "JEM FMEA/CIL Preparation"
11) CR-99145 "JEM Limited Life Item List Preparation"
12) CR-99146 "JEM ORU Data Preparation"
13) CR-99147 "JEM Maintainability Prediction Data Preparation"
14) CR-99050 "JEM EEE Parts Control Plan"
15) CR-99051 "JEM Approve Parts List"
16) CR-99287C "ESD Management Requirements for the EEE Parts", October 31, 1997
17) CR-99302 "JEM Safety and Product Assurance Plan"
18) CRS-94010 "JEM Mechanical Parts Control"
19) CRS-94020 "JEM Special Control Item Control Requirements"
20) CRS-94021 "JEM Acceptance Data Package (ADP) Preparation"
21) CRS-95005 "Software Fault Analysis Procedure"
22) R SOP-20A "Handling Procedures for Parts Data"

Other Document: (Japanese)
1) "Nuclear Safety", Prof. Syunsuke Kondo, dohbun-syoin
2)"Basic Guideline for Safety Assessment to Japanese Experiment Module (JEM) Attached to the Space Station", Safety Assessment Sub-Committee of Space Activities Commission, April 24, 1996
3) "Safety and Product Assurance for JEM", Norikazu Hara, ISTS98-o-2-09V, May, 1998