宇宙機の安全と信頼性

概要

世界で起きた最近の宇宙機の事故を思い出してみると、どこの国のどの機関も規模の大きさに違いはあるものの、失敗を経験していることが判る。この中から宇宙開発事業団が最も近い過去に経験した H－Ⅱ８号機の事故発生状況を少し詳しく見ながら、宇宙機に対して一般的に採用されている主要な安全技術の一部を再確認する。安全とは何か、信頼性とはなにか、そしてリスクとは何かを考えると、物事に対し合理的な対処をするために、これらを定量的に表すことが不可欠で、確率概念が必要となる。しかし、宇宙機の安全及び信頼性分野を支えている筈の現行の確率理論は、その基礎的な部分に問題があると言わざるを得ない状況がある。この問題に全面的な回答を与えているものが、物理学者 E.T.ジェインズが主導した拡張論理としての確率理論である。

静岡大学機械システム工学科のために

平成 15 年 10 月 15 日

原　宣一

１．宇宙機とは

宇宙機とは人工衛星とそれを宇宙に運ぶ輸送機である打ち上げロケットの両方を指している。英語でSpace Craftというと人口惑星を指すことが多い。欧米では、観測センサをペイロードと呼び、それを搭載する衛星をビークル（乗り物）とも言っている。ここではこれらを含めて簡単にロケットと衛星の両方をまとめて宇宙機と呼ぶ。

逆に、宇宙機の範疇に入らないものは航空機を含む乗り物、建造物、地上設備、地上装置や地上機器などである。

宇宙機には共通に特別の難しさがある。それらは、

１）　軽量化が厳しく要求される。

２）　殆ど保全が効かない　（ハッブル宇宙望遠鏡は例外）

３）　環境が厳しい　　（宇宙放射線、デブリ、熱、真空）

宇宙機には次のようなものがある。

人工衛星（通信衛星、放送衛星、気象衛星、地球観測衛星、測位衛星）

惑星探査機　（ボイジャー、ハレー探査機、火星探査機）

宇宙ステーション（ミール、スカイラボ、ISS）

ロケット

現在、世界では主なものとして次のようなロケットが運用されている。

（中国）長征３

（日本）H-ⅡA

M-V

（欧州）アリアンV

（ロシア）プロトン

ソユーズ

（米国）　デルタⅣ

アトラス

タイタンⅣ

スペース・シャトル

２．宇宙分野における最近の事故

最近の宇宙機の大きな事故として次のようなものが思い出される。

1996年６月、アリアンV型１号機が１段目の制御ソフトのバグにより異常飛行を起こし、指令により破壊された。アリアンV型は２号機も２段目のエンジン不具合により軌道投入に失敗した。但し、衛星の制御用ロケットでどうにか静止軌道まで到達できたのでESAでは２号機を失敗としてカウントしていない。

スペース・シャトルは1986年１月に25回目の飛行であったチャレンジャー

が個体ロケット・ブースタ（ＳＲＢ）のシール部分から火炎が吹き出し外部タンク（ＥＴ）を破壊させ、爆発事故を起こした。今年の１月には 113 回目の飛行となるコロンビアが打ち上げ時に外部タンク（ＥＴ）の表面を覆っている断熱材のブロックがはげ落ち、これがオービタの前縁部にあたり、断熱材を損傷させてしまった。再突入の際にこの部分から高温ガスが入り込み機体を破壊させてしまった。

Ｈ－Ⅱロケットは 1998 年２月に打ち上げた５号機が２段エンジンの燃焼室の溶接部分不良により漏れだした高温ガスが電気系統を損傷させ、衛星を目的の軌道には投入させられなかった。目的の軌道には入れられなかったもののこの衛星（きく６号）を使った実験はかなりの部分を実施することはできた。

Ｈ－Ⅱロケット６番目の打ち上げであった８号機は 1999 年１１月に打ち上げられたが１段エンジンの燃料供給ポンプの入り口部分にあるインジューサが疲労破壊を起こし、燃焼停止に至った。衛星軌道に投入出来ないことが確実になり指令破壊がかけられた。

宇宙科学研究所のＭ－Ｖロケット４号機は 2002 年２月に打ち上げられたが１段ロケットのノズルが損傷し軌道投入に失敗した。

世界の主なロケットの打ち上げ実績を調べて見ると 2001 年１２月末現在で以下の表のようになる。

世界のロケット成功率　　２００１年１２月末現在

ロケット	初回打ち上げ	成功数	総打ち上げ	成功率
アトラス	１９６２／５	１６４	１８１	0.906
デルタ	１９６０／５	２７３	２８９	0.945
タイタン	１９６４／５	１９４	２１１	0.919
ＳＴＳ	１９８１／４	１０６	１０７	0.991
アリアン	１９７９／１２	１３６	１４５	0.938
プロトン	１９６５／７	２５６	２８９	0.886
長征	１９７０／４	５８	６５	0.892
Ｍ	１９７０／９	２２	２６	0.846
Ｎ／Ｈ	１９７５／９	２８	３１	0.909

この表に示されるように、どのロケットも 100%の実績は示していない。シャ

トルでさえもコロンビアの事故を入れると0.98になる。成功率は0.85から0.99であると言えよう。この数字は比率であって、野球選手の生涯打率のようなものである。次に打ち上げるロケットの成功確率とは異なるものである。

過去の実績は相対比率であって、成功確率ではないことに留意が必要である。失敗しても、その故障原因を究明し取り除くことによって、同じ失敗は繰り返さないという確信のもとに、次の成功確率は十分高いと考えられるからこそ打ち上げるのである。

３．Ｈ－Ⅱロケット８号機の打ち上げと指令破壊

Ｈ－Ⅱロケット８号機の事故例を少し詳細に見てみる。

Ｈ－ⅡロケットとＨ－ⅡＡ型と外見上の大きな違いは２本の個体ロケットが細長いことである。

打ち上げ射場は種子島の南端で東側に面あり太平洋に面している。射点から北側と西側に限界線が引かれている。

８号機は静止衛星打ち上げであったので垂直に飛び上がった後、東に向かって飛んでいく。１段と２段エンジンでパーキング軌道に入り、エンジンを止め惰性で赤道上空まで飛んでいく。赤道付近で２段を再着火し、再び加速して楕円軌道に入る予定であった。

ロケットは大気圏コースを（必然的に）取ることから、瞬時落下点軌跡は、種子島の対蹠点で誤差が少なくなる。

安全確保の初歩的でかつ重要な対策は離れていることである。つまり、「君子危うきに近寄らず」を実践することに他ならない。

打ち上げの時には、射点の近くだけでなく、ＳＲＢやフェアリング、１段の落下域は船舶や航空機が入らないようにお願いする。

テレメータの情報を基に飛行中のロケットがその時点でエンジン停止をしたらどこに落ちるかをプロットしたものが真空中落下予測点軌跡である。空気がないものとしての計算結果であるからこのような名称がついている。

８号機はプロット中の落下予測点軌跡がフェアリング落下予想区域に入ってからその進みが止まり、プロットが妙な動きをした。プロットが止まることはエンジンの推進力が無くなったことを示している。

測度データによるプロットも加速が止まったことを示した。

高度データによるプロット計画から外れてしまい、その後どんどん落下していることを示した。

ロケットの動きを監視しているレーダ局のアンテナ上下角は最高で50度近くまでになる。５度以上あれば問題なく受信できる。

８号機は通信が途絶する直前に指令破壊信号が送信された。ロケットは予定

の飛行からそれた場合、２次被害を与えないように破壊する装備が付けられていて、地上側にもそのための施設を用意してある。安全確保の手段として、被害の拡大を防ぐことも重要な要素である。

原子炉における安全確保はもっぱら多重防御が強調されている。この中の一つに炉心冷却装置がある。

有人飛行のスペース・シャトルにおいても民家に突っ込む可能性が高くなると爆破される。爆破の権限を持っているのは米国空軍のレンジ・セーフテイ担当官である。迷っている時間はないので、色々な状況を想定してシミュレーションによる訓練が行なわれる。ロケットの指令破壊担当者も同じように訓練して打ち上げに臨んでいる。

シャトルの場合、打ち上げた後の飛行中止モードは当初から４種類が計画されていた。

RTLS は打ち上げ直後の不具合で、射点近傍の滑走路に降りるもの。

TAL は大西洋を越えた地点の滑走路に降りるもの。このため、用意された滑走路の天候が悪くて打ち上げが出来ないこともある。

AOA は兎に角地球周回軌道に入って一周して降りてくるもの。

ATO は軌道に乗ってしまうもの。

これまで ATO は１回あった。ミッション期間を短くして早めに降りてきた。NASA の文書には指令破壊のことを明記した文書は無い。これは空軍の権限とされているからである。

飛行安全システムの中心的技術は電波による指令破壊信号の送信である。８号機から送信周波数が変更になっている。

打ち上げ直後はアンテナ上下角が小さく海面の反射等で上手く電波を捕らえられない。このため空間に糸を張り、人間が目視で飛行経路を監視するシステムがスカイスクリーンである。しかし、最近はカメラとモニタスクリーンに置き換えられた。

地上系のハードウエア構成はレーダ・アンテナ系、テレメータ受信アンテナ系、コマンド送信アンテナ系、計算コンピュータおよびモニタ画面等で構成されている。

ロケットには、破壊信号を受ける電子機器群にタンクを破壊するための爆破線と普段は絶対に作動しないようにするセーフ・アーム装置などが搭載されている。

ミッションの目的には直接関係のない指令破壊であり、それなりの費用がかかるものであるが、世界中で見れば指令破壊も少ないとは言えず、まだまだ無くせないものである。

ロケットに特徴的な部品は火工品であろう。鈍感型起爆管、セーフ・アーム

装置、延時起爆管、導爆線、隔壁型起爆管、カッタ組立、破壊用火工品、等がある。

火工品の特徴は高エネルギー密度部品でありながら高信頼度であること。タンクやモーター・ケースの破壊はノイマン効果を利用して爆破エネルギーを集中させている。爆破薬と発射薬との相違は燃焼速度の差である。個体ロケットの推進薬は火薬と呼ばれるが燃焼速度が遅いものであることは言うまでもない。このような知識が必要なため、ロケットの設計者には何も国家資格は必要でないが、火工品の取り扱いには国家が定めた資格を持っていなければならない。

4．宇宙機の安全確保

安全を確保する活動を安全保証（Safety Assurance）という。保証とは確実なものとすることである。

さて、NASA では安全保証の目的を 1993 年まで次の事項の発生を避けることであると定めていた。

1） 人命の喪失
2） 人身の障害
3） 装置若しくは財産の損傷あるいは喪失
4） ミッション又は試験の不成功
5） 過大なリスク（大衆が非難するような事象）

つまり安全の対象は人命だけでないということである。

その後少し表現の修正はあったが大きな変更はなかった。1999 になって NASA は安全確保の対象順位として優先順序をつけることを明確にした。

1） 大衆
2） 宇宙飛行士
3） NASA 職員
4） 設備

の順である。これにより、宇宙飛行士の乗ったシャトルであっても大衆の安全を優先させて爆破限界線を越えた時には爆破することも止む無しとしていることが読みとれる。

安全とは危険でないこと。つまり安全は危険と反対の概念であり、原子力分野も同じ概念である。

安全と安全性は区別して使われているような場合もあるが、この違いを定義することは今や無益である。「・・・性」は状態を示すために使われるが「安全」はもともと状態を示す用語である。

NASA は安全を、「負傷、死亡、若しくは疾病または施設・設備若しくは財産

の破損や損失を引き起こす要因がないことをいう。」と定義している。

しかし、よく考えると安全とはリスクが許容出来るほど小さい状態をいうという定義が適切である。最近の欧州の安全関係文書ではこのようになってきている。

「価値」の意味を人間に取って大事なものと広く取れば、安全とは価値が脅かされない状態と言えるのである。

ハザードとは日本語に無い概念で、「事故をもたらす要因が潜在または顕在する状態を言う。(NASA)」

事故の定義は良い。NASA では Accident、Incident、Close Call、というランク付けがある。NASDA でも事故報告書とヒヤリハット報告書を定めている。Close Call はヒヤリハットに相当する。

さて、リスクの定義が問題である。NASA を始め多くの文書で次のようになっている。

事故が起きた場合の損失の大きさとその事故が起きる可能性の度合いを組み合わせた（通常、掛け合わせた）概念をいう。

しかし、NASA においても、リスクにおいて掛け合わせるものは何かがしっかり把握されていないようである。例えば国際宇宙ステーション（ISS）では３ｘ４のリスク・マトリックスで安全を評価しているだけに留まっている。

リスクは高い、低いと比べることに意義がある。比べる対象は何か文書に明示された基準であることも、自分の心の中にしか存在しない漠然としたものに過ぎないこともある。そして、比べることができるのは一次元量に限られることは中学生が数学で習うことである。

従って、リスクは横軸の損失を価値の単位で表し、縦軸を確率で表したものを掛け合わせたもの、つまり損失の期待値であると定義することが適切である。リスクを損失の期待値であると定義したのは意志決定論のワルドが最初である。このことから、リスクは価値の次元を持つことが明白である。

世の中で、ハザードという用語はあまり使われていず、リスクもハザードも混同されている。つまり識別すべきはハザードまたはリスク事項であって、識別されたリスクを評価しなければならない。これが安全解析（またはハザード解析）で、ハザードを識別しリスクを評価するのである。

さて、安全解析の第一歩は如何にハザードを識別するか、である。「怖いもの知らず」であってはならないのである。

ハザードの識別は経験によることが大きい。FTA（故障の木解析）を行ってハザードを識別することにはなっているが、FTA 自体が経験によるところが大きい。

ハザードが識別されたら設計で対処することになる。このとき、安全技術要

求は何かを調べて落ちがないようにする。そして、設計が決まればリスク解析を行い、リスクが小さいことの確認を行う。途中で何回かの安全審査を行うことも安全確保の重要な要素と認識されている。

発生確率が小さいか否かの判定が設計したものの信頼度を見ることになる。信頼度については後述するように現状では問題点があると言わざるを得ない。

宇宙ステーションのみならず典型的な安全技術要求に故障許容要求がある。人命の喪失にたいして 2FT を要求するとは、二つの故障または一つの故障と一つの運用ミス、あるいは二つの運用ミスが同時に起こっても安全でなければならないというものである。

「故障を許容するとは何事か」と言う人は誤解している。「人間はミスする機械は故障する」ということを認め、それでも安全なようにしなければならないという考え方を取っているのである。

ハザードな操作系にはインヒビット（セーフ・アーム装置は一例）を設けなければならないということも安全技術要求の一つである。

通常、安全技術要求で安全率が規定されている。安全率 1.5 以上という要求は、構造の軽量化のための努力を如何にやろうとも、許容応力の最大作用応力に対する比が 1.5 を下回ってはならない、という要求である。安全率が高ければ安全というものでもない。粗雑な計算では安全率が高くても危ないかもしれない。宇宙機では安全率を高く取りすぎて重くなり性能が出ないと却って危ないことになる。技術の現状（State of the Arts）を示す数値でもある。

なお、疲労破壊が予想される部位では荷重のサイクル数に対する安全係数を設定して疲労破壊が起こらない内に取り替えることが安全確保の手段である。

5．宇宙機の信頼性とその問題点

信頼性があるか無いかを表現するために信頼度という用語がある。JIS の定義では「アイテムが与えられた条件で、規定の期間中、要求された機能を果たす確率」とされている。

信頼度の定義はこれで良いが、JIS でも確率の定義が定められていないところが問題である。実世界の確率は暗黙のうちにフォン・ミーゼスによる確率定義が採用されているのであるが、その定義では多くの矛盾が生じる。信頼度を要求された場合果たして、その要求を満足しているか否か示せるであろうか。もし、信頼度要求を満たしているかいないか示せないのであれば要求しても無駄である。信頼性は無視するというものと高い信頼性が望まれるものとでは明らかに対処が異なってくるであろう。

現状で暗黙理に採用されている正統派統計学の確率定義ではこの確率が満たされているか否かが示せないのである。従来、計算では要求を満足していると

いうことで済ませてきた。その計算が如何なる仮定に基づくものであるかを誰も質問することなく、済まされてきた。分布を仮定するとは、体よく答えを仮定しているきらいがあるのである。仮定の妥当性を質問することさえ諦められてきたように見える。独立性の仮定ですら、そのようにしないと計算できないからそうされてきた。これらのことはまさに驚くべきことではないか。

信頼性確保のために定性的に行われてきたことは、何も悪くはないので信頼度はこのようなものでも済まされてのであろう。しかし、本来信頼性は定量的に表現出来ないものなのであろうか、これを考えて見なければならない。

なお、最近では欧州が先導して信頼性という概念に保全性を加えてデペンダビリティと言うようになってきている。

通常、信頼度の推定のために信頼度ブロック図を描いて信頼度計算を行っている。

信頼度計算の例としてH－Ⅱロケット基本設計終了時のものを示す。信頼度は確率であるから、少数点以下で9でない数値の後は一桁程度しか意味を持たない。小数点以下で0でない数値が現れた後にもう一桁程度しか意味を持ち得ないことと同じである。つまり有効桁に注意すべきである。

システムの信頼度はサブシステムの信頼度から計算し、だんだん要素が細かくなり最後は部品レベルになる。部品の信頼度はどのように求められるかが問題である。1960 年代から電子機器部品についての信頼度予測法としてMIL-HDBK-217F という文書が教科書的存在であった。しかし、データが古い等の問題が多く文書の改訂維持も行われなくなった。NASA ではもはや使われていない。代替として PRISM が発表されているが本質的な問題の解決にはなっていない。

部品レベルではその信頼度は9が多く並ぶレベルまで高くないと、システムレベルでは高い信頼度であると言えない。果たして試験が出来る個数程度で高信頼度であると言えるものであろうか。

信頼性を定量的に表すために確率を使って信頼度を定義したものの、その確率定義に疑義があるので、何らかの仮定を置かない限り信頼度が求まらないのである。

6．拡張論理としての確率理論

正統派統計学の採用している確率は不合理であり矛盾を呈するものであることを明確に述べているのが E.T.ジェインズによる拡張論理としての確率理論である。

この本の趣旨を極めて簡単に述べると次のようになる。

事象の発生に関する命題の真偽は関係する情報を得ることによってその妥当

性が変化する。

強い３段論法におけるものと同様に弱い３段論法においても論理演算であるブール代数が成立する。

推論の基盤として、この妥当性に数値が対応すること、この対応を常識に一致させること、及び首尾一貫性を基本的な要求（デシダレータと呼ぶ）とする。

これから得られた確率はベルヌーイ、ラプラスの流れに沿ったものである。

ラプラスの確率が非難された「等しく起こりやすい」という表現の部分は論理的な帰結として導かれるものであった。また、これに基づく多くのパラドックスは安易に無限操作を持ち込んだことにあった。

シャノンはデシダレータの視点を変えて表現したシャノンの条件から情報エントロピーを導き出した。

論理としての確率理論は現代物理学の基礎をなす考え方であり、情報理論の基礎をも支えている。

正統派統計学の頻度概念による確率理論は、合理性と首尾一貫性に基づいていないので、時に不合理であり矛盾を来している。

ラプラスの定義はもともとベルヌーイが最初に示したものである。Equally likely は論理的帰結であった。

フォン・ミーゼスは定義に極限値を採用しているが、実世界にはあり得ないもの。

コルモゴロフの確率は公理に基づいているのでその確率理論は微動だにしないが、その公理体系が実世界を写していない。実世界では相互背反でない事象を取り扱う場面が多い。

拡張論理としての確率理論では、結局命題の真偽対する確信の度合いに割り当てた数値が確率である。この数値の割り当て方は最大エントロピー法によって割り当てたものでなければならないことになる。

具体的な割り当て方は、等確率の原理とベイズの定理が大きな役割を果たすものである。

拡張論理としての確率理論の全体図を示す。重要なことは論理的推論の帰結として理論式が導かれていることである。まず、デシダレータとシャノンの条件は殆ど同義で不確かなものに対して人間が理解できる考え方なのである。デシダレータから確率の積の規則と和の規則が導きだされ、確率理論の基礎をなしている。これら二つの規則から無差別の原理が導かれ、ラプラスの確率定義となる。一方シャノンの条件から情報エントロピーが必然的に導かれ、情報理論の基礎を作っている。さらに、不変量の考え方は人間の理解できる表現で不変であるべき量なのであるが、現実世界にこの不変量の考え方で推論すると有名なガウスの誤差分布則が出てくるし、これを３次元において応用したものが

ハーシェル・マクスウエルの気体分子の速度分布則に他ならない。このようにして導かれた統計力学がマクロの世界で現実をよく説明している。アインシュタインの相対性原理においても同様な考え方がなされている。

人間に都合の良いように推論した結果のみが自然を説明できることは一見不思議なように見えるが、よく考えるとそうでなければ人間は自然を理解出来ないことも判る。

終わりに

宇宙機はなかなか100%の成功率も、或いは100%の成功確率も得られないものであることを説明した。主たる理由は、宇宙開発が重力との戦いであるからである。ロケットに比べれば、船や機関車や飛行機でさえも、これらは等重力ポテンシャル面をすべっているようなものである。

このように１００%の成功が困難な宇宙開発を多額の金をかけて行う必要があるのかを冷静に考えてみると、宇宙開発も人類の目的達成のために必要なことの一つであると結論できる。

それでは人類の目的とは何かを途中の考察を省略して結論だけを示すと、私の哲学的考察結果は宇宙の寿命内で自然を理解することになるのである。

参考文献

E.T. Jaynes, “Probability Theory: The Logic of Science”, Cambridge University Press, 2003.4

原、冨田、「一回の成功情報がもたらす信頼度の向上」、第15回信頼性シンポジウム、2002年11月

原、「少数の属性試験結果から得られる確信の度合い」、第14回信頼性シンポジウム、2001年11月

原、「リスク評価再考」、第13回信頼性シンポジウム、2000年11月

原、「FMEA手法の改良提案」、第30回信頼性・保全性シンポジウム、2000年7月

（おしまい）