

アポロ計画のリスク許容値と確率論的リスク評価

原 宣一

(宇宙開発事業団安全・信頼性管理部勤務)

はじめに

人間が初めて月に降り立って30年が経過した。NHKはこれを記念し、「宇宙デジタル図鑑・アポロ月着陸30年・大いなる遺産」という番組を放映した。これを見ていて、ある論文を読みかけのまま放っておいたことを思い出した。それはアポロ計画のリスク管理はどのようなものであったかを概説し、今後のスペース・シャトル運用におけるリスク管理をどのように行おうとしているのかを示すものである。

NASDAは今後の改革の一つとして、開発プロジェクトのリスク管理をしっかり行うことを挙げている。本論文は時宜を得た参考文献に違いなく、急ぎ翻訳を試みた。以下は興味深い記述について要約し、私の解説を{ }で書き添えたものである。終わりに本論文の逐語訳も添付した。

論文の標題

標題は「スペース・シャトルの確率論的リスク評価」(Shuttle Probabilistic Risk Assessment) となっている。

{まず「リスク管理をする」ということはどのようなリスクがあるかを識別し、それらリスクの大きさを評価して全体としてのリスクを小さくするための資源割り当てを最適にすることである。また、リスクという言葉は多くの場面で使われるようになって意味合いが広がっているが、本来リスクとは被害の大きさとそれが起こる確率を乗じたもの(正確には被害の期待値)である。従って、リスクの大きさを評価するということはリスクを定量的に扱わねばならないということになり、確率論的リスク評価(PRA)という言葉が使われる、論文の中では定量的リスク評価(Quantitative Risk Assessment)という言葉も出てくるがPRAと同義であり、本論文の中だけでも区別なしに使われている。}

定量的リスク評価

定量的リスク評価は17世紀にまで遡る。この頃から輸送の通行安全頻度の統計が取られ生命保険産業の基礎を成した。しかし、實際上この確率論的リスク評価が使われたのは数多くの観察が可能な保険業など狭い範囲に長らく留まっていた。この理由は相対頻度の概念を基礎におく確率の定義に由来するもので、本来この定義では意思決定問題に使いようがなかったからである。このため、

統計学者の一派と物理学者を味方とする主観確率論者またはベイジアンと呼ばれる一派との論争が長らく続いたまま今日に至っている。

{本論文では現行の頻度概念では無理があり、主観確率のほうが適切でないかということを示唆するだけに留まっている。現行の信頼性工学が頻度概念に基礎を置いているし、NASAを初め世の中の大勢が頻度概念で済ましていることに遠慮しているように思われる。}

アポロ計画での定量的リスク評価

アポロ計画では当初において定量的数値目標を持つべきだとの結論に達し、ミッション遂行に対し百分の一のリスクを許容し、乗組員の安全について千分の一のリスクを許容した。そして、定量的リスク把握のため、サービス・モジュールやルナ・モジュールの確率モデルの作成まで行ったが、途中で定量的リスクを掴むことを止めてしまった。その代わりに、各種の審査を行うことで済ませた。特に重視したのは故障モードおよび影響解析(FMEA)であり、この結果識別された単一故障点品目の設計審査を重視した。このプロセスをFMEA/CILプロセスと呼んでいる。

{乗組員の安全についてNASA幹部が千分の一のリスクを許容したということは、その数値が高いと言うべきか低いと言うべきかであるが、英断には違いない。現在の労働災害統計で最も高いとされている鉱業で年間千分の一より高く、漁業や林業がこれより低い。癌による死亡は年間千分の一より高く、最近の報道で日本人のサラリーマンの自殺は年間五千分の一とのことであった。これらの数字と、当時米国がソ連との冷戦下での月着陸競争であったことを考え合わせると、十分高い数字のリスク許容目標であったと思われる。}

FMEA/CILプロセスとは定性的に重要品目の洗い出しとその設計が納得できるものであることを確認する文書の作成様式およびその承認手順であり、国際宇宙ステーション(ISS)計画においてもNASAはこの実施を重要視している。}

アポロ計画で定量的リスク評価を断念した理由

FMEA/CILプロセスもリスクに焦点が合っていないなどいくつかの欠点があるにも拘わらず、NASAはアポロ計画の途中で定量的リスク評価を止めてしまった。この理由として次のようなことが考えられる。

- (1) FMEA/CILの欠点はアポロ時代には目立たなかった。
- (2) 重要なものでも定量的アプローチを適切(3)に処理することが難しかった。
- (4) 作ってみた定量的モデルからの予測が実感とかけ離れたものでしかなかった。

そして、試験費用が豊富に用意されていたことが背景にあったことであろう。

{定量的リスクモデルを作ってみたが実感とかけ離れたものでしかなかった理由として、著者はNASAが頻度概念の確率に拘っていたからであると暗に言っているようである。}

シャトルの定量的リスク評価

チャレンジャーの事故の後、ロジャース委員会がNASAに対してPRAを実施すべきだとの勧告があつてシャトルの運用に対する定量的リスク評価の研究が進んだ。出来上がった定量的リスク評価のモデルはコンポーネントレベルまでの詳細さで構成されており、NASAだけでなく契約者の経験も組み込まれている。また、飛行する都度それらのデータも組み込むことが出来るようになっている、生きたモデルである。

{PRAはロジャース委員会の委員の一人であつたカリフォルニア工科大学のノーベル物理学賞に輝くリチャード・ファインマン教授が強く主張したものである。教授は事故調査の中で、多くの人とインタビューした結果、シャトルで致命的な故障が起きる確率について、大雑把に言って現場の人は百分の一と考えているのに反し、管理部門の長は十万分の一と考えているとして、その答えの開きを問題視した意見書を残している。なお、余談ながら都立科学技術大学の千代島雅氏は著書「天才物理学者たちの世界を欺いた科学の10大理論」の中でファインマン教授の電磁気学と陽電子に関する2つの理論を槍玉に上げ、厳しく批判している。}

シャトルのリスク管理

定量的リスク評価の技術はアルゴリズムの改良とコンピュータの進歩により劇的に進歩した。故障の木解析(FTA)用の故障の木や事象の木解析(ETA)用の事象の木は自動的に短時間で手軽にラップトップ・パソコンでも作図出来るようになった。これらの進歩があつてリスク管理が定量的に出来るようになった。確率の数値が必要な部分はモンテカルロ法によっているがこの場合も時間はそんなにからない。

{著者はアポロ時代の定量的アプローチの断念は確率の定義にあるように示唆しながら、ここではコンピュータの進歩が頻度概念でもモンテカルロ法で解決出来るかのように言っている。モンテカルロ法はコンピュータによる数百回のシミュレーションで統計を取り、その頻度を用いて確率とする手法。原始的で粗野な方法であるが、わかり易い。ロケットの飛行安全用ソフトで昔から多用されている。ラップトップの性能はこの論文が書かれた2,3年前からさらに数倍は向上している。}

ゼロベースのリスク管理の概念

緊縮予算の下でのシャトルの運行とリスク管理という観点から考察を進めた結果、ゼロベースのリスク管理という概念に到達した。シャトルの運行に絶対的に必要な工程とはペイロードの積み込み以外にはなくこれがゼロベースである。これに加えての試験や点検はそれを省いたときのリスクの大きさととの兼ね合いで実施を図るというのがゼロベースのリスク管理である。シャトル運用コストと安全リスクとの兼ね合いは正確な定量的リスク評価PRAが根幹であり、将来シャトルの運用を商業ベースの民間の会社に移した時にも安全がおろそかにされないための保証ともなる。

{ゼロベースのリスク管理の概念は定量的リスク管理が常識になった時代には基礎的な概念になると思われる。}

著者について

{著者のジョセフ・フラゴラ氏はSAIC社の技師である。SAIC社は社員37000人を有し、創立30周年を迎えている。変わっているのは社員が所有するエンジニアリング会社であることだろう。NASAのJSCではISSプログラムを支援する会社の一つとしてNASAを支援している。}