信頼度のジレンマ

原　宣一

はじめに

信頼性を図る尺度である信頼度についてお話いたします。

最初に、最近と言っても１０年近く前に調べた結果ですが、ロケットの事故の例をいくつか見てみましょう。本当の最近でも宇宙技術として大躍進があったわけではありませんので、大きくは変わっていません。

アリアンＶ型は欧州宇宙局（ＥＳＡ）の開発した大型ロケットですが１号機、２号機が失敗しています。

スペース・シャトルもチャレンジャー号とコロンビア号を失っています。

Ｈ２ロケットも最初の４機は成功したのですが５号機と８号機で失敗しています。都合により順序を入れ替えていましたので、７号機が８号機の打ち上げが後に予定されていたのですが、結局、７号機は信頼性に自信が持てないとの理由で打ち上げられませんでした。

固体ロケットのミュー５型ロケットも４号機で失敗しています。Ｈ２Ａロケットでは６号機で失敗しております。

宇宙分野における最近の事故

アリアンＶロケット：
１号機、1996年６月、１段制御ソフト
２号機、1997年10月、２段エンジン不具合

スペース・シャトル：
チャレンジャー、1986年１月、SRBシール漏れ
コロンビア、2003年１月、耐熱タイル損傷

Ｈ－Ⅱロケット：
５号機、1998年２月、２段エンジン・燃焼室
８号機、1999年11月、１段エンジン・ポンプ

Ｍ－Ⅴロケット：
４号機、2000年２月、１段ノズル

Ｈ－ⅡＡロケット：
6号機、2003年11月、SRB

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

世界中のロケットで累積の成功率を見ますと、この表は２０

０１年１２月現在で少し古くなってしまいましたが、０．８５から０．９５ぐらいであることが判ります。

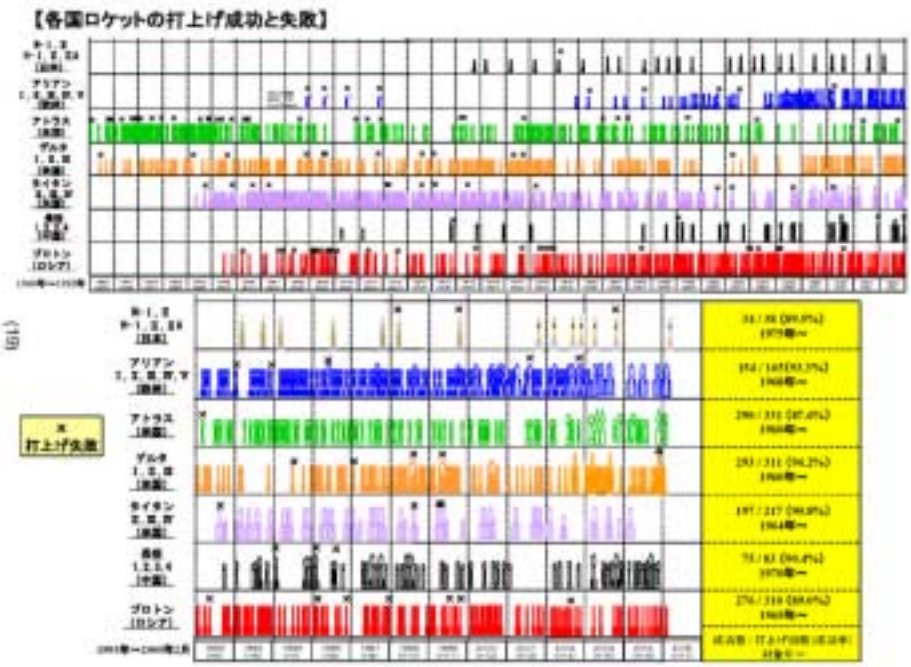
スペース・シャトルは有人機ですので、さすがに高かったのですが、それでもコロンビアを失いもしたから、現在は０．９８強に下がっています。

横軸に時間軸をとって一目でわかるようにした図があります。同じロケットですとだんだん失敗しなくなっていることが見て取れます。中国の長征ロケットも最近は失敗が少ないようです。

世界のロケットの例をみますと、絶対に失敗しないロケットというものはないと断言できます。こんなことを威張っても仕方がありませんが。

失敗が少ないロケットを信頼性の高いロケットと言っております。

信頼性が高い、信頼性がより高い、あるいは信頼性が極めて高いと言っても、言葉の表現ではあいまいですので、信頼性の高い、低い、の程度を数値で表したものが信頼度なのです。



1．信頼度表現の必要性

最初に一つの例から考えてみます。

ある会社が新しい品物を5個納める契約を受けたものとします。その品物は作るのに非常に難しくて必ずしも成功するとは限りません。

発注者は「十分信頼性のあるものを作ってください」と受注会社に頼みます。

するとその会社は「任せておいて下さい。十分信頼性のあるものを作って見せますから」と胸を叩いて請け負います。

さて、納められた品物を使ってみますと、5個のうち成功したのは2個だけでした。

発注者は「十分信頼性のあるものを作るように頼んだのにたった2個しか成功しなかった。お金を少し返せ。」と文句を言います。

納めた会社は「十分信頼性のあるものを作ったから2個も成功した」と反論します。

発注者が裁判に訴えたらどちらが勝つでしょうか。

これは最初の契約の仕方が悪かったことは間違いありません。

最初から「5個のうち3個以上成功すること」とでも契約書に書いておけば良かったのでしょう。

さて、もし品物が非常に高価なもので1個しか買えない場合はどうでしょうか。

「信頼性があるもの」という表現では両者で解釈の齟齬が生じる可能性があります。

もちろん「１００％確かなものを作れ。もし失敗したら費用の１０倍を返して貰う」というような契約にできれば発注者は安心です。このような契約を受けてくれるところがあれば、それに越したことはありません。

しかし、受注会社としては、そのような契約では如何に契約金額が魅力的であっても受けられないでしょう。あるいは自社製品に保険をかけることによって１０倍の弁償にも対処しようとするかも知れません。そうなれば、契約金額には保険料を加算しなければなりません。保険会社が妥当な額の保険金で受けるかどうかは判りません。

逆に安ければ失敗しても良いというものでもありません。

結局、失敗しても賠償しろとは言わないが出来るだけ信頼性の高いものをつくること、というような要求で済まざるを得ないのです。

そして、信頼度という言葉は出来るだけ信頼性の高いという言葉の表現として使われます。

数値表現で信頼度０．８以上のものという表現であれば少しは話の取り違えが少ないと期待できます。

このことからも信頼度は必要な数値です。

2. 信頼度の定義

日本の工業規格であるＪＩＳには信頼性用語の定義があります。

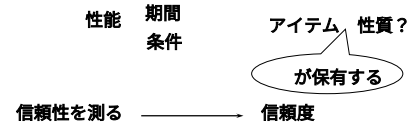
これによると信頼性とはアイテムが所定の期間、所定の環境下で、所定の性能を発揮する性質とされています。アイテムとは品目のことです。

そして、信頼度の定義はアイテムが所定の期間、所定の環境下で、所定の性能を発揮する確率とされています。

つまり信頼度とはアイテムの成功確率であるということになります。

1）定義・・・信頼性

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性質 （JIS Z 8115）



7

1）定義・・・信頼度

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（JIS Z 8115）

- **確率がJISで定義されていない！**
- **信頼度要求は結果を得ても、要求を満たしたことの証明にならない**
- **信頼度要求は無駄か？　　否。精神規定？**
- **英語では信頼性も信頼度も Reliability**

8

ところがＪＩＳには確率の定義が載せられていません。

ＪＩＳを定めた人たちは、確率の定義がいくつもあるということを知らなかったのでしょうか。

現行の信頼性工学では、暗黙のうちに頻度概念の確率の定義が使われています。この点が間違いであったというのが私の主張です。

詳しくは確率の話のところに譲りますが、ここでは確率は確信の度合いであるとだけ言っておきます。

一般によく誤解されているのが成功率です。これは信頼度ではありません。最初の数機が成功したからと言って、信頼度１００％とは言えないでしょう。逆に、１号機が失敗したから、２号機目は信頼度０％だというのもあまりにも悲観的過ぎます。

１００機も打ち上げて失敗したのが２，３機しかない場合は、成功率を使って信頼度９７％であるとか９８％であるというのは妥当です。数が多ければ、成功率を信頼度と考えて構いません。

それでは、最初の１号機は信頼度がないのでしょうか。折角精魂込めて開発したものなのに、信頼度がありませんということでは困ってしまいます。

頻度概念の確率では駄目な理由がこのことからだけでも察せられるでしょう。

3．信頼度ブロック図

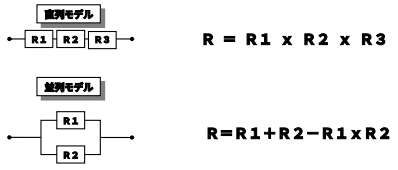
電子機器に対しては、信頼度予測のハンドブックとして有名な文書があります。MIL-HDBK-217という文書番号がついていて、宇宙開発の関係者には大きな影響を与えてきました。

この文書の信頼度予測の考え方は次のとおりです。

システムの信頼度はサブシステムの信頼度から合成できて、サブシステムの信頼度はそれを構成するコンポーネントの信頼度から合成できる。また、コンポーネントの信頼度はそれを構成する部品の信頼度から合成できる、とするものです。

部品の信頼度はどうするのかと言いますと過去で使った実績を使うというのです。

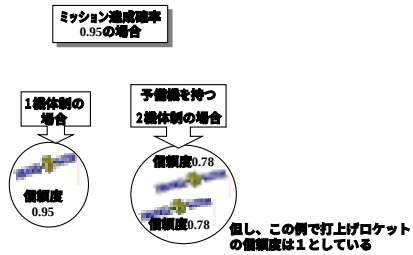
2）信頼度ブロック図



システムの信頼度とその構成要素との間の機能的関連を示す線図

9

3）予備機を持つ必要性



10

サブシステムの信頼度を合成してシステムの信頼度を求めるのは次のようにやります。

まずシステムのブロック図を描きます。

これはシステムがどのようなサブシステムからどのような構成になっているかを論理的に描いたものです。

これには基礎的なものに直列モデルと並列モデルがあります。

一般的にはこれらが組み合わさった複雑なものになります。

もしシステムが三つのサブシステムの直列モデルで表されるならば、サブシステムそれぞれの信頼度をＲ１、Ｒ２、Ｒ３としますとシステムの信頼度はそれらを乗じたものになります。

３段式ロケットは各段が成功しないと全体が成功したことになりませんから、このようなモデルで表されるでしょう。

並列モデルのシステム信頼度計算は少し複雑な式になります。

システムが冗長系を持つ場合には並列モデルになります。

並列モデルではどちらかのサブシステムが成功すればシステムの成功になりますので、冗長系の信頼度は一つの信頼度より高くなります。

これに対して直列系ではどんどん信頼度が低くなってしまいます。このため、部品の信頼度は高いことが要求されるのです。

簡単な例を数字であたってみます。

衛星のミッション達成の信頼度として９５％要求されたとします。

予算がなくて1機しか打ち上げられないと、その衛星の信頼度がそのまま９５％の高いものでなければならないことになります。

しかし、２機打ち上げられる余裕がありますと、個々の衛星の信頼度は７８％で良いことになります。

一般に信頼度が低くて済む衛星は安く作れますから場合によっては数を多く打つほうが良い場合もあります。

前の前のＮＡＳＡ長官ゴールディンが就任したときにベター・ファスター・チーパーを掲げましたが、この標語は後者でいこうとしたものと言えます。

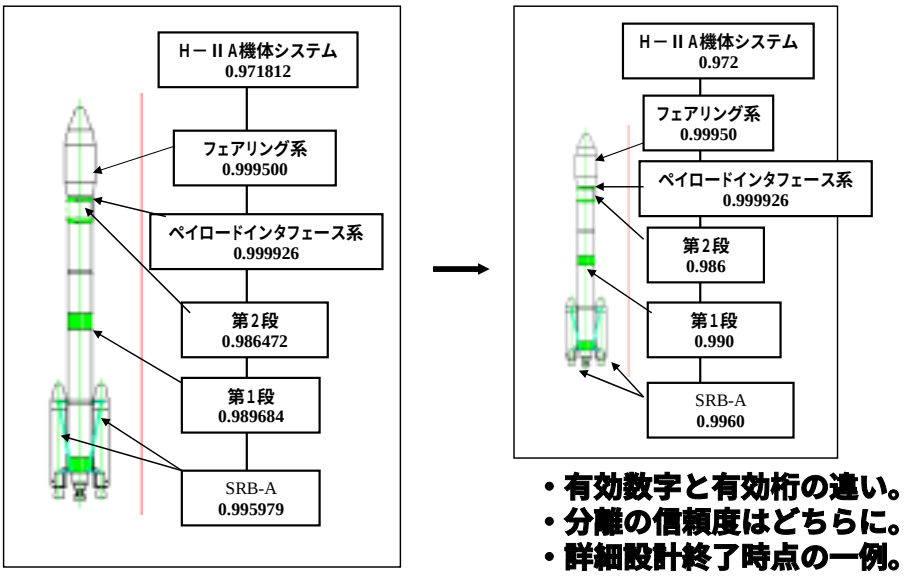
信頼度計算の具体例として、ロケットの場合を紹介します。Ｈ２Ａロケット詳細設計終了時点での報告例です。

もちろん、現在はこのような数字も一切外には出さないことになっていますので、数値は仮想の一例です。

このような形で直列系モデルになっていると理解してください。

ＳＲＢ・Ａと名づけられた固体ロケットは２機取り付けられていますが、これらは1機でも失敗するとロケット全体の失敗になりますからブロック図では並列モデルでなく直列モデルになります。ブロック図は論理的に描くということはそういうことです。

４）信頼度計算の現状・・・H-ⅡAロケット



- 有効数字と有効桁の違い。
- 分離の信頼度はどちらに。
- 詳細設計終了時点の一例。

この図で指摘しておかなければならないのは、まず信頼度数値の有効桁です。小数点以下９（または０）が続いたあとの一桁だけが意味を持つということです。実際に、９が続いた後の二桁目を四捨五入して書き直したのが右図ですが、システムの信頼度は変わらないことが判ります。

エクセルなどでは桁数を同じにしたほうが簡単なのでそうしても構いませんが、報告書では意味のない数値を羅列すると、「この人は判っていない」と思われます。

前の宇宙開発委員長であった井口さんが思い出話をホーム頁「宙の会」に書かれていますが、まさにこの点の皮肉も書かれていらっしゃいます。

この図では分離の信頼度がどちらに入っているのか良く見えないということがあります。第１段に分離の装置が付いているのなら、分離の信頼度は第１段に入れるべきでしょう。

４．信頼度計算の問題点

現在の信頼度計算はかなり問題を含んでいると言わざるを得ません。

システムの信頼度は結局末端の部品の信頼度から合成されるわけですが、部品の信頼度の決め方が問題です。

前述のミルハンドブック２１７では部品の故障率から各種のファクタを乗じて求めることを指導しています。部品点数法と部品ストレス解析法とありますが、要するに出来る限りの知識で故障率を推定しなさいということです。

環境ファクタ、品質ファクタ、ストレスファクタなどを考慮しなさいということですが、これらのファクタの決め方が判りませんので、「いい加減」になってしまうことが避けられないでしょう。

故障率と寿命とは関連がないのですが、ミッション寿命が決められた衛星の信頼度を故障率で出しているという論理的矛盾もあります。

ミルハンドブック２１７は長年使われてＦ改定までなされたのですが、米国はすでにこの文書を放棄しています。性格的に料理のレシペみたいな文書でしかないことが判ったのでしょうか。

その後、無くては困るということだったのかＰＲＩＳＭという文書が作られていますが、２１７とそれほど違いはありません。

現在は両者をあわせたような２１７プラスという文書があるようです。

新しく開発したような高信頼度の部品の信頼度をどのように決めるかが問題です。部品レベルなら十分の数を試してみることが出来るかもしれません。それでも、１０００個の試験結果ら０．９９９９９９の信頼度があるというのは無理でしょう。

0．９９９９９９の信頼度が欲しければ少なくとも１００万個の部品を試験が必要かもしれません。そして、一度も失敗がないか、失敗があればその原因を突き止め、対策を採らなければならないでしょう。

現在の頻度概念の確率理論では、試験結果から信頼度を求めるには、信頼水準をおいて推定することになります。しかし、信頼水準を何％にすれば良いのか指針がありません。

通常の設計では漠然とした情報から、高信頼度が必要な部分は冗長系を組んだりしますが、これも良く考えると冗長系を組んでもそれほど大きさや質量が増えないという要素があって出来ることです。

最初に信頼度配分をして、大体の構成を決めて生きますが、経験的に決めているということに過ぎません。人為的であり、作為的でありますが設計とはそういうものです。

4）信頼度計算の現状・・・問題点

システム → エレメント → コンポーネント → 部品まで

部品の信頼度はどのように決められるか。 → 問題が多い。
MIL-HDBK-217F（電子機器の信頼度予測）の方式。 → 米国は破棄。
組立の信頼度はどのように組み込むか。 → １とする？
高信頼度を部品の試験結果から決められるか。 → 無理。

信頼度配分は可能か

12

5）MIL-HDBK-217Fの概要

部品故障率：λ_{PART} 故障数／10^6 時間

$$\lambda_{PART} = \lambda_b \times \pi_E \times \pi_Q \times \pi_S$$

環境ファクタ：π_E
品質ファクタ：π_Q
ストレス・ファクタ：π_S

基礎故障率：λ_b
(例) MOS FET λ_b=0.060

その他のファクタ：π_T π_A、π_M、π_R、π_L、π_P
部品点数法
部品ストレス解析法

13

（閑話）

ここで、理論の正しさとはどういうことか、数学、科学、工学で違いを見てみましょう。

数学では論理的に正しいことが理論の正しさです。

ただし、ゲーデルは不確定定理で矛盾のないことを証明できないことを証明しています。

科学では実世界が正しいのであって、実世界を説明する理論はどこまで実世界を説明できるかの程度問題です。ニュートン理論よりもアインシュタインの相対性理論の方が広く説明が付くというものです。しかし、量子理論とは相容れないものです。宇宙誕生の瞬間を考えると両方の理論が相容れないと困るので考え出されたのが超ひも理論であり、その最先端がＭ理論ということになっています。

工学では役に立てば良いのであって理論的である必要は必ずしもないのですが、大きな予算が必要なときは説得力が必要です。数学、科学の成果を使って合理的に説明が出来るほうが望ましいのです。

（閑話休題）

5．西澤潤一教授のＬＳＩ予想

最後に現行の信頼性工学がむしろ誤導した例として私が西澤潤一教授のＬＳＩ予想と名付けた例をご紹介いたします。

西澤教授は大きな研究を幾つもされています。集積回路も研究されていたのですが、大規模集積回路（ＬＳＩ）は歩留まりが悪くてものにならないだろうと予測されて力を入れなかったということを話されています。

その後のＬＳＩの発達は素晴らしいものがあります。パソコンのＣＰＵでインテルのペンチアム３で６００万個のトランジスタが１個のチップに作られています。ペンチアム４は一挙に５５００万個のトランジスタです。現在主流のデュアル・コアはこの倍です。そしてクアッド・コアだとさらに２倍で２億個を超えているのでしょう。

何故、集積回路についても専門家であった西澤教授の予測が完全に外れたのでしょうか。

世界で最初電子コンピュータＥＮＩＡＣは１８００本の真空管が使われていました。

このコンピュータを動かすためには全部の真空管が作動しなければなりませんが、１８００本もあるとどこかの真空管が切れてしばしば真空管を取り替えなければならなかったのです。その間、コンピュータは作動停止です。

システムが部品の直列系で表されるとき、システムの信頼度は部品の信頼度の積になるというのが信頼性工学の一番の基礎ですから、大規模集積回路では全部を正しく作るのは非常に難しいことになると考えられたからです。

確かに、現在の集積回路の製作工程は超クリーンルームで製作されます。

また、集積回路のような固体回路では、真空管と違ってヒータのような部分がありませんから、一度正常に動くものは何時までも動きます。

それでも、外れた予測をされた一番の理由は信頼性工学が教える直列系の式にあったわけです。

（開話）・・・理論式の正しさ

数学　論理的に正しいか否かを評価
→　ゲーデルの不完全性定理

科学　どこまで自然を説明できるかを評価
→　ニュートン力学とマクスウエルの電磁気理論
→　アインシュタインの相対性理論と量子力学
→　超ひも理論、M理論　（？）

工学　如何に役立つかで評価
→　数学、科学を利用
・可能性が示されない物は開発に移行できない

（開話休題）

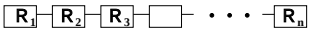
14

6）西澤潤一博士とLSI予想

ENIACは1800本の真空管が使われていて寿命が短かった（事実）

集積度を高くすると歩留まりが悪くてものにならない　（予想）

$R = R_1 \cdot R_2 \cdots R_n$



現実は、超ＬＳＩが実用化
Pentium IIIは600万個のトランジスタを集積
Pentium 4 は5500万個のトランジスタを集積

信頼度理論が間違い？

15

西澤先生は信頼性シンポジウムでこのお話をされたときに、実際は「信頼性工学と違うよ」と話されて終わっています。

皆さんはこの大きな違いがどこから来たものかお分かりでしょうか。

実は、信頼度の計算式でシステムの信頼度が個々のサブシステムの信頼度の積になるというのには、条件があるのです。

それは個々のサブシステムが論理的に独立である場合に成り立つということなのです。

集積回路の場合は、全部のトランジスタを一挙に製作します。このような製作過程で作られたシリコン基板上の個々のトランジスタが相互に論理的に独立とは言えないのです。むしろ、ソフトウエアのコピーに近く相互依存性が高いわけです。

従って、信頼度の積であるというのは非常に悲観的な数値になってしまうので実態とはかけ離れてしまうのです。

それでは独立でない場合はどうすれば良いのかというと、現在の信頼性工学では、まったく議論がなされていません。

7）現行の信頼性工学の問題点

（現行） **要素の信頼度　→システムの信頼度**
要素の信頼度は？
MIL-HDBK-217Fは信ずるに足るか？
故障率データベースの有効性？
頻度概念確率の定義では論理的に無理？

（改善策） **ラプラス流の確率の定義に戻す**
論理の一貫性が保てる
システムの信頼度は情報に基づき割り当てる

16

おわりに

信頼度評価が必要なことは最初に述べました。

そして現在の信頼性工学がその役割を果たしていないのではないかと疑問を呈しました。

私は、まず確率の概念を頻度概念から確信の度合いに変えるべきであると主張しています。

確率は確かさの度合いであるということが周知徹底すれば、信頼度も情報に基づき割り当てるものであることが理解され、常に実感とあう信頼度表現ができると思うのです。

（平成 20 年 5 月 25 日）