

科学技術と安全

安全という概念は極めて多岐多様にわたるため、一般的に述べることは殆ど不可能であると思われる。しかし、いくつかの大前提が存在することも事実であろう。たとえば、ある年代の日本人にとってはよく理解していることと思われるが、「色は匂えど散りぬるを我が世誰ぞ常ならむ……」が科学技術システム設計の大前提の一つであろう。端的に言えば、故障に至るまでの時間の問題はあるにせよ、故障は避けられない、ということである。



さらに、問題を複雑にしていることに、人間が犯す誤りがある。このように考えると、故障や誤りの発生を前提としないシステムが成り立つわけがないことがわかる。一方、多くの日本人は“risk taking”と言う概念を持っていないのではないかと疑われる。まさかの時は神風が吹くと期待して、危機感を持たないことにしているように思われてならない。これは明らかに不合理な態度である。

故障のないシステムを構成することは出来ないとしても、二値論理で構成されるシステムが危険側には決して壊れない、さらに入力いわゆる間違いが危険側には決して発生しないと仮定するいわゆる Fail-Safe 論理システムの構成については、“Basic Properties and a Construction Method for Fail-Safe Logical systems” by H. Mine U Y. Koga, IEEE Trans. Elec. Comp., E-16, 1967, pp. 1568-1575. に構成の困難さが詳しく報告されているとおり、一般的に構成できるとは言い難い。

このように考えると、システム的设计においては、考え得るあらゆる形の故障の生起を仮定せずに行ってはならないと考えられる。物事の存在は証明できても存在しないことの証明は不可能であるので、故障が起こらないことを仮定してはならない。「これで大丈夫。」と思った時が危機の始まりである。

評議員 長谷川 利治

(南山大学数理情報研究センター長 数理情報学部教授)