ためになる「安全学」

向殿政男
明治大学 理工学部 情報科学科 教授

第５回 信頼性と安全性の関係

信頼性を上げれば安全性は上がる、というのはほとんどの場合そのとおりである。したがって、安全性の向上は信頼性を上げることで対応すれば事足れりと考えている人がいるが、実はこの考えは間違いである。信頼性と安全性はお互いに深い関係にあるが、本質的には異なった概念である。たとえば、新幹線で安全が確認できないために列車が止まっているとしよう。この時点でだけ考えると、新幹線に乗って移動するという本来の機能からすれば信頼性はゼロであるが、衝突・脱線でケガをするという危害を受ける可能性がなく、安全性は100%である。危ないときには止める、危険が予想されるときには実行しないというように、信頼性を下げてでも安全性を高めることがあり得ることを考えると、両者が異なった概念であることがわかる。いや、信頼性と言ったときには、本来の要求された機能を果たしながら安全性が保たれていることに関する信頼性を問うているのだ、と答える人がいるかもしれないが、このことが安全性と信頼性が異なった概念であることを如実に表している。なんだか話がこんがらがってきたので、もう少し根本から考えてみることにしよう。

信頼性とは、そもそも要求する機能をどれだけ果たせるかを問うているのであって、機能を失った後の状態は問題にしていない。一方、安全性は、故障等で機能を失った後の状態も問題にしているのである。すなわち、信頼性は、正しく機能している（イエス：1）か、していない（ノー：0）かの比率を問題にしていて、1である確率を高くすることを目指している。また、一般的には正しく機能していれば安全性も確保されている場合が多いので、信頼性が高ければ安全性も高くなる。これが、信頼性を高めれば安全性が上がるとしばしば考えられる所以である。しかし、問題は故障等の不具合の発生時、正しい機能を失ったときである。故障したときには、危険になることも安全になることもある。安全性は、故障等の不具合が発生したときにも安全であることを目指している。信頼性と安全性、どこが違うのかと問われれば、目的が違う、すなわち、本来の機能を目指すのか安全を目指すのかの違いである、と答えることができる。前述のように、本来の機能と安全であるという機能の両方を含んだ機能を考えてその信頼性を問うという発想もあり得るが、基本的に本来の機能と安全の機能とは別の概念で、分けて考えるべきである。

信頼性と安全性とは異なった概念であるから、両者はその手法も異なっている。信頼性を上げるには、故障しないような高信頼の部品をつくる（フォールトアボイダンス）とか、たとえ故障しても他の部品で補って機能を正しく保つ（多重系、冗長系、フォールトトレランス）とか、チェックや監視等（時間冗長とか情報冗長）の技術に重点が置かれる。一方、安全性を上げるためには、たとえ部品が故障しようとも、常に安全側になるように設計の段階で構造的につくる（フェールセーフ）のが本質である。

Profile

向殿政男 ―*Mukaidono Masao*―

1942 年生まれ。1965 年明治大学工学部電気工学科卒業、1970 年明治大学大学院工学研究科博士課程修了、工学博士。1970 年明治大学工学部電気工学科専任講師、同電子通信工学科教授を経て、現在、同理工学部情報科学科教授。私立大学情報教育協会会長や明治大学校友会会長なども務める。専門は、情報科学（特に、ファジィ理論、人工知能）、安全学、多値論理。著書に『国際化時代の機械システム安全技術』（日刊工業新聞社）、『よくわかるリスクアセスメント－事故未然防止の技術－』（中災防新書・中央労働災害防止協会）、『安全設計の基本概念』、『制御システムの安全』（ともに日本規格協会）など。

このためには、安全側がどのような状態であるかがわかっていなければならない。上の例でいえば、列車は止まっていれば安全であり、飛行機は飛ばなければ安全である。一方、信号でいえば、赤信号が安全側であり、青信号は危険側である。これはおかしいと思われるかもしれない。青信号は安全を、赤信号は危険を意味すると教わっている身からすると、一見、矛盾しているように思えるかもしれない。なぜ、青信号が危険側かというと、青信号が出ていると列車は出発するし、自動車は止まらないで走り続ける。リスクの高い本来の任務を実行するから、青信号は実はリスクの高い状態に対応していて危険側なのである。一方、赤信号ならば止まるので事故は起こり得ないから、安全側なのである。このことは、信号が故障で間違えた場合を考えれば明らかになる。青信号が故障で赤信号になった場合には、不便ではあるが事故にはつながらない。これは安全側の故障であり、赤信号は安全側になる。逆に、赤信号であるべきときに青信号に故障すると、ことは重大である。大事故につながる可能性がある。この故障は危険側故障であり、青信号が危険側であることがわかる。

故障の発生は認めるが、それが常に安全側故障になるように構造的につくるのが、安全性設計の基本である。たとえば、止まっていることが安全側ならば、故障したら止めてしまうというのが安全の技術的な対応であり、安全が確認されるまで動かさないようにするのが、安全の組織的対応である。

～信頼性と安全性～

- **信頼性**
  （与えられた条件下で、与えられた期間、）要求機能を遂行できる能力
- **安全性**
  リスク（人への危害または資材の損傷の危険性）が、許容可能な水準に抑えられている状態

ところで、飛んでしまった飛行機に、安全側はあるのであろうか。もちろん、飛行中にエンジンが止まれば、あとは落ちるだけであり（危険側故障）、この場合には、いかに飛行を継続させるかが課題となる。すなわち、安全側が存在しない場合には、正しい機能をいかに継続させるかという信頼性の話になる。この場合、信頼性で安全性を確保していることになる。このように、信頼性と安全性とは、お互いに深い関係にあり、両者は不可分の関係にある。それでは、どちらを優先すべきであろうか。安全側が存在する場合には、安全性を確保してからその信頼性を高めるという、その順番を間違えてはいけない。ただし、止まってばかりの新幹線は利用されなくなり、誤報の多い火災報知機はスイッチを切られる運命にあるように、信頼性に裏打ちされていない安全性は、実効性に問題が生ずることを忘れてはならない。