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９回 フェールセーフ技術 ～ハイボールの原理に学ぶ～

“技術で安全を守る”、これが安全確保の第一ステップです。人間が注意して危険を回避しようとする前に、機械設備側で技術的に安全を確保するべきです。これは、安全学が主張する大事なポイントの１つです。しかし一方で、機械設備は故障することはあるし、劣化するし、放っておくといつかは壊れるものです。いえ、今すぐ故障してしまうおそれさえあるのです。したがって、なるべく壊れにくい信頼度の高い部品類を使うとか、壊れないように頑丈な構造にするというアプローチや、保守点検をして前もって怪しげな部品を取り替えてしまうというアプローチ等が採られています。さらに、コンピュータで監視して、怪しいときには切り替えたり、訂正したり、警報を発したりするというようなアプローチもあります。ただしこの場合、安全装置の役割を果たしているコンピュータも故障するし、ソフトウエアにはバグが付きものであることを忘れてはいけません。だからこそ重要になるのは、壊れるのは仕方がないこととして故障の発生を認めたうえで、壊れても安全が確保されるようにしておく、というアプローチです。

安全の世界で、壊れても大丈夫というアプローチは、壊れたときには安全側になるようにする、という考え方です。その最も典型的な技術がフェールセーフ、すなわち、壊れて(フェールして)も、安全(セーフ)であるようにする技術です。そんなことが可能か、といわれるかもしれませんが、物理現象をうまく利用することで実現できる場合が多々あります。この典型的な例を鉄道の信号機に見てみましょう。

図表―1は、ボール信号と呼ばれる昔の列車用の信号機です。ボールが高い位置(ハイボール)にあるときは、現代の緑信号を表していて列車の進行を許可し、ボールが地上にある(ローボール)ときには、赤信号として列車の進行をストップさせるものです。ボール信号機の故障とは、ロープなどが切れたりすることに相当するでしょう。このときには、ハイボール(緑信号)であっても、ボールは重力で落下してローボール(赤信号)になり、列車は進行することができません。故障すると列車は止まるという安全側(赤信号)になって、迷惑を被ることはあっても、人命にかかわるような大事故につながる心配はありません。逆に、ハイボールを赤信号(停止信号)に対応させると、故障すると停止信号が伝わらず、大惨事につながる可能性があります。許可信号(緑の信号)に対してハイボールを対応させることによって、フェールセーフ(故障すると必ず安全側に固定される)が実現されます。なぜならば、故障したからといって、ローボールが重力に逆らってハイボールになることはないからです。重力がある限り、この原理は裏切られません。この背景には、“許可を表す緑信号には、エネルギーの高い物理的状態を対応させなければならない”という深遠なる安全の原理があります。これを私は、“ハイボールの原理”と呼んでいます。

最近、ウイスキーの炭酸割りであるハイボール

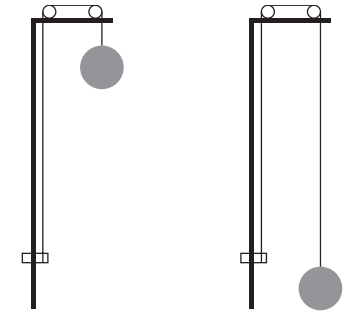
Profile

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。

が人気ですが、お酒のハイボールと前述の信号のハイボールとが、次のような逸話として結びついています。昔、英国で、駅近くの酒場のカウンターで列車待ちをしながら、ちびりちびりとウイスキーを飲んでいた英国紳士が、ハイボールを見て、急いで(ウイスキーは強いのでそのままいっきに飲むと体によくないから)ウイスキーを炭酸で割って薄くして、そしていっきに飲んでホームに向かった、という言い伝えからです。お酒のハイボールの語源には諸説があるようですが、このように安全の原理と結びついていると考えるとわかりやすいし、安全関係の人間にとってうれしい話ではありませんか。

列車の信号機は、本来、一種の安全装置です。安全装置にフェールセーフの技術を採用したのが先のボール信号ですが、これはもう、本質的安全の技術の典型です。鉄道では、これ以外にも、たとえば踏切のしゃ断機は、故障すると列車が来なくても下りてしまう構造になっているなど、古くからフェールセーフが列車を動かす場合の大前提になっていました。鉄道以外にも、たとえば、原子力発電では、最後の最後は重力で制御棒が炉心に落下して核分裂が止まるようなフェールセーフ構造が組み込まれたりしています。フェールセーフは、大惨事につながる可能性のあるシステムでは、技術で安全を確保するときの大前提として考えるべきものになっています。これは、“止める技術”というよりは、”止まる技術”というべきでしょう。



図表―1　ボール信号機

私たちの日常生活でも、失敗しても大丈夫という構造を前もって組み込んでおけば、安心して物事に集中し、努力することができると思います。そういえば、人間は間違えるものですので、人間が間違えても大丈夫なようにするフールプルーフという技術、すなわち、フール(馬鹿な間違えをしても)プルーフ(防止する)技術の方が日常生活には関係が深いかもしれません。フェールセーフ技術やフールプルーフ技術は、技術で安全を守るために最初に考えるべき基本的な技術です。そして、信号機やしゃ断機などのフェールセーフ技術に見るように、安全を技術的に確保するには、構造と原理があります。たしかに新しさは感じられないかもしれませんが、安全技術の専門家は、まず、この勉強から始めるべきしょう。安全装置やコンピュータを用いて“止める技術”の前に、本質的安全設計である“止まる技術”をあらゆる安全の分野で、もっと真剣に検討すべきであると考えます。