



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8回

本質的安全設計 ～安全設計のスタートはここから～

“元から絶たねばダメ”とは、臭いに限ったことではありません。あらゆることに対して真であり、これは、安全に関しても同じです。安全とは、許容可能なリスクしか残っていない状態であり、それが維持されていることでした。では、機械や設備等の安全はいつの段階で実現させるべきでしょうか。もちろん、答えは“元から”すべきであり、この場合の“元から”は、明らかに製造・設置に入る前の設計段階からです。設計の段階から危険性がないように、すなわち、初めから危険なところ（危険源）が存在しないように、またはリスクが少ないようにしておくのが理想的です。これが本質安全設計、または本質的安全設計の考え方です（両者の違いについては後で解説しますが、この2つの用語は安全が本質的に実現されているという意味です）。

とがっているところがあったり、バリ（材料を切ったり削ったりした際に材料の端にできる出っ張り）が残っていたりしたら、初めからとがった先を丸くしたり、バリを取ったりしておくことです。体が挟まれる可能性があるのならば、初めから体が入らないように狭くしておくことです。高いところから落ちそうならば、初めから低くしておくことです。材料に毒性があるのならば、毒性のないものに変える、爆発する可能性があるのならば、爆発しないものを使用する、燃える危険性がある場合には不燃材料を使う、電気の火花が危険源になるならば、電気を使用しないようにする

等のことです。平面交差をやめて立体交差にするようなことです。また、巻き込まれる可能性がある場合には、巻き込まれても人力で脱出ができるくらいの小さなエネルギーにすることも本質安全設計です。このように、もともと危険が存在しないもしくは小さくなるように設計の段階から考えておけば、機械・製品・設備等が故障しても、また人間が間違えても、大きなケガをするようなことはありません。

しかし、機能として、とがったところがどうしても必要であったり、エネルギーを小さくしては用をなさないという場合があります。このようなときには、とがったところやエネルギーの大きな個所に、人間が到達できない構造にすることが考えられます。たとえばシュレッターでは、指が入らないように入り口を狭くしたり、紙を切り刻む刃の部分には手が届かないように奥深くしておく、等の構造にすることです。しかし、この場合には、危険源がなくなったわけではありません。普段は人間が危険源に近づけない構造にするだけで、修理や保守等では人間が近づく可能性があります。そこで、さらなる対策となる全自動化も、この範疇に含まれます。これは構造を工夫するのに加えて、故障の確率を小さくして人間が修理などで危険源に近づかなくて済むようにして危害の発生確率を低くする信頼性も関係してきます。

なお、リスクとは、危害の発生確率と危害のひどさの組み合わせでした。したがって、リスクを小



Profile

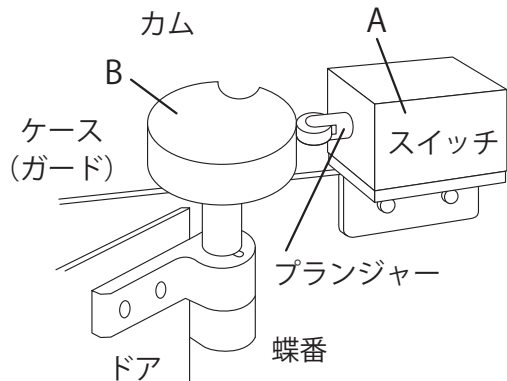
向殿政男 — Mukaidono Masao —

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。

さくするもう1つの方法に、危害の程度を小さくすることが考えられます。すなわち、危険源をなくすることはできないが、事故が起きたときに危害の程度を小さくするように、エネルギーを小さくしたり、毒性を弱めたりする方法があります。これらの方法も、本質安全設計に近い設計方法です。

筆者は、危険源が初めから存在しないように設計することを「本質安全設計」と呼び、危険源は存在するが、そのリスクを下げるために人間が近づけない構造にして、かつ修理等で人間が近づく機会を少なくするよう信頼性を上げる方法と、エネルギー等を小さくして危害の程度を小さくする方法を含めて「本質的安全設計」と呼んでいます（本質的安全設計には、本質安全設計を含みます）。本質的安全設計でどうしてもリスクを小さくできないときに、次のステップとして安全装置を設置します。しかし、安全装置も故障をします。安全装置が故障をしても危険側にならないような構造に設計するのも安全装置への本質的安全設計の適用と考えられます（フェールセーフ—壊れるときは安全側になる—等が、その典型例です）。

ここでは、この例の1つとして、構成品間のポジティブな機械的作用の原理について紹介します。ポジティブモードの結合とは、機械的構成部品が直接、または剛体要素を介して他の機械的構成部品に直接連動することです。図表—1はその例で、ドアを開くと危険なロボットや機械などの



図表—1 ポジティブモードの結合

電源が切れる安全装置の構造です。ドアが閉じているとき（ガードに平行時）には、カムBのへこんだところにスイッチのプランジャーが入り、接点がばね等で閉じて電源は入っています。ドアが開けられると、カムが回転してプランジャーが押されてスイッチの接点が強制的に切られます（強制分離というタイプのスイッチ）。接点が癒着をしているとドアは開きません。ドアが開いたということは接点が開いて電源が切れていることを保証しています。ドアもカムもプランジャーも剛体で、正の（ポジティブな）力がこれらをとおして、直接、接点に伝わる構造になっています。

上記のように機械・施設・設備等のハードウェア側の安全化にも階層と奥深さがあり、そのスタートは本質的安全設計からです。