フールプルーフとフェイルセイフ

できることなら事故は起こしたくない．いったん事故が起こると，工場であればラインを止め，鉄道事故であれば全路線を停止させて事故の復旧にあたらねばならなくなる．損失額は膨大なものになる．

事故には，機器側の原因を理由に事故が起こる場合と，ユーザー(人間)側の原因を理由に事故が起こる場合とがある．機器側を原因とした事故の場合，装置の工夫・改良によって事故を防止することができる．ユーザー側を原因とする事故の場合，その多くはヒューマンエラーである．エラーは気の緩みや怠惰によって起こるのだから，人間自身がエラーを起こさないよう努力すべきだという考え方がある．一方，慣れや疲労による注意の低下，知識・経験の不足がエラーを誘発することは人間工学的によく知られている．エラーを防ぐための圧力が，作業員に極度の緊張や疲労を与え，作業環境を悪化させてしまう可能性もある．過去の大事故を詳細に分析すると，ヒューマンエラーが原因となっているケースが多いのも事実であり，「人間は間違える」ことを前提としながら，事故を防ぐための積極的なエラー防止対策が必要となる．

●フールプルーフ―エラーの未然防止　エラー防止対策には主に 2 つの考え方がある．1 つはエラー発生以前に，エラーそのものが起きないよう対策をたてることで，エラーの未然防止である．さらに，エラーを未然に防止する 1 つの考え方にフールプルーフがある．間違った操作ができないようにあらかじめ設計しておくことである．

例えば自動車のオートマチック車の場合，ブレーキを踏まないとシフトレバーをパーキング(P)の位置から動かすことができないようになっている．ブレーキを踏んだままであれば，シフトレバーを後退(R)やドライブ(D)に動かしても，突然車が動き出すことがないので安全である．日常生活の中には，ほかにもフールプルーフの設計思想に基づいたものが多くある．正しい向きにしか入らない電池ボックス，ドアを閉めないと動かない電子レンジ，一方向からしか差し込めないフロッピーディスク，ふたを開けると自動的に止まる脱水機などは，いずれも間違った操作ができないようになっており，広い意味でフールプルーフの設計思想に基づいている．

●フェイルセイフ―エラー対処　もう 1 つはエラーが起こっても，エラーによる被害の拡大を防いだり，エラー前の状態に回復できるようにするエラー対処である．代表的な考え方の 1 つにフェイルセイフがある．これは，故障や事故などの異常時に，安全側に作動する仕組みのことである．

フェイルセイフの代表例としてよく紹介されるのが原子力発電所である．原子

力発電所では，何らかのトラブルにより発電所が停電しても，制御棒の働きによって，炉心が安全に停止するよう設計されている．また踏み切りの遮断機は，遮断棹が上がっている状態に力を多く必要とするように設計されている．そのため，停電などにより遮断機が作動しなくなっても，自重によって遮断棹は降りたままとなり，踏切内への進入を防止することができる．列車の自動停止装置（ATS），石油ストーブ転倒時の自動消化装置などもフェイルセイフの例である．パソコン使用中に停電が発生すると，それまでのデータがすべて消去されてしまう．手術中の停電は人命にかかわる．こうしたトラブルを防ぐために利用されるのが無停電電源装置である．無停電電源装置は，あるシステムが故障したときにそれを補助するバックアップシステムの役割を果たしている．この場合のバックアップシステムに該当するものも，フェイルセイフに含めることがある．

●それでも人は過ちを犯す　フールプルーフやフェイルセイフは，人間がエラーを犯さない対策をハード側に埋め込む設計思想である．正しく機能しているうちは，安全なシステムといえる．しかしいくら安全なシステムでも，ユーザー側が間違った使い方をすると，新たな暴走が生まれる危険性がある．例えば車がさまざまなフールプルーフを搭載し，安全性が増してゆくと，ユーザーはその安全性を過信し，多少運転が荒くなる可能性がある．また，自動消火装置のついたストーブを足で蹴飛ばして消化するといった誤用は，本来の機能を無視した人間ならではの逸脱行為といえる．

安全を重視した設計は，使いやすさとトレードオフの関係になることから，その設計をユーザーが無視するケースもある．カーナビゲーションシステムは運転中の注視が法律上制限されている．そのため，多くのメーカーは，車が動き出すとナビ画面を別の画面に切り替える工夫をしている．これは安全運転にとってはフールプルーフだが，ユーザーにとっては，走行中に位置確認ができないという不便さがある．そこで走行中でもナビ画面をみられるように設定を変更してしまうというケースも出ている．

「人間は間違える」ことを前提に，フールプルーフやフェイルセイフなどのエラー防止対策が開発され，一定の成果をもたらしている．しかし時として人間は，安全システムに目を背けた非合理的な行動を取ることがある．フールプルーフ・フェイルセイフなどのシステムを工夫しても，人間の非合理的な行動を食い止めないと，事故を100％未然に防ぐことは不可能であろう。今後は，人間が非合理的な行動を選択することを大前提として，事故防止のための安全設計システムを開発してゆく必要がある。　［宮本聡介］

参考文献

[1] 芳賀 繁『失敗のメカニズム―忘れ物から巨大事故まで』角川書店，2003
[2] 海保博之・宮本聡介『ワールドマップ安全安心の心理学』新曜社，2007