フェールセーフとフォールトレランス
（フェイルセーフとフォールトトレランス）

明治大学　向殿政男

安全装置の設計に用いられている重要な考え方であるフェールセーフとフォールトトレランスについて紹介をしておきます。安全装置も故障することがあります。安全装置がなるべく故障しないように信頼度高く作るという信頼性の考え方と、壊れた時に安全側になるように構成しようとする安全性の考え方があり、両方とも安全の実現には大事な考え方です。

機械は故障するものであるという大前提に立って，安全を確保する考え方の代表が，フェールセーフとフォールトトレランスです．フェールセーフ（Fail Safe）とは，失敗しても安全であるということを，フォールトトレランス（Fault Tolerance）とは，欠陥があってもそれを許容するということを意味しています．機械が故障しても、とにかく安全だけは確保しようとするのがフェールセーフで，出来るだけ機械の正しい機能を維持することで安全を確保しようとするのが，フォールトトレランスです．フェールセーフが直接，安全性を目標にしているのに対して，フォールトトレランスは，信頼性の向上を目標にしています．

安全性と信頼性，お互いの深い関係にありますが，実は異なった概念です．安全性は，人間に危害が加わらないようにしようとすることに対して，信頼性は，機械の正しい機能を維持しようとすることを目標にしています．一般に，信頼性が上がれば安全性も上がると考えられますが，信頼性を下げることで安全性を高めることがありますので，根本的に異なった概念なのです．例えば，新幹線で，安全が確認されないので，列車を止めてしまえば，人を運ぶという本来の機能は失われて信頼性は下がりますが，脱線などをして人が傷つくことはないということを考えれば，安全性は確保されているのです．少しぐらい安全が確認されていなくても，ほとんどの場合には問題がないので，走り続ければ，信頼性は高まり，効率は上がるかもしれませんが，いったん事故が発生すると，どんなことになるか保証はありません．

機械は部品から構成されていますが，機械の部品が故障した場合，常に機械は安全側になるように構成することが，フェールセーフの第一歩です．一般に，部品の故障には，機械の状態を危険側に導くもの(危険側故障)と，安全側に導くもの(安全側故障)とがあります．フェールセーフでの部品の故障に関する要請は，故障の発生は認めるが，安全側に導く故障しか認めないようにするというものです．これは非対称故障とも呼ばれます．こんなことが可能かというと，実はかなりの場合に，物理現象などを利用して，工夫を凝らすことで可能になります．例えば，故障が発生すれば必ず踏み切りは閉じられるという重力を利用した踏み切りの例などは昔から有名です．ここで重要なことは，安全側の存在です．例えば,止まれば安全（停止安全），人間がそばに居なければ安全（隔離安全）などが考えられます．停止安全では，ロボットは動かなければ安全，新幹線は走らなければ安全，飛行機

は飛ばなければ安全，等々ですが，安全であっても本来の機能を果たしていない状態です．機械が故障したら，このような安全側の状態にしてしまうというのが，フェールセーフの考え方です．

もし，飛んでいる飛行機に故障が生じた場合の安全側はあるのでしょうか？残念ながら，現在までのところ，それは見出されて居ません．このような場合には，とにかく故障しないようにするか，又は，本来の機能を維持するようにするしか道はありません．部品が故障しないようにするには，高信頼の部品を使って，はじめから不具合が生じないようにするのが正道でしょう．しかし，部品はいつかは故障します．そこで，一つや二つの部品やサブシステムが故障しても，他の部品やサブシステムがこれに取って代わって本来の機能を維持する，という多重系の考え方が生まれてきます．Ａが壊れたらＢでカバーする，もしＢが壊れたらＣでカバーするという考え方です．これがフォールトトレランスの考え方です．多重系，すなわち冗長系によって信頼度を上げ，結果的に安全性を維持しようとするものです．

このように，フェールセーフとフォールトトレランスとは，根本的に異なった概念です．時々，新聞報道などでは，多重系に基づく安全装置（厳密には多重に基づく高信頼性装置と呼ぶべきでしょう）を誤ってフェールセーフと呼ぶことがありますが，これはフォールトトレランスであって，フェールセーフというのは間違いであると思います．

機械を構成する部品が故障しても，機械の状況が安全側になるように機構として組み込んであるフェールセーフの場合と，機能を出来る限り維持することで安全を確保しようとする信頼性の場合とは，それぞれ，確定論と確率論に基づく安全性の立場と言えますが，前者のほうが格段に安全性が高いことを理解する必要があります．もちろん，非対称故障やフェールセーフの原理に基づく装置が絶対ということはなくて，それがどのくらいの確からしさで働くかという信頼性の概念がそこに入り込んでくる可能性がありますが，最初から機構として安全が組み込まれているということが重要なのです．一方，フォールトトレランスの場合には，冗長系という機構を導入しているので，各サブシステムの独立性が保障されて居れば，高い信頼度を得ることが出来ます．人命を預かるような分野では，まずフェールセーフの立場でシステムを考えるべきではないでしょうか．あくまでも安全側が見出せない場合や，またはフェールセーフが実現できない場合，更にはフェールセーフがコスト的に実現困難な場合に，初めてフォールトトレラントによる方法を検討する必要があるのではないでしょうか．

フェールセーフという考え方は，安全が確認されない限り，危険の可能性がある本来の（便利で効率的な）機能を実行させない，逆に，本来の機能を実行中でも，安全が確認されなくなったら，その機能を止めて安全を確保する，という考え方に繋がります．この発想は，リスクアセスメントと共に,今後の安全の思想の重要な指針になるのではないかと考えています．

なお、人間側がエラーをしても、安全が保たれるような構造に作る考え方にフールプル

ーフがありますが、ここでは深くは入り込まないようにします。
（向殿，北野他著、安全学入門～安全の確立から安心へ～、研成社、2009－8、pp.69-75より）