フェイルセーフ　fail-safe

[簡単に]

機械や装置が故障しても、安全状態になるように働く仕組み

[詳しく]

フェイルセーフとは、機械が停電で止まったり、故障をしても、安全状態になるように向かう仕組みをいいます。停電などにより（核分裂を妨げる）制御棒を動かす機械が作動しなくなっても、制御棒を捉まえている電磁石の電気が切れ、制御棒自身の重さによって原子炉内に落下して挿入され、核分裂を止める仕組みなどがあります。

[角度を変えて]

フェイルセーフの考えは原子力分野に限定したものではなく、鉄道技術、ロボット技術、情報処理などの分野にもあります。例えば、鉄道の踏切では、停電などにより遮断機が動かなくなった場合、遮断棒自身の重さによって降りたままとなり，人や車が踏切内へ入ることを防ぐ仕組みがあります。

＜フェイルセーフの他分野の事例＞

○鉄道信号保安用語（JIS E3013 2001）1015

装置が故障した場合でも安全側状態になり，危険側に動作しないこと。鉄道信号の装置故障時には，制限（列車を停止又は速度低下）側を現示する。

○サービスロボット用語（JIS B 0187）

ロボット及びロボットシステムの要素が故障を生じても、あらかじめ定められた安全側の状態に保持される機能又は性質

○情報処理用語（（セキュリティ））JIS X 0008 2001 ISO 2382-8

故障が生じたときにセキュリティ破壊の招来を避けることに関する用語

○レーザー製品安全基準（JIS C6801）

部品の故障が人体障害を起こさないような設計上の配慮。故障形態では、この配慮によってシステムが動作不能となる。

[誤解に注意]

エラーが起きた後の被害の拡大や状態回復の一つとして、フェイルセーフ（機械の故障による問題の拡大を防ぐための仕組み）という考え方がある。それに対し、エラーが起きる前に起きないよう対策をたてる考えの一つとしてフールプルーフ（例えば、人間の誤操作による問題を防ぐための仕組としてインターロック）がある。

平成 23 年度に実施したウェブアンケート調査では、フェイルセーフの意味がわかるとした人は 25%程度であった。カタカナで理解が困難な用語の一つと考えられるので、「安全動作」というように言い換えて説明することも場合によっては有効である。

[関連語]

非常用炉心冷却装置（ECCS）　→　親見出し参照(p85)

フールプルーフ　→　エラーを未然に防止する考え方の一つ

インターロック　→　フールプルーフを実現するための一つの仕組み。人間の誤操作による問題を防ぐ

【参考文献】

1)宮本聡介，”フールプルーフとフェイルセーフ---14．災害心理学”丸善出版
(http://pub.maruzen.co.jp/index/kokai/oyoshinri/570.pdf)

2) 向殿政男，“フェールセーフ技術 ～ハイボールの原理に学ぶ～” 明治大学
(http://www.sys.cs.meiji.ac.jp/~masao/kouen/dai9anzengaku.pdf)

3)原子力用語（JIS Z 4001 1999）

4)鉄道信号保安用語（JIS E3013 2001）1015

5)サービスロボット用語（JIS B 0187）

6)情報処理用語（(セキュリティ)）JIS X 0008 2001 ISO 2382-8

7)レーザー製品安全基準（JIS C6801）