工作所発 ういんど～ず注意報 第68報 '10.1.7.
（有） 山下ソフトウェア工作所
http://members2.jcom.home.ne.jp/yamasoft/

フェール・セーフ

電車のドアは圧搾空気で開閉しています。シューっと空気が抜ける音がするでしょ。ドアを開けるときに圧搾空気を注入します。注入した空気を抜くとドアが閉まります。逆じゃないかって？　いえいえ、逆だと走行中に

空気が抜けたらドアが開いて乗客が転落、大事故になります。万が一のときに安全側に動作するように、という設計概念ですね。

コンピュータ・ソフトのプログラムを組むにも、万が一のときに安全側に動作するようにと考えて組んでいます。プログラムはコンピュータへの命令を順番に書いていくのですが、場合によっては順番をとばしたり、別のプログラムに移ったりさせます。コンピュータのプログラムは「場合によって」という判定のかたまりです。

あるプログラムのテスト中に、権限がないユーザーには表示しない部分を表示してしまうという不具合を発見しました。プログラムが想定外の原因で中断したあと、再開したら起きました。原因は「権限が〝無〟のユーザーの場合は表示を消す」というプログラムになっていたからです。

コンピュータはＹｅｓかＮｏかの世界なのですが、この場合の判定は「権限が〝無〟＝Ｙｅｓか、そうではない＝Ｎｏか」なのです。中断したときに権限のデータ消えてしまったのですから、〝有〟でも〝無〟でもない＝Ｎｏの判定となり、表示してしまったのです。安全を考えたら判定は「権限が〝有〟かそうではないか」とし、そうではないのとき表示を消すようにしておけば、権限のデータが消えていたとしても表示することはなかったのです。

まあ、プログラムを組むときに万が一までなかなか考えつかないものです。想定外の中断がなければ見逃していたかもしれません。以後、フェール・セーフへの心がけは社是です。

歴史の古い鉄道はドアの他にもいろいろと安全を考えています。それでも盲点があります。線路の信号装置は列車がバックすることを考えていません。ですから、朝のラッシュ時にバックして停車位置を直すには、装置の設定や安全確認などでけっこう大変な作業らしいです。

決められた線路を走る鉄道に比べ、大空を飛び交う飛行機は鉄道以上に安全が考えられているはずです。飛行中に万が一エンジンが停まったら、グライダーのように大空をゆうゆうと滑空して難なく着陸、あるいは海に着水できます、プロペラ機までは。しかしジェット機は後退翼ですからゆうゆうと滑空できません。ジェットエンジンの推進力を頼りに飛ぶので、空気の抵抗を減らすため翼を後退

させました。ん〜、安全とは？　確率・統計の計算上問題ない、あ〜そうですか。

　鉄道にしろ飛行機にしろ運転は訓練を受けたプロ達ですが、自動車はそうではありませ

ん、素人です。確率・統計で大丈夫でしょうか？　高速道路でアクセル・ペダルがマットに引っかかって戻らなくなり、スピードがでたまま壁に衝突、乗っていた人が死亡したというハイブリット車の事故が報道されました。事故を追跡した雑誌によると、ブレーキ・ペダルを踏んでも効かなかった、エンジンのスイッチも数秒間押し続けないと切れないようになっていたとか。え？　数秒間押さないと切れないスイッチって、パソコンと同じなんですか？

　パソコンはよくフリーズします。プログラムがいくら判定しても同じ個所を繰り返してしまい、その間に他のアクションを受付けなくなる状態です。原因は機器の故障のこともあれば、プログラムのミス（想定外の事象に出くわした）ってこともあります。無限ループとも呼んでいます。こうなると、もう強制終了するしかありません。そのためにはスイッチを数秒間押し続ける（あるいは電源を抜く）ことになります。

　現在の鉄道も航空機も自動車もたくさんのコンピュータを組み込んでます。ということはプログラムのかたまりです。人命に直接かかわるようなプログラムはコーディング（組立段階）からフェール・セーフに徹しているんでしょうね、きっと。でないと、怖い。

　さらに、万々が一プログラムがフリーズしても安全側に作動するメカニズムになっていると安心なのですがねぇ・・・

フェール‐セーフ【fail-safe】
　安全装置の一。たとえ誤りや失敗が起きても、安全を保障するための機構。機械やシステムを暴走させないための歯止めや異常時の自動停止機能を含む。【広辞苑】
［軍］偶発戦争防止系統；（汽車、飛行機の）安全装置　【日語外来語辞典】

電車のバック
　福知山線の運転手にはプレッシャーに作用したようです。国鉄時代に運転手が居眠りしいているうちに上り坂でバックしてしまい、後続の列車と衝突する事故がありました。

滑空
　御巣高山の事故はエンジンのトラブルではありません。だからダッチ・ロールしながらも地面への激突は避けられたのですが・・・　ニューヨークでは離陸したとたん鳥が突入してエンジンがほぼ停止したものの目の前の川にみごと着水。このハドソン川の奇蹟も確率・統計のうち？

アクセルが戻らない
　オートマ車じゃなければ、クラッチ・ペダルでエンジンと車輪を切り離せたのに・・・　かのハイブリット車にマニュアル車は無い！