生業プログラマ必読！リスクを減らす考え方＆しくみ　宇宙船の設計で考える?!

モノづくりの最新コモンセンス「機能安全」

第3回　評価を繰り返して「安全」を目指す…リスク・マネジメント

森本 賢一

図1　安全とは…許容できる残存リスクしか残っていない状態

リスクとは，ある危険の発生しやすさと，それが発生したときの影響度を掛けたものです．危険の根源を本質安全によって排除したり回避したりできない場合，機能安全によってリスクを小さくする必要があります．機能安全は危険そのものを排除する対策ではないので，危険そのものはなくなりません．そのため，リスクも完全な0にはなりません．ある程度のリスクは残ってしまいます．これを残存リスクといいます．

機能安全では，

安全＝許容できないリスクが存在しない状態のこと

と定義しています．すべての残存リスクが許容できる程度になった状態を安全な状態だ，と考えます（**図1**）．

安全な状態になるために作られたシステムを安全保護システムと呼ぶこととします．安全保護システムは，それが動作しなかった場合に発生してしまうリスクのレベルに応じて，必要となる信頼性のレベルが高くなります．ちゃんと動作しない確率が高いものを安全保護システムとして使えないからです．このように許容できるリスクを明確にして対策を練ることが，信頼性設計のスタートとなります．システムの設計の前にしっかりとリスクについて考えておくことが大切です．

このようにリスクについてしっかり向き合うことを，リスク・マネジメントといいます．今回はこのリスク・マネジメントについて解説します．

リスク・マネジメントとは

リスク分析やリスク・マネジメントと聞くと，「関所」のようなイメージをもつ方がいるかもしれません．例えば新しいビジネスを立案し，その計画や設計に「リスクがない」ことを上司に報告します．このようなときに行う最終チェック，もしくは最後の仕上げ，というイメージがあるかもしれません．でもこれはかなり大きな間違いです．

機能安全や，ISO-9001が2015年度の改定で参照するISO-31000でも，リスク・マネジメントとは「反復プロセス」であると考えています．最終チェックというよりも，業務プロセスや開発プロセスの一部であり，活動をよりよくするために反復されるべきものです．

第1回　業界用語「機能安全」と「本質安全」（2015年8月号）
第2回　「リスク」「安全」…用語の定義（2015年9月号）