信頼性と安全性

明治大学 名誉教授
向殿　政男

1 まえがき

私たちの身の回りには、ICT 技術を用いた大規模で複雑なシステムが、例えば、原子力発電や化学プラントから通信システムや都市交通システムまで、色々と浸透してきている。また、未来に向けたスマートグリッドやスマートシティと呼ばれるようなものまで、構築されようとしている。このような複雑に連携し合った大きなシステムを我々は正しく構成し、それを検証、維持できるのだろうかという不安を感じる。とくに、個々の構成部分の信頼性を追求して行くだけで、私たちの安全な生活は保証できるのであろうかという疑問が湧く。主として信頼性はハードなどの施設・設備の問題であるが、安全性は私たちの身体的な傷害や精神的な障害の問題である。最終目標は安全性のはずであるが、信頼性だけを追求して、安全性が実現できると考えるのは素朴すぎるのではないだろうか。本来、信頼性と安全性は異なった概念と技術であるからである。システムが大型になって全体を把握するのが困難になると共に、いったん事故が発生すると取り返しがつかないような場合には、安全性のほうを重視して追求する観点が不可欠なはずある。とくに、ソフトウェアを含んだコンピュータがシステムの制御や監視に組み込まれる場合には、信頼性だけを追求する傾向があるので、上記の観点は必須なはずである。

ここでは、上記の問題意識に対して、少しでも参考になればと、信頼性と安全性の関係について、複雑なところには入り込まないで、シンプルで基本的なところから考えなおしてみることにする。

2 信頼性という概念と安全性という概念

工学システムにおいて信頼性とは、素朴には、「与えられた機能を果たし続けること」であり、安全性とは、「人に危害を及ぼさないこと」である。一般的に、信頼性が高ければ高いほど、安全性は保たれている可能性が高いと考えられるので、安全性の問題は信頼性の問題に帰着できるという人もいる。しかし、これは正しくはない。例えば、安全性が確認できない場合に列車を止めてしまうことを考えてみれば分かる。列車は走るという本来の機能は果していないので信頼性は低くなるが、人が事故に遭うことがないという点からは安全性は確保されている。信頼性を下げることで安全性が確保されることもあり得る。また、安全性は、信頼性と共に状況にもよる。例えば、煙を検出する火災報知機が、故障して機能を果たさなくなったとき、煙が発生していない状態での故障ならば、すぐには安全性の問題にはならないが、故障中に煙が発生したならば、即座に安全性の問題につながる。また、煙の出ない火災だってあり得るし、更に、煙検知の機能としては正常に果たし続けていても、その機能維持のために火災報知機自体の温度が上がってしまって、火災につながるようなことがあるかもしれない。火災の最中は、火災報知機は火災を通報できないであろう。本体が燃えているからである。安全性の本質は、火災を出さないこと、人に危害が及ぼさないことである。信頼性と安全性の事情は、かなり微妙である。

安全性と信頼性の関係で最も大事なことの一つに、安全を保つという機能が果たされている信頼度、すなわち、安全性に対する信頼性という考え方はあり得るはずである。その機能が果たされなくなったら、安全性が損なわれ、人に危害が及ぶことになる。信頼性は、機能が果たされなくなった後のことを考慮していない。いくら信頼性が高くても、いつかは壊れることになる。機能を果たさなくなった後の状態を信頼性は考慮していないのである。しかし、安全性はそこも含めて考えている。以上のように、信頼性と安全性はお互い強い関係はあるが、異なった概念であることは明らかである。

英語では、信頼性は reliability、安全性は safety であり、reliable は頼れる、safe は安全である、ことを意味している。前者は動的であるが、後者は状態であって静的である。この事情は、日本語の信頼と安全についても同様である。なお、日本語の・・性（英語の・・ty）は、・・であること、・・の特性、・・の能力などを表していると考えられる。素朴なイメージとしては、信頼性には、もともと、度合の意味が入っているように思われる。どのくらいの信頼性かと尋ねられたら、例えば、80％とか、0.8 とかのように数値で答える雰囲気がある。一方、安全性は、イエス（1）かノー（0）かであるイメージが強い。安全であるか安全でないかのどちらかである（実は、これは正しくないことが、次項

以降で詳しく紹介する)。もし、どのくらいの安全性かと問われれば、数値で答えるよりは、まあまあ、とか、かなり、とかの定性的な答えが返ってきそうである。どうもその内容は、どのくらいの程度の怪我や危害なのか、その“ひどさ”に重点があるように思われる。このように、信頼性と安全性の概念については、奥の深い、幅の広い議論があり得そうであるが、話が込み入ってきそうなので、ここでは、工学システムの範囲に限って、基本に帰り、信頼性と安全性の定義から考えてみることにする。

3 信頼性と安全性の定義

信頼性（Reliability）とは、JIS では、「アイテムが与えられた条件で規定の期間中、要求された機能を果たすことができる性質」、及び、その定量的な尺度である信頼度（Reliability）は、同様に、「アイテムが与えられた期間与えられた条件下で機能を発揮する確率」と定義されている[1]。なお、幸いなことに、日本語では、信頼性と信頼度という二つの言葉を持っているが、英語では、上のように Reliability 一つである。広い意味の Reliability（日本語の信頼性）と狭い意味の Reliability（日本語の信頼度）とを文脈で使い分けているが、近年では、前者に対してはディペンダビリティ（Dependability）という用語が使われるようになってきている。ディペンダビリティには、信頼性だけでなく、保全性（maintainability）や可用性（availability）の概念が含まれている。

安全性の定義は、JIS では、「人への危害または損傷の危険性が、許容可能な水準に抑えられている状態」[1] となっている。なお、安全度なる数量的な概念は、JIS にはない。安全規格を作成するための国際的なガイドラインである ISO/IEC ガイド 51[2] では、「許容可能でないリスクが存在しないこと（freedom from risk which is not tolerable）」と安全性を定義している。上の JIS の安全性の定義で、「人への危害または損傷の危険性」をリスクと解釈すると、両者の定義は一致する。すなわち、安全性は、「リスク」という概念と「許容可能」という概念を経由して定義されている。ここで、両概念をもう少し詳しく見てみよう。「リスク」とは、「危害の発生する確率とその危害のひどさの組み合わせ」[2]、及び、「許容可能なリスク」とは、「現在の社会の価値観に基づいて、与えられた条件下で、受け入れられるリスクのレベル」[2]、と定義されている。ここで重要なことは、安全とは、リスクゼロのことではなく、それから受ける便益（ベネフィット）や必要な対策コストを考えて、許容可能（仕方がないけど受け入れる）や受け入れ可能な程度までリスクが低減されているとき、安全という、という定義である。リスクゼロ（絶対安全）の存在はあり得ないとして最初から放棄している。では、どの程度のリスクならば、安全といえるかというのは、時代により、社会により、与えられた条件（使用者、寿命、温度・湿度・環境など）により、異なるとしている。

安全性の定義から、安全性と信頼性の関係がある程度見えてくる。すなわち、安全とはリスクがある低いレベルに抑えられている状態で、リスクとは、危害の発生確率と危害のひどさの組み合わせなので、安全性を高めるためには、危害の発生確率を低くするか、危害が発生したときにそのひどさ（例えば、怪我の程度）を小さくするか、またはその両方で実現できることになる。リスクを構成している上の二つの要因のうち、前者が主として確率に基づく安全性に関連し、後者が主として構造に基づく安全性に関連している。すなわち、安全性は、危害が発生しないように信頼性高く作る技術と、危害が発生したときにひどさを下げる技術の両方で実現される。主として、前者が信頼性技術に、後者が通常言われる安全性技術に関連する。

4 信頼性技術と安全性技術

信頼性技術には、システムの信頼度を高く構築する技術と、信頼度を評価する技術とがある。通常、信頼性技術というと確率論を用いて信頼度を評価する後者の技術をいう場合もあるが、本質は、前者の高信頼化技術にある。一方、安全性技術には、前述のように、信頼性を高める技術と事故が発生した時に危害を小さくする技術とがあり、通常、前者に注目が集まるが、後者の技術が本質的である。なぜならば、安全性では、事故が発生した時に危害を小さくする技術を先に適用し、その後で、危害が発生しないように高信頼化の技術を適用すべきであるからである。安全の分野では、故障しないように信頼性高く作るという概念を確率安全と呼び、故障したら安全側になるようにして危害を小さくするには、通常、構造を用いて実現されるので、構造安全と呼んで区別をしている。確率安全と構造安全は、根本的に異なった概念である。しかし、安全性を高める技術としては、両者とも必須である。

信頼性技術の例には、例えば、コンポーネントそのものが故障しないように高信頼に作るフォールトアボイダンスという技術や、冗長系（多重系）を用いて、全体として信頼性を上げるフォールトトレラントの技術等がある。なお、フォールトトレラントには、構造を工夫することで信頼性を上げるという構造と確率の両方が考慮されている。一方、構造を用いて安全を実現する例としては、例えば故障したら必ず安全側になるように構成するフェールセーフ技術や、

人間が間違えづらいように、また、たとえ間違えても危険にならないように構成するフールプルーフ技術などが典型的である。表 1 に信頼性技術と安全性技術の幾つかを挙げておくが、他の多くの技術が両者に関係している。例えば、故障モード影響解析（FMEA：Failure Mode and Effects Analysis）や故障木解析（FTA：Fault Tree Analysis）などの技術は、どちらにとっても重要な技術である。

5 本質的安全と機能安全

システムには、通常、果たすべき二つの機能がある。そのシステムが本来果たすべき本来機能と、安全を確保する安全機能である。ここで、安全機能とは、機械システムの場合は、「故障がリスクの増加に直ちにつながるような機械の機能」[3] と定義されている。安全機能には、システム本体が実現している安全機能と、安全防護柵や安全装置等の付加的に追加された安全方策が果たす安全機能とがある。この二つの安全機能は、それぞれ分けて、本質的安全及び機能安全と呼ばれる。後者の機能安全とは、簡単に言えば、本来の機能を果たしているシステムを安全に制御する装置や導入された安全装置等が果たす安全機能のことである。この場合には、その装置が正しく働いていること、すなわちその信頼度が重要となる。その機能を失ったとき、直ちに安全性の問題が生ずることになる。最近は、ソフトウェアとコンピュータを含む電子機器などが主要な安全機能を実行している大規模で複雑なシステムが増えてきており、機能安全は、このような場面で重要な働きをする [4]。

機械システムにおけるリスクの低減方策には、スリーステップメソッドと言われる基本的に施すべき順番が国際規格で定められている [5]。第一ステップは、本質的安全設計を行うことであり、第二ステップは、安全防護策や安全装置を施すことであり、第三のステップは、使用上の情報の提供、すなわち、警告ラベルなどで表示したり、残留リスクを避けるためのマニュアルや説明書などを提供することである。この順番から言えば、最初にやることは、システム本体に安全機能を持たせることで、これは構造安全や本質的安全 [6] に対応する。第二ステップとしては機能安全を持たせることで、これが確率安全に対応している。残ったリスクに対してはその情報を提供して、使用者に安全の確保を委ねる、これが現在の安全確保の世界の常識である。前述した､危害を小さくする安全技術（構造安全）を先に施し、次にそれが正しく機能する信頼性技術（機能安全）を施すべきであると記したのは、このことに対応をしている。

表１：信頼性技術と安全性技術の例

信頼性技術	安全性技術
信頼性理論	本質的安全設計技術
信頼性評価技術	安全装置、防護柵（ガード）
冗長性、多重性	フェールセーフ
フォールトトレランス	フールプルーフ
フォールトアボイダンス	インターロック
モニタリング、状態監視技術	フォールトレジスタンス
故障診断	タンパレジスター
検査技術	衝突安全

6 あとがき

一般的なシステムにおける信頼性と安全性の話を紹介してきた。それでは、ソフトウェアにおける信頼性と安全性は、どのように考えられるのだろうか。コンピュータやソフトウェアは、論理の世界である。人間に危害を与える機械は物理の世界であり、危害を受ける人間は生理的な体を持つと共に心理や情理の世界にある。ソフトウェアに信頼性の概念は存在しても、自分自身の中に安全性の概念を含むことは可能なのだろうか。コンピュータやソフトウェアが、現実にシステムの安全性を高め、社会に貢献しているのは、現実社会の機械や人間と直接結びついているからである。この場合、論理の世界と物理の世界や人間の世界との整合性を意識しない限り、真の安全は実現できないはずである [7]。すなわち、ソフトウェアの世界に、信頼性の概念はあっても、安全性の概念を取り込むには、機械的な物理の世界や人間の生理、心理、情理の世界と直接結びつかない限り難しいのではないだろうか。このことに関しての答えは、まだよく分からないが、少なくとも、ソフトウェアの世界にも構造と確率の話は明らかに存在する。本稿で、繰り返し信頼性と安全性の違いとお互いの関係について、構造と確率の話を通して述べてきたのは、ぜひ、この関係を明確に理解して、ソフトウェアの世界における安全性について考えてみていただきたいからである。現実のシステムにおいては、少なくとも、安全性と信頼性とが融合しない限り、意味のある真の安全は実現できないことだけは明らかである。

【参考文献】

[1] JIS Z 8115 デイペンダビリティ（信頼性）用語
[2] ISO/IEC ガイド 51（JIS Z 8051), 安全側面 — 規格への導入指針 , 2014
[3] ISO13849-1（JIS B 9705-1）, 制御システムの安全関連部
[4] IEC 61508（JIS C 0508）, 電気・電子・プログラマブル電子安全関連系の機能安全
[5] ISO 12100（JIS B 9700）機械類の安全性 — 設計の一般原則 , リスクアセスメント及びリスク低減
[6] 向殿政男：本質安全という概念について , 品質 , Vol.42, No.3, 日本品質管理学会 , 2012-3
[7] 向殿政男：コンピュータ安全と機能安全 , IEICE Fundamentals Review, Vol.4, No.2, pp.129-135, 電子通信情報学会 , 2010-10