ためになる「安全学」

向殿政男
明治大学 理工学部 情報科学科 教授

第10回 安全確保のためにコンピュータを使う ～機能安全という発想～

コンピュータなしの生活は、もはや考えられない時代になっています。“私はパソコンを使わない”と主張する人がいようとも、身近なところでは家電製品や携帯から、社会では自動車や電車や銀行まで、情報通信技術(ICT)なしには、現実的に生活が成り立ちません。事実、職場でも事務的な仕事はもちろん、モノづくりの基本である機械、設備、プラント等のシステムでは、コンピュータを中心にしたICTの技術が、機能や性能、効率等の高度化を担う最も大事な領域になっているはずです。

それならば、安全を担う部分にコンピュータの高度な機能を使わない手はないと考えるのは自然な発想です。ところが一方で、安全に直接かかわる部分にはコンピュータは使用すべきでないと主張する人々がいます。一般的にも永らく、そう考えられてきました。なぜなら、コンピュータを構成している半導体などの電子部品はどのように壊れるか保証はないし、ソフトウエアにバクがないことを保証することはほとんど不可能だからです。システムの本来の機能の高度化等にコンピュータを使うのはよいが、安全確保の部分に限ってはコンピュータに任せるわけにはいかないという主張です。コンピュータと安全との関係は、一体、どうなっているのでしょうか。

安全確保の部分にコンピュータを使うべきでないという主張は、安全は構造的に、本質的に、確実に実現すべきであって、もし故障等の不具合が発生しても、常に安全側になるようなフェールセーフ構造を組み込んでおくべきである、ということです。壊れるかもしれないハードウエアや不完全なソフトウエアに、確率的に人間の命を任せるわけにはいかないという主張です。一方で、世の中に絶対安全が存在しない以上リスクは必ず存在し、ある確率で事故は起こるものであるから、コンピュータの高度な機能を使うことによって事故の起きる確率を小さくし安全性を高めることができるのであれば、コンピュータを安全のために積極的に使っていこうという主張もあります。前者の主張は確定論的安全、後者は確率論的安全と区別され、前者の典型が本質的安全、構造的安全の考え方であり、後者の典型が、ここで紹介する機能安全という新しい考え方です。

システムにはさまざまな安全を確保する機能(安全機能)が組み込まれていますが、その中で、安全装置のように安全を監視し、安全を実現するためだけに設けられる装置があります。その装置が実現する安全機能のことを、機能安全と言います。この安全のための装置に、コンピュータのようなICTの技術を応用しようということです。すなわち、まずシステムを安全関連系(ここでは安全装置と考えて結構です)と非安全関連系に分け、安全関連系だけは徹底的に信頼度を高くつくろうという発想で、コンピュータを導入し正しく働く確率を高くすることでシステム全体の安全を確保しようという考え方です。

ただし、安全関連系が故障してもシステムは必

Profile

向殿政男 ―*Mukaidono Masao*―

1942 年生まれ。1965 年明治大学工学部電気工学科卒業、1970 年明治大学大学院工学研究科博士課程修了、工学博士。1970 年明治大学工学部電気工学科専任講師、同電子通信工学科教授を経て、現在、同理工学部情報科学科教授。私立大学情報教育協会会長や明治大学校友会会長なども務める。専門は、情報科学（特に、ファジィ理論、人工知能）、安全学、多値論理。著書に『国際化時代の機械システム安全技術』（日刊工業新聞社）、『よくわかるリスクアセスメント－事故未然防止の技術－』（中災防新書・中央労働災害防止協会）、『安全設計の基本概念』、『制御システムの安全』（ともに日本規格協会）など。

ずしも危険になるとは限りません。ここでいう「正しく働く確率」とはもう少し厳密にいえば、危険になるような安全関連系の故障（これを危険側故障と言います）の確率をいかに少なくするかを問うということです。具体的には、そのシステムが担う安全の重要度に対応して、安全関連系の安全の度合いを故障率で定めようとするものです。これを安全度水準（SIL：Safety Integrity Level）と呼び、実際には 4 段階にレベル分けされたものが提案されています（**図表―1**）。その故障率は、非常停止装置のようにたまにしか使わない（低頻度要求モードの）安全装置に関しては、要求があった時に何回に 1 回失敗するかの確率によって指定されます。そして監視装置や頻繁に使用される（連続、または高頻度モードの）安全装置に対しては、1 時間当たりどのくらいの危険側故障が発生するかの確率によって指定されます。

それでは、コンピュータを含んだ安全関連系は、どのように設計・製造すればよいのでしょうか。これに関しては、国際安全規格として、“電気・電子・プログラマブル電子安全関連システムの機能安全（IEC61508）”が定められています。ハードウエアの故障に対しては、ランダム故障対策として多重系を用いて信頼度を上げる手法等が、ソフトウエアの不具合（バグ）に対しては、システマティック故障としてソフトウエアを製作するプロセスを規定して信頼度を上げる手法等が指定されています。さらに、従事する人間や組織の独立性、および従事する技術者の能力なども規定されています。

図表―1　安全度水準（SIL）

安全度水準（SIL）	低頻度作動要求モード	高頻度作動要求または連続モード
	作動要求当たりの機能失敗平均確率	単位時間当たりの危険側故障率
1	10^{-2} ～ 10^{-1}	10^{-6} ～ 10^{-5}
2	10^{-3} ～ 10^{-2}	10^{-7} ～ 10^{-6}
3	10^{-4} ～ 10^{-3}	10^{-8} ～ 10^{-7}
4	10^{-5} ～ 10^{-4}	10^{-9} ～ 10^{-8}

機能安全では、以上のように、システムが任されている安全の重要度に対応して、安全関連系が持っていなければならない故障率の低さ（逆に言えば、許される故障率）を指定しています。コンピュータを安全確保に使うためには、リスクに基づく機能安全の考え方は避けられないでしょう。今後、あらゆるシステムに機能安全の考え方が入ってくるものと思われます。

ところで、確定論的安全と確率論的安全のどちらを優先すべきかという疑問を持った人がいるかもしれませんが、現実には、両者は不可分の関係にあります。構造的に安全を実現しても、それが正しく機能する確率を考慮せざるを得ないし、危険側故障確率が指定されても、それを実現する構造を考慮せざるを得ないからです。コンピュータの出現で、今後の安全技術は、両者の融合に向け動き出す時代を迎えたと言えるでしょう。新しい時代の安全技術には、それなりの安全の哲学と理念が必要です。