リスク分析による事故の回避を考える

機能安全規格IEC 61508とソフトウェア開発

中島 裕生

機能安全の規格であるIEC61508は2010年に改訂され，2012年からは，欧州では関連指令2006/42/ECによってほとんどの産業機械に対して適合が義務付けられる．機能安全とは何か，IEC61508とは何かを把握し，特にそのソフトウェア要求事項についてを考察する．（編集部）

1．機能安全とは

機能安全（Functional Safety）という考えが規格IEC 61508によって公開されて，10年を超えようとしている．日本人にとって斬新だったのは，リスク分析による事故の回避，抑制という安全認識の導入だった．日本では暗黙の了解とされがちな絶対的安全という認識から，リスク分析による事故の回避，抑制への移行，つまり事後責任から事前責任へというパラダイム転換も乗り越えるべき課題であった．2010年にIEC 61508第2版が発行され，多くの個別製品派生規格が本規格を元に制定されている．これを見ると，IEC 61508が世界から支持された規格であり，機能安全という考えが世界に普及しつつあるとしても過言ではない．この規格の法的側面として関連深いのはEU（欧州連合）の新機械指令2006/42/ECである．指令（Directive）の意味するところは，EU加盟各国が指令を国内法に組み入れる義務を負っていることである．さらに，この指令に適合していなければEU内での製品の流通ができないなどの強制力も持っている．現時点では，IEC 61508が整合規格にはなっていないので，IEC 61508への適合だけではEU諸国などで商品を販売するのに必要なCE適合としては不十分である．しかし，本規格への適合は，製造物責任（PL：Product Liability）の観点からも強く推奨されている．この2006/42/ECは，2012年からほぼ全ての産業機械に対して指令への準拠が求められ，EUへの輸出関連企業にとって関心が高いところである．

表1　ISO 61508の派生規格の例

分　野	名　称	内　容
医療機器分野	IEC 62304	ライフサイクル
	IEC 60601	医療機器の安全性
自動車分野	ISO 26262	DIS
鉄道分野	IEC 62278	RAMS：Reliability，Availability，Maintainability，Safety
	IEC 62279	ソフトウェア安全性
	IEC 62280	安全に関する情報伝達
	IEC 62425	システムの安全性
FA分野	IEC 62061	産業機械E/E/PE（電気/電子/プログラマブル電子）制御システム
	IEC 61800-5-2	電子制御モータ可変速ドライブ
	IEC 13849-1	機械安全制御システム

そこで，本稿ではIEC 61508第2版をもとに機能安全を概観してみる．IEC 61508は，パート1～パート7までである膨大な規格である．規格全体を俯瞰（ふかん）しながら，ソフトウェアの規格であるIEC 61508-3に焦点を当てて規格の枠組みを明らかにし，今後，規格書を読まれる読者の便宜を図りたい．

ソフトウェアに焦点を当てたのは，近年ますますその占める役割が大きくなっているだけでなく，ソフトウェアがハードウェアと同じように工業製品として認知されるための試金石をIEC 61508-3が提示していると考えられるためである．その意味でも，IEC 61508はシステムとしてもソフトウェアとしても意欲的な規格だと著者は捕らえている．ソフトウェアの話題にいく前に，IEC 61508の規格としての位置付け，使用する言葉の定義，特徴とコンセプトを説明する．

2．規格としての位置付け

産業機器の安全関連システム，それを構成するハードウェアおよびソフトウェアの機能安全に関する国際規格IEC 61508は，IEC（国際電気標準会議）が10年を要する作業の後，1998年～2000年に初版を発行した．2010年には

KEYWORD——IEC61508，ISO/IEC Guide51 リスク・マネージメント，安全関連システム，決定論的原因故障