

国際安全規格の概要

ISO/TC199 国内審議会委員
日本信号㈱

蓬原弘一*

1. はじめに

従来世界貿易の円滑化には、主として関税の引き下げによるような措置がGATT（関税と貿易に関する一般協定）で強調されてきた。しかし、'80年代以降、規格・基準の非関税障壁が問題視されるようになり、'95年のWTO/TBT協定（貿易の技術的障害に関する協定）では、加盟国は国際規格に基づいて国家規格を定めることで合意している。これにより、国際安全規格も21世紀制定に向けて急速に進みつつある。本稿では、この国

際安全規格案を一部説明し、併せてその特徴の一部を一緒に述べる。

2. 規格の構成

国際安全規格（案）類の第1の特徴は規格の構成方法にある。従来、多くの場合安全は個別の製品の中だけで扱われてきた。しかし、個別の製品規格の中でいずれの部分が安全に係わるのか、必ずしも明確でない。このため、国際安全規格案では各種個別の製品の安全に係わる部分を抜粋して体系化し、機械類の安全性確保の一般則をできる限り定めようとしてきている。

規格を機能別に分類して、その組み合わせで個別

*安全研究室 室長 工学博士

ISO/IECガイド51（安全規格作成のためのガイドライン）		
国際標準化機構（ISO）規格例	規格分類 （機械類の安全性）	国際電気標準会議（IEC）規格例
1) 機械類の安全性——基本概念 一般設計原則規格（ISO 12100） 2) リスクアセスメント規格（ISO 14121）	← 基本安全規格（A）： 全ての規格類で共通に適用できる基本概念、設計原則を扱う規格	
3) インタロック規格（ISO 14119） 4) ガードシステム規格（ISO 14120） 5) システム安全関連部規格（ISO 13849） 安全距離規格（ISO 13852） 突然の起動防止規格（ISO 14118）	グループ安全規格（B）： 広範囲の機械類で利用できるような安全、または安全装置を扱う規格	→ 6) 電気設備安全規格（IEC 60204-1） 非常停止規格（IEC 13850） 7) センサ機能安全規格（IEC 61496） 8) センサ応用規格（IEC 62046） 9) 電気的安全機能規格（IEC 61508） EMC規格（IEC 61000-4）
個別の製品規格（C）： 特定の機械に対する詳細な安全要件を規定する規格 （個別の製品は基本安全規格とグループ安全規格を利用して作成すること。但し、不足する場合並びに規格が要求を満たさない場合は新しく規定してよい。） 製品例：工作機械、産業用ロボット、鍛圧機械、無人搬送車、化学プラント、輸送機械など。		

図1 国際安全規格の階層化構成（規格案を含む。規格名称は簡略化して示してある。）

の製品規格を定めるような規格構成方法を規格の階層化と呼んでいる。

図1に国際安全規格の階層化構成を示す。同図でISO/IECガイド51とは、ISO（国際標準化機構）とIEC（国際電気標準会議）が共同で安全規格制定の指針として示した合意事項である。この指針では、同図の（A）（B）（C）で示すように、安全規格を基本安全規格とグループ安全規格と個別の製品規格の3種類に分けて制定すべきと規定し、（B）の規格は（A）の規格を、（C）の規格は（A）（B）の規格を各々できる限り利用して作成するように定めている。図1の左右には、この規格構成による具体的規格例が規格名称を簡単化して示してある。表1は図1につけた番号の

規格内容と正式な規格名称を示す。

3. 安全性の定義

例えば鋸歯が剥き出しで回転している状況や、たとえ鋸歯を蓋で被っていても誰れかが開けてしまつて何時災害が起るか分らないような潜在的危険状態を“リスクが存在する”と表現する。

国際規格では安全は「受け入れ不可能なリスクがないこと」と定義される。これが国際安全規格の第2の特徴である。

図2は上述の安全性決定のプロセスを示している。図2で三角形の面積はリスクの大きさを示す。△ABCは最初に見積ったリスクの大きさで、それが受け入れ不可能な場合、少くとも許容可能な

表1 国際安全規格例（規格案を含む）の内容説明

国際安全規格（案）	規 格 の 内 容
1) ISO/CD 12100 （機械類の安全性：基本概念，設計のための一般原則）	第1部と第2部から成る。第1部では機械類に関する安全規格の作成上で基本となる用語の概念と，安全性確保の方法に対する考え方が示される。第2部は現時点で利用可能な技術を用いて，第1部の概念や考え方を表現するための助言を与える。
2) ISO 14121 （リスクアセスメントの原則）	リスクアセスメント関連の用語の定義とリスクアセスメントの方法に関する一般原則が述べてある。付録に各種危険源が表で示される。
3) ISO 14119 （ガード付きインターロック装置）	ガードに例えば扉を付けて扉が閉じているときだけ機械の運転を可能にし，扉を開いているときは機械を停止させるような装置の種類とその動作原理の解説，設計上の要求事項，各種インターロックの選択指針が示される。
4) ISO 14120 （固定及び可動のガードの設計及び構造に関する一般的要求事項）	種々のガードが例示してある。ガードの設計及び構造に関する一般的要求事項と，各種ガードに対する選択の方法が示される。
5) ISO 13849 （制御システムの安全関連部）	第1部と第2部から成る。第1部では機械の安全に関わる制御部分の設計手順が示され，図3の安全方策のカテゴリーによるリスクの大きさ評価の方法が説明される。第2部では，各種制御要素で配慮すべき故障モードが示される。
6) IEC 60204-1 （機械の電気設備，一般的要求事項）	機械類で要求される電氣的な安全確保手段，素材，機器に関する要求事項とソフトウェア，文書作成の要求事項が規定される。感電，電気火災に対する保護の要求事項を含む。
7) IEC 61496-1 （電気検知保護設備：一般的要求事項及び試験）	人を保護するためのセンサ及びその周辺機器に対する一般的要求事項と試験方法が規定される。要求事項は安全性達成のための設計要件を含み，試験はEMCに対する規定を含む。
8) IEC 62046 （人検出保護設備の機械類への適用）	機械可動部停止による安全確保への電気検知保護設備の適用に関する規格。システムの停止機能の保証方法が電気，油圧，空圧を含めて規定される。また，各種センサにおける安全距離の算定方法が示される。
9) IEC 61508 （機能的安全性：安全関連システム）	第1部から第7部までである。システムの安全性を確保するには，危険な区域で危険な状況がないようにすることと，たとえ危険な状況が生じても災害にしないための安全対策が必要となる。機能的安全性の本規格は後者に属し，特に電氣的装置による対策を扱う。この対策には，電氣的／電子的システムが存在し，特に電子的システムにはソフトウェアを含む。

リスクの大きさ（ ΔADE ）にまで、できるなら広く受け入れられるリスクの大きさ（ ΔAFG ）までリスク低減の方策を実施しなければならない。ここにリスクの見積りには、合理的に予見可能な設備の誤使用を含むこととされる。この点で国際規格案は製造物責任対策（PLP）を含む。

4. リスクアセスメント

傷害又は健康上の障害を生じ得るような潜在的危険を“危険源”又はハザードと呼ぶ。リスクはこの危険源の存在が人にどの程度の被災をもたらすかを示し、国際安全規格で用いられる用語類の中でも最も重要な概念である。リスクアセスメントとは予め明らかに想定される危険源に対してリスクの見積りを行い、その結果リスクが大きい場合に実施した安全方策とその見積り結果を比較する作業（リスク比較と呼ばれる）である。国際安全規格の第3の特徴は、安全方策の決定がこのリスクアセスメントに基づくことである。

図3にリスクアセスメントの具体的実施方法の例を示す。同図には想定される危険源(図1の規格例2では約90種が例示してある。)に対するリスクレベルの見積り方法、並びに、その見積り結果と施した安全方策の比較方法が示されている。リ

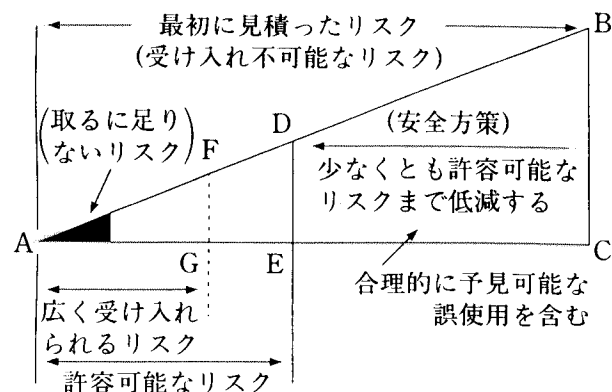
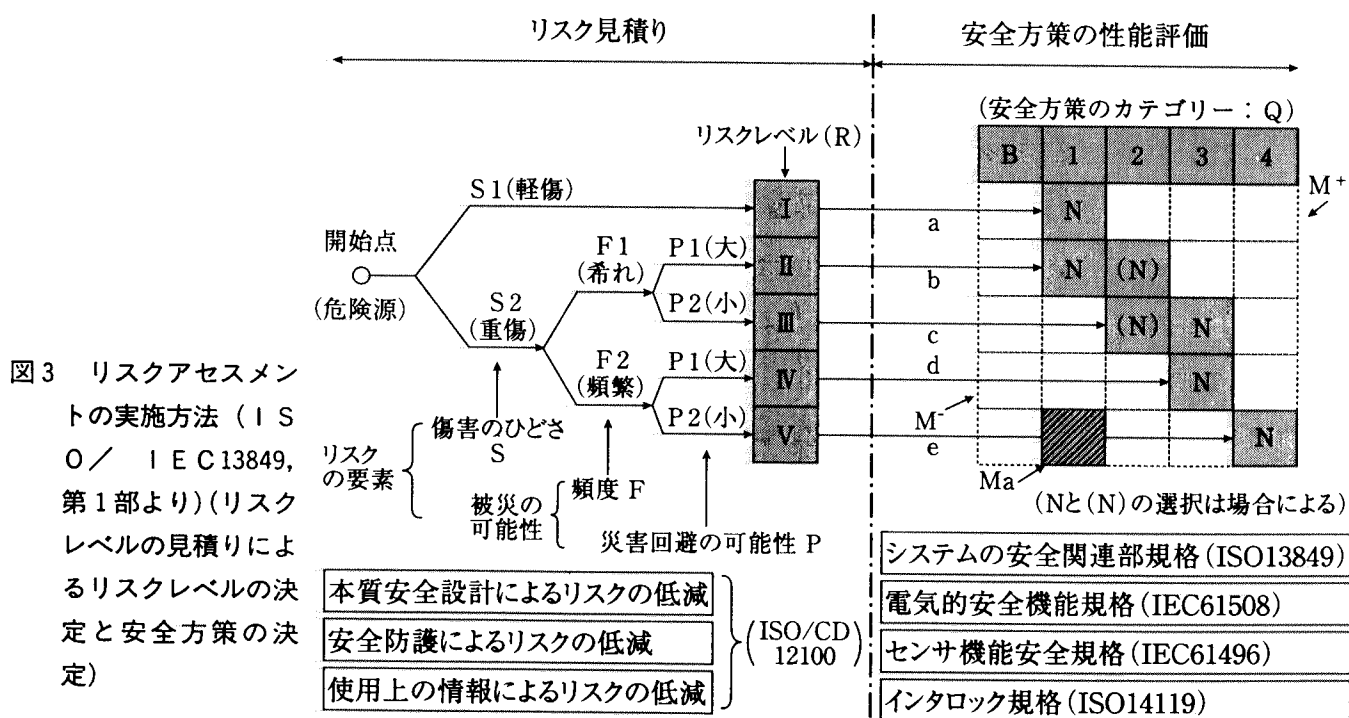


図2 安全性決定のプロセス(IEC61508,第5部より)

スクレレベル（R）は、図1の規格例2に基づいて、傷害のひどさSと被災の可能性、即ち人の危険源への接近の頻度F及び被災回避の可能性Pをリスク見積り要素とし、危険源に対して各々S1、S2とF1、F2とP1、P2のいずれかを選択して定める。図3でリスクレベルはローマ数字の大きい値ほど大きい。上述のリスクの見積り結果が大きい場合、安全方策を実施しなければならない。

安全方策の実施は図3の左下に示すように基本的方法が図1の1の規格で示される。本質安全設計によるリスクの低減とは、安全性確保の工学的原則（工学的に当然とされる原理）を用いた安全方策である。安全防護方策とは機械の危険な所を



防護柵で囲ったり(図1の3で示す)、機械の制御装置とは別に外から安全装置を追加するような処置である。使用上の情報によるリスク低減とは、例えば取扱い説明書で示される安全性確保上の注意事項や機械自体に貼り付けた文書、標識などによる低減策である。但し、「設計上の不備を使用上の情報で補ってはならない」とされる。

実施の安全方策が見積られたリスクレベルに見合うか否かは、図3の一点鎖線の右側に示す安全方策性能評価との比較に基づいて査定される。

安全方策の性能評価とは、安全性確保実証の機能評価を意味している。例えばブレーキ性能が常にチェックされておれば、そのブレーキには高レベルの安全性評価を与える。危険を通報するためのセンサの例では、常に危険を通報できることが自動的にチェックされ、通報能力がないときそれを利用した装置の使用を停止できれば、そのセンサには高レベルの安全性評価を与える。この安全性評価レベルは安全方策のカテゴリー(分類)と呼ばれる。図3ではこの分類Qを5通りで示してある。上述の例では、安全確保機能のチェックの頻度が高ければ、カテゴリー3～4が振り当てられ、チェック頻度が低くれば低いカテゴリー2が振り当てられる。カテゴリー1はこのような機能チェックが行われず、通常のメンテナンスに基づいて信頼性に依存し、但し常識的処置(例えば、安全確保機能を簡単に無効化できないような処置)を施した方策である。カテゴリーBとは、上述の分類に入らない方策であって、安全方策として認めることのできない方策である。このような方策の分類と評価の方法の例は図3の右下の規格類で詳述される(規格内容は表1参照)。

安全方策の決定にはリスクレベル(R)に対してaからeの矢印で示すN又は(N)のレベルの安全方策カテゴリーが推奨される。M⁻の領域は方策の能力(性能)の不足を意味している。例えば、リスクレベルVに対する安全方策はカテゴリー4でなければならないが、もし方策が不足して図に示すようにMaである場合、リスクレベルII以下になるように、例えば機械可動部のもつエネル

ギーを低下させてS2をS1にするような措置や、メンテナンス時を配慮しつつ機械を自動化することによって、F2をF1にし、かつP2をP1にするような措置を実施しなければならない。実施した方策がM⁺の領域である場合、もっと工夫して生産性の向上をはかってよいことを意味している。

5. 独立性に基づく信頼性向上

安全性の確保を重要視するシステムでは、少くとも、図3のように潜在する危険源に対してリスク低減のための安全方策を必要とする。この場合、実施される安全方策には、それが制御システムであれば、例えばハードウェアとしての電気系や機械要素の欠陥(故障)、ソフトウェア上の欠陥(バグ)による不具合を考えることができる。しかし、安全性を確保する上で生じる欠陥は上述のような不具合だけでない。国際規格案では、例えば図3で適切な安全方策として妥当性の確認に誤りが生じてしまうような欠陥を配慮しており、これが国際規格案の第4の特徴である。

国際規格案では図3における安全方策決定に対してその妥当性確認を責任をもって行う人を、図1の9では、評価者(アセッサ)と呼んでいる。この評価者には設備やシステムの立案/設計/設置(一般的にはシステムのライフサイクルを配慮した建設活動)に責任をもつ人達とは独立した権限と資格が要請される。表2に評価者の独立性を能力上で3通りに分類した例を示す。評価者の独立性の能力は担当者の発言力(評価者がシステム建設責任者の影響を受けることのない立場の程度)として示され、独立した個人/部署/(外部)組織の順に独立性は高いとされる。同表の(a)は図3の左側、特に傷害のひどさ相当からみた評価者の独立性の高さを示し、(b)は図3の右側の安全方策カテゴリーに対応する評価者の独立性の高さを示している。表(a)では災害発生時の影響が大きいと想定されるほど、安全方策に対する妥当性確認の評価者は独立性が高くなければならない。表(b)では、安全方策のカテゴリーが高いレベルで要請されるほど、その妥当性確認の評

表2. 評価者の独立性の例 (IEC61508, 第1部, HR:強く推奨, NR:推奨しない)

(a) 独立性の 最低レベル	災害発生時の影響			
	無視可能	小さい	大きい	悲劇的
独立した個人	HR	HR	NR	NR
独立した部署	—	HR	HR	NR
独立した組織	—	—	HR	HR

(b) 独立性の 最低レベル	(カテゴリー相当)			
	1	2	3	4
独立した個人	HR	HR	NR	NR
独立した部署	—	HR	HR	NR
独立した組織	—	—	HR	HR

評価者は独立性が高くなければならない。

表2は実施した安全方策に対して安全性の立証を行うべき建設責任者と、その証明の適合を認可する評価者を分離し、かつ評価者を独立させることによって設備又はシステムの安全性を確保するような考え方に基づく。この“分離と独立”には、それを証明するための文書が必要とされ、この文書の信頼性に基づいて安全性が確保されることを意味している。

システムの“分離と独立”は上述の安全性確保制度に限らず、例えば制御システムの立案時に安全に係わる部分と安全に係わらない部分の分離においても、安全に係わる部分の独立性が重要視される。この場合の独立性は、例えばシステムの立上げや生産性改善のための改修工事等で安全に係わらない部分に関する作業が安全に係わる部分に影響しないことを保証して、工事後の安全性を確保する意味をもつ。安全に係わる部分の独立性が保証できない場合、これらの工事を実施する度に、たとえ安全に係わらない部分の工事であっても制御システム全体に対して表2に基づく妥当性の確認を行って、その結果を文書化すべきことになる。制御システムにおいて安全に係わる部分の独立性の保証は、このような建設時及び建設後のシステム運用上の手続きを簡略化する意味をもつ。

6. む す び

国際規格案について、規格例を説明しつつ4通りの特徴を述べた。これらをまとめると以下の通りである。

イ) 極めて体系的である。これにより種々のシステムへの適用が可能となる。これは従来の個別製品規格を組織的、かつ科学的に見直し

た場合の必然の結果と考えることができる。

ロ) 危険源と被災の可能性の概念を定めて、この二つの概念の組み合わせとしてリスクの概念を定めることにより、安全性をリスクの大きさで定義する。また、リスク低減の方策として工学的手法を明確に定めている。

ハ) リスク低減の方策は、制度上の安全性確保に規格が拡張されている。

国際規格案の推進は次の二つの経済効果をもつと考えられる。

- (1) 国際規格案は安全工学的知見所有の専門家を要請しており、これにより21世紀の知識・情報産業社会対応の新制度創出が可能となる。特に、この制度には経験豊富な高齢者の適用が可能で、我国の現状からみてその成立が極めて有効かつ緊急であると考えられる。
- (2) 機械類において機能上で安全に係わる部分は全機能の平均5%程度(生産性を高くすれば10%程度)と推測され、経済上からも同程度で考えられる。よって、これを新製品の高付加価値化として投入できれば、国際的規模で相当大きな新規産業の創出が考えられる。このため、早急な対応が望まれる。

急速な国際規格の進展に対して、日本は非常に苦慮している。しかし、国内規格の国際標準化は21世紀に向けて避けて通れない状況にある。本稿で述べた国際安全規格の内容は、従来日本には不在で、かつ技術的レベルが高い。幸いに、技術目標が定まった場合の日本人の対処の巧みは秀でていると考えられるので、近い将来、国際安全規格適合の付加価値を付けた製品が盛んに日本から世界に提供される状況を期待したい。