# 機能安全規格について

## 安全とは

「安全」は一般的に使用される用語であるが、日本で使われる意味と、国際規格での意味が異なります。
日本では「管理体制を作り、人を訓練し、規制強化すれば危険は無くすことができる」が基本思想です。従って、危険がないことがすなわち「安全」と捉えられていました。
国際規格では危険をすべて無くすことは無理だが、重大事故は決して起こさない、が基本思想です。このとき重大か否かを判断する指標が必要になるためリスクを導入します。国際規格による「安全」はリスクが許容値以下になることを意味します。リスクという指標を用いることで、得られる安全とリスク低減施策のための投入コストとの比較が可能になり、リスクとコストのバランスから我慢・許容できる領域(ALARP)の探求が可能となります。

**日本**

- 管理体制を作り、人を訓練し、規制強化すれば危険は無くせる
- 危険が無いこと＝「安全」

**国際規格**

- 危険を全て無くすことは無理だが、重大事故は決して起こさない
- リスク＝事故発生頻度(確率)×事故による損害規模
- リスクが許容値以下になる＝「安全」

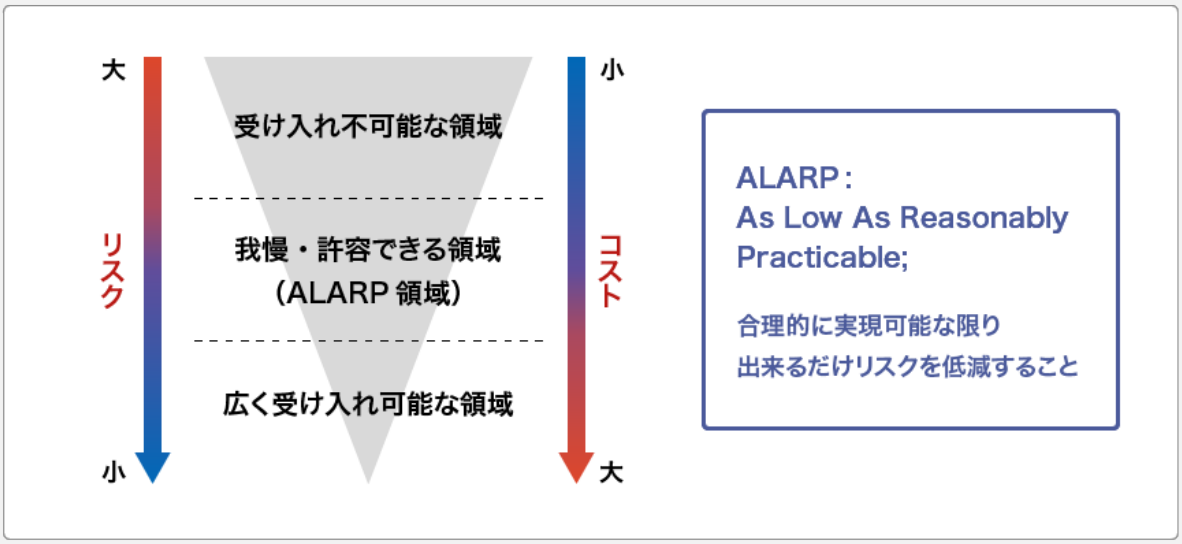


図1. リスクの図

# 機械類の安全

国際規格ではリスク低減プロセスも規格として策定しています。ISO12100では、リスクアセスメント→設計者による保護方策→使用者による保護方策の順番で、リスク低減を進めることを規定しています。リスクアセスメントでは機械の使用状況や使用範囲を決定し、危険の同定を行います。続けてリスクの推定・評価・判定を行い、初期リスクを算出します。

一般には初期リスクは過大で容認できないため、次の設計者による保護方策以降でリスク低減を検討します。

設計者による保護方策では

ステップ1:本質的安全設計方策、

ステップ2:安全防護・付加防護方策、

ステップ3:使用上の注意

の順番でリスク低減を検討します。

ステップ2の一部が機能安全規格として策定されています。

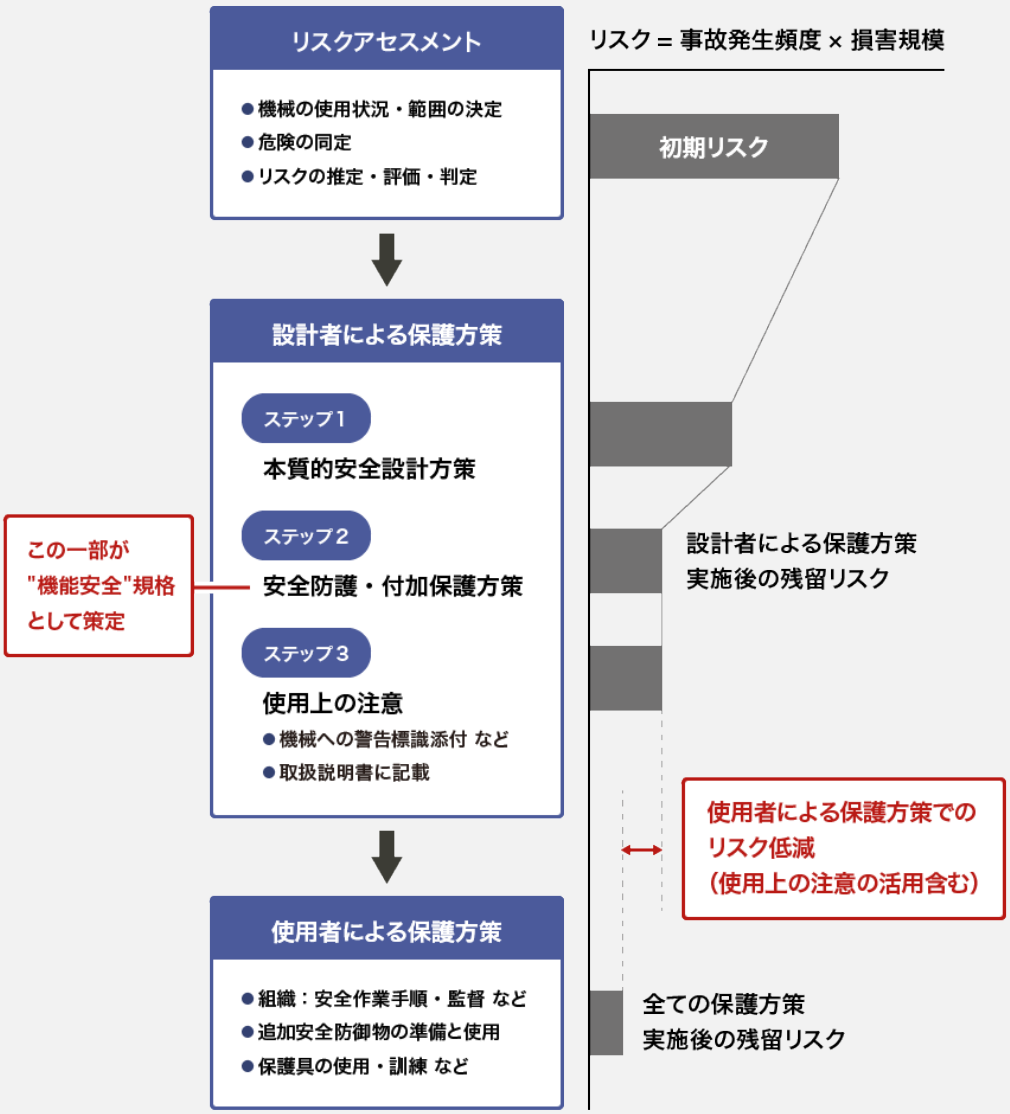


図2. リスク低減プロセスの図

## 機能安全のスコープ

機能安全の本来の意味は安全関連システム(いわゆる安全装置)が正しく働いたときに達成される安全のことです。制御対象機器と制御装置から構成される本体システムと、本体システムの状態を監視し、本体システムが安全になるように制御する安全関連システムとで、全体システムが構成されています。このとき、本体システムに障害が発生して危険な状態に陥る可能性があったとしても、安全関連システムの働きによってそれを阻止して安全な状態を維持し、「機能安全」を実現します。
IEC61508は、安全関連システムにCPUなどのコンピュータシステムを用いる際に適用される規格です。

- 機能安全:安全関連システム(安全装置)が正しく働いたときに達成される安全を示す
- この図では、本体システムに障害発生しても、安全関連システムの働きで安全な状態を維持し、「機能安全」を実現している

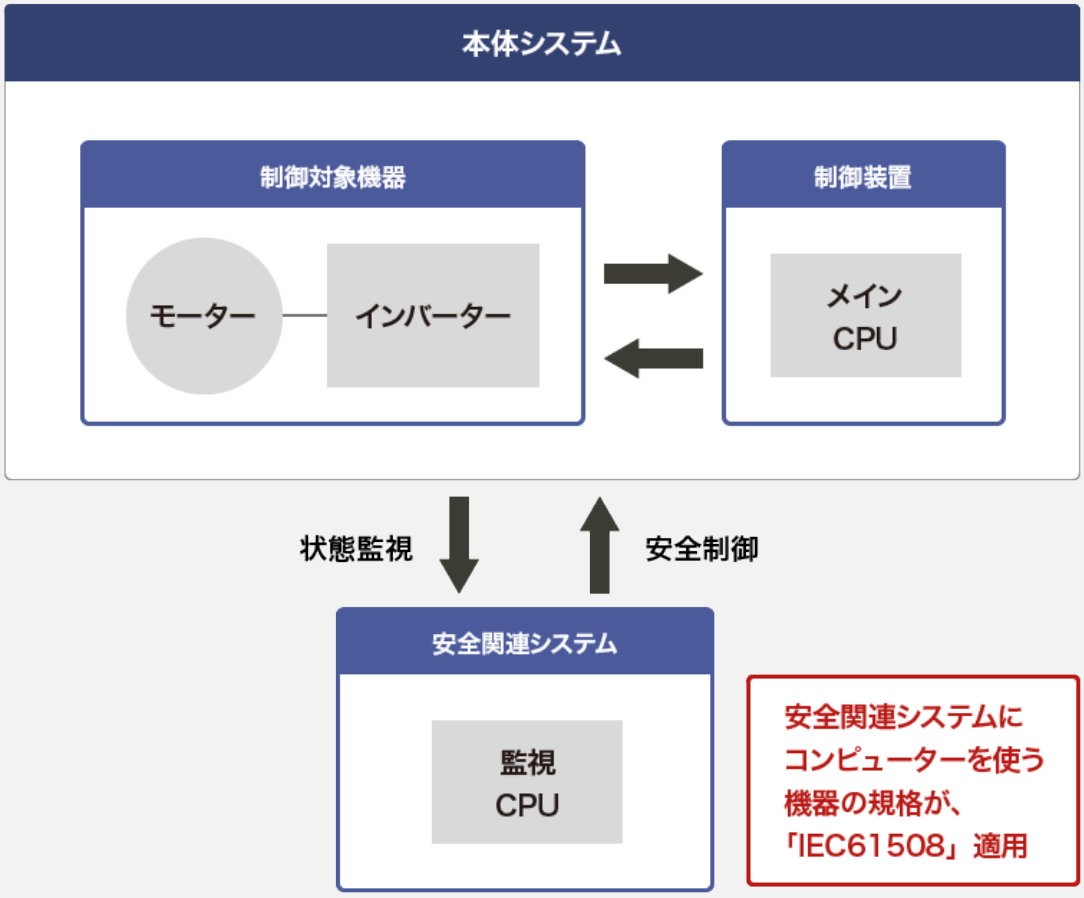


図3. 機能安全の図

## 安全関連規格体系

国際安全規格は、ISO(国際標準化機構)、IEC(国際電気標準会議)の2つの団体によって策定されます。
A規格は基本安全規格と呼ばれ、共通に利用できる基本概念や設計原則を扱う規格です。A規格は基本的な概念を規定しており、このレベルでは電気系は機械系に包含されるため、ここでは機械類の安全性を定めています。
B規格はグループ安全規格と呼ばれ、広範囲の機械類に適用する安全を扱う規格です。A規格をベースとして、より具体的な機械を想定しています。B規格では、機械系と電気系の規格がそれぞれ策定されています。代表的な機能安全規格IEC61508はB規格の中の1つであり、上位A規格に含まれるISO12100やISO14121をベースにして策定されています。
C規格は個別機械安全規格と呼ばれ、特定の機械に対する詳細な安全規格です。C規格では、工作機械、電動エレベータ、建設機械、鉄道、自動車など各個別製品の安全規格が含まれています。これらの安全規格はB規格であるIEC61508をベースにして策定されています。
C規格がまだ存在しない分野の機械類については、上位のB規格、A規格に基づいて安全設計をすることが必要になります。

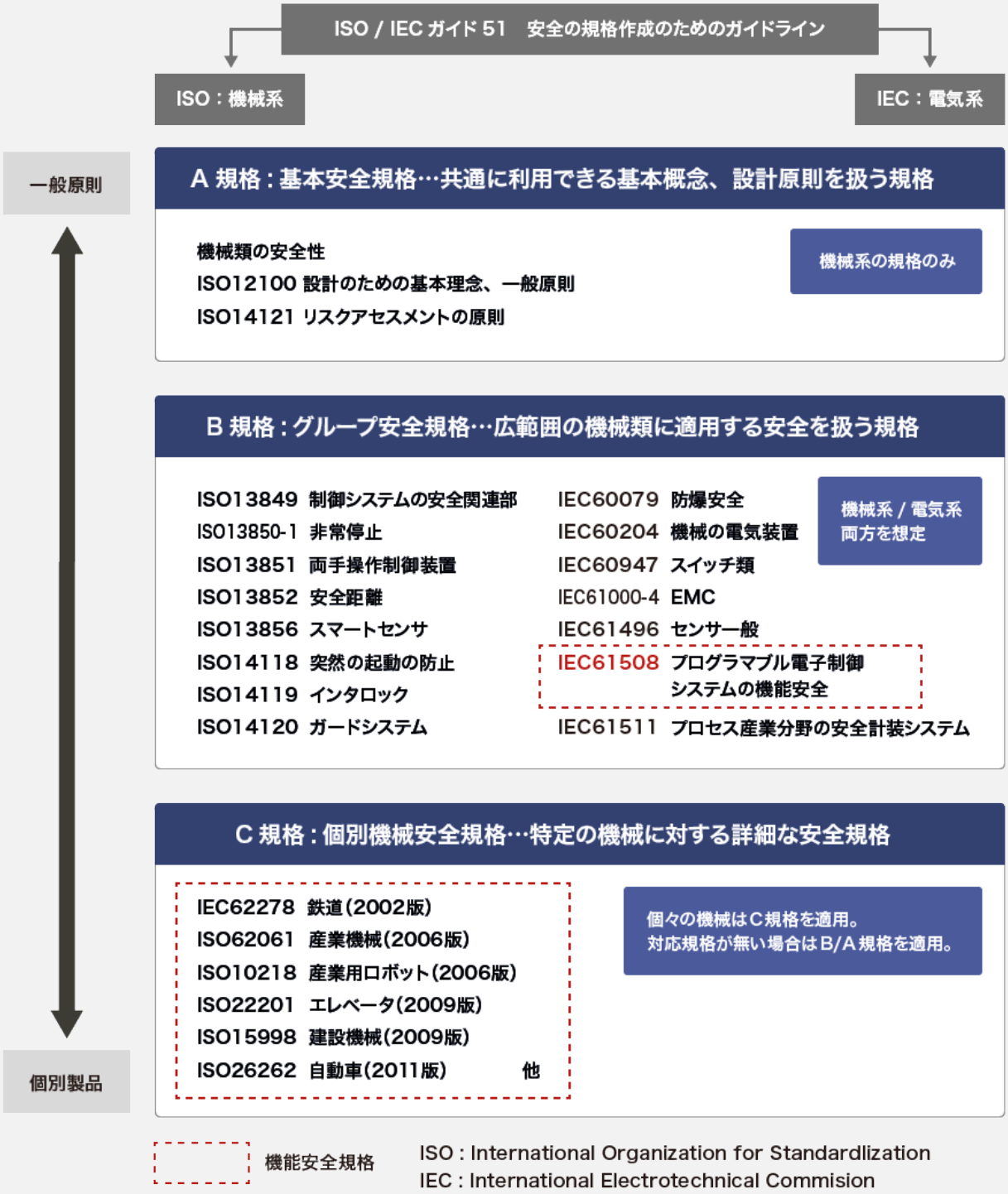
ISO / IEC ガイド 51　安全の規格作成のためのガイドライン
ISO：機械系
IEC：電気系
一般原則
A 規格：基本安全規格…共通に利用できる基本概念、設計原則を扱う規格
機械類の安全性
ISO12100 設計のための基本理念、一般原則
ISO14121 リスクアセスメントの原則
機械系の規格のみ
B 規格：グループ安全規格…広範囲の機械類に適用する安全を扱う規格
ISO13849 制御システムの安全関連部
ISO13850-1 非常停止
ISO13851 両手操作制御装置
ISO13852 安全距離
ISO13856 スマートセンサ
ISO14118 突然の起動の防止
ISO14119 インタロック
ISO14120 ガードシステム
IEC60079 防爆安全
IEC60204 機械の電気装置
IEC60947 スイッチ類
IEC61000-4 EMC
IEC61496 センサー一般
IEC61508 プログラマブル電子制御システムの機能安全
IEC61511 プロセス産業分野の安全計装システム
機械系 / 電気系 両方を想定
C 規格：個別機械安全規格…特定の機械に対する詳細な安全規格
IEC62278 鉄道(2002版)
ISO62061 産業機械(2006版)
ISO10218 産業用ロボット(2006版)
ISO22201 エレベータ(2009版)
ISO15998 建設機械(2009版)
ISO26262 自動車(2011版)　他
個々の機械はC規格を適用。
対応規格が無い場合はB/A規格を適用。
個別製品
機能安全規格
ISO : International Organization for Standardlization
IEC : International Electrotechnical Commision

図4. 安全関連規格体系

## 機能安全関連規格の動向

品質を維持、向上させるための規格としてISO9000が1987年に策定され、つづいて1996年には企業活動が環境に及ぼす影響を最小限に食い止めるように配慮することを目的としてISO14000が策定され、規格への遵守が強く求められています。この品質、環境に続く、規格に関する「第3の波」である機能安全の規格IEC61508が2000年に策定され、原子力、鉄道など各個別分野でIEC61508を基に機能安全規格が策定されています。


図5. 機能安全関連規格の動向


製品に関する詳細・お問い合わせは、営業担当員または下記へ

株式会社 日立情報通信エンジニアリング

神奈川県横浜市西区みなとみらい2−3−3
クイーンズタワーB 25階 〒220−6122
営業統括本部


お問い合わせは下記ページから
お問い合わせフォームにお進みください。

機能安全規格 認証取得支援・開発サービス
https://www.hitachi-ite.co.jp/products/kinouanzen/index.html