

第3部：推奨されるリスクアセスメント手法・基準

1. はじめに

この第3部では第1部、第2部で説明した内容を基に、エネルギーが危険源となる機械類に限定した場合に私が推奨するリスクアセスメントの手法・基準を説明します。

国際安全規格は広い分野をカバーしています。そのため規格をそのまま適用してリスクアセスメント手法・基準を作ると使い勝手の悪いものになる可能性があります。(現に使い勝手の悪い基準を作り苦しんでいる企業が多く見られる。)

ここで述べる「推奨されるリスクアセスメント手法・基準」は、国際規格で規定されているリスクアセスメントの内容を論理的に解釈して説明した第1部、第2部の内容をベースに、各社が自社の方針を取り入れて実用的な基準に仕上げるための参考資料になるようにとまとめたものです。

なお読んでいただければ分かりますが、この第3部で述べる内容は一部を除いてこれまでどの組織・個人も言及してないものです。

概要は下記のとおりです。

- (1) エネルギーが危険源となる機械類を対象としたリスクアセスメントである。
- (2) 機械類の制限の決定ステップにおいては、機械が使用される環境・条件等を示した「設備仕様書」とは別にユーザーとしてどのような使い方をしたいのか、そのためどのようなことに配慮した機械にして欲しいのかといった要求を「安全要求仕様書」として作成してメーカーに伝えることが大切である。
- (3) 危険源の同定ステップにおいては、エネルギーに起因する危険源、特に重大な災害を引起す可能性のある重要危険源の見逃しを防ぐことが最重要課題。そのための手段としてユーティリティ追跡法 (Utility oriented Hazard Identification Method : UHIM (別名「T-I法」)) に基づきユーティリティ線図 (電気配線図、蒸気配管図、空圧配管図、油圧配管図 等) を用いて「エネルギーに起因する危険源の候補」をリストアップすることを推奨する。
- (4) リスクの見積もりステップでは「危害のひどさ」と「危害の発生確率」の組み合わせで評価する。この場合、
 - ・「危害のひどさ」は「生じた危害が日常生活あるいは会社生活 (仕事) に影響する度合い」で区分することを推奨する。
 - ・「危害の発生確率」は「危険事象の発生 (の可能性)」のみで評価することを推奨する。この場合、「危険事象の発生 (の可能性)」を機械本体、制御装置、機械部品等の信頼性 (用いる保護方策が有する危険事象の発生を抑止する能力) で評価するようにする。(これにより「危害の発生確率」を評価する指標とされている「人の危険源への暴露」および「危害の回避又は制限の可能性」は不要となる。)

- (5) 「用いる保護方策が有する危険事象の発生を抑止する能力」を【本質安全化】、【隔離安全化】および【停止安全と隔離安全を組み合わせたインタロック化】に区分する。
- (6) 【本質安全化】あるいは【隔離安全化】の方策を講じれば確定的に安全は確保される。
- (7) 【停止安全と隔離安全を組み合わせたインタロック化】は、①危険状態の検知要素、②危険を検知した時のエネルギーの制限／遮断要素、および、③検知要素やエネルギーの制限／遮断要素が正常であるかどうかを監視する要素、の3要素が構築されているかどうか、および、それぞれの要素がフェールセーフな要素であるかどうかで評価できる。
- (8) 停止安全と隔離安全を組み合わせたインタロック化は上記の他にシステムが「安全確認型システム」かそれとも「危険検出型システム」かに区別することで評価できる。
- (9) リスクの評価ステップで「危害のひどさ」と「危険事象の発生（の可能性）」の二つを組み合わせて評価する方法として「マトリクス法」を推奨する。
（「危険事象発生の可能性」の各レベルに任意の数値を与えて加算（積算）する「数値法（加算／積算法）」は誤った順位を示すことが多いので推奨しない。）
- (10) リスク順位は「危険事象発生の可能性」よりも「危害のひどさ」に重きを置いて決める。
- (11) 「危険事象発生の可能性」を【本質安全化】、【隔離安全化】、【停止安全と隔離安全を組み合わせたインタロック化】で評価する本方式においては、用いられる保護方策が確実に安全を保障する場合を『被災の可能性』が『（ほとんど）ない』と評価する方式なので、「（ほとんど）ない」の区分に該当する場合は「危害のひどさ」が「致命的」「重大」でもリスク順位は低くなる。
- (12) リスク順位を基に「許容不可能」、「やむを得ず許容」、「許容可能」、「広く受け入れ可能」の4区分に分ける時点で、どちらに区分すべきか迷う組み合わせについては、会社の業態と安全に対する姿勢を反映して決定する。「やむを得ず許容」および「許容可能」に該当する組み合わせは事故・災害が発生した時にマネジメントリスクを引き起こす可能性があるため、安全部門、設計部門だけでなく経営層も含めた事業組織として決めることが求められる。

2. 対象とする危険源

ここで対象とするのは、生産に使用される設備で国際安全規格の「機械類，機械（machinery, machine）」*¹に該当するものです。

* 1 機械類，機械（machinery, machine）： 連結された部品又はコンポーネントで構成される駆動部分を備え、又は 備えることを意図したものであって、構成要素である連結部品又はコンポーネントのうち、少なくとも一つは、特定の目的のために稼動し、かつ、 協働するもの

そのため、人力のみによって動かされるものは、機械には該当しないのでここでの対象とはしません。

このように「機械類、機械」に限定すると、人または環境に危害を及ぼす**危険源**は「エネルギー」であり、「危害が生じる」ということは「**機械類の持つエネルギーが人または環境に傷害を与えること**」として現わされます。この人または環境に**傷害を与えるエネルギーの形態、およびその及ぶ範囲**を考えることでリスクを具体的に表現することができます。これが以下に述べるリスクアセスメントの手法・基準を考える場合の基本となります。

2-1 リスクとは

国際安全規格ではリスクは「危害の発生確率と危害のひどさの組み合わせ」と定義されています。具体的には「ある危険源にさらされて被災した場合にどの程度の危害のひどさになるのか」ということと「その危険源にさらされ被災する状態になる確率（可能性）はどの程度か」を組み合わせることによってリスクの大きさを判断する、ということです。

2-2 危険源とは

国際規格では「危険源とは危害を引き起こす潜在的根源」と定義されています。附属書 B1, B2 では様々な種類（機械的、電氣的、熱的 等）に分けた危険源が解説されています。附属書 B1, B2 に記載されている危険源は表面的な形態は異なりますがすべてエネルギーです。「危害を引き起こす潜在的根源」とは「エネルギー」、すなわち「エネルギーが危害を引き起こす根源である」と考えた場合、国際規格の分類とは別に危険源をエネルギーの種類に応じて次のように分けることができます。

危険源とは

- ① 【エネルギー源】：電気、蒸気、化学物質 等 人に危害を与えるエネルギーそのもの
- ② 【有効なエネルギー】：①のエネルギー源が生産に必要な別のエネルギー形態（回転、往復動 等）に変換されたもの
- ③ 【無効なエネルギー】：
 - ①②のエネルギーが
 - a. 生産に関係しない別のエネルギーに変換されて環境に放出されたもの
粉塵、放射熱、騒音 等
 - b. 設備不良・異常により生産に使用されないでそのまま環境に放出されたもの
 - ア. 設備異常または継時劣化により破損した設備本体より放出されるエネルギー
 - イ. 配線・配管の被覆の不良あるいは劣化／損傷により放出されるエネルギー（感電あるいは火傷を生じさせる）
 - ウ. 配管接続部のゆるみ、腐食・損傷により漏れた物体が持つエネルギー（薬傷、感染、あるいは爆発火災を生じさせる）

上記危険源のうち b.のア. イ. ウ. は、設備の強度設計、材質選定、適切な施工、日常

の設備管理ができなければこれらの異常によるエネルギーの放出が設備あるいは配線・配管のどの部分で生じるのか予測することができません。「配線・配管を含むすべての設備が危険源である」という前提に立ったのではリスクアセスメントになりません。

「設備仕様書」及び「安全要求仕様書」（表 3-1 「安全要求仕様書」参照）に従って使用場所、環境、機械にかかる負荷に対して破損／劣化しない設備を設計／制作する。設備劣化が防げない場合はその場所を特定して日常の設備管理を徹底し、劣化による異常が発生する前に更新等を行う。このような対策をとることで上記 b.の ア．イ．ウ．の危険源が生じるのを防ぐ（管理できるようにする）のは設備管理の基本です。この基本ができてない設備（配線・配管を含むすべての設備がいつどこで故障／破損するかわからない設備）を用いての生産などできるものではありません。そこでこのホームページでは「設備管理の基本はできている」という前提に立ちます。すなわちこれら b.の ア．イ．ウ．に該当する「場所が特定できない危険源」は対象外とします。

【有効なエネルギー】【無効なエネルギー】は、【エネルギー源】からエネルギーの供給を受けて生じる（エネルギーの供給を受けなければ危険源にならない）危険源です。そこで私はこれらの危険源をエネルギーから誘引された危険源という意味で「誘引危険源」と呼んでいます。

冒頭に述べたようにここで対象とするのは、生産に使用される設備なので、人に危害を与える次のエネルギーについては対象としていません。

- ④ 人が行動する時のエネルギー（人が自ら持つエネルギーで尖った角や刃物に接触して切傷する、床や段差につまずき転倒して骨折する、他人を突き飛ばしたり殴ったりしてけがをさせる）
- ⑤ 人が行動することで新たに得たり与えたりするエネルギー
 - ・ 人が高所に昇ることで得た位置エネルギー
 - ・ 人が使用することで工具・治具等に与えた（工具・治具等が得た）運動エネルギー

2-3 危険源の特徴

危険源はエネルギーそのもの、有効なエネルギー、あるいは無効なエネルギーなので、次の特徴を持ちます。

- ・ 危険源はエネルギーにより動くもの、あるいはエネルギーを放出するものであるから、そのエネルギーの及ぶ範囲（【危険区域】）は限定される。
- ・ 危険源のエネルギーが及ぶ範囲の外（【危険区域外】）であれば人は危険源により危害を被ることはない。
- ・ この危険源のエネルギーが及ぶ範囲内（【危険区域内】）に人が入り、かつ回避しなければ、人は危険源のエネルギーを受けて直ちにあるいはエネルギーの蓄積によりある時

間後に危害を被る。

【プレスの場合】

図 3-1 のように可動要素であるスライドと固定部であるボルスタとの間に人体を入れた状態で回避しなければスライドのエネルギーを受けて押しつぶされます。この場合、右図のようにスライドの可動範囲が危険区域になり、これ以外の区域において人体はスライドのエネルギーを受けることはありません（危害を被らない）。

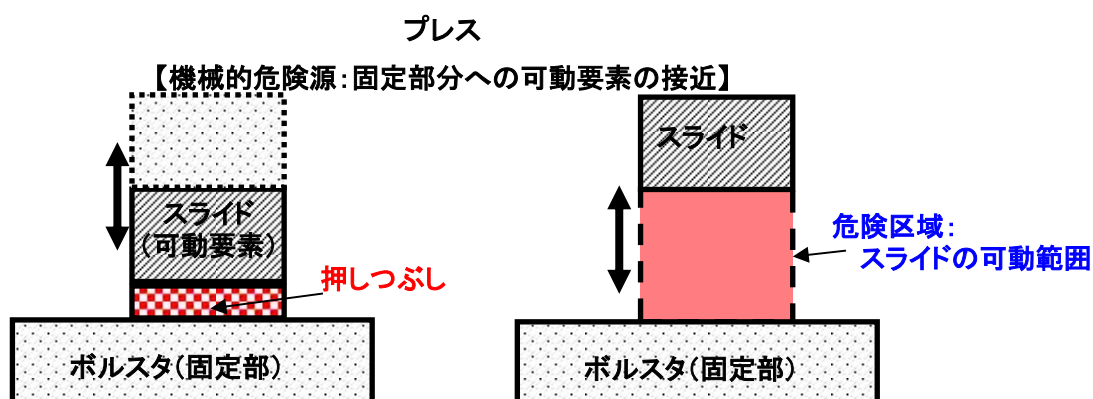


図3-1 プレスのスライドによる被災

【ロボットの場合】

図 3-2 のように可動要素であるロボットアームの可動範囲に人体を入れた状態で回避しなければアームのエネルギーを受けて衝撃、突き刺し、アーム間での捕捉により被災します。この場合、右図のようにアームの可動範囲が危険区域になり、これ以外の区域において人体はアームのエネルギーを受けることはありません（危害を被らない）。

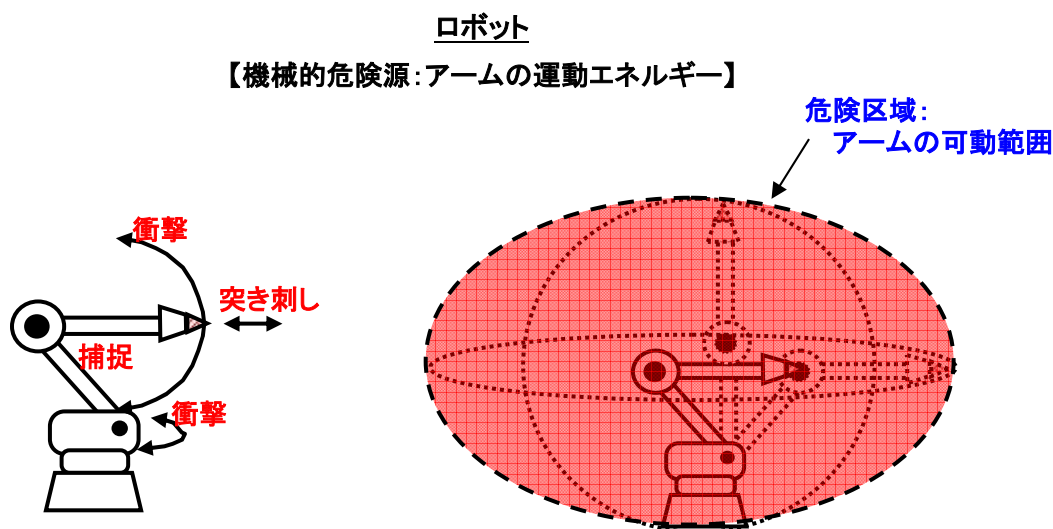


図3-2 ロボットのアームによる被災

【物質あるいはエネルギーを放出する場合】

図 3-3 のように危険源から切り屑、騒音、熱、放射線、化学物質等が放出される場合、これらの飛散範囲に人体を入れた状態で回避しなければこれらのエネルギーを受けて難聴、熱傷、放射線障害、中毒等の危害を被ります。この場合、右図のように物質あるいはエネルギーの飛散する範囲（騒音、放射線、化学物質等では人体に影響を及ぼす許容値以上の範囲）が危険区域になり、これ以外の区域において人体は物質のエネルギーあるいは飛散するエネルギーにより影響を受けることはありません（危害を被らない）。

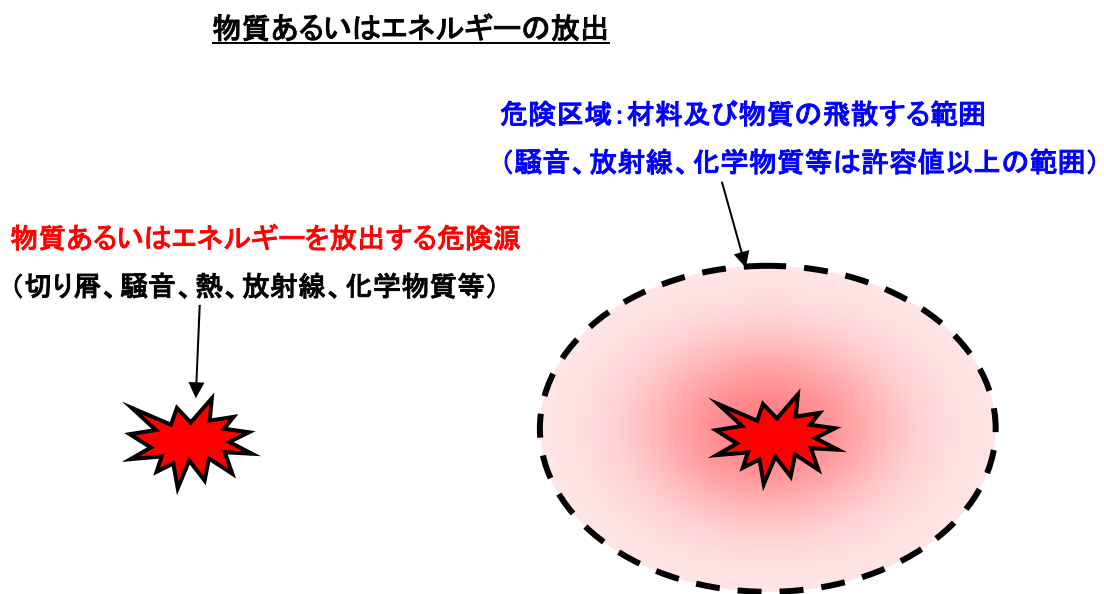


図3-3 物質あるいはエネルギーの飛散による被災

【エネルギーが種類の異なる複数の場合】

図 3-4 のように可動要素であるロボットアームが固定部との間で材料の加工を行うため例えば粉塵が飛散する場合は、図 3-2 で示したロボットアームの可動範囲だけでなく図 3-3 で示した粉塵の飛散範囲に人体を入れた状態で回避しなければ被災します。この場合は右図のようにアームの可動範囲の加え粉塵の飛散範囲が危険区域になります。この場合でもこれ以外の区域においては人体はエネルギーを受けないので危害を被むことはありません。

ロボット(その2)

【機械的危険源:アームの運動エネルギー】+【物質の飛散】

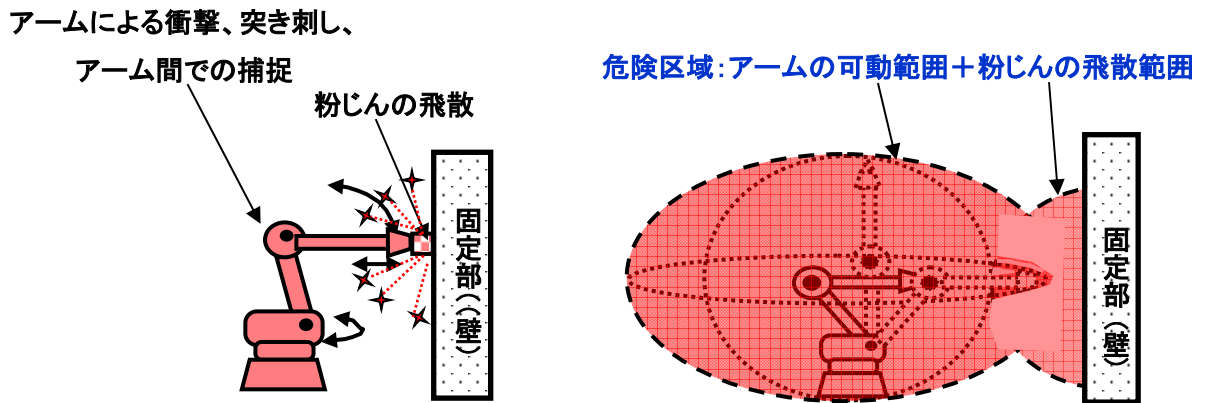


図3-4 ロボットのアームによる被災及びエネルギー物質の飛散による被災

いずれにしても「危険源にはそのエネルギーが人体に危害をもたらす限定された危険区域が存在し、人がこの危険区域の中に入らない限り被災することはない」、ということです。この危険区域は目には見えませんが計算あるいは実測することで確定することができます。

上記のことを踏まえた上で、危害の発生プロセスとして示される図 3-5 の危険状態、危険事象とはどういう状態、事象なのかについて考えます。

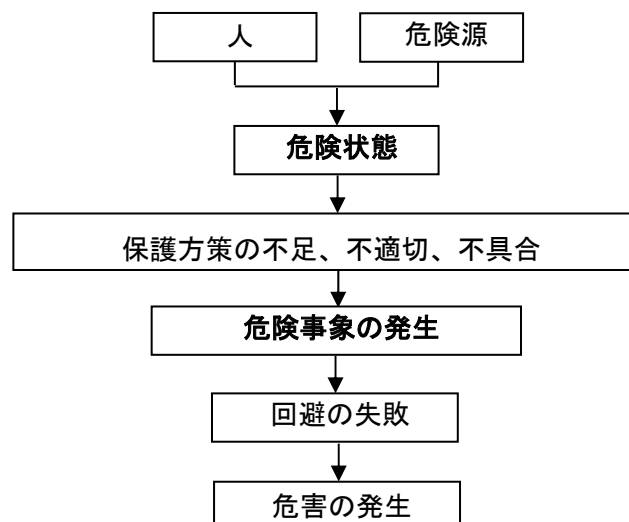


図3-5 危害の発生プロセス

危険状態は一般に図 3-6 の上に示す図のように危険区域と人の存在区域の重なった状態（共存する状態）で、その範囲は危険区域の一部として説明されています。しかし人は自由に行動するので人の存在区域は危険区域も含めた広い範囲になるだけでなく、その境界を明確にすることはできません。このことを踏まえると人の存在区域と危険区域の関係は図 3-6 の下の図のようになり、危険状態の範囲は危険区域と全く同じ範囲になるということになります。

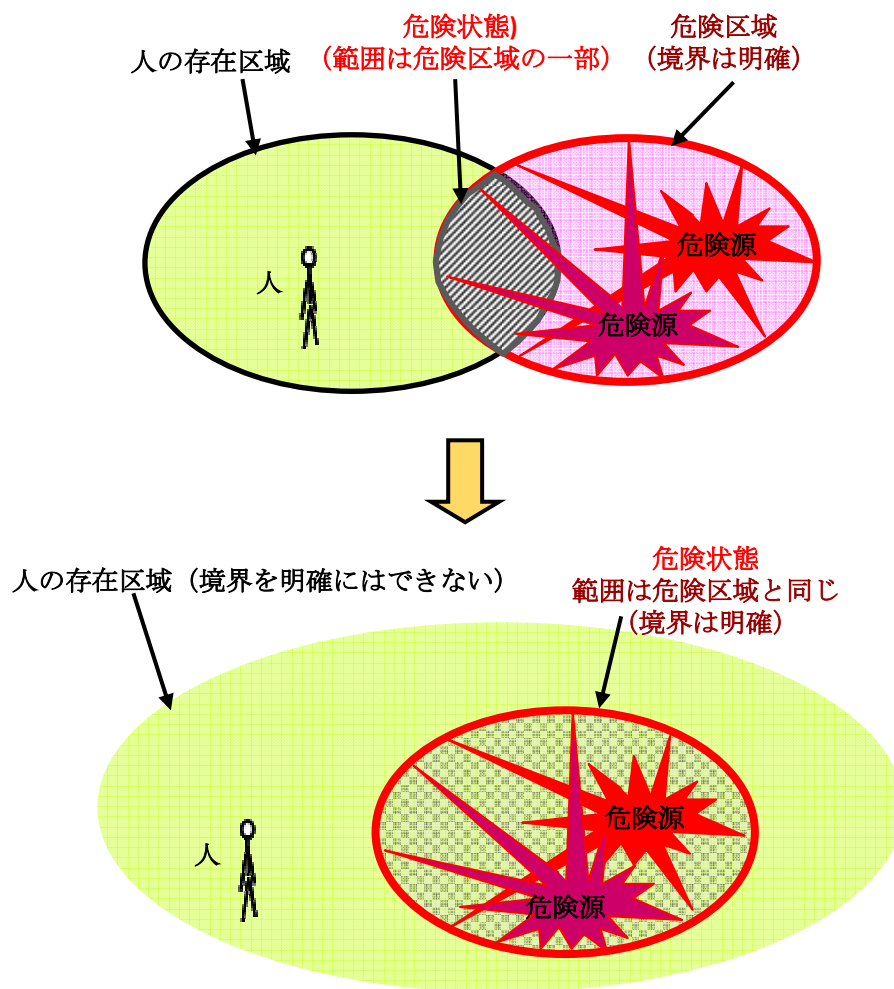


図3-6 人の存在区域、危険区域、危険状態の関係

明確な境界を持つ危険区域と自由に動き回る人の存在区域が重なるという状態は、危険区域に人が自由に入れる状態、すなわち機械側になんの保護方策も施されていない状態を意味します。この危険状態を防ぐために機械側に保護方策を行うのですが、図 3-5 には「保護方策の実施」というプロセスが記されていません。保護方策を施さなくても安全が確保される場合もあるので省いたのか？と推測されますがわかりにくい図です。そして「保護方策に不足、不適切、不具合があると危険事象（人が危険源のエネルギーを受けて怪我

をする可能性のある事象)が発生する」と説明されています。

「保護方策の実施」についての言及なしに「保護方策に不足、不適切、不具合があると危険事象が発生するという流れになっており、理解しにくい図です。

図 3-5、図 3-6 で示される危険事象およびリスクの発生するプロセスは、論理的に考えると以下のように解釈することができます。

- ・危険源にはそのエネルギーが人体に危害を及ぼす危険区域が存在する。
- ・危険区域は危険源のエネルギーが及ぶ範囲であり限定されている（境界がある）。
- ・自由に動く人がこの限定された危険区域の中に入らない限り被災することはない。
- ・危険事象は危険区域の中に人が入ることによって生じる。
- ・リスクは危険事象の発生（危険区域への人の侵入）により生じる。
- ・危険事象の発生を防ぐために行う対策は保護方策と呼ばれ、この保護方策の技術レベルにより危険事象発生の確率（危険事象が発生する可能性の大～小）が決まる。

重要なのは危険区域へ人が侵入する危険事象の発生をいかに抑えるか、ということです。そこで以下では上記の考えをベースにしてリスクアセスメントを考察していきます。

3. リスクアセスメントとは

厚生労働省はリスクアセスメントを次のように説明しています。

「製造業における危険性又は有害性を特定し、それによる労働災害（健康障害を含む）の重篤度（被災の程度）とその災害が発生する可能性の度合いを組み合わせることでリスクを見積もり、そのリスクの大きさに基づいて対策の優先度を決めた上で、リスクの除去又は低減の措置を検討し、その結果を記録する一連の手法」

国際安全規格を基にすると次のようになります。

「事故の未然防止を図るため、機械・設備の使用条件を明確にした上で、すべての危険源を同定する*2 とともに、各危険源についてリスクの大きさを見積り、大きなリスクを持つ危険源については保護方策を施すことでそのリスクが受け入れ可能なリスクに低下するようにするための科学的、体系的手法」

日本規格協会（JSA） - 標準化教育プログラム〔機械安全分野〕 第 1 章国際安全規格 （明大名誉教授 向殿政男） P16 参照

*2 国際安全規格では「同定する(与えられた危険源リストにある危険源と同じかどうかを判定すること)」と言いますが、リストに載ってない新たな危険源は存在しないのか？ という疑問があります。

国際安全規格では「各危険源のリスクの大きさを見積る」までがリスクアセスメントで、「大きなリスクを持つ危険源についてはそのリスクが受け入れ可能なリスクに低下するように保護方策を施す」プロセスはリスクアセスメントに含んでいません。

しかし、選定された保護方策により、どの程度にまでリスクが低減できるのかを評価しなければリスクアセスメントは完結しないという観点からリスクアセスメントを考える方もおられます。

私も同様の観点に立っているので保護方策を含めてリスクアセスメントの説明を行います。

4. リスクアセスメントのプロセス

リスクアセスメントは図 3-7 のフローに従いますので、以下、ステップ 1～ステップ 4（5 を含む）に分けて説明します。なお、ステップ 6 の「リスクに応じた適切な保護方策の採用によるリスク低減」は、ステップ 3 において一緒に述べます。

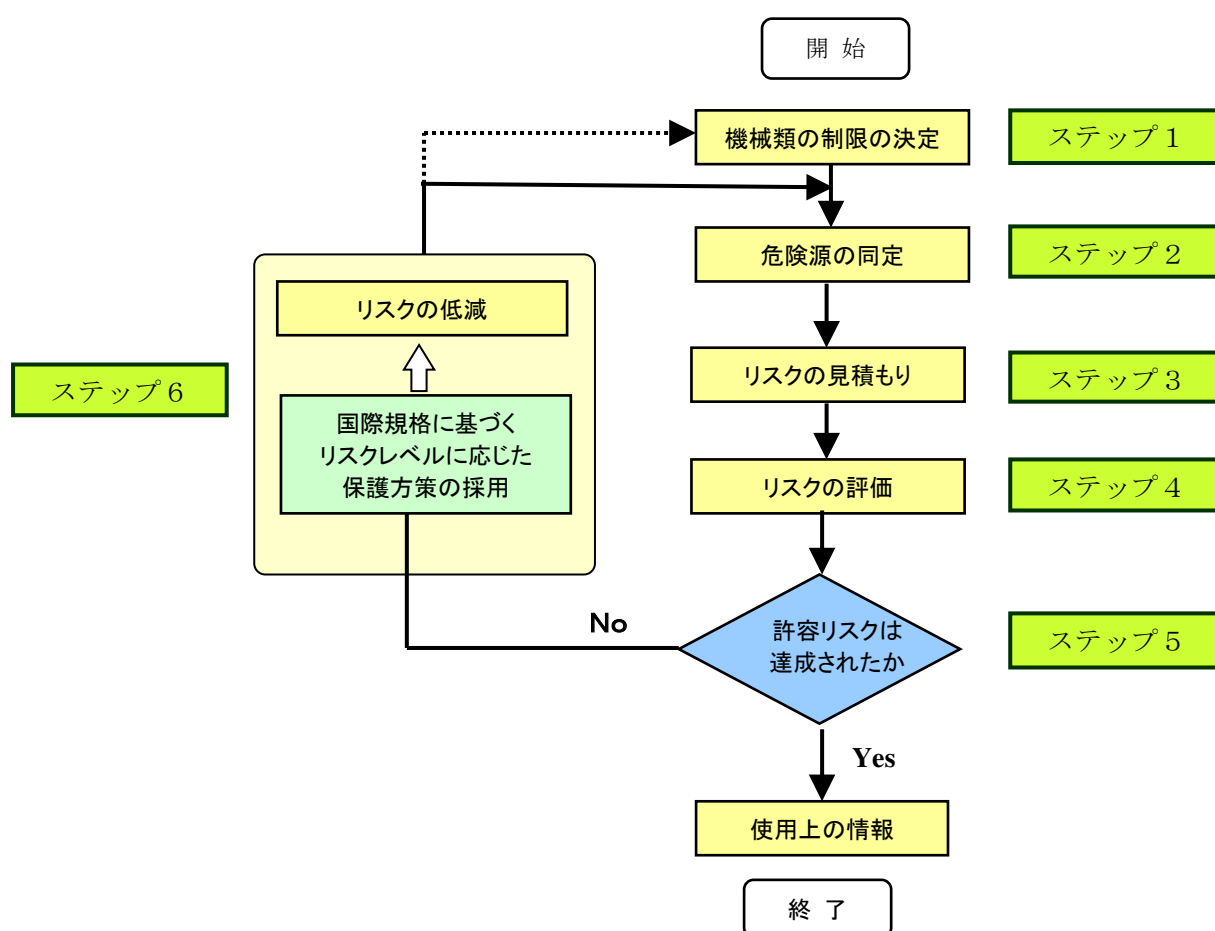


図3-7 リスクアセスメントのフロー

ステップ 1 機械類の制限の決定

ステップ 1 では設備をどのような条件下で使用するのかを明確にします。これらについてはメーカーが「設備仕様書」を作成してユーザーに提示するのが一般的ですが、作業に従事する人の安全を確保するためにはユーザーが必要な情報を提示しなければメーカーが

考え機械に組み込む安全対策だけで不十分な場合が多々あります。そのためにはユーザーとしてどのような使い方をしたいのか、そのためどのようなことに配慮した機械にして欲しいのか（予見可能な誤使用を含む）といった要求を「安全要求仕様書」としてメーカーに伝えることが必要となります。

被災の可能性は、機械の損傷・破損時も生じますが、最も可能性が高いのは人が稼働している機械に関与する作業で下記のようなものです。

- ① 生産条件の変わらない状態における原材料の供給、製品の取り出し作業
- ② 生産条件の変更（生産量の変更、品種の切り替え）に伴う原材料の切替え、治具の交換、および、品質確認のためのサンプリング作業
- ③ 品質あるいは設備の異常に対処するための作業

注1）一般に①を「定常作業」②を「非定常作業」③を「異常処置」と区分することが多いのですが、それぞれを区分する論理はなにか？という問に明確に答えたものを見たことがありません。論理が明確でないため定義が企業や業態により異なる「定常作業」「非定常作業」「異常処置」といった言葉の安易な使用は混乱を招く原因になりますのでここでは極力使用しません。みなさんも注意してください。

注2）これらの作業については手順が定められて教育・訓練がなされているものもあれば手順が定められてないものもあります。

一般に手順が定められて教育・訓練がなされておれば「安全は確保されている」と考えられがちですが（リスクアセスメントにおいてこのような判断基準を採用している企業は結構多い）、品質や設備の異常が生じた時に「生産効率の低下を防ぎたい」との思いから、定められた手順を省略したり、危ないとわかっている作業（安全装置の無効化を含む）を行ったりして被災した（重篤な障害）事例は多々あります。国際安全規格ではこれらは合理的に予見可能な誤使用として対策をとることを求めています。**「手順を定めて教育・訓練を実施しているので安全は確保されている（リスクは低い）」という判断基準を設けるのは危険（間違い）**です。

注3）①②は場所とこれに対処する作業が決まっていますが、③の「品質あるいは設備の異常」については発生する場所が不特定で対処する作業も決まってない場合が多くあります。

この場合に「そのような機械の可動部に接触する作業はない／しない（その部分で品質あるいは設備の異常は起こらない）」として危険源リストに挙げずなんの対策も取らないで放置した危険源での重大事故・災害が結構発生しています。

「作業（保全担当者を含む）は、保護方策がない限り必ず危険源・危険区域に接近・侵入する」との前提に立ってリスクアセスメントを行うことが大切です。

人が稼働している機械に関与する作業は下記の各段階で生じるので、まずは各段階におい

てこれらの作業を抜けなくリストアップすることが重要です。

- ①設備受け入れ時の調整運転段階
- ② 日々の始動、立上げ段階
- ③ 定常運転段階
- ④ 立下げ段階
- ⑤ 保守（メンテナンス）段階
- ⑥ 異常処置段階
- ⑦システムの改造・更新段階

上記をもとに「設備仕様書」とは別に「安全要求仕様書」としてユーザーからメーカーに提示すべき項目・要件を5W1Hに従い表3-1にまとめましたので、参考にしてください。

表3-1「安全要求仕様書」として提示する項目・要件(参考)

	作業、設備	法規制の有無
設備・作業の目的 (Why)	・設備本来の使用目的（最終製品の物性・形状・品質、生産量）： ・設備の移動・搬送、組立、調整等の有無、目的、内容： ・異なる用途での設備使用・転用の可能性：	
使用場所、環境 (Where)	・設備の設置（作業）場所（屋内、屋外）： ・設備の設置（作業）環境（温度、湿度、騒音、風雨）： ・設備可動範囲内およびエミッション源／電源近傍での運転／保全作業（部品、治具の交換を含む）： ・作業空間（広さ、高所、視認性）の制限：	作業環境(管理濃度、騒音、照度)
誰が（何人で） (Who)	・作業人数： ・熟練度： ・共同作業の有無： ・第三者が存在する可能性：	法定資格者
設備の寿命、作業タイミングの制約 (When)	・寿命及び補修までの猶予（希望）期間： ・希望する作業形態、時間（連続、非連続）： ・人がかかわる操作に必要な余裕度（時間）：	法定点検
使用原材料、道具、治具(What)	・原材料／中間製品の物性・形状： ・提供可能なユーティリティ： ・人が用いる治具・道具に対する要求（重量、形状、操作性等）：	使用規制、届出、定期検査
どのような行動（操作・作業）をする (How)	・作業姿勢： ・予見可能な誤使用：	

ここではこれ以上「安全要求仕様書」の内容についての説明はしませんが、安全技術応用研究会で作成した（私も参加）『安全要求仕様書』の手引きに「安全要求仕様書」の目的、具体的内容について詳細に記載されています。参考にされたい方は安全技術応用研究会にお問い合わせください。

ステップ2 危険源の同定

国際安全規格の附属書 B1, B2 では様々な種類（機械的、電氣的、熱的 等）に分けた危険源が解説されています。危険源の同定は一般にこの附属書 B1, B2 の表を用いて該当する危険源がないか調べる（同定する）というやり方が行われていますが、この方法を実際にやってみると次のような問題に直面します。

- （1）機械の図面と附属書 B1, B2 とを見比べながら「この部分が危険源に該当する」と同定するにはかなりの経験を必要とする。経験の浅い設計者には荷が重い。
- （2）特に重度の危害を与える重要危険源の見逃しが生じていないかどうかの客観的な確認方法がない。これもかなりの経験を積まないと見逃す可能性があるので経験の浅い設計者にやらせる場合は経験豊富なベテランがその内容をチェックする必要があります。

附属書 B1, B2 に記載されている危険源は表面的な形態は異なりますがすべてエネルギーです。「危害を引き起こす潜在的根源」とは「エネルギー」、すなわち「エネルギーが危害を引き起こす根源」です。生産現場で用いられるエネルギーは電気、蒸気、圧縮空気のようにユーティリティとして供給されます。そして、各ユーティリティの使用先は図面に記載されています。すなわちユーティリティの図面に記載されている使用先と附属書 B1, B2 を見比べることにより、重要危険源の見逃しを防ぐことができます

ステップ2-1 ユーティリティ追跡法（Utility oriented Hazard Identification Method : UHIM（別名「T-I法」）による危険源の同定

「2-2 危険源とは」で述べたように危険源は特別なものを除きエネルギーです。生産現場で使用されるエネルギーは図 3-8 のように電気、蒸気、圧縮空気のようなユーティリティとして供給されます。

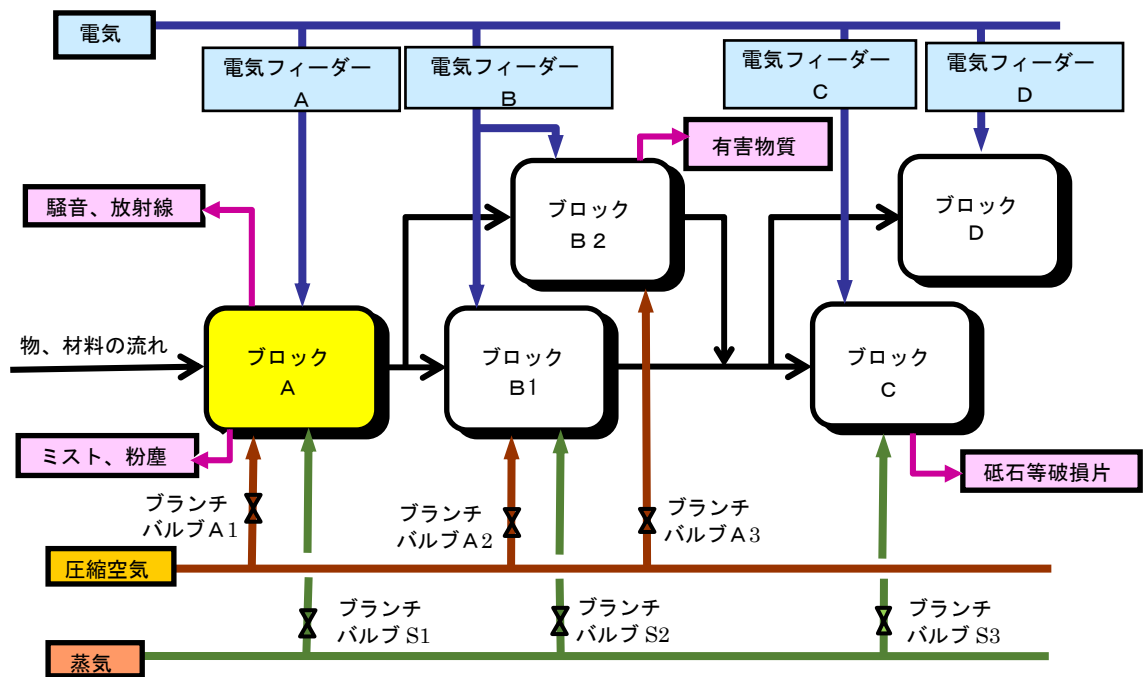


図3-8 設備の各ブロックへのユーティリティの供給

ユーティリティとして供給されたエネルギーが「3-2 危険源とは」で述べた【有効なエネルギー】、【無効なエネルギー】にどのように変換されて危険源となるのかを電気エネルギーについて示したのが図 3-9 です。

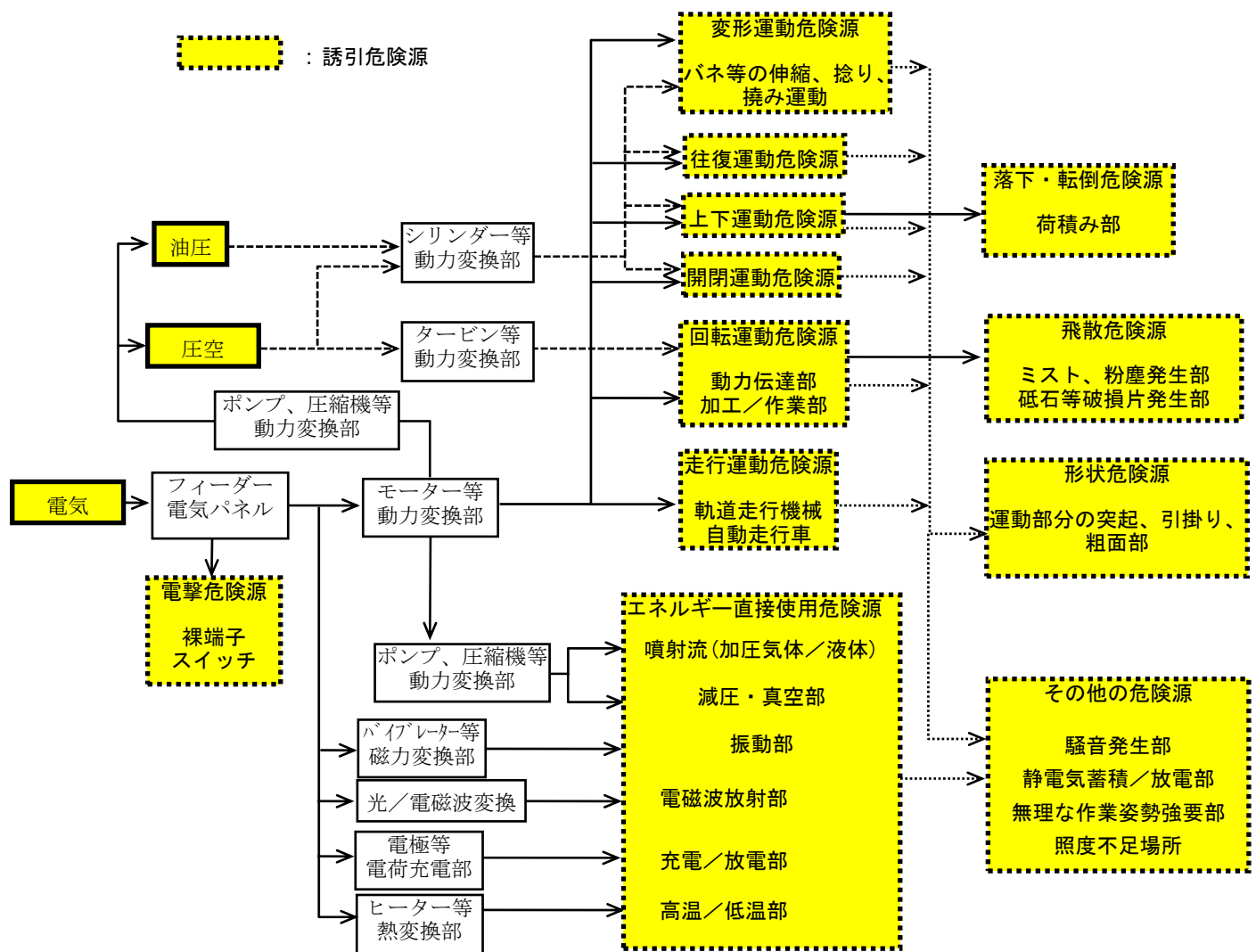


図3-9 電気エネルギーの流れと誘引される危険源との関係

ユーティリティはユーティリティ線図（電気配線図、蒸気配管図、空圧配管図、油圧配管図 等）にその使用先（モーター等動力変換部、パイプレーター等磁力変換部、光/電磁波変換部、ヒーター等熱変換部 等）が記載されています。そこでユーティリティ線図を用いてその使用先の一つ一つを「エネルギーに起因する危険源の候補」としてリストアップし（チェックリストを作成）、これが危険源（特に大事な重要危険源）になるのかどうかを国際安全規格の附属書 B1, B2 等を参考に調べることで抜けのない危険源の同定ができます。

電気（動力）配線図の例を図 3-10 に示します。赤丸のついている電気の変換部（配電盤、分電盤）及び使用先（モーター、ヒーター等）が危険源の候補になります。

配電盤、分電盤、電灯盤、制御盤を赤点線で囲ってありますが、これは図 3-9 のフィーダー、電気パネル（電撃危険源）に該当することを示すためです。

つのブランチバルブから供給されるのが基本です。(図 3-8 設備の各ブロックへのユーティリティの供給 参照)

同一ブロックに複数の供給元からエネルギーが供給されると、一つの供給元を停止させてもブロック内の機械で停止しないものが存在することになるので危険です。そこでユーティリティ線図を用いて、一つのブロックに対して供給される電気、油空圧、蒸気等のユーティリティが一つの電気パネル、一つのブランチバルブからしか供給されないようになっているのかどうか（一つのブロックに複数の電気パネル、ブランチバルブからのユーティリティが供給されていないかどうか）を調べ（図 3-11 に示すようにブロック A への電気、圧縮空気の供給例参照）、供給元が複数ある場合は一つに統合（一元化）することが肝要です。

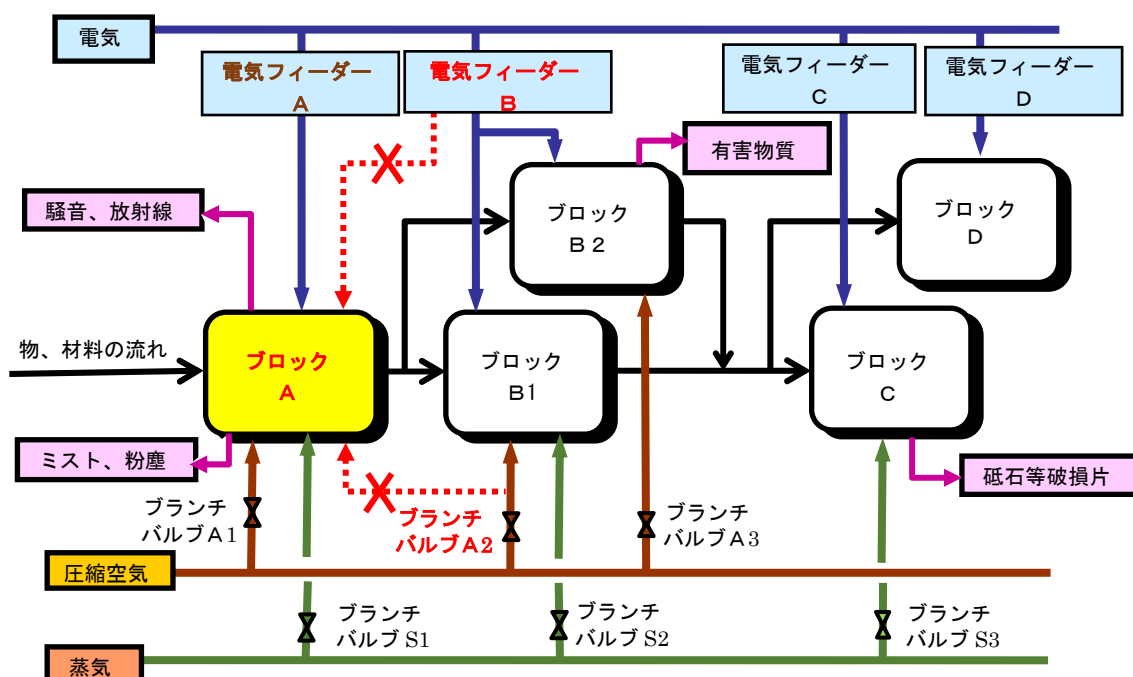


図3-11 設備の各ブロックへのユーティリティの供給

ステップ3 リスクの見積り

リスクの見積もりは、一般的には ISO 12100 に従い、図 3-12 のように「危害のひどさ」と「危害の発生確率」の2つの指標を組み合わせることで評価されます。このうち「危害の発生確率」は、「人の危険源への暴露」「危険事象の発生」「危害の回避又は制限の可能性」の3つの指標で構成されます。

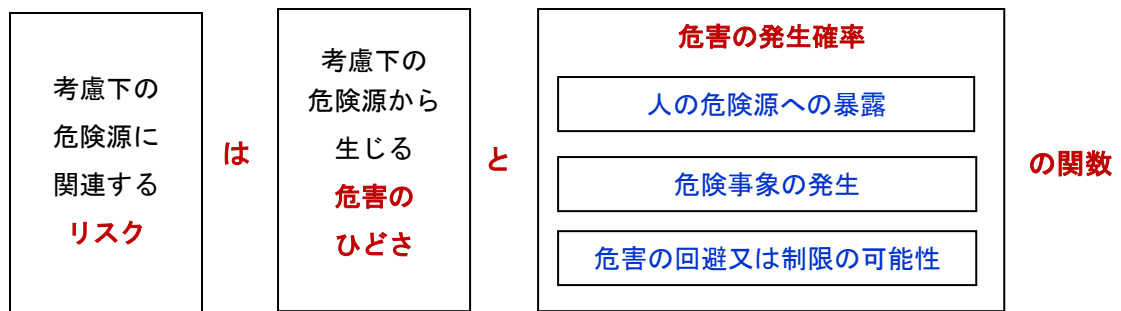


図3－12 ISO 12100 で示されるリスク評価の要素

以下、「危害のひどさ」及び「危害の発生確率」（「人の危険源への暴露」、「危険事象の発生」、「危害の回避又は制限の可能性」）のそれぞれについて、どのような評価基準にすればよいのか、私の考えを述べます。

ステップ3－1 「危害のひどさ」の評価

「危害のひどさ」については一般に「致命傷」「重傷」「軽傷」（「微傷」）といった3～4段階に分けているケースが多くみられます。ここでの問題点は、「重傷」「軽傷」といった名称のそれぞれがどういう状態を指すのかの定義があいまいなために判定者によるバラツキが大きいということです。

この問題点を解消するために私は、

「危害のひどさを日常生活あるいは会社生活（仕事）に影響する度合いで区分する」

ことを推奨します。（第2部 2. どうすればリスク評価のバラツキを少なくできるのか (2) 危害のひどさ（傷害の程度）〔S〕 参照）

この場合の障害の程度を細分する判断基準は下記3点です。

- ①被災したばあい、日常生活あるいは会社生活に影響する機能障害になるのか
- ②機能障害になった後、治療を受けることで日常生活あるいは会社生活に復帰できるのか
- ③治療を受けている間あるいは治療終了後も介護を必要とするのか

上記判断基準に従った場合の分類を図3-13に示します（第2部 2. どうすればリスク評価のバラツキを少なくできるのか (2) 危害のひどさ（傷害の程度）〔S〕 の図2-1再掲）。

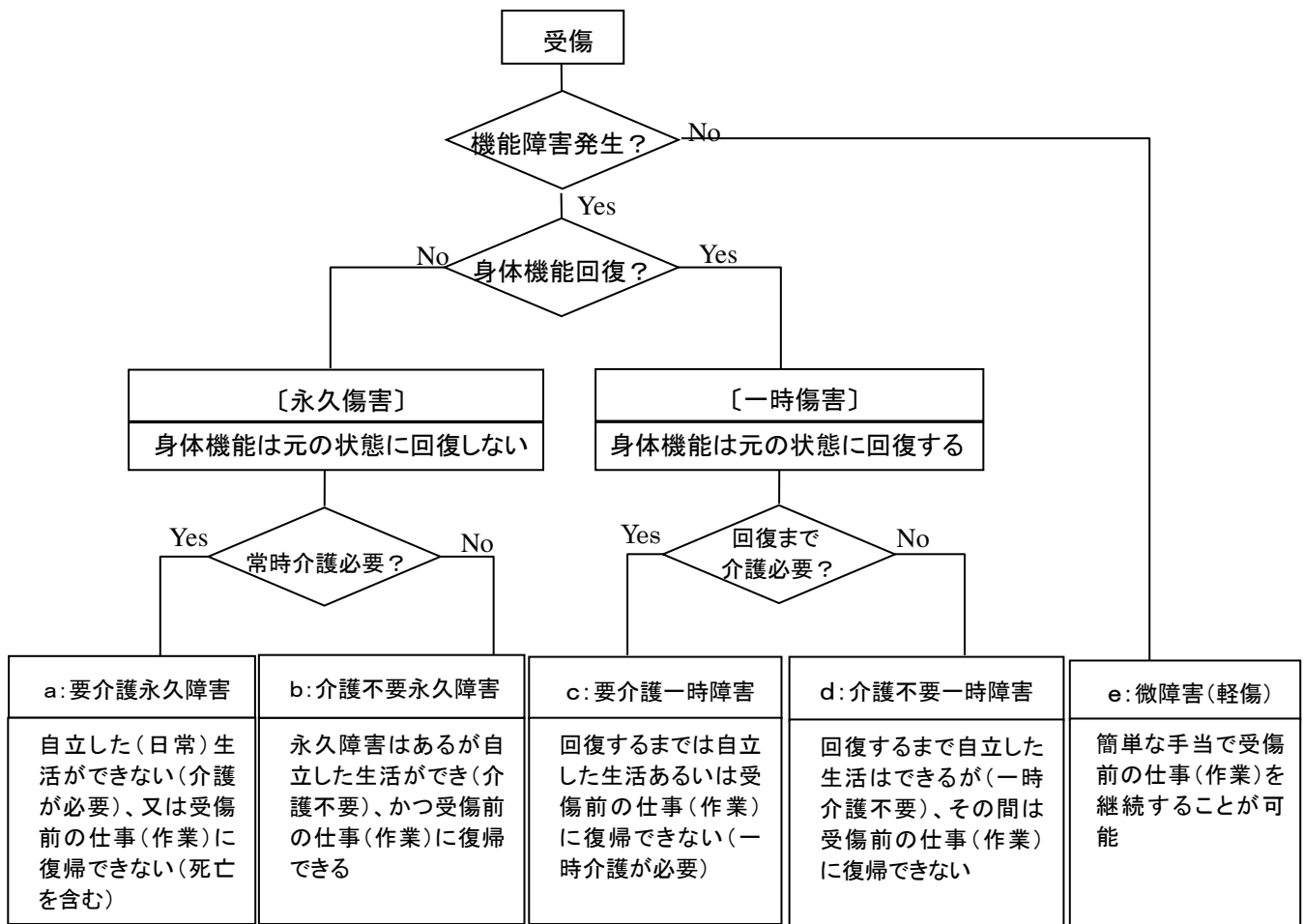


図3-13 危害のひどさの区分

この分類に従えば図 3-13 のように「危害のひどさ」は 5 段階に分類されます。これをそのまま使用するか、それとも一般に使用されている 4 段階（「致命傷」「重傷」「軽傷」「微傷」）にまとめるのか、についてはそれぞれの会社で自主的に決めていただければと思います。

図 3-13 の区分に従えば、身体の中のどの部位にどの程度の障害を受けた場合どの区分になるかを判断することができます（表 3-2 参照）

例えば、厚生労働者の「害補償保険法施行規則 別表第一」に示される障害等級は、表 3-2 の a, b に該当することがわかります。

表3-2 各区分への障害等級の割り付け(例)

区分	a	b	c	D	e
障害の レベル	後遺障害等級 1～13 級に該当 (頭部・胴部・ 脚・腕の骨折・ 内部損壊)	後遺障害等級 14 級に該当 (足指・手指 の複雑骨折)	後遺障害に該当 せず (頭部・胴部・ 脚・腕の単純骨 折、内臓打撲)	後遺障害に 該当せず (上肢、下肢 の単純骨折)	後遺障害に該当 せず (表皮、及び表 皮に近い肉の損 傷)

しかし、危険源のどのような状態（エネルギー、形態）に対してどのような姿勢で被災するかによって表 3-2 のどの区分の障害になるかは、表 3-3 に示すように各種危険源の持つエネルギーと被災（人体）部位の脆弱性により決まるものであり、詳細に検討しなければ決めることができません。

表3-3 危害のひどさを判断する際に考慮すべき要素(例)

事故の型（例）	危害のひどさを判断する際に考慮すべき要素	
	危険源	人
挟まれ、 巻き込まれ	・回転エネルギー ・回転体の形状（大きさ） ・表面形状（凹凸、摩擦係数、硬度） ・挟まれ、引き込まれ隙間	・人体の部位（頭、胴体、手、足、指）
墜落・転落	・高さ（位置エネルギー） ・落下して当たる場所の状態（硬い／柔らかい、液体／個体／粉体等）	・転落時の姿勢（転落方向） ・落下して当たる身体部位（頭、腰、足、手等）
飛来	・危険源の保有エネルギー（重量、飛来速度） ・大きさ、形状（塊、粉等）、硬度	・当たる身体部位（目、手、胴体 等）
高温物との 接触	・温度 ・高温物（液体・気体・個体）の熱容量 ・接触時間 ・接触の形態（物に接触、液体・気体を浴びる）	・接触の身体部位（目、手、全身等）

(安全技術応用研究会 橘良彦氏資料を基に作成)

設計者が表 3-3 に掲げた要件をすべて把握・検討した上で当該危険源にかかわる作業において生じる危害のひどさを決定するためにはかなりの知識と経験を要します。そのため設計者個々人の能力に依存して危害のひどさを判断させるようにすると必ず設計者によるばらつきが生じ、その結果、社内で使用する機械の安全レベルが設計者により異なってしまう、という大きな問題を抱えることになり好ましくありません。

そこで推奨するのが、区分は図 3-13（表 3-2）に従うが、危険源の種類毎に、危険源の持つエネルギーと被災部位を考慮して表 3-4 のように定量的な値を設定する（決める）というやり方です。

表3-4 危険源のエネルギーと被災部位を考慮した危害のひどさの判断基準(例)

危害のひどさ の区分 危険源での 被災状態区分	死亡・致命傷 永久機能傷害 (区分 a)	重傷 永久機能傷害(区分 b) 一時的機能傷害(区分 c)	中傷 一時的機能傷害 (区分 d)	軽傷 軽微な傷害 (区分 e)
挟まれ・巻き込まれ (被災部位)	頭部・胴部・脚・腕 の骨折・内部損壊	足指・手指の複雑骨折 頭部・胴部・脚・腕の単 純骨折、内臓打撲	足指・手指の単純 骨折	表皮、及び表皮 に近い肉の損 傷
墜落・転落 (高さ)	h_1 m 以上	h_2 m 以上～ h_1 m 未満	h_3 m 以上～ h_2 m 未満	h_3 m 未満
重量物との激突 (重量)	w_1 kg 以上	w_2 kg 以上～ w_1 kg 未満	w_3 kg 以上～ w_2 kg 未満	w_3 kg 未満
飛来・落下物との接触 (重量)	m_1 kg 以上	m_2 kg 以上～ m_1 kg 未満	m_3 kg 以上 ～ m_2 kg 未満	m_3 kg 未満
高熱物との接触 (温度)	t_1 °C 以上	t_2 °C 以上～ t_1 °C 未満	t_3 °C 以上～ t_2 °C 未満	t_3 °C 未満
感電 (電圧)	220V 以上	110V 以上～220V 未満	24V 以上～110V 未満	24V 未満

注 1 挟まれ・巻き込まれ危険源については、表 3-2 に示す被災部位で区分

注 2 挟まれ・巻き込まれ以外の危険源については、各々の危険源が持つエネルギーの大きさを表す指標（重量、温度 等）で区分。

各々の危険源においてどの部位を被災するのは人が危険源に暴露する形態（作業内容）により異なるが、ここでは同じ条件下でも被災の程度が大きくなる被災部位の代表として「頭部」「胴部」を選定。

注 3 表中の w_1 ～ w_3 、 m_1 ～ m_3 、 t_1 ～ t_3 については、参考資料があればそれを参考に、ない場合は適当な仮定をおいて設定する。いずれにおいても各社で自主的に決める。

（例として、感電に関しては「安全システム構築総覧（増補改訂版）安全技術応用

研究会 編著」を参考にした値を記載してある)

なお、「仮定」は定期的に見直し、必要に応じて基準の改定を行うことが必要。

個々の定量的な数値を「信頼のおける参考資料のない状態で設定する」というやり方なので戸惑うかもしれませんが、このように定量的に判断する基準にしておけば設計者によるばらつきが生じることはありません。これがこの方式の第一の狙いです。この場合、知識と経験が豊富な設計者を集めて $w_1 \sim w_3$ 、 $t_1 \sim t_3$ 等を決めるようにするとともに、どういう考えに基づき数値を決めたのか（「多数決で決めた」でもよい）を文書化しておく、そして定期的に、あるいは事故・災害が発生した時には必ず見直すように制度化しておけば（これが重要）見直すたびに数値の根拠が少しずつ明確になり客観性を持ってくるようになるので、社内の関係者全員が納得できる評価基準に進化する、というのがこの方式の第二の狙いです。

ステップ3-2「危害の発生確率」の評価

「危害の発生確率」は、図 3-14 に示す a.b.c.の 3つの指標で評価されます。

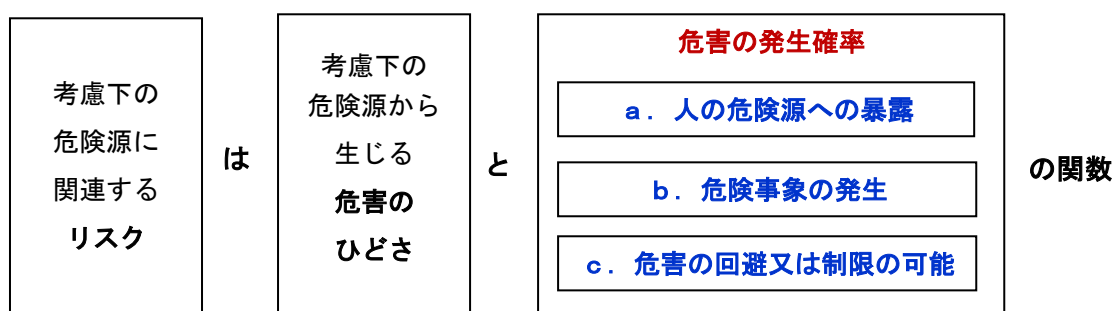


図3-14 ISO 12100 で示されるリスク評価の要素(再掲)

一方、危害は図 3-5 のプロセスで発生するとされています。

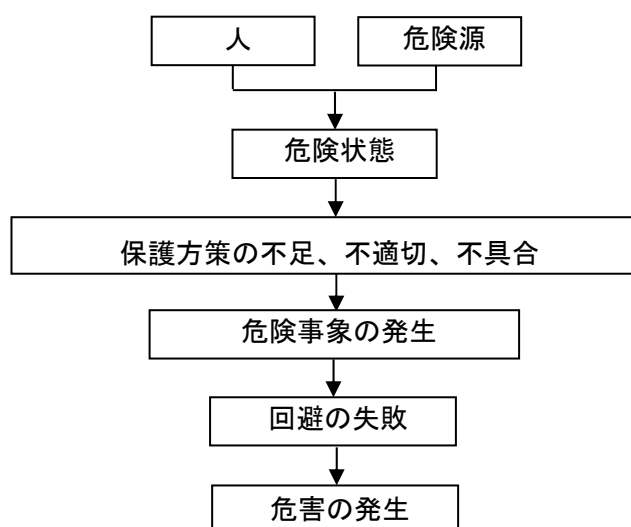


図3-5 危害の発生プロセス(再掲)

図 3-5 より、「危害の発生確率」は「危険源に暴露し、回避できないときに危険源に挟まれ巻き込まれたりして被災する確率（可能性）である」と解釈されていると思いますが、「危険源とはなにか?」「危険源に“暴露する”“回避する”とは具体的にどういう状態をいうのか?」ということを論理的に理解した上で検討しないと「危害の発生“確率”」といった、わかったようでわからない“確率”という言葉に振り回されて実用的な判断基準にならなくなるので注意が必要です。

このホームページでは生産現場でもっとも数が多く、かつ重大災害を引き起こしている生産設備（機械設備）に、また、対象とする危険源は「3-2 危険源とは」で述べたように下記のエネルギーに限定しています。

- ① 【エネルギー源】：電気、蒸気、化学物質 等 人に危害を与えるエネルギーそのものの
- ② 【有効なエネルギー】：①のエネルギー源が生産に必要な別のエネルギー形態（回転、往復動 等）に変換されたもの
- ③ 【無効なエネルギー】：①②のエネルギーが（粉塵、放射熱、騒音 等）別のエネルギーに変換されて環境に放出されたもの

上記のことを踏まえたうえで「危害の発生確率」に用いられている3つの指標 a.b.c.について考察します。

これら3つの指標については本ホームページの第1部 現行リスクアセスメント手法の問題点とその原因で述べたように次のような問題を持っています。

(1) 3つの指標が「危害の発生確率」に関与する割合

3つの指標が「危害の発生確率」に関与する割合は同等なのかどうか、また、それぞれは独立して関与するのか（相互に関連していることはないのか）、ということはどこにも言及されていません。

(2) 指標：「人の危険源へ曝露の頻度や時間」

(2-1) 用いる保護方策との関係

「人の危険源への曝露頻度や時間」は用いる保護方策の種類（安全を確保する能力）により大きく変わり、保護方策がしっかりしていれば危険源・危険区域に人が侵入する（暴露する）ことはできません。すなわち「人の危険源への曝露の頻度や時間」は保護方策の種類（安全を確保する能力）で評価できる、言い換えれば、保護方策が有する安全を確保する能力に置き換えることができる、ということになります。

(2-2) 作業内容・条件による曝露頻度・時間の変動

「人が危険区域に侵入することはない」と評価して保護方策を実施しなかった危険区域に人が侵入するのは、本来の作業（段取り、保守、教示等を含む）に

はない異常処置（予見される誤使用）が主です。（例：何らかの原因でたまたま生じた材料の位置ずれをガードのない場所よりちょっと手を出して修正する）

このような作業は工程の安定度に左右され、もともと想定されてないか又は想定されたとしても「頻度の非常に低い作業」なので、これらについては危険区域への暴露頻度・時間は非常に低いと評価されます。そのため危害のひどさが致命傷、重傷でも「リスクは低い」として無視される可能性があります。また、このような作業は仮にあったとしても、作業内容・条件は都度異なるので頻度・時間は一定せず暴露頻度・時間を定量化することはできません（機械の新設時に異常処置頻度を「1時間に1回」とか「1年に1回」といったように設定する設計者はまずいないでしょう。）

上記(2-1),(2-2)より「人の危険源へ暴露の頻度や時間」を「危害の発生確率」の評価指標として用いるのは好ましくない、ということになります。

(3) 指標：「危険事象の発生」

「危険事象の発生」は一般に

- ①機械本体、制御装置、機械部品等の信頼性
- ②災害や健康障害履歴
- ③類似機械とのリスクの比較

といった項目を勘案して確率（可能性）が「高い」～「低い」を評価する、とされています。しかし、

- ・「災害や健康障害履歴」は同一の機械を設計するのであれば過去のデータが参考となりますが、異なる仕様、異なる保護方策の機械に関しては参考となりません。
- ・「類似機械とのリスクの比較」も類似機械が存在し、そのリスクが明確になっていれば参考となりますが、新規機械については類似機械がない場合があるし、たとえ参考とする類似機械があったとしてもその評価が現在検討中の機械についても当てはまるかどうかをしっかりと検証した上でないと参考にできません。

これらのことを考えると、「**危険事象の発生**」は**機械本体、制御装置、機械部品等の信頼性を基に評価するのが適切である**、ということになります。この場合の「機械本体、制御装置、機械部品等の信頼性」とは、具体的には用いる保護方策が安全を確保する能力です。すなわち、「危険事象の発生（確率）」も「人の危険源への暴露の頻度や時間」と同じく用いる保護方策の種類（安全を確保する能力）により評価できる、ということになります。

「暴露の頻度や時間」および「危険事象の発生（確率）」の両者とも採用する保護方策の安全を確保する能力と関係している（密につながっている）、ということは「暴露

の頻度や時間」と「危険事象の発生（確率）」をそれぞれ独立したものとして個別に評価することはできない、ということを意味しています。

(4)指標：「危害の回避又は制限の可能性」

「危害の回避又は制限の可能性」は人間の技能（運転技能・経験、危険事象を回避する俊敏性等）に依存した手段です。人が間違いを犯す確率は、その人が置かれた物理的、生理的、心理的（個人、集団）状況に依存しており、決してゼロにはならないだけでなく、その人の日々の体調や精神状態、また生産計画等により変動します。すなわち「危害の回避、又は、制限の可能性」に用いられる手段が危害の発生確率を低下させることのできる能力は低いだけでなくバラつきも大きい、ということであり、「危害の回避又は制限の可能性」を「危害の発生確率」の評価指標として用いるのは適切でない、ということになります。

これらを踏まえると「**危害の発生確率**」は、図 3-15 のように「人の危険源（危険区域）への暴露」および「危害の回避又は制限の可能性」を除いた「危険事象の発生（の可能性）」、すなわち「**用いる保護方策が有する危険事象の発生を抑止する能力のみで評価する**」のが良い、ということになります。これが私の推奨する方式です。

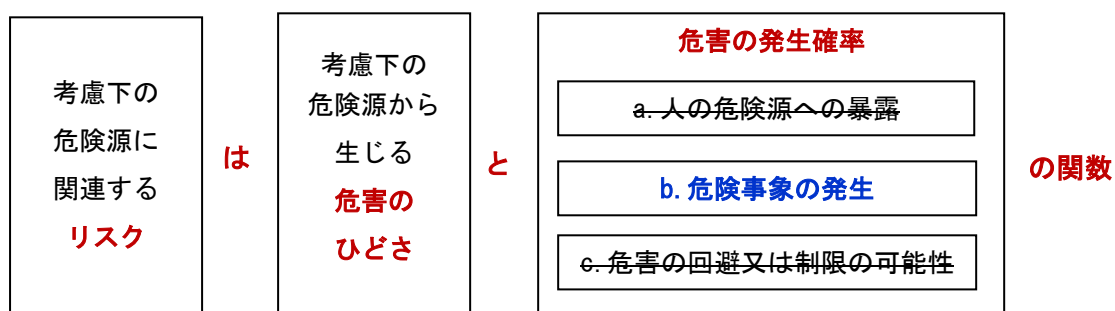


図3-15 推奨されるリスクの評価指標

ステップ3-3「危険事象の発生（の可能性）」の評価

(1)危険事象の発生（の可能性）とは

危害は図 3-5 のプロセスで発生するとされています。

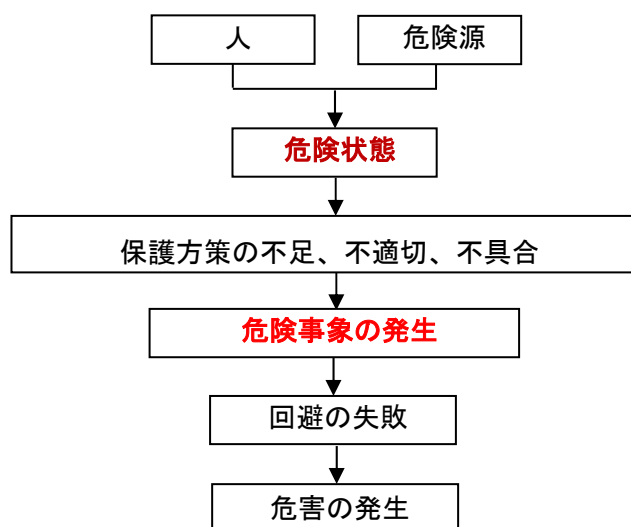


図3-5 危害の発生プロセス(再掲)

図 3-5 で「危険源に人が暴露することで危険状態が発生する」「この危険状態における人の被災を防止するために保護方策が採られるが、この保護方策に不足、不適切、不具合があると危険事象が発生する」と説明されていますが、これだとあいまいさが残ります。

危険源はエネルギーであり、「3-3 危険源の特徴」で述べたように

- ・ 危険源の持つエネルギーの及ぶ範囲（【危険区域】）は限定される。
- ・ 危険源の持つエネルギーの及ぶ範囲（危険区域）内に人が入ることで危険状態が発生する。

ということです。

この危険状態の発生を防止するための方策は、次の2つしかありません。

- ① 危険源のもつエネルギーをゼロにする ($H(\text{Hazard})=0$) または人に危害を与えることのない程度のエネルギーレベルにする ($H(\text{Hazard})\approx 0$)

危険区域に人が入る場合は、危険源への供給エネルギーを遮断（あるいは制限）するとともに危険源が保有しているエネルギーを人に危害を与えることのない程度のエネルギーレベル ($H\approx 0$) にまで低下させる。

- ② バリアを作るなどして人が危険区域に侵入できないようにする ($E(\text{Exposure})=0$)

危険区域に人が入ることができないように危険区域をカバーや安全柵で囲う。

確実に①②が達成できるかどうかは用いられる保護方策の能力（技術レベル）により変

化します。

すなわち、「危険事象の発生（の可能性）」は、保護方策が有する「危険源をなくす（ $H = 0$ ）または人に危害を与えることのない程度のエネルギーレベルにする（ $H \approx 0$ ）」能力あるいは「人の危険源・危険区域への侵入（暴露）を防ぐ（ $E = 0$ ）」能力で決まるということです。

注）国際安全規格の 3 ステップメソッドについて

国際安全規格では 3 ステップメソッドに従いリスクの低減を図るとされています。

ステップ 1：本質的安全設計方策の実施

ステップ 2：安全防護及び付加保護方策の実施

ステップ 3：使用上の情報の作成

気をつけていただきたいのは、この 3 ステップメソッドは下記のように安全設計の手順を示したもので、安全方策そのものの順位（優劣）を示すものではないということです。

・ステップ 1 の本質的安全設計方策

「生産に必要な機能・機構の中に安全を組み込んだ（余分な金をかけない）設計をしなさい」という意味であり、本質的安全設計方策に記載されている方策の一部を実施したからといって安全が確保されるものではありません。（例：作業者の身体的負担の軽減、誤操作の抑止を図るための「人間工学的（ボタンの配置、作業姿勢、照明 等）な対策」は本質的安全設計方策の一つですが、これを実施したからといって確実に安全が保証されるということにはなりません。）

・ステップ 2 の安全防護及び付加保護方策

「ステップ 1 の本質的安全設計方策だけでは対処できない危険源については、（余分な時間と金をかけても）安全に特化した防護策とその防護策が機能しない万が一の時に必要となる付加保護方策を実施しなさい」という意味です。

エネルギーである危険源のリスク低減は 3 ステップメソッドの順番（安全設計の順序）ではなく、次に述べる【本質安全化】、【隔離安全化】、【停止安全と隔離安全を組み合わせたインタロック化】の順序で検討する必要があります。

以下、この 3 つの方策について説明します。

I：【本質安全化】：

(1) 本質保護方策

危険源（エネルギー）を使用しない、あるいは、使用する場合は危険源の持つエネルギーを軽い打撲といった許容される被災の程度にまで低下させる。

(2) リスク予防設計

生産設備に採用する機械は、できるだけ危険源となる部位、範囲が少なくなるものを

選択する。

(1)は国際安全規格等の「本質的安全設計方策」の一つとして述べられているものです。

国際安全規格が規定している「本質的安全設計」と区別して「本質安全設計」と呼ばれることが多いのですが「本質安全設計」と「本質的安全設計」とがきちんと区別されずに使用されている事例が多くみられるので、このホームページでは混乱をさけるため「**本質安全設計**」の代わりに「**本質保護方策**」という言葉を使用しています。

これで対応できれば**危険事象は発生しない**ので理想ですが、生産設備においては危険源となるほどの大きなエネルギーを使用せずに生産できる設備は非常に少ない（ほとんどない）というのが現実です。

(2)はリスク予防設計と呼ばれるものです。

同一の製品を製造する機械設備でもメーカーにより危険源となる（エネルギーを与えられて可動する）部位の数に差があります。危険源となる部位の数が多ければ多いほど必要な保護方策の数が多くなり、コストアップになるだけでなく、生産時あるいはメンテナンス時には保護方策の解除等に要する時間が増え生産性を阻害することになります。**同じ機能を果たす機械の場合は危険源の数が少ない機械を選択することが重要である**、ということです。

(2)は危険源を完全に無くしてしまう「本質保護方策」ではありませんが、危険源そのものの数が減るという意味で私は【本質安全化】の範疇にいられています。

安全技術応用研究会ではこのリスク予防設計の重要性を啓発するために「Advanced Safety Design へのアプローチ ―リスクの少ない機械設計の提案―」と題した冊子を2017年に作成しました（私も作成に参加）。具体例も多数掲載していますので、参考にいただければと思います。

II 【隔離安全化】：

- (1) 人が危険源に接触できないように、危険区域をカバーや安全柵（固定式ガード）で完全に囲う。
- (2) 切り屑、騒音、熱、放射線、化学物質等を飛散させる危険源を図 3-16 に示すように完全に囲い込むことで危険区域を小さくする。

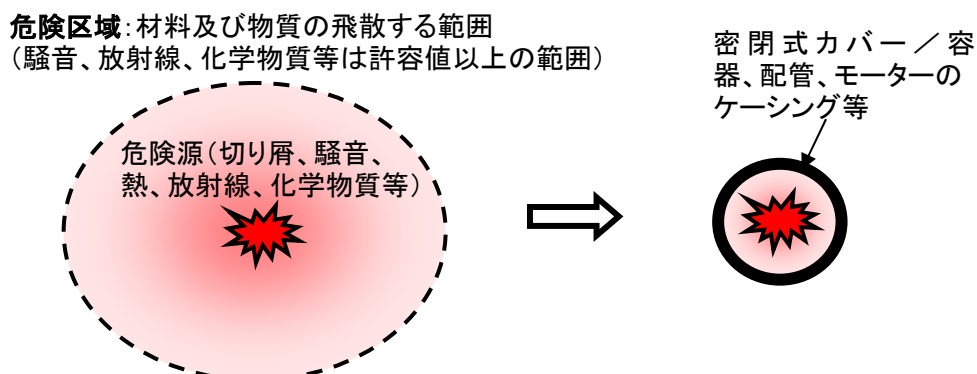


図3-16 危険源の囲い込みによる危険区域の縮小化

カバーや安全柵（固定式ガード）に必要とされる要件／注意点は、国際安全規格等に記載されており、規格の要件を満足すれば危険事象は（ほとんど）発生しないといえます。

Ⅲ【停止安全と隔離安全を組み合わせたインタロック】

原材料の供給、生産銘柄の変更、設備のメンテナンス等により、危険区域内に人が入らざるを得ない設備については、一般に次の①②の方策を組み合わせで安全を確保します。

- ① 隔離安全化された危険区域（設備）の一部に入口を設置して、人がこの入口から危険区域に入ろうとする状態をセンサ等で検知した場合は危険源へのエネルギー供給を停止する、もしくは、人が危害を被らない程度にまで危険源へのエネルギー供給量を低下させる（制限する）。
- ② 人が危険区域の中に存在してない（人が危険区域の外に出た）ことをセンサ等で検知した場合にのみ危険源へのエネルギー供給を開始／継続できるようにする。

上記①②を満足する保護方策は、図 3-17 に示すインタロックを組むことで構築されます。

図 3-17 のインタロックは下記 a. b. c. の 3 要素を組み合わせで構築されます。

- a. 検知要素（人が危険区域の中にいない）
- b. エネルギーの制限／遮断要素
- c. 監視要素（検知要素および制限／遮断要素が正常かどうかを監視）

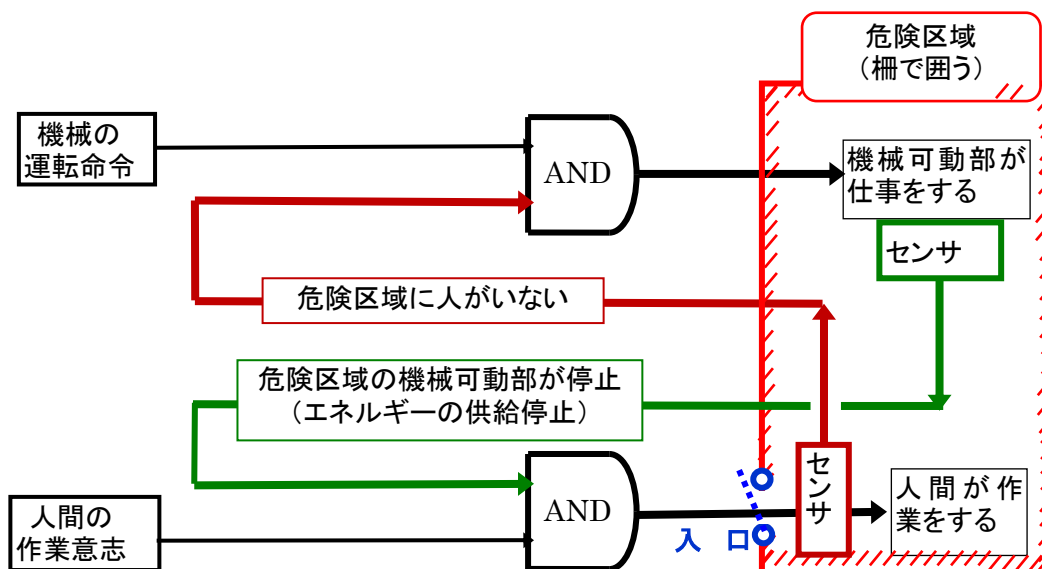


図 3 - 17 停止安全と隔離安全を組み合わせたインタロック

すなわち停止安全と隔離安全を組み合わせた保護方策においては、a. 検知要素、b. エネルギーの制限／遮断要素、c. 監視要素、で構築される安全制御システムが確実に機

能するかどうかの度合い（レベル）によって危険事象が発生する可能性が決まる、ということになります。

以下上記 a. b. c. で構築される安全制御システムが有する危険事象発生の可能性を評価する考え方として、下記 2 つについて説明します。

- i. a. 検知要素、b. エネルギーの制限／遮断要素、c. 監視要素の 3 手段とフェールセーフな要素で評価

安全制御システムを a. b. c. の 3 手段で構築しているか、また、これらに用いられる要素はフェールセーフであるか否かで評価する

- ii. 「安全確認型システム」および「危険検出型システム」をベースとした危険事象発生可能性の評価

a. b. c. の 3 手段で構築される安全制御システムが安全確認型であるかそれとも危険検出型であるかで評価する

i. は構造とそれを構成する要素の信頼性を基に評価する方式、ii. は「安全状態とはどういう状態をいうのか」「安全情報はどのように伝えなければならないのか」という論理に基づいた評価方式です。下記に説明したように考え方が異なるので評価のレベル分けに違いが生じます。内容を理解した上で選択していただければと思います。

i. a. 検知要素、b. エネルギーの制限／遮断要素、c. 監視要素の 3 手段とフェールセーフな要素で評価

上記 a. b. c. の 3 要素で構築される安全制御システムの信頼性は、国際安全規格においては P L（Performance Level）で評価されます。P L は「カテゴリ（安全制御システムの構造）」、「DC（危険側故障の検出率）」、「MTTFd（危険側故障を生じるまでの平均的な時間）」、「CCF（共通原因による複数故障の可能性）」を基に求められます。専門外の者（私もその一人）にとってこの内容を理解するのは大変ですが、簡単に説明すると下記ようになります。

【カテゴリ】

安全機能（検知要素、エネルギーの制限／遮断要素）の構成（一重系か二重系か、信頼性が高いか否か）および、監視機能の有無／チェック頻度、を指標として、表 3-5 のように B～4 の 5 段階に区分されます。

表3-5 安全制御システムのカテゴリ分類

安全カテゴリ	安全機能の構成	安全機能の監視機能	安全機能の維持能力
B	一重系	なし	部品に欠陥(故障)が生じると安全機能は維持されない
1	一重系(故障しにくい信頼性の高い部品を使用)	なし	同上、ただし欠陥(故障)は生じにくい
2	カテゴリ1と同じ	故障の有無の検出系(一重系)を組み込み、故障の有無を定期的(設備の始動時、サイクル開始時等)に検出する	次の故障検出までに欠陥(故障)が生じた場合は安全機能が維持されない
3	二重系(異種のものを組み合わせ)	故障の有無の検出系を異種の組み合わせによる二重系にして、故障の検出を常時行う	二重系なので故障が単一であれば安全機能は維持されるが、故障が複数になると維持されない
4	同上	同上、ただし故障の検出能力は安全カテゴリ3よりも高い	単一の故障に加え故障が累積しても安全機能が損なわれる確率は極めて低い

注) 国際安全規格におけるカテゴリの分類(オリジナル)は表3-6に示す通りですが、これだとわかりにくいので表3-5のように編集し直しました。

表3-6 安全カテゴリの分類と要求事項

カテゴリ	要求事項の要約	安全機能の維持能力
B	・機械制御システム安全関連部の目的機能を実現すること	・欠陥発生時、安全機能を損なう場合が十分起こりえる
1	・カテゴリBの要件を、満たすこと ・十分吟味された高信頼のコンポーネントを使用し、安全の確保は、安全原則に従うこと	・カテゴリBと同様であるが、安全関連部の安全確保機能の信頼性が高い
2	・カテゴリBの要件を、満たすこと ・安全の確保は、安全原則に従うこと ・安全機能は、適当な間隔でチェックされること	・安全機能の消失はチェックによって検出されるが、チェック間隔時間の間では、安全機能は損なう
3	・カテゴリBの要件を、満たすこと ・安全の確保は、安全原則に従うこと ・設計要件: 単一故障で安全機能を損なわないこと ・単一欠陥は、できる限り検出されること	・単一故障で安全機能は損なわれない ・すべてではないが、故障の検出ができる。未検出故障の蓄積によって、安全機能を損なう場合がある
4	・カテゴリBの要件を満たすこと ・安全の確保は、安全原則に従うこと ・設計要件: 単一故障は安全機能実行時、もしくはその前に、検出されること。これが実施できない時は、故障の蓄積で安全機能を、損なわないこと	・故障が生じた場合、常に安全機能は損なわれない ・故障は、安全機能実施の前の段階で安全機能実施が必ず間に合うように、予防措置として検出される

【D C】（危険側故障の検出率）

安全関連部に危険側故障（故障するとエネルギーが遮断できない、機械が止まらない）が生じた時にこれを検出して有効な対策を打てるかどうかの可能性（%）を示すパラメータで、全危険側故障率に対して検出できる危険側故障率の比率で表されます。

【MTTFd】（危険側故障を生じるまでの平均的な時間）

安全関連部が危険側故障を起こすまでにかかる平均的な時間です。

【CCF】（共通原因による複数故障の可能性）

共通、例えばある一つの原因によって複数の系統の安全関連部が損なわれてしまうような故障に対する耐性を示す指標です。

上記の内容を要約すると安全制御システムには次のことが要求されているということがわかります。

- ①故障しにくい構成要素（部品等）およびシステムを採用する
- ②故障の有無（正常に機能すること）を監視する
- ③故障しても危険側故障（機械が止まらない）にはならないようにする

①②を満足しない場合は故障の頻度が高くなり機械の止まる回数が増えて生産性が落ちるという問題は生じますが、故障しても危険側故障にはならない（故障した場合は必ず機械が止まる）③の対策ができておれば①②の対策ができてなくても安全は確保されるということがわかります。

③の「故障しても危険側故障にはならない方策」は「フェールセーフ」と呼ばれます。そのためには

- ・安全が確保されたことを示す情報（＝安全情報（エネルギー））を用いて機械の運転を開始／継続するシステムとする。（安全情報が伝わらないと機械は自動停止する）
 - ・機械の運転を許可する安全情報は、周辺に存在するノイズよりも高いエネルギーのものを用いる。
 - ・故障した場合は情報（エネルギー）が伝わらない物性を持つ（例：ヒューズ）材料を用いる
 - ・故障した部品及びその破片等により安全機能が妨げられることのない構造にする
- といった要件を満たす必要があります。

これらの要件については国際安全規格等に記載されていますが、現在国際安全規格では「フェールセーフ」という言葉を使用していません。「フェールセーフ」については下記を参照してください。

「産業安全分野におけるフェールセーフ技術」 梅崎重夫 安全工学 VoL4／ No. 3 (2002)

以上をまとめると、【停止安全と隔離安全を組み合わせたインタロック化】システムにおける危険事象発生の可能性は、次の2つの指標で評価することができます。

- ・検知要素、エネルギーの制限／遮断要素、監視要素を構築しているか
- ・それぞれの要素はフェールセーフな要素であるか

エネルギーである危険源による「危険事象の発生（の可能性）」は、保護方策が有する「危険源をなくす（ $H=0$ ）または人に危害を与えることのない程度のエネルギーレベルにする（ $H\rightleftharpoons 0$ ）」能力あるいは「人の危険源・危険区域への侵入（暴露）を防ぐ（ $E=0$ ）」能力で決まり、この能力を決める保護方策は【本質保護方策(本質安全化の一つ)】、【隔離安全化】、【停止安全と隔離安全を組み合わせたインタロック化】の3つに集約されます。

【本質保護方策（ $H=0$ or $H\rightleftharpoons 0$ ）】および【隔離安全化（ $E=0$ ）】は確定的に安全を保障しますので被災の可能性（危害の発生確率）はゼロです。すなわち、被災の可能性（危害の発生確率）が高いか低いかを決めるのは【停止安全と隔離安全を組み合わせたインタロック化】の構成が

- ・検知要素、エネルギーの制限／遮断要素、監視要素の3つを構築しているか
- ・それぞれの要素はフェールセーフな要素であるか否か

で決まるということが出来ます。

このことを踏まえると危険事象発生の可能性は図 3-18 のように4段階にレベル分けすることができます。

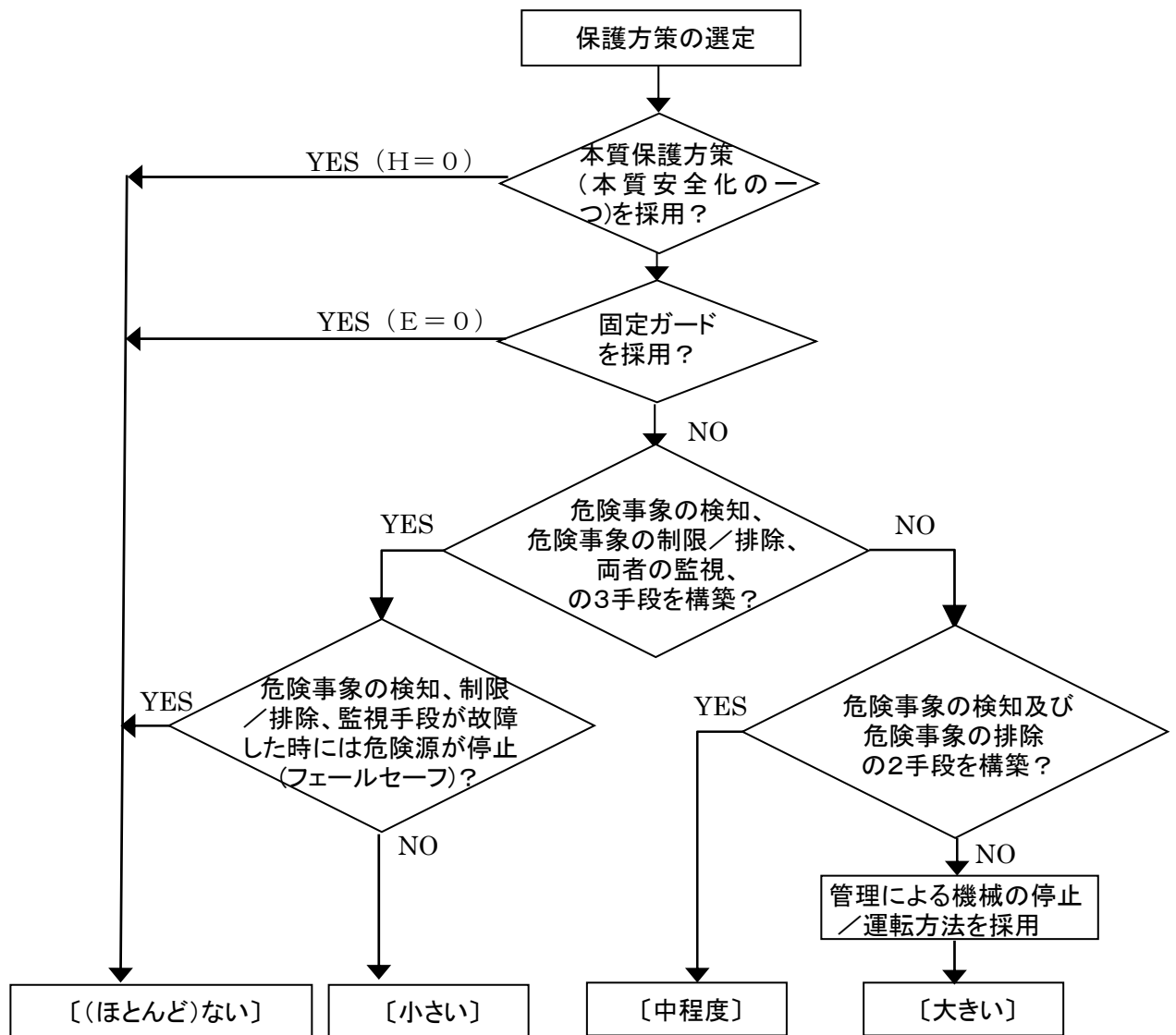


図3-18 【本質安全化】、【隔離安全化】、【停止安全と隔離安全を組み合わせ
たインタロック化】をベースとした危険事象発生の可能性

ii. 「安全確認型システム」「危険検出型システム」をベースとした危険事象発生の可能性 の評価

「安全確認型システム」「危険検出型システム」の詳細な説明は本ホームページの「確定的安全と確率的安全」に説明してありますので、これを見てください。

「安全確認型システム」「危険検出型システム」が安全を確保できるレベルは次のようになります。

①危険検出型システム：

人が危険源に曝露する危険な状態（危険区域への侵入）が生じてないか否かを確認

（検知）して、危険な状態の証拠が確認された時に危険情報をエネルギーの形で出して設備の運転を停止させるシステム

危険な状態の確認（検出）手段および危険回避手段を危険検出型のシステムで構築している場合、仕様どおりに製作・施工されておれば通常は $H=0$ 又は $E=0$ を実現できるが、危険な状態の確認（検出）手段あるいは危険回避手段が故障した場合は $H=0$ 又は $E=0$ にならないことがある。

②安全確認型システム：

人が危険源から隔離された安全な状態にある（人は危険区域の外にいる）かどうかを確認（検知）して、安全な状態の証拠が確認された時だけ安全情報をエネルギーの形で出して機械の運転を許可する。安全状態が確認できなくなった場合は安全情報（エネルギー）が自動的に途切れて機械の運転が停止してしまうシステム

安全な状態の確認（検出）手段および危険回避手段を安全確認型のシステムで構築している場合、仕様どおりに製作・施工されておれば $H=0$ 又は $E=0$ を確実に実現できるし、故障した場合は自動的に機械の運転が停止するので、いかなる場合でも安全が確保される。

【停止安全と隔離安全を組み合わせたインタロック化】を「安全確認型システム」か「危険検出型システム」かで評価する場合、危険事象発生の可能性は図 3-19 のように 3 段階にレベル分けすることができます。

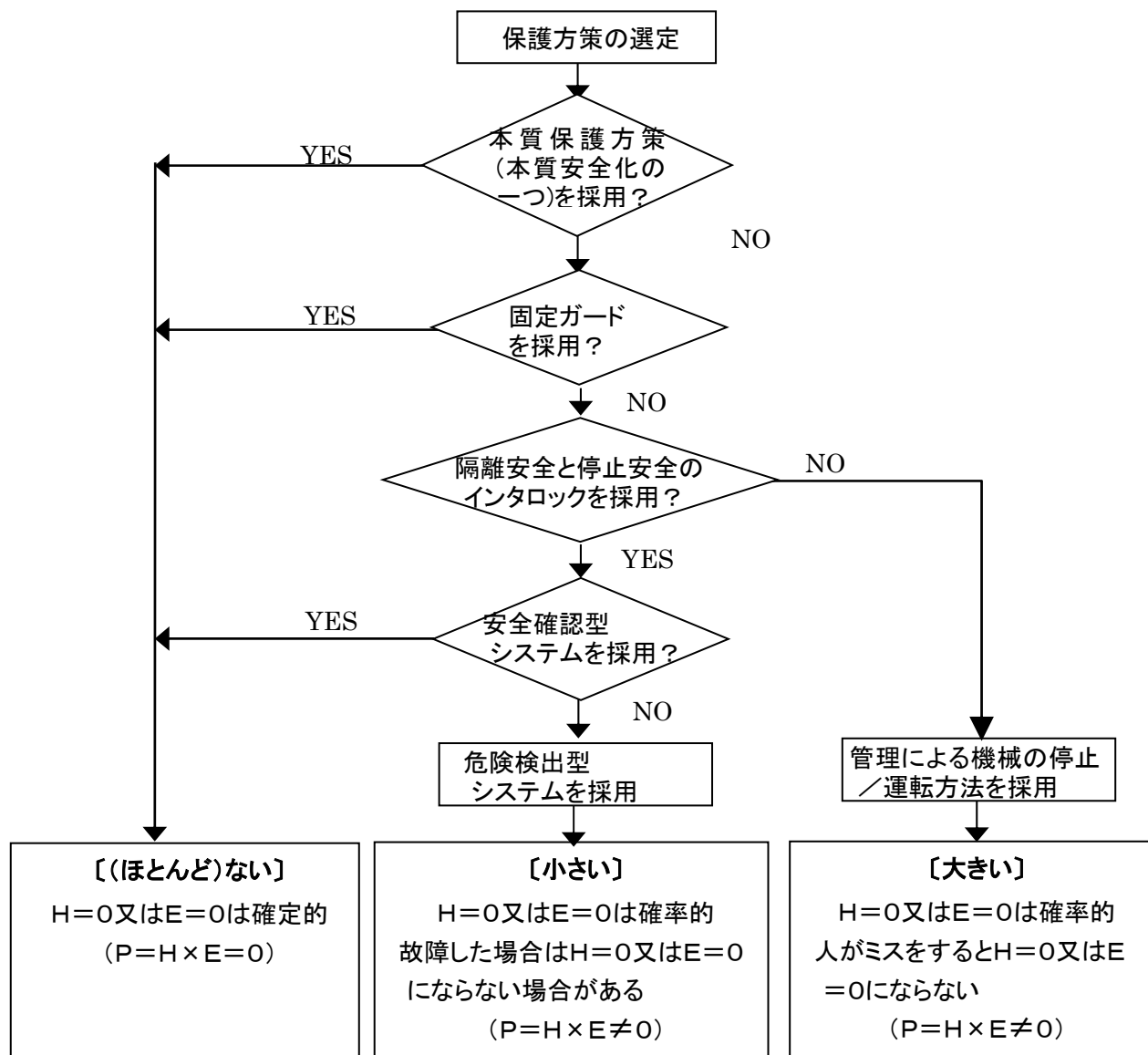


図3－19 保護方策に安全確認型又は危険検出型を用いた場合の危険事象発生の可能性

ステップ3-4 マトリクス法によるリスクの見積もり

これまで説明した内容から、リスクは「危害のひどさ」と「危険事象の発生（の可能性）」の二つを組み合わせることで評価できることが分かります。

この二つを組み合わせるリスクを評価する方法には「マトリクス法」「数値法（加算／積算法）」「ツリー法」がありますが、推奨するのは「マトリクス法」です。

世の中では「数値法（加算／積算法）」が多く採用されていますが、「**危害のひどさ及び被災の可能性（＝危険事象発生の可能性）**」の各レベルに**任意**の数値を与えても加算（積算）結果の値の大小が**合理的なリスク順位**を与える（私はこれを「数値法の神話」と呼んでいます）ことは決してありません。」

これについては

第2部：実用的なリスクアセスメント基準の構築に向けて

3. どのような手法でリスクを見積もり、リスクを評価すればよいのか（「数値法の神話」とは）

・本文 (1) リスクの見積もり方法〔定性評価、定量評価〕（「数値法の神話」）

に詳細に説明してありますので、これを見てください。

（ツリー法についてもその問題点を述べてあります）

(1) リスクの見積もりに使用する指標と各指標の評価レベル

リスクの評価指標である「危害のひどさ」「被災の可能性（＝危険事象発生の可能性）」を次のようにレベル分けします。

【危害のひどさ】

「表 3-44 危険源のエネルギーと被災部位を考慮した危害のひどさの判断基準（例）」に示した下記4つのレベル

「死亡・致命傷（永久機能傷害(区分 a)）」

「重傷（永久機能傷害(区分 b)および一時的機能傷害(区分 c)）」

「中傷（一時的機能傷害(区分 d)）」

「軽傷（軽微な傷害(区分 e)）」

【被災の可能性（＝危険事象発生の可能性）】

図 3-18 【本質安全化】、【隔離安全化】、【停止安全と隔離安全を組み合わせたインタロック化】をベースとした危険事象発生の可能性

に示した下記4つのレベル

〔(ほとんど) ない〕

〔小さい〕

〔中程度〕

〔大きい〕

(2) マトリクス法におけるリスク順位の決め方

「危害のひどさ」と「被災の可能性（＝危険事象発生の可能性）」の $4 \times 4 = 16$ の組み合わせについてリスク順位を決め、それを基に4つのリスクグループに分けるという作業を行います。

まずどのような考えでリスク順位を決めるのかですが、私の考えは下記の通りです。

- ・「被災の可能性(発生状況)」よりも「危害のひどさ」に重きを置いてリスク順位を決める（表3-7に茶色矢印で示す）
- ・「被災の可能性」が「(ほとんど) ない」の場合の保護方策は $H = 0$ 又は $E = 0$ が確定的なので（確実に安全が保障される）、「危害のひどさ」が「致命的」「重大」でもリスク順位は低い。（表3-7「(ほとんど) ない」の欄（青着色部）参照）

表3-7 マトリクス法によるリスク順位

危険事象発生の可能性 (被災の可能性)	危害のひどさ			
	死亡・致命傷	重傷	中傷	軽傷
大きい	⑬	⑭	⑪	⑧
中程度	⑮	⑬	⑨	⑦
小さい	⑫	⑩	⑥	⑤
(ほとんど) ない	④	③	②	①

ステップ４，５ マトリクス法におけるリスクの評価

(1) リスクレベルの設定

リスクレベルは

第２部：現行リスクアセスメント手法の問題点解消のための考え方

3 どのような手法でリスクを見積もり、リスクを評価すればよいのか（数値法の神話）

(2) リスクレベルの区分分け

に説明した下記４つのレベルに分けます。

「許容不可能」：使用者として絶対に受け入れられないレベル

「やむを得ず許容」：使用者として基本的には受け入れられないが、安全方策の技術上／コスト上の制約および本機械を用いて生産する製品に対する社会の要求等を考慮して止むを得ず受け入れるレベル

「許 容 可 能」：使用者として求める安全方策がすべて満足されているわけではないが、メーカーとしてやるべき安全方策は実施されており、仮に事故が生じてもＰＬ上は免責となるレベル

「広く受け入れ可能」：使用者として求める安全方策がすべて実施されているレベル

表 3-8 にリスクレベルの区分に応じてどのような対応(製作・使用)にするのかの基準例を示します。

表3－8 リスクレベルの区分に応じた対応(製作・使用)基準例

リスクレベルの区分		対応(製作・使用)基準
Ⅳ	許容不可能 (絶対に受け入れられないレベル)	〔製作、使用禁止〕 本リスクを有する設備は、いかなる事情があっても製作／使用しない
Ⅲ	やむを得ず許容 (止むを得ず受け入れるレベル)	〔マネジメントリスクを評価してリスクの責務を負う経営層が判断〕 製作／使用両者の事業責任者(経営層)が許可した場合に限り製作／使用が可能
Ⅱ	許容可能 (PL上免責対象となるレベル)	〔製作、使用OK(ただし、評価に間違いがないかを再チェックする)〕 設備の使用者側(製造ラインの責任者)が許可した場合は製作／使用が可能
Ⅰ	広く受け入れ可能 (使用者側が求めるレベル)	〔製作、使用OK〕 製作／使用に関して許可を受ける必要なし

注 1) 「やむを得ず許容」のレベルは災害が生じた時にマネジメントリスクが生じる可能性の高いレベルなので、【経営層が判断して許可する】という基準にしてあります。

注 2) マネジメントリスクの例については下記を見てください。

第2部：現行リスクアセスメント手法の問題点解消のための考え方

4. リスクの区分に応じた処置基準をどのように設定すればよいのか

(1) リスクレベルの対応(製作・使用)基準(会社のポリシー)の表2-3-2-2 マネジメントリスク 評価基準例

(2) リスク順位とリスクレベルの結びつけ

リスク順位はある程度機械的に決定できますが、これらの組み合わせを「許容不可能」、「やむを得ず許容」、「許容可能」、「広く受け入れ可能」の4区分にどのように振り分けるのか、ということに関しては注意が必要です。

なにも考えないでリスク順位とリスクレベルの振り分けを行うと、安全方策の技術上／コスト上の制約から機械そのものが作れなくなる（その結果社会が必要とする製品を供給できなくなる）などの問題が生じます。（このような問題が生じるので評価結果に例外を設けるあるいは補正を行うことでこの問題を回避するといった苦肉の策を用いてアセスメント規定を運用している企業があります。）

このような問題点が生じるのは、リスクの順位付けおよび区分分けをしっかりと検討していないためです。

表3-9 を見てください。

表3-9 マトリクス法によるリスク順位

危険事象発生の可能性 (被災の可能性)	危害のひどさ			
	死亡・致命傷	重傷	中傷	軽傷
大きい(危険事象の検知／排除手段なし、管理で対応)	⑬	⑭	⑫	⑧
中程度(危険事象の検知／排除手段あり)	⑮	⑬	⑨	⑦
小さい(危険事象の検知／排除／監視手段あり)	⑪	⑩	⑥	⑤
(ほとんど)ない(危険事象の検知／排除／監視手段はすべてフェールセーフ)	④	③	②	①

⑬⑮⑭の赤で表示した組み合わせを「許容不可能」のグループ（茶色の線で囲った範囲）にする。また⑤④③②①の白で表示した組み合わせは「広く受け入れ可能」におよび⑦⑥の青で表示した組み合わせは「許容可能」のグループ（青色の線で囲った範囲）に区分す

ることについてはそれほど問題ないと思います。

問題は枠を赤／黄あるいは黄／青に半分ずつ塗り分けてある⑬⑫⑪および⑩⑨⑧の組み合わせです。

⑬⑫⑪（赤／黄）：「許容不可能」にすべきかそれとも「やむを得ず許容」にすべきか

⑩⑨⑧（黄／青）：「やむを得ず許容」にすべきか、それとも「許容可能」にすべきか
これについては立場により意見が異なりなかなか決まらないと思います。

厳しいレベルに設定するのか緩やかなレベルに設定するのか、ここは会社の業態と安全に対する姿勢が反映される部分です。

特に⑬⑫⑪については事業を止めるのか（赤）それともマネジメントリスクを背負って
も生産に踏み切るのか（黄）を決めることになるので、安全担当部門、設計部門だけで決めることはできません。経営層も含めた事業組織として決める必要があります。

危険事象発生の可能性（＝被災の可能性）を「ii. 「安全確認型システム」「危険検出型システム」に記載した手法で区分したもの（図 3-19 参照）について、表 3-9 がどのようなものかを示したのが表 3-10 です。この場合も経営層も含めた事業組織として決める必要のある組み合わせが存在します。

表3-10 マトリクス法によるリスク順位
（「安全確認型システム」「危険検出型システム」による判断）

危険事象発生の可能性 (被災の可能性)	危害のひどさ			
	死亡・致命傷	重傷	中傷	軽傷
大きい(管理で対応)	⑫	⑪	⑩	⑦
小さい(危険検出型)	⑨	⑧	⑥	⑤
(ほとんど)ない (本質安全、安全確認型)	④	③	②	①

5. まとめ

本第3章は危険源がエネルギーであるものについてのリスクアセスメントについて説明したものです。冒頭でも述べましたが要約すると下記ようになります。

- （1）「機械類の制限の決定」においては、機械が使用される環境等を示した「設備仕様書」とは別に、ユーザーとしてどのような使い方をしたいのか、そのためどのようなことに配慮した機械にして欲しいのかといった要求を「安全要求仕様書」として作成してメーカーに伝えることが大切である。
- （2）「危険源の同定」においては、エネルギーに起因する危険源、特に重大な災害を引

起こす可能性のある重要危険源の見逃しを防ぐことが最重要課題である。そのためには、ユーティリティ追跡法（Utility oriented Hazard Identification Method：UHIM（別名「T－I法」））に基づきユーティリティ線図（電気配線図、蒸気配管図、空圧配管図、油圧配管図）を用いて「エネルギーに起因する危険源の候補」をリストアップしてから危険源同定を行うことが推奨される。

- (3) リスクは「危害のひどさ」と「危害の発生確率」の組み合わせで評価する。この場合、
- ・「危害のひどさ」は「生じた危害が日常生活あるいは会社生活（仕事）に影響する度合い」で区分することを推奨する。
 - ・「危害の発生確率」は「危険事象の発生（の可能性）」のみで評価することを推奨する。この場合、「危険事象の発生（の可能性）」は機械本体、制御装置、機械部品等の信頼性（用いる保護方策が有する危険事象の発生を抑止する能力）で評価するようにする。（これにより「危害の発生確率」を評価する指標とされている「人の危険源への暴露」および「危害の回避又は制限の可能性」は不要となる。）
- (4) 「用いる保護方策が有する危険事象の発生を抑止する能力」は【本質安全化】、【隔離安全化】および【停止安全と隔離安全を組み合わせたインタロック化】に区分できる。
- (5) 【本質安全化】あるいは【隔離安全化】の方策を講じれば確定的に安全は確保される。
- (6) 【停止安全と隔離安全を組み合わせたインタロック化】は、①危険状態の検知要素、②危険を検知した時のエネルギーの制限／遮断要素、および、③検知要素やエネルギーの制限／遮断要素が正常であるかどうかを監視する要素、の3要素が構築されているかどうか、および、それぞれの要素がフェールセーフな要素であるかどうかで評価できる。
- (7) 【停止安全と隔離安全を組み合わせたインタロック化】は上記の他にシステムが「安全確認型システム」かそれとも「危険検出型システム」かに区別することでも評価できる。
- (8) 「危害のひどさ」と「危険事象の発生（の可能性）」の二つを組み合わせで評価する方法として「マトリクス法」を推奨する。
- （「危険事象発生の可能性」の各レベルに任意の数値を設定して加算（積算）する「数値法（加算／積算法）」は誤った順位を示すことが多いので推奨しない。）
- (9) リスク順位は「危険事象発生の可能性」よりも「危害のひどさ」に重きを置いて決める。
- (10) 「危険事象発生の可能性」を【本質安全化】、【隔離安全化】、【停止安全と隔離安全を組み合わせたインタロック化】で評価する方式は、用いる保護方策が確実に安全を保障する場合を『被災の可能性』が『（ほとんど）ない』と評価する方式なので、「（ほとんど）ない」の区分に該当する場合は「危害のひどさ」が「致命的」「重大」でもリスク順位は低くなる。
- (11) リスク順位を基に「許容不可能」、「やむを得ず許容」、「許容可能」、「広く受け入れ

可能」の4区分に分ける時点で、どちらに区分すべきか迷う組み合わせについては会社の業態と安全に対する姿勢を反映して決定する。「やむを得ず許容」、「許容可能」に該当する組み合わせは、事故・災害が発生した時にマネジメントリスクを引き起こす可能性があるので、安全部門、設計部門だけでなく経営層も含めた事業組織として決めることが求められる。

第3部は国際規格に述べられているリスクアセスメントの内容を論理に基づき解釈するとともに各社が自社の方針に従い使いやすい基準を構築できることを目的として作成したものです。第3部で述べたリスクアセスメントのやり方は、一部を除いてどの組織・個人も言及していないものです。

国際安全規格は広い分野をカバーできるように規定してあるので、そのまま適用してリスクアセスメント規定を作成すると使い勝手の悪いものになる可能性があります。

リスクアセスメントは外部で学んだことをそのまま適用すればよいというものではありません。「ステップー3 危害のひどさ」や「ステップー4, 5 マトリクス法におけるリスクの評価」で述べたように、それぞれの会社がそれぞれの考えに従って決めなければならない内容があり、その中にはマネジメントリスクを引き起こす可能性があるものを含んでいます。中身をしっかり検討してマネジメントリスクの生じない（生じたとしても軽くて済む）リスクアセスメント基準を構築していただければと思います。

ここで説明した内容が各社のリスクアセスメント基準の構築および既存基準の改良に寄与できることを願っています。