リスクアセスメントの目的と停止カテゴリについて

長岡技術科学大学　名誉教授　杉本　旭

1. はじめに

リスクアセスメントの責任者は経営者である。なぜなら，やむを得ず結果として生じた労働災害（accident）に対する第一義的責任（被害者の補償・救済）を負うのは経営者であるからである。そこで，補償の可能性をリスクで表し，安全管理の最善を尽くしてリスク低減を図り，許容リスクを実現する。このように，許容リスクとは，経営者が負いうる責任に対する「許容」の判断だと考えることができる。一方，リスクアセスメントそのものの目的が停止カテゴリを決めることだというグローバルな安全にとって重要な点がわが国では十分理解されていないようだ。

もともと事故は，事故（事象）の前での停止の失敗で経験される。事故が起こった時，なぜ，もう少し早く止めなかったのか。事故は防ぐ，予防するというのでなく，事故の経験を拒否するという考えで“安全”があるということである。リスクは，単なる結果責任（補償の期待値）でなく，停止の失敗に対する責任と考えなければならない。経営者による許容リスクの判断を，被害者はそのまま許容事故として受け入れるわけではない。事故の可能性（リスク）が残る限り，特に，大きな被害が予測される作業では，労働者から，暗黙とはいえ，事故の前の停止に対する厳しい要求がなされると考えて当然である。しかし，残念なことに，この要求は事前には届かない。いつもそうだが，事が起こって再発防止の段階になって，事故の前の停止が軽んじられた不条理を思うのである。

“事故は，事故前の停止で防ぐ”とする安全の停止原則は，抽象的で具体性を欠くとされるリスク概念に事故を防ぐとする安全の魂が息づく。事故前の停止の失敗で生ずる被害がリスクであるとすれば，改めて停止手段（安全装置）の認証性の問題が生ずる。事故は，停止手段の危険側の誤りで生ずることになり，欧州では，安全装置の故障に対する事故前の停止の保証（フェールセーフ性）を停止カテゴリとして階層化し，リスクベースの安全が認証制度とともに施行されている。最高位の停止カテゴリでは，危険のとき停止するばかりでなく，停止手段（安全装置）が故障した場合，停止して修理を要求し，また，修理を完了しない限り停止が解除できないとする条件が叶って安全装置に認証が与えられる。わが国では事故を防ぐための基準を持たないため，主観的となって，許容リスクは普遍的安全の意味を持たない。一方，欧州では，“事故前の停止”を共通の原理として事故防止に共通の基準を定めており，改めて，リスク低減を事故防止に求める欧州の安全について，その基本とするところを考える。

2. 事故の責任と安全の責任

もともと安全は，事故の可能性に対して，リスクや信頼性など，確率論をベースとする予測手法が採られるが，事故が起こると，一変して，何が原因か誰の責任かというように，決定論の扱いとなって混乱を生ずる。重大責任が課せられるようなことを，事前に確率で扱うという安全の考え方そのものに混

乱の理由があると言っていい。

事故には責任が伴うが，原因調査を厄介なものにさせるのは，法律違反に対する責任（罰）の理由として原因を明らかにする必要があるからである。結果（事故）に対して何を原因とするかは，法律との関係で変わる。場合によっては，再発防止のキーとなるような客観的な原因とは全く別の理由が原因とされることにもなる。例をあげよう。

事故を防ぐために設置する安全装置は，もともと故障が許されない。故障は絶対には避けられないという現実に対してわが国の法律（安衛則）で始業点検が義務付けられる。一方，欧州では，事故前の停止の手段としての要求から，安全装置は故障に対して機械を停止させ，正常に修理がなされるまで機械を動かせない。これを安全装置の設計条件とし，認証取得（CEマーキング）を市販の条件としている。安全装置の目的が“事故前の停止”であり，安全側故障の保証が認証性を示し，リスクアセスメントの結果に応じて停止カテゴリの選定を規格として定めている。一方，わが国では，許容リスクにおける「許容」が曖昧であり，事故に対する責任は結果に委ねられ，結局，事故の結果は人間の責任に委ねられることになる。欧州の事故前の停止原則は，事故防止がそのままリスク低減の効果を示すが，事故防止の基準的方法を規定しないリスク概念に重大事故の防止を期待するのは無理である。

裁判鑑定を依頼される度に，著者は“欧州の安全装置なら事故を防げたはず”の証言を繰り返してきたのだが，責任は管理する縦割り行政の多様な判断に委ねるべきこととして，事故の原因は安全装置の欠陥とならず，安全装置の保全担当者の過失責任の問題とされるが，事故が起こってからの結果責任を裁くわが国では，如何ともしがたい。

偶然の結果（accident）とはいえ，どの国も，事故後の責任追及は避けられない。事故は，もともと発生を許さないことが現に発生したという事実を示すからである。しかし，被害者への賠償や加害者への罰など過失責任の追及では，安全問題の解決に何も寄与しない。“安全の責任”は事故の責任（結果責任としての被害者への補償・救済とする経営者の責任）とは異なり，事故の回避はもともと失敗が許されないことから生ずる。指摘するまでもないが，許容リスクという概念を示すだけでは，安全の責任は果たせない。

もともと安全は，原因に働きかけて，結果（事故）を安全な状態へとコントロールすること（事故を防ぐこと）である。しかし，このコントロールは明らかに時間的制約を受ける。原因が分らなければ事故を防げないし，たとえ分っても制限時間内に回避しなければ事故は防げない。

事故の原因調査を引き受けるときにいつも思うのだが，もう少し早く止めれば事故は防げたはずなのに，なぜ止めなかったのか。事故は，事故の回避に固執しすぎて停止操作が遅れた結果として発生する。当たり前なのだが，この当たり前のことを軽んじて事故を発生させている。事故の後に停止させるのでは間に合わない。安全の責任は，事故前の停止の要求に応えること，そして事故前の停止の失敗で事故の責任（経営者の結果責任）が生ずるという関係である。ただし，停止が遅れて事故の前とする条件を逸脱してしまうことがある。“止まる”には，「止まる」の他に「止める」があって，“固有安定停止”と“制御による不安定停止”の本質的な違いがある点に注意が必要だが，この違いはエントロピが関って生ずる安定性の違いとしてすでに述べてあるので，ここで触れるのは控えたい。いずれにせよ，事故は防ぐのでなく，一時停止させて事故の経験を拒否するという考え方で理解すべきである。

もう一つ，よく言われる安全は“危険から離れているから安全だ”である。隔離の安全でもあるが，これもうっかりすると結果責任が人間に委ねられることになりかねない。安全と思われた状態（位置）も，また置かれた環境も，大抵は変化して，事故が起こってから何が原因か，誰の責任の問題が結果論に委ねることになる。安全は最初に決めてそれで終わりというわけにいかず，常にモニターがなされ，変化に対応して修正がなされる制御の対象だということを忘れてはならない。

3. トップの無過失責任

ところで，リスクベースの現代社会にリスクゼロはあり得ないとされる。労働の現場では，危険の残る仕事が教育訓練を行ったという理由で労働者に委ねられる。ならば，リスクの現実として生ずる事故の責任を企業（トップ）が負うと考えられて当然ではないか。実は，これは，過失の如何によらず，事故の責任（補償・救済としての結果責任）を経営者のトップが負うとする無過失責任の考え方である。グローバルに共有する事故の責任原則だが，意外にもわが国の労働安全の法体系は基本的には無過失責任の考えで作られている。

もともと“不確実”を扱う賭けのルールがあって，リスクとは，賭けの失敗の時に果たすべき責任を，どのように責任能力として準備するかを明確にするための指標である。過失責任は，責任能力のない弱者に結果（事故）の責任を負わせることで混乱を生じてきたと考えていいだろう。欧州規格の理念として，“負いきれない責任は負わせない”があると聞く。そこで，無過失責任とされる労働安全には，災害による労働者の被害救済の責任を企業（トップ）が負うと決めることで混乱を防ごうとする意図がある。

事故の責任は，単なる結果責任ではなく，事故を，“事故前の停止の失敗”とする共通の認識があって，その限界でやむを得ず生じた事故に対する補償・救済の責任者として，経営者トップの立場が明確となる。しかし，事故を結果責任とするわが国では，事故の責任は，法律が関与して複雑である。安全の理由を整えて，事故の責任に予め系統だって対処するのは殆ど不可能である。事故の可能性が残る限り，トップは事故前に停止を強制し，自らに掛かる事故の責任を回避すること以外に方法はない。トップによる停止の強制に異論を唱える法律はあり得ず，よって自らの責任で停止を解くこと（運転再開）も自由である。改めて，結果（事故）をトップの無過失責任とすることが何よりも重要である。事故前の停止の要求（安全の責任）が，安全管理体制による合意（正当性）を以て実行されるからである。また，安全工学の体系化を目指す学問的立場から，停止による安全原則は普遍的であり，複雑な結果責任の議論への介入を避ける条件で安全工学の体系化が可能となると期待される。いずれにせよ，事故前の停止原則を共有し，安全の証明性（限界の証明性：許容リスク）のグローバルな共通化が何よりも重要だということである。

ところで，わが国では，リスクアセスメントに事故の免責を期待する人が多い。安全対策の限界で生じた事故の責任は，日本語の「責めに任ずる」というような結果に対して負うべき「責め」ではなく，結果（事故）の予測に対する説明責任に応えて，救済の準備を整えるとする応答責任（responsibility）である。結果としての救済の責任は免除されないという欧州安全の整合性については，著者が1984年に初めてフランスの国立労働安全研究所INRSを訪問したときに教えられたことである。当時の機械研究部長Dr.Vautrinが特に強調していたのは，安全の中心課題は合理的な救済制度を構築することであった。さらに，「安全は，事故を防ぐ／減らす／被害を小さくすること以上に，救済制度の合理性を担保する条件として規格化・整合化して企業に均しく守らせることに意味がある」との説明であった。かくして労働安全のトップの責任は，安全ルールの要求に応えること（安全の説明責任に応える責任能力）と，結果として生ずる被害の救済要求に応える責任（結果としての事故の責任）であり，ともに，そのための必要（requirement）に応えるべき応答責任（responsibility）に位置づけられる。後で示すように，欧州の安全のルールは，事故の前の停止を安全の責任としており，その追及の限界（State of the art）で生ずる事故前停止の失敗が事故の責任の対象になるという関係で責任が階層で示される。事故の責任と安全の責任は，ともにトップの責任だが，特に，トップの責任で技術者に要求するインタロック（事故前の停止手段）は，残留リスクに伴う事故の可能性を減少させるのに大きな効果を示すであろう。

4.「停止」の責任能力とリスク

リスクそのものは事故を防ぐ能力も，また事故後の責任に対処する能力も有しない。許容リスクによって，リスクとして許容される条件で事故が発生すると考えなければならない。その場合，当然,「事故の前になぜ停止しなかったのか」に対する正当な理由が問われるからである。改めて，リスクは，事故前の停止を安全の原理として共有することで,“安全”に係っているのである。

すでに述べたように，事故前の停止の失敗で事故が起こるという事実に基づけば，安全は事故前の停止を確保すること（安全の責任能力）である。私たちは，もともと“停止できないシステム”に安全はなく，“停止を許容しない安全管理”では責任が果たせないことを十分に承知している。大きな被害はもとより，小さな被害であっても人に傷害を与える以上,停止による事故防止が無視されてはならない。リスクアセスメントの結果としての残留リスクは，予め備えるトップの「停止の責任能力」の理由を明確に示すための指標とみることができる。改めて，事故は，事故前の停止原則に対する危険側誤りで生ずると考えることができるから，よって，事故前の停止の原則の限界で生ずる被害であるリスクは，非対称誤り特性の確保／改善で低減されると考えることができる。生産は正常時,停止を要さない。しかし，トラブルが発生し，その処理，故障修理等で人間による介入を依頼する。そのときは当然だが，システムは停止して人間を呼んで，待つのである。誤りが停止として生ずるのを安全上絶対と考えるのは，誤り（故障）をシステムは自分で修理できないから，人間に修理を依頼せざるを得ないからである。トラブルシュータとしての人間の掛け替えのない存在が人間だという関係で，人間を受け入れる条件として“故障→停止”が原理として演繹化されるまで構造化されていると理解される。

一般に，操作の担当者に「停止」の義務を課すとする安全管理が導入される。これによれば，機械への接近は停止して行わねばならず，人の不安全行動とは,明らかに,「停止する前の機械に接近すること」と定義されるだろう。近年，自動車の製造ラインなどでは「止めて，呼んで，待つ」を義務とする作業管理が導入されているが，トップの責任能力によって構成される“停止管理システム”として重要な意味を持つ。

5. リスクと停止カテゴリ

機能を優先し，停止を避け，機能の信頼性（アベイラビリティ）の追求の結果がリスクとして評価され，リスクは，停止管理システムとしてトップの有

表1 リスクアセスメントに基づく停止カテゴリの選択

停止カテゴリ （リスクの大きさ）	手段	対応
カテゴリ B （補償可能な微小被害）	停止スイッチ	人間の教育訓練、停止操作を人間に委ねる。
カテゴリ 1 （小リスク：リスク依存）	安全スイッチ	扉を開くときに安全スイッチによる停止信号によって機械が停止する。
カテゴリ 2、3 （やや大きい：リスク依存）	インタロック （多重系）	停止操作を行わないと機械に接近できない、安全確認型のインタロックを整備する。
カテゴリ 4 （大きいリスク） リスクに関わらず 発生を許容しない被害	フェールセーフ ・インタロック	停止が確認されるまで扉が開かない。故障を考慮したフェールセーフなインタロックを整備する。 （経験を許容しない被害に適用する）

すべき安全の責任能力に根拠を与え，現実の事故は停止操作によって防止される。ところで欧州規格には，「停止」の完全性（integrity）に対する停止カテゴリが規定されている。残留リスクに対して事故前の停止が要求されるが，停止の要求レベルはリスクによって異なる。表1に停止カテゴリの概要を示す。詳細は，関連規格に譲るが，リスクが十分小さければ，不安全行動を教育で補って，操作担当者に停止操作を委ねることができるだろう。リスクが大きくなければ，安全スイッチによって扉を開くときに停止信号が出るようにする。少々リスクが大きい場合は，停止操作を行わないと機械に接近できない安全確認型のインタロックが準備される。最後に，リスクが大きく，事故前の停止には誤りが許されないという状況では，停止操作を不可欠とするだけでなく，実際に停止が確認されるまで扉が開かないように，“非対称故障特性”を考慮したフェールセーフなインタロックが構成される。このように，停止カテゴリは，リスクに応じて選択される停止能力を階層で示している。フランク・ナイトがリスク論で言うように，人知を超えて最後に残る真の不確実は絶対には避けられない。このような不慮の事故に対してトップは結果責任（救済）を負うとする覚悟が必要である（決定論）。同じ理由で，停止をもってしても，絶対と言える安全の責任は果たし得ない。そうである限り，労働安全の責任は，トップの停止の責任能力に対し試されるのである。

6．事故前停止の運用と非対称誤り特性

安全には積極的な安全と消極的な安全がある。安全の確認に基づいて危険の可能性のある仕事を行う。仕事に対する積極的な安全の立場である。これに対して確認できないとき停止するのが消極的安全である。仕事に対しては消極的だが，事故防止の効果は絶対的である。停止による安全を確保した上で，停止を回避する積極的操作を行って仕事を確保し，さらに仕事の効率を改善しようとするのが安全運用システムの全様である。図1は，安全運用システムの例をBS提案による欧州規格（火を用いない場合の圧力装置の安全）で示している。3つの要素が関係してシステムを構成するが，規格には詳細な説明がないので，筆者なりに，これらの要素が安全にどう関わるか考えてみる。

積極的な安全は，まず，危険から離れた状態を“安全”と定めて，危険に近づかないよう積極的な制御を行う。安心して仕事をするために事前に安全な場所を確保するという考え方である。ここに重要なことは，安全は最初に設定して終りということでなく，常にモニタリングして，調整すべき制御の対象だということである。現実にも，例えば自動車の運転のように，生ずる変化に対応してハンドルやブレーキで調整を行って，なるべく安定した運転（速度）が継続できるよう心掛ける。これが本来の仕事

図1　欧州規格（EN/BS764-7：火なし圧力装置の安全）

のための安全の条件を整える機能制御（Regulating control）である。

変化に応じて速度を調整して安全状態を維持する制御であり，“速度”を操作量として“危険との間隔”を制御量とする位置制御（サーボ）に類似する制御だと分る。したがって，制御目標 x と誤差 σ（標準偏差）を用いて $x \pm \sigma$ のように対称誤り特性で示され，誤りは危険側か安全側か区別しないから，信頼性を上げて限界とするか，そうでなければ，危険側の誤りに対処するための制御によるバックアップを構成する。

そこで，仕事中に誤って侵す危険への接近を捉えて仕事に介入し，減速して接近を遅らせ，併せて安全状態に復帰させるとする調整制御（Monitoring control）が導入される。もともと機能制御は仕事を決められた条件（安全な状態）で仕事を行うことで高い効率を確保しようとするもので，誤った仕事を本来の仕事に復帰させる調整制御であるから，危険側誤りを著しく改善すると期待されるが，実は，機能的非対称誤り特性と見なされ本来の非対称誤り特性とは区別される。

ところで，リスクとは，不確実性を扱う場合の指標だが，フランク・ナイトによれば，基準を共有しない不確実性は“真の不確実性”であり，比較に用いる指標とはならない。あくまでもリスクは，停止を基準とし，事故前停止が必ずしも成功しない場合の被害であって，停止による安全の証明法を指向しない機能制御は，それ自身たとえ事故を減らす効果が見られても，信頼性（アベイラビリティ）における効果とみるべきであって，あくまでも，調整制御のバックアップがあって安全性の効果が認められるのだとする理解が必要である。重要なので繰り返すが，リスクは，本来，事故前の停止の限界で生ずる被害の予測としてのみ合意性（認証性）が認められるのである。

非対称誤りは，危険や故障が“停止”として生ずる安全システムの有すべき特性だが，近年の危険監視システムはコンピュータの持つ対称誤り特性のために，厳密には非対称誤り特性とは認められない。一般に，コンピュータによる監視機能は完璧だの認識があるが，結局事故が起こった時，コンピュータの故障停止の保障の限界から，結果としての責任が人間に課せられる点に注意が必要である。

事故前の停止原則に準拠して安全の責任を最終的に負うのが安全遮断システム（safety system with shut-down）である。調整制御にも危険側誤りが避けられないと述べたが，事故は，事故の前の停止の失敗で生じ，原因は，調整制御による“停止”に対する機能的失敗と見なされる。ここでもう一度，事故とは何かに戻ると，事故（結果）には原因が存在し，時間軸上，先に原因があって後から結果（事故）が生ずる因果律を示す事故のプロセスが存在する。“停止”とは，このプロセスを停止することであり，事故前の停止とは，停止が事故の前に完了することである。そうなると，危険側誤りとは事故前に設定された停止（基準）に対して遅れる側の誤り，また安全側の誤りとは反対に停止が早まる側の誤りであり，したがって非対称誤り特性とは，停止の誤りが早まる側だけしか生じない（危険側誤りを殆ど生じない）誤り特性であると言うことができる。そうなると，安全とは，非対称誤り特性（早まる停止を許容するとする条件）で事故前の停止を確保することであり，安全運用システムとは，非対称誤り特性によって事故前停止が確保されている条件で，停止を回避する積極的操作を行って，効率の良い仕事を実現するためのシステムとまとめることができる。

危険への接近を監視して，事故前の最後の停止判断を行う安全遮断システムは，一般に言うインタロックに他ならない。しかし，ここで論ずるように，インタロックの選択には非対称誤り特性に係って特に注意が必要である。

まず，安全遮断システムはフェールセーフでなければならない。事故は停止すべきとき停止できないために発生し，“故障”は言い訳にならない。フェールセーフを意味する非対称誤り特性は，故障に対する停止を要求し，正常に修復がなされない限り停止が解除されないとする安全側誤りを要求する。もう一つの事故の原因は，停止の遅れる側の誤りである。原子力発電所のように停止手段が失われるようなシステムは例外だが，殆どの事故は停止操作の遅れで

発生すると考えていい。事故前の停止原則は，一般に遅れる側の停止誤りを誘引するため，停止操作が遅れて事故が起こる強い傾向がある。停止装置の故障や，制御の不調などによる無暗な停止は，仕事の立場からは迷惑とされるが，安全の立場からは，安全側の誤りとして許容される。

このように，安全は，安全遮断システム（インタロック）の有する2つの非対称誤り特性で確保されると言っていい。しかし，事故前の停止を安全原則とする限り，仕事効率を求める立場からの要求に対する配慮が重要になる。重要なことは，危険への接近による停止をできるだけ回避して，安全で効率的な仕事を総合的に検討し，その検討結果が図1で示される安全運用システムと考えることができる。著者らは，安全遮断システム（インタロック）にフェールセーフを適用する研究を行ったが，停止を安全の原理とする限り，安全運用システムを構成する機能制御，調整制御とともに，安全遮断システム（インタロック）の有すべき2つの非対称誤り特性の重要性について正しい理解を求めたい。

7. おわりに

わが国では，従来，リスクが小さければ安全だと思い込み，事故の免責と読み替えて，安全の責任能力を低下させてきたと言える。本来，大きなリスクは，事故の重大な責任に備えて高い停止カテゴリの停止手段が選択される。また，たとえ低リスクであっても，安全の責任があくまでも事故前の停止の要求が無視されてはならない。改めて，安全の責任能力におけるリスクの役割について，正しい理解を求めたい。

責任（responsibility）は，事故の責任（結果に対する責任）と安全の責任（停止の責任能力）とからなることを示したが，トップが責任能力の概念をもたないために，トラブルとなる場合がある。例えば，事故が起こった後で，事故の原因と責任に関わって，被害者となった労働者が労災保険の適用を受けるか否かの判断を裁判に委ねるという状況である。ここで示したように，労働安全で最も重要なことは，合理的な救済制度を確立することである。救済制度の合理性を担保するために安全のルールがあって，救済の対象とできない労働条件は安全のルールによってもともと排除されるという考え方である。労災保険の適用外で生ずるような災害はもともと許可をしないという判断で，本来の労働条件が確認されるというのが，トップの責任であるということである。以上，参考になれば幸いである。

＜参考文献＞

(1) Pressure equipment-Part7: Safety for unfired, BS EN764-7（2002）pp.6
(2) 杉本旭，安全の責任ついて考える～技術者の身に着けるべきグローバルな安全感覚，建設機械施工，Vol.69, No.1（2017-1）pp.84-87