入門講座

リスクベース工学入門–2

リスクベース工学の基礎

Fundamentals of Risk Based Engineering

酒井信介
Shinsuke Sakai
東京大学　大学院工学系研究科
機械工学専攻　教授

1 緒言

これまでのメナンス段階で多く採用されてきた画一的な検査方式の場合、事業者側から見たとき、検査時の手順が機械的であり、容易に処理ができるという利点がある。また、規制側から見たときにも、法規への適合性の判断が容易で、客観的な判断ができるという利点が考えられる。その一方で、画一的な検査方式の場合、検査規準の策定段階では、最新の学術レベルを反映して慎重に内容が検討されるものの、ひとたび発効されて、運用される段階になると検査時においては規格への適合性が最大の関心事となり、その時点で学術的内容にまで立ち入って検討する割合が少なくなってしまうことが懸念される。つまり、事業者側から見たとき、思考停止に陥りがちで、規格の手順に書かれていない事態が発生していたとしても、見過ごされてしまう可能性もある。検査の手順があまりにも画一的であると、最新の学術的知見や、合理的検査装置などの仕組みが柔軟に検査に反映できない、という問題もある。さらには、事業者側で、検査規準が実態に合っていないと感ずることがあったとしても、規準という重みが故に、明らかに無駄なことに対しても、形式的な対応をせざるを得なくなる。

欧米では、このような画一的検査の不合理性は早くから認識されており、この問題の解決のために幅広い分野でリスク保全技術が進められている。リスクに基づく検査方式、つまりリスクベース検査 (RBI) の場合には、こと細かく規制を行う画一的検査方式を採用しない。その代わりに、検査時においては、そのつど厳格なリスク評価を要求し、その結果にもとづく検査プログラムの見直しが求められる。リスクベース検査の導入によって、上述の画一的検査方式の問題点はかなり解消されることが期待される。実際、リスクベース検査がうまく機能する場合には、安全レベルの向上とともに、無駄な検査の省略にもつながるため、検査コストの削減に成功しているケースもある。今後、メンテナンスの比重が高まることを考えると、リスクベース検査の導入は急務であるといえる[1,2]。

リスクの定義として「損傷の発生確率×被害」を用いるが、この評価のためには、対象機器の損傷モードを特定し、その損傷モードの発生確率を求め、その結果として起きる事象の被害を予測しなければならない。その際、確率論的取り扱いが随所に必要になり、また損傷確率に関しては、データベースの整備が求められる[3]。客観的な判断ができない場合には、エキスパートの主観による判断も必要となるが、このような能力をもつエキスパートの人材養成をすることも求められる。事業者が可能な限りリスク緩和の努力をして合理的なレベルまでリスク低減したことをもって許容レベルに到達したと判断するのである。

本稿においては、リスクベース検査を中心とするリスク保全技術を遂行するにあたって必要となるリスクベース工学の基礎的事項について概説する。

2 リスク評価のための予備知識

工学上のリスク評価では、確率論的な取り扱いがたびたび出てくるので、統計学の基礎知識は必要である。また、信頼性工学は随所で用いられ、その中でも破損確率の評価手法は原理や、解析技法について理解しておくことが必要である。下記のような統計学上の用語は最低限理解しておくことが望まれる。

標本確率、累積分布関数、確率密度関数、平均値、
分散、標準偏差、変動係数

特に、リスク評価で重要となるのは破損確率の評価である。基本的な考え方は荷重と強度の特性を考え、

荷重　＞　強度

を破損と定義した上で、破損が生起する確率を求めることである。その際、荷重や強度のばらつきを考慮する。しかし、リスクベース工学のようにメンテナンスを対象としている場合、このような手順で破損確率を算出することはほとんど行われない。その理由は、このようなばらつきのデータは、十分に整っていないためである。

そこで、検査記録に基づいて、想定される損傷モードの生起する確率を予測していくほうが現実的である。この際には、ベイズの定理が重要である。米国石油協会 (API) のリスクベース検査ガイドラインにおいても、検査データに基づく損傷頻度の評価に用いられるのは標本統計学ではなく、ベイズ統計学である。この理由は、検査データの特性を鑑みて、ベイズ統計学による評価の方が合理性をもつためである。その代表的な特性としては以下のような事項が挙げられる。

- 検査データの評価のためには、検査有効度のような漠然とした因子が入ってくる
- 破損頻度は、一般に小さなサンプル数で評価しなければならない
- 個別のプラント内機器の評価に既存のデータベースを活用するにあたっては、個別データと一般データを融合する手段が必要
- 損傷モードが途中から遷移する場合に、毎回更新するような手続きが適当

このような、特性に対応するためには、事前分布に対してベイズ更新によって事後分布を与えるベイズ統計学が適している。詳細は文献[1,2]を参照されたい。

標本統計学とベイズ統計学の対比を概念的に図1に示す。標本統計学では、多くの標本データ群から、破損確率を推定する。検査結果は、そのつどデータ群に追加されていく。この評価の過程には主観が入る余地はなく、客観的手順であるといえる。一方、ベイズ統計学では、破損確率の候補を主観に基づいて複数選び、個々の候補に対して確からしさ (確信度) も併せて割り当てる。主観的要素が入るので主観的確率と呼ばれることもある。検査の結果、破損が観察されるか否かに応じて、確信度を更新していくのである。更新する手続きはベイズの定理に基づく。検査を行う前の確信度の分布のことを事前分布、これを検査後にベイズの定理によって更新した後の分布を事後分布と呼ぶ。

この他、多くの乱数を発生して試行を繰り返すモンテカルロ法などのシミュレーション技法が用いられる。システムの故障確率を精度よく求めるためにはシステムをモデルとして表現することが必要である。システムのモデル化にあたっては、フォールトツリーアナリシス (Fault Tree Analysis、FTA)、イベントツリーアナリシス (Event Tree Analysis、ETA) の理解が求められる。FTA、ETAの内容については、4.2節で説明される。実際の評価にあたっては、損傷事例に関するデータベースの活用が不可欠であり、データベースとしてどのようなものが利用できるのかを把握しておくことが、極めて重要である。

リスクベース工学をメンテナンスの段階に適用する場合に、検査と関連付けて管理することが有効である。このような考え方をリスクベース検査 (RBI) と呼ぶ。この際に、重要となる概念が80-20の経験則 (パレート則) と呼ばれるものである。図2にその概念図を示す。横軸のA～Sはシステム内の機器を、縦軸は各機器が保有する相対リスクを示す。システム全体のトータルのリスクのうちの80%は、実はシステム全体の中のわずか20%の機器に集中していることを示している。もし、そうであれば全ての機器に同じ優先順位で検査を実施することは明らかに不合理であり、確実に20%の機器を

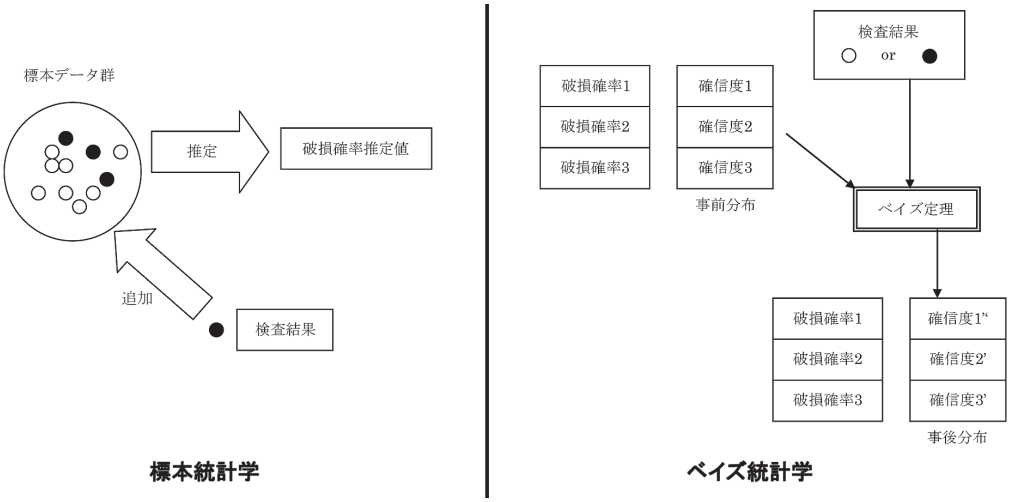

図1　標本統計学とベイズ統計学の対比

特定した上で、検査プログラムの優先順位を高めることが重要である。これが、リスク保全技術の基本的考え方である。このような考え方を80-20の経験則と呼ばれる。

3 リスク評価の手順

図3に、リスク評価のための一般的な手順のフローチャートの例を示す。原理的には、リスク評価の手順はおおよそ共通しているものと考えられる。

まず、①において解析を行う枠組みを明確にすることから始める。ここでは、リスク解析を行う範囲の明確化を行う。例えば、個人のレベルの評価であるのか、組織のレベルの評価であるのか、さらに広範囲に地域の評価であるのかなどを明確にする。もし、評価から除外する部分がある場合には、その理由を明確にしておかなければならない。また、この段階で、利害関係や解析の影響の及ぶ範囲も明確にしておくことが望ましい。最終的なアウトプットとして求められるものが、定性的なものであるのか定量的なものであるのかも明確にしておく。そのいずれかによってリスク評価で採用するアプローチが異なってくる。

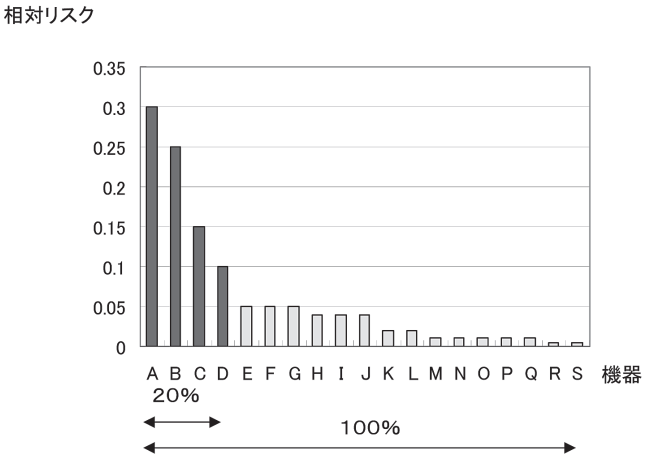

図2　システム内のリスクの分布の概念図

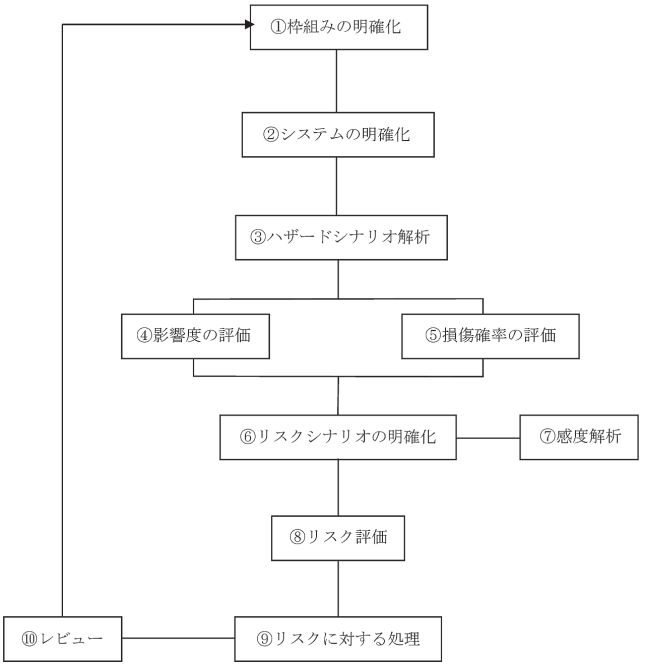

図3　リスク評価の手順

②の段階では、評価対象とするシステムの明確化を行う。システムの特性を評価するためには、システムを適確にモデル化する必要がある。このモデル化の情報は、次のハザードのシナリオ解析においても活用される。

③においては、機器の損傷に伴ってどのような被害、もしくは影響度があるのかを明確にするための前段階として、まずは異常事態のときに何が起きるのかというシナリオを漏れなく抽出する。その際に、実際に観察された現象のみではなく潜在的に生じ得る現象の予測が求められるために、注意深い検討が必要である。この段階がわが国においては、どちらかというと前向きに受け止められない傾向にあり、たとえシナリオ抽出を行っても、開示することには困難が伴うものと考えられる。しかし、前述した通りリスク評価においては、まさにこの部分が重要なのであり、積極的に開示することをもって高い評価を与える社会的風土を形成することが極めて重要であると考えられる。

④においては、これまでの評価でハザードのシナリオに基づいて異常事態が発生した結果として、どのような被害、あるいは影響度があるかを特定する。被害を測る指標としては、リスク解析の目的や、解析者の関心などに依存して、決定される。極端な場合には、事故時の予測死者数のようなものも考えられるし、それ以外に、事故時の復旧コスト、被害の及ぶ面積の大きさ、喪失されるシステム機能の大きさ、など対象とする機械構造物に応じてさまざまなものが考えられる。

⑤の段階では、異常事態が発生する確率、もしくは損傷確率の評価を行う。この評価においては、データの蓄積が重要であり、損傷事例データベースがあれば活用する。定量的リスク評価を行う場合、この部分がやはり一つのネックになる部分である。この背景には、リスク評価を意識した組織だったデータの蓄積が行われていないことが一因であるものと推察される。例えば、一般に事故事例データベースというと、事故が起きたときのみのデータを記録することを考えるが、損傷確率の評価のためには、これのみでは情報不足であって、正常に動作した場合のデータもまた必要なのである。損傷データの記録がないということの説明としてよく聞かれることとして、「機器を破損するまで使うことはなく、その前に交換してしまう」ということがある。しかし、たとえこのよう

な場合であっても、供用していた期間を情報として蓄えておくことによって、破損確率評価に活用することは可能なのである。一方で、たとえこのようなデータベースを企業が社内で持っていたとしても、なかなか外部には出てこないのが現状であろう。わが国に損傷データベースがない場合には、海外のデータが利用されることもある。

⑥においては、異常時にどのようなシナリオが展開していくかを明確にすることを行う。このために、後述するFTAやETAなどの論理解析が活用される。この際、想定されるシナリオが膨大である場合には、全てのシナリオに対してリスク評価することは時間と労力の観点から困難を伴うことも多い。この場合には、⑦の感度解析を活用する。つまり、入力変数の微小変化が結果に及ぼす影響の度合いを調査し、感度の大きな因子を重点的に解析することにより合理化される。また、このような変数は重要度が高い因子として抽出できるので、データ精度を高めるための優先順位を決定するための目安とすることもできる。

⑧のリスク評価においては、まずリスクの基準を明確にする。技術的側面からの明確化以外にも、文化的、社会的、人道的、法律的などさまざまな観点からの基準も考えられる。影響度と損傷確率の両者の評価結果を用いて、後述の定量的リスク評価、もしくは定性的リスク評価を行った上で、リスク基準との比較を行う。この結果に基づき⑨のリスクに対する処理を決定する。リスク処理の概要は5章で示される。リスク基準とリスク評価の結果の比較によって、その余裕の程度に応じて意思決定を行う。最終的な結果は、正確に文書化するとともに⑩に示すように第三者の専門家による厳正なレビューが望まれる。このレビューの結果、不適切と判断される部分があれば、①に戻ってリスク評価の精度を高める努力を行う。

次章において、リスク評価の技術的側面の中の主要な部分についてもう少し詳しく述べる。

4 システムの評価

4.1 リスク源の特定

リスク解析の手順として、リスク源の特定をすることがまず必要になるが、このためには評価対象のシステムについて熟知していなければならない。その際、これまでには経験のない事象から派生する事故シナリオについても、特定することが求められる。リスク源の特定のために用いられる技術を表1に、その特徴とともにまとめて示す。このように、リスク源の特定を行う解析の段階や、求められる詳細さの程度、解析分野などに応じて適切な手法を選択する。

4.2 システムの表現

4.1節で述べた各種手法により、リスク源の特定が行われるが、対象とするシステムによっては、リスク源となる損傷事象の評価に対して、より詳細な検討が求められることがある。例えば、原子力プラントや化学プラント装置では、事故の原因となる機器の損傷は、単独の事象としていきなり発生するのではなく、何らかの起因事象から事象の連鎖の結果として発現することが多い。このような場合に、システム事故の特性をより適切に表現するために、事象の過程の順序や組み合わせを図式表現することが行われる。図式表現のうち代表的なものはフォルトツリー (Fault Tree、FT) とイベントツリー (Event Tree、ET) である。解析まで含めて表現するときには、フォルツトリーアナリシス (FTA)、イベントツリーアナリシス (ETA) と呼ばれる。FTAとETAは、完全に独立なものではなく補完的に用いられる。

図4に典型的な、FTの例を示す。このように、FTでは、最終的な事故事象を頂上事象として、この事象に関与し得る事象を後ろ向きに遡って特定していく。図中に表現されるようにFTは原則的にANDやORの論理ゲートから成るブール論理線図として表現される。この手順を進めていくと、やがてそれ以上に遡る必要のない基本事象へと到達する。このような事象を基本事象と呼び図中では○印で示している。長方形は複数の故障事象の組み合わせによって生じた故障事象を示す。FTの作成過程において、故障原因の究明が十分でない故障事象がたびたび現れるが、このような事象は図中のようにダイヤモンドの記号で示しておく。ANDゲートは、このゲートを通過して破損が伝播するためには、このゲートに入力されている全ての機器が故障する必要があることを示し、並列システムを示している。このゲートでは、一つの機器だ

表1 リスク源の特定方法

名称	特徴
予備的ハザード解析 (PHA)	詳細解析を用いて主たるハザードの特定をする前に、予備的に行われる解析。通常は、予備設計段階で用いられる手法で、ハザードとなり得る要素ごとに、ハザードの状況や、潜在的な事故、影響などを表形式にまとめる。
故障モード・影響度解析 (FMEA)	システムにおける各構成機器を系統的に検査することにより、起り得る結果から開始し、全ての可能性がある原因を得るために遡って故障モードの特定を行う。故障モードの特定は可能な限り広範であることが必要である。全ての故障モードを取り扱うと膨大な量となるため、サブシステムに分けた解析が行われる。
故障モード・影響度・致命度解析(FMECA)	FMEA の論理的な拡張であって、故障事象がそれによって生じうる影響の重要度に従って分類される。各故障モードの致命度を決定するために、故障頻度と故障の影響の両者を主観的に評価する。解析の複雑さを排除するため、各機器または各サブシステムは相互に独立であることを仮定する。影響度の評価は定性的であるため、故障モード間の相対比較、感度解析などに利用される。
ハザード・運転性解析 (HAZOP)	化学産業やプロセス産業のプラントのハザードや運転上の問題を特定するために広く利用されている方法で、FMEA 手法を特に配管系の流体とプロセスユニットに基づくシステムに適合させたもの。プロセス流れ図を用い、各プラント項目を順番に考慮する。これにより、発生する可能性のある問題を考慮することができる。結果は、一般に表形式のワークシートにまとめられる。
インシデントデータベース	重大事故に至る以前のインシデント情報は上記の各種解析法において極めて重要である。利用可能なデータベースを調査し、活用することが必要。

けが故障しても直ちに機器の損傷というわけではないので、ある程度の冗長性を有することになる。一方、ORゲートは全ての機器が機能しなければシステム全体が正常に動作しないことを示し、直列システムであることを示している。ほとんどの工学システムは直列及び並列システムの組み合わせで表現できる。フォルトツリーではなくて、信頼性のブロック図として表現する場合には、直列系、並列系の図示は図5のようになる。フォルトツリーは破損時の論理関係を、信頼性ブロック図は成功時の論理関係を表現していることに注意が必要である。実際のシステムでは、ブロック図はさらに複雑なものとなるが、この場合には故障モードの特定にカットセットという考え方が用いられる。例えば、システムブロック図が図6のように表現されるとき、複数の機器が同時に破損すると、直ちにシステム破損に結びつく組み合わせがある。このケースではAB、DE、ACE及びBCDが該当する。この組み合わせをカットセット、もしくは最小カットセットと呼び、頂上事象はこれらの最小カットセットのいずれかが生じたときに発生するものとして識別できる。このようにカットセットを見出すことにより、解析の手間を大幅に減ずることができる。FTは、予め検討すべき故障モードが限定されており、このモードの詳細解析をすることに関心がある場合に有用な解析手段である。

一方、ETの典型的な図示表現を図7に示す。ETの場合には、FTとは逆に起因事象から出発して事象が伝播していく過程を時間経過に従って、追跡していく。解析は、最終的な故障事象が現れるまで続ける。従って、一つのETからは、非常に多くの故障事象が現れることになる。関心のある故障事象が限定されているときには、非常に多くのETを描かなければならない場合もあり、必ずしも効率的であるとはいえない。このような場合には、むしろFTを利用すべきであろう。ETの場合には、特定の故障モードが生起することによって、後続の生起事象がどのようになるか、という点に関心がある場合に有用なツールである。ETとFTは補完的な関係にあり、しばしば組み合わせて用いられる。例えば、FTにて、ある特定の故障モードについて詳細に分析した後に、この故障モードの発生によってどのような後続の事象が派生するかを知りたければ、FTの頂上事象をETの起因事象として解析すればよい。あるいは、ETの結果導かれる故障事象についてより詳細な解析をしたければ、ETの帰結として得られる事象をFTの頂上事象として解析すればよい。ETのばあい、あらゆる生起状態について解析しようとすると分岐の数が莫大にふくれ上がることがある。例えば図6のシステ

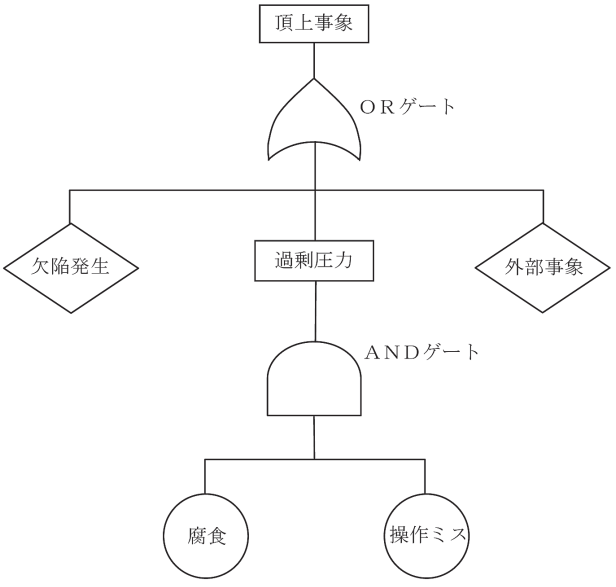

図4　典型的なフォルトツリー

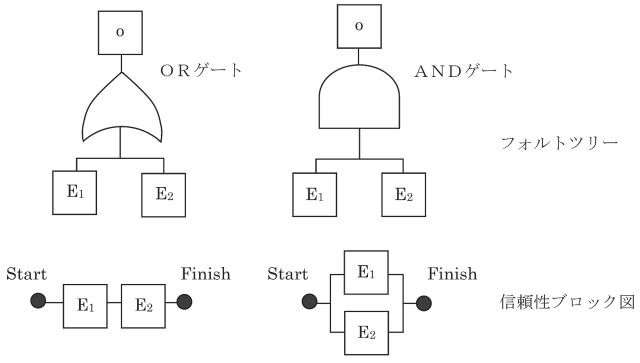

図5　AND、ORゲート

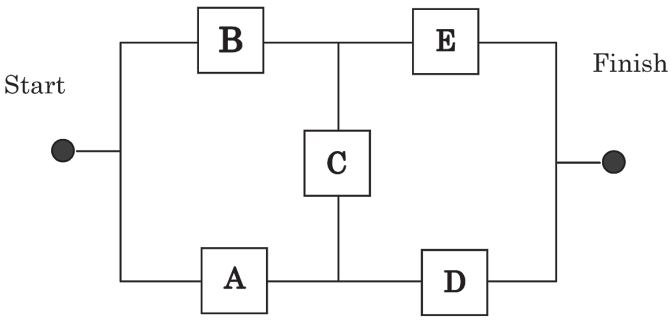

図6　複雑なシステムの例

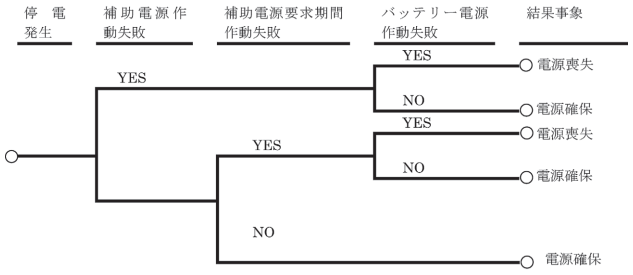

図7　イベントツリーの例

ムでは5つの機器で構成されるため、完全なFTを描くと32(=2^5)個のパスが存在することになる。FTの場合と同様に、ETの場合にも複雑なシステムについて最小カットセットを見出すことにより、解析を簡素化することができる。膨大なシステムになると最小カットセットの抽出は容易ではないが、自動的に評価する手法も提案されている。

4.3　定性的リスク解析と定量的リスク解析

工学におけるリスクは、「故障確率×影響度」で定義されるが、予備的解析の段階ではこれらのデータを完全に収集することは困難であるので、まずは主観に基づいていくつかの階層レベルに分類する。例えば、図8に典型的なリスク表示図を示す。ここでは、故障頻度と影響度を各々三段階ずつに分類しているが、分類数については必要度に応じて適宜決定すればよい。このようにして構成した二つの軸から表現したマトリックスのことをリスクマトリックスと呼ぶことがある。両者のレベルの程度に応じてリスクを分類し、本図においてはリスクの大きさを濃淡の濃さで表現している。例えば、高リスクと判定された機器を中リスクに移動するよう、点検政策を考えたり、あるいは低リスクと判定された機器は点検政策の見直しにより中リスクとなるようにするなどの検討を加えることができる。このように、主観に基づいてリスクのランクづけを行う解析手法を定性的リスク解析と呼ぶ。定性的リスク評価は、複数の検討対象の相対的な比較に用いられ、評価されるリスクは絶対的尺度を示すものではない。膨大な部品点数の全てに対して詳細な定性評価をすることは、多くの労力を要するので、初期の段階で注目するべき機器のスクリーニングをすることが求められる。このような目的で用いられるのが定性的リスク評価である。従ってスクリーニングされた機器に対して、より厳密なリスク評価を行うためには定量的リスク評価を行う。

定量的リスク評価では、故障確率と影響度を数値として求め、リスク値をその積として評価する。故障確率の評価にあたっては、FT、ETのいずれについても、各事象の生起確率を割り当てた上で、定量的に評価する。また、破損確率の評価にあたっては、信頼性工学の各種手法が活用され、一次近似法のような近似解析手法や、モンテカルロシミュレーションのような技法が活用される。モンテカルロ法の効率的解析のためには、層別サンプリング法、重点サンプリング法のような方法も活用される。損傷データ数が非常に少ない場合には、稀少データの解析法であるベーズの定理の活用が有効である。

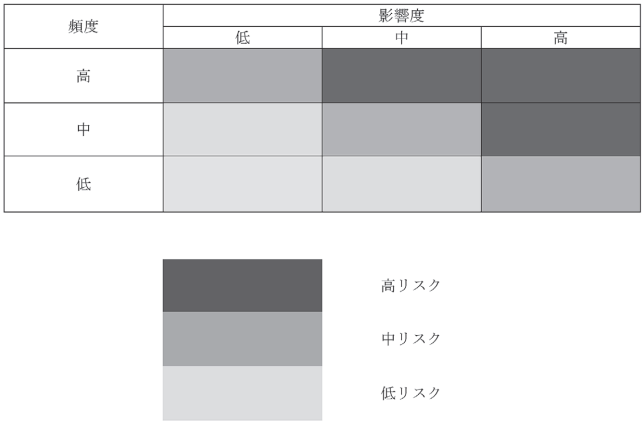

図8　リスクマトリックスの例

4.4　エキスパートパネルの要件

リスク評価において必要となる損傷モードの特定や、損傷確率の評価、その結果としておきる影響度の評価などについては、客観的に決められるものばかりではなく、エキスパートの主観に頼らなければならないケースが出てくる。多くのリスク関連の規格やガイドラインではエキスパートパネルの設置に関する記載があり、資格要件なども書かれることもある。一般にエキスパートパネルの要員としては、次のような技量を有する人を想定することが多い。

(1) 材料・腐食の専門家 (2) プロセスの専門家 (3) 運転員・メンテナンス部隊 (4) 装置管理要員 (5) リスク評価の専門家 (6) 環境・安全評価の専門家 (7) 経済・ビジネスの専門家

今後、リスク評価の促進のためには、このエキスパートの技量を有する人材確保が重要であり、いかにして人材育成していくか、ということが重要な要素となることが考えられる。また、リスク評価の認定にあたっては、エキスパートパネルの資格要件の明確化も重要な要素となろう。

5　リスク解析後の処理

リスク評価の終了後に、リスクの評価値と基準とを比較して、許容レベルを越えている場合には、何らかの意思決定が要求される。以下にその代表的な処理と、その概要を表2に示す。

表2　リスク解析結果に対する代表的処理

リスク回避	リスクが起きる対象をあえて選択しないということ。このようなことが、常に可能なオプションとは限らないが、危険性、生起確率、または両者が深刻である場合には、唯一のとり得る手段である。
リスクの低減	ある事象の生起確率の低減または、影響事象の厳しさの低減を通じてリスクを軽減する努力をする。システムの規模を小さくする、制御手段を投入するなどの措置をとる。
リスク移転	保険などの他の経済的なメカニズムによって経済的なリスクを他の集団と共有のリスクにするか、または完全に移転することができる。影響事象が経済的なものである場合に適用可能。
リスクの許容	たとえ基準を超すようなことがあっても、他の手段が講じられるまでの時間が限られている場合にのみ適用可能。

最終的に、許容可能レベルまでリスクを低減することが理想であるが、技術的にもコスト削減の面からも実用的でないことが多い。このような場合に、リスクの許容基準の考え方として、現実的な最小値に目標値を設定する、という考え方が採用される。このような考え方は、As Low As Reasonably Practicalの頭文字をとってALARPと呼ばれる。As Low As Reasonably Attainable（ALARA）も同様の考え方である。リスク緩和のために、対策を講じた場合に、それに比例してリスクが減少する場合には、未だリスク緩和の努力が求められることになる。このようなリスク緩和の努力に応じて、その対策によってリスク減少を実現できる領域をALARP領域と呼ぶことがある。

リスクに関連する規格などでは、規制者に対して、次のような要求をすることが多い。まず、全ての合理的に予見できるハザードが同定されていること、それに伴うリスクが評価されていること、そのリスクを除去するために適切な対策がとられているか、または合理的実用と考えられる程度に小さなALARP値まで減少されていること、である。

6 まとめ

ここでは、リスクベース工学の背景と基礎事項について、概要をまとめた。API580などの代表的なリスクベース検査ガイドラインにおいても、基本的な流れは同じである。今後、リスクベース工学をメンテナンス段階に適用するにあたって本稿を参考にしていただけると幸いである。

参考文献

1）酒井信介：圧力技術，42（2004）5，284-290.
2）酒井信介：圧力技術，43（2005）1，22-27.
3）酒井信介：圧力技術，45（2007）1，39-44.

（2008年11月4日受付）