連　載

プラントの安全性評価

第 3 回　潜在危険性の特定（その 2）

日本防災システム協会 副幹事長
松岡 俊介

前回に引き続き、潜在危険性の特定手法として活用できる以下の方法について、それぞれの特徴、適用上の留意点等を述べる。

（1）予備的危険性評価（PHA）
（2）故障モード・影響解析／故障モード・影響・重大性解析（FMEA/FMECA）
（3）作業安全解析／誤操作解析（JSA/HRA）

予備的危険性評価（PHA）

この手法は、アメリカ国防省がシステム安全プログラムに関する軍標準 MIL-STD-882B として 1987 年に開発したもので、化学プロセス産業の分野でもプロセスの開発、立地選定、概念設計などプロジェクトの初期段階で適用し、設備コストと影響を最小に抑えつつ主要な潜在危険性を洗い出し、消去、最小化または制御するための基本方策の立案などに活用されている。

また、その名前が示すように、プロジェクトの次の段階すなわち基本計画や基本設計の段階で、HAZOP や FTA などのより詳細な危険性評価を行うために、予備的に潜在危険性をスクリーニングする場合にも用いられる。

PHA は、以下のような基本計画や概念設計に関する要素やデータがあれば適用することができる（①と②だけでも適用可）。

① 取り扱う主要な化学物質
② 取り扱う主要な化学プロセス（反応、蒸留、分離、移送など）
③ 主要プロセス条件（流量、温度、圧力、組成など）
④ 主要な機器データ（能力、サイズなど）
⑤ 設備レイアウト
⑥ 運転方法、運転環境

PHA は、HAZOP におけるガイドワードや「ずれ」のような独特の方法や概念はもっておらず、基本的にはチームによるブレーンストーミング（すなわち思いつき）方式に従っている。MIL-STD-882B では、PHA の基本手順を以下のように規定している。

（1）入手可能な資料、情報（上記 ①～⑥）を揃え、対象となる概念設計の範囲を定義する。
（2）潜在危険性を特定する（火災、爆発、毒性ガス流出など）
（3）ひとつの潜在危険性について主要な原因を洗い出す（機器の損傷、リーク、運転異常、誤操作など）
（4）各原因による潜在危険性の主要な影響（起こりうる最悪の結果）を特定する（プラントの損傷、死亡、環境汚染など）
（5）原因と影響の各組み合わせを 4 つの危険性カテゴリーのどれかに分類する。
　Ⅰ：無視できる
　Ⅱ：低い
　Ⅲ：重大
　Ⅳ：破局的
（6）最後に、潜在危険性を消去または低減する方策または検討事項を提案する。

表 6 に、「Cl2（塩素）貯蔵容器を搬入し、反応器に Cl2 を供給する」という基本的な設計概念に対して PHA を実施した事例を示す。安全対策検討項目として、貯蔵量の最小化、安全計装システム、付

表 6　予備的危険性評価（PHA）の例

工場　：ABC 会社 XYZ 工場
装置／設備名称　：Cl2 反応プロセス
設計概念　：Cl2 貯蔵容器を搬入し、反応器に Cl2 を供給する（流量等プロセス条件は未定）
P&ID No.　：なし
実施日：2007.5.24

潜在危険性	原因	主な影響	危険性カテゴリー	アクション No.	安全対策検討項目	担当
1　毒性ガスの流出	1.1 Cl2 貯蔵容器の損傷またはリーク	Cl2 大量流出による死亡の可能性	Ⅳ	A1.1-1	Cl2 貯蔵量の最小化（液化 Cl2 ⇒ Cl2 ガス）	プロセス
				A1.1-2	Cl2 検知による自動散水設備を配備した建屋に貯蔵容器を収容	建築／安全
				A1.1-3	Cl2 漏洩・拡散シミュレーションの実施（適切な貯蔵容器置場の選定）	プロセス
				A1.1-4	Cl2 貯蔵容器の健全性確認手続の制定	保守
				A1.1-5	Cl2 流出に対する非常警報／通報システムの設置、制定	安全
	1.2 プロセス異常による未反応 Cl2 の排出	Cl2 大量流出による死亡の可能性	Ⅲ	A1.2-1	異常反応プロセス条件の検討	プロセス／安全
				A1.2-2	未反応 Cl2 排出に対する検知警報／緊急運転停止システムの設置	プロセス／制御
				A1.2-3	未反応 Cl2 回収／中和システムの追加	プロセス
	1.3 Cl2 供給ラインの損傷またはリーク	Cl2 流出による死亡の可能性	Ⅲ	A1.3-1	二重管採用の検討	プロセス
	1.4 Cl2 貯蔵容器の接続時のリーク	Cl2 流出による死亡の可能性	Ⅲ	A1.4-1	Cl2 貯蔵容器の接続／切り離し作業について作業安全分析の実施	プロセス／安全

危険性カテゴリー：　Ⅰ：無視可　Ⅱ：低　Ⅲ：重大　Ⅳ：破局的

帯設備、運転手順、保守手順、非常時システム、追加すべき安全性評価／災害影響評価など、計画、設計、運転、保守、安全に関する基本的な課題が幅広く指摘されており、プロジェクトの初期段階に PHA を実施することの有効性を示している。

故障モード・影響解析／故障モード・影響・重大性解析（FMEA/FMECA）

故障モード・影響解析（FMEA）は、本来、電気、電子、通信、航空・宇宙産業等の大規模かつ複雑なハードウェアシステムの信頼性解析に使用されてきたシステム的な解析手法のひとつである。すなわち、システムを構成する機器・部品の故障モードをすべて洗い出し、各故障モードが引き起こすシステム機能に対する影響を特定し、改善方策を提案する。各故障モードの頻度データが揃っていれば、システムの機能喪失の頻度を定量的に算定することもできる。

一方、故障モード・影響・重大性解析（FMECA）は、FMEA をさらに拡張してシステム機能に対する影響の重大さを評価し、影響度ランクの割付を行う。

これらの手法は、1970 年代にアメリカで実施された原子力発電所の定量的リスク解析[4]において FTA、ETA とともに導入されその有用性が認められたあと、化学産業分野においても定性的な安全性評価手法として利用されるようになった。

FMEA/FMECA は、上述のように本来、機械システムを対象としているが、化学プロセスの安全性評価においては、純粋な機械システムよりも人間－機械系を対象とすることが多いため、人間の誤操作も故障モードのひとつとして取り扱う。

また、HAZOP と同様に、個々の故障モードは他の故障モードとは無関係な独立事象として取り扱い、単一の故障モードからのシステム機能への影響を評価し、他の故障モードとの同時発生による影響の評価は行わない（できない）。

化学プロセスの安全性評価手法として FMEA/FMECA を適用する場合は、部品レベルよりも機器レベルの故障モードを取り上げる。これに誤操作モードを加えて、システムへの影響を特定するが、システム機能よりも安全への影響に重点がおかれる。

HAZOP の場合、設計意図からのずれ（プロセス異常）をもれなく洗い出すために HAZOP ガイドワードという独特の手段が考案されている。一方、FMEA では、システムを構成する機器・部品の特定と、各機器・部品の故障モードを落ちなく洗い出すことが重要であるが、そのための手段は特別用意されてはおらず、機械、電気、電子、化学など異なる専門家によるスタディチームの編成や、機器故障データ集の故障モードリストの活用などによって抜け落ちをなくす必要がある。

FMEA では、まず対象の解析レベル（スタディノード）を設定する（プロセスレベルまたは機器レベル）。プロセスレベルを設定した場合の基本的な作業手順を以下に示す。

表 7　故障モード・影響解析（FMEA）の例

工場：
装置／設備名称　　：硫安プラント
スタディノード No.　：N-01　反応セクション
スタディノード概要　：建家内に設置された反応器、硫酸水溶液供給システム、アンモニア水溶液供給システム、硫安（AMS）溶液タンクおよび払出しライン
設計意図／運転条件　：硫酸とアンモニアを反応させて硫安（AMS）を製造し、AMS タンクに抜き出し後、出荷設備に移送する
P&ID No.　　実施日：2007.5.24

システム	機器	機器情報	故障モード	システム機能／安全への影響	影響度ランク	考慮されている対策	アクション No.	安全対策検討項目	担当
1 硫酸水溶液供給システム ・供給タンク D-1 ・供給ポンプ P-1 ・供給ライン ・流量比制御弁 FrCV-1A（アンモニア水溶液の流量が追随する）	1.1 流量比制御弁 FrCV-1A	常時運転、材質は硫酸仕様	1.1a 故障全開	（1）反応器に過剰硫酸水溶液流入、オフスペック製品（高硫酸濃度）	中	硫酸水溶液ラインに流量計、AMS 製品分析	A1.1-1	硫酸水溶液流量高による反応セクション緊急停止／アラームの設置検討	プロセス
				（2）供給タンクが空となり、供給ポンプが空引きし損傷する可能性	中	供給タンクに液面計	A1.1-2	AMS タンク液面低による供給ポンプ緊急停止／液面低アラームの設置検討	プロセス
				（3）反応器または AMS タンクの液面上昇、溢流の可能性	中	オペレータによる AMS タンクの監視	A1.1-3	AMS タンク液面高による反応セクション緊急停止／液面高アラームの設置検討	プロセス
				（4）アンモニア水溶液流量が追随増加し、反応器の温度／圧力上昇、破壊の可能性	大	反応器に安全弁（大気放出）	A1.1-4	反応器圧力高／温度高による反応セクション緊急停止／圧力高・温度高アラームの設置検討	プロセス
			1.1b 故障全閉	（1）流量計故障（誤信号）による全閉の場合、硫酸水溶液の供給停止とともにアンモニア水溶液の供給も停止し、反応停止に至る	中	硫酸水溶液ラインに流量計	A1.1-5	硫酸水溶液流量低による反応セクション緊急停止／流量低アラームの設置検討	プロセス
				（2）機械的故障による全閉（固着）の場合、アンモニア水溶液の供給は継続するので、AMS タンクにアンモニア水溶液が流入し、建家内にアンモニア蒸気発生、中毒危険	大	建家内にアンモニア検知警報器	A1.1-6	密閉式 AMS タンクの採用検討、建家内換気設備の能力増強を検討（緊急時対応）	機械／建築
			1.1c 固着（作動停止）	（1）全開状態または全閉状態で固着した場合は、上記 1.1.a または 1.1.b に同じ		流量比制御弁の定期保守、	A1.1-7	現在の定期点検／保守手順の見直し（FrCV-1A/B に適切か）	保守
				（2）通常時開度で固着した場合は、他の異常が同時発生しない限り大きな影響なし	小	流量比制御弁の定期保守、		A1.1-7 におなじ	
			1.1d 外部漏洩	（1）建家内に少量の硫酸蒸気発生、薬傷危険	中	流量比制御弁の定期保守、制御弁材質は酸仕様		A1.1-7 におなじ	
	1.2 硫酸水溶液供給タンク D-1		省略						
	1.3 硫酸水溶液供給ポンプ P-1		省略						
	1.4 硫酸水溶液供給ライン		省略						

（1）解析条件を設定する（そのプロセスを構成する機器の特定、機器の運転状態／運転条件、考慮しない故障モード／影響／安全対策など）潜在危険性を特定する（火災、爆発、毒性ガス流出など）。
（2）ひとつの機器を選び、形式、運転条件等の機器情報を把握する。
（3）その機器に考えられる故障モードをすべて洗い出す。何らかの操作を行う場合は、誤操作モードも特定する。
（4）各故障モード、誤操作モードごとに故障箇所における直接的な影響、他の機器およびシステム全体に対する機能および安全上の影響を特定する（この場合、安全対策はないものと仮定する）。
（5）FMECA の場合は、次に影響度ランクを決める（大、中、小など）。
（6）考慮されている故障／誤操作に対する予防的な対策および影響を緩和する対策を洗い出す。
（7）最後に、安全対策の改善、追加等に関する検討事項を提案する。

表 7 に硫酸アンモニウム（硫安）プラントにおける硫酸水溶液供給システムに対して FMEA を実施した事例（一部）を示す。この表には仕切り弁等における誤操作についての解析結果は示されていないが、それらを含めると FMEA は、HAZOP と同程度の解析結果が得られることを示唆している。

表 8　誤操作解析（HRA）における性能形成因子と誤操作誘発状態

性能形成因子の分類	誤操作誘発状態
設備、機械	e1　不適切なレイアウト e2　不適切、操作不可能、間違いやすい計装、計器 e3　集団的な定型からの逸脱（左ねじ） e4　不適切な物理的制限（酸とアルカリの接続口が同じ口径） e5　機能性を犠牲にした外観（オペレータに役立つテープ、マークの禁止） e6　不適切なラベル表示 e7　使えなくなっている機器（保守ミス、故障、劣化） e8　不適切な工具 e9　滑りやすい床
作業手順	m1　不適切な運転・作業手順 m2　不適切なフィードバック m3　難しすぎるタスク m4　誤操作機会の多すぎるタスク m5　たいくつな長時間の監視 m6　連絡の不徹底
工場ポリシー	p1　ポリシーと実際の作業との矛盾 p2　矛盾した優先順位 p3　神経質すぎる統制
作業者自身	h1　知識不足（教育・訓練不足、不適格、） h2　技能・技術力不足（教育・訓練不足、不適格） h3　思慮不足（怠慢、過信、他人依存、不注意、配慮不足、見落とし、） h4　体調不良（病気、疲れ、眠気、） h5　心理状態不良（あわて、あせり、やる気なし、気がかり、反発、イライラ）

解析問題:　オペレータ操作ーⅠ＝基本タスク１＋基本タスク２＋基本タスク３
（すべての基本タスクに成功しなければオペレータ操作ーⅠは達成されない。）

オペレータ操作ーⅠ　：原料供給タンクから原料をポンプでプロセスに供給する。
基本タスク１　：作業開始に備え、現場に待機する。
基本タスク２　：現場の電話でプロセス側からの起動指令を受ける。
基本タスク３　：ポンプを起動する。
基本タスク2失敗に対する安全対策　：プロセス側から現場に向かう。

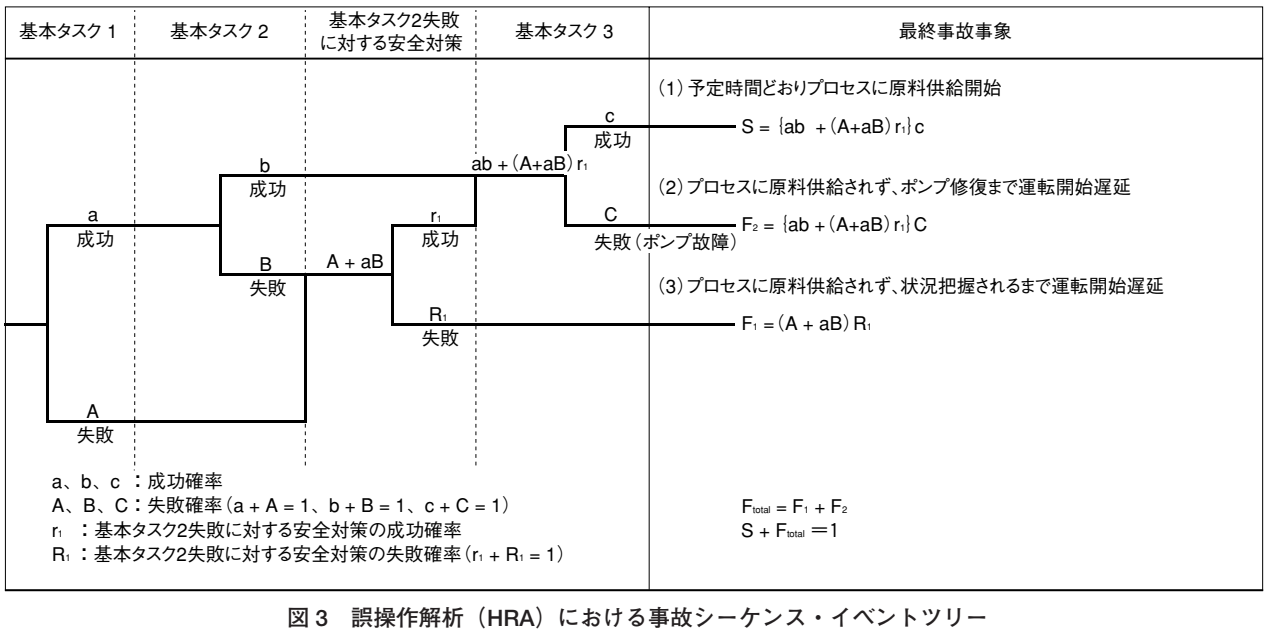

図 3　誤操作解析（HRA）における事故シーケンス・イベントツリー

作業安全解析／誤操作解析（JSA/HRA）

これらの手法は、人間の失敗に起因する潜在的事故の特定に用いられる。オペレータの誤操作は、What-If、HAZOP、FTA などでも扱われるが、これらの手法では、誤操作はどちらかといえばプロセスや設備への影響、すなわちハード面における潜在事故に焦点が当てられる。

これに対して、作業安全解析（JSA）は、要求された作業を実行する個々の作業者の安全確保に焦点をあてる。解析の対象は、操作・作業手順、作業環境、作業機具・機械などである。独特の特定手法はなく、チェックリストや What-If などの手法が用いて、機器や設備の運転・操作や各種作業の過程における誤操作や、使用する機具類、運転設備、周辺構造物等と作業者の間の不適合による潜在的な不安全状態を洗い出し、作業者に対する影響・結果の重大さを評価する。

一方、誤操作解析（HRA）は、What-If や HAZOP と同様にプロセスの安全性評価を目的とする。しかしながら、What-If や HAZOP が主として機械－機械系（マシン－マシン・インタフェース）の不具合を対象とするのに対し、HRA は人間－機械系（ヒューマン－マシン・インタフェース）における誤操作を対象とし、誤操作の要因とオペレータおよびプロセス・機器双方に対する影響を特定する。

誤操作の要因分析においては、まず人間の性能に影響を与える因子（性能形成因子）に着目する。性能形成因子は、個性や熟練度など作業者個人の内的な因子と、工場ポリシー、要求タスク、設備設計、設備状態、教育・訓練など外的な因子に分かれる。この性能形成因子が作業者の能力、限界あるいはニーズに適合していない場合（誤操作誘発状態という）、作業者はミスを犯しやすくなると考え、作業の各ステップにおいて誤操作誘発状態を特定し、それらを排除し誤操作を防止するための対策を提案する。**表 8** に、性能形成因子と関連する誤操作誘発状態の類型を示す。

HRA は通常、次の 3 段階の分析で構成される[5]。

①エルゴノミクス分析：設備設計、レイアウト、プロセス操作、作業環境等について作業者のニーズ、限界に適合していない項目を洗い出す。

②タスク分析：各作業手順（必要ならいくつかの基本タスクに分割）について、What-If などにより作業者の失敗事象（実行しない、遅い、早い、不適切、他のことをする等）を洗い出し、失敗事象に関連する誤操作誘発状態とタスク失敗の影響・結果を特定、既存安全対策を評価し改善事項を提案する。

③誤操作事故シーケンス分析：ひとつの作業を構成する基本タスクの成功・失敗による最終的な事故の形態とそこに至る経路を HRA イベントツリーまたは従来のイベントツリーにより分析する。基本タスクの失敗確率データから各事故シーケンスの発生確率を推定し、ランク付けすることができる。従来のイベントツリーによる分析例を**図 3** に示す。

HRA は単独の誤操作解析として活用できるが、他の方法と組み合わせればより有効な結果が得られる。たとえば、HAZOP、FMEA、FTA などによって重大な結果をもたらす誤操作を特定したあと、HRA によってその誤操作の要因について詳細に分析するやりかたが推奨される。

潜在危険性の特定手法の比較

最後に、これまで説明した潜在危険性の特定に使用できる 6 つ手法について、特徴、適用、分析結果などを比較したものを**表 9** に示す。

本連載の第 1 回目でも述べたが、最近の安全法規の改正によって要求されている既設化学プラントの潜在危険性の特定・把握作業を行う場合は、チェックリスト、What-If、HAZOP、FMEA/FMECA、あるいは JSA/HRA の中から対象設備のプロセスや運転の特性を考慮して適切なものを選定すればよいことが、この表からもわかる。

参考文献

4）WASH-1400 "Reactor Safety Study: An Assessment of Accident Risks in Commercial Nuclear Power Plants", October 1975

5）Guidelines for Hazard Evaluation Procedures Second Edition with Worked Examples, 1992, Center for Chemical Process Safety （CCPS） of American Institute of Chemical Engineers （AIChE）

表 9　潜在危険性の特定手法の比較

項目		予備的危険性評価（PHA）	チェックリスト	What-If	HAZOP	故障モード影響解析（FMEA/FMECA）	作業安全解析／誤操作解析（JSA/HRA）
1	手法のベース	・思いつき	・過去の事例、経験	・思いつき	・機械的、自動的	・過去の事例	・思いつき
2	分析の方法、手段、工夫	・危険性キーワードリスト（事前準備要）	・潜在危険性チェックリスト（事前準備要）	・What-If 質問（機器故障、誤操作、事故事象など）、 ・What-If 質問リスト	・HAZOP ガイドワード（なし、逆、増、減、過多、過少、以外）、 ・ずれリスト	・機器の故障モード	・タスク分析、 ・性能形成因子、 ・誤操作誘発状態、 ・イベントツリー
3	専門知識または経験の必要性	低い	高い	低い	高い	高い	高い
4	分析作業の所要時間	短い	中間	中間	長い	長い	長い
5	分析作業の所要人数	1 人またはグループ	1 人またはグループ	グループ	グループ	グループ	グループ
6	分析の対象（スタディノード）	工場、装置、設備、 プロセスセクション	工場、装置、設備、 プロセスセクション	装置、設備、プロセスセクション	プロセスライン	プロセスセクション、機器	装置、設備、 操作／作業手順
7	分析の出発点	危険性キーワードの特定（例：毒性流体の流出）	チェックリストの各チェック項目	What-If 質問の創出（例：もしポンプが停止したら？）	設計意図からのずれ（例：流れなし）	故障モードの特定（例：弁の故障開、閉、固着、リーク）	作業手順項目に対する What-If 質問の創出
8	考慮される潜在危険性の原因 ① プロセス内部の現象 （プロセス異常、運転異常）	○ 考慮	○	○	○	×	×
	② プロセス外部の現象 （漏洩、流出、火災、爆発）	○	○	○	× 考慮しない	×	×
	③ 計器、機器の故障	△ 場合により考慮	○	○	○	○	△
	④ 機器、配管の損傷、破壊	○	○	○	×（1）	○	△
	⑤ 誤操作	△	○	○	○	△	○
9	得られる分析結果 ① 考えられる原因	○ 含む	×	×	○	○	○
	② 起こりうる結果	○	○	○	○	○	○
	③ 既存安全対策	× 含まない	×	○	○	○	○
	④ 調査・検討事項	○	○	○	○	○	○
	⑤ リスクランク、重要度等	○	×	×	○	○	○
10	手法に適した時期 ① 概念設計段階	◎ 最適	○	◎	×	×	×
	② 基本設計段階	○ 適	○	◎	○	○	○
	③ 詳細設計段階	× 不適	◎	○	◎	◎	◎
	④ 建設、工事段階	×	◎	○	×	×	◎
	⑤ 運転段階	×	◎	○	◎	◎	◎
備 考					（1）熱交換器チューブのピンホール、破壊は考慮（内部現象）