SE Report

供用状態にある石油化学・石油精製プラントのリスクアセスメント

九州大学名誉教授

松山　久義 Hisayoshi Matsuyama

1. はじめに

2011年[1] と2012年[2),3)] に石油化学プラントで重大事故が発生した後、各方面から供用状態にあるプラントのリスクアセスメントの重要性が指摘された。しかし、方法論が確立しているのは、プラントの機能設計終了時に行われるリスクアセスメントだけであって、供用状態にあるプラントのリスクアセスメントについては、確立した方法論が存在しない。

したがって、その後約10年間にわたって、各事業所は独自に方法論を模索して来た。その結果、危険源の特定に関しては、HAZOP（Hazard and Operability Studies）に頼るだけでなく、HAZOP では特定できない危険源で、かつ、事故原因の90％以上[4)] を占める “漏洩” の特定に努力が注がれるようになるという望ましい状態になった。

しかし、最終事象の発生頻度の推算に関しては、LOPA（Layer of Protection Analysis）が与える初期事象の発生頻度の数値、および、防御層の失敗確率の数値を用いる事業所が、未だに多数存在するという残念な状態にある。

本稿では、プラントの機能設計終了時のリスクアセスメントと供用状態にあるプラントのリスクアセスメントの目的の相異を示し、後者において、LOPA の与える数値を用いることが誤りである理由を説明し、さらに、後者において使用すべき決定論的アプローチを紹介する。

2. リスクアセスメントの手順

リスクアセスメントの手順を**図1**に示す。手順（4）で求めた初期事象の発生頻度と防御層の失敗確率から、手順（5）において最終事象の発生頻度を評価するときには “多重防御層”[5)] を用いると便利である。多重防御層は、スイスチーズモデルを、石油化学・石油精製プラントにおける事象の進展を表現するために具体化したもので、その概念図を**図2**に示す。

一般に、着目する最終事象の引金になる初期事象は複数個存在し、対象プラントで発生する可能性のある最終事象も複数個存在するので、対象プラントにおける事象の進展を表現する多重防御層は、**図3**のような構造になる。

図2に示した概念図では、第3層が第2層をバックアップするように描いてあるが、第2層が第3層をバックアップするように設計されている場合もあるので、**図3**では、第2層と第3層に順序を付けずに1つのボックスの中に示した。また、リスクアセスメントでは、第4層の効果を評価しないので、第4層は省略した。

多重防御層を利用すると、確率論に従って、着目する最終事象の発生頻度 s_k は、**式（1）**によって与えられる。

図１　リスクアセスメントの手順

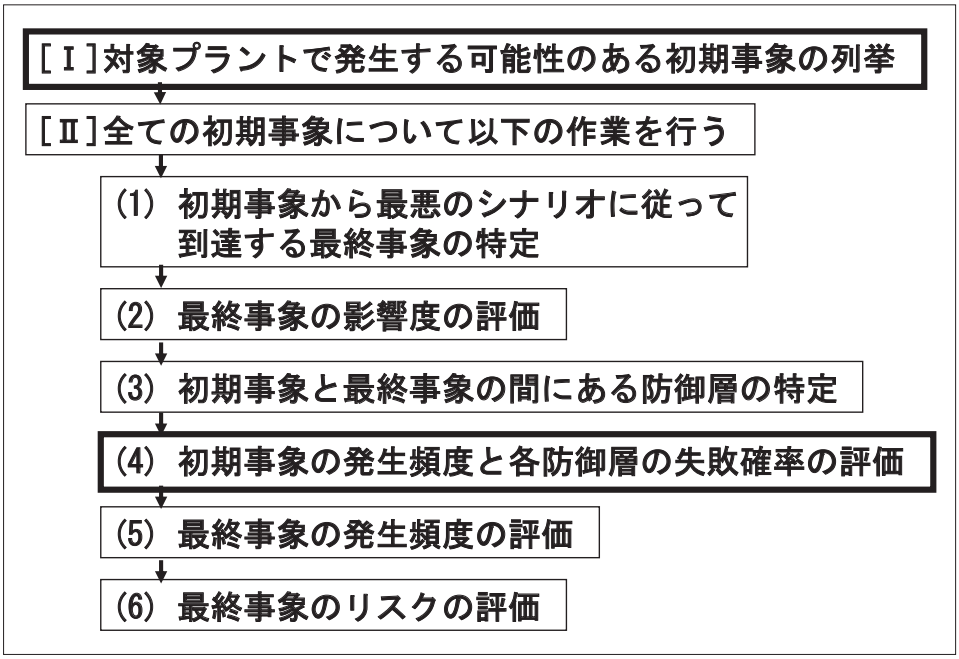
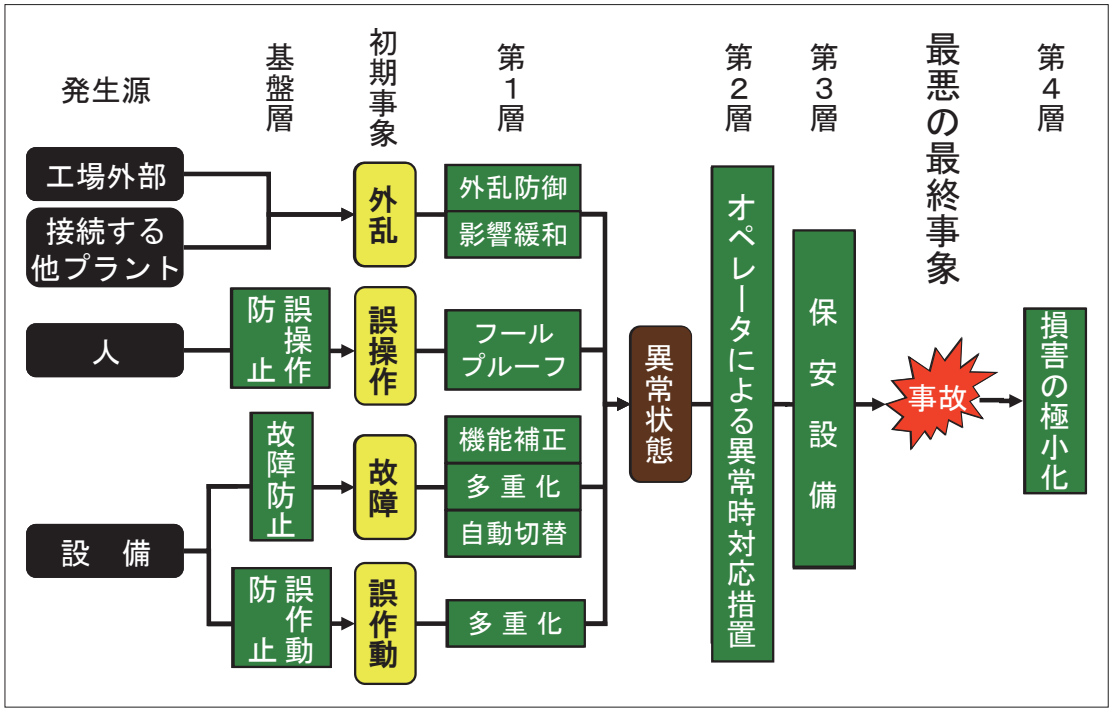


図２　多重防御層の概念図



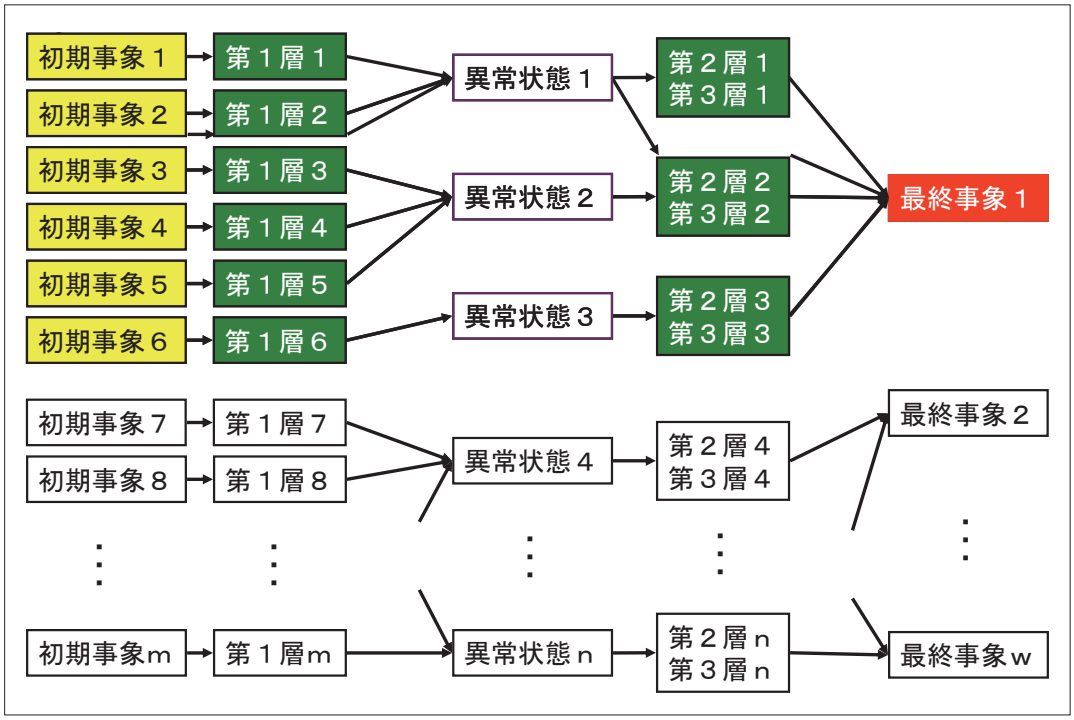
$$s_k = \sum_{j \in J_k} \left[\left(\sum_{i \in I_j} f_i p_i \right) q_j r_j \right] \qquad (1)$$

ここで、f_i は初期事象 i の発生頻度、p_i は第1層 i の失敗確率、q_j は第2層 j の失敗確率、r_j は第3層 j の失敗確率、I_j は異常状態 j の原因となる初期事象の添字の集合、J_k は最終事象 k に到達し得る異常状態の添字の集合である。また、存在しない防御層については、その失敗確率を1と定義する。

3. 機能設計終了時のリスクアセスメント

プラントのライフサイクルは、設計、製作、建設、供用、廃棄の5つのフェーズに分割される。設計のフェーズは、さらに、機能設計

図３　多重防御層の一般的構造



と詳細設計とに分割される。機能設計とは、プラントを構成する各アイテムの機能と容量を決定し、アイテム間の結合状態を P&ID（Piping and Instrumentation Diagram）として表現するフェーズである。

機能設計終了時に、機能設計の保安上の弱点（防御層の不足）を探索するためにリスクアセスメントが行われる。その手順は**図1**に示したとおりであり、手順［Ｉ］については、HAZOP と呼ばれる手法が実用化されている。

また、手順（4）においては、初期事象の発生頻度と防御層の失敗確率の数値が必要になるが、ベンダーが提供する故障確率や、AIChE/CCPS（米国化学工学会、AIChE：American Institute of Chemical Engineers/化学プロセス安全センター CCPS：Center for Chemical Process Safety）が推奨する LOPA によって与えられる数値を用いる。LOPA は、対象プラントに類似の健全なプラントにおける実績等から、初期事象の発生頻度と防御層の失敗確率の数値を推算する方法論である。以上のように、機能設計終了時のリスクアセスメントは、HAZOP、LOPA 等の方法論とともに確立されている。

4. 供用状態におけるリスクアセスメント

供用状態におけるリスクアセスメントは、供用状態（運転、検査、4M[※1]条件の変更、補修・改善工事等）の保安上の弱点と、設計、製作、建設から受継いだ保安上の弱点を探索するために行われる。確率論的アプローチによれば、詳細設計、製作、建設、供用の保安上の弱点は、初期事象の発生頻度の増大、防御層の失敗確率の増大として顕在化することになるので、次に示す2つの難問に遭遇する。

【難問1】

影響度の大きな最終事象（事故）のリスクが許容できることを示すためには、対象プラントでは発生したことがない初期事象の発生頻度の数値、および、失敗したことがない防御層の失敗確率の数値を求めて、それらが極めて

※1
4M
4M とは、物事を Man（人）、Machine（機械）、Material（材料）、Method（方法）の4つの要素で考える手法

小さいことを示さなければならない。

【難問2】

リスク低減活動の効果は、初期事象の発生頻度の低下、あるいは、防御層の失敗確率の低下として顕在化するはずであるから、それらの数値を求めてリスク低減活動の効果を確かめなければならない。

難問1に対して、多くの事業所で採用されている誤った解決法は、初期事象の発生頻度と防御層の失敗確率の数値として、LOPA が与える数値を用いることである。LOPA が与える数値は、健全なプラントの実績等から推算した数値であるので、それらを用いてリスクアセスメントを行っても、機能設計の保安上の弱点（防御層の不足）しか見付けることができない。

詳細設計、製作、建設、供用に保安上の弱点があれば、初期事象の発生頻度、および、防御層の失敗確率が増大するはずであるから、LOPA の与える数値で代用できるはずがない。

5. 決定論的アプローチ

難問1と難問2を解決するために、現在利用できる化学・物理的知識、および、標準化された技術的知見（規格、技術標準等）によって導かれた“初期事象が発生しないための条件”、および、“防御層が失敗しないための条件”を基にした決定論的アプローチを採用する。

決定論的アプローチでは、初期事象の発生頻度、および、防御層の失敗確率を**表1**、および、**表2**のように定義する。発生頻度1～3、および、失敗確率1～3については、対象プラントにおける着目する初期事象の実績、および、着目する防御層の実績から決定することができる。また、初期事象の発生頻度0は、初期事象が発生しないための条件が満足されていることを表し、防御層の失敗確率0は防御層が失敗しないための条件が満足されていることを表す。

確率論的アプローチで遭遇する難問1は、決定論的アプローチでは、初期事象が発生しないための条件が満足されていること、および、防御層が失敗しないための条件を満足されていることを示すことで解決できる。

表1と**表2**のように、初期事象の発生頻度と防御層の失敗確率を定義すると、最終事象の発生頻度 s_k は**式（2）**で与えられる。使用した記号の意味は、**式（1）**と同様である。ただし、防御層が存在しない場合には、それの失敗確率を3と定義する。

$$s_k = \underset{j \in J_k}{\mathrm{Max}} \left[\mathrm{Min} \left\{ \underset{i \in I_j}{\mathrm{Max}} \mathrm{Min}(f_i, p_i), q_j, r_j \right\} \right] \quad (2)$$

式（2）によって得られた最終事象の発生頻度の意味は、**表1**に示した初期事象の発生頻度の定義と全く同じである。

最終事象の重要度の分類とリスクレベルの分類は、企業、事業所、対象プラントによって異なる可能性があるが、ここでは、重要度

表 1　初期事象の発生頻度の定義

発生頻度	定　義
3	発生したことがあり、復元しただけで再発防止策は未実施
2	発生したことがあり、再発防止策は実施したが再発しないという保証がない
1	発生したことはないが、発生しないという保証がない
0	次回定期修理まで、発生しないという保証がある

表 2　防御層の失敗確率の定義

発生頻度	定　義
3	失敗したことがあり，復元しただけで再発防止策は未実施
2	失敗したことがあり，再発防止策は実施したが再発しないという保証がない，あるいは，作動したことがない
1	作動したことがあり，失敗したことはないが，失敗しないという保証がない
0	次回定期修理まで，失敗しないという保証がある

については5段階、リスクレベルについては4段階に分類した例を、それぞれ、**表3**と**表4**に示す。また、最終事象の発生頻度、重要度、リスクレベルの関係を表すリスクマトリックスの例を**表5**に示す。

リスクの低減活動は、初期事象が発生しないための条件を満足させる活動か、防御層が失敗しないための条件を満足させる活動であり、その効果は、**式（2）**に代入するだけで確認できる。このようにして、決定論的アプローチを用いれば、難問2も解決できる。

6. まとめ

プラントの機能設計終了時に行われるリスクアセスメントと供用状態にあるプラントのリスクアセスメントの目的の相異について述べ、後者に対して LOPA により与えられる初期事象の発生頻度の数値、および、防御層の失敗確率の数値を用いることが誤りであることを説明した。

また、後者については、確率論的アプローチではなく、決定論的アプローチを採用すべきであることを示し、その手続の概略について紹介した。

決定論的アプローチの基盤となるのは、“初期事象が発生しないための条件” と “防御層が失敗しないための条件” である。これらの条件を探索することは、安全工学の重要な役割の1つであると考える。

表 3　最終事象の影響度の分類の例

影響度	定　義
A	死亡者発生
B	事故であり、死亡者は発生しないが、人的・物的損害発生
C	法的には事故であるが、人的損害が無く、物的損害も軽微
D	法的には事故ではないが、生産性、品質に関する損害発生
E	法的には事故ではなく、生産性、品質に関する損害も軽微

表 4　リスクレベルの分類の例

リスクレベル	定　義
Ⅳ	直ちに操業を停止すべきである
Ⅲ	許容できないので、次の機会に必ずリスク低減策を実施すべきである
Ⅱ	暫定的には許容できるが、出来るだけ早く、リスク低減策を立案して実施すべきである
Ⅰ	永続的に許容できる

表 5　リスクマトリックスの例

影響度　小 ⟷ 大

発生頻度	E	D	C	B	A
大 3	Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅳ
↕ 2	Ⅰ	Ⅱ	Ⅱ	Ⅳ	Ⅳ
↕ 1	Ⅰ	Ⅰ	Ⅱ	Ⅱ	Ⅲ
小 0	Ⅰ	Ⅰ	Ⅰ	Ⅰ	Ⅰ

参考文献

1）竹田裕二：第二塩化ビニルモノマー製造施設爆発火災事故とその後の取組み，高圧ガス，55（4），342-347，2018.
2）穂坂真吾：レゾルシン製造装置の爆発火災事故，高圧ガス，55（3），233-237，2018.
3）田邊弘彦：アクリル酸製造施設の爆発・火災事故とその後の取組み，高圧ガス，55（11），1155-1160，2018.
4）小作幸生ら：高圧ガス事故の統計と解析（コンビナート等保安規則適用事業所），高圧ガス，59（11），850-854，2022.
5）松山久義：石油化学・石油精製のための TPM 活動（3）－安全衛生環境活動の補強（1），日本設備管理学会誌，33（1），29-36，2021.

まつやま●ひさよし

1968年東京大学工学系研究科博士課程単位取得退学。同大学工学部助手、同講師、九州大学工学部助教授、同教授を経て、早稲田大学情報生産システム研究科教授を2010年定年退職。2009年～2011年日本設備管理学会会長。1992年より高圧ガス認定検査実施者調査委員。専門分野：プロセスシステム工学