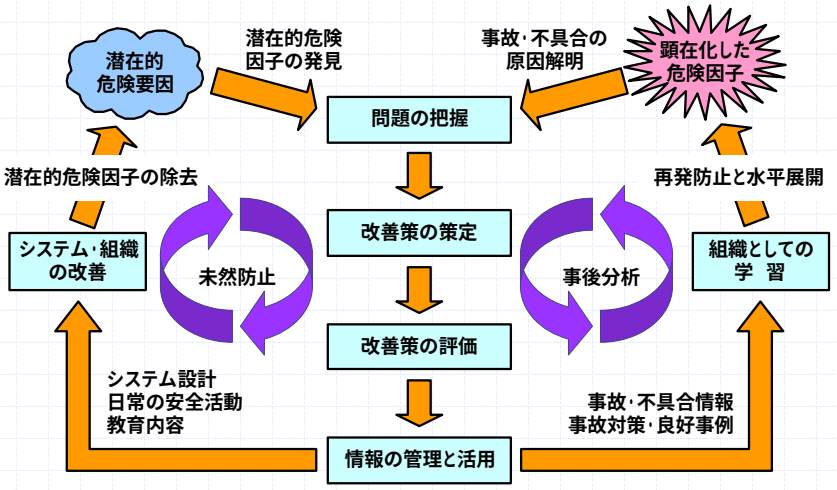
安全学基礎
ー ハザードの同定 ー

システム創成学科

リスク評価手法（1）

- 未然防止的手法
  - システムの運用開始前の設計段階で考えられる危険源とその影響を予測し、あらかじめ対策を立てて事故や不具合を防止する。
- 事後分析的手法
  - 事故や不具合が起きた後で、その原因を分析して再発防止や類似事象の防止（水平展開）を行う。

未然防止と事後分析



出展：吉村, 2002に基づく

リスク評価手法（2）

- 定性的手法／定量的手法
  - 結果を明示するという点で定量的評価は望ましいが、改善策の策定には定性的評価が不可欠であるし、評価には非明示的前提が存在することを忘れてはいけない。
- 決定論的手法／確率論的手法
  - 不確かさや知識の不完全性から、確率論的手法による裏付けは不可欠であるが、実務上は決定論的手法が実用的である。

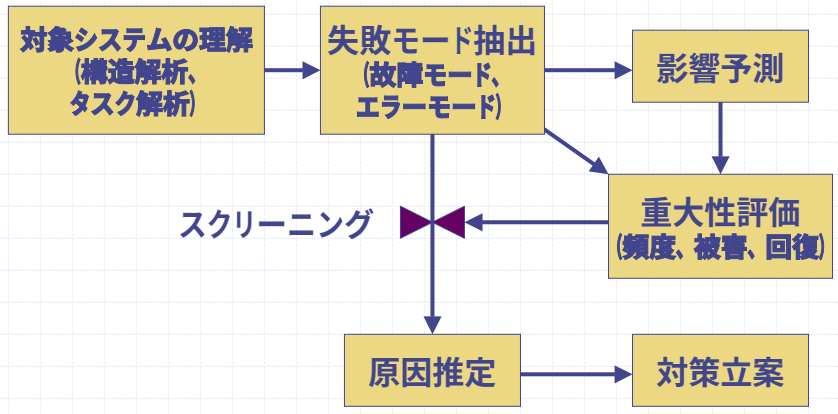
リスク評価の手順

1. 目的、システム、損害の定義
2. ハザードの同定
   what-if分析、FMEA、HAZOP、・・・
3. システムのモデル化
   ETA、FTA、GO、GO-FLOW、DFM、・・・
4. リスクの定量評価
5. 感度解析、不確かさ解析
6. 結果の文書化

FMEA（失敗モード影響解析）

- システムの各構成要素に生じる可能性のある失敗（故障、エラー）の形態を列挙し、それがシステム全体に与える影響を定性的に評価することによって、重大な危険源をボトムアップに特定する手法
- 1950年代に軍用航空産業で開発
- 機器故障にもヒューマンエラーにも適用可

FMEAの手順



FMEAワークシート

構成要素	失敗モード	影　響	重大性	原　因	対　策
冷却水ポンプ	停　止	システム全停止	5	電源喪失	補助電源
手動操作によるポンプ起動	起動遅れ	計画遅れ	3	技能不足	操作訓練

- **構成要素**
  - 階層構造を用いて、工学システムや人間が行うタスクを基本的構成要素に分解し、構成要素を網羅的に列挙する。

FMEAワークシート

構成要素	失敗モード	影　響	重大性	原　因	対　策
冷却水ポンプ	停　止	システム全停止	5	電源喪失	補助電源
手動操作によるポンプ起動	起動遅れ	計画遅れ	3	技能不足	操作訓練

◆故障・エラーモード

- 各構成要素（機器、操作）において発生する可能性がある失敗（故障、エラー）の形態を要素ごとに列挙する。

FMEAワークシート

構成要素	失敗モード	影　響	重大性	原　因	対　策
冷却水ポンプ	停　止	システム全停止	5	電源喪失	補助電源
手動操作によるポンプ起動	起動遅れ	計画遅れ	3	技能不足	操作訓練

◆影　響

- 失敗が発生した場合に、上位システムにどんな影響をあたえ、最終的にどんな損害に発展するかを失敗モードごとに記述する。FMEAでは同時に複数の失敗を考慮する必要はない。

FMEAワークシート

構成要素	失敗モード	影　響	重大性	原　因	対　策
冷却水ポンプ	停　止	システム全停止	5	電源喪失	補助電源
手動操作によるポンプ起動	起動遅れ	計画遅れ	3	技能不足	操作訓練

◆重大性

- 失敗モードごとに失敗の重大性を発生頻度、影響の重大性、回復の可能性など、いくつかの指標に基いて定性的・準定量的に評価して記述する。

FMEAワークシート

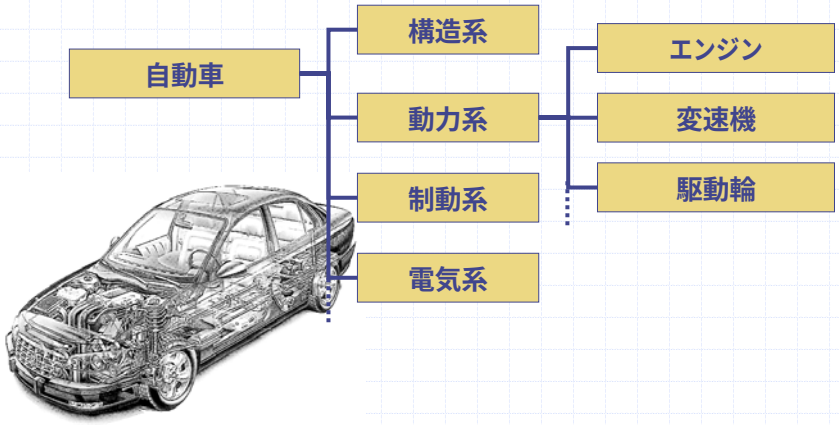
構成要素	失敗モード	影　響	重大性	原　因	対　策
冷却水ポンプ	停　止	システム全停止	5	電源喪失	補助電源
手動操作によるポンプ起動	起動遅れ	計画遅れ	3	技能不足	操作訓練

◆原因と対策

- 失敗の考えられる原因について記述する。また、失敗発生の防止策、拡大抑制策、影響緩和策などを記述する。

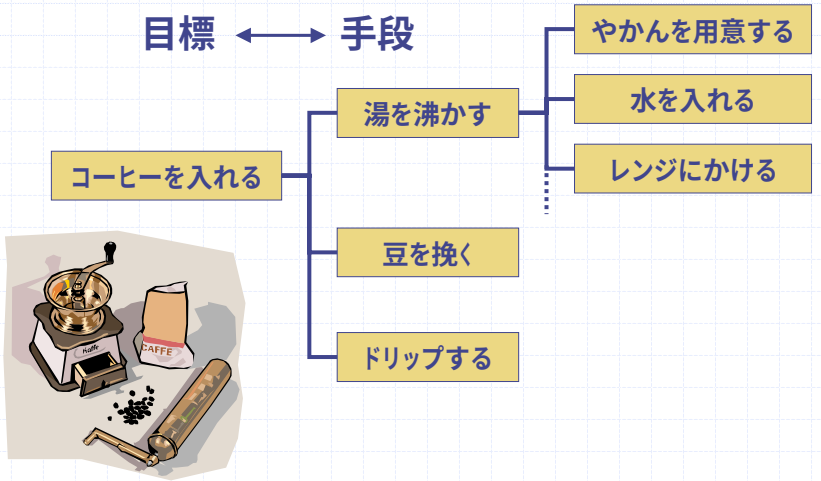
技術システムの全体部分階層

全体 ⟷ 部分



タスクの目標手段階層

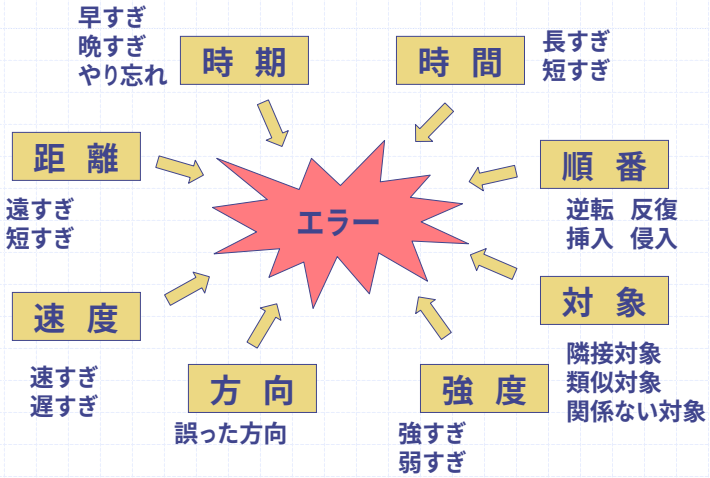
目標 ⟷ 手段



故障モード

- 過去の実績や類似設備機器の実績から、起り得る故障モードを予測
- 機械部品
  - 変形
  - 破損、破断
  - 摩耗
  - 腐食
  - 固着
  - 漏洩
  - ゆるみ、ずれ、振動
- 電気部品
  - 断線、開放
  - 短絡
  - 絶縁不良
  - 出力断、出力不足
  - 出力不安定
  - 発熱、過熱

エラーモード（基本的表現形）



出展：E.Hollnagel, 1993

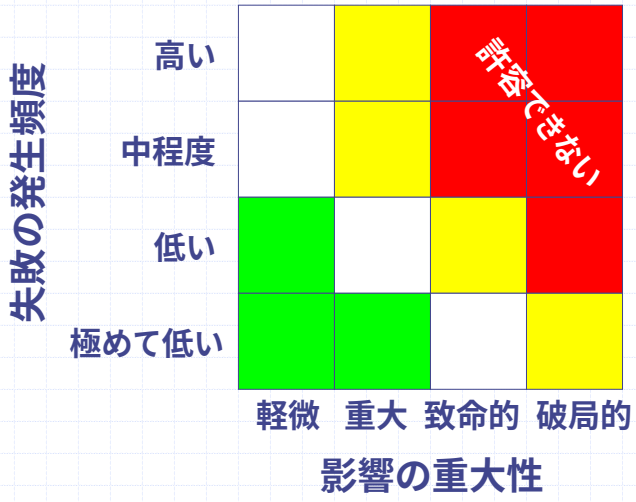
発生頻度の定性的評価

- 極めて低い
  - 運用期間中の発生は無視できる程度
- 低い
  - 運用期間中の発生はほとんど予想できない
- 中程度
  - 運用期間中に少数回の発生が十分予想される
- 高い
  - 運用期間中に繰り返し発生することが予想される

影響の重大性の定性的評価

- 軽微
  - システム運用にはまったく支障なく、直ちに復旧可能
- 重大
  - システム運用に支障を及ぼすが、容易に復旧可能
- 致命的
  - システム停止を余儀なくされ、復旧に長期間を要する
- 破局的
  - 周辺環境（第3者）に損害を与え、復旧は困難

重大性の総合評価（リスクマトリックス）



対策立案のためのガイド

- 発生防止策
  - その構成要素そのものを排除する。
  - 失敗発生の原因（環境）を排除する。
- 拡大抑制策
  - 失敗の影響伝播径路を排除する。
  - 失敗を検出して影響を機能的に封じ込める。
- 影響緩和策
  - 影響が発生しても大きくならないようにする。
  - 復旧の方法を考える。

HAZOP（ハザード操作性解析）

- FMEAが構成要素と失敗モードに着目するのに対して、プロセスパラメータとその偏差に着目する手法がHAZOP
- パラメータ、偏差、原因に関するガイドワードが用意されていていて解析に便利
- 1960年代に化学工業で開発

HAZOPワークシート

パラメータ	偏　差	影　響	重大性	原　因	対　策
入口流量	流量なし	プロセス停止	4	スラグの詰り	フィルターの設置
	流量減	出力低下	3	バルブの誤作動	定期点検の実施

- パラメータ
  - システム状態を規定するプロセスパラメータ（流量、圧力、温度、強度など）を網羅的に列挙する。

HAZOPワークシート

パラメータ	偏　差	影　響	重大性	原　因	対　策
入口流量	流量無し	プロセス停止	4	スラグの詰り	フィルターの設置
	流量減	出力低下	3	バルブ誤作動	定期点検の実施

◆偏　差
- 各パラメータの目的状態からのずれの形態を網羅的に列挙する。

ガイドワード
ー パラメータ、偏差、原因の網羅的組合せ ー

◆適用対象に応じて用意することが可能

◆ 流　量
- 過　大
  - ポンプ出力が過大
  - 入口圧力の上昇
  - 管路抵抗の減少
  - 流体密度の上昇
  - ・・・・・・・・・・
- 過　小
- な　し
- 逆　流

◆ 温　度
- 高すぎる
  - 気温の変化
  - 熱交換器の故障
  - 火災
  - ・・・・・・・・・・
- 低すぎる
  - 気温の変化
  - 圧力の低下
  - 熱交換器の故障
  - ・・・・・・・・・・