安全工学と失敗学

事故や災害をなくすための工学的取組み

安全工学

事故や災害を起こさないためにどうすべきかを考える工学分野

機械安全、電気安全、化学安全などの各分野において
装置、製品またはサービスなどの設計段階から、
製造、物流、消費、廃棄の各段階までの全工程をカバー

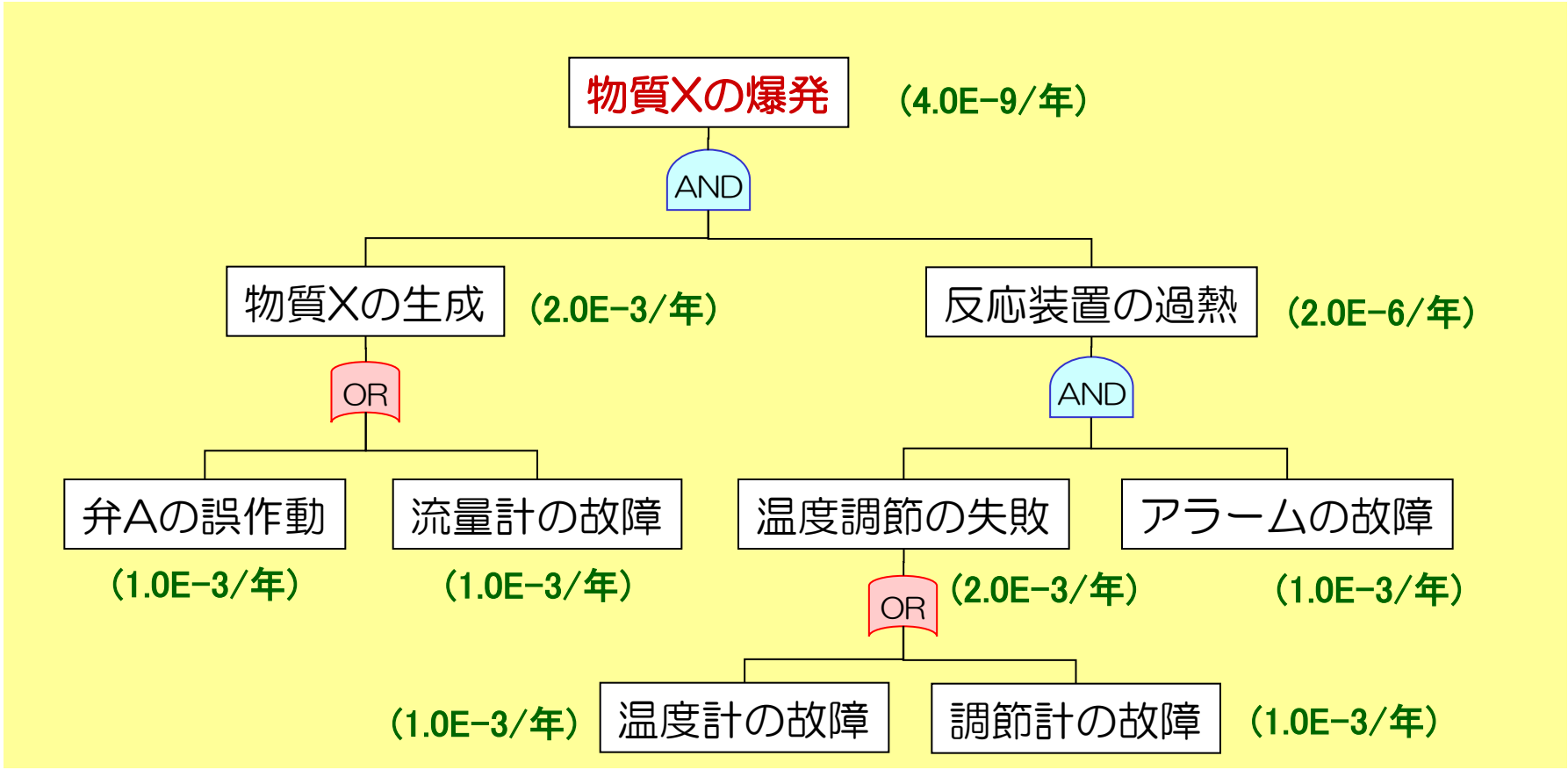
事故や災害発生の原因究明および事故や災害の発生防止
に必要な科学および技術に関する系統的な知識体系

過去の事故や災害を教訓とし、事故や災害を予防するため
の各種安全性評価手法や設計手法などが開発されてきた

安全性評価手法（1）

フォルトツリー分析（Fault Tree Analysis ： FTA）

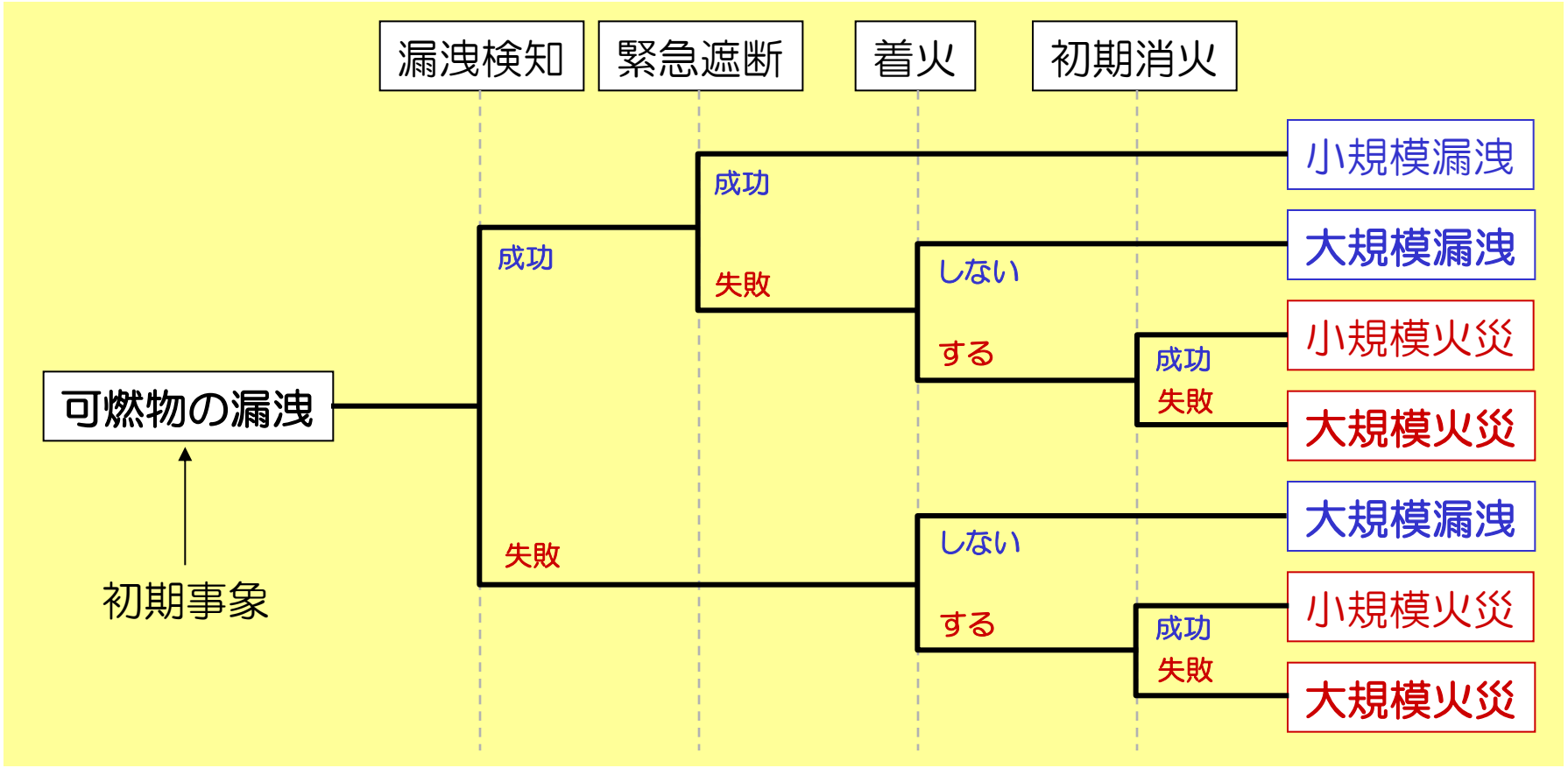
特定の頂上事象を想定し、その事象が発生する要因を
階層的に検討し、頂上事象の発生確率を定量的に解析する



安全性評価手法（2）

イベントツリー分析（Event Tree Analysis ： ETA）

まず初期事象を設定し、そこからの事故進展を考慮して
階層的に検討し、最終事象の発生確率を定量的に解析する



安全設計（1）

インターロック（Interlock）

安全が確認されたときに初めて機械の運転を許可、または危険を検知したときに機械を自動的に停止するシステム

- 蓋を開けると自動的に停止する洗濯機
- 蓋を開けるとスタートせず、自動的に停止する電子レンジ
- ギアがパーキングに入っていないとエンジンが掛からない自動車
- 冷却水が流れていないとスタートできない分析装置

フェールセーフ（Fail-Safe）

問題が発生しても自動的に安全側で停止するシステム設計

- 転倒したときに自動的に消火するストーブ
- センサが故障したら自動的にシャットダウンするシステム
- 停電時には初期状態に戻し、通電後に自動復帰しないシステム
- 手を離すと自動的に止まるセルフガソリンスタンドのノズル
- 異常時には安全に壊れる装置（破裂板など）

安全設計（2）

フェールソフト（Fail-Soft）

故障が生じても全停止せず、機能の一部を保持して稼動を続行させる設計思想

フェールセーフは安全性を優先⇔フェールソフトは継続性を優先

- 一部のエンジンが停止しても安全に飛行を続ける航空機
- パンクしても短距離なら安全に走行できるランフラットタイヤ

フォールトトレランス（Fault-Tolerance）

システムの一部に不具合が起きても、予備の装置などにより正常な運転を継続する設計思想（多重化、冗長化）

- 油圧系や電気系を複数用意してある航空機の冗長設計
- ポンプが故障で停止しても自動起動する予備ポンプシステム
- 停電時には蓄電池から電気を供給する無停電システム（UPS）

安全設計（3）

フールプルーフ（Fool-Proof）

誰がどのように操作してもトラブルが起きない設計
うっかり誤操作や意図した省略操作等を防ぐことが目的
（一部はインターロックやフェールセーフと重複）

- 扇風機の羽根カバー
- ファイルを削除しようとすると警告が出るPCソフト
- 正しい向きにしか入らない形状の電池ボックス
- マンホールの丸い蓋
- 重要なスイッチは鍵を差し込まないとONにできないシステム
  （回転機器などの修理中に、間違ってONにならない）

失敗学

起きてしまった失敗の**原因究明**、**失敗防止**、および**失敗知識の配布**を通じて似たような失敗を起こさないための学問分野

過去の多くの事故、災害、不祥事、その他の失敗事例を集め、失敗の種類、原因、シナリオを分類する

過去の事例を分類別に整理することで、人間が陥り易い過ちを教訓として抽出する

これを元に、新たな設計や作業などにおける同様の失敗を防止する（多くの失敗は過去に同様の失敗事例がある）

過去の失敗事例は「**失敗知識データベース**」として一般に公開し、積極的な活用を促す

失敗の分類

1. 材料の破壊 2. 構造の倒壊 3. 構造の振動 4. 想定外の外力 5. 想定外の制約	設計時の技術的要因
6. 火災・天災からの逃げ遅れ 7. 連鎖反応での拡大 8. 冗長系の非作動	使用時の技術的要因
9. 作業で手を抜く 10. 設計で気を抜く 11. 個人や組織の怠慢 12. 悪意の産物	人的・組織的要因

失敗のシナリオ例

ヒューマンエラー（人的ミス）...41%

- 不注意 (33%)
- 手順を守らない (8%)

エンジニアの設計能力不良 ...94%

- 無知 (26%)
- 誤判断 (16%)
- 調査、検討の不足 (39%)
- 環境変化への対応不良 (8%)
- 未知 (4%)

組織の問題 ...73%

- 企画不良 (5%)
- 価値観不良 (37%)
- 組織運営不良 (30%)

安全工学と失敗学

安全工学

より安全なシステムを作り上げるための、安全性評価や安全設計のための学問

失敗学

過去の様々な失敗事例を蓄積・体系化し、失敗の起こる原因やメカニズムから対策を検討する学問

新たなシステム、製品、作業などを考える際に、事故防止のためには、一面的なアプローチではなく、多面的な検討が効果的

安全工学的なアプローチと失敗学的なアプローチの併用