Innovative R&D by NTT

リスク分析・評価手法について

2018.9.28

NTTセキュアプラットフォーム研究所

五郎丸秀樹

索引

1．社会セキュリティとリスクの関係

本発表の箇所

ISO31000 **リスクマネジメント**

IEC/ISO31010
リスクアセスメント技法

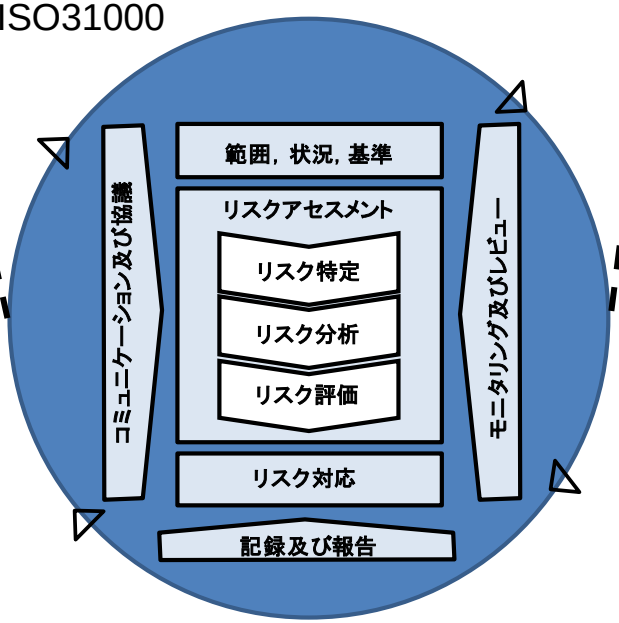
• • •

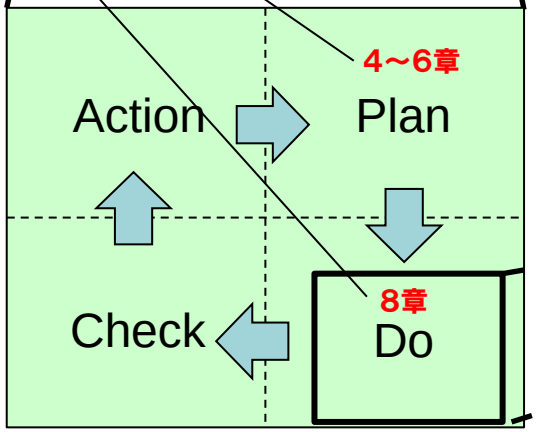
ISO22301
事業継続マネジメントシステム

ISO22320
緊急事態管理-危機対応

ISO22325
緊急事態管理能力の評価

• • •

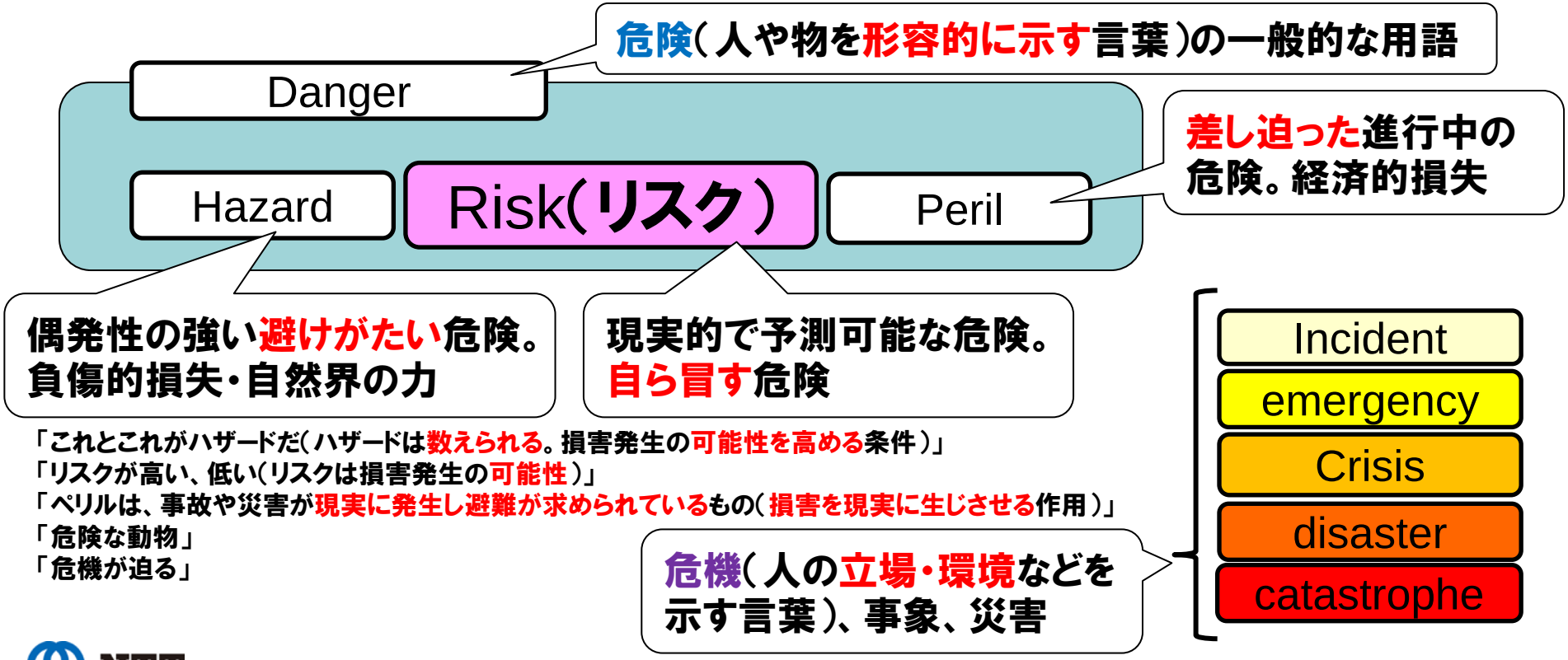




ISO22320
緊急事態管理-危機対応

2. リスクとは

- 「リスク」の言葉自体がリスク
  - 不明瞭で似た意味の言葉が多い
    - Risk(リスク): 自由意思で冒す危険「イタリア語：危険を冒す」「ラテン語：勇気をもって試みる」「アラビア語：明日の糧」



2. リスクとは

- 分野や時代によって使われ方が違う
  - 分野
    - 社会リスク：事業継続の中断・阻害による損失
    - 情報リスク：情報（紙も含む）の機密性、完全性、可用性の損失
    - サイバーリスク：情報システムの可用性の損失
    - 製品安全リスク：製品安全の損失
    - 環境リスク：環境の悪化
    - 金融リスク：投機により損失にも利得にもなりうる

    負の影響

    正の影響
  - 時代
    - 昔は限られた分野のみ使用
      - 1960年代以前では、宇宙開発、軍事産業などごく限られた分野でだけ使用
      - 1960年代末から米国国防省（DOD)の規格MIL-STDシリーズが産業界で活用
      - 1970年代に商用原子力施設の安全を評価するためにリスクアセスメントが実施
    - ISO/IECGuide73：2002のリスクの定義
      - 「事象の発生確率と事象の結果の組み合わせ」
        - » 備考1 用語「リスク」は一般的に少なくとも好ましくない結果を得られる可能性がある場合にだけ使われる
    - ISOGuide73：2009のリスクの定義
      - 「諸目的に対する不確かさの影響」
        - » 備考1 影響とは、期待されていることから良い方向・悪い方向へ逸脱すること

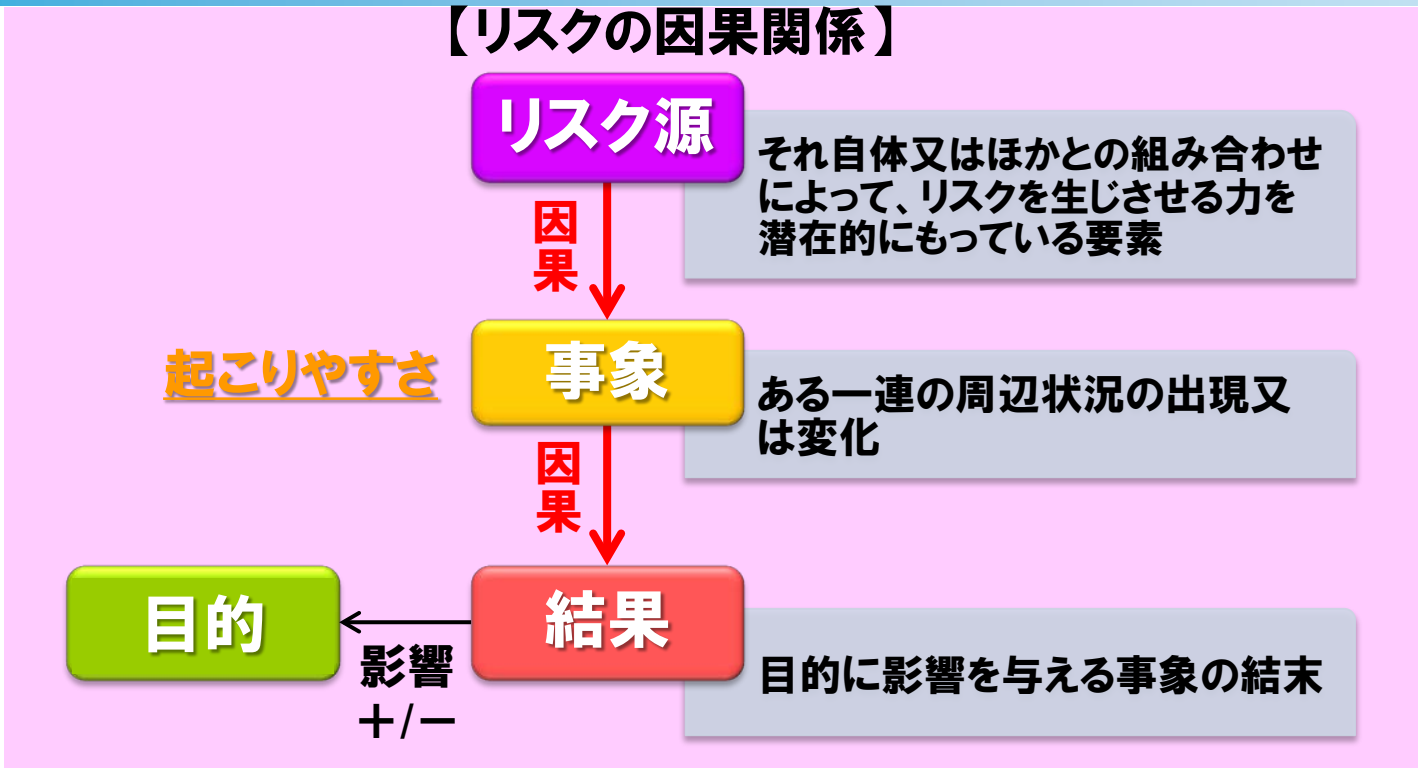
国際標準規格の最新版の汎用的な「リスク」を使用する

リスクの定義(ISO 31000)

- **リスク**
  目的に対する不確かさの影響

- **注記1　影響とは、期待されていることからかい(乖)離することをいう。影響は、好ましい方向、好ましくない方向および両方に進み、そして「機会と脅威」へと導いたり創造したり帰着したりすることがある。**
- **注記2　目的は、異なった側面とカテゴリーがあり、異なったレベルで設定されることがある。**
- **注記3　リスクは、リスク源、起こり得る事象、それらの結果、そしてそれらの起こりやすさとの組み合わせによって表現されることが多い。**

リスクの定義(ISO 31000)



- 注記1　影響とは、期待されていることからかい(乖)離することをいう。影響は、好ましい方向、好ましくない方向および両方に進み、そして「機会と脅威」へと導いたり創造したり帰着したりすることがある。
- 注記2　目的は、異なった側面とカテゴリーがあり、異なったレベルで設定されることがある。
- 注記3　リスクは、リスク源、起こり得る事象、それらの結果、そしてそれらの起こりやすさとの組み合わせによって表現されることが多い。

3．1　各業界の状況

航空業界

人的要因による分析評価手法をいち早く開発し大きく発展した

- 4M-4E
- RCA(根本原因分析)
- SHEL
- ASRS(航空安全報告システム)

原子力業界

炉心溶解に至る確率を計算するためリスク評価としてHRA(人間信頼性解析）が発展

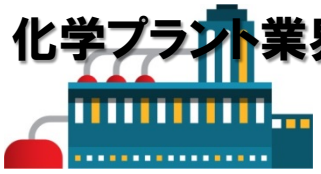
- HRA [THERP, ATHEANA]
- HPES，J-HPES
- H2-SAFER

医療業界

専門化・分業化により適用が遅れていたが，医療の実態に合わせ変更した分析評価手法が使われ始めた

- VA-RCA
- Medical-SAFER

化学プラント業界



規格などで分析評価手法としてHAZOPが推奨されていたため定着した

- HAZOP
- **相対危険度分析手法**
- **チェックリスト法**
- PHA

自動車業界

規格などで分析評価手法としてFMEAが業界で推奨されていたため定着した.

- FMEA
- FTA
- HAZOP

NTT

3．1　各業界の状況

航空業界

・4M-4E

各業界で**重視している箇所**に合わせて**独自に発展**

- 航空業界：人と**環境**（他の人，機械など）
- 原子力業界：人の**過誤率**
- 医療業界：**人的要因の特定**
- 化学プラント業界：正常時からの**逸脱の有無**
- 自動車業界：**評価対象**（ハードウェア，業務のプロセス等）

など

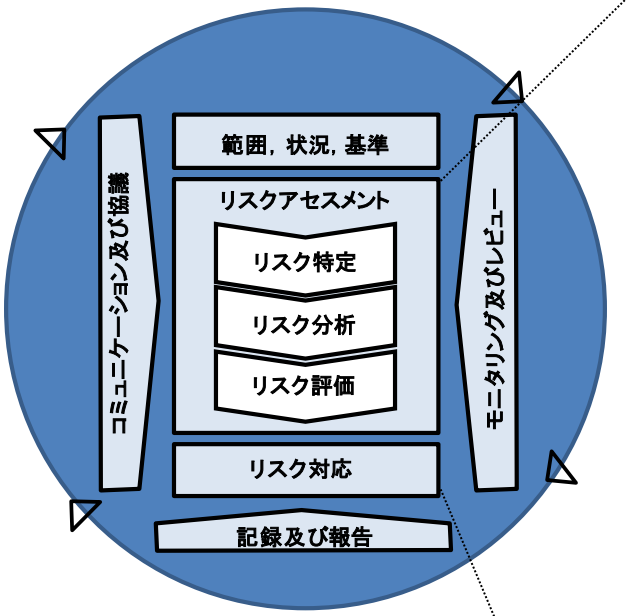
50種類以上存在し、乱立状態

自動車業界　規格などで分析評価手法として FMEAが業界で推奨されていた ため定着した.

・FMEA
・FTA
・HAZOP

3．2　分類について

ISO 31000



IEC/ISO 31010

分析評価手法
ブレーンストーミング
構造化又は半構造化インタビュー
デルファイ法
チェックリスト
予備的ハザード分析（PHA）
HAZOP スタディーズ
ハザード分析及び必須管理点（HACCP）
環境リスクアセスメント（毒性リスクアセスメント）
構造化“Whatif”技法（SWIFT）
シナリオ分析
事業影響度分析（BIA）
根本原因分析（RCA）
故障モード・影響解析（FMEA）
故障の木解析（FTA）
事象の木解析（ETA）
原因・結果分析（CCA）
原因影響分析（特性要因図（魚骨線図））
防護層解析（LOPA）
決定木解析
人間信頼性分析（HRA）
ちょう（蝶）ネクタイ分析
信頼性重視保全（RCM）
スニーク回路解析（SCA）
マルコフ解析
モンテカルロシミュレーション
ベイズ統計及びベイズネット
FN 曲線
リスク指標
リスクマトリックス
費用／便益分析（CBA）
多基準意思決定分析（MCDA）

手法は31種類

3．2　分類について

IEC/ISO31010の**分類は不十分**

- **リスクアセスメントの種類として6種類、リスク特定の方法として3種類示しているが、全てに適用しているわけではない。**
- **リスク特定の適用性について「適用不可」の部分もあるが、内容を見ると必ずしも適用不可とは限らない（例えばRCAでは背後要因を調べる営みであり、他の手法との違いが必ずしも明確ではない）。**

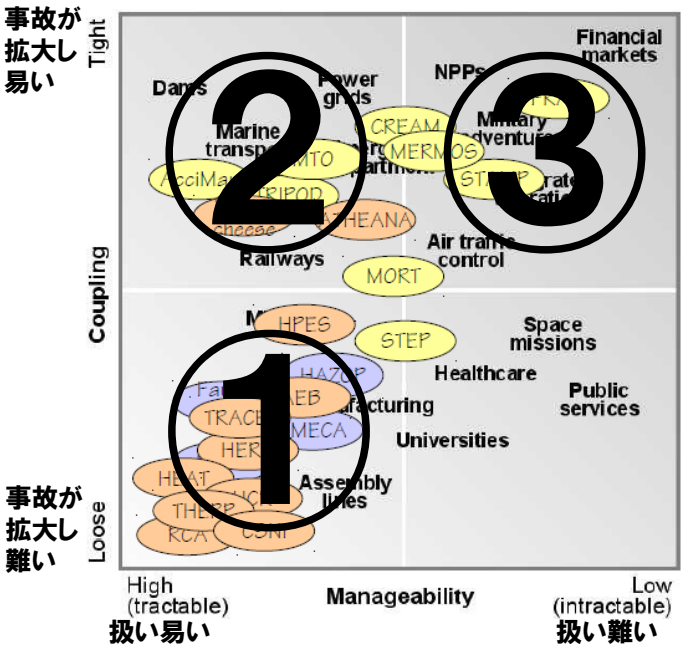
IEC/ISO 31010

分析評価手法	リスクアセスメントの種類	リスク特定方法	適用性
ブレーンストーミング	支援法		推奨
構造化又は半構造化インタビュー			
デルファイ法			
チェックリスト	洗出し法	証拠に基づく方法	
予備的ハザード分析（PHA）			
HAZOP スタディーズ	機能分析	系統的アプローチ・帰能的推論法	
ハザード分析及び必須管理点（HACCP）		系統的アプローチ	
環境リスクアセスメント（毒性リスクアセスメント）	シナリオ分析		
構造化“Whatif”技法（SWIFT）	支援法	系統的アプローチ	
シナリオ分析	シナリオ分析		
事業影響度分析（BIA）			可
根本原因分析（RCA）			不可
故障モード・影響解析（FMEA）	機能分析		推奨
故障の木解析（FTA）	シナリオ分析	系統的アプローチ	可
事象の木解析（ETA）			
原因・結果分析（CCA）			
原因影響分析（特性要因図（魚骨線図））			推奨
防護層解析（LOPA）	管理策のアセスメント		可
決定木解析			不可
人間信頼性分析（HRA）	支援法		推奨
ちょう（蝶）ネクタイ分析	管理策のアセスメント		不可
信頼性重視保全（RCM）	機能分析		推奨
スニーク回路解析（SCA）			可
マルコフ解析	統計的手法		
モンテカルロシミュレーション			不可
ベイズ統計及びベイズネット			
FN 曲線			可
リスク指標			
リスクマトリックス			推奨
費用／便益分析（CBA）			可
多基準意思決定分析（MCDA）			

3．2　分類について

事故の誘発度(Coupling：システム内機能の結合度)を**縦軸**に，システムの**管理難易度**(Manageability)※1を**横軸**にして「対象サービス」と「24種類の手法」を図で分類

Hollnagelの分類†



①事故が拡大し難く，かつ扱い易いシステム
　対象：郵便局や製造業など
　手法：FMEA, FTA, RCA, J-HPES 等
②事故が拡大し易く，かつ扱い易いシステム
　対象：ダムや電車など
　手法：ATHEANA, AcciMap 等
③事故が拡大し易く，かつ扱い難いシステム
　対象：原子力発電所や金融相場など
　手法：FRAM, STAMP等

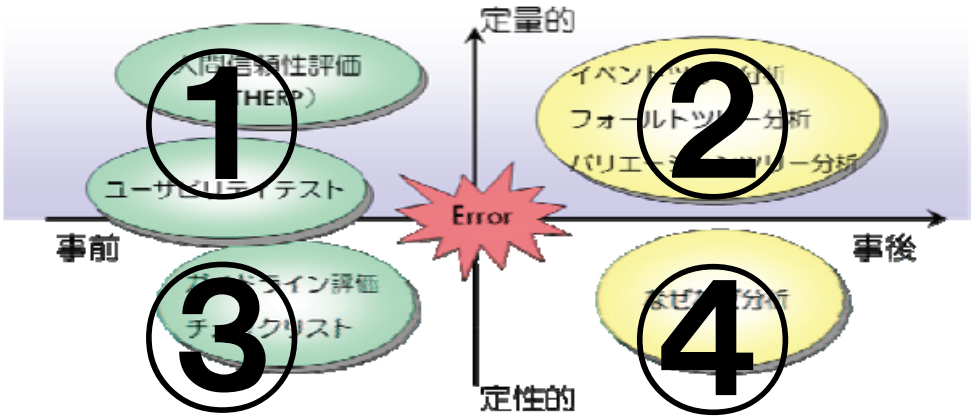
※1：**管理難易度　＝　精密度**(Description)　×　**不安定度**(Instability)　×　**理解難度**(Comprehensibility)
（精密度：単純⇔複雑，不安定度：安定⇔不安定，理解難度：判り易い⇔判り難い）

†：下記参考文献を基に発表者が手を加えて記述した。

•Erik Hollnagel, Josephine Speziali: Study on Developments in Accident Investigation Methods: A Survey of the State-of-the-Art (2008), https://hal.archives-ouvertes.fr/hal-00569424/document

3．2　分類について

尾崎らの分類†



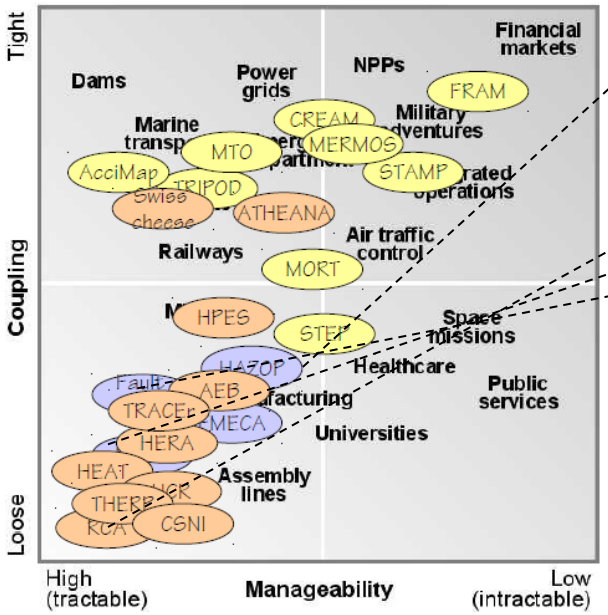
①：THERPなどのHRA
②：ETA, FTA, VTA
③：ガイドライン評価やチェックリスト
④：なぜなぜ分析（RCA）

定量・定性を縦軸に，事前・事後を横軸に分析評価手法を分類

†：下記参考文献を基に発表者が手を加えて記述した。
・尾崎禎彦，大井 忠：原子力プラント運転・保守におけるヒューマンエラー評価技術に関する研究-分析・評価ツール-，福井工業大学研究紀要 第41号(2011).

3．2　分類について

Hollnagelの分類



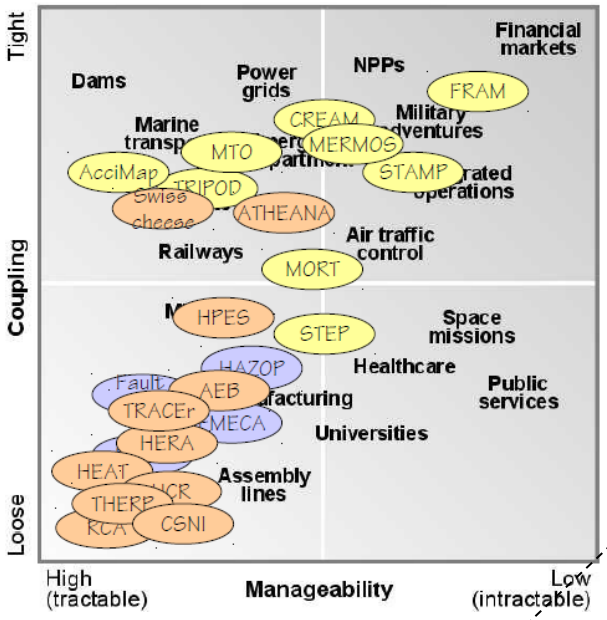
IEC/ISO 31010

分析評価手法
ブレーンストーミング
構造化又は半構造化インタビュー
デルファイ法
チェックリスト
予備的ハザード分析（PHA）
HAZOP スタディーズ
ハザード分析及び必須管理点（HACCP）
環境リスクアセスメント（毒性リスクアセスメント）
構造化“Whatif”技法（SWIFT）
シナリオ分析
事業影響度分析（BIA）
根本原因分析（RCA）
故障モード・影響解析（FMEA）
故障の木解析（FTA）
事象の木解析（ETA）
原因・結果分析（CCA）
原因影響分析（特性要因図（魚骨線図））
防護層解析（LOPA）
決定木解析
人間信頼性分析（HRA）
ちょう（蝶）ネクタイ分析
信頼性重視保全（RCM）
スニーク回路解析（SCA）
マルコフ解析
モンテカルロシミュレーション
ベイズ統計及びベイズネット
FN 曲線
リスク指標
リスクマトリックス
費用／便益分析（CBA）
多基準意思決定分析（MCDA）

Hollnagelは24種類，
IEC/ISO 31010では31種類の手法を挙げているが，
重なっている手法は4種類であること

3．2　分類について

Hollnagelの分類

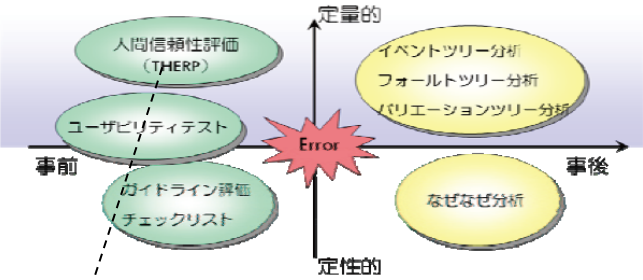


と　の殆どがHRA

IEC/ISO 31010

分析評価手法
ブレーンストーミング
構造化又は半構造化インタビュー
デルファイ法
チェックリスト
予備的ハザード分析（PHA）
HAZOP スタディーズ
ハザード分析及び必須管理点（HACCP）
環境リスクアセスメント（毒性リスクアセスメント）
構造化“Whatif”技法（SWIFT）
シナリオ分析
事業影響度分析（BIA）
根本原因分析（RCA）
故障モード・影響解析（FMEA）
故障の木解析（FTA）
事象の木解析（ETA）
原因・結果分析（CCA）
原因影響分析（特性要因図（魚骨線図））
防護層解析（LOPA）
決定木解析
人間信頼性分析（HRA）
ちょう（蝶）ネクタイ分析
信頼性重視保全（RCM）
スニーク回路解析（SCA）
マルコフ解析
モンテカルロシミュレーション
ベイズ統計及びベイズネット
FN 曲線
リスク指標
リスクマトリックス
費用／便益分析（CBA）
多基準意思決定分析（MCDA）

尾崎らの分類



尾崎らやIEC/ISO 31010ではHRAとして一括りにまとめているが，HollnagelはHRAを細かく分けている．

3．2　分類について

JIS Q 31010

チェックリスト
予備的ハザード分析（PHA）
ブレーンストーミング
構造化又は半構造化インタビュー

分析評価手法の適切な分類は存在しない

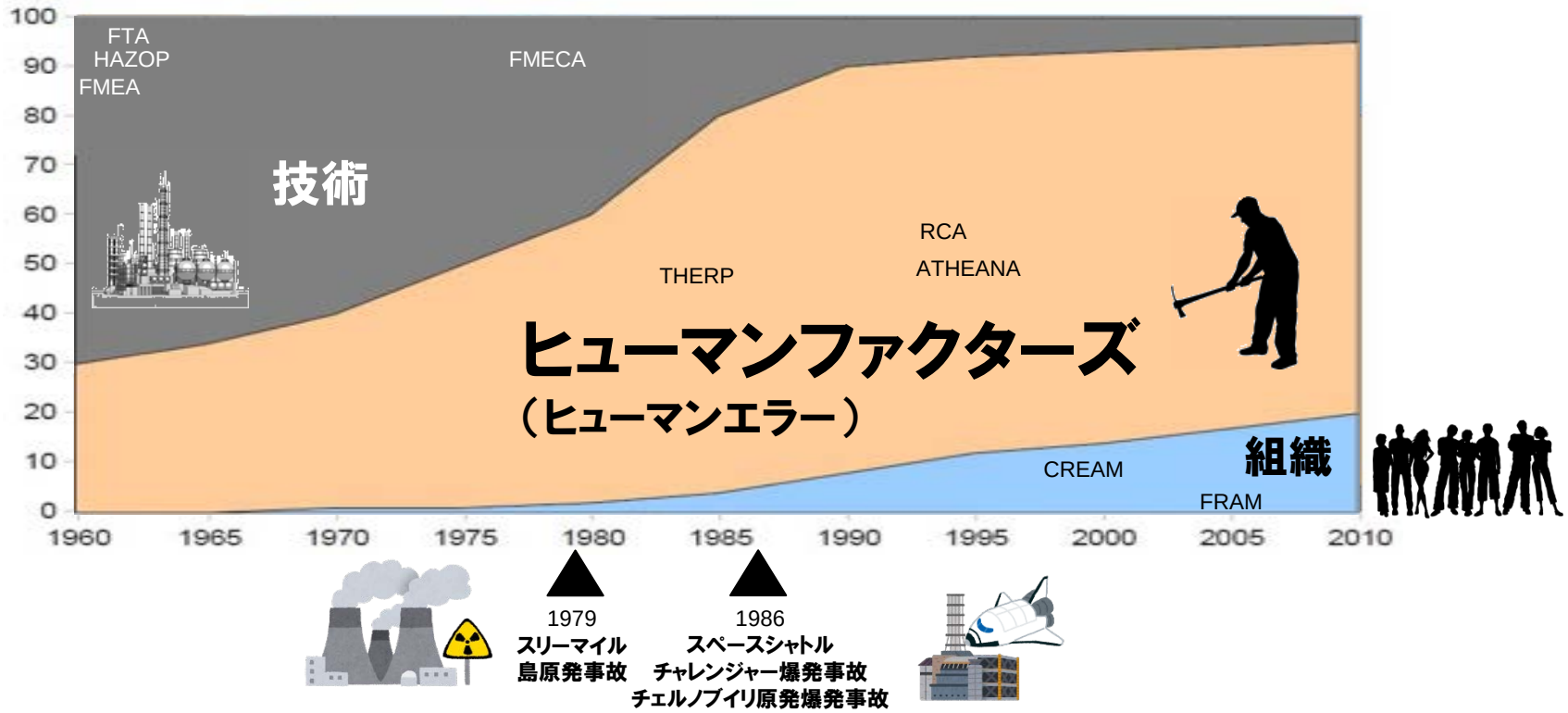
分類する評価者の観点の違い

- **粒度**が異なる
- 取り上げる手法の**範囲**が異なる

費用／便益分析（CBA）
多基準意思決定分析（MCDA）

3．3　歴史的背景

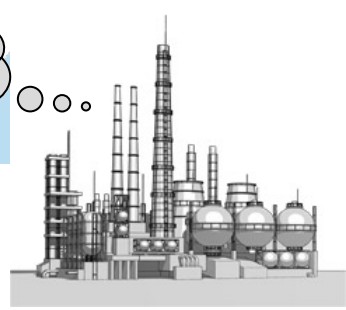
- **産業事故における主要な要因**
  - 昔は技術的要因（機械の故障等）が主．今は大幅に減少
  - ヒューマンファクターズが現在の**要因の主流**
  - **組織**要因による事故が増加し，**安全管理**が必要



事故(Accident)における各要因の割合（1960年～2010年）†

†：下記参考文献を基に発表者が手を加えて記述した。
Erik Hollnagel : On How (Not) To Learn from Accidents,
http://www.uis.no/getfile.php/Konferanser/Presentasjoner/Ulykkesgransking%202010/EH_AcciLearn_short.pdf

3．3．1　技術の時代



- **時代：18世紀後半～**
- **事故の捉え方**
  - **「技術（機械）自体に問題がある」という産業革命以来の見方。**
    - **産業革命以前は自然災害が死亡事故の主流**

- **主な評価分析手法**
  - FMEA（FMECA),HAZOP,FTA **【信頼性工学で使用されている手法】**
  - **主に軍事・宇宙航空分野で使用**

FMEA(Failure mode and effects analysis：**故障モード・影響解析**）

- **故障モード※1からのボトムアップで，その影響を明らかにする技法**
  - **単独故障モードの特定だけ使用可能．複合故障モードの特定には使用不可**

単位作業	作業要素（サブプロセス）	故障モード	影響	影響解析			重要度（RPN）	対策概要	対策番号
				頻度	影響度	検知度			
購入リスト作成	1.1要求者から要望を聞く	1.1a購買者の内容の聞き漏れ	必要品を買わないこと	5	4	3	60	最後に復唱	A.1.1.1

※1：故障モードとは，故障している，又は正しく動作していないと観測される状態である。例えば，断線，短絡，折損，摩耗，特性の劣化など（JIS Q 31010:2009, JIS Z8115:2000)

参考：HAZOP†

- HAZOP（Hazard and Operability Studies）
  - **設計・運転上の意図からの「ずれ」すなわちプロセス異常をほぼ自動的に想定**
    - HAZOP **ガイドワード**と呼ばれる7種類の手引き用語を使用

HAZOP**ガイドワード例**

語句	定義
No 又は not	想定された結果のどの部分も達成されない，又は想定された状態が存在しない
より多く（より高く）	アウトプット又は運転条件の量的増加
より少なく（より低く）	量的減少
と同様に	量的増加（例，材料の追加など）
の一部	量的減少（例，混合物の一つだけ又は二つのコンポーネント）
逆又は反対	反対（逆流など）
以外	意図したもののどの部分も達成されない，全く異なる事態が生じる

Case No	ガイドワード	具体的内容	根本原因	頻度	安全対策（検知システム）
Case 1,2	None ？No	類似名患者	自分で確認しない	たまに	周囲からの展開
Case 1,2	More	類似名患者	患者が集中する	たまに	周囲からの展開(2重の防護壁が必要)
Case －	Less				

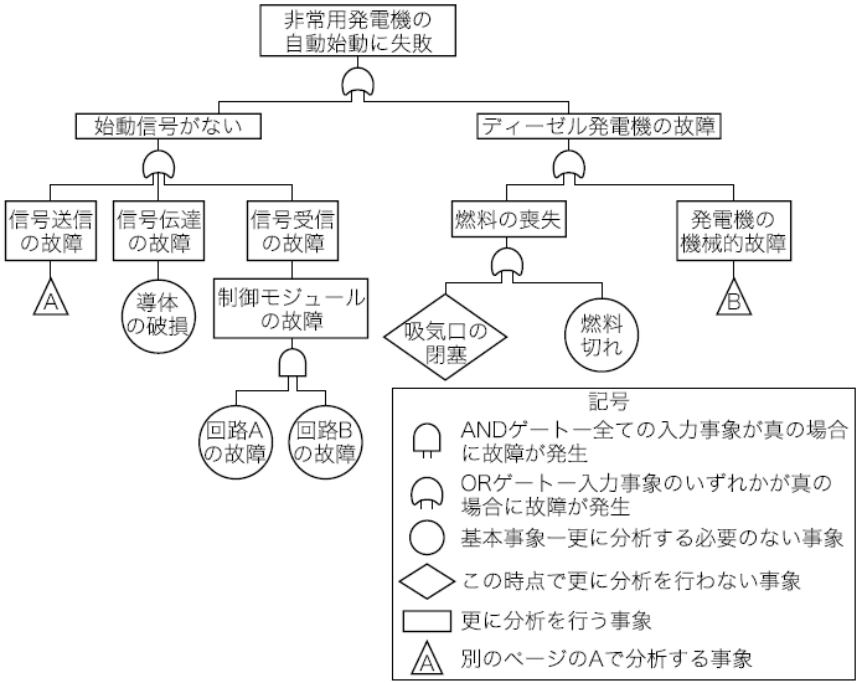
HAZOP**実施例**

†：下記参考文献を基に発表者が手を加えて記述した。

・**日本規格協会**. **リスクマネジメント - リスクアセスメント技法** JIS 31010:2010. **日本規格協会**, 2010.
・**土屋 仁**：HAZOPを用いた医療事故分析，**鈴鹿医療科学大学大学院**(2014)，http://www.suzuka-u.ac.jp/information/bulletin/pdf/2014/15_01_tuchiya.pdf

参考：FTA†

- FTA (Fault Tree Analysis)
  - **上位（ハザード）から論理展開し因果関係（発生要因）を明示する手法**
    - **その発生が好ましくない事象について、発生経路、発生要因及び発生確率をフォールトの木を用いて解析**



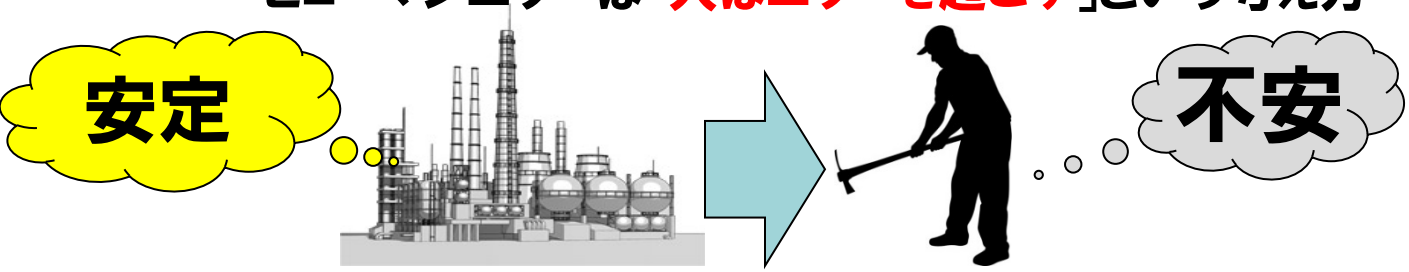
FTA**実施例**

†：**下記参考文献を基に発表者が手を加えて記述した。**

・**日本規格協会**. **リスクマネジメント - リスクアセスメント技法** JIS 31010:2010. **日本規格協会**, 2010.

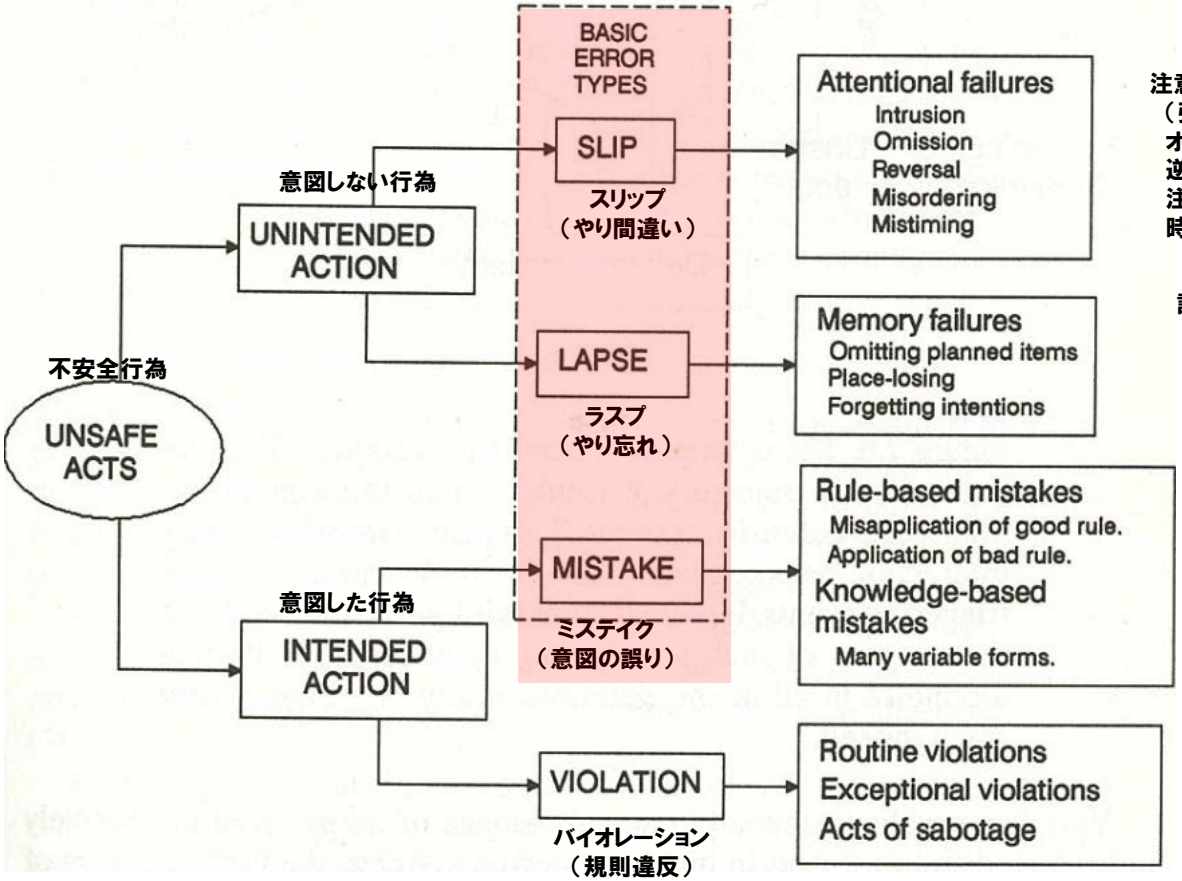
3．3．2　ヒューマンファクターズの時代

- **時代：1950年代～**
- **事故の捉え方**
  - **技術からヒューマンエラーへ**
    - **技術が発達し技術的要因が減り，ヒューマンエラーに焦点が当たっていった**
    - **ヒューマンエラーは「人はエラーを起こす」という考え方**



参考:ヒューマンエラー

基本的なエラーの範囲



- Swainの形態別定義†
  - オミッションエラー
    - 実行すべきことをしない
  - コミッションエラー
    - 実行すべきでないことをする

注意不足
（強い習慣による）侵入
オミッション（必要なことをしない）
逆に実施（順序や位置を逆にする行為）
注文間違い（順序間違い）
時機を誤る（タイミング違い）

記憶の間違い
計画した行為を省略（抜け）
進捗の見失い
意図の度忘れ

ルールベースのミステイク
良いルールの誤用（不適切な状況で適用された健全な規則）
悪いルールの適用（不健全な規則の適用）
知識ベースのミステイク
多くの可変的な形（規則が適用されていない状況での判断誤り，不十分な知識や経験）

日常的な違反
例外的な違反
破壊活動行為

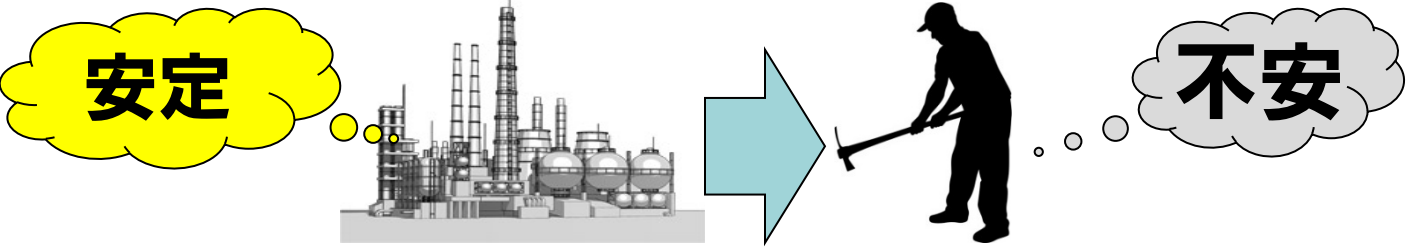
Reasonの不安全行為の定義†

†:下記参考文献を基に発表者が手を加えて記述した。

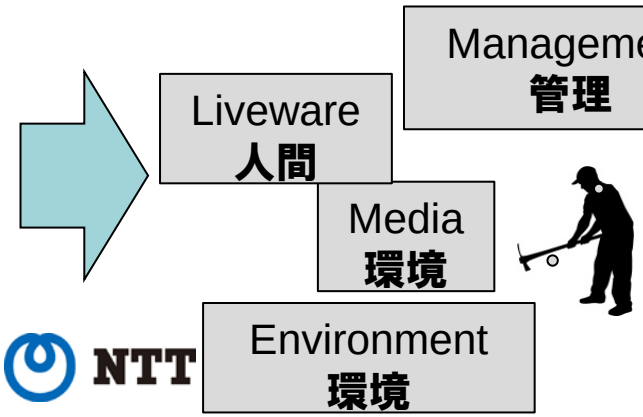
•James Reason: Human Error, Cambridge University Press (1990).
• Swain, A. D. & Guttmann, H. E. : Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application, U.S. NRC-NUREG/CR-1278 (1980).

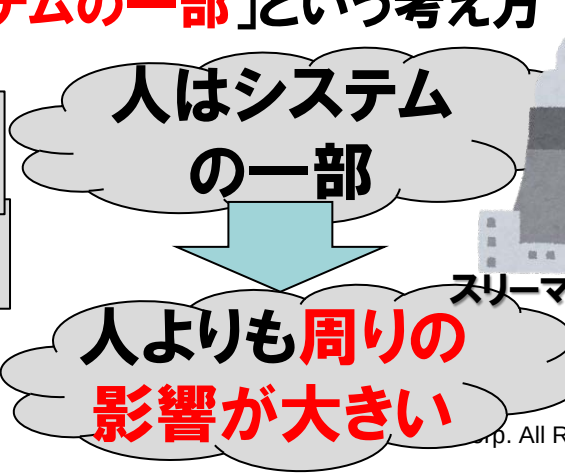
3．3．2　ヒューマンファクターズの時代

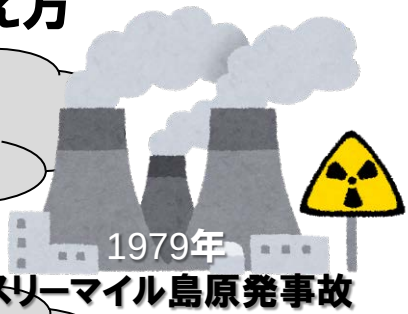
- 時代：1950年代～
- 事故の捉え方
  - 技術からヒューマンエラーへ
    - 技術が発達し技術的要因が減り，ヒューマンエラーに焦点が当たっていった
    - ヒューマンエラーは「人はエラーを起こす」という考え方



  - ヒューマンエラーからヒューマンファクターズへ
    - ヒューマンファクターズは「人はシステムの一部」という考え方







3．3．2 ヒューマンファクターズの時代

PRA(Probabilistic Risk Assessment：確率的リスクアセスメント)の1つ

- HRA(Human Reliable Analysis：人間信頼性解析)
  - 第一世代HRA：THERP(1983)

「人的過誤率」とも呼ばれている

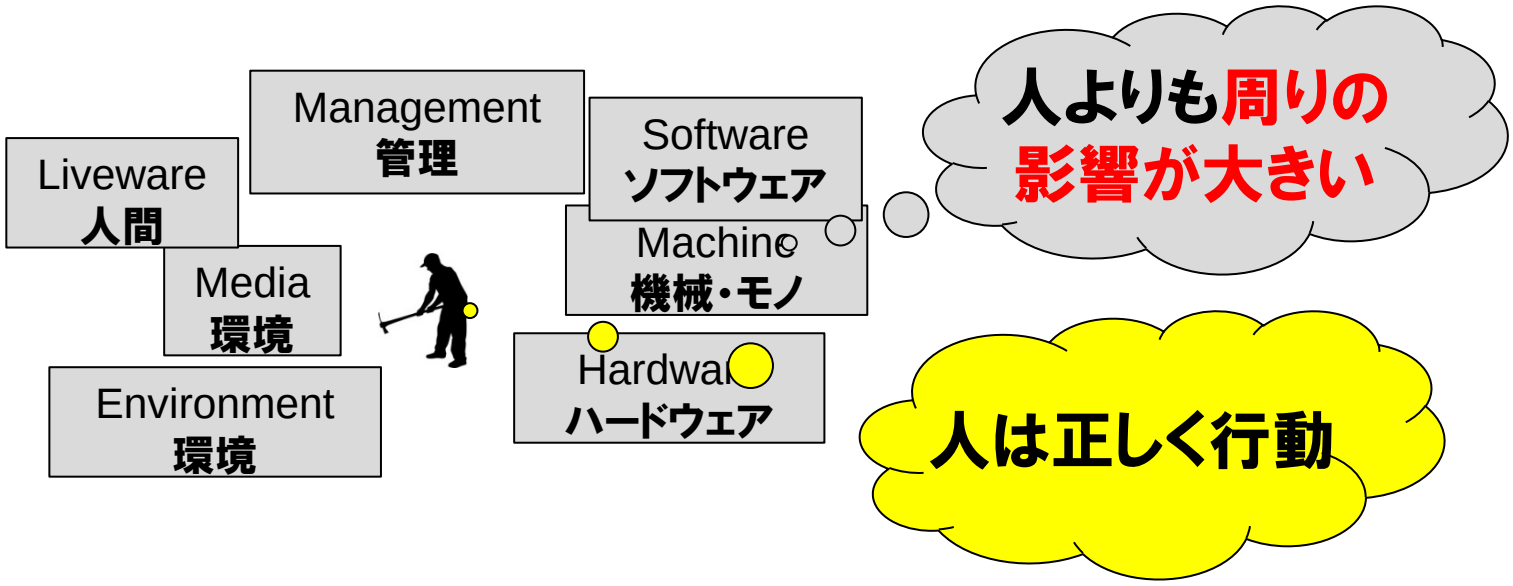
人間はシステムの一部

  - HEP(Human error probability:ヒューマンエラー確率)をPSF(Performance shaping factor:行動形成要因)で補正
  - 行動上のエラーのみに焦点を当てている(問題分析のエラーや認知的ミステイクを無視)

  - 第二世代HRA：ATHEANA(1996)

人間は正しいが状況に依存

  - PSF(行動形成要因)が主。HEP＝P(エラー｜状況)・P(状況)
  - 1979年のスリーマイル島の原発事故の反省から問題分析のエラーや認知的ミステイクも焦点



参考：THERP†

- Technique for Human Error Rate Prediction(1983）
  - **第一世代HRAであり、HEP(Human error probability:ヒューマンエラー確率）をPSF(Performance shaping factor:行動形成要因）で補正**
    - **行動上のエラーのみに焦点を当てている（問題分析のエラーや認知的ミステイクを無視）**
  - **系統的人間信頼性評価: ヒューマンエラーの発生確率を予知し、ヒューマンエラー単独またはマンマシンシステムの劣化を評価すること**
    - **炉心溶融に至るケースをFTAで洗い出し，そのイベントへのヒューマンエラー確率の寄与をTHERPで評価し、炉心溶融の発生確率(10^{-5}/炉心年を目安）を求めている**

Item	*Display or Task*	*BHEP*	*EF*
(1)	ディジタル表示である	0.001	3
	アナログ表示である		
(2)	見やすいリミットマークがある	0.001	3
(3)	見にくいリミットマークがある	0.002	3
(4)	リミットマークがない	0.003	3

Basic HEP：基本HEP

Error Factor：エラー補正因子

標準HEP(normal-HEP)

↓ PSFによる修正

基本HEP(basic-HEP：BHEP)

↓ EFによる修正

BHEP／EF ≦ HEP ≦ BHEP×EF

ヒューマンエラー確率のデータベースの例

†：下記参考文献を基に発表者が手を加えて記述した。

・尾崎禎彦，大井 忠：原子力プラント運転・保守におけるヒューマンエラー評価技術に関する研究-分析・評価ツール-，福井工業大学研究紀要 第41号(2011).

・高野研一:「安全率を考える」第5 大規模システムと安全率，“J. of the Jpn. Landslide Soc”., Vol.44 No.6 421 pp.78-83 (2008).

参考：人よりも周りの影響の方が大きい

- **基本的帰属錯誤　対応バイアス**
  - 内的な性格に帰属→他人の行動
    - お年寄りに席を譲る
      - 他人は「あの人は親切な人だ」
      - 本人は「親切だから譲った，のではなく，困っている人がいたから譲った」

- **行為者観察者効果　認知バイアス**
  - 外的なものに帰属→自分の行動
  - 見る人の立場によって変わってくる（記憶・知覚　認知バイアス），
    - 毎回遅刻する人
      - 他人は「あの人はだらしない人だ」
      - 本人は「バスがなかなか来なかった」

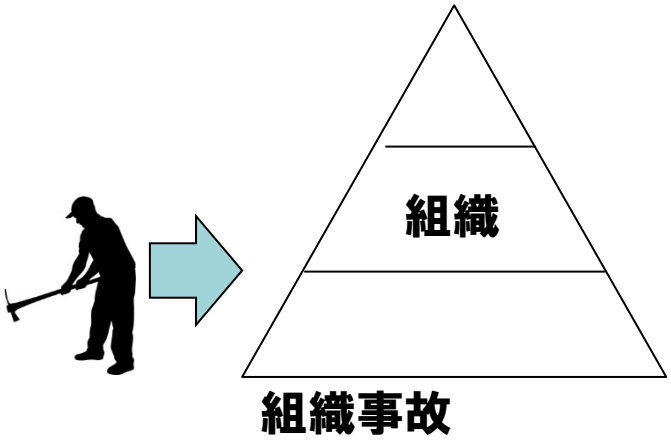
他人に対しては、気質的または個性的な面を重視しすぎて、状況的な面を軽視しすぎる傾向

3．3．3　安全管理の時代

1979年
スリーマイル島原発事故

1986年
スペースシャトルチャレンジャー爆発事故
チェルノブイリ原発爆発事故

- **時代：**1995年代～
- **事故の捉え方**
  - **「個人から組織へ（組織事故）」**



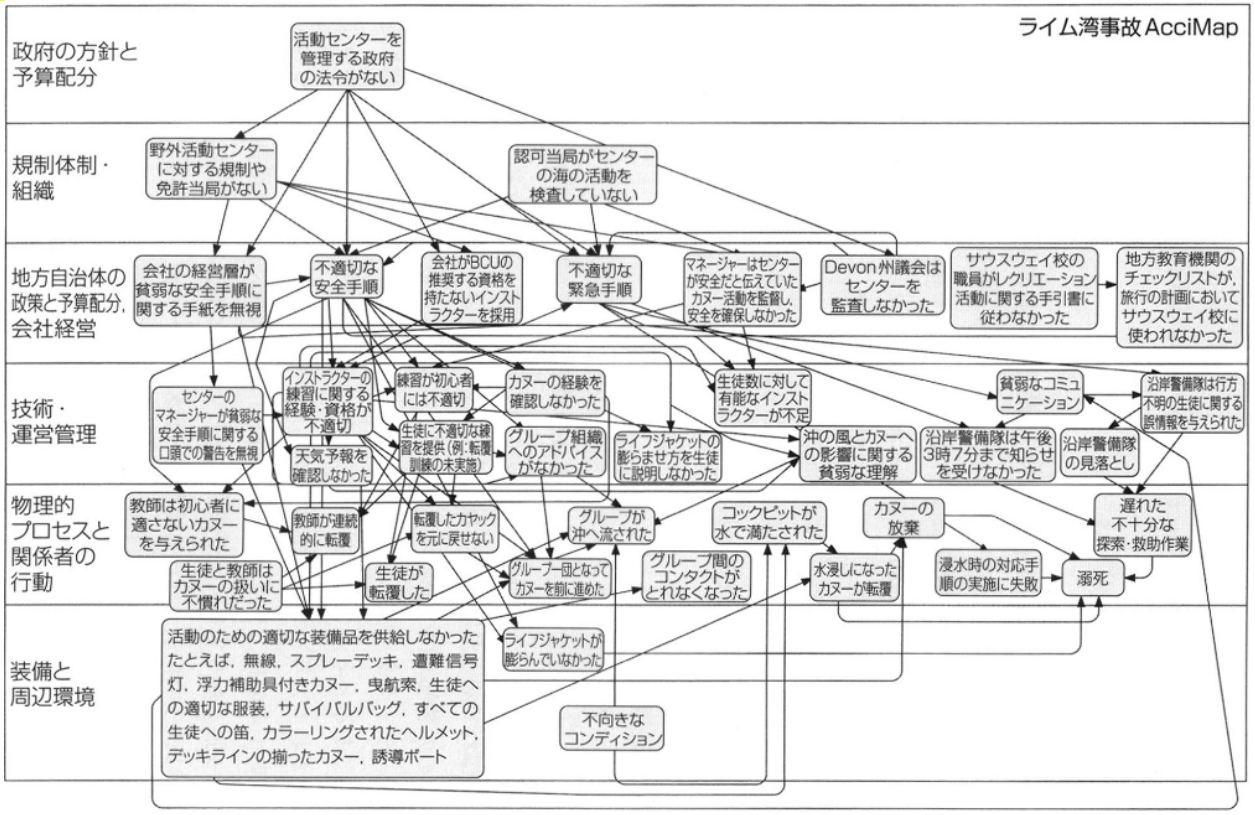
組織事故

主な手法：

AcciMap (1997)，HFACS(2003)

参考：AcciMap†

- 事故原因がシステム全体に渡るときに，それを視覚的に表現する事故分析法
  - 時間とともに経済的・生産性圧力がどのように業務遂行に影響し，システムの防御性や業務遂行の減退をもたらす，という組織事故の考え．

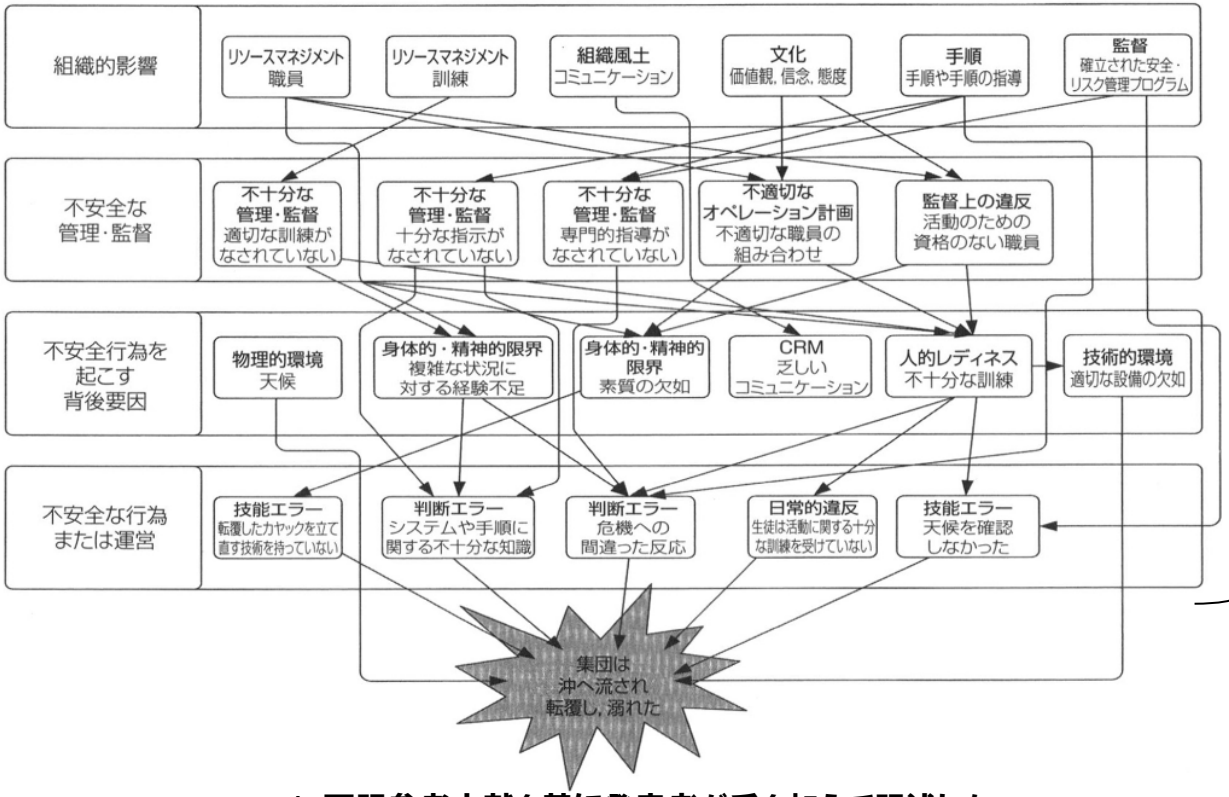


†：下記参考文献を基に発表者が手を加えて記述した。

・ポール・サイモン他5名、小松原明哲訳：事故分析のためのヒューマンファクターズ手法、海文堂出版、2016

参考：HFACS †

- Human Factors Analysis and Classification System
- **組織の4つのレベルにおける失敗モード分類を提供する（不安全行為、不安全行為の前提要因、不安全な監督要素、そして組織の影響要素）**
  - Wiegmann and Shappell (2003)**は、スイスチーズモデルが航空事故分析のモデルとして使えるように、モデルの各レベルの問題形態の詳細分析を検討し、**Reason**のモデルと航空事故報告の分析に基づき、**HFACS**を開発**



4つのレベルの細分化

組織的影響レベルでは3つのカテゴリーが用いられる
- リソースマネジメント（例えば、要員配置・配員、過度なコスト削減、貧弱な設計）
- 組織風土（例えば、組織構造、運営方針、組織文化）
- 組織プロセス（例えば、時間圧、指示命令、リスク管理）

不安全な管理・監督カテゴリーは4つの管理システムの問題により構成される。
- 不十分な管理・監督
- 不適切なオペレーション計画
- 既知の問題修正の失敗
- 監督上の違反

不安全行為を起こす背後要因のレベルは3つのカテゴリーから成る。
- オペレーターの状態（不適切な心的状態、不適切な生理的状態、身体的・精神的限界）
- 環境要因（物理的環境、技術的環境）
- 人員要因（CRM (Crew Resource Management**例えばチームワークやリーダーシップの欠如**),**人的レディネス（例えば不十分な訓練や、貧弱な食習慣））**

不安全行為にはエラーと違反があり、3つの基本的なエラータイプが定義されている。
- 技能エラー
- 判断エラー
- 知覚エラー

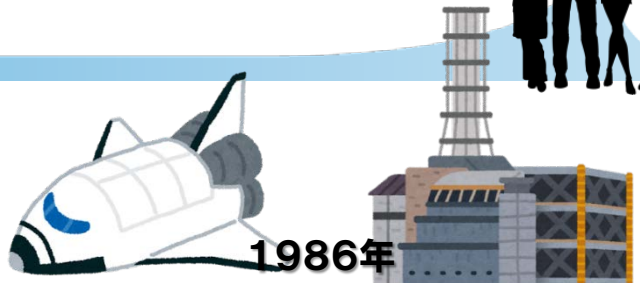
違反は
- 日常的違反
- 例外的違反

†：下記参考文献を基に発表者が手を加えて記述した。

・ポール・サイモン他5名、小松原明哲訳：事故分析のためのヒューマンファクターズ手法、海文堂出版、2016

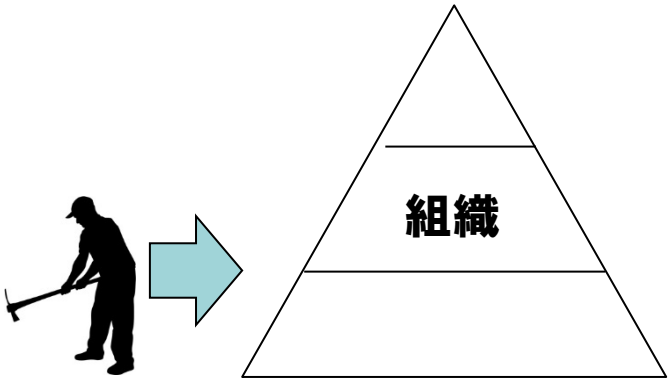
3．3．3　安全管理の時代

1979年
スリーマイル島原発事故



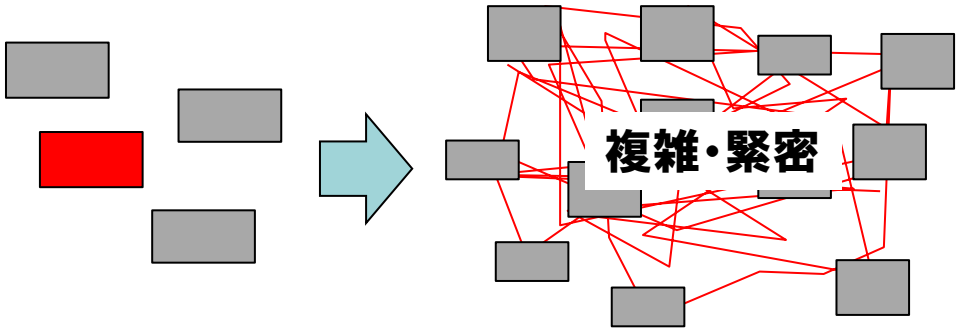
1986年
スペースシャトルチャレンジャー爆発事故
チェルノブイリ原発爆発事故

- 時代：1995年代～
- 事故の捉え方
  - 「個人から組織へ（組織事故）」
  - 「要素機能の不具合から複雑な要素機能間の共鳴へ（機能共鳴型事故）」



組織事故

主な手法：
AcciMap (1997)，HFACS(2003)



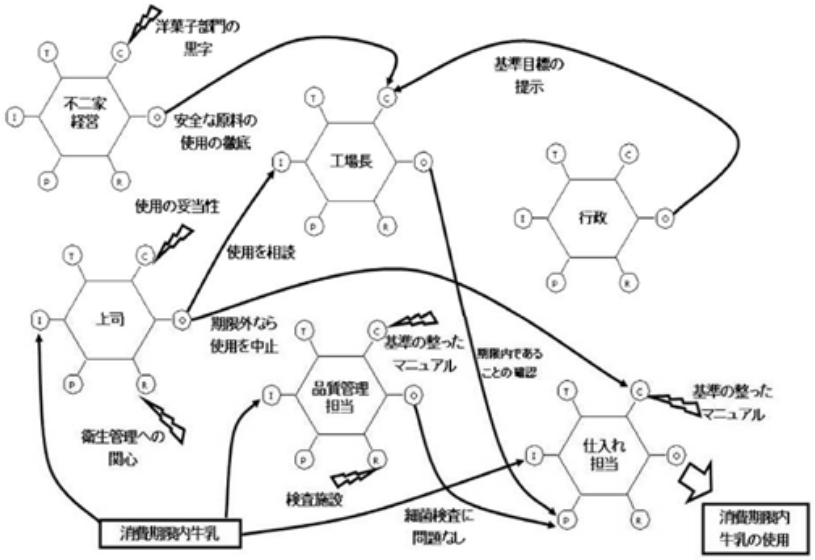
機能共鳴型事故

主な手法：
STAMP(2002)，FRAM(2004)

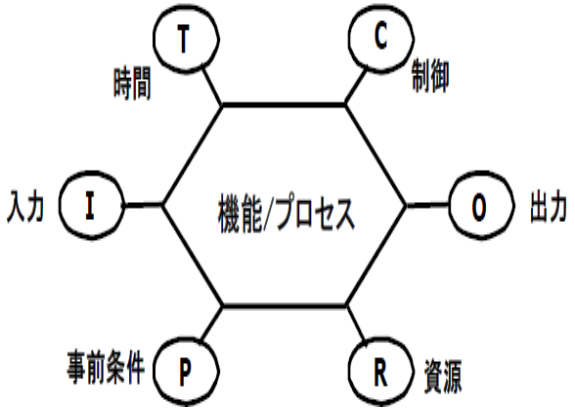
参考：FRAM†

Functional Resonance Accident Model

- E.Hollnagelが提案した事故分析モデル．RCA(根本原因分析：例えば連関図，時系列図，FTA,TVA等)の手法では分析しきれない「機能共鳴型事故」に対応するため．
- システムを構成する機能同士の変動がどのように連鎖し，共鳴して事故が起こるかという状況を表すモデル
- FRAMの基本記号は，入力(Input)から入った情報が人間の行動や機能の働きの結果，出力(Output)となって出されるという流れ



FRAM分析結果例



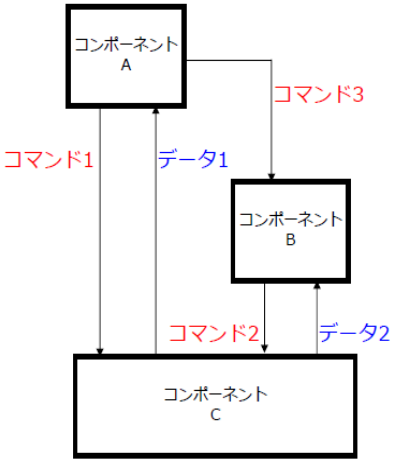
機能の六角形表現

†：下記参考文献を基に発表者が手を加えて記述した。

・三角竜二：エラーマネジメントに関する調査研、究第2グループエラーマネジメント研究会平成19年度活動報告(2008).

参考：STAMP/STPA†

- STAMP（Systems-Theoretic Accident Model and Process）：**システム理論に基づく事故モデル**
- STPA（STAMP based Process Analysis）：**STAMPに基づく安全解析法**
- **システムを構成するサブシステムやコンポーネントに不具合がなくとも，サブシステムやコンポーネントの組み合わせによって全体のシステムにおける不具合が発生するという機能共鳴型事故の考え．**



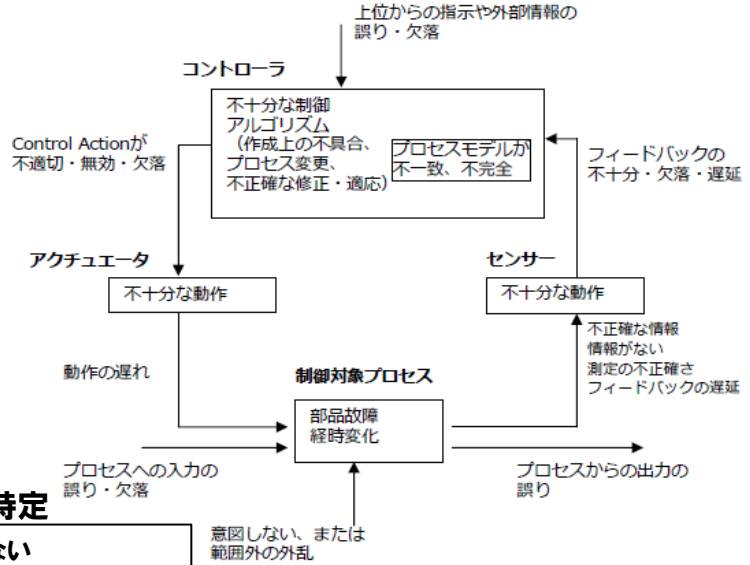
Control Structure

コンポーネント間のデータの授受を識別

赤字：Control Action（指示コマンド）
青字：フィードバックデータ

ガイドワードから非安全制御動作（UCA）を特定

1. “Not Provided”**必要なコントロールアクションが供給されない**
2. “Incorrectly Provided”**誤った非安全なコントロールアクションが供給される**
3. “Provided Too Early, Too Late, or Out of Sequence”**意図しないタイミングで供給される**
4. “Stopped Too Soon”**途中で止まる（または必要以上に長く実施される）**



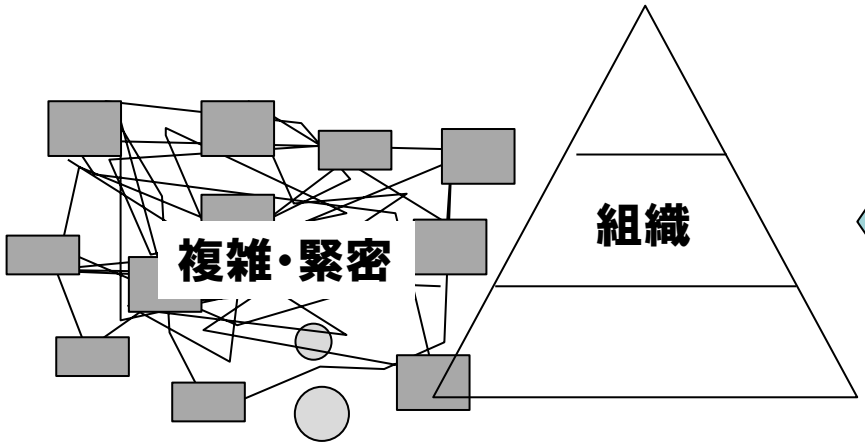
Control Loop Diagram

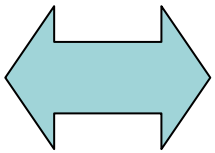
ハザード要因（HFC）を特定

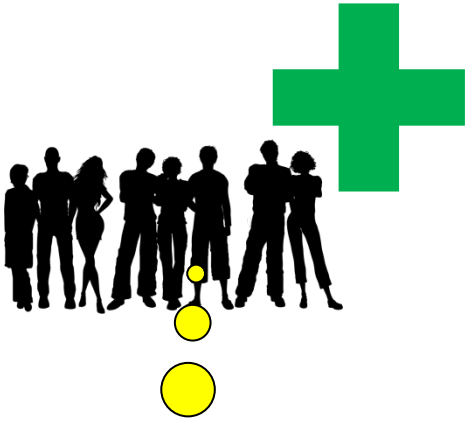
†：**下記参考文献を基に発表者が手を加えて記述した。**
・IPA:**はじめての**STAMP/STPA**～システム思考に基づく新しい安全性解析手法～**、2016

3．4　事故のモデル

- 「複雑な要素機能の共鳴が事故を起こす」
- 「事故は個人よりも組織の影響が大きい」
- 「人が事故を防ぐ」







事故要因は個人から組織へ
機能共鳴による事故

ノーマルアクシデント・組織事故

人が事故を防ぐ
うまくいくことを増やす

高信頼性組織、安全文化、レジリエンス工学

3．4　事故のモデル

1. **ノーマル・アクシデント理論**（NAT: Normal Accident Theory（1984））
   - **システムにとって**アクシデントは避けられない**システムの固有の特性**
   - 1979**年のスリーマイル島の原発事故がきっかけ。事故をもたらした組織的要因の解明のため。**

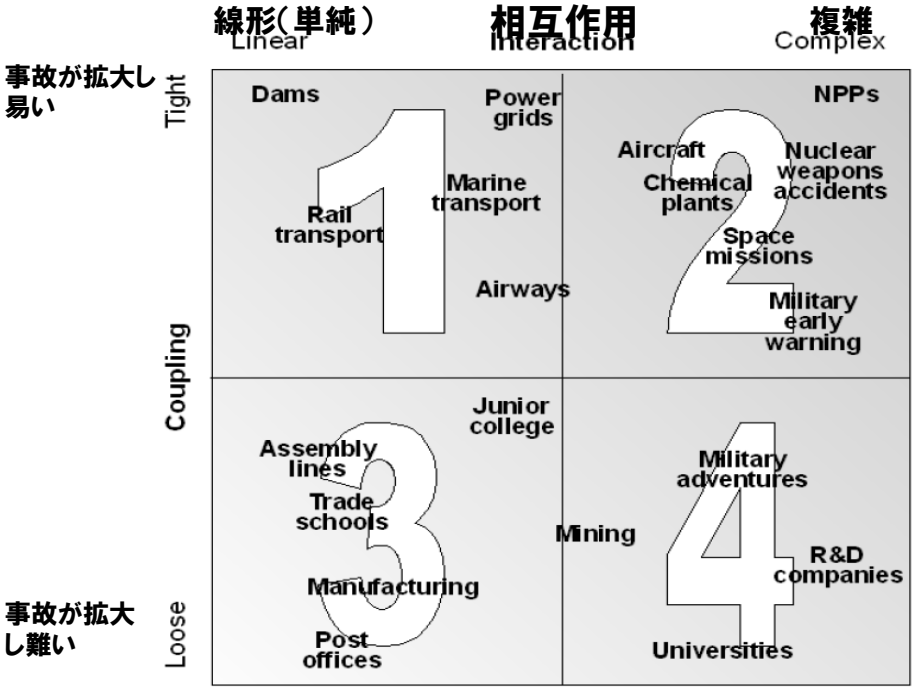
2. **高信頼性理論**（HRT: High Reliability Theory（1980**年代後半**））
   - NAT**に対抗する理論。バークレー・グループと**Weick & Sutcliffe**の研究が有名.**
   - **事故の**危険性が高い状況下にあっても高い信頼性**を保っている組織**（HROs）**の分析**

3. **安全文化**
   - **安全文化の概念は**1986**年のチェルノブイリ事故に関する**IAEA**の事故調査から生み出された**
   - Reason:「**組織事故**」（1997）**において、理想的な安全文化は、経営トップの性格やその時の経営状態にかかわらず，**安全性を最大にするという目標**に向かってシステムを動かし続ける**エンジン**のような役割を果たすもの。**

4. **レジリエンス工学**（2006）
   - **人間工学におけるレジリエンス。レジリエンスとは、**予期できなかった条件下**でも、求められる**オペレーションを継続可能**にする本質的能力。**
   - **うまくいかない事象を減らす事よりも、**うまくいく事象の数を増加させること**

参考：ノーマル・アクシデント理論†

- Normal Accident Theory (NAT)
  - **システムにとって**アクシデントは避けられない**システムの固有の特性**
    - **複雑さ**(Complex)**と事故の拡大し易さ**(Tight)**がアクシデントを引き起こす**
    - **ノーマルとは、アクシデントの頻発性や予測可能性の意味ではなく、システムにとって避けられない、という意味**
  - Charles Perrow **が唱えた理論。**1979**年のスリーマイル島の原発事故がきっかけ**



システムの誘発度と複雑度の図

事故の誘発度(Coupling：**システム内機能の結合度)を縦軸に，システムの複雑度**(Interaction:**相互作用**)**を横軸にして各システムを4つに分類**

†下記の参考文献を基に発表者が手を加えて記述した。
・藤川なつこ: 高危険組織の構造統制と組織化—ノーマル・アクシデント理論と高信頼性理論の統合的考察ー、経済科学第60巻3号, pp.51-69 (2013).
・ Erik Hollnagel, Josephine Speziali: Study on Developments in Accident Investigation Methods: A Survey of the State-of-the-Art (2008), https://hal.archives-ouvertes.fr/hal-00569424/document
・Charles Perrow: “Normal Accidents: Living With High-Risk Technologies (Princeton Paperbacks)”, Princeton Univ Pr(1998).

参考：高信頼性組織†

- **高信頼性組織**（HROs：High−Reliability Organization）
  - **定義は「つねに過酷な条件下で活動しながらも事故発生件数を相応量以下に抑えている組織」**
  - **2つの潮流**
    - Roberts(**バークレーグループ**)
      - **高信頼性の実績を残す組織を取り上げ、ノーマルアクシデントの課題を解決できていることを示した**※2**。**
    - Weick & Sutcliffe
      - **人の多様性を推奨する文化（直接のコミュニケーションと多種多様な人たちからなる作業）によって、システムの多様性に対処できることを示した。**

HROsの特徴

機能	組織行動	特徴
A 不測の事態の予測・認識	① 失敗から学ぶ	（ア）報告を指導・奨励する
		（イ）失敗を分析する
		（ウ）失敗をシステム全体の中でとらえる
		（エ）システムの各構成要素が相互依存的であることを理解させる
		（オ）迅速に学習する
	② 現場の状況に敏感である	（ア）常に不測の事態の発生に気を配る
		（イ）現場の状況を重視する
	③ 予測を単純化しない	（ア）状況の示す意味合いに注意を払う
		（イ）多様な人々の間で意見を交わす
B 不測の事態の抑制・対応	④ 復旧能力を高める	（ア）考え方や対応のモードを変える
		（イ）能力を持つ者の非公式な集まりで対応策を生みだす
		（ウ）即応力を育成する
	⑤ 専門能力を尊重する	（ア）専門能力を持つメンバーに助けを求める
		（イ）専門能力のあるメンバーに意思決定権を委譲する

†：下記参考文献から一部抜粋し転記した。

・藤川なつこ: 高危険組織の構造統制と組織化—ノーマル・アクシデント理論と高信頼性理論の統合的考察ー、経済科学第60巻3号, pp.51-69 (2013).
・長谷川尚子：不測の事態を抑止し，対処できる組織の要件～高信頼性組織レジリエンス，安全文化を踏まえて～，REAJ誌2014Vo..36.No.2, pp.113-120 (2014).
・中西晶：高信頼性組織への招待、REAJ誌、Vol.34 No.5 (2012)

参考：安全文化（Reason）†

- **安全文化**（Safety Culture）
  - **理想的な安全文化**
    - 経営トップの性格やその時の経営状態にかかわらず，**安全性を最大にするという目標**に向かってシステムを動かし続ける**エンジン**のような役割を果たす．
    - このエンジンの駆動力は，リスクに対して継続的に注意を向け，警戒を怠らないこと
  - **警戒状態を継続するのに最も良い方法**
    - 安全情報システムを構築して正しい種類のデータ（ヒヤリハット事象や軽微な事象）を集め，
    - 重大な兆候の定期的なチェックや，教訓の収集・分析・普及を行うこと
  - **背景**
    - 表面的なエラーや故障だけではなく，組織要因が関与して発生（特にチェルノブイリ事故）
    - 組織事故：長年の安全性軽視や工程優先などの**組織要因によって「潜在条件のぬけ道」を通じて徐々に防護が無力化**し，不安全行為が引き金となって防護が崩壊し，大惨事を引き起こす

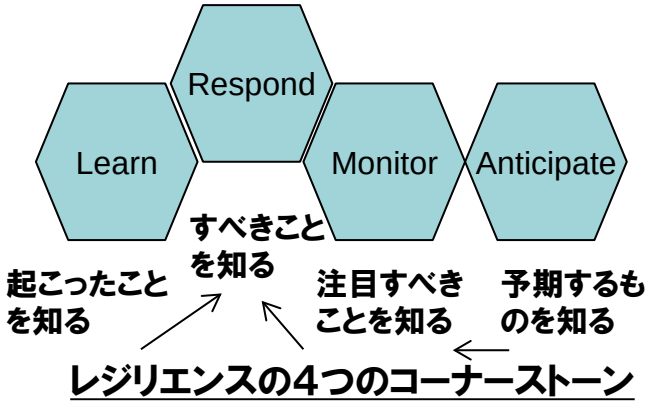
Reasonによる安全文化

報告する文化	自らのエラーやニアミスを報告しようとする組織の雰囲気を指す． 安全情報システムが有効に機能するには「報告する文化」を作り上げることが必要である．
正義の文化	効果的な「報告する文化」は，組織が非難や処罰をどのように行うかにかかっている．許容できる行動と許容できない行動の境界に関して，組織メンバーの中で合意が形成され，この合意（判断基準）に基づいて非難・処罰が行われることにより，「正義の文化」が醸成される．
柔軟な文化	ある種の危険に直面した時などに，中央集権型の階層構造からフラットな専門職構造へと一時的に移行するような柔軟さを指す．この柔軟さが機能するには，元々の中央集権型の構造が，規則や規制，標準化によるものではなく，規律正しい階層構造によって共有された価値観・仮定に基づくものでなければならない．
学習の文化	必要な時に安全情報システムから正しい結論を導き出して，大きな改革を実施する意思・雰囲気を指す．学習が深化すると望ましくない結果を生んだ行動の前提条件が絶えず見直されるようになり，継続的な改善に向けた努力と資源を持てるようになる．

†：下記参考文献から一部抜粋し転記した。
・長谷川尚子：不測の事態を抑止し，対処できる組織の要件～高信頼性組織レジリエンス，安全文化を踏まえて～，REAJ誌2014Vo..36.No.2, pp.113-120 (2014).

参考：レジリエンス工学†

- Resilience Engineering
  - **組織がトラブルを回避するために，a．悪いことが起きないようにする，b．悪いことが悪化しないようにする，c．起こってしまった悪いことからリカバリーする，ための能力を指す**（Westrum）．
  - **目的は、うまくいかない事象を減らす事よりも、うまくいく事象の数を増加させること**
  - **第一人者：** Erik Hollnagel
  - **人間工学におけるレジリエンスは，2000年初頭から「レジリエンス工学**（Resilience Engineering）**」として提唱された．**



レジリエンスの4つのコーナーストーン

能力を実現するための4つの基軸

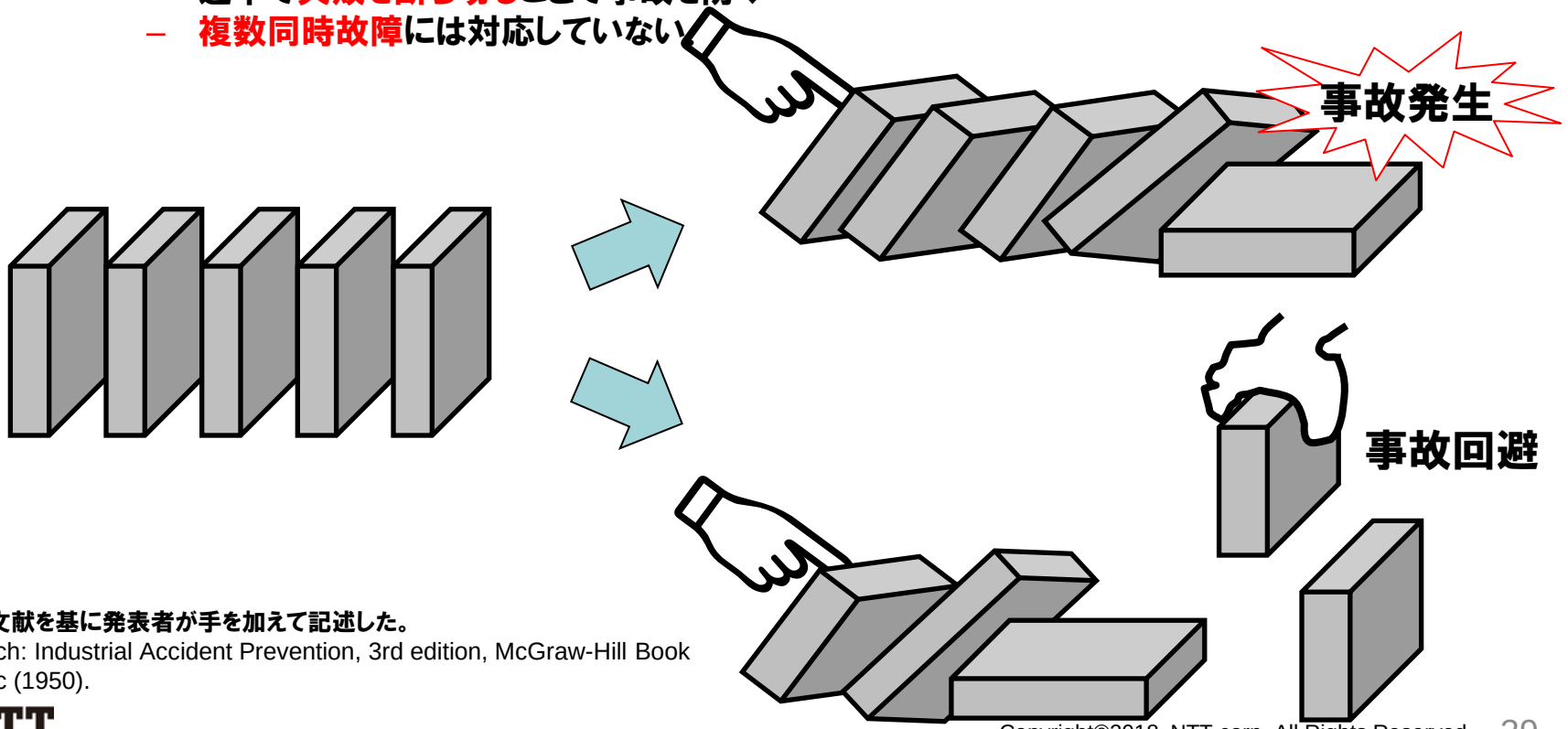
学習	事実，すなわち経験に基づく教訓の抽出を指す．重要な点は，失敗事例だけでなく成功事例からも学ぶ，すなわち「なぜ（事故が）起こったのか？」ではなく，「なぜ（事故が）起こらなかったのか？」を学ぶ点である．
監視	危機の監視，すなわちシステムの内外に脅威が訪れていないかどうかの監視を指す．何らかの指標を用いたシステムのパフォーマンスや環境の変化の評価などが該当する．
予測	可能性の予測，すなわち先を見据えた脅威や変化の予測を指す．将来起こりえて，かつシステムの能力に影響を及ぼしそうな出来事，状態，変化の予測が該当する．
対応	現実への対応，すなわち実際に発生した混乱や障害への対応を指す．具体的には，a．発生した事態を発見して状況を査定し，b．事態の重要性や対応の必要性を認識・評価し，c．いつどのように対応すれば有効かを探索・決定することである．

†：下記参考文献から一部抜粋し転記した。

・長谷川尚子：不測の事態を抑止し，対処できる組織の要件～高信頼性組織レジリエンス，安全文化を踏まえて～，REAJ誌2014Vo..36.No.2, pp.113-120 (2014).
・Erik Hollnagel他3名：“ Resilience Engineering in Practice: A Guidebook”, Ashgate Publishing Limited(2010).

3．4　事故のモデル

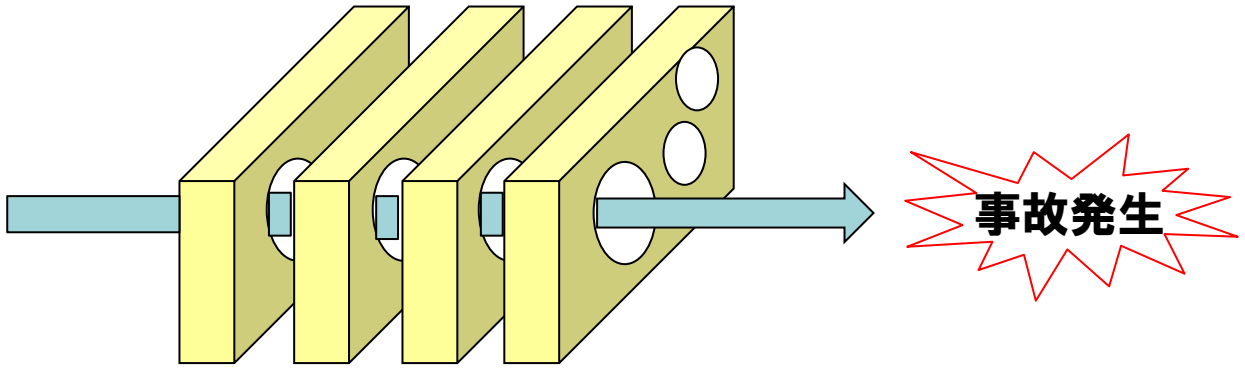
- **単純線形モデル†**
  - Heinrich**のドミノモデル**（1930）、**連鎖モデル**（Sequential Model)**とも呼ばれる**
    - **事故は１つの根本原因からの連続的な失敗から発生**
      - RCA、FMEAやFTA**はこのモデルに近い分析評価手法**
    - **単一故障（１つの根本原因）に対応．**
      - **途中で失敗を断ち切ることで事故を防ぐ**
      - **複数同時故障には対応していない**



†：下記参考文献を基に発表者が手を加えて記述した。
H.W. Heinrich: Industrial Accident Prevention, 3rd edition, McGraw-Hill Book Company Inc (1950).

3．4　事故のモデル

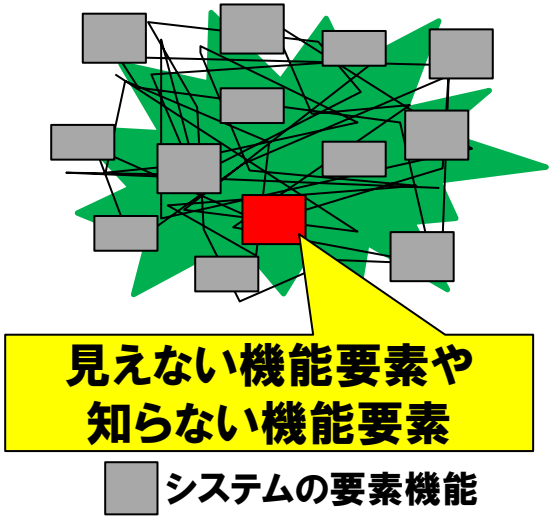
- **複雑線形モデル†**
  - Reason**のスイスチーズモデル（**1990**）とも呼ばれる**
    - **事故は複数の防護壁の劣化**
      - AcciMap (1997)，HFACS(2003)**はこのモデルに近い分析評価手法**
    - **組織事故を想定（複数同時事故）**
      - **システムや要素の相互間の複合要因による機能共鳴型事故には十分対応していない．**

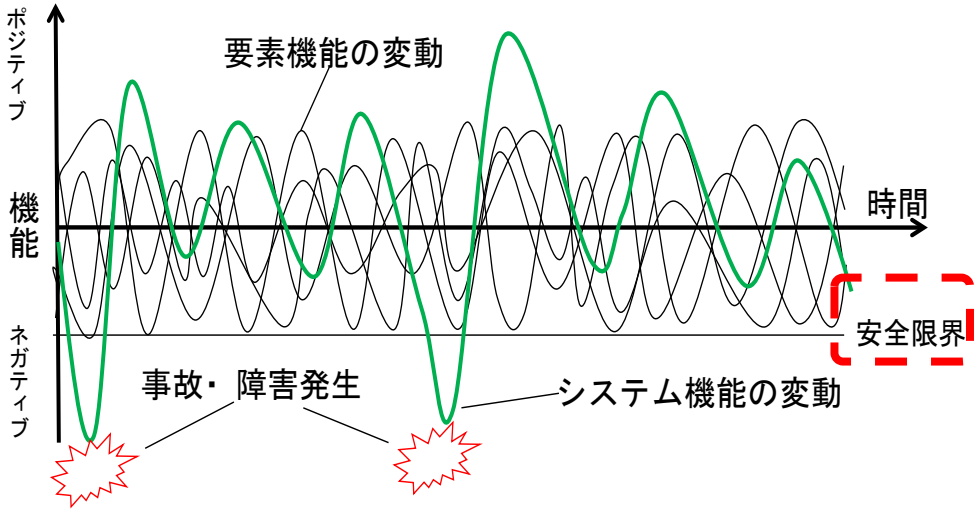


†：下記参考文献を基に発表者が手を加えて記述した。
James Reason :Human error: models and management, British Medical Journal 320 (7237), pp.768-770 (2000).

3．4　事故のモデル

- **非線形モデル†**
  - **機能共鳴モデルやシステミックモデル とも言われている**
    - STAMP，FRAMがこのモデルに対応可能な分析評価手法である
    1. **各要素機能が動的に変動.**
    2. **変動周期が共鳴し**
    3. **安全限界を超えた大きな変動により事故が発生**





†:下記参考文献を基に発表者が手を加えて記述した。
古田一雄: レジリエンス工学　残留リスクにどう向き合えばいいのか、 総合資源エネルギー調査会原子力の自主的安全性向上に関するWG 第6回会合資料4、
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/genshiryoku/anzen_wg/pdf/006_04_00.pdf

End