Innovative R&D by NTT

ISO31000に基づいたリスク分析・評価手法について

2017.12.6

NTTセキュアプラットフォーム研究所

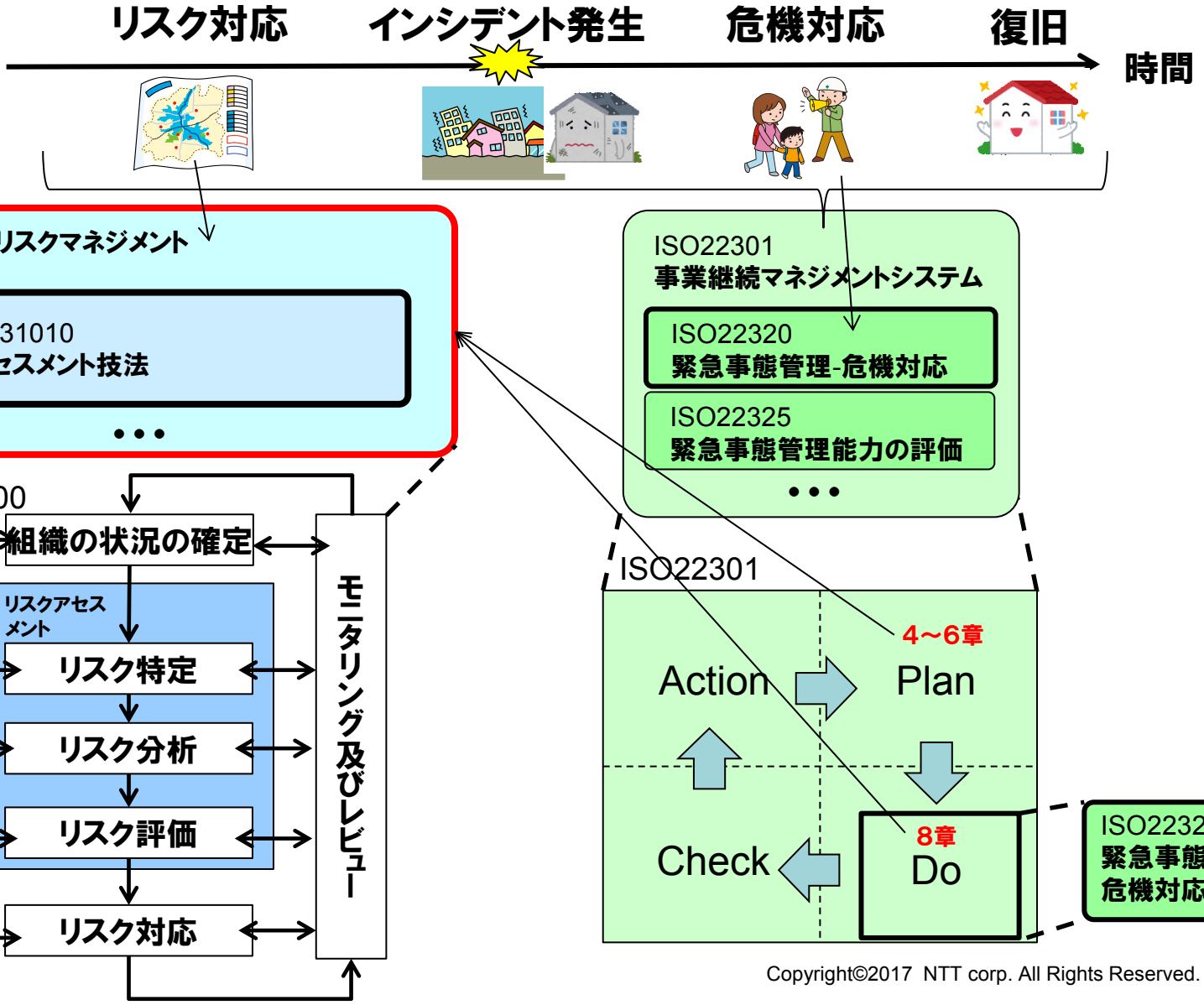
五郎丸秀樹

索引

1. 社会セキュリティとリスクの関係
2. リスクとは
3. ISO31000について
4. ISO31000のリスクマネジメントプロセス
5. リスク分析評価手法について

1．社会セキュリティとリスクの関係

本発表の箇所



参考：ISO 22301†の4～6章

Innovative R&D by NTT

ISO31000 リスクマネジメント

- 4 組織の状況 （Plan）
  - 4.1 組織及びその状況の理解
    - b)事業継続方針と，組織の目的及び組織の総合的なリスクマネジメント戦略を含むその他の方針とのつながり
    - c)組織のリスク選好
      - 状況を明確にするに当たって，組織は次を実施しなければならない。
        - 1)事業継続に関係するものを含め，組織の目的を明確に述べる。
        - 2)リスクを生じさせる不確かさを生む内部及び外部の要因を定義する。
        - 3)リスク選好を考慮に入れて，リスク基準を設定する。
        - 4) BCMSの目的を定義する。
  - 4.3 BCMS の適用範囲の決定
    - 4.3.2 BCMSの適用範囲の決定方法
      - 適用範囲を定めるに当たって，組織は，除外事項を文書化し，説明しなければならない。いかなる除外事項も，事業影響度分析，又はリスクアセスメント並びに適用される法令及び規制の要求事項によって決定された，BCMS の要求事項を満たす事業及び業務を継続できる組織の能力及び責任に影響を与えてはならない。
- 5 リーダーシップ （Plan）
  - 5.2 経営者のコミットメント
    - トップマネジメントは，関連する役割に対して，責任及び権限を割り当て，組織内に伝達することを次に示す事項によって確実にしなければならない。
      - リスク許容基準及びリスクの許容可能レベルを定める。
- 6 計画 （Plan）
  - 6.1 リスク及び機会に対処する活動
    - BCMSの計画を策定するとき，組織は，4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し，次の事項のために対処する必要があるリスク及び機会を決定しなければならない。
      - BCMSが，その意図した成果を達成できることを確実にする。
      - 望ましくない影響を防止又は低減する。
      - 継続的改善を達成する。
    - 組織は，次の事項を計画しなければならない。
      - a)上記によって決定したリスク及び機会に対処する活動

†：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: 社会セキュリティ−事業継続マネジメントシステム−要求事項 JIS 22301:2013(ISO 22301：2012)..

参考：ISO 22301 †の8章

- 8 運用（Do）
  - 8.2 事業影響度分析及びリスクアセスメント

IEC/ISO31010
リスクアセスメント

    - 組織は，事業影響度分析及びリスクアセスメントのために，次の内容を含む正式に文書化したプロセスを確立し，実施し，維持しなければならない。
      - a)アセスメントの状況を設定し，基準を定め，事業の中断・阻害を引き起こすインシデントの潜在的な影響を評価する。
      - b)法的，及び組織が同意するその他の要求事項を考慮する。
      - c)体系的な分析，リスク対応の優先順位付け，及びそれらに係るコストを含める。
      - d)事業影響度分析及びリスクアセスメントから必要とされるアウトプットを定義する。
        - » 注記 事業影響度分析及びリスクアセスメントを実施する順序を決める様々な手法がある。
  - 8.3 事業継続戦略
    - 8.3.1 決定及び選択
      - 戦略の決定及び選択は，事業影響度分析及びリスクアセスメントのアウトプットに基づかなければならない。
    - 8.3.3 保護及び軽減
      - 対応が必要であると特定されたリスクに対して，組織は次のような事前対策を考慮しなければならない。
        - » a)事業の中断・阻害の発生の起こりやすさを低減する。
        - » b)事業の中断・阻害の時間を短縮する。
        - » c)事業の中断・阻害が組織の重要な製品及びサービスに及ぼす損害の大きさを抑制する。
      - 組織は，自らのリスク選好に応じて，適切なリスク対応策を選択し，実施しなければならない。
  - 8.4 事業継続手順の確立及び実施
    - 8.4.2 インシデント対応の体制
      - 組織は，人命を最優先とし，また関係する利害関係者と協議し，重大なリスク及び影響について外部に伝えるか否かを決定し，その決定を文書化しなければならない。伝える決定を下した場合には，組織は，必要に応じて，メディアを含め外部へのコミュニケーション，警報及び警告のための手順を確立し，実施しなければならない。

†：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：社会セキュリティ−事業継続マネジメントシステム−要求事項 JIS 22301:2013(ISO 22301：2012).

2. リスクとは†

- 「リスク」の言葉自体がリスキー
  - 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」

危険(人や物を形容的に示す言葉)の一般的な用語

Danger

Hazard

Risk(リスク)

Peril

差し迫った進行中の危険。経済的損失

偶発性の強い避けがたい危険。負傷的損失・自然界の力

現実的で予測可能な危険。自ら冒す危険

「これとこれがハザードだ(ハザードは数えられる。損害発生の可能性を高める条件)」
「リスクが高い、低い(リスクは損害発生の可能性)」
「ペリルは、事故や災害が現実に発生し避難が求められているもの(損害を現実に生じさせる作用)」
「危険な動物」
「危機が迫る」

危機(人の立場・環境などを示す言葉)、事象、災害

- Incident
- emergency
- Crisis
- disaster
- catastrophe

†：下記参考文献を基に発表者が手を加えて記述した。

・Tomoichi_Sato：リスクという言葉自体がリスキーである,http://brevis.exblog.jp/13335724/.
・Wikipedia：リスク,https://ja.wikipedia.org/wiki/%E3%83%AA%E3%82%B9%E3%82%AF.
・後藤健太：リスクとはなにか,http://www.ccore.co.jp/plus/risk/.
・Stephen Asbury：リスクの歴史,http://japan.irca.org/resources/inform/archive/5/3/1/.
・平澤　敦：リスク＝危険＝危機＝クライシス？～身近で遠い日常・専門用語～,http://www.yomiuri.co.jp/adv/chuo/opinion/20121217.html.

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

†：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(IEC/ISO 31010：2009).
・日本規格協会：リスクマネジメント−用語−規格において使用するための指針 TR Q 0008:2003(ISO/IEC Guide 73:2002).
・日本規格協会：リスクマネジメント−用語 JIS Q 0073：2010(ISO Guide 73：2009).

3. ISO31000について†

- **リスクマネジメントの枠組み**
  ISO 31000　Risk management – Principles and guidelines:
  リスクマネジメント－原則及び指針
  - 2009年11月15日に発行

- **なぜISO 31000か？**
  - **あらゆる組織が利用できる、リスク一般を対象とした、汎用的な規格とすることを意図してつくられた（共通の枠組みであって、特定分野に言及しない）**

- **他のマネジメントシステムとの親和性**
  - ISO 22300　**社会セキュリティ**
  - ISO/IEC 27000　**情報セキュリティマネジメントシステム**
  - ISO 9000　**品質マネジメントシステム**
  - ISO 14000　**環境マネジメントシステム**

†: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−原則及び指針 JIS Q 31000:2010 (ISO 31000:2009).

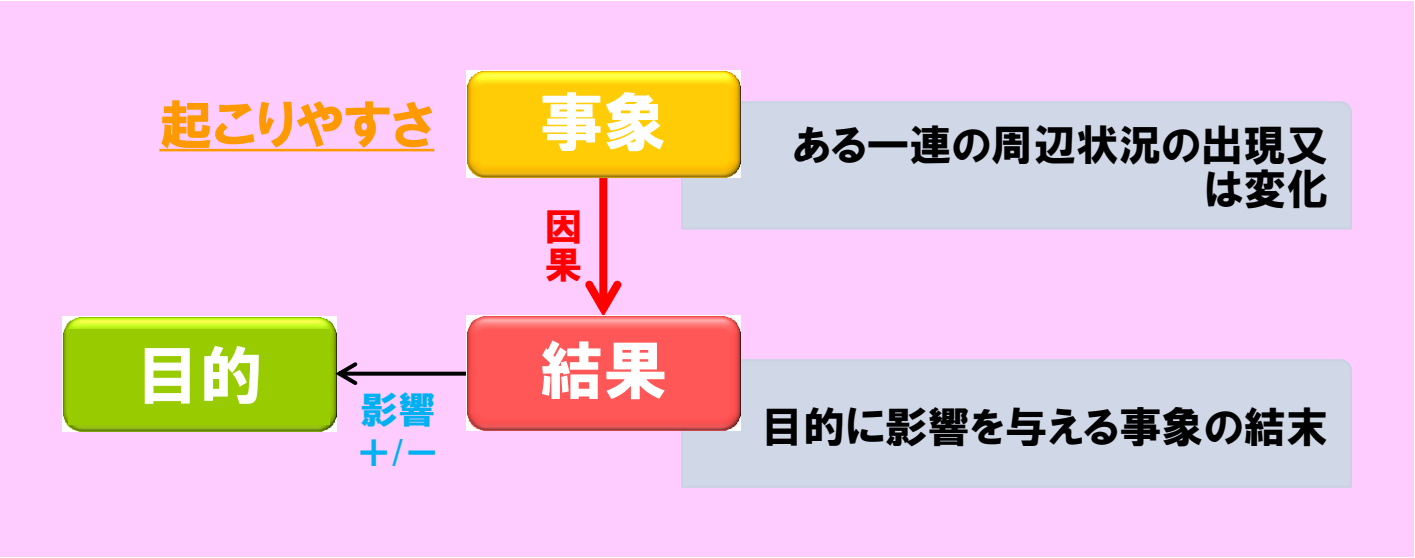
3. ISO31000について†

- ISO31000のリスク
  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、好ましい方向及び／又は好ましくない方向にかい(乖)離することをいう。
- 注記2　目的は、例えば、財務、安全衛生、環境に関する到達目標など、異なった側面があり、戦略、組織全体、プロジェクト、製品、プロセスなど、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、起こり得る事象、結果、又はこれらの組み合わせについて述べることによって、その特徴を記述されることが多い。
- 注記4　リスクは、ある事象(周辺状況の変化を含む。)の結果とその発生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。

†: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−原則及び指針 JIS Q 31000:2010 (ISO 31000:2009).

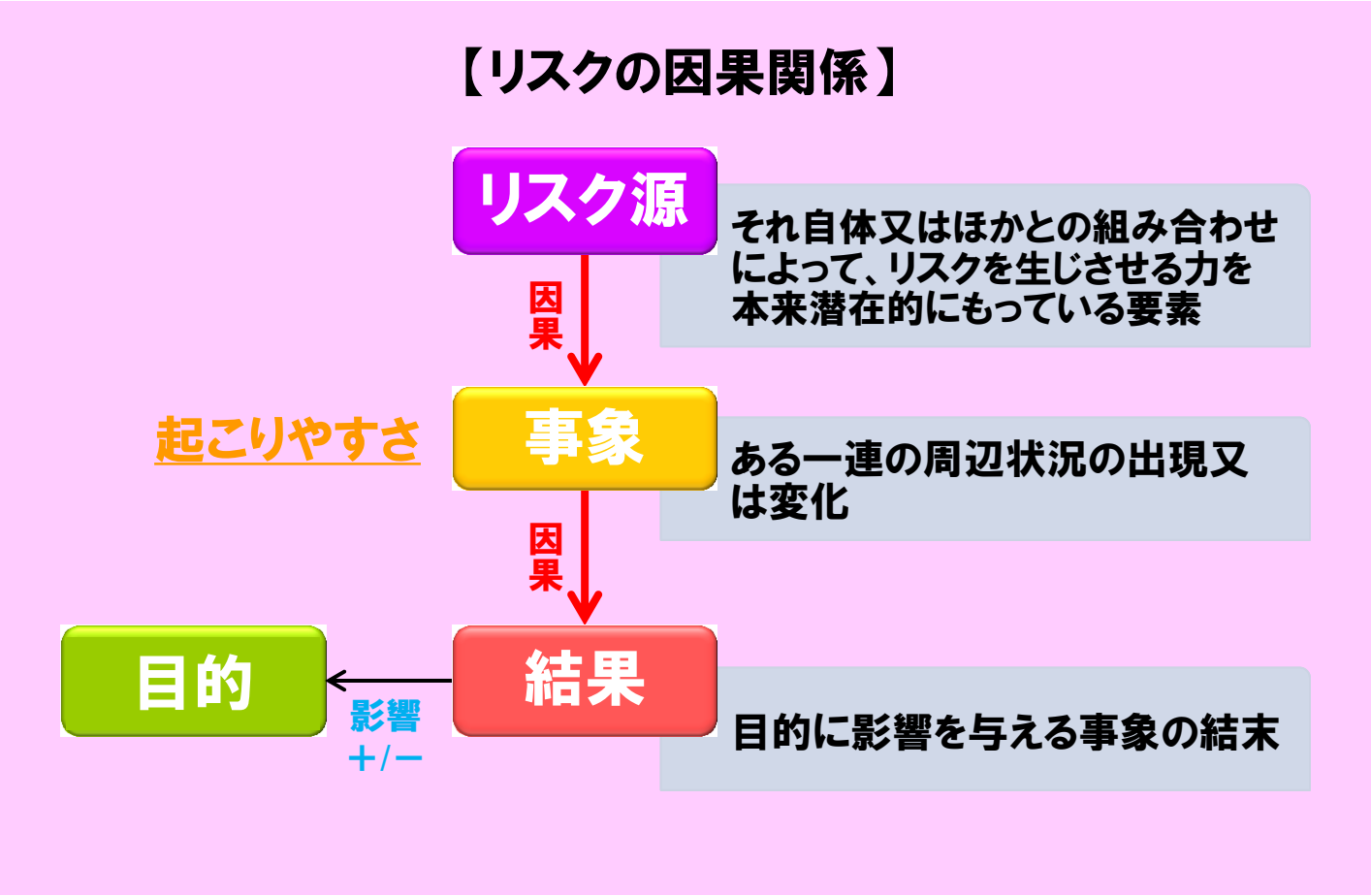
3. ISO31000について†



- 注記1　影響とは、期待されていることから、好ましい方向及び／又は好ましくない方向にかい(乖)離することをいう。
- 注記2　目的は、例えば、財務、安全衛生、環境に関する到達目標など、異なった側面があり、戦略、組織全体、プロジェクト、製品、プロセスなど、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、起こり得る事象、結果、又はこれらの組み合わせについて述べることによって、その特徴を記述されることが多い。**
- **注記4　リスクは、ある事象(周辺状況の変化を含む)の結果とその発生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。**

†: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−原則及び指針 JIS Q 31000:2010 (ISO 31000:2009).

参考:リスクの因果関係†



- リスク源　注記　リスク源は、有形の場合も無形の場合もある。

【参考】リスク因子、要因ともいう。事象や結果に対する直接的又は間接的な原因となり得る。

†: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−原則及び指針 JIS Q 31000:2010 (ISO 31000:2009).

参考:リスクの因果関係の説明例(火災)

- リスクの名称:
  木造住宅の火災による人的・物的損害のリスク
- リスクの分析(概要):
  防災都市づくりを目指す自治体は木造住宅密集地域の防火対策が急務である。
  木造住宅はコンクリート造りの住宅と比較して、着火・延焼しやすく、火災となれば、人命が失われ、又は火傷を負い、住宅・家財を失うリスクが大きい。
  着火するには、酸素、可燃物、可燃物の発火点以上の熱(火源)が必要であり、さらに延焼するには、着火後の自身の熱によって、燃焼を続けることである。
  可燃物は、発火点が低い程、着火しやすく、燃焼性(燃焼温度、燃焼に必要な酸素量等)が高い程、延焼しやすい。

【木造住宅の火災による人的・物的損害のリスクの因果関係】

リスク源
- 熱(火源)
- 酸素
- 可燃物(低発火点、燃焼性の高さ)

因果

起こりやすさ

事象

着火・延焼

因果

影響 +/−

目的

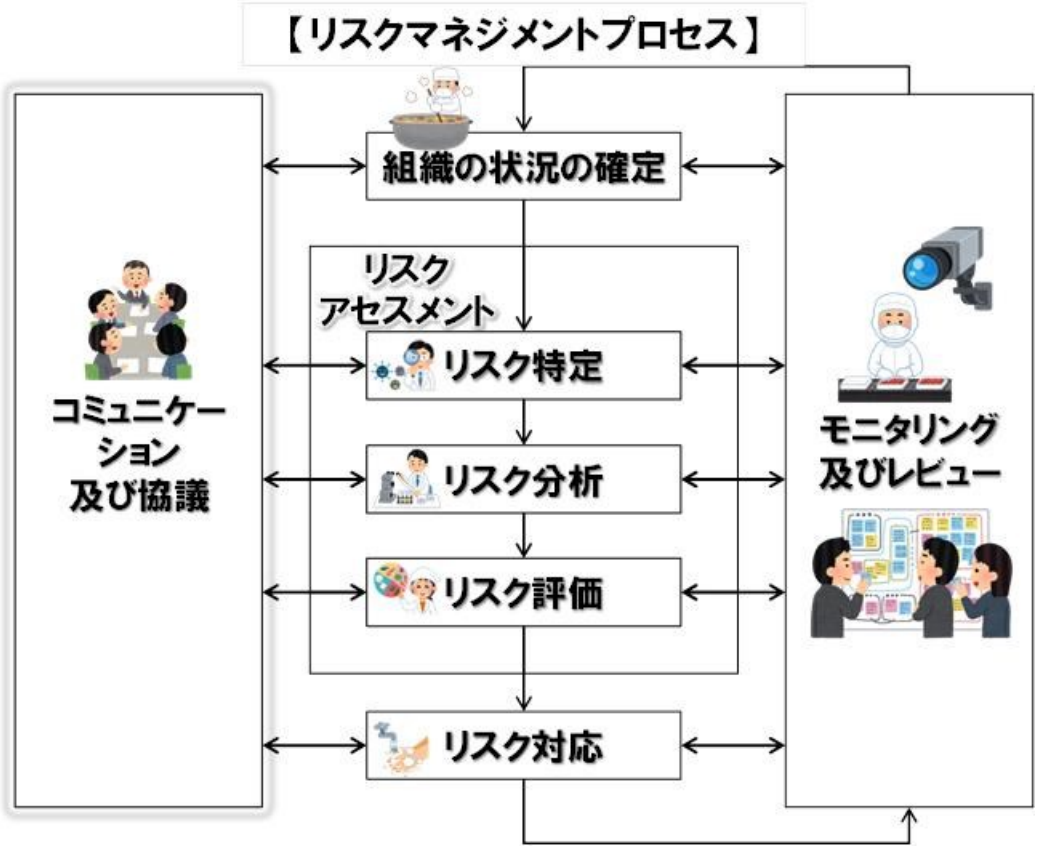
生命、身体、財産の保護

結果

死亡、火傷、財産焼失

4. ISO31000のリスクマネジメントプロセス†

- コミュニケーション、協議及び組織の状況の確定の活動、並びにリスクの特定、分析、評価、対応、モニタリング及びレビューの活動に対する、運用管理方針、手順及び実務の体系的な適用。



†: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−原則及び指針 JIS Q 31000:2010 (ISO 31000:2009).

4．1　組織の状況の確定†

- リスクを運用管理する場合に考慮すべき外部及び内部の要因を規定し、リスクマネジメント方針に従って**適用範囲**及び**リスク基準**を設定すること。

  – **リスク基準**を規定する場合に考慮するのが望ましい要素には，次の事項を含めることが望ましい。
    - 原因及び発生し得る**結果の特質及び種類**，並びにこれらをどのように測定するか。
    - **起こりやすさ**をどのように規定するか。
    - 起こりやすさ及び／又は結果を考える時間枠。
    - **リスクレベル**をどのように決定するか。
    - ステークホルダの見解。
    - リスクが受容可能又は**許容可能になるレベル**。
    - 複数のリスクの組合せを考慮に入れるのが望ましいか，また，考慮に入れる場合には，どのような組合せをどのように考慮するか。

リスク分析で活用

†: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−原則及び指針 JIS Q 31000:2010 (ISO 31000:2009).

4．2　リスク特定†

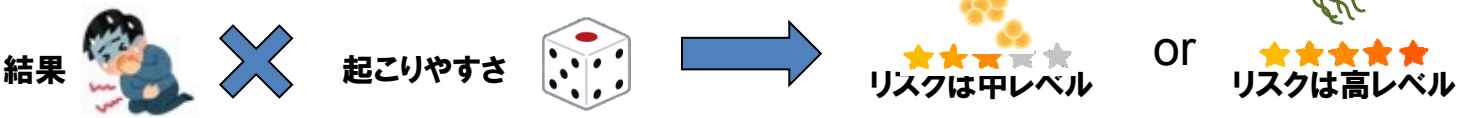
- **リスクを発見、認識及び記述するプロセス**
  - 注記1　リスク特定には、リスク源、事象、それらの原因及び起こり得る結果の特定が含まれる。
  - 注記2　リスク特定には、過去のデータ、理論的分析、情報に基づいた意見、専門家の意見及びステークホルダーのニーズを含むことがある。

- 組織は、リスク源、影響を受ける領域、事象（周辺状況の変化を含む。）、並びにこれらの原因及び起こり得る結果を特定することが望ましい。リスク特定のねらいは、組織の目的の達成を実現、促進、妨害、阻害、加速又は遅延する場合もある事象に基づいて、リスクの包括的な一覧を作成することである。ある機会を追及しないことに伴うリスクを特定することが重要である。包括的に特定を行うことが極めて重要である。なぜならば、この段階で特定されなかったリスクは、その後の分析の対象からは外されてしまうからである。
- リスク源が組織の管理下にあるか否かにかかわらず、たとえ、リスク源又はリスクの原因が明らかではないかもしれないリスクであっても、リスク特定に含めることが望ましい。

†: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−原則及び指針 JIS Q 31000:2010 (ISO 31000:2009).

4．3　リスク分析†

- リスクの**特質を理解**し、**リスクレベルを決定**するプロセス
  - 注記1　リスク分析は、リスク評価及びリスク対応に関する意思決定の基礎を提供する。
  - 注記2　リスク分析は、リスクの算定を含む。
- リスクレベル
  結果とその起こりやすさとの組合せとして表される、リスク又は組み合わさったリスクの大きさ



- リスク分析には、（特定した）リスクの理解を深めることが含まれる。
- リスク分析には、リスクの原因及びリスク源、リスクの好ましい結果及び好ましくない結果、並びにこれらの結果が発生することがある起こりやすさに関する考慮が含まれる。結果及び起こりやすさに影響を与える要素を特定することが望ましい。リスクは、結果及び起こりやすさ、並びにリスクのその他の属性を決定することによって分析される。


リスクレベル

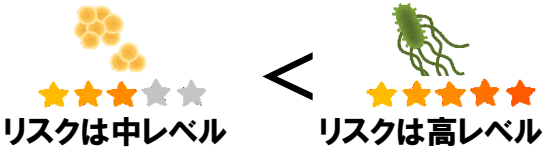

リスク源


影響を与える要素

†：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−原則及び指針 JIS Q 31000：2010 (ISO 31000：2009).

4．4　リスク評価†

- **リスク及び／又はその大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス**
  - 注記1　リスク評価は、リスク対応に関する意思決定を手助けする。



- リスク基準
  リスクの重大性を評価するための目安とする条件
- リスク評価の目的は、リスク分析の成果に基づき、どのリスクへの対応が必要か、対応の実践の優先順位はどうするかについて意思決定を手助けすることである。

- リスク評価には、組織の状況を考慮して確定されたリスク基準と、リスク分析プロセスで発見されたリスクのレベルとの比較が含まれる。この比較に基づいて、対応の必要性について考慮することができる。

†: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−原則及び指針 JIS Q 31000:2010 (ISO 31000:2009).

参考:リスクアセスメントの例(なりすましによるシステムの不正利用)

- 顧客がアクセスするシステムへの**なりすまし**による**不正利用**のリスクをアセスメントする

4．5　リスク対応†

Innovative R&D by NTT

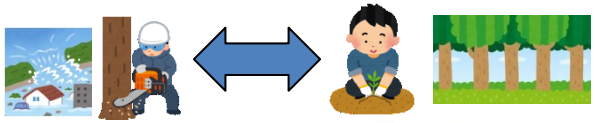
- **リスクを修正するプロセス**
  - 注記1　リスク対応には、次の事項を含むことがある。

1. リスクを生じさせる活動を、**開始又は継続しない**と決定することによって、リスクを回避すること。

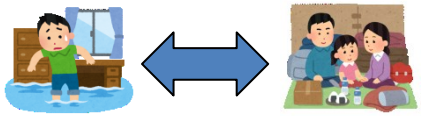
2. ある機会を追及するために、**リスクをとる又は増加**させること。

3. リスク**源を除去**すること。

4. **起こりやすさ**を変えること。



5. **結果**を変えること。



6. 一つ以上の他者とリスクを**共有**すること（契約およびリスクファイナンシングを含む。）。

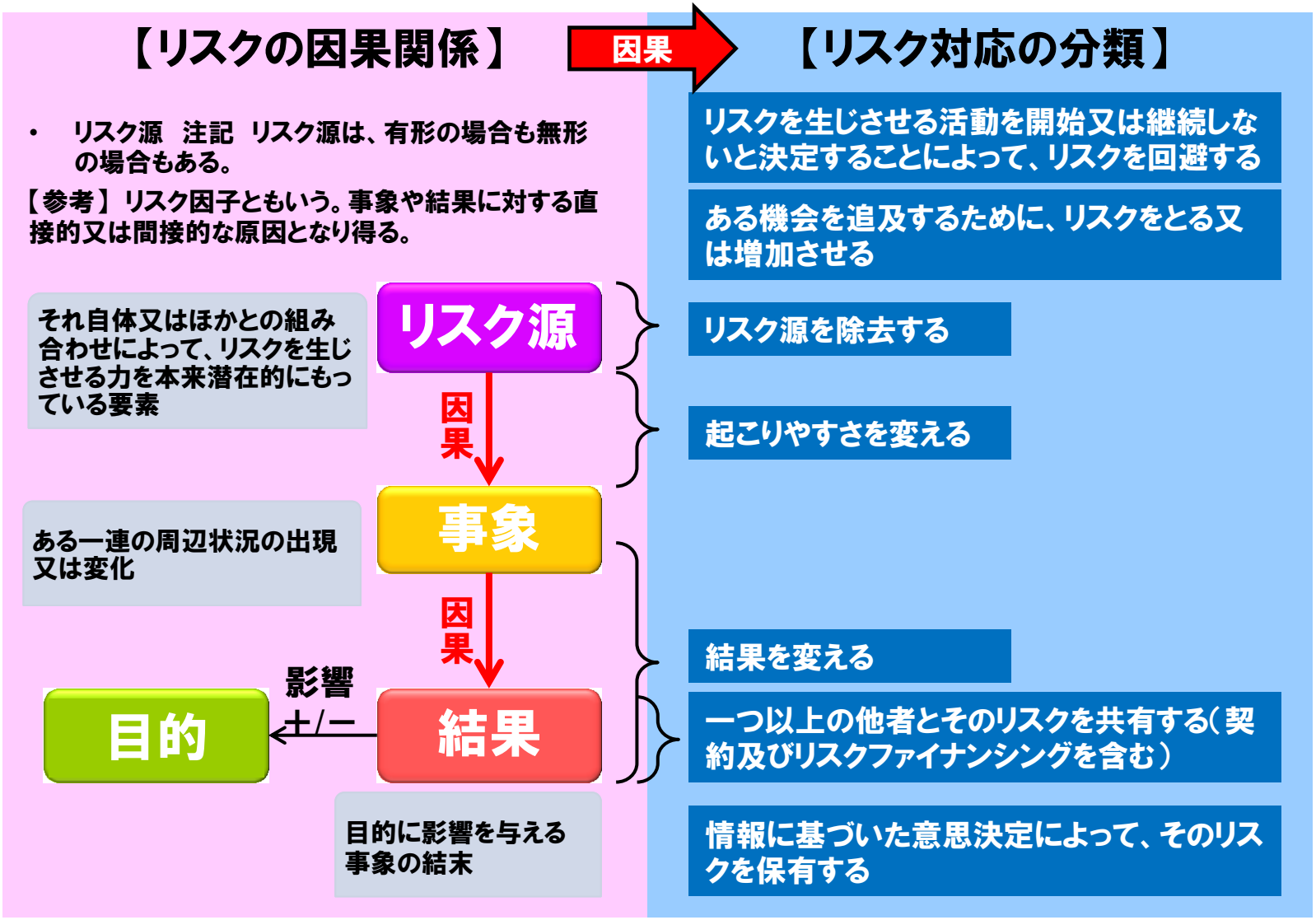
7. 情報に基づいた意思決定によって、リスクを**保有**すること。

  - 注記2　好ましくない結果に対処するリスク対応は、“リスク**軽減**”、“リスク**排除**”、“リスク**予防**”及び“リスク**低減**”と呼ばれることがある。
  - 注記3　リスク対応が、**新たなリスクを生み出したり**、既存のリスクを修正したりすることがある。

NTT

†：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−原則及び指針 JIS Q 31000：2010 (ISO 31000：2009).

参考：リスク対応の7つの基本活動とリスクの因果関係



5．1　各業界の状況†

Innovative R&D by NTT

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

†: 下記参考文献を基に発表者が手を加えて記述した。

・行待 武生：ヒューマンエラー防止のヒューマンファクターズ、(株)テクノシステム、2004.
・河野 龍太郎：ImSAFER によるヒューマンエラー事例分析、http://www.jichi.ac.jp/msc/wordpress/wp-content/uploads/2010/08/ImSAFER-PPT5.pdf.

5．1　各業界の状況

各業界で**重視している箇所**に合わせて**独自に発展**

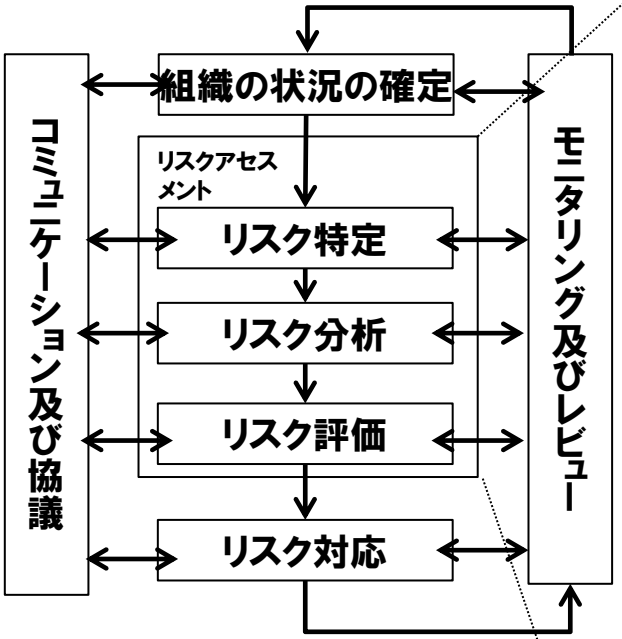
- 航空業界：人と**環境**（他の人，機械など）
- 原子力業界：人の**過誤率**
- 医療業界：**人的要因の特定**
- 化学プラント業界：正常時からの**逸脱の有無**
- 自動車業界：**評価対象**（ハードウェア，業務のプロセス等）

など

50種類以上存在し、乱立状態

5．2　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

5．2　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 †

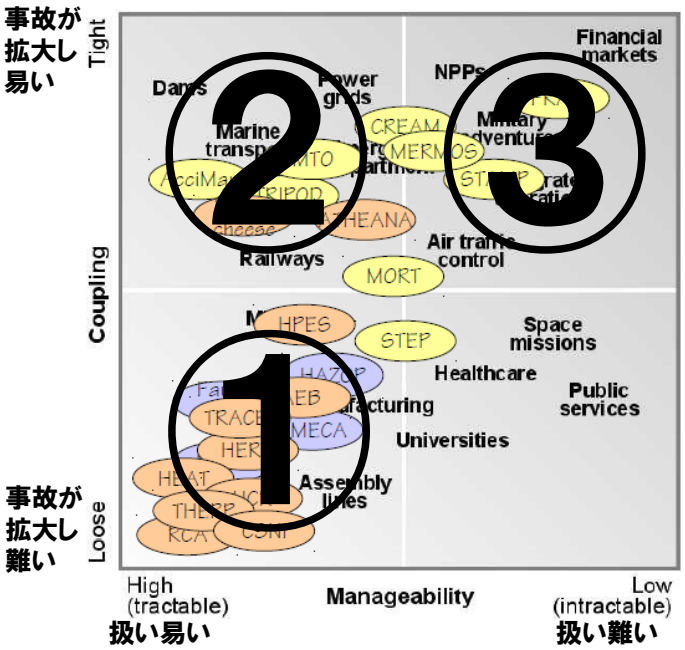
分析評価手法	リスクアセスメントの種類	リスク特定方法	適用性
ブレーンストーミング	支援法		推奨
構造化又は半構造化インタビュー		系統的アプローチ	
デルファイ法			
チェックリスト	洗出し法	証拠に基づく方法	
予備的ハザード分析（PHA）		帰能的推論法	
HAZOP スタディーズ	機能分析	系統的アプローチ	
ハザード分析及び必須管理点（HACCP）			
環境リスクアセスメント（毒性リスクアセスメント）	シナリオ分析		
構造化“Whatif”技法（SWIFT）	支援法	系統的アプローチ	
シナリオ分析	シナリオ分析		
事業影響度分析（BIA）			可
根本原因分析（RCA）			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		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）			

†: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(IEC/ISO 31010:2009).

5．2　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

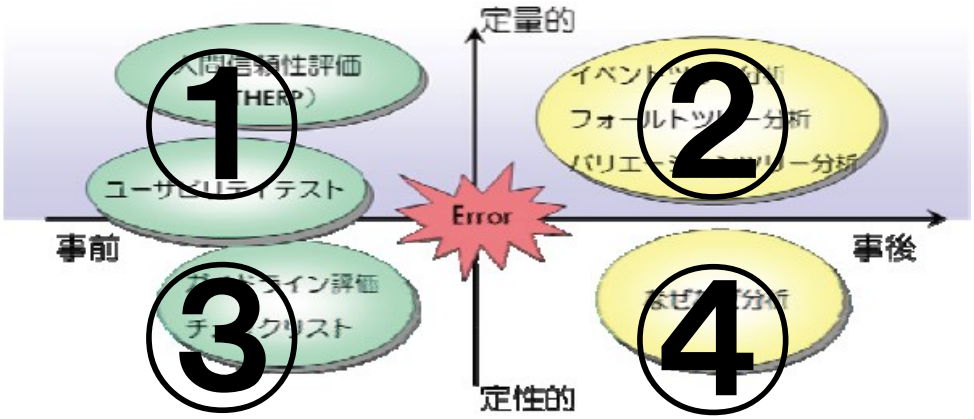
※1：**管理難易度　＝　精密度**(Description)　×　**不安定度**(Instability)　×　**理解難度**(Comprehensibility)
（精密度：単純⇔複雑，不安定度：安定⇔不安定，理解難度：判り易い⇔判り難い）

†：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
•Erik Hollnagel:On How (Not) To Learn from Accidents,http://www.uis.no/getfile.php/1322751/Konferanser/Presentasjoner/Ulykkesgransking%202010/EH_AcciLearn_short.pdf.

5．2　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）

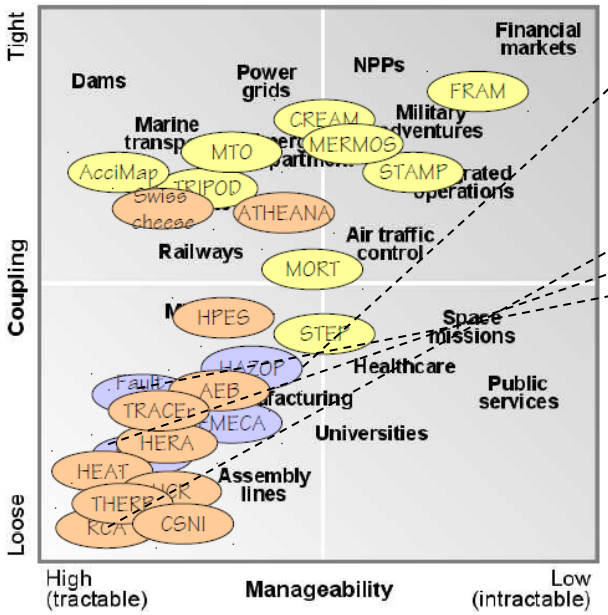
定量・定性を縦軸に，事前・事後を横軸に分析評価手法を分類

†：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.

5．2　分類について

Innovative R&D by NTT

Hollnagelの分類



IEC/ISO 31010

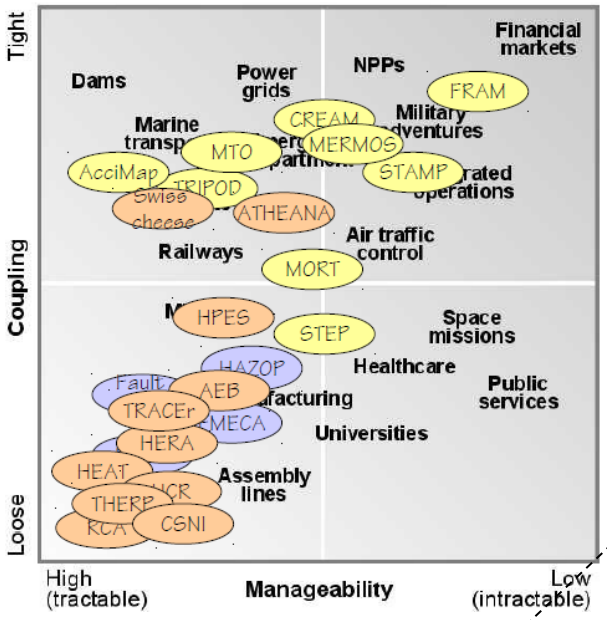
分析評価手法
ブレーンストーミング
構造化又は半構造化インタビュー
デルファイ法
チェックリスト
予備的ハザード分析（PHA）
HAZOP スタディーズ
ハザード分析及び必須管理点（HACCP）
環境リスクアセスメント（毒性リスクアセスメント）
構造化“Whatif”技法（SWIFT）
シナリオ分析
事業影響度分析（BIA）
根本原因分析（RCA）
故障モード・影響解析（FMEA）
故障の木解析（FTA）
事象の木解析（ETA）
原因・結果分析（CCA）
原因影響分析（特性要因図（魚骨線図））
防護層解析（LOPA）
決定木解析
人間信頼性分析（HRA）
ちょう（蝶）ネクタイ分析
信頼性重視保全（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

5．2　分類について

Innovative R&D by NTT

Hollnagelの分類

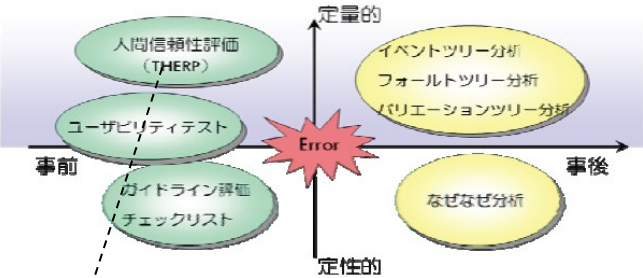


と　の殆どがHRA

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．

5．2　分類について

Innovative R&D by NTT

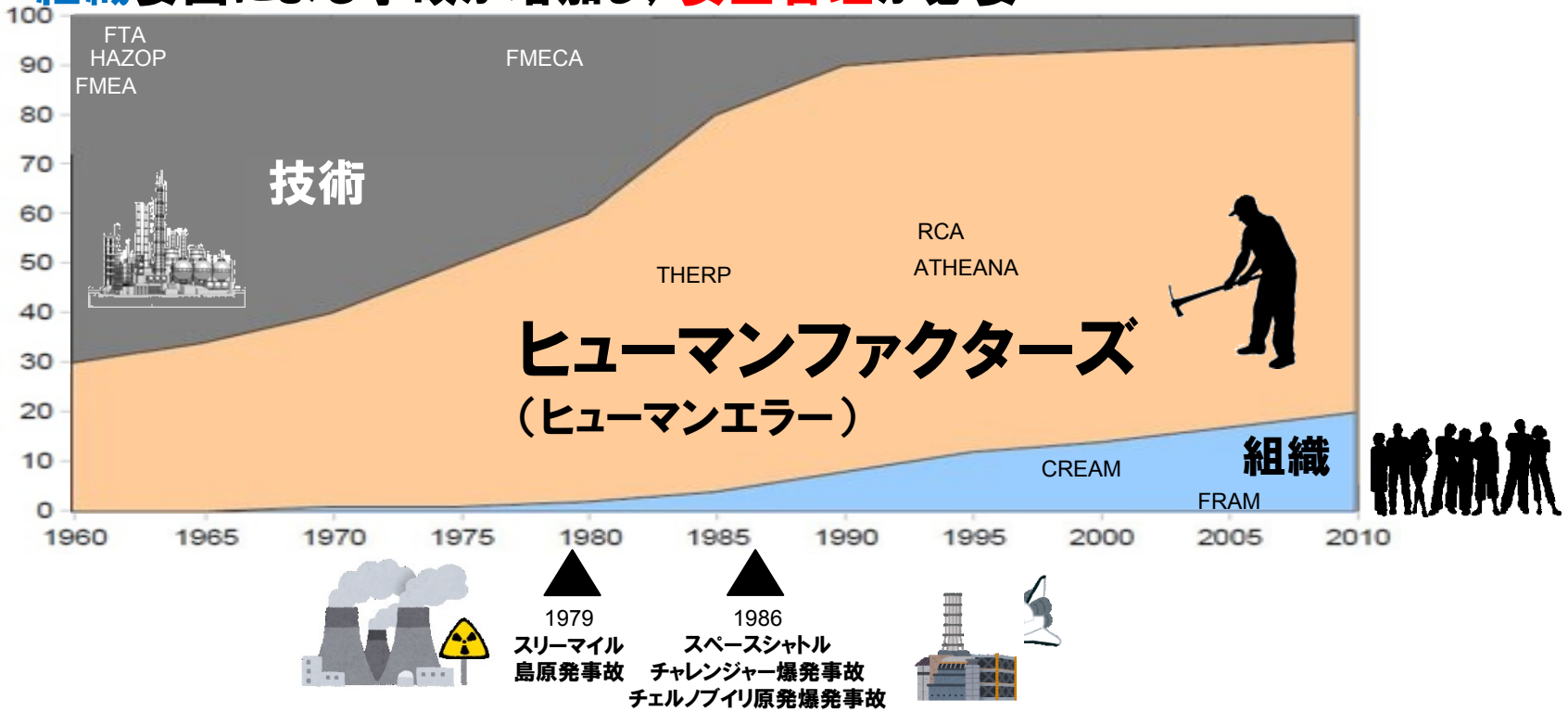
分析評価手法の適切な分類は存在しない

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

5．3　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

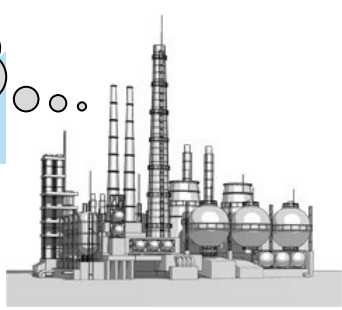


事故（Accident）における各要因の割合（1960年～2010年）

†：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/1322751/Konferanser/Presentasjoner/Ulykkesgransking%202010/EH_AcciLearn_short.pdf.

5．3．1　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				

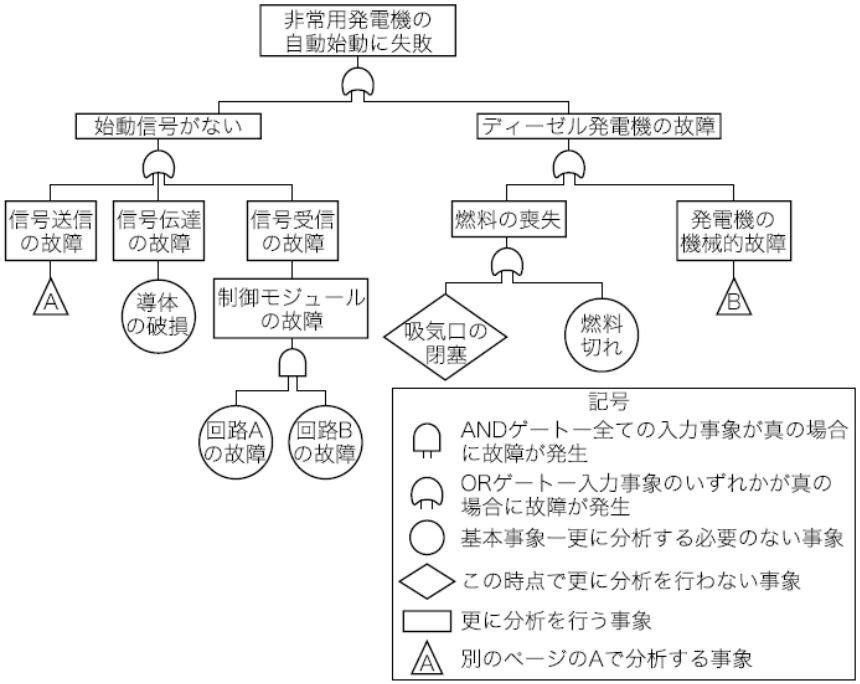
HAZOP**実施例**

†：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**



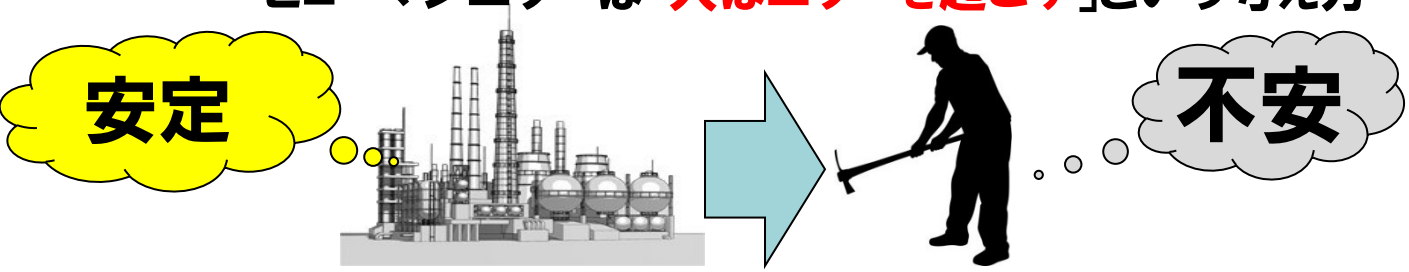
FTA**実施例**

†：**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.

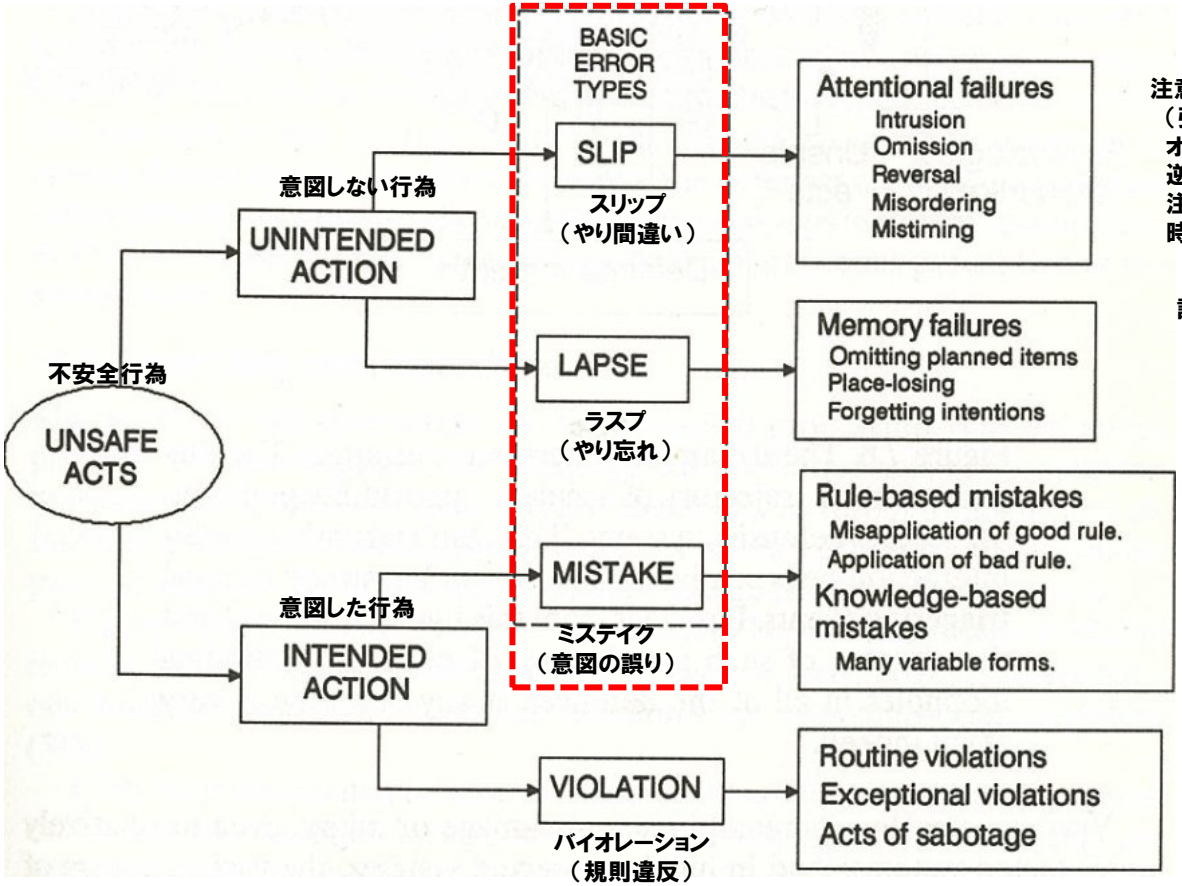
5．3．2　ヒューマンファクターズの時代

- **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



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

- 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

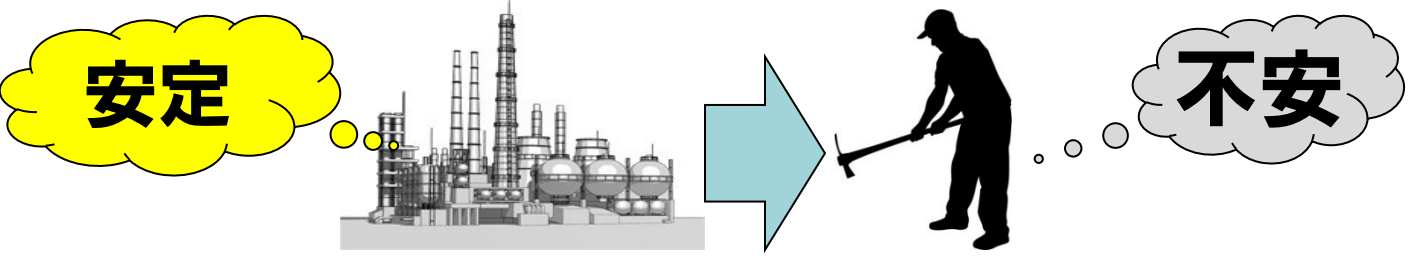
Reasonの不安全行為の定義†

†:下記参考文献を基に発表者が手を加えて記述した。

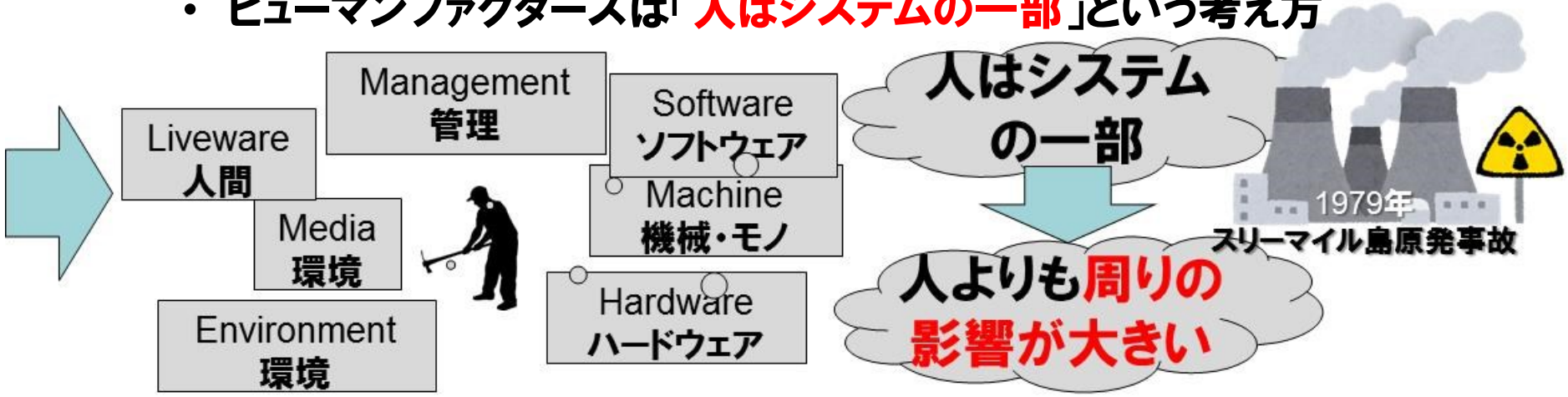
•James Reason: Human Error, Cambridge University Press,1990.
• Swain, A. D. & Guttmann, H. E. : Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application, U.S. NRC-NUREG/CR-1278, 1980.

5．3．2　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



5．3．2 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)

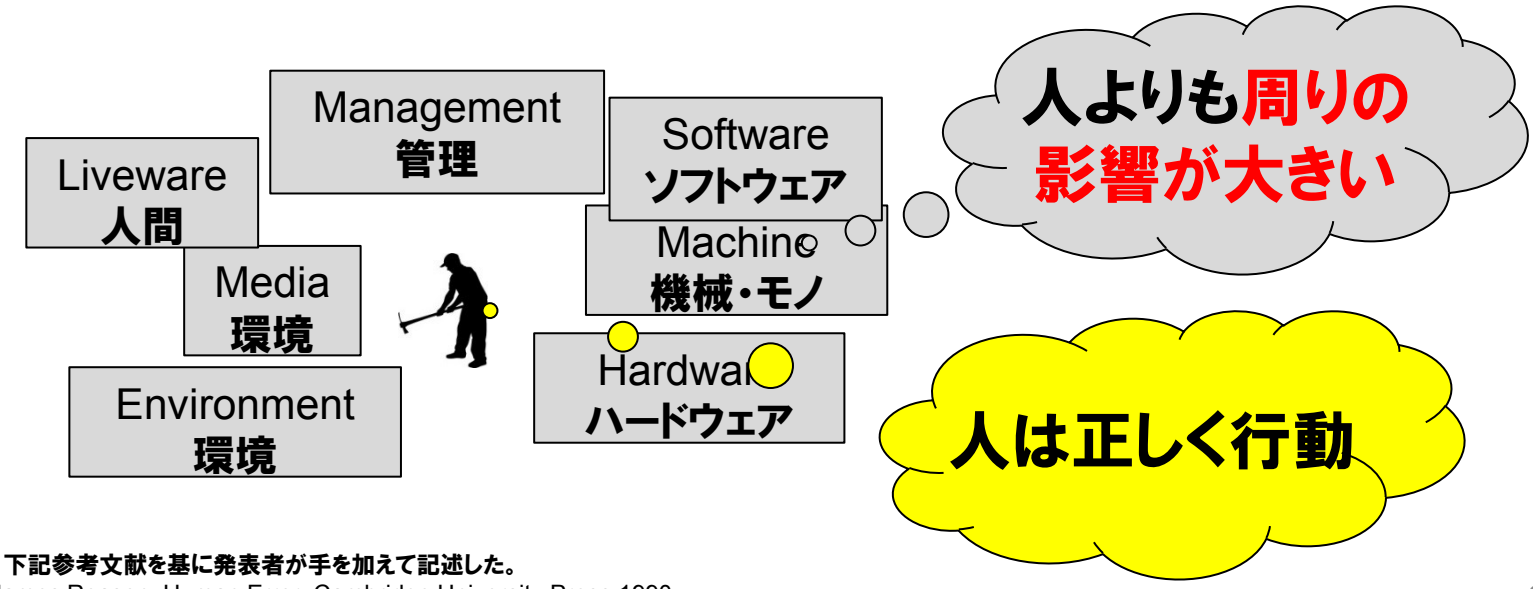
人間はシステムの一部

「人的過誤率」とも呼ばれている

    - 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



†：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.

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

ヒューマンエラー確率のデータベースの例

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

†：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」

困っている人がいたから譲った

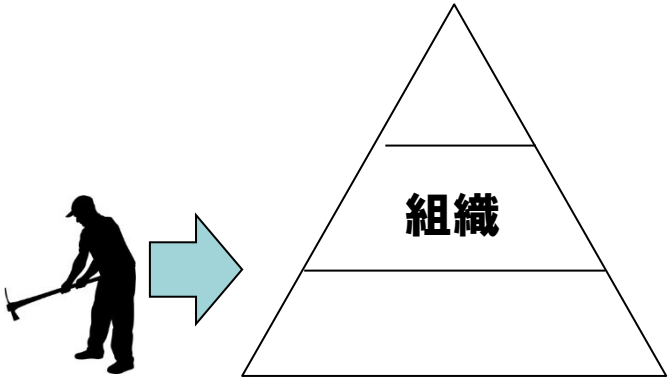
- **行為者観察者効果　認知バイアス**
  - 外的なものに帰属→自分の行動
  - 見る人の立場によって変わってくる（記憶・知覚　認知バイアス），
    - 毎回遅刻する人
      - 他人は「あの人はだらしない人だ」
      - 本人は「バスがなかなか来なかった」

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

†:”放送大学：錯覚の科学 第12回”を基に発表者が加工

5．3．3　安全管理の時代†

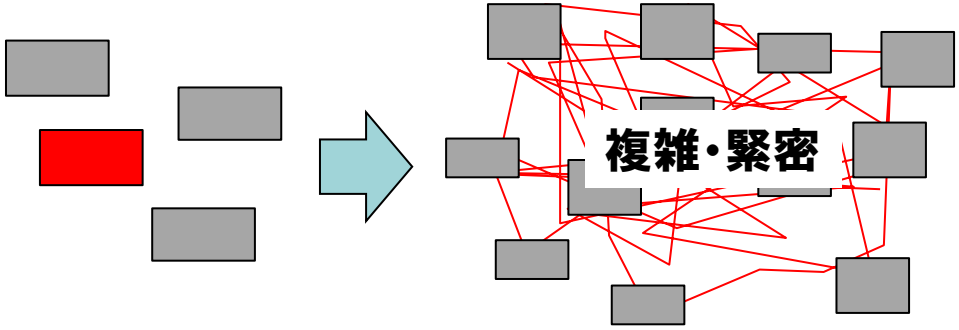
- **時代：**1995年代～
- **事故の捉え方**
  - **「個人から組織へ（組織事故）」**
  - **「要素機能の不具合から複雑な要素機能間の共鳴へ（機能共鳴型事故）」**



組織事故

主な手法：

AcciMap (1997)，HFACS(2003)



機能共鳴型事故

主な手法：

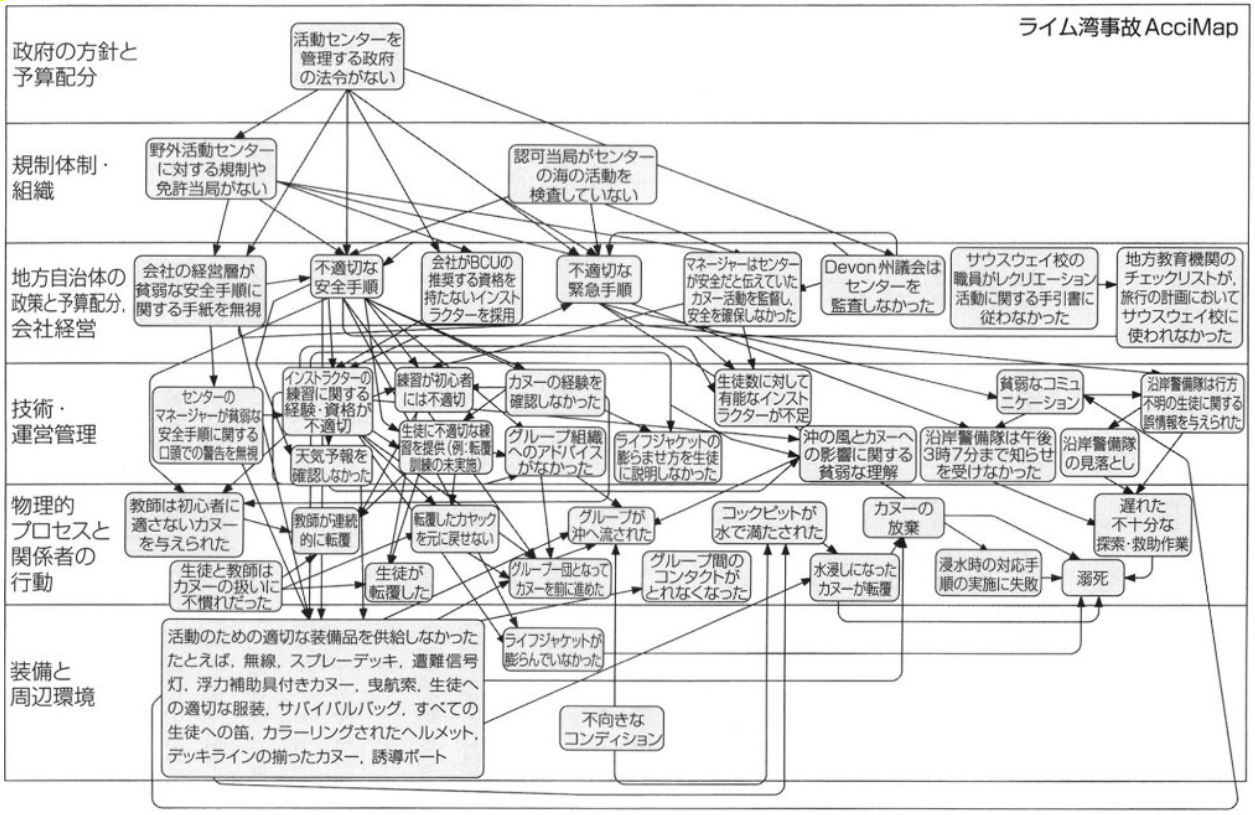
STAMP(2002)，FRAM(2004)

NTT†：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：自己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：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．

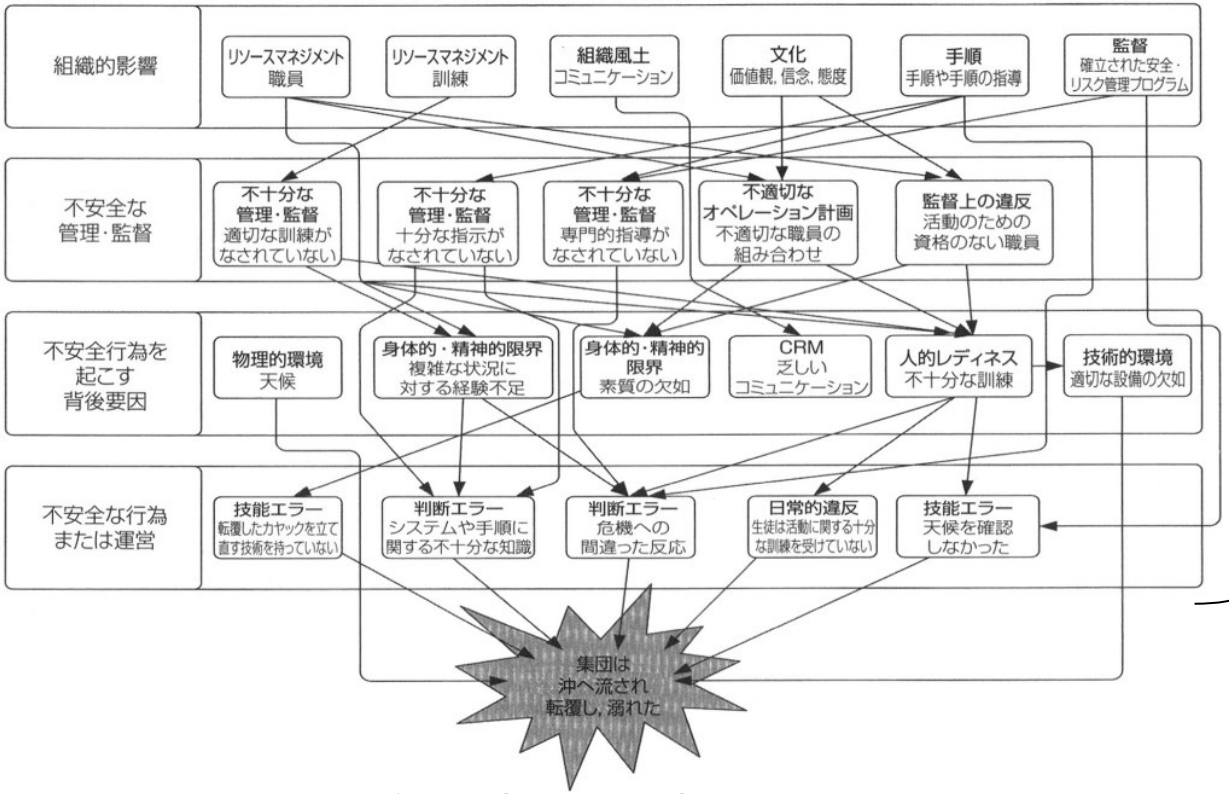


†：下記参考文献を基に発表者が手を加えて記述した。

・ポール・サイモン他5名、小松原明哲訳：自己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

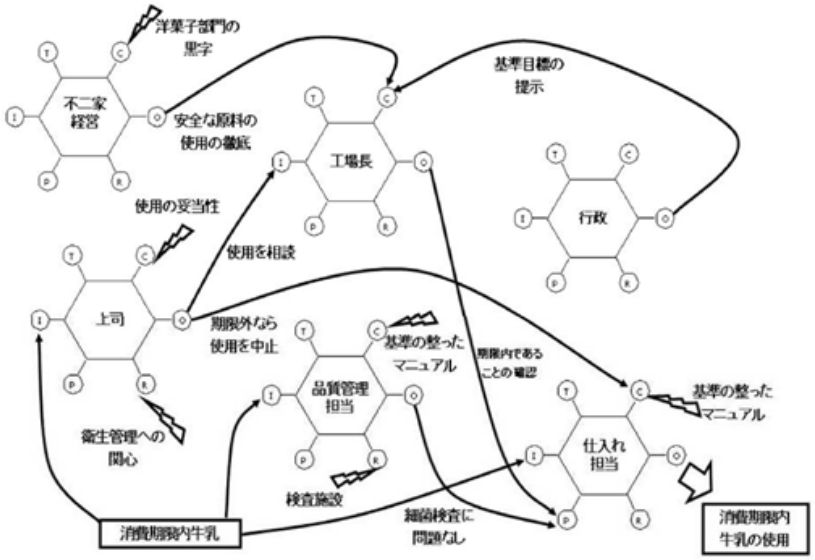
†：下記参考文献を基に発表者が手を加えて記述した。

・ポール・サイモン他5名、小松原明哲訳：自己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

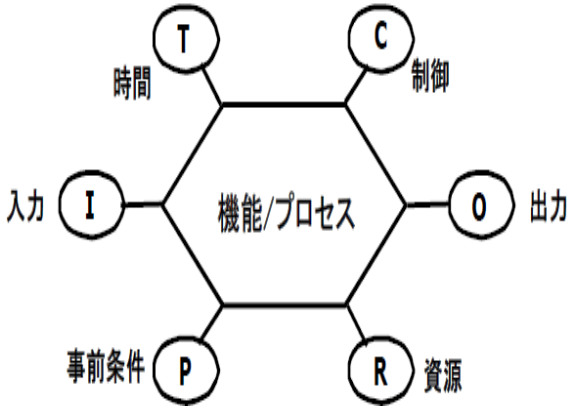
参考：FRAM†

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



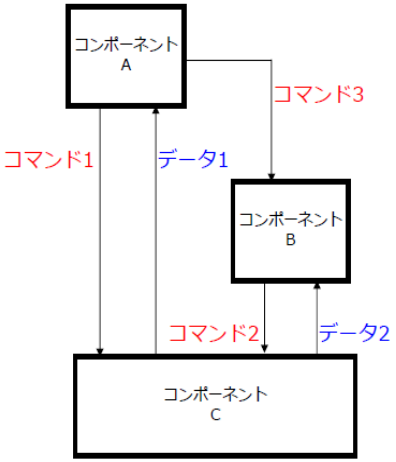
機能の六角形表現

†：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．**



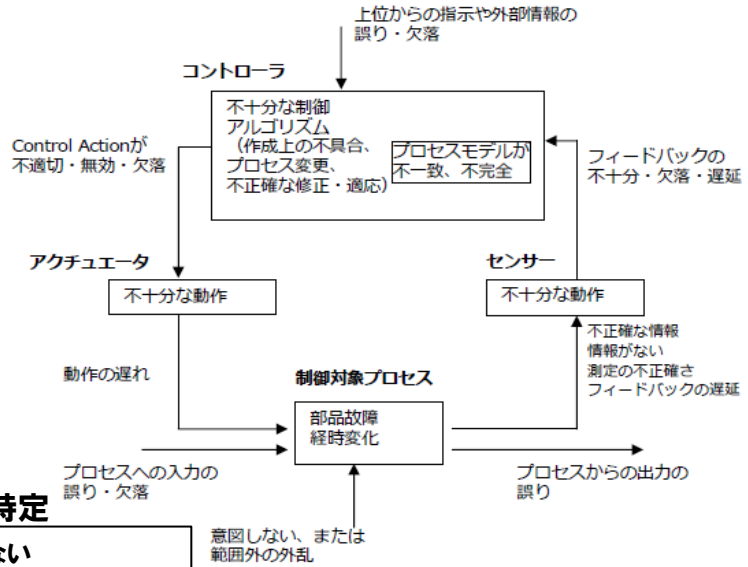
Control Structure

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）**



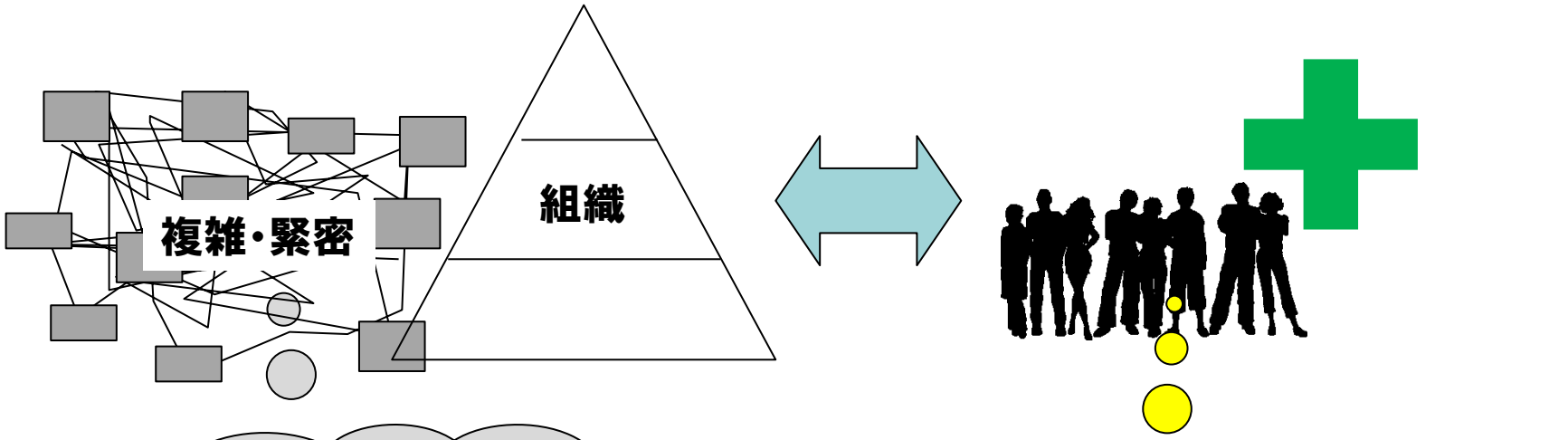
Control Loop Diagram

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

5．4　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

5．4　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。

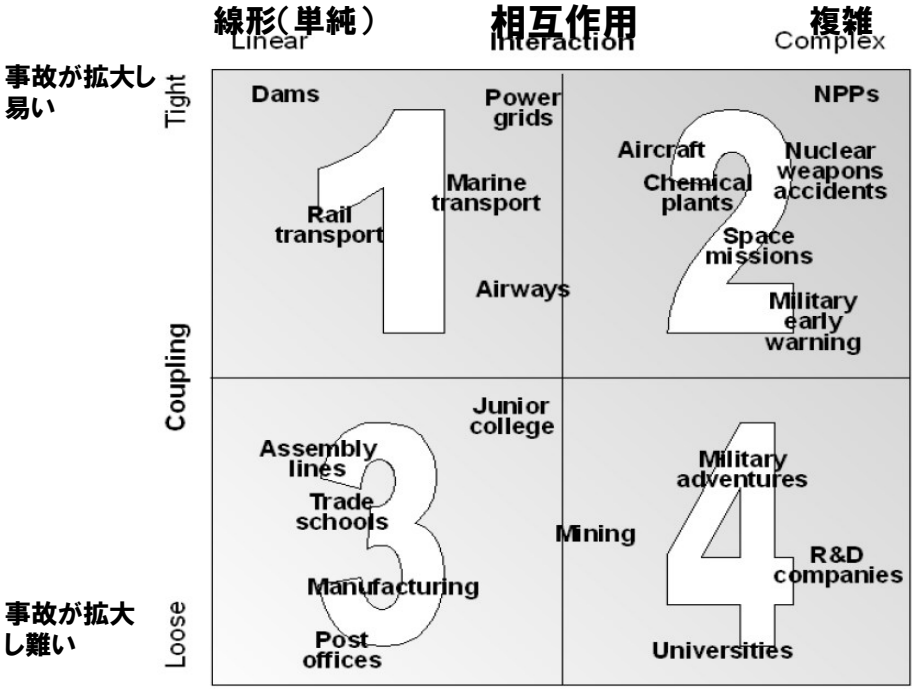
2. **高信頼性理論**（HRT: High Reliability Theory（1980年代後半））
   - NATに対抗する理論。バークレー・グループとWeick & Sutcliffeの研究が有名.
   - 事故の**危険性が高い状況下にあっても高い信頼性**を保っている組織（HROs）の分析

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―、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

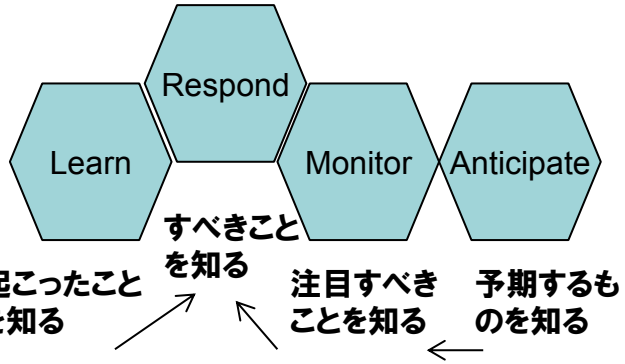
Reasonによる安全文化

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

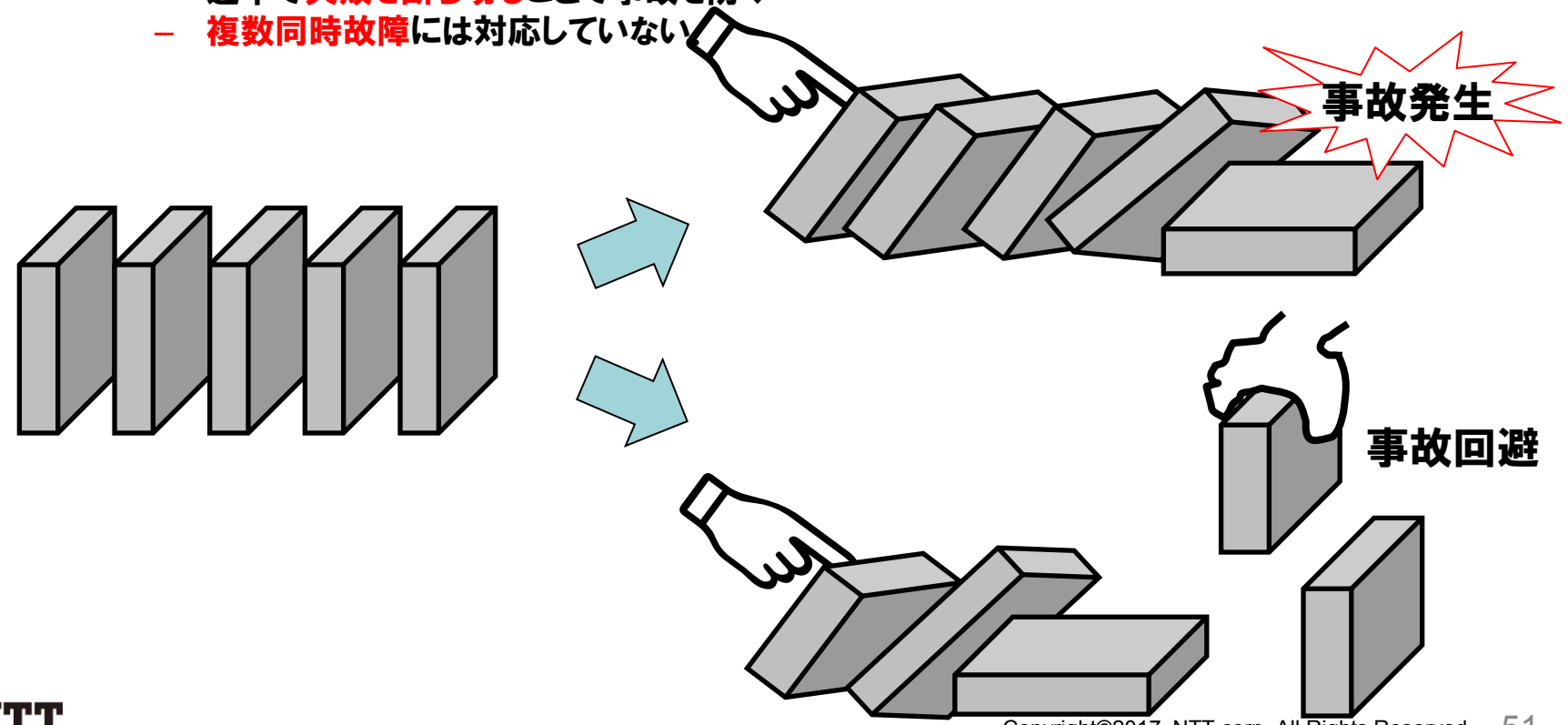
学習	事実，すなわち経験に基づく教訓の抽出を指す．重要な点は，失敗事例だけでなく成功事例からも学ぶ，すなわち「なぜ（事故が）起こったのか？」ではなく，「なぜ（事故が）起こらなかったのか？」を学ぶ点である．
監視	危機の監視，すなわちシステムの内外に脅威が訪れていないかどうかの監視を指す．何らかの指標を用いたシステムのパフォーマンスや環境の変化の評価などが該当する．
予測	可能性の予測，すなわち先を見据えた脅威や変化の予測を指す．将来起こりえて，かつシステムの能力に影響を及ぼしそうな出来事，状態，変化の予測が該当する．
対応	現実への対応，すなわち実際に発生した混乱や障害への対応を指す．具体的には，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).

5．4　事故のモデル†

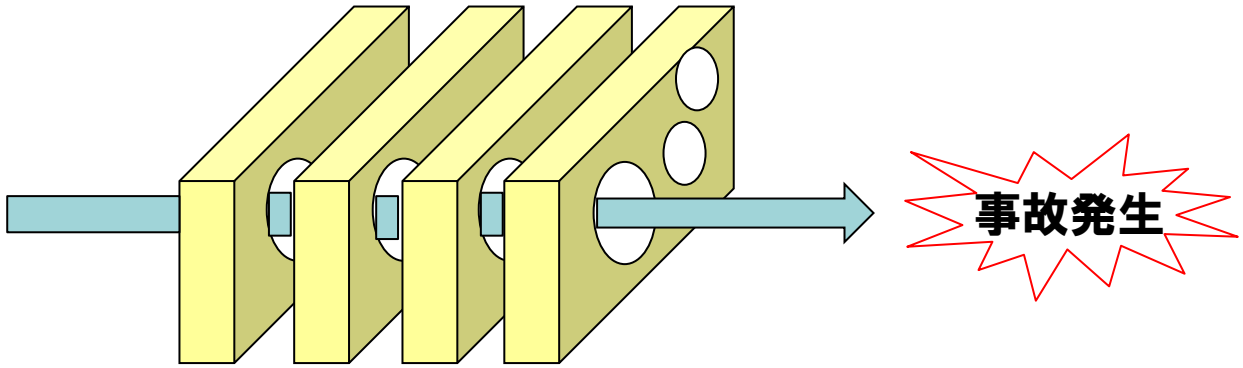
- **単純線形モデル**
  - Heinrich**のドミノモデル**（1930）、**連鎖モデル**（Sequential Model）**とも呼ばれる**
    - **事故は1つの根本原因からの連続的な失敗から発生**
      - RCA、FMEAやFTA**はこのモデルに近い分析評価手法**
    - **単一故障（1つの根本原因）に対応．**
      - **途中で失敗を断ち切ることで事故を防ぐ**
      - **複数同時故障には対応していない**



†：“H.W. Heinrich: Industrial Accident Prevention, 3rd edition, McGraw-Hill Book Company Inc、1950.”**を基に発表者が手を加えて記述した**

5．4　事故のモデル†

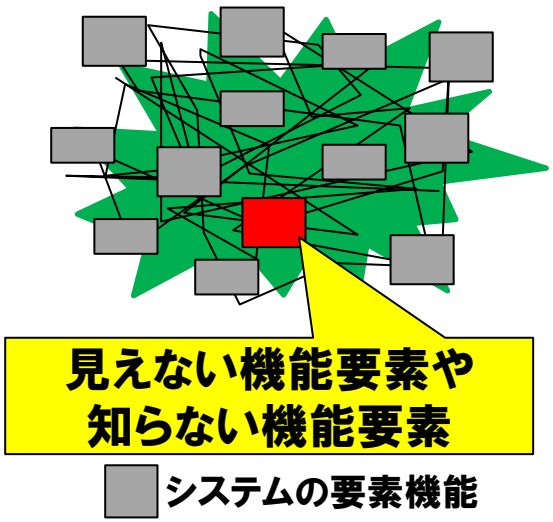
- **複雑線形モデル**
  - Reasonのスイスチーズモデル（1990）とも呼ばれる
    - 事故は複数の**防護壁の劣化**
      - AcciMap (1997)，HFACS(2003)はこのモデルに近い分析評価手法
    - 組織事故を想定（複数同時事故）
      - **システムや要素の相互間の複合要因**による機能共鳴型事故には十分対応していない．

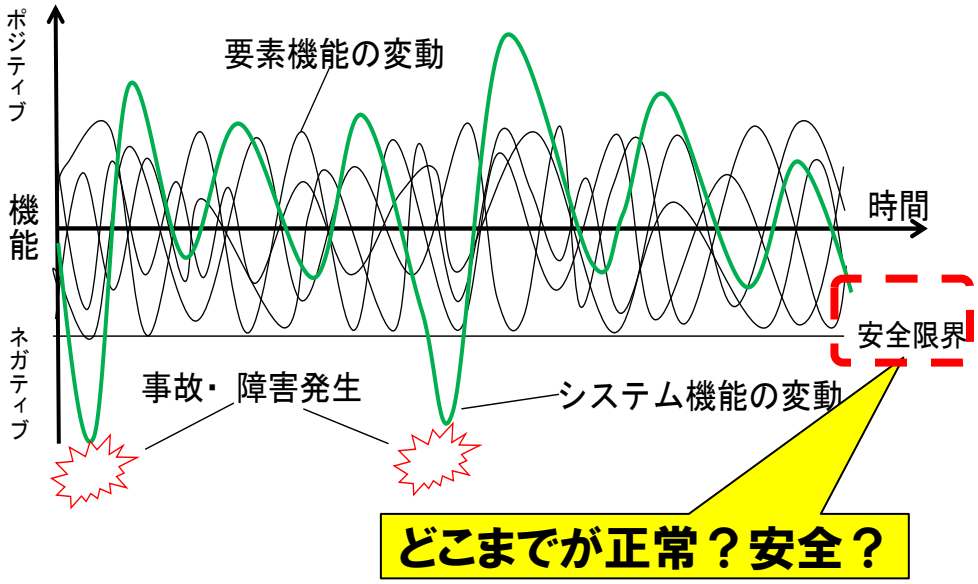


†：下記参考文献を基に発表者が手を加えて記述した。
・ポール・サイモン他5名、小松原明哲訳：自己分析のためのヒューマンファクターズ手法、海文堂出版、2016

5．4　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。
・Erik Hollnagel , 小松原 明哲 訳. 社会技術システムの安全分析　FRAMガイドブック. 海文堂出版,2013.
・システム安全性解析手法WG. はじめてのSTAP/STPA. IPA, 2016.

参考：認知行動療法との比較†

- 認知行動療法の3つの系譜
  - 第１世代：行動療法系
    - 行動療法系は**行動を変えること**で問題解決していく

  - 第2世代：認知療法系
    - 認知は考えること．その**考えを変えていくこと**で問題解決していく

  - 第3世代

    - **コントロールよりも受け入れること**．自分の行動の仕方，および考え方を受け入れることで問題解決していく
      - マインドフルネス認知療法など．
    - 「受け入れる」ということで自分をあるがままにしていくことが**森田療法と同様**．
      - **レジリエンス工学**の「安全を向上させるためには，うまくいかなかった物事について，その数を減らそうとするよりも，**多数のうまくいった物事についてさらに改良を図るほうが，より容易でもあるし効果的**でもある」という考えにも近い

†:”放送大学：認知行動療法　第1回”を基に発表者が加工

End

付録

参考：4M-4E †

- 4M-4Eは、5M、7Eの場合もある
- **要因**：4M+α
  - Man ：**作業者本人、上司や同僚などの人間要素**
  - Machine ：**道具、機械、設備などの要素**
  - Media ：**照明、騒音を始めとする環境の要素、情報環境なども含まれる。情報伝達、表示、作業マニュアルなどもこれに該当する。**
  - Management ：**制度や管理体制など、管理的な要素**
  - Mission ：**作業の目的、目標に関する要素**
- **対策**：4E+α
  - Education **教育、訓練**
  - Engineering **技術、フェールセーフ**
  - Enforcement **強化徹底：規程、手順、注意喚起**
  - Example **模範、事例紹介**
  - Eliminate **排除、自動化**
  - Easy to understand **わかり易く：覚えないで計器の脇に印**
  - make Easier **やり易い：作業し易い高さ**

メリット：
・解析者の先入観などをある程度は排除できる。

デメリット
・トラブル事例の分析を目的とした手法であるため、ヒューマンエラー自体が要因の中に入ってしまい、ヒューマンエラーの要因分析が行われないままに分析が終わってしまう恐れがある。

		Man：人間（当事者）	Machine：機械・モノ	Media：環境	Management：管理
具体的要因					
対策	Education 教育・訓練				
	Engineering 技術・工学				
	Enforcement 強化・徹底				
	Examples 模範・事例				

†：下記参考文献を基に発表者が手を加えて記述した。
・佐々木崇裕、原田要之助：運用におけるヒューマンファクターに着目した情報セキュリティ対策について、情報処理学会研究報告、Vlo.2014-EIP-63 No13 (2014).

参考：RCA†

- **根本原因故障分析**（Root Cause Analysis）
  - RCFA（Root Cause Failure Analysis）、**損失分析とも呼ばれる**
  - **すぐ目に見える兆候だけに対処するのではなく，根本又は発端となる原因の特定を試みる。評価は，「物理的要因→人的要因→マネジメント又は根本要因」と進めることが多い。**
  - **因果関係が強く再現性が高いものに有効であるが、因果関係が緩く複数の要因が絡むような場合では有効ではない。**

- **手順**
  1. **分析チームの結成、RCA の適用範囲及び目的の設定、故障又は損失のデータ及び証拠の収集**
  2. **原因を究明するための構造化分析の実施**
  3. **解決策の立案及び勧告の実施、実施した勧告の成否の検証**

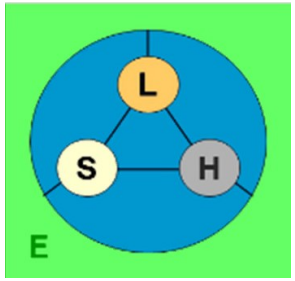
- **構造化分析は，次のうちの一つで構成してよい。**
  - **“なぜなぜ5 回”技法。繰り返し“なぜ”を問いかけて，原因及び副原因の層を剥いでいく。**
    - **例：なぜ自動車事故が起こったのか←なぜ対向車とぶつかったのか←なぜ対向車線にはみだしたのか←なぜ雨でスリップしたのか←なぜタイヤがすり減っていたのか←なぜ車検でタイヤの交換をしなかったのか←車検に費やす予算が限られていた**
  - **故障モード・影響解析**（FMEA）、FTA
  - **特性要因図（魚の骨線図又は石川線図ともいう）、連関図**

†：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(IEC/ISO 31010：2009).

参考：SHEL †

- **SHEL：もともとはヒューマンファクター工学の説明モデルとして提案されたものが、フレームワークとして使われるようになったもの**

L(**中心**)：**作業者本人**(Liveware)
S：**ソフトウエア**(Software) **作業手順や作業指示の内容**
H：**ハードウエア**(Hardware) **作業に使われる道具、機器、設備など**
E：**環境**(Environment) **照明や騒音、温度や湿度、作業空間の広さな どの作業環境にかかわる要素**
L：**周りの人たち**(Liveware) **その人に指示、命令をする上司や、作業を一緒に行う同僚な**
M,m:**マネジメント**(Management)**コミットメント、安全管理体制、リスクマネジメント**
P:**患者**(Patiant)
C:**コンピュータ**(Computer)



SHEL
Elwin Edwards(1972年）

ICAO SHEL
Frank H Hawkins(1975年）

M-SHELL
JIHF(1999年）

m-SHELL
河野龍太郎(2003年）

P-mSHEL
河野龍太郎(2002年）

C-SHEL
稲垣敏之(2003年）

†：**下記参考文献を基に発表者が手を加えて記述した。**
・**前田壮六：ヒューマンファクター2、メルマガ講座　ヒューマンファクター講座**（４）、http://jaem.la.coocan.jp/nhgk/ihgk0058008.pdf（**現在アクセス不可**）

参考：ASRS(航空安全報告システム)†

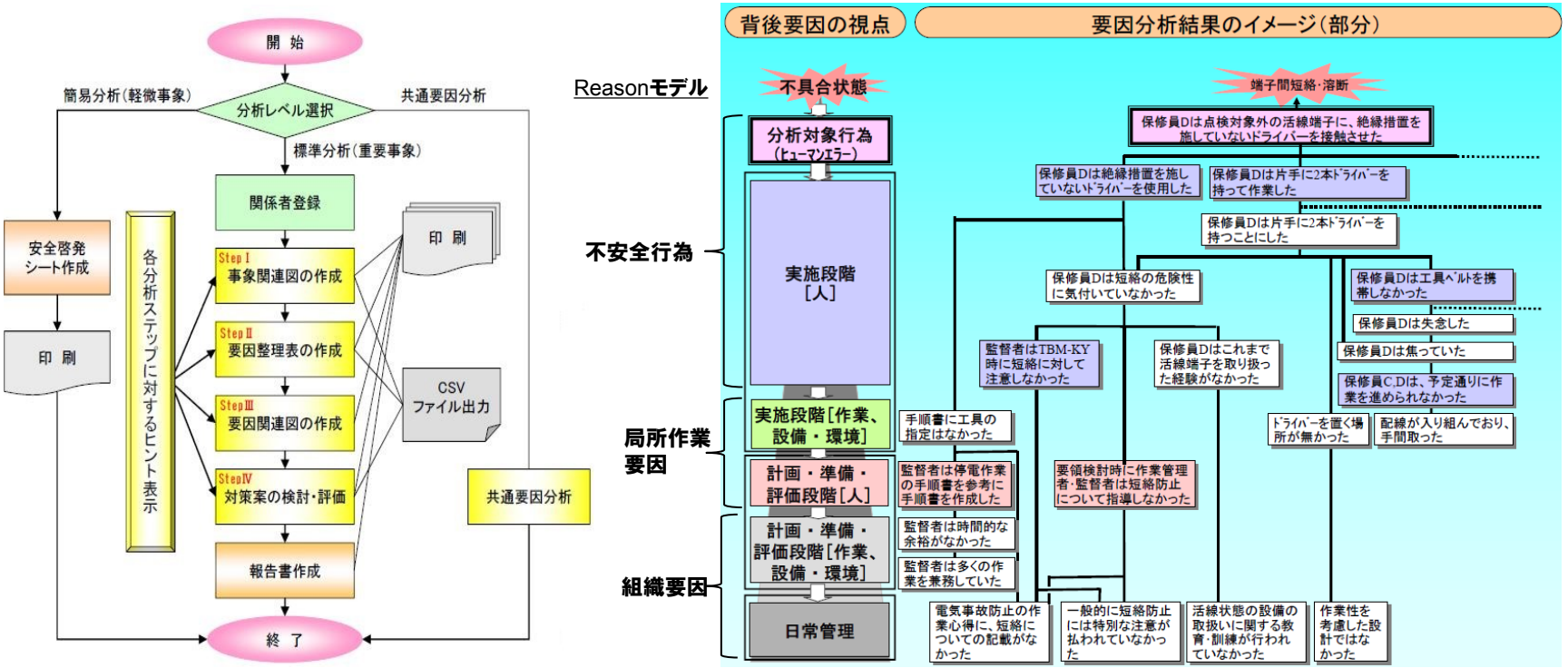
- Aviation Safety Reporting System
  - **制度概要**
    - 1976年設立。自発的なインシデント報告を収集、分析しフィードバックし、収集した情報は、①航空当局の是正、②航空政策立案、計画及び改善、③ヒューマンファクターの研究の基盤強化に用いられる
    - 運営主幹はNASA
  - **報告者**
    - 運航乗務員、整備士、客室乗務員、管制官　など
  - **報告対象**
    - 航空の安全を脅かす恐れがあると考えられた事象あるいは状況に関与したり、これを目撃したときの情報
  - **安全報告制度の具備すべき要件として、**
    - **免責性（報告者が処罰されないこと）**
    - **秘匿性（匿名性を堅持すること）**
    - **公平性（第三者機関が運用すること）**
    - **簡易性（手軽に報告できること）**
    - **貢献性（安全推進に貢献していること）**
    - **フィードバック（確実に役立っていることを本人に伝えること）（自己顕示欲、表現欲を充足させること）**

†：下記参考文献を基に発表者が手を加えて記述した。
・国土交通省：自発報告制度の各国制度比較表、http://www.mlit.go.jp/common/001031410.pdf
・日本財団：平成15年度 ヒューマンファクター概念に基づく海難・危険情報の調査活用等に関する調査研究　最終報告書、
http://nippon.zaidan.info/seikabutsu/2003/00988/contents/0016.htm

参考：HINT-HFC(J-HPES)†

Human Performance Incidents Analysis Tool ― Human Factors Research Center

- 1990年には、米国原子力発電協会(INPO)が開発したヒューマンファクタ分析・評価手法(HPES)を、HFCの研究成果を基に日本版として全面的に改良し、「J-HPES」を開発。
- 1993年には、パソコン用の「J-HPES分析支援システム」を開発、これがHINT-HFCの原型となった。
- HINT-HFCは、「ヒューマンエラーはエラーの当事者が持つ個人の要因にのみ依存するのではなく、人間の取り巻く要素との関係に着目すべき」というReason博士の概念を拡張した背後要因の枠組みを構築した。



HINT/J-HPESの概念図

†:下記参考文献を基に発表者が手を加えて記述した。

・財団法人電力中央研究所:HINT-HFC ヒューマンパフォーマンス事象分析支援ツール(2009), http://criepi.denken.or.jp/research/pamphlet/hint_hfc.pdf
・社会経済研究所ヒューマンファクター研究センター:ヒューマンファクター事象分析手法の研修・分析の支援、http://criepi.denken.or.jp/jp/hfc/seminar/date/pamphlet01.pdf