CIGS キヤノングローバル戦略研究所 The Canon Institute for Global Studies

第2回日本医療安全学会学術総会
2015年3月5日(土)～3月6日(日) 東京大学本郷キャンパス

# リスク評価
# - 定性リスク分析と定量リスク分析

氏田 博士
キヤノングローバル戦略研究所
環境安全学研究所

# 目　次

- 安全とリスク
- 安全設計と安全評価
- 事故モデルと人間特性

- 確率論的リスク評価(PRA, Probabilistic Risk Analysis)とは
- リスク情報活用

- 人間信頼性評価(HRA, Human Reliability Analysis)とは

# 「システム安全」の考え方

- システム思考「部分最適は全体最悪を生む」の認識

  過不足のないバランスの取れたシステムの設計と運用

- 安全目標「どこまで安全なら安全と言えるか？」

  “How safe is safe enough?”

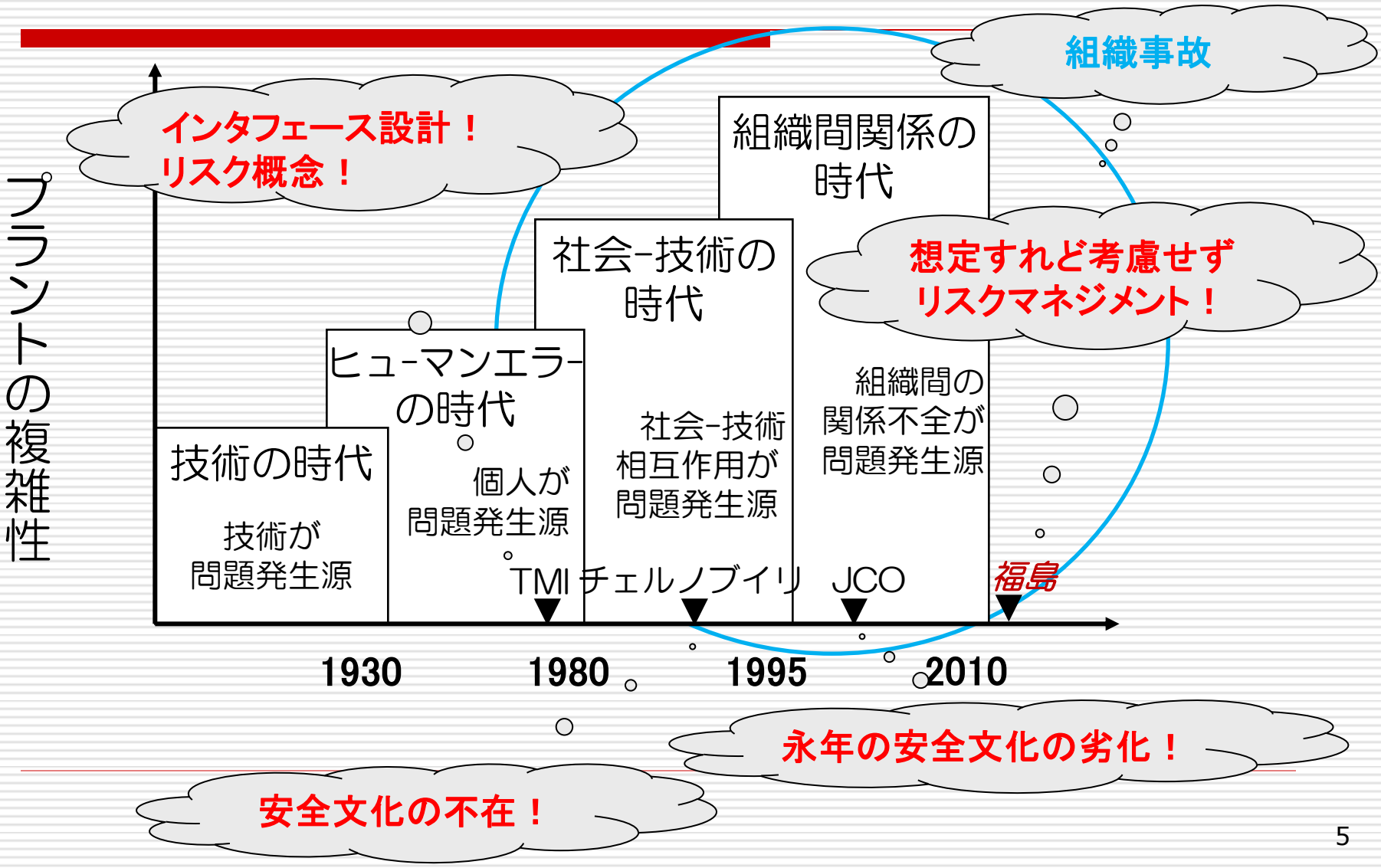
  - 確率論的リスク評価、PRA

- 技術システムの選択「有用感と安心」
  - リスクベネフィット解析
  - リスクコミュニケーション

# システム思考

1)　目的指向：トップダウン
　システム工学の最終目標は、目的を満足するシステムを実現すること
　そのための手段や形式は問わない
　システム的な思考法は必然的にTop Down的な形式をもつ
2)　多数の代替案を考慮：最適化
　ある目標を達成する手段は一つではなく、多数の代替案の中から、予め定められた評価基準に従って最適な案を選択
3)　システムの階層構造を考慮－上のレベルで同形性を探る：バーズアイ
　直面している問題を常に一段上のレベルから見る
4)　部分と全体との関係を重視－システム内の階層性で同形性を探る：分析力
　サブ問題やサブシステムを扱う時、常にシステム全体との相互関係を重視
　システム全体のバランスと同時に部分の果たす役割を積極的に考慮
5)　システムのライフサイクル全体に対する考慮
　システムが大規模であればあるほど、計画段階から交替を考慮
　計画→設計→製作→運用→廃棄のライフサイクル全体への考慮を重視
6)　学習と進化の考慮
　環境や状況の変化に適応できるように学習と進化を考慮

# ◘ 安全とリスク
## 安全問題のスコープの広がり（Reason, 1993）



# 安全思想（深層防護）の再構築 -スイスチーズモデル（Reason, J）

リスクマネジメント：
1.安全想定

危　険

津波対策

建物の
配置と設計

レジリエントシステム　！

電源供給の多様性
長期冷却システム
（動的・静的機器）

シビアアクシデント対策
（PCVベント）

可動式冷却装置、
ベントシステム、
水源の多様性

リスクマネジメント：
2.安全社会システム

苛酷事故
対策

電源対策

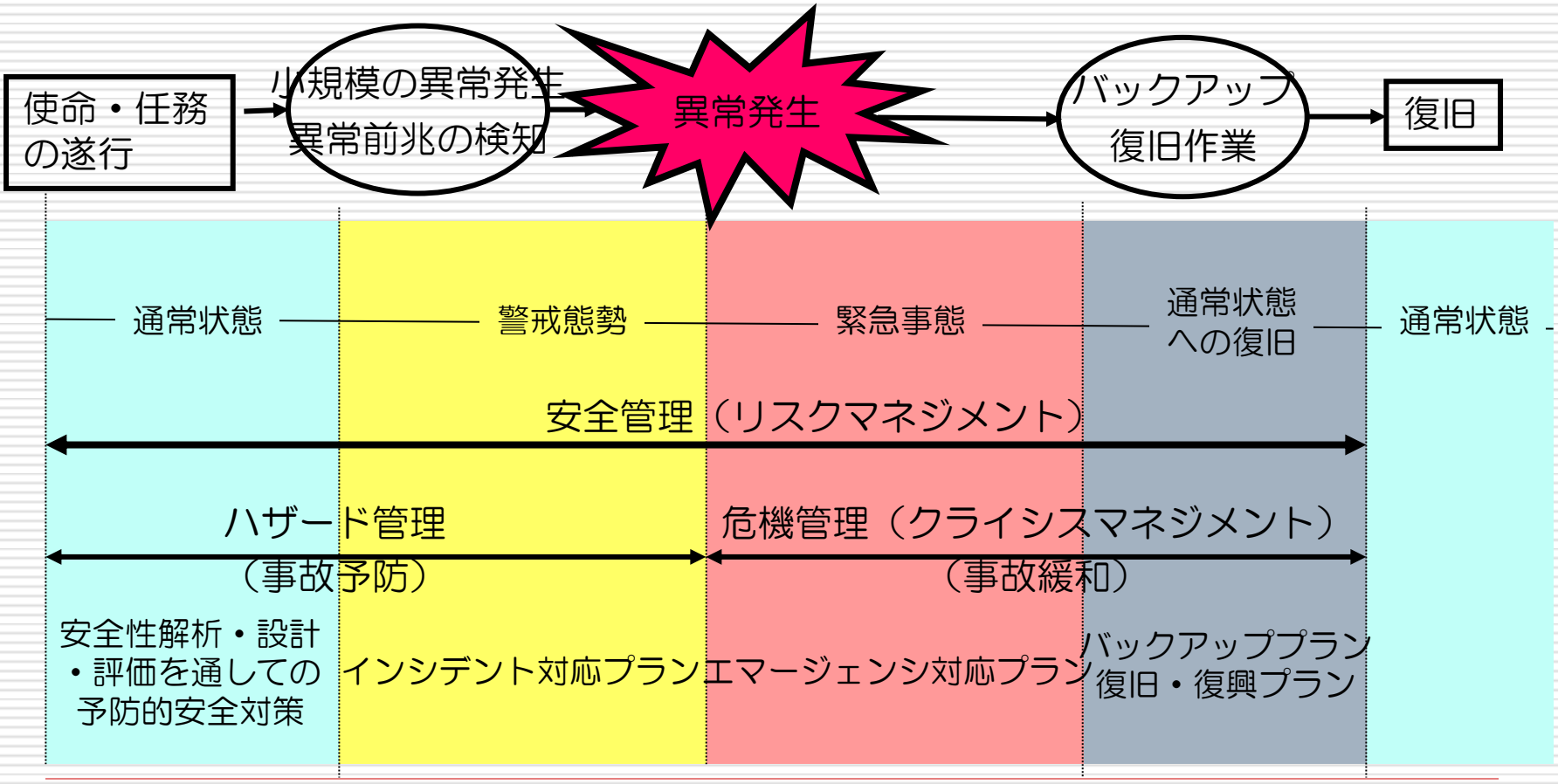
最終的な
ソフトバリア：
危機管理

事故

防　災

深層防護の誤謬−安全文化の劣化−組織事故の連鎖を断つ
3.安全設計（ハードバリア）の再構築
4.安全運用（ソフトバリア）の確立

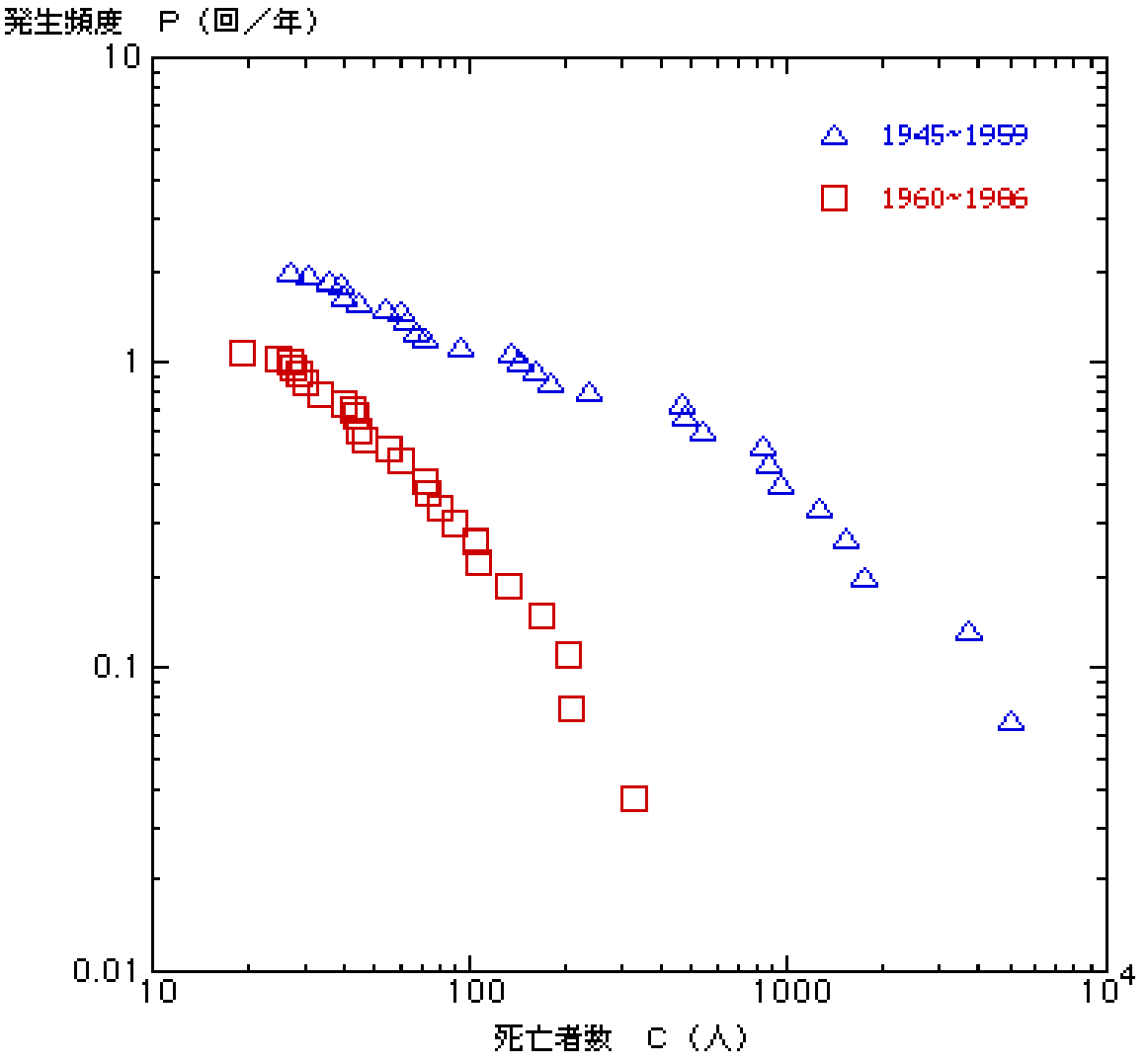
# リスクマネジメント - 事故の予防と防止



# 日本の台風災害リスクの時系列変化

## リスクカーブ

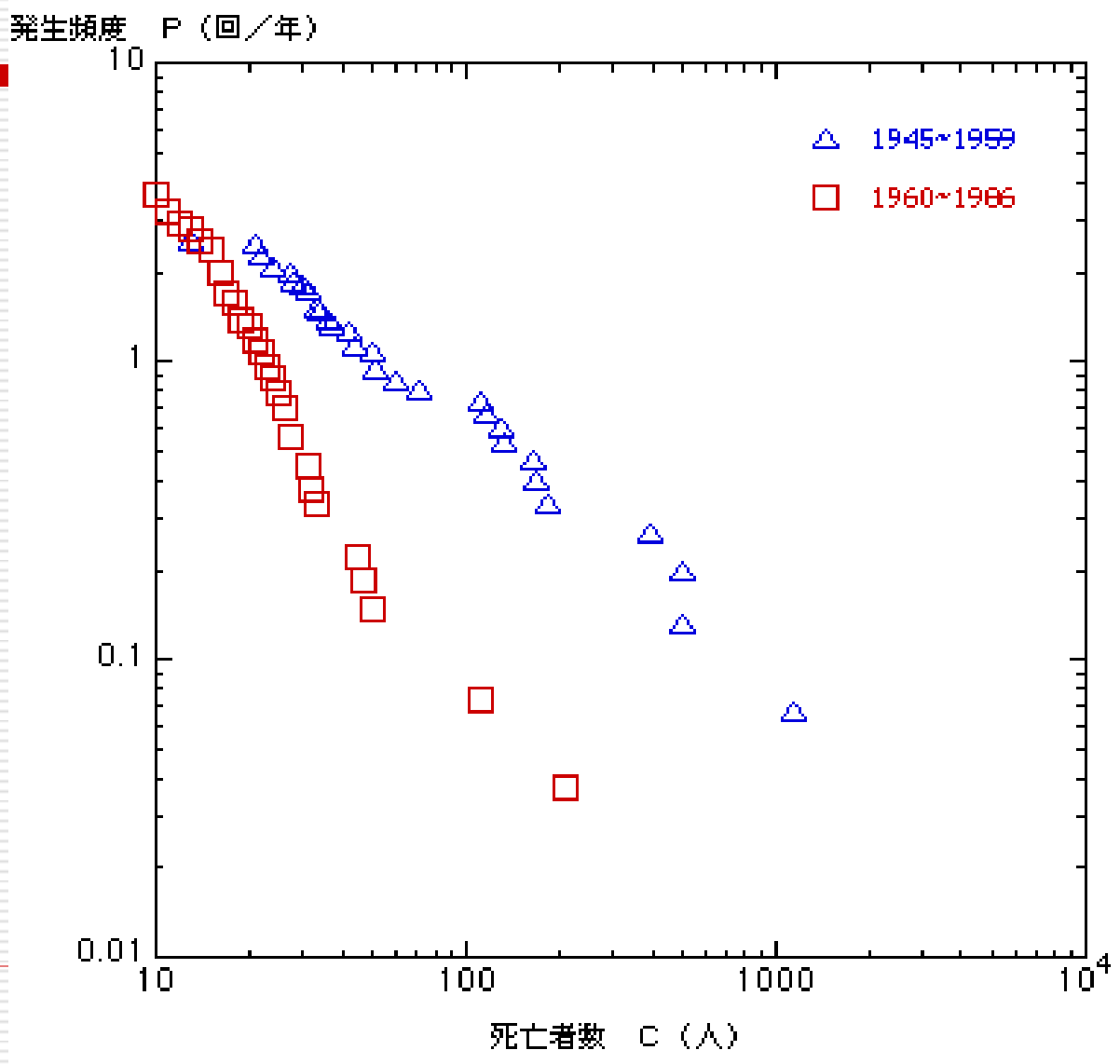
災害抑制
システム
（危機管理）




下岡　浩：第６回確率論的安全評価(PSA)に関する国内シンポジウム論文集（平成５年１月）

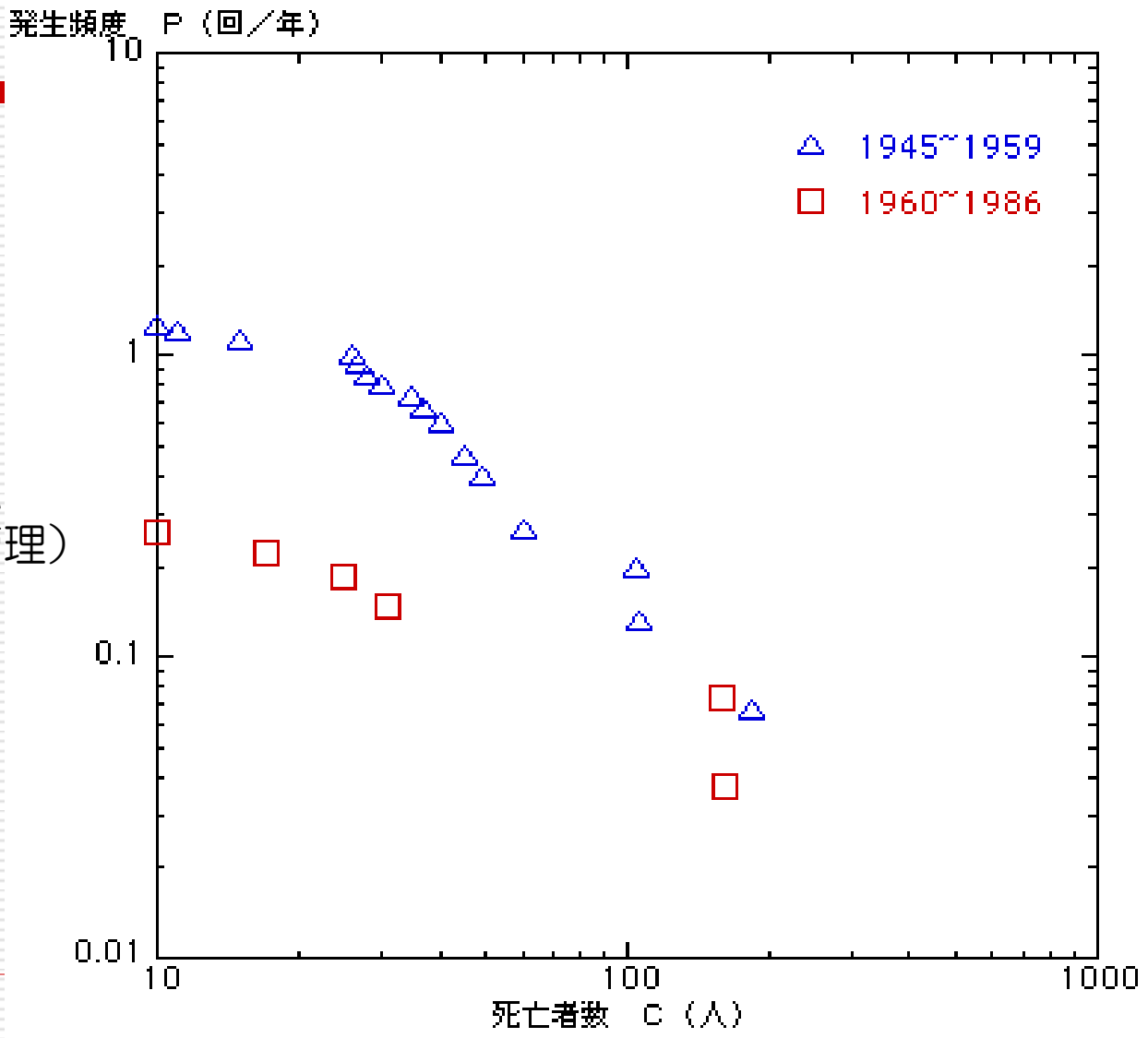
# 日本の船舶事故リスクの時系列変化

災害抑制
システム
（危機管理）



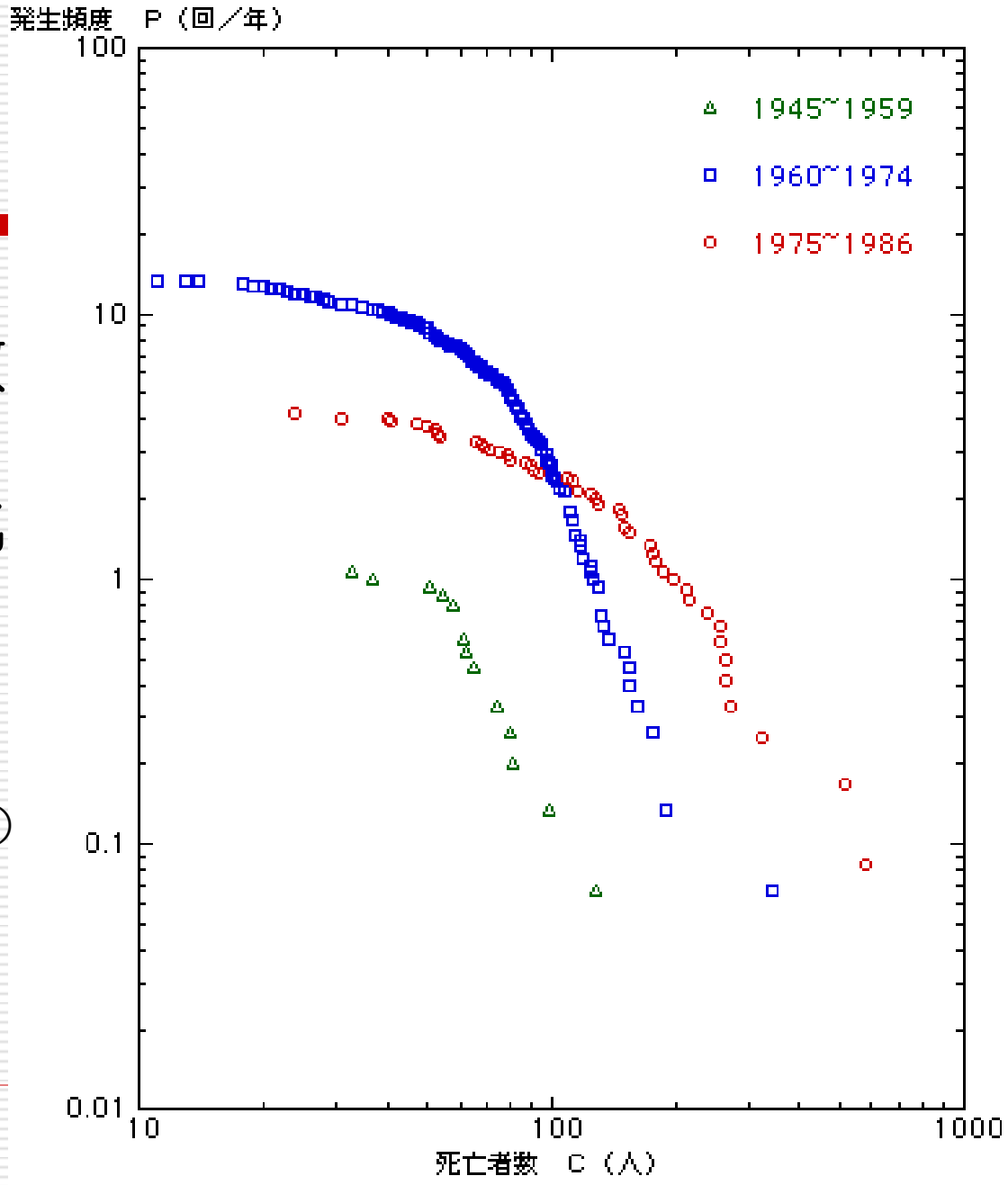
# 日本の鉄道事故リスクの時系列変化

安全
システム
（ハザード管理）



# 世界の航空機事故リスクの時系列変化

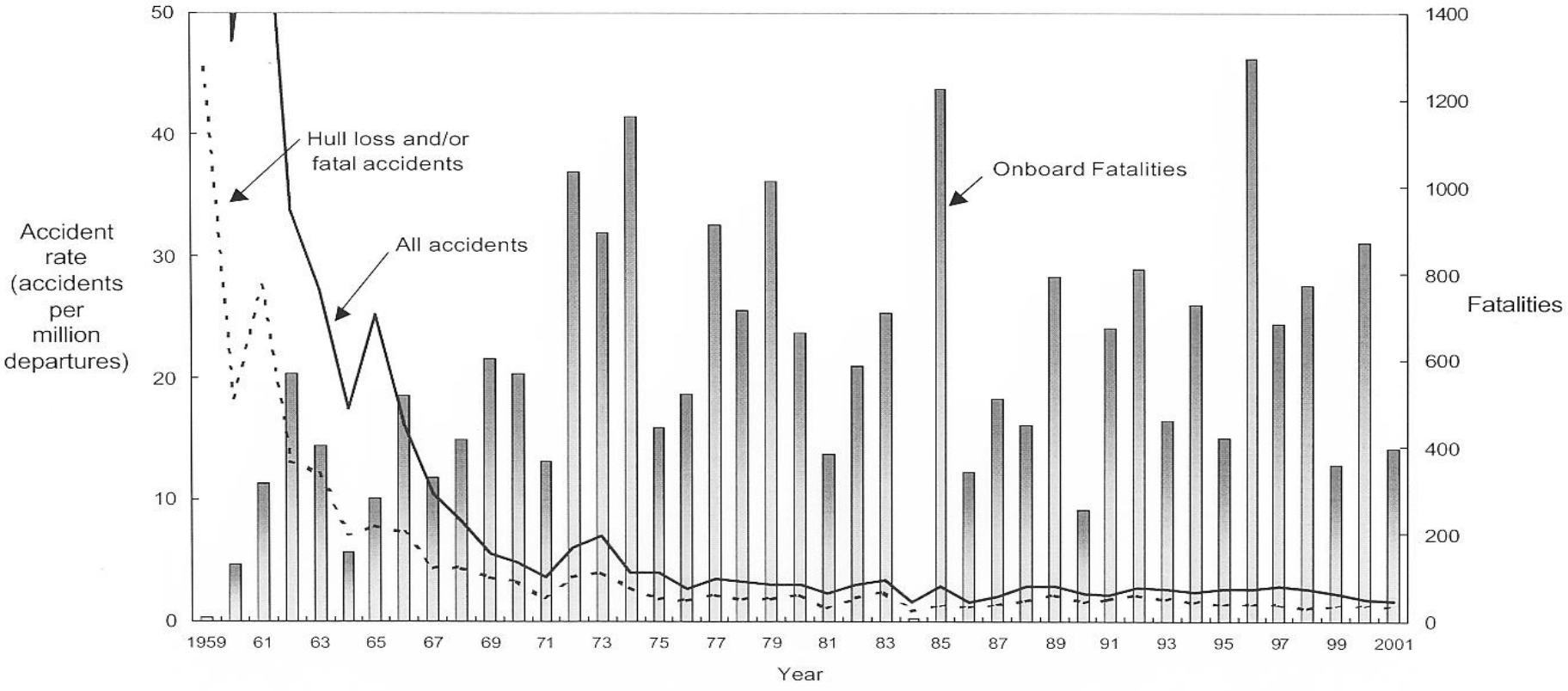
安全
システム
（ハザード管理）



# 商業航空機事故件数の変化

## Accident Rates and Fatalities by Year

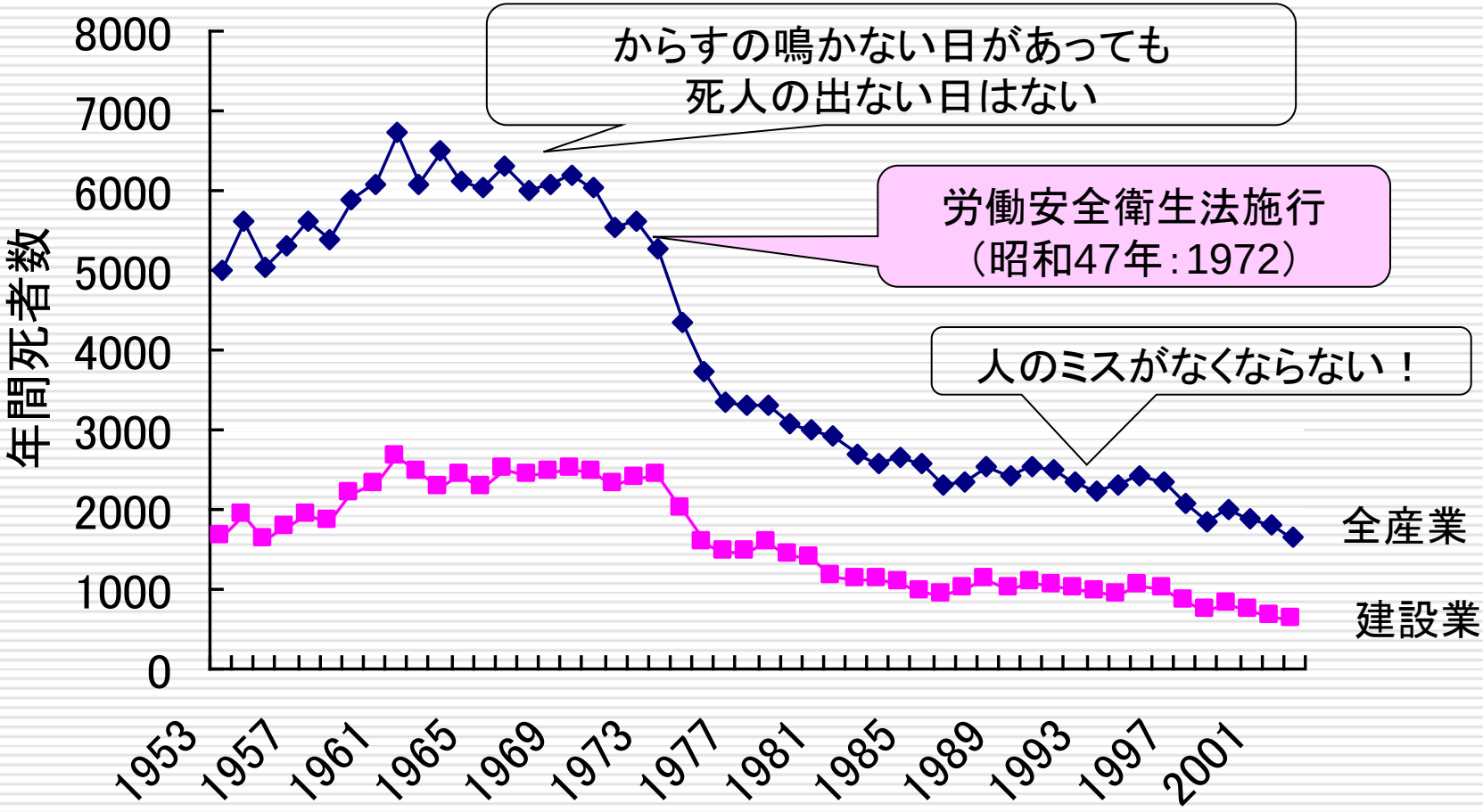
**All Accidents - Worldwide Commercial Jet Fleet - 1959 through 2001**




10

2001 STATISTICAL SUMMARY, JUNE 2002

# 労働災害【死亡数】の変化




資料出所：労働省「死亡災害報告」


休み
ここでひと休み

# ロ 安全設計と安全評価

## 安全設計のための深層防護(Defense-in-Depth) -セキュリティ対策も同様

- 最前線の故障の防止、拡大緩和、事故への波及防止に重点
- 環境への影響が大きいシステムほど後備系への配慮が増加

1. 故障の防止
2. 故障の拡大緩和：自己制御性、固有の安全性(本質安全)
3. 事故への波及防止：フェイルセイフ、フールプルーフ、冗長設計、多様性
4. 事故の拡大緩和
5. 環境への影響の緩和：避難

# システムの安全評価1

- 深層防護のバリアごとに安全評価する**確定論**的手法
  - 単一故障基準：考えられる初期事象を現象で分類しそのうちもっとも厳しい事象を代表として想定し（設計基準事故Design Basis Accident）、
  - それに加え安全に関わる機器のうちもっとも重要な機器の一つが故障すると想定し(単一故障基準Single Failure Criterion）、
  - それでも安全性が十分に確保できることをもって安全を担保できるものと評価

  - 単一故障基準Single Failure Criterionの破綻
  - LOCAは、現実的には起こらないだろう(NRC)
  - 設計と運用の乖離

# システムの安全評価2

- リスク概念に基づくシステム全体のバランスを評価する**確率論**的手法
  - 確率を考えるという過程に事象の網羅性が担保されやすい
  - 評価にリスクという基準が存在するため合理的な判断可能
    ー安全目標：どこまで安全対策をやれば十分かを定量的に議論
  - ライフサイクルを通して、時間的推移も考慮した安全性の判断可能
  - システム構築初期のハード的に実現した安全対策に加え、
  - 商用に入ってからの日常の実運用での安全確保も評価可能
    - 点検頻度、許容待機時間などの決定は、本来リスクベース
    - 化学プラント：定検期間延長；1年→2年→
  - 将来的な建設延長や計画変更に伴う経済的なリスクも大幅に低減
  - 事象発生時の社会的、経済的なリスクも低減
  - 不確定性の大きく予測の困難な事象も、専門家判断で定量化可能
    - 地震リスク評価、人間信頼性評価

# 安全のための方法論と手法

| | 確定論 | 両論併用 | 確率論 |
|---|---|---|---|
| 設計手法 | △ | ○ | × |
| 運用手法 | × | ○ | △ |
| 評価手法 | △ | ◎ | ○ |

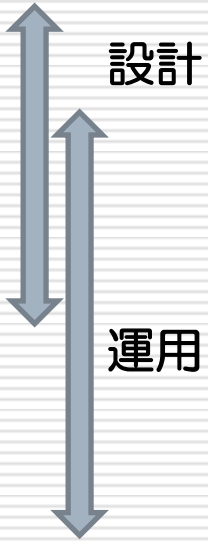
◎：有用、　○：可能、　△：支援、　×：不可


休み
ここでひと休み

# ◘ 事故・エラーのモデル

（氏田、2014.4）←　（Hollnagelの分類）

| 事故のモデル | エラーのモデル | 探索原理、分析方法 | 解析の目標、対策 |
|---|---|---|---|
| ドミノ<br>（故障の連鎖） | 機器故障と<br>ヒューマンエラー | 原因 - 結果　因果関係 | 原因と連鎖の排除 |
| スイスチーズ<br>（多様性の喪失） | システムエラー<br>（共通原因故障） | リスク分析<br>リスク評価 | 防護とバリアの維持 |
| 組織事故<br>（深層防護の誤謬） | 安全文化の劣化 | 行動科学<br>安全文化チェックリスト | 組織文化のモニタと<br>制御（組織学習） |



# エラーって何？

- 安全と品質保証と性能と経済性

- 刑法　　：ケア、　　性悪説、規範的人間像
- 人間工学：アテンション、性善説、もろい人間像？
  - To *err* is human, to forgive divine
- *認知科学：文脈の中での限定合理性に基づく判断と神の目から見た判断*
- *組織学：ハードから人間から組織へ、安全文化の課題*

- 標準(スタンダード：慣例・道徳)と基準(ルール：法・規制)
  - 社会の変化に応じて、規範も変化する

- 根本原因分析：未然防止-「安全とは、人間とは」の視点で！
- セキュリティ問題(悪意)の扱い？

# 組織(行動)経済学の3つのアプローチ

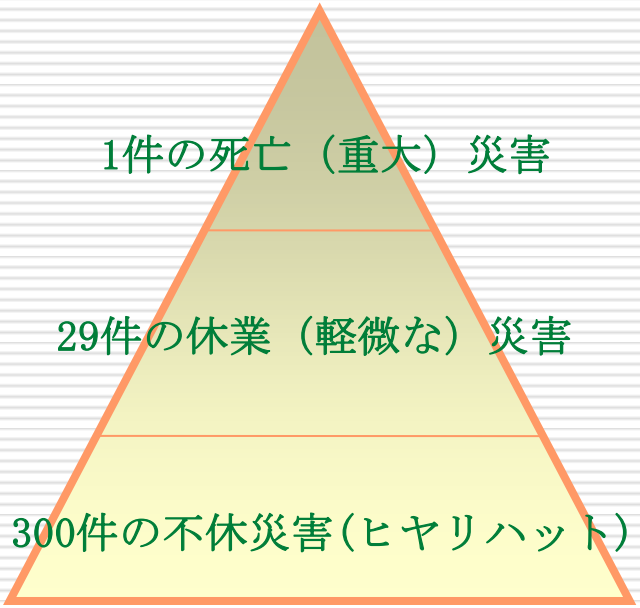
( 組織は合理的に失敗する: 菊澤研宗著　2009)

| | 取引コスト理論<br>(めんどくさがり) | エージェンシー理論<br>(情報格差) | 所有権理論<br>(わがまま) |
|---|---|---|---|
| 分析対象 | 取引関係 | エージェンシー関係<br>(プリンシパルとエージェンシー) | 所有関係 |
| 非効率性 | • 機会主義的行動<br>• 埋没コスト | • モラルハザード<br>• アドバースセレクション<br>(レモン市場) | 外部性 |
| 制度解決 | 取引コスト節約制度<br>(仲間–集権型–分権型組織) | エージェンシーコスト削減<br>(情報の対象化)制度 | 外部性の内部化(所有権配分)制度 |
| 事例 | • ガダルカナル白兵突撃<br>• ワンマン経営–社外監視<br>• *硫黄島・沖縄戦(良好事例)* | • インパール作戦<br>• ワークシェアリング | • ジャワ軍政<br>• 仲間意識と組織的隠蔽 |

共通の仮定:限定合理性と効用極大化

# 組織分析の新しい考え方

「Heinrichの法則」：労働災害の分野




- レジリエンス工学
  - 事故の予防に役立つ良好事例や
    事故の悪化を防止した行為などの
    組織の良い点を更に強化
    ＝ヒヤリハットの精神そのもの！
  - 緊急時の柔軟な組織対応
    ＝リスクマネジメントそのもの！
    ＝高信頼性組織HROも同様の発想！
    ＝リスクリテラシーも同様の発想！

まとめると、

- 柔軟な組織作り
  - レジリエンス工学：良好事例に学ぶ；事例分析
  - 高信頼性組織：良好組織の実態に学ぶ；エスノメソドロジー
  - リスクリテラシー：組織のリスク対応事例に学ぶ；事例分析

# 目　次

- 安全とリスク
- 安全設計と安全評価
- 事故モデルと人間特性

- 確率論的リスク評価(PRA, Probabilistic Risk Analysis)とは
- リスク情報活用

- 人間信頼性評価(HRA, Human Reliability Analysis)とは

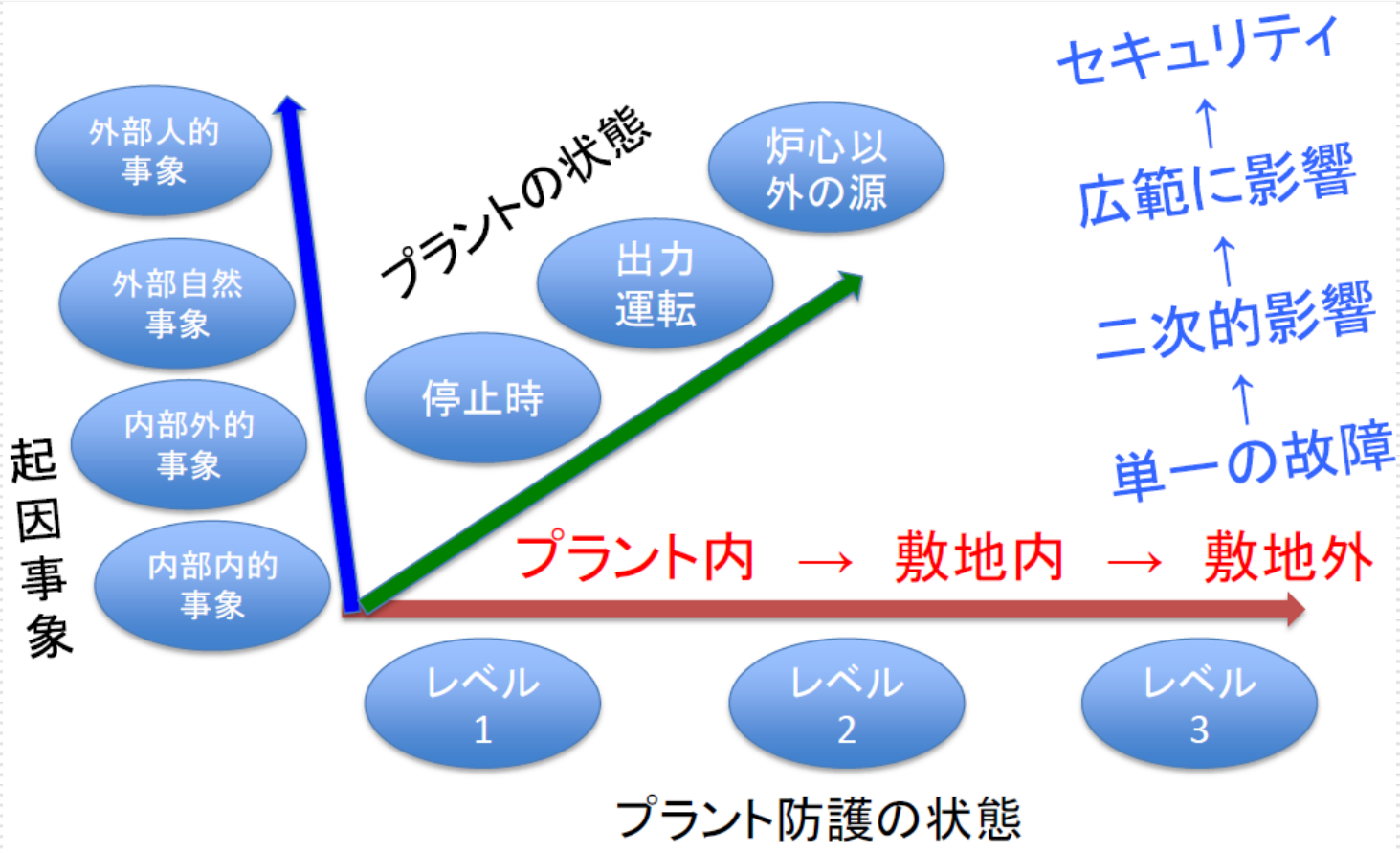
# QRA(定量的リスク解析)

- Tolerability of risk from nuclear power stations, HSE(Health & Safety Executive) publication, ISBN 011 836368 1
- 電気･電子･プログラマブル電子安全関連系の機能安全、JIS C 0508
- 安全度水準決定方法、JIS C 0508-5

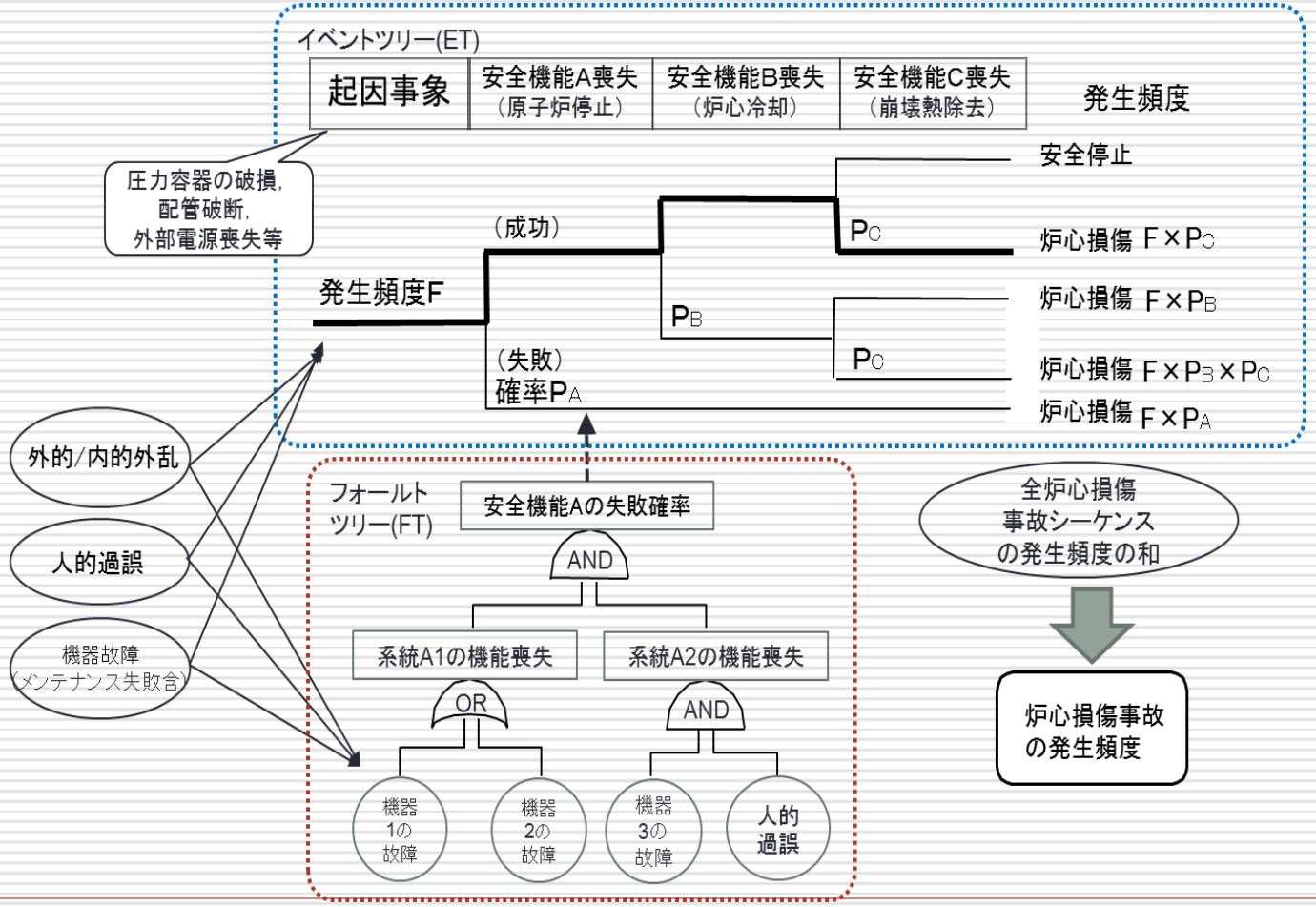
- Ⅰ：許容できないリスク
- Ⅱ：好ましくないリスク（リスク軽減が非現実的なときに許容）
- Ⅲ：リスク軽減費用が改善効果を超えるときに許容
- Ⅳ:無視できるリスク

| 結果 / 頻度 | 破局的 | 重大 | 軽微 | 無視可能 |
|---|---|---|---|---|
| 頻繁 | I | I | I | II |
| かなり | I | I | II | III |
| たまに | I | II | III | III |
| あまり | II | III | III | IV |
| 起こりそうにない | III | III | IV | IV |
| 信じられない | IV | IV | IV | IV |

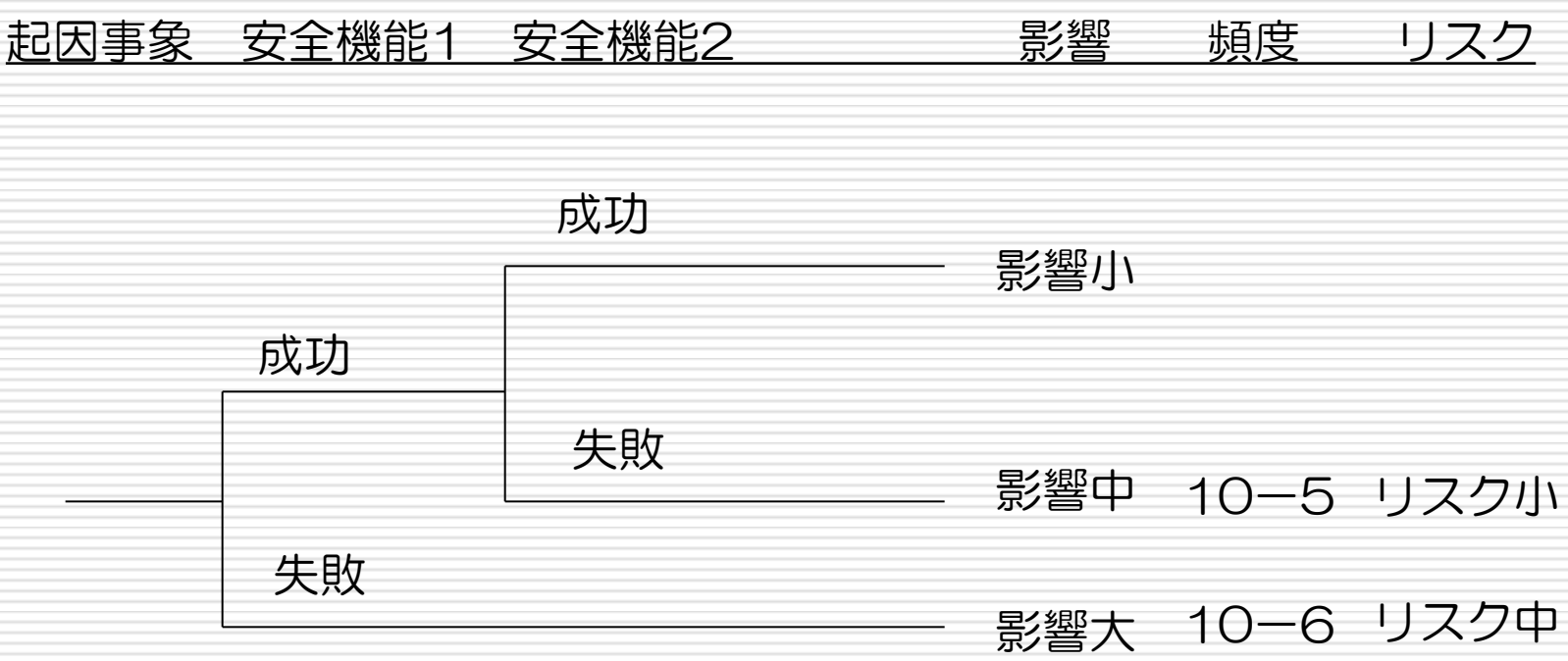
# リスク評価のスコープ


外部人的事象
外部自然事象
内部外的事象
内部内的事象
起因事象
プラントの状態
炉心以外の源
出力運転
停止時
セキュリティ
広範に影響
二次的影響
単一の故障
プラント内 → 敷地内 → 敷地外
レベル1
レベル2
レベル3
プラント防護の状態

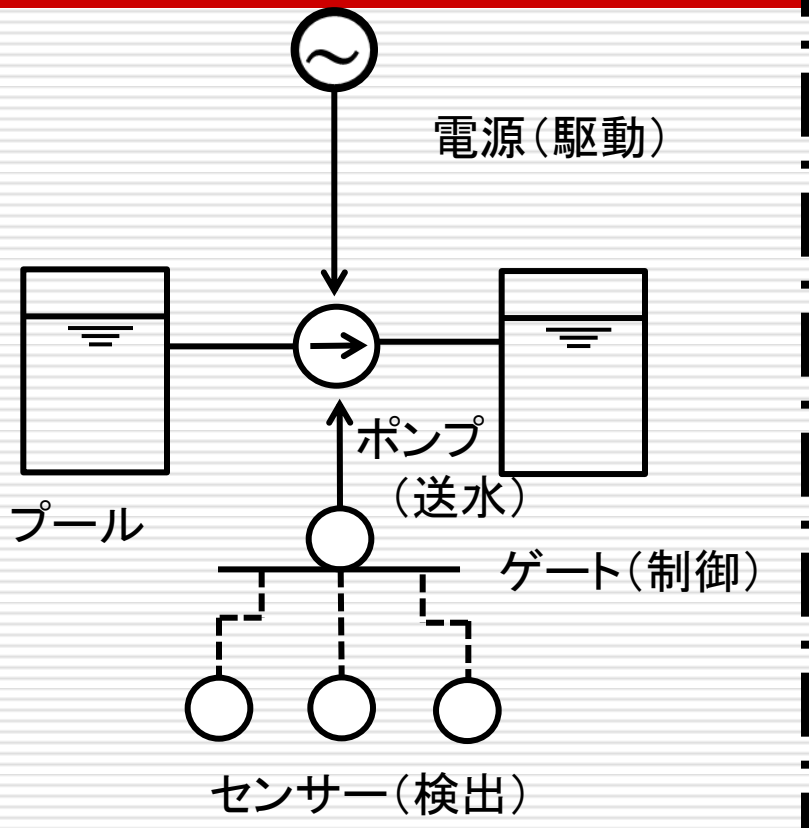
# レベル1PRA


イベントツリー(ET)
起因事象
安全機能A喪失
（原子炉停止）
安全機能B喪失
（炉心冷却）
安全機能C喪失
（崩壊熱除去）
発生頻度
圧力容器の破損，
配管破断，
外部電源喪失等
安全停止
（成功）
PC
炉心損傷 F×PC
発生頻度F
PB
炉心損傷 F×PB
（失敗）
確率PA
PC
炉心損傷 F×PB×PC
炉心損傷 F×PA
外的/内的外乱
人的過誤
機器故障
（メンテナンス失敗含）
フォールト
ツリー(FT)
安全機能Aの失敗確率
AND
系統A1の機能喪失
系統A2の機能喪失
OR
AND
機器
1の
故障
機器
2の
故障
機器
3の
故障
人的
過誤
全炉心損傷
事故シーケンス
の発生頻度の和
炉心損傷事故
の発生頻度

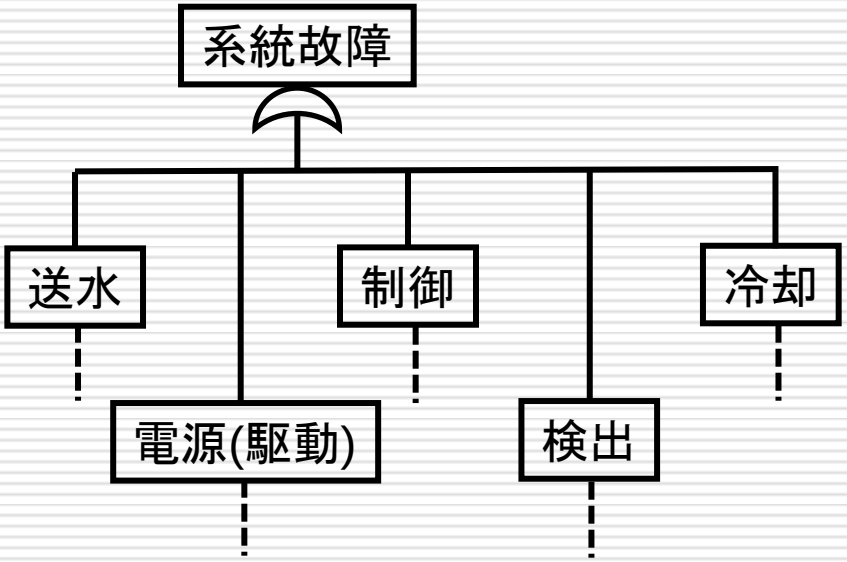
# イベントツリーの作成と評価（深層防護のレベル）



# フォルトツリー作成-階層１：機能の分類

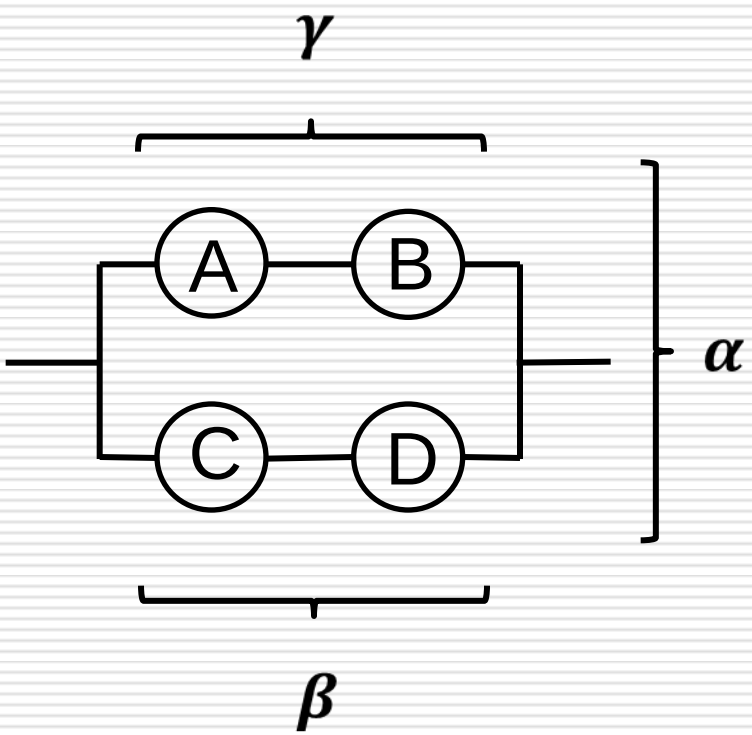



系統構成

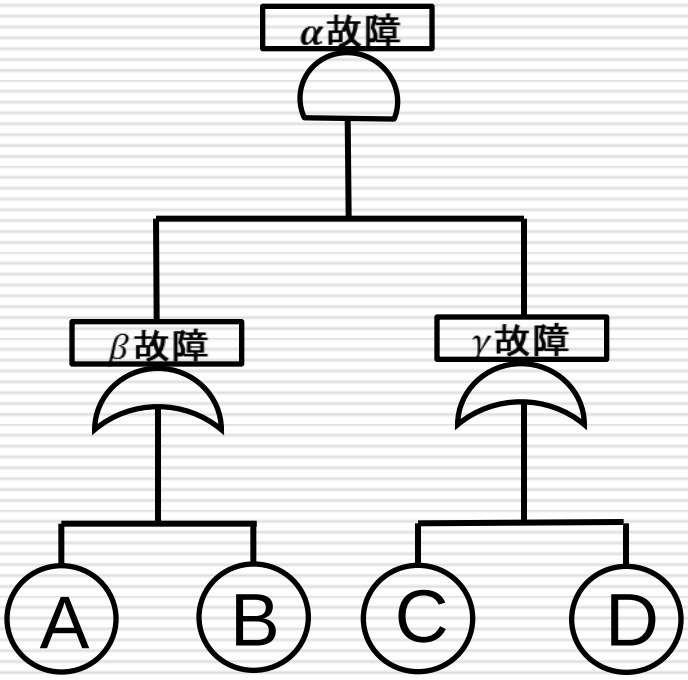



フォールトツリー

# フォルトツリー作成-階層２：機器の構成（ブロック分割）




系統構成（系並列）



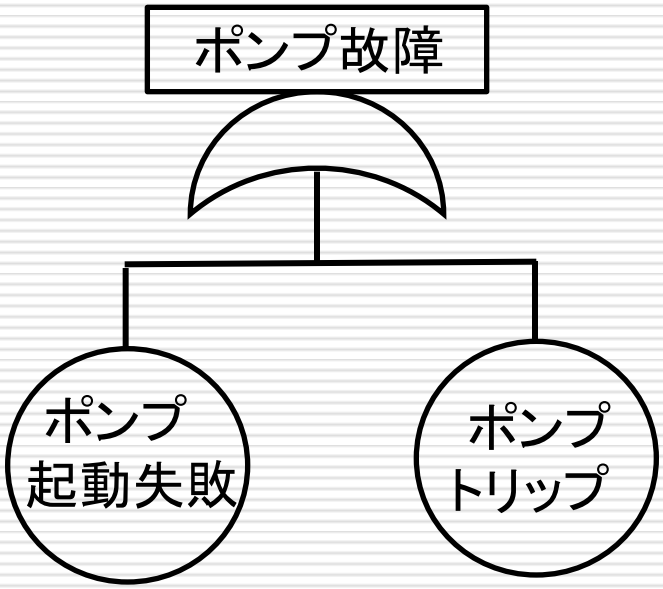

フォールトツリー

# フォルトツリー作成-階層３：運転（故障）モード

機器：ポンプ

運転モード：起動及び
運転継続要求

運転モード



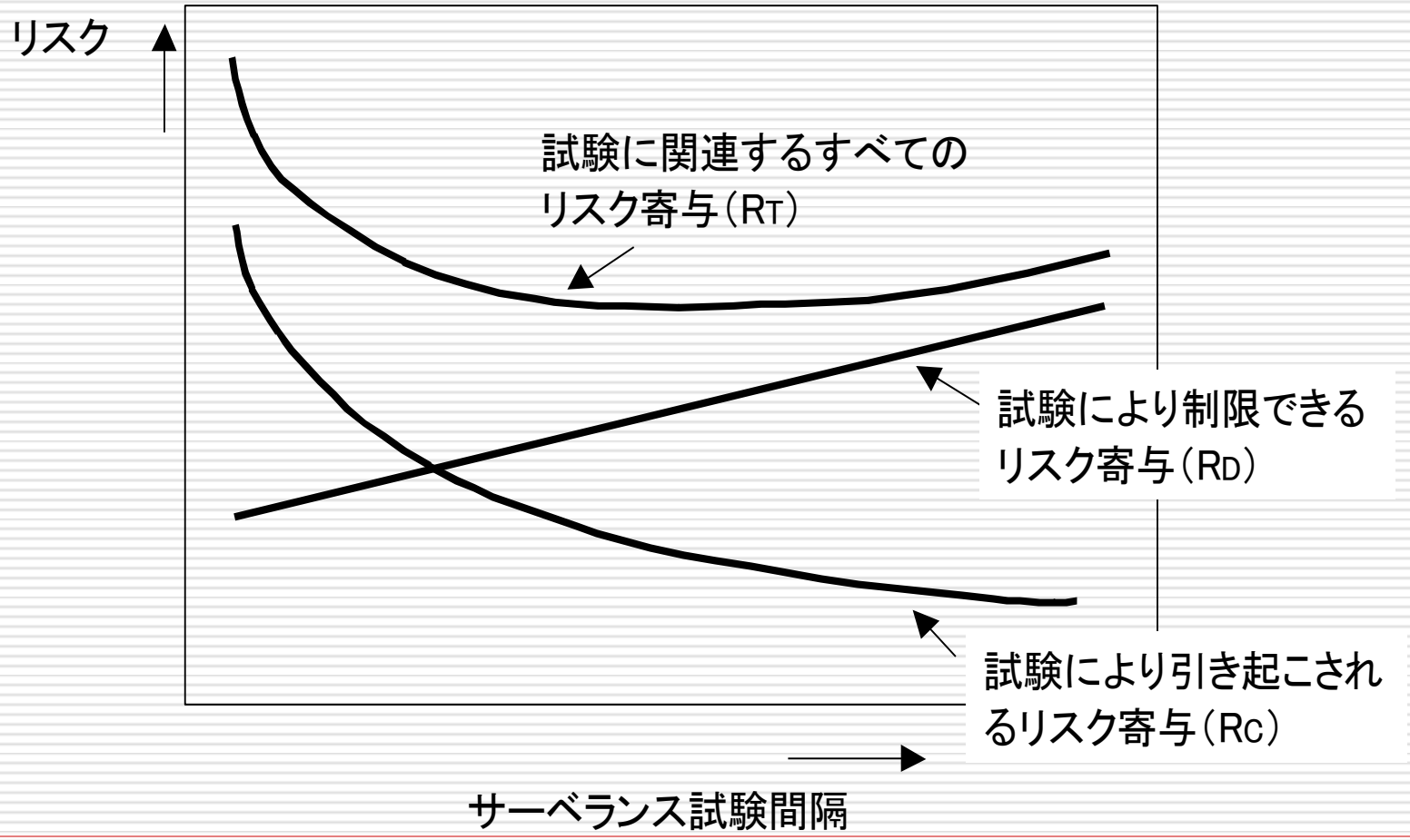

フォールトツリー


休み
ここでひと休み

# リスク情報の活用分野例

| 利用分野 | 利用方法 | PSAの役割 |
|---|---|---|
| AM等によるリスク低減策の検討 | 安全上重要な事故シーケンス、機器、運転操作、従属性等を同定し、リスク低減策検討の参考とする | 設計や手順、規制等の永続的な変化の安全への影響を評価 |
| 規制行為の価値／影響解析 | NRCにおいて、規制行為を追加（削除）することの正当性を、リスク低減の価値と負担増加の影響をドル換算で評価して、検討している | |
| サーベランス試験評価 | 試験頻度を変えて、炉心損傷への影響を評価し、最適化を図る | |
| 許容待機除外期間評価 | 待機状態の機器の故障が発見されたとき、プラントの運転継続の許される時間がテックスペックに定められている<br>許容待機時間の一時的変更の炉心損傷頻度への影響を評価し、安全上許容できるかの判断に用いる | 短期間の変化の安全への影響を評価 |
| コンフィギュレーション管理 | サーベランス試験、故障機器の検査、補修等のための安全設備の構成状態（コンフィギュレーション）の変化を考慮して炉心損傷頻度を評価し、安全上許容できるか否かの判断に用いる | |
| メンテナンスルール | NRCのメンテナンスルールでは、安全に関連する機器の性能を監視することが要求されており、安全上重要な機器の選定にPRAによる重要度指標を用いる | 機器や設備の信頼性の安全への影響を評価 |
| 等級別品質保証 | 品質保証のレベルを安全上の重要度に応じて定める | |
| 検査計画 | 供用期間中検査の計画を安全上の重要度に応じて定める | |

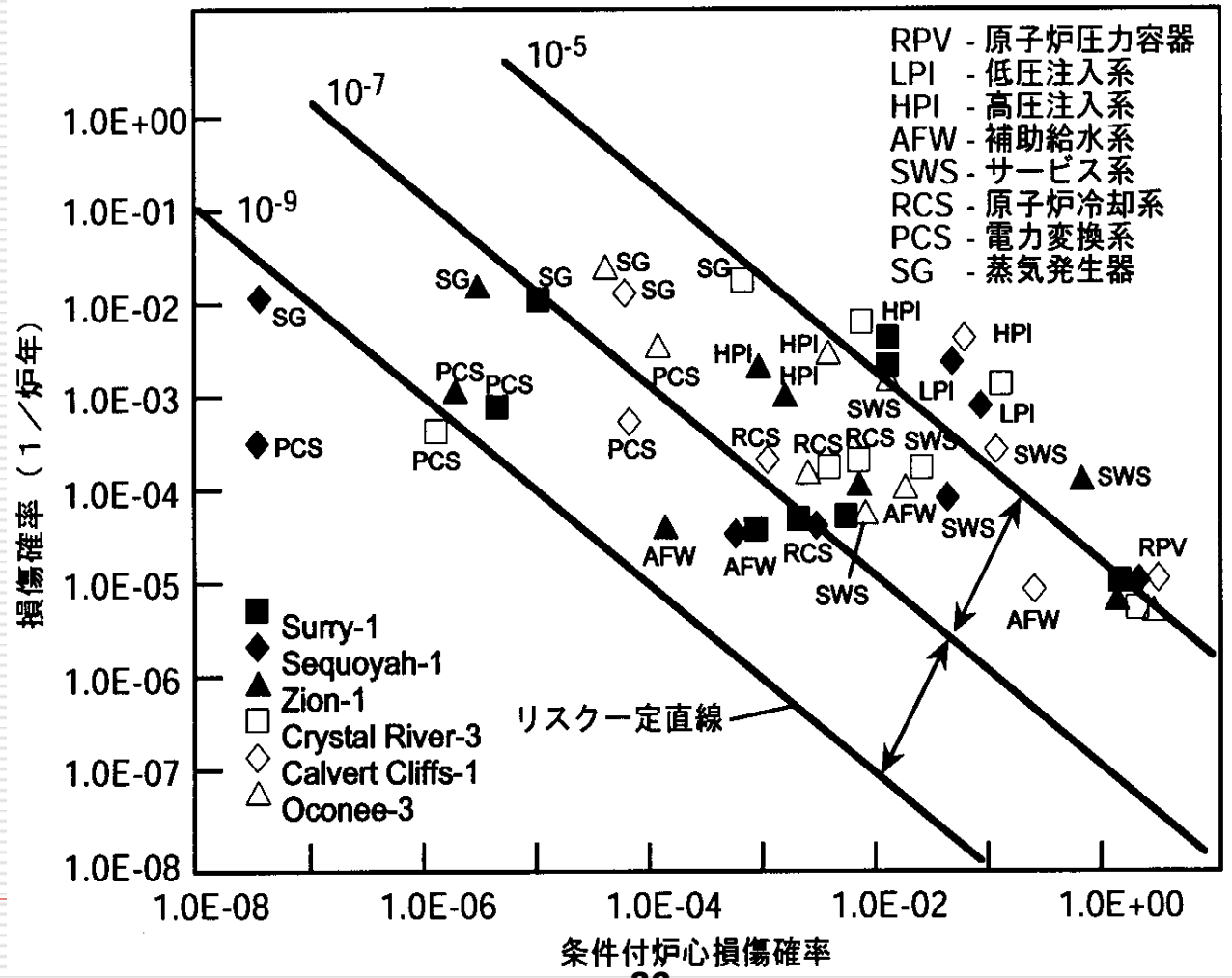
# サーベランス試験の間隔とリスク寄与



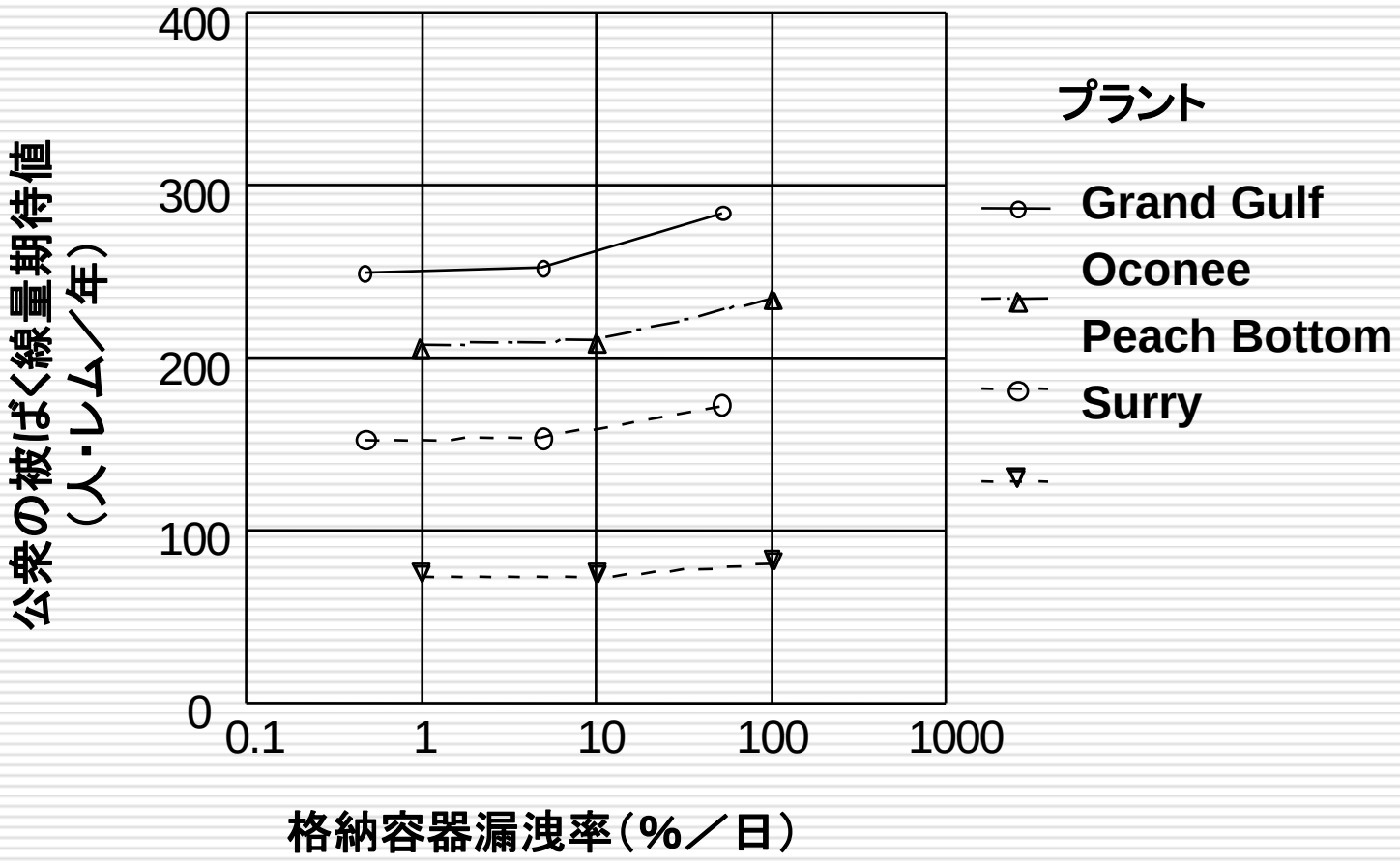
# リスクベースの供用期間中検査の採用によるメリット

| 系統 | 要素数 | 現行ASME Section-XI 検査要求箇所 | リスクベース評価により | |
|---|---|---|---|---|
| | | | 検査要求箇所 | 被ばく量（従来比） |
| 原子炉冷却系 | 890 | 161 | 16 | 1／15 |
| 低圧注入系 | 644 | 32 | 20 | 2／3 |

# PWR発電所の主要な機器・系統の破断によるリスク(炉心損傷頻度)への寄与の評価



# 格納容器漏洩に対するリスクの感受性



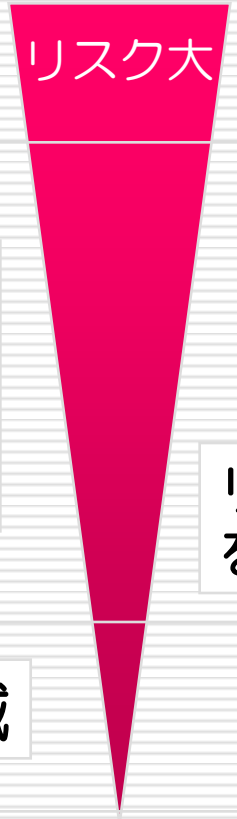
# リスク情報の活用
## パフォーマンス・ベースト（性能ベース）
## リスクインフォームド規制の例

原子炉格納容器漏洩率試験の改定案
（10 CFR 50, Appendix J）

NUREG-1493で漏洩率試験間隔等の変更についてリスクの観点から技術的に検討

- 総合漏洩率試験（タイプA）
  - 現行10年に３回　→10年に１回
  - （前２回の試験で性能を満足する場合に限る）
- 局所漏洩率試験（タイプB,C）
  - 各機器の性能に基づく
  - 現行２年に１回　→　最長10年に１回（タイプB）
    最長５年に１回（タイプC）

# 英国の安全目標の基本的考え方




受容されない領域

リスクは正当とされない

安全限度

リスク低減が不可能か、費用が改善に見合わない場合のみ、我慢する

コスト
ベネフィット
解析

我慢できる領域
ALARP領域
(合理的に達成可能な限り低くする努力)

リスク低減の費用が、改善を上回る場合我慢できる

安全目標

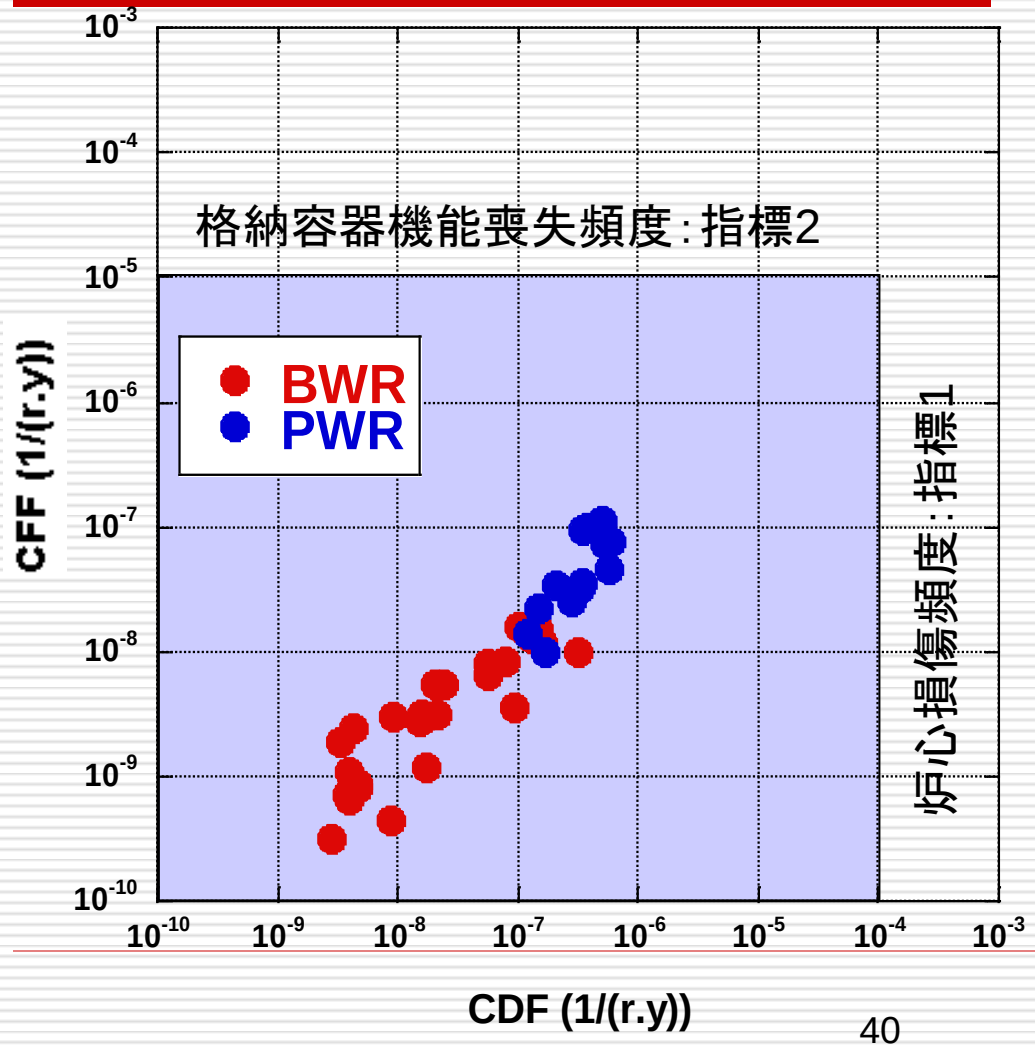
広く受容される領域

リスクがこのレベルに維持されていることを保障し続けるべき

リスク
ベネフィット
解析

無視できるリスク

# 日本の既設52基の炉心損傷頻度及び格納容器機能喪失頻度




- 既設52基の「出力運転時の内的事象」のPSAの結果（2004年）は，性能目標の値を十分に下回っている
- 条件付死亡確率を仮に1にしても，安全目標を満たすことが分る

原子力安全・保安院，「軽水型原子力発電所における「アクシデントマネジメント整備後確率論的安全評価」に関する評価報告書」（平成16年10月）

# 目　次

- 安全とリスク
- 安全設計と安全評価
- 事故モデルと人間特性

- 確率論的リスク評価(PRA, Probabilistic Risk Analysis)とは
- リスク情報活用

- 人間信頼性評価(HRA, Human Reliability Analysis)とは

# □人間信頼性解析（HRA: Human Reliability Analysis ）とは-必要性

- 安全評価で人間の信頼性を評価することは不可欠
  - □ 完全な自動化システムは存在しない
    - 設計時にエラーの組み込み
    - 同一システムでも運用で信頼性は異なる
    - 機械の故障をバックアップするのは人間
    - 想定外事象におけるシステムの安全性は人間の信頼性に依存
- 適切なHRAなしには適切な確率論的リスク評価(PRA)はありえない、と言っても過言ではない
- リスク評価の一手法であるHRAは、プラント全体の挙動を人間との関係を見ながら評価するので、プラントの総合的なシステム設計にも必須の手法

# 人間信頼性解析–続き (HRA: Human Reliability Analysis )

- ある状況において人間が取るべき行動から逸脱する確率を評価

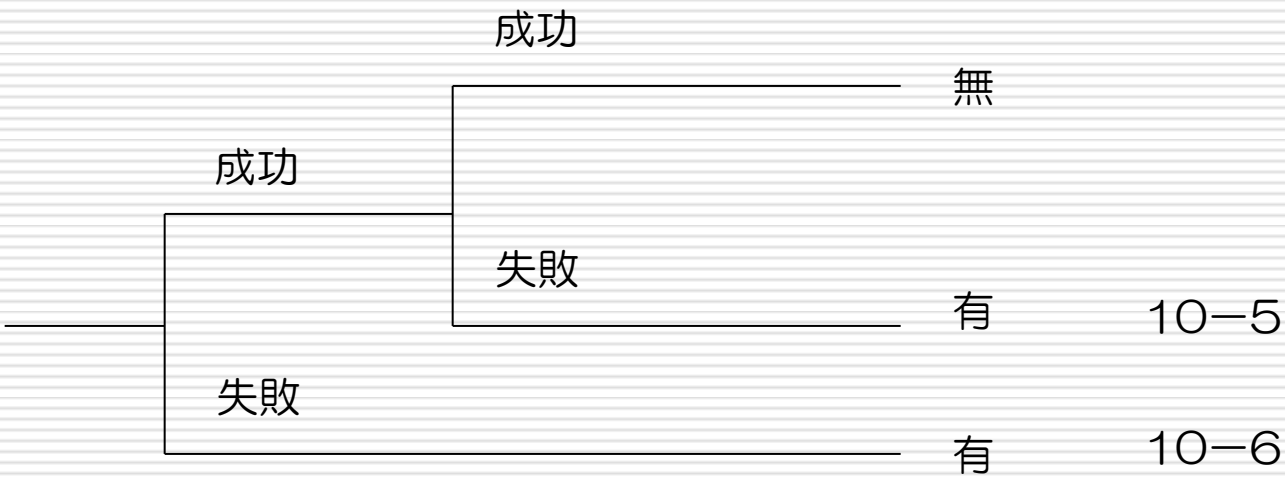
- 緊急時に期待される対応(主にETの分岐)
  - 時間に強く依存
  - *OAT(Operator Action Tree)*
  - TRC (Time Reliability Correlation)
  - HCR(Human Cognitive Reliability correlation)

- 通常時の操作(主にFTの一部)
  - 操作ステップの組み合わせ
  - リカバリも評価
  - *THERP(Technique for Human Error Rate Prediction)*
  - SLIM-MAUD(Success Likelihood Index Methodology - Multi-Attribute Utility Decomposition)

# 人間信頼性評価（HRA1）

緊急時に期待される対応(主にETの分岐)ー時間に強く依存

*OAT(Operator Action Tree)*



# 診断エラー確率

| 診断余裕時間（分） | ヒューマンエラー率（HEP） |
|---|---|
| <2 | 1.0 |
| 2<= <5 | 0.5 |
| 5<= <10 | 0.2 |
| 10<= <20 | 0.1 |
| 20<= <30 | 0.01 |
| 30<= <40 | 0.001 |
| 40<= <50 | 0.004 |
| 50<= <60 | 0.002 |
| 60分以上 | 0.0001 |

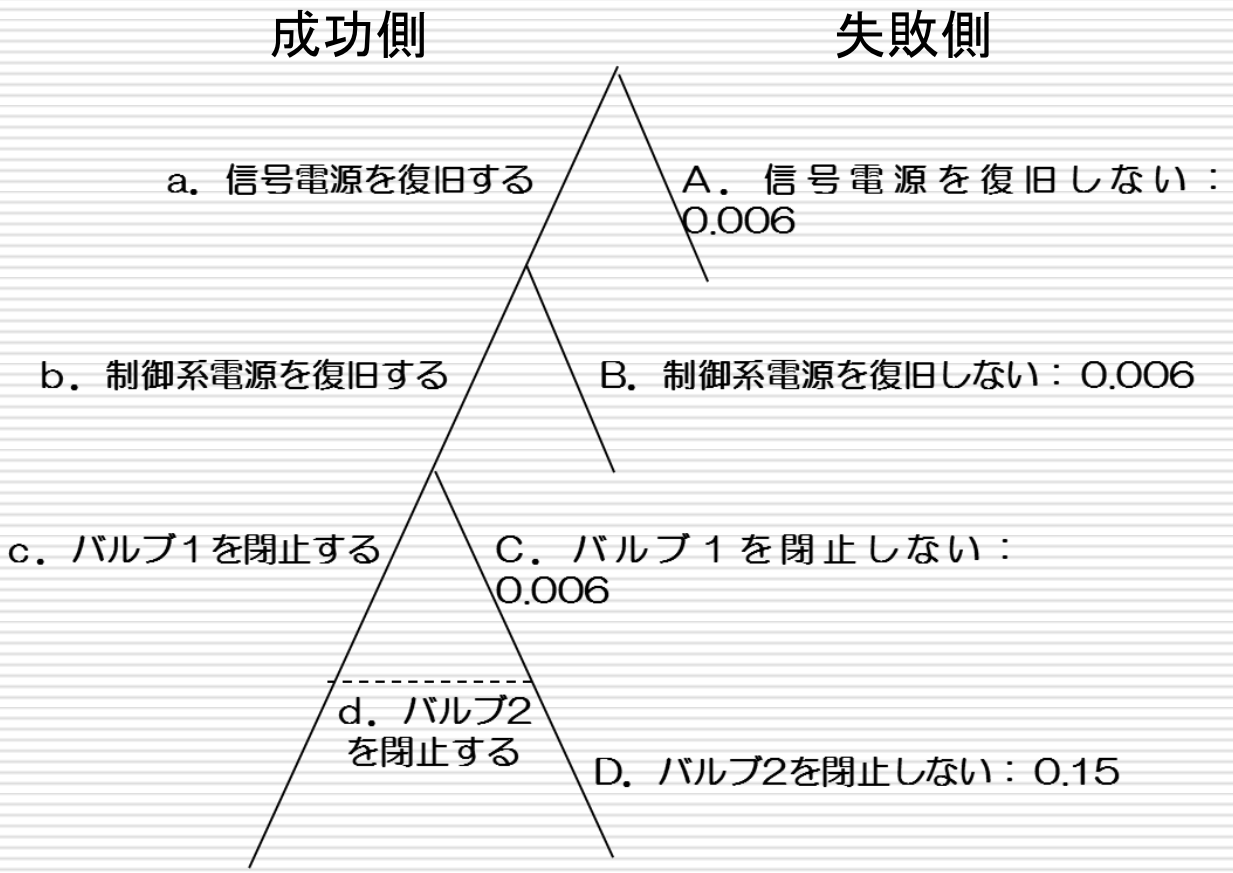
# 操作エラー確率

| 操作内容、場所 | 操作に要する時間(分) | ヒューマンエラー率(HEP) |
|---|---|---|
| 単純、制御室内 | 5 | 0.0001 |
| 複雑、制御室内 | 10 | 0.001 |
| 単純、現場 | 20 | 0.005 |
| 複雑、現場 | 30分以上 | 0.01 |

# THERP手法-手順１

- 解析の背景、前提の確認
- ↓
- 現地調査、状況聞き取り
- ↓
- タスク分析
- ↓
- HRAイベントツリー作成
- ↓
- 標準的ヒューマンエラー確率（Nominal HEP)評価
- ↓

# HRA-Event Tree
## ー操作イベントツリーの作成




現実的な意味を持たない枝を刈り込む

# THERP手法-手順２

- PSFの影響考慮
- ↓
- 基本ヒューマンエラー確率(Basic HEP)評価
- ↓
- 従属性の影響評価
- ↓
- ヒューマンエラー確率(HEP)評価
- ↓
- タスク全体の成功／失敗確率評価
- ↓
- リカバリー効果の補正
- ↓
- 結果の要約、知見の文書化

# PSFに関する修正

具体的指針に基づき修正

例:照明が暗い場合には計器読みとりの失敗確率の標準値の修正

ストレスレベルによる修正係数

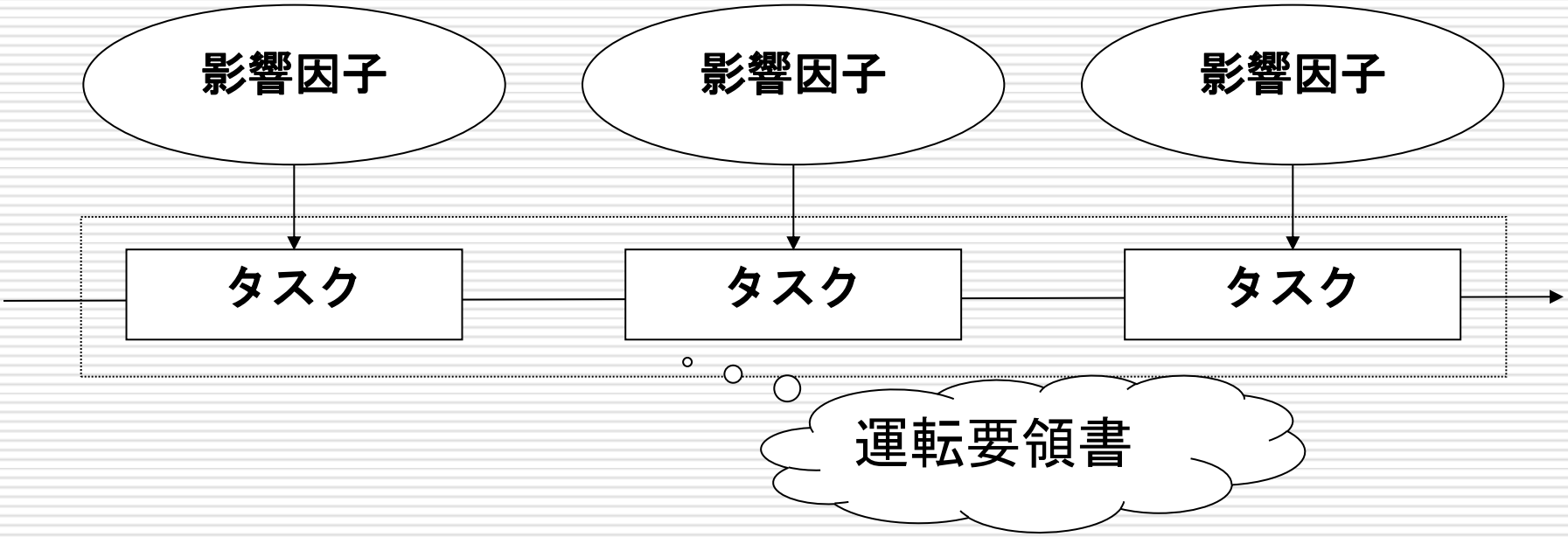
| ストレスレベル | | 熟練運転員 | 新人運転員 |
|---|---|---|---|
| 極めて低い | | ×２ | ×２ |
| 中程度 | ルーチンタスク | ×２ | ×４ |
| | ダイナミックタスク | ×５ | ×１０ |
| 極度に高い | ルーチンタスク | ×５ | ×１０ |
| | ダイナミックタスク | 0.25(EF=5) | 0.5(EF=5) |

# 従属性に関する修正

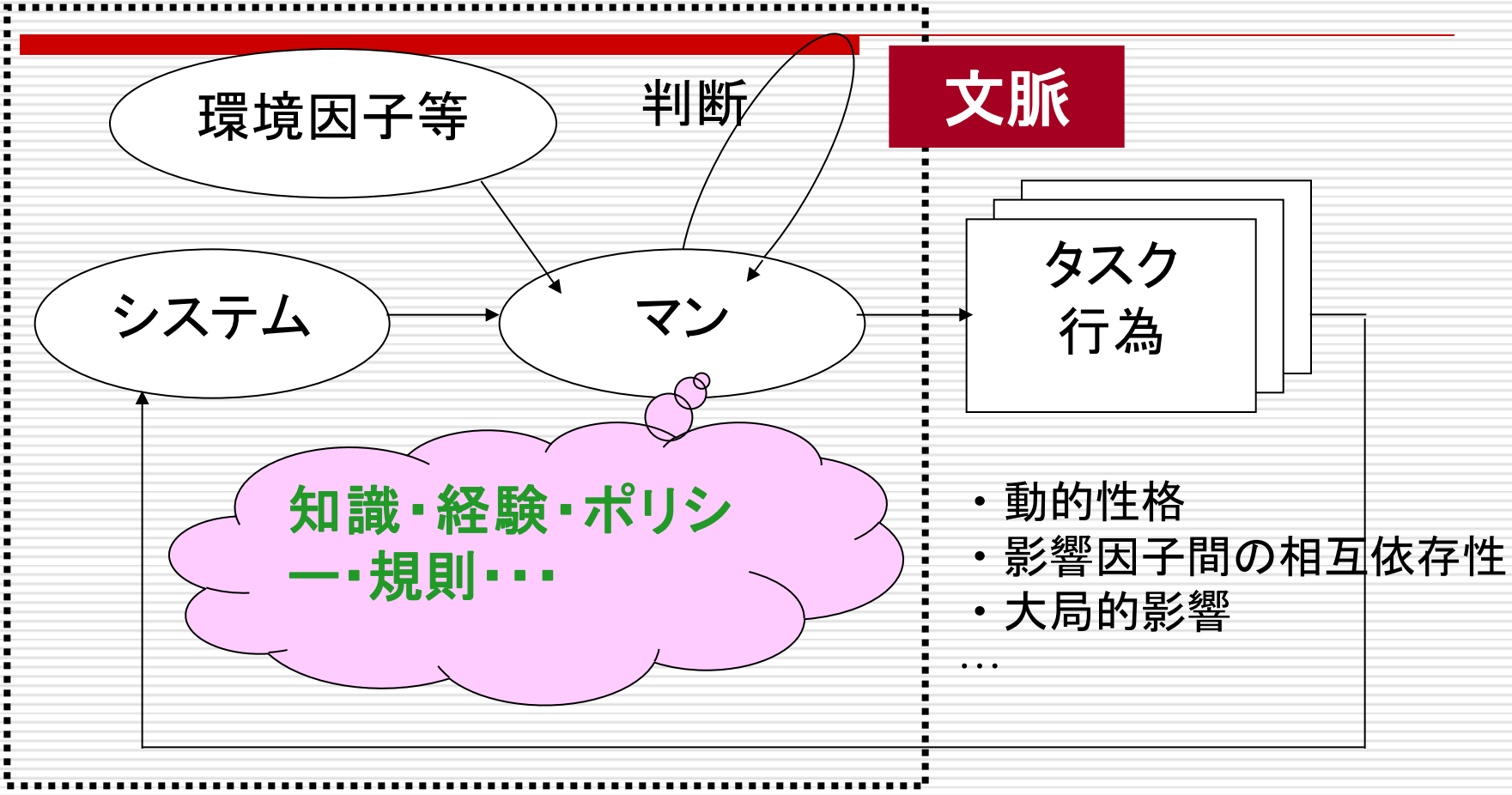
- 複数の作業単位実行する場合の従属性
  - ある作業員が3系統の冗長化されている測定系を校正する場合、
  - もし校正手続きを誤って理解していれば3系統とも誤校正
  - 運転員-Aが行う操作を運転員-Bがダブルチェック
  - Aが上級者であればBがその誤りを発見する確率は低くなる
- 従属性のレベル
  - ゼロ、低レベル、中レベル、高レベル、完全従属
  - Pr(F|先行作業失敗) =1 :完全従属時
  - =(1+BEP)/2 :高レベル従属時
  - =(1+6BEP)/7 :中レベル従属時
  - =(1+19BEP)/20 :低レベル従属時
  - = BEP :ゼロ従属
- 誤りからの復旧（リカバリー）確率を考慮に入れた修正も必要

# HRA1への批判（THERPの場合）

・人間の内的メカニズムのモデル化が欠如
  ・タスク構造主体の見方
  ・文脈性に欠如したパフォーマンス影響因子の扱い



# HRA2の開発: ATHEANA, CREAM, MERMOS




CREAM (Cognitive Reliability & Error Analysis Method)-Hollnagel

MERMOS (Methode d'Evaluation des Missions Operateurs pour la Securite )-EDF

# 第二世代人間信頼性評価（HRA2）

・ATHEANA (A Technique for Human Event Analysis)
[NUREG/CR-1624, 2000]

人間はある特定の状況においては一意の行動をするはずであり、
　対応時のエラーの誤差幅が大きいのではなく、
　エラーに導く状況の多様性が大きい
人間行動が情況に支配されるとすれば、
　分析対象は人にエラーを強要する情況であり、
　エラー率はエラー強制情況（EFC）の発生確率に依存

**エラー率　*HEP* = *P*（エラー｜情況）・*P*（情況）**

右辺第１因子の条件付き確率は、ある特定の情況でエラーを起こす確率
　人の認知特性で決まるが、この確率が１に近いと考える
*HEP*はほとんどEFCの生起確率である第２因子に左右され、
　*HEP*の評価はこの確率の評価を行うことと同じ

# 考　察

- 人間信頼性解析(HRA) は、システム評価に有効な道具
- そのためにもその方法論の確立が望まれる
- 現在利用されているHRA は、人間をシステムの一部と見なす方法論
- 新たなHRA は、人間は状況に依存して正しい対応するという仮説の上に作成された方法論であり、現実の人間行動をより忠実に表現

- HRAは、ロジカルなPRAとファジーな人間を扱うHFの接点であり、PRAからの要求とHFからできることのせめぎあいから現実的に可能な妥協点を見出すという視点が重要
- HRAでは、手法やデータの厳密性より考慮する範囲の網羅性を重視すべき

- 本来は、リスク評価の一つの重要な手法であるHRAであるが、プラント全体の挙動を人間との関係を見ながら評価するので、プラントの総合的なシステム設計には必須の手法
- 設計者が設計の基本として用いることを期待
- 組織信頼性解析（ORA）の研究は必要

# お疲れさまでした