2014年度第一回 日本セキュリティマネジメント学会 ITリスク学研究会
東京電機大学 2014年7月4日

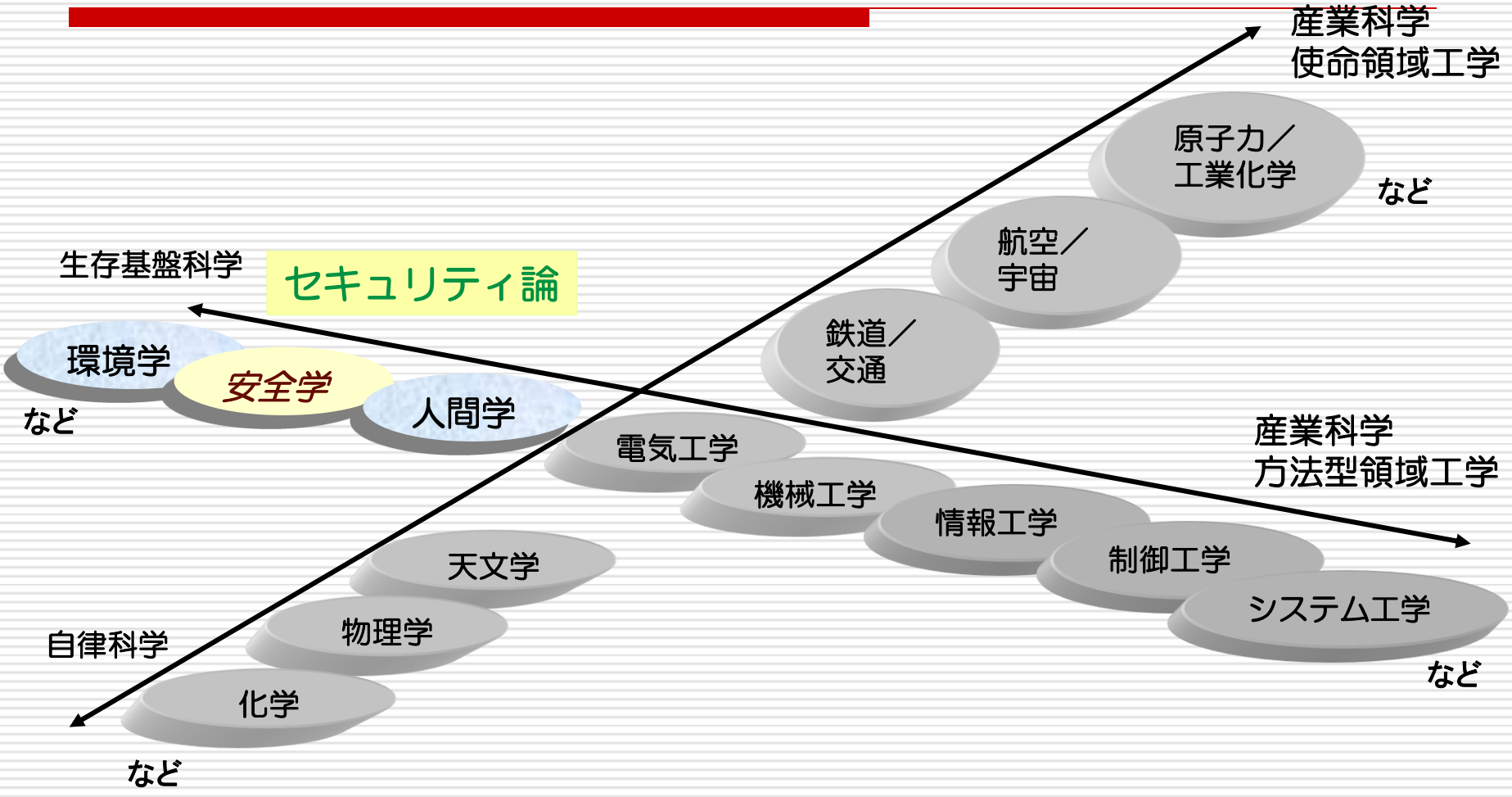
事故とエラーのモデルに基づく安全・セキュリティのための個人及び組織の在り方

氏田　博士
キヤノングローバル戦略研究所

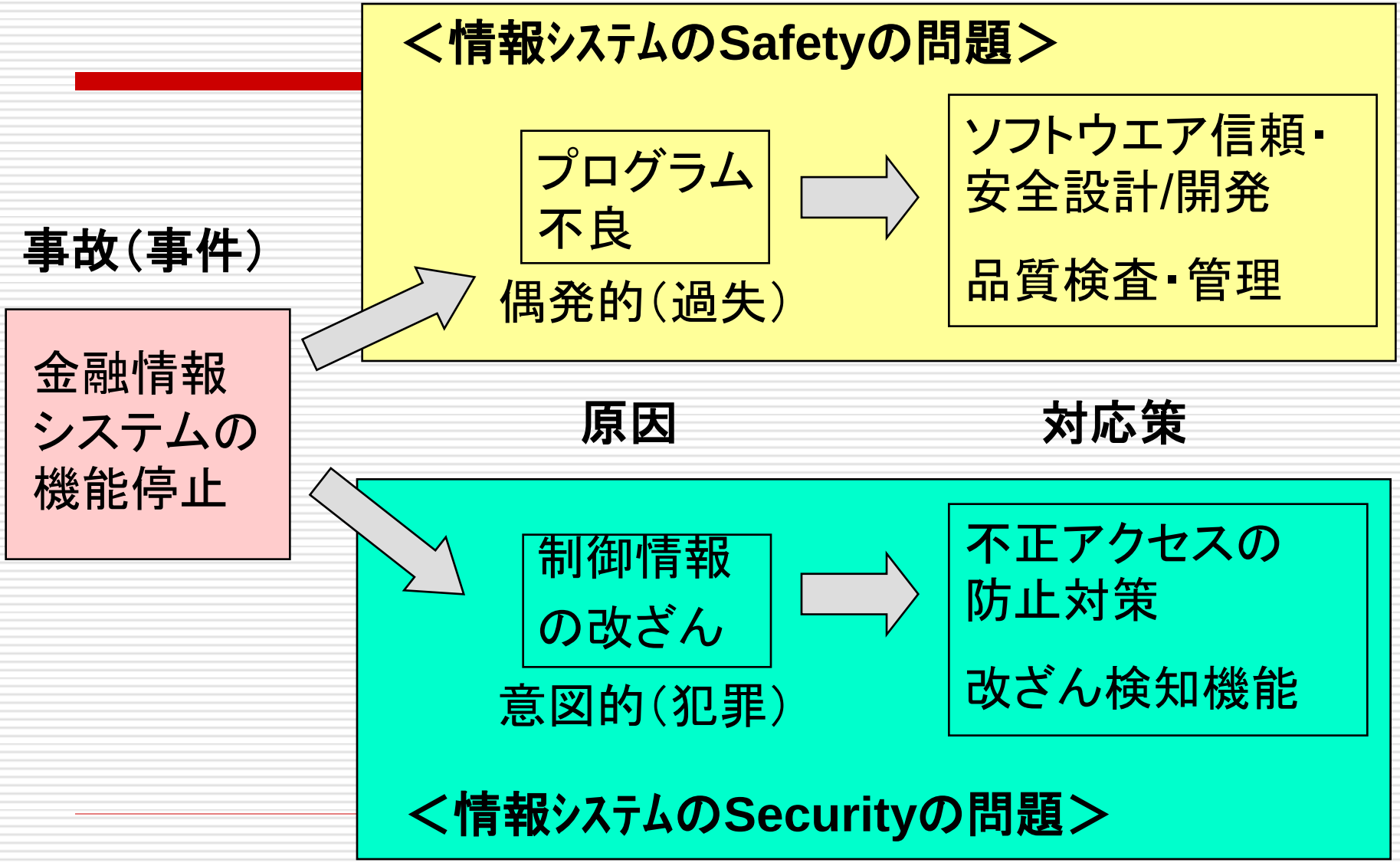
講演内容

- 安全・セキュリティ問題
- 事故モデルとは
- エラーとは
- 人間特性
- 安全性向上
- レジリエントシステム

安全学・セキュリティ論の位置付け



（狭い概念）セキュリティと安全性：セイフティ

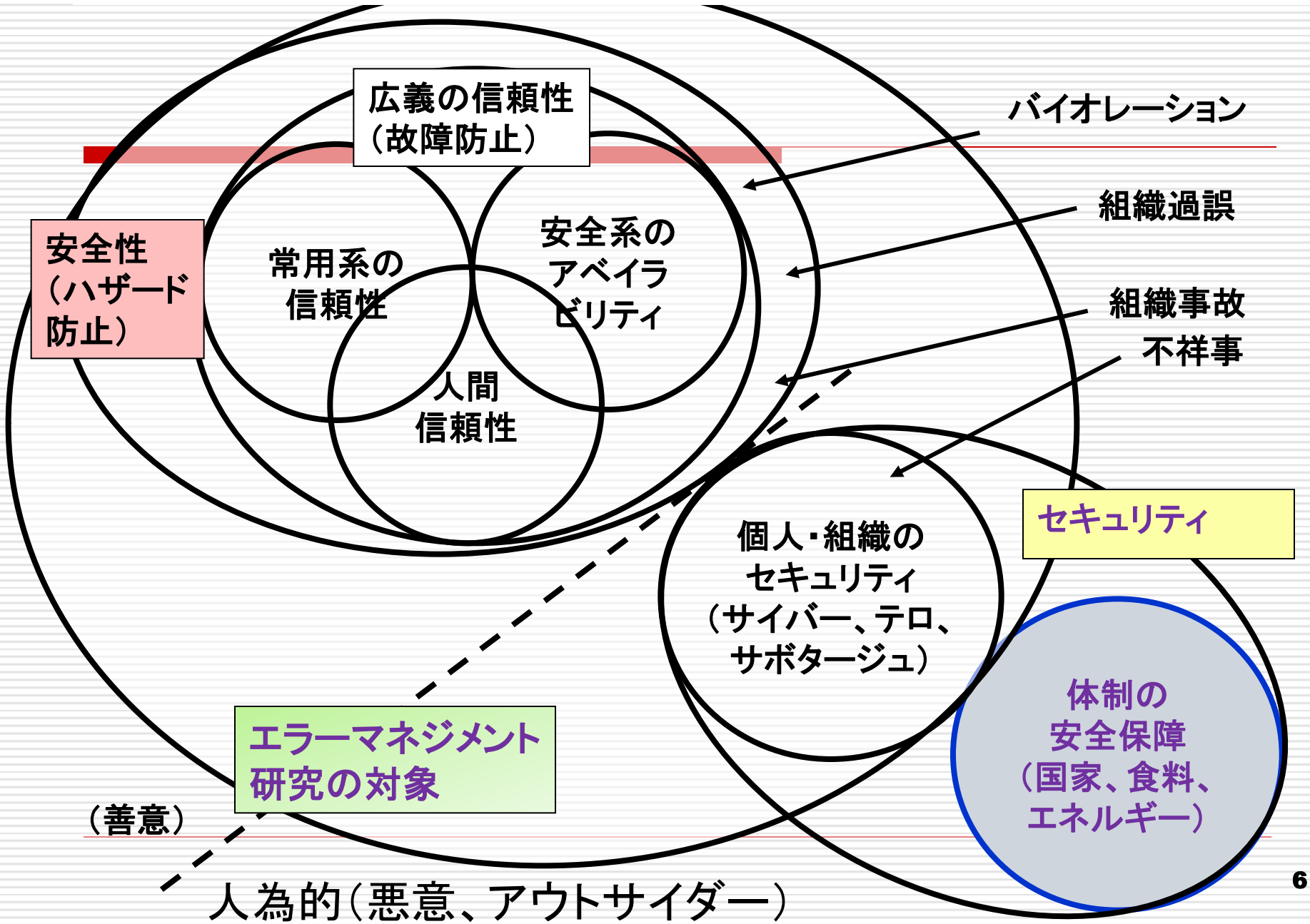


組織事故と不祥事-エラーマネジメント研究会

- 【組織事故の定義】
  - 組織内部の要因で組織を揺るがす規模まで拡大した事故
  - 同時に倫理的問題を含み、不祥事にいたる場合が多い
  - 安全問題（善意の行為だがエラーとなる）との関連性が高い
  - 組織内に潜む欠陥が知らず知らずに拡大し、その影響が組織全体や社会に及ぶ（Reason）

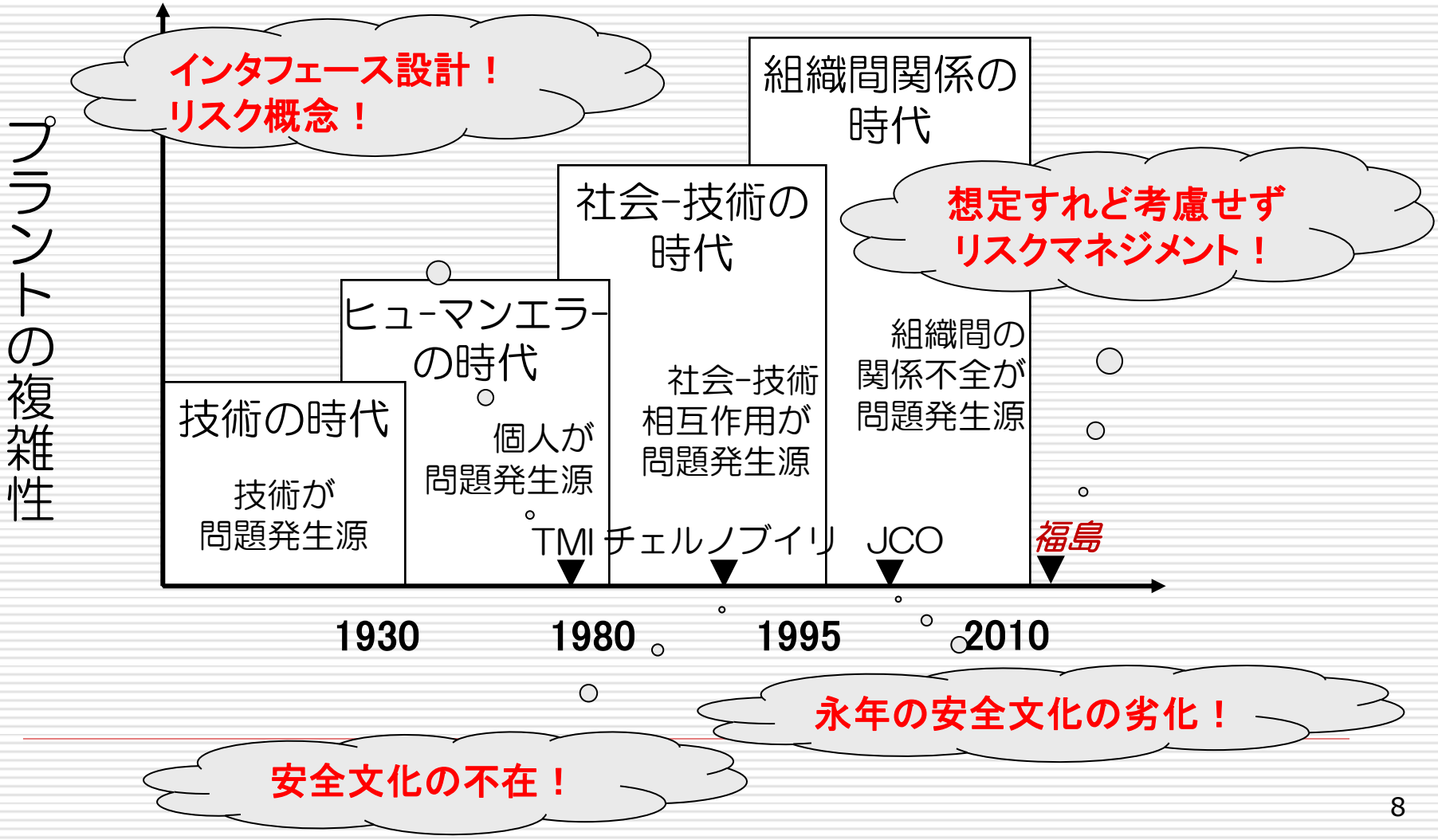
- 【不祥事の定義】
  - 組織事故やイベントの原因やその対応あるいは外部対応に、道徳的・倫理的問題が含まれ、社会的問題にまで拡大した事象
  - 事故そのものを問題とせず、組織の社会性を問題とする
  - セキュリティ問題（本質的に悪意があると社会から指弾された）との関連性が高い

信頼性、安全性、セキュリティの概念図




休み
ここでひと休み

安全問題のスコープの広がり（Reason, 1993）



事故モデルと分析方法・対策・管理との関係

Barrier and Accident Prevention, E. Hollnagel

事故モデル	探索原理、分析方法	解析の目標、対策	管理(様々なレベルのETTOに対し)
連続 (例:ドミノ、ツリー、ネットワーク)	原因 - 結果関係 (特定の原因と明確なリンク)	探索と破壊 原因の排除と封じ込み	ヒューマンエラー (個人)
疫学的 (例:スイスチーズ、病理学システム)	媒介と潜在条件 (チェックリスト、FMEA)	防護とバリア	パフォーマンスの逸脱 (組織)
システム志向 (例:機能的共鳴；FRAM、制御理論、カオス)	パフォーマンスの変動 →機能的共鳴	モニタと制御 (特に、組織の)	パフォーマンスの変動 (複合効果)

ETTO［効率-完全性トレードオフ］：人間の持つ効率と完全性のトレードオフ

- 後で誰かが確認する／前に誰かが確認した
- 負の報告：情報がないから全てが安全

・ 効率÷完全性　＞１　⇒　効率優先行動
・ 日常的な行動であり、揺らぎを持っている
・ 揺らぎが重なり合って（機能共鳴）事故になる⇒　“当たり前”の重なりが事故を起こす

事故・エラーのモデルと分析方法・対策の関係
（氏田、2014.4）

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 （故障の連鎖）	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 （多様性の喪失）	システムエラー （組織過誤）	リスク分析 リスク評価	防護とバリアの維持
組織事故 （深層防護の誤謬）	安全文化の劣化	行動科学 安全文化チェック	組織のモニタと制御

福島第一事故　2011
地震と津波による原子力発電所の状況

プラントの位置	原子炉数	地震後	津波後	津波の高さ
東通り	1	冷温停止	冷温停止	---
女川	1-3	自動緊急停止	冷温停止	設計: 9.1m 地盤高: 13.8m (実効高: 13m)
福島第一 (1F)	1-3	自動緊急停止	*冷却材喪失*	設計: 5.7m 地盤高: 10m (1F1-4) 13m (1F5&6) (実効高: 14-15m)
	4-6	冷温停止	*冷温停止*	
福島第二 (2F)	1-4	自動緊急停止	冷温停止	設計: 5.2m 地盤高: 12m (実効高: 6.5-7m, Locally >14m)
東海第二	－	自動緊急停止	冷温停止	地盤高: 8m (実効高: 5.4m)

リスクの想定可能性による3段階の分類
ー科学技術に対する公衆の不安はレベル3のリスクに起因

	内容	例	対応
レベル１	想定可能なリスク	想定事故	確定論で評価可能
レベル２	想定できないが、誤差幅として想定しているリスク	事象の不確かさ、手法の未成熟、因果関係がシナリオ・環境依存	確率論で評価可能
レベル３	誤差幅としても想定できない予想外のリスク その当時において、技術的に予想できないあるいは理解できない事象による危険	応力腐食割れ コメット機墜落 タコマ海峡橋崩壊 ・公害･環境問題:社会的にリスク概念や危険の実態が認知されない 水俣,黒４ダム	法律的には、リスクの予見性の議論 価値論の問題

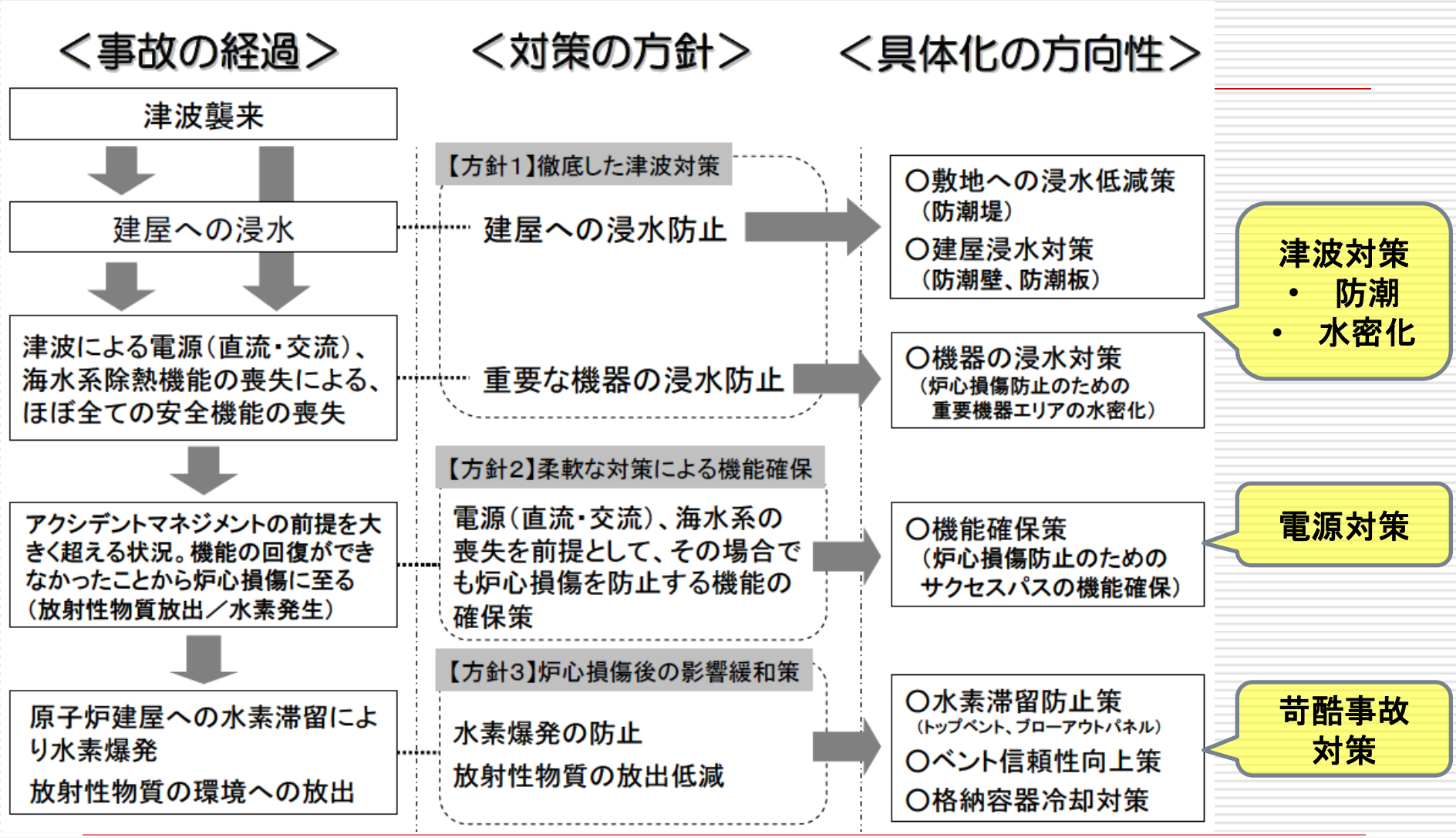
組織学習

- 個人シングル：個人のパフォーマンスの向上
- 個人ダブル：個人の規範を変更
- 組織シングル：組織のパフォーマンスの向上
- 組織ダブル：組織の規範を変更

- ルールの強化：個人シングル
- ルールの作成：個人ダブル
- ルールの交換：個人ダブル(個人にとっての環境と見れば)
- ルールの交換：組織シングル(組織内で知識を共有と見れば)
- ルールセットをエリート戦略：組織シングル
- ***目的選択確率変化(行動の介入、環境変化)：組織ダブル***
- ***共進化(協調学習、競争学習)：組織ダブル***

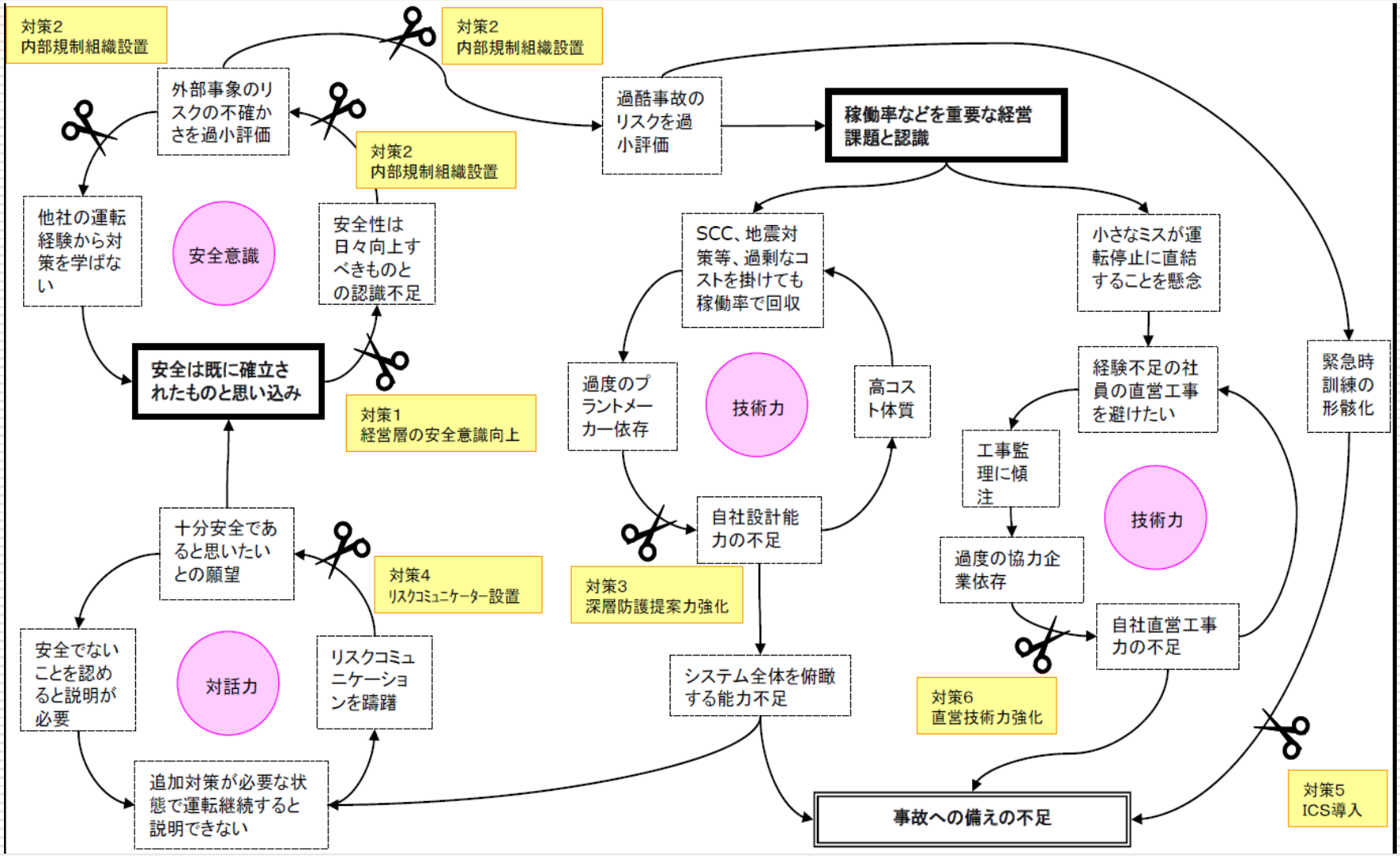
- 今回の事故の問題は、現場でのダブルループ学習は実現できていたが、そのループが本店にまで至らなかった
- 政府レベルでまた本店レベルにおいても、米国の３．１１事例対応や規格基準の様々な動向を取りこむべきダブルループ学習ができていない

事故の経過と対応方針の関連



東京電力（株）、「福島原子力事故調査報告書」、平成 24 年6 月20 日

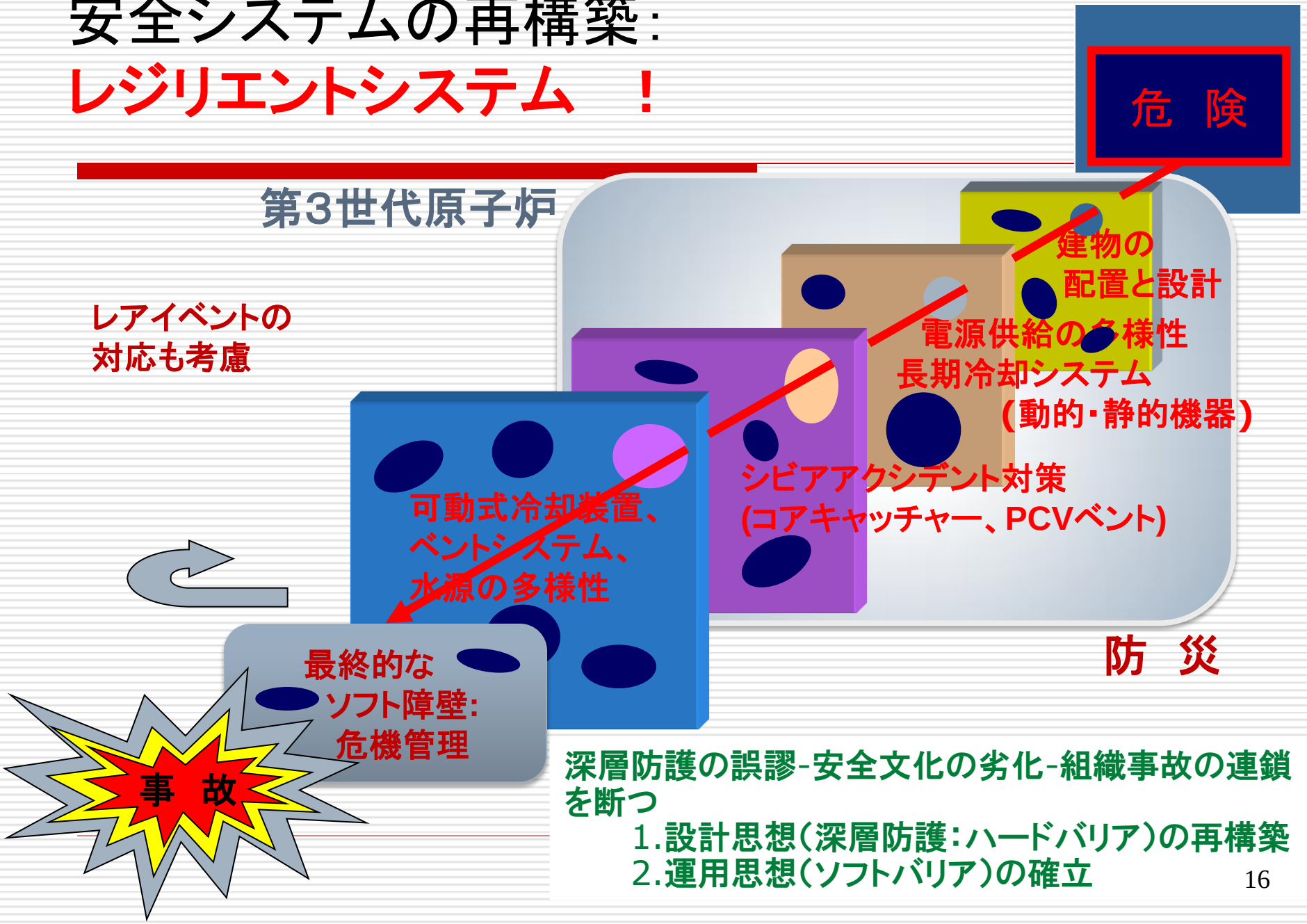
事故への備えが不足した負の連鎖の遮断



ICS：インシデントコマンドシステム

東京電力（株）、「福島原子力事故の総括および原子力安全改革プラン」H25.3.

安全システムの再構築:
レジリエントシステム　！



深層防護の誤謬-安全文化の劣化-組織事故の連鎖を断つ

1. 設計思想(深層防護:ハードバリア)の再構築
2. 運用思想(ソフトバリア)の確立

安全思想の再構築

	安全想定 （レアイベントの扱い）	安全設計 （ハードウエア）	安全運用 （ソフトウエア）	安全社会システム （制度設計）
事故予防	LOCA（冷却材喪失事故）からLOPA(電源喪失事故)へ（PSA知見） 初期事象（レアイベント）の見直し＊1	「止める・冷やす・閉じ込める」の原則の再検討		
事故緩和				
緊急時対応	苛酷事故の見直し	B-DBA対応強化	B-DBAのAM策 緊急時対応能力開発（手順書、訓練） 緊急時組織の在り方	緊急時国家体制整備
総合対策	設計基準事故（確定論）とPRAの評価関係見直し	安全設計指針の改定 PRA評価の深層防護への反映 多様性、静的機器、可搬性機器、水密性 新型炉への反映	PRA評価の反映（深層防護の誤謬による安全文化の劣化から組織事故に至る連鎖を断つ）	国策民営化の在り方 推進-規制-電力-メーカーの制度設計＊2 セイフティネットとしての保険国家補償 PRA評価の規制への反映＊3 安全目標の設定

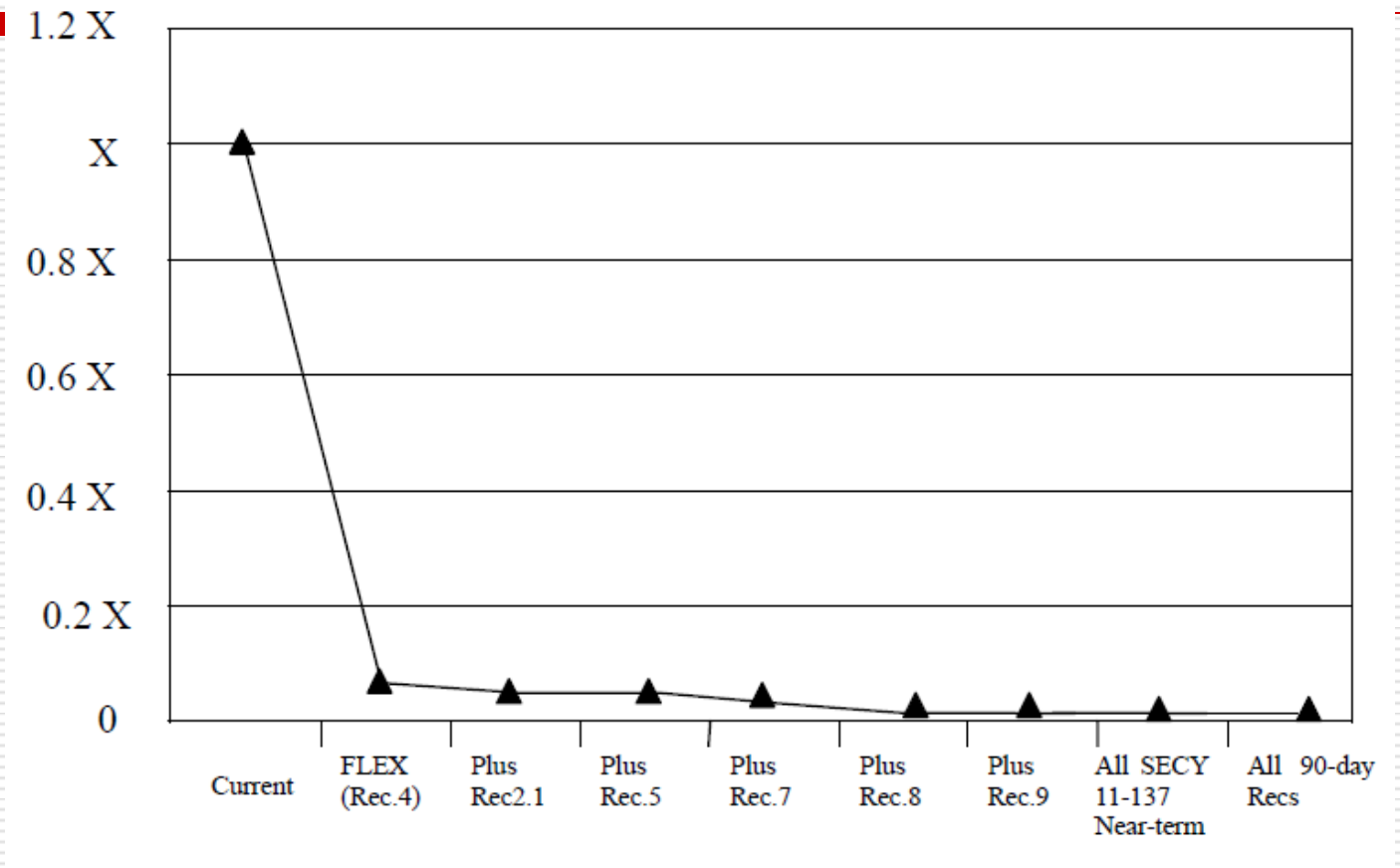
＊1 エキスパートパネルの設置（役所から独立した組織）

＊2 型式認定とサイト評価（NRC方式の導入）

＊3 RIR宣言（規制の合理化）（保安院発足時への回帰）

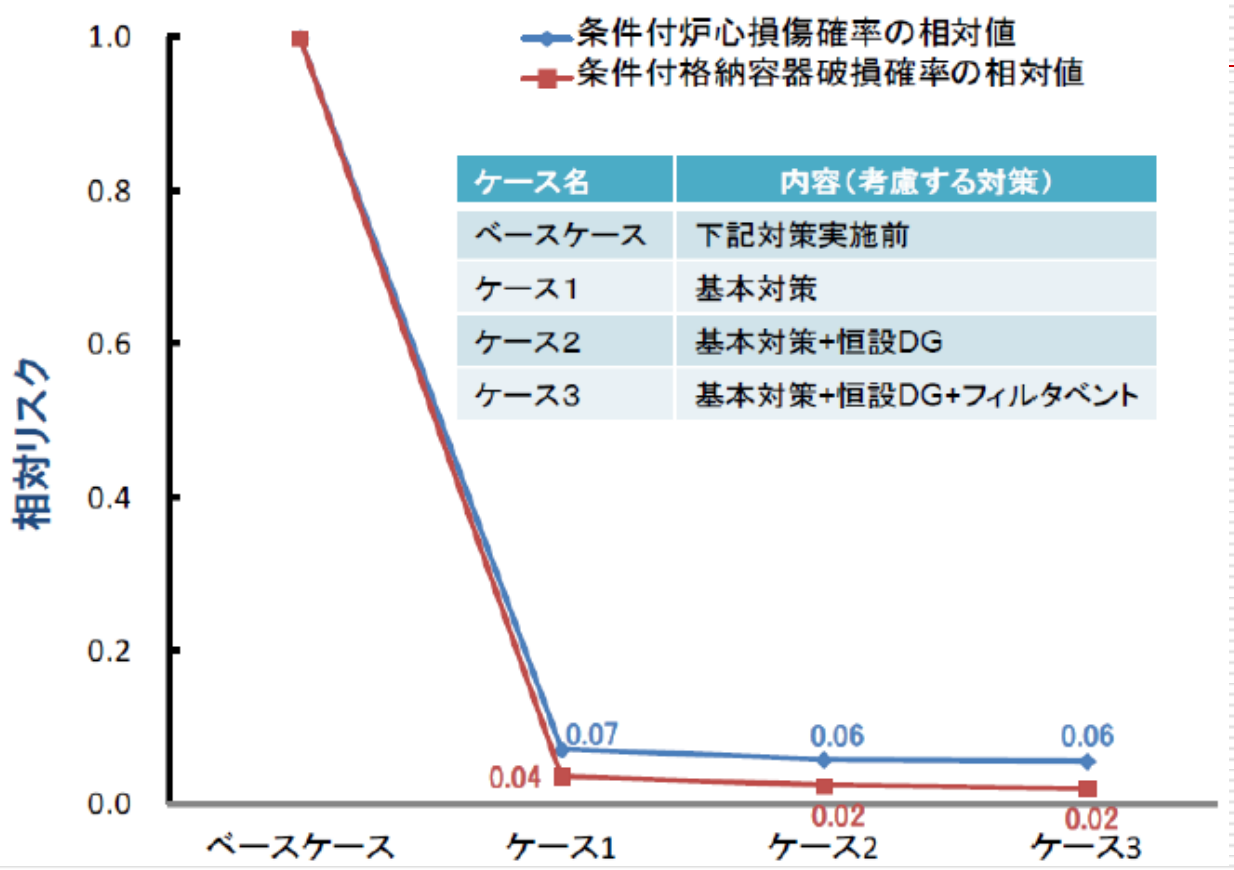
- *NRCと協調して安全思想を再構築し、IAEAと協調して世界へ発信*

FLEX によるリスク低減効果(安全性向上)



福島第一事故の教訓を早期に実現するための統合的な安全確保の取り組み
(米国原子力エネルギー協会NEI（Nuclear Energy Institute) による多重防護強化策の提案)
平成24 年2 月1 日 原子力安全委員会事務局

対策によるリスク低減効果



ケース名	内容（考慮する対策）
ベースケース	下記対策実施前
ケース1	基本対策
ケース2	基本対策+恒設DG
ケース3	基本対策+恒設DG+フィルタベント

条件付炉心損傷確率の相対値及び条件付格納容器破損確率の相対値は，ともにベースケースに対して，ケース1の段階ですでに十分に低くなり，ケース2，ケース3の対策を取り入れても，ほとんど寄与しない

PRAの実施方策の日米比較

日本と米国は、安全評価の基本は確定論的な評価であったが、米国はリスクベースの確率論的手法に基づく規制に移行した。日本は確率論的手法こそ導入したが、規制への反映は行われていない。

3．11を契機に確率論的な規制への移行が強く望まれる。

米国	日本
● NRC は 1990 年 代 に Risk-Informed Regulation導入 ➢ 規制の合理化(経済合理性) ➢ NRCとINPO (NEI)の独立性と協調 ● 規制・電力の作業量低減 ➢規制書類作成 ➢テストメンテナンス項目 ● 電力の自由度向上 ● 電力の安全意識向上 ● IPEEE （個別プラントの外的事象のPRA） 真の安全追求（リスク認識） ● PRAの実用化	● 安全評価は、確定論を堅持し、PRAは補足的役割のまま ➢ 恣意的な規制 ➢ 保安院と電力の敵対性と癒着性（相互依存）（JANSIが対応する組織だが） ✧ 作業量膨大 ● 書類作成量大 ● QA業務の煩雑化 ✧ 些末な数字イジリ ✧ 本質安全の議論なし ● 本当の安全を考える余裕なし ● 福島第一の津波PRA実施 （評価のみ、反映なし） 書類上の形式的安全（リスク認識なし） ● PRAはご参考（反映する枠組みなし）

➢ *日本人の安全に対する意識(金太郎飴的発想、言霊意識)の問題*

➢ *安全問題を本質的に考えない（言葉遊びに終始）*

➢ *RIRへの転換の再チャレンジ（保安院発足時への回帰））*

➢ *徹底した議論と明文化*

➢ *推進-規制-電力-メーカーの制度設計の問題（メーカーの製造責任の不在)*

➢ *型式認定（メーカー）＆サイト評価（電力）*

➢ *NRC方式の導入（メーカーは海外展開のために、NRCの型式認定は必須）*


休み
ここでひと休み

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下の判断と
　　神の目から見た判断

・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？

ヒューマンエラーの分類

分類： ヒューマンエラー解析の基礎

（1）影響による分類
- ヒューマンエラーの結果として生じる影響によって分類
- 運営組織の管理・社会的責任・ヒューマンエラー対策の優先順位付けに有効
- 結果論に基づくものであり、工学的立場からはあまり有効でない

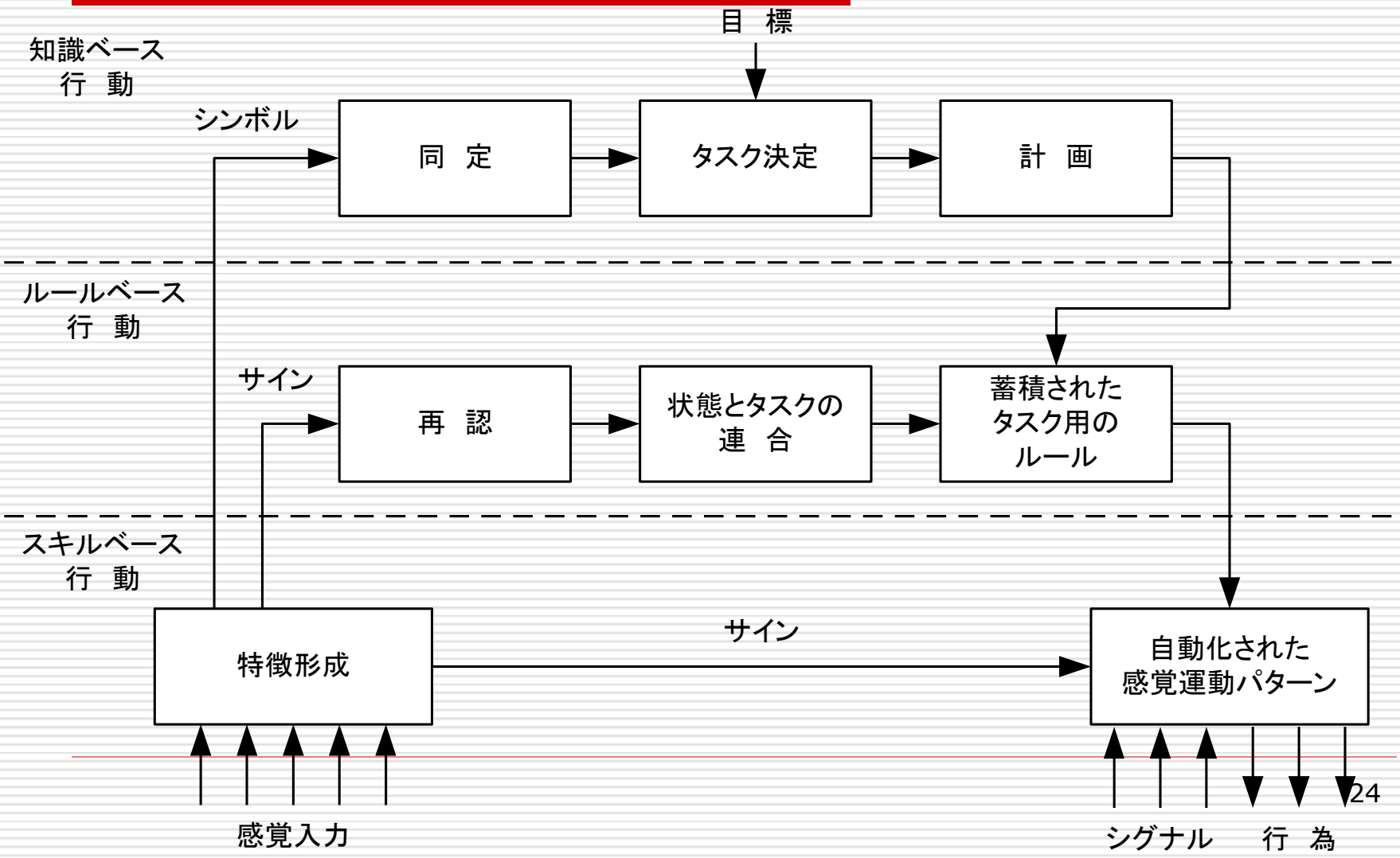
（2）原因による分類
- ヒューマンエラーが発生する原因によって分類

（3）表面的形態による分類
- 人間が取った行動によりヒューマンエラーを分類

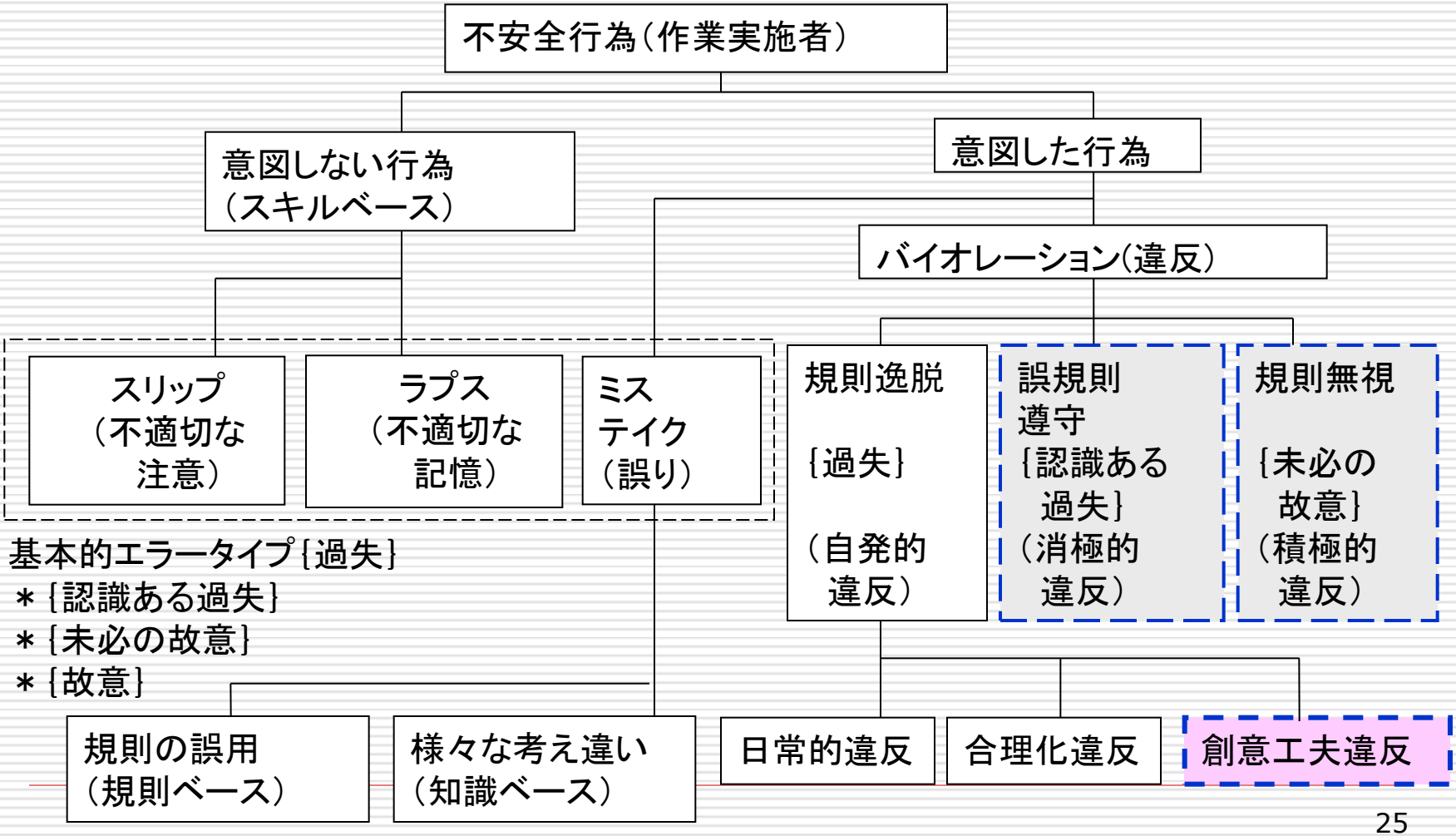
（4）発生機構による分類
- 人間の認知過程のどこで発生したのかにより分類

ヒューマンエラーの発生機構による分類

ReasonのGeneric-Error Modeling System (GEMS)
RasmussenのSRKモデル



不安全行為の分類（Reason, Jを改変）



エラーや故障から学ぶ3段階のフィードバックループ

	解析のループ	統計のループ	解析･統合のループ
評価方法	個別事象に対する根本原因分析（RCA)＊（臨床医学）	故障統計による故障傾向評価 集積RCA（社会医学）	リスク解析による統合システム評価（人間ドック）
対策	直接的な改善	故障の共通な特徴に応じた改善	安全上クリティカルな個所の改善 -総合安全の向上
フィードバックの対象	類似システムへの適用性大	類似システムへの適用性大	個別システム
フィードバックの規模	局所的･限定的	中規模	システム全体

＊共通要因分析

- 体感と全体理解の相互作用が本質
- 故障モードの定義が大切

レジリエントシステム

JCO事故調査報告書 （吉川弘之委員長）より

- 二律背反のジレンマ

- 安全性を向上させると効率が低下する
- 規則を強化すると創意工夫がなくなる
- 監視を強化すると士気が低下する
- マニュアル化すると自主性を失う
- フールプルーフは技能低下を招く
- 責任をキーパーソンに集中すると集団はばらばらとなる
- 責任を厳密にすると事故隠しが起きる
- 情報公開すると過度に保守的となる

ここまで分析することが根本原因分析：RCAでは?!

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)

	限定合理性		効用極大化
	取引コスト理論	エージェンシー理論	所有権理論
分析対象	取引関係	エージェンシー関係 (プリンシパルとエージェンシー)	所有関係
非効率性	機械主義的行動 (埋没コスト)	モラルハザード アドバースセレクション (レモン市場)	外部性
制度解決	取引コスト節約制度 (仲間-集権-分権)	エージェンシーコスト削減制度	外部性の内部化制度
事例	• ガダルカナル白兵突撃 • ワンマン経営-社外監視 • 硫黄島・沖縄戦	• インパール作戦 • ワークシェアリング	• ジャワ軍政 • 仲間意識と組織的隠蔽

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)

- 合理性-効率性-倫理性の不一致

- 不条理(組織は合理的に失敗する)の定義
  - 全体合理性と個別合理性の不一致
  - 効率性と正当性(倫理性)の不一致
  - 長期的帰結と短期的帰結の不一致

- 人間の限定合理性の問題に帰結
- 組織の歴史的不可逆性原理
- 資源利用コストと制度形成コストのトレードオフ
- 自律的批判的合理的構造-クリティカルマネージングフロー
- 開かれた組織


休み
ここでひと休み

認知バイアス

成功すれば難しい状況で意思決定するための知恵とされ、
失敗すればエラーの原因とされる認知メカニズム

- 問題を単純化して意思決定
- 間違ってはいないと思う答で決着
- 統計的変動性を無視して意思決定
- 類似している部分に重きをおいて意思決定
- 過去からの発生頻度に重きをおいて意思決定
- 習慣にもとづいて意思決定
- 保守的に意思決定、その他

マスコミの影響

- 民衆に影響を与えるマスコミの取材傾向
  - 恐怖を売るのが商売（政治家、法曹家、メディア）
  - 情緒に重点が置かれる傾向
  - 被害者の取り上げ方に偏りがある
  - 日本／日本人に偏る傾向
  - 緊迫性のないことを軽視する傾向
  - 話題性／新規性に偏る傾向
  - 慢性的リスクを軽視する傾向
- 寺田寅彦：正しく怖がる
- モンテニュー：最も恐れるものは恐怖

人間の考え方は、社会から制約を受ける

- バカの壁
  - 「話せば分かる」の大嘘
  - 知識と常識（経験の裏づけ、誰でも分かる)は違う
  - 科学的事実と科学的推論
- パラダイムシフト
  - アインシュタインはなぜ偉いのか？
- シミュレーションのパラドクス
  - 合理的仮定で解析しても、結果は社会的要請に合致

ソーシャルエンジニアリングの主な手法

- なりすまし：他人になりすまして、必要な情報を収集する。電話を利用することが多いが、電子メールや手紙を使ったり、FAX を利用することもある
- ゴミ箱漁り：トラッシング（Trashing）とか、Dumper Diving と呼ばれているが、ゴミとして廃棄された物の中から、目的の情報を取得する。オフィスからゴミとして出されたハードディスク、フロッピーディスク等の磁気媒体やCD、DVD、マニュアル、報告書等、重要書類等の印刷物を回収して、有効な情報を取得する
- サイト侵入：清掃員、電気・電話工事人、警備員等になりすまして、オフィスや工場等のサイトに侵入する
- のぞき見：他人のものをこっそりのぞき見する。情報が机上やコンピュータ上に露出しているものを意識的にのぞき見したりして、情報収集を行う
- メーリングリスト、ブログ等：メーリングリスト等の質問メッセージを利用して、質問者の技術レベル、利用システム、ソフトウェア、セキュリティ等の情報を収集する

ケビン・ミトニック：欺術
ソーシャルエンジニアリング

6つの人間の脆弱性(Six weapons of influence)

―ロバート・B・チャルディーニ「影響力の武器」2007 年9月 誠信書房 *(参考)*

(A) 返報性: 親切や贈り物、招待等を受けると、それを与えてくれた人に対して将来お返しをせずにいられない気持ちになる

(B) コミットメントと一貫性: 自由意志によりとった行動がその後の行動にある拘束もたらすことで、代表的なものに以下のような手法がある

①ローボールテクニック: 最初にある「決定」をさせるが、決定した事柄が実現不可能である事を示し、最初の決定より高度な要求を認めさせる方法。例えば、特売の商品を購入しにきた客に、購入の手続きの最中に在庫がなく当該の商品は購入できないが、色違いの少し高いものならあると言って高い商品を購入させてしまう

②ドア・イン・ザ・フェィス テクニック: 最初に実現不可能な要求を行い、対応できない状況の中で、それに比べて負担の軽い要求をしてそれを実現させる方法。例えば、法外な借金の依頼を最初に行い、断られたら少額の借金を申し出てそれを承諾させる

③フット・イン・ザ・ドア テクニック: 最初に誰もが断らないようなごく軽い要求を行ってもらい、次のより重い要求の承諾を得る方法。例えば、最初に簡単な署名を依頼し、その後時間がかかる調査に協力してもらう

(C) 社会的証明: 他人が何を正しいと考えているかによって、自分が正しいかどうかを判断する特性

(D) 好意: 好意を持っている人から頼まれると、承諾してしまうというもの。パーティを開いて、商品を購入させる場合、好意を持っている隣人がホスト役として販売を行うと、そうでない場合に比べて簡単に購入してしまう

(E) 権威: 企業・組織の上司等権威を持つものの命令に従ってしまう

(F) 希少性: 手に入りにくい物であるほど、貴重なものに思え、手に入れたくなってしまう特性

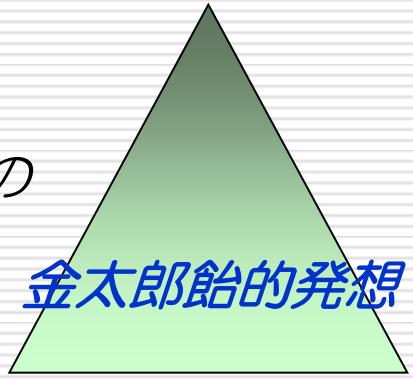
チームパフォーマンスの阻害要因 ー人間関係の中から（参考）

・権威勾配
  ・ アメリカの心理学者ミルグラム（Milgram,S）：電気ショック 実験
・同調行動
  ・ アッシュ（Asch.S.E）：社会的影響過程を明らかにする実験
  ・ 線分の長さの比較実験
・社会的手抜き
  ・ ニューヨークで起こったキティ・ジェノバーズ事件
  ・ リンゲルマン（Ringelmann）効果 ：綱引き
  ・ ラタネ（Latane,B.）ら：「社会的手抜き」と命名
・集団浅慮
  ・ ジャニス（Janis,I.L.）：ケネディ政権のピッグズ湾侵攻
  ・ ブッシュジュニア政権のイラク進攻
・リスキーシフト
  ・ ワラック（Wallach,M.A.）&コーガン（Kogan,N.）：報酬とリスク実験

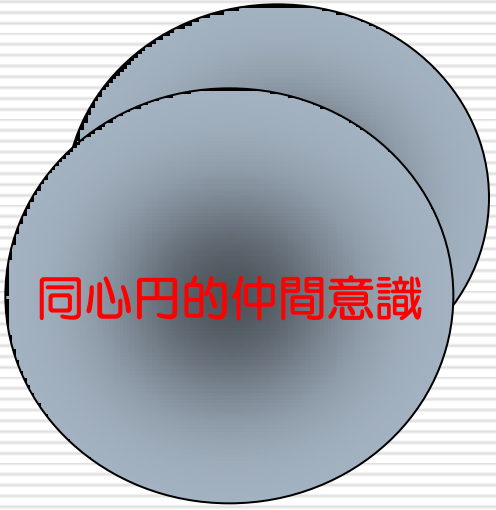
日本における安全追求の阻害要因である「金太郎飴的発想」と「同心円的仲間意識」

固定的な階層構造組織→皆でわたれば怖くない化

ボトムアップの
意思決定構造
→
トップマネジメントの
不在
→
・意思決定の遅延
・安全の価値の無理解



多層の
派閥構造
→
機能体の
共同体化
→
・癒着
・非能率



日本人は、下士官として超優秀
兵士：ロシア人、下級士官：フランス人、参謀：ドイツ人、将軍：アメリカ人

日本における安全追求の阻害要因である

「言霊意識」- 井沢元彦「言霊(コトダマ)の国」解体新書

日本は、いまだに「言霊：言葉に出すとそれが現実になる」に支配されている

- 「自分の国は自分で守る」という「世界の常識」を口にすると、「平和の敵」
- 受験生の前で「滑って転んだ」、「落ちた」は、タブー
- 結婚式で、終わるの切れるの分かれるのは、厳禁
- ４は「死」、９は「苦」に通じる

- 安全であれば問題ないのに安心を求める姿勢
- リスクリテラシーがあることが本当の意味で安心に生きる道
- リスクを考慮すること自体が不吉とする考え方

- 安心ですよというポジティブな言葉は作る
- リスクがあるよと言うネガティブな言葉は作らなかった

- 言葉に対する感受性を大いに高める
- 芸術、文藝の分野には良い方向に威力を発揮
- 科学技術、経済、政治、その他現代社会の根底の部分に悪影響

日本における安全追求の阻害要因である「東大話法」1 - 安冨歩『原発危機と「東大話法」』（2012年1月）

- 1.自分の信念ではなく、自分の立場に合わせた思考を採用する。
- 2.自分の立場の都合のよいように相手の話を解釈する。
- 3.都合の悪いことは無視し、都合のよいことだけ返事をする。
- 4.都合のよいことがない場合には、関係のない話をしてお茶を濁す。
- 5.どんなにいい加減でつじつまの合わないことでも自信満々で話す。
- 6.自分の問題を隠すために、同種の問題を持つ人を、力いっぱい批判する。
- 7.その場で自分が立派な人だと思われることを言う。
- 8.自分を傍観者と見なし、発言者を分類してレッテル貼りし、実体化して属性を勝手に設定し、解説する。
- 9.「誤解を恐れずに言えば」と言って、嘘をつく。
- 10.スケープゴートを侮蔑することで、読者・聞き手を恫喝し、迎合的な態度を取らせる。

日本における安全追求の阻害要因である「東大話法」2 - 安冨歩『原発危機と「東大話法」』（2012年1月）

- 11.相手の知識が自分より低いと見たら、なりふり構わず、自信満々で難しそうな概念を持ち出す。
- 12.自分の議論を「公平」だと無根拠に断言する。
- 13.自分の立場に沿って、都合のよい話を集める。
- 14.羊頭狗肉。
- 15.わけのわからない見せかけの自己批判によって、誠実さを演出する。
- 16.わけのわからない理屈を使って相手をケムに巻き、自分の主張を正当化する。
- 17.ああでもない、こうでもない、と自分がいろいろ知っていることを並べて、賢いところを見せる。
- 18.ああでもない、こうでもない、と引っ張っておいて、自分の言いたいところに突然落とす。
- 19.全体のバランスを常に考えて発言せよ。
- 20.「もし○○○であるとしたら、お詫びします」と言って、謝罪したフリで切り抜ける。

日本における安全追求の阻害要因である「東大話法」3 - 「立場主義者」

1. 役を果たすためには、なんでもやらなくてはならない。
2. 立場を守るためには何をしてもいい。
3. 人の立場を侵害してはいけない。

- 原発事故でメディアに登場してきた御用学者たちは、「我が国」という言葉を使うことで、事故を起こしたのは「我」ではなく「我が国」だから我関せず、まるで傍観者のようにヌケヌケと「原発は安全だ」と言い続けることができる
- 日本の企業では、横領などの個人的な犯罪は厳しく処罰されるが、見込み違いの過剰投資や明らかにムダな新規事業など企業ぐるみで行った失策は、まず間違いなく責任の所在があやふやにされる。"みんなでやった失敗"ということにして、悪事を微分化することで、責任と罪悪感を分散する
- 「東大話法」で事の本質をごまかすエリートたちから身を守るには、「東大話法」はあくまでテクニックで内容がないので、適当に言っていることを真に受けて対応する

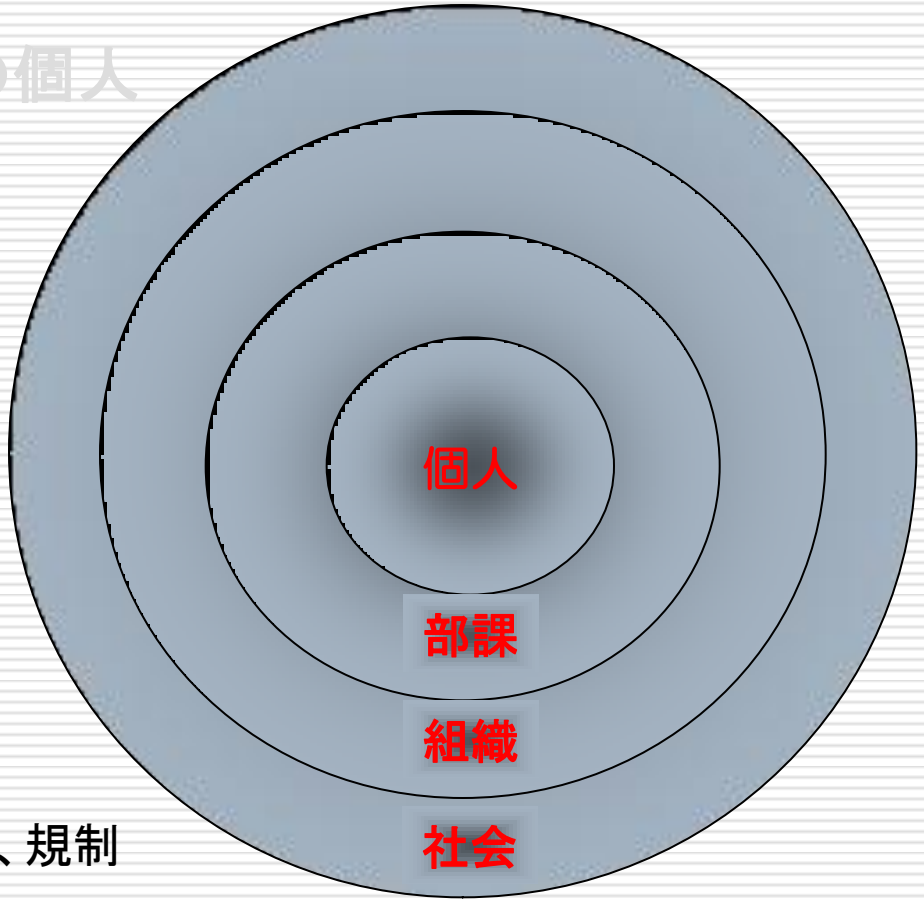

休み
ここでひと休み

倫理感の醸成

- 会社人間の前に社会人
- 組織の一員の前に一個の個人

- *皆でわたれば怖くない*

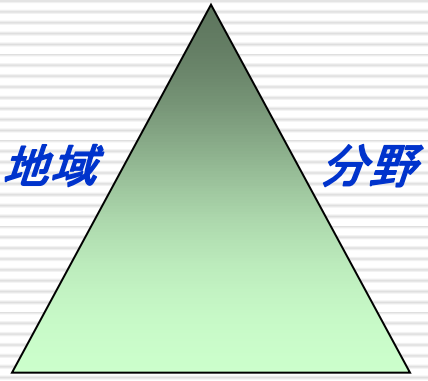
- 専門家倫理、技術者倫理
- 企業倫理綱領 、内部監査、内部告発
- CSR、創業者精神、トップの精神
- 社会道徳、外部監視の目、規制



有機的な組織を作る（柔軟な文化とする）

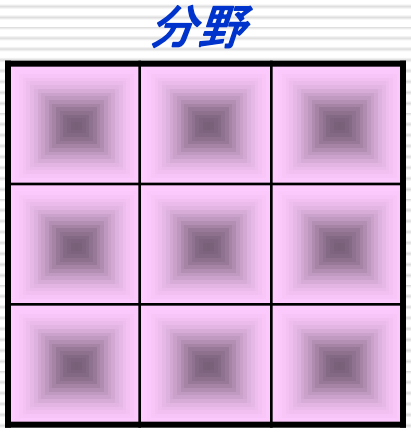
- [堺屋,1993]オーケストラ型からジャズ型への変換が必要
- 最近のインターネットの普及で、社員が直接的に社長に意見具申できる、新規提案をする、などの形態である程度実現しつつある
- 最近流行りの知識管理は、このようなフラットな組織つくりのための技術

機能体の共同体化 →
ボトムアップ



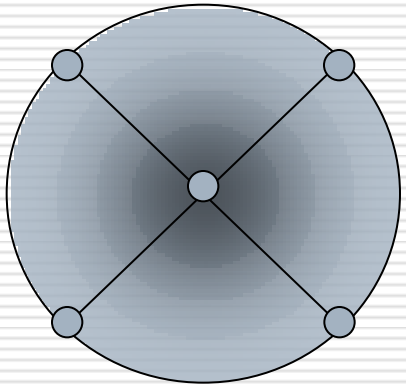
（日本的大企業）階層構造

機能体の維持
トップダウン



（ABB）マトリクス組織

地域 分野



ネットワーク型組織

有機的な組織を作る（柔軟な文化とする）

- [堺屋,1993]オーケストラ型からジャズ型への変換が必要
  - 最近のインターネットの普及で、社員が直接的に社長に意見具申できる、新規提案をする、などの形態である程度実現しつつある
  - 最近流行りの知識管理は、このようなフラットな組織つくりのための技術
  - 安全文化すなわち安全組織のチェックリストは、このような組織の変容を評価できることが必要

- 個人と組織のダブルループ学習を如何に実現するか?
  - トップの意思表示とコミュニケーションスキルとボトムアップ(情報共有)
  - 第三者機関(外部の圧力、社会の目)の利用
  - 地域との共生(リスクコミュニケーション)
  - 技術的安全と社会的安心

文明史からの考察

- 古代ローマ帝国、大英帝国の衰退時

-都市生活、海外旅行、温泉、軽薄趣味、文字より漫画、健康志向、グルメ、新興宗教、ポピュリズム、女権拡張、新規性志向

- トインビー：文明衰退論

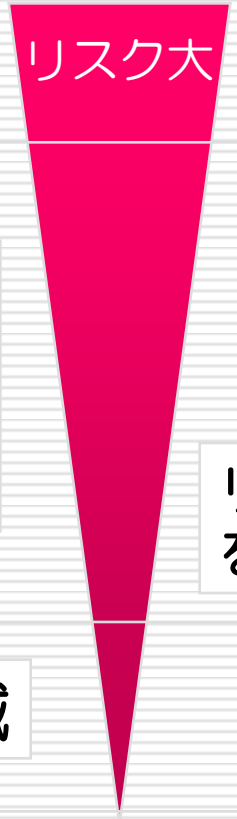
「われわれはつねに、自らの内にある“虚ろなるもの”によって裏切られるのであり、他者に裏切られるのではない」

「自らを保ち続ける：独自の価値観、伝統、制度の維持」

- サッチャリズム：社会的公正より個人の自由

-自助努力、競争原理、自由市場、、、

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

リスク
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

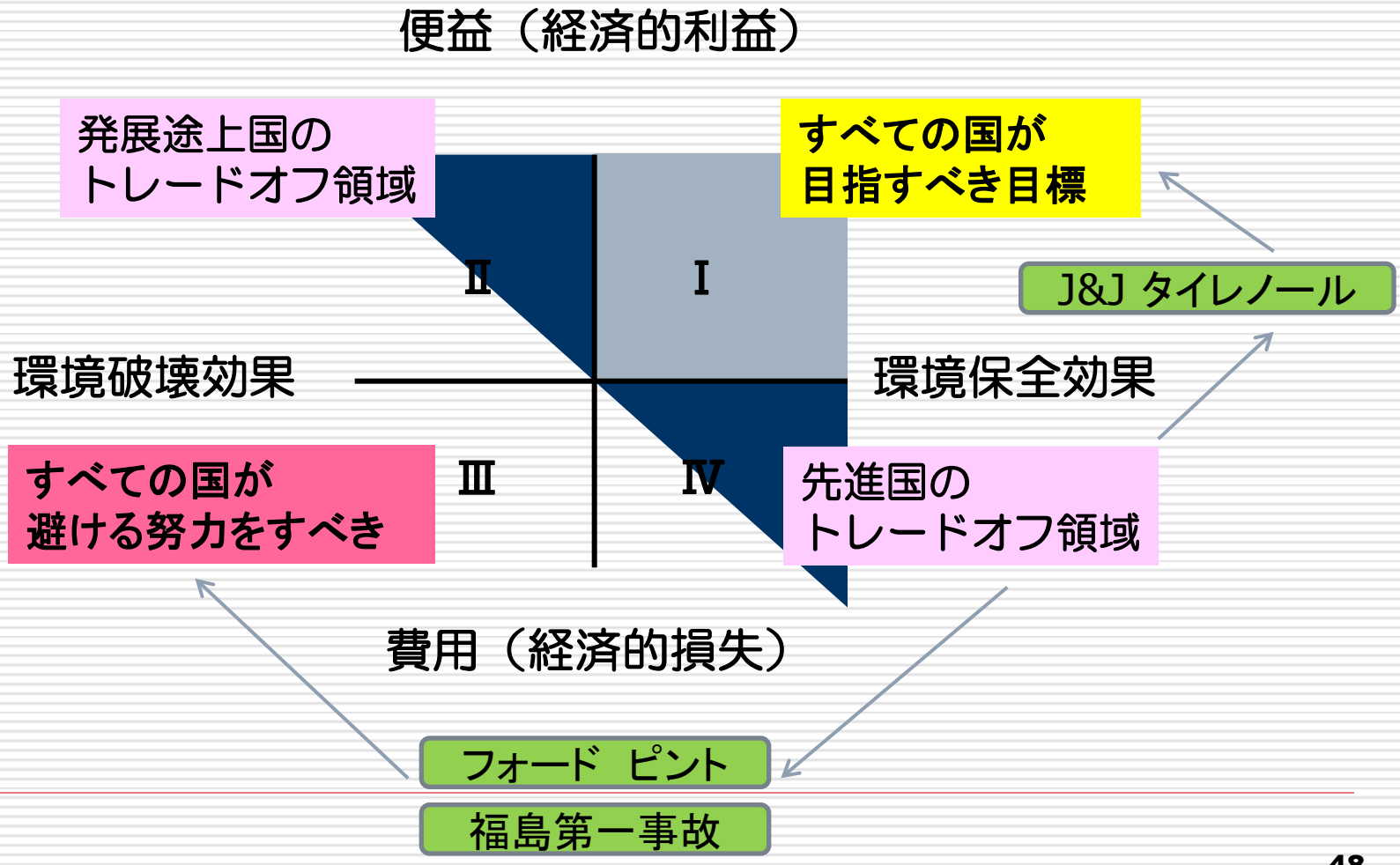
安全目標

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

無視できるリスク

リスクベネフィット解析に基づく環境保全と経済性の関係：中西,1994

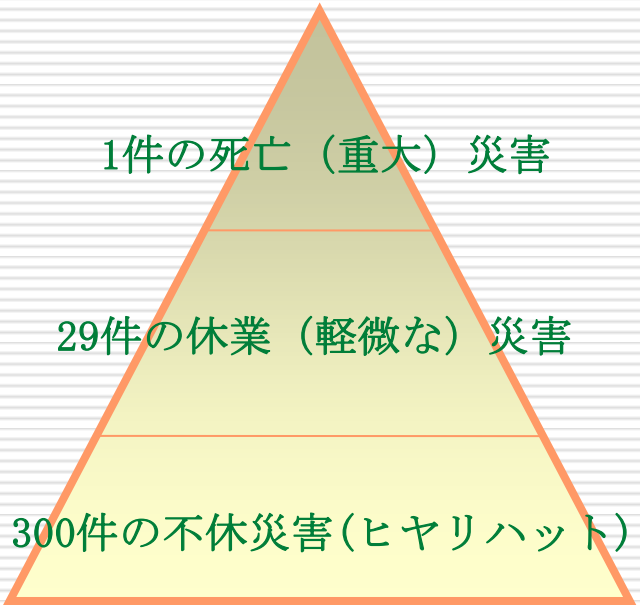



休み
ここでひと休み

組織分析の新しい考え方

- レジリアンスエンジニアリング
  - 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！
  - 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！

「Heinrichの法則」：労働災害の分野



まとめると、

- 柔軟な組織作り
  - レジリアンスエンジニアリング：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：組織のリスク事例に学ぶ；事例分析

を参考として事例分析を試みる

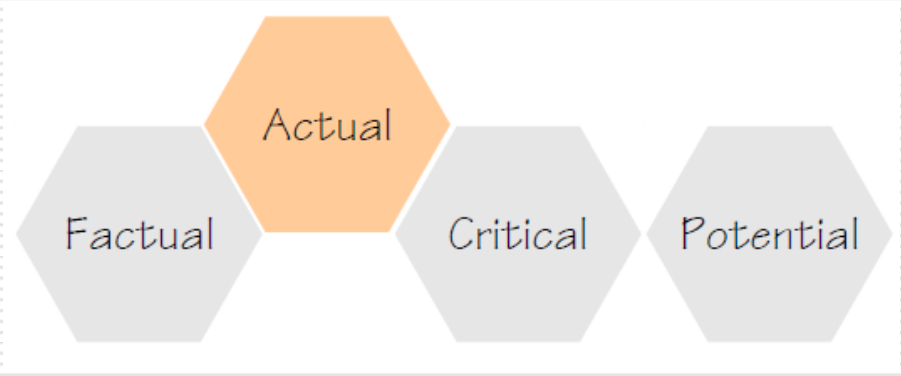
レジリアンス（柔軟で強靭）をデザインする

エリック・ホルナゲル
Safety Culture, Safety Management, and Resilience Engineering
2009年11月20日ATEC航空安全フォーラム

弾

これらを組織の全階層で実行できる能力と信頼度を向上することにより、安全向上と管理能力の向上を同時に実現でき、予測・計画・生産の力量が強化できる。

即応力：何をすべきか分かり、
対応する実行力がある



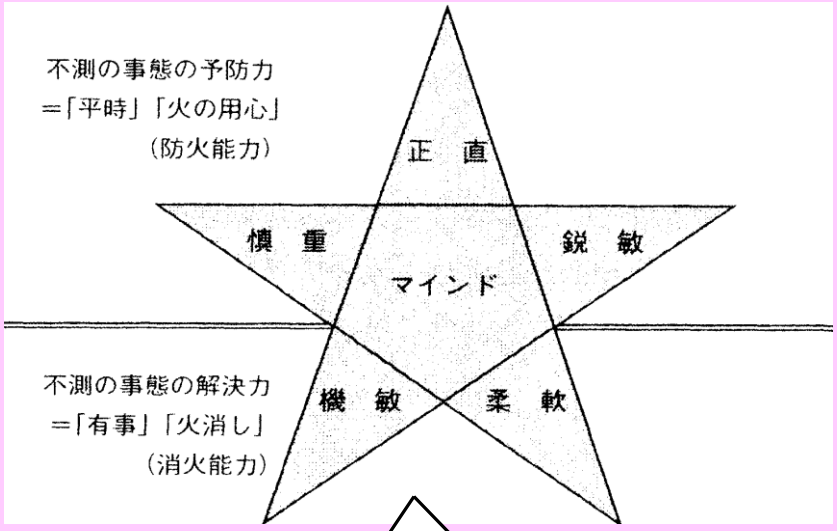
予測力：何が起こりそうか
判断でき承知する。

学習力：何が発生し
たか理解する。

監視力：何に眼を光らせるべき
か分かる。

中西の高信頼性組織の基本モデル

第一層（表層）	組織プロセス	**高信頼性組織の条件**
第二層（中層）	組織マネジメント	評価報酬　情報共有　内部統制 教育訓練　意思決定
第三層（深層）	組織文化	信頼の文化　正義の文化 勇気の文化　学習の文化



リスクリテラシー　:福知山線脱線

-事例で学ぶリスクリテラシー入門、林 志行

- **リスクマネジメント(＝レジリアンス能力？)の観点から分析**

リスクリテラシー ―――― 分析	解析力			伝達力		実践力	
	収集力	理解力	予測力	ネットワーク力(内部)	コミュニケーション力(外部)	対応力(今ある危機対応)	応用力
個人レベル	•加速度事故例	•スピードのリスク認識	•脱線のリスク認識	—	—	—	—
組織レベル	•事故例収集:*信楽鉄道衝突、日比谷線脱線*	•過密ダイヤの影響範囲	•事故の大きさの認識	•事故の重要性の組織伝達	—	•:被害の拡大防止	•**ATSの早期導入** •**教育システム見直し**
外部対応	•不祥事例収集	•事故の重要性分類	•当日の宴会、ゴルフコンペの問題性	—	•置石説	•メディア広報	•抜本対策:組織の是正 •過密ダイヤ改定

- **倫理感よりリスク感の養成！**

リスクリテラシー 能力の評価：1F1注水経緯分析– 新たな枠組みによる

リスクリテラシー ＼ 分析レベル		平時					有事	
		解析力			伝達力		実践力	
		収集力	理解力	予測力	ネットワーク力（情報発信）	コミュニケーション力（影響力）	対応力（今ある危機対応）	応用力（抜本対策）
個人		・津波被害事故例	・津波被害のリスク認識	・電源喪失のリスク認識	—	—	・海水注入継続判断	・緊急時訓練
組織	現場	・事故例収集：貞観津波	・地震・津波PSA実施による影響範囲評価	・事故の大きさの認識	・現場の情報共有	・指揮系統（現場） ・免震棟での一元化 *・中装–緊対室連絡*	・淡水・海水注入 ・ベント操作 ・被害の拡大防止	・免震棟整備・消防車配備 ・指揮系統 ・津波対策 ・AM対策
	管理部門	・事故例収集：貞観津波、JNES津波PSA、ルブレイエ・マドラス炉浸水	*・津波被害のリスク誤認識*	*・電源喪失のリスク誤認識*	*・本店/現場の情報共有*	・TV会議システム（2F） *・本店–現場の指揮系統の乱れ*		・教育/訓練システム見直し
外部対応（官邸、等）		・海外テロ対策事例収集：米国9.11テロ–B.5.b.	・事故の重要性分類 *・地震・津波リスク誤認識*	・外部事象の重要性 *・インフラ被害リスク誤認識*		*・メディア、地方自治体、海外広報* *・官邸/本店/現場の指揮系統の乱れ*	*・初期対応の遅れ* *・政府指揮系統*	・メーカ・協力企業の支援 ・外部の支援 ・抜本対策：組織改革（規制/電力）

- 緑は良好事例、*赤は失敗事例*
- 解析力は平時、実践力は有事
- 伝達力のうち、ネットワーク力は平時、コミュニケーション力は有事
- 組織を現場と管理部門に分割

54

1.1　福島第一（1F)と福島第二（2F)の共通点と2Fの特徴

福島第一（1F)と福島第二（2F)の共通点と2Fの特徴

1Fと2Fの共通点	2Fの特徴	備考
・発電所対策本部の適切なガバナンス	・外部電源の１系統が機能維持	
・発電所の外の組織(本店、メーカ等）から迅速な支援、物資の調達を受けられる体制の整備	・重要な設備の津波被害が軽微	
・強い使命感と安全文化を醸成	・比較的短時間で事故収束	
・耐震設計が有効に機能	・計器類機能維持	
・事故時対応に適切なマネジメント時からの職場環境づくり	・照明及び通信手段確保	
・事前に準備されていた各種対策の有効性	・中央操作室のランプで確認	
・非常時体制の整備	・本部で主要パラメーターを継続監視	共通点多い 相違は、電源とそれによる情報の有無
・食料備蓄	・パラメーター変動から計器類の故障の有無を確認	
・本店及び3発電所が共有のテレビ会議システム	・高汚染、高線量の極限状態での対応ではない	
・AM設備及びマニュアルが準備		
・十分な知識		
・深層防護的な考え		
・免震重要棟の設置(中越沖地震の経験）		

おわり

お疲れさまでした

ソフトバリアの概念

ハードによる安全障壁（ハードバリア）
- 深層防護（止める、冷す、閉じ込める）
- 多重防護（臨界管理：距離、形状、濃度、容量）

ソフトによる安全障壁（ソフトバリア）
：ハードバリアを期待される状態に維持管理し、
必要なときに期待された機能を発揮させ、
さらに万一ハードな防護壁が機能しなかった場合に
災害を防止するために必要な人間の活動と
これを保証する手順書、規定、法令、組織、社会制度など
- ソフトウェア（安全ロジック、使い勝手）
- ヒューマンウェア
（運転員、保守員、組織、文化、こちらが運用に近い）

フォード社ピント衝突火災(製造物責任)

第二象限→第三象限(安全も経済性も損失)の例

1973年：ピントが停止中に追突され、炎上し、運転者死亡

燃料タンクの設計不良(配置不良－スタイリング優先)

タンク回り保護機能の欠如（弱いバンパ、衝撃吸収策欠如)

－開発期間短縮（２年を１年）、コスト削減

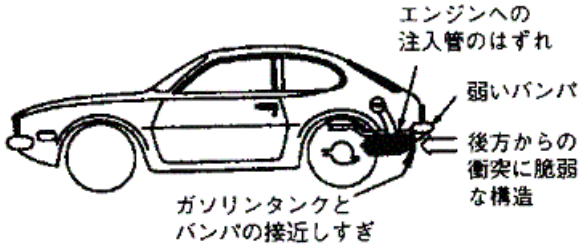


図1　1971年，1972年型フォード・ピントの構造欠陥

運輸省勧告に対する請願書

（コストベネフィット解析）

安全性向上によるコスト低減：4,950万ドル

(死者：20万ドル＊180人,,,)

車両製造コストの増加：13,700万ドル

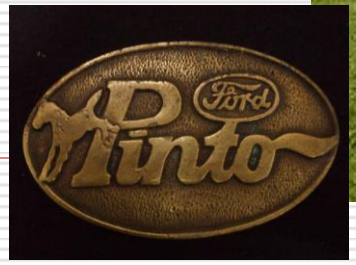
(11ドル＊1,250万台)

陪審評決

補填賠償：280万ドル

懲罰賠償：12,500万ドル

社会的信用失墜、改造コスト



（ジョンソン・エンド・ジョンソン：タイレノール事件対応で社会的信用獲得）

第四象限→第一象限

- 1982年に米国で何者かに毒物を混入されたタイレノール（頭痛薬）が売られ、7人が死亡するという事件
- ジョンソン・エンド・ジョンソン（J&J）は直ちにすべてのタイレノールを回収し、異物を混入できない構造に
- これは危機管理の模範として伝説に

- 1982年9月に、全米を震撼させる「タイレノール」事件が発生
- J&Jの医薬品部門で全米の主力商品だった家庭用鎮痛剤「タイレノール」にシアン化合物が混入され、シカゴを中心に7名が死亡

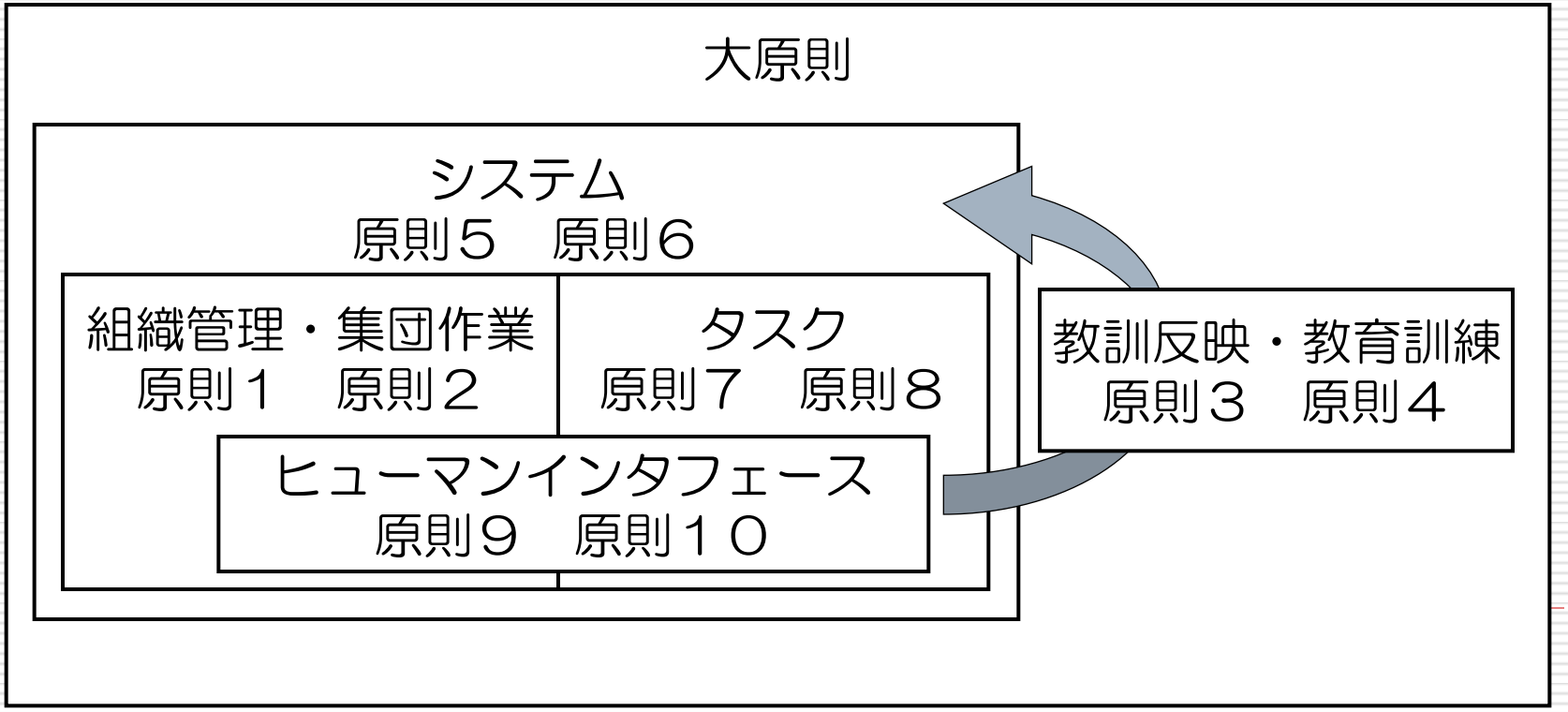
- J&Jは全「タイレノール」商品の回収（**3100万本**）、マスコミを通じた積極的な情報公開、新聞への警告広告の掲載、対策チームの設置など素早い対応（**1億ドルの損失**）
- 陣頭指揮をとった当時のJ&Jバーク会長は、単なる危機管理として対応することに終わらず、「消費者への責任」を第一に考えた体制を策定
- これは、J&Jの企業理念である「我が信条、Our Credo」の第一の責任に立ち返った意思決定

- 事件終結後、J&Jのこの事件における対応は、一般消費者をはじめ政府・産業界からこれまで以上に高く評価された
- 全社員が一丸となった努力の結果、予想をはるかに越える速さで市場を回復

59

ヒューマンファクターの原則1
（原子力学会、HMS部会）

大原則
「安全確保においては、
ハードとソフトの双方による安全防護障壁を考慮に入れた
システムズ・アプローチを実施せよ」



ヒューマンファクターの原則2

組織管理および集団作業
原則１「経営から現場までが一体となって安全管理に努めよ」
原則２「インタフェース設計や教育訓練の工夫により円滑なチーム協調を促進せよ」

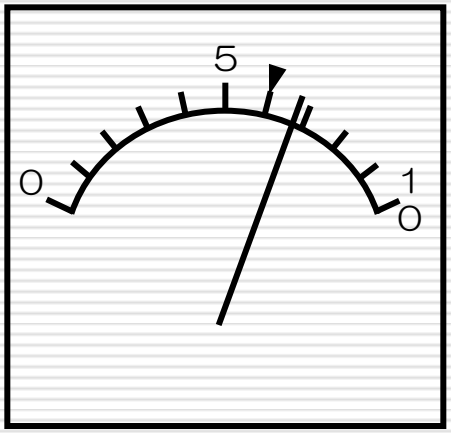
教訓の反映および教育訓練
原則３「エラーの根本原因まで分析し、教訓を活用するシステムを確立せよ」
原則４「実効的な教育・訓練プログラムを用意し、効果を持続させるシステムを確立せよ」

システム設計
原則５「人間中心設計に則り、組織、チーム、人間、認知の順に概念設計せよ」
原則６「システムの安全評価においては人間信頼性を考慮せよ」

タスク設計
原則７「人間、機械の各々に期待する役割と特性を明確にしてタスクを割り当てよ」
原則８「作業負荷が適正範囲になるようにタスク設計せよ」

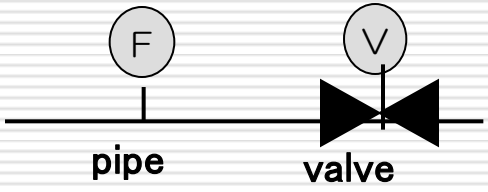
ヒューマンインタフェース設計
原則９「人間の身体能力や作業性に配慮して機器・道具・作業環境などを設計せよ」
原則10「情報の重要度とユーザのメンタルモデルに基いてインタフェース設計せよ」

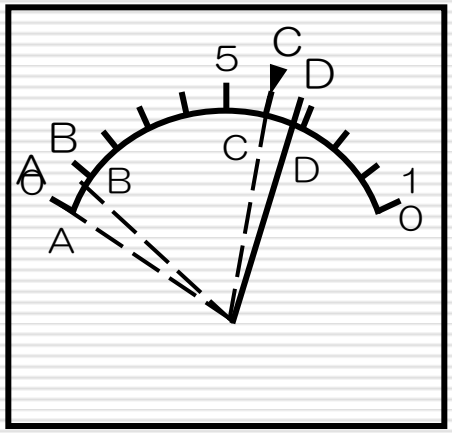
エコロジカルインタフェース
シグナル、サイン、シンボル、 Rasmussen



シグナル

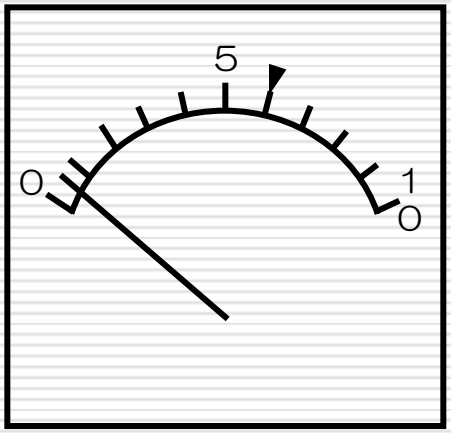
ダイアルノブを回して針を設定指示の点に調節する





サイン

もしバルブが開いており、
　指示値がCならば: OK
　指示値がDならば: 流量調整
もしバルブが閉じており、
　指示値がAならば: OK
　指示値がBならば: メータの校正



シンボル

もしバルブが閉じているのに流量がゼロでないならばどこかで漏洩しているかもしれない

原因別死亡者数

(「反原発」の不都合な真実：藤沢数希著　2012)

対象	死亡者数/年	報道価値	一般の反応
放射能、O157、狂牛病	0-100人	高	パニック
HIV、殺人、熱中症	100人-5,000人	中	社会的問題
交通事故、大気汚染、自殺、喫煙	5,000人-20万人	低	日常茶飯事

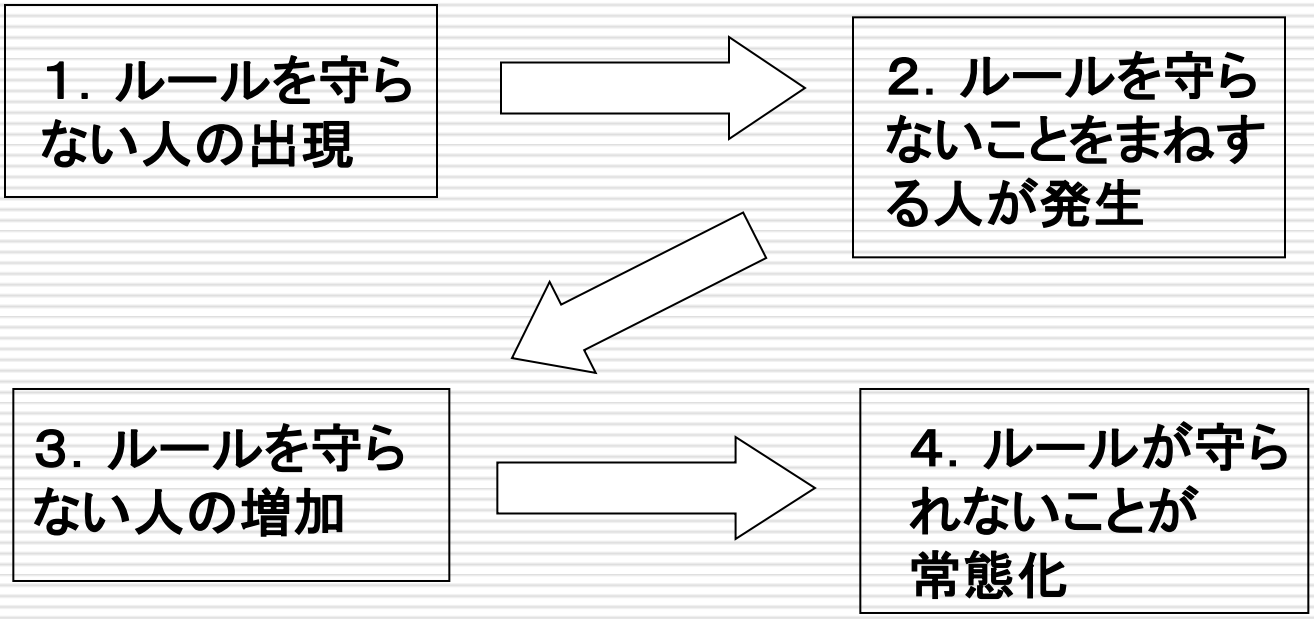
人間の特性-人間の認知特性（参考）

- 環境に存在するものを，他との空間的，時間的，意味的関連性の中で認知
  - 刺激が感覚受容器から神経を伝達して大脳中枢へ至るボトムアッププロセス
  - 知識，文脈，記憶，経験行為，動機などを積極的に利用しながら理解，確認を行うトップダウンプロセス

- 注意機構には以下の特性が知られている.
  - 注意の動揺：注意の集中による認知の明瞭さを一定に保つことは難しい
  - 先入の法則：注意されているものが先んじて意識に入る
  - カクテルパーティー効果

- 認知バイアス：限定合理性
  - ヒューリスティック過程、システム1：感情；経験則と恐怖；類似性の法則
    - 係留、代表性、利用可能性（実例）、情動（良い悪い）単純接触効果
    - 知覚的顕著性 ：関連性，鮮明性、作業記憶の容量制約
  - アナリティック過程 、システム2：理性
    - メンタルモデル ：信念（確証）バイアス 、後知恵バイアス

ルールの形骸化の過程（参考）（破れ窓の理論:アメリカの犯罪心理学者）



- NYの復活：ジュリアーニ市長
- 悪戯書きへの対応

➢ルールを守らない人が出現するのが根本原因だが、その点についての説明無

noblesse oblige

「高い身分または地位には、
勇気、仁慈、高潔、寛大などの徳を備える義務」

- センスと意欲と能力
- 価値観の問題

自分の志を高く保つこと
（恥を知ること）

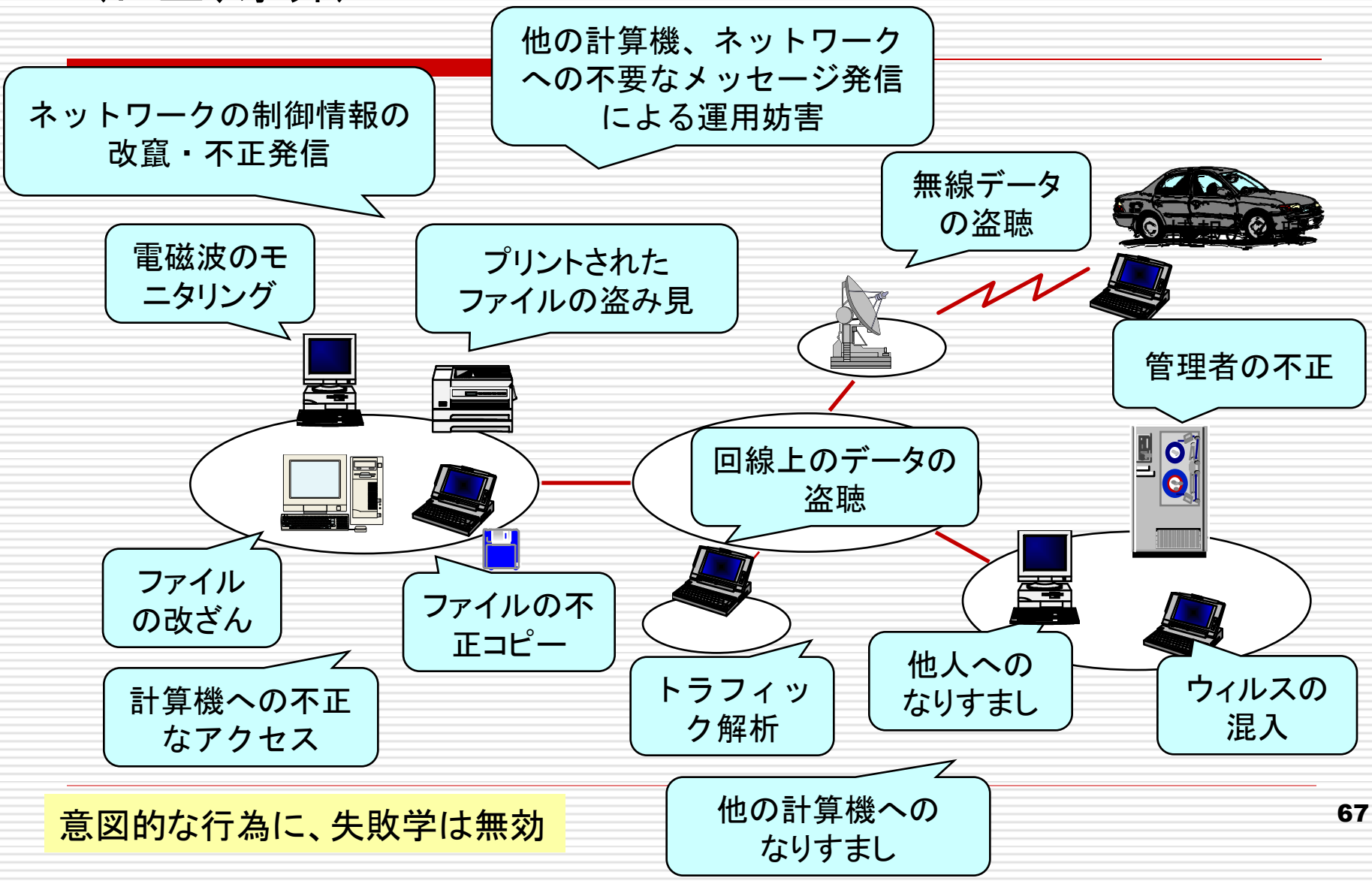
- マズロー
(Maslow,A.H.)
欲求5段階説

自己実現の欲求

**ケビン・ミトニック：欺術（詐欺の話術）
ソーシャルエンジニアリング**

**高信頼性組織、レジリアンスエンジニアリング
の方向性か？**

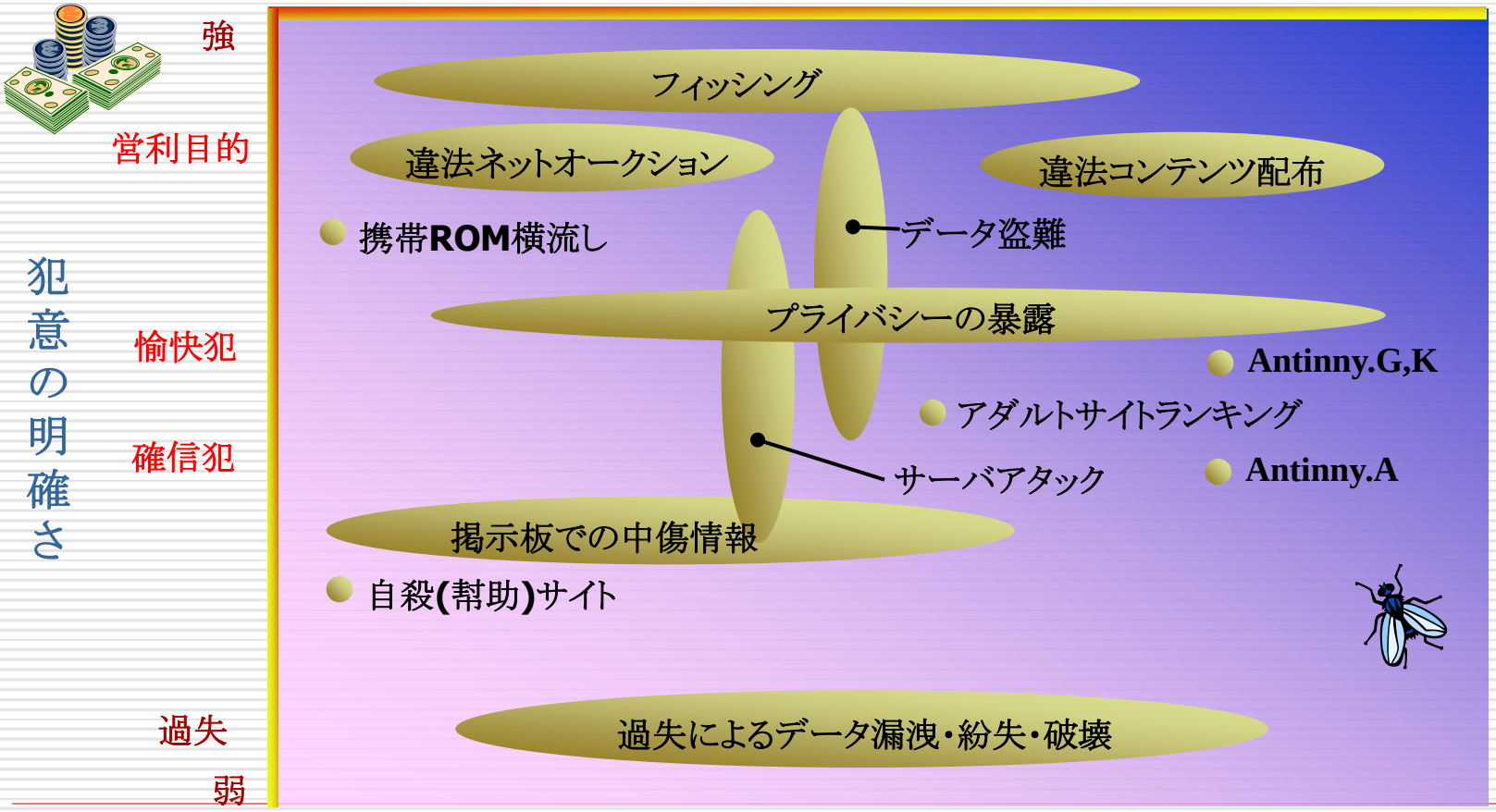
情報セキュリティ脅威の例
（日立、永井）



意図的な行為に、失敗学は無効

ネット社会におけるセキュリティ被害の様相

（日立、荒砥）



心理学の有効な対象は？営利目的には無効？　意図的な行為に、失敗学は無効

リスク評価に関する他分野(航空・原子力)との共通点・相違点

- 共通点
  - システム安全工学のリスク解析・評価手法(ETA,FMECA,FTA等)の適用による対策立案アプローチ

- 相違点(特徴)
  - 脅威の発生論理
    - オープン・分散システムのため多種多様で複雑
    - システム拡張／変更や新しい攻撃の出現等で変化

    ⇒ **モニタリングシステムの整備が重要な分野**
  - リスクデータ(可能性、影響)
    - 悪意の脅威の発生可能性(確率)データの入手困難
    - 影響評価の多様性
      - システム停止、企業イメージ、ビジネス機会喪失

情報システムのリスク分析・評価技法

（日立、永井）

- 定性的手法
  - チェックリスト利用方法
    - 情報資産や利用環境についてチェックポイントを上げたリストを用いて調査分析（通産等の基準・ガイドを参考にリスト作成）
  - 質問表利用方法
    - 職務担当別、階層別に質問表で調査し、脆弱性を洗い出し、回答のウエイト付けと相対評価で優先対策を決定
  - シナリオ分析法
    - 脅威と影響・損失の多岐のシナリオを作成・評価して対応策を示す
  - マトリックス利用法
    - 右図の発生可能性と影響を表現した

    マトリックス表に各脅威を位置づけて評価

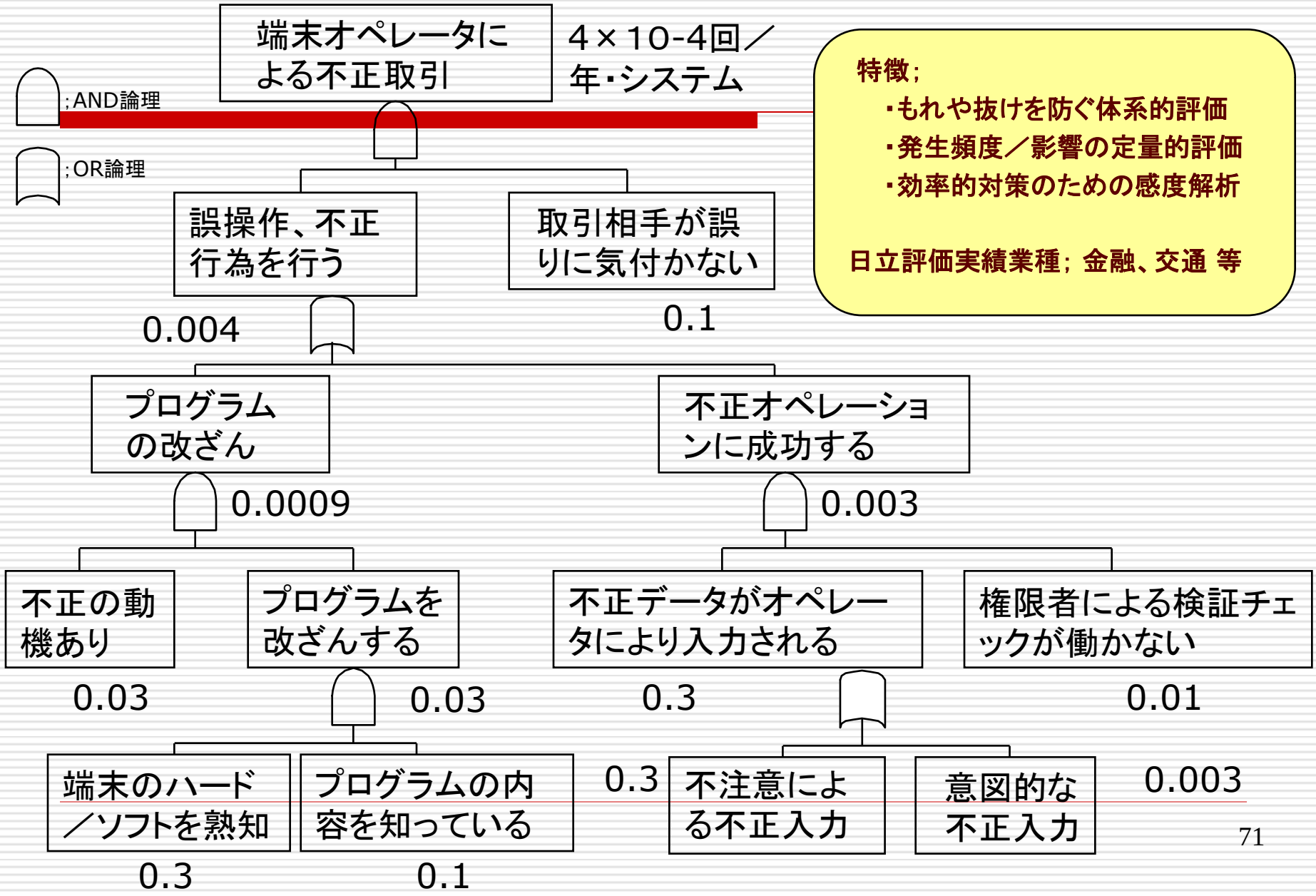
ユーザ影響度＼発生可能性	一般的手段で発生可能	特別な知識が必要	特別なツールが必要
顧客データの破壊	脅威X　リスク大		
顧客データの改ざん			
顧客データの暴露			
⋮		リスク小	脅威Y

- 定量的手法（脅威の頻度×損失額をリスクとしてランク付け評価）
  - ALE(Annual Loss Exposure)法
    - 年間予想損失額ALEを以下のように近似計算して評価

      ALE = F × I；発生頻度F（回/年）を係数化；グレード付けf1,…,fn

      予想損失額I（金額/回）を係数化；グレード付けi1,…,in
  - **FTA法；脅威の発生過程を表現したツリー構造の論理図を作成して解析・評価**

Fault Tree の簡単な具体例 （日立、永井）



特徴；
- ・もれや抜けを防ぐ体系的評価
- ・発生頻度／影響の定量的評価
- ・効率的対策のための感度解析

日立評価実績業種；金融、交通 等

今後必要なセキュリティ対策のアプローチ

【従来のセキュリティ対策 】
✧個別的対策（FW設置，ウイルス対策）
✧事後対策
✧外部攻撃対応中心

【今後のセキュリティ対策 】
✧ポリシー策定による体系的セキュリティ対策
✧予防対策、ライフサイクル全般の対策強化
✧外部だけでなく、内部も合わせた全体対策