2013-7-5学術会議安全工学シンポジウム特別講演

安全設計思想について

向殿政男
明治大学　名誉教授

安全の常識

- 機械設備は劣化等でいつかは壊れるものである
- 人間はいつかは間違えるものである（時には、認知症の人、意識を失う人、悪意の人もいる）
- 組織やルールに完全なものはあり得ない
- 絶対安全は存在しない（リスクゼロはあり得ない）

安全とは何か？

安全の定義

「安全とは，人とその共同体への損傷，ならびに人，組織，公共の所有物に損害がないと客観的に判断されることである」＊

＊）文部科学省：「安全・安心な社会の構築に資する科学技術政策に関する懇談会」報告書(2004-4)

安全の定義
～機械安全での例～

- 「受け入れ不可能なリスクが存在しないこと」
- 「受け入れることの出来ないリスクからの開放」（ISO/IECガイド51）
- 「人への危害又は資（機）材の損傷の危険性が，許容可能な水準に抑えられている状態」
  （JIS Z 8115 デイペンダビリティ（信頼性）用語）

危害（Harm）の定義

- 人体の受ける物理的傷害　若しくは　健康障害

- 財産若しくは環境の受ける害

・情報，組織，企業、社会，心・・・等の受ける害

リスク（Risk）の定義

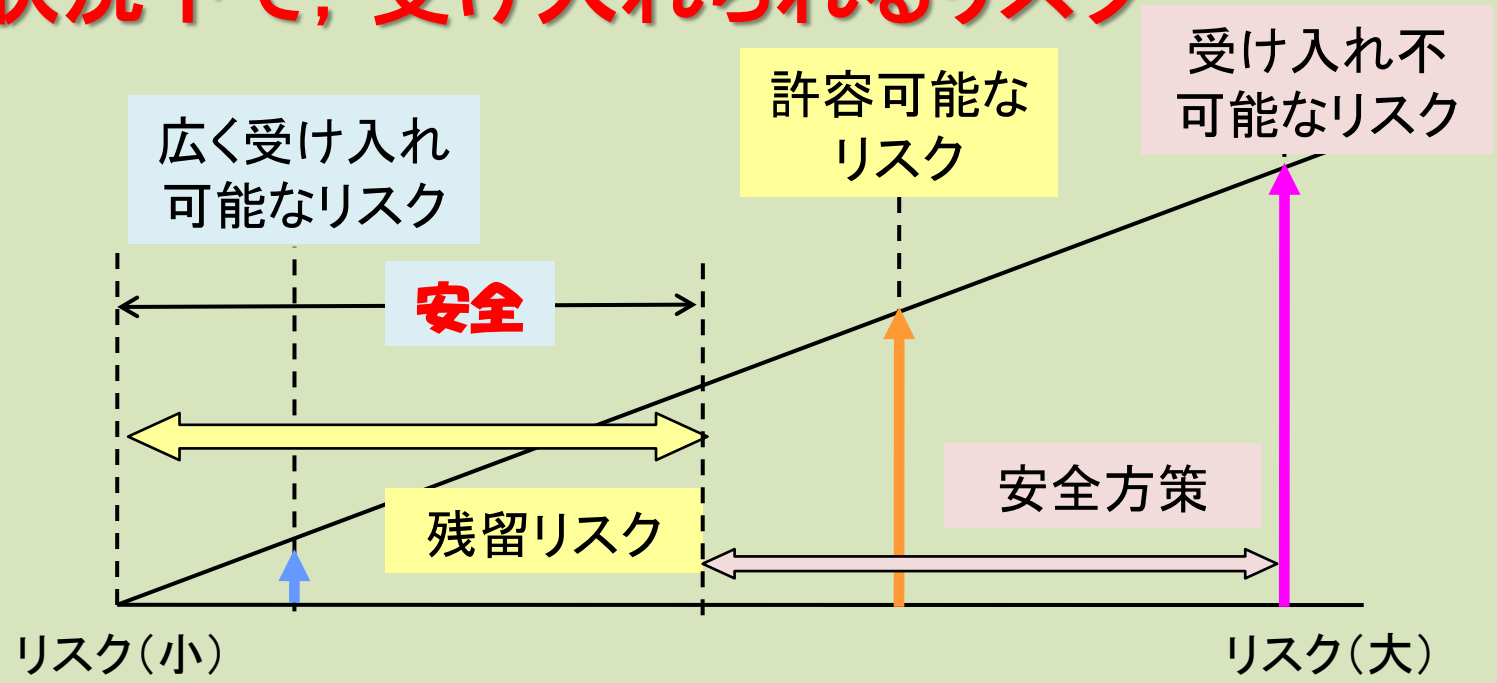
- **リスクとは？**

危害の発生する**確率**及び
危害の**ひどさ**の
組み合わせ

- **安全性確保の手法**
  - **確率を下げる**・・・信頼性を確保することで安全を確保する：信頼性技術
  - **ひどさを下げる**・・・構造で安全を守る：安全性技術

許容可能なリスク（Tolerable Risk）の定義

- その時代の社会の価値観に基づく所与の状況下で，受け入れられるリスク



- 安全と言っても、**残留リスク**は、存在している！

どこまでやったら安全か

～安全目標～

安全の判定基準

- コストベネフィット基準
- 危険効用基準
- 消費者期待基準
- 標準逸脱基準
- ・・・・・
- →安全目標、安全基準、技術基準

安全目標とは

- 目指すべき安全水準の目標**（努力目標）**
- 満たすべき安全水準の基準（→構造基準、性能基準、リスク基準）**（最低基準）**
- 国の基準等は、最低基準である。これを満たすのは当たり前で、危険源を網羅し、いかに安全レベルを高めるかが課題。最終責任は事業者にある。
- 技術基準のあるべき姿：**State of the Arts**（常に最新の知見に基づき見直すこと）

例：放射線における安全基準

- 自然界では、世界的は平均では、**年間2.4 mSv/年**の**自然放射能**が存在するという
- 被ばくした放射線量が、**100 mSv/年**未満では、放射線がんを引き起こすという**科学的な証拠はない**
- 安全度を高くとって、1/100である**1msv/年**を、一般公衆が1年間にさらされてよい**人工放射線の限度**（国際放射線防護委員会:ICRPの勧告）としている（自然放射線やX線検査などでの医療被曝は除く）。
- ICRPは、**緊急時**は**1～20msv/年**の放射線は、問題ないとしている
- **医療法**施行規則第30条の27(許容線量)による値では、年間(全身)の最大許容被曝線量として、**50mSv/年**と定めている

安全目標の比較例

～学術会議安全目標小委員会で検討中～

- 死亡／生涯の確率で比較をする
- BA(最も低い許容可能リスクの確率)とUA(最も高い許容可能なリスク)のペアで考える
- 案：BAを10^{-6}／生涯、UAを10^{-3}／生涯
- 0.1%ルール：リスクが0.1%以下ならば許容する

（1／生涯の0.1%= 10^{-3}／生涯,14歳の死亡率の0.1%水準=5× 10^{-6}／生涯：10^{-5}／年～10^{-8}／年）

- 保険:被害のひどさを金で換算し、組合せを掛け算で解釈する
- 船:死亡を1億6700万円（HSE:1,336,800ポンド)

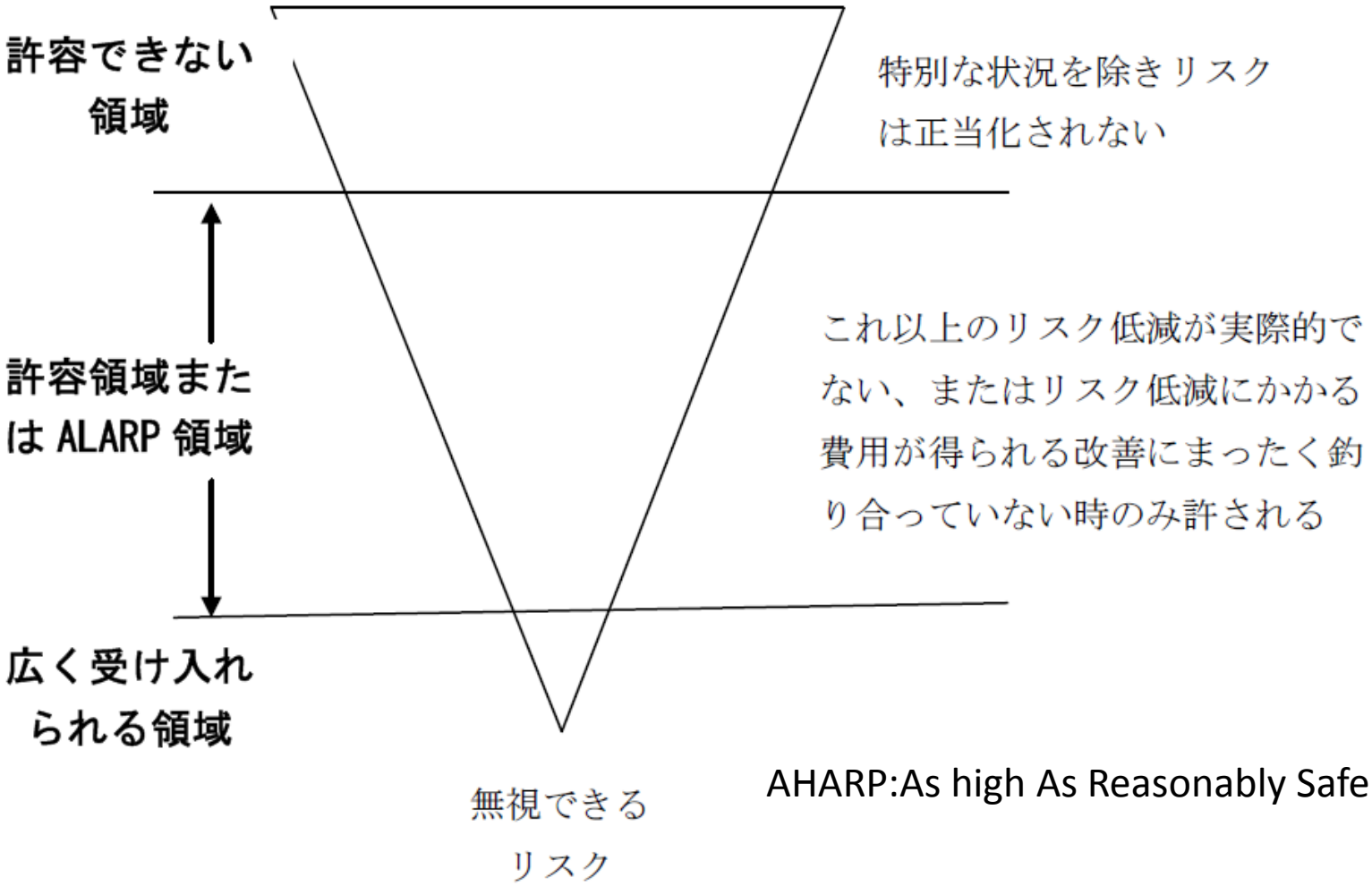
安全目標決定で気になるポイント

- ベネフィット、コストをどのように考慮するのか？
- 死亡以外の危害をどのように配慮するのか（傷害の度合い、経済的損失、心理的ストレス、住民の移住）？
- 安全以外の他のリスクや価値観とのコンフリクトをどのように配慮するのか？
- ごく稀で、極めて被害の大きなリスクに対してどのように考えるか？
- 信頼されていないもの、不確定なものに対すてどのように考えるのか(予防原則)
- 数値だけで比較をするのは如何なものか？
- ・・・・・

安全目標は条件によって変わる

- 時代によって変わる、社会の価値観によって変わる
- 分野によって変わる（製品、食品、医療、・・・・）
- システムによって変わる（止められるか、止まれば安全か、能動的安全、受動的安全）
- 立場によって変わる
  - 利益を受ける側と被害を受ける側
  - 専門家と素人(非専門家)
  - 個人で受けるリスクと集団で受けるリスク
  - 自ら行うか人に強制されるか（主体的に選択できか、与えられてしまうか）
- できるだけ共通の部分を探そう！

ALARP (As Low As Reasonably Practicable)の原理



AHARP:As high As Reasonably Safe

幅を持った安全基準の提案

- 危険側の高いリスク値（UA）と安全側の小さなリスク値（BA）の幅を持たせて安全基準を決める
- BA以下は安全としてこれ以上のリスク低減は追求しない
- リスクがBAを超えたら警告を発する
- リスクがUAを超えたら発売禁止とする
- BAとUAの範囲内で、企業はリスクの低減の度合いで安全の競争をしてもらう

安全設計思想

安全確保のステージ

- **未然防止**方策
↓(予防安全：設計安全、寿命予測)
- 事故を起こさない
↓(運用安全：保守・点検・修理)
- 危害のひどさを下げる
↓（衝突安全：拡大防止、再稼働）
- **再発防止**対策（事後安全）

(事故調査：原因究明)

・過去の歴史に学べ

・事故データを収集せよ

・緊急時を考えておけ

・全ステージを総合的に考えておけ

→正常な終焉（死に方設計）**廃棄**

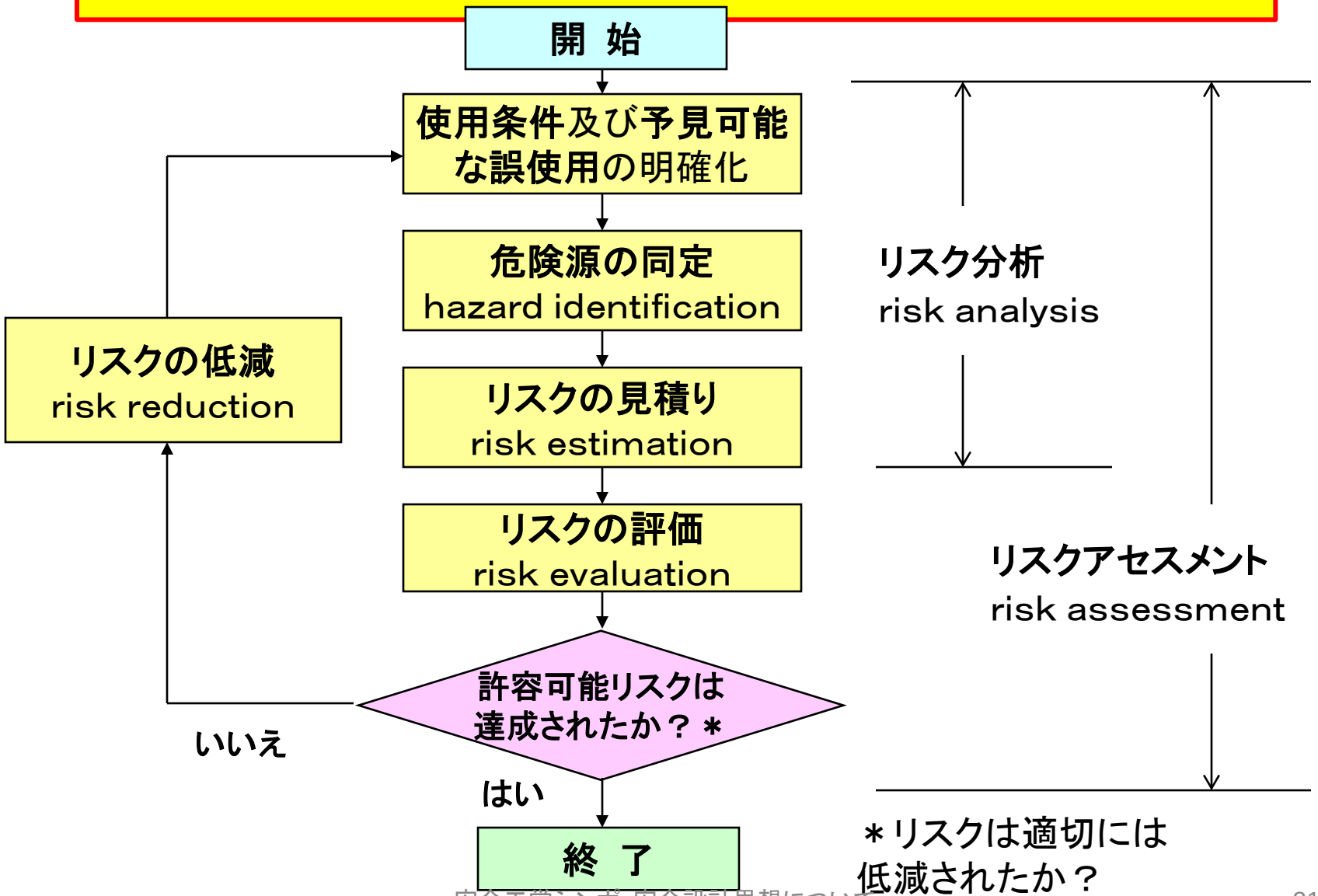
安全設計おける常識
～安全設計思想～

- **事後より事前に**（再発防止より未然防止）
- **下流より上流で**（安全装置より安全設計）
- **被害を受ける側より被害を与える側が**（人間の注意の前に施設・設備の安全化）
- **力からの小さいものより力の大きなものが**（消費者より企業が、現場よりトップが）
- ・・・

優先して方策を施すのが原則

リスクアセスメントの手順

（ISO/IECガイド51より）



スリーステップメソッド

～リスク低減には順番がある～

（1）本質的安全設計によるリスクの低減
（2）安全防護対策(安全装置等)による
　　リスクの低減
（3）使用上の情報の提供による
　　リスクの低減
↑設計製造側の役割

↓作業者の役割

＊使用上の情報に基づき、教育、訓練、組織・体制・管理、個人防具による
リスクの低減

本質的安全設計

（1）はじめから危険源が無いように設計せよ

（2）危険源のエネルギー等を下げて事故が起きても危害の酷さを小さくするように設計せよ

（3）危険源に人間が近づかなくて済むように設計せよ

（4）修理等の非定常作業をしなくて済むように信頼度高く設計せよ

安全設計の考え方の例

- 信頼性と安全性の概念
- 本質的安全設計
- 構造安全と確率安全
- フェールセーフ
- フォルトトレランス
- フールプルーフ
- フェイルソフト
- フォルトアボイダンス

- インターロック
- フォルトレジスタンス
- タンパレジスター
- 冗長性，多重性
- 多様冗長、独立性
- 機能安全
- ・・・・

安全設計における視点

- 機能を如何に維持させるか・・・信頼性の問題
- 安全性を如何に確保させるか・・・安全性の問題
- 科学的根拠（物理的、化学的、数理的根拠）に基づく客観性を重視すること
- 科学と価値（安全と安心）の関係を考慮すること
- 未然防止を第一義とすること
- 安全学からの視点：技術的、組織的、人間的側面から総合的に対応すること
- 安全学からの視点：ライフサイクル全体のわたり体系的に対応すること

安全設計の考え方

構造安全

- 機械設備が故障しても安全側になる･･･フェールセーフの構造
- 人間が間違えても大事には至らない･･･
  フールプルーフの構造

（コンフリクトはあり得る）

確率安全

- 信頼性を上げることで安全性を実現する･･･
  多重系、フォールトトレランス、多重防護の構造、数量化、機能安全

両者の融合が必須

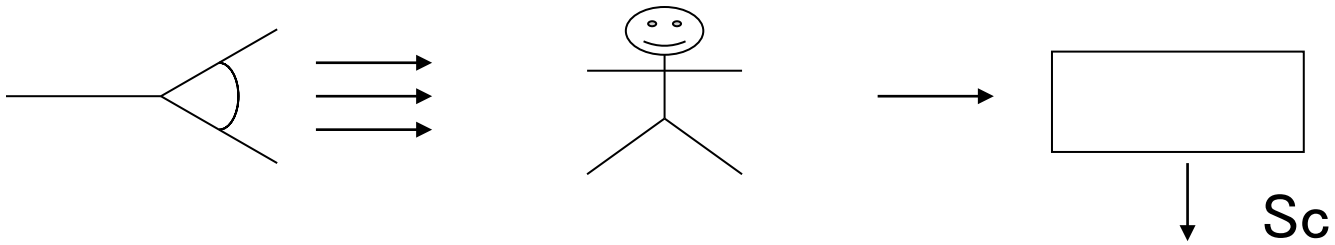
例：危険検出型と安全確認型

＊安全なシステムの作り方

1．危険検出型－－危険であることを検出して、この危険情報により作業を止める／回避する(ない時は続行)

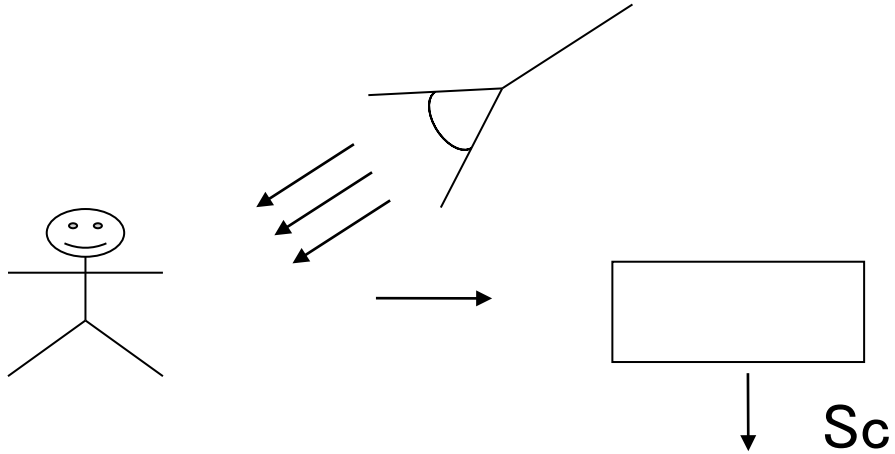
2．安全確認型－－安全でることを確認して、安全情報を受けているときだけ作業を続行する(ない時は実行しない)

Two types of light beam sensors



Safety : Absence of human

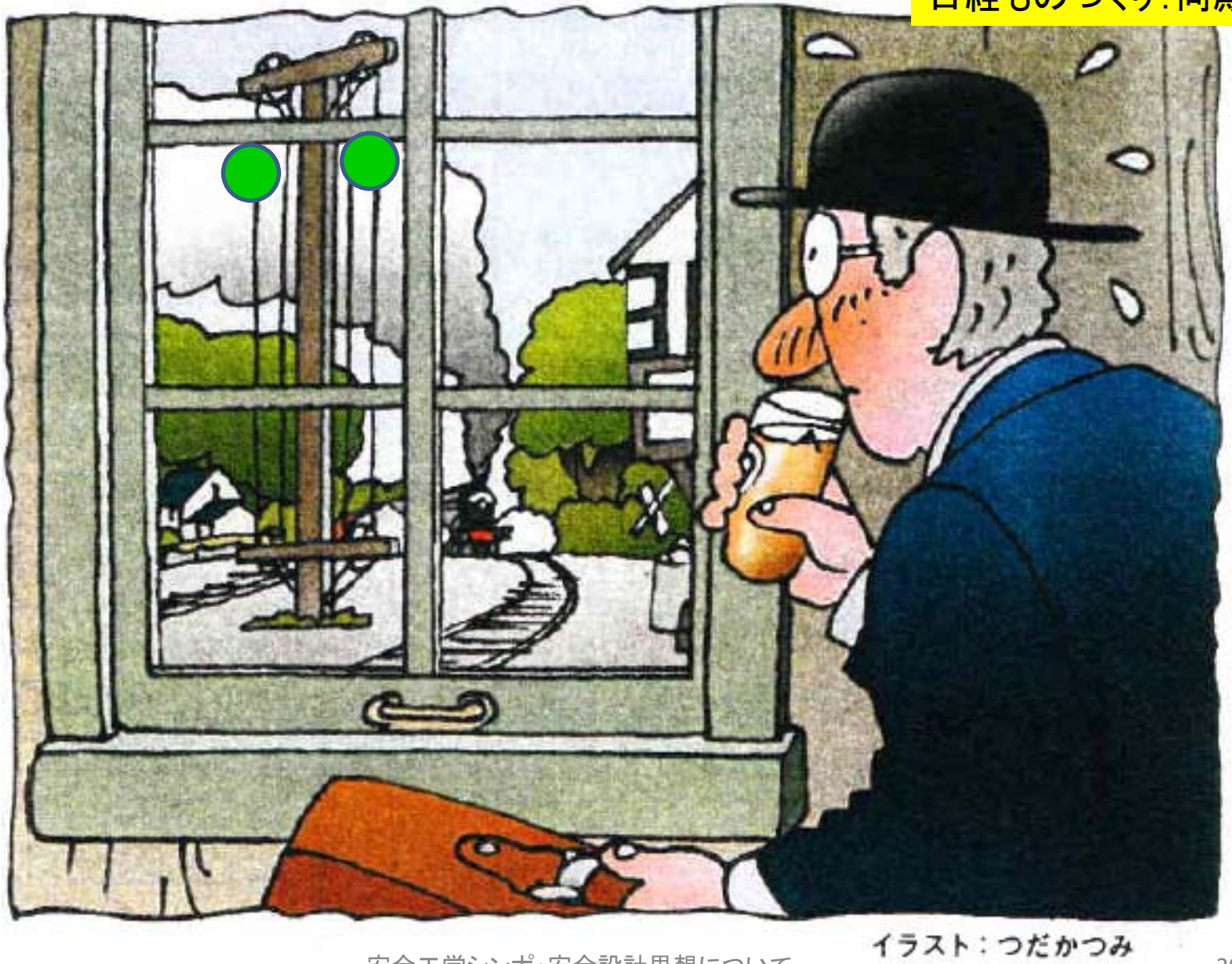
(a) Transmission type



Safety : Presence of human

(b) Rader type

ハイボールの原理
日経ものづくり：向殿



例：長期使用に対する望ましい対応策

メーカのこころへ：未然防止方策

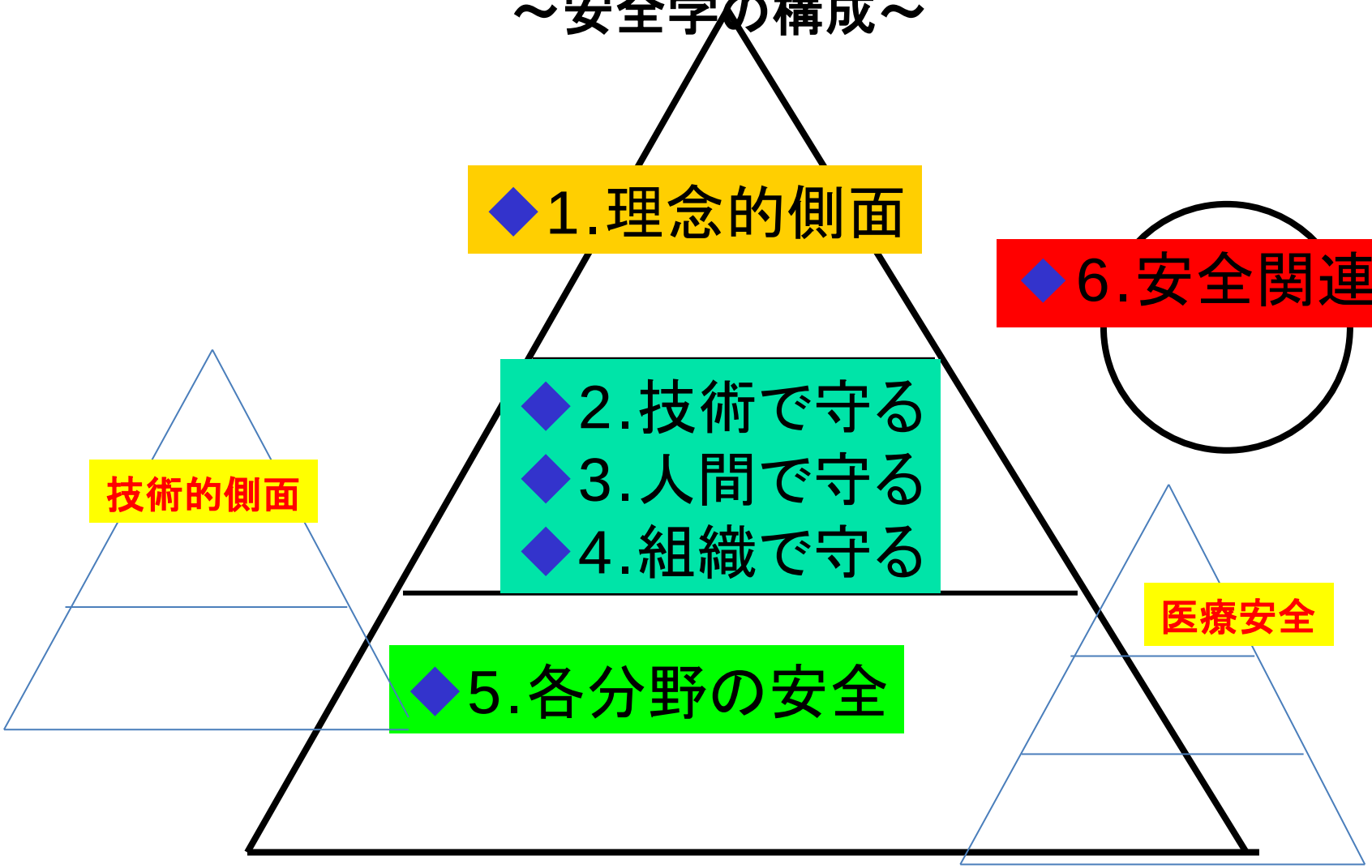
- 壊れ方(死に方）設計をやれ
- 劣化したら止まる(動かない、電源が入らない)設計をやれ
- 寿命と共に使えなくなる機能（自動停止機能）
- 劣化したら前以て分かる、知らせる設計をやれ
- 弱いところを前以て作っておく設計
- 敢えて壊してみる実験をせよ（加速劣化試験）

安全学と安全設計思想

安全学の構築

- 安全は、**技術、人間、組織〔仕組み〕**を総合して初めて、実現される
- 安全に関する学問は，**技術的側面**だけでなく**人間的側面，社会的側面**を含めて，安全工学や安全科学を含んだ更に広い学問体系である**安全学**として確立
- **安全学**は、**自然科学、人文科学、社会科学を包含した文理融合型、領域横断型の学問体系**
- ただし、それを支える**理念(安全哲学)**がなくてはならない

◆安全曼荼羅
～安全学の構成～



安全思想の分類

- 安全哲学
- 利用する立場(個人、消費者、作業者、社会、等)の安全思想:安全受容思想、**安全文化**
- 管理・規制する立場の安全思想:**安全管理思想**、安全規制思想、法理念　Regulatory Science
- 作る立場の安全思想:**安全設計思想**

まとめ

安全における難しさ

～安全学からの視点～

- 適切なリスクの判断は難しい（リスクは小さければ小さいほど良いというものでもない：少しぐらいのリスクは、あった方が良い場合が多い）
- 正当にこわがることはなかなか難しい

- 安心するとかえって危険
- 人間は、痛い目に遭わなければ、対応しない（転んだ後の杖）
- 災害は忘れたことにやってくる（安全は風化する）
- 事故が起きた時の対応を事前に考えておけ
- 安全の責任は、事前に分かっていることを何処まで対応したかの責任

安全と価値観

- 安全と安心は明確に分けるべきである
- 安心には価値観が関与しており、科学（安全）と価値観（安心）は分けて考えるべきである
- 科学的事実を明らかにし(安全）、それを受け入れるか否かは、民衆が判断する(安心)
- 特にリスクの高い影響の大きなシステムに関しては、安心を得られない場合には、いくら科学的に安全であっても、作らないという判断はあり得る

安全・安心の方程式

＊**情報の公開と透明性**が信頼を生む

- **リスクコミュニケーションの重要性**
- **安全が実現されている＋実現している人間・組織を信頼している→**

安全×信頼＝安心＜1

安全の基本は情報公開である

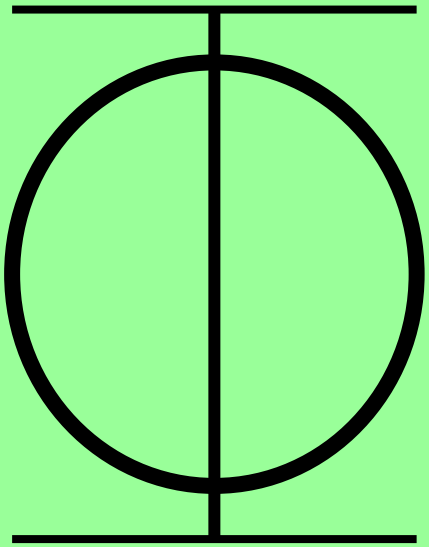
- 残されているリスクが最悪を考えてどのようなものであるかを事前に情報開示しておくこと
- 安全を合理的に、客観的に判断するためには必須のこと
- 良い情報も悪い情報の公開：隠さない
- 民衆がパニックに陥るだろうからとか、理解できないだろうからという理由で、残留しているリスク情報を開示しないというのは、正しくない。
- ただし、我々民衆も、冷静にリスクを判断する科学リテラシーや安全文化を身につける必要がある。それが正しく怖がるための基本である。

新しい安全の文化創造へ

～より高度な安全の実現に向けて～

- 安全思想の体系化
- 安全学の確立
- 技術者倫理の確立
- 企業トップの安全意識の向上・安全の価値を重視した経営
- 消費者力の向上
- 報道力の向上
- 安全を支援する社会制度の確立（税制・保険・認証・投資等の活用）
- 大学における安全教育・安全/保全技術者の育成と待遇改善
- 安全文化の向上
- 日本は、安全・安心を基本とした国づくりへ(Japan is back)

安全はΦ型で！



目指すべきは
Φ型

・大局的、包括的、総合的観方ができること
・専門分野を一つ持っていること
・真理は0と1の間にあり