

2017-5-29 営業秘密保護推進研究会  
サーバーリスクマネジメント人材育成シンポジウム  
東京工業大学キャンパスイノベーションセンター 特別講演

# 安全学のすすめ

—IoT時代の事業・製品・セキュリティーを  
安全性の共通理念で横串にする—

明治大学名誉教授  
向殿政男

**機械安全・製品安全における  
安全の確保  
～経営者の役割～**

# 企業のトップに課せられている 三つの安全

- 顧客の安全・・・製品安全
- 従業員の安全・・・労働安全・機械安全
- 企業体の安全・・・経営安全

の三つをすべて理解し、率先して取り組まなければならない役割がある

\*そのためには、理念を明確にして、率先して、  
(1)体制・仕組みを作り、(2)施設・設備を安全化し、  
(3)人材育成すること  
が必須

# 企業の競争力は安全にあり

- 企業は、社会の中で、持続的に存続すること、企業価値の向上を目指す
- 安全は利潤を生み、競争力の源泉である
- **リスクマネジメント**(金融、経営、品質、環境、安全等の各種のリスクを組織経営の全体的視点で総合的、統一的に対応する)において安全の価値を最も重視する時代(**トップの力: 経営層**)
- **リスクアセスメント**(**現場の力: 実務層**)

# 経営層と実務層の橋渡し

## リスクマネジメントについて

- 経営層が組織的にリスクを管理することであり、いろいろなリスクを対象としている。安全はその中の一つ
- リスクマネジメントは、価値判断を生み出す

## リスクアセスメントについて

リスク分析(risk analysis:使用条件の明確化、危険源(ハザード)の同定、リスクの見積もり)とリスク評価(risk evaluation)

- リスクアセスメントには、現場レベル(設計段階、設置・生産ライン段階、作業現場段階等)に重きがある

両者をつなぐ人材の存在は必須:安全人材育成(安全資格者制度、……)

# **労働安全衛生法における事業者と 労働者との間の管理者**

- **総括安全衛生管理者(工場長等がなる),**
  - 安全管理者
  - 衛生管理者
- **安全・衛生推進者**
  - 産業医(医師)
- **作業主任者**

# リスクアセスメントにも階層がある

- 経営層（リスクマネジメント）：安全への投資判断（安全はコストではなく投資である）

↑

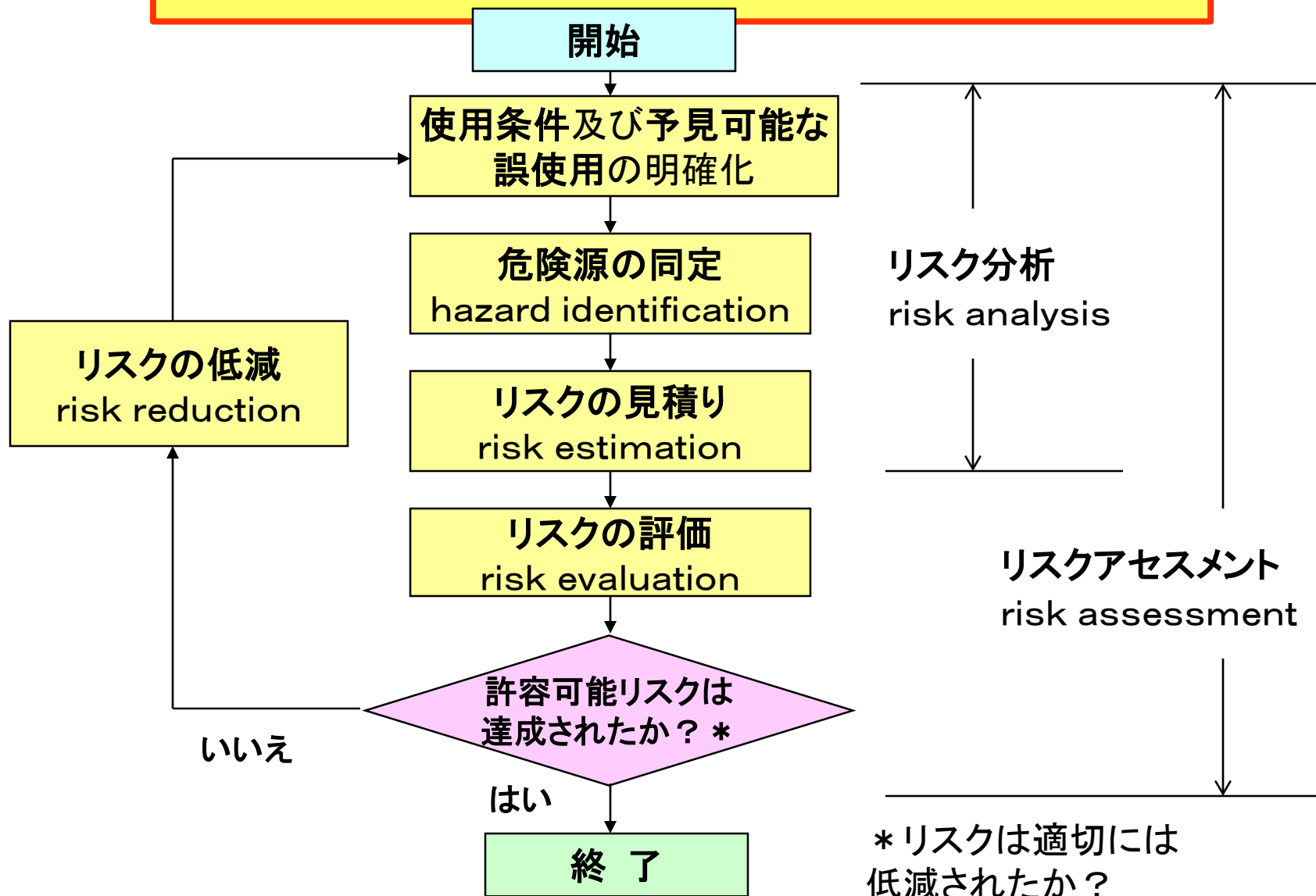
管理者（繋ぎ人材）

↓

- **設計**のリスクアセスメント
- **製造**ライン・インテグレータのリスクアセスメント
- **現場**のリスクアセスメント

# リスクアセスメントの手順

(ISO/IECガイド51より)



# 国際的な安全の定義

- 「許容不可能な**リスク**がないこと」
- 「許容することが出来ない**リスク**からの解放」(ISO/IECガイド51)
- **許容可能なリスク**:「現在の時代の社会の価値観に基づいて、与えられた状況下で、受け入れられるリスクのレベル」

# スリーステップメソッド

(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**

**\* 訓練、個人防具、組織・体制・管理  
によるリスクの低減**

# 国際安全規格の階層化構成



## 機械類の安全性—基本概念:一本化

(一般設計原則規格 (ISO 12100))  
(リスクアセスメント規格 (ISO 14121))

**A**  
基本安全規格:  
全ての規格類で共通に利用できる  
基本概念,設計原則を扱う規格

インタロック規格 (ISO 14119)  
ガードシステム規格 (ISO 14120)  
システム安全規格 (ISO 13849-1)  
安全関連部品規格 (ISO 13849-2)  
安全距離規格 (ISO 13852)  
非常停止規格 (ISO 13850)  
突然の起動防止規格 (ISO 14118)  
両手操作制御装置規格 (ISO 13851)  
マットセンサ規格 (ISO 13856)  
階段類の規格 (ISO 14122)

**B**  
グループ安全規格:  
広範囲の機械類で利用できる  
ような安全, 又は安全装置を扱  
う規格

電気設備安全規格 (IEC 60204)  
センサー一般安全規格 (IEC 61496)  
センサ応用規格 (IEC 62046)  
機能安全規格 (IEC 61508)  
スイッチ類規格 (IEC 60947)  
EMC規格 (IEC 61000-4)  
トランス規格 (IEC 60076)  
防爆安全規格 (IEC 60079)

**C**  
個別機械安全規格:  
特定の機械に対する詳細な安全要件を規定する規格

製品例: 工作機械, 産業用ロボット, 鍛圧機械, 無人搬送車, 化学プラント, 輸送機械など

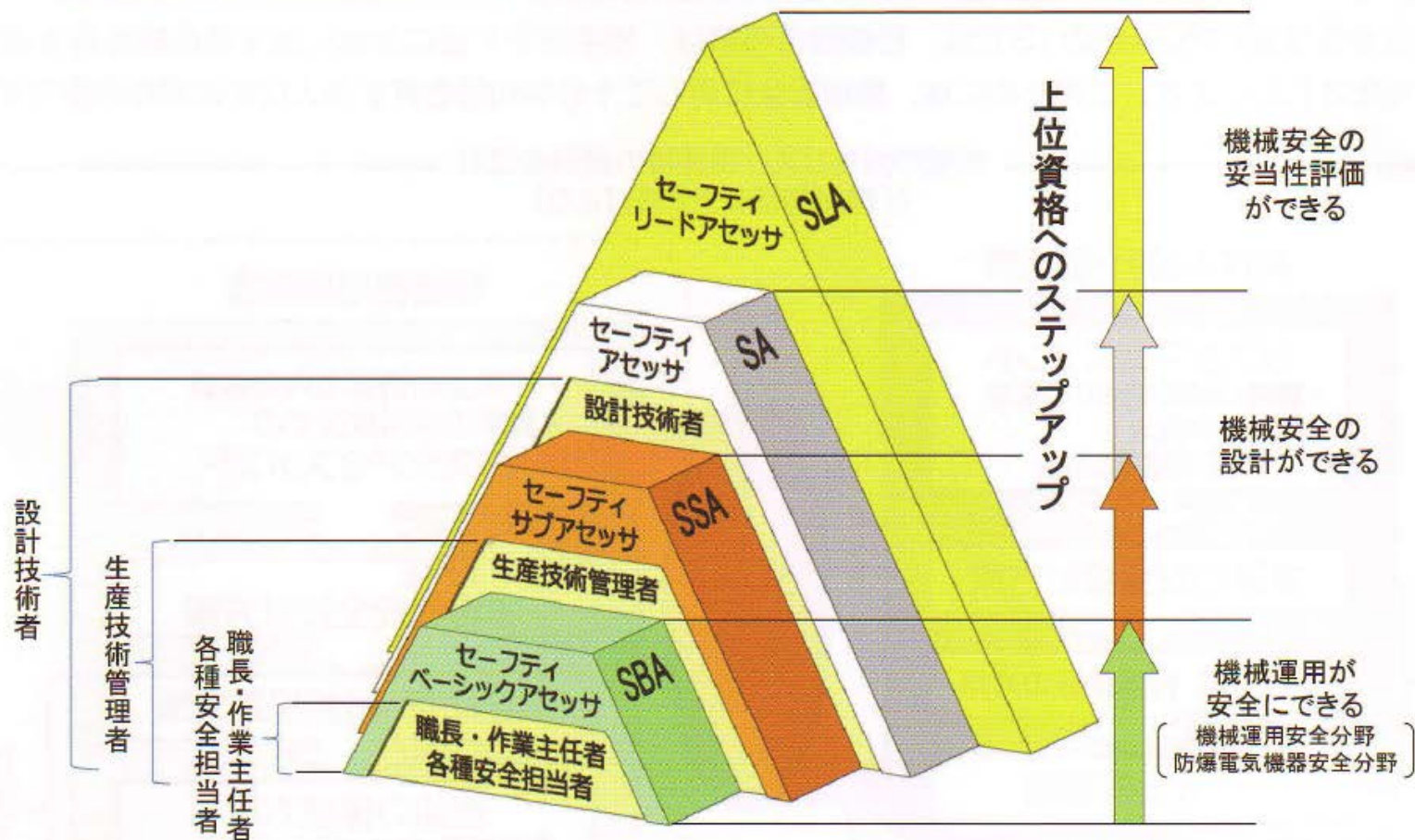
# R-Map (松本浩二氏の資料)

発生頻度

|   |                                            |              |           |      |              |            |              |
|---|--------------------------------------------|--------------|-----------|------|--------------|------------|--------------|
| 5 | (件/台・年)<br>10 <sup>-4</sup> 超              | 頻発する         | C         | B3   | A1           | A2         | A3           |
| 4 | 10 <sup>-4</sup> 以下<br>～10 <sup>-5</sup> 超 | しばしば<br>発生する | C         | B2   | B3           | A1         | A2           |
| 3 | 10 <sup>-5</sup> 以下<br>～10 <sup>-6</sup> 超 | 時々<br>発生する   | C         | B1   | B2           | B3         | A1           |
| 2 | 10 <sup>-6</sup> 以下<br>～10 <sup>-7</sup> 超 | 起りそうに<br>ない  | C         | C    | B1           | B2         | B3           |
| 1 | 10 <sup>-7</sup> 以下<br>～10 <sup>-8</sup> 超 | まず<br>起り得ない  | C         | C    | C            | B1         | B2           |
| 0 | 10 <sup>-8</sup> 以下                        | 考えられ<br>ない   | C         | C    | C            | C          | C            |
|   |                                            |              | 無傷        | 軽微   | 中程度          | 重大         | 致命的          |
|   |                                            |              | なし        | 軽傷   | 通院加療         | 重傷<br>入院治療 | 死亡           |
|   |                                            |              | なし        | 製品発煙 | 製品発火<br>製品焼損 | 火災         | 火災<br>(建物焼損) |
|   |                                            |              | 0         | I    | II           | III        | IV           |
|   |                                            |              | 危 害 の 程 度 |      |              |            |              |

厚生労働省  
機械安全教育対象者

SA/SBA資格者



セーフティアセッサ資格認証制度について

# IoT時代の安全性とセキュリティ

# IoT時代が新しい社会を切り開く

- \* 技術と人間と組織・環境とがお互いの**情報共有して協調**できる時代へ (**繋がる時代へ**)
- \* ICT技術の進展でそれが可能になってきた(センサー技術、インターネット技術、AI技術、ビッグデータ技術、クラウド技術、……)
- \* 第4次産業革命？
- **Industry 4.0**を主導する**ドイツ**
- **Industry of the Futur**を推進する**フランス**
- **Connected Industries**を目指す**日本**
- ...

# 例：生産工場の現場も変わる

例えば、

- 人間からバイタルデータやRFID等で個人の体調、経歴、能力等を発信することができる
- 機械・設備側から、自分の状況の発信と共に、使用者等人間に対して、相手の状況に応じて知的に対応することができる
- 組織・制度・環境等から機械設備、使用者等に情報提供して、総合的に判断して管理することができる

⇒生産性の向上、効率化、柔軟性向上、働き方改革、労働災害の減少、...

# デジタル情報でモノと人と環境が 繋がる世界のリスクとは？

- 情報空間(論理)と物理空間(物理)が人間空間(生体、感情、心理、倫理、思想・文化)とが繋がる世界
- 人の命に結び付く事故は、エネルギー等に基づく**物理的現象**。サイバー空間の脅威は、**情報の世界**。両者が**つながると、サイバー空間の脅威が人間生命に直接関係してくることになる**
- 「人の命や身体に危害を及ぼす製品の危険源」と「サイバーセキュリティ脅威」を具体的に紐づけられないと意味がない
- サイバーフィジカルシステム(CPS)として取り扱うべき
- 事業リスク、人の命や身体を毀損する製品リスク、IoT情報セキュリティリスク等の管理が、シームレスに繋がってくるという事実

# 新しい安全設計思想が必要な時代

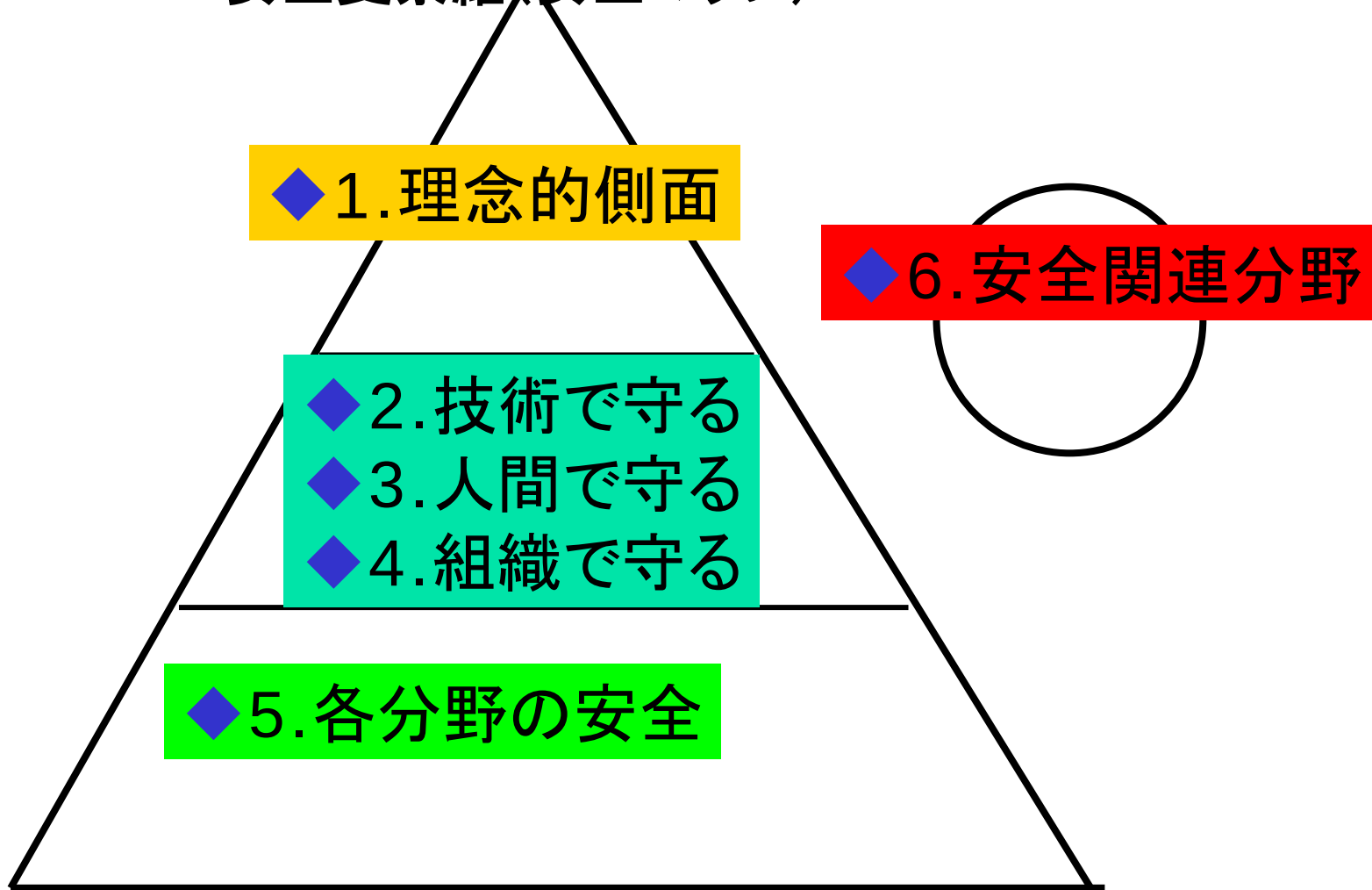
- 論理の世界(サイバー空間)と物理の世界(モノの世界)と心理の世界(人間の世界)は、そう簡単に結びつくのか？
- サイバー**セキュリティ**の専門家は、人間の生命が物理的に脅かされる**セーフティ**(安全)の世界を知らなければシステムの設計できないことになる
- 繋がることによるリスクの発生！⇒  
経営者にとっての新しいリスク
- 経営者も現場もこのことを十分に理解していない！

# 安全学について

# 安全学への動機づけ

- 各分野の安全は、他の安全の分野に学べ
- 他の安全分野に学ぶには、その内容、やっていることの意味が理解できなければならない
- そのためには、まず、安全の用語の統一をして、お互いに話が通じるようにしなければならない
- 安全に共通する部分や共通概念を統一して体系化、標準化する必要がある⇒安全学
- その共通の下で、自分の分野を掘り下げ、どこが異なり、どこに特徴かを知って、初めて他の安全分野に学ぶことができる

# ◆安全学の観点から ～安全曼荼羅(安全マップ)～



| 安全の構造     | (製品や機械の) 安全性             | サイバーセキュリティ                 |
|-----------|--------------------------|----------------------------|
| 何から(危険源)  | 故障、ヒューマンエラー、自然災害         | (人、組織、国の) 悪意、脆弱性           |
| 何を(対象)    | 人命(身体傷害、健康障害)            | 情報(漏洩、改ざん、完全性)             |
| 何によって(対策) | 技術(機械安全)、制度、人            | 技術(暗号)、システム、人              |
| 誰が(責任者)   | 国(各省庁)、企業経営者、管理者、技術者、作業者 | 国(含む:警察)、企業経営者、管理者、技術者、運用者 |
| 何のために     | 災害防止、企業価値向上              | 機密保護、財産保護、企業価値向上           |
| 何の名の下に    | 人命尊重                     | 社会の安定                      |

# 安全は総合的な学問

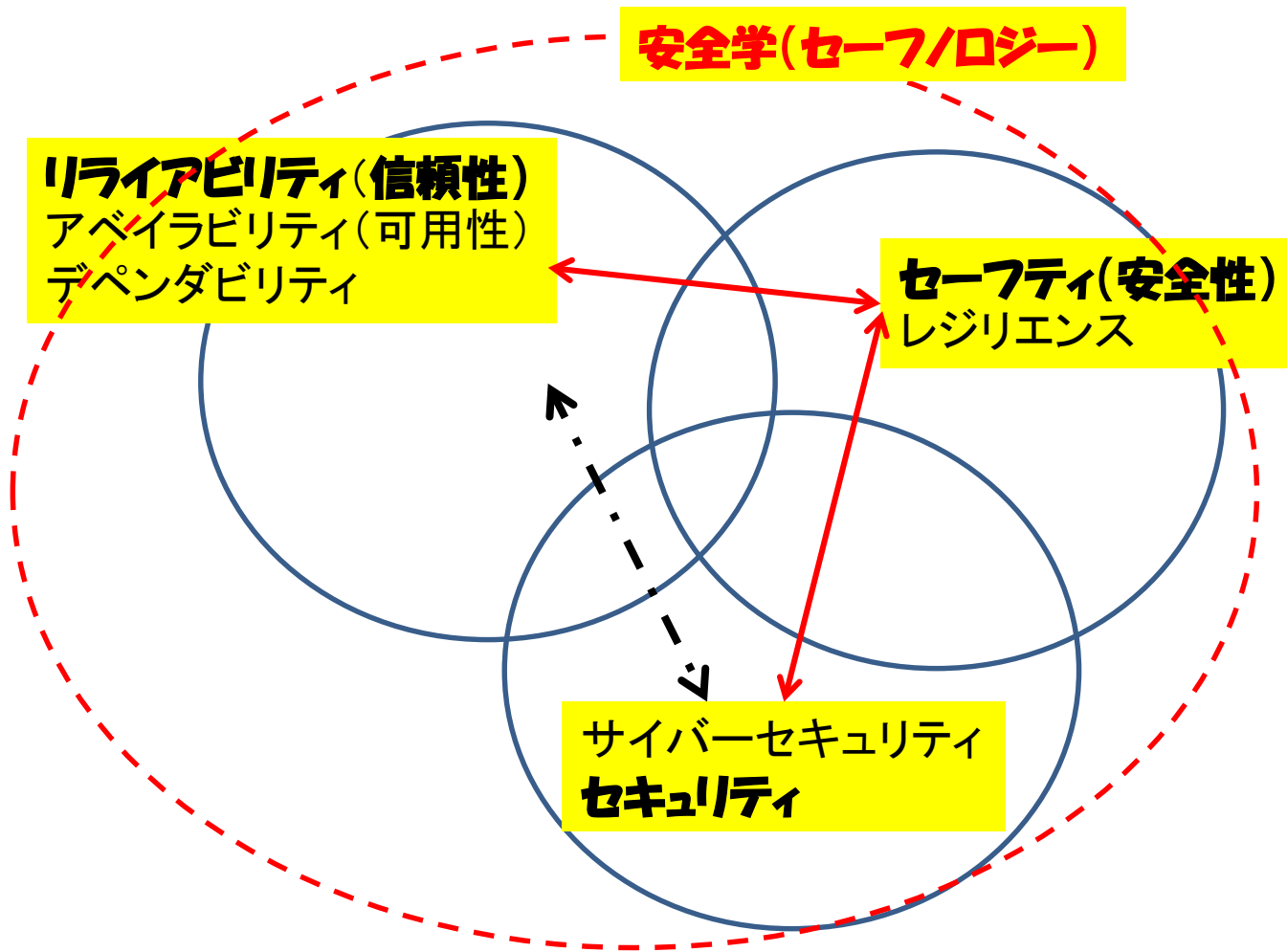
- 安全は総合的な学問である(安全学:人間的側面、技術的側面、組織的側面:体系的、総合的な視点と取り組みが必要)
- 絶対安全はない(人間は間違える、機械設備は故障する、ルールで全てを網羅できない)
- 安全は、ステークホルダー全員で創り出していくものである(多重安全、協調安全)
- . . . .

# 安全学での提案

1. 安全は俯瞰的に、総合的に観よ
2. 安全は、国、企業、個人の全体で構築せよ
3. 安全はトップダウンで推進せよ
4. 安全はコストではなく投資だ
5. 安全人材に投資せよ

# 経営者と実務層の橋渡し

# セーフティ、セキュリティ、リライアビリティが融合に向かう



三つの概念を表わす新しい言葉（広義の安全性）を作る必要性

# 経営層と現場をつなぐ橋渡し人材 の必要性

- \* トップが安全に納得して投資出来るためには
  - トップにコスト/安全の有効性を説明できる中間層（橋渡し）の人材が必要
  - 広義の安全性（セーフティ、セキュリティ、リライアビリティ）を現場に指示・調整し、また、現場の意見を経営層に集約・説明できる中間層（橋渡し）の人材が必要
- \* そのためには
  - 広義の安全性（セーフティ、セキュリティ、リライアビリティ）を融合しつつ総合的に、横串を刺す考えの人材が必要である
  - 安全の共通概念を理解する人＝安全学の素養のある人が、各組織、各部門、経営層に広がる必要がある

# まとめ

- サイバーセキュリティの世界は、機械安全・製品安全の世界から学ぶ必要があるだろう
- サイバーセキュリティ人材は、安全学を学ぶ必要があるだろう
- 企業はキュリティとセーフティ(安全性)とリライアビリティ(信頼性)を統一した概念として対応する必要がある ⇒ **広義の安全性**
- 経営と広義の安全性との両方に対して、総合的に共通概念として理解できる人材が必要  
⇒ **橋渡し人材**