サイバーセキュリティに影響を与える経営の視点

2015年2月2日

横浜国立大学　大学院　環境情報研究院
教授　野口　和彦

経営からみた情報セキュリティ

- 情報システムをどのように事業に活用するかは、重要な経営課題
  - セキュリティは、情報システム活用のための重要機能
  - 情報セキュリティだけ切り取って議論することに問題がある
  - 経営にとって重要なことは、どのような車を造るかということであって、ブレーキの性能をどうするかではない
  - ブレーキ機能を軽んじた車は、事故を起こす

攻めるための基盤としての守り

- 変化する社会状況下では、現状維持にも投資が必要

- 目指す状況を実現するための対応の重要性を認識していれば、コストも投資も同じこと
  - 現在から未来を見れば、投資
  - 未来から現在を見れば、費用

- 経営者は、経営効率を考える
  - 情報システム担当者は、情報セキュリティの投資効果（費用の必要性）を経営の言葉で説明することが重要
  - 情報システムに関する経営視点でのリスクの把握が重要
    - 環境の変化でリスクも変化する

ISO31000のリスクの定義

- 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、よい方向及び／又は悪い方向に逸脱すること。
  - 注記2　諸目的は、例えば財務・安全衛生・環境に関する到達目的など、さまざまな側面をもち、戦略・組織全体・プロジェクト・製品・プロセスなどさまざまなレベルで設定され得る。

中略

  - 注記5　不確かさとは、事象、その結果、又はその起こりやすさに関する情報、理解、若しくは知識が、たとえ部分的でも欠落している状態である。

- リスクの定義によって生まれるリスクマネジメントの意義
  - リスクマネジメントを実施することによって、少しずつ企業が目指している状況に近づけているという実感が持てることが大切

リスク把握の前提となる内外の状況特定

外部の状況

- 文化、政治、法律、規制、経済及び環境（海外、国内、地域的なものに係らない）
- 外部のステークホルダーの認知度と評価
- 組織の目的に影響を与える主な要因及び動向
- 科学技術の変化

内部の状況

- 認知度、価値観及び文化
- 方針とプロセス
- 内部ユニットのステークホルダー
- 制度（例：ガバナンス、職務、責務等）
- リソースや知識の観点からみた可能性（例：資本金、人材、能力、プロセス、システム、技術力等）
- 達成しようとしている目的及びその戦略

経営が目指す経営の最適化

- ポジティブな影響とネガティブな影響の**最適化**

  - ポジティブな影響に傾きやすい経営者の関心
  - ネガティブな影響に関する楽観視
- 現状
  - 利益の最大化と安全への対応が同じ枠組みで議論されていない ⇩
  - 利益が優先され、事故・不祥事が起こりやすくなる

安全における経営の問題を考える

- 安全は、現場の問題であると意識が強い
  - 安全を現場の問題として処理すると、「悪魔のサイクル」に突入する場合がある
- 安全に影響を与える最大の要因は、経営者の価値観
  - 経営者は、その価値観を人事、組織構築、予算編成に示すべし

- リスクマネジメントを経営意思徹底の仕組みとして構築

リスクマネジメントは、マネジメントである

- マネジメント ≠ 管理

- リスクマネジメントの変化：サッカーを例に
  - 今までのリスクマネジメントは、点を取られることへの対応
  - 今のリスクマネジメントは、試合に勝つための対応

⇩

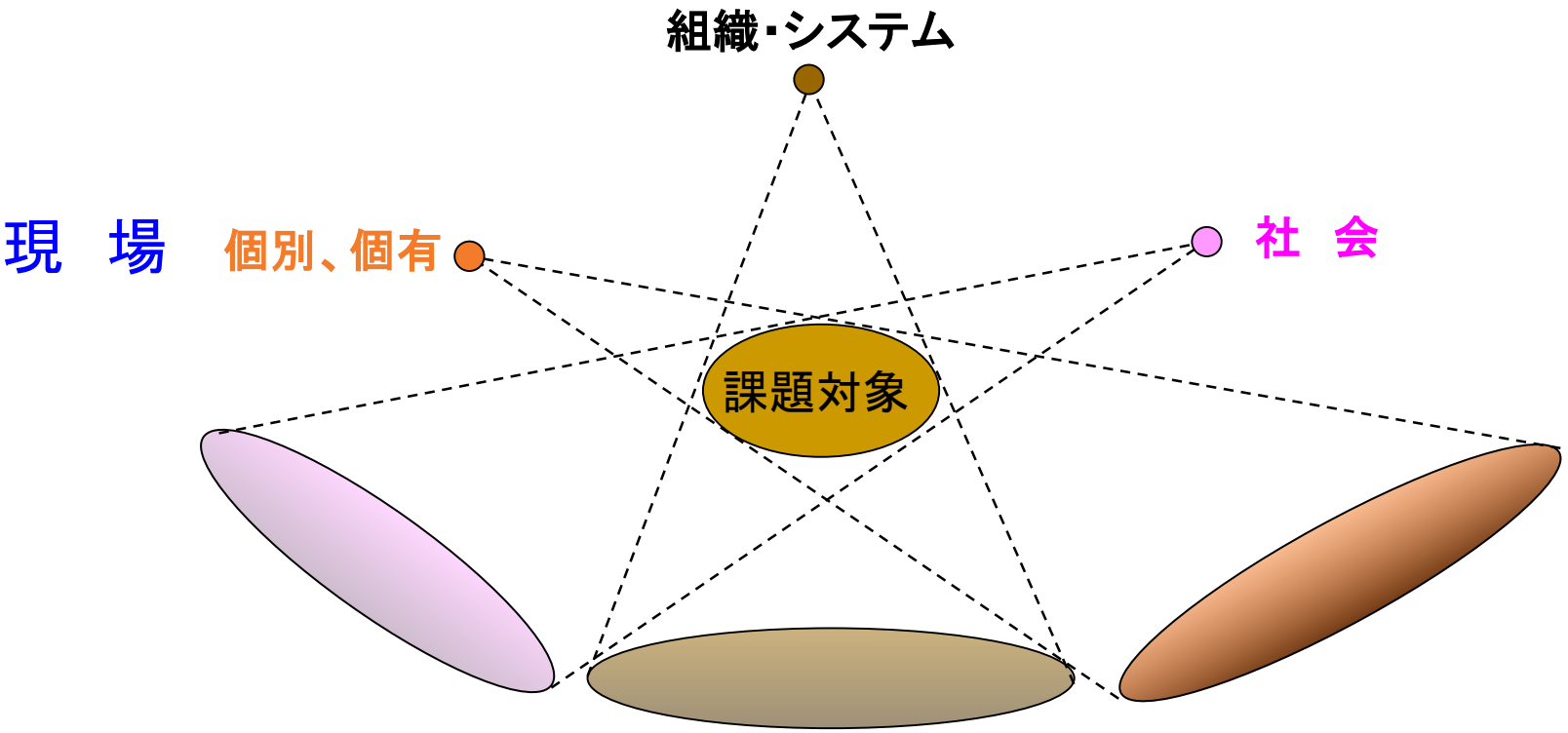
  - 部分最適化 ⇨ 全体最適化へ

⇩

- 安全も全体最適化の中で考えることが重要

多様な視点で問題チェックが必要な社会

- 視点によって問題の見え方や最適解が異なる
  - 「何が起きるか」と、「どのような影響があるか」は同じではない
- 現場のことは、現場が一番わかっているわけではない



何故起きるのか

要因は？

- 本質的危険性の顕在化防止
- 経営上の問題
- 組織運営上の問題
- システム上の問題
- 事前分析力
  - ＊見逃されやすい位置的分析
  - ＊人的ファクターの取り扱い
- ヒューマンファクターの取り扱い

リスクマネジメントにおける経営者の課題

- 業務ミッションと経営方針の明確化
  - 現状は組織の経営理念や社会的存在意義からみた安全活動の位置づけや**安全目標自体が明確になっていない**
  - 安全活動を行うための**必要な投資検討が不十分**

- 経営最適化のためのリスクリテラシーの醸成
  - 再発防止では、致命的な影響は避けられない
  - 未然防止の為の投資が課題
  - 重要なものほど、失った場合のダメージは大きい

目標とする経営実現のために経営が果たす役割

- 経営における安全の重要性と安全目標の明示
  - 環境の変化によって目標が変化する場合もある
- 目指す安全レベルのための資源投資責任
  - 目標実現の最終責任は経営者に
- 経営継続のための安全価値の重要性の制度化
  - 組織を最適化（安全価値を含む）する人事組織と評価制度の構築

- 予防活動の徹底
  - リスク顕在化の予兆の見極め
  - PDCAの継続
    - システムのPDCAと施策のPDCA
    - チェックできる計画であることが重要