資料5

「日本的経営と情報セキュリティ研究会」報告書の概要

平成27年1月29日

IPA　情報セキュリティ分析ラボラトリー

日本的経営と情報セキュリティ研究会

- 本研究プロジェクトでは、実務家の他、法学・経営学・会計学・心理学等の専門家の知恵を結集して、企業人に役立つセキュリティ対策を策定するための、組織風土の面の留意点を浮き彫りにする。
- 研究会概要
  - 2012年5月設置、2012年12月までに全7回の研究会
  - 2012年10月に「組織の帰属意識等のインターネット調査」実施
  - 2013年1月~2月　報告書レビュー
- 構成委員

座長：林 紘一郎 教授（情報セキュリティ大学院大学 教授）

- 浅井達雄 教授（長岡技術科学大学 名誉教授 ）
- 大杉謙一 教授（法学、中央大学 法科大学院）
- 加賀谷哲之 准教授（会計学、一橋大学商学研究科 ）
- 北野晴人氏（ビジネス。日本オラクルテクノロジー製品事業統括本部担当ディレクター）
- 林幹人 准教授（経営学、桜美林大学 ビジネスマネジメント学群 ）
- 柿崎環 教授（法学、横浜国立大学 国際社会科学研究科）
- 竹村和久 教授（社会心理学、早稲田大学）

オブザーバ

- 生貝直人氏（情報・システム研究機構）事務局兼務（成果物の執筆等）
- 竹村敏彦助教（関西大学）
- 藤江一正（IPA　理事長）
- 仲田雄作（IPA　理事）
- 笹岡賢二郎（IPA　参与、セキュリティセンター長）

（1）日本的経営の変容と情報セキュリティの必要性ー日本的経営とは

1. 右肩上がりが前提（高度成長期　60年代～80年代）
2. 関係依存型システム
   - 社員は家族、長期的・終身雇用システム
   - 横並びでの昇進・人事慣行
   - 性善説
3. 性善説（マクレガーのY理論）
   - 企業と社員の関係は、長期的関係性に基づく
   - 社内の利害関係者との情報共有重視
   - 株主、監査役さえ同じ仲間という意識

全社一丸となって高い業績を達成

（1）セキュリティ経営の必要性

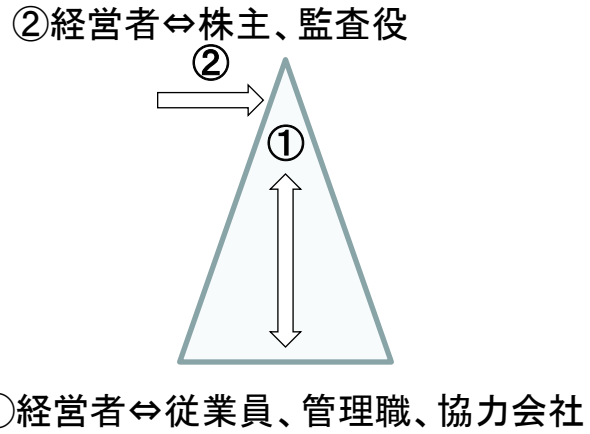
1. 停滞・右肩下がりの経営環境（90年代～）
2. 大きな変容
   - 社員は家族から業績評価重視へ
   - 競争原理の導入
     - 従来の情報共有は行われにくく
   - 性善説⇒性悪説
     - 従来の社内の利害関係者との情報共有重視、株主、監査役さえ同じ仲間という意識

     ⇒むしろ不正や不祥事の温床か

セキュリティ経営が不可欠

（2）セキュリティ経営

1. 従来の情報セキュリティ対策
   - 情報システム回りの狭い意味の情報資産（形式知）の管理に重点
   - 現場レベル・中間管理職レベルの対応にとどまる
2. 経営陣の強力なコミットメントに基づく経営戦略への位置づけ
   - 企業価値の向上
   - 社会的責任の遂行
3. 新たな情報セキュリティ対策が不可欠
   - 経営陣のトップマネジメントの元、
     法令順守、情報資産管理、事業継続
4. セキュリティ経営のためには、
   経営層によるリスクマネジメントが重要
   - 情報セキュリティ対策のため方針決定
   - コーポレートガバナンス
   - 適切な開示・リスク評価



経営層のリーダシップによるセキュリティ経営（1）

1. 合理的なリスク判断：経営者の判断原則

- 善管注意義務
  - 合法性を前提とし
  - すべての選択肢の利害得失を検討し、経営方針を決定
- （しかし）リスク判断の非一貫性
  - 確実な選択肢よりも不確実だが損失の高くなる可能性のある選択肢を選びやすい
    - 原発事故【国会事故調によれば人災】
    - オリンパス事件
- どうすれば改善できるか（ガバナンスや情報開示？）
  - 第三者のチェック（社外取締役の導入　等）
    - 潜在的リスクで、有事に致命的なダメージがある事案については、将来の不確実なリスクを過小判断しがちで、相互けん制が苦手な内部の経営判断だけでは、不適切。
  - リスク情報の開示

経営層のリーダシップによるセキュリティ経営（2）

2. 情報共有文化の再構築

- Need To Knowの原則を確立
  - 業務上必要な人のみにアクセス権限を付与する
  - 業務上不要な人にはアクセス権限を与えない

3. 残留リスクの認識

- 低確率なリスクを「想定外」から「残留リスク」へ
- リスクの社会的増幅への適切な対応
  - 安易に想定外に流れていないか？想定外として目をそらしてはならない
- **残留リスク**とは**当面の対策は講じない**ものの、無視するのではなく、定期的リスク分析の見直し。
  - 即ち、新たな知見や発見、対策技術の進歩等の事情が変われば速やかに対策を講じることが前提

リスクの社会的増幅、Kaspersonら（1988）：あるリスク事象（例えば原子力関連施設の事故や不祥事など）が生じると、その影響はそのリスク事象の範囲を超えて広がっていくこと　例：リスク事象→会社→原子力発電→原子力産業→科学技術への不信

経営層のリーダシップによるセキュリティ経営（3）

4. 適切なセキュリティ投資の水準を算定

金額の合理的な見積もりの可能性×発生の蓋然性

- 低　⇒　リスク情報として情報開示⇒**残留リスク！との認識**
- 高　⇒　引当金＞**投資規模？**

発生の確率が相当程度低い場合には、リスクに関わる情報を積極的に開示することにより、残留リスクとしての認識を確保する。一方で、それが高い場合は、必要とされる投資規模を引当金として確保するのか、それを下回る投資規模での対応に留めるのかの判断を一貫した基準に基づき行う必要がある

経営判断はどうあるべきか（社会心理学の知見）：不確実な将来リスクに楽観的になる傾向

- 確実な選択肢よりも不確実だが損失の高くなる可能性のある選択肢を選びやすい
  - 原発事故：A案という確実な選択肢ではなく、想定外にするという選択肢を選んだ
    - ◆ 合理的な経営判断はA案か？（300億円＜1500億円）

A案	B案
○○メートルの防潮堤（例えば300億円）を建設 期待値（費用）：100%×300億円＝300億円（電力）	例えば3%（※）の確率で5兆円（除染費用＋賠償費用） ※原発稼働30年×1000年に1回の大地震＝3% 期待値（費用）：3%×5兆円＝1500億円（国＋電力）

  - オリンパス事件：当該年度に赤字決算を公表するという確実な選択肢ではなく、隠ぺい・先送りという選択肢を選んだ
- しかし、経営者は遠い将来のリスクを過小評価
  - 自分の在任中（3年？）に起こるかが判断基準？
    - 300億円＞150億円（0．3%×5兆円） ← 1500億円
- 1500億円≠電力の負担、むしろ国民負担（社会的増幅）
  - 経営者は国民負担ではなく自社の負担で考える？
  - 社会的責任の遂行の限界？
- 潜在的リスクに対して、経営者が長期的な視点で、かつリスクの社会的増幅も踏まえつつ、合理的な経営判断をすることは困難なのか？

経営判断はどうあるべきか（例1）

- 不祥事に際しては、「災い転じて福となす」を目指す
  - 参天製薬事件
    - 2000年6月14日朝、参天製薬社長宛に、現金2000万円を要求する脅迫文。「応じない場合は異物を混入した目薬をばらまく」との内容。異物を混入した現物が添付。
    - 翌日午後3時、同社は厚生省にリコール決定し、午後7時には記者会見を開いて、社長自らが事件の概要と一般目薬約250万個を回収すると発表
    - **リコールに伴い、13億円の減益修正**が行われたが、**同社の株価はすぐに回復**
    - 参天製薬には何の落ち度もなく、むしろ被害者ともいえる**事件を契機として、消費者の安全を最優先する企業姿勢を社会に示すことができた**といえよう。

⇒社会的責任の遂行を通じて企業価値の維持・向上を実現

経営判断はどうあるべきか（例2）

- 参天製薬事件の真逆が同時期に発生
  - 雪印集団食中毒事件
    - 2000年6月25日、「雪印低脂肪乳」を飲んだ子供が嘔吐や下痢などの症状
    - 6月29日、事件のプレス発表と約30万個の製品の回収をするも、その後も被害の申告者が爆発的に増え、14,780人の被害者が発生
    - その際、報道陣にこの事件を追及された当時社長が、会見の延長を求める記者に、「そんなこと言ったってねぇ、わたしは寝ていないんだよ!!」と発言。社長はすぐに謝ったものの、この会話が広く配信されたことから世論の指弾
    - その後、**雪印グループの製品が全品撤去**に至るなど、**親会社の不祥事とは言え、グループ会社全体の経営が悪化**。
    - その後もBSE問題に端を発する雪印牛肉偽装事件（雪印乳業本体ではなく、子会社不監督）を発生させ、イメージダウンは決定的になり、**グループの解体・再編を余儀なくされる結果**

⇒社会的責任の遂行を疎かにし、企業価値に致命的ダメージ

経営判断はどうあるべきか（例3）

IPA

- **タカタリコール問題（エアバック）**
  - 2008年　最初のリコール
  - 2009年米国で2件の死亡事故
  - 2013年4月　各自動車メーカ　世界で約400万台をリコール
  - **2014年6月　各自動車メーカ　追加リコール（高湿度地域限定でのリコール　原因調査中）　→　原因を解明していない**
  - 2014年8月～10月　追加リコール
  - 2014年10月　連邦検察当局が捜査していると報道
  - 2014年11月　ホンダ追加リコール、トヨタ、ダイハツも追随
  - 2014年11月　　タカタ社、第2四半期報告書にて、2015年3月期純損益250億円の赤字見通し
  - 2014年11月20日　米上院　公聴会でタカタ社、ホンダを聴取
  - 2014年11月26日　米高速道路交通安全局（NHTSA）　調査リコールの範囲を全米に広げるようタカタ社に命令
    - 運輸省は1企業に科すことのできる罰金の上限を3500万から3億ドルに引き上げるように議会へ求めている

○2008年から継続するリコール=>消費者・当局の不信
○情報隠ぺいの疑い
○HPで文書公開のみ

- **トヨタの予防リコール**
  - エアバッグの大規模リコールをめぐり、トヨタ自動車は12月4日新たに19車種18万5000台のリコール。廃車の解体作業中にエアバッグのガスを発生させるタカタ製部品が破裂。原因はまだ分かっていないが、トヨタは同じ タイプの部品を搭載している車種を**予防的にリコール**する異例の措置に踏み切った。

付録：セキュリティ経営の概念