リスクマネジメントの視点による情報開示

2018年2月1日

横浜国立大学　大学院　環境情報研究院
リスク共生社会創造センター　センター長
教授　　野　口　和　彦

情報開示とリスクマネジメントの３つの視点

- 企業のリスクに関する情報開示の視点
- サイバーセキュリティリスクの低減対応策としての情報開示
- 情報開示のリスク

企業のリスクに関する情報開示の視点

- コーポレートガバナンスの視点では、自社のリスク情報開示は必須
- 各企業が自社の方針として決定すべき事項
  - 小さな問題まで情報開示を行うという開放性の明示
  - 情報セキュリティレベルの明示による自社の信頼性向上
    - 自社のセキュリティレベルを客観的に評価する能力が必要
  - セキュリティレベルの高さの明示が、サイバーテロのターゲットとして選ばれる可能性はないか？
- 開示先は、ステークホルダー
  - 規則で決まっている事項は、規則に準じる
  - 企業の横並び意識を変えることができるかが課題

サイバーセキュリティリスクの低減対応策としての情報開示

- 問題が発生した企業
  - 情報開示によって、セキュリティは向上するかが課題
    - 情報開示がセキュリティ向上につながる組織のメカニズムはあるか？
      - 決められた情報開示の判断基準に従って淡々と報告する姿勢では、セキュリティの向上に繋がらない
    - 情報に関する問題が発生した場合の根本原因分析能力が必要
- 行政
  - 情報開示を形式的なものにしない為の行政の工夫が重要
  - 問題を発生情報を受けて、セキュリティの高度化に結びつける仕組みも必要
    - 新たに発生した問題に対して有効な助言を出す機能が必要
    - 繰り返す事象に対して適切な助言を出せる機能が必要
    - 情報開示がもたらす様々なリスクを事前に洗い出す事が必要

サイバーセキュリティリスクの低減対応策としての情報開示

- 他の企業
  - 他の企業と横並びではなく、自社の特徴を示す情報開示ができるかが課題
  - 他の企業で発生した事象を如何に自社の対策に結びつける仕組みも情報セキュリティの能力
    - 単なる事例の反映ではなく、その問題の本質を対応策として展開が可能か？
    - 事象が発生した企業と、自社との差異を考慮した対応を可能にする能力が必要
      - 使用しているシステム（事業内容、システムハード、ソフト、運営体制・技術力、使用可能な資金等）の差異を整理した上で、有効な対応を考える能力が重要
      - 情報を受けてから、一定の時間内に対応を展開する仕組み・機能が重要である

情報開示の社会視点からのリスク

- 情報開示による好ましい影響の可能性
  - サイバーセキュリティに関する国の制度の高度化
    - サイバーセキュリティに関する企業を超えた仕組みの構築
    - 国としての先見性の明示
  - 一つの経験の有効活用

- 情報開示による好ましくない影響の可能性
  - 労力の増大・仕組みの煩雑化
  - 情報開示自体が目的化し、セキュリティの向上に役立たない可能性
    - 企業の形式的なパフォーマンスとしての情報開示に陥る可能性
  - 情報の誤った理解による企業の過大対応、社会不安の増大の可能性