

<セキュリティマインドを持った企業経営に係る検討>

IoT時代のビジネスとサイバーセキュリティの関係を如何に考えるべきか

「IoTシステムを通じて新たなサービスを提供するに当たっては、市場における個人・企業が当該サービスに期待する品質の要素としての安全やセキュリティ、すなわち「セキュリティ品質」がカギ
(サイバーセキュリティ戦略(H27.9閣議決定))

「経営層」の意識改革 → 経営戦略として捉える
(サイバーセキュリティ人材育成総合強化方針(H28.3サイバーセキュリティ戦略本部決定))

セキュリティ対策はやむを得ない「費用」ではなく積極的な「投資」であるとの認識

サイバーセキュリティに関する取組が市場や出資者といった多様な関係者から正当に評価されるには如何にすべきか

例：企業価値を高めるサイバーセキュリティ投資の取組に係る情報発信等

経営者のメリット⇒
経営層に直接

経営層にわかる
視点・言葉で

他人事から
自分事へ

効用と比較してセキュリティリスクを許容し得る程度まで低減

提供する機能やサービスを全うする(機能保証)という観点からリスクを分析し総合的に判断

ビジネスにおけるサイバーセキュリティの観点からのリスクマネジメントに何が必要か

例：セキュリティ等に関し、経営層と実務者層との間の意思疎通を高める取組

専門的事項
⇒橋渡し人材層

「企業価値を高めるサイバーセキュリティ投資」の“考え方”の構築

- “情報化”により生み出される価値とその防護
- 企業価値、市場価値を高める取組
(「セキュリティ品質」とブランド価値)
- 企業における取組についての積極的な発信等

“考え方”の実装のためのツール

- 経営層の認識を高めるコンテンツ作成
- ケースメソッドの開発
- 情報発信・開示手法の整備
- 取締役会の権限・責務(会社法)
- リスク対策
 - 経営ガイドライン(経済産業省)の普及・促進
 - セキュリティガバナンス
 - サイバーリスクに関する保険 等