**認識するべき経営者のセキュリティ対策３原則**

**サイバーセキュリティ経営ガイドライン　Ｖｅｒ２．０（経済産業省）**

1. IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めること
2. 系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策を実施すること
3. 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報開示等、関係者の適切なコミュニケーションを行うこと

この3原則により、経営者による「知らない」「担当者に任せている」といった責任転嫁や、「委託先のやったこと」「下請けの責任」といった擦り付け、また根拠を説明できない安易な「大丈夫」等は全て通用しないという方針が定まったのです。（注１）

「サイバー攻撃や情報漏洩（セキュリティ被害）」を100％防ごう」というものではなく、「事件が起こった際に、早期検出し被害を最小限にそして”世間に咎められない様な”対策をしておこうというものです。何かしらのセキュリティインシデントが起こった場合に、企業が生き残れる最低限の体制を構築する事を目指しています。

　　　　　 　　（注１）サイバーセキュリティ.COM参照

**経営者からＩＴ責任者へのセキュリティ対策指示１０項目**

1. サイバーセキュリティリスクの認識、組織全体での対応方針の策定
2. サイバーセキュリティリスク管理体制の構築
3. サイバーセキュリティリスク対策のための資源（予算、人材等）確保
4. サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
5. サイバーセキュリティリスクに対応するための仕組みの構築
6. サイバーセキュリティ対策におけるＰＤＡサイクルの実施
7. インシデント発生時の緊急対応体制の整備
8. インシデントによる被害に備えた復旧体制の整備
9. ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
10. 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

この10項目は、経営者がきちんと指導し企業内で必ず実施するよう求めているものです。

経営者のリーダーシップの下で、サイバーセキュリティに対する適切な投資（ＩＴ，セキュリティ）が行われ、企業のサイバーセキュリティ対策強化が行われることを最大の目的としています。セキュリティ対策の実施を「コスト」と捉えるのではなく、将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要です。つまりセキュリティ投資は必要不可欠かつ経営者としての責務です。

サイバー攻撃は年々高度化、巧妙化しきており、サイバー攻撃によって純利益の半分以上失う企業が出るなど、深刻な影響を引き起こす事件が発生しています。

経営者が適切なセキュリティ投資を行わず社会に対して損害を与えてしまった場合、社会からリスク対応の是非、さらに経営責任や法的責任が問われる可能性があります。