経営層がとるべきサイバーセキュリティ対策　10か条

1 サイバーセキュリティリスクの重要性について経営会議において情報を分析する。

サイバーセキュリティリスクの重要性について取締役会等の経営会議において協議・分析し、その結果に基づき、経営層が共通した認識の下で意思決定を行う。

2 サイバーセキュリティリスクに関する検討組織を設置する。

経営層が情報を分析して施策に反映させるために専門の検討機能を組織し、自社におけるサイバーセキュリティリスクの評価を行う。評価結果を経営会議におけるインプット資料として活用して経営方針を立案し、予算確保等、対策推進のための社内資産を確保する。

3 危機管理を統括する既存部門とCSIRTの連携を強化する。

経営リスクとサイバーセキュリティリスクを統括管理するために組織連携を強化する。サイバー攻撃が発生した際のシナリオを事業継続計画に含め、その発動の際には、危機管理を統括する既存部門と CSIRT が連携するよう組織を整備する。

4 PDCAサイクルを実施する組織からリスク対応について定期的な報告を受ける。

情報セキュリティの改善活動を統括する立場として、橋渡し人材を主体とする PDCA サイクルを実施する組織を発足し、経営層として直接進捗を確認する。最新動向、世間のインシデント状況、自社の対応状況等を踏まえて、重視するサイバーセキュリティリスクへの対応状況について定期的に報告を受ける。報告をもとに、経営層が重視するサイバーセキュリティリスクへの対応状況を確認する。

5 経営層として情報共有に努める。

経営層が関与することの組織的な効果を踏まえ、サイバーセキュリティリスクに関わる情報共有に努める。

6 危機管理コミュニケーション力を高める。

危機が発生した際に適切な情報開示ができるよう、危機管理コミュニケーション力を高める。経営層自身が適切な有事対応できるよう、平時より能力を高める。

7 有事に備えた現場担当者教育を強化する。

サイバー攻撃等の有事に備えて、日頃から現場担当者・管理者の教育を行い、体制を強化する。攻撃を最初に検知するのは現場担当者であり、これを踏まえた教育を行う。

8 監査機能を積極活用する。

経営層が重視するサイバーセキュリティリスクに対応した対策を確実に実施するために、システム監査やセキュリティ監査等の監査機能を積極的に活用する。監査を忌避する風潮を打破し、ガバナンス強化の仕組みとしての活用を図る。

9 サイバーセキュリティリスクへの取組について積極的な情報開示に努める。

株主や投資家等を含め、多様な利害関係者に向け、サイバーセキュリティリスクへの取り組みについて積極的な情報開示に努める。

10 自社のセキュリティ水準の将来目標を定め、目標達成や進捗状況を管理する。

中長期の事業計画と整合したサイバーセキュリティ対策を計画し、実行する。自社が目標とする中長期のセキュリティ水準を定め、目標達成や進捗状況を内部監査の実施を通じて確認する。