［サイバーセキュリティの経営課題］　文責：河東岩夫、作成日：平成 28 年 10 月 22 日

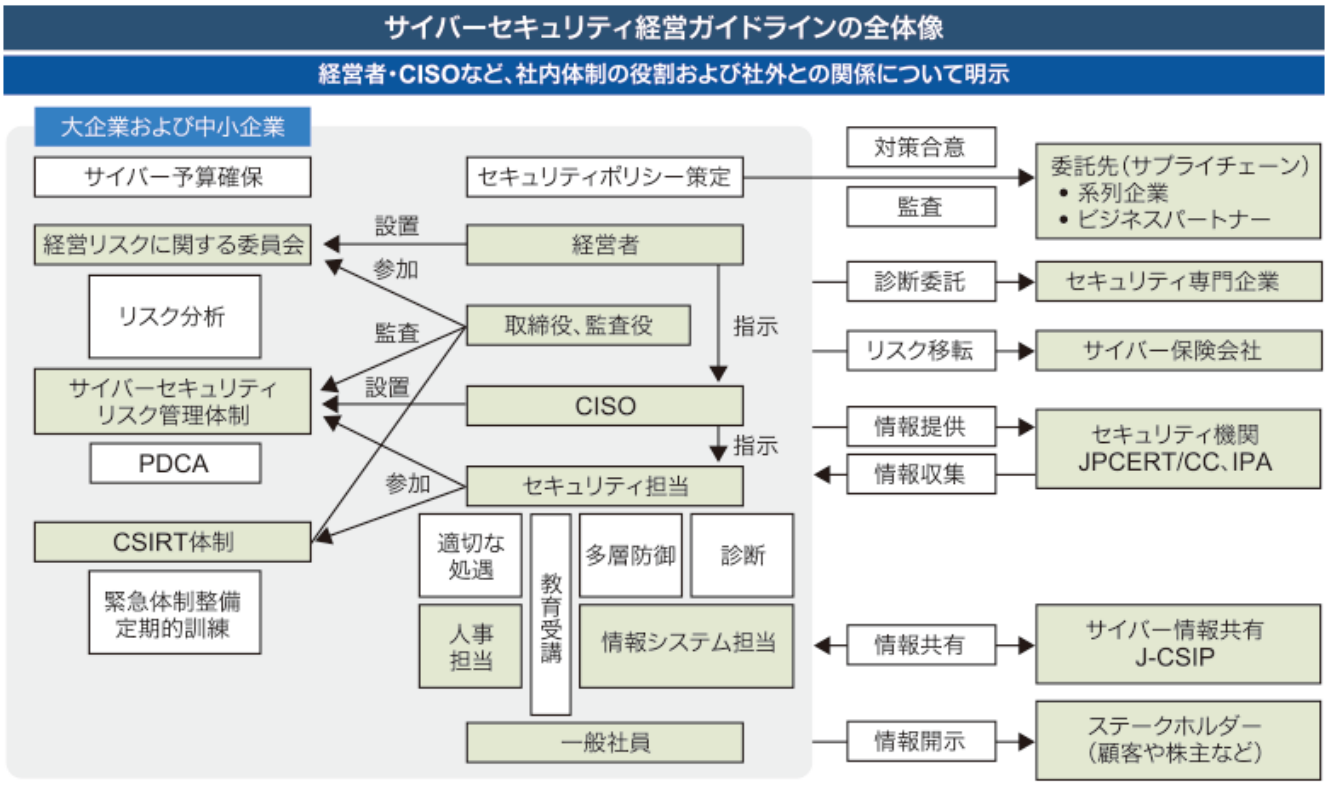
経営層がサイバーセキュリティに取組む必要性の理由は次の３つにあると言われている。

理由１：サイバーセキュリティは経営リスクであり、事象発生時の被害は事業の存続に影響する

理由２：サイバーセキュリティは情報部門だけではなく組織全体の問題であり、改善ぼ継続には経営層の理解が必要である

理由３：サイバーセキュリティは投資であり、IOT の活用等、時代の変化に応じた事業の成長を行う上で、それを武器に積極的な事業計画を実現する

上記の理由からマクニカネットワークスの資料「セキュリティ対策現場と経営の一体感を促進するための取り組み」に基づき、経産省・IPA 情報の引用も含めて、以下に経営ガイドラインの全体像と１０の主要な経営課題を筆者が編集・記載した。



No.	経営課題
1	サイバーセキュリティリスクの認識、組織全体での対応の策定
2	サイバーセキュリティリスクの管理体制の構築
3	サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
4	サイバーセキュリティ対策フレームワーク構築(PDCA)と対策の開示
5	系列企業やサプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対応の実施及び現状対策
6	サイバーセキュリティ対策のための資源(予算、人材等)の確保
7	IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
8	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のための環境整備
9	緊急時の対応体制(緊急連絡先や初動対応マニュアル、CSIRT)の整備、定期的かつ実践的な演習の実施
１０	被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備