

- リーダーシップを取ってサイバーセキュリティ対策を推進していただくため、「**サイバーセキュリティ経営ガイドライン**」に沿った対応をお願いしたい。その中でも、最近の国内外の動向を踏まえ、特に以下の取組を強化していただきたい。

### <サイバーセキュリティ経営ガイドライン（ポイント）>

#### 1. 経営者が認識すべき3原則

- (1) 経営者が、リーダーシップを取って対策を進めることが必要
- (2) 自社のみならず、サプライチェーン全体にわたる対策への目配り
- (3) 平時及び緊急時のいずれにおいても、社内外関係者との積極的なコミュニケーションが必要

#### 2. 経営者がCISO等に指示すべき10の重要事項

リスク管理体制の構築	指示1 組織全体での対応方針の策定 指示2 管理体制の構築 指示3 予算・人材等のリソース確保
リスクの特定と対策の実装	指示4 リスクの把握と対応計画の策定 指示5 リスクに対応するための仕組みの構築 指示6 PDCAサイクルの実施による継続的改善
インシデントに備えた体制構築	指示7 緊急対応体制の整備 指示8 事業継続・復旧体制の整備
サプライチェーンセキュリティ	指示9 サプライチェーン全体の状況把握及び対策
関係者とのコミュニケーション	指示10 情報収集、共有及び開示の促進

#### 1. セキュア・バイ・デザインの実践

- ・ ITサービス・製品等提供事業者に対して**セキュリティ慣行を求める**（JC-STARラベル取得済み製品の優先購入等）。

#### 2. 中小企業向け施策の積極的活用（促進）

- ・ 中小企業においては、「**サイバーセキュリティお助け隊サービス**」など**中小企業向け施策の活用**も検討する。
- ・ 大企業においては、**パートナーシップ構築の観点**からも、中小企業のビジネスパートナーに**同サービス等の活用を促す**。

#### 3. 価値創造経営の一環としての位置付け

- ・ サイバーセキュリティに対する投資を、**中長期的な企業価値向上に向けた取組の一環**として位置付ける。その関連性について、投資家を含む**利害関係者から理解を得るための活動（対話・情報開示等）**を積極的に行う。