企業経営で期待されるサイバーセキュリティの考え方（案）

資料３

本考え方は、企業がサイバーセキュリティに取り組む際に、経営層に期待される“認識”を示すとともに、経営戦略を企画する人材層に向けた実装のためのツールを示すことを目的として、取りまとめたものである。

ITが企業活動の基盤となり、サイバー攻撃等のリスクを理解し、コントロールしつつ、ビジネスチャンスへの挑戦が当たり前のことになっている。また、内部統制システムの構築・運用の一環として、サイバーセキュリティの確保は企業が果たすべき社会的責任という側面も併せ持つようになっている。今後、IoTシステムの普及に伴い、安全なIoTシステムを創出するための高いセキュリティ品質は、企業価値や国際競争力の源泉となることから、企業としての「挑戦」と「責任」としてサイバーセキュリティ対策に積極的に取り組むことが期待される。

Ⅰ　基本的考え方

○2つの基本的認識

①サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新する、新しいものづくり戦略の一環として考えていく必要がある。
②全てがつながる社会においては、サイバーセキュリティに取り組むことはいわば社会的なルールであり、自社のみならず社会全体の発展にも寄与することとなる。

○3つの留意事項

①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、新たな脅威への対処を先取りする真の「リスクマネジメント」として経営者がリーダーシップをもって取り組む必要がある。
②対策が不十分な企業からの情報流出を防ぐため、海外を含め、サプライチェーン全体でのサイバーセキュリティ確保が必要である。
③企業のサイバーセキュリティに係る取組等について積極的に示していくことにより企業価値の向上につなげていく。

Ⅱ　企業の視点別の取組

①サイバーセキュリティを強く意識し、積極的に競争力強化に活用する企業

（期待される認識）
・高いレベルのセキュリティ品質の実現をブランド価値の向上につなげる。
（実装に向けたツール）
・IoTセキュリティガイドライン等／情報発信

②IT化・セキュリティをビジネスの基盤として捉えている企業

（期待される認識）
・セキュリティ対策を担当者任せにするのでなく、経営者自らがリーダーシップをとって対策する。
（実装に向けたツール）
・「サイバーセキュリティ経営ガイドライン」／企業等がセキュリティ対策に取り組むインセンティブ　／情報開示

③自らセキュリティ対策を行う上で、事業上のリソースの制約が大きい企業

（期待される認識）
・経営者自らサイバーセキュリティ対策に関心を持ち取り組むべきだが、リソースには限界があることから、効率的にすすめる方策を検討
（実装に向けたツール）
・効率的なセキュリティ対策のサービス利用／相談窓口・セミナー等の活用

○サイバーセキュリティに関する情報発信の状況等、引き続き情勢の把握に努め、経営層の意識を高めるための取組を行う。