企業経営のためのサイバーセキュリティの考え方（１）

企業が自発的に行うサイバーセキュリティの取組が促進されるよう、企業経営のためのサイバーセキュリティに係る基本的考え方とともに、経営層に期待される“認識”や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。

※普及啓発・人材育成専門調査会の下に設置された、「セキュリティマインドを持った企業経営ワーキンググループ」（主査：林紘一郎 情報セキュリティ大学院大学教授）を通じ、検討を実施。

基本方針　　ーサイバーセキュリティは、より積極的な経営への「投資」へー

グローバルな競争環境の変化

- ITの発展によるビジネスの変革が、消費者向けのビジネスから企業間取引へと拡大
- サイバー空間と実空間の融合がさらに進み、チャンスもリスクも一層増大

サイバーセキュリティをやむを得ない「費用」でなく、積極的な経営への「投資」と位置づけ、企業としての「挑戦」と、それに付随する「責任」として取り組むことが期待される

I.基本的考え方

二つの基本的認識

＜①挑戦＞

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ものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。

＜②責任＞

全てがつながる社会において、サイバーセキュリティに取り組むことは社会的な要求・要請であり、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。

三つの留意事項

＜①情報発信による社会的評価の向上＞

- 「セキュリティ品質」を高め、品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。
- そのような取組に係る姿勢や方針を情報発信することが重要。

＜②リスクの一項目としてのサイバーセキュリティ＞

- 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、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。
- 経営層のリーダーシップが必要。

＜③サプライチェーン全体でのサイバーセキュリティの確保＞

- サプライチェーンの一部の対策が不十分な場合でも、自社の重要情報が流出するおそれあり。
- 一企業のみでの対策には限界があるため、関係者間での情報共有活動への参加等が必要。

企業経営のためのサイバーセキュリティの考え方（２）

II.企業の視点別の取組

企業が投資すべき対象や経営リスクは様々であり、各企業の人的・金銭的資源にも限りがあることから、ITの利活用やサイバーセキュリティへの取組において、各企業の事業規模のみならず、その認識の違いなどを踏まえて取り組んでいく必要がある。

ITの利活用を事業戦略上に位置づけ、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しようとしている企業 （積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）	【経営者に期待される認識】 • 積極的なITの利活用を推進する中で、製品やサービスの「セキュリティ品質」を一層高め、自社のブランド価値の向上につなげるべく、システムの基盤におけるセキュリティの向上、情報・データの保護、製品等の安全品質向上に取り組む。 • 様々な関係者との協働が重要であるため、情報提供に主体的に取り組む。 • 決して現存する標準や取り組みなどに満足することなく、実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、変革していく存在となることが期待される。 【実装に向けたツール】 • IoTセキュリティに関するガイドライン（「IoTセキュリティのための一般的枠組」等） • 自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信
IT・セキュリティをビジネスの基盤として捉えている企業 （IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略に組み込むところまでは位置づけていない企業）	【経営者に期待される認識】 • 経営者のリーダーシップによって、社会的責任としてのサイバーセキュリティ対策に取り組む。 • サプライチェーンやビジネスパートナー、委託先を含めた対策を行う。 • 平時・緊急時のいずれにおいても、情報開示などの適切なコミュニケーションを行う。 【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上での保険等のリスク管理手法の活用 • サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信
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 （主に中小企業等でセキュリティの専門組織を保持することが困難な企業）	【経営者に期待される認識】 • サプライチェーンを通じて中小企業等の役割はますます重要となる中、消費者や取引先との信頼関係醸成の観点から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。 • 外部の能力や知見を活用しつつ、効率的に進める方策を検討する。 【実装に向けたツール】 • 効率的なセキュリティ対策のためのサービスの利用（中小企業向けクラウドサービス等） • サイバーセキュリティに関する相談窓口やセミナー、地域の相談員等の活用