

企業経営のためのサイバーセキュリティの考え方とは？



内閣サイバーセキュリティセンター(NISC)が、企業経営のためのサイバーセキュリティに係る基本的な考え方と、各企業の視点に合わせた取組方法（経営層に期待される認識と実装のためのツール）を公表しています。

二つの基本的認識

■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。

■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寄与することとなる。

三つの留意事項

■情報発信による社会的評価の向上

- ・セキュリティ対策を品質向上等に有効な経営基盤の一つとして位置付け、企業価値を高める。
- ・サイバーセキュリティに係る取組の姿勢や方針を情報発信する。

■リスクの一項目としてのサイバーセキュリティ

- ・サイバーセキュリティは、機能保証という観点から、リスクの一項目であることを認識する。
- ・リスクマネジメントとして、経営者がリーダーシップをとって取り組む。

■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

- ・一部のサプライチェーンの対策が不十分な場合でも自社の情報流出のリスクがあることを認識する。
- ・情報共有活動への参加や入手した情報を有効活用する環境等を整備する。

企業の視点別取組

視点 取組	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企業	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までは位置づけていない企業	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	自社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。	・経営者のリーダーシップで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委託先等を含めた対策を行う。	・経営者自らサイバーセキュリティ対策に関心を持って取り組む。 ・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	・IoTセキュリティに関するガイドライン等を活用 ・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	・サイバーセキュリティ経営ガイドラインに基づき対策を実施 ・保険などのリスク管理手法の活用 ・経営上の重要課題として取り組んでいることを情報発信	・効率的なセキュリティ対策のためのサービスの利用 ・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

出典：平成28年8月2日公表 内閣官房 内閣サイバーセキュリティセンター「企業経営のためのサイバーセキュリティの考え方の策定について」

京都中小企業情報セキュリティ支援ネットワーク(Ksisnet)
IT相談窓口(公益財団法人京都産業21 お客様相談室)

相談内容：情報セキュリティ対策、情報漏えい・流出事案等
※毎週月曜日～金曜日の9:00～17:00(祝日を除く)

TEL 075-315-8660 メールアドレス okyaku@ki21.jp

公益財団法人京都産業21 お客様相談室(〒600-8813 京都市下京区中堂寺南町134 京都府産業支援センター内)

お困りの
ときは!!