Sec04-01 ECサイトのサイバーセキュリティ対策の実践のために

1. サイバーセキュリティ対策として考慮すべき事項と必要なスキル・知識
   1. 【2018年6月12日暫定作成】
   2. 【引用】Bib40-06-3 次世代システムの構築に必要なスキル・知識
   3. 総論
      1. サイバーセキュリティの被害に遭った場合、組織の存立が危ぶまれる事態になりえることを自覚する
      2. ・世の中で起こっているセキュリティ被害を対岸の火事だと思っている経営者、ITは導入しているにも関わらずセキュリティ対策のための費用はないとして対策に後ろ向きの経営者、最も重要な情報にアクセスする権限を持ちながら、セキュリティに関しての意識の低い経営者。これらの経営者が最大のセキュリティリスク
      3. 国は、大企業のみならず、中小企業も、「サイバーセキュリティ経営ガイドライン」を参照することを求めている
      4. 【参考】「中小企業向けサイバーセキュリティ対策の極意」を引用

ドキュメントを参照: [guidebook](http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/jigyou/guidebook/)

* + - 1. 東京都が中小企業の経営者向けに、サーバーセキュリティ対策として認識すべきことをイラストを交えてまとめたもの
      2. 経営者が認識すべきことであるが、それを認識させるためにも、担当者が理解していることが重要
  1. 【参考】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【NISC】

ドキュメントを参照: [keiei.pdf](http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf)

* + 1. 基本方針－サイバーセキュリティは、より積極的な経営への「投資」へ－
       1. グローバルな競争環境の変化
       2. 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
       3. 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
       4. 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
    2. 基本的な考え方
       1. 二つの基本的認識
          1. ＜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
          2. ＜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
       2. 三つの留意事項
          1. ＜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。

* + - * 1. ＜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。

* + - * 1. ＜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。

* + 1. サイバーセキュリティ対策として考慮すべき事項
       1. サイバーセキュリティ対策は、事業継続を脅かすリスクの１つ。
          1. わかっていますか？

1. Sec01-02-10 ウェブサイト開設等における運営形態の選定方法に関する手引き

ドキュメントを参照: [narisumashi\_manual.pdf](https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf)