

## ☐ Sec01-01-02\_「中小企業向けサイバーセキュリティ対策の極意」の改訂案（素材）

### ⊕ 改訂履歴

### ⊕ リンク

### ■ ① 【Mission03】 経営者は事前に何を備えればよいのか

### ☐ ① 【Mission03-A】 経営者は事前に何を備えればよいのか【守り】

- サブタイトル【組織維持のために】経営者、管理者が、自組織の現状として認識すべきこと
- 管理者が知っておくべきこと（管理者を設置していない場合は経営者が自ら知っておくべきこと）

### ☐ 総論

- 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
  - ・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
- 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

### ☐ ② 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。

- 組織の社会的責任の認識

### ⊕ ③ Mission3-1 サイバーセキュリティ対策が経営に与える重大な影響

### ⊕ ③ Mission3-2 情報セキュリティ対策を怠ることで企業が被る不利益

### ⊕ ③ Mission3-3 経営者に問われる責任

### ☐ ③ 参考

- ⊕ 【参考】情報セキュリティ対策を怠ることで企業が被る不利益【中小企業の情報セキュリティ対策ガイドライン案】 

- ⊕ 【参考】経営者が負う責任【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】 

- ⊕ 【参考】経営者が認識すべき「3原則」【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】 

- ⊕ 経営者として取り組むべき「重要 7項目の取組」【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】 

### ⊕ ③ 【コラム】組織の姿勢3分類(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（2016年8月2日）【NISC】より)

### ☐ ② 投資効果（費用対効果）を認識する

### ⊕ ③ Mission3-4 投資効果（費用対効果）を認識する

### ☐ ② 【自社の対策状況把握】自社のIT活用・セキュリティ対策状況を自己診断する

### ⊕ ③ Mission3-5 ITの活用診断

### ⊕ ③ Mission3-6 サイバーセキュリティ対策診断

② ビジネスを継続するために（守りのIT投資とサイバーセキュリティ対策）

- 組織を維持するために経営者、管理者が認識し、実践すべきことは？

③ Mission3-8 業務の効率化、サービスの維持のために

③ Mission3-9 【経営者が認識すべき】サイバーセキュリティ経営の3原則

③ Mission3-10 【経営者がやらなければならない】サイバーセキュリティ経営の重要10項目

① 【Mission03-B】経営者は事前に何を備えればよいのか【攻め】

② ビジネスを発展させるために（攻めのIT投資とサイバーセキュリティ対策）

- ③ 【持続的発展のため】組織の発展を目指した戦略的なIT活用とサイバーセキュリティ対策

③ 【コラム⇒各項目】ITの最新トレンド対応

- デジタル・トランスフォーメーション(DX)時代に、「ビジネスを発展させるために」（攻めのIT投資）に活用すべきITと 活用におけるサイバーセキュリティ対策（Society5.0時代のサイバーセキュリティ対策）

④ Society5.0時代に必要なセキュリティ対策

- ディープラーニング、ロボット、ビッグデータ、IoT、クラウドサービス等の技術の活用の必要性和、活用におけるセキュリティ対策の記述の充実

IoT関連セキュリティ対応【担当：早出】

クラウドサービス

5Gセキュリティ対応【担当：早出】

BYODセキュリティ対応

- APIセキュリティ
- ブロックチェーンにおけるセキュリティ
- インターネットアクセスにおけるセキュリティの新技术

IDと認証セキュリティ【担当：中山】

③ Mission3-11 次世代技術を活用したビジネス展開

③ 【コラム】攻めのIT投資対応

- ④ AIが人間をアシストする「インテリジェント・ワークプレイス」の活用におけるサイバーセキュリティ対策【担当：中山】

③ Mission3-12 IoT、ビッグデータ、AI、ロボットの活用

③ Mission3-13 IoTが果たす役割と効果

③ Mission3-14 人工知能（AI）が果たす役割と効果

③ Mission3-15 IoTを活用する際のサイバーセキュリティ上の留意点

③ Mission3-16 IoTを活用する一般利用者のためのルール

③ 参考

⊕ ③ 【コラム】サイバーセキュリティ分野で機械学習が活用される背景 [Expand - Collapse](#)

⊕ ③ 【コラム】サイバー・フィジカル・セキュリティ対策フレームワーク対応【担当：早出】

☐ ① 【Mission03-C】【組織維持のため】網羅的なサイバーセキュリティ管理と実践（予防・予兆・事象発生時のための備え）

☐ ② セキュリティホールを減らす網羅的・体系的な対策の策定方法

■ ⇒中小企業の情報セキュリティ対策ガイドライン第3版として、一括で提示

■ ③ Mission3-XX 情報セキュリティ5か条

■ ③ Mission3-XX 情報セキュリティ基本方針

⊕ ③ ③ Mission3-17 新・5分でできる自社診断シート

⊕ ③ ③ Mission3-18 情報セキュリティハンドブックひな形（従業員向け）

⊕ ③ ③ Mission3-19 情報セキュリティ関連規程の明文化

■ ③ ③ Mission3-XX 情報資産台帳の作成

⊕ ③ ③ Mission3-20 リスク分析シート

■ ③ ③ Mission3-XX 中小企業のためのクラウドサービス安全利用の手引き

■ ① 【Mission04】もしもマニュアル