Expand - Collapse

Sec01-10ガイドブック構成検討用【Webページ構成】（概要案）

- 【2017年12月1日】

はじめに

- 【適用範囲】本資料の目的、対象、期待する効果

目的

- システム管理者が、経営者に対して、情報セキュリティ対策の実施に投資することを説得できるように
- 経営者が情報セキュリティ対策の必要性を認識し、システテ管理者に対して、対策の実施を指示するように

サイバーセキュリティに対する組織の姿勢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)

【レベル１】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。小企業・零細企業の多く

【レベル2】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、必要十分な対策が講じられていない企業
- 必要以上のサイバーセキュリティ対策のため、業務の効率化、競争力強化を阻害している企業

【レベル3】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企業

目標

現状認識

- セキュリティ被害は対岸の火事ではないことを認識できるレベル
- 手間がかかってもやらなければならないと認識できるレベル

ステップ１

- とりあえず最低やらなければならないことを認識し速やかに実践できるレベル

ステップ2

- IT投資効果を明確にしていないため、適正規模のセキュリティ対策の実施を阻害していることを認識できるレベル
- 予算がなくても、ITを活用するなら、対策費が必要で、それはIT投資の中で捻出するものであることを認識できるレベル

ステップ３

Expand - Collapse

- どこまでやれば、どの程度安全になるかを認識できるレベル
- 対策を実施するために知識・ノウハウが必要であることを認識できるレベル
- 専門家（CIO、CISO）が必要であることを認識できるレベル

⊟ ステップ４

- IT投資効果のPDCAサイクルが確立し定期的にIT資産の分析を行い最適なポートフォリオ管理を行うことを認識できるレベル

⊟ 【現状認識】何のために情報セキュリティ対策を行う必要があるのか

⊟ 【脅威の現状認識】過去の事例

- 【現状認識】インシデント発生の事例

⊟ 【参考】

- 最近の主な出来事（情報セキュリティ白書2016より）
- 事象シナリオ（数種）【総務省】【主な事象を例示】
- 事故・被害の事例（一般利用者の対策｜国民のための情報セキュリティサイト【総務省】）

⊟ 【脅威の動向認識】今後起こりうるケース

⊟ その他最近の傾向

- 物理セキュリティ
- 新技術関連

- セキュリティ対策の現状（統計値等）【傾向値を例示】

⊟ 【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の自己診断

- ITの活用診断
- サイバーセキュリティ対策診断
- 情報セキュリティ対策診断

⊟ 【ステップ１】【今やろう】全ての従業員、個人が知っておくべきこと

- 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でも、最低限にやるべきこと

⊟ ☆ 【即効性のある予防対策】最低限の対策（本格的な対策前でも今すぐに）

- 人的対策
- 管理的対策
- 物理的対策
- 技術的対策

- ☆ 【緊急時対応】インシデントレスポンス

⊟ 参考してほしいドキュメント

- 情報セキュリティハンドブックVer2.0【NISC】

⊟ 【ステップ2】【組織を維持するために】【守りのIT】経営者、管理者に認識していただきたいこと

Expand - Collapse

- 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知っておくべきこと）
- どんな情報資産があるか
- リスクの認識
- 組織の社会的責任の認識

- 【ステップ3】【組織維持のため】【守りのIT】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）
  - 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
  - PDCA
    - 体系的な対策の策定
      - 情報資産台帳【IPAサンプルベース】
      - 脅威の状況【IPAサンプルベース】
      - 対策状況チェックリスト【IPAサンプルベース】
        - 残留リスクの許容
      - 従業員向け「情報セキュリティハンドブック」【IPAサンプルベース】
      - 情報セキュリティポリシー【IPAサンプルベース】
    - 実施
    - 評価
    - 見直し
  - 参考してほしいドキュメント
    - 中小企業の情報セキュリティ対策ガイドライン第2版【IPA】
    - サイバーセキュリティ経営ガイドライン解説書【IPA】
    - 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】
- 【ステップ4】【組織の発展のため】【攻めのIT】組織の発展を目指した戦略的なIT活用とセキュリティ対策
  - 東京都の方針
    - ICTの一層の活用
      - データやシステムをオープンに
      - IoT時代の個人情報の高度利用
    - TOKYO創業ステーション
    - 中小企業におけるIoTの普及
      - 日本商工会議所が支援
  - 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
  - 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
  - IT活用の必然性

Expand - Collapse

- ITを活用したサービスを継続するためには、情報セキュリティ対
- 情報発信とセキュリティ対策

【付録】役立つ情報のインデックス

- 用語解説
- セキュリティ侵害以外のインシデントと対策
- インシデント発生時に役立つ対策の解説
- 【レベル2】PDCAサイクルのそれぞれのセキュリティ対策の知識
- セキュリティ関連法規【IPAガイドライン案】
- 各種ガイドライン
- セキュリティ関係機関
- 参考文献・参考サイト
- 普及・啓発・教育教材