Expand - Collapse

- Bib10-02 経営者向けセキュリティ対策のポイント
  - 【2018年2月8日】
  - すぐに
    - まずは、9か条の遵守
    - サンプルを参考に、職員向けハンドブックの作成
  - 経営者としての意識
    - 後付けのセキュリティ対策は大きな投資が必要
    - 今後セキュリティ対策は、IT化投資の一環で考える
    - セキュリティ対策がIT投資の無駄にならないように
      - 業務効率化や生産性向上のための「守りのIT投資」が、セキュリティ対策により利用に過度の制限が付くことによりIT投資が無駄になる可能性がある
        - Cloud, File共有, mail, USB, DVD,
    - 最大のセキュリティリスクは経営者
  - 対策を検討する前に、現状を把握
    - 情報資産（情報、情報機器）のリスク分析
      - 情報・データ
      - 情報システム（コンピュータ）
      - 情報システム（ネットワーク）
      - 情報システム（アプリケーション・サービス）
      - 業務
    - ビジネス上の重要書もしくは危険度の評価（被害想定）
      - 業務遂行上の必要度
      - ビジネスへの寄与度（協商力の維持や向上）
      - 侵害された場合の社会的影響度（第三者の被害や社会問題の可能性）
      - 侵害された場合の信用や評価への悪影響
      - コンプライアンスへの影響
    - 対策はリスクの高いものを優先する
      - （侵害の発生頻度が高く、侵害が顕在化した場合の経済的、社会的損失の大きさ（深刻さ）（直接被害額、間接被害額）を勘案してセキュリティ対策の優先度を決める。発生頻度を減らす、被害を減らす、保証を考える）
    - リスク＝侵害の可能性×侵害による想定被害
      - リスク＝情報資産に対する脅威（侵害する行為の発生頻度）×情報資産の重要度（機密性レベル＋完全性レベル＋可用性レベル）×脆弱性（実際に侵害が起きる可能性）
    - 経済的、社会的損失とは
      - 顧客に対する金銭的補償

Expand - Collapse

    - サービスを復旧させるための費用
    - サービスが止まったことによる機会損失
    - 社会的信用の喪失による機会損失
  - （侵害の発生頻度が高く、侵害が顕在化した場合の経済的、社会的損失の大きさ（深刻さ）（直接被害額、間接被害額）を勘案してセキュリティ対策の優先度を決める。発生頻度を減らす、被害を減らす、保証を考える）
  - 残留リスクをどこまで許容できるかは、経営者の判断
  - そのうえで管理的、人的、物理的、技術的対策をセキュリティポリシーとして策定（サンプルを参考に）

- まずは人的対策を
  - 侵害の70～80%は、内部職員のミス、故意
  - 人的対策、管理的対策、物理的対策を行い、それでもカバーできないことを技術的対策
  - 情報リテラシーを高めることが重要
  - 悪意があれば、技術的な対策はすり抜けられる
  - 退職者のセキュリティ対策も重要
  - ログを取っていることを示すだけでも職員に対する抑止効果は大きい
  - 技術的対策はどれだけ投資してもリスクは残る

  - 職員教育
    - セキュリティ侵害の70～80%は、人のミス、故意

    - 外部委託するなら、RFPを作って確実な審査（評価）ができる状態で
      - そうでなければ、業者に騙される

    - リスク評価、管理的対策はコンサルに頼んでも完全にはならない
    - まずは、営利企業である委託先候補の提案を鵜呑みにしない内部職員のスキルと知識の向上
    - 職員は、社会人の常識としてのITパスポート試験レベルを必須とする

- ビジネスの発展のために
  - 守りのIT投資としてのセキュリティ対策でも対策が第三者評価を受ければ、ビジネス拡大につながる攻めのIT投資にもなる
  - ISMS認証制度、プライバシーマーク
  - ビジネスの拡大・発展のための「攻めのIT投資」は、未知の世界でセキュリティリスクも高くなる。リスクの大きさと経済的効果を勘案して、セキュリティ対策の投資を考える

- 組織と役割
  - IPAは情報処理を振興する機構で、IT化を推進するために阻害要因の一つであるセキュリティ対策の情報を公開して啓発活動を行っている
  - 国の施策は、内閣サイバーセキュリティセンター（NISC）を中心に、METI、総務省、警察庁がそれぞれにセキュリティ対策の実施を行っている

Expand - Collapse

- 東京都はTCYSSを設置。東京都、警視庁、セキュリティ関係公的
  リティ関係機関で構成。情報を共有し、東京都に相談窓口を開設