Expand - Collapse

- Sec01-12相談対応において一般論として説明する内容
  - 【2017年12月1日】
  - 個別
    - 1　迷惑メール対策としては、
      - 不審なメールを絶対開かないこと。併せて、不審なメールを開かないよう経営者を含め社員全員に徹底指導すること。また、
      - メールレンタルサービスに対し、不審なメールに対しては、フィリタリングを掛けられないかを確認する。
    - 2　情報セキュリティーのための投資については、
      - サイバーセキュリティ対策の中で最もコストがかかるのが技術的対策。しかし全てのリスクに対して技術的対策をすることは困難。セキュリティー被害を受けた場合、その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要。また、システムを入れる際に、セキュリティーも同時に入れるなど、ＩＴとセキュリティー対策を一緒にすることも大切である。更に、経営者を含め、社員全員に対し、セキュリティーポリシーやガイドブックを作成したり、併せてＩＴパスポートの試験を受けさせることも大切である。
  - 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
  - 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
    - 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
    - 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
    - セキュリティ侵害の70～80%は、人のミス、故意
    - 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
  - まずは、人的対策、管理的対策、物理的対策、それでもカバーできないことを技術的対策
    - 技術的対策はどれだけ投資してもリスクは残る
    - 残留リスクをどこまで許容できるかは、経営者の判断
    - まずは情報資産（情報、情報機器）のリスク分析
    - 対策はリスクの高いものを優先する
    - 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）

Expand - Collapse

- （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[illegible]（深刻さ）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）
- 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）

⊟ 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、業者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

⊟ 守りのIT投資

⊟ 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

⊟ 攻めのIT投資
- 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

⊟ 組織について
- 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
- 東京都はTCYSSを設置。東京都、警視庁、セキュリティ関係公的機関、民間セキュ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