Expand - Collapse

- Sec01-15各種ガイドブック等での対策ポイント
  - 【2017年12月1日】
  - ■脅威の現状（マイクロソフト）
    - 1/3
      - 3 社に 1 社は、ライセンスが付与されていないソフトウェアの入手およびインストール時にマルウェアが見つかっています。（The Software Alliance (BSA | ザ・ソフトウェア・アライアンス) 調査）
    - 200 日以上
      - 侵入されてから、マルウェアを発見するまで 242 日かかっています(中央値)。（McKinsey & Co. 高度ネットワーク社会で出来ることとそのリスク: 企業への示唆 2014 年 1 月）
    - 4.2 億円
      - データ侵害に対する平均的なコストは 4.2 億円にのぼり、生産性低下など試算すると 360 兆円に達します。（McKinsey & Co. 高度ネットワーク社会で出来ることとそのリスク: 企業への示唆 2014 年 1 月）
    - 90%
      - 企業の 7 割はセキュリティ事故を経験、また 9 割は未知の脅威が侵入済みです。（トレンドマイクロ IT Japan 2015 2015 年 7 月）
  - ■中小企業経営者向け
    - ■経営者が認識する必要な「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））
      - 原則１ 情報セキュリティ対策は経営者のリーダシップのもとで進める
      - 原則２ 委託先における情報セキュリティ対策まで考慮する
      - 原則３ 情報セキュリティに関する関係者とのコミュニケーションは、どんなときにも怠らない
    - ■企業 として実施する「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））
      - 取組１ 情報 セキュリティ に関するリスクを認識し組織全体での対応方針を定める
      - 取組２ 情報セキュリティ対策を行うための資源（予約、人材など）を確保する
      - 取組３ 情報セキュリティのリスクを把握し、どこまで情報セキュリティ対策を行うのかを定めたうえで担当者に実行させる
      - 取組４ 情報セキュリティ対策に関する定期的な見直しを行う

Expand Collapse

- 取組５ 業務委託する場合や外部ITシステムやサービスを利用する場合は、自社で必要と考える情報セキュリティ対策が担保されるようにする
- 取組６ 情報セキュリティに関する最新動向を収集する
- 取組７ 緊急時の社内外の連絡先や被害発生時に行うべき内容について準備しておく

- ■セキュリティポリシー策定項目（中小企業の情報セキュリティ対策ガイドライン（第2版））
  - 1 組織的対策
  - 2 人的対策
  - 3 情報資産管理
  - 4 マイナンバー対応
  - 5 アクセス制御及び認証
  - 6 物理的対策
  - 7 IT機器利用
  - 8 IT基盤運用管理
  - 9 システムの開発及び保守
    - 社内でシステム開発を行う場合
  - 10 委託管理
    - 業務委託を行う場合
  - 11 情報セキュリティインシデント対応及び事業継続管理
  - 12 社内体制図
    - 従業員数２名以上
  - 13 委託契約書サンプル
    - 委託先と秘密情報や個人情報等の重要な情報の授受が発生する場合

- ■緊急時の対応（中小企業の情報セキュリティ対策ガイドライン（第2版））
  - ① 緊急時における 指揮命令と対応の優先順位決定
  - ② インシデントへの対応（インシデントレスポンス）
  - ③ インシデントの影響と被害分析
  - ④ 情報収集と自社に必要な情報の選別
  - ⑤ 社内関係者への連絡と周知
  - ⑥ 外部関係機との連絡

- ■情報セキュリティ ５か条（中小企業の情報セキュリティ対策ガイドライン（第2版））
  - ソフトウェアはつねに更新しよう

Expand - Collapse

- 機器に応じたマルウェア対策をしよう
- パスワードなど、認証を強化しよう
- 業務に使うすべてのサービスの設定を見直そう
- 脅威や攻撃の手口を知ろう

- ■サイバーセキュリティ経営の３原則 （サイバーセキュリティ経営ガイドライン Ver 1.0【METI】）
  - （１）経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
  - （２）自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要
  - （３）平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

- ■サイバーセキュリティ経営の重要１０項目（サイバーセキュリティ経営ガイドライン Ver 1.0【METI】）
  - ３．１．リーダーシップの表明と体制の構築
  - ３．３．リスクを踏まえた攻撃を防ぐための事前対策
  - ３．４．サイバー攻撃を受けた場合に備えた準備

- ■ サイバーセキュリティ経営チェックシート（サイバーセキュリティ経営ガイドライン Ver 1.0【METI】）
  - (1)サイバーセキュリティリスクの認識、組織全体での対応の策定
  - (2)サイバーセキュリティリスク管理体制の構築
  - (3)サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
  - (4)サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
  - (5)系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握
  - (6)サイバーセキュリティ対策のための資源（予算、人材等）確保
  - (7)ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
  - (8)情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
  - (9)緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
  - (10) 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

Expand - Collapse

- ■個人向け
  - ■インターネットを安全に利用するための情報セキュリティ対策９か条【NISC・IPA】
    - OS やソフトウェアは常に最新の状態にしておこう
    - パスワードは貴重品のように管理しよう
    - ログインID・パスワード絶対教えない用心深さ
    - 身に覚えのない添付ファイルは開かない
    - ウイルス対策ソフトを導入しよう
    - ネットショッピングでは信頼できるお店を選ぼう
    - 大切な情報は失う前に複製しよう
    - 外出先では紛失・盗難に注意しよう
    - 困ったときはひとりで悩まず まず相談
  - ■初心者の3原則【総務省】
    - 原則 1 ソフトウェアの更新
    - 原則 2 ウイルス対策ソフト（ウイルス対策サービス）の導入
    - 原則 3 IDとパスワードの適切な管理
- ■事例・トッピクス
  - ■中小企業における組織的な情報セキュリティ対策ガイドライン事例集【IPA】
    - Case 1. 従業員の情報持ち出し
    - Case 2. 退職者の情報持ち出し、競合他社への就職
    - Case 3. 従業員による私物PCの業務利用と Winnyの利用による業務情報の漏洩事故
    - Case 4. ホームページへの不正アクセス
    - Case 5. 無許可の外部サービスの利用
    - Case 6. 委託した先からの情報漏えい
    - Case 7. 在庫管理システム障害の発生
    - Case 8. 無線LANのパスワードのいい加減な管理
    - Case 9. IT管理者の不在
    - Case 10. 電子メール経由でのウイルス感染
  - ■最近の主な出来事（情報セキュリティ白書2016より）
    - 標的型攻撃により日本年金機構から個人情報が流出
    - インターネットバンキングの不正送金、被害額は過去最悪を更新
    - オンライン詐欺・脅迫被害が拡大
    - 広く普及しているソフトウェアの脆弱性が今年も問題に
    - DDoS攻撃の被害が拡大、IoT端末が狙われる

Expand Collapse

- 重要インフラへの攻撃と重要インフラのセキュリティを強化する国内の取り組み
- 法改正による政府機関のセキュリティ強化
- 企業のセキュリティ強化に経営層の参画が重要
- セキュリティ人材育成への取り組み
- 自動車・IoTのセキュリティ脅威が高まる

■情報セキュリティ 10 大脅威（組織）【IPA】

- 標的型攻撃による情報流出
- 内部不正による情報漏えいとそれに伴う業務停止
- ウェブサービスからの個人情報の搾取
- サービス妨害攻撃によるサービスの停止
- 踏み台にならないため、利用している機器も含めて管理
- ウェブサイトの改ざん
- 脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加
- ランサムウェアを使った詐欺・恐喝
- インターネットバンキングやクレジットカード情報の不正利用
- ウェブサービスへの不正ログイン
- 過失による情報漏えい