中小企業の生き残り作戦！

情報セキュリティ(1)
ISMS構築の手順
リスクアセスメント

株式会社IMEコンサルティング
代表取締役　立居場誠治

定期経営セミナー開催要領

- 場所
  大田区産業プラザ(Pio)　蒲田
- 日時
  6/22(金), 7/20(金)
  18:30から2時間程度
- テーマ
  –企業経営関連のテーマを時期と希望により選定する
- 集客
  –お仲間の勧誘など、ご協力をお願いしたい

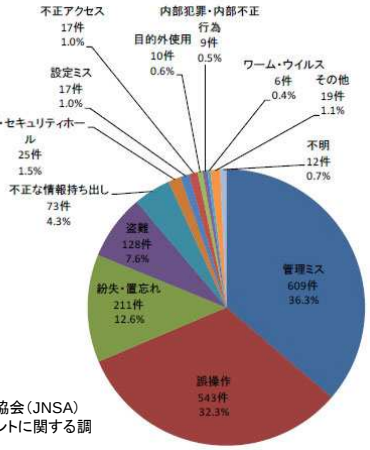
情報漏えい

漏えい原因件数比率

「管理ミス」36.3%
（前年比14.6%減少）

「誤操作」32.3%
（前年比8.3%増加）

「紛失・置忘れ」12.6%
（前年比4.7%増加）



出典：日本ネットワークセキュリティ協会（JNSA）
「2010年 情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」

ISMS構築の手順

1. ISMSの適用範囲を定義する
2. ISMSの基本方針を策定する
3. リスクアセスメントの体系的な取り組み方法を策定する
4. リスクを識別する
5. リスクアセスメントを実施する
6. リスクに対応した選択肢を明確にし、評価する
7. リスクに対応した管理目的及び管理策を選択する
8. 適用宣言書を作成する
9. 経営陣から残留リスクの承認並びにISMS導入及び運用の許可を得る

情報リスクとは何か

- そもそもリスクとは、何なのか?
- リスクについて考えるにあたっては、
- 以下の3点がキーワードとなる。
  –情報資産
  –脅威
  –脆弱性

リスクアセスメントの手法

GMITSでは、大別すると4つのリスクアセスメント手法を掲げている。

– ベースラインアプローチ
– 非形式的アプローチ
– 詳細リスク分析
– 組み合わせアプローチ

- GMITSは、ISO/IECが公表している技術報告書「ISO/IECTR13335 」で、情報セキュリティマネジメントのためのガイドラインと呼ばれるもので、情報セキュリティにおけるマネジメントの指針を技術的側面から示している。

GMITS : Guideline for the Management of IT Securityの略
参考資料GMITSは、JISでもTR X 0036として公表されている

リスクアセスメントの手順

- ISMS適用範囲の決定

1. リスクアセスメント手順の作成
2. 情報資産の洗い出し
3. 資産価値の評価
4. 脅威の分析
5. 脆弱性の分析
6. リスク値の産出
7. リスク対応評価

リスクアセスメント

- 管理するリスクの決定

1. リスクアセスメント手順の作成

2. 情報資産の洗い出し	3. 資産価値の評価
4. 脅威の分析	5. 脆弱性の分析
6. リスク値の産出	7. リスク対応評価

