中小企業の生き残り作戦！

情報セキュリティ(2)
ISMS認証基準付属書
詳細管理策

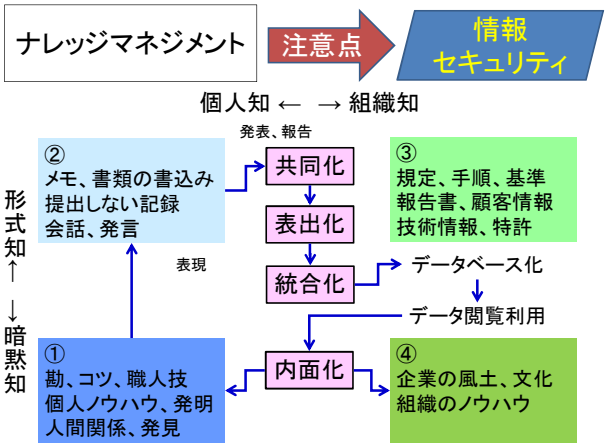
株式会社IMEコンサルティング
代表取締役　立居場誠治

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
  7/20(金)，8/31(金)，9/20(木)
  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

情報関連リスク例

中分類	No	小分類
情報システム関連	1	情報システムの障害、故障
	2	通信回線、システム障害、故障
	3	受発注、生産管理システムの不具合停止
	4	システムのバグ
	5	システムの陳腐化
	6	システムのバージョンアップの失敗
	7	システム構築、統合の失敗
	8	サイバーテロ、ハッキング等
	9	ワーム、ウイルス感染
オペレーション	1	情報システムのオペレーションミス
	2	受発注、生産管理システムの操作ミス
	3	メールの送受信ミスによる情報流出
	4	FAXの送受信ミスによる情報流出
	5	郵便、宅配等の発送間違い
	6	機密情報持出時の紛失・流出
	7	退職等による情報・技術等の流出・喪失
	8	操作ミスによるデータの消滅・逸失
情報漏えい	1	顧客、取引先情報漏えい
	2	個人情報の漏えい
	3	機密情報の漏えい
	4	技術、原価情報の漏えい
	5	経営情報の漏えい



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

ISMS認証基準付属書詳細管理策

1.情報セキュリティ基本方針
2.組織のセキュリティ
3.資産の分類及び管理
　→ マネジメントシステムに関する全般的な項目

4.人的セキュリティ
5.物理的及び環境的セキュリティ
6.通信及び運用管理
7.アクセス制御
　（6,7：情報システム等専門的な内容）
8.システムの開発及び保守
　→ ISMSに関する技術的な機能

9.事業継続管理
10.適合性
　→ 災害対応や法的準拠など、組織の存続にかかわる内容

1.情報セキュリティ基本方針

情報セキュリティ基本方針の策定が重要であることを指摘すると共に、セキュリティ基本方針の策定を規定している。

1.(1)情報セキュリティ基本方針

2.組織のセキュリティ

組織が情報セキュリティマネジメントに取り組む姿勢を規定している。

2.(1)情報セキュリティ基盤
2.(2)第三者によるアクセスのセキュリティ
2.(3)外部委託

運営委員会で管理する
専門家による助言は、社内の情シスでもOK！

3.資産の分類及び管理

組織が持つ情報資産を明らかにすると共に、
その責任者を明らかにすることを規定している。

3.(1)資産に対する責任
3.(2)情報の分類

4.人的セキュリティ

人的な問題によって起こりうるリスクを軽減するために、職務定義や利用者の訓練、事故への対処方法などを規定している。

4.(1)職務定義及び雇用におけるセキュリティ
4.(2)利用者の訓練
4.(3)セキュリティ事件。事故及び誤作動への対処

情報漏えい・流出原因の8割以上は人的要因！
実行性には重要なポイント

5.物理的及び環境的セキュリティ

物理的環境でのセキュリティについて話及し、施設の入退室管理、装置の設置や保護などを規定している。

5.(1)セキュリティが保たれた領域
5.(2)装置のセキュリティ
5.(3)その他の管理策

過剰設定に注意！
ICカードによる入退室管理は必須ではない

6.通信及び運用管理

情報通信や盾報処理全般に関する運用上のセキュリティポイントについて規定している。

6.(1)運用手順及び責任
6.(2)システムの計画作成及び受入れ
6.(3)悪意あるソフトウェアからの保護
6.(4)システムの維持管理
6.(5)ネットワークの管理
6.(6)媒体の取扱い及びセキュリティ
6.(7)情報及びソフトウェアの交換

7.アクセス制御

利用者に焦点を合わせたアクセスや、ネットワークおよびオペレーティングシステムなど、個々の情報処理装置に対するアクセスを規定している。

7.(1)アクセス制御に関する事業上の要求事項
7.(2)利用者のアクセス管理
7.(3)利用者の責任
7.(4)ネットワークのアクセス制御
7.(5)オペレーティングシステムのアクセス制御
7.(6)業務用ソフトウェアのアクセス制御
7.(7)システムアクセス及びシステム使用状況の監視
7.(8)移動型計算処理及び遠隔作業

8.システムの開発及び保守

基盤システムや業務用ソフトウェア、または利用者開発型のソフトウェアのセキュリティ確保について規定しています。

8.(1)システムのセキュリティ要求事項
8.(2)業務用システムのセキュリティ
8.(3)暗号による管理策
8.(4)システムファイルのセキュリティ
8.(5)開発及び支援過程におけるセキュリティ

9.事業継続管理

災害やセキュリティ障害によって、事業活動が継続できなくなった際の管理策について規定している。

9.(1)事業継続管理の種々の面

10.適合性

情報システムの設計、運用が法的要求事項に適合するよう求めており、その際の管理策について規定している。

10.(1)法的要求事項への適合
10.(2)セキュリティ基本方針及び技術適合のレビュー
10.(3)システム監査の考慮事項