情報セキュリティマネジメント試験合格講座 07

- 情報セキュリティ諸規程

1. 情報セキュリティポリシ
   組織の情報資産を適切に取り扱うための方針や基準を明文化したもの。
   標準的には、「情報セキュリティ基本方針（ポリシ）」、「情報セキュリティ対策基準（スタンダード）」、「情報セキュリティ実施手順（プロシージャ）」の三階層の文書構成をとり、基本方針で定められた内容が階層を追って具体化される。

   ✓ 情報セキュリティポリシの策定
   PDCA サイクルの、P：Plan(計画)にあたり、情報セキュリティマネジメントを確立するための計画段階である。

   ➢ 情報セキュリティポリシの標準的な策定手順
   （1）組織・体制を確立
   （2）基本方針の策定
   （3）守るべき情報資産を把握と分類
   （4）情報資産のリスクアセスメント
   （5）導入対策・管理策の取捨選択
   （6）対策基準の策定
   （7）対策基準の周知徹底
   （8）実施手順の策定

   ➢ 情報セキュリティポリシの承認と発行
   「基本方針」や「対策基準」は、組織の最終的な意思決定者である経営者レベルが関与し、情報セキュリティの全社的な組織であるセキュリティ委員会などで策定、承認及び見直しも行うこととされている。実際の作業はワーキンググループや情報セキュリティ部門で行い、承認を情報セキュリティ委員会で行うことがある。これに対して「実施手順」は、一般的に、情報システム毎、あるいは部門毎に作成・管理され、各部門の部門長が承認者となる。

2. 情報セキュリティ基本方針（ポリシ）
情報セキュリティの目標と、その目標を達成するために企業・組織がとるべき行動を社内外に宣言する文書。事業、組織、所在地、資産及び技術の特徴を考慮して策定する。有効性・妥当性を維持するために改善を行い、すべての従業員に対して周知させる必要がある。

✓ 情報セキュリティ基本方針の策定
「なぜセキュリティが必要か」という「Why」について規定し、何をどこまで守るのか、誰が責任者かを明確にする。情報セキュリティのための経営陣の方向性及び支持を規定する。

3. 情報セキュリティ対策基準（スタンダード）
求められる情報セキュリティレベルを確保、維持するために必要となる対策の内容や遵守事項などを記述する文書。組織的に情報セキュリティ対策を行うためのルール集であり、人事規程や就業規程など、企業の構成員が守るべき規程類に相当する。

✓ 情報セキュリティ対策基準の策定
基本方針で作成した目的を受けて、「何を実施しなければならないか」という「What」について記述する。実際に守るべき規程を具体的に記述し、適用範囲や対象者を明確にする。

4. 情報セキュリティ実施手順（プロシージャ）
情報セキュリティ対策基準が求める対策を実施するための詳細な手続きや手順などを記述する文書。

✓ 情報セキュリティ実施手順の策定
対策基準で定めた規程を実施する際に、「どのように実施するか」という「How」について記述する。マニュアル的な位置づけの文書であり、詳細な手順が示される。

5. 個人情報保護方針／プライバシポリシ（Privacy Policy）
組織が個人情報保護法に基づき収集した個人情報を、どのように扱うのかを定めた文書のこと。具体的な利用目的や利用の範囲および、どのような手段で管理・保護を行うかなど規定される。

6. 無形資産
   特許、商標権、著作権などの知的財産権、顧客情報、ブランドなど、企業で培われた価値、従業員の経験・技能などのように物理的な実体を伴わない資産。

7. コーポレートガバナンス(Corporate Governance)
   企業経営を規律するための仕組み。企業経営の透明性を確保するために、企業は誰のために経営を行っているか、トップマネジメントの構造はどうなっているか、組織内部に自浄能力をもっているかなどの視点で、企業活動を監督・監視する。

8. IT ガバナンス
   IT を適切に活用する組織能力。コーポレートガバナンスにとって、不可欠な要素のひとつ。経営陣及び取締役会が担うべき責務であり、IT が組織の戦略と組織の目標を支え、あるいは強化することを保証する、リーダーシップの確立や、組織構造とプロセス構築の仕組み。

9. 情報セキュリティガバナンス
   コーポレートガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること。実現を促すツールとして、情報セキュリティ対策ベンチマーク、情報セキュリティ報告書モデル、事業継続計画策定ガイドラインが提言されている。

10. 内部統制
    経営戦略や事業目的等を、組織として機能させ達成していくための仕組み。

11. IT 統制
    内部統制およびその他の基本的要素を機能させることにより IT が有効かつ適正に利用されるように監視、記録、統制を行い、組織の健全性を保証する仕組み。アクセス制限などの予防統制とモニタリングなどの発見統制、全般統制と業務処理統制などの分類がある。

12. 固有リスク
    JIS Q 31000:2010(リスクマネジメントー原則及び指針)では「業務の性質や本来有する特性から生じるリスク」と定義されている。

13. 統制リスク
JIS Q 31000:2010(リスクマネジメントー原則及び指針)では「監査手続を実施しても監査人が重要な不備を発見できないリスク」と定義されている。

14. エンタープライズアーキテクチャ
既存の業務と情報システムの全体像及び将来の目標を明示し、業務手順や情報システムの標準化、組織の最適化などを進めることによって、組織運営の効率化を図り、IT ガバナンスを強化し、経営の視点から IT 投資効果を高める方策。

15. IT 経営力指標
経済産業省が策定した、IT の活用度合いを測る上で、IT 活用による新ビジネスモデル創出力や IT 基盤の構築度合いなどの七つの機能を評価軸として四つのステージで評価する指標。

16. BI(Business Intelligence)
企業内の膨大なデータを蓄積し、分類・分析・加工することで、企業の迅速な意思決定に活用しようとする手法。

17. コンティンジェンシープラン(Contingency Plan)
緊急時対応計画。計画の策定対象が潜在的に抱える脅威が発生した場合に、その緊急事態を克服するため取るべき手続きが記述された危機管理の計画。

18. BCP(Business Continuity Plan)
事業継続計画。自然災害、大火災、テロ攻撃などの緊急事態に遭遇した場合において、事業資産の損害を最小限にとどめつつ、中核となる事業の継続あるいは早期復旧を可能とするために、平常時に行うべき活動や緊急時における事業継続のための方法、手段などを取り決めておく計画。

〔問題集〕

- ✓ **石川敢也(共著)「情報セキュリティマネジメント要点整理＆予想問題集」 翔泳社**
- ✓ **情報セキュリティマネジメント試験合格講座** http://rakupass.com/security/