関連分野の知識項目 07

- システム監査

1. インシデント
   思いがけない出来事、偶発現象。適切な処理が行われないと事故となる可能性のある保安上の脅威となる事象。

2. アクシデント
   思いがけない事故、不運な災難、予期しない故障。偶然に起こってしまった良くない(嬉しくない)事象。

3. ヒヤリハット
   重大な災害や事故に直結する可能性があった事象。ハインリッヒの法則によれば、「重大な事故の陰には 29 倍の軽微な事故、300 倍の異常が存在する」。

4. RTO(Recovery Time Objective)
   BCP(Business Continuity Plan、事業継承計画)などで策定される目標復旧時間。システムが停止してから業務が復旧するまでの時間的な目標。

5. RPO(Recovery Point Objective)
   どの時点までデータをバックアップしているかを定めた目標復旧時点。例えば「RPO 0」なら最新のバージョンに、「RPO 7」なら一週間前のデータに復旧できる。

6. ファシリティマネジメント(Facility Management)
   土地、建物、構築物、設備などの業務用不動産を経営にとって最適な状態で保有、運営して、維持するための総合的な管理手法。

7. SPD (Surge Protective Device)
   電源線や通信線に繋がったままの状態で、過電圧や過電流から通信機器を守るための仕組みや、対策として設置するサージ防護デバイス。

8. UPS(Uninterruptible Power Supply)
   電源の瞬断に対処したり, 停電時にシステムを終了させたりするのに必要な時間だけ電力を供給することを目的とした装置。

9. 内部統制（Internal Control）
組織のルールや業務プロセスを、適切に運用することや、そのための仕組みや業務の適正を確保するための体制。

10. 統制環境
組織の気風を決定し、統制に対する組織内のすべての者の意識に影響を与えるとともに、基本的要素の基礎となり、リスク評価とリスク対応、統制活動、情報と伝達、モニタリング、IT への対応に及ぼす基盤。

11. IT 統制
効果的な内部統制の実現のための目標を設定し、ITを取り入れて企業内の情報システムを管理するもの。IT を有効かつ効果的に利用することであり、IT が有効かつ適正に利用されるように監視、記録、統制を行う体制。

- ✓ 監視（モニタリング）
システムの稼動状況の把握し、サーバへアクセスする際に承認が得られているか、予定された通りの作業を実施しているかの確認を行う作業。

- ✓ 記録（ロギング）
システムの稼働状況、オペレータの操作、データベースやネットワークへのアクセス状況などを、時系列で記録に残す作業。

- ✓ 統制（コントロール）
システムへのアクセスやログインを制御し、承認されていないアクセスや許可されていないログイン、予定されていない操作を抑止し制御する作業。

12. IT 全般統制
業務処理統制が健全かつ有効に機能する基盤・環境を構築すること。IT を利用した情報システムを適切に管理、運用することによって、業務の実行管理が有効に機能するような環境を構築・維持していく作業。

13. IT 業務処理統制
個々の業務処理システムにおいて、データの正確性、正当性、網羅性、維持継続性を確保する作業。

14.

15. コーポレートガバナンス(Corporate Governance)
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、監視する仕組み。

〔参考〕
- ✓ ガバメント(Government):支配。政府。法的拘束力のある統治。
- ✓ ガバナンス(Governance):統治。組織や社会のメンバーや利害関係者が、主体的に関与を行なう、意思決定、合意形成。

16. IT ガバナンス
企業が競争優位性の構築を目的としてIT戦略の策定及び実行をコントロールし、あるべき方向へと導く組織能力。ITへの投資、効果、リスクを継続的に最適化する為の組織的な仕組み。

17. コンプライアンス(Compliance)
法令順守(遵守)。事業活動に関わる法令、会計基準、規範、倫理、ガイドラインを順守すること。

18. 職務分掌
組織において、それぞれの職務が果たすべき責任や職責を果たす上で必要な権限を明確に規定するために、職務ごとの役割を整理して配分する作業。

19. CSA(Control Self-Assessment、統制自己評価)
監査部が被監査部門を評価するのではなく、被監査部門が、自らの活動を主観的に検証し、評価すること。

20. 可監査性(Auditability)
処理の正当性や内部統制を効果的に監査、またはレビューできるように情報システムが設計・運用されていること。

21. システム監査
被監査部門ら独立した客観的な立場で、情報システムを総合的に点検・評価し、システムが経営に貢献しているか、不正が行われていないかなどを判断して、助言や勧告を行う活動。

22. 監査証跡(Audit Trail)
システム監査人が追跡できるように、情報システムのデータ処理内容や処理過程を、時系列に記録したもの。

23. 監査証拠(Audit Evidence)
監査人が監査報告書に記載する監査意見(評価・指摘・勧告)を立証するために必要となる事実が記載された資料。

24. システム監査基準
経済産業省が策定した、システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範。

25. システム管理基準
経済産業省が策定した、組織体が主体的に経営戦略に沿って効果的な情報システム戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範。

26. 情報セキュリティ監査
情報資源全般を対象として、運用管理状況や情報セキュリティ対策実施状況の適切性を判断するための監査。

27. 情報セキュリティ監査基準
経済産業省が策定した、情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範。

28. 情報セキュリティ管理基準
経済産業省が策定した、組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロール(管理策)を整備・運用するための実践的な規範。