情報セキュリティマネジメント試験合格講座 01

- 情報セキュリティの基礎用語

1. 情報セキュリティ(Information Security)
   情報の機密性、完全性、可用性を維持すること。さらに、真正性、責任追跡性、否認防止、信頼性などの特性を維持することを含めることもある。

2. 機密性(Confidentiality)
   アクセス権を持つものだけが、情報にアクセスできることを確実にする特徴のこと。認められていないプロセスに対して、情報を非公開にできる特性。

3. 完全性(Integrity)
   情報が正確であり、改ざんされたり破壊されたりせず、正当性、正確性、網羅性、一貫性を維持できる特性。

4. 可用性(Availability)
   情報を必要に応じて利用できる特徴のこと。認められた利用者が、必要なときに情報にアクセスできる特性。

5. 真正性(Authenticity)
   利用者、プロセス、システムなどが、主張どおりであることを確実にする特性。

6. 責任追跡性(Accountability)
   情報資産へ行われたある操作についてユーザと動作が一意に特定でき、過去に遡っても追跡できる特性。

7. 否認防止(Non-Repudiation)
   行った操作や発生した事象を後になって否認されないように証明することができる特性。

8. 信頼性(Reliability)
   情報システムにおいて実行した処理に欠陥や矛盾がなく、期待した処理が確実に行われ整合性が取れていることを確実にする特性。

9. 有効性（Effectiveness）
   計画した活動を実行し、計画した結果を達成した程度。

10. プロセス（Process）
    インプットをアウトプットに変換する、相互に関連するまたは相互に作用する一連の活動。

11. 情報資産（Information Asset）
    セキュリティ対策において守るべき対象物。情報そのものだけでなく、情報を取り扱う仕組みも含めた概念。

12. 方針（Policy）
    トップマネジメントによって正式に表明された組織の意図および方向付け。

13. ステークホルダ（Stakeholder）
    意思決定もしくは活動に影響を与え、影響されることがある、または影響されると認知している、あらゆる人または組織。

14. 情報セキュリティガバナンス（Governance of Information Security）
    組織の情報セキュリティ活動を指導し、管理するシステム。

15. 監視（Monitoring）
    システム、プロセスまたは活動の状況を明確にすること。状況を明確にするために、点検、監督、または注意深い観察が必要な場合もある。

16. 監査（Audit）
    監査基準が満たされている程度を判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセス。

17. レビュー（Review）
    確定された目的を達成するため、対象となる事柄の適切性、妥当性および有効性を決定するために実行される活動。

18. 検証（Verification）
    客観的証拠を提示して、規定要求事項が満たされていることを確認すること。

19. 属性（Attribute）
人手または自動的な手段によって、定量的または定性的に識別できる対象物の特性または特徴。

20. 事象（Event）
ある一連の周辺状況の出現または変化。発生が一度以上であることがあり、幾つかの原因をもつことがある。事態（Incident）または事故（Accident）と呼ばれることがある。

21. リスク（Risk）
目的に対する不確かさの影響。「影響」とは、期待されていることから、好ましい方向または好ましくない方向に乖離（かいり）すること。

22. リスクレベル（Level of Risk）
結果と起こりやすさの組合せとして表現されるリスクの大きさ。

23. 脆弱性（Vulnerability）
組織体制や情報システム、物理環境、業務プロセスなどに内在し、損失を発生しやすくしたり、拡大させたりする欠陥や弱点。

24. 脅威（Threat）
情報資産の機密性、完全性、可用性を脅かす存在。情報システムに悪影響を与えて損失を発生させる直接の原因。

25. 攻撃（Attack）
資産の破壊、暴露、改ざん、無効化、盗用、認可されていないアクセスや使用の試み。

26. 情報セキュリティインシデント（Information Security Incident）
望まない情報セキュリティ事象、または予期しない情報セキュリティ事象であって、事業運営を危うくし、情報セキュリティを脅かす確率が高いもの。

27. 抑止・抑制
人の意識やモラル・倫理観に対して働きかけて、犯罪や不正行為を思いとどまらせること。

28. 予防・防止
システムの脆弱性を改善したり、セキュリティ対策を施したりすることで、被害を受けにくい堅牢な状態にすること。

29. 検知・追跡
攻撃や不正を速やかに発見するとともに、原因や影響範囲の特定に必要な情報を取得すること。

30. 要求事項(Requirement)
明示されている、通常暗黙のうちに了解または義務として要求されている、ニーズまたは期待。

31. 不適合(Nonconformity)
要求事項を満たしていないこと。

32. 是正(ぜせい)処置(Corrective Action)
不適合の原因を除去し、再発を防止するための処置。

33. パフォーマンス(Performance)
測定可能な結果。定量的または定性的な所見のいずれにも関連し得る。

34. 継続的改善(Continual Improvement)
パフォーマンスを向上するために繰り返し行われる活動。

35. マネジメントシステム(Management System)
方針、目的およびその目的を達成するためのプロセスを確立するための、相互に関連または相互に作用する、組織の一連の要素。

〔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/