情報セキュリティマネジメント試験合格講座 06

- リスクマネジメント

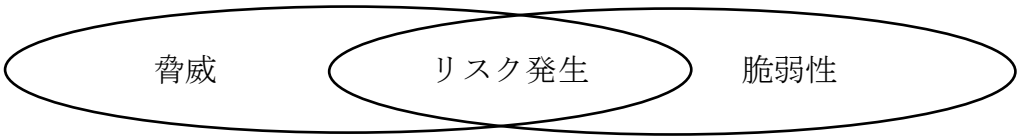
1. 脅威／脆弱性／リスク

   - ✓ 脅威:システム又は組織に危害を与える事故の潜在的原因
   - ✓ 脆弱性:脅威によって影響を受ける内在する弱さ
   - ✓ リスク:ある脅威が脆弱性を利用して損害を与える可能性
   - ✓ リスク因子:脅威と脆弱性

2. リスクマネジメント(Risk Management)
   リスクについて、組織を指揮統制するための調整されたプロセス。一般的に、(1)リスクの特定→(2)リスクの大きさの算定→(3)リスクの大きさの評価→(4)対策の導入の手順になる

3. リスクアセスメント(Risk Assessment)
   リスク特定、リスク分析、リスク評価までの全てのプロセス。守るべき対象である情報資産で発生する可能性のある脅威と、脅威の発生確率や発生した場合の影響度等を評価する方法のこと。

4. リスクの発生可能性
   リスクの発生可能性＝脅威×脆弱性



5. リスク基準
   リスクの重大性を評価する目安の条件。リスクに対する対応の判断、対応する場合の優先順位の決定を判断するための指標。

6. リスク評価
   リスクの重大さを決定するために、算定されたリスクを、与えられたリスク評価基準と比較するプロセス。

7. リスク対策基準
基本方針の内容を受けて具体的なルールである管理策。管理策は、情報セキュリティ上のリスクを減らすための対応策のことで、(1)技術的対策、(2)管理的対策(人的対策・組織的対策・物理的(環境的)対策を含む)の二つに分類される。

8. リスク選好(Risk Appetite)
組織に追求する又は保有する意思があるリスクの量及び種類。

9. 残留リスク(Residual Risk)
リスク対応後に残るリスク。特定されていないリスクも含まれる場合がある。「保有リスク」とも呼ばれる。

10. リスクコミュニケーション
顧客、潜在顧客、株主、関係省庁等の関係者において必要な情報が何かを把握し、情報を提供すること。

11. リスク分析
リスクの特性を理解し、リスクを算定し、リスクレベルを決定するプロセス。リスク評価及びリスク対応に関する意思決定の基礎を提供する。

- ✓ ベースラインアプローチ
既存の標準や基準をもとにベースライン(自組織の対策基準)を策定し、チェックしていくリスク分析手法。

- ✓ 非形式的アプローチ
コンサルタント又は組織や担当者の経験、判断によりリスクアセスメントを行うリスク分析手法。

- ✓ 詳細リスク分析
情報資産に対して、資産価値、脅威、脆弱性、セキュリティ要件を識別し、リスクを評価していくリスク分析手法。

- ✓ 組合せアプローチ
複数のリスク分析手法を併用するアプローチ。よく用いられるのは、ベースラインアプローチと詳細リスク分析の組合せで、両方のメリットが享受できる。

12. 定性的リスク分析
リスクの発生確率と影響度の査定、その組み合わせを基にして、リスク分析や対応の優先順位を決めるプロセス。

13. 定量的リスク分析
特定したリスクが目標全体に与える影響を分析して、数値によるリスクの等級付けを行うプロセス。

14. リスクマトリックス
縦軸を発生頻度や発生確率、横軸を損失の影響度として、リスクの大きさを表現した図。

リスクマトリックスの例

	影響度 小	影響度 大
発生頻度 大	昼飯のことを考えて講義に集中していない	講義中に爆睡している
発生頻度 小	教科書を持ってこない	講義を欠席する

15. リスクコントロール
危険の発生を防止し、損害を最小限に食い止めるための手段。リスクの回避、防止、低減、分散、結合が該当する。

16. リスクヘッジ（Risk Hedge）
将来の危険を予測して起こりうるリスクを回避したり、リスクの大きさを軽減したりする工夫のこと。

17. リスクファイナンシング（Risk Financing）／リスクファイナンス
リスクそのものを変えるのではなく、リスクの財務的影響を最小限に軽減させる手段。リスクの移転、保有が該当する。

18. リスク回避
脅威発生の要因を停止あるいは全く別の方法に変更することにより、リスクが発生する可能性を取り去る対応。リスクを保有することによって得られる利益に対して、保有することによるリスクの方が極端に大きな場合に有効。例えば、外部とのネットワーク接続の遮断、Web での情報公開を停止するなど。

19. リスク低減
脆弱性に対して情報セキュリティ対策を講じることにより、脅威発生の可能性を下げる対応。発生頻度を減少する損失予防、影響を小さくする損失軽減、情報資産を分散しておくリスク分離、集中させて管理し易くするリスク結合（集中）に分類できる。例えば、保存する情報を暗号化しておく、生体認証を利用した入退室管理を行う、従業員に対する情報セキュリティ教育の実施など。

20. リスク移転／リスク共有
リスクを他社などに移す対応。リスクがすべて移転できたり、共有できたりするわけではなく、金銭的なリスクなど、リスクの一部のみが移転可能である。例えば、リスク保険などで損失を充当したり、システムの運用を他社に委託したりするなど。

21. リスク保有
リスクの影響が小さいため、特にリスクを低減するためのセキュリティ対策を行わないで受容する対応。実施すべきセキュリティ対策が見当たらない場合や、コストに相当するリスク対応の効果が得られない場合等にも選択される。

22. ISSO（Information System Security Officer）
情報システムセキュリティ責任者。IT セキュリティプログラムマネージャおよびコンピュータセキュリティ責任者はリスクマネジメントを含む組織のセキュリティ導入計画に対して責任を負う。

〔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/