情報セキュリティマネジメント試験合格講座 午後試験対策 06

- サイバーセキュリティ経営の原則

1. サイバーセキュリティリスクの認識
   経営者は、IT 活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要である。

   サイバーセキュリティリスクは経営に重大な影響を及ぼす可能性がある一方で、新しいリスクであるために、従来の企業におけるリスク対策の延長上では対策が進みにくいことから、サイバーセキュリティリスク対策を進める上で、経営者がリーダーシップを発揮することが必要不可欠である。

   サイバーセキュリティ対策において、経営者によるリーダーシップが求められる具体的な事項として、例えば以下のものが考えられる。

   - ✓ サイバーセキュリティリスクを経営課題として位置づける。
   - ✓ CISO などを任命し、役割と責任を明確にするとともに経営者が実施を支援する。
   - ✓ 組織のサイバーセキュリティ対策の効果をチェックし、必要に応じて対策の見直しを行う。
   - ✓ 自社のビジネスパートナーなどとサイバーセキュリティ対策を共有し、連携して実施する。
   - ✓ これらを実施するために、サイバーセキュリティ対策に必要な情報を収集し、経営層に報告するための体制を構築する。

2. 経営者によるリーダーシップ
   自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、IT システム管理の委託先を含めたサイバーセキュリティ対策が必要である。

3. 適切なコミュニケーション
   平時および緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要である。

4. サイバーセキュリティ対応方針の策定
サイバーセキュリティリスク対策を実施するための対策方針、すなわちセキュリティポリシを策定する。

策定したセキュリティポリシは、会社の行動などの規範にするものであるため、経営層の承認を得ることによって自組織内部に対して権威付ける必要がある。

また、組織内に対しては周知徹底を図るために、また組織外に対してはセキュリティに関してその会社の姿勢を公に示すために、策定したセキュリティポリシを内部に浸透させるための活動と、外部に発信するための活動とが必要となる。

✓ 実施内容
(1) セキュリティポリシを策定し、経営者に承認を得る。
(2) 策定したセキュリティポリシを組織の内外に示す。

5. リスク管理体制の構築
サイバーセキュリティ対策を実施するためには、サイバーセキュリティリスク管理体制を構築することが重要である。

サイバーセキュリティリスク管理体制を構築する手順として、経営者は、セキュリティポリシに基づきCISOなどを任命する。CISOなどが主体となって、経営リスクに対応するサイバーセキュリティリスク管理体制を構築し、各関係者の責任の明確化などを検討する。

✓ 実施内容
(1) セキュリティポリシに基づき、CISOなどからなるサイバーセキュリティリスク管理体制を構築する。
(2) サイバーセキュリティリスク管理体制においてCISOなどや各関係者の責任を明確にする。
(3) 組織内のリスク管理体制が既に存在する場合、サイバーセキュリティリスク管理体制との関係を明確に規定する。

6. リスクの把握、目標と対応計画策定
サイバーセキュリティリスクを把握し、リスクに応じた対策の目標と計画を策定する。

✓ 実施内容

(1) 組織内に存在する資産の中で、守るべき資産を特定する。
(2) サイバー攻撃の脅威を識別する。
(3) サイバーセキュリティリスクが事業にいかなる影響があるかを推定し、リスクを把握する。
(4) サイバーセキュリティリスクの影響の度合いに応じた、リスクの低減、回避、移転などの目標や計画を策定する。また、サイバーセキュリティリスクの影響の度合いに従って対策しないと判断したものを残留リスクとする。

● リスク分析手法の種類

7. 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、チェックしていく方法。簡単にできる方法であるが、選択する標準や基準によっては求める対策のレベルが高すぎたり、低すぎたりする場合がある。

8. 非形式的アプローチ
コンサルタントまたは組織や担当者の経験、判断によりリスク分析を行う方法。短時間に実施することが可能であるが、属人的な判断に偏る恐れがある。

9. 詳細リスク分析
情報資産に対し「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。厳密なリスク評価が行えるものの多大な工数や費用がかかる。

10. 組合せアプローチ
複数のアプローチの併用。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。ベースラインアプローチと詳細リスク分析の両方のメリットが享受できる。

11. リスク対応方法の検討
リスク対応には、大きく分けて(1)低減、(2)保有、(3)回避、(4)移転があり、事業に与える影響の度合いに従いこれらの対応方法を決定する。

一般的にリスク発生可能性が高いもの、あるいはリスクが発生した場合の損害が大きいものについては、低減、回避、移転などの対応を検討する。

一方、リスク発生可能性が低く、かつリスクが発生した場合の損害が小さいものについては、対策を取らず残留リスクとして保有（受容）することになり。また特に「許容できるリスクのレベル」を超えているが、対策をしないで保有する残留リスクは、経営的な判断が必要になる場合があるため、経営層がその残留リスクは受容できる範囲であることを承認する必要がある。

(1) 低減
脆弱性に対してサイバーセキュリティの様々な対策を講じることにより、脅威発生の可能性を下げることである。例えば、マルウェア対策ソフトを導入する、外部記憶媒体の接続を制限するなどが該当する。

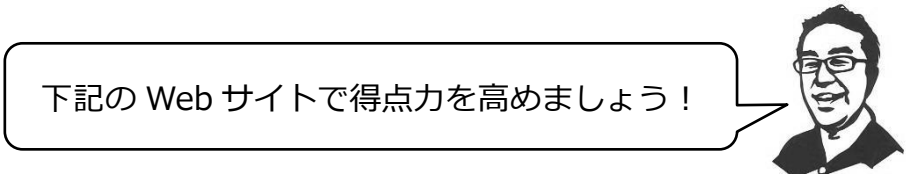
(2) 保有
リスクの持つ影響力が小さいため、特段リスク低減のための対策を講じず、許容範囲内として受容することである。

- ✓ 残留リスク
  対策を講じた後に残ったリスク、および対策されずに残ったリスク。

(3) 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で、リスクが発生する可能性を取り去ることである。例えば、外部からの不正アクセスという脅威に対し、機密情報が保存されているサーバは外部接続を行わないことなどが該当する。

(4) 移転
リスクを他者などに移すことであり、保険の活用や守るべき資産を外部の専門企業へ委託することなどが該当する。

出典：IPA「サイバーセキュリティ経営ガイドライン」



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