関連分野の知識項目 11

- ガイドライン

1. システム管理基準
   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。

2. ソフトウェア管理ガイドライン
   ソフトウェアの違法複製等を防止するため、法人や団体等を対象として、ソフトウェアを使用するに当たって実行されるべき事項をとりまとめたもの。

3. 情報セキュリティ管理基準
   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、適切な管理策を整備・運用するための実践的な規範。情報セキュリティマネジメントにおける管理策のための国際標準規格である ISO/IEC 17799:2000（JIS X 5080:2002）を基にしている。

4. 情報セキュリティ監査基準
   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。

   ✓ 情報セキュリティ監査
   独立かつ専門的な立場から、組織体の情報セキュリティの状況を検証または評価して、情報セキュリティの適切性を保証し、情報セキュリティの改善に役立つ的確な助言を与える活動。

   ✓ 情報セキュリティ監査人
   情報セキュリティ監査を実施する者。情報セキュリティ監査を実施する目的および対象範囲、並びに権限と責任は、文書化された規程または契約書等により明確に定められていなければならない。

(1) 独立性

(ア) 外観上の独立性

情報セキュリティ監査人は、情報セキュリティ監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。

(イ) 精神上の独立性

情報セキュリティ監査人は、情報セキュリティ監査の実施に当たり、偏向を排し、常に公正かつ客観的に監査判断を行わなければならない。

(ウ) 職業倫理と誠実性

情報セキュリティ監査人は、職業倫理に従い、誠実に業務を実施しなければならない。

(2) 専門能力

情報セキュリティ監査人は、適切な教育と実務経験を通じて、専門職としての知識および技能を保持しなければならない。

(3) 守秘義務

情報セキュリティ監査人は、監査の業務上知り得た秘密を正当な理由なく他に開示し、自らの利益のために利用してはならない。

5. 情報セキュリティ監査基準 実施基準ガイドライン

「情報セキュリティ監査基準」のうち実施基準に係る基本的な考え方を踏まえ、特に留意すべき事項、および情報セキュリティ監査実施上の手順について示したもの。

6. 情報セキュリティ監査基準 報告基準ガイドライン

「情報セキュリティ監査基準」のうち、報告基準に係る基本的な考え方を踏まえ、特に留意すべき事項および情報セキュリティ監査報告書の雛形について示したもの。

7. 情報システム安全対策基準

情報システムの機密性、保全性および可用性を確保することを目的として、自然災害、機器の障害、故意、過失等のリスクを未然に防止し、また、発生したときの影響の最小化および回復の迅速化を図るため、情報システムの利用者が実施する対策項目を列挙したもの。

8. コンピュータ不正アクセス対策基準
コンピュータ不正アクセスによる被害の予防、発見および復旧並びに拡大および再発防止について、企業等の組織および個人が実行すべき対策をとりまとめたもの。

9. コンピュータウイルス対策基準
コンピュータウイルスに対する予防、発見、駆除、復旧等について実効性の高い対策をとりまとめたもの。

✓ コンピュータウイルス
第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、 次の機能をひとつ以上有するもの。

(1)自己伝染機能
自らの機能によって他のプログラムにコピーすることにより、他のシステムに伝染する機能。
(2)潜伏機能
発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能。
(3)発病機能
プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をしたりする機能。

10. サイバーセキュリティ経営ガイドライン
経済産業省では、独立行政法人情報処理推進機構が、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「三原則」と、責任者となる担当幹部（CISO など）に指示すべき「重要 10 項目」をまとめたもの。

✓ サイバーセキュリティ経営の三原則
(1) 経営者は、IT 活用を推進する中でリスクを認識し、リーダーシップによって対策を進めることが必要。
(2) 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セキュリティ対策が必要。
(3) 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。

11. ソフトウェア等脆弱性関連情報取扱基準
関係者に推奨する行為を定めることにより、脆弱性関連情報の適切な流通および対策の促進を図り、コンピュータウイルス、コンピュータ不正アクセス等によって不特定多数の者に対して引き起こされる被害を予防することで、高度情報通信ネットワークの安全性の確保に資することを目的とするためのガイドライン。

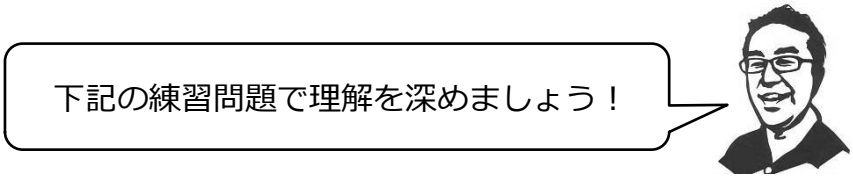
12. 事業継続計画策定ガイドライン
事業継続計画の構築を検討する企業にとって、考え方の理解を促すガイドラインであり、基本的な考え方から具体的な計画の構築手順を説明している。

- ✓ BCP（Business Continuity Plan）
潜在的損失によるインパクトの認識を行い実行可能な継続戦略の策定と実施、事故発生時の事業継続を確実にする継続計画。事故発生時に備えて開発、編成、維持されている手順および情報を文書化した事業継続の成果物。

  - ➢ BCP の特性
「目標復旧時間(RTO、Required Time Objective)」を定めること。この目標復旧時間は、事故・災害・事件などが発生した場合に、その発生時から基幹事業の再開までの企業が設定した時間である。

- ✓ BCM（Business Continuity Management）
組織を脅かす潜在的なインパクトを認識し、利害関係者の利益、名声、ブランドおよび価値創造活動を守るため、復旧力および対応力を構築するための有効な対応を行うフレームワーク、包括的なマネジメントプロセス。

- ✓ リスクファイナンシング
リスクが具現化し、損害が生じてしまう場合に必要な資金繰りをあらかじめ計画して準備しておく手法。



- ✓ **情報セキュリティマネジメント試験合格講座** http://rakupass.com/security/