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 01

- 基本用語の定義と関連する法律

1. 組織
   企業、地方公共団体などの法人その他団体。

2. 内部者
   役員、従業員（契約社員を含む）および派遣社員などの従業員に準ずる者（以下、総称して「役職員」）または、役職員であった者のうち、以下の二つのどちらかでも満たした者。

   （ア）組織の情報システムや情報（ネットワーク、システム、データ）に対して直接またはネットワークを介したアクセス権限を有する者

   （イ）物理的にアクセスしうる職務についている者（清掃員や警備員などを除く）

3. 内部不正
   違法行為だけでなく、情報セキュリティに関する内部規程違反などの違法とまではいえない不正行為も内部不正に含む。内部不正の行為としては、重要情報や情報システムなどの情報資産の窃取、持ち出し、漏えい、消去、破壊などを対象とする。また、内部者が退職後に、在職中に得ていた情報を漏えいする行為などについても、内部不正として取り扱う。

4. 重要情報
   組織が活用する情報のうち、その情報に対する内部不正により事業に影響を及ぼす可能性があるもの。企業や組織は情報が重要情報か否かを適切に判断する。また、重要情報には、格付けによって重要度を付与し、重要度ごとに取り扱いを定める。

5. 業務委託
   業務の一部を、業務委託契約(準委任契約、または請負契約)を結び委託すること。契約社員および労働者派遣業法で定義する労働者派遣は含まない。

6. 委託先
業務委託される側の組織。

7. 情報機器
通信機能を持つ、PC やサーバ、ノート PC やスマートデバイスなどのモバイル機器など。

8. 「望ましい」、「望まれる」
文末が「ねばならない」「する」「必要である」は、必須と考えられる対策を示している。「望ましい」「望まれる」という表現になっている対策は、より対策を強化したい場合を想定している。ただし、「例えば」で始まる文章は、どちらも規定していない。

9. 個人情報の保護に関する法律（個人情報保護法）
個人情報の漏えいや不正利用などから、個人の権利や利益を保護するために、個人情報を取り扱う事業者の順守すべき義務（安全管理措置や従業員と委託先の監督義務など）を規定している。

この義務規定に事業者が違反し、不適切な個人情報の取り扱いを行っている場合には、事業を所管する主務大臣が事業者に対し勧告、命令などの措置をとることができる。命令に従わなかった場合には、罰則の対象になる。

10. 行政手続における特定の個人を識別するための番号の利用などに関する法律（マイナンバー法）
マイナンバーをその内容に含む個人情報（特定個人情報）の利用範囲を限定するなど、一般の個人情報よりも厳格な保護措置を定めている。

正当な理由なく特定個人情報を提供したり、業務で知りえたマイナンバーを不正な利益を図る目的で第三者に提供・盗用したりした場合などの不正行為に対し、直接罰（行政命令などを経ることなく直ちに個人や組織に、刑事罰が適用されるもの）が設けられている。

マイナンバーを取り扱う事業者には、マイナンバーおよび特定個人情報の漏えいや不正利用を防ぐため、必要かつ適切な安全管理措置や従業者に対する監督が求められている。

11. 不正競争防止法
「営業秘密」の保護に関する規定が置かれており、内部者などが営業秘密を不正に使用・開示などを行うことに対して、民事上の差止請求などが認められているとともに、違法性の高い侵害行為については刑事罰も適用される。ただし、営業秘密として認められるには、その情報が有用かつ公然と知られておらず、秘密として管理されていることが必要になる。

12. 労働契約法
従業員が在職中に漏えいなどの内部不正を起こした場合に、従業員が労働契約に違反していることで、解雇、懲戒処分、損害賠償請求などを行う場合に関係する。従業員の内部不正によって会社に損害が生じた場合に、その従業員は労働契約上の債務不履行若しくは不法行為に基づく損害賠償請求の対象となることもある。

13. 労働者派遣法
従業員は、労働契約に付随する義務として秘密保持義務を負うが、派遣先企業と派遣労働者との間には労働契約が存在しない。

派遣先企業は、派遣労働者に秘密保持義務を直接負わせることはできないため、企業を介して派遣労働者に秘密保持をさせるためには、労働者派遣法への考慮が必要になる。

14. その他の法令
内部者による不正行為に関連する法制度としては、上記以外にも刑法（例えば窃盗罪、横領罪、背任罪など）や民法（例えば契約責任、不法行為責任など）、労働法理（例えば秘密保持義務違反、競業避止義務違反など）、公益通報者保護法も存在する。

- 内部不正を防ぐための管理のあり方

15. 基本方針（経営者の責任、ガバナンス）
組織における内部不正防止では、組織全体において効果的な対策を推進する上で経営者の関与が非常に重要であり、経営者のリーダーシップによる基本方針の策定および組織的な管理体制の構築が必要である。

経営者は経営課題のひとつとして、内部不正対策を捉えなければならない。その際には、情報資産に関わる機密性、完全性、可用性の観点からリスク管理の一環として、内部不正対策を検討することが重要である。

経営者が主導する形で、内部不正対策の体制と仕組みを構築し、運用させることで内部不正防止に対する意識や取り組みを組織内に徹底させることが可能となる。そして、結果的に個人情報保護および内部統制強化、企業に対する法的要請などにも対応できることに繋がる。

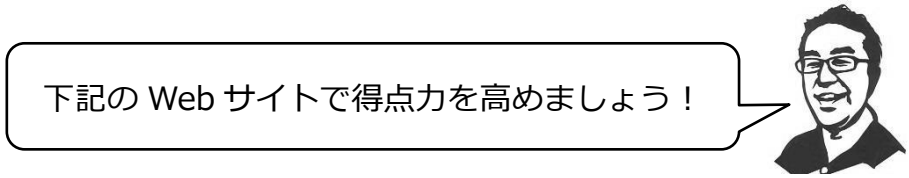
16. 機密性
情報へのアクセスを許可された人だけが情報を使うことができるようにすること。例えば、情報を漏えいしないことなど。

17. 完全性
情報および情報の処理方法が正確であり、権限のない者による情報の改変がないこと。例えば、情報を改ざんされないことなど。

18. 可用性
情報へのアクセスを許可された利用者が、必要なときはいつでも情報や情報システムにアクセスできるようにすること。例えば、システム障害が発生し、情報や情報システムが利用できない状態にならないことなど。

19. 経済産業省「サイバーセキュリティ経営ガイドライン」
経営者のリーダーシップによってサイバーセキュリティ対策を推進するため、サイバー攻撃から企業を守る観点より、経営者が認識すべき 3 原則と、経営者がセキュリティの担当幹部（CISO など）に指示をすべき重要 10 項目をまとめている。

出典：IPA「組織における内部不正防止ガイドライン」 2017 年 1 月改訂（第 4 版）



- ✓ **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/