

1. ISO27001認証制度を取得するための管理策について

ISO27001認証制度では、セキュリティ対策の具体的な指針として、管理目的及び管理策を設けています。

第1講では、個人情報保護法について学びますが、その前に**管理目的及び管理策**の内容を確認しておきましょう。個人情報保護法に深く関わる内容が、管理策として盛り込まれています。

管理目的及び管理策は11分野に分けられ、それぞれの**目的と管理策が規定**されています。ISO27001認証制度を取得しようとする企業は、この管理策に基づいてセキュリティ対策を講じていくことになります。

2. 附属書A管理目的及び管理策11分野の内容

1 セキュリティ基本方針

組織の情報セキュリティに対する方向性を示し、従業員の指針となるもの。「情報セキュリティ基本方針文書」に盛り込み、全従業員や外部関係者に通知・公表する。

2 情報セキュリティのための組織

情報セキュリティを実施する上で組織体制の整備に必要な事項を内部および外部組織で記載。

3 資産の管理

組織が持つ情報資産を適切に保護し、維持するための管理、責任、分類について。

4 人的資源のセキュリティ

従業員による誤り、盗難、不正行為、または設備の誤用等、人的な問題によって起こり得るリスクを軽減するための管理策。機密保持契約や、教育・訓練、事件・事故が起こった際の対処等。

5 物理的および環境セキュリティ

業務施設や情報を外部の物理的侵害から保護するための管理策。入退室管理、装置の設置や保護等。

6 通信および運用管理

情報通信や情報処理全般に対する運用上のセキュリティポイント。悪意のあるソフトウェアからの保護、情報のバックアップや各種記録の重要性等。

7 アクセス制御

許可された者だけがシステムやネットワークにアクセスでき、不許可の者のアクセスを防ぐための管理策。パスワード管理システム等。

8 情報システムの取得、開発および保守

情報システムにおいて、データの妥当性確認、改ざん防止、暗号化によるデータの機密保護、システムが保有するファイルの管理、および情報システムの開発・支援過程におけるセキュリティ上のポイント。

9 情報セキュリティインシデントの管理

情報システムに関連するセキュリティ事象及び弱点の報告、是正処置のための責任体制の整備、法的処置のための証拠収集等。

10 事業継続管理

災害やセキュリティ障害によって事業活動が継続できなくなった際の管理策。

11 順守

情報システムに関連する法令、規則や契約上の義務に違反しないための管理策、システム監査のポイント等。

3. 法的要求事項への準拠について

管理目的及び管理策のひとつである「順守」について、もう少し詳しく説明してみましょう。

順守の重要なポイントは・・・

法的要求事項の順守

すなわち、**情報システムに関する法令や規則、契約上の義務を順守すること**です。ISO27001認証制度に規定されている事項に加え、当然のことながら、それ以外の法律もきちんと守ることが求められています。

情報システムに関する法令や規則には、さまざまなものがあります。たとえば、**刑法、民法、商法、不正競争防止法、電子署名法、著作権法、個人情報保護法**等です。これらの法令や規則のうち、**情報セキュリティに深く関連する法律のひとつが個人情報保護法**です。

ISO27001認証取得の際の従業員の重要な役割は、情報セキュリティの内容を理解して実践することですから、個人情報保護法についてもしっかりと学んでおきましょう。

4. 個人情報保護法ってどんな法律？

個人情報保護法とは・・・

- ・平成17年4月1日より全面施行。
- ・個人情報を取り扱っている事業者（個人情報取扱事業者）に対し、個人情報の適正な取り扱いに関するルールを定めたもの。

この法律により、個人情報を取り扱う事業者には、個人情報を保護するためのさまざまな義務と責任が課せられることになりました。

5. 個人情報とは、どんな情報のこと？

個人情報とは・・・

氏名、生年月日、住所、電話番号等、その情報単体、または他の情報と照合することで特定の個人を識別できる情報のことをいいます。

例「123abc@xxx.co.jp」

→記号や数字のみのメールアドレスなら個人情報には該当しない

例「sato-ichiro@xxx.co.jp」

→「xxx社のサトウイチロウさん」と分かるものは個人情報に該当する

該当するもの	該当しないもの
・ 氏名 ・ 本人の判別が可能な画像、写真、音声 ・ 特定の個人を認識できるメールアドレス（例／sato-ichiro@xxx.co.jp等、xxx社のサトウイチロウさんと分かるもの） ・ 氏名と会社名等が記載された名刺 ・ 氏名等、他の情報と照合すれば特定の個人を識別することができるもの（例／生年月日、住所、連絡先、学歴、病歴、勤務成績、役職、年収、財産、趣味、嗜好、思想、家族構成、商品購入履歴等） ・ 官報、電話帳、職員録等に公表されている情報 ・ 雇用管理情報（履歴書、社員名簿、給与の額、健康状態、人事考課、住宅事情、労働組合関係情報等） ・ 嗜好（好きな食べ物、好きなブランド、喫煙の有無等）	・ 生存していない人に関する情報 ・ 所在地、財務情報等法人に関する情報 ・ 記号や数字の文字列だけから個人を特定できないメールアドレス（例／123abc@xxx.co.jp等） ・ 特定の個人が識別不可能な統計情報

雇用管理情報に、さまざまな個人情報が含まれていることから、**個人情報保護法に則した情報の取り扱いが必要**だといえます。

履歴書等採用に際して得た情報も同様です。採用の際に提出された個人情報は、**採用の判断材料とする目的で提出されたものであり、その目的の範囲内で使用する**必要があります。

