

プライバシーマーク推進体制図



会社組織でいえば「代表取締役」ということになります。

個人情報保護委員会



委員長

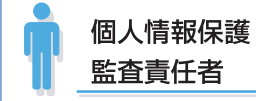


委員

【委員長の役割】

- ・PMS推進における最高責任と権限を有す。
- ・マネジメントレビューを実施。
- ・個人情報保護管理者を事業者の内部の者から任命。
- ・個人情報保護監査責任者を事業者の内部の者から任命。
- ・個人情報保護教育責任者を任命。
- ・システム管理者を任命。
- ・入退室管理者を任命。
- ・PMSの確立、実施、維持、見直しに必要な資源を提供。
- ・PMSの確立、実施、維持、見直しでの職務・役割を定める。
- ・その他、情報セキュリティに関する、緊急時の判断を行う。

内部監査委員会



個人情報保護
監査責任者



監査員

個人情報保護の内部監査に関する一切の件と責任を有する責任者。

【監査の責任者の役割】

- ◆9.2 内部監査
- ・監査を指揮すること
- ・監査を指揮すること
- ・報告書を作成し、事業者の代表者に監査結果の報告すること
- ・監査員の選定及び監査の実施において、監査の客観性及び公平性を確保すること

【監査員の役割】

- ◆9.2 内部監査
- ・規程で定める認定基準を満たしている者
- ・個人情報保護監査責任者の指示に従い内部監査の実施
- ・監査員は監査を実施する際、客観性及び公平性を保たなければならない責務がある

教育・研修委員会



責任者

個人情報保護を考える上で、社員教育は避けて通れません。トップマネジメントより任命を受け、教育を立案及び計画し、実施し、教育実施状況及び結果をトップマネジメントに報告。



メンバー

個人情報保護推進ワーキンググループ



個人情報保護管理者 (管理者)

個人情報保護の一切に関する権限と責任を有する責任者ということになります。

【管理者の役割】

管理者が主語になっている要求事項は一つしかありません。
「5.3.2 役割責任及び権限の割当て」
『PMSの見直し及び改善の基礎として、トップマネジメントに個人情報保護マネジメントシステムの運用状況を報告しなければならない。』
しかし、これだけなのでしょうか？
その役割は、「組織」が主語になっている要求事項と考えることができます。
例えば、「組織」を「管理者」と置き換えると、その責任がはっきり見えてきます。

- ・PMSを実施、維持運用するための責任と権限を有す。
- ・トップマネジメントにかわり、関連担当者への指示及び協力を要請。
- ・PMSの実施状況を、トップマネジメントに報告。
- ・特例措置の承認。
- ・PMSの年間計画を記載した「個人情報保護年間計画書」を立案し、トップマネジメントの承認を得る。



推進メンバー



推進事務局

事務局は、管理者を補佐するための組織となります。そのため、管理者から権限や責任の一部を委譲されることが必要です。

- ・申請書の査読や必要な文書の更新、保管といった実作業
- ・活動の内容については、定期的に報告し、承認を得る

上記のような場合以外でも、組織が大きい場合、個人情報保護に関する教育として、事務局のメンバーをローテーションで交代させ、多くの従業員に個人情報保護に関する活動に触れさせることも有効です。
また、事務局メンバーを経験した人々を内部監査員としてアサインすることで、内部監査員の育成を図ることも可能です。



苦情・相談窓口

苦情や相談といった問合せに応じる責務を持つ役職ということになります。会社の規模や個人情報の運用形態によっては、管理者が兼務することが可能です。しかし、個人情報の開示への対応がより詳細に定められ、また保有個人データに関する開示等(利用目的の通知、開示、内容の訂正、追加又は削除、利用の停止又は消去、第三者提供の停止)の請求等への対応へも必要があります。

部門単位



業務の責任者

組織の規模が大きくなると、全社にわたる個人情報の管理を1人で行うことは不可能でしょう。このような場合は、部署ごとに「個人情報保護管理者」を置き、管理者の権限と責任の一部を委譲するような形式にすれば良いでしょう。単に、申請書類の通過点にするといった形式も可能ですし、個人情報のリスク分析結果やそれに基づく対策の承認までを含めて、権限と責任を委譲することも可能です。
組織が直面する個人情報のリスクの大きさや、運用の形態にあわせて決定することが望ましいでしょう。

※ この枠内はプライバシーマーク推進体制の範囲を示しており、枠外は企業内での関連組織(者)を意味します。



品質マネジメントシステム実行委員会



環境マネジメントシステム実行委員会



情報セキュリティマネジメントシステム実行委員会

プライバシーマーク制度もマネジメントシステムを基幹として作成されており、他のマネジメントシステムとの連携が円滑に運用していくうえで非常に重要なポイントとなります。そのためにも、各マネジメントシステム間での相談・連絡窓口を設けておくことと良いでしょう。



情報セキュリティアドバイザー

会社の中にたくさんある情報のうち、個人情報だけを選んでセキュリティ対策を施すことはさきわめて困難です。個人情報を保護するためのセキュリティは、会社の中にあるすべての情報に関するセキュリティであると考えるのが普通でしょう。個人情報保護推進責任者だけでは、個人情報にしか責任や権限が及ばないこととなります。組織の情報資産すべてにおけるセキュリティに関してアドバイスを受けられる体制を整えておくことが望ましいでしょう。



法務部など

個人情報保護またはプライバシーマークに係わる法規制類(個人情報保護法、マイナンバー法、不正アクセス行為の禁止等に関する法律など)については、コンプライアンスの側面からも遵守事項、罰則事項、また改定内容・最新版を常に把握しておく必要があります。社内または社外に法規制類の責任・管理部署(者)を総務部、法務部、顧問弁護士などから設けておくことと良いでしょう。



人事総務部など

個人情報保護またはプライバシーマークでは、法規制、PMSに違反した従業員を社内で懲戒することが要求されており、就業規則の中での罰則(訓告、減給、停職、懲戒免職など)を適用するケースが一般的です。そのようなことから、社内に社内規定の責任・管理部署(者)を総務部、人事部などから設けておくことと良いでしょう。

責任者選定時の注意事項

- ① 個人情報保護管理者と個人情報保護監査責任者が同一人物でないこと。
- ② 個人情報保護管理者及び個人情報保護監査責任者は、代表者によって内部から指名されていること。
- ③ 会社法上の監査役、監査委員、又は会計参与が、体制の一部を占めていないこと。