連載

使いこなして何ぼ!!のISO

…ＩＳＯコンサルティングの現場から…

第42回 「役に立つPマークのポイントご紹介します」の2回目

㈱ソフィア　平松　徹

1. 安全管理措置では経産省のガイドラインを参考にすると良い

リスクマネジメントでは、予想されるリスクを洗い出し、それに対する予防処置を検討し、対策として確実に実施することが必要です。その予防処置はPMSでは安全管理措置といわれ、PMSの構築ではその安全管理措置を具体的にどのようにするかが重要です。その際に経済産業省のガイドラインが非常に役に立ちます。ガイドラインでは安全管理措置を次の4つに分けています。

●組織的安全管理措置　人的安全管理措置
物理的安全管理措置　技術的安全管理措置

一つひとつ見ていきます。

2. 組織的安全管理措置

まず、組織的安全管理措置です。
ガイドラインに次のようにあります。
組織的安全管理措置とは、安全管理について従業者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認することをいう。
具体的に記載されていることをまとめました。

(1)個人データの安全管理措置を講じるための組織体制の整備

1) 役割・責任を明確にする。

①それぞれの部署、従業者など特定し明確にする。
②職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定める。
③個人情報保護管理者を設置する。
④作業責任者の設置及び作業担当者を限定する。情報システム運用責任者の設置及び担当者を限定する。
⑤監査実施体制を整備し、監査責任者を設置する。

2) 報告連絡体制の整備

①規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制
②個人情報の漏えい、滅失又はき損の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制(個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図る。)
③漏えい等の事故による影響を受ける可能性のある本人への情報提供体制
④漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制

(2)個人データの安全管理措置を定める規程等の整備と規程等に従った運用

①建物、部屋、保管庫等の安全管理に関する規程等を整備し運用する。
②委託先についての「選定基準」、「委託契約書のひな型」、委託先における委託した個人データの取扱状況を

確認するための「チェックリスト」等を整備し運用する。
③規程等に従って業務手続が適切に行われたことを示す監査証跡を保持する。(個人データに関する「情報システム利用申請書」、ある従業者に特別な権限を付与するための「権限付与申請書」、情報システム上の利用者とその「権限の一覧表」、建物等への「入退館(室)記録」、個人データへの「アクセスの記録」、「教育受講者一覧表」等)

(3)個人データの取扱状況を一覧できる手段の整備

①個人データについて、取得する項目、明示・公表等を行った利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳を整備する。
②個人データ取扱台帳の内容を定期的に確認し、最新状態を維持する。

(4)個人データの安全管理措置の評価、見直し及び改善

①監査計画の立案と、計画に基づく監査(内部監査又は外部監査)を実施する。
②監査実施結果を取りまとめ、代表者へ報告する。
③監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直しをし、改善する。

(5)事故又は違反への対処・手順を整備する

①事実調査、原因の究明　②影響範囲の特定　③再発防止策の検討・実施　④影響を受ける可能性のある本人への連絡　⑤主務大臣等への報告　⑥事実関係、再発防止策等の公表

3. 規程に記載することが望まれる事項

そして、個人データの取扱いに関する規程等に記載することが望まれる事項の例として次の内容の記載があります。「個人情報取扱い規程」などを作成するときはぜひ参考にすべき内容です。

①作業責任者の明確化

- 個人データを取得する際の作業責任者の明確化

②手続の明確化と手続に従った実施

- 「取得・入力」「移送・送信」「利用・加工」「保管・バックアップ」「消去・廃棄」という、個人データの取扱いの流れに従い手続を明確にする。
- 権限を与えられていない者が立ち入れない建物、部屋で作業を実施する。

③作業担当者の識別、認証、権限付与

- 作業担当者の、業務上の必要性に基づく限定。IDとパスワードによる認証、生体認証等による作業担当者の識別をする。
- 作業担当者に付与する権限を限定する。
- 作業担当者に付与した権限を記録する。

④作業担当者及びその権限の確認

- 手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況を確認する。
- アクセスの記録、保管と、権限外作業の有無の確認をする。

⑤各工程での具体的安全措置の例

「取得・入力」

- 入力できる端末装置の限定、端末に付与する機能の限定(個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにするなど。)

「移送・送信」

- 個人データを移送・送信する場合の個人データの暗号化(公衆回線を利用して個人データを送信する場合)
- 移送時におけるあて先確認と受領確認(配達記録郵便等の利用)
- FAX等におけるあて先番号確認と受領確認
- 個人データを記した文書をFAX機等に放置することの禁止
- 暗号鍵やパスワードの適切な管理

「利用・加工」

●作業担当者に付与した権限、例えば、複写、複製、印刷、削除、変更等の記録

「保管・バックアップ」

●個人データを保管・バックアップする場合の個人データの暗号化

●暗号鍵やパスワードの適切な管理

●媒体を保管する場合の施錠管理、部屋、保管庫等の鍵の管理

●媒体の遠隔地保管

●バックアップから迅速にデータが復元できることのテストの実施

●バックアップに関する各種事象や障害の記録

●個人データの保管・バックアップ業務を行う作業担当者に付与した権限の記録、バックアップの実行、保管庫の鍵の管理等の記録

「消去・廃棄」

●個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去、例えば、意味のないデータを媒体に1回又は複数回上書きするなど。

●個人データが記録された媒体のシュレッダー、メディアシュレッダー等での物理的な破壊。

4. 人的安全管理措置

次が人的安全管理措置です。従業者に対するもので、ガイドラインでは次のような内容になっています。

人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。具体的には次の記載内容です。

①雇用契約の際に従業者と個人情報について持ち出さないなどの非開示契約の締結をする

●採用時だけでなく個人情報について特に業務で関係する際も締結する。また退職後なども一定期間有効にしておく。

●個人情報にアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記する。

●違反した場合の罰則の規程の整備。

②内部規程等の周知・教育・訓練の実施

●安全管理についての役割責任の明確化、教育・訓練の実施、そしてその確認をする。

5. 物理的安全管理措置

3番目が、物理的安全管理措置です。入退館や保管、機械装置などへの物理的な面での安全管理措置です。ガイドラインには次のようにあります。

物理的安全管理措置とは、入退館(室)の管理、個人データの盗難の防止等の措置をいう。具体的には、次のような内容になっています。

①入退館（室）管理の実施

●個人情報を取り扱う業務、情報システムは入退室館管理をしていることが必要。

②盗難等の防止

●個人情報を持つ書類媒体を施錠保管する。

●個人情報を持つ書類、媒体、携帯パソコン、情報システム操作マニュアルなどを机上に放置しない。また離席時にはスクリーンセーバーを起動する。

●個人情報を含むものと含まないものを分離して保管する。

③機器・装置等の物理的な保護

●盗難、破壊、破損などの安全管理上の脅威、漏水、火災、停電などの環境上の脅威から物理的に保護をする。

6. 技術的安全管理措置

最後が技術的安全管理措置です。

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

IT技術を通して、個人データを技術的に保護していこうとするものです。

具体的には、次のような内容で、取り組み事例なども豊富に記載されています。

①個人データへのアクセスにおける識別と認証

●IDとパスワード管理を実施する。

パスワードの有効期限の設定、同一パスワード､類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗したIDを停止する等の措置を講じる。

●アクセス権限を有する者が使用できる端末又はアドレス等のなどの識別と認証をする。

MACアドレス認証、IPアドレス認証、電子証明書や秘密分散技術を用いた認証等の実施

②個人データへのアクセス制御

●アクセス権限を付与すべき者の最小化、また付与する権限の最小化。情報システムの利用時間の制限

休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等

●情報システムへの無権限アクセスからの保護ファイアウォール、ルータ等の設定

●アクセス可能なアプリケーションの無権限利用の防止

アプリケーションシステムに認証システムを実装する､業務上必要となる者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする､業務上必要な機能のみメニューに表示させる等

●情報システムに導入したアクセス制御機能の有効性を検証する。

ウェブアプリケーションのぜい弱性有無の検証など

③個人データへのアクセス権限の管理

●アクセスできる者を許可する権限管理の適切かつ定期的な実施

④個人データのアクセスの記録

●アクセスや操作の成功と失敗の記録を保持する。

●採取した記録については漏えい、滅失及びき損から適切に保護する。

●個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留意する。

⑤個人データを取り扱う情報システムについての不正ソフトウェア対策

●ウイルス対策ソフトウェアを導入する。

●オペレーティングシステム、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（セキュリティパッチ）を適用する。

●不正ソフトウェア対策の有効性・安定性を確認する（パターンファイルや修正ソフトウェアの更新の確認など）

⑥個人データの移送（運搬、郵送、宅配便配送等）、送信時の対策

●移送時に紛失・盗難が生じた際の対策をとして、媒体に保管されている個人データを暗号化する。

●盗聴される可能性のあるインターネットや無線LAN等のネットワークで個人データを送信する際、個人データを暗号化する。（メールに添付してファイルを送信するときなど）

⑦個人データを取り扱う情報システムの動作確認時の対策

●情報システムの変更時に、情報システム又は運用環境のセキュリティが損なわれないことを検証する。

⑧個人データを取り扱う情報システムの監視

●個人データを取り扱う情報システムの使用状況を定期的に監視する。

●個人データへのアクセス状況を操作内容も合わせ監視する。

●情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。

以上、経済産業省の個人情報についてのガイドラインをまとめました。もともとのガイドラインはいろいろなことを列記しているだけなので、かなりわかりにくい内容になっています。それでも、Pマーク審査としてはこのガイドラインの内容は審査基準としては最も重要なもののひとつです。また、具体例も豊富に列挙されていますので、PMSの構築では外せないものになっています。ぜひとも参考にしてください。 I

（ひらまつ　とおる　代表取締役）