安全管理措置

講じなければならない措置	手法例	ヒント
基本方針の策定 （通則編GL8-1）	● 個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定。	・義務ではありませんが、策定しておくことで、従業員教育に役立ちます。
個人データの取扱いに係る規律の整備（通則編GL8-2）	● 個人データの取得、利用、保存等を行う場合の基本的な取扱方法を整備する。	・既存の業務マニュアル・チェックリスト・フローチャート等に個人情報の取扱いの項目を入れるのも一案。

1 組織的安全管理措置（通則編GL8-3）

(1)組織体制の整備
(2)個人データの取扱いに係る規律に従った運用
(3)個人データの取扱状況を確認する手段の整備
(4)漏えい等の事案に対応する体制の整備
(5)取扱状況の把握及び安全管理措置の見直し

2 人的安全管理措置（通則編GL8-4）

従業者の教育

3 物理的安全管理措置（通則編GL8-5）

(1)個人データを取り扱う区域の管理
(2)機器及び電子媒体等の盗難等の防止
(3)電子媒体等を持ち運ぶ場合の漏えい等の防止
(4)個人データの削除及び機器、電子媒体等の廃棄

4 技術的安全管理措置（通則編GL8-6）

(1)アクセス制御
(2)アクセス者の識別と認証
(3)外部からの不正アクセス等の防止
(4)情報システムの使用に伴う漏えい等の防止

安全管理措置：①組織的安全管理措置、②人的安全管理措置

講じなければならない措置	手法例	ヒント
1 組織的安全管理措置		
①組織体制の整備	● 個人データを取り扱う従業者が複数いる場合、責任ある立場の者とその他の者を区分する。	• リスク分散の観点から、誰かがチェックできると良いということです。
②個人データの取扱いに係る規律に従った運用 ③個人データの取扱状況を確認する手段の整備	● あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が確認する。	• 業務日誌やチェックリスト等を活用し、確認を。
④漏えい等の事案に対応する体制の整備	● 漏えい等の事案の発生時に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認する。	• 「ほう・れん・そう」の中に、個人情報の漏えい事案を。
⑤取扱状況の把握及び安全管理措置の見直し	● 責任ある立場の者が、個人データの取扱状況について、定期的に確認を行う。	• ①～④のプロセスで気づいたリスクがあれば、改善を。
2 人的安全管理措置		
従業者の教育	● 個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。 ● 個人データについての秘密保持に関する事項を就業規則等に盛り込む。	• 集合研修に限らず、朝礼等の際に定期的に注意喚起を。

安全管理措置：③物理的安全管理措置

講じなければならない措置	手法例	ヒント
3 物理的安全管理措置		
①個人データを取り扱う区域の管理	● 個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧等できないような措置を講ずる。	• 誰でも見られる場所に放置しない。
②機器及び電子媒体等の盗難等の防止	● 個人データを取り扱う機器、個人データが記録された電子媒体又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する ● 個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。	• 書類や電子媒体をきちんと管理。
③電子媒体等を持ち運ぶ場合の漏えい等の防止	● 個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。	• 電子媒体にはパスワードを。置き忘れ等にも注意を。
④個人データの削除及び機器、電子媒体等の廃棄	● 個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄したことを、責任ある立場の者が確認する。	• 書類であれば、焼却、シュレッダー処理を、機器・電子媒体等であれば、データ削除ソフトウェアの利用や物理的な破壊等を。

安全管理措置：④技術的安全管理措置置

講じなければならない措置	手法例	ヒント
４技術的安全管理措置		
①アクセス制御	● 個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。	• 必要のない者の個人情報へのアクセスを制限するため、個人情報を含むファイルにパスワードを。
②アクセス者の識別と認証	● 機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。	
③外部からの不正アクセス等の防止	● 個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。 ● 個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。	• セキュリティ対策ソフトウェアを最新の状態に。
④情報システムの使用に伴う漏えい等の防止	● メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。	• それほど難しい操作ではないので、メール送信時にはパスワードを。

安全管理措置：漏えい等の事案が発生した場合の対応

対象事案

- ✓ 個人データ（特定個人情報に係るものを除く。）の漏えい、滅失又は毀損
- ✓ 加工方法等情報（匿名加工情報の加工の方法に関する情報等）の漏えい
- ✓ これらのおそれ

望ましい対応

①事業者内部における報告及び被害の拡大防止

②事実関係の調査及び原因の究明

③影響範囲の特定

④再発防止策の検討及び実施

⑤影響を受ける可能性のある本人への連絡（事案に応じて）

⑥事実関係及び再発防止策等の公表（事案に応じて）

＋

努力義務

個人情報保護委員会等への速やかな報告

※事業分野によっては、**認定個人情報保護団体**や権限の委任を受けた**事業所管大臣**が報告先となることがあります。
※なお、別途、業法等で監督当局への報告が義務付けられている場合もある為、注意が必要です。

漏えい等の事案が発生した場合の報告ルート