自己点検チェックリスト

このチェックリストは、自社内での個人情報の取扱いが、個人情報保護法上求められる個人情報の安全管理のために必要な各項目を満たしているのかについて、自己点検を実施するための参考資料です。
チェックがつかない項目については、個人情報保護法ガイドライン（通則編）（以下「ガイドライン」という。）の参照先の記載も参考にし、早急に対策を実施いただく必要があります。
チェック開始にあたり、事前準備として自社で個人データをどの程度取り扱っているのか確認することは重要です。
取扱件数　　件
※事前準備なしでもチェックを行うことは可能です。

項番	安全管理のために必要な措置	チェック	確認事項	ガイドライン参照先
1	基本方針の策定	□	個人データの適正な取扱いの確保について会社組織全体として取り組むために、基本方針を策定していますか？ ※この項目は義務規定ではありませんが、策定することは重要です。	8-1
2	個人データの取扱いに係る社内ルールの整備	□	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定めた社内ルールを整備していますか？ 手法例； 既存の業務マニュアル・チェックリスト等に個人情報の取扱いに関する項目を盛り込む ※チェックがつかない場合、個人情報保護委員会のHPに掲載されている「個人データ取扱要領（例）」をご確認ください。	8-2
3	組織的安全管理措置	□	(1)個人データを安全に取り扱うための組織体制は整備できていますか？ 手法例； 個人データを取り扱う従業者が複数いる場合、個人データの取扱いについて責任ある立場の者とその他の者を区分する	8-3(1)
		□	(2)個人データの取扱いに係る社内ルールに従った運用がされていますか？また、それを確認するための手段はありますか？ 手法例； あらかじめ整備された個人データの取扱いに係る社内ルール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	8-3(2)(3)
		□	(3)漏えい等の事案が発生した場合に対応する体制は整備できていますか？ 手法例； 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決め、従業者に周知する	8-3(4)
		□	(4)個人データの取扱い状況の把握及び安全に取り扱うためのルールや体制の見直しはできていますか？ 手法例； 責任ある立場の者が個人データの取扱いについて、定期的に点検するとともに、適宜取扱方法（ルールや体制）の見直しを行う	8-3(5)
4	人的安全管理措置	□	従業者に、個人データの適正な取扱いを周知徹底するとともに、適切な教育を行っていますか？ 手法例； 個人データの適正な取扱いに関して、 ・朝礼等の際に定期的な注意喚起を行う ・定期的な研修を行う ・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	8-4

項番	安全管理のために必要な措置	チェック	確認事項	ガイドライン 参照先
5	**物理的安全管理措置**	□	**(1)個人データを取り扱う区域を管理していますか？** 手法例; 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の者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	8-5(1)
		□	**(2)個人データを取り扱う機器及び電子媒体等の盗難等を防止するための対策を実施していますか？** 手法例; ・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。 ・パソコンのフォルダ内に個人データが保存されている場合は、当該機器をセキュリティワイヤー等により固定する。	8-5(2)
		□	**(3)(電子媒体等を持ち運ぶ場合)持ち運ぶ際に個人データが漏えいしないための対策を実施していますか？** 手法例; 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対策を実施する。	8-5(3)
		□	**(4)個人データの削除及び個人データが記録された機器、電子媒体等を適切に廃棄していますか？** 手法例; 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	8-5(4)
6	**技術的安全管理措置** **※技術的安全管理措置は、情報システム(パソコン等の機器を含む。)を使用して個人データを取り扱う場合(インターネット等を通じて外部と送受信等する場合を含む。)に講ずる必要があります。**	□	**(1)個人データへの不要なアクセスを防止できるよう制御していますか？** 手法例; 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する	8-6(1)
		□	**(2)個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有するか、確認したうえでアクセスを許可していますか？** 手法例; 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、正当なアクセス権を有する従業者であるかを識別・認証する	8-6(2)
		□	**(3)外部からの不正アクセス等を防止するための対策を実施していますか？** 手法例; ・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 ・情報システム及び機器にセキュリティ対策ソフトウェア等を導入する ・セキュリティ対策ソフトウェア等を最新状態とする **※不正アクセス等を防止するための注意点！** たとえば、個人データを取り扱うウェブサイト・通販サイト(ECサイト)の構築、保守・運用する場合には、次のような対策を行うことが考えられます。 ・ウェブサイトのプログラム修正、システムのバージョンアップなど変更・修正を加えた場合は、リリース前にセキュリティチェックシートなどを使用し、ウェブサイトに脆弱性がないか網羅的に確認を行いましょう。 ・ウェブサイトの運用にあたっては、OSやソフトウェアの脆弱性対策情報を収集し、必要に応じ速やかにセキュリティパッチを適用しましょう。また、定期的に、ウェブサイト全体を対象として脆弱性診断を行うことも有効です。	8-6(3)
		□	**(4)情報システムの使用に伴う漏えい等を防止するための対策を実施していますか？** 手法例; 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、当該ファイルにパスワードを設定する	8-6(4)

項番	安全管理のために必要な措置	チェック	確認事項	ガイドライン 参照先
7	委託先の監督 **※個人情報の取扱いの委託とは、個人情報の取扱業務を自社以外の事業者へ依頼することです。** **例えば、次のような業務で委託に該当する場合があります。** **・各種申込書類等の手続き** **・個人情報を含む書類の廃棄** **・コールセンター** **・通販サイトの構築・運用** **・HPの一部での予約受付サイトの運営** **※通販サイトや予約受付等個人情報の取扱いを含むシステムの運営を依頼する場合も委託となります。**	□	**個人データの取扱いの全部又は一部を委託する場合、個人データの安全管理が図られるよう、以下の（1）～（3）の観点で、委託先に対する必要かつ適切な監督を行っていますか？** （1）適切な委託先の選定 前項までに定める個人情報の安全管理のために必要な措置が、委託先において確実に実施されるか、委託先選定時に確認する （2）委託契約の締結 委託契約には、個人データを安全に管理するために必要な対応として両社同意した内容及び委託先での取扱状況を委託元が把握できる規定を盛り込むことが望ましい （3）委託先における個人データ取扱状況の把握 定期的に監査を行う等により、委託契約に盛り込んだ内容が適切に実施されているかを調査し、必要に応じて委託内容の見直しを検討することが望ましい **※安全管理を委託先に任せきりにしない！** たとえば、個人データを取り扱うウェブサイト・通販サイト（ECサイト）の構築、保守・運用を委託する場合には、次のような対策を行うことが考えられます。 ・委託先が適切なシステム上のセキュリティ対策を含む安全管理を実施しているか契約前に確認し適切な事業者を選定すること ・セキュリティ対策等の内容を明確にして契約に盛り込むこと(6　安全管理措置（3）参照) ・契約書に記載されたセキュリティ対策等の実施状況について定期的に報告を求めるなど確認を行うこと	3-3-4