自己点検チェックリスト

このチェックリストは、部会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資料である。

| | | | |
|---|---|---|---|
| 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部会全体として取り組むために、基本方針を策定しているか？<br><br>⇒取扱ルールを策定済み。 |
| 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部会内ルールを整備しているか？<br><br>⇒取扱ルールを策定済み。 |
| 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るか？<br>手法； 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<br><br>⇒個人データを取り扱うのは責任者のみである。 |
| | | ☑ | （2）個人データの取扱いに係る部会内ルールに従った運用がされているか？また、それ を確認するための手段はあるか？<br>手法； あらかじめ整備された個人データの取扱いに係る部会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<br><br>⇒個人データを取り扱うのは責任者のみである。 |
| | | ☑ | （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るか？<br>手法； 漏えい等の事案の発生時に備え、部会員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<br><br>⇒個人データを取り扱うのは責任者のみである。 |
| | | ☑ | （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 はできているか？<br>手法； 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<br><br>⇒責任者が個人データを維持・管理している。 |
| 4 | 人的安全管理措置 | ☑ | 部会員に、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るか？<br>手法； 個人データの適正な取扱いに関して、会議等の際に定期的な注意喚起を行う<br><br>⇒責任者が個人データを維持・管理している。またその旨は部会員に衆知している。 |

| | | | |
|---|---|---|---|
| 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るか？<br>手法； 個人データを取り扱うことのできる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<br><br>⇒責任者が個人データを維持・管理しており、他の者は閲覧できない。 |
| | | ☑ | （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 ているか？<br>手法； 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、当該機器を移動できないように固定する。<br><br>⇒責任者管理のデスクトップPC内に有り持ち出し不可。 |
| | | ☑ | （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 を実施しているか？<br>手法； 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。<br><br>⇒持ち運ぶことはない。 |
| | | ☑ | （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 いるか？<br>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<br><br>⇒個人データの削除や廃棄は責任者が交代するときに移管に伴い実施する。 |
| 6 | 技術的安全管理措置<br>※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るか？<br>手法； 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<br><br>⇒個人データを取り扱う機器は責任者のデスクトップPCのみであり、責任者以外はアクセスできない。 |
| | | ☑ | （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るか？<br>手法； 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 クセス権を有する部会員であるかを識別・認証する<br><br>⇒個人データは責任者のデスクトップPCにのみ存在するので他の者はアクセス不可。また、個人データの元になるメールはサーバに存在するが、アカウントおよびパスワードで識別されている。 |
| | | ☑ | （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るか？<br>手法； ・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<br><br>⇒個人データを保存する管理者のデスクトップPCで全て行われている。 |
| | | ☑ | （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るか？<br>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<br><br>⇒個人データを含むファイルを送信することは無い。 |
| 7 | 委託先の監督 | ☑ | 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、委託先に対する必要かつ適切な監督を行っていまるか？<br><br>⇒委託先は無い。 |