人的安全管理措置

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。

【人的安全管理措置として講じなければならない事項】

①雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結

②従業者に対する内部規程等の周知・教育・訓練の実施

なお、管理者が定めた規程等を守るように監督することについては、法第21条を参照。

【各項目を実践するために講じることが望まれる手法の例示】

①「雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結」を実践するために講じることが望まれる手法の例示

・従業者の採用時又は委託契約時における非開示契約の締結

＊雇用契約又は委託契約等における非開示条項は、契約終了後も一定期間有効であるようにすることが望ましい。

＊個人情報に関する非開示の義務を、就業規則等の社内規程に規定することも考えられる。なお、社内規程に個人情報に関する非開示の義務を規定する場合には、特に、労働基準法第89条及び第90条などの労働関連法規を遵守する必要がある。

＊個人情報に関する非開示契約の締結の際に、営業秘密を対象とする秘密保持契約をあわせて締結する場合であっても、個人情報保護と営業秘密の保護はその目的・範囲等が異なるため、従業者の「納得感」の向上の観点からは、個人情報保護に関する契約と営業秘密に関する秘密保持契約は峻別する（別書面であるか否かは問わない）ことが望ましい。

・非開示契約に違反した場合の措置に関する規程の整備

＊個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についても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ことが望ましい。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。

②「従業者に対する内部規程等の周知・教育・訓練」を実践するために講じることが望まれる手法の例示

・個人データ及び情報システムの安全管理に関する従業者の役割及び責任を定めた内部規程等についての周知

・個人データ及び情報システムの安全管理に関する従業者の役割及び責任についての教育・訓練の実施

・従業者に対する必要かつ適切な教育・訓練が実施されていることの確認

物理的安全管理措置

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。

【物理的安全管理措置として講じなければならない事項】

①入退館（室）管理の実施

②盗難等の防止

③機器・装置等の物理的な保護

【各項目を実践するために講じることが望まれる手法の例示】

①「入退館（室）管理」を実践するために講じることが望まれる手法の例示

・個人データを取り扱う業務の、入退館（室）管理を実施している物理的に保護された室内での実施

・個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置

②「盗難等の防止」を実践するために講じることが望まれる手法の例示

・個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止

・離席時のパスワード付きスクリーンセイバ等の起動によるのぞき見等の防止

・個人データを含む媒体の施錠保管

・氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管

・個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

③「機器・装置等の物理的な保護」を実践するために講じることが望まれる手法の例示

・個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護

技術的安全管理措置

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。

【技術的安全管理措置として講じなければならない事項】

①個人データへのアクセスにおける識別と認証

②個人データへのアクセス制御

③個人データへのアクセス権限の管理

④個人データのアクセスの記録

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

⑥個人データの移送・送信時の対策

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

⑧個人データを取り扱う情報システムの監視

【各項目を実践するために講じることが望まれる手法の例示】

①「個人データへのアクセスにおける識別と認証」を実践するために講じることが望まれる手法の例示

・個人データに対する正当なアクセスであることを確認するために正当なアクセス権限を有する者であることの識別と認証（例えば、ＩＤとパスワードによる認証、生体認証等）の実施

＊ＩＤとパスワードを利用する場合には、パスワードの有効期限の設定、同一又は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ことが望ましい。

・個人データへの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識別と認証（例えば、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」を実践するために講じることが望まれる手法の例示

・個人データへのアクセス権限を付与すべき者の最小化

・識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）の実施