酒井事務所ニュース　NO．２５５

平成２７年7月２５日　　発行
社会保険労務士法人酒井事務所

千代田区飯田橋３－１１－１３　ダヴィンチ飯田橋９Ｆ
ＴＥＬ　０３－３２３０－４６００
ＦＡＸ　０３－３２３０－４６０９

マイナンバー（マイナンバー）の適切な管理について

１．組織的安全管理措置

職名	役割と責任
個人情報取扱責任者 （以下「取扱責任者」）	・特定個人情報の取得、利用、保存、提供、削除・廃棄等の作業の責任者 ・マイナンバー関係事務を外部に委託する場合の委託先に関する監督の責任者
マイナンバー事務取扱担当者 （以下「事務取扱担当者」）	・マイナンバー関係事務を処理するために必要な限度で、マイナンバー及び特定個人情報（以下「特定個人情報等」という。）の取得、利用、保存、提供、削除・廃棄等の作業に従事する者 ・事務取扱担当者以外の者は、マイナンバー関係事務に従事させることができない ・「特定個人情報」とは、マイナンバーをその内容に含む個人情報をいいます

２．物理的安全管理措置

入退館は、不審者の立入を予防して情報漏えい等を防止するとともに、後に入退館状況の確認ができるように、下記各号を参照し、適宜の方法で管理するものとする。

(1) 社員は、業務終了後は速やかに退社し、業務終了後に社内にみだりに立ち入ってはならない。
(2) 会社を最後に退社した記録（社員名・退館時刻等）を残す。
(3) 会社の休日等、会社が閉鎖されている間に入館する場合は、上長の承認を得なければならない。
(4) 訪問者を会社に入館させる場合は、個人情報やマイナンバーを取り扱う事務を実施する区域及び個人情報やマイナンバーを取り扱う機器等に訪問者が近づくことのないように注意しなければならない。
(5) 入退館管理をする役職者は、入退館の状況を定期的に確認する。

特定個人情報ファイルを取り扱う情報システムを管理する区域及び特定個人情報を取り扱う事務を実施する区域は、下記各号を参照し、適宜の方法で管理するものとする。

(1) 外部からは容易に入室できない室内とする。
(2) 壁又は間仕切り等の設置や作業を覗き見されにくい座席配置などの保護措置を講じた区域とする。
(3) 情報取扱区域は取扱責任者が管理する。
(4) 取扱責任者は、情報取扱区域の状況を定期的に点検する。

情報取扱区域における機器等の管理は、下記各号を参照し、適宜の方法で管理するものとする。

(1) 特定個人情報等を取り扱う機器は、離席時にロックするとともに、10 分程度でパスワード付きのスクリーンセーバー等が起動するように設定する。
(2) 特定個人情報等を取り扱う機器は、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記憶媒体又はスマートフォン、パソコン等の記録機能を有する機器を接続できない措置を講じ、又は取扱責任者の承認を得ずに接続することを禁ずる。
(3) 特定個人情報等が記載された書類及び特定個人情報等が記録された電子媒体は、施錠できる保管場所に保管し、机上等に放置してはならない。
(4) 特定個人情報等を取り扱う機器を情報取扱区域外に持ち出す場合は、取扱責任者の承認を得なければならない。
(5) 会社が管理すべき特定個人情報等は、社員の私物パソコン等で取り扱ってはならない。

３．技術的安全管理措置

特定個人情報ファイルを情報システムで取り扱う場合は、下記各号を参照し、適宜の安全管理措置を講ずるものとする。

(1) 特定個人情報等を取り扱う機器を特定する。
(2) 前号の機器を使用する事務取扱担当者を限定する。
(3) 事務取扱担当者が使用する機器に装備されているユーザーアカウント制御機能により、情報システムを取り扱うことのできる事務取扱担当者を限定する。
(4) 前号のユーザーアカウント制御機能におけるＩＤ・パスワードは付与される者ごとに異なるものとする。
(5) パスワードは、氏名、社員番号、生年月日等、他人に推測されやすいものを使用してはならない。
(6) パスワードは、メモを机上等に放置するなど他人が容易に認識可能な状態で管理してはならない。
(7) 退職・配転等により不要となったＩＤは速やかに削除・停止し、再利用してはならない。
(8) 情報システム及びパソコン等の機器にセキュリティ対策ソフトウェア等を導入して適切な設定をする。
(9) 情報システム及びパソコン等の機器のオペレーティングシステム、ソフトウェア等を常に最新の状態に更新する。
(10) 端末には取扱責任者が認めるソフトウェアのみをインストールできることとする。

特定個人情報等を外部に送信する場合に、下記各号を参照し、適宜の技術的安全管理措置を講ずるものとする。

(1) 通信経路を暗号化する。
(2) 送信するデータを暗号化する。
(3) 送信するデータにパスワードによる保護をかける。

事務取扱担当者・個人情報取扱責任者の業務について

１．特定個人情報等の取得

(1) 本人等からマイナンバーが記載された書類等（マイナンバーカードの IC チップを読み取る等による電子的方式を含む。）の提出を受けるときは、原則として、事務取扱担当者が直接受け取るものとする。
(2) 本人等からマイナンバーが記載された書類等の提出を受けるときは、当該書類等を封筒に入れた状態で直接受領する等、他人が特定個人情報等を容易に確認できない状態で提出を受けるものとする。

(3) 本人等からマイナンバーが記載された書類等の提出を受けて取りまとめる作業のみを担当する事務取扱担当者を定めることができる。この事務取扱担当者は、書類の不備がないかの確認等の必要な事務を行った後は、速やかに入力等を担当する事務取扱担当者に受け渡しを行い、自分の手元に特定個人情報等を残してはならない。
(4) 事務取扱担当者以外の従業者は、特定個人情報等が記載された書類等又はその可能性のある書類等を受け取った場合は、速やかに事務取扱担当者に受け渡さなければならない。
(5) 事務取扱担当者は、従事しているマイナンバー関係事務の処理以外の目的で、取得したマイナンバーを含むメモ、複写、印刷物、データのコピーその他の控えを作成してはならない。

２．特定個人情報の入力

取得した特定個人情報等を情報システムに入力する作業を担当する事務取扱担当者は、下記各号を遵守するものとする。

(1) 物理的安全管理措置及び技術的安全管理措置が施された場所及び機器で、入力作業を実施する。
(2) 取扱責任者が承認した場合を除き、入力を行う端末に、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記憶媒体又はスマートフォン、パソコン等の記録機能を有する機器を接続してはならない。
(3) 従事しているマイナンバー関係事務の処理以外の目的で、マイナンバーを含むメモ、複写、印刷物、データのコピーその他の控えを作成してはならない。
(4) 従事しているマイナンバー関係事務の処理以外の目的で、特定個人情報ファイルを複製し、加工し、又は新たに特定個人情報ファイルを作成してはならない。

３．特定個人情報の利用等

特定個人情報等の利用・加工、保存等（以下「利用等」という。）の作業を担当する事務取扱担当者は、下記各号を遵守して作業を実施する。

(1) 物理的安全管理措置及び技術的安全管理措置が施された場所及び機器で、利用等の作業を実施する。
(2) 取扱責任者が承認した場合を除き、利用等の作業を行う端末に、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記憶媒体又はスマートフォン、パソコン等の記録機能を有する機器を接続してはならない。
(3) 従事しているマイナンバー関係事務の処理以外の目的で、マイナンバーを含むメモ、複写、印刷物、データのコピーその他の控えを作成してはならない。
(4) 従事しているマイナンバー関係事務の処理以外の目的で、特定個人情報ファイルを複製し、加工し、又は新たに特定個人情報ファイルを作成してはならない。
(5) 特定個人情報等を管理するシステムの複製データ、特定個人情報等の利用等の作業のために作成した電子データ及び行政機関へ提出する書類を作成するために出力したチェックリスト等は、利用等の必要がなくなり次第速やかに削除し、必要のない複製データ等が存在しないようにしなければならない。

４．特定個人情報の提供等

特定個人情報等の移送・送信・提供の作業を担当する事務取扱担当者は、紛失・盗難による情報漏えい等を防止するため、下記各号を参照し、適宜の保護措置を遵守して作業を実施する。

(1) 特定個人情報等が記載された書類を本人に返却・交付する場合や行政機関等のマイナンバー利用事務実施者に提出する場合（以下「提供」という。）は、封筒への封緘、目隠しシールの貼付等により、他人が特定個人情報等を容易に確認できない状態で交付・提出する。ただし、マイナンバー利用事務実施者に提出する場合は、当該マイナンバー利用事務実施者の指定する提出方法に従う。
(2) 郵送等の方法により特定個人情報等を提供する場合には、あて先を複数回確認のうえ送付する。ただし、マイナンバー利用事務実施者に提出する場合は、当該マイナンバー利用事務実施者の指定する提出方法に従う。
(3) 特定個人情報等が記載された書類を取扱区域外に持ち出す場合は、封筒への封入をし、鞄で搬送する等、紛失・盗難を防ぐための方策を講ずる。
(4) 特定個人情報等が記録された機器・電子媒体等を取扱区域外に持ち出す場合は、施錠できる搬送容器を利用する等、紛失・盗難を防ぐための方策を講ずる。
(5) 特定個人情報等が記録されたデータをインターネット・メール等により外部に送信する場合は、取扱責任者の承認を得た上で、技術的安全管理措置を講じ、送信先のメールアドレスに間違いないかを複数回確認のうえ送信する。ただし、マイナンバー利用事務実施者にデータを提出する場合は、当該マイナンバー利用事務実施者の指定する提出方法に従う。

５．特定個人情報の削除・廃棄

特定個人情報等の削除又は廃棄（以下「廃棄等」という。）の作業を担当する事務取扱担当者は、下記各号を参照し、適宜の方法で作業を実施する。

(1) 特定個人情報が記載された書類等を、焼却、溶解、復元不可能な程度に裁断可能なシュレッダーによる裁断等の復元不可能な手段で廃棄する。
(2) 特定個人情報等が記載された書類等のマイナンバー部分を復元不可能な程度にマスキングする。
(3) 特定個人情報等が記載された書類又は電子媒体等の中のマイナンバーを、容易に復元できない手段で削除する。
(4) 特定個人情報等が記録されたデータのバックアップ内のマイナンバーも削除する。
(5) 特定個人情報等が記録された機器及び電子媒体等を廃棄する場合は、専用のデータ削除ソフトウェアの利用等によりデータを完全消去し、又は物理的な破壊等によりデータを復元不可能にして廃棄する。
(6) 特定個人情報等が記録された機器及び電子媒体等をリース会社等に返却する場合は、専用のデータ削除ソフトウェアの利用等によりデータを完全消去する。
(7) 削除又は廃棄の担当者が取扱責任者に廃棄等の完了を報告し、取扱責任者が確認する。
(8) マイナンバー若しくは特定個人情報ファイルを削除し、又はこれらのものが記録された電子媒体を廃棄した場合は、削除又は廃棄した記録を保存する。
(9) 削除又は廃棄の作業を委託する場合は、委託先が確実に削除又は廃棄を実施したことについて証明書等により確認し、前号の廃棄の記録に証明書等を添付する。

６．特定個人情報の取扱状況の記録

(1) 特定個人情報等の取得、利用、保存、提供及び削除・廃棄等にあたっては、後に取扱状況を確認できるように、適宜の方法で、特定個人情報の取扱状況が分かる記録を保存するものとする。取扱状況の記録には、マイナンバーを記載してはならない。
(2) 特定個人情報の取扱状況については、取扱責任者が、定期的に点検する。