特定個人情報安全管理措置規則

第 1 章　総則

（目的）

第 1 条　本規則は、情報の安全管理措置として、組織的・人的・物理的・技術的において、本連盟における個人番号その他の特定個人情報の適切な管理のためにとるべき具体的事項を定めることを目的とする。

第 2 章　組織的安全管理措置

（個人番号事務取扱担当者）

第 2 条　本連盟は、個人番号関係事務に従事する者を特定し、個人番号事務取扱担当者に任命する。

2　事務取扱担当者は、連盟の個人番号関係事務を処理するために必要な限度で、次の各号の事務を行う。

（1）特定個人情報等の取得、利用、保存、提供又は消去・破棄等の作業

（2）個人番号が記載された書類等を作成し、行政機関等の個人番号利用事務実施者に提出し、本人に交付する作業

3　事務取扱担当者は、特定個人情報等の取扱いに関し、不正なアクセス、データの粉失・破壊・改ざん・漏えい等の事故又は法令若しくは本連盟諸規程に違反する行為の発生又はその兆候を把握した場合は、直ちに個人番号取扱責任者に報告しなければならない。

4　事務取扱担当者が変更となった場合は、確実な引継ぎを行い、会長が引継ぎの完了を確認しなければならない。

（個人番号取扱責任者）

第 3 条　本連盟は、特定個人情報等の取扱いの管理に関する事項を行うために必要な知識及び経験を有していると認められる従業者のうちから個人番号取扱責任者を置く。

2　個人番号取扱責任者は、次の各号の権限と責任を有する。

（1）　事務取扱担当者に対する必要かつ適切な監督

（2）　特定個人情報等の取扱状況の記録及びその管理

（3）　個人番号利用事務等を外部に委託する場合の委託先の選定、委託契約締結の承認、委託先における特定個人情報等の取扱状況の把握

3　取扱責任者は、特定個人情報等の取扱いに関し、不正なアクセス、データの紛失・

破壊・改ざん・漏えい等の事故又は法令若しくは連盟規程に違反する行為の発生又はその兆候を把握した場合、連盟役員に報告しなければならない。

（従業員の役割と責任）

第 4 条 特定個人情報の取得、利用、保存、提供、削除、廃棄等の作業は、個人情報取扱責任者が責任者になり、その監督のもとで実施する。

2 個人番号事務取扱担当者以外の従業員は、連盟の個人番号関係事務に従事することができない。

3 事務担当者は、連盟の個人番号関係事務を処理するために必要な限度で、個人番号及び特定個人情報の取得、利用、保存、提供、削除、廃棄等の作業に従事することができる。

4 本連盟が個人番号関係事務を外部に委託する場合の委託先に関する監督は、取扱責任者が責任者となり、その監督のもとで実施する。

（特定個人情報の取得）

第 5 条 特定個人情報等の取得を担当する事務取扱担当者は、連盟が他人から個人番号の提供を受ける場合に、情報漏えい等を防止するため、下記各号を遵守して個人番号その他の特定個人情報を取得する。

（1） 本人等から個人番号が記載された書類等（個人番号カードの 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） 本人等から個人番号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いれた状態で提出を受けるものとする。

（3） 本人等から個人番号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ね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、従事している個人番号関係事務の処理以外の目的で、取得した個人番号を含むメモ、複写、印刷物、データのコピーその他の控えを作成はならない。

（特定個人情報の入力）

第 6 条　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、情報漏えい及び個人番号の不正利用等を防止するため、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）　従事している個人番号関係事務の処理以外の目的で､個人番号を含むメモ､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）　従事している個人番号関係事務の処理以外の目的で、特定個人情報ファイルを作成してはならない。

第 3 章　人的安全管理措置

（個人番号事務取扱担当者の教育）

第 7 条　事務取扱担当者は、特定個人情報等の取扱いに関する留意事項等について、定期的に教育研修をうけなければならない。

（監督及び教育研修）

第 8 条　本連盟は、特定個人情報等が連盟諸規程に基づき適正に取り扱われるよう、事務取扱担当者に対しる必要かつ適切な監督を行う。

２　本連盟は、特定個人情報等の取扱いに関する連盟諸規程を従業者に遵守させ、特定個人情報等の適正な取り扱いに関する従業者の意識を高めるための啓発その他の教育研修を実施する。

（従業者の研修）

第 9 条　従業者は、本連盟が決定した方針に基づく研修を受けなければならない。

第 4 章　物理的安全管理措置

（入退室等の管理）

第 10 条　事務所の入退室は、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、後に入退室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） 従業者は、業務終了後は速やかに退館し、業務終了後に事務所にみだりに立ち入ってはならない。
（２） 事務所を最後に退室した記録(従業者名・退室時刻等)を記録として残す。
（３） 本連盟の休日等、事務所が閉鎖されている間に入室する場合は、個人情報保護管理責任者の承認を得なければならない。
（４） 訪問者を事務所に入室させる場合は、個人情報や個人番号を取り扱う事務を実施する区域及び個人情報や個人番号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） 個人情報保護管理責任者は、入退室の状況を定期的に確認する。

(情報取扱区域の管理)

第 11 条 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、情報漏えい等を防止するために、下記各号を理解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)

第 12 条 情報取扱区域において特定個人情報等を取り扱う機器・電子媒体等は、粉失・盗難による情報漏えい等を防止するため、下記各号を理解し、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） 本連盟か管理すべき特定個人情報等は、従業者の私物パソコン等で取り扱ってはならない。

第 5 章　技術的安全管理措置

（技術的安全管理措置）

第 13 条　本連盟は、本安全管理措置規則に従い、特定個人情報等及びこれら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、情報システムの監視等の、特定個人情報等に対する技術的な安全管理措置を行う。

（情報システムへのアクセス管理）

第 14 条　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、情報漏えい等を防止するため、下記各号を参照し、敵宣の安全管理措置を講じるものとする。

（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、職員番号、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インストールできることとする。

２　特定個人情報等を外部に送信する場合に、通信経路における情報漏えいを防止するために、下記各号を理解し、適宣の技術的安全管理措置を講じるものとする。

（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。

（附則）

第 1 条　本規則は、平成２７年１２月４日より実施する。