個人情報・特定個人情報安全管理細則

制定　2019 年 4 月 1 日

公益財団法人日本ライフセービング協会

第 1 章 総 則

（目 的）

第 1 条　本細則は、「個人情報・特定個人情報保護規程」（以下「保護規程」という。）に基づき、公益財団法人日本ライフセービング協会（以下「本協会」という。）における個人データ及び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

（従業者の役割と責任）

第 2 条　個人データ及び特定個人情報の取得、利用、保存、提供及び削除・廃棄等の作業は、個人情報取扱責任者（以下「取扱責任者」という。）が責任者となり、その監督のもとで実施する。

2．個人情報取扱担当者が取り扱う個人データの範囲は、当該個人情報取扱担当者が担当する業務の実施に必要な範囲に限定し、できる限り明確にする。

3．個人情報取扱担当者は当該業務の実施に必要な範囲の人員に限定し、みだりに他の従業者に個人データを取り扱わせてはならない。

4．個人番号事務取扱担当者（以下「事務取扱担当者」という。）以外の従業者は、本協会の個人番号関係事務に従事することができない。

5．事務取扱担当者は、本協会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（以下「特定個人情報等」という。）の取得、利用、保存、提供及び削除・廃棄等の作業に従事することができる。

6．本協会が個人データの取扱い又は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 3 条　特定個人情報等の取得を担当する事務取扱担当者は、他人から個人番号の提供を受ける場合に、紛失による情報漏えい等を防止するため、下記各号を遵守して特定個人情報等を取得する。

(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磁的方式を含む。以下同じ。）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、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、個人番号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してはならない。

（個人データ・特定個人情報の入力）

第4条　取得した個人データの情報システムへの入力を担当する個人情報取扱担当者は、情報漏えい等を防止するため、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（本細則第３章）及び技術的安全管理措置（本細則第４章）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) 入力したデータを暗号化又はパスワードにより保護した場合の暗号鍵・パスワードは、入力作業中は入力を担当する者が管理し、定期的に取扱責任者が管理の状況を点検する。

(4) 入力作業のほか、個人データの移送・送信、利用・加工、保存又は削除・廃棄等、あらかじめ権限を付与されている作業以外の作業を行ってはならず、権限外の作業を行う場合は、取扱責任者又は上長の承認を得なければならない。

２．取得した特定個人情報等の情報システムへの入力を担当する事務取扱担当者は、情報漏えいや個人番号の不正利用等を防止するため、前項各号のほか、下記各号を遵守して作業を実施する。

(1) 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。
(2) 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。

（個人データ・特定個人情報の利用等）

第５条　個人データの利用・加工、保存等（以下「利用等」という。）を担当する個人情報取扱担当者は、情報漏えい等を防止するため、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（本細則第３章）及び技術的安全管理措置（本細則第４章）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) 利用等の対象となるデータ及びそのバックアップデータを暗号化又はパスワードにより保護した場合の暗号鍵・パスワードは、利用等を担当する者が管理し、定期的に取扱責任者が管理の状況を点検する。
(4) 利用等の作業のほか、あらかじめ権限を付与されている作業以外の作業を行ってはならず、権限外の作業を行う場合は、取扱責任者又は上長の承認を得なければならない。

２．特定個人情報等の利用・保存等の作業を担当する事務取扱担当者は、情報漏えい等を防止するため、前項各号のほか、下記各号を遵守して作業を実施する。

(1) 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。
(2) 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すみやかに削除し、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。

（個人データ・特定個人情報の移送・送信等）

第 6 条　個人データの移送・送信・交付を担当する個人情報取扱担当者は、個人データの性質及び量等に応じて、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、適宜の保護措置を講じて作業を実施する。

(1) 個人データが記載された書類を他者に交付する場合は、封筒への封緘等により、他人が個人データを容易に確認できない状態で行う。

(2) 郵送等により個人データを移送する場合は、封筒への封緘等により、他人が個人データを容易に確認できない状態にした上、あて先を複数回確認のうえ送付する。

(3) ＦＡＸ送信により個人データを送信する場合は、あて先番号を確認の上、あらかじめ電話によりあて先に送信する旨を伝え、送信後に受領確認を行う。個人データが記載された書類等は確実に回収し、ＦＡＸ機等に放置してはならない。

(4) 個人データが記載された書類を本細則第 10 条に規定する管理区域又は取扱区域の外に持ち運ぶ場合は、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。

(5) 個人データが記録された機器・電子媒体等を管理区域又は取扱区域の外に持ち運ぶ場合は、持ち運ぶデータの暗号化、パスワードによる保護等を行った上で電子媒体に保存し、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。

(6) 個人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、取扱責任者又は上長の承認を得た上で、本細則第 15 条に規定する情報漏えい等の防止措置を講じた上、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し、受信確認を行う。

２．特定個人情報等の移送・送信・交付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、前項各号を参照し、適宜の保護措置を講じるとともに、下記各号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又は特定個人情報が記録されたデータを個人番号利用事務実施者に提出する場合は、当該個人番号利用事務実施者の指定する提出方法に従う。

(2) ＦＡＸ又はインターネット・メール等により特定個人情報等のデータを送信する場合は、取扱責任者の承認を得なければならない。

（個人データ・特定個人情報等の削除・廃棄）

第 7 条　個人データの削除又は廃棄を担当する個人情報取扱担当者は、個人データを確実に削除・廃棄するために、下記各号を参照し、適宜の方法で作業を実施す

る。

(1) 個人データが記載された書類等を、焼却、溶解、復元不可能な程度に細断可能なシュレッダーによる細断等の復元不可能な手段で廃棄する。

(2) 個人データが記載された書類又は電子媒体等の中の個人データを、容易に復元できない手段で削除する。

(3) 個人データが記録された機器及び電子媒体等を廃棄する場合は、専門業者の依頼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。

(4) 個人データ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、専門業者へ確認の上、データを完全消去する。

(5) 削除・廃棄の担当者が個人情報保護管理者又は取扱責任者に削除・廃棄の完了を報告し、個人情報保護管理者又は取扱責任者が確認する。

(6) 個人データの削除又は廃棄を実施した記録（削除・廃棄の日、削除・廃棄の方法、作業担当者）を保存する。

(7) 削除・廃棄の作業を委託する場合は、委託先が確実に削除・廃棄を実施したことについて証明書等により確認し、前号の記録に削除・廃棄の証明書等を添付する。

２．特定個人情報等の削除又は廃棄を担当する事務取扱担当者は、特定個人情報等を確実に削除・廃棄するために、前項各号を参照し、適宜の保護措置を講じるとともに、下記各号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等の個人番号部分を削除する場合は、復元不可能な程度にマスキングする。

(2) 特定個人情報等が記録された電子媒体等の中の個人番号を削除する場合は、容易に復元できない手段で削除する。

(3) 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個人番号も削除する。

（個人データ及び特定個人情報等の取扱状況の記録）

第８条　本協会における個人データの取扱いが法令及び本協会諸規程を遵守していることの検証・監査を可能とするために、下記各号を参照し、適宜の方法で個人データの取扱状況の記録を保存するものとする。

(1) システムログを保存する。

(2) 個人データの取得、利用、保存、提供及び削除・廃棄の状況が記載・記録されたデータ等を保存する。

(3) 個人データの取扱状況の記録に含まれる事項

①　個人情報データベース等の利用・出力状況

② 個人データが記載又は記録された書類・媒体等の持ち運び等の状況
③ 個人情報データの削除・廃棄の状況
④ 個人データの取扱を外部に委託した場合に、委託先における個人データの消去・廃棄を証明する記録
⑤ 個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）

２．本協会における特定個人情報等の取扱いが法令及び本協会諸規程を遵守していることの検証・監査を可能とするために、前項各号を参照し、適宜の方法で特定個人情報等の取扱状況の記録を保存するものとする。この場合、当該取扱状況の記録には、個人番号を記載・記録してはならない。

第３章 物理的安全管理措置

（入退館等の管理）

第９条 本協会本部の入退館は、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、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社し、業務終了後に本協会本部にみだりに立ち入ってはならない。
(2) 本協会の休日等、本協会本部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。
(3) 訪問者を本協会本部に入館させる場合は、取扱責任者が承認した場合を除き、次条に規定する管理区域及び取扱区域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。
(4) 事務局長は、入退館の状況を定期的に確認する。

（管理区域・取扱区域の安全管理）

第10条 個人情報データベース等（個人情報ファイル）を取り扱うサーバ及びメインコンピュータ等の情報システム（以下「情報システム」という。）を管理する区域（以下、「管理区域」という。）並びに個人データを取り扱う事務を実施する区域（以下「取扱区域」という。）は、情報漏えい等を防止するために、下記各号を参照し、適宜の方法で管理するものとする。

(1) 外部からは容易に立ち入る事ができない室内とする。
(2) 取扱区域について、座席配置の工夫及びのぞき込みを防止する措置の実施により、権限を有しない者による個人データ及び特定個人情報等の閲覧等を防止する保護措置を講じる。

(3) 管理区域は、取扱責任者が承認した場合を除き、情報システムを操作する権限を有する従業者以外の者が立ち入れない区域とする。
(4) 管理区域は、取扱責任者が承認した場合を除き、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の持込及び持運びを禁止し、取扱責任者は、必要に応じて当該機器の持込・持運びの検査を実施できるものとする。
(5) 取扱責任者が管理区域及び取扱区域の状況を定期的に点検する。

（機器等の管理）
第 11 条　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（以下、「機器及び電子媒体等」という。）は、紛失又は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、適宜の方法で管理するものとする。
(1) 個人データを取り扱う機器は、離席時に個人データが見えないように設定する。
(2) 機器及び電子媒体等を、施錠できるキャビネット、書庫又は金庫で保管する。
(3) 個人データを取り扱う機器について、セキュリティワイヤーで固定する等、容易に外部に持ち運ぶことができない措置を講じる。
(4) 個人データを取り扱う機器は、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取扱責任者の承認を得ずに接続してはならない。
(5) 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を机上に放置してはならない。
(6) 本協会が管理すべき個人情報を従業者の個人所有機器で取り扱ってはならない。
(7) 情報システムの操作マニュアルを机上に放置してはならない。
(8) 機器及び電子媒体等を管理区域又は取扱区域の外に持ち運ぶ場合は、取扱責任者の承認を得なければならない。
(9) 機器及び電子媒体等を管理区域又は取扱区域の外に持ち運ぶ場合は、記録された個人データの暗号化やパスワードによる保護等を行う。
(10) 個人データが記載された書類を管理区域又は取扱区域の外に持ち運ぶ場合は、封筒への封緘等により、他人が個人データを容易に確認できない措置を講ずる。
(11) 機器及び電子媒体等を管理区域又は取扱区域の外に持ち運ぶ場合は、施錠できる搬送容器を利用する。

２．特定個人情報等を取り扱う機器、特定個人情報等が記録された電子媒体又は特定個人情報等が記載された書類等は、紛失又は盗難による情報漏えい等を防止するため、前項各号を参照し、適宜の方法で管理するものとする。

第４章 技術的安全管理措置

（アクセス制御）

第 12 条　個人情報取扱担当者及び事務取扱担当者、並びにこれらの者が取り扱う個人情報データベース等及び特定個人情報ファイルの範囲を限定するために、下記各号を参照し、適宜の方法でアクセス制御を行うものとする。

(1) 個人番号と紐付けてアクセスできる情報の範囲を限定する。

(2) 個人情報データベース等又は特定個人情報ファイルを取り扱うことのできる情報システムを限定する。

(3) ユーザーＩＤに付与するアクセス権により、情報システムにアクセスできる従業者を限定する。

(4) ユーザーＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。

（アクセス者の識別と認証）

第 13 条　情報システムを使用する個人情報取扱担当者や事務取扱担当者が正当なアクセス権を有する者であることを識別・認証するために、下記各号を参照し、適宜の措置を講ずるものとする。

(1) ＩＤ・パスワード等の識別情報により、識別と認証を実施する。

(2) 識別情報の発行、変更及び廃止・削除は、取扱責任者が行う。

(3) ＩＤ・パスワードは付与される者ごとに異なるものとし、パスワードの最低文字数・有効期限等は取扱責任者が定める。

(4) パスワードは、氏名、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。

(5) ＩＤ・パスワードを複数人で共同利用してはならない。

(6) ＩＤ・パスワードは、机上に放置するなど他人が容易に利用できる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) 情報システムへのアクセスは、業務時間内に限って行うものとする。

（外部からの不正アクセス等の防止）

第 14 条　情報システムを外部からの不正アクセス又は不正ソフトウェアから保護するために、下記各号を参照し、適宜の措置を講ずるものとする。

(1) 情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置して、不正アクセスを遮断する。

(2) 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（ウイルス対策ソフトウェア等）を導入する。

(3) 情報システム、機器及びソフトウェアに装備されている自動更新機能により、オペレーティングシステムやソフトウェア等を最新の状態に更新する。

(4) 機器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。

(5) 情報システム及び個人情報へのアクセスや操作の成功と失敗の記録（ログ）を定期的に分析し、不正アクセス等を検知する。

（情報システムの使用に伴う情報漏えい等の防止）

第 15 条　情報システムの使用に伴う情報漏えいや情報の外部への送信に伴う通信経路における情報漏えい等を防止するために、下記各号を参照し、適宜の措置を講ずるものとする。

(1) 情報システムの設計時に安全性を確保し、情報システムのぜい弱性を突いた攻撃への対策を講じることも含めて継続的に見直しを実施する。

(2) 通信の経路を暗号化する。

(3) 通信の内容を暗号化する。

(4) 送信するデータに暗号化やパスワードによる保護をかける。

第 5 章 委託先の監督

（委託先の選定及び委託契約の締結）

第16条　本協会が個人データの取扱い又は個人番号関係事務を外部に委託する場合は、個人情報保護管理者又は取扱責任者の監督下で、委託先に対して次の各号の事項を実施するものとする。

(1) 委託先の選定にあたり、個人データ又は特定個人情報等に関して本協会が実施する組織的、人的、物理的及び技術的な安全管理措置と同等の措置が、委託する業務内容に沿って委託先において確実に実施されることについて、あらかじめ確認する。

(2) 委託先との間で次の事項を含む契約を締結する。

① 委託した個人データ及び特定個人情報等に関する秘密保持義務

② 委託した個人データ又は特定個人情報等の事業所内からの持ち運びの禁止
③ 委託した業務以外の目的で個人データ又は特定個人情報等を利用することの禁止
④ 再委託に関する事項
再委託は原則として禁止し、再委託がやむを得ない場合は、書面による本協会の許諾を得て再委託するものとし、委託先が再委託先と連帯して責任を負うことの確認
⑤ 再委託先が更に再委託する場合も、書面による本協会の許諾を得て再委託するとともに、再々委託先が再委託先及び委託先と連帯して責任を負うことを要し、更に再委託が繰り返される場合も同様である旨の確認
⑥ 委託先が委託先の従業者に対して個人データ又は特定個人情報等の安全管理に関して必要な監督・教育を実施すること
⑦ 委託先における契約内容の遵守状況についての報告
⑧ 委託した個人データ又は特定個人情報等に関する漏えい事故等が生じた際の委託先の責任
⑨ 委託契約終了時の個人データ及び特定個人情報等の返却、抹消及び廃棄

（委託先の監査）
第 17 条　本協会は、取扱責任者の監督のもとで、委託先に対し、適宜、契約内容が順守されていることの報告を求めるなどして、委託先における個人データ及び特定個人情報等の取扱状況を調査し、必要に応じて委託の内容等を見直すものとする。

第 6 章 雑則

（細則内容の変更）
第 18 条　この細則に定める内容については、法令の制定もしくは改廃、または本協会の経営状況及び社会情勢の変化等により必要がある場合には、本協会は職員代表と協議のうえ、理事会で議決し変更することがある。

（解釈）
第 19 条　この細則の解釈に疑義が生じた時は、本協会は職員の代表と協議の上決定し、協議が整わない場合は代表理事が決定する。

附 則
第 1 条 本細則は、2019 年 4 月 1 日より実施する。