個人情報の保護に関する運用管理規程

目　次

第１章　総則

（目的）

第１条　特定非営利活動法人いわい地域支援センター個人情報の保護に関する規程第３２条第１項に基づき運用管理規程を設ける。この規程は、各事業所（以下（以下「当事業所」）において、情報システムで使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取扱い及び管理に関する事項を定め、当事業所において、個人情報を適正に保存するとともに、適正に利用することに資することを目的とする。

（対象）

第２条　この規程において対象とするものは次に掲げるものとする。

１　対象者は、情報システムを扱う全ての職員である。

２　対象システムは、生活支援システムである。

３　対象情報は、全ての個人情報に関する情報である。

第２章　組織的安全管理

（システム管理者、運用責任者の任命）

第３条　当事業所に情報システム管理者を置き、理事長をもってこれに充てること。

２　理事長は必要な場合、情報システム管理者を別に指名すること。

３　情報システムを円滑に運用するため、情報システムに関する運用を担当する責任者（以下「運用責任者」）を置くこと。

４　運用責任者は理事長が指名すること。

５　情報システムに関する取扱い及び管理に関し必要な事項を審議するため、理事長のもとに情報システム管理委員会を置くこと。

６　情報システム管理委員会の運営については、別途定めること。

７　その他、この規程の実施に関し必要な事項がある場合については、情報システム管理委員会の審議を経て、理事長がこれを定めること。

（作業担当者の限定）

第４条　本規程が対象とする業務に携わる担当者は別表に定める通りとする。

（マニュアル書の整備）

第５条　運用責任者は、情報システムの取扱いについてマニュアルを整備し、職員に周知の上、常に利

用可能な状態にしておくこと。
（監査体制と監査責任者の任命）
第６条　情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（監査責任者）を置くこと。
２　監査責任者の責務は本規程に定めるものの他、別に定めること。
３　監査責任者は理事長が指名すること。
４　情報システム管理者は、監査責任者に毎年４回、情報システムの監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。
５　監査の内容については、情報システム管理委員会の審議を経て、理事長がこれを定めること。
６　情報システム管理者は必要な場合、臨時の監査を監査責任者に命ずること。
(苦情の受付窓口の設置)
第７条　利用者又は職員からの、情報システムについての苦情を受け付ける窓口を設けること。
２　苦情受け付け後は、その内容を検討し、直ちに必要な措置を講じること。
（事故対策）
第８条　情報システム管理者は、緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照できるような媒体に保存し保管すること。

第３章　物理的安全管理

（入退室管理）
第９条　役職員及び個別業務従事者は、タイムカード等により事業者への入退所に関する記録を残さなければならない。
２　各事業所内事務室は、事業所毎に定める建物管理規則に従い、夜間または事務室担当職員不在時には必ず施錠しなければならない。
３　業務が終了次第、役職員及び個別業務の従事者は、退所時間を記録し、速やかに事業所を離れること。
（電子情報端末の保全）
第１０条　個人情報を取り扱うコンピュータ等電子情報端末は、ワイヤーロックや施錠できる場所への保管等、盗難防止対策を付さなければならない。
（記録媒体の取扱い）
第１１条　事業所に個人情報が保存されている記録媒体が存在する場合は、運用責任者が必ず管理を行い必ず施錠できる場所での保管、利用目的達成後の完全消去等、安全で適切な管理を行うこと。
（情報資産の持出の管理）
第１２条　役職員及び個別業務の従事者は、あらゆる情報資産（情報機器、ソフトウェア、記録媒体等）を事前の許可無く事業所外へ持ち出してはならない。
２　前項に係らず、研究・発表その他の目的のために持ち出す場合、運用責任者、担当者は、予め「情報資産持出申請書」に目的、内容、持出先、持出期間等所定の事項を記入・作成し、情報システム管理者の許可を得なければならない。

第４章　技術的安全管理

（セキュリティ対策）

第１３条　事業所電子計算組織を構成する電子情報端末は、別表配置基準に基づき配置し、セキュリティ対策を行う。
（情報システムへのアクセス制限、点検等アクセス管理）
第１４条　運用責任者は、職務により定められた権限によるデータアクセス範囲を定め、必要に応じてハードウェア・ソフトウェアの設定を行う。また、その内容に沿って、アクセス状況の確認を行いｍ監査責任者に報告する。
（他電子計算組織との結合、不正アクセス・ウィルス対策）
第１５条　事業所電子計算組織と、事業所の機関以外のものの電子計算組織とを通信回線その他の方法により結合する場合には、外部からの不正な侵入を防ぐための電子防火壁を設置し、電子情報端末にはウィルス対策ソフトを導入する。その構成についてシステム管理台帳にその内容を示す。
（通信上の安全対策）
第１６条　事業所電子計算組織には、通信暗号化装置設置によるデータ暗号化を行い、通信上の安全確保を行う。
（不正ソフトウェア対策）
第１７条　事業所電子計算組織で使用可能なアプリケーションは、運用責任者による審査を経て、システム管理台帳に登録されたものに限られる。登録を希望するアプリケーションが生じた場合には、運用責任者を通じ情報システム管理者へ申請を行い、審査を経なければならない。基本ソフト等のセキュリティ更新プログラム導入については運用責任者より指示を行う。
（外部記憶媒体への書き込み禁止）
第１８条　事業所電子計算組織内の電子情報端末において、外部記憶媒体による持ち出し権限を有するもの以外は、外部記憶媒体からの読み込み可とし、書き込みは不可とする。
（作成者の識別および認証）
第１９条　情報システム管理者は、電子保存システムを使用する職員の登録を管理し、そのアクセス権限を規定し、不正な利用を防止すること。
２　パスワードの最低文字数、有効期間等を別途規定すること。
３　認証の有効回数、超過した場合の対処を別途規定すること。
４　職員は、自身の認証番号やパスワードを管理し、これを他者に利用させないこと。
５　職員は、電子保存システムの情報の参照や入力を（以下「アクセス」）に際して、認証番号やパスワード等によって、システムに自身を認識させること。
６　システム管理者は、電子保存システムを正しく利用させるため、職員の教育と訓練を行うこと。
７　職員は、作業終了あるいは離席する際は、必ずログアウト操作を行うこと。
８　電子保存システムにおいて保存されている情報の情報の作成責任者は××であること。
（情報の確定手順と、作成責任者の識別情報の記録）
第２０条　職員は、電子保存システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。
２　代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
３　本規程が対象とする情報システムの作成データの「確定」については、付表に記す。
（更新履歴の保存）
第２１条　職員は、電子保存システムへの情報入力に際して、確定操作（入力情報が正しい事を確認す

る操作）を行って、入力情報に対する責任を明示すること。
２　代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
（機器・ソフトウェアの品質管理）
第２２条　運用責任者は、機器・ソフトウェアの品質保持のため、保守点検を行う。
（見読化手段の管理）
第２３条　電子保存に用いる機器及びソフトウェアを導入するに当たって、システムの機能を確認し、これらの機能が見読性の確保に適合するように留意すること。
２　システムの機能要件に挙げられている機能が支障なく運用される環境を整備すること。
３　保存義務のある情報として電子保存された情報（以下「電子保存された情報」）の安全性を確保し、常に利用可能な状態に置いておくこと。
（見読目的に応じた応答時間とスループット）
第２４条　運用責任者は、応答時間の劣化がないように維持に努め、必要な対策をとること。
（システム障害対策）
第２５条　運用責任者は、障害時の対応体制が最新のものであるように管理すること。
（ソフトウェア・機器・媒体の管理）
第２６条　記録媒体は、記録された情報が保護されるよう、別の媒体にも補助的に記録する。
２　品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写する。
（不適切な保管・取り扱いによる情報の滅失、破壊の防止策）
第２７条　運用管理責任者は新規の業務担当者には、操作前に教育を行う。
（記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止策）
第２８条　記録媒体は、記録された情報が保護されるよう、別の媒体にも補助的に記録する。
２　品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写する。
（媒体・機器・ソフトウェアの整合性不備による復元不能の防止策）
第２９条　運用責任者は、電子保存システムで使用されるソフトウェアを、使用の前に審査を行い、情報の安全性に支障がないことを確認すること。
２　運用責任者は、ネットワークや可搬型媒体によって情報を受け取る機器について、必要に応じてこれを限定すること。
３　運用責任者は、定期的にソフトウェアのウィルスチェックを行い、感染の防止に努めること。
４　電子保存システムの記録媒体を含む主要機器は独立した電算機室に設置すること。
５　電算機室の出入り口は常時施錠し、運用責任者がその入退出を管理すること。
６　電算機室には無水消火装置、漏電防止装置、無停電電源装置等を備えること。
７　設置機器は定期的に点検を行うこと。
８　記録媒体は、記録された情報が保護されるよう、別の媒体にも補助的に記録すること。
９　品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写すること。
（情報の継続性の確保策）
第３０条　機器やソフトウェアに変更があった場合においても、電子保存された情報が継続的に使用出来るよう維持すること。

第５章　人的安全管理

（職員の責務）
第３１条　職員は、規程第３条第２項の定めに従い、入社時に「個人情報に関する誓約書」を退社時に「退職後の機密保持に関する誓約書」を事務局に提出しなければならない。
２　個別業務の委託先の従業者及び派遣会社社員（以下
個別業務の従事者」という）は、業務開始に先立ち、「個人情報に関する誓約書」を勤務先に提出しなければならない。
（職員の教育）
第３２条　情報システム管理者は、事業所における役員、管理職者、一般職員、派遣会社社員及び委託業務従事者に対する個人情報保護の趣旨を啓蒙する研修の機会を定期的に設け、人権擁護の意識の涵養に努めなければならない。
２　研修に参加した職員は、自書署名により出席したことを記録する。
３　欠席者に対しては、教材を配布し教育内容を周知するなど確実に実施する。
（定期または不定期なシステム取り扱い及びプライバシー保護に関する研修）
第３３条　運用責任者は、情報システムを使用する職員に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行うこと。また、研修時のテキスト、出席者リストを残すこと。

第６章　委託先の管理

（委託契約における安全管理に関する条項）
第３４条　業務を当事業所外の所属者に委託する場合は、守秘事項を含む業務委託契約を結ぶこと。契約の署名者は、その部門の長とする。また、各担当者は委託作業内容が個人情報保護の観点から適正且つ安全に行われていることを確認する。
（保守会社における守秘義務契約の締結）
第３５条　システムの導入にあたっては、保守時における守秘義務条項を含む業務委託契約の締結を行い、必要時には保守会社の体制を確認する。
（保守要員専用のアカウントの作成及び運用管理）
第３６条　運用責任者は、保守会社における保守作業に関し、保守専用のアカウントを登録し、その作業者、作業内容、につき報告を求め適切であることを確認する。
（メッセージログの採取と確認）
第３７条　運用責任者は、保守会社における保守作業に関し、作業内容のメッセージログを残すよう義務付けるとともに、その作業者、作業内容、につき報告を求め適切であることを確認する。

第７章　データの廃棄

（個人情報の廃棄）
第３８条　個人情報の廃棄は、破砕、完全消去など再利用できない状態に処分し、「個人情報評価・管理票」に廃棄日を記入する。
（データの抹消）
第３９条　電子計算組織や複合機等のリース会社への返却を行う等電子情報端末の利用を停止する場合には、完全なデータ抹消処理を要するため、必ず運用責任者に連絡すること。

附則

この規程は、平成１７年４月１日から施行する。

＜関連規程＞
①個人情報の保護に関する規程
②苦情受け付け・解決に関する規程