

システム等運用管理規程

第1章（総則）

（目的）

第1条 本規程は、組合の情報セキュリティ基本方針及び個人情報保護管理規程に従い、当組合の業務を取り扱うシステム（以下、「情報システム」という）及び個人情報等を含むデータの安全かつ合理的な運用及び適正な管理を図るとともに、データの漏えい、滅失、毀損等の防止を図るために必要な事項を定めることを目的とする。

（適用対象）

第2条 本規程の適用対象は、組合における全ての情報システム及び個人情報又は組合に関し外部に知られることを適当としないデータ又は事故等が発生した場合に、その復元等が著しく困難となるおそれのあるデータまたは情報（記録様式、媒体の種類を問わない。以下「データ」または「情報」という。）とする。

第2章（組織的な対策）

（管理運営体制）

第3条 本規程の実施にかかる管理運営体制は次の実務責任者により構成されるものとする。

- (1) 本規程の実施にかかる管理責任者として、「データ保護管理者」を置くものとし、原則として個人情報取扱責任者が就任するものとする。
- (2) データ保護管理者の指示のもとに本規程の実施にかかる実務担当者として「データ保護担当者」を置くものとし、原則として個人情報保護管理担当者が就任するものとする。
- (3) 本規程の適正な実施にかかる監査の実施者として「情報システム監査責任者」を置くものとし、原則として監事が就任するものとする。

（実務責任者の責務等）

第4条 データ保護管理者は以下の責務等に基づいて実務を行うものとする。

- (1) 本規程に定める組織的、人的、技術的、物理的安全対策の実施により情報システム及びデ

ータの取扱について、適正かつ円滑な運用を図る。

- (2) 情報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。
- (3) 情報システム及びデータの取扱についての苦情対応窓口を設置する。
- (4) 監査結果に基づく是正等の必要な措置を講じる。
- (5) 情報システム及びデータを取扱う担当者として、当該取扱が必要となる業務ごとに「事務担当者」を任免し、アクセス権限を付与する。
- (6) 情報システム及びデータについて不正利用が行われた場合、またはその疑いが見込まれる場合、「事務担当者」が使用した電子メール、インターネットへのアクセス、その他情報システム及びデータの使用履歴及び内容について調査することが出来るものとする。

2 データ保護担当者は、以下の責務等に基づいて実務を行うものとする。

- (1) 情報システム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する。
- (2) 個人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。
- (3) 機器やソフトウェアに変更があった場合においても、情報が継続的に使用できるよう維持する。
- (4) 情報システム等への事務担当者の登録並びにアクセス権限を定める。
- (5) 事務担当者への教育及び周知を実施する。
- (6) 情報システム等にかかる安全管理の見直し及び改善の基礎として、データ保護管理者に情報システム等の運用状況を報告する。
- (7) 情報システム等にかかるマスタの管理及び変更追加時におけるデータ保護管理者への報告等により、正常な稼動状況を維持管理する。

3 情報システム監査責任者は、以下の責務等に基づいて実務を行うものとする。

- (1) 情報システム及びデータの取扱にかかる監査を実施し、その結果について監査報告書をもってデータ保護管理者に報告する。
- (2) 監査の実施においては、監査の客観性及び公平性を確保する。

(事務担当者の責務)

第5条 事務担当者は、付与されたアクセス権限に基づき情報システムを利用することが出

来る。この場合において、法令及び関連規程を遵守することはもとより、以下の責務等に基づいて実務を行うものとする。

- (1) 自身のアクセス権限にかかるパスワード等の情報を管理し、これを他者に利用させない。
- (2) 1号に定める管理が正当に行われなかったために生じた事故や障害に対しては、当該担当者が責任を負う。
- (3) 情報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。
- (4) 付与されたアクセス権限を越えた操作を行わない。
- (5) 情報システム及び参照した情報を、業務の目的外に利用しない。
- (6) 加入者等のプライバシーを尊重し、職務上知ることが必要な情報以外の情報にアクセスしてはならない。
- (7) 利用者は、法令上の守秘義務の有無に関わらず、アクセスにより知り得た情報を目的外に利用し、又は正当な理由なしに漏らしてはならない。異動、退職等により職務を離れた場合においても同様である。
- (8) システム等の異常を発見した場合、速やかにデータ保護管理者またはデータ保護担当者に報告し、その指示に従う。
- (9) 不正アクセスを発見した場合、速やかにデータ保護管理者またはデータ保護担当者に報告し、その指示に従う。
- (10) 離席する際は、窃視防止策を実施する（ログアウトまたはスクリーンロック等）。
- (11) ウィルスに感染又はその恐れを発見した場合、ネットワークから端末を切り離すとともに、速やかにデータ保護管理者またはデータ保護担当者に報告し、その指示に従う。
- (12) 電子メール等の利用に際し、公序良俗に反する、著作権または他者の財産を侵害するおそれがあるものなど組合の信用、品位を傷つけるおそれのある内容を発信、公開してはならない。

（予防処置及び是正処置）

第6条 組合は、加入者、システム利用者等からの苦情、緊急事態の発生、監査報告、外部審査機関等からの指摘により、システムの機能、運用状況等に問題がある場合には、問

題に対する予防処置及び是正処置（以下、「処置等」という）のための責任及び権限を定め、処置等の手順を定めて、これを実施する。

2 前項に定める処置等は、以下の手順で行うものとする。

- (1) 発生した問題の内容を確認のうえ、問題の原因を特定する。
- (2) 発生した問題の処置等を立案する。
- (3) 立案された処置等について、期限を定めて実施して、実施結果を確認する。
- (4) 実施された処置等の有効性を確認する。
- (5) 発生した問題について、問題の内容、原因、実施した処置等の実施結果及び有効性を記録する。

（事故への対応）

第7条 組合は、事故が発生した場合、再発防止策を含む適切な対策を速やかに講じなければならない。

2 データ保護管理者又はデータ保護担当者は、事故等発生の予防のため、情報システムの扱う情報について、予見されるリスクを洗い出すとともに、事故発生時の危険度を明確にして、リスク分析に努める。

（監査）

第8条 本規程における法令、関連通知への準拠状況及び情報システムの運用状況及びデータの取扱いについて、少なくとも年に1度、第4条第3項に定める監査を受けなければならない。

2 データ保護管理者は、情報システム監査責任者から監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な処置等を講じなければならない。

3 データ保護管理者は必要な場合、臨時監査を情報システム監査責任者に進言することができる。

（苦情・質問受付）

第9条 組合は、個人情報の取扱い及び情報システムの運用に関し、加入者及びシステム利

用者からの苦情及び質問の受付窓口（以下「受付窓口」という。）を設置するものとする。

- 2 受付窓口は、直接または間接的に苦情を受けた際に、速やかに対応しなければならない。
- 3 受付窓口は、受付けた苦情・質問を整理し、データ保護管理者に報告しなければならない。
- 4 データ保護管理者は、受付窓口の報告を受け、問題点の指摘等がある場合には、直ちに必要な処置等を講じる。

（守秘契約）

第10条 組合の役職員等（雇用形態を問わず、組合内において組合に関連する業務に従事する全ての者をいう。）は在職中のみならず、退職後においても業務中に知り得た個人情報等第2条に定める本規程の適用対象に関する守秘義務を負う。

- 2 役職員等を採用するにあたり、雇用契約等締結時に前項の守秘義務契約を締結するものとする。

（業務委託契約）

第11条 組合業務を外部委託する場合には、以下の処置を実施するものとする。

- 2 守秘事項を含む業務委託契約を結ぶものとする。
- 3 第2項に定める契約に、次に示す事項を規定し、十分な個人情報の保護水準を担保しなければならない。

(1) 個人情報の安全管理に関する事項

(2) 事業所内からの個人情報の持出しの禁止

(3) 個人情報の目的外利用の禁止

(4) 再委託に関する事項

(5) 個人情報の取扱状況に関する委託者への報告の内容及び頻度及び第6項に定める監査への協力事項

(6) 契約内容が遵守されていることを委託者が確認できる事項

(7) 契約内容が遵守されなかった場合の処置

(8) 事件・事故が発生した場合の報告・連絡に関する事項

- (9) 漏えい事案等が発生した場合の委託先の責任に関する事項
 - (10) 一連の委託業務終了後に関する事項（終了報告、確実に情報を消去する等）
 - (11) 確実に削除又は破棄したことを証明書等により確認できる事項
 - (12) 保守要員のアカウント情報の管理に関する事項（適切に管理することを求める）
 - (13) 従業者に対する監督・教育
- 4 再委託は原則として禁止するものとし、やむを得ない事情等により委託先事業者が再委託を行う場合は、当組合による再委託の許諾を要件とする。この場合、再委託先において、委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とし、組合との業務委託の契約書に再委託での安全管理に関する事項を加えるものとする。
- 5 組合の情報システム等の保守・改修・管理を委託する等により、役職員以外の者（保守要員という。以下同じ。）が組合内で作業する場合において、データ保護管理者またはデータ保護担当者は、以下の確認を実施する。
- (1) 保守要員用のアカウントの確認（保守要員個人の専用アカウントを使用すること）。
 - (2) 保守作業等の情報システムに直接アクセスする作業の際には、作業員・作業内容及び作業結果の確認（原則として日単位）。
 - (3) 清掃等、直接情報システムにアクセスしない作業の場合の定期的なチェック。
 - (4) 保守契約における個人情報保護の徹底。
 - (5) 保守作業の安全性についてログによる確認。
- 6 委託先（再委託先を含む）における法令、契約等に基づく個人情報保護にかかる措置の遵守状況を確認する為、定期的または必要な都度、立ち入り監査を実施するものとする。

第3章（人的な対策）

（教育の実施）

第12条 データ保護管理者及びデータ保護担当者は、情報セキュリティの重要性と、個人情報の適切な取扱、及び安全管理について意識面及び技術面の向上を目的として、役職員に対し必要かつ適切な監督及び継続的な教育を行うものとする。

第4章（物理的な対策）

（入退出管理）

第13条 部外者（原則として組合の役職員以外の者をいう。以下同じ。）の立ち入りを制限する必要がある物理的な領域を以下のように定義する。

- (1) 組合の役職員が執務する場所または部屋を「執務室等」という。
- (2) 個人情報保管されているサーバー及び記録媒体を設置または保管する場所または部屋を「サーバー室等」という。
- 2 部外者が執務室等またはサーバー室等に立ち入る場合、入退室記録の作成等の管理を実施する。
- 3 データ保護管理者またはデータ保護担当者は、サーバー室等の出入口を常時施錠管理し、その入退室を記録・管理する。
- 4 サーバー室等への入退出は、データ保護管理者の承認を得て行うものとする。なお、部外者の入退出においてはその者の身分等について確認するものとする。
- 5 サーバー室等は、組合の役職員の常駐または防犯カメラによる常時監視し得る措置をとる等のセキュリティが保たれた管理領域とする。
- 6 データ保護管理者は、入退室に関し、問題が確認されたつど、適切な措置を講ずる。

（執務室等及びサーバー室等の安全管理）

第14条 データ保護管理者は、執務室等及びサーバー室等における火災、その他の災害、盗難に備えて、非常電源装置、無停電装置、自動消火装置、監視カメラ、入退制限装置などによる必要な保安処置を講じなければならない。

- 2 データ保護管理者は、情報システム等の正常稼働維持のため、執務室等及びサーバー室等の温度、湿度等の環境を適切に保持するものとする。

（記録機器及び端末の安全管理）

第15条 サーバー等の記録機器及びPC等の端末は、以下のいずれかの対策により盗難防止措置を講ずるものとする。

- (1) 盗難防止用ワイヤーロックで固定する。

(2) 執務室等またはサーバー室等を施錠し、管理する。

2 PC等端末の使用に際しては、部外者の通る方に画面を向けず、窃視防止フィルムを貼るなどの、窃視防止に努めるとともに、離席時など、特定の時間（5分以内）使用しなかった場合は、なりすましによる使用を防ぐため、パスワード付きスクリーンロック又は、自動ログオフ機能を設定するものとする。

3 サーバー等の記録機器及びPC等端末の廃棄及びレンタル・リース切れによる返却等に当たっては、以下(1)または(2)の手続きを行った上で当該処理を行うものとする。

(1) ハードディスク等の既存情報を上書処理により書き換え、情報の完全消去を行う。

(2) ハードディスク等の物理的破壊によるデータ消去を行う。

4 前項に定める情報の消去または物理的破壊を外部業者に委託する場合は、情報を完全消去した証明書を受領し、証明書を保管管理するものとする。

(ネットワーク管理)

第16条 情報システムのネットワーク（以下、「LAN」という）は、インターネット、仮想プライベートネットワーク（以下、「VPN」という）等の当組合の外部と情報交換ができるネットワークとは技術的な安全対策を適用した上で接続するものとする。

2 事務担当者は、LANに端末を接続する場合、データ保護管理者の承認を得なければならない。

3 事務担当者が私有（組合が支給したもの以外をいう。）のPCを持ち込み、LANに接続することは、原則禁止とする。ただし、業務上やむを得ず接続を要する場合は、データ保護管理者の承認を得て行うこととする。この場合、PCの使用にあたっては、本規程を準用するものとする。

4 委託先等の部外者が情報システム等保守のためPC等を持ち込んでLANに接続する場合、データ保護管理者の承認を得なければならない。

(外部機関との情報交換)

第17条 医療保険者、保守会社、通信事業者、運用委託業者等の外部機関と情報を交換する場合、相手外部機関との間で、責任分界点や責任の所在を契約書等で明確にするもの

とする。ただし、法令等で情報交換が必要な外部機関と接続する場合は、この限りではない。

(電子媒体の管理)

第18条 データ保護管理者が特に許可した場合を除き、情報のバックアップ業務以外には外部記憶媒体へのデータ等の複写を禁止するものとする。

- 2 電子媒体の廃棄は、原則破壊処理とする。
- 3 個人情報を記録した可搬型記録媒体（FD、CD-ROM、DVD、USBメモリ等）は、施錠できるキャビネットに保管する。
- 4 個人情報を可搬型記録媒体で授受する場合は、授受の記録を残すものとする。
- 5 個人情報を記した電子媒体の廃棄に当たっては、安全かつ確実に行われることを、データ保護管理者が作業前後に確認し、結果を記録に残すものとする。

(情報の持出し及び情報機器の管理)

第19条 情報の持出しに関して、持出し対象となる情報を規定し、それ以外の情報の持出しを禁止するものとする。情報機器の持ち出しは禁止する。

- 2 持出し対象となる情報をまとめて、利用者に公開するものとする。
- 3 持出し対象となる情報の持出しについては、情報の暗号化、ファイル交換ソフトのインストール禁止の実施及び次の措置を講ずるとともに、データ保護管理者の承認等を条件とする。

(1) 起動パスワードを設定する。

(2) ウィルス対策ソフトをインストールする。

(3) 別途定めたもの以外のアプリケーションはインストールしない。

4 盗難、紛失時は、以下のように対処することとする。

(1) 持出した情報及び情報機器の盗難、紛失時には、速やかにデータ保護管理者に届け出る。

(2) 届出を受け付けたデータ保護管理者は、その情報及び情報機器の重要度に従って対応する。

(データ等の消去及び電子媒体の廃棄)

第20条 情報システム等で保有するデータ及び電子媒体に収録されたデータについては、法令の定めた保存期間の間保存・管理するものとする。ただし、法令の定めのない場合については、以下の期間、保存・管理するものとする。

(1) 情報システム等で保有するデータについては5年

(2) 電子媒体に収録されたデータについては3年

(3) (1)のバックアップを目的としたデータについては5年

2 保存期間経過後の消去及び廃棄方法について、破碎処理または溶融処理する等復元不可能な状態にしなければならない。なお、消去及び廃棄した場合、その証明書等を管理するものとする。

3 行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25年5月31日・法律第27号。）第2条第8項に定める個人番号データ（情報システム等で保有するものに限る）については、第1項に定める期間を資格喪失又は扶養削除の日から3年間とする。

第5章（技術的な対策）

(アクセス権限等)

第21条 データ保護担当者は、第4条第1項第5号に定めるアクセス権限について、役員等の採用時、異動時、退職時に合わせ、速やかに利用者の認証情報の登録、変更、削除及び認証情報の発行処置を実施するものとする。

2 データ保護担当者は、情報システム等の使用について利用者等の申請により、情報システムへのアクセス権限を審査し、ID・パスワードの設定等本人認証のための措置を実施のうえ、利用者登録を実施する。利用者登録実施後、利用者の認証に必要なデバイスまたは認証情報を利用者へ交付する。

3 利用者には、原則として利用者権限を付与し、管理者権限は付与しない。

4 保守等のため外部からサーバ等へアクセスする場合でも、特定個人情報へのアクセス権限は付与しない。

(サーバー等記録機器の管理)

第22条 データ保護管理者は、サーバーへのアクセス状況・稼動状況を定期的に確認し、問題がある場合は、速やかに必要な処置を講ずるものとする。

- 2 データ保護管理者は、職務により定められた権限による情報アクセス範囲及び第26条に定めるアクセス権限とは別に管理者権限の付与に関する事項を定め、これに基づきハードウェア及びソフトウェアの設定を行うとともに、情報システム、情報への使用状況を監視するため、アクセスログを取得出来るものとする。
- 3 異常なアクセスを検知したときは警告を発して、ネットワークを切断する等の対処をするものとする。
- 4 情報のバックアップを定期的実施する。

(ネットワーク管理)

第23条 組合のLANは、法に定める場合を除き、他の法人格のある外部機関と共用しない。

また、インターネット等のオープンなネットワークと物理的または論理的に遮断する等の安全管理措置を実施するものとする。なお、インターネット等のオープンなネットワークに関し、母体企業のLANを使用する場合の管理については、母体企業の管理に準ずる。

- 2 インターネットの利用について、以下の条件の下で管理するものとする。
 - (1) インターネット利用は、業務上必要な場合に限られ、私的利用は禁止とする。
 - (2) データ保護管理者は、ホームページを含む不正アクセスや改ざんの防止のため、インターネットに係る各サーバー、ルータ等に適切な管理策等の処置を講じ、ファイアウォール及びプロキシサーバーを設置する等、許可された通信以外の通信を遮断する措置を実施する。
 - (3) 当組合の情報を、ホームページを用いてインターネットへ公開、又は公開情報を変更・削除する場合は、データ保護管理者の承認を得なければならない。
 - (4) データ保護管理者は、ホームページの利用状況を監視し、不正アクセスやホームページの改ざんの有無を確認し、問題がある場合は、適切な処置（予防・是正）を講ずる。
- 3 電子メールの利用について、以下の条件の下で管理するものとする。

- (1) 電子メールの私的利用は、禁止とする。
- (2) 受信メールの自動転送については、組織外へのメール転送を原則禁止とする。
- (3) 個人情報を含む情報を電子メールで送信する場合、個人情報を含む情報に暗号化処置等を講ずるなど、情報の安全性に留意して、ファイルとして添付して送信することとする。
この場合、復号用パスワードは別に送信し、紛失または誤送に備える。
- (4) 電子メールに個人情報が含まれる場合は、必要でなくなった都度、速やかに削除することとする。

(ウイルス対策等)

第24条 セキュリティパッチは、以下または以下に準じた手順に基づいて適用するものとする。なお、インターネット等のオープンなネットワークに関し、母体企業のLANを使用する場合の管理については、母体企業の管理に準ずる。

- (1) 情報システムのサーバー及び端末には、ベンダーからの保証がない限り、原則として修正プログラムは適用しない。
 - (2) インターネットへの接続を許可された端末については、オペレーティングシステムやパッケージソフト等のパッチなどの修正プログラムがメーカーより発行された場合、既存システムの影響を考慮してデータ保護管理者の指示に基づいて実施する。
- 2** ウィルス対策として、以下または以下に準じた措置を実施するものとする。
- (1) 悪意のあるソフトウェア等から保護するため、全てのサーバー、端末にアンチウィルスソフトを導入し、パターンファイルは常に最新のものを使用する。
 - (2) 定期的にソフトウェア等のウィルスチェックを行ない、感染の有無を確認する。
 - (3) アンチウィルスソフトは、常に稼働させておくこととする。
 - (4) 業務上許された情報取得分については、ウィルスチェックを行い、問題のないことを確認後に使用する。
 - (5) 電子メールサーバーは、すべての着信メールについてウィルスチェックを行ない、感染の有無を確認する。
 - (6) ネットワークに接続するサーバーと端末は、配信型のアンチウィルスソフトの利用を可能とし、パターンファイルの更新は自動更新で行う。

- (7) ネットワークに接続していない PC は、データ保護管理者またはデータ保護担当者が常に更新情報の入手に努め、最新パターンファイルを入手し更新する。
- (8) インターネットに接続していない LAN は、最新のパターンファイルを、インターネットに接続したサーバーにより取得し、情報システムサーバーに手動で更新・配信する。
- (9) 電子媒体の使用時においては、ウィルス等の不正なソフトウェアの混入がないか事前に確認しなければならない。

(電子署名・タイムスタンプ)

第 2 5 条 法令で署名または記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う。

- (1) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施す。
- (2) 電子署名を含む文書全体にタイムスタンプを付与する。
- (3) 上記タイムスタンプを付与する時点で有効な電子証明書を用いる。

附 則

この規程は、平成 2 8 年 8 月 1 日より施行する。

改訂 平成 3 0 年 3 月 1 日