運 用 管 理 規 程

目　次

１．総則

１．１　目的

運用管理規程（以下、「本規程」という）は、福岡県医師国民健康保険組合（以下、「当組合」という）の情報セキュリティ基本方針（以下、「ポリシー」という）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）の安全かつ合理的な運用を図り、併せて法令に保存が義務付けられている書類の電子媒体による運用（電子保存システム）の適正な管理を図るために必要な事項を定めることを目的とする。

１．２　適用対象

１）情報システム

情報システムとは、当組合で運用する適用、給付、徴収に係る医療保険業務に適用する医療保険システム、健診、検診に係る保健業務に適用する保健システム及び当組合の人事・給与、資産管理、財務会計等に係る業務に適用する業務システム並びにこれらのシステムへの接続機器などをいう。

２）適用する情報

管理対象となる情報は、情報システムで取り扱う電子情報だけでなく、情報システムへ入力する前の紙媒体の情報や、従業者の履歴書等全ての個人情報を適用対象とする。なお、個人情報には、特定個人情報も含む。特定個人情報は、個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報を指す。

個人情報保護法においては、保護の対象は、「生存する」個人情報であり、死者に関する情報については、保護の対象とならない。番号法における特定個人情報についても同様の取扱いとなるが、特定個人情報のうち、個人番号については、生存者の個人番号であることが要件でないため、死者の個人番号も保護の対象となる。

法令の定める業務範囲の手続において、個人番号の記入欄のある様式を用いて得られた情報については、様式に個人番号の記入がない個人情報も特定個人情報と同様に取り扱う。

１．３　標準規格

システム管理者は、システム変更・改定時の対象とするため、当組合でフォローすべき法令及び標準規格の列挙を行い、変更状況を確認し維持する。

２．組織的な対策

２．１　管理運営体制

２．１．１　体制及び責任者

１）ポリシーの遵守及び本規程の実施に必要な事項について、情報システム管理委員会（以下、「委員会」という）の審議を経て、本規程に定める。

２）運用責任者は、情報システムを安全に運用並びに改善するに必要な資源を用意する。

３）システム管理者は、本規程に定められた組織的、人的、技術的、物理的対策を実施して、情報システムを円滑に運用できるようにする。

４）委員会は、情報システムを複数の部門で運用する必要がある場合、情報システム部門管理者（以下、「部門管理者」という）を各部門に任命して、情報システムを円滑に管理運営できるようにすることができる。

５）委員会は、情報システムを監査するため、公平かつ客観的な立場にある情報システム監査責任者（以下、「監査責任者」という）を置き、内部の者から指名する。

２．１．２　管理者及び利用者の責務

１）運用責任者の責務

ａ）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。

ｂ）加入者又は利用者からの、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。

ｃ）監査責任者に監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な処置を講じる。

２）システム管理者の責務

ａ）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。

ｂ）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。

ｃ）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。

ｄ）情報システムの利用者の登録を、人事異動等による利用者の担当業務の変更等に併せて管理し、そのアクセス権限を規定し、不正な利用を防止する。

ｅ）情報システムを正しく利用させるため、作業手順書の整備を行い利用者の教育と訓練を行う。

ｆ）情報システムの安全管理の見直し及び改善の基礎として、運用責任者に情報

システムの運用状況を報告する。

３）監査責任者の責務

ａ）監査責任者は、監査計画を立案し、監査を指揮し、監査報告書を作成し、運用責任者に報告する。

ｂ）監査責任者は、情報システムの監査を円滑に実施するため、情報システムに関する監査を担当する監査員を置くことができる。

ｃ）監査員の選定及び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。

４）情報システム部門管理者の責務

ａ）情報システム部門管理者（以下、「部門管理者」という）は、自部門のシステムの管理に責任を持つ。

ｂ）部門管理者は、自部門のマスタを管理する。

ｃ）自部門のマスタに変更・追加が生じた場合には、速やかに書面をもって関連部署部門管理者ならびにシステム管理者に提出する。

ｄ）制度改正が生じる場合、改正事項の解析とプログラム修正計画書を情報システム管理委員会に提出し、承認を得る。

ｅ）マスタの変更の際に、過去の情報に対する内容の変更が起こらない機能を備える。

５）利用者の責務

ａ）利用者は、情報システムの情報の参照や入力（以下、「アクセス」という）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。

ｂ）利用者は、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。

ｃ）利用者が、正当な認証番号及びパスワード等の管理を行わないために生じた事故や障害に対しては、その利用者が責任を負う。

ｄ）利用者は、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。

ｅ）利用者は、与えられたアクセス権限を越えた操作を行わない。

ｆ）利用者は、情報システム及び参照した情報を、目的外に利用しない。

ｇ）利用者は、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。

ｈ）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。

ｉ）利用者は、システムの異常を発見した場合、速やかにシステム管理者に連絡

し、その指示に従う。

j）利用者は、不正アクセスを発見した場合、速やかにシステム管理者に連絡し、その指示に従う。

k）利用者は、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）。なお、不特定多数の者が出入する部署においては、必要に応じて、偏光フィルム等による窃視防止処置を講ずる。

l）ウィルスに感染又はその恐れを発見した場合は、ネットワークから端末を切り離すとともに、システム管理者へ連絡し、指示を仰ぎ、その指示に従う。

２．２　具体的な対策

２．２．１　予防処置及び是正処置

1）委員会は、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で、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、これを実施させる。

2）運用責任者は、適切な情報システムの運用を維持するため、少なくとも年に１回、本規程に関わる次の事項を委員会に報告して、本規程の見直しについて審議する。

a）監査及びシステム管理者の運用状況に関する報告

b）苦情を含む外部からの意見

c）前回までの見直しの結果に対するフォローアップ

d）安全管理 GL 等の標準規格や法令等の規範の改正状況

e）社会の情勢等の変化、国民の認識の変化、技術の進歩などの諸環境の変化

f）情報システムの運用状況の変化

g）内外から寄せられた改善のための提案

3）処置等は、以下のような手順で行う。

a）発生した問題の内容を確認して、問題の原因を特定する。

b）発生した問題の処置等を立案する。

c）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。

d）実施された処置等の有効性を確認する。

e）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。

２．２．２　事故への対応

1）委員会は、事故が発生した場合は、再発防止策を含む適切な対策を速やかに講じる。事故については、発生の事実及び再発防止策等の事実を速やかに公表する。

2）運用責任者等は、事故等発生の予防に努めるため、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して、事故発生時の危険度を明確にして、リスクを回避する方法を提示するリスク分析を行う。リスクには、事業継続性を考慮して、災害及び障害も含める。

3）運用責任者等は、リスク分析の結果は、台帳に記入して維持・管理する。

4）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文書に定め、利用者に周知の上で常に利用可能な状態におく。

２．２．３　非常時の対策

1）システム管理者は、災害、サイバー攻撃などにより医療保険サービスの提供体制に支障が発生する「非常時」の場合を想定して、非常時と判断するための基準、手順、判断者等の判断する仕組み、システムの閉塞及び縮退運用等の手順（以下、「非常時運用」という）及び正常状態への復帰手順を定めた事業継続計画（以下、「ＢＣＰ」という）を策定する。

2）システム管理者は、ＢＣＰを利用者に周知の上、常に利用可能な状態におく。

3）システム管理者は、非常時はＢＣＰに則って、非常時運用を行う。

4）システム管理者は、正常状態への復帰後に、非常時運用した間の情報整合性を図る等、必要な処置を実施する。

5）非常時に異常状態を通知する必要がある機関の連絡先一覧を準備して、非常時には速やかに連絡を取る。

２．２．４　監査

1）当組合は、本規程の「医療情報システムの安全管理に関するガイドライン」への準拠状況及び情報システムの運用状況を毎年３月に監査する。

2）運用責任者は、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る。

3）監査の内容については、監査責任者が定める。

4）運用責任者は必要な場合、臨時の監査を監査責任者に命ずることができる。

２．２．５　苦情・質問受付

1）苦情・質問の受付け窓口（以下、「受付窓口」という）は、個人情報の取扱い及び情報システムの運用に関して、加入者及びシステム利用者からの苦情及び質問を受け付ける。

2）受付窓口は、直接又は間接的に苦情を受けた際に、別途定められた手順に則って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・質問を整理して、システム管理者に報告しなければならない。

4）システム管理者は、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。

２．３　守秘契約

１）当組合の業務従事者は在職中のみならず、退職後においても業務中に知った個人情報に関する守秘義務を負う。

２）法令上の守秘義務のある者以外を採用する場合は、雇用及び契約時に守秘・非開示契約を締結する。

２．４　業務委託

２．４．１　委託契約

業務を当組合外の所属者に委託する場合は、以下の処置を実施する。

１）国際規格又は日本工業規格の認定取得状況を確認し、委託に値するか確認を行う。

１）守秘事項を含む業務委託契約を結ぶ。契約の署名者は、その部門の長とする。

２）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にかつ安全に行われていることを確認する（委託先が、許可なく個人情報を含む情報を組織外に持出すことは禁止する）。

３）業務委託の契約書には、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する。

ａ）個人情報の安全管理に関する事項

ｂ）事業所内からの個人情報の持出しの禁止

ｃ）個人情報の目的外利用の禁止

ｄ）再委託に関する事項（再委託する場合は、再委託の許諾を要件とする。また、再委託する事業者にも委託先と同等の義務を課すこと）

ｅ）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

ｆ）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

ｇ）契約内容が遵守されなかった場合の処置

ｈ）事件・事故が発生した場合の報告・連絡に関する事項

ｉ）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

ｊ）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）

ｋ）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

ｌ）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）

ｍ）従業者に対する監督・教育

２．４．２　再委託

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。さらに、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する。さらに、当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。

２．４．３　作業確認

１）システム管理者は、作業の管理・監督のため、システムの改修及び保守において、以下のような確認を実施する。

ａ）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)。

ｂ）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、作業者・作業内容作業結果の確認（原則として日単位)。

ｃ）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。

ｄ）保守契約における個人情報保護の徹底。

ｅ）保守作業の安全性についてログによる確認。

２）システム管理者は、必要と認めた場合は適時監査を行う。

３．人的な対策

運用責任者及びシステム管理者は、情報セキュリティの重要性と、個人情報の適切な取り扱い、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、必要かつ適切な監督及び継続的な教育を行う。

３．１　マニュアルの整備

システム管理者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におく。

３．２　研修の内容

システム管理者は、情報システムの利用者に対し、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。また、研修時のテキスト、出席者リストを残す。

３．３　職員への周知

１）システム管理者は、情報及び情報機器の持出しについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におく。

２）システム管理者は、利用者に対し、情報及び情報機器の持出しについて研修を行う。また、研修時のテキスト、出席者リストを残す。

４．物理的な対策

４．１　立入り領域の制限

４．１．１　立入り領域の定義

１）執務室等

当組合の職員が執務する施錠できる場所また部屋を執務室等という。

２）サーバー室等

スタッフの常駐または施錠できるセキュリティが保たれた管理領域を「サーバー室等」という。

４．１．２　執務室等

部外者が執務室等に立ち入る場合は、その執務室の管理レベルに合わせた入退室記録の作成、同伴等の管理を実施する。

４．１．３　サーバー室等

１）システム管理者は、個人情報が保管されている機器（以下、「サーバー」という）及び記録媒体をサーバー室等に設置する。

４．２　情報システム

４．２．１　サーバー室等管理

１）システム管理者は、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、無停電装置などによる必要な保安処置を講じなければならない。

２）システム管理者は、サーバー室等の温度、湿度等の環境を適切に保持する。

４．２．２　端末管理

１）盗難の恐れがある端末（ノートＰＣ等）は、盗難防止用ワイヤーロックで固定するか、使用しない際は鍵のかかる保管庫に保管管理する。

２）端末の使用に際しては、画面を廊下側に向けない、窃視防止フィルムを貼るなどの、窃視防止に努める。

３）ＰＣの廃棄及びレンタル・リース切れによるＰＣの返却等に当たっては、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、その後情報を消去する。

４）情報を削除または廃棄した記録を保存する。

５）情報の消去処理を外部業者に委託することができるが、その場合は、消去証明書を受領するものとする。

４．２．３　ネットワーク管理

１）情報システムのネットワーク（以下、「ＬＡＮ」という）は、インターネット等の当組合外と情報交換ができるネットワークとは技術的な対策を適用した上で接続する。

２）ＬＡＮへ接続を行う場合、利用者はシステム管理者に申請し、承認を得る。

3）私有のＰＣを持込み、ＬＡＮに接続することは、原則禁止とする。業務上やむを得ず、接続を要する場合は、システム管理者の許可を得て行うこととする。ただし、この場合、ＰＣの使用にあたっては、業務用端末に準じた取扱いとする。
4）システム保守のため委託先等の部外者がＰＣを持込みＬＡＮへ接続する場合は、システム管理者に申請し、許可を得てから行うこととする。

４．２．４　外部機関との情報交換

1）医療保険者等、保守会社等、通信事業者、運用委託業者等の外部機関と医療保険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。
2）システム管理者は、外部機関と医療保険情報を交換する場合、リスク分析を行い、安全に運用されるように技術的及び運用的対策を講じる。
3）リスク分析及びその技術的及び運用的対策の内容を文書化して、維持・管理する。
4）定期的に監査を行って、外部機関との契約事項、技術的対策及び運用的対策が適切に実施されていることを確認する。

４．２．５　電子媒体の管理

1）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録媒体への個人情報の複写を禁止する。
2）電子媒体の廃棄は、原則粉砕処理とする。
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し、その所在を台帳に記録し、管理する。
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。
5）個人情報を記した電子媒体の廃棄にあたっては、安全かつ確実に行われることを、システム管理者が作業前後に確認し、結果を記録に残す。

４．３　情報及び情報機器の持出し及びリモートアクセス管理

４．３．１　対象となる情報及び情報機器

1）委員会は、情報及び情報機器の持出しに関してリスク分析を実施し、持出し対象となる情報及び情報機器を規定し、それ以外の情報及び情報機器の持出しを禁止する。
2）委員会は、持出し対象となる情報及び情報機器をまとめて、利用者に公開する。

４．３．２　情報の持出し管理

1）情報は、所属、氏名、連絡先、持出す情報の内容、格納する媒体、持出す目的、

期間をシステム管理者に承認を得て持出す。
2）持出す情報については、暗号化、パスワードを設定する等、容易に内容を読み取られないようにする。
3）持出した情報は、例えばファイル交換ソフト（Winny 等）がインストールされた情報機器で取り扱わない。

４．３．３　情報機器の持出し管理

1）情報機器は、所属、氏名、連絡先、持出す情報の内容、格納する媒体、持出す目的、期間をシステム管理者に承認を得て持出す。
2）持出す情報機器については、以下のような対策を施す。
ａ）起動パスワードを設定する。起動パスワードは、推定しやすいものは避け、また定期的に変更する。
ｂ）ウィルス対策ソフトをインストールしておく。
ｃ）別途定められている以外のアプリケーションはインストールしない。
3）持出した情報機器には、別途定められている以外のアプリケーションをインストールしない。
4）持出した情報機器をネットワークに接続、または他の外部媒体を接続する場合は、ウィルス対策ソフトやパーソナルファイアウォールを用いる等して、情報端末が情報漏洩、改ざん等の対象にならないような対策を施す。
5）システム管理者は、情報が格納された可搬媒体及び情報機器の所在について台帳に記録する。システム管理者は、その内容を定期的にチェックし、所在状況を把握する。

４．３．４　情報機器のリモートアクセス管理

1）外部からアクセスを許容する情報機器（以下、「リモート端末」という）については、以下の内容を別に定める。
ａ）リモート端末及びリモートアクセス要件
ｂ）リモート端末がリモートアクセス要件を保持していることを確認する手順
ｃ）情報システムに不正な侵入等の攻撃を防止する技術的対策
2）リモート端末がリモートアクセス要件を保持していることを定期的に確認する。

４．３．５　盗難、紛失時の対応

1）持出した情報及び情報機器の盗難、紛失時には、速やかにシステム管理者に届け出る。
2）届け出を受け付けたシステム管理者は、その情報及び情報機器の重要度に従って対応する。

５．技術的な対策

５．１　利用者の登録・認証

１）システム管理者は、職員等の採用時、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の処置を取る。

２）システム管理者は、情報システムの利用者等の申請を受け、情報システムへのアクセス権限を審査して、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（以下、「認証情報等」という）を利用者に交付する。

３）ＩＤ・パスワード認証

ａ）利用者ＩＤの付与は、個人単位とし共有することはない。Administrator 等のＯＳのディフォルトＩＤは使用せず、個別ＩＤとする。

ｂ）パスワードは８桁以上の英数記号を組み合わせたものとする。

ｃ）パスワードの有効期限は、原則２ヵ月以内とし、利用者が更新する。システム管理者は、２ヵ月以上パスワードを更新しない利用者に対し、警告を与え、速やかに更新させるものとする。

ｄ）利用者が、パスワードの盗難・紛失の事実を知った後、システム管理者へ速やかにパスワードの初期化依頼を提出する。システム管理者は、利用者からのパスワード紛失の申請書を受け、利用者登録の確認後、パスワードの初期化を行い、利用者へ知らせることとする。

ｅ）利用者は、パスワードの初期化の通知後は、速やかにパスワードを変更することとする。

ｆ）利用者登録時は、システム管理者の登録処理による初期値のパスワードとし、その後速やかに、利用者が個々のパスワードへ変更する手順とし、システム管理者であってもパスワードを推定できない仕組みとする。

４）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。

５．２　サーバー管理

５．２．１　サーバーの運用

１）システム管理者は、サーバーへのアクセス状況・稼働状況を定期的（月１回以上）に確認し、問題がある場合は、速やかに処置を講じる。

２）システム管理者は、個々のサーバー及び端末機のクロックを定期的（月１回以上）に確認するとともに、誤差が生じている場合は標準時間に設定し直す。

５．２．２　アクセス管理

１）システム管理者は、職務により定められた権限による情報アクセス範囲を定め、以下の内容に沿って、ハードウェア及びソフトウェアの設定を行う。

ａ）情報区分とアクセス権限に基づくアクセスできる情報の範囲を定め、アクセ

ス管理を行う。

b）利用者のアクセスにおいては、利用者の認証を行う。利用者の認証には、「第５．１節　利用者の登録・認証」にある原則に依らず、システム管理者の承認の上で、管理者権限を付与する。管理権限は、原則２名以下とする。

2）システム管理者は、情報システム、情報への使用状況を監視するため、以下の事項を含むアクセスログを取得する。

a）利用者ＩＤ

b）端末ＩＤ

c）操作の日時

d）情報へのアクセス結果（誰が、いつ、誰の情報に、どのようなアクセスをしたか)

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。

4）システム管理者は、取得したアクセスログを情報システムの重要度に合わせ定期的（月１回以上）に検証し、問題のないことを確認する。問題がある場合は、速やかに適切な処置を講じる。

5）システム管理者は、管理状況を運用責任者に報告をする。

6）アクセスログは、重要度に合わせ定めた方法・場所・期間に従い保管する。

7）アクセスログを廃棄する場合は、「第４．２．５節　電子媒体の管理」に準じて実施する。

8）アクセスログは、特定の担当者以外アクセスできない仕組みとする。また、アクセスログへのアクセス確認を別人が実施する。

５．２．３　情報のバックアップ

1）情報システムの重要度に応じて、システムファイル及び情報のバックアップを定期的に取得する。

2）バックアップの作業に当たる者は、その作業の記録を残し、部門管理者の承認を得る。

3）バックアップ媒体は、施錠できるキャビネット、耐火金庫等に保管し、その所在を台帳に記録し、管理する。

4）バックアップ媒体は１年間に１回新品に交換する。媒体に品質の劣化が予想される場合や、劣化原因と思われる障害が発生した場合は、直ちに新品に交換を行う。

5）部門管理者は、記録媒体及び機器のログを確認し、記録媒体の劣化や機器の不具合を確認する。エラー・警告のログが発見された場合は、直ちに新品の記録媒体に記録を複写する。

6）情報が毀損した時に、バックアップされた情報を用いて毀損前の状態に戻せることを確認し、リストア手順を規定する。

５．２．４　リスク対応（障害対策）

１）システム管理者は、情報システムに係る障害が発生した場合には、事態の掌握・収拾及び被害を最小限に止め、復旧作業の軽減、時間の短縮等を図るため、次の処置を講じなければならない。

２）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。

３）利用者に対し事故発生時には、速やかに報告することを周知させる。

４）業務上において情報漏洩等のリスクが予想されるものに対し、運用ルール等の見直しを実施する。

５）基幹システム以外の部門システムで障害が発生した場合は、当該部門の部門管理者に報告し、部門管理者は、担当ＳＥと連携して復旧対策を講じるとともに、障害内容をシステム管理者に報告する。

６）部門管理者は、障害内容が部門間インターフェイスの要因であると判断した場合は、関係部門に報告するとともに、システム管理者に報告し、復旧対策の指示を待つ。その際は、状況に応じて伝票での運用に切り替え、通常業務の稼働に努める。

５．３　端末管理

１）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。

２）持出した情報機器には、別途定められている以外のアプリケーションをインストールしない。

３）全端末の時刻情報はサーバー時刻と同期させる。

５．４　ネットワーク管理

５．４．１　ＬＡＮ管理

１）個人情報にアクセスするための当組合の情報システムネットワーク（以下、「ＬＡＮ」という）は、インターネット等の当組合外と情報交換ができるネットワークとは物理的に遮断する。

２）ＬＡＮを利用できる情報システムを制限・管理し、許可されていない情報機器の接続を制御する。

３）外部のネットワークとＬＡＮを接続する場合は、適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止する。

５．４．２　インターネットの利用・管理

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。情報及びソフトウェア等のダウンロード、インストール等が業務上必要なインターネットサイトは、原則ホワイトリストで指定して通信先を限定する。

２）システム管理者は、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し、許可された通信以外の通信を遮断するとともに許可された通信の状況を記録する。システム管理者は、定期的（月１回以上）に通信状況を監査する。

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、システム管理者へ申請する。システム管理者は、内容の確認後に、登録・変更を実施する。

４）システム管理者は、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）を講じる。

５．４．３　電子メールの利用・管理

１）システム管理者は、メールアカウントを申請に基づいて発行する。

２）システム管理者は、職員の退職時に当該職員のメールアカウントを速やかに削除する。

３）電子メールの私的利用は、禁止とする。

４）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。ただし、業務の遂行のために予め許された指定メールアドレスへの転送は、信頼のおける転送方法をもって実施する場合のみ可能とする。

５）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。

６）電子メールに個人情報が含まれる場合は、送信・受信した後に速やかに削除することとする。

５．５　一般的な運用事項

５．５．１　ウィルス対策

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、ＰＣの利用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ウィルスサーバーにより取得し、情報システムのウィルスサーバーに手動で更新・配信する。

５．５．２　電子媒体の管理

1）媒体使用時は、必ずウィルス等の不正なソフトウェアの混入がないか確認する。

６．その他

本規程は、平成２７年７月１日より施行する。