組合記号番号
東 － ８０５

システム等運用管理規程

セントラル警備保障健康保険組合

（令和３年４月１日から施行）

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、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　取扱うすべてのシステム（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、データの漏洩、滅失、改ざん、毀損等の防止を図るため、必要な事項を定めたものである。

（適用対象）

第２条　本規程の適用対象は、組合における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、その復元が著しく困難となる惧れのあるデータ又は情報（記録様式、媒体の種類を問わず、以下総称して「データ又は情報」という）並びに情報システムに関わるすべての関係文書（以下「システム仕様書」という）とする。

第２章（ 組織的な対策 ）

（管理責任体制）

第３条　本規程の実施にかかる管理責任体制は、次の３つの「責任者」から構成される。

(1) 管理責任者として「データ保護管理者」を置き、個人情報取扱責任者をもって充てる。

(2) データ保護管理者の指示を受け対応に当たる実務担当者として「データ保護担当者」を置き、個人情報保護管理担当者をもって充てる。

(3) 本規程の適正な実施にかかる監査実施者として「情報システム監査責任者」を置き、監事が就任するものとする。

（責任者の責務）

第４条　データ保護管理者は、以下の責務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、物理的、技術的安全対策の実施により、情報システム及びデータ又は情報の取扱い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又は情報の取扱いについての「苦情対応窓口」を設置する。

(4) 情報システム及びデータ又は情報を取扱う担当者として、取扱いが必要となる業

務ごとに「事務担当者」を指名し、必要なアクセス権を付与する。

(5) 情報システムの取扱いに関する「作業手順書」を整備する。

(6) 各種の安全対策については「年間推進計画」を立て、進捗管理を行いながら推進し、継続的改善につなげるものとする。

(7) 情報システム及びデータ又は情報について不正利用が行われた場合、又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又は情報の利用履歴とその内容について調査するものとする。

(8) 監査結果報告に基づく是正等、必要な処置を講じる。

2　データ保護担当者は、以下の責務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について、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しておく。

(3) 情報システムの正常な稼動状況を維持・管理する。

(4) 機器やソフトウェアに変更があった場合でも、データ又は情報が継続的に使用できるよう維持する。

(5) 作業手順書について、事務担当者への研修を実施し周知を図る。

(6) 各種の点検については「年間点検計画」を立て、これに基づき実施し、記録を残す。

(7) 情報システムにかかる安全管理の見直し及び改善の機会として、情報システムの運用状況及び点検の分析結果を、年１回、定期的にデータ保護管理者に報告する。

3　情報システム監査責任者（以下、「監査責任者」という）は、以下の責務に基づいてシステム監査を執り行うものとする。

(1) 情報システム及びデータ又は情報の取扱いにかかる監査を、所定のチェックリストに基づき、年１回、定期的に実施し、監査結果報告書をもってデータ保護管理者にその結果を報告する。

(2) 監査の実施に当たっては、監査の客観性及び公平性を確保するものとする。

（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に基づき担当業務に必要な情報システムを利用する。この場合、法令及び関連規程の遵守はもとより、以下の責務に基づいて実務を行うものとする。

(1) 自身のアクセス権に関わるＩＤ、パスワードの情報を管理し、これをいかなる他者にも教えず、利用させないこと。

(2) 上記の管理を適正に行わなかったために生じた事故や損害については、当該担当者がその責めを負う。

(3) 情報システムへのデータ入力の際は、確定操作を行うことにより、入力情報に対する責任を負う。
(4) 職務上知り得たデータ又は情報を、本来業務の目的外に利用してはならない。
(5) 法令上の守秘義務の有無にかかわらず、正当な理由なしにデータ又は情報を他に漏らしてはならない。
(6) 加入者等のプライバシーを尊重し、付与されたアクセス権を越えた操作を行ってはならず、業務上必要なもの以外のデータ又は情報にアクセスしてはならない。
(7) 離席する場合は、他の者に情報を盗み見られぬよう、適宜、適切な手立てをとること。
(8) システムの異常あるいは不正アクセスを発見した場合は、速やかにデータ保護管理者に報告し、その指示に従うこと。
(9) ウイルスに感染又はその惧れを発見した場合、電源は切らずに、端末をネットワークから切り離すとともに、速やかにデータ保護管理者に報告し、その指示に従うこと。
(10) インターネット、電子メールの利用の際は、私的な利用は行わず、公序良俗に反し又は他人の権利・財産を侵害する惧れを招く行為など、組合の信用、品位を傷つける内容の発信、公開をしてはならない。
(11) 特定個人情報（マイナンバー）を取扱う場合は、所定の場所にて行うこと。

（是正処置及び予防処置）

第６条 データ保護管理者は、加入者等からの苦情、緊急事態の発生、監査結果報告、所管官庁等からの指摘によりシステムの運用状況に問題があると分かった場合は、直ちに定められた手順に従って、必要な是正処置あるいは予防処置（以下、「処置」という）を実施しなければならない。

２ 前項の処置の手順は、以下のとおりである。
(1) 発生した状況を正常に復するため、一次（応急）対応を実施する。
(2) 発生した問題の内容を十分に確認の上、問題の真の原因を特定する。
(3) その上で、真の原因を取除くための処置（再発防止策）を立案する。
(4) 期限を定め、立案に基づき是正処置を実施し、実施結果を確認する。
(5) 実施した処置の有効性を確認し、評価を行う。
(6) 上記 (1)～(5)について、記録を残す。

３ 情報システムを適切に維持・運用していくため、データ保護管理者は、個人情報保護にかかる安全管理措置の全体状況、並びに次の事項について、年１回、定期的に組合会において報告を行い、必要の都度、本規程の見直しについて審議するものとする。
(1) 直近のシステム監査結果報告
(2) １年間の運用状況に関する報告（推進計画及び点検計画の実施結果、並びに事故

等の発生状況を含む）

(3) 苦情を含む、内外からの声・ご意見（所管官庁からの要改善指摘を含む）

(4) 前回までの見直し結果に対するフォローアップ（昨年度の報告からの改善結果報告）

(5) 規範となる関係法令等の改正状況

(6) 社会情勢の変化や国民の意識の変化、技術の進歩など、組合を取巻く環境の変化

（事故発生時の対応）

第７条 データ保護管理者は、事故が発生した場合、被害を最小限に抑えるべく適切な対策を速やかに講じるとともに、事故発生の事実とその対応状況、再発防止策を含む今後の見通しについて、事業主及び所管官庁に所定の報告をするとともに、速やかに公表しなければならない。

２ データ保護管理者は、事故発生の予防に努めるため、情報システムで取扱うデータ又は情報について予見されるリスクを洗い出し、事故発生時の危険度と影響範囲を明確にして、そのリスクを回避するための方策を検討・分析すること。なお、これには事業継続性を考慮して災害や重大な障害を含め、検討・分析の結果を残すこと。

（非常時の対策）

第８条 データ保護管理者は、前条とあわせ、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した非常の場合を想定するとともに、非常時と判断するための判断基準と対応の手順、緊急連絡網、システムの一時停止あるいは縮小運用等、非常時の運用手順、並びに正常状態への復旧手順までを定めた「事業継続計画」（以下、「ＢＣＰ」という）を策定するものとする。

２ データ保護管理者は、ＢＣＰについて役職員に周知させるとともに、常に利用可能な状態にしておく。

３ データ保護担当者は、「緊急連絡先一覧表」を、年１回、定期的に確認し、常に最新版に維持しておく。

４ 政府が発する緊急事態宣言等、役職員の健康・生命に関わる重大事案が発生した場合は、所管官庁の示達、事業主が設置する対策本部の指示に従って行動するものとする。

（システム監査）

第９条 本規程における法令、関連通知、「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、並びに情報システムの運用状況及びデータ又は情報の取扱いについて、年１回、定期的にシステム監査を受けなければならない。

２ データ保護管理者は、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った場合は、直ちに必要な処置を講じなければならない。

３ データ保護管理者は、必要であると判断した場合は、監査責任者に対し臨時監査を要請できる。

（苦情対応窓口）

第１０条　受付窓口者は、加入者等から苦情を受けた際、別途定められた手順に従い、速やかに対応しなければならない。

２　受付窓口者は、受付けた苦情等を整理し、データ保護管理者に報告する。

３　データ保護管理者は、これを受け、問題点の指摘等があった場合は、直ちに必要な処置を講じる。

（守秘義務）

第１１条　雇用形態のいかんにかかわらず、組合の業務に従事するすべての役職員は、在職中はもとより退職後であっても、職務上知り得た第２条に定めるすべての適用対象に対する守秘義務を負う。

２　役職員の雇用契約等の締結内容には、必ず守秘義務及び賠償責任の条項を含めるものとする。

（委託先の管理）

第１２条　組合の業務を外部へ委託する場合は、以下の処置を実施すること。

２　必ず業務の委託に先立ち、守秘義務を含む「業務委託契約」を結ぶものとする。
なお、契約の署名者は、組合の理事長及び委託先の代表者とする。

３　業務委託契約には、以下の事項を規定し、十分なセキュリティレベルを担保しなければならない。

(1) 守秘義務を含む、個人情報の安全管理に関すること
(2) 個人情報の目的外利用の禁止
(3) 委託先事業所内からの個人情報の持出し禁止
(4) 再委託の禁止
(5) 委託業務の従事者に対する管理・監督及び教育に関すること
(6) 契約内容が遵守されていなかった場合の処置
(7) 事故発生時の報告・連絡に関する事項
(8) 重大事案が発生した場合の委託先の責任・賠償に関すること
(9) 業務の区切りにおいて、継続利用が必要なデータ又は情報以外は、成果物の納入と同時に、都度、確実に消去又は廃棄する旨
(10) 確実に消去又は廃棄したことの証明に関すること
(11) 反社会的勢力の排除

４　やむを得ず再委託を行う場合は、組合の事前許諾を要件とする。その場合、再委託先において、委託先と同等の個人人情報保護に関する対策及び契約が締結されていることを必須条件とする。

５　情報システムの保守・管理において組合の役職員以外の者が作業する場合は、データ保護管理者の事前許可を要する。なお、作業終了後は、必ず作業報告書の提出を求め、実施内容を確認すること。

６　委託先（再委託先を含む）における関係法令及び契約に基づく個人情報に対する安全管理措置の遵守状況を確認するため、年１回、定期的にあるいは必要の都度、立入り監査又はこれと同等の項目を書面にて確認できることとする。

７　データ保護担当者は、契約の有効期間、主要な契約条項の維持状況について、一覧形式の「委託先管理簿」を作成して管理を行うとともに、年１回、定期的に委託継続の可否判定を含め、見直しを行うものとする。

第３章（ 人的な対策 ）

（教育の実施及び個別の対策）

第１３条　データ保護管理者は、情報セキュリティの重要性と個人情報の適切な取扱い及び安全管理についての意識面・技術面の向上を目的とし、すべての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。

２　データ保護担当者は、「年間教育計画」に基づき教育を実施し、有効性評価を含む実施記録を残すこと。

３　業務に関わる書類の持帰りは、一切禁止する。

４　書類の字句の修正に修正液等を用いてはならない。必ずだれが修正したかがわかるようにしておくこと。

５　個人情報を含む書類のコピーは原本と同等の取扱いとし、用済み後は速やかにシュレッダーすること。

６　外出・退出時には、書類の収納・施錠、機器及び端末の電源をオフすること。

７　個人情報を含め組合の業務内容一切に関し、ＳＮＳ等のソーシャルメディアへ投稿してはならない。

（作業手順書の整備）

第１４条　データ保護管理者は、作業手順書について、事務担当者が常に利用可能な状態におくものとする。

（研修の実施）

第１５条　データ保護担当者は、事務担当者に前条の内容を周知させるため、定期的に情報システムの取扱い及び個人情報保護に関する研修を行い、記録を残すこと。

第４章（ 物理的な対策 ）

（執務室の安全管理）

第１６条　部外者の立入りを制限するため、以下のように物理的な対策をとったセキュリティエリアを設け、役職員が執務する場所並びに個人情報を取扱うシステム・機器の設置場所及び記録媒体の保管場所を「執務室」とする。

レベル	部外者の扱い	エリア
レベル 1	部外者が立入り可能	応接室、共用部
レベル 2	部外者の立入り制限	執務室
レベル 3	関係者のみ立入り可	倉庫、女性休憩室

2　レベル２以上のエリアへ立入り可能な部外者は、清掃、点検、保管物引取りの関係業者のみとする。

3　部外者が執務室に立入る場合は、受付でその資格と要件を確認し「入退室記録簿」へ記入させ、立会いを実施する。

4　執務室への入室は、カードリーダー設置の常時施錠エリアである共用部に一旦入らなければ入室できない。さらに、執務室はテンキーによる常時施錠とし、その入退室状況は監視カメラにて記録・管理し、セキュリティが保たれた領域とする。

5　データ保護担当者は、入退室記録を定期的に確認し、問題があった場合は、適切な処置をとること。

6　執務室内で使用するすべての鍵・カードは、予備を含め「鍵・カード管理簿」に登録し、３ヶ月に１回、定期点検を行うとともに、役職員の異動のタイミングに合わせ、速やかに回収、貸与の手続きを行う。

7　データ保護担当者は、執務室内の「レイアウト図及び主要機器・端末の配置図」を、年１回、定期的に見直しし更新すること。

8　データ保護管理者は、執務室での火災、その他の災害に備え、消火器、消火設備、耐震面の配慮を行うとともに、執務室内の室温を適切に保つよう配慮すること。

9　消火器、消火設備については、役職員の全員が使用できるようにしておくこと。

（機器及び端末の安全管理）

第１７条　執務室内の情報システムに関わるすべての機器及びＰＣ等の端末は、以下の安全対策を行う。

(1) 盗難防止用ワイヤーロックによる固定。

(2) 外部から個人所有の記録媒体、ノートＰＣ等の情報端末を持込んではならない。

(3) 各人が使用しているＰＣには、標準装備以外の壁紙、スクリーンセーバー、及びデータ保護管理者が事前に許可していないソフトウェア、アプリケーションを無断でインストールしてはならない。

(4) 携帯電話、スマートフォンはマナーモードにし、執務室内では使用しないこと。

(5) 離席時には、スクリーンセーバーや自動ログオフの設定にて対応する。

2　データ保護担当者は、執務室内のすべてのＰＣについて、一覧形式の「ＰＣ管理簿」（ソフトウェアを含む）を作成し、半年に１回、定期的に見直しし更新すること。

3　機器及び端末の廃棄並びにレンタル・リース切れによる返却に当たっては、既存情報

の完全消去を行い、消去あるいは廃棄の処理証明を残す。

４　機器及び端末は床面に直置きせず、転倒の防止策をとること。

５　配線は足に引っかかったりすることがないよう、適切に処理すること

６　当組合の現状の業務処理及び運用状況にかんがみ、テレワークの導入は差し控えることとする。

（ネットワークの管理）

第１８条　情報システムのネットワークは、他のネットワークとは互いに物理的に完全分離し、一切の接続を認めない。ただし、組合の業務処理に欠かせない、法令に定めるところの法人格の外部機関との接続は、この限りではない。

２　ネットワークの完全分離を確保するため、２つの異なるネットワークの端末から１つのプリンターに出力すること、あるいはＦＡＸ機能を持つコピー機に出力することは、行ってはならない。

３　電子メールのアカウントについては、所定の手続きを経てシステム提供元から交付を受け、あるいは抹消処理する。なお、定められた形式以外のアカウントを用いてはならない。

４　個人情報を含むデータの送信に伴う暗号化処理については、システム提供元の仕様・取決めに従う。

５　インターネット、電子メールにおいて、関係先以外からのメール及び添付ファイルは不用意に開くことなく削除し、ごみ箱からも速やかに、都度、抹消すること。

６　データ保護担当者は、ホームページの運用状況について、定期的に異常の有無を確認すること。

（外部との情報交換）

第１９条　データ保護管理者は、医療保険者、保守会社、通信事業者、運用委託業者等、外部機関と情報交換する場合、相手機関との間での責任分界点、責任の所在を契約書上で明確にしておくこと。

２　データ保護管理者は、外部機関との情報交換においてリスクが生じていないか、年１回、定期的にリスク分析を行い安全に運用されているかを確認すること。

（記録媒体の管理）

第２０条　執務室内で使用するすべての記録媒体は、「記録媒体管理簿」に登録したものを用い、月１回、定期点検を行う。

２　組合から業務上の結果報告として関係先へ記録媒体を提出する場合は、所定の記録を残すこと。また、関係先から業務上の処理結果として記録媒体を受領する場合も、同様とする。

３　記録媒体はすべて、施錠可能なキャビネット内に保管すること。

４　記録媒体を使用するときは、必ず使用前にウイルスチェックを行うものとする。

５　記録媒体に記録されたデータの保管期間については、法令の定めによるものとする。

6　記録媒体の特性を考慮し、記録媒体によるデータのバックアップは行わないものとする。
7　記録媒体は物理的破壊によって廃棄し、記録を残すこと。
8　執務室内で利用できるＵＳＢの本数は３本のみとし、予備は置かず、データ保護管理者のもとで一元管理する。
9　業務上、ＵＳＢにてデータを移行する場合は、必ずウイルスチェックののち行うこととし、作業後はＵＳＢ内のデータを、都度、消去すること。
10　文書・記録の紙媒体については、法令の定めに基づき保管期間を厳守し、一定期間を過ぎたものは外部の倉庫にて保管・管理し、廃棄期限をむかえたものは溶解処理の上、処理証明を残す。

（システム仕様書）

第２１条　データ保護管理者は、利用している情報システムに関して、技術的概要及び双方の役割分担等を定めた仕様書一式の所在を明確にしておくとともに、所定の場所に最新版を保管しておかなければならない。なお、仕様書の外部への持出し、複製は禁止する。
2　情報システムで保有するデータの保管期間については、システム提供元の仕様・取決めに基づく。

第５章（ 技術的な対策 ）

(アクセスの管理)

第２２条　利用者のアクセス権は、システムごとにシステム提供元が定める。

	システム名	閉域網接続	付与	システム提供元
1	KOSMO-net21	ｴﾝﾄﾘｰ VPN	ID 付与・ﾊﾟｽﾜｰﾄﾞ設定	大和総研 BI
2	統合専用端末	ｴﾝﾄﾘｰ VPN	ID 付与・ﾊﾟｽﾜｰﾄﾞ設定	大和総研 BI
3	ﾈｯﾄﾊﾞﾝｷﾝｸﾞ	ｲﾝﾀｰﾈｯﾄ VPN	ID 付与・ﾊﾟｽﾜｰﾄﾞ設定	みずほ
4	ﾎﾟｰﾀﾙ	IP-VPN	ID 付与・ﾊﾟｽﾜｰﾄﾞ設定	CSP（事業主）
5	独自端末	ｲﾝﾀｰﾈｯﾄ VPN	ﾊﾟｽﾜｰﾄﾞ設定	組合にて単体設置

2　データ保護管理者は、役職員の異動のタイミングに合わせ、速やかに利用者ＩＤの登録・付与、変更、抹消の手続きを行うものとする。
3　データ保護管理者は、利用者からの申請に基づき、その資格と要件を確認の上、担当業務に必要な範囲で各システムの提供元へアクセス権発行の申請を行い、利用者にその結果を通知する。
4　付与されたＩＤ及び自ら設定したパスワードについては、各人が責任をもって管理し

なければならない。なお、パスワードは英数字を組合せた７ケタ以上にすること。

５　パスワードは、けっして他人に教えてはならず、ＰＣ周辺や机の上に表示・貼付しないこと。また、操作画面上の囲み枠の中の「パスワードを保存する」の □ にチェックを入れない（有効にしない）こと。

６　パスワードの更新については、各システムでの設定に従うものとする。

７　データ保護管理者は、利用者のアクセス状況、システムの稼動状況を、月２回、定期的に確認し、問題がある場合は適切な処置をとること。なお、システムへのアクセス状況、データの処理状況の適否の判断については、システム提供元のアクセスログを利用して行う。

８　データ保護管理者は、年１回、定期的にアクセスログの点検結果の分析を行い、必要に応じ適切な処置をとること。

９　データ保護管理者は、年１回、定期的にＩＤの棚卸しを実施し、理事長に報告すること。

10　仕様書に基づきシステム提供元にてバックアップを行っているデータ以外で、個人情報を含まないデータについて、業務上バックアップが必要なものは、専用のハードディスクに手動にて行う。

（ウイルス対策）

第２３条　ウイルス対策については、システム利用の仕様に基づき、システム提供元にて対策を実施する。

２　それ以外のネット接続端末については、以下を遵守すること。

(1) 悪意のあるソフトウェア等から保護するため、端末にアンチウイルスソフトを導入し、パターンファイルは常に最新版に自動更新されるよう設定する。なお、ＯＳについても、同様とする。なお、統合専用端末については、手動にてインストールする。

(2) 年２回、定期的にソフトウェアのウイルスチェックを行い、感染の有無を確認する。

３　記録媒体を含め、業務上のデータの取得分については、都度、ウイ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。

４　電子メールの着信メールについては、提供元にてウイルスチェックを行う。

（電子署名）

第２４条　法令で署名又は記名・押印が義務付けられた文書において記名・押印を電子署名に代える場合は、以下の条件を満たすこと。

(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し、付与する時点で有効な電子証明書を用いる。

2　データ保護管理者は、電子的に受領した文書に電子署名がある場合の署名検証手順を定める。具体的には、電子署名が有効である間に電子署名の検証に必要となる関連する電子証明書や失効情報等の情報を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策を実施する。

附 則　この規程は、令和３年４月１日から施行する。