情報システム運用管理規程

（目的）

第１条　この規程は、ユウガグループ（以下「当グループ」という。）における、情報システムの安全かつ合理的な運用を図り、併せて、法令に基づき保存が義務づけられている情報（以下「保存義務のある情報」という。）の電子媒体による運用の適正な管理を図るために、必要な事項を定めるものとする。

（定義）

第２条　情報システムとは、個人情報に関わる情報を、電子媒体への保存や検索をするためのソフトウェアおよびそれらに接続する機器のことをいう。

２　この規定において掲げる用語の定義は、以下の通りとする。

(1)　被保護者

当グループのサービスを受けている患者や利用者と、個人情報保護の観点から守られるべき当グループの職員をいう。

(2)　個人情報保護管理責任者

各部署で個人情報保護について、統括的責任と権限を有する者をいう。詳細は、各部署の管理規程に準ずる。

(3)　個人情報保護管理担当者

個人情報保護管理責任者から自己に代わり必要な個人情報保護を遂行するために選任された者をいい、各部署から１名以上選任される。詳細は、各部署の管理規程に準ずる。

(4)　システム管理責任者

情報システムの運用管理について、統括的責任を有する者をいう。

３　情報システムは、次の各号に掲げる基本原則に則り運用する。

(1)　保存義務のある情報の電子媒体による保存については、情報の真正性、見読性、保存性を確保する。

(2)　情報システムの利用にあたっては、守秘義務を遵守し、被保護者個人の情報を保護する。

(3)　情報システムのセキュリティについては、機密性、完全性、可用性を確保する。

（情報システムの管理体制）

第３条　情報システムの管理体制は、以下のとおりとする。

(1)　システム管理責任者は情報企画室が充たる。

(2)　各部署に情報システムの運用管理と監視の担当者（以下「システム運用監視担当者」という。）を置き、各部署の長が勤務場所や職種等を考慮し、１名以上選任する。

システム運用監視担当者は、システム管理責任者の指示に従い、情報システムの運用管理と監視を行わなければならない。

(3)　個人情報を保管するサーバー機は、施錠できる場所に設置し、管理する担当者が不在になる場合は、必ず施錠しなければならない。

（システム管理責任者）

第４条　システム管理責任者は、次の各号に掲げる任務を行う。

(1)　情報システムの運用管理を統括し、本規程を当グループの職員に周知するとともに、規程に基づき作成された文書を管理・保管する。

(2)　必要に応じて利用マニュアル及び仕様書やFAQ等を整備する。

(3)　コンピュータウイルスの進入および外部からの不正アクセスに対して必要な対策を講じる。

(4)　情報システム利用者に対して、情報システムの安全な運用の履行状況や所属、データを保有する個人情報保護管理責任者の依頼に応じて、情報へのアクセス制限を適宜実施する。

(5)　コンピュータに格納された情報は、機械的な故障等により情報が滅失したり見読不能となることのないよう、バックアップの措置を講じる。また、バックアップファイル及び記録媒体の取り扱いや保管は、厳重に行うものとする。

(6)　職員に対して、情報システムの安全な運用に必要な知識及び技能の研修や情報発信を行う。

(7)　個人情報に関するシステム上のトラブルが発生した場合、管理記録を作成し、３年間保管する。

管理記録には、以下の事項を入れること。

①発生日時
②発見者
③トラブルの内容
④対応完了日時
⑤対応者
⑥対応内容

（システム運用監視担当者）

第５条　システム運用監視担当者は、次の各号に掲げる任務を行う。

(1)　情報システムが安全で合理的に運用されているかを監視し、運用上に問題が生じた場合は、速やかにシステム管理責任者に報告する。

(2)　最低月１回、担当部署のパソコンについて、コンピュータウイルスのチェックおよび、ＯＳが最新に保たれているか否かと、システム管理責任者が許可していないソフトをインストールしていないか、個人情報保護管理責任者が許可していないショートカットやファイルがデスクトップに貼付けていないか（ごみ箱にも入っていないか）を監督する。

(3)　利用マニュアル及びFAQ等を整備し、必要に応じて速やかに利用できるよう担当部署に周知する。

(4)　職員に対して、知り得た情報システムの安全な運用に必要な知識及び技能につい

て、担当部署に周知し、各部署への情報の共有化も積極的に推進する。

(5) 情報システムの有効活用を図り、機器の配置及び利用についての要望をシステム管理責任者へ報告する。
また、情報システム（接続機器を含む）に問題が生じた場合は、直ちにシステム管理責任者に報告する。

（個人情報保護管理担当者）

第６条 個人情報保護管理担当者は、次の各号に掲げる任務を行う。

(1) 情報システム利用者が異動等により利用状況に変更があった場合は、システム管理責任者へ速やかに報告しなければならない。

(2) 個人情報推進委員会で許可していないソフトを使って、個人情報を取り扱っていることを知った場合は、個人情報推進委員会で承認を得るまで、直ちに使用を中止させなければならない。

(3) モバイル端末で個人情報を取り扱う場合は、個人情報が保護できるよう、使用のガイドラインを取り決め、文書化し、利用者への周知徹底と、正しく運用されているかの監査の実施を監督しなければならない。

(4) 自部署の情報システム利用者が退職または休職する場合は、退職（休職）日までに職員マスタへ退職（休職）日を登録し、情報へのアクセス制限を実施しなければならない。

（庶務）

第７条 庶務（セントポーリアの庶務代理担当者を含む）は、新規採用者に対して、入社時に個人情報保護に関する誓約書（別紙様式１）に署名押印をさせ、退職後も保管しなければならない。

（情報システム管理運営委員会）

第８条 情報システムの安全かつ合理的な運用を図るため、情報システム管理運営委員会を置く。

２ 情報システム管理運営委員会は、原則月１回開催し、システム管理責任者とシステム運用監視担当者が参加するものとする。

３ 情報システム管理運営委員会に関する事項は別に定める。

（利用資格者の定義と責務）

第９条 情報システムを利用できる者は、次の各号に掲げる利用資格者とする。

(1) 当グループの職員

２ 個人情報保護管理責任者は、利用資格者の職種等により、利用制限を課すことができる。

３ 利用資格者は次の責務を負う。

(1) 情報システムの利用にあたっては、利用者認証に関する情報（以下「ＩＤ及びパスワード」という。）を取得するために、個人情報保護に関する誓約書

（別紙様式１）に署名押印すること。

(2)　利用者認証に関しては、次の事項を遵守しなければならない。

① 利用者は、情報システムを使用する際に必ず自己の認証を行う。

② 利用者は、ＩＤ及びパスワードを他人に教えてはならない。また、他人が容易に知ることができる方法でＩＤ及びパスワードを管理してはならない。もし、他人に知られたり、誤った管理により知られる可能性があると思われた場合は、速やかにシステム管理責任者に届け出て、ＩＤ及びパスワードの更新を行わなければならない。

③ 利用者が正当なＩＤ及びパスワード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。

(3)　情報システムから電子媒体等で持ち出す事を目的に個人を特定できる情報を取り出す場合、被保護者の個人情報を保護するため、事前に個人情報保護管理責任者または理事長の許可を得なければならない。また、電子媒体等で持ち出し、使用目的を終えたものについては、その破棄方法等について許可を出した者に報告しなければならない。

ただし、現場で、業務の必要に応じて、被保護者及び被保護者家族、あるいは、本人の承諾を得て第三者に提供する情報はこの限りではない。

(4)　研究・教育・研修を目的に、担当部署以外の情報を取り出す場合には、データを保有する部署の個人情報保護管理責任者または理事長の許可を必要とする。

(5)　電子媒体や電子メール等の添付ファイルによる送信で、個人情報に関わる情報の持ち出しや提供、受け渡しをする場合は、メディア全体をパスワードで保護（ロック）するか、ファイルに暗号化を施さなければならない。

また、 モバイル端末で個人情報を取り扱う場合は、端末をロックする設定をして使用しなければならばい。

(6)　個人情報をプリントアウトした場合や電子媒体（パソコンのハードディスクを含む）に保存した場合には、紛失、毀損、盗難等の防止に十分留意し、使用目的を終えたものについては、裁断や破壊をするなど、個人情報が復元できない状態にして廃棄しなければならない。

また、モバイル端末で個人情報を取り扱っている場合も、紛失、毀損、盗難等の防止に十分留意し、使用目的を終えた情報については、速やかにデータを削除しなければならない。

(7)　個人のパソコンや電子媒体を、個人情報を記録しているネットワークやパソコンへ接続する場合は、個人情報保護管理責任者または担当者の事前承認を必要とする。

また、接続する際は、接続先がウイルスに感染していない事を確認しなければならない。ウイルス感染の確認は、外部から電子媒体を持ち込み使用する場合や不審なメールからの添付ファイルを開く場合、インターネットからファイルをダウンロードした場合も同様に実施すること。

(8)　自己では解決できない情報システムの動作の異常及び安全性の問題点、ある

いはウイルス感染等を発見したときは、直ちにシステム管理責任者またはシステム運用監視担当者に報告しなければならない。

(9) 職員以外の者が立ち入る場所またはその近くにおいて、モニターに表示された画面を通じて被保護者の個人情報が本人以外の外部の者の目に触れないように留意しなくてはならない。特に、離席する際、周りに職員がいない場合はコンピュータのロックをしなければならない。
また、デスクトップ画面に、個人情報の入ったファイルやフォルダ、またはそのショートカットを置いたりせず、外部の者に簡単にアクセスされないようにすること。

(10) システム管理責任者が許可したソフト以外の使用およびインストールを行ってはならない。新たなソフトの使用が必要な場合は、事前にシステム管理責任者に申請し、許可を受けなければならない。
なお、今まで個人情報を取り扱ったことのないソフトを使って、新たに個人情報の取り扱いを開始する場合には、事前に個人情報推進委員会の承認を得なければならない。

(11) 当グループ職員は、自部署の新入職員向けのオリエンテーションで、個人情報保護管理担当者から情報システムの適正な運用についての説明を受けなければならない。

(12) システム管理責任者やシステム運用監視担当者からの運用及び安全性に関する通知を理解し、遵守しなければならない。

(情報の開示)

第 10 条　情報の開示に関しては、各部署の管理規程に準ずる。

(情報システムの監査)

第 11 条　情報システムの運用が安全かつ合理的に行われているかの監査は、各部署の監査時に実施する。

(罰則)

第 12 条　監査の結果問題があった場合及び本規程に違反があった場合の罰則については、各部署の管理規程に準ずる。

附　則　　この規程は、平成１７年４月１日から施行する。

附則（平成２８年９月２８日変更）

この規程は、平成２８年９月２８日から施行する。

附則（平成２９年４月１日変更）

この規程は、平成２９年４月１日から施行する。

附則（令和元年１２月２５日変更）

この規程は、令和２年１月１日から施行する。