公立八鹿病院組合情報セキュリティ基本方針

令和８年４月１日組合規程第２号

（目的）

第１条　公立八鹿病院組合情報セキュリティ基本方針（以下「基本方針」という。）は、公立八鹿病院組合（以下「当組合」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、情報セキュリティ対策について基本的な事項を定め、情報資産の適正管理を行うことを目的とする。

（定義）

第２条　本基本方針において、次に掲げる用語の意義は、当該各号の定めるところによる。

（１）　ネットワーク　コンピュータ等の情報機器を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（２）　情報システム　コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組をいう。

（３）　機密性　認められた者のみが、情報資産にアクセスできる状態を確保すること。

（４）　完全性　情報資産が破壊、改ざん又は消去されていない状態を確保すること。

（５）　可用性　情報資産にアクセスすることを認められた者が、必要なときに中断されることなく、情報資産にアクセスできる状態を確保すること。

（６）　情報セキュリティ　情報資産の機密性、完全性及び可用性を維持することをいう。

（７）　情報セキュリティポリシー　本基本方針及び情報セキュリティ対策基準をいう。

（８）　ＨＩＳ系（医療情報システム系）　電子カルテや部門システム等の患者情報を取扱う情報システム及びデータをいう。

（９）　作業系　インターネットに接続された情報システム及びその情報システムで取扱うデータをいう。

(10)　職員等　次に掲げる者をいう。

ア　地方公務員法（昭和25年法律第261号）第３条第２項に規定する一般職に属する当組合の職員

イ　地方公務員法第３条第３項に規定する特別職に属する職員（当組合が任用する職員に限る。）

ウ　その他当組合が任用する職員

エ　労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和60年法律第88号）に基づき当組合の業務に従事している者

(11)　情報　職員等が職務上作成し、又は取得した紙等の有体物及び電磁的に記録されたものをいう。

(12)　個人情報　個人に関する情報で、特定の個人を識別することができ、又は他の情報と照合することにより、特定の個人を識別することができる情報をいう。ただし、次に掲げる情報を除く。

ア　法人その他の団体の事業情報に含まれるその役員に関する情報

イ　事業を営む個人に関する情報に含まれる当該事業に関する情報

(13)　電磁的記録媒体　情報が電子的に記録されている磁気テープ、磁気ディスク、フロッピーディスク、光ディスク、メモリカード、ＵＳＢメモリ等の媒体をいう。

(14)　外部委託事業者　当組合の業務委託を受けた全ての事業者等をいう。

(対象とする脅威)

第３条　情報資産に対する脅威として、次の各号に掲げる脅威を想定し、情報セキュリティ対策を実施する。

（１）　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）　情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３）　地震、落雷、火災等の災害によるサービス及び業務の停止等

（４）　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５）　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

(行政機関の適用範囲)

第４条　本基本方針の適用範囲は、当組合の内部部局並びに公立八鹿病院組合議会及び議会事務局並びに公立八鹿病院組合監査委員及び監査委員事務局とする。

(情報資産の適用範囲)

第５条　本基本方針が対象とする情報資産は、次の各号に掲げるとおりとする。

（１）　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

（２）　前号で取り扱う情報（これらを印刷した文書を含む。）

（３）　システム関連文書（情報システムの仕様書、ネットワーク図等）

(職員等の遵守義務)

第６条　職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあたって情報セキュリティポリシーを遵守し、情報資産を適切に管理しなければならない。

(情報セキュリティ対策)

第７条　第３条に規定する脅威から情報資産を保護するために、次の各号に掲げる情報セキュリティ対策を講じる。

（１）　組織体制　当組合の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（２）　情報資産の分類と管理　当組合の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３）　情報システム全体の強靭性の向上　情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次に掲げる対策を講じる。

ア　ＨＩＳ系においては、他の領域から論理的に分離し、患者情報の不正な持出し及び漏えいを防止するための対策を講じる。

イ　作業系においては、必要に応じて不正通信の監視機能の強化等の情報セキュリティ対策を実施する。

（４）　物理的セキュリティ　サーバ室、通信回線及びパソコン等のハードウェアの管理について、物理的な対策を講じる。

（５）　人的セキュリティ　情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（6） 技術的セキュリティ　コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（7） 運用　情報セキュリティポリシーの実効性を確保するため、情報システム等の稼動状況の監視や情報セキュリティポリシーの遵守状況の確認のため、運用面における必要な対策を講ずる。また、緊急事態が発生した場合に迅速な対応を可能とするため、危機管理対策を講ずる。

（8） 業務委託と外部サービスの利用　業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

（9） 評価・見直し　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第８条　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

（情報セキュリティ対策の評価及び見直し）

第９条　情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

（情報セキュリティ対策基準の策定）

第10条　本基本方針に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

（情報セキュリティ実施手順の策定）

第11条　情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより当組合の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

附　則

この規程は、令和８年４月１日から施行する。