医療情報システム運用管理規程

○○病院

第１章　総則

（目的）

第１条　本規程は、医療情報システムの適切な安全管理を確保し、サイバー攻撃等の情報

セキュリティインシデントによる患者医療情報の流出や不正利用を防止すること、

また医療の継続性を維持することを目的とする。

（適用範囲）

第２条　本規程は、○○病院（以下、「当院」という。）の職員および医療情報システム・

サービス事業者（以下「事業者」という。）に適用される。

第２章　体制構築

(医療情報システム安全管理責任者の設置)

第３条　当院は、事務責任者を「医療情報システム安全管理責任者」とする。

２．医療情報システム安全管理責任者の職務は、情報セキュリティ方針の策定およ

び教育・訓練を含む情報セキュリティ対策の推進とする。

第３章　医療情報システムの管理・運用

(サーバ、端末ＰＣ、ネットワーク機器の台帳管理)

第４条　当院は、○○課を「医療情報システムの管理部門（以下、「管理部門」とい

う。）」とする。

２．管理部門は、医療情報システムで用いるサーバ、端末ＰＣ、ネットワーク機器

について、機器台帳を作成し管理を行う。

３．機器台帳には、医療情報システム等の設置場所、利用者、ＩＤ・パスワード、

利用権限等を記載し、医療情報システム等の管理を適正に行う。

(リモートメンテナンス（保守）を利用する機器の確認)

第５条　管理部門は、リモートメンテナンス（保守）を利用している機器について事業者

に確認し、台帳に記載のうえ、医療情報システム安全管理責任者に報告する。

(医療情報セキュリティ開示書（ＭＤＳ／ＳＤＳ）の提出)

第６条　管理部門は、医療情報システムのセキュリティに関するリスク評価およびリスク

管理のため、事業者へ当該医療情報システムに関する医療情報セキュリティ開示書

（ＭＤＳ／ＳＤＳ）の提出を求める。

(利用者のアクセス利用権限設定)

第７条　管理部門は、利用者の職種・担当業務別の情報区分ごとにアクセス利用権限を設

定する。

２．情報の種別、重要性、利用形態に応じて情報区分管理を行い、利用者や利用者

グループごとに利用権限を規定する。

３．管理者権限を与えるアカウントは最低限のユーザーとする。

(不要なアカウントの削除または無効化)

第８条　管理部門は、機器台帳等の情報に基づき、退職者や長期間使用されていないアカ

ウント等、不要なアカウントが含まれていないかを確認する。

２．不要なＩＤは不正アクセスに利用されるリスクがあるため、適宜削除または無

効化する等の対応を行う。

(セキュリティパッチの適用)

第９条　管理部門は、不正ソフトウェア対策のため、パターンファイルの更新を含め、セ

キュリティ・ホール（脆弱性）が報告されているソフトウェアへのセキュリティパ

ッチ（最新ファームウェアや更新プログラム）を適用し、常に最新のものを保つこ

ととする。

(パスワード管理)

第１０条　パスワードは、英数字、記号が混在した８文字以上とし、定期的に変更する。

２．二要素認証が実装されている医療情報システムに関しては、二要素認証を採用

し、パスワード管理の安全性を向上させる。

３．パスワードの使い回しは禁止とし、複数の機器や外部サービス等で同一のパス

ワードを設定しない。

４．医療情報システム等の端末ＰＣにおいて、ユーザーＩＤやパスワードをモニタ

ー等に付箋で貼る等の行為は禁止とする。

(ＵＳＢストレージ等の外部記録媒体・情報機器の接続制限)

第１１条　ＵＳＢストレージ等の外部記録媒体や情報機器に対する接続については、バッ

クアップを目的とする以外は、原則、使用しない。ただし、業務上やむを得ない場

合で、医療情報システム安全管理責任者の承認を得たものについては、その限りで

はない。

２．やむを得ず、ＵＳＢストレージ等の外部記録媒体を使用する際は、利用前に記

録媒体へのウイルススキャンを実施する。

３．ＵＳＢストレージ等の外部記録媒体・情報機器記録媒体や情報機器等の使用に

ついては、医療機関内のみとし、外部への持ち出しは禁止とする。

(アクセスログの管理)

第１２条　管理部門は、医療情報システムが適切に運用されているかを確認するため、医

療情報システム内に記録されている利用者のアクセスログを、必要に応じ、確認す

る。

２．アクセスログは、利用者、ログイン時刻、操作内容等が特定できるように記録

する。

(不要なソフトウェア及びサービスの停止)

第１３条　管理部門は、必要に応じ、バックグラウンドで動作している不要なソフトウェ

アおよびサービスが作動していないか、プログラム一覧やタスクマネージャー等で

確認する。

２．不要なものがある場合は、所属長および医療情報システム安全管理責任者に相

談の上、停止するなどの対策を講じる。

(接続元制限の実施)

第１４条　管理部門は、ネットワーク機器に対し、不正アクセス対策として接続元制限を

実施する。

　　　２．接続元制限は、ＵＴＭ（統合脅威管理）等の設置により、セキュアなネットワ

ークを構築することにより実施する。

第４章　インシデント発生に備えた対応

(連絡体制図の整備)

第１５条　医療情報システム安全管理責任者は、情報セキュリティインシデント発生に備

え、事業者、厚生労働省、警察等の外部関係機関との緊急連絡先を明示した連絡体

制図を作成し、院内の関係部署へ周知する。

(データ・システムのバックアップと復旧手順の確認)

第１６条　管理部門は、インシデント発生時に診療を継続するために必要な情報を検討

し、情報システムやデータ等のバックアップを適切に確保し、その復旧手順を整

備・確認する。

(事業継続計画（ＢＣＰ）の策定)

第１７条　医療情報システム安全管理責任者は、院内の関係部署と連携し、サイバー攻撃

を想定した事業継続計画（ＢＣＰ）を策定する。

２．事業継続計画（ＢＣＰ）は、医療情報システムの故障およびサイバー攻撃等で

障害が発生した場合でも、病院機能を可能な限り維持しまたは早期に復旧し、病

院内の全職員が協力して、可能な限り医療サービスの提供を維持することを基本

方針とする。

第５章　雑則

（幹部会での協議）

第１８条　この規程に定めるもののほか必要な事項は、幹部会にて協議し、別に定めるも

のとする。

［附則］

この規程は、令和　　年　　月　　日から施行する。