

公立森町病院 サイバーセキュリティを確保する
ための基本方針

令和7年12月22日

公立森町病院

版	日付	内容	改定 履歴
1.0 版	令和 7 年 12 月 22 日	初版	

目次

1	目的.....	4
2	定義.....	4
3	対象とする脅威.....	5
4	適用範囲.....	5
5	職員の遵守義務.....	5
6	情報セキュリティ対策.....	6
7	情報セキュリティ監査及び自己点検の実施.....	7
8	基本方針の見直し.....	7
9	情報セキュリティ対策基準の策定.....	7
10	情報セキュリティ実施手順の策定.....	7

サイバーセキュリティを確保するための基本方針

1 目的

本基本方針は、公立森町病院、森町家庭医療クリニック及び森町訪問看護ステーション（以下「病院等」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に、病院等が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2 定義

(1) ネットワーク

ネットワークコンピュータ等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みのことをいう。

(3) 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。

(4) 情報セキュリティ基本方針

本基本方針をいう。

(5) 機密性（confidentiality）

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(6) 完全性（integrity）

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(7) 可用性（availability）

情報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、情報にアクセスできる状態を確保することをいう。

(8) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（オンライン資格確認、電子処方箋などに関する事務）に関わる情報システム及びデータをいう。

(9) 医療情報システム系

電子カルテシステム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。

(10) インターネット接続系

医療情報システム系を除く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。

(11) 通信経路の分割

医療情報システム系とインターネット接続系の両環境間の通信環境を論理的に分離したうえで、安全が確保された通信だけを許可できるようにすることをいう。

(12) 職員

病院等の情報資源に接する職員、会計年度任用職員、非常勤職員及び業務委託先職員、派遣職員のうち病院等に勤務するものをいう。

3 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、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

4 適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は、病院等とする。なお、森町役場の提供するシステム及び情報の範囲内においては森町情報セキュリティポリシーが適用されるものとする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ① ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
- ② ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- ③ 情報システムの仕様書及びネットワーク図等のシステム関連文書

5 職員の遵守義務

職員は、情報セキュリティの重要性について共通の認識を持つこと。情報セキュリティポリシーに定める情報及びシステム等を使用する場合は、情報セキュリティポリシー

の対策基準及び情報セキュリティ実施手順を遵守しなければならない。

6 情報セキュリティ対策

上記3の対象とする脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

病院等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

病院等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じん性の向上

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、次の三段階の対策を講じる。

- ① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持出し不可設定や端末への多要素認証の導入等により、患者情報の流出を防ぐ。
- ② 医療情報システム系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、患者情報の流出を防ぐ。
- ③ インターネット接続系においては、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対策

サーバ、情報システム室、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) 人的セキュリティ対策

情報セキュリティに関し、職員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対策

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

情報システムの監視、本基本方針の遵守状況の確認、業務委託を行う際のセキュリティ確保等、本基本方針の運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時の対応計画等を策定するよう努める。

(8) 業務委託と外部サービス（クラウドサービス）等の利用

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（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(9) 本基本方針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。本基本方針の見直しが必要な場合は、適宜見直しを行う。

7 情報セキュリティ監査及び自己点検の実施

本基本方針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。

8 本基本方針の見直し

情報セキュリティ監査及び自己点検の結果、本基本方針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、リスクを検討した上で、本基本方針を見直す。

9 情報セキュリティ対策基準の策定

上記6、7及び8に規定する対策等を実施するための、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については、公立森町病院情報セキュリティポリシーの情報セキュリティ対策基準を準用する。

10 情報セキュリティ実施手順の策定

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については、公立森町病院情報セキュリティポリシーの実施手順書を準用する。

なお、情報セキュリティ実施手順は、公にすることにより病院等の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。