大館市立総合病院
情報セキュリティ基本方針

令和８年４月１日　策定
令和８年４月１日　施行

１．目的

大館市立総合病院情報セキュリティ基本方針（以下「基本方針」という。）は、大館市立総合病院（以下「当院」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、当院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

⑴　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。

⑵　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をいう。

⑶　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。

⑷　情報セキュリティポリシー

本基本方針及び対策基準をいう。

⑸　機密性

情報資産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。

⑹　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をいう。

⑺　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をいう。

⑻　医療情報システム系

診療に関わる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。

⑼　ＬＧＷＡＮ接続系

大館市が整備するＬＧＷＡＮ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。

⑽　情報系

外部ネットワークに直接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。

⑾　会計系

企業会計に関わる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。

⑿　専用ネットワーク系

⑻～⑾に含まれない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。

⒀　通信経路の分割

情報系と医療情報システム系、会計系のそれぞれの環境間の通信環境を分離した上で、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。

⒁　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着がないなどの安全が確保された通信をいう。

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。

⑴　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

⑵　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、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

⑶　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

⑷　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

⑸　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

基本方針の適用範囲は、以下のとおりとする。

⑴　対象情報システムの範囲

当院が保有するすべての情報システムを適用範囲とする。

ただし、事務局職員が利用するＬＧＷＡＮ系端末に保存された情報資産は、大館市情報セキュリティ基本方針の適用対象となるため、本基本方針の対象外とする。

⑵　対象の情報資産の範囲

対象とする情報資産は、情報システムで取扱う電子情報だけでなく、情報システムから出力された紙情報及び情報システム仕様書等システム関連文書もこれに含めるものとする。

⑶　適用対象者

適用対象者は、当院の情報資産及び情報システムを利用するすべての職員等及び委託事業者とする。

５．情報セキュリティ対策

上記３の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。

⑴　組織体制

当院の情報システムについて、情報セキュリティ対策を推進する組織体制を確立する。

⑵　情報資産の分類と管理

当院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。

⑶　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、次の二段階の対策を講じる。

①　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を行うことにより、診療情報の流出を防ぐ。

②　情報系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

⑷　物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

⑸　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。

⑹　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。

⑺　運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシー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、緊急時対応計画を策定する。

⑻　業務委託の利用

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。

６．情報セキュリティ監査及び自己点検の実施

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。

７．情報セキュリティポリシーの見直し

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。

８．医療情報システム運用管理規程の策定

上記５、６及び７に規定する対策等を実施するために、遵守事項及び判断基準等、具体的な手順を定める医療情報システム運用管理規程を策定する。

なお、情報セキュリティ対策基準は、公にすることにより当院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。