青森市民病院
情報セキュリティ基本方針

令和8年4月1日　改定

青森市民病院

目次

青森市民病院情報セキュリティ基本方針

1　目的

青森市民病院情報セキュリティ基本方針（以下「基本方針」という。）は、当院が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産について、当院が実施する情報セキュリティに関する基本的な事項を定めることにより、行政の適正かつ円滑な運営を図りることを目的とする。

2　定義

(1)ネットワーク

青森市民病院内部の接続及び青森市民病院外部との接続のための通信網、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

電子計算機（ネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

(3)医療情報資産

青森市民病院が所管するネットワーク・情報システム及び情報システムの開発と運用に係る情報並びに青森市民病院固有の業務により取得及び作成した情報及びそれらが紙等の有体物に出力又は記録された情報をいう。

(4)職員等

当院の職員及び外部委託事業者をいう。

当院からの指揮命令を受けて業務に従事する者すべてを含むものであり、また、雇用関係のある者のみならず、理事、派遣労働者等も含む。

(5)個人情報

個人情報の定義は、「個人情報の保護に関する法律」（以下「法」という。）で規定されている「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」をいう。

(6)情報セキュリティ対策

医療情報資産を脅威から保護するために行う対策をいうもので、物理的セキュリティ対策、人的セキュリティ対策、技術及び運用におけるセキュリティ対策から構成される。

(7)機密性

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

(8)完全性

医療情報資産が破壊、改ざんまたは消去されていない状態を確保することをいう。

(9)可用性

医療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、医療情報資産にアクセスできる状態を確保することをいう。

3　対象とする脅威

医療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 対象範囲

この情報セキュリティ対策基準が対象とする範囲は、次のとおりとする。

(1)対象者

当院の業務に携わるすべての職員等

(2)対象範囲

当院が所管するすべての医療情報資産

5 職員等の順守義務

職員及び会計年度任用職員等（以下「職員等」という。）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、業務の遂行に当たって情報セキュリティポリシー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の脅威から医療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)管理体制

当院の医療情報資産について、情報セキュリティ対策を推進する管理体制を確立する。

(2)医療情報資産の分類と管理

当院の保有する医療情報資産を、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)物理的セキュリティ

サーバ、ネットワーク、端末等の管理について、物理的な対策を講じる。

(4)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。資産について、情報セキュリティ対策を推進する管理体制を確立。

(5)技術的セキュリティ

アクセス制限、不正プログラム対策、セキュリティ情報の収集等の技術的対策を講じる。

(6)運用
情報システムの監視、情報セキュリティポリシーの順守状況の確認、侵害時の対応や業務継続計画の策定等、運用面での対策を講じる。

(7)法令等の遵守
当院の医療情報資産について、法令を遵守することを求める。

(8)業務委託
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。

(9)評価及び見直し
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、適宜情報セキュリティポリシーの見直しを行う。

7 情報セキュリティ監査及び自己点検の実施

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

8 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、保有する医療情報資産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。

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。

10 情報セキュリティ対策実施手順の策定

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を策定するものとする。