能美市立病院情報セキュリティ基本方針

システム管理委員会

１ 目的

本病院は、受診患者に関する個人情報を数多く保有している。
これらの情報は患者本人の同意が得られるかあるいは法令に定めのある場合以外は第三者に提供してはならない。

なお、これらの個人情報を職員個人が保有するケースも頻繁にあり、こうした個人情報を、漏洩や災害事故等の脅威から防御することは、患者のプライバシー保護や医療サービスの継続的かつ安定的な提供のため、そして基本的な権利保護の視点からも必要不可欠である。

また、国の「医療におけるIT 化の推進」により、診療情報の電子化が進められる中、情報システムを取り巻く環境の変化により、情報資産は改ざんや漏えいを目的とした不正アクセスや、コンピュータウイルス等の発生など、様々な脅威にさらされている。これにより、それぞれの情報資産に個別の対応策を適用するという手法では、十分な情報セキュリティを確保することは困難になっている。

このため、能美市立病院情報セキュリティ対策の基本的な方針として「能美市立病院情報セキュリティ基本方針」を定めるものとする。

２ 定義

（１）情報資産
電磁的に記録された情報及び紙の情報をいう。

（２）個人情報
本病院で定義されている個人情報をいう。

（３）医療情報システム
診療情報を取り扱うシステム（ハードウエア及びソフトウエアを含む。）及び情報を電磁的に記録する媒体で構成された病院業務処理を行う仕組みをいう。

（４）ネットワーク
医療情報システムが相互に接続するための通信網及び通信を行うための機器で構成され、情報処理を行う仕組みをいう。

（５）ＬＡＮ
病院内で構成される医療情報システムを運用するためのネットワークをいう。

（６）外部
病院外のネットワークをいう。

（７）職員
本病院の全ての職員（当院が業務を委託する業者職員を含む）をいう。

（８）システム利用者
職員および医療情報システムの使用を許可された者をいう。

（９）サーバ室
医療情報システムのサーバ、バックアップデータ及びネットワーク機器の集中保管庫の設置室をいう。

（１０）アクセス

ネットワークを介して他の端末と接続し、システム利用者の認証手続等を使用することにより、端末間で情報の転送や利用ができる状態にすることをいう。

（１１）情報セキュリティ

医療情報システム及び情報資産について、以下の３つの性質を満足させることをいう。

ア 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、情報資産にアクセスできる状態を確保すること。

イ 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。

ウ 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。

3 情報セキュリティ対策の構成

（1） 能美市立病院の情報セキュリティ対策は、次に掲げるものから構成するものとする。

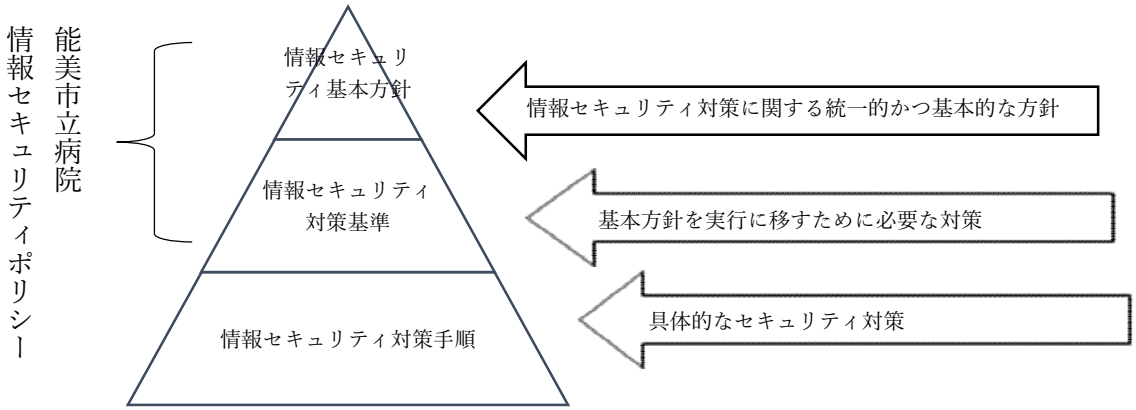
ア 情報セキュリティ対策に関する統一的かつ基本的な方針について規定する「能美市立病院情報セキュリティ基本方針」。

イ アの基本方針を実行に移すために必要な対策を規定する「能美市立病院情報セキュリティ対策基準」。

ウ 具体的なセキュリティ対策を規定する「病院情報セキュリティ対策手順」。

（2）「能美市立病院情報セキュリティ基本方針」は、当院の情報セキュリティ対策の最高位に位置するものである。また「能美市立病院情報セキュリティ基本方針」及び「能美市立病院情報セキュリティ対策基準」を総称して「能美市立病院情報セキュリティポリシー」という。

情報セキュリティ対策の構成



4 対象範囲

能美市立病院情報セキュリティ基本方針の対象範囲は、全ての職員とする。

5 職員の義務

（1）職員は、能美市立病院情報セキュリティポリシーを遵守しなければならない。

（2）職員は、外部委託業者に業務を委託する場合には、契約等を通じ能美市立病院情報セキュリティポリシーを遵守させるために必要な措置を講じなければならない。

6 情報セキュリティ対策の推進体制

能美市立病院における情報セキュリティ対策については、次に掲げる職員又は組織により管理及び推進を行うものとし、その職務内容は次に定めるとおりとする。

（1）医療情報システム最高責任者

能美市立病院における全ての医療情報システム、情報資産及び情報セキュリティ対策に関する最終決定権限及び責任を有する最高責任者とし、院長をもってこれに充てる。

（2）医療情報システム運用責任者

能美市立病院における情報セキュリティ対策に関する適正な運用を管理し、情報管理者を統括する。副院長をもってこれに充てる。

（3）システム管理者

医療情報システムの運用、システム保全、情報資産に関する管理責任者とし、総務課システム管理係の所属職員をもってこれに充てる。

（4）情報担当者

各部署の情報セキュリティ対策に関する推進担当者とし、システム管理委員をもってこれに充てる。各部署に複数のシステム管理委員が存在する場合、その中から責任者を1名選出する。

（5）管理部総務課

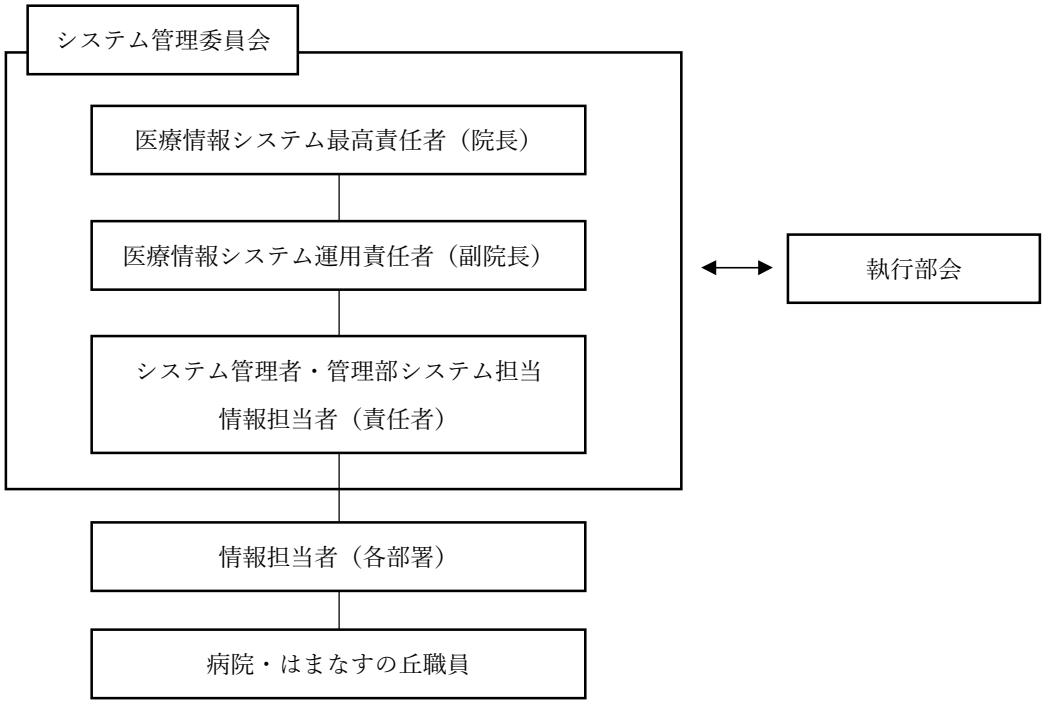
定期的にセキュリティ状況の報告・確認を行う。必要に応じてセキュリティ対策の検討や課題の検討を行う。

（6）システム管理委員会

能美市立病院における医療情報システムの運用検討、情報セキュリティ対策の推進等を目的として設置されたもので、情報セキュリティポリシーの策定及び変更に関する審議等を行う。

（7）執行部会

能美市立病院における最高決定機関であり、システム管理委員会の審議事項について決定する。



7 情報資産の分類

情報資産をその機密度、価値度に応じて分類し、それぞれに対応したセキュリティ対策を講ずる。

（1） 機密度

レベル１ 下記以外の情報資産（機密性を有しないもの）

レベル２ レベル３以外の病院の業務に関わる情報資産（機密性を有するもの） 9

レベル３ 個人情報及び漏えいにより病院の信頼を著しく害する情報資産

（2） 価値度

レベル１ 下記以外の情報資産

レベル２ 失われた場合、再構築するために相当の経費を要する情報資産

レベル３ 失われた場合、再構築することが困難な情報資産

8 対象とするリスク（損害や影響を発生させる可能性をいう）および脅威（リスクを引き起こす要因をいう）

情報資産に対する以下のリスクおよび脅威を想定し、情報セキュリティ対策を実施する。

（1）リスク

ア 情報資産の漏えい・重要情報の詐取

イ 情報又は情報資産の誤った若しくは不適正な発信や公表

ウ 情報資産の破壊・消去

エ システム運用の機能不全等による業務中断

（2）脅威

ア 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
イ 部外者による意図的な要因
ウ 内部不正・内部過失等による要因
エ 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
オ 大規模・広範囲にわたる疾病による要員不足

9 情報セキュリティ対策

情報資産を脅威から保護するため、情報セキュリティ対策基準を規定し、情報セキュリティ対策手順を別途定める。

１０ 情報セキュリティ対策の評価及び見直し

（1）情報セキュリティ対策は、策定することによって完結する一過性の取組みではなく、策定後の日常的な取組みにより確保されるものである。その実施状況を常に検証するとともに、情報セキュリティを取り巻く状況の変化に対応するため、情報セキュリティ対策の見直しを適宜行う。

（2）情報セキュリティ対策の実効性をシステム管理委員会で協議し、能美市立病院情報セキュリティポリシーの内容に関する必要な変更について執行部会に提案を行う。

（3）執行部会は、能美市立病院情報セキュリティポリシーの変更内容を審議し決定する。

（4）情報セキュリティ対策手順は、システム管理者が必要に応じて変更し、システム管理委員会へ報告する。

１１ 関連法規の遵守

（1） 職員は、次に掲げる法令等を遵守の上、情報資産を職務の遂行に用いなければならない。
ア 不正アクセス行為の禁止に関する法律（平成11年法律第128号）
イ 著作権法（昭和45年法律第48号）
ウ 個人情報の保護に関する法律(平成 15 年法律第 57 号)
エ 能美市個人情報保護法施行条例（令和5年能美市条例第2号）

（2） 情報セキュリティ対策の規定に違反した職員は、地方公務員法（昭和 25 年法律第 261 号）及び能美市職員の懲戒の手続及び効果に関する条例（平成 17 年条例第 29 号）に基づき、懲戒処分等の対象となる場合がある。

（3） 前号に該当する職員が、その規定違反を理由とする財産的損失を能美市立病院に生じさせたときには、生じた損失について賠償するものとする。

制定日 令和8年4月1日