サイバーセキュリティ基本方針

地方独立行政法人りんくう総合医療センター（以下「当センター」という。）は、当センターが保有する情報資産の安全性を確保し、安全かつ継続的な医療の提供を実現するため、サイバーセキュリティ基本方針（以下「本方針」という。）を次のとおり定める。

第１条（目的）

本方針は、2024 年（令和 6 年）に改正された地方自治法第 244 条の 6 等の法令に基づき、当センターにおけるサイバーセキュリティの確保に関する基本的事項を定め、情報資産の機密性、完全性及び可用性を維持するとともに、医療提供体制の安定的な運営を確保することを目的とする。

第２条（定義）

本方針において使用する用語の定義は、次のとおりとする。

情　報　資　産：当センターが保有し、又は管理する情報システム、当該システムで取り扱う情報、並びにこれらに関する文書及び電磁的記録媒体をいう。

情 報 シ ス テ ム：コンピュータ、ネットワーク及びこれらに関連する機器並びにソフトウェアの総体をいう。

サイバーセキュリティ：情報資産の機密性、完全性及び可用性を維持し、サイバー攻撃や意図的な要因による漏えい・破壊・改ざんを防止することをいう。

職　　員　　等：当センターの役員、職員、非常勤職員及び業務委託事業者をいう。

第３条（適用範囲）

本方針は、当センターの全ての情報資産及びこれを取り扱う職員等に適用する。

第 4 条（対象とする脅威）

当センターは、次に掲げる脅威を想定し、サイバーセキュリティ対策を講じなければならない。

- 不正アクセス、マルウェア感染（ランサムウェアを含む）、サービス不能攻撃等のサイバー攻撃
- 職員等の過失又は内部不正による情報漏えい等
- システム障害、設備障害、電力・通信・水道供給等のインフラ障害等による業務停止
- 地震、火災等の災害による情報資産の毀損
- 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
- 医療提供体制に重大な影響を及ぼす事象

第 5 条（基本原則）

当センターは、情報資産の重要性に応じて適切な管理を行い、機密性、完全性及び可用性を確保するため、組織的、人的、物理的及び技術的な対策を総合的に講じなければならない。 また、情報システム全体の強靭性を向上させるため、通信経路の分割（分離）や、安全が確保された無害化通信を実施する等の高度な対策を講じるものとする。さらに、外部の事業者へ業務を委託する場合や外部サービス（クラウドサービス等）を利用する場合には、事前に必要な情報セキュリティ対策が確保されていることを確認し、適切な措置を講じるものとする。

第 6 条（職員等の責務）

職員等は、本方針及び関連規程を遵守し、情報資産の適正な取扱いに努めなければならない。

第 7 条（組織体制）

当センターは、最高情報セキュリティ責任者（CISO）を置き、情報セキュリティ対策の総括を行わせるものとする。 当センターは、情報セキュリティ対策を推進するため、情報システム・セキュリティ委員会を設置する。

第 8 条（監査及び自己点検）

当センターは、本方針及び関連規程の遵守状況を確認するため、定期的に監査及び自己点検を実施する。 監査の結果、改善が必要な事項が認められた場合は、速やかに必要な措置を講じるものとする。

第 9 条（公表の制限）

本方針に基づき策定する具体的な対策基準や実施手順のうち、公にすることにより当センターの運営又はセキュリティに支障を及ぼす恐れがあるものは非公開とする。

第 10 条（見直し）

当センターは、サイバーセキュリティを取り巻く環境の変化や監査結果等を踏まえ、本方針を適宜見直し、継続的な改善を図るものとする。