富岡地域医療企業団情報セキュリティ基本方針

令和８年３月 24 日
管理規程第２号

（趣旨）

第１条　富岡地域医療企業団情報セキュリティ基本方針（以下「基本方針」という。）は、富岡地域医療企業団（以下「企業団」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、企業団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。

（定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）　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及びその構成機器（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、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

（３）　情報資産　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電磁的記録媒体並びにネットワーク及び情報システムで取り扱う情報（電磁的に記録されたものに限る。）をいう。

（４）　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。

（５）　情報セキュリティポリシー　本基本方針並びに別に定める公立富岡総合病院情報システム運用管理要綱及び公立七日市病院情報システム運用管理要綱（以下「運用管理要綱」という。）をいう。

（６）　機密性　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。

（７）　完全性　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。

（８）　可用性　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。

（適用範囲）

第３条　基本方針が適用される範囲は、企業長、富岡地域医療企業団病院組織規程（平成 30 年３月 29 日管理規程第２号）第３条に規定する部、議会事務局及び監査委員事務局とする。

（職員等の遵守義務）

第４条　前条に規定する適用範囲に属する正職員、非常勤職員、会計年度任用職員及び委託職員を含む全ての職員（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その他情報セキュリティ対策に関わる各種実施手順を遵守しなければならない。

（対象とする脅威）

第５条　情報資産に対する脅威として、次の各号に掲げる脅威を想定し、情報セキュリティ対策を実施する。

（１）　サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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）　大規模かつ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、通信の途絶等の提供サービスの障害からの波及等

（情報セキュリティ対策）

第６条　前条に規定する脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じるものとする。

（１）　組織体制　企業団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ものとする。

（２）　情報資産の分類と管理　企業団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するよう努め、当該分類に基づき情報セキュリティ対策を行うよう努めるものとする。

（３）　物理的セキュリティ　サーバ等、情報システム室等、通信回線等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ものとする。

（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ものとする。

（５）　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ものとする。

（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、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定するものとする。

（情報セキュリティ監査等の実施）

第７条　情報セキュリティポリシーの遵守状況を検証するため、必要に応じて情報セキュリティ監査又は自己点検を実施する。

（情報セキュリティポリシーの見直し）

第８条　情報セキュリティ監査等の結果、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、情報セキュリティポリシーを見直す。

（運用管理要綱の策定）

第９条　前３条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運用管理要綱を策定する。

２　運用管理要綱に基づき、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よう努めるものとする。なお、情報セキュリティ実施手順は、公にすることにより企業団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。

（その他）

第 10 条　この規程に定めるもののほか、情報セキュリティ対策の実施に関し必要な事項は、別に定める。

附　則

この規程は、公布の日から施行する。