奈良県立病院機構　情報セキュリティ基本方針

１．目的

この基本方針は、地方独立行政法人奈良県立病院機構（以下「法人」という。）が保有する情報全般（以下「情報資産」という。）の機密性、完全性及び可用性を維持するとともに、情報漏えいを防止するため、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

（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、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。

（３）　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。

（４）　情報セキュリティポリシー

この基本方針、情報セキュリティ対策基準（事務系ネットワーク)、情報セキュリティ実施手順及び医療情報システム・運用管理規程をいう。

（５）　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。

（６）　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。

（７）　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。

（８）　マイナンバー利用事務系(個人番号利用事務系)

個人番号利用事務に関わる情報システム及びデータをいう。

（９）　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(10)　無害化通信

インターネットメール本文のテキスト化や支給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無い等、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。

（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、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．情報資産の範囲

この基本方針が対象とする情報資産は、次のとおりとする。

（1） 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

（2） ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

（3） 情報システムの仕様書及びネットワーク図等のシステム関連文書

5．適用対象者

法人の役員、職員、派遣契約その他の契約等により法人の業務に従事する全ての者（以下「利用者」という。）に適用する。

6．法令等の遵守

利用者は、情報セキュリティに関する法令、国の指針、ガイドラインその他の規範を遵守する。

7．情報セキュリティ組織体制

法人の情報資産について、情報セキュリティ対策を推進するため、総務担当理事を最高情報セキュリティ責任者とし、法人全体の組織体制を確立する。

（1）事務系ネットワークに係る組織体制

事務系ネットワーク、事務系情報システム等の情報資産の管理及び情報セキュリティ対策に関して、最高情報セキュリティ責任者が最終決定権限及び責任を有する。

事務系ネットワークについては、最高情報セキュリティ責任者の下に情報セキュリティ対策基準（事務系ネットワーク）において定める統括情報セキュリティ責任者等を設置する。

（2）医療系ネットワークにかかる組織体制について

医療系ネットワーク、医療系情報システム等の情報資産の管理及び情報セキュリティ対策に関して、医療情報システム運用責任者が最終決定権限及び責任を有する。

医療系ネットワークについては、各センターの院長を医療情報システム運用責任者とし、この下に医療情報システム・運用管理規程において定めるシステム管理者等を設置する。

（3）CSIRT の整備について

最高情報セキュリティ責任者は、法人の全てのネットワークにおける情報セキュリティインシデントに対処するための体制（CSIRT:Computer Security Incident Response Team）を整備し、情報セキュリティインシデント発生時には、再発防止策等を実施するために必要な措置を指示する。

8．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。

（1） 情報資産の分類と管理

法人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。

（2） 情報システム全体の強靭性の向上

情報システム全体に対し、次の二段階の対策を講じる。

①インターネット接続系においては、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。

②マイナンバー利用事務系においては、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、支給端末からの情報持ち出し不可設定や支給端末への多要素認証の導入等により、個人情報の流出を防ぐ。

（3） 物理的セキュリティ

サーバ等、情報システム室等、通信回線等及び利用者のパソコン等の管理について、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、利用者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。

（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。

（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、業務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。

（7） 業務委託と外部サービスの利用

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、業務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。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

9．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。

10. 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、情報セキュリティポリシーを見直す。

11. 情報セキュリティ教育・訓練の実施

上記5の適用対象者に対して、情報セキュリティの重要性の認識と、情報資産の適正な利用・管理のために必要な教育・訓練を実施する。

12. 情報セキュリティ関連規程等の策定

上記8～11に規定する対策等を実施するために、事務系ネットワークについては、情報セキュリティ対策基準（事務系ネットワーク）において、医療系ネットワークについては、医療情報システム・運用管理規程において、具体的な遵守事項及び判断基準等を定め、具体的な手順については、実施手順を策定するものとする。また、実施手順は、公にすることにより本法人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。

附　則

この基本方針は、令和元年５月１日から施行する。

附　則

この基本方針は、令和４年４月１日から施行する。

附　則

この基本方針は、令和５年３月１日から施行する。