

身延町早川町国民健康保険病院一部事務組合
情報セキュリティポリシー

身延町早川町国民健康保険病院一部事務組合情報セキュリティ基本方針

1 目的

この基本方針は、身延町早川町国民健康保険病院一部事務組合（以下「組合」という。）が保有する情報資産を取り扱う環境の機密性、完全性及び可用性を確保、維持するため、本組合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ことを目的とする。

2 定義

この基本方針において、次の各号に掲げる用語の意義は、それぞれ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、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

電子情報、紙媒体、情報システム、ネットワーク機器、その他これらに準ずるものをいう。

(4) 情報セキュリティ

情報資産の気密性、完全性及び可用性を確保することをいう。

(5) 情報セキュリティポリシー

この基本方針及び情報資産を活用するに当たって、セキュリティ上保護すべき対象範囲、対策、組織体制等についての方針を明文化するものをいう。

(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。

(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係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、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) 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、消去等、重要情報の搾取、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、プログラム上の欠陥、操作ミス、故障等の非意図的の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等の停止等。
- (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 情報セキュリティの適用範囲

(1) 行政機関の範囲

この基本方針が適用される組織の範囲は、組合事務局、議会、監査委員及び公平委員会に適用する。また、組合の業務に従事するすべての職員（再任用職員、会計年度任用職員等を含む。）並びに委託業務者等は、本基本方針を遵守しなければならない。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ① ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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章を含む。）

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章

5 職員等の遵守義務

職員、再任用職員、会計年度任用職員（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実施手順及びこれに関連する法令等を遵守しなければならない。

6 情報セキュリティ対策

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) 組織体制として、本組合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。
- (2) 情報資産の分類と管理として、本組合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行う。
- (3) 物理的セキュリティ対策として、ネットワーク、情報資産を設置する場所の安全性の確保、当該場所への入退室の管理等の物理的な対策を行う。
- (4) 人的セキュリティとして、情報セキュリティに関する職員等の権限と責務の啓発、情報資産が発生した場合の職員等の報告義務等の人的な対策を行う。
- (5) 技術的セキュリティ対策として、情報資産を不正なアクセスから保護するため、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行う。
- (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、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、緊急時の対策を行う。

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、定期的に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

情報セキュリティポリシーの遵守事項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となった場合には、情報セキュリティポリシーを見直すものとする。

9 情報セキュリティ対策基準の策定

前6、7及び8に規定する対策等を実施するために、職員等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ものとする。

1 0 情報セキュリティ実施手順の策定

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。

1 1 非公開

実施手順書は、具体的な対策が定められており、当組合の情報セキュリティ対策に重大な影響を及ぼすおそれがあることから、非公開とする。

1 2 違反に対する対応

情報セキュリティポリシー及び実施手順に違反した者に対しては、その違反の程度に応じて地方公務員法（昭和25年法律第261号）の規定による懲戒、その他関係法令に基づく厳正な対応を行う。

1 3 その他

この基本方針に関し必要な事項は、別に定める。