

情報セキュリティ基本方針

1 目的

本組合が取り扱う情報資産には、住民の個人情報のみならず行政運営上重要な情報など、外部への漏えい等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産並びに情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、住民の財産、プライバシー等を守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。ひいては、このことが本組合に対する住民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるIT革命の進展により、電子商取引の発展や電子自治体の実現が期待されているところである。本組合がこれらに積極的に対応するためには、管理している全てのネットワーク及び情報システムが高度な安全性を有することが不可欠である。

そのため、本組合の情報資産の機密性、完全性及び可用性^(注)を維持するための対策を整備するために王寺周辺広域休日応急診療施設組合情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については本組合の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

(注)：国際標準化機構(ISO)が定めるもの(ISO7498-2：1989)

機密性(confidentiality)：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性(integrity)：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性(availability)：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

2 用語の定義

(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

電子計算機(ハードウェア及びソフトウェア)及び記録媒体で構成され、処理を行う仕組みをいう。

(3) 情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。なお、情報資産には電子媒体にコピーされた情報、電子化される情報の入力となる紙媒体、出力される紙媒体の情報及び文書情報も含むものとする。

(4) 情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(5) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

3 情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本組合が保有する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

4 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、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・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

5 適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は、管理者部局、行政委員会、議会事務局とする。

(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、情報システム、これらに関する設備、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

6 職員等の義務

本組合が保有する情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

7 情報セキュリティ対策

上記4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) 組織体制

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全庁的な組織体制を確立する。

(2) 情報資産の分類と管理

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

サーバ等、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。

(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。

(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、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切に対応するため、緊急時対応計画を策定する。

8 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自己点検を実施する。

9 情報セキュリティポリシーの見直し

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。

10 情報セキュリティ対策基準の策定

上記7、8及び9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情報セキュリティ対策基準を策定する。