京都府後期高齢者医療広域連合情報セキュリティ基本方針

（目的）

第１条　この基本方針は､京都府後期高齢者医療広域連合（以下「広域連合」という。）が保有する住民の個人情報及び行政運営上重要な情報資産をさまざまな脅威から保護するため、情報資産を取り扱う職員等が守るべき事項や職員等の情報セキュリティに対する意識向上のための教育、情報資産へのアクセス制御等の技術的な対策等の基本的な考え方を定めるものであり、広域連合における情報セキュリティ水準を維持及び向上させることを目的とする。

なお、本基本方針については、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

（定義）

第２条　この基本方針及び対策基準において、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）情報システム　コンピュータ、ネットワーク並びにコンピュータ又はネットワークに付随するハードウェア及びソフトウェア等の全部又は一部で構成された情報処理に用いる仕組みをいう。

（２）ネットワーク　コンピュータ及び周辺機器の多目的利用並びに各種オンラインシステムの情報伝送を目的として構築された情報通信基盤をいう。

（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）機密性　情報資産のアクセス権限をもつ者のみが、当該情報資産にアクセスできることを確実にすることをいう。

（５）完全性　情報資産が正確で、かつ完全である状態を確実にすることをいう。

（６）可用性　情報資産のアクセス権限をもつ者が必要なときに、当該情報資産にアクセスできることを確実にすることをいう。

（７）情報セキュリティポリシー　情報資産に対する情報セキュリティ対策を総合的、体系的かつ具体的に取りまとめたものを総称し、普遍性を備えた部分である基本方針及び情報資産を取り巻く状況の変化に依存する部分である対策基準で構成されるもの（以下「セキュリティポリシー」という。）をいう。

（８）ファイアウォール　外部から組織内のネットワークに侵入されることを防ぐシステムをいう。

（９）無線ＬＡＮ　ケーブルを使わず、電波等による無線通信で情報伝送を行うネットワークをいう。

(10) 管理区域　ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための区域（以下「情報システム管理区域」という。）や電磁的記録媒体の保管庫をいう。

(11) 複合機　プリンター、イメージスキャナ、ファクシミリ等の機能が一つにまとめられた機器のことをいう。

（対象とする脅威）

第３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）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

（６）その他情報資産へのあらゆる侵害行為

（適用範囲）

第４条　この基本方針の適用範囲は、次の各号に掲げるとおりとする。

（１）行政機関の範囲

本基本方針が適用される行政機関は、広域連合の広域連合長の事務部局、議会及び行政委員会とする。

（２）適用範囲

本基本方針が適用される範囲は、広域連合が後期高齢者医療制度を運営するにあたり構築されたネットワーク、情報システム及び情報資産とする。

（３）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、情報システム及び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

（職員等の遵守義務）

第５条　職員、非常勤職員及び臨時職員（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セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

（情報セキュリティ対策）

第６条　第３条に掲げる脅威から情報資産を保護するために、次の事項に掲げる事項についてそれぞれの情報セキュリティ対策を講じる。

（１）組織体制

広域連合の情報資産について、情報セキュリティ対策を推進し、管理するための情報セキュリティ管理体制を確立する。

（２）情報資産の分類と管理

広域連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

サーバ等を集約し保管するデータセンター（以下「データセンター」という。）及び広域連合事務所等の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、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、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。

（情報セキュリティ監査及び自己点検の実施）

第７条　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。

（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及び自己点検の結果、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、セキュリティポリシーを見直す。

（情報セキュリティ対策基準の策定）

第９条　第６条、第７条及び第８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情報セキュリティ対策基準を策定する。

（情報セキュリティ実施手順の策定）

第１０条　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。

２　情報セキュリティ実施手順は、公にすることにより後期高齢者医療制度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。