兵庫県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　本基本方針は、兵庫県後期高齢者医療広域連合（以下、「広域連合」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、広域連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。

（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、その構成機器(ハードウエア及びソフトウエア）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

本基本方針及び情報セキュリティ対策基準をいう。

(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)　システム利用団体

広域連合の情報システムを利用する兵庫県内の全ての市町

(9)　職員

広域連合の職員（一般職、特別職を問わない。また、非常勤職員、臨時職員及び契約等により当該業務に従事する者を含む。）をいう。

(10)　利用者

システム利用団体において広域連合の情報システムを利用する者をいう。

(11)　外部委託事業者

広域連合から情報システムの開発・運用や、データの保管等を委託された外部委託事業者をいう。

(12)　監査

広域連合の管理の下にある情報資産に対して実施する情報セキュリティ監査をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、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)　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

(2)　情報資産の無断持ち出し、無許可ソフトウエ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

（適用範囲と情報資産の範囲）

第４条　本基本方針が適用される範囲は、職員、利用者及び外部委託事業者とする。

２　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)　広域連合が管理するすべてのネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体並びに情報システムへ入力する紙媒体の情報

(2)　前項に関する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)　前二項に関する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

（遵守義務）

第５条　職員、利用者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持ち、業務の遂行に当たって情報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

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する全組織的な組織体制を確立する。

(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、情報システム室等、通信回線等及び職員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、利用者及び外部委託事業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及び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。

（情報セキュリティ監査及び自己点検の実施）

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、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。

（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。

（情報セキュリティ対策基準の策定）

第９条　第６条から第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広域連合の事業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

（施行期日）

この基本方針は、平成１９年６月２５日より施行する。

附則

この基本方針は、平成２７年１２月２８日より施行する。