宮城県後期高齢者医療広域連合
情報セキュリティポリシー

平成２８年１０月　第３版

目　次

第１章　情報セキュリティ基本方針

第１章 情報セキュリティ基本方針

１　目的

宮城県後期高齢者医療広域連合（以下「広域連合」という）の取り扱う情報には，被保険者の住民基本台帳情報・税情報・診療報酬請求明細書情報等の重要なものが数多くあり，部外に漏洩した場合には極めて重大な結果を招く情報が数多く含まれている。

これらの情報資産を人的脅威や災害，事故等から防御することは，広域連合に対する被保険者をはじめとする住民や市町村からの信頼の向上に寄与するものであり，被保険者の権利，プライバシー等を守るためにも，また，継続的かつ安全・安定的な後期高齢者医療制度の実施を確保するためにも必要不可欠である。

また，ＩＴ技術の進展により，効率的な制度運営の実現が求められている中で，ネットワーク及び情報システムが高度な安全性を確保することは，業務を行う際の必要不可欠な前提条件となる。

このため，広域連合の情報資産の機密性，安全性及び可用性を維持するための対策を整備することを目的として，宮城県後期高齢者医療広域連合情報セキュリティポリシー（以下「情報セキュリティポリシー」という）を定め，情報セキュリティの確保に最大限取り組むものである。

このうち情報セキュリティ基本方針は，広域連合の情報セキュリティ対策の基本的な方針として，広域連合情報セキュリティポリシーの対象，位置付けを定めるものとする。

2　情報セキュリティポリシーの構成

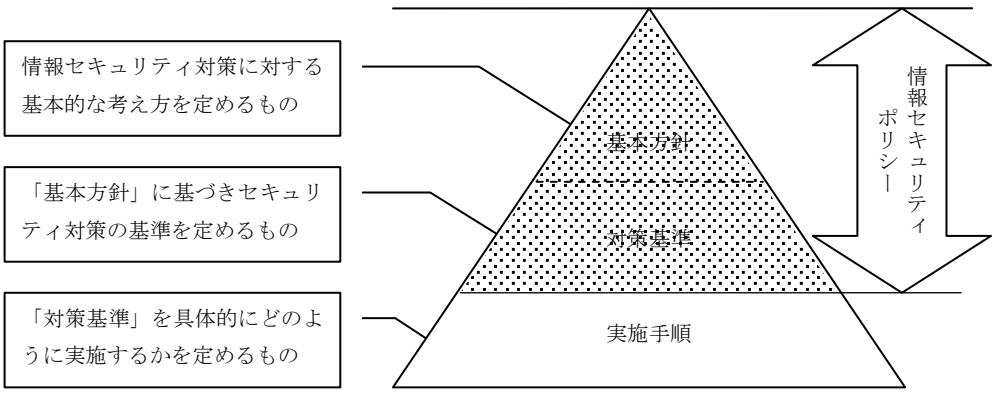
広域連合情報セキュリティポリシーは，「情報セキュリティ基本方針」（以下「基本方針」という。）と「情報セキュリティ対策基準」（以下「対策基準」という。）の二層で構成される。

(1)　基本方針

情報セキュリティに対する取組姿勢を表すもので，情報セキュリティ対策における基本的な考え方を定めるもの。

(2)　対策基準

「基本方針」に基づき情報セキュリティを確保するために，遵守すべき行為及び判断等のすべての情報セキュリティ対策の基準を定めるもの。なお，情報セキュリティポリシーには含まれないものの，「対策基準」に定められた内容を具体的にどのような手順に従って実行していくのかを示すもの（運用マニュアル）を，「広域連合情報セキュリティポリシー実施手順」という。



3　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（ハードウェアおよびソフトウェア）をいう。

(2)　電磁的記録媒体

　ハードディスク，フロッピーディスク，ＣＤ－ＲＯＭ，磁気テープ，光磁気ディスク，その他これらに類する，電子情報を記録するための媒体をいう。

(3)　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。

(4)　広域連合電算処理システム

　資格管理・保険料賦課・保険料収納・給付に関する業務を処理する情報システムをいう。

(5)　内部情報システム

　財務会計，文書管理，グループウェア等に関する業務を処理する情報システムをいう。

(6)　パソコン等端末

　広域連合電算処理システム，財務会計システム等に接続され，情報の記録及び入出力機能を有するハードウェア及びソフトウェアで構成するコンピュータ及び周辺機器をいう。

(7)　情報資産

　広域連合で取り扱う全ての情報をいう。

(8)　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。

(9)　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。

(10)　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。

(11)　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。

(12)　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。

(13)　個人情報

　個人に関する情報であって，特定の個人が識別され，又は識別され得るものをいう。

(14)　職員

　職員，非常勤職員，臨時職員を含む広域連合の全職員及び宮城県内関係市町村の後期高

齢者医療担当職員をいう。

※宮城県内関係市町村の後期高齢者医療担当職員の適用範囲は，広域連合で行われる後期高齢者医療制度運営に関係する業務とする。

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　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

6　職員の遵守義務

職員は，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。

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

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情報セキュリティ委員会を設置する。

(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重要度に応じて分類し，当該分類に基づき情報セキュリティ対策を講じる。

(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の措置を講じる。

８　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，情報セキュリティ監査及び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

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。

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。

１１ 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。なお，情報セキュリティ実施手順は，公にすることにより行政運営に重大な支障を及ぼす恐れがあることから非公開とする。