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

令和７年３月　第４版

目　次

第１章　情報セキュリティ基本方針

1	目的　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	1
2	情報セキュリティポリシーの構成・・・・・・・・・・・・・・・・・・・・・・・・	1
3	定義　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	2
4	対象とする脅威　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	3
5	適用範囲　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	3
6	職員の遵守義務　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	3
7	情報セキュリティ対策　・・・・・・・・・・・・・・・・・・・・・・・・・・・・	3
8	情報セキュリティ監査及び自己点検の実施　・・・・・・・・・・・・・・・・・・	4
9	情報セキュリティポリシーの見直し　・・・・・・・・・・・・・・・・・・・・・	5
10	情報セキュリティ対策基準の策定　・・・・・・・・・・・・・・・・・・・・・・	5
11	情報セキュリティ共通実施手順の策定　・・・・・・・・・・・・・・・・・・・・	5

※　第１版　平成１９年１２月

第２版　平成２６年　４月　組織変更に伴い一部修正

第３版　平成２８年１０月　全部改正

第４版　令和　７年　３月　一部改正

第１章 情報セキュリティ基本方針

１　目的

本基本方針は、宮城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。

２　情報セキュリティポリシーの構成

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。

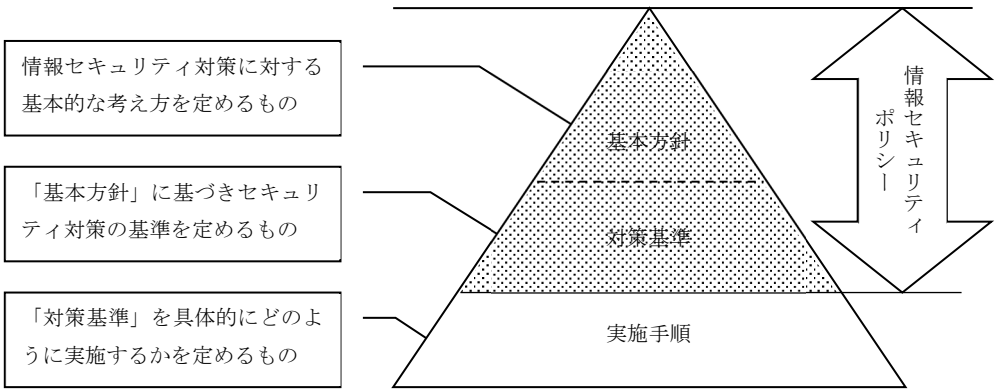
（１）　基本方針

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、全ての行為及び判断において遵守すべき基準を定めるもの。

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を、情報セキュリティ共通実施手順（以下「実施手順」という。）という。



３　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）　電磁的記録媒体

　ハードディスク、CD-ROM、USB メモリ、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）　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。

（６）　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。

（７）　情報セキュリティポリシー

　本基本方針及び対策基準をいう。

（８）　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。

（９）　情報資産

　広域連合で取り扱う全ての情報をいう。

（１０）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。

（１１）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。

（１２）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。

（１３）マイナンバー利用事務系

　マイナンバーを利用する事務に関わる情報システム及びデータをいう。

（１４）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。

（１５）職員

職員、会計年度任用職員、非常勤職員を含む広域連合の全職員をいう。

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、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

基本方針が適用される行政機関は、広域連合事務局、議会事務局、監査委員事務局及び選挙管理委員会とする。

（２）　情報資産の範囲

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共通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「重要度」として分類し、当該分類に基づき情報セキュリティ対策を講じる。

（３）　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の対策を講じる。

①　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持出し不可設定や端末への多要素認証の導入により、住民情報の流出を防ぐ。

②　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

（４）　物理的セキュリティ

サーバ、通信回線、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。

（５）　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。

（６）　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。

（７）　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、業務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）　業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

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て情報セキュ

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失を分析し、リスクを検討した上で、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、判断基準等を定める対策基準を策定する。

なお、対策基準は、公にすることにより行政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。

１１　情報セキュリティ共通実施手順の策定

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実施手順を策定するものとする。

なお、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おそれがあることから非公開とする。