徳島県後期高齢者医療広域連合
情報セキュリティポリシー
基　　本　　方　　針

第 1.3 版

改　定　履　歴

版 数	改 定 年 月 日	改　定　内　容
1.0	平成 19 年 4 月 1 日	・新規制定
1.1	平成 27 年 10 月 1 日	・基本方針「２　定義　⑷　個人情報」について，追加変更
1.2	平成 28 年 11 月 1 日	・「基本方針」と「対策基準」を分割（対策基準は非公開のため） ・改訂履歴を「基本方針」と「対策基準」に分割 ・構成「対策基準」，「実施手順」の内容変更 ・基本方針「２　定義」のうち，「⑶　情報資産」の内容追加及び「⑼　職員等」の号を追加 ・基本方針「４　セキュリティポリシーの対象範囲」において，字句の削除 ・基本方針「８　情報資産への脅威」の内容変更及び字句の追加
1.3	平成 29 年６月 14 日	・基本方針「２　定義」のうち，「⑷　個人情報」の内容修正及び「⑹　ドキュメント」に字句追加

※1.2 版から基本方針と対策基準を分割

＜目　次＞

はじめに　徳島県後期高齢者医療広域連合情報セキュリティポリシーの構成

徳島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「ポリシー」という。）とは，広域連合が保有する情報資産に関するセキュリティ対策について，総合的，体系的及び具体的に取りまとめたものである。

ポリシーは，広域連合の情報資産を取り扱う全職員等に浸透，定着させるものであり，安定的な規範であることが要請される。しかし，一方では，情報セキュリティ対策は，情報処理技術や通信技術等の進展に伴う急速な状況の変化に，柔軟に対応することも必要である。

このようなことから，ポリシーは，一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と，情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層から成るものとして策定することとする。また，ポリシーに基づき，ネットワーク及び電算システムごとに，具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定することとする。

情報セキュリティポリシーの構成

文書名		内容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針に従い，情報資産を保護・管理するために遵守すべき事項を可能な限り具体的かつ網羅的に記載した情報セキュリティ対策の基準
	情報セキュリティ実施手順	情報セキュリティ対策基準に基づき，情報資産ごとに詳細なガイドライン等を具体的に定めた実施手順

第１　徳島県後期高齢者医療広域連合情報セキュリティ基本方針

１　目的

広域連合が取り扱う情報資産には，後期高齢者医療事務に係る被保険者等の個人情報のみならず行政運営上重要な情報など，部外に漏えい等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おり，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，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。また，近年のＩＴ革命の進展により，電子政府や電子自治体の実現も期待されている。広域連合がこれらに積極的な対応をするためには，広域連合が管理しているすべてのネットワーク及び電算システムが高度な安全性を有することが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，完全性及び可用性（注１）を維持するための対策を整備するため，徳島県後期高齢者医療広域連合情報セキュリティポリシーを定めることとし，情報セキュリティの確保に最大限取り組むこととする。

このうち情報セキュリティ基本方針においては，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，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１）：国際標準化機構（ISO）が定めるもの（ISO 7498－2：1989）

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完全防護すること。

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　定義

⑴　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及びその機器で構成され，処理を行う仕組みをいう。

⑵　電算システム

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，周辺機器及びネットワークをいう。

⑶　情報資産

ネットワーク及び電算システムの企画，開発及び運用保守に係るすべての情報並びにネットワーク及び電算システムで取り扱うすべての情報のみならず，電算システムから出力された紙による記録及び関係団体等から提供を受けた紙による情報をいう。

⑷　個人情報

生存する個人に関する情報であって，当該情報に含まれる氏名，住所，生年月日その他の記述又は個人別に付けられた番号，記号その他の符号，画像若しくは音声によって当該個人を識別できるもの（一般人が通常入手し得る関連情報と照合することに

より，当該個人を識別することができるものを含む。）をいう。なお，個人情報には行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）第２条第８項に規定する特定個人情報も含まれる。

ただし，特定個人情報のうち，個人番号については，生存者の個人番号であることが要件でないため，死者の個人番号も保護の対象となる。また，法令の定める業務範囲の手続において，個人番号の記入欄のある様式を用いて得られた情報については，様式に個人番号の記入がない個人情報も特定個人情報と同様に取り扱う。

⑸　セキュリティ

情報資産の機密の保持及び正確性，安全性の維持。許可されていない第三者から情報資産等を守ることをいう。

⑹　ドキュメント

システム設計書，ネットワーク設計書，システム仕様書，ネットワーク仕様書，プログラム仕様書，オペレーション仕様書，コード一覧表等ネットワーク及び電算システムに必要な仕様書類等をいう。

⑺　記憶媒体等

磁気的，光学的に記憶させている電子媒体のみならず，電算システムから出力された紙による記録及び関係団体等から提供を受けた紙による記録も含む。

⑻　データ

ネットワーク及び電算システムに係る入出力帳票，記憶媒体及びドキュメントをいう。

⑼　職員等

現に職員である者及び過去に職員であった者をいう（非常勤職員及び臨時職員を含む）。

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，広域連合の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，体系的及び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最高位に位置するものである。

4　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの対象範囲は，広域連合における情報資産に接するすべての職員等とする。

5　職員等の義務

職員等は，情報セキュリティの重要性について共通の認識を持つとともに，情報資産の利用に当たっては情報セキュリティポリシーを遵守するものとする。

6　情報セキュリティ管理体制

広域連合の情報資産について，適切に情報セキュリティ対策を推進，管理するための

体制を確立するものとする。

7　情報資産の分類

情報資産をその重要度に応じて分類し，それに応じたセキュリティ対策を行うものとする。

8　情報資産への脅威

情報セキュリティポリシーを講ずる上で，情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。

特に認識すべき脅威は，次のとおりである。

⑴　権限を有しない者による不正アクセス又は不正操作による情報資産の持出し，盗聴，改ざん，消去，機器及び記憶媒体の盗難等

⑵　職員等及び外部委託者による意図しない操作，故意の不正アクセス又は不正操作による情報資産の持出し，盗聴，改ざん，消去，機器及び記憶媒体の盗難並びに規定外の電算システムの機器操作によるデータ漏えい等

⑶　地震，落雷及び火災等の災害並びにテロ，事故，故障等によるサービス及び業務の停止

9　情報セキュリティ対策

広域連合の情報資産を上記８の脅威から保護するため，以下の情報セキュリティ対策を講ずるものとする。

⑴　人的セキュリティ対策

情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めるとともに，すべての職員等に情報セキュリティポリシーの内容を周知徹底するため，教育，訓練を行う。

⑵　物理的セキュリティ対策

電算システムを設置する施設への不正な立ち入り等から保護するため，入退室や機器管理上の物理的な対策を講ずる。

⑶　技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため，情報資産へのアクセス制御，コンピュータウィルス対策等を実施する。

⑷　運用におけるセキュリティ対策

情報セキュリティポリシーの実効性を確保するため，また，不正アクセスされること及び不正アクセスによって他の電算システムに対して被害を及ぼすことを防ぐため，ネットワークの監視，セキュリティポリシーの遵守状況の確認等，必要な措置を講ずる。また，障害及び緊急事態が発生した際の迅速な対応を可能とするための対策を講ずる。

１０　情報セキュリティ対策基準の策定

広域連合の情報資産について，上記９の情報セキュリティ対策を講ずるに当たっては，職員等が遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。そのため，情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

なお，情報セキュリティ対策基準は，公開することにより広域連合の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

１１　情報セキュリティ実施手順（運用マニュアル）の策定

情報セキュリティ対策を確実に実施していくためには，個々の情報資産に関する対策の手順を具体的に定めておく必要があることから，情報セキュリティ対策基準に基づき，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，公開することにより広域連合の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

１２　評価，見直し

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価，ネットワーク及び電算システムの変更，新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ，適宜情報セキュリティ対策基準の見直しを実施するものとする。