

島根県後期高齢者医療広域連合

情報セキュリティ基本方針

平成19年6月

## —目次—

第1条	目的	1
第2条	定義	1
第3条	対象機関	1
第4条	情報セキュリティ管理組織体制	2
第5条	職員の義務	2
第6条	委託に伴う措置	2
第7条	情報資産の分類	2
第8条	情報セキュリティ対策	2
第9条	情報セキュリティ対策基準	2
第10条	情報セキュリティ対策実施手順	3
第11条	義務違反者に対する措置	3
第12条	情報セキュリティ対策実施状況の点検及び監査	3
第13条	評価及び見直し	3

## 島根県後期高齢者医療広域連合情報セキュリティ対策基本方針

### (目的)

第1条 島根県後期高齢者医療広域連合情報セキュリティ対策基本方針（以下「基本方針」という。）は、情報のセキュリティ対策についての基本的考え方及び方策を定め、島根県後期高齢者医療広域連合（以下、「広域連合」という。）が管理する情報資産を適切に保護することを目的とする。

### (定義)

第2条 この基本方針における用語の意義は、次の各号に規定する。

#### (1) 情報セキュリティポリシー

情報のセキュリティ対策に関する組織的な取組方針を明文化したもので、基本方針及び情報セキュリティ対策基準のことをいう。

#### (2) 情報システム

コンピュータ（ハードウェア、ソフトウェア）、ネットワーク又は記録媒体を用いて事務処理を行うための情報処理の仕組みをいう。

#### (3) ネットワーク

コンピュータを相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）で構成された情報通信基盤をいう。

#### (4) 情報

職務の遂行に伴ってコンピュータ及び記録媒体に記録されたデータをいう。

#### (5) 情報資産

情報及び情報システムをいう

#### (6) 情報セキュリティ

広域連合が管理する情報資産を脅威から保護し、情報資産の「機密性」、「完全性」及び「可用性」を保護することをいう。

ア 「機密性」 権限のない者への重要な情報の漏えいを防止すること。

イ 「完全性」 情報の改ざん、破壊による被害を防止すること。

ウ 「可用性」 権限のある者に対し、いつでも情報の利用を可能とすること。

#### (7) 脅威

自然の脅威（地震、火災、風水害等）、情報システムの脅威（情報システムの故障、誤作動等）及び人的な脅威（不正行為、誤操作等）などで、情報資産に対して障害や損害を与える原因となるものをいう。

### (対象機関)

第3条 情報セキュリティポリシーの対象機関は、広域連合事務局、選挙管理委員会、監査委員及び議会とする。

### (情報セキュリティ管理組織体制)

第4条 広域連合が管理する情報資産について、統一的な情報セキュリティ対策を確保するため、全庁的な組織体制を整備する。

(職員の義務)

第5条 特別職及び臨時職員等を含むすべての職員（以下「職員等」という。）は、情報セキュリティ対策の重要性について共通の認識を持つとともに、業務の遂行に当たっては、情報のセキュリティ対策に関する法令及び情報セキュリティポリシー等を遵守する義務を負うものとする。

(委託に伴う措置)

第6条 委託契約を締結し、情報資産の取扱いに関する業務の委託を受けた業者及びその社員等（以下「委託業者等」という。）に情報資産の取扱いに従事させる場合は、契約等に基づき、情報セキュリティポリシーを遵守させるための必要な措置を講ずるものとする。

(情報資産の分類)

第7条 情報資産は、その重要度に応じて分類を行い、その区分に応じた適切な保護対策を講ずるものとする。

(情報セキュリティ対策)

第8条 情報資産を脅威から保護するために、次の各号に定める情報セキュリティ対策を講ずるものとする。

(1) 物理的セキュリティ対策

情報システムを設置する施設への不正な立ち入りや、情報資産に対する脅威から保護するために物理的な対策を行う。

(2) 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、職員等及び委託業者等に対して情報セキュリティ対策の重要性を認識させるために有効と考えられる教育、研修、啓発活動などの対策を行う。

(3) 技術的セキュリティ対策

情報システムの誤操作、不正アクセス等から情報資産を保護するため、情報資産へのアクセス制御等の技術的な対策を行うとともに、情報システムの開発・導入・更新時における開発環境及び品質確保等の対策を行う。

(4) 情報システム運用上のセキュリティ対策

情報システムに対する運用方法の誤り、誤操作あるいは不正アクセス等から情報資産を保護するため、運用、保守及び監視等の対策を行うとともに、緊急事態が発生した場合に迅速かつ適切な対応を可能とするための危機管理対策を行う。

(情報セキュリティ対策基準)

第9条 広域連合における情報セキュリティ対策の統一基準となる情報セキュリティ対策基準（以下、「対策基準」という。）を定め、想定される脅威に対応するための対策要件

を規定する。

(情報セキュリティ対策実施手順)

第10条 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手法、手順を明記した「情報セキュリティ対策実施手順」(以下「実施手順」という。)を策定するものとする。

(義務違反者に対する措置)

第11条 情報セキュリティポリシーに違反した職員等は、地方公務員法(昭和25年法律第261号)等により懲戒処分の対象となる場合がある。

(情報セキュリティ対策実施状況の点検及び監査)

第12条 情報セキュリティポリシーが遵守されていることを確認するため、定期的に情報セキュリティ対策の実施状況の点検及び監査を行う。

(評価及び見直し)

第13条 情報セキュリティ対策の実施状況の点検及び監査結果や状況の変化を踏まえ、適時、情報セキュリティポリシー及び実施手順の見直しを実施するものとする。