

情報セキュリティ基本方針

1 目的

鹿児島県国民健康保険団体連合会（以下「連合会」という。）は、診療報酬の審査支払業務、保険者事務の共同電算処理業務、保健事業等の事業、介護給付費の審査支払業務及び障害介護給付費支払業務等を行うために、個人の診療内容等個人情報を中心とする重要かつ膨大な情報を取り扱っている。そのため、連合会として社会的な信用の失墜はあってはならないものと考えている。そこで、ISO27001を意識した情報セキュリティポリシーを作成し、個人の情報を「情報資産」として保護、管理し、セキュリティの強化を図ることにより、更なる信頼向上を目指す。

本基本方針は、連合会が保有する個人情報を含む情報資産の機密性、完全性及び可用性を維持し、直面するリスクに対応するため、連合会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 定義

(1) 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。

(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) 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。

(4) 情報

情報システム及びネットワークで取り扱われる情報（電子媒体に記録されたデータ及び電子データ）及び紙媒体に記載された情報をいう。

(5) 情報資産

連合会にとって価値を持つもので、情報及び情報システム、ネットワークをいう。

(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) 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。

(8) 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。

(9) 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。

(10) 脅威

システム又は連合会に損害を与える可能性がある事象の潜在的な原因。

(11) 情報セキュリティ委員会

情報セキュリティに関する重要事項を決定する機関。

3 情報セキュリティポリシーの構成

連合会情報セキュリティポリシーは、情報セキュリティ対策における基本的な考え方を定めた、「情報セキュリティ基本方針」と、この情報セキュリティ基本方針に基づき、すべての情報システムに共通の情報セキュリティ対策の基準を定めた「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。また、情報セキュリティポリシーに基づき、個々の情報資産に関する具体的な情報セキュリティ対策の実施手順として、「情報セキュリティ実施手順」を策定する。

情報セキュリティポリシーは、連合会の情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティの対策の最高位に位置するものである。

当連合会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を実行に移すための、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いた個々の情報資産に関する具体的な対策手順

4 適用範囲

(1) 組織範囲

本基本方針が適用される組織は、連合会におけるすべての組織とする。

(2) 人的範囲

本基本方針が適用される人的範囲は、連合会に所属する全ての役員、職員、審査委員、嘱託員及び臨時職員とする。

(3) 情報資産の範囲

本基本方針が対象とする情報資産は、連合会が所有する全ての情報資産とする。

5 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) 部外者の侵入、不正アクセス、ウイルス攻撃、業務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、無許可ソフトウェ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業務の停止等

6 職員等の遵守義務

役員、職員、審査委員、嘱託員及び臨時職員（以下「職員等」という。）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5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

連合会の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

連合会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、通信回線等及び職員等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、職員等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

情報資産を様々な脅威から適切に保護するため、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。

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。その結果に応じ是正処置及び予防処置を実施する。

9 情報セキュリティポリシーの見直し

連合会は情報セキュリティポリシーが引き続き適切、妥当、有効であることを確実にするために、あらかじめ定めた間隔（少なくとも年1回）で情報セキュリティポリシーの見直しを情報セキュリティ委員会で実施する。また、情報セキュリティ監査及び自己点検の結果、情報セキュリティ委員会の判断により、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も情報セキュリティポリシーを見直す。

1 0 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。

1 1 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連合会の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。

以上

平成22年4月1日

鹿児島県国民健康保険団体連合会

理事長 本田 修一