北海道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１９年８月６日広域連合長決裁

序　北海道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

北海道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。）は、本広域連合が所掌する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、体系的かつ具体的に取りまとめたものである。

情報セキュリティポリシーは、本広域連合が所掌する情報資産に携わる職員、委託事業者等にも浸透、普及、定着されるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティ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」と情報資産を取巻く状況の変化に依存する部分「情報セキュリティ対策基準」の２層に分けて構成する。（下表参照）

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すべてのネットワーク及び情報システムに共通の情報セキュリティ対策の基準

北海道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

本広域連合は、業務の執行に当たり、市町村から後期高齢者医療制度の被保険者となる７５歳以上の高齢者等に係る住基情報や所得情報の提供を受けることとなるなど、重要かつ膨大な個人情報を取り扱うため、外部への漏えい等が発生した場合には極めて重大な結果を招くこととなる。

したがって、取り扱う情報を様々な脅威から防御することは、被保険者等の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが本広域連合に対する被保険者等からの信頼の維持向上に寄与するものである。

本基本方針は、被保険者等が安心・信頼して後期高齢者医療を受けることができるようにするとともに、本広域連合における継続的かつ安定的な行政事務の執行を確保するために、本広域連合が実施する情報セキュリティ対策に関して基本的な事項を定めることを目的とするものである。

2　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（ハードウエア及びソフトウエア）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)　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。

(4)　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。

(5)　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。

(6)　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。

3　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、サービス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、無許可ソフトウエ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　適用範囲

(1)　機関の範囲

本基本方針が適用される機関は、本広域連合のすべての執行機関（広域連合長、選挙管理委員会及び監査委員）及び議会事務局とする。

(2)　情報資産の範囲

本基本方針が対象とする情報資産は、本広域連合が管理し、及び保有する次に掲げるものとする。ただし、本広域連合を構成する市町村において取り扱われるものを除く。

ア　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

イ　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。）

ウ　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

5　職員の遵守義務等

本基本方針が適用される機関に属するすべての職員（特別職、非常勤職員及び臨時職員を含む。以下同じ。）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本基本方針及びこれに基づく情報セキュリティ対策基準（以下「情報セキュリティポリシー」と総称する。）並びに情報セキュリティ実施手順を遵守しなければならない。

また、本広域連合から委託を受けて情報資産を取り扱う事業者等に対しても、契約を通じて、又は別途取り決めを行うことにより、情報セキュリティポリシー並びに情報セキュリティ実施手順を遵守させるための措置を講じるものとする。

6　情報セキュリティ対策

上記３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

本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し、管理するための組織体制を確立し、その役割、責任等を定める。

(2)　情報資産の分類と管理

本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)　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。

(4)　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。

(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。

7　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。

8　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。

9　情報セキュリティ対策基準の策定

上記６、７及び８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。

10　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本広域連合の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。

附 則

この基本方針は、平成１９年８月６日から施行する。