群馬県後期高齢者医療広域連合
情報セキュリティポリシー
（抜粋）

第１章　情報セキュリティ基本方針

１．目的

群馬県後期高齢者医療広域連合（以下「広域連合」という。）は、高齢者の医療の確保に関する法律（昭和５７年法律第８０号）に基づき、被保険者の資格の管理に関する事務や医療給付に関する事務、保険料の賦課に関する事務、保健事業に関する事務等を遂行する。

これらの事務の遂行に当たっては、住民の個人情報をはじめとする、重要な情報を取り扱う必要があり、その適正な管理には十分な対策を講ずる必要がある。

群馬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「情報セキュリティポリシー」という。）は、広域連合の情報資産の機密性、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の基本方針と基準を定めることを目的とする。

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及び通信回線、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）　情報資産

ネットワーク、情報システム、情報システムに関する施設・設備、情報システムで取り扱う情報及びシステム関連文書等をいう。

（４）　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。

（５）　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。

（６）　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。

（７）　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。

（８）　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。

（９）　関係市町村

広域連合を組織する群馬県内の市町村をいう。

（10） 関係所管部局

次に掲げる事務を行う関係市町村の部局をいい、支所等において当該事務を行う場合にあっては当該支所等を含むものとする。

（ア） 保険料の徴収の事務及び被保険者の便益の増進に寄与するものとして高齢者の医療の確保に関する法律施行令（平成１８年政令第２９４号）で定める事務

（イ） 群馬県後期高齢者医療広域連合規約（平成１９年2月１９日群馬県指令市第２１５－１号群馬県知事許可。以下「広域連合規約」という。）第４条ただし書に掲げる事務

（ウ） 広域連合規約第４条に掲げる事務のうち、広域連合との委託契約等に基づき行う事務

（エ） （ア）から（ウ）までに掲げる事務に係る情報システムの開発及び運用等に関する事務及び関係市町村の情報セキュリティの運用に関する事務

３．対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

（１） 意図的な脅威

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、サイバー攻撃をはじめとする部外者の侵入、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、重要情報の詐取、内部不正等

（２） 偶発的な脅威

（ア） 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、外部委託管理の不備、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

（イ） 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

（ウ） 電力供給の途絶、通信の途絶、水道供給の途絶等の提供サービスの障害からの波及等

（３） 自然災害等の脅威

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） 行政機関の範囲

本情報セキュリティポリシーが適用される行政機関は、広域連合長の事務部局（以下「広域連合事務局」という。）、広域連合の議会の事務部局（以下「広域連合議会事務局」という。）、広域連合の行政委員会及び行政委員の事務部局（以下「広域連合行政委員会等事務局」という。）、関係市町村の関係所管部局とする。

（２） 情報資産の範囲

本情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。

（ア） 広域連合が保有する情報資産

① 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

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

（イ） 関係市町村の庁舎内の情報資産

① 広域連合又は関係市町村が保有する情報システムやネットワークに接続される情報資産のうち、広域連合側のセグメントに設置されるネットワーク機器、情報システム及びこれらに関する設備、電磁的記録媒体

② 広域連合規約第４条に掲げる広域連合の事務として取り扱う情報（印刷した文書も含む。）

③ 前記①項に掲げる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．職員等の遵守義務

広域連合及び関係市町村の関係所管部局の職員、非常勤職員及び臨時職員（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。

６．情報セキュリティ対策

前記３項の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

（１） 組織体制

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

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、建物等、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

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（内部監査を含む。）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

前記６項、７項及び８項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。

なお、情報セキュリティ対策基準は、公に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おそれがあることから非公開とする。

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。