石川県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１日　策定

令和 元 年９月１日　一部改定

令和７年１２月１日　一部改定

石川県後期高齢者医療広域連合

○　石川県後期高齢者医療広域連合情報セキュリティ基本方針

（目次）

構成

この情報セキュリティポリシーは、情報セキュリティを確保するための統一的な対策を定めるものであり、一定の普遍性を備えた石川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及び情報資産を取り巻く状況の変化に依存する石川県後期高齢者医療広域連合情報セキュリティポリシー対策基準、対策基準を具体的なシステムやその取扱い手順等に展開して個別の実施事項を定める石川県後期高齢者医療広域連合情報セキュリティポリシー実施手順で構成する。

注意

石川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対策基準及び実施手順は、実施するセキュリティ対策を具体的に記述してあるため、外部からの攻撃の参考になり得ることから、取扱注意とする。

石川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

（趣旨）

第１条　この石川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（以下「基本方針」という。）は、情報資産の機密性（権限のない者への重要な情報の漏えいを防止することをいう。）、完全性（情報の改ざん、破壊による被害を防止することをいう。）及び可用性（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をいう。）を維持し、想定される脅威から広域連合が管理する情報資産を適切に保護するため、情報セキュリティに対する基本的な指針を定めるものとする。

（定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（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（ハードウェア及びソフトウェア）をいう。

（２）　情報システム　コンピュータ、ネットワーク及び電磁的記憶媒体で構成され、情報処理を行う仕組みをいう。

（３）　情報　情報システム及びネットワークで扱うデータをいう。

（４）　情報資産　情報、情報システム及びネットワークをいう。

（５）　情報セキュリティ　想定される脅威から情報資産の機密性、完全性及び可用性を維持することをいう。

（６）　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。

（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)　マイナンバー利用事務系（個人番号利用事務系）　個人番号利用事務（社会保障、地方税若しくは防災に関する事務）をいう。

(11)　基幹系　後期高齢者医療広域連合電算処理システムに関わる専用回線に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

(12)　情報系　インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(13)　無害化通信　インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確

保された通信をいう。

（想定される脅威）

第３条　この基本方針において、保護すべき情報資産に対して想定される主な脅威とは、次に掲げるものをいう。

（１）　不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入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）　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、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

（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）　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

（５）　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

（適用範囲）

第４条　この基本方針が対象とする行政機関および情報資産の適用範囲は、次に定めるところによる。

（１）　行政機関の範囲　石川県後期高齢者医療広域連合事務局、議会、選挙管理委員会、公平委員会及び監査委員

（２）　情報資産の範囲

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

（職員の義務）

第５条　臨時・非常勤職員等（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。

（情報資産の分類）

第６条　広域連合は、情報資産を重要度に応じて分類し、その重要度に応じた情報セキュリティ対策を講ずるものとする。

（情報セキュリティ対策の種類）

第７条　広域連合は、情報資産を脅威から保護するため、次に掲げる情報セキュリテ

ィ対策を講ずるものとする。

（１）　組織体制

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する全庁的な組織体制を確立する。

（２）　情報資産の分類と管理

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実施する。

（３）　情報システム全体の強靭性の向上

情報システム全体に対し、次の対策を講じる。

①　マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

（４）　物理的セキュリティ対策

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、情報システムを設置する施設への不正な立ち入り、情報資産の損傷及び破壊等から保護するための物理的な対策を講じる。

（５）　人的セキュリティ対策

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、職員等に対して情報セキュリティの重要性を認識させるための十分な教育及び啓発を行う等の人的な対策を講じる。

（６）　技術的セキュリティ対策

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情報資産を保護するための技術的対策を講じる。

（７）　運用におけるセキュリティ対策

誤操作等から情報資産を保護するためのシステムの運用、ネットワーク監視及び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。

（８）　緊急時におけるセキュリティ対策

情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（９）　業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサー

ビスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

(10)　評価・見直し

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し、運用改善を行い情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、情報セキュリティポリシーの見直しを行う。

（情報セキュリティポリシー対策基準）

第８条　広域連合は、基本方針に基づき、想定される脅威に対応するため、情報資産の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ポリシー対策基準（以下「対策基準」という。）を別に定める。

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。

（情報セキュリティ実施手順の策定）

第９条　広域連合は、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。

（最高情報セキュリティ責任者の設置）

第１０条　広域連合は、広域連合における全ての情報資産のセキュリティ管理を統括するため、最高情報セキュリティ責任者（ＣＩＳＯ:Chief Information Security Officer、以下「ＣＩＳＯ」という。）を置く。

２　ＣＩＳＯは、事務局長をもって充てる。

３　ＣＩＳＯは、広域連合における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権及び責任を有する。

４　ＣＩＳＯは、情報セキュリティインシデントに対処するための体制（ＣＳＩＲＴ:Computer Security Incident Response Team、以下「ＣＳＩＲＴ」という。）を整備し、役割を明確化する。

（統括情報セキュリティ責任者の設置）

第１１条　広域連合は、ＣＩＳＯを補佐し、情報セキュリティを確保するため、統括情報セキュリティ責任者を置く。

２　統括情報セキュリティ責任者は、事務局次長をもって充てる。

３　統括情報セキュリティ責任者は、広域連合の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有し、情報セキュリティに関する権限及び責任を有する。

４　統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。
５　統括情報セキュリティ責任者は、広域連合の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、ＣＩＳＯ の指示に従い、ＣＩＳＯが不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。
６　統括情報セキュリティ責任者は、本広域連合の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。
７　統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。
８　統括情報セキュリティ責任者は、緊急時にはＣＩＳＯ に早急に報告を行うとともに、回復のための対策を講じなければならない。

（情報セキュリティ責任者の設置）
第１２条　広域連合は、職員が情報資産の適切な利用を行うため、各所属に情報セキュリティ責任者を置く。
２　情報セキュリティ責任者は、各課の課長をもって充てる。
３　情報セキュリティ責任者は、所属内の情報資産に対して、情報セキュリティに関する包括的な権限及び責任を負う。
４　情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。
５　情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員、非常勤職員及び臨時職員（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

（情報セキュリティ管理者の設置）
第１３条　広域連合は、情報資産の適切な管理を行うため、情報セキュリティ管理者を置く。
２　情報セキュリティ管理者は、各課の課長補佐若しくは課長が指定した職員をもって充てる。ただし、課員が少ない課の場合は課長が兼務してもよいものとする。
３　情報セキュリティ管理者は、その所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。
４　情報セキュリティ管理者は、その所掌する課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情

報セキュリティ責任者、統括情報セキュリティ責任者及びＣＩＳＯ へ速やかに報告を行い、指示を仰がなければならない。

（情報システム管理者の設置）

第１４条　広域連合は、情報資産の適切な開発及び管理を行うため、情報システム管理者を置く。

２　情報システム管理者は、情報システムを開発又は情報資産を管理する情報セキュリティ責任者をもって充てる。

３　情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

４　情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

５　情報システム管理者は、対策基準に基づき、開発又は管理する情報資産を保護するため、具体的な手法及び手順を記述した情報セキュリティ実施手順（以下「実施手順」という。）を設計書及び運用手順書等に定めなければならない。

（情報システム担当者の設置）

第１５条　広域連合は、情報資産の適切な開発及び管理に関する実施体制を明確にするため、各情報システムに情報システム担当者を置く。

２　情報システム管理者は、所属内から情報システム担当者を指定するものとする。

３　情報システム担当者は、情報システム管理者の指示に従い、情報システムの開発、設定の変更、運用、更新等の作業を行わなければならない。

（情報セキュリティ委員会等の設置）

第１６条　広域連合は、情報セキュリティ対策に関して、広域連合で統一した対応を行うため、情報セキュリティ委員会（以下「委員会」という。）を置く。

２　情報セキュリティ委員会は、本広域連合における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない

３　委員会の組織及び運営については、別に定める。

（情報セキュリティ監査統括責任者）

第１７条　広域連合は、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策情報について監査を行うため、情報セキュリティ監査統括責任者を置く。

２　情報セキュリティ監査統括責任者は、事務局次長をもって充てる。

３　情報セキュリティ監査統括責任者は、広域連合の全てのネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について監査を行う権限及び責任を有する。

（兼務の禁止）

第１８条　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

２　監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

（ＣＳＩＲＴの設置・役割）

第１９条　広域連合は、情報セキュリティインシデントに対処するためＣＳＩＲＴを設置する。

２　ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化すること。

３　ＣＩＳＯは、ＣＳＩＲＴに所属する職員を選任し、その中からＣＳＩＲＴ 責任者を置くこと。

また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員を定めること。

４　ＣＩＳＯは、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備すること。

５　ＣＩＳＯによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供すること。

６　情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、総務省、都道府県等へ報告すること。

７　情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

８　情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行うこと。

（情報セキュリティに関する監査の実施）

第２０条　情報セキュリティ監査統括責任者は、基本方針及び対策基準が遵守されていることを検証するため、定期的又は必要に応じて情報セキュリティ監査を実施するものとする。

（情報セキュリティに関する自己点検の実施）

第２１条　統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システム並びに特定個人情報の管理状況について、定期的又は必要に応じて自己点検を実施するものとする。

（改定）

第２２条　統括情報セキュリティ責任者は、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技術の進歩及び情報セキュリティに関する社会状況の変化に迅速かつ的確に対応するため新たに対策が必要になった場合には、必要に応じて基本方針及び対策基準の見直しを行

うものとする。

附　則

この基本方針は、平成１９年８月１日から施行する。

附　則

この基本方針は、令和元年９月１日から施行する。

附　則

この基本方針は、令和７年１２月１日から施行する。