情報セキュリティポリシー

事務局編

議会編

監査委員編

選挙管理委員会編

令和８年３月
千葉県後期高齢者医療広域連合

情報セキュリティポリシー

事務局編

事務局編

■新規制定／改定一覧

版数	制定／改定年月日	制定／改定内容	承認者	作成部署
初版	平成 19 年 11 月 12 日	新規制定	副広域連合長	業務課
2版	改訂:平成 28 年1 月1 日	行政手続における特定の個人を識別するための番号の利用等に関する法律の実施に伴う全部改定	広域連合長	総務課
3版	改訂:平成 29 年2 月1 日	情報提供ネットワークシステムを通じた情報連携開始に伴う安全管理措置に準拠させるための一部改定	事務局長	総務課
4版	改訂：平成31 年2 月1 日	認証方式に生体認証を追加するための一部改訂	事務局長	総務課
5版	改訂：令和 2 年4 月1 日	外部セキュリティ監査の指摘事項へ対応するための一部改定	事務局長	総務課
6版	改訂:令和 5 年 4 月 1 日	個人情報保護法の適用開始に伴う改訂	事務局長	総務課
7版	改訂:令和 6 年 4 月 1 日	標準システムのクラウド化に伴う改訂	事務局長	総務課
8版	改訂:令和 6 年 12 月 1 日	クラウドサービス利用に対する対応、業務委託先管理の強化、情報資産の分類の細分化、サイバーレジリエンスの強化等に伴う改訂	事務局長	総務課
9版	改訂:令和 8年 3 月 31 日	「地方公共団体におけるサイバーセキュリティを確保するための方針の策定又は変更に関する指針」への対応に伴う改訂	事務局長	総務課

事務局編

情報セキュリティ基本方針

目次

1　目 的

本基本方針は、広域連合が保有する情報資産の機密性、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

この情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、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）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。

（５）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。

（6）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。

（7）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。

（8）個人情報

個人情報の保護に関する法律（平成１５年法律第５７号）第２条第１項に規定する「個人情報」（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律２７号。以下「番号法」という。）第２条第９項に規定する「特定個人情報」を含む。）及び死者に関する情報であって個人情報の保護に関する法律第２条第１項各号のいずれかに該当するものをいう。

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）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、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

4　適用範囲

（1）行政機関の範囲

本基本方針が適用される行政機関は、広域連合の事務局とする。

ただし、情報セキュリティポリシーの対象となる業務を外部に委託する場合には、別途、情報セキュリティポリシーに準拠した内容の外部委託契約を締結する。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

5　職員等の遵守義務

本広域連合に属する職員及び会計年度任用職員（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

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

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行う。

（3）物理的セキュリティ

広域連合内のサーバ、通信回線、端末等の管理について、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）外部サービス（クラウドサービス）の利用

外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定等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。

（８）情報の保管期間

情報システムで取り扱う情報は、法令に定められた保管期間に準じて保管する。また、情報システムへのアクセスログを記録し、その記録を最低５年保管する。

（９）事故の予防と対応

広域連合は、情報セキュリティポリシーの遵守により、情報漏えい事故等の発生の予防に努める。万一、事故が発生した場合には、その

事実を速やかに公表し、再発防止策を含む適切な対策を速やかに講じる。

7　情報セキュリティ監査及び自己点検の実施

（1）情報システムの適正な運用とその有効性を維持するために、毎年１回内部監査又は自己点検を実施する。ただし、高度な技術を要する監査が必要な場合は、外部の専門家による外部監査を導入する。

（2）広域連合は、監査結果又は自己点検結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じる。

8　情報セキュリティポリシーの見直し

（1）情報セキュリティポリシーは、以下のような場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで改訂する。

（ア）ＩＴ技術の発展及び情報セキュリティポリシーの整合性を維持する必要がある場合

（イ）社会環境の変化及び情報セキュリティポリシーの整合性を維持する必要がある場合

（ウ）法令、標準規格等と情報セキュリティポリシーの整合性を維持する必要がある場合

（2）改訂された情報セキュリティポリシーは、職員等に十分周知する。なお、改訂後即時に情報セキュリティ基本方針は住民へ公表する。

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、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。策定した情報セキュリティ実施手順を利用者に周知の上、常に利用可能な状態におく。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。

１１ 事業計画の策定

情報セキュリティ対策実施手順として、情報セキュリティに関する研修・訓練・教育、当情報セキュリティポリシーの遵守状況の点検、監査の実施について年度ごとに定めた、情報セキュリティ対策における事業計画を策定する。

情報セキュリティポリシー

議会編

■新規制定／改定一覧

版数	制定／改定年月日	制定／改定内容	承認者	作成部署
初版	令和 8 年 3 月 31 日	新規策定	議長	議会事務局

議会編

情報セキュリティ基本方針

目次

1　目的

本基本方針は、千葉県後期高齢者医療広域連合議会（以下「議会」とする。）が保有する情報資産の機密性、完全性及び可用性を維持するため、議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

この情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、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）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対策基準をいう。なお、情報セキュリティ対策基準は、情報システムの利用状況等を考慮し、必要に応じて策定する。

（5）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。

（6）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。

（7）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）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、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

4　適用範囲

（1）行政機関の範囲

本基本方針が適用される行政機関は、議会とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

5　職員等の遵守義務

議会事務局職員及び議員（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を遵守しなければならない。

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、情報システムの利用状況等を考慮し、必要に応じて以下の情報セキュリティ対策を講じる。

（1）組織体制

議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

議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実施する。

（3）物理的セキュリティ

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、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。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

情報セキュリティポリシー

監査委員編

監査委員編

■新規制定／改定一覧

版数	制定／改定年月日	制定／改定内容	承認者	作成部署
初版	令和 8 年 3 月 31 日	新規策定	事務局長	監査委員事務局

監査委員編

情報セキュリティ基本方針

目次

議会編

情報セキュリティ基本方針

1　目的

本基本方針は、千葉県後期高齢者医療広域連合監査委員（以下「監査委員」とする）が保有する情報資産の機密性、完全性及び可用性を維持するため、監査委員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

この情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、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）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対策基準をいう。なお、情報セキュリティ対策基準は、情報システムの利用状況等を考慮し、必要に応じて策定する。

（5）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。

（6）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。

（7）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）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、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

4　適用範囲

（1）行政機関の範囲

本基本方針が適用される行政機関は、監査委員とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

5　職員等の遵守義務

監査委員事務局職員及び監査委員（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を遵守しなければならない。

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、情報システムの利用状況等を考慮し、必要に応じて以下の情報セキュリティ対策を講じる。

（1）組織体制

監査委員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

監査委員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）物理的セキュリティ

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、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。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

情報セキュリティポリシー

選挙管理委員会編

選挙管理委員会編

■新規制定／改定一覧

版数	制定／改定年月日	制定／改定内容	承認者	作成部署
初版	令和 8 年 3 月 31 日	新規策定	事務局長	選挙管理委員会事務局

選挙管理委員会編

情報セキュリティ基本方針

選挙管理委員会編

目次

1　目的

本基本方針は、千葉県後期高齢者医療広域連合選挙管理委員会（以下「選挙管理委員会」とする）が保有する情報資産の機密性、完全性及び可用性を維持するため、選挙管理委員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

この情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、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）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対策基準をいう。なお、情報セキュリティ対策基準は、情報システムの利用状況等を考慮し、必要に応じて策定する。

（5）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。

（6）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。

（7）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）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、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

4　適用範囲

（1）行政機関の範囲

本基本方針が適用される行政機関は、選挙管理委員会とする。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

5　職員等の遵守義務

選挙管理委員会事務局職員及び選挙管理委員（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を遵守しなければならない。

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、情報システムの利用状況等を考慮し、必要に応じて以下の情報セキュリティ対策を講じる。

（1）組織体制

選挙管理委員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

選挙管理委員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実施する。

（3）物理的セキュリティ

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、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。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。