

## 長崎県市町村職員共済組合個人情報保護方針

長崎県市町村職員共済組合（以下「組合」という。）は、「個人情報の保護に関する法律」に基づき、以下の方針により、組合が保有する個人情報の保護に努めます。

### 1 法令の遵守

組合は、組合が保有する個人情報の保護に関する法令等を遵守します。

### 2 組織及び体制

組合は、個人情報保護管理者を設置し、個人情報の適正な管理を行うとともに職員等に対し、個人情報の保護及び適正な管理方法について研修を実施し、個人情報の適正な取扱いを徹底します。

### 3 個人情報の取得と利用

組合は、個人情報の取得にあたり、その利用目的、利用方法等を明らかにし、取得した個人情報はその範囲内で業務遂行上必要な場合に限り利用します。

### 4 個人データの管理

組合は、個人データの正確性を保持し、また個人データの漏えい、滅失、き損等を防止するための適正な対策を講じます。

### 5 個人データの第三者提供

組合は、法令に基づく場合等を除き、本人の同意を得ることなしに、個人データを第三者に提供しません。

### 6 保有個人データの開示、訂正等、利用停止等

組合は、本人が自己の個人データについて開示、訂正等又は利用停止等の請求があったときは適切に対応します。

### 7 継続的改善

組合は、適切な個人情報の保護を維持するため、常に個人情報の取得及び管理の状況等を把握し、必要に応じて個人情報の保護のための措置を改善します。

平成19年5月1日

(個人情報の取扱いに関する問合せ先)  
長崎県市町村職員共済組合 総務課  
電話番号095-827-3137

令和7年9月1日一部改正  
(平成29年5月30日適用)

長崎県市町村職員共済組合

長崎県市町村職員共済組合個人番号及び特定個人情報の適正な取扱いに関する基本方針

(平成28年6月20日制定)

長崎県市町村職員共済組合（以下「組合」という。）は、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に基づき、以下の方針により、組合が保有する個人番号及び特定個人情報（以下「特定個人情報等」という。）を安全かつ適正に取り扱います。

1 法令及びガイドライン等の遵守

組合は、特定個人情報等に関する法令及び特定個人情報の適正な取扱いに関するガイドライン（事業者編）等を遵守します。

2 安全管理措置に関する事項

組合は、特定個人情報等の漏えい、滅失又は毀損の防止等、特定個人情報等の管理のために、必要かつ適切な安全管理措置を講じます。

3 特定個人情報等の収集、保管、利用、提供及び廃棄

組合は、特定個人情報等の具体的な取扱いを定める取扱規程等を策定し、当該規程等にしがって、特定個人情報等の収集、保管、利用、提供及び廃棄を適切に実施します。

4 継続的改善

組合は、特定個人情報等の安全かつ適切な取扱いを維持するため、常に特定個人情報等の収集及び管理の状況等を把握し、必要に応じて特定個人情報等の適正な取扱いのための措置を改善します。

平成28年6月20日  
長崎県市町村職員共済組合

# 長崎県市町村職員共済組合情報セキュリティ基本方針

平成28年6月20日制定  
令和5年2月27日一部改正  
令和6年6月1日一部改正

長崎県市町村職員共済組合情報セキュリティ基本方針（平成20年7月8日制定）の全部を改正する。

## 1 目的

本基本方針は、長崎県市町村職員共済組合（以下「組合」という。）が保有する情報資産を様々な脅威から防御し、機密性、完全性及び可用性を維持するために必要な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) 情報資産

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、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、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

### (2) 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その構成機器（ハードウェア及びソフトウェア）をいう。

### (3) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

### (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) マイナンバー事務系

個人番号利用事務又は個人番号関係事務に関わる情報システム及びデータをいう。

(10) インターネット接続系

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。

(11) 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。

### 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、ウイルス攻撃及びサービス不能攻撃等のサイバー攻撃並びに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、重要情報の詐取及び内部不正等
- (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及び機器故障等の非意図的な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情報システム運用の機能不全等
- (5) 電力供給、通信及び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) 適用対象者の範囲

本基本方針が適用される者は、組合業務従事者とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、2 (1) のとおりとする。

### 5 職員等の遵守義務

職員、非常勤職員、派遣職員及び臨時職員（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

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

組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組織体制を確立する。

### (2) 情報資産の分類と管理

組合の情報資産を機密性、完全性及び可用性により重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

### (3) 情報システム全体の強靱性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、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、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

サーバ機器等、サーバ室、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。

### (5) 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。

### (6) 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及び不正アクセス対策等の技術的対策を講じる。

### (7) 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、業務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切に対応するため、緊急時対応計画を策定する。

### (8) 業務委託と外部サービスの利用

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。

外部サービスを利用する場合には、利用に係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。

(9) 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。

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。

情報セキュリティ実施手順は、公にすることにより組合の業務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

この改正は、令和5年4月1日から施行する。

この改正は、令和6年6月1日から施行する。