福井坂井地区広域市町村圏事務組合情報セキュリティ基本方針

福井坂井地区広域市町村圏事務組合

改訂履歴

年月日	改定内容等
令和８年４月１日	初版策定（令和８年４月１日施行）

福井坂井地区広域市町村圏事務組合情報セキュリティ基本方針

1　目的

福井坂井地区広域市町村圏事務組合情報セキュリティ基本方針は、本組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、地方自治法第２４４条の６に基づき、本組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

（１）　情報セキュリティ

情報資産の機密を保持し、情報資産の正確性及び完全性を維持し、並びに定められた範囲での利用可能な状態を維持することをいう。

（２）　情報資産

情報システム及び情報通信ネットワークの開発及び運用管理に係るファイル（データを記録している電磁的記録をいう。）及びドキュメント（情報システムの設計書、操作手引書、プログラムリスト、ネットワーク構成図その他のコンピュータの運用に関する文書をいう。）、情報システム及び情報通信ネットワークで取り扱うデータに係るファイル並びに情報システム及び情報通信ネットワークを構成する機器をいう。

（３）　情報セキュリティポリシー

福井坂井地区広域市町村圏事務組合情報セキュリティ管理規程（令和８年訓令甲１号。）及び下記９に規定する情報セキュリティ対策基準をいう。

（４）　情報セキュリティ対策

情報セキュリティを確保するために実施する各種の対策をいう。

（５）　機密性

情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

（６）　完全性

情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

（７）　可用性

許可された利用者が必要なときに情報アクセスできることを確実にすること。

（８）　コンピュータ処理

コンピュータを使用して行われる情報の入力、蓄積、編集、加工、修正、更新、検索、消去、出力又はこれらに類する処理をいう。

（９）　電磁的記録

電子的方式、磁気的方式その他人の知覚によっては認識することができない方

式で作られた記録をいう。

(10)　データ

コンピュータ処理に係る情報で電磁的記録媒体に記録されているものをいう。

(11)　情報システム

コンピュータ、電気通信回線等により情報処理の業務を一体的に行う仕組みをいう。

(12)　情報通信ネットワーク

コンピュータを相互に接続するための通信網並びにこれを構成するハードウェア及びソフトウェアをいう。

(13)　管理者

福井坂井地区広域市町村圏事務組合規約（昭和 45 年福井県指令地第 371 号。以下「規約」という。）第 7 条第 1 項に規定する管理者をいう。

(14)　副管理者

規約第 7 条第 3 項に規定するもののうち管理者の属する市町の副市町長の職にある者をいう。

(15)　職員等

規約第 10 条に規定する職員、非常勤職員、臨時職員等をいう。

3　適用範囲

本基本方針が適用される範囲は、管理者、副管理者、職員等並びに本組合の保有する情報資産とする。

4　対象とする脅威

情報資産に対する脅威として、次の各号に掲げる脅威を想定し、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情報システム運用の機能不全等

（5）　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

5　職員等の遵守義務

職員等は、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するとともに、福井坂井地区広域市町村圏事務組合個人情報の保護に関する法律施行条例（令和５年条例第２号）その他の関連する法令等を遵守し、情報資産を適切に管理しなければならない。

6　情報セキュリティ対策

上記４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実施する。

（１）　組織体制

本組合の保有する情報資産について、情報セキュリティ対策を推進する本組合の全体的な組織体制を確立する。

（２）　情報資産の分類と管理

本組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）　物理的セキュリティ

サーバ、管理区域、通信回線及び通信回線装置並びに職員等の利用する端末や電磁的記録媒体等の管理について、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

コンピュータ及びネットワークの管理、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事項の確認、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正に対処するため、緊急時対応計画を策定する。

（７）　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。

（８）　評価・見直し

情報セキュリティポリシーの遵守事項を検証するため、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。情報セキュリティの見直しが必要な場合は、適宜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

情報セキュリティポリシーの遵守事項を検証するため、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となった場合には、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。

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組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。