福山地区消防組合情報セキュリティ基本方針

福山地区消防組合
福山地区消防組合監査委員

２０２６年（令和８年）３月３１日共同策定

第１　目的

福山地区消防組合及び福山地区消防組合監査委員（以下、本組合等という。）が取扱う情報資産には、個人情報や行政運営上の情報等が漏えい、改ざん及び破壊等により、個人や組織に重大な被害を引き起こすものがある。これら情報資産を災害、事故、人的脅威等から守ることは、住民のプライバシー及び財産等の保護、また、正確、安全かつ継続的に住民サービスを行う上でも必要不可欠である。

このため、本組合等の情報資産について、次の情報セキュリティを確保する必要がある。

１　機密性

許可された者のみが、情報にアクセスできることを確実にすること。

２　完全性

情報及び処理方法の正確さと完全さ（抜け、漏れのないこと）を確保すること。

３　可用性

必要な時に情報及び関連する資産にアクセスできること。

本方針は、本組合等の取扱う情報資産の機密性、完全性及び可用性を維持するため、情報資産及びそれを取扱う情報システムに対するすべての情報セキュリティ対策の基本となるものである。

第２　定義

この方針において、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

コンピュータを相互に接続するための通信回線網及びその構成機器（ハードウェア及びソフトウェア）で構成され、処理を行う仕組みをいう。

２　情報システム

情報処理又は通信を行うコンピュータ（ハードウェア及びソフトウェア）、記録媒体及びネットワークをいう。

３　情報資産

職員等が職務上作成、又は取得したすべての情報（記録媒体に記録された情報、紙等に出力された情報、作成途中のファイル並びに一時的に作成するファイルを含む。）をいう。

４　記録媒体

ＣＤ－Ｒ、ＤＶＤ－Ｒ、ＵＳＢメモリ、ＨＤＤ、ＳＳＤ等の情報を記録するための装置をいう。

５　アクセス

情報システムを通じて情報資産の参照、更新を行うことをいう。

６　職員等

本組合等が保有する情報システム、情報資産に関わる一般職の職員及び特別職の職員並びに本組合等の情報資産を取扱うすべての者（外部委託事業者は除く。）をいう。

７　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８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。

８　情報セキュリティインシデント

情報セキュリティに関する障害・事故及びシステム上の欠陥をいう。

９　約款による外部サービス

約款への同意又は簡易な登録等により、利用可能となるインターネット上で提供されるサービスをいう。

第３　対象機関等

本方針の対象となる機関は、次のとおりとする。

１　福山地区消防組合

２　福山地区消防組合監査委員

第４　対象範囲

本方針の対象範囲は、対象機関において保有する情報資産及び情報資産を取扱う情報システムとする。

なお、特殊性を持つシステムにおいては、本方針に加え、別途方針を定めることができる。ただし、本方針の水準を下回ってはならない。

第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を認識し、本方針を遵守しなければならない。

第６　管理体制

本組合等の情報資産について、情報セキュリティ対策を適切に推進、管理するための体制を確立する。

第７　情報資産への脅威

情報セキュリティ対策を講じるに当たって、情報資産に対する次の脅威に十分に考慮しなければならない。

１　人的脅威

誤操作、持ち出し、不正行為、パスワードの不適切管理等

２　物理的脅威

侵入、破壊、故障、停電、災害等

３　技術的脅威

不正アクセス、盗聴、コンピュータウイルス、改ざん、消去等

第８　情報資産の分類

情報資産はその重要性に基づいて分類し、それらの脅威や脆弱性に応じた情報セキュリ

ティ対策を施し管理する。

第９　情報セキュリティ対策

情報資産への脅威・脆弱性を十分に考慮し、次の情報セキュリティ対策を講じなければならない。

なお、遵守すべき行為及び判断の基準は、「福山市情報セキュリティポリシー」における「情報セキュリティ対策基準」の例による。

１　人的セキュリティ対策

情報資産を取扱うに当たって、職員等の権限や責任及び遵守すべき事項を定め、それらが遵守されるように十分な教育、啓発及び訓練を行うこと。

２　物理的セキュリティ対策

情報資産の取扱い場所及び情報システムの設置場所への不正な立ち入りや機器の破損等を防ぐために物理的な対策を講じること。

３　技術的セキュリティ対策

情報資産への不正アクセス等を防ぐために、アクセス制御やコンピュータウイルス対策等の技術的な対策を講じること。

４　運用面のセキュリティ対策

情報セキュリティ基本方針を確実に運用していくために、侵害時及び緊急時の対策等の運用面での対策を講じること。

第１０　情報セキュリティ対策基準

情報セキュリティ対策として遵守すべき行為及び判断の基準は「福山市情報セキュリティポリシー」における「情報セキュリティ対策基準」の例による。

第１１　情報セキュリティ実施手順

情報セキュリティ対策を実施するため、具体的な取扱方法については、「福山市情報セキュリティポリシー」における「情報セキュリティ実施手順」の例による。

第１２　点検・監査

情報セキュリティ基本方針の遵守状況について、点検及び監査を定期的かつ継続的に実施する。

第１３　評価・見直し

情報セキュリティ対策の点検・監査の結果及び情報セキュリティを取り巻く環境の変化等を踏まえ、適宜、情報セキュリティ基本方針の評価及び見直しを実施する。

第１４　違反に対する対応

情報セキュリティ基本方針に違反した者に対しては、厳格な対応を行う。