福山市議会情報セキュリティ基本方針

２０２６年（令和８年）３月１３日制定

福　山　市　議　会

福山市議会情報セキュリティ基本方針

情報セキュリティ基本方針

情報セキュリティ基本方針

第１　目的

本市議会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、プライバシー及び財産等の保護、また、正確、安全かつ継続的に議会活動を行う上でも必要不可欠である。

このため、本市議会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状態を確保すること。

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、中断されることなく、情報及び関連する資産にアクセスできる状態を確保すること。

本方針は、本市議会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　情報セキュリティポリシー

本情報セキュリティ基本方針及び情報セキュリティ対策基準のことをいう。

２　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。

３　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。

４　情報資産

議員が職務上作成、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、作成途中の情報並びに一時的に作成する情報を含む。）をいう。

５　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。

６　議員

本市議会の議員をいう。（会派を含む。）

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。

第３　対象範囲

本方針は、本市議会の議員に適用する。

なお、本市議会の議会事務局職員及び議会事務局で使用されるシステムのセキュリティ対策については、福山市情報セキュリティポリシー及び福山市情報セキュリティ実施手順によるものとする。

本方針の対象範囲は、本市議会が保有する情報資産及び情報資産を取扱う情報システム（クラウドサービスを含む。）とする。

なお、特殊性を持つシステムにおいては、情報セキュリティポリシーに加え、別途セキュリティポリシーを定めることができる。ただし、本情報セキュリティポリシーの水準を下回ってはならない。

第４　議員の遵守義務

議員は、情報セキュリティの重要性を認識し、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。

第５　管理体制

本市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６　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７　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８　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る。

なお、遵守すべき行為及び判断の基準は、情報セキュリティ対策基準において示す。

１　人的セキュリティ対策

情報資産を取扱うに当たって、議員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。

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実施する。

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実施する。

４　運用面のセキュリティ対策

情報セキュリティポリシー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実施する。

５　業務委託先及び外部サービスのセキュリティ対策

情報資産の処理を委託する場合は、委託先の情報セキュリティ体制を確認し、契約書にセキュリティ要件を明記し、定期的な監視・監査を実施する。

第９　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として、「情報セキュリティ対策基準」を策定する。

第１０　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「情報セキュリティ実施手順」を策定する。

第１１　点検・監査

情報セキュリティポリシーの遵守状況について、点検及び監査を定期的かつ必要に応じて実施する。

第１２　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、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、リスクを検討した上で、適宜、情報セキュリティポリシーの見直しを実施する。

附　則

この方針は、２０２６年（令和８年）３月１８日から施行する。