秩父市サイバーセキュリティを確保するための方針

１　目的

秩父市サイバーセキュリティを確保するための方針（以下、「方針」という。）は、本市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、 本市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）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。

（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

秩父市情報セキュリティ基本方針に関する規程をいう。

（５）外部要員

情報システム等の開発、管理業務等を委託契約等に戻づいて作業する者。市の公の施設の管理を行う指定管理者を含む。

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）自然の脅威（地震、火災、風水害等）

（２）情報システムの脅威（情報システムの故障、誤動作等）

（３）人的な脅威（不正行為、誤操作等）

４　適用範囲

（１）行政機関の範囲

方針が適用される行政機関は、市長部局、行政委員会、監査委員、議会事務局とする。

（２）情報資産の範囲

方針が対象とする情報資産は、次のとおりとする。

ア 情報システム並びに情報システムの開発、運用及び保守を行うための資料等、情報を管理する仕組み

イ ネットワーク及び情報システムで取り扱う情報（これらを印刷したものを含む。）

５　順守義務

常勤職員（特別職を含む）、会計年度任用職員、臨時的任用職員、行政委員会の委員、監査委員、労働者派遣事業により本市の事務に携わる者（以下「職員等」という。）及び外部要員は、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、以下の情報セキュリティ対策を講ずる。

（１）組織体制

本市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

本市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）情報システム全体の強靭性の向上

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、取り扱う情報資産の分類に応じた対策を講じる。

（４）物理的セキュリティ

サーバ、情報システム室等、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、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。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（クラウドサービス）の利用

ア 業務委託を行う場合には、契約に係る規定を整備し対策を講じる。

イ 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。

（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、適宜情報セキュリティポリシーの見直しを行う。