大井町情報セキュリティ基本方針

１ 目的

大井町情報セキュリティ基本方針（以下「基本方針」という。）は、町が所管する電子情報資産の機密性、完全性及び可用性を確保するため、様々な脅威に対する抑止、予防、検知及び回復について、組織的かつ体系的に取り組むための統一的な方針並びに電子情報資産の安全管理対策を実践するにあたっての基本的な考え方及び方策を定めることを目的とする。

２ 適用範囲

この基本方針は、町が保有する情報資産、情報資産に関する業務に携わる職員及び町の事務事業の委託を受けた者（以下「受託者」という。）に適用する。

３ 用語の定義

（１）情報資産

情報及び情報システムをいう。

（２）情報

情報システムからの出力帳票及び電磁的記録情報をいう。

（３）情報システム

ネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成され、処理を行う仕組みをいう。

（４）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及びその構成機器をいう。

（５）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。

（６）機密性

情報にアクセスすることが認められた者だけがアクセスできることを確実にすることをいう。

（７）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をいう。

（８）可用性

認められた者が必要なときに情報にアクセスできることを確実にすることをいう。

４ 管理体制

情報セキュリティ対策を推進・管理するための組織体制を整備するものとする。

５ 情報資産の分類及び管理

情報資産については、情報の機密性、完全性及び可用性を踏まえた情報資産の分類を行い、その重要性に応じて、適切な管理を行うものとする。

６ 情報セキュリティ対策

情報資産を、故意（盗聴、不正アクセス、改ざん、破壊、窃盗等）、過失（入力ミス、操作ミス等）、災害（火災、地震等）、故障等の脅威から守るため、次に掲げる対策を講ずる。

（１）物理的セキュリティ対策

情報システムの設置場所、情報の保管場所等への不正な立入り、情報資産への損害及び利用の妨害等から保護するための物理的な対策を講ずる。

（２）人的セキュリティ対策

情報セキュリティに関する権限や責任及び遵守すべき事項を定め、職員及び受託者に対する周知及び徹底を図るとともに、十分な教育・啓発が行われるよう必要な対策を講ずる。

（３）技術的セキュリティ対策

情報資産を不正アクセス等から保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術的対策を講ずる。

（４）運用等における対策

情報システムの監視及び情報セキュリティ対策の遵守状況の確認等の運用面の対策を講ずる。

（５）緊急時におけるセキュリティ対策

緊急事態が発生した場合に、迅速かつ適切な対応が可能となるような危機管理対策を講ずる。

７ 情報セキュリティ対策基準の策定

基本方針に基づき、情報セキュリティ対策を実施するに当たっての遵守すべき事項及び判断等の統一的な基準として、情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。 なお、情報セキュリティ対策基準は、公にすることにより本町の行政運営に支障を及ぼすおそれがあることから非公開とする。

８ 情報セキュリティ実施手順の策定

基本方針及び対策基準に基づき、情報セキュリティ対策を具体的に実施するために、情報セキュリティ実施手順（以下「実施手順」という。）を定めるものとする。 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町の行政運営に支障を及ぼすおそれがあることから非公開とする。

９ 法令等の遵守

情報セキュリティ対策を実施するに当たっては、法令等を遵守しなければならない。

１０ 職員及び受託者の義務

職員及び受託者は、情報セキュリティの重要性について共通の認識をもつとともに、業務の遂行において、法令及び情報セキュリティ対策を遵守する義務を負う。

１１ 情報セキュリティ対策に違反した職員及び受託者への対応

情報セキュリティ対策に違反した職員及び受託者については、その重大性、 発生した事案の状況等に応じて厳正に対応する。

１２ 情報セキュリティ監査の実施

情報セキュリティ対策が遵守されていることを検証するため、定期的に監査を実施するものとする。

１３ 評価及び見直し

情報セキュリティ監査の結果等に基づき、基本方針、対策基準、実施手順に定める事項及び情報セキュリティ対策についての評価を定期的に実施するとともに、情報セキュリティを取り巻く状況の変化等に対応して、基本方針、対策基準、実施手順及び情報セキュリティ対策の見直しを実施するものとする。