

Ⅷ 運用管理

1 管理すべき文書

基本方針	情報セキュリティ基本方針
対策基準	情報セキュリティ対策基準
実施手順及び 管理台帳等	共通実施手順書
	業務システム実施手順書
	情報セキュリティ法規制等登録簿
	セキュリティ管理記録一覧表
	情報セキュリティ業務分掌職務権限一覧表
	電子情報資産管理台帳
	セキュリティ区画管理台帳
	インターネットアクセス制御管理台帳
	モデム接続管理台帳
	ウイルス対策管理台帳
	情報システム外部委託管理手順書
内部セキュリティ監査マニュアル	
その他	ネットワークシステム管理運用要綱
	インターネット管理運用要領
	OA機器管理運用要領
	電子メール利用基準

2 インターネット関連の運用

インターネットの利用は、情報収集や情報伝達が容易である反面、情報漏えいの事故につながりやすいことやコンピュータウィルスの感染経路になることもある。本市が被害者若しくは加害者にならないため、適切な運用を行う。

(1) 電子メール

電子メールの利用については、電子メール利用基準に従うものとする。

(2) ホームページの閲覧等

ホームページの閲覧等インターネットの利用については、インターネット管理運用要領に従うものとする。

3 新規システムの導入管理

新規情報システムの導入及びシステム開発にあたっては、次の事項を遵守しなければならない。

遵守事項	管理手順
開発環境の分離	①運用システムと開発するシステムは、次の単位で分離すること。 a ネットワークのセグメント b 開発室 c サーバ ただし、物理的に困難な場合又は開発段階における事前テスト時はこの限りではない。
開発データの保護	①開発用のデータに個人情報等重要な情報が含まれる場合はマスキングを行うこと。 ②委託先から外部へ流出しないよう管理すること。 a 原則として、業務の再委託を禁止する b データ保管場所の確認 c データ管理の「覚書」等の徴取 ③開発終了時は確実に開発データを消去すること
システム検証の実施	①仕様段階でのセキュリティ要求事項の検証 ②試験成績書の作成 ③試験成績書に基づく検査の実施 ④導入事前テストの実施

4 情報システムの外部委託管理

(1) 遵守事項

情報システムを外部委託する場合には、情報セキュリティ基本方針を理解させ、確実に実行させるとともに、許可された者の不正アクセスを防止するため、以下の事項を遵守する。

①委託先に情報セキュリティに関する規定及び個人情報保護に関する規定が存在すること。

②契約書上で機密保持契約がなされること。

③上記に合わせ作業員個人との機密保持契約（誓約書）を提出させること。

(2) 情報システムの外部委託に関する手順の詳細は、情報システム外部委託管理手順書に定める。

5 セキュリティ情報の収集

(1) 目的

情報セキュリティポリシーの有効性の維持及びセキュリティ事故の防止を図るため、積極的に情報収集を行う。

(2) 外部環境情報の活用

情報政策課は、セキュリティ技術、セキュリティ事故情報、法規制の制定、改定など入手した外部環境情報を情報セキュリティポリシーの見直しに活用する。

また、必要に応じて各システム管理者に周知する。