

## Ⅸ 監視・検証、監査及び評価・見直し

### 1 監視及び検証

#### (1) 目的

- ・許可されない不正なアクセス（ウイルスも含む）の認識
- ・システムの性能低下の把握
- ・情報セキュリティポリシーの有効性の改善

#### (2) 監視及び検証の対象及び手段

分類	対象及び手段		主管部門
システムの運用監視	対象	内部からのアクセス	各システム管理者
	手段	サーバのシステムログ、イベントログ監視	
外部からの不正アクセスの監視	対象	外部からの不正アクセス	情報政策課
	手段	侵入検知システム等による監視	
ネットワーク脆弱性の検証	対象	サーバ、ルータ、ファイアウォールの脆弱性	情報政策課
	手段	脆弱性検査ツールによる検証	
ウイルスの監視	対象	ウイルス感染	各システム管理者
	手段	ウイルス対策ソフトの機能による監視	
ネットワークの性能監視	対象	ネットワークのトラフィック	情報政策課
	手段	専用モニタリング装置による監視	

#### (3) 監視及び検証の手順

- ①各システム管理者は、計画を立案し、計画どおり監視又は検証の実施を行う。
- ②各システム管理者は、監視及び検証の結果に基づき、適切な措置を講ずる。
- ③各システム管理者は、監視及び検証の結果を適宜情報政策課へ報告を行う。
- ④情報政策課は、各システム管理者からの報告を情報セキュリティポリシーの見直しに活用する。

### 2 情報セキュリティ監査

#### (1) セキュリティ内部監査員

- ①情報セキュリティ監査チームリーダーは、セキュリティ内部監査員の互選によるものとする。
- ②セキュリティ内部監査員は次の研修のいずれかを受講する。
  - ・外部研修機関によるセキュリティ内部監査員研修
  - ・上記の研修受講者による内部研修

#### (2) 監査の種類

定期監査	監査される活動の状況及び重要性に基づいて、情報セキュリティ監査チームが作成した情報セキュリティ監査計画書に従い、実施する監査
臨時監査	定期監査以外に、セキュリティ評価委員会の判断により臨時的に行われる監査

### (3) 監査の手順

- ①情報セキュリティ監査チームリーダーは、被監査部門との独立性を考慮し、セキュリティ内部監査員を選任する。
- ②セキュリティ内部監査員は、次の内容を踏まえ、情報セキュリティ監査実施計画書を作成する。
  - ・ 監査スケジュール
  - ・ 監査対象の抽出
  - ・ 監査チェックリスト
- ③実施計画書に基づき、監査を実施する。必要に応じて、監査の全部又は一部を外部の専門家に委託することができる。
- ④監査結果を記録し、情報セキュリティ評価委員会へ報告する。
- ⑤必要により助言、フォローアップを行う。

### 3 情報セキュリティポリシーの評価及び見直し

情報セキュリティポリシーを効果的に運用するため、次に掲げる要因により情報セキュリティポリシーの実効性を評価し、必要に応じて見直しを行う。

- ・ 社会環境の変化及び市民からの要望
- ・ 関連する法規制の改正
- ・ 本市、国及び他の地方公共団体のセキュリティ事故事例
- ・ 有識者からの助言及び情報セキュリティ対策技術の進展
- ・ 情報セキュリティポリシーの遵守状況（内部セキュリティ監査結果等）
- ・ 内部環境の変化

## X 情報セキュリティポリシーに関する文書及び記録管理の遵守事項

### 1 文書の管理

- a 許可された利用者が容易に利用することができるように管理すること。
- b 情報セキュリティ基本方針と情報セキュリティ対策基準との準拠性を維持するために適宜見直しを行い、必要に応じて改定を行うこと。
- c 更新履歴を管理すること。
- d あらかじめ定められた責任権限によって承認されること。
- e 廃止文書は速やかに除去し、常に最新版を利用できるように管理すること。

### 2 記録の管理

- a 必要と認められる期間、保管すること。
- b 許可された利用者が容易に利用することができるように管理すること。
- c 損傷、劣化及び紛失を防ぐ適切な措置を行うこと。

対策基準 改訂履歴

Ver.	制定／改訂 承認年月日	改訂項目	改訂内容	改訂理由
初版	H15.3.31	—	初版制定	—
第2版	H19.3.30	III管理体制 1 組織 2 責任及び権限 (6)	構成員の変更 項目の変更	組織改変に伴う組織体制及び構 成員を各要綱に委任するもの。 項目について修正するもの。
第3版	H22.3.31	V 人的セキュリティ対策 1 職員の責任及び権限 2 教育及び訓練 3 セキュリティ事故への対応  VII 技術的セキュリティ対策 4 コンピュータウイルス対策  VIII 運用管理 5 セキュリティ情報の収集  IX 監視・検証、監査及び評 価・見直し 1 監視及び検証	組織名の変更	組織改変に伴い、組織名を修正するもの。