静岡市監査委員

情報セキュリティ基本方針

令和８年４月１日
静岡市監査委員

改 版 履 歴

版　数	施　行　日
第1版	令和８年４月１日

1　目的

静岡市監査委員情報セキュリティ基本方針（以下「基本方針」という。）は、監査委員がその職務を遂行するに当たり取り扱う情報資産について、機密性、完全性及び可用性を確保するための基本的な考え方を示すことを目的とする。

2　定義

基本方針における用語の意義は、それぞれ次に定めるところによる。

（1）情報

文書（メモ等を含む。）、図画及び写真（これらを撮影したマイクロフィルムを含む。）並びに電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）をいう。

（2）情報システム

コンピュータ、ソフトウェア、ネットワーク及び周辺機器で構成され、情報の処理を行う仕組みをいう。

（3）情報資産

情報（文書、資料その他電子的情報を含む。）及び情報システムをいう。

（4）電子記録媒体

磁気、光学、半導体その他の原理により電磁的記録を保持することを目的とした媒体をいう。

（5）記録媒体

電子記録媒体及び紙媒体をいう。

（6）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。

（7）機密性

情報にアクセスすることを認可された者だけがアクセスできることをいう。

（8）完全性

情報及び処理の方法が正確かつ完全である状態をいう。

（9）可用性

許可された利用者が必要なときに情報にアクセスできることをいう。

(10) 情報セキュリティインシデント

情報資産の不正使用、業務妨害行為、データの破壊及びそれらに至るための行為等の情

報セキュリティに対する脅威及び脆弱性から発生する障害をいう。

(11) 脅威

自然災害、悪意のある行為等情報資産に被害を与える要因をいう。

(12) 脆弱性

情報セキュリティの弱い部分及び情報セキュリティを弱める環境等の脅威を発生しやすくさせる要因をいう。

(13) 監査委員

地方自治法（昭和 22 年法律第 67 号）第 195 条の規定に基づき静岡市に置かれる監査委員をいう。

(14) 監査等

地方自治法第 198 条の３に規定する監査等をいう。

3　適用範囲

（1）対象者の範囲

基本方針が適用される対象者の範囲は、監査委員とする。

（2）情報資産の範囲

基本方針が適用される情報資産の範囲は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

4　基本方針の位置付け

基本方針は、監査等の実施において情報資産の適正な管理を実現するための対策の最上位に位置するものとする。監査委員は基本方針を遵守し、必要に応じて静岡市情報セキュリティ委員会が定める静岡市情報セキュリティポリシーに準じた適切な対応を行うものとする。

5　監査委員の責務

（1）公的責任と信頼の確保

監査委員は、職務上取り扱う情報が、市民の財産や権利、利益に関わる公的資産であることを認識し、これを慎重かつ確実に管理しなければならない。情報漏えい、改ざん、紛失等のリスクを常に意識し、監査制度への信頼を損なうことのないよう、正確かつ誠実な情報の取扱いを徹底しなければならない。

（2）独立性と中立性の維持

監査委員は、監査機能の独立性及び中立性を確保するため、情報の管理に当たっては、必要な範囲での情報隔離に努め、外部からの不当な影響を排除することで、公正な監査体制の構築を図らなければならない。

（3）リスク管理の適正な確保

監査委員は、情報資産に対するリスクへの対応が適切に行われるよう、必要な注意を払わなければならない。特に、個人情報や非公開情報など、漏えいが重大な影響を及ぼす情報については、厳格な管理が確保されるよう必要な配慮を行わなければならない。

（4）継続的改善と柔軟な対応

監査委員は、情報セキュリティ対策を一過性の措置とせず、定期的に情報管理を自己点検するとともに、技術動向、脅威環境、業務内容等の変化に応じて、柔軟に見直す姿勢を持ち続ける。

6　情報セキュリティ対策

情報資産を脅威から防御し、又は情報資産の脆弱性を解消するため、次の情報セキュリティ対策を講ずるものとする。

（1）情報セキュリティ最高責任者の設置

監査委員が保有する情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する者として情報セキュリティ最高責任者を置き、代表監査委員をもって充てる。

（2）情報セキュリティ対策基準の策定

情報セキュリティ最高責任者は、（3）から（9）までに掲げる事項について、監査委員が遵守すべき範囲を定める情報セキュリティ対策基準（以下「対策基準」という。）を策定する。

（3）情報セキュリティ組織運営対策

対策基準の適用範囲における情報セキュリティの推進及び向上のための組織体制を確立する。

（4）情報資産管理

情報資産の作成、複製、入手、保管、利用、送信、持ち出し、消去及び廃棄に関する取扱いを明確にする。

（5）物理的セキュリティ

サーバ等のハードウェアの設置環境、情報を取り扱う機器及び設備等について、情報セキュリティの確保に必要な対策を講ずる。

（6）人的セキュリティ

情報セキュリティの確保を図るため、監査委員が服務上遵守すべき事項を明確にする。

（7）ＩＴ資産管理

業務で利用するハードウェア、ソフトウェア、ライセンス等のＩＴ資産の適正な運用等について、情報セキュリティの確保及びライセンスコンプライアンスの向上に必要な対策を講ずる。

（8）情報セキュリティインシデント対応

情報セキュリティインシデントが発生した場合において、迅速かつ適切な対応を行うための手順等を明確にする。

（9）基本方針及び対策基準違反等への対応

基本方針及び対策基準の遵守違反が発生したときの調査、違反行為者等に対する指示、例外措置等について、必要な対策を講ずるものとする。

7　基本方針の公開

基本方針は、公開するものとする。

8　情報セキュリティに関する自己点検

監査委員は、情報資産の適切な保護と情報セキュリティ水準の継続的な向上を図るため、定期的に情報セキュリティに関する自己点検を行うものとする。

9　基本方針及び対策基準の見直し

基本方針及び対策基準は、社会的な情報技術の進展及び脅威やリスクの変化に対応するため、必要に応じて見直しを行う。この見直しは、情報セキュリティ最高責任者の権限により行うものとし、その内容については、適宜、監査委員協議会において報告するものとする。