君津市監査委員情報セキュリティ基本方針

策定日　令和８年３月 30 日

１ 目的

本基本方針は、君津市監査委員（以下「監査委員」という。）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、監査委員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

電子情報の伝達を目的として設置される通信回線網をいう。

（２）情報システム

タブレット型端末、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）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（５）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（６）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（７）情報資産

情報システム、ネットワーク、記録媒体、帳票、重要情報を含む文書及びシステム設計書その他のドキュメント類ならびにこれらで取り扱われている情報をいう。

（８）脅威

部外者の侵入、不正アクセス、ウィルス攻撃及び情報資産の持ち出し等による情報資産の漏えい、破壊、改ざん、消去等をいう。

３ 適用範囲

（１）行政機関の範囲

本基本方針が適用される範囲は、監査委員及び監査委員事務局職員（以下「事務局職員」という。）とする。 ただし、事務局職員についてこの基本方針に定めのない事項は、君津市情報セキュリティ基本方針に関する規則（平成 28 年３月 30 日）を適用する。

（２）情報資産の範囲

本基本方針は、２(７)に規定する情報資産のうち、漏えい、破壊、改ざん、消去等又はそのおそれから保護するために管理を要するものを対象とする。

４ 遵守義務

監査委員及び事務局職員は、情報セキュリティの重要性について共通の認識を持ち、情報資産を適切に取り扱わなければならない。

５ 情報セキュリティ対策

２(８)に規定する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じる。

（１）情報資産の分類と管理

監査委員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。

（２）物理的セキュリティ

タブレット型端末及び通信回線等の管理について、物理的な対策を講じる。

（３）人的セキュリティ

情報セキュリティに関し、監査委員及び事務局職員が遵守すべき事項について、教育及び啓発を行う等の人的な対策を講じる。

（４）技術的セキュリティ

タブレット型端末等の管理、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。

（５）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、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

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。

ウ　ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

６ 情報セキュリティ点検の実施

情報セキュリティ対策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点検を実施する。

７　情報セキュリティ対策の見直し

情報セキュリティ点検の結果及び情報セキュリティを取り巻く状況の変化を踏まえ、５に掲げる情報セキュリティ対策を定期的又は必要に応じて見直し、情報セキュリティの向上を図る。

附 則（令和８年３月 30 日君監第 146 号）

この方針は、令和８年４月１日から施行する