石垣市監査委員サイバーセキュリティ基本方針

令和８年３月

石垣市監査委員

版数	作成年月日	作成改訂理由
第1版	令和8年3月25日	新規制定

〈 改 定 履 歴 〉

１　目的

石垣市監査委員サイバーセキュリティ基本方針（以下「本方針」という。）は、石垣市監査委員（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サイバー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

本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）情報

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。）

（２）情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

（３）情報資産

情報及び情報システムをいう。

（４）ネットワーク

コンピュータ等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）をいう。

（５）サイバーセキュリティ

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を許可された者だけが、情報にアクセスできる状態を確保することをいう。

（７）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。

（８）可用性

情報にアクセスすることを許可された者が、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。

（９）ＬＧＷＡＮ接続系

総合行政ネットワークに接続された情報システム及びその情報システムで取り扱うデータをいう。

(10) インターネット接続系

インターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

３　対象する脅威

情報資産に対する脅威として、以下の脅威を想定し、サイバーセキュリティ

対策を実施する。

（１）不正アクセス、ウィルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去・搾取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作ミス、設定ミス、保守の不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

４　適用範囲

（１）適用機関の範囲

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（以下「監査委員等」という。）とする。

（２）情報資産の範囲

本方針が対象とする情報資産は、監査委員等が保有する情報資産とする。

５　監査委員等の遵守義務

監査委員等は、サイバーセキュリティの重要性について共通の認識を持ち、業務の遂行に当たり、本方針等を遵守しなければならない。

６　サイバーセキュリティ対策

３に規定する脅威から情報資産を保護するために、次に掲げるサイバーセキュリティ対策を講じる。

（１）情報資産の分類と管理

監査委員等の保有する情報資産をその重要性に応じて分類し、適切なサイバーセキュリティ対策を行う。

（２）情報システム全体の強靭性の向上

サイバーセキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、ＬＧＷＡＮ接続系の情報システム及びインターネット接続（内部）系の情報システムからなる強靭性向上対策を講じる。

（３）物理的セキュリティ対策

監査委員事務局内への不正な立ち入りの防止等、情報資産を保護するために物理的な対策を講じる。

（４）その他のセキュリティ対策

その他のサイバーセキュリティ対策については、石垣市サイバーセキュリティ基本方針に基づき石垣市が講じる対策に依拠するとともに、その対策を遵守する。

７　サイバーセキュリティに関する自己点検の実施

本方針の遵守状況を検証するため、定期的又は必要に応じてサイバーセキュリティに関する自己点検を実施し、運用改善を行い、サイバーセキュリティの向上を図る。

8　本方針の見直し

サイバーセキュリティに関する自己点検の結果又はサイバーセキュリティを取り巻く状況の変化に対応するため新たに対策が必要になった場合には、本方針の見直しを実施する。

9　サイバーセキュリティ対策基準の策定

サイバーセキュリティ対策を実施するために、必要に応じて、具体的な遵守事項、判断基準等を定める情報セキュリティ対策基準等を策定する。

なお、当該対策基準等は、非公開とする。