可児市監査委員情報セキュリティ基本方針

策定日　令和８年２月 10 日

（目的）

第１条　本基本方針は、可児市監査委員（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。

（定義）

第２条　本基本方針において、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)　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ならびに当該コンピュータ等のハードウェア及びソフトウェアをいう。

(2)　情報システム

コンピュータ、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、改ざんまた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)　LGWAN 接続系

人事給与、財務会計及び文書管理等 LGWAN 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。

(8)　インターネット接続系

インターネットメール、ホームページ管理システム等に関わる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。

(9)　無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウィルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

(10)　監査委員等

各監査委員、監査委員事務局職員のことをいう。

（対象とする脅威）

第３条　監査委員は、情報資産に対する脅威として、次の各号に掲げる脅威を想定し、情報セキュリティ対策を実施する。

(1)　不正アクセス、ウイルス攻撃、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、重要情報の詐取、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・設定ミス、メンテナンス不備、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

(3)　地震、落雷、火災等の災害によるサービス及び業務の停止等

(4)　大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

(5)　電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

（適用範囲）

第４条　本基本方針が適用される行政機関は、地方自治法((昭和 22 年４月 17 日法律第 67 号)第 195 条に定める監査委員及び可児市監査委員条例(昭和 57 年４月１日条例第 21 号)に定める機関とする。

２　本基本方針が適用される情報資産は、次のとおりとする。

(1)　ネットワーク及び情報システムならびにこれらに関する設備及び電磁的記録媒体

(2)　ネットワーク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。）

(3)　情報システムの仕様書及びネットワーク図等のシステム関連文書

（監査委員等の遵守義務）

第５条　監査委員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって本基本方針を遵守しなければならない。

２　本基本方針に定めのない事項については、可児市情報セキュリティ基本方針の例による。

（情報セキュリティ対策）

第６条　監査委員は、第３条の脅威から情報資産を保護するために、次のとおり情報セキュリティ対策を講じる。

(1)　監査委員が保有する情報資産の重要性を機密性、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)　情報システムに対し、次の対策を講じる。

ア　LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

イ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施するとともに、高度な情報セキュリティ対策として、都道府

県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(3)　監査委員等が管理するパソコン等の端末について、物理的な対策を講じる。

(4)　情報セキュリティに関し、監査委員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(5)　コンピュータ等の管理、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。

(6)　情報システムの監視、情報セキュリティの遵守状況の確認等、運用面の対策を講じる。

(7)　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。外部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。

(8)　本基本方針の遵守状況を検証するため、定期的または必要に応じて自己点検を実施し、運用改善を行い情報セキュリティの向上を図るとともに、必要に応じて本基本方針の見直しを実施する。

付　則

本基本方針は、令和８年４月１日から施行する。