佐賀東部水道企業団
監査委員
情報セキュリティポリシー
（基本方針）

佐賀東部水道企業団

監査委員

令和８年３月

目次

１．目的

情報セキュリティ基本方針（以下「基本方針」という。）は、佐賀東部水道企業団（以下「企業団」という。）の監査委員が保有する情報資産を事故、災害、不正侵入、漏えい、改ざん、サービス利用妨害等の様々な脅威から保護するための必要な対策について、組織的かつ継続的に取り組むための基本的な考え方を定めるものである。本基本方針に基づき、企業団監査委員会における情報セキュリティ対策を適切に実施し、その水準を維持・向上させることを目的とする。

２．定義

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

(1) 機密性

認可されたものだけが情報にアクセスできる状態をいう。

(2) 完全性

情報が破壊、改ざん又は消去されていない状態をいう。

(3) 可用性

情報にアクセスすることを認可されたものが、必要な時に情報にアクセスできる状態をいう。

(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) 情報システム

コンピュータに係るハードウェア、ソフトウェア、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。

(6) 情報資産

ネットワーク及び情報システムの開発と運用にかかる全ての情報並びにネットワーク及び情報システムで取扱う全ての情報をいう。

(7) 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。

(8) 情報セキュリティポリシー

基本方針から構成されるものとする。

(9) 関係者等

企業団監査委員の情報資産を取扱う構成員（監査委員）およびその事務に従事する企業団職員（企業長、再任用短時間職員及び会計年度任用職員を含む。）をいう。

３．対象とする脅威

情報資産に対する脅威として、以下を想定し、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、重要情報の搾取、内部不正

(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、内部・外部監査機能の不備、外部委託管理の不備、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

(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

(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

(5) 電力供給又は通信の途絶、その他社会基盤の障害からの波及

(6) その他、企業団監査委員の情報資産の機密性、完全性、可用性を脅かす脅威

４．適用範囲

情報セキュリティポリシーは、企業団監査委員の情報資産を取扱う関係者等及び外部委託者に適用する。

５．関係者等の遵守義務

関係者等は、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情報セキュリティポリシーを遵守しなければならない。

６．情報セキュリティ対策

上記３の脅威から情報資産を保護するために、企業団の情報セキュリティ対策基準および関連規定を適用する。

７．情報セキュリティポリシーの見直し

情報セキュリティポリシーの遵守状況について、必要に応じて確認を行い、その結果に基づき基本方針の見直しを行う。