庄内広域水道企業団情報セキュリティポリシー
（基本方針）

庄内広域水道企業団

令和８年４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、庄内広域水道企業団（以下「企業団」という。）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、企業団における情報セキュリティ対策を実施し、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。

⑴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。

⑵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。

⑶可用性

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

⑷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。

⑸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。

⑹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係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。

⑺情報セキュリティ

情報資産の機密性、完全性及可用性を維持することをいう。

⑻情報セキュリティポリシー

基本方針及び情報セキュリティ対策基準からなる。

⑼職員等

企業団の情報資産を取扱う全ての職員（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．対象となる脅威

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、企業団が保有する情報資産並びに情報資産を取扱う職員及び外部委託者に適用する。

５．職員等の遵守義務

職員等は、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、以下のとおり情報セキュリティ対策を講じる。

(1)組織体制

企業団の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2)情報資産の分類と管理

企業団の情報資産を重要度に基づいて分類し、分類に応じた情報セキュリティ対策を実施する。

(3)物理的セキュリティ

サーバー、通信回線、職員等のパソコン等の管理について、物理的な対策を講ずる。

(4)人的セキュリティ

情報セキュリティに関し、職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)技術的セキュリティ

ネットワーク及び情報システムの管理、アクセス制御、不正プログラム対策、不正アクセス対策等に対し、技術的な対策を講じる。

⑹運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を実施するとともに、情報資産に対するセキュリティ侵害が発生した際に迅速かつ適正に対応するための事後対策を予め講じる。

⑺業務委託と外部（クラウドサービス）の利用

外部委託する場合には、外部委託事業者を選定し、情報セキュリティ要件を明確にした契約を締結し、外部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（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。

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。

⑻評価・見直し

情報セキュリティポリシー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監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

７．情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシー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監査を及び自己点検を実施する。

８．情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する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、情報セキュリティポリシーを見直す。

９.情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

１０．情報セキュリティ運用マニュアルの策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ運用マニュアルを策定するものとする。なお、情報セキュリティ運用マニュアルは、公にすることにより企業団の事業運営に重大な支障を及ぼすおそれがあることから非公開とする。