○芳賀中部上水道企業団情報セキュリティ基本方針

令和８年２月１８日規程

（目的）

第１条　この基本方針は、芳賀中部上水道企業団（以下、企業団という）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、企業団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　この基本方針において、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、その構成機器（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)　情報セキュリティポリシー　本基本方針及び情報セキュリティ対策基準をいう。

(5)　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。

(6)　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。

(7)　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。

(8)　水道管理事務系　施設監視システム、マッピングシステム及び水道料金・会計システムに関わる情報システム及びデータをいう。

(9)　庁内 LAN 接続系　庁内 LAN 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（水道管理事務系

を除く)。

(10)　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。

(11)　通信経路の分割　庁内 LAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(12)　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、コンピュータウイ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。

(情報資産に対する脅威)

第３条　情報資産に対する脅威は、次に掲げるとおりとする。

(1)　情報機器の盗難、不正アクセス、コンピュータウイルスによる攻撃、部外者の侵入等の意図的要因による情報資産の漏えい、破壊、改ざん、消去等

(2)　情報資産の管理の不備、ソフトウェアの無許可での使用、プログラム上の欠陥、誤操作、メンテナンスの不備、情報機器の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、電力供給又は通信の途絶等による情報システムの運用障害等

(適用範囲)

第４条　この基本方針が適用される執行機関及び議決機関は、企業長、監査委員及び議会とする。

(情報資産の範囲)

第５条　この基本方針が対象とする情報資産は、次に掲げるとおりとする。

(1)　ネットワーク、情報システム及びこれらの運用又は管理に必要な設備並びに電磁的記録媒体

(2)　ネットワーク又は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)　ネットワーク又は情報システムに関する仕様書、図面等のシステム関連文書

（職員等の遵守義務）

第６条　職員、臨時・非常勤職員等（以下「職員等」という）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。

（情報セキュリティ対策）

第７条　企業団は、前条に規定する脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講ずるものとする。

(1)　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こと。

(2)　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こと。

(3)　情報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次の対策を講じること。

ア　水道管理事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、利用者情報等の流出を防ぐ。

イ　庁内 LAN 接続系においては、庁内 LAN サーバ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。

ウ　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。

(4)　サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じること。

(5)　情報セキュリティに関する職員等への十分な教育及び啓発等の人的な対策を講じること。

(6)　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こと。

(7)　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講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するための対策を講じること。

(8)　業務委託を行う場合には、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こと。

(9)　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こと。

(10)　業務において、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こと。

（情報セキュリティの点検及び監査の実施）

第８条　情報セキュリティポリシーの遵守状況を確認するため、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する。

（情報セキュリティポリシーの見直し）

第９条　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は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ対策基準の策定）

第１０条　企業団は、情報セキュリティ対策を適切に行うため、具体的な判断基準、遵守事項、手続等を定めた情報セキュリティ対策基準を策定するものとする。

２　情報セキュリティ対策基準は、公開により企業団の情報セキュリティの維持に著しい支障が生じるため、非公開とする。

附則

この基本方針は、令和８年４月１日から施行する。