広島県水道広域連合企業団
サイバーセキュリティを確保するための方針

令和８年３月

第１章　　広島県水道広域連合企業団　情報セキュリティ基本方針

第１ 目的

基本方針は、水道企業団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、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。

第２ 用語の定義

１　情報

情報システムで取扱う電磁データをいう。

２　情報資産

情報及び情報を管理する仕組み（情報システム並びに情報システムの開発、運用及び保守のための資料等を含む。）をいう。

３　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。

４　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。

５　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。

６　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。

７　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。

８　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。

９　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。

１０　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

１１　LGWAN 接続系

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扱うデータをいう（マイナンバー利用事務系を除く。）。

１２　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扱うデータをいう。

１３　通信経路の分割

LGWAN 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。

１４　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。

第３ 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、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、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

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

第４ 適用範囲

１　組織の範囲

本基本方針が適用される組織は、水道企業団の保有する情報資産に関する業務に携わる議会、企業長、副企業長、補助職員、監査委員、選挙管理委員会、外部委託事業者及び指定管理者とする。

２　情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。なお外部に情報提供したことによる二次利用されたデータや、電磁的記録媒体等に情報を記録したものを外部に交付することにより、管理責任が水道企業団から離れたものを除く。

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

(2)　ネットワーク及び情報システムで取扱う情報（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。

(4)　水道企業団が保有する水道役務に係る下記情報システム。

区分	分類	システム名称	システムの概要
通信基盤	通信基盤	通信回線、PC・モバイル・タブレット端末等	インフラ基盤に関連するシステム
業務系システム	施設管理系システム	管路情報管理	地理情報システムを利用して配水管等の位置情報及び施設情報を管理するシステム
		給水装置工事受付	給水装置に係る申請・届出を管理するシステム
		指定給水装置工事業者管理	給水装置工事の適正な施工を認める「指定給水装置工事事業者」の情報を登録・管理するシステム
		施設・設備台帳	浄水場や配水場等の機械、電気･計装設備の情報を管理するシステム
		地下埋設物協議受付	地下埋設工事に係る事故防止のため、工事の施工に伴う協議を受付・管理するためのシステム
		管網解析	配水管網内の水理状況、水質状況をシミュレーションするシステム
	料金系システム	検針・水道料金スマートメーター	水道使用者のメータ水量を検針するためのシステム及び検針した値を使用者の個人情報等とともに一元的に管理するシステム
	工務系システム	電子入札、電子契約	入札に係る業務、契約締結に係る業務をオンラインで行うシステム。
		営繕積算、土木積算	実勢価格や現場実態を反映した適正な価格設定、土木工事等に係る費用を算出するためのシステム
		工事管理システム	工事の受発注、施工の進捗管理、図面や工程管理など、工事に関する各種データを一元管理するシステム
施設監視系システム	施設監視系システム	浄水場等の運転制御システム	浄水処理を適切に行うために、各種機器の働きを制御する一連のシステム
		広域運転監視	物理的に離れた場所で稼働している運転監視システムを一元的に運用監視するためのシステム。

第５ 職員等の遵守義務

水道企業団の保有する情報資産に関する業務に携わるすべての職員（再任用職員、非常勤職員、臨時職員及び県市町等からの派遣職員等を含む）、議員、各委員、外部委託事業者及び指定管理者の職員（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及び情報セキュリティ実施手順を遵守する義務を負う。

第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、次の情報セキュリティ対策を講じる。

１　組織体制

水道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団的な組織体制を確立する。

2　情報資産の分類と管理

水道企業団の保有する情報資産を機密性、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。

3　情報システム全体の強靭性の向上

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、次の三段階の対策を講じる。

(1)　マイナンバー利用事務系においては、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、住民情報の流出を防ぐ。

(2)　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。

(3)　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　物理的セキュリティ

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。

5　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。

6　技術的セキュリティ

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。

7　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、業務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、緊急時対応計画を策定する。

8　業務委託と外部サービスの利用

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、利用にかか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。

9　ゼロトラスト・アーキテクチャ

情報システム全体の強靭性向上の一環として、いかなるアクセス要求も信頼せず、常に検証するゼロトラスト・アーキテクチャの考え方を取り入れ、情報資産の保護を強化する。

第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及び自己点検を実施する。

第８ 情報セキュリティの評価及び見直し

情報セキュリティ監査及び自己点検実施による検証結果等を踏まえるとともに、情報セキュリティを取り巻く状況の変化に対応するため、セキュリティポリシー及び実施手順の見直しを適宜行うこと。

第９ 情報セキュリティ対策基準の策定

上記６、７及び８の情報セキュリティ対策を講じるに当たり、遵守すべき行為、判断等の基準を統一的に定めるため、必要となる基本的な要件を明記した対策基準を策定するものとする。

なお、対策基準は公にすることにより水道企業団の行政運営に重大な支障を及ぼすことがあることから非公開とする。

第１０ 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、個々の情報システムについて具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより水道企業団の行政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。

附　則

この方針は、令和８年３月１日から施行する。