竹田市情報セキュリティ基本方針
【上下水道事業版】

令和８年４月１日

１．目的

上下水道事業は、安全で良質な水を安定的に供給することと生活排水施設を整備することにより、住民生活および地域社会の基盤を支える重要な公共サービスである。その運営にあたっては、上下水道施設の運転管理や料金徴収業務をはじめ、各種の情報システムおよび住民等の個人情報を含む情報資産を適切に取り扱うことが不可欠である。

近年、サイバー攻撃や自然災害、機器の障害、人為的なミスなどに起因する情報セキュリティ上の脅威は増大しており、万一の事故は上下水道サービスの停止や個人情報の漏えいといった深刻な事態を招くおそれがある。そのため、情報セキュリティの確保は、住民の信頼を維持し、上下水道事業を持続的に運営していくうえで最重要課題の一つである。

このような状況を踏まえ、上下水道事業における情報資産を保護し、安定した事業継続を確保することを目的として、本「情報セキュリティ基本方針」を策定する。本方針は、上下水道事業に従事する全職員等が遵守すべき情報セキュリティの基本的な考え方を示すものであり、具体的な対策基準の拠り所とするものである。

２．定義

（１）ネットワーク　上下水道課において設置する端末、機器及びその他の関係機関を相互に接続するためのネットワーク及びその構成機器（ハードウエア及びソフトウエア）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すべての情報並びにネットワーク及び情報システムで取り扱うすべての情報をいい、紙等の有体物に出力された情報も含むものとする。

（４）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。

（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）内部情報系　上下水道料金システム等、上下水道課にて利用が限定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）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係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。

（１０）通信経路の分割　内部情報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。

（１１）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ないなど、安全が確保された通信をいう。

３．対象とする脅威

（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及び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、無許可ソフトウエ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及び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、落雷及び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よる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、排水処理の停止等のインフラの障害からの波及等

４．適用範囲

（１）本基本方針が適用される範囲は、上下水道課、関連する事業所及び上下水道施設の維持管理や料金徴収を上下水道事業から委託する外部事業者とする。

（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。

①　ネットワーク、情報システム、これらに関する設備、電磁的記録媒体

②　ネットワーク及び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

５．職員等の遵守義務

上下水道課に勤務する職員、非常勤職員及び臨時職員等（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。

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、以下の情報セキュリティ対策を講じる。

（１）組織体制

情報資産について、情報セキュリティ対策を推進する上下水道課での組織体制を確立する。

（2）情報資産の分類と管理

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）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。

（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

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）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。

（7）業務委託とクラウドサービスの利用

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。

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。

（8）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、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、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。

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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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。

なお、情報セキュリティ対策基準は、具体的な情報セキュリティ対策が記載されているため、公にすることにより上下水道事業の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

本方針は、令和８年４月１日から施行する。