久吉ダム水道企業団
情報セキュリティポリシー
（公表用）

久吉ダム水道企業団

令和８年８月

目　　次

第１章　情報セキュリティ基本方針

第１　目的　・・・

第１章　情報セキュリティ基本方針

第１　目的

本基本方針は、久吉ダム水道企業団（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。

第２　定義

本基本方針において、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。

(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) 情報資産

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、これらで取り扱う情報並びに情報システムの仕様書、ネットワーク構成図その他の情報システムに関連する文書をいう。

(6) 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。

(7) 完全性

情報が正確かつ完全な状態で保持され、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。

(8) 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。

第３　対象とする脅威

企業団は、情報資産に対する脅威として、次に掲げる脅威を想定し、必要な情報セキュリティ対策を実施する。

(1) ランサムウェアその他のサイバー攻撃による情報資産の漏えい、破壊、改ざん、消去、情報システムの機能停止又は業務継続への支障等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用、操作又は設定の誤り、機器の故障、メンテナンスの不備、委託事業者による管理の不備その他の非意図的な要因による情報資産の漏えい、破壊、改ざん又は消去等

(3) 地震、落雷、火災、風水害その他の災害による情報システムの停止又は業務の中断等
(4) 電力供給、通信その他のインフラの障害による情報システム及び業務への影響等
(5) その他、情報セキュリティ上の脅威となる事象

第４　適用範囲

１　組織の範囲

本基本方針は、企業団の事務局、議会及び監査委員並びに企業団の業務に従事する者を対象とする。

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り扱う情報（これらを印刷した文書を含む。）
(3) 水道料金その他水道使用者に関する情報
(4) 水道施設、配水管等の位置、構造その他の施設に関する情報
(5) 水道管理その他水道事業の運営に関する情報
(6) 情報システムの仕様書、ネットワーク構成図その他のシステム関連文書

第５　職員等の遵守義務

企業団の職員、会計年度任用職員その他企業団の業務に従事する者（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しなければならない。

第６　情報セキュリティ対策

企業団は、第３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じる。

(1) 組織体制

情報セキュリティ対策を適切かつ継続的に実施するため、企業団の規模及び組織の実情に応じた情報セキュリティの管理体制を整備する。

(2) 情報資産の分類及び管理

企業団が保有する情報資産を、その重要性、機密性、完全性及び可用性に応じて分類し、当該分類に基づき適切な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、通信設備、職員等が使用するコンピュータその他の情報資産について、盗難、紛失、損傷、不正な持ち出しその他の物理的な脅威から保護するための対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関して職員等が遵守すべき事項を定めるとともに、必要な教育、研修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、ネットワーク及び情報システムについて、アクセス制御、不正プログラム対策、不正アクセス対策、情報漏えい対策その他必要な技術的対策を講じる。

(6) 運用

情報システムの適切な運用、情報セキュリティポリシーの遵守状況の確認、情報資産の管理及び業務委託における情報セキュリティの確保等、情報セキュリティの適切な運用に必要な対策を講じる。

また、情報セキュリティインシデントが発生した場合又はそのおそれがある場合に、迅速かつ適切に対応するための体制を整備する。

(7) 業務委託及び外部サービスの利用

情報システムの運用、保守その他の業務を委託する場合には、委託事業者に求める情報セキュリティ上の要件を明確にし、必要な対策が確保されるよう適切な管理を行う。

外部サービス（クラウドサービス等）を利用する場合には、利用に係る情報セキュリティ上の要件を定め、必要な対策を講じる。

(8) 評価及び見直し

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し、その結果を踏まえて情報セキュリティ対策の改善を図る。

第７　情報セキュリティ監査及び自己点検の実施

企業団は、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　情報セキュリティポリシーの見直し

企業団は、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又は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な対策が必要となった場合には、情報資産に対する脅威及びその影響等を踏まえ、必要に応じて情報セキュリティポリシーを見直すものとする。

第９　情報セキュリティ対策基準の策定

第６から第８までに規定する情報セキュリティ対策を実施するため、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ものとする。

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、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実施手順を策定するものとする。

情報セキュリティ実施手順は、情報セキュリティ対策の具体的な実施方法その他の情報を含み、これを公開することにより企業団の情報セキュリティの確保に支障を及ぼすおそれがあることから、原則として非公開とする。

附　則

この方針は、令和８年８月２０日から施行する。

第２章　情報セキュリティ対策基準（概要）

情報セキュリティ基本方針に基づき、久吉ダム水道企業団が保有する情報資産を適切に管理し、情報セキュリティを確保するために必要な基本的事項を定めています。

第１　組織体制

情報セキュリティに関する責任者等を定め、役割及び責任を明確にするとともに、必要な体制を整備します。

１　情報セキュリティ最高責任者
２　統括情報セキュリティ責任者
３　情報セキュリティ責任者
４　情報セキュリティ管理者
５　情報システム管理者
６　情報システム担当者
７　情報セキュリティチーム
８　兼務
９　ＣＳＩＲＴ

第２　情報資産の分類と管理

情報資産の重要性等に応じた分類及び管理方法を定め、適切な取扱いを行います。

１　情報資産の管理責任
２　情報資産の分類
３　情報資産の保管及び利用
４　情報資産の複製、加工及び提供
５　情報資産の持ち出し
６　情報資産のバックアップ
７　情報資産の廃棄
８　情報資産の管理に関する詳細事項

第３　情報システムの運用

情報システムの導入、運用、変更、廃止等における管理事項を定め、適切な運用を行います。

１　情報システムの管理
２　情報システムのバックアップ及び復旧
３　アクセス管理及び認証
４　ソフトウェア等の管理及び更新
５　不正プログラム等への対策
６　ネットワークの利用及び管理
７　電子メールの利用
８　モバイル端末等の利用
９　外部サービス等の利用
10　情報システムの変更及び廃止

第４　物理的セキュリティ

情報システム及び情報資産を設置する場所への立ち入り、機器の管理、災害・事故等への対策について定めます。

１　サーバ等の管理
２　管理区域等の管理
３　通信回線及び通信回線装置の管理
４　職員等が利用する端末及び電磁的記録媒体等の管理

第５　人的セキュリティ

職員等に対する教育、研修、情報セキュリティ上の遵守事項及び事故発生時の対応等について定めます。

１　職員等の遵守事項
２　研修・訓練
３　情報セキュリティインシデントの報告
４　ＩＤ及びパスワード等の管理

第６　技術的セキュリティ

不正アクセス、マルウェア等の脅威から情報システムを保護するため、アクセス制御、認証、ネットワーク及び端末等の管理について定めます。

１　コンピュータ及びネットワークの管理
２　アクセス制御
３　業務システムの管理及び保守
４　不正プログラム対策
５　不正アクセス対策
６　セキュリティ情報の収集

第７　運用

情報セキュリティに関する監視、記録、インシデントへの対応、自己点検等について定めます。

１　情報システムの監視等
２　情報セキュリティポリシーの遵守状況の確認
３　情報セキュリティインシデントへの対応
４　例外措置
５　法令等の遵守
６　違反時の措置

第８　業務委託と外部サービス（クラウドサービス）の利用

業務を外部委託する場合やクラウドサービス等を利用する場合における、情報セキュリティ上の確認事項及び管理方法を定めます。

１　業務委託における情報セキュリティ
２　委託契約における情報セキュリティ対策
３　委託事業者の管理及び再委託

４　委託事業者によるアクセスの管理
５　情報セキュリティインシデントへの対応
６　業務終了時の情報資産の取扱い
７　外部サービス（クラウドサービス）の利用
８　業務委託及び外部サービスに関する詳細事項

第９　評価・見直し

情報セキュリティ対策の実施状況を確認・評価し、必要に応じて対策基準等の見直しを行います。

１　監査
２　自己点検
３　情報セキュリティポリシー及び関係規程等の見直し
４　評価・見直しに関する詳細事項

第10　用語の定義

本基準で使用する情報セキュリティに関する用語を定義します。

附　則

この基準は、令和８年８月２０日から施行する。

※　なお、情報セキュリティ対策の具体的な実施方法、システム構成、管理手順その他の詳細については、情報セキュリティ確保の観点から公開していません。