阪神水道企業団情報セキュリティポリシー

（情報セキュリティ基本方針）

制　　定　平成24年３月30日
一部改正　平成28年３月29日
一部改正　平成29年４月１日
一部改正　平成30年４月１日
一部改正　令和３年１月７日
一部改正　令和３年４月１日
一部改正　令和５年４月１日

阪神水道企業団

阪神水道企業団情報セキュリティポリシー

—目　次—

第１章　情報セキュリティ基本方針
１　目的 ･･･ 1
２　定義 ･･･ 1
３　対象範囲 ･･･ 1
４　基本方針の公開 ･･ 1
５　組織体制 ･･･ 1
６　情報資産の分類及び管理 ･･････････････････････････････････････ 1
７　情報資産への脅威 ･･ 2
８　情報セキュリティ対策基準の策定 ･･････････････････････････････ 2
９　職員の責務 ･･ 2
10　教育及び訓練 ･･ 2
11　情報セキュリティ点検等の実施 ････････････････････････････････ 2
12　評価及び見直し ･･ 2

第１章　情報セキュリティ基本方針

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、阪神水道企業団（以下「企業団」という。）が保有する情報資産を事故、災害、不正進入、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水準を維持し、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　認可された者だけが情報を利用できることをいう。

⑵　完全性　情報が破壊、改ざん又は消去されていないことをいう。

⑶　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情報を利用できることをいう。

⑷　ネットワーク　企業団の内部機関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）並びに電磁的記録媒体（以下「記録媒体」という。）で構成されるシステムをいう。

⑸　情報システム　企業団の業務で使用する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るシステムをいう。

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り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、完全性及び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　情報資産の情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたもの。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　企業団に勤務する全ての職員をいう。

３　対象範囲

この基本方針の対象範囲は、企業団が保有する情報資産並びに情報資産を取り扱う職員及び外部委託業者に適用する。

４　基本方針の公開

この基本方針は、一般に公開する。

５　組織体制

情報セキュリティ対策を組織的に推進するため、全庁的な組織及び体制を確立する。

６　情報資産の分類及び管理

情報資産は、情報の機密性、完全性及び可用性を踏まえ、その重要度に応じて分類するととも

に、的確に管理する。

７　情報資産への脅威

情報セキュリティを講ずる上で、情報資産に対する脅威の発生度合いや影響を考慮する。特に認識すべき脅威は次のとおりである。

⑴　意図的脅威　故意の不正アクセス又は不正操作によるデータ及びプログラムの持ち出し、盗聴、改ざん、消去、機器及び媒体の盗難、規定外の情報処理装置の接続・操作による漏えい等

⑵　偶発的脅威　意図しない設定ミスや誤操作によるデータ及びプログラムの漏えい、変更、機器及び媒体の故障等

⑶　環境的脅威　地震、落雷、火災等の災害及び事故による業務の停止等

８　情報セキュリティ対策基準の策定

基本方針に基づき、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準（以下「対策基準」という。）を定める。対策基準は、公開することにより企業団の情報セキュリティを侵害する恐れがあるため、原則非公開とする。

９　職員の責務

職員は、情報資産を安全に管理することの重要性について、共通の認識を持つとともに、職務の遂行に当たって、情報セキュリティポリシー（以下「ポリシー」という。）及び関連する法令等を遵守し、責任ある行動を執らなければならない。

10　教育及び訓練

基本方針の適用範囲である情報資産に係る全ての職員に対し、その職務に応じて必要な情報セキュリティに関する教育及び訓練を必要に応じて実施する。

11　情報セキュリティ点検等の実施

ポリシーで定める事項及び情報セキュリティ対策の実施状況について、必要に応じて点検等を実施する。

12　評価及び見直し

情報セキュリティ監査の結果等を踏まえ、ポリシーで定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く環境の変化等に対応するために、ポリシーの見直しを実施する。