阪神水道企業団情報セキュリティポリシー

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
一部改正　令和６年４月１日
全部改正　令和８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

本基本方針は、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。

２　定義

⑴　ネットワーク

コンピューター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。

⑵　情報システム

ハードウェア、ソフトウェア、クラウドサービス、ネットワーク及び電磁的記録媒体（以下「記録媒体」という。）で構成され、情報処理を行う仕組みをいう。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務に関わる情報システム及びデータをいう。

⑼　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り扱うデータをいう。

⑽　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。

⑾　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。

⑿　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、コンピューターウイルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

⒀　職員等

企業団の情報資産を取り扱う者のうち、一般職の職員、再任用職員、会計年度任用職員、任期付職員、臨時的任用職員、特別職の職員、出向・派遣職員及び人材派遣により企業団業務に従事する者をいう。

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。

⑴　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

⑵　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、監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等による情報資産の漏えい・破壊・消去等

⑶　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

⑷　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

⑸　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障害からの波及等

4　適用範囲

⑴　組織の範囲

本基本方針が適用される組織は、企業長の事務部局、企業団議会及び監査委員とする。

⑵　情報資産の範囲

ア　情報システム及びこれらに関する設備及び記録媒体

イ　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。）

ウ　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　職員等の責務

職員等は、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。ただし、企業団議会議

員、監査委員及び委託事業者等については、企業団の情報資産を取り扱う場合に限り、必要な範囲で本ポリシーを遵守するものとする。

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。

⑴　組織体制

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庁的な組織体制を確立する。

⑵　情報資産の分類と管理

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。

⑶　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。

ア　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、機密性の高い情報の流出を防ぐ。

イ　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。

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。

⑷　物理的セキュリティ

サーバー、サーバー室、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。

⑸　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。

⑹　技術的セキュリティ

コンピューター等の管理、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。

⑺　運用

情報システムの監視、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、ポリシーの運用面の対策を講じる。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。

⑻　業務委託と外部サービス（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。

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。

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。

⑼　評価及び見直し

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又は自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。ポリシーの見直しが必要な場合は、適宜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

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又は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又は自己点検の結果、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可能性及び発生時の影響を分析し、リスクを検討したうえで、必要に応じてポリシーを見直す。

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を定める情報セキュリティ対策基準（以下「対策基準」という。）を策定する。

なお、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、非公開とする。

10　情報セキュリティ実施手順の策定

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明記した情報セキュリティ実施手順（以下「実施手順」という。）を策定する。

なお、実施手順は、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、非公開とする。