坂戸、鶴ヶ島水道企業団監査委員情報セキュリティ基本方針

1　目的

坂戸、鶴ヶ島水道企業団監査委員情報セキュリティ基本方針（以下「基本方針」という。）は、監査委員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、監査委員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。

⑵　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。

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　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。

⑸　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。

⑹　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。

⑺　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。

3　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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

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の障害からの波及等

4　適用範囲

基本方針が対象とする情報資産は、監査委員が取り扱う次のものとする。

ただし、企業長が監査事務局として従事する企業団職員の使用に供する情報資産については、その取扱いは坂戸、鶴ヶ島水道企業団情報セキュリティポリシーに従うものとし、基本方針の適用範囲外とする。

⑴　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

⑵　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。）

⑶　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　監査委員の遵守義務

監査委員は、情報セキュリティの重要性について共通の認識を持つとともに、活動及び業務の遂行に当たって関係法令等及び情報セキュリティ基本方針を遵守する義務を負うものとする。

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、次の情報セキュリティ対策を講じる。

⑴　組織体制

監査委員の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

⑵　情報システム全体の強靭性の向上

インターネット接続系において、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。

⑶　物理的セキュリティ

情報システムを設置する施設の管理について、物理的な対策を講じる。

⑷　人的セキュリティ

情報セキュリティに関し、監査委員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。

⑸　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。

⑹　運用

情報システムの監視、基本方針の遵守状況の確認、外部委託を行う際のセキュリティ確保等、基本方針の運用面の対策を講じるものとする。また、情報セキュリティ対策の運用においては、基本方針のほか関係法令等に従い取り組むほか、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講じるよう努める。

⑺　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、利用に係る規定を整備し対策を講じる。

⑻　評価・見直し

基本方針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。基本方針の見直しが必要な場合は、適宜行う。

７　情報セキュリティ監査及び自己点検の実施

基本方針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　情報セキュリティ基本方針の見直し

情報セキュリティ監査及び自己点検の結果、基本方針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、発生時の損失等を分析し、リスクを検討した上で基本方針を見直す。

附則

この基本方針は、令和８年４月１日から施行する。