三井水道企業団情報セキュリティポリシー

（目的）

第１条　三井水道企業団情報セキュリティポリシー（以下「セキュリティポリシー」という。）は、三井水道企業団（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し、情報資産を事故、災害、不正侵入、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の維持、向上を目的とする。

（定義）

第２条　セキュリティポリシーにおいて、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) 職員等

企業団の情報資産を取扱う全ての職員（企業長、再任用職員及び会計年度任用職員、外部委託業者を含む。）をいう。

(2) 情報資産

ア　行政文書

イ　情報システム、ネットワーク及びこれらに関する設備、記憶媒体

ウ　情報システム及びネットワークで取り扱う情報（データ及び印刷された文書を含む。）

エ　情報システムの仕様書、運用手順書及びネットワーク図等のシステム関連文書

(3) 情報システム

企業団内において使用するハードウェア、ソフトウェア、ネットワーク、記憶媒体で構成されるものであって、これら全体又は一部で業務処理を行うものをいう。

(4) 部門システム

企業団において使用する情報資産全体又は一部で業務処理を行う以下のシステムをいう。

水道料金検針徴収システム、財務会計システム、給水受付システム、マッピングシステム、施設台帳システム、人事給与システム、例規システム、配水場監視制御システム

(5) ネットワーク

インターネットへの接続、情報システム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。

(6) 記憶媒体

情報システムで使用される磁気ディスク、磁気テープ、光ディスク、フラッシュメモリ、その他これらに類する媒体をいう。また、記憶媒体のうち取り外し及び持ち出しが可能な記憶媒体を可搬記憶媒体という。

(7) 脅威

情報資産の価値を失わせる要因（不正アクセス、誤操作、ウィルス感染、災害等）及び潜在的な原因をいう。脅威は（8）脆弱性により誘引され、顕在化するものである。

(8) 脆弱性

構造上の欠陥、定期点検の不備、職員教育不備等の情報資産に関連した様々な弱点により、情報資産の障害や損害を発生及び増加させる可能性のことをいう。脅威の存在しない脆弱性については、障害や損害を発生させる可能性がない。

(9) 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安全なレベルで維持することをいう。

(10) 機密性

許可されたものだけが情報にアクセスできる状態をいう。

(11) 完全性

情報及び処理方法の正確さ並びに完全である状態をいう。

（12）可用性

情報にアクセスすることを許可されたものが、必要な時に確実にアクセスできる状態をいう。

（13）セキュリティインシデント

外的要因、内的要因に関わらず、情報セキュリティに対する事故や攻撃であって、企業団の事務及び情報セキュリティが脅かされる状態をいう。

（適用範囲）

第３条　セキュリティポリシーは、企業団が保有する情報資産を取扱う全ての職員等に適用する。

（情報資産における脆弱性）

第４条　情報セキュリティ対策においては、情報資産における脆弱性を考慮し、脆弱性対策度合いや脅威の影響を想定する。特に当該各号については十分な措置を講じる。

（1）物理的脆弱性

地震、落雷、火災等の災害や事故、故障、格納する建築物、筐体の破損（施錠状態を含む）広範囲にわたる疾病に伴う要員不足等によるサービス停止等

（2）人為的脆弱性

無許可ソフトウェア、ハードウェア（記憶媒体を含む）の使用、使用環境の設計、設計開発の不備、意図しない操作、誤操作、規定違反の情報システム操作による情報漏えい、機器、媒体の無許可持ち出し等

（3）技術的脆弱性

サイバー攻撃による、故意の不正アクセス又は不正操作によるデータやプログラムの持ち出し、盗聴、改ざん、消去、機器及び可搬記憶媒体の破壊、盗難等

（情報セキュリティ対策基準の策定）

第５条　情報セキュリティ基本方針を実行に移すため、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について、具体的な遵守事項及び判断基準を明記した情報セキュリティ対策基準を策定する。

（情報セキュリティ基本方針の公開）

第６条　セキュリティポリシーには、企業団のセキュリティに関する内容が含まれることから、情報セキュリティ確保の観点において、情報セキュリティ基本方針のみ公開し、情報セキュリティ対策基準は公開しない。

（職員等の義務）

第７条　情報資産を取り扱うに当たり、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、関係法令及びセキュリティポリシーを遵守しなければならない。

（教育及び訓練）

第８条　企業団は、情報セキュリティ基本方針の適用範囲である情報資産を取り扱う全ての者に対して、意識向上を主とした積極的な情報セキュリティ教育を必要に応じて行う。また、セキュリティインシデント発生時における職員の対応力を向上させるため、必要に応じて訓練を行う。

２　企業団の情報資産を取り扱う全ての者は、企業団が必要に応じて提供する情報セキュリティ教育及び訓練を受けなければならない。

（情報セキュリティの点検及び見直し）

第９条　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点検を実施する。

２　点検の結果、情報セキュリティに見直しが必要となった場合や、情報資産を取り巻く状況の変化に迅速かつ適切に対応するために、新たな対策等が必要になった場合は、情報セキュリティポリシーの見直しを適宜行う。