津島市上下水道部情報セキュリティ基本方針

１　目的

本基本方針は、津島市上下水道部が扱う情報システムのうち、津島市情報セキュリティポリシーの適用範囲外となる情報システム（以下、部門システムという。）について、情報資産の機密性、完全性及び可用性を維持するための対策（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

（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、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）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。

（４）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。（５）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。

（５）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。

（６）津島市上下水道部情報セキュリティポリシー

本基本方針及び津島市上下水道部情報セキュリティ対策基準をいう。

（７）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。

（８）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。

（９）部門システム系

津島市情報セキュリティポリシーの適用範囲外となる情報システムのうち、LGWAN 接続系及びインターネット接続系以外のものをいう。

(10) 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。

(11) 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、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。
(12) 部門システム
上下水道部において使用する情報システムで、津島市情報セキュリティポリシーの適用範囲外となるものをいう。

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。
（１）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
（２）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、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
（３）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
（４）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
（５）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
（１）行政機関の範囲
本基本方針が適用される行政機関は、上下水道部管理課、工務課、又吉配水場、神守配水場及び下水終末処理場とし、部門システムを取扱う場合に適用されるものとする。
（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　津島市上下水道部情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務
津島市上下水道部情報セキュリティポリシーは、津島市上下水道部が所掌する情報資産のうち部門システムに関する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であり、情報セキュリティ対策はこれによらなければならない。
津島市上下水道部が所掌する情報資産のうち部門システムに携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行

に当たって津島市上下水道部情報セキュリティポリシー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、以下の情報セキュリティ対策を講じる。

（１）管理体制

津島市上下水道部の情報資産について、情報セキュリティ対策を推進・管理するための体制を確立する

（２）情報資産の分類と管理

津島市上下水道部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、その重要度に応じた情報セキュリティ対策を行うものとする。

（３）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。

①LGWAN 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。

②インターネット接続系においては、ウイルス対策ソフト等による情報セキュリティ対策を実施する。

③部門システム系においては、LGWAN 接続系及びインターネット接続系とは接続せず、部門システムのみの閉域網で情報システムを構築する。

（４）物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（５）人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等及び外部委託事業者に津島市上下水道部情報セキュリティポリシーの内容を周知徹底する等の対策を講ずる。

（６）技術的セキュリティ

情報資産を外部からの不正なアクセス等から適切に保護するため、セキュリティホールへの迅速な対応を行うとともに、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を講ずる。

（７）運用

ネットワークの監視、津島市上下水道部情報セキュリティポリシーの遵守状況の確認、システム開発等の外部委託を行う際のセキュリティの確保等の運用面の対策を講ずる。また、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ずる。

（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。
（９）評価・見直し
津島市上下水道部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し、運用改善を行い、情報セキュリティの向上を図る。津島市上下水道部情報セキュリティポリシーの見直しが必要な場合は、適宜津島市上下水道部情報セキュリティ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
津島市上下水道部情報セキュリティポリシーが遵守されていることを検証するため、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ものとする。

８　津島市上下水道部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及び自己点検の結果、津島市上下水道部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及び発生時の損失等を分析し、リスクを検討したうえで、津島市上下水道部情報セキュリティポリシーを見直す。

９　津島市上下水道部情報セキュリティ対策基準の策定
津島市上下水道部の様々な情報資産について、６の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、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を明記した津島市上下水道部情報セキュリティ対策基準を策定する。
なお、津島市上下水道部情報セキュリティ対策基準は、公にすることにより津島市の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。

10　津島市上下水道部情報セキュリティ実施手順の策定
津島市上下水道部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津島市上下水道部情報セキュリティ実施手順を策定するものとする。
なお、津島市上下水道部情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。