津島市情報セキュリティポリシー

平成１５年１０月　１日　　策定
平成１８年　６月　１日　一部改正
平成１９年　６月　１日　一部改正
平成２４年　１月　１日　一部改正
平成２７年１０月　１日　一部改正
令和　５年　３月２４日　一部改正
令和　８年　３月３１日　一部改正

津島市

＜　目　次　＞

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、津島市が所掌する情報資産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を総称する。情報セキュリティポリシーは、津島市が所掌する情報資産に関する業務に携わる全職員、非常勤職員等の運用従事者（以下「職員等」という。）及び委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。

しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に柔軟に対応することも必要である。

よって、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）とに分け、下記２階層に分けて策定する。

① 情報セキュリティ基本方針
② 情報セキュリティ対策基準

文　書　名		内　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準

また、必要に応じ、情報セキュリティポリシーに基づく具体的な情報セキュリティ対策の実施手順として「情報セキュリティ実施手順」を策定することとする。

第1章　情報セキュリティ基本方針

1　目的

津島市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部への漏えい等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産や情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠であり、ひいては、このことが津島市に対する市民からの信頼の維持向上に寄与するものである。

そのため、津島市の情報資産の機密性、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）を整備するために津島市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については津島市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

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）及び電磁的記録媒体（以下「記録媒体」という。）で構成され、処理を行う仕組みをいう。

(2)　情報システム

業務系のコンピュータ（ネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、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

情報が不正に破壊、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だけが、必要なとき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。

(6)　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。

(7)　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（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(8)　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（マイナンバー利用事務系を除く。）。

(9)　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。

(10) 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。

3 情報資産への脅威

情報資産が脅威にさらされる発生度合や発生した場合の影響を考慮し、特に認識すべき脅威を以下のとおり定める。

(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・削除、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、火災等の災害並びに事故、故障等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

情報セキュリティポリシーの適用範囲は、市長部局、行政委員会、議会事務局、消防本部とする。

教育委員会及び市の経営する地方公営企業については、市長部局が管理するネットワークを扱う部署を適用範囲とし、適用範囲外となる部署においても、別途、情報セキュリティポリシーに準拠した各組織における情報セキュリティポリシーを策定し、遵守することにより、市全体の情報セキュリティレベルを維持することとする。

(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 コンピュータ、情報システム及びネットワーク並びにこれらに関する設備及び記録媒体

② コンピュータ、情報システム及びネットワークで取り扱う情報

③ 情報システム仕様書及びネットワーク構成図等のシステム関連文書

5 情報セキュリティポリシーの位置付けと職員等及び委託事業者の義務

情報セキュリティポリシーは、津島市が所掌する情報資産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。

津島市が所掌する情報資産に関する業務に携わる全ての職員等及び委託事業者は、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

3 節で示した脅威から情報資産を保護するため、以下の情報セキュリティ対策を講ずるものとする。

(1) 管理体制

津島市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ものとする。

(2) 情報資産の分類

津島市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。

① 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、住民情報の流出を防ぐ。

② 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。

③ 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。高度な情報セキュリティ対策として、インターネット通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(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、全ての職員等及び委託事業者に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対策

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、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。

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、利用する運用手順を定め、ソーシャルメディアサービスごとの責任者を定める。

7　情報セキュリティ監査及び自己点検の実施

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　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、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、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

津島市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情報セキュリティ対策基準を策定する。

なお、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 情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するための対策手順として情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、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。