糸島市サイバーセキュリティを確保するための方針

令和８年３月 30 日　７糸情第 104 号
令和８年３月 31 日　７糸議第 513 号
令和８年３月 31 日　７糸教総第 830 号
令和８年３月 31 日　７糸選第 312 号
令和８年３月 31 日　７糸公第 40 号
令和８年３月 31 日　７糸監第 157 号
令和８年３月 31 日　７糸農委第 952 号
令和８年３月 30 日　７糸固評委第２号
令和８年３月 31 日　７糸業第 410 号

第１章　総則

（目的）

第１条　この方針は、糸島市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、本市が実施する情報セキュリティ対策についての方針を定めることを目的とする。

（定義）

第２条　この方針において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

⑴　職員等　糸島市の情報資産を取扱う特別職、一般職の職員、派遣労働者、糸島市が貸与するコンピュータを使用して委託業務を行う委託先事業者の社員等をいう。

⑵　コンピュータ　パソコン及びサーバ（いずれもソフトウェアを含む。以下同じ。）並びにその周辺機器で、機器内部に情報を記録可能なものをいう。

⑶　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。

⑷　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。

⑸　情報資産　情報システムを構成する機器及びそのシステムで取り扱うすべての電磁的記録（電磁的記録の印刷物及び電磁的記録の入力の基となった届出書等の紙媒体の文書を含む。）並びに情報システムの開発、運用に係る紙媒体の文書をいう。

⑹　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。

⑺　記録媒体　情報を記録するための媒体で、ハードディスク、USBメモリ、CD-R、DVD-R等をいう。

⑻　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。

⑼　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。

⑽　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。

(11) 情報セキュリティポリシー　本市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たものをいう。

（対象とする脅威）

第３条　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

（適用範囲）

第４条　この方針が適用される機関は、市長、議会、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会及び公営企業管理者の権限を行う市長及び消防長とする。

２　この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

（職員等の遵守義務）

第５条　職員等は、情報セキュリティの重要性について共通の認識を持ち、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しなければならない。

（情報セキュリティ対策）

第６条　第３条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) 組織体制

本市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。

(2) 情報資産の分類と管理

本市の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3)　情報システム全体の強靭性の向上

取り扱う情報資産の重要性及び使用する情報システムの目的等に応じてネットワークの通信経路を分割し、情報システム全体の強靭性向上対策を講じる。

(4)　物理的セキュリティ

サーバ、情報システム室、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。

(5)　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。

(6)　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。

(7)　運用

情報システムの監視、情報セキュリティ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、情報セキュリティポリシーの運用面の対策を講じるものとする。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。

(8)　業務委託と外部サービスの利用

①　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。

②　約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

③　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する。

(9)　評価・見直し

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。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第７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情報セキュリティ監査及び自己点検を実施する。

（情報セキュリティポリシーの見直し）

第８条　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、情報セキュリティポリシーを見直す。