浜田市議会情報セキュリティ基本方針

1　目的

本基本方針は、浜田市議会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、浜田市議会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及び通信装置（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。

3　対象とする脅威

情報資産に対する脅威として、次に掲げる脅威を想定し、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、外部委託管理の不備、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

⑴　対象機関の範囲

本基本方針が適用される機関は、議会とし、次に掲げる者（以下これらを「議員等」という。）に適用する。ただし、「浜田市情報セキュリティポリシー」で適用される情報資産を取り扱う場合は、当該「浜田市情報セキュリティポリシー」を適用するものとする。

ア　議員

イ　議会事務局職員（会計年度任用職員、派遣その他の議会事務局で勤務する職員を含む。以下同じ。）

⑵　情報資産の範囲

ア　ネットワーク、情報システム及びこれらに関する施設、設備、電磁的記録媒体

イ　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。）

ウ　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　議員等の遵守義務

議員等は、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本基本方針を遵守しなければならない。

6　議会事務局職員の遵守義務

上記５に定めるもののほか、議会事務局職員は、浜田市情報セキュリティポリシー及び実施手順を遵守しなければならない。

7　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、以下の対策を講じる。

⑴　組織体制

ア　議会の最高情報セキュリティ責任者（CISO：Chief Information Security Officer）は、議長とする。

イ　議会事務局長は、議会の情報セキュリティに関する実務責任者として、必要な措置を講ずるものとする。

ウ　議会事務局長は、必要に応じて情報セキュリティ担当者を指名し、情報資産の管理及び情報セキュリティ対策の実施を行わせることができる。

エ　議会は、執行機関の情報セキュリティ担当部門と連携し、必要な情報共有及び協力を行うものとする。

⑵　情報資産の分類と管理

議会が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、当該分類に基づき情報セキュリティ対策を行う。

⑶　物理的セキュリティ

情報資産を収容する施設・設備及びパソコン、モバイル端末等の情報機器の管理について、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、議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。

⑸　技術的セキュリティ

情報システムの管理、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、情報セキュリティポリシーの遵守状況の確認等の運用管理を実施するとともに、情報資産に対するセキュリティ侵害が発生した場合には、速やかに市の関係部局と連携し対応する。

⑺　外部サービス（クラウドサービスを含む。）の利用

外部サービス（クラウドサービスを含む。）を利用する場合には、必要に応じて利用にかかる規程を整備し対策を講じる。

8　情報セキュリティ監査及び自己点検の実施

本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。

9　本基本方針の見直し

情報セキュリティ監査及び自己点検の結果、本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、本基本方針を見直す。

10　他の執行機関等における方針との関係

浜田市の他の執行機関等が管理運用するネットワーク及び情報システムを利用する場合は、当該執行機関等の定める方針によるものとする。

附　則

令和８年４月１日施行