日置市議会
情報セキュリティ基本方針

令和８年４月

１．目的

本基本方針は、日置市議会（以下「市議会」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するため、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

(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。）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) 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。

(4) 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。

(5) 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。

(6) 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並びに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、改ざん及び消去、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、操作及び設定のミス、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) 大規模かつ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) 適用の範囲

本基本方針は、市議会議員及び議会事務局職員（以下「議員等」という。）に適用する。

(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。

ア ネットワーク及び情報システム並びにこれらに関する施設、設備及び電磁的記録媒体

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、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は、本基本方針及び情報セキュリティに関する各種規程等を遵守しなければならない。

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、次の情報セキュリティ対策を講ずる。

(1) 組織体制

市議会の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

市議会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、当該分類に基づき情報セキュリティ対策を講ずる。

(3) 物理的セキュリティ

通信回線及び議員等のタブレット、パソコン等の管理について、物理的な対策を講ずる。

(4) 人的セキュリティ

情報セキュリティに関し、必要に応じて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ずる。

(5) 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ずる。

(6) 運用

情報システムの監視、情報セキュリティ対策の遵守状況の確認、業務委託を行う際のセキュリティ確保等、本基本方針及び情報セキュリティに関する各種規程等の運用面の対策を講ずる。

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切に対応するため、緊急時対応計画を策定する。

(7) 業務委託と外部サービス（クラウドサービス）の利用

ア　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ずる。

イ　外部サービス（クラウドサービス）を利用する場合には、必要に応じて利用に係る規程を整備し対策を講ずる。

ウ　ソーシャルメディアサービスを利用する場合は、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

情報セキュリティ対策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。

8．情報セキュリティ対策の見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティ対策の見直しが必要となった場合又は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となった場合には、本基本方針及び情報セキュリティに関する各種規程等を見直す。

9．情報セキュリティ対策基準

上記6から8までに規定する対策等を実施するための具体的な遵守事項、判断基準等については、日置市行政情報セキュリティポリシーの規定により定める情報セキュリティ対策基準の例によるものとする。

10．情報セキュリティ実施手順

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については、日置市行政情報セキュリティポリシーの規定により定める情報セキュリティ実施手順の例によるものとする。

11．その他

本基本方針に定めるもののほか、市議会の情報セキュリティ対策に関し必要な事項は、日置市情報セキュリティポリシーの規定の例によるものとする。