

千歳市議会情報セキュリティ基本方針

令和8年4月1日 制定

1 目的

この基本方針は、本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、本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

この基本方針における用語の意義は、次に定めるところによる。

(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等で構成され、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、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、マネジメントの欠陥、機器故障等の非意図的な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) 実施機関の範囲

千歳市議会（議員活動に関わる議会事務局を含む）

(2) 情報資産の範囲

この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マニュアル等のシステム関連文書

表1. 情報資産の例

情報資産の種類	情報資産の例
①ネットワーク	通信回線、ルータ等の通信機器等
②情報システム	パソコン、貸与タブレット、オペレーティングシステム、ソフトウェア等
③電磁的記録媒体	端末、通信回線装置等に内蔵される内蔵電磁的記録媒体、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体等
⑤ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ等（これらを印刷した文書を含む。）
⑥システム関連文書	プログラム仕様書、オペレーションマニュアル、端末管理マニュアル等

5 議員の遵守義務

議員は、情報セキュリティの重要性について共通の認識を持ち、議員活動に当たって本基本方針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、以下の情報セキュリティ対策を講じる。

(1) 組織体制

本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。

ア 議長を情報セキュリティ責任者とする。情報セキュリティ責任者は、情報セキュリティ対策の統括的な権限及び責任を有する。情報セキュリティ責任者は、緊急時等における連絡体制の整備、本基本方針の遵守に関する意見の集約並びに議員に対する教育、訓練、助言及び指示を行う。

イ 議会事務局長を情報セキュリティ管理者とする。情報セキュリティ管理者は、情報セキュリティ対策に関する管理責任を有する。情報セキュリティ管理者は、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

ウ 議員は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者に報告し、必要に応じて議会運営委員会で協議し、議長（情報セキュリティ責任者）が対処を決定する。

(2) 情報資産の分類と管理

本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実施する。

(3) 物理的セキュリティ

通信回線、パソコン、貸与タブレット等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、議員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。

(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じる。

(6) 運用

情報システムの監視、本基本方針の遵守状況の確認や必要に応じた監査等、本基本方針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。

(7) 外部サービスの利用

外部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。

(8) 評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。本基本方針の見直しが必要な場合は、適宜見直しを行う。

7 情報セキュリティ監査及び自己点検の実施

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。

8 情報セキュリティ基本方針の見直し

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。

9 情報セキュリティ対策基準の策定

上記6、7及び8に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を必要に応じて策定する。

なお、情報セキュリティ対策基準は、公にすることにより本市議会の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。

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情報セキュリティ実施手順を必要に応じて策定する。

なお、情報セキュリティ実施手順は、情報セキュリティ対策基準と同様に非公開とする。