十和田市議会サイバーセキュリティを確保するための方針

制　定：令和８年３月

十 和 田 市 議 会

目　次

十和田市議会サイバーセキュリティを確保するための方針

1　目的

本方針は、十和田市議会（以下「本市議会」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、本市議会が実施する情報セキュリティインシデント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）情報資産

本市議会が保有し、又は管理する情報（紙媒体、電磁的記録媒体及びクラウド上のデータを含む。）並びに本市議会が管理する情報システムをいう。

（2）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。

（3）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。

（4）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。

（5）情報セキュリティポリシー

本方針及び情報セキュリティ対策基準をいう。

（6）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。

（7）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。

（8）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。

（9）情報セキュリティインシデント

情報管理やシステム運用に関して保安上の脅威（障害・事故・システム上の欠陥）となる事象をいう。

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、プログラム上の欠陥、操作ミス、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、通信の途絶等のインフラ障害からの波及等

４　適用範囲

（1）情報資産の範囲

本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、情報システム及びこれらに関する設備、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

（2）職員等の範囲

本方針が対象とする職員等は、次のとおりとする。

市議会議員（本市議会が管理する情報資産（貸与端末、非公開資料等）を保有又は利用する範囲に限る。）、議会事務局職員及び会計年度任用職員

５　職員等の遵守義務

（1）役割

議会における情報セキュリティ対策を推進するため、次に掲げる者の役割を定める。

①　議会事務局長

議会における情報セキュリティ管理の総括、必要な指示及び関係者との調整

②　議会事務局における情報セキュリティ担当者

情報資産の取扱いに係る運用管理、教育・注意喚起（議員向け研修を含む。）、情報セキュリティインシデントの一次対応及び必要な報告

③　市議会議員、議会事務局職員及び会計年度任用職員

情報資産の適切な取扱い及び本方針の趣旨の尊重

（2）義務

議会の情報資産に係る情報セキュリティインシデントを認知したものは、速やかに議会事務局の情報セキュリティ担当者に報告しなければならない。

議会事務局長は、平時から市の関係部局と連携し必要な支援・助言を受けつつ、必要に応じて関係部局その他関係機関と連携し、被害拡大防止及び再発防止のための措置を講ずる。

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、市の関係部局の助言を得て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ための体制を確立する。

（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、安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。

（3）情報システム全体の強靭性の向上

議会事務局が利用する情報システムについては、市の情報システム担当課と連携し、市の情報セキュリティ対策基準等に準拠して、通信経路の分割、無害化、不正通信の監視その他必要な技術的対策を講じる。

（4） 物理的セキュリティ

通信回線等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、外部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切に対応するための体制を整える。

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、見直すものとする。

附　則

本方針は、令和８年４月１日から施行する。