

東郷町議会
情報セキュリティポリシー

< 東郷町議会 >

< 改訂履歴 >

版 数	発行（改定）年月日	改 訂 内 容
第 1 . 0 版	令和 8 年 4 月 1 日	初版

目 次

東郷町議会情報セキュリティ基本方針.....	1
第1章 基本的考え方.....	1
第2章 定義.....	1
1 ネットワーク.....	1
2 情報システム.....	1
3 情報セキュリティ.....	1
4 情報セキュリティポリシー.....	1
5 機密性.....	1
6 完全性.....	1
7 可用性.....	2
8 インターネット接続系.....	2
第3章 対象とする脅威.....	2
第4章 適用範囲.....	2
1 組織の範囲.....	2
2 情報資産の範囲.....	3
第5章 遵守義務.....	3
第6章 情報セキュリティ対策.....	3
1 組織体制.....	3
2 物理的セキュリティ.....	3
3 人的セキュリティ.....	3
4 技術的セキュリティ.....	3
5 運用.....	3
6 業務委託と外部サービス（クラウドサービス）の利用.....	4
第7章 情報セキュリティ監査及び自己点検の実施.....	4
第8章 情報セキュリティポリシーの評価・見直し.....	4

東郷町議会情報セキュリティ基本方針

第1章 基本的考え方

東郷町議会情報セキュリティ基本方針（以下「本基本方針」という。）は、東郷町議会（以下「本町議会」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、本町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。

また、本基本方針は、地方自治法の一部を改正する法律（令和6年法律第65号）による改正後の地方自治法第244条の6第1項で定めるサイバーセキュリティを確保するための方針に位置付けるものとする。

なお、東郷町議会議員（以下「議員」という。）個人が、議員活動の中で取得した情報資産は、本基本方針の対象外とする。

第2章 定義

本基本方針において、次の各号に掲げる用語の意義は、当該各号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。

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 情報セキュリティポリシー

本基本方針及び必要に応じて作成した情報セキュリティ対策基準をいう。

5 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。

6 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。

7 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。

8 インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

第3章 対象とする脅威

情報資産に対する脅威として、次の各号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。

- 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、火災等その他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

第4章 適用範囲

1 組織の範囲

本基本方針が適用される組織は、本町議会とする。

ただし、「東郷町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、「東郷町情報セキュリティポリシー」を遵守するものとする。

2 情報資産の範囲

本基本方針が対象とする情報資産は、次の各号に掲げるとおりとする。

- (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

第5章 遵守義務

議員及び議会事務職員は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行にあ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。

第6章 情報セキュリティ対策

上記第3章に掲げる脅威から情報資産を保護するために、次の各号に掲げる情報セキュリティ対策を講じる。

1 組織体制

本町議会の保有する情報資産について、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 物理的セキュリティ

パソコン等の管理について、物理的な対策を講じる。

3 人的セキュリティ

情報セキュリティに関し、議員及び議会事務局職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。

4 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。

5 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。

6 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、情報セキュリティ要件を明記した契約を締結し、委託先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する。

外部サービス（クラウドサービス）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。

第7章 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点検を実施する。

第8章 情報セキュリティポリシーの評価・見直し

情報セキュリティの自己点検の結果、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、リスクを検討した上で本情報セキュリティポリシーを見直す。

情報セキュリティ対策を推進する組織体制

<p>最高情報セキュリティ責任者 (CISO : Chief Information Security Officer)</p>	<p>(ア)議長を CISO とする。CISO は、本町議会における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。 (イ)CISO は、本基本方針に定められた自らの担務を、情報セキュリティ責任者その他の基本方針に定める責任者に担わせることができる。</p>
<p>情報セキュリティ責任者</p>	<p>(ア)議会事務局長を CISO 直属の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、CISO を補佐しなければならない。 (イ)情報セキュリティ責任者は、本町議会の情報セキュリティ対策、全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。</p>
<p>情報セキュリティ・システム管理者</p>	<p>(ア)議会事務局局長補佐を情報セキュリティ・システム管理者とする。 (イ)情報セキュリティ・システム管理者は、町議会の情報セキュリティ対策に関する権限及び責任を有する。 (ウ)情報セキュリティ・システム管理者は、所管する情報システムにおける開発、設定の変更、見直し等を行う権限及び責任を有する。</p>
<p>情報システム担当者</p>	<p>情報セキュリティ・システム管理者の指示等に従い、情報システム開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。</p>

自己点検シート

チェック項目	はい	いいえ
端末にパスワードを設定しているか。	<input type="checkbox"/>	<input type="checkbox"/>
OS やセキュリティソフトは最新か。	<input type="checkbox"/>	<input type="checkbox"/>
離席時に画面ロックをかけているか。	<input type="checkbox"/>	<input type="checkbox"/>
不審なメールの添付ファイルを開いていないか。	<input type="checkbox"/>	<input type="checkbox"/>
重要資料を公共の場で不用意に広げていないか。	<input type="checkbox"/>	<input type="checkbox"/>

令和 年 月 日

議員名 _____