

久御山町議会情報セキュリティ基本方針

令和8年4月制定

1. 目的

この基本方針は、久御山町議会（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。

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、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）機密性

情報にアクセスすることを認められた者が、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。

（7）インターネット接続系

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。

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、

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

(3) 地震、地雷、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

本基本方針が対象とする情報資産は、本町議会が取り扱う次のものとする。

ただし、久御山町が議会事務局職員の使用に供する情報資産については、その取り扱いについては久御山町情報セキュリティポリシーに従うものとし、本方針の適用範囲外とする。

(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

5. 議員等の遵守義務

議員及び議会事務局職員（以下、「議員等」という。）並びに委託事業者等は、情報セキュリティの重要性を認識するとともに、活動及び業務の遂行に当たって情報セキュリティ基本方針及び関係法令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じる。

(1) 組織体制

本町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) 情報資産の分類及び管理

情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に応じた情報セキュリティ対策を実施する。

(3) 情報システム全体の強靱性の向上

不正通信の監視機能の強化等の情報セキュリティ対策を講じる。

(4) 物理的セキュリティ

情報システムを設置する部屋、通信回線及び議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、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。

(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

情報セキュリティ基本方針の遵守状況の確認、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切に対応するための危機管理対策を講じるよう努める。

(8) 業務委託と外部サービスの利用

業務委託を行う場合は、委託業者を選定し、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じる。外部サービスを講じる場合は、利用に係る規定を整備し、対策を講じる。

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、情報セキュリティ基本方針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になった場合等には、情報セキュリティ基本方針を見直す。