愛川町議会情報セキュリティ基本方針

１　目的

本基本方針は、愛川町議会（以下「議会」という。）が保有し、又は利用する情報資産について、その機密性、完全性及び可用性を維持するため、議会が実施すべき情報セキュリティ対策に関する基本的事項を定め、もって議会運営の公正性、信頼性及び継続性を確保することを目的とする。

２　定義

本基本方針において使用する用語の意義は、愛川町議会の個人情報の保護に関する条例（令和５年愛川町条例第７号）で使用する用語の例によるほか、次の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、その他構成機器（ハードウエア及びソフトウエア）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。

(7)　インターネット接続系　インターネットメール、Ｗｅｂ閲覧、議会ホームページ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を取り扱うデータをいう。

３　情報資産への脅威

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、無許可ソフトウエ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)　本基本方針は、次に掲げる者に適用する。

ア　議員

イ　議会事務局職員

ウ　会計年度任用職員、委託事業者その他関係者

(2)　情報資産の適用範囲

ア　議会が管理又は利用する情報及び文書

イ　議会独自に設置した情報機器（議員用ＰＣ等）

ウ　議会独自に設置したネットワーク及びインターネット接続環境

エ　本会議及び委員会の会議録データ

オ　本会議の映像配信に係るシステム及びデータその他議会運営に必要な情報資産

5　管理体制及び遵守義務

(1)　議会は、情報セキュリティ対策を推進するため、議会事務局長を情報セキュリティ管理責任者とする。

(2)　議員及び職員等は、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)　情報資産の分類及び管理

ア　本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。

イ　本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行う。

(2)　情報システム全体の強靭性の確保

ア　情報セキュリティの強化を目的とし、業務の効率性及び利便性の観点を踏まえ、情報システム全体に対し、対策を講じる。

イ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を講じる。

(3)　物理的セキュリティ対策

ア　サーバ、通信回線及び議員専用のパソコン等の管理について、物理的な対策を講じる。

(4)　人的セキュリティ対策

ア　情報セキュリティに関し、議員及び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。

(5)　技術的セキュリティ対策

ア　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)　運用及び監視

ア　情報システムの監視、本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、本基本方針の運用面の対策を講じるものとする。

イ　情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、被害の拡大防止、原因の把握及び再発防止に必要な措置を講じるものとする。

7　業務委託及び外部サービス

上記６の対策にあたっては、必要に応じて町部局の協力を得るものとする。

(1)　業務委託を行う場合は、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情報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。

(2)　外部サービス（クラウドサービス）を利用する場合には、利用に係る規程を整備し対策を講じる。

(3)　ソーシャルメディアサービスを利用する場合には、利用に係る規定を整備し、管理体制を明確にする。

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

９　情報セキュリティ対策の基準の策定

上記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を定める情報セキュリティ対策基準を策定する。

令和８年３月２５日策定