野々市市議会情報セキュリティ基本方針

１　目的

野々市市議会情報セキュリティ基本方針（以下「基本方針」という。）は、野々市市議会（以下、「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、議会の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）情報資産　次に掲げるものをいう。

ア　ネットワーク及び情報システム並びにこれらに係る機器及び設備

イ　情報システムの設計図書、ネットワーク構成図等（以下「システム関連文書」という。）

ウ　議会が業務上作成し、又は取得した電子データ

（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）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。

（８）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次の脅威を想定し、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、重要情報の詐取及び内部不正等
（２）情報資産の無断持ち出し、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、監査機能の不備、委託管理の不備、マネジメントの欠陥及び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活動・業務の停止
（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、通信の途絶及び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、議会が取り扱う次のものとする。ただし、市長が議会事務局の職員（再任用職員を含む。）、会計年度任用職員、臨時的任用職員及び労働者派遣契約（事業所等が労働者派遣をすることを約する契約をいう。以下同じ。）により派遣されている者の使用に供する情報資産については、その取り扱いは野々市市情報セキュリティに関する要領に従うものとし、本基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システム関連文書

５　議員及び議会事務局職員の遵守義務

議員及び議会事務局の職員（再任用職員を含む。）並びに会計年度任用職員、臨時的任用職員、労働者派遣契約により派遣されている者等（以下「議員等」という。）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、活動及び業務の遂行に当たって、本基本方針及び関係法令を遵守する義務を負うものとする。

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、以下の情報セキュリティ対策を講じる。
（１）組織体制

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を議会

運営委員会とする。

（２）情報システム全体の強靭性の向上

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

情報システムを設置する施設の管理について、物理的な対策を講じる。

（４）人的セキュリティ対策

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。

（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、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。

また、情報セキュリティ対策の運用にあたっては、本基本方針及び関係要綱等に従って取り組むとともに、緊急事態発生時に迅速に対応できるよう、危機管理対策を講じる。

（７）外部委託

外部委託をする場合には、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。

外部サービスを利用する場合は、利用に係る規定を整備し対策を講じる。

７　議員等からのセキュリティ障害の報告

議員等は、利用しているコンピュータ等（私物の端末を含む。）にセキュリティ障害を発見した場合には、速やかに、議会運営委員会に報告しなければならない。

８　情報セキュリティ監査及び点検の実施

本基本方針が遵守されていることを検証するため、定期的又は必要に応じて、議会運営委員会において情報セキュリティ監査及び点検を実施する。

９　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点検の結果、本基本方針の見直しが必要に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、保有する情報及び利用する情報システムに係る脅威の発生の可

能性及び発生時の損失等を分析し、リスクを検討した上で、本基本方針を見直す。

附　則

この基本方針は、令和８年４月１日から施行する。