三条市議会情報セキュリティ基本方針

第１　目的

三条市議会（以下「議会」という。）における情報資産に対する安全対策を推進するため、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。

第２　定義

１　ネットワーク

サーバ、パーソナルコンピュータ（以下「パソコン」という。）その他機器を相互に接続するための通信網及びこの通信網を構成する機器をいう。

２　情報処理システム

ネットワーク、ハードウェア、ソフトウェア及び記憶媒体で構成された情報を処理する仕組みをいう。

３　情報資産

議会活動のために管理する以下のものとする。

(1) ネットワーク、情報システム及びこれらに関する設備、モバイル端末、電磁的記録媒体

(2) ネットワークおよび情報処理システムで取り扱う情報

(3) ネットワーク構成図及び情報処理システムの仕様書等のシステム関連文書

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　情報セキュリティ対策

情報セキュリティを確保するための対策をいう。

６　情報セキュリティポリシー

この方針をいう。

７　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。

８　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。

９　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。

10　情報セキュリティインシデント

情報セキュリティに関する障害・事故及び欠陥のことをいう。

第３　対象とする脅威

情報資産に対する脅威として以下のものを想定し、情報セキュリティ対策を実施する。

１　意図的要因（故意）

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盗の意図的な要因による情報資産の漏えい・破壊・改ざん・消去等。

２　非意図的要因（過失）

情報資産の無断持ち出し、無許可ソフトウェアの使用や端末接続等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、認証情報又はパスワードの不適切管理、搬送中の事故等による情報資産の盗難、機器の交渉等による情報資産の漏えい・破壊・消去等。

３　災害等による要因

地震、落雷、火災等の災害や電力供給、通信の途絶等のインフラの障害によるサービス及び業務の停止等。（大規模・広範囲の疾病等による要員不足に伴う機能不全等を含む。）

第４　適用範囲

１　対象機関の範囲

情報セキュリティポリシーが適用される機関は、議会とする。ただし、三条市長が管理運営する情報資産（以下「執行部の情報資産」という）は除くものとする。

２　対象者の範囲

情報セキュリティポリシーが適用される対象者は、情報資産に接する全ての議員及び職員（臨時的任用職員及び会計年度任用職員を含む。）（以下「議員等」と総称する。）とする。

また、議員等の私物端末についても、情報資産に接する場合においては情報セキュリティポリシーの対象とする。

３　執行部の情報資産の運用

議会事務局職員（臨時的任用職員及び会計年度任用職員を含む。）が執行部の情報資産を運用する際は、三条市情報セキュリティポリシーを遵守するものとする。

第５　情報セキュリティ対策

議会が所管する情報資産を上記第３に規定する脅威から保護するために、以下の情報セキュリティ対策を講じる。

対策の具体的な遵守事項及び判断基準等は、議長が別に定めることとする。

なお、遵守事項及び判断基準等は、公にすることにより議会活動に重大な支障を及ぼすおそれがあることから非公開とする。

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体制を確立する。

２　情報資産の分類と管理

議会が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。

３　物理的セキュリティ

サーバ、情報処理システム室、通信回線及び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

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などの人的な対策を講じる。

５　技術的セキュリティ

パソコン等の管理、アクセス制御、不正プログラム対策及び不正アクセス対策等の技術的な対策を講じる。

６　運用

情報処理システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託及び外部サービス（クラウドサービス）の利用等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。

第６　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、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。

第７　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、保有する情報資産及び利用する情報処理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、情報セキュリティポリシーを見直す。

第８　議員等の遵守義務

議員等は、情報セキュリティの重要性について共通の認識を持ち、議会活動又は業務の遂行に当たっては、情報セキュリティポリシー及び情報セキュリティ関係法令等を遵守しなければならない。また、契約等により情報資産の利用を認められた外部の事業者等についても業務内容に応じた情報セキュリティを確保させなければならない。

附　則

この方針は、令和８年４月１日から実施する。