竹富町議会情報セキュリティ基本方針

（目的）

第１条 この基本方針は、竹富町議会（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、情報セキュリティ対策に関する基本的な事項を定めることを目的とする。これにより、円滑な議会運営と町民の信頼確保を図る。

（定義）

第２条 この基本方針において、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）情報資産：議会が保有し、又は管理する情報、データ、情報システム、ネットワーク及び電子機器（タブレット端末等）をいう。

（2）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。

（3）機密性：許可さ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。

（4）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。

（5）可用性：許可された者が、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。

（6）インシデント：情報資産の機密性、完全性又は可用性が損なわれ、又はそのおそれがある事象（情報漏えい、ウイルス感染、端末の紛失等）をいう。

（適用範囲）

第３条 この基本方針は、議会が保有し、又は管理する情報資産、及びこれらを取り扱うすべての竹富町議会議員（以下「議員」という。）に適用する。

２ 議会事務局職員の情報セキュリティ対策については、竹富町本庁（執行機関）の情報セキュリティ基本方針等の例による。

（管理体制）

第４条 議長は、議会における情報セキュリティ対策の最高責任者とする。

２ 議会事務局長は、最高責任者を補佐し、情報セキュリティ対策の運用管理、議員への教育・研修や注意喚起、インシデント発生時の連絡調整を行う。

（議員の遵守義務）

第５条 議員は、情報セキュリティの重要性を認識し、次に掲げる事項を遵守しなければならない。

(1)ID やパスワード等を適切に管理し、第三者に開示又は提供しないこと。

(2)貸与されたタブレット端末等の機器について、紛失、盗難又は破損がないよう適切に

保管すること。
（3） 私有の電子機器や電磁的記録媒体等を議会ネットワークに接続する場合は、事前に承認を得ること。
（4） インシデント又はその疑いを発見した場合は、速やかに議長又は議会事務局に報告すること。

（情報セキュリティ対策）
第６条 議会は、情報資産に対する脅威から保護するため、次に掲げる対策を講ずる。
（1）人的対策：情報セキュリティ意識向上のため、議員に対する教育及び研修を定期的に実施する。
（2）技術的対策：不正アクセスやウイルス感染を防止するため、アクセス制御、暗号化、端末の利用制限等の措置を講ずる。
（3）物理的対策：端末や機器の紛失、盗難その他物理的な脅威を防止するための措置を講ずる。
（4） 外部委託・外部サービスの利用：クラウドサービス等の外部サービスを利用する際は、適切なセキュリティ要件を確保する。

（インシデントへの対応）
第７条 インシデントが発生した場合は、被害の拡大防止を最優先とし、速やかに原因調査及び再発防止策を講ずる。
２ 議会は、インシデントへの対応にあたり、必要に応じて町本庁（執行機関）の関係部局と連携し、支援又は助言を得るものとする。

（点検、監査及び見直し）
第８条 議会は、本基本方針の実施状況について、定期的に自己点検等を行う。
２ 議会は、技術の変化、社会情勢の推移、又は点検の結果等に応じて、本基本方針を適宜見直すものとする。

附 則 この方針は、令和８年４月１日から施行する。