吉野川市議会情報セキュリティ基本方針

1　目的

本基本方針は、吉野川市議会（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

本基本方針において、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）　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及びその構成機器（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）　吉野川市議会情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（5）　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。

（6）　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。

（7）　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。

（8）　インターネット接続系

会議システム等の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

議会の情報資産に対する脅威として、次の各号に掲げる脅威を想定し、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又は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、改ざん及び消去、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、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） 大規模又は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、通信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

（１） 本基本方針が適用される機関は、議会（吉野川市議会事務局の職員及び会計年度任用職員（以下「職員等」という。）を除く。）とする。

（２） 本基本方針が対象とする情報資産は、次のとおりとする。

ア　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

イ　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。）

ウ　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　吉野川市議会議員等の遵守義務

吉野川市議会議員（以下「議員」という。）は、情報セキュリティの重要性を認識し、吉野川市議会情報セキュリティポリシー及び情報セキュリティ実施手順に従わなければならない。

６　職員等の遵守義務

職員等は、情報セキュリティの重要性を認識し、吉野川市情報セキュリティポリシー及び吉野川市情報セキュリティ実施手順に従わなければならない。

７　情報セキュリティ対策

３に掲げる脅威から情報資産を保護するために、次の各号に掲げる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ため、議会事務局長を実施責任者とする情報セキュリティ管理体制を整備する。

（２） 情報資産の分類と管理

議会の情報資産を機密性、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実施する。

（３） 物理的セキュリティ

タブレット端末、記録媒体等の管理について、物理的な対策を講じる。

（４） 人的セキュリティ

議員に対し、情報セキュリティに関する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

タブレット端末等の管理、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、吉野川市議会情報セキュリティポリシーの遵守状況の確認を行う際のセキュリティ確保等、吉野川市議会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。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は、速やかに市の担当部局と連携し対応する。

（７） 外部サービス（クラウドサービス）の利用

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

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

8　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、定期的又は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。

9　吉野川市議会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、吉野川市議会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、リスクを検討したうえで、吉野川市議会情報セキュリティポリシーを見直す。

10　吉野川市情報セキュリティ対策基準の策定

本基本方針に基づき、具体的な遵守事項及び判断基準を定める吉野川市議会情報セキュリティ対策基準を策定する。

11　情報セキュリティ実施手順の策定

吉野川市議会情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定する。

なお、情報セキュリティ実施手順は、公開することにより議会の運営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。