益田市議会情報セキュリティ基本方針

1　目的

この基本方針は、益田市議会（以下「市議会」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、市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

（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（ハードウェア及びソフトウェア）をいう。

（2）情報システム
電子計算機(ネットワーク、ハードウェア及びソフトウェア)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）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
インターネットメール、ホームページ管理システム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で取り扱うデータをいう。

3　対象とする脅威

市議会の情報資産に対する脅威として、次に揚げる事項を想定し、必要な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・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）本基本方針が適用される機関

議会及び議会事務局

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

① ネットワーク、情報システム、これらに関する設備、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ネットワーク図等のシステム関連文書

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職員（会計年度任用職員及び非常勤職員、臨時職員を含む。）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を遵守しなければならない。

6 組織体制

市議会は、情報セキュリティ対策を推進する組織体制を確立する。

7 情報資産の分類と管理

本市議会の保有する情報資産は、機密性、完全性及び可用性に応じて分類し、分類に応じた管理を行う。

8 情報セキュリティ対策

上記3で示した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

策を講ずるものとする。

（１）物理的セキュリティ

通信回線及び端末等の管理について、物理的な対策を講じる。

（２）人的セキュリティ

情報セキュリティに関し、議員及び議会事務局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。

（３）技術的セキュリティ

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。

（４）運用及び緊急時対応

情報システムの監視、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。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には、速やかに市の関連部局と連携し対応する。

（５）業務委託と外部サービス（クラウドサービス）の利用

① 業務委託を行う場合には、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。

② 外部サービス（クラウドサービス）を利用する場合には、利用にかかる規定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、運用手順を定めた上で発信できる情報を規定し、利用するサービスごとの責任者を定める。

９　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監査及び自己点検を実施する。

１０　益田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、益田市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かかる脅威の発生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、益田市議会情報セキュリティポリシーを見直す。

１１　益田市議会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た益田市議会情報セキュリティ対策基準を策定する。

なお、益田市議会情報セキュリティ対策基準は、公にすることにより本市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。

１２　情報セキュリティ実施手順の策定

益田市議会情報セキュリティ対策基準に基づき、具体的な運用手順を定めた情報セキュリティ実施手順を別に定める。

なお、情報セキュリティ実施手順は、公にすることにより本市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。

令和８年３月１９日　策定