諫早市議会情報セキュリティ基本方針

令和８年４月
諫早市議会

目　次

諫早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、諫早市議会（以下「本市議会」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、本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）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）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想定するものは、次のとおりとする。

（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、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）組織の範囲

本基本方針が適用される組織は、本市議会とする。

ただし、「諫早市情報セキュリティの基本方針に関する規則（令和８年規則第６号）」が適用される情報資産を取り扱う場合は、「諫早市情報セキュリティの基本方針に関する規則」を遵守するものとする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとし、諫早市議会議員（以下「本市議会議員」という。）個人が、議員活動の中で取得した情報資産は、基本方針の対象外とする。

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ネットワーク図等のシステム関連文書

5　本市議会議員及び議会事務局職員の遵守義務

本市議会議員、議会事務局のすべての職員（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、業務の遂行に当たって情報セキュリティ基本方針及び「諫早市議会会議用システム及びタブレット端末機使用基準」等の議会で策定した情報セキュリティに関する個別の基準（以下「個別基準」という。）を遵守しなければならない。

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ずる。

（１）組織体制

本市議会の情報資産について、適切に情報セキュリティ対策を管理・推進する組織は、議会運営委員会とする。

（２）情報資産の分類と管理

本市議会の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実施する。

（３）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、情報資産の分類に応じたセキュリティ対策を実施する。

（４）物理的セキュリティ対策

通信回線及び端末等への物理的な対策を講ずる。

（５）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ずる。

（６）技術的セキュリティ対策

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ずる。

（７）運用

情報システムの監視、情報セキュリティ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、情報セキュリティ基本方針の運用面の対策を講ずるものとする。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等に迅速かつ適正に対応するため、危機管理対策を講ずるよう努める。

（８）業務委託と外部サービスの利用

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ずる。

外部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ずる。

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。

（９）評価・見直し

情報セキュリティ基本方針や個別基準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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティ基本方針や個別基準の見直しが必要な場合は、適宜見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

情報セキュリティ基本方針や個別基準が遵守されていることを検証するため、必要に応じて議会運営委員において情報セキュリティ監査及び自己点検を実施する。

8　情報セキュリティ基本方針等の見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティ基本方針や個別基準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害等を分析し、リスクを検討したうえで、情報セキュリティ基本方針や個別基準を見直す。

9　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、必要に応じて具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

なお、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。

１０　情報セキュリティ実施手順の策定

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に、必要に応じて具体的な実施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。