

大牟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、本市議会の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、本市議会における情報セキュリティ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) 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。

(2) 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をいう。

(3) 情報システム

コンピュータ、ソフトウェア、ネットワーク等で構成され、情報処理を行う仕組みをいう。

(4) 機密性

情報にアクセスすることを認められた者のみが、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) クラウドサービス

インターネット経由でソフトウェア、データ又はサービスを利用できる仕組みをいう。

(8) 無許可ソフトウェア

利用可否の決定による許可を経ないで利用しようとするソフトウェアをいう。

3 対象とする脅威

情報資産に対する脅威として、以下を想定し、情報セキュリティ対策を講じる。

(1) 不正アクセス、ウィルス攻撃、サービス不能攻撃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

この基本方針が対象とする情報資産は、次に掲げるものであって、本市議会が保有し、又は管理するものとする。

- (1) 情報システム及びネットワーク並びにこれらに関する設備及び記録媒体
- (2) 情報システム及びネットワークで取り扱う情報(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 議員及び事務局職員（以下「職員」という）の責務

議員及び職員は、情報セキュリティの重要性について共通の認識を持ち、議会運営及び議会活動に当たってこの基本方針及び関連する法令等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じる。

(1) 組織体制

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

情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき管理を行う。

(3) 物理的対策

情報資産を損傷、破壊、盗難等から保護するために機器管理上の物理的な対策を講じる。

(4) 人的対策

情報セキュリティに関し、議員及び職員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。

(5) 技術的対策

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じる。

(6) 運用に関する対策

情報システムの監視、クラウドサービス利用における対策、情報セキュリティ対策の実施状況の確認及び緊急事態が発生した際の迅速かつ適切な対応に関する対策その他運用に関して必要な対策を講じる。

(7) 評価及び見直し

情報セキュリティに関する状況の変化等に基づき、情報セキュリティの状況を評価するとともに、必要に応じて運用改善及びこの方針の見直しを行い、情報セキュリティの向上を図るものとする。

7 他の執行機関等における方針等との関係

他の執行機関等が管理し、運用する情報システム及びネットワークの利用については、他の執行機関等における情報セキュリティに関する方針等によるものとする。

8 その他

この基本方針ほか情報セキュリティに関し必要な事項は、別に定める。

令和8年3月24日策定