焼津市議会

情報セキュリティポリシー

（情報セキュリティ基本方針）

令和８年４月

静岡県焼津市議会

第１章　　情報セキュリティ基本方針

１　目的

情報セキュリティ基本方針は、焼津市議会（以下「本市議会」という。）が保有する情報資産を人的脅威や災害、事故等から防御することを目的とする。

２　定義

（１）個人情報

氏名、生年月日その他の記述等により特定の個人を識別できるものをいう。

単独では個人を識別できない情報でも、他の情報と容易に照合することができ、それにより特定の個人を識別できものを含む。ただし、公人として公表しているものを除く。

（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（ハードウェア及びソフトウェア）をいう。

（３）記録媒体

電磁的記録媒体並びに紙媒体をいう。

（４）情報システム

本市議会が管理するコンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

（５）公文書

本市議会議員及び市職員が職務上作成し、又は取得した文書及び電磁的記録をいう。（図面及び動画等を含む。）

（６）情報資産

情報システム及び公文書をいう。

（７）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。

①機密性（漏らさない）

情報にアクセスすることを認められた者だけが、アクセスできる状態を確保すること。

②完全性（壊さない）

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。

③可用性（必要な時に使える）

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、アクセスできる状態を確保すること。

３　適用範囲

情報セキュリティ基本方針が適用される範囲は、本市議会議員及び本市議会事務局職員（以下「市議会議員等」という。）とする。

4　遵守義務

市議会議員等は、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関係法令、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。

5　情報セキュリティ管理体制

情報セキュリティ対策を推進・管理するための組織体制を確立する。

6　情報資産の分類

情報資産をその重要度に応じて分類し、それに応じた情報セキュリティ対策を行う。

7　情報資産への脅威

情報資産に対する脅威として、特に認識すべき脅威は、以下のとおりとする。

（1）部外者の侵入による機器又は情報資産の漏えい・破壊・盗難・改ざん・消去等

（2）内部不正による機器又は情報資産の漏えい・破壊・盗難・改ざん・消去等

（3）故意の不正アクセスやコンピュータウィルス攻撃等のサイバー攻撃

（4）プログラム上の欠陥、操作・設定ミス、メンテナンス不備、機器故障等の非意図的要因による機器又は情報資産の漏えい・破壊・盗難・改ざん・消去等

（5）地震、落雷、火災等の災害によるサービス及び業務の停止

8　情報セキュリティ対策

情報資産を脅威から保護するため、以下の情報セキュリティ対策を実施する。

（1）人的セキュリティ対策

情報セキュリティに関し、市議会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。

（2）物理的セキュリティ対策

情報資産への損傷・妨害等から保護するために、機器管理上の物理的な対策を講ずる。

（3）技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、コンピュータウィルス対策等の技術的対策を講ずる。

（4）運用

情報セキュリティポリシーの実効性を確保するため、運用面における必要な措置を講ずる。また、セキュリティ侵害が発生した場合に迅速かつ適切に対応するための体制を整える。

9　情報セキュリティ対策基準の策定

情報セキュリティ対策を講ずるにあたっては、遵守すべき事項及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定する。

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を遵守し、情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ実施手順を策定する。

11　情報セキュリティポリシーの公開

情報セキュリティ対策基準及び実施手順については、議会運営に重大な支障を及ぼす恐れがあることから、非公開とし、基本方針についてのみ公開するものとする。

12　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。

13　見直し

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は、情報セキュリティを取り巻く状況の変化に対応するため、必要に応じて見直しを実施する。

変更が必要な場合には、直ちに必要部分を変更し、その内容を全ての対象者に通知する。