高松市議会情報セキュリティ基本方針

令和８年４月１日

目次

１．目的

この基本方針は、本市議会が保有する、情報セキュリティ対策の基本的な方針として、この基本方針と高松市議会情報セキュリティ対策基準（以下「対策基準」という。）で構成する高松市議会情報セキュリティに関する方針（以下「情報セキュリティポリシー」という。）の位置付けと適用範囲等に関し必要な事項を定めることにより、本市議会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とともに、危機発生時における適切な対応を図ることを目的とする。

２．定義

情報セキュリティポリシーにおいて、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た、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。

３．対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

a) 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、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

b) 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

c) 地震、落雷、火災等の災害によるサービスや業務の停止等

d) 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

e) 電力供給の途絶、通信の途絶又は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） 対象範囲

本基本方針は、本市議会が保有する情報資産の利用者（以下「利用者」という。）に適用する。

（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情報

５．利用者の遵守義務

利用者は、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．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

本市議会の保有する情報資産について、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

本市議会の保有する情報資産を、機密性、完全性、可用性の維持の程度からなる重要性分類ⅠからⅢに分類し、当該分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じて取るべき管理方法と情報セキュリティ対策を実施する。

a)　重要性分類Ⅰ

ア　行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書。

イ　行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きいもの。

ウ　行政事務で取り扱う情報資産のうち、基本的に公表することを前提としていないもの。

b)　重要性分類Ⅱ

行政事務で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないもの。

c)　重要性分類Ⅲ

上記ａ）及びｂ）以外の情報資産

（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に、業務の効率性や利便性の観点を踏まえ、不正通信の監視機能の強化等の高度な情報セキュリティ対策を行う。

（４） 物理的セキュリティ

サーバ、サーバ等を管理する区域、通信回線や利用者のパソコン等（貸与するタブレット端末を含む。）の管理について、物理的な対策を講じる。

（５） 人的セキュリティ

情報セキュリティに関し、利用者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等の必要な対策を講じる。

（６） 技術的セキュリティ

コンピュータやサーバ（クラウドサーバを含む。）等の管理、アクセス制御、不正プログラム対策や不正アクセス対策等の技術的な対策を講じる。

（７） 運用

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行う。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、緊急時対応計画を策定する。

（８） 業務委託と外部サービス（クラウドサービス）の利用

a) 業務委託する場合には、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く措置を講じる。

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

c) 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。情報セキュリティポリシーの見直しが必要な場合は、

適宜情報セキュリティポリシーの見直しを行う。

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。

８．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、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、情報セキュリティポリシーを見直す。

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、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、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ものとする。

なお、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。

11．その他

この基本方針に定めるもののほか必要な事項は、別に定める。