豊見城市情報セキュリティ基本方針

（第 6 版）

令和 8 年 3 月　　改　　定

平成 19 年 1 月　　策　　定

豊見城市

豊見城市情報セキュリティ基本方針の改定の履歴

版数	改定年月	改定内容	承認者	作成部署
初版	平成19年1月	新規制定	豊見城市情報化推進委員会	企画部　企画振興室
第2版	平成29年7月	①地方公共団体における情報セキュリティポリシーに関するガイドライン（平成27年3月版総務省改定）に基づくもの ②平成29年度組織改革に伴う部及び課の統廃合によるもの	豊見城市情報化推進委員会	企画部　企画情報課　情報班
第3版	平成30年6月	平成30年度組織改革に伴う部及び課の統廃合によるもの	豊見城市情報化推進委員会	総務企画部　企画財政課　情報班
第4版	令和元年5月	①地方公共団体における情報セキュリティポリシーに関するガイドライン（平成30年9月版総務省改定）に基づくもの ②平成31年度組織改革に伴う部及び課の統廃合によるもの	豊見城市情報化推進委員会	総務企画部　IT管財課　IT推進班
第5版	令和5年10月	①地方公共団体における情報セキュリティポリシーに関するガイドライン（令和5年3月版総務省改定）に基づくもの ②令和5年度組織改革に伴う部及び課の統廃合によるもの	豊見城市情報化推進委員会	総務企画部　デジタル推進課システム管理班
第6版	令和8年3月	①　地方自治法改正への対応 ②　地方公共団体における情報セキュリティポリシーに関するガイドライン（令和7年3月版総務省改定）に基づくもの	豊見城市DX推進本部	企画部　デジタル推進課　システム管理班

目次

1 目的

本基本方針は、本市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。また、当該基本方針については、地方自治法（昭和 22 年法律第 67 号）第 244 条の 6 第 1 項に規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

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） 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。

（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） 機関の範囲

本基本方針が適用される機関は、次のとおりとする。

① 市長部局

② 教育委員会

③ 議会

④ 選挙管理委員会
⑤ 監査委員
⑥ 農業委員会
⑦ 固定資産評価審査委員会
⑧ 消防本部
⑨ 地方公営企業

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、(1)に示す機関が所掌する資産のうち、次のとおりとする。

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およびネットワーク図等のシステム関連文書

(3) 職員等の範囲

本基本方針が適用される職員及び職員に準ずる者(以下「職員等」という。)は、次のとおりとする。

① （1）に示す機関に所属し、（2）に示す情報資産を取り扱う職員、再任用職員、会計年度任用職員及び派遣職員
② ①に準じて（2）に示す情報資産を取り扱う特別職（市長、副市長、教育長、議員及び各行政委員会等の委員等）及び教職員等

5 職員等の遵守義務

職員等は、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

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2) 情報資産の分類と管理

本市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) 物理的セキュリティ

サーバ、サーバ室、メンテナンス室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ

情報セキュリティに関し、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。

(5) 技術的セキュリティ

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

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。

(7) 業務委託と外部サービス(クラウドサービス)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じる。

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。

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。

(8) 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、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失等を分析し、リスクを検討したうえで、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。

ただし、市長部局が整備するネットワークと論理的または物理的に分離されているネットワークについては、当該ネットワークを所管する機関が必要に応じて個別に対策基準を策定するものとする。なお、情報セキュリティ対策基準は、公にすることによりサイバー攻撃を受けるリスクがあることから、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、情報セキュリティ実施手順は、公にすることにより本市の行政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。