

延岡市情報セキュリティ基本方針

[第 2 版]

【平成16年3月制定】

【平成21年3月一部改定】

序 情報セキュリティポリシーの構成

情報セキュリティポリシーとは、本市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、本市が所掌する情報資産に関する業務に携わる全職員、非常勤職員、臨時職員（以下「職員等」という。）及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、①情報セキュリティ基本方針②情報セキュリティ対策基準の2階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順として情報セキュリティ実施手順を策定することとする（下表参照）。

情報セキュリティポリシーの構成

文 書 名		内 容
情報セキュリティ ポリシー	情報セキュリティ 基本方針	情報セキュリティ対策に関する統一 的かつ基本的な方針。
	情報セキュリティ 対策基準	情報セキュリティ基本方針を実行に 移すための全ての情報システムに共 通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		情報システム毎に定める情報セキュ リティ対策基準に基づいた具体的な 実施手順。

延岡市情報セキュリティ基本方針

目次

1	目的	1
2	定義	1
	(1) ネットワーク	1
	(2) 情報システム	1
	(3) 行政情報	1
	(4) 情報資産	2
	(5) 情報セキュリティ	2
3	情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務	2
4	情報セキュリティ管理体制	2
5	行政情報の分類	2
6	情報資産への脅威	2
	(1) 部外者による脅威	2
	(2) 職員等又は外部委託事業者による脅威	2
	(3) その他の脅威	3
7	情報セキュリティ対策	3
	(1) 物理的セキュリティ対策	3
	(2) 人的セキュリティ対策	3
	(3) 技術及び運用におけるセキュリティ対策	3
8	情報セキュリティ対策基準の策定	3
9	情報セキュリティ実施手順の策定	3
10	情報セキュリティ監査及び自己点検の実施	4
11	情報セキュリティポリシーの見直し	4

延岡市情報セキュリティ基本方針

1 目的

本市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、情報資産を様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。

また、近年のいわゆるIT革命の進展により、電子商取引の発展や電子自治体の構築が現実のものとなっている。本市が電子自治体を構築するためには、全ての情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、本市の情報資産の機密性、完全性及び可用性（注）を維持するための対策（情報セキュリティ対策）を整備するために本市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

（注）：国際標準化機構（ISO）が定めるもの（ISO7498-2：1989）

- ・機密性（Confidentiality）
情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
- ・完全性（Integrity）
情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
- ・可用性（Availability）
許可された利用者が必要なときにアクセスできることを確実にすること。

2 定義

（1）ネットワーク

本市における市長部局、議会事務局、各行政委員会、消防、上下水道局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）及び記録媒体で構成され、処理を行う仕組みをいう。

（2）情報システム

電子計算機（ハードウェア及びソフトウェア）、ネットワーク及び記録媒体で構成され、処理を行う仕組みをいう。

（3）行政情報

情報システムの開発と運用に係る全ての情報及び情報システムで取り扱う全てのデータをいう。なお、紙等の有体物に出力された情報も含むものとする。

(4) 情報資産

情報システム及び行政情報をいう。

(5) 情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

3 情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

情報セキュリティポリシーは、本市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

したがって、市長をはじめとして本市が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

4 情報セキュリティ管理体制

本市の情報資産について、情報セキュリティ対策を推進・管理するための体制を確立するものとする。

5 行政情報の分類

行政情報をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6 情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

(1) 部外者による脅威

- ・部外者の侵入による情報資産の破壊・盗難
- ・故意の不正アクセス又は不正操作による情報資産の破壊・盗難・改ざん・消去等

(2) 職員等又は外部委託事業者による脅威

- ・情報資産の持出、誤操作
- ・アクセスのための認証情報又はパスワードの不適切管理
- ・故意の不正アクセス又は不正行為による情報資産の破壊・盗難・改ざん・消去等
- ・搬送中の事故等による情報資産の盗難
- ・規定外の端末等の接続によるデータ漏洩等

(3) その他の脅威

- ・コンピュータウイルス
- ・地震、落雷、火災等の災害
- ・事故、故障等によるサービス及び業務の停止

7 情報セキュリティ対策

上記6で示した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ものとする。

(1) 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

(2) 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等及び外部委託事業者に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

(3) 技術及び運用におけるセキュリティ対策

情報資産を外部からの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、ネットワーク管理等の技術面の対策、また、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずる。

また、緊急事態が発生した際に迅速な対応をとるための危機管理対策を講ずる。

8 情報セキュリティ対策基準の策定

本市の様々な情報資産について、上記7の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為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ものとする。

9 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て情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、市長部局の長等が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ対策基準及び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恐れのある情報であることから非公開とする。

10 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。

11 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。