

勝浦町情報セキュリティポリシー

令和8年1月30日 全部改正

勝浦町長
勝浦町議会事務局
勝浦町教育委員会
勝浦町選挙管理委員会
勝浦町農業委員会
勝浦町監査委員
勝浦町固定資産評価審査委員会

目次

- 第1章 総則(第1条・第2条)
- 第2章 情報セキュリティ基本方針(第3条―第12条)
- 第3章 情報セキュリティ対策基準(第13条―第22条)

第1章 総則

(趣旨)

第1条 勝浦町の各情報システムが取り扱う情報には、個人情報や行政運営上重要な情報など、外部に漏えい等した場合には極めて重大な事態を招く情報が多数含まれている。したがって、情報セキュリティ対策を組織として統一して推進するため、組織として意思統一され明文化された文書として、勝浦町情報セキュリティポリシー(以下「情報セキュリティポリシー」という。)を定めるものとする。

(情報セキュリティポリシーの構成)

第2条 情報セキュリティポリシーは、情報セキュリティ対策における基本的な考え方を定める情報セキュリティ基本方針(以下「基本方針」という。)及びこの基本方針に基づき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を定める情報セキュリティ対策基準(以下「対策基準」という。)から構成する。

情報セキュリティポリシー体系図

区分		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

第2章 情報セキュリティ基本方針

(目的)

第3条 本基本方針は、勝浦町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、勝浦町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。

(定義)

第4条

- (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 基本方針及び対策基準をいう。
- (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。

- (8) マイナンバー利用事務系(個人番号利用事務系) 個人番号利用事務(社会保障、地方税若しくは防災に関する事務)又は戸籍事務等に関わる情報システム及びデータをいう。
- (9) LGWAN接続系 LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう(マイナンバー利用事務系を除く。)
- (10) インターネット接続系 インターネットメール及びホームページ管理システム等に関わるインターネットに接続された情報システム並びにその情報システムで取り扱うデータをいう。
- (11) 通信経路の分割 LGWAN接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。
- (12) 無害化通信 インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

(対象とする脅威)

第5条 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、ウイルス攻撃又は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、重要情報の詐取又は内部不正等
- (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又は機器故障等の非意図的的要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷又は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、通信の途絶又は水道供給の途絶等のインフラの障害からの波及等

(適用範囲)

第6条

- (1) 行政機関の範囲 本基本方針が適用される行政機関は、町長、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、地方公営企業の管理者及び町議会事務局をいう。適用行政機関の範囲外であっても、本基本方針の対象となる情報システムを利用する場合にあつては、本基本方針の適用範囲とする。
- (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

(職員等の遵守義務)

第7条 町の情報資産に接する非常勤職員及び会計年度任用職員を含む全ての職員(以下「職員等」という。)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。

(情報セキュリティ対策)

第8条 第5条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 本町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 本町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) 情報システム全体の強靱性の向上 情報セキュリティの強化を目的とし、業務の効率性・利便性の観点から踏まえて情報システム全体に対し次の三段階の対策を講じる。
 - ア マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により住民情

報の流出を防ぐ。

イ LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

ウ インターネット接続系においては、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実施する。高度な情報セキュリティ対策として、徳島県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ サーバ、サーバ室、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。

(5) 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。

(6) 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及び不正アクセス対策等の技術的対策を講じる。

(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及び業務委託を行う際のセキュリティ確保等の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。

(8) 業務委託と外部サービス(クラウドサービス)の利用

ア 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。

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

ウ 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。

(情報セキュリティ監査及び自己点検の実施)

第9条 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。

(情報セキュリティポリシーの見直し)

第10条 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となった場合には、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。

(情報セキュリティ対策基準の策定)

第11条 第8条から第10条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。また、情報セキュリティ対策基準は、公にすることにより本町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。

なお、総務防災課情報技術係が管理する業務用ネットワークから物理的又は論理的に完全に分離されている場合、セキュリティポリシーに関する対策基準のガイドラインとして、それぞれ必要な対策基準を設け、対応を行うことができるものとする。教育委員会、勝浦病院においては、それぞれ「教育情報セキュリティポリシーに関するガイドライン」(文部科学省)及び「医療情報システムの安全管理に関するガイドライン」(厚生労働省)が策定されていること

から、これらのネットワークやシステム等に係る対策基準についてはそれぞれのガイドラインが適用し、必要な対応を行うものとする。

(情報セキュリティ実施手順の策定)

第12条 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。ただし、情報セキュリティ実施手順は、公にすることにより本町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。