第１章　情報セキュリティ基本方針

１.目的

東彼杵町は、町がたずさわる電子情報資産（以下、「情報資産」という）を、過失、事故、災害、犯罪などの脅威から守り、機密性、完全性、可用性を保持するため、情報セキュリティ対策として本ポリシーを定め、適切に運用を行うこととする。

本基本方針は、地方自治法（昭和 22 年法律第 67 号）第 244 条の 6 第 1 項の規定に基づく、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づける。

２.定義

本ポリシーにおける用語の定義は、次のとおりとする。

(1) ハードウェア
コンピュータ及びその周辺機器をいう。

(2) ソフトウェア
コンピュータを動作させるための命令･手順を記述したもの及び記録媒体(ハードディスク、ＣＤ－ＲＯＭ、ＦＤ等）に収めたものをいう。

(3) ネットワーク
東彼杵町が管理する全行政機関のハードウェアを相互に接続するための通信網及び構成する機器（ハブ、ルータ等）をいう。

(4) 情報システム
東彼杵町が管理するコンピュータシステムで、ハードウェア、ソフトウェア及びネットワークを用いる業務処理の仕組みをいう。

(5) 情報資産
情報システム及び情報システム構築、保守、運用のための全ての情報、加えて情報システムで扱う情報をいう。
※情報システムから印字された紙の情報もこれに含む。

(6) 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。
・機密性とは、権限のない者への情報の漏洩を防止することをいう。
・完全性とは、情報の改ざん、破壊による被害を防止することをいう。
・可用性とは、必要な場合、常に情報の利用を可能にすることをいう。

(7) 職員
本ポリシーにて職員とは、特別職及び一般職の職員並びに、会計年度任用職員を含む全ての職員のことをいう。

(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、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及びその情報システムで取り扱うデータをいう。

(11) 通信経路の役割

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、コンピューター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。

３.適用範囲

本ポリシーは、東彼杵町の全ての行政機関（町長部局、行政委員会、議会事務局、地方公営企業）に適用し、対象となる情報資産は次のとおりとする。

(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及びネットワーク図等のシステム関連文書

東彼杵町議会における地方自治法第244条の6第1項の規定に基づくサイバーセキュリティを確保するための方針は、本ポリシーをもってこれに充てるものとする。

４.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洩・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洩・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

５.職員の責務

(1) 遵守義務

全ての職員は、情報資産の取扱いにあたり、関係法規の規定及びこの基本方針並びに情報セ

キュリティ実施手順を遵守しなければならない。

(2) 懲戒処分等

本ポリシーに違反した職員及びその監督責任者は、当該違反により生じた損害に応じて、地方公務員法に則り、懲戒等の処分の対象とする。

(3) 外部委託業者への通達

外部委託業者が情報資産を取り扱う場合は、契約等を通じ、この基本方針を遵守させるための必要な措置を講じなければならない。

６.情報セキュリティ基準構成

東彼杵町の各情報資産に対する個々の対策について、以下の対策基準を定める。

(1) 情報セキュリティ管理の組織・体制

情報セキュリティの運用及び推進のため、第２章に定める情報セキュリティ委員会を始めとする組織・体制を定める。

(2) 情報資産の分類と管理責任

各情報資産について重要度により分析を行ない、それに見合う管理方法について定める。

(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とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

・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。

・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。

・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、都道府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対策

情報資産を保管又は設置する施設への不正な立ち入り、情報資産への破壊、漏洩等から保護するための物理的な対策について定める。

(5) 人的セキュリティ対策

職員に対して、情報セキュリティの重要性、責任の認識、非常時等の対応についての人的対策及び啓蒙活動について定める。

(6) 技術的セキュリティ対策

情報資産を不正アクセス等から保護するためのアクセス制御、ネットワークの管理等についての技術的な対策について定める。

(7) 運用管理

情報資産の管理、監視、保全及びウィルス対策等について定める。また、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、並びに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の東彼杵町情報セキュリティインシデント対応計画（以下「緊急時対応計画」という。）の策定について定める。

⑻ 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、判断すべき基準を定める。

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、運用責任者を定める。

⑼ 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、適宜情報セキュリティポリシーの見直しを行う。

７.基本方針の公表

本基本方針を策定又は変更したときは、遅滞なくこれを公表しなければならない。

８.情報セキュリティ対策基準について

本基本方針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、情報セキュリティ対策基準は、公にすることにより東彼杵町の行政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する。

９.情報セキュリティ実施手順について

情報セキュリティに関する実施手順は、情報セキュリティ対策基準に基づき、情報セキュリティ管理者もしくは情報セキュリティ担当者が定めるものとする。

なお、情報セキュリティ実施手順は、公にすることにより東彼杵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。