吉備中央町情報セキュリティ基本方針

平成２９年７月１日策定
令和７年８月４日改定

１　目的

この基本方針は、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、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。

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、電磁的記録媒体及びこれらを接続するネットワークで構成され、情報処理を行う仕組み。町においては、町が管理する構成機器（貸借契約等により町が借り受けている機器を含む。)を利用し、与えられた処理手順に従って演算、加工、記録及びその他の一連の処理を行うことにより、多種の事務的な処理を行う処理体系、組織をいう。

（３）住民情報処理

情報システムで処理するもののうち、住民記録、税及び福祉等の住民情報が含まれる処理を行うものをいう。

（４）内部情報処理

内部事務処理のための情報処理で、財務会計、電子メール、掲示板等の情報処理を行うものをいう。

（５）業務所管課

情報システムを使用して、所管する住民情報処理及び内部情報処理を行う課等をいう。

（６）サーバ等

ネットワーク上で情報を処理し、接続された端末機に情報を提供するコンピュータ（汎用コンピュータを含む。）をいう。

（７）端末機

コンピュータのうち、情報の入出力のために、ネットワークによりサーバに接続されたワークステーション、パーソナルコンピュータ（以下「パソコン」という。）等をいう。

（８）周辺機器

端末機に接続して情報の入出力を行うプリンタ、スキャナ、外部記録装置等をいう。

（９）情報機器

情報処理システムを構築するためのコンピュータ、ネットワーク機器、端末機、周辺機器等をいう。ただし、特別なプログラムを導入せず、かつ、ネットワークに接続しないコンピュータ、周辺機器等を除く。

（１０）電算室
　サーバ、汎用コンピュータ及びネットワーク中枢機器等を設置している賀陽庁舎３階電算室をいう。
（１１）電子情報
　情報システム並びに情報システムの開発、保守及び運用に係る全ての電子情報（電子的、磁気的、その他人の知覚によって認識することができない方式で作られた記録をいい、プログラム等のソフトウェアを含む。）をいう。
（１２）情報資産
　ネットワーク及び情報システムで取り扱う電子情報等をいう。
（１３）データ
　情報システムに係る入出力帳票又は電磁的記録媒体に記録されている電子情報等をいう。
（１４）記録媒体
　電子情報を保管する記録装置のうち、取りはずして使用することが可能な磁気ディスク、光磁気ディスク、磁気テープその他これらに類するものをいう。
（１５）アクセス
　電磁的記録媒体に対して、データの書き込み、読み出しを行うことをいう。
（１６）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。
（１７）情報セキュリティポリシー
　この基本方針及び情報セキュリティ対策基準をいう。
（１８）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。
（１９）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。
（２０）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。
（２１）ＣＩＳＯ（シーアイエスオー）
　最高情報セキュリティ責任者（Chief Information Security Officer）の略称。情報セキュリティを統括する責任者をいう。
（２２）ＣＳＩＲＴ（シーサート）
　情報セキュリティインシデント対応チーム（Computer Security Incident Response Team）の略称。情報システムに対するサイバー攻撃等による情報セキュリティ上の事故（インシデント）が発生した際に、状況の把握・分析、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制をいう。

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、外部委託管理の不備、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）実施機関の範囲
　情報セキュリティポリシーが適用される実施機関は、町長、教育委員会、選挙管理委員会、農業委員会、監査委員、固定資産評価審査委員会、公平委員会、地方公営企業及び議会とする。
（２）情報資産の範囲
　この基本方針が対象とする情報資産は、次のとおりとする。
①　ネットワーク、情報システム及びこれらに関する設備、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

５　職員等の遵守義務
　職員、特別職非常勤職員、会計年度任用職員及び臨時的任用職員（以下「職員等」という。）並びに外部委託業者は、情報セキュリティの重要性について共通の認識を持ち、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
　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
　町の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。
（３）物理的セキュリティ
　サーバ等、電算室等、通信回線等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、外部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。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切に対応するため、緊急時対応計画を定める等の必要な措置を講じる。

（7）業務委託と外部サービスの利用

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。

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。

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。

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。情報セキュリティ対策基準は、公にすることにより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。

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。情報セキュリティ実施手順は、公にすることにより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。