○菰野町情報セキュリティポリシー管理要綱

平成25年３月29日訓令第１号

改正

平成30年９月18日訓令第10号

令和５年３月31日訓令第２号

令和８年３月30日訓令第２号

菰野町情報セキュリティポリシー管理要綱

目次

第１章　情報セキュリティ基本方針

第１節　通則

（目的）

第１条　この訓令は、本町における情報セキュリティの確保に関する基本的かつ統一的な考え方を菰野町情報セキュリティポリシーとして示すことにより、本町が保有し、又は業務上取り扱う情報資産の機密性、完全性及び可用性を維持し、安全かつ効率的な行政サービスの提供を維持し、もって行政に対する町民の信頼を確保することを目的とする。

２　情報セキュリティポリシーのうち、本町が実施する情報セキュリティ対策の基本的な事項を情報セキュリティ基本方針（以下「基本方針」という。）に定める。

３　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。

４　本基本方針を策定又は変更したときは、地方自治法第244条の６第２項の規定に基づき、遅滞なくこれを公表するものとする。

（定義）

第２条　基本方針において、次の各号に掲げる用語の意義は、以下に定めるところによる。

（１）　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。

（２） 情報セキュリティポリシー　本訓令に掲げる情報セキュリティ基本方針及び情報セキュリティ対策基準を包括し、本町の基本的な情報保護対策の考え方をあらわすものをいう。

（３） 情報　磁気ディスク等（伝送路を含む。）に記録されたもの（単体では意味を成さなくても、ソフトウェア等により意味を成す場合は、これに該当する。）をいう。

（４） 情報資産　情報及び情報システム並びに情報システムの開発と運用に係る全ての文書をいう。

（５） 電子計算機　コンピュータ本体（基本ソフトウェアを含む。）及び周辺機器並びに記録媒体をいう。

（６） ネットワーク　電子計算機を相互に接続するための通信網及びその構成機器（ソフトウェアを含む。）で構成され、情報処理を行う仕組みをいう。

（７） 情報システム　電子計算機及び業務処理用アプリケーション（ソフトウェアを含む。）で構成され、情報処理する仕組み（ネットワークもこれに該当する。）をいう。

（８） 磁気ディスク等　電子計算機に使用される磁気ディスク、磁気テープ、光ディスクその他これらに類する電磁的又は光学的記録媒体をいう。

（９） サーバ等　電子計算機のうち、データを大量に処理する装置及びその周辺機器並びにネットワークの中核を成す機器（ホストコンピュータ、ルータ等もこれに該当する。）をいう。

(10) 電子計算機室　サーバ等を運用管理する目的で設置している部屋をいう。

(11) 職員　地方公務員法（昭和25年法律第261号）第３条第２項に規定する一般職の職員（会計年度任用職員を含む。）をいう。

(12) 職員等　職員並びに派遣契約等により本町の業務に従事する者及び委託事業者の従業者その他本町の情報資産を取り扱う者をいう。

(13) 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。

(14) ＬGWAN接続系　総合行政ネットワーク（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。）。

(15) 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。

(16)　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。

(17)　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ない等、安全が確保された通信をいう。

(18)　ＣＳＩＲＴ（Ｃｏｍｐｕｔｅｒ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃｉｄｅｎｔ　Ｒｅｓｐｏｎｓｅ　Ｔｅａｍ）　組織におけるサイバーセキュリティインシデントへの迅速かつ効果的な対応を目的としたチームをいう。

(19)　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。

(20)　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。

(21)　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。

第２節　基本方針

（情報セキュリティポリシーの位置付け）

第３条　情報セキュリティポリシーは、本町の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、情報セキュリティ対策の最高位に位置するものである。

（適用範囲）

第４条　情報セキュリティポリシーが適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

２　情報セキュリティポリシー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

３　情報セキュリティポリシーの対象者は、本町の情報資産を取り扱う全ての職員等とする。

（職員等の遵守義務）

第５条　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。

（情報セキュリティ管理体制）

第６条　情報セキュリティ対策を適切に推進し、管理するための体制を確立するものとする。

（情報資産の分類と管理）

第７条　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行うものとする。

（対象とする脅威）

第８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、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、風水害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

（情報セキュリティ対策）

第９条　本町の情報資産を前項に規定する脅威から保護するため、重要性の分類にしたがって、次の情報セキュリティ対策を講じるものとする。

（１）　物理的セキュリティ対策　電子計算機室等への不正な立入り、情報への損傷・妨害等からの保護、災害等に対する予防措置等について物理的な対策を講じる。

（２）　人的セキュリティ対策　情報資産に接する職員の情報セキュリティに関する権限、責任等を定めるとともに、全ての職員に情報セキュリティポリシーの内容を周知徹底

するため、研修を行う。

（３） 技術的セキュリティ対策　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、情報へのアクセス制御、コンピュータウイルス対策等を実施する。

（４） 運用　情報セキュリティポリシーの実効性を確保し、不正アクセスされること及び不正アクセスによって他の情報システムに対して被害を及ぼすことを防止するため、ネットワークの監視等の運用面における必要な措置を講じるとともに、障害が発生した際の迅速な対応を図るため、障害時の対応を講じる。

（５） 情報システム全体の強じん性の向上　業務の効率性及び利便性に配慮しつつ、マイナンバー利用事務系、ＬGWAN接続系及びインターネット接続系の区分に応じ、通信経路の分割、無害化通信その他必要な措置を講じるものとする。

（６） 業務委託及び外部サービス（クラウドサービス）の利用　委託事業者の選定、契約、監督等により、必要な情報セキュリティ対策が確保されるよう措置を講じるものとする。

（７） 緊急時対応計画（インシデント対応計画）　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、必要な体制及び手順を整備するものとする。

（８） ソーシャルメディアサービスの利用　本町がソーシャルメディアサービスを利用する場合は、運用手順を定め、発信できる情報及び責任体制を明確化するものとする。

（情報セキュリティ対策基準の策定）

第10条　本町の情報資産について、前項に規定する情報セキュリティ対策を講じるに当たっては、職員が遵守すべき事項及び判断の基準を統一的なレベルで定める必要があることから、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。

２　情報セキュリティ対策基準は、具体的なセキュリティ対策の内容が含まれるため、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表とする。

（情報セキュリティ実施手順の策定）

第11条　情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定するものとする。

２　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表とする。

（評価、見直し）

第12条　情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ、基本方針、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について、適宜情報セキュリティ対策基準の見直しを実施するものとする。

（情報セキュリティ監査及び自己点検の実施）

第13条　情報セキュリティポリシーが遵守されていることを検証するため、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ものとする。

（違反への対応）

第14条　情報セキュリティポリシー及び実施手順に違反した者については、その重大性、発生した事案の状況等に応じて適切な措置を講じるものとする。

２　前項の措置には、委託事業者等に対する契約に基づく措置を含むものとする。

第２章　情報セキュリティ対策基準（非公表）

第３章　情報セキュリティ実施手順（非公表）

附　則

（施行期日）

１　この訓令は、公布の日から施行する。

（菰野町ワードプロセッサー及びフロッピーディスク等管理要綱の廃止）

２　菰野町ワードプロセッサー及びフロッピーディスク等管理要綱（平成４年要綱第１号）は、廃止する。

附　則（平成30年９月18日訓令第10号抄）

１　この訓令は、令達の日から施行する。

附　則（令和５年３月31日訓令第２号）

この訓令は、令和５年４月１日から施行する。

附　則（令和８年３月30日訓令第２号）

この訓令は、令和８年３月31日から施行する。