「香美町情報セキュリティ基本方針」

令和 4 年 10 月

目　　次

は　じ　め　に

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

本町は、町民の個人情報や行政運営上重要な情報などの重要な情報を多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、町民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。また、本町には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。

これらの状況を鑑み、本町における情報資産に対する安全対策を推進し、町民からの信頼を確保し、さらに地域に貢献するため、以下に積極的に取り組むことを宣言する。

（1）情報セキュリティ対策に取り組むための全庁的な体制を確立する。

（2）情報セキュリティ対策の基準として情報セキュリティ対策基準を策定し、その実行のための手順等を盛り込んだ実施手順を策定する。

（3）本町の保有する情報資産を適切に管理する。

（4）情報セキュリティ対策の重要性を認識させ、当該対策を適切に実施するために、職員等に対して必要な教育を実施する。

（5）情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定める。

（6）情報セキュリティ対策の実施状況の監査及び自己点検等を通して、定期的に対策の見直しを実施する。

（7）全ての職員等は、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を遵守する。

（8）地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献する。

令和　　４年１０月　１８日
最高情報セキュリティ責任者

第１章　総則

（目的）

第１条　香美町情報セキュリティ基本方針（以下「基本方針」という。）は、情報の安全確保に対する基本的な指針を示すことにより、香美町（以下「町」という。）が管理する情報資産を適切に保護するための基本的な事項を定めることを目的とする。

（用語の定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(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　職務の遂行に伴って電子計算機及び記録媒体に記録されたデータをいう。

(3)　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。

(4)　脅威　自然の脅威（地震、落雷、火災、風水害等）、情報システムの脅威（情報システムの故障、誤作動等）及び人的な脅威（コンピュータウイルス、不正行為、誤操作等）をいう。

(5)　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。

(6)　情報セキュリティポリシー　本基本方針及び情報セキュリティ対策基準をいう。

(7)　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。

(8)　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。

(9)　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。

(10)　職員等　地方公務員法で規定された特別職、一般職の及び臨時的に雇用した職員等の総称をいう。

(11)　関係機関の職員等　教育委員会、選挙管理委員会など、事務部局以外の地方公共団体に勤務し、町が管理する情報資産を職務で利用する者の総称をいう。

(12)　外部要員　業務委託先社員（システム開発業務を委託する外部業者等）等、契約に基づいて町の機関で作業する者の総称をいう。

(13) 基幹系（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 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（基幹系を除く。）。

(15) 情報系　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 系と情報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無い等、安全が確保された通信をいう。

（対象とする脅威）

第３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

（適用範囲）

第４条　この基本方針の適用範囲は、次に定めるところによる。

(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、公営企業管理者及び議会とする。

(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。

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

（適用除外）

第５条　この基本方針及び香美町情報セキュリティ対策基準（以下「対策基準」という。）に基づく対策の実施が困難であると判断した要件に関しては、その理由や対策未実施の場合の影響等を考慮したうえで、適用を除外することを認める。

２　対策基準に基づく対策の実施が困難であると判断した要件及びその理由を明確に記載した適用除外申請書により申請する。

（職員の義務）

第６条　職員等及び関係機関の職員等は、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。

２　職務上知り得た秘密を漏らしてはならない。また、その職を退いた後も同様とする。

（関係機関の職員等の参加）

第７条　関係機関の職員等は、情報資産の利用範囲に応じて、前条と同様の義務が生じ得るもの

とし、町が実施する情報セキュリティ対策に積極的に関与する。

（外部要員の管理）

第８条　外部要員を使用する職員は、契約等に基づき、第５条と同様の内容を外部要員に対しても義務づけ、管理する。

第２章　情報セキュリティ対策

（情報の安全対策）

第９条　町が管理する情報資産を脅威から保護するため、次に掲げる情報セキュリティ対策を講ずる。

(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。

①　基幹系においては、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。

②　LGWAN 系においては、LGWAN と接続する業務用システムと、情報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。

③　情報系においては、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)　物理的なセキュリティ　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、物理的な対策を講ずる。

(5)　人的セキュリティ　職員及び関係機関の職員等並びに外部要員に対して情報資産の安全確保の重要性を認識させ、情報の安全対策の啓発に有効と考えられる教育活動等の対策を講ずる。

(6)　技術的セキュリティ　情報システムの誤操作、不正アクセス等から情報資産を保護するため、情報資産へのアクセス制御等の技術的な対策を講ずる。

(7)　情報システムセキュリティ　情報システムの誤作動、不正利用、情報漏えい等から情報資産を保護するため、開発環境及び品質保持に必要な対策を講ずる。

(8)　ネットワークセキュリティ　ネットワーク障害、不正アクセス等から情報資産を保護するため、ネットワークの可用性確保、ネットワーク監視等の必要な対策を講ずる。

(9)　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、業務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。

(10)　業務委託と外部サービスの利用

①　情報資産に関係する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、外部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。

②　外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

③　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。

(11)　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。

第３章　情報セキュリティ監査及び自己点検の実施

（情報の安全対策に関する監査の実施）

第１０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。

第４章　情報セキュリティポリシーの見直し

（見直し）

第１１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になった場合には、情報セキュリティポリシーを見直す。

第５章　法令等の遵守

（法令等の遵守）

第１２条　全ての適用対象者は、職務遂行において、関連法令等に従わなければならない。

第６章　罰則

（罰則）

第１３条　職員が、この基本方針等に定める情報セキュリティ対策に違反した場合には、情報資産の利用に制限を加えるなど、相当の処分を行うことができる。

第７章　情報セキュリティ対策基準

（情報セキュリティ対策基準）

第１４条　上記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。

第８章　情報セキュリティ実施手順

（情報セキュリティ実施手順）

第１５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。

２　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。

附　則

この基本方針は、平成１７年１２月　１日から施行する。

附　則

この基本方針は、平成２１年　４月　１日から施行する。

附　則

この基本方針は、平成２４年　４月　１日から施行する。

附　則

この基本方針は、平成２７年１０月　５日から施行する。

附　則

この基本方針は、平成３０年　１月１５日から施行する。

附　則

この基本方針は、令和　４年　１月３１日から施行する。

附　則

この基本方針は、令和　４年１０月１８日から施行する。