笠松町情報セキュリティ基本方針規程

（目的）

第１条　本基本方針は、本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､本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、当該各号に定めるところによる。

（１）　情報資産　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

（２）　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及びその構成機器（ハードウェア及びソフトウェア）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）　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。

（５）　笠松町情報セキュリティポリシー　本基本方針及び笠松町情報セキュリティ対策基準規程（平成１５年笠松町訓令乙第２号。以下「対策基準規程」という。）をいう。

（６）　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。

（７）　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。

（８）　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。

（９）　マイナンバー利用事務系　個人番号（行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）第２条第５項）に規定する個人番号をいう。）利用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。

（１０）　ＬGWAN接続系　ＬGWAN（地方公共団体の組織内ネットワークを相互に接続し、情報の高度利用を行うためのネットワークをいう。）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。）。

（１１）　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。

（１２）　通信経路の分割　ＬＧＷＡＮ接続系とインターネット接続系を分離した上で、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。

（１３）　無害化通信　インターネット接続系に関わるメール本文のテキスト化や端末への画面転送等において、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、次に掲げる脅威を想定し、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

（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　本基本方針は町の所掌する情報資産に関する業務に携る全ての職員（会計年度任用職員、嘱託員等を含む。以下「職員等」という。）に適用する。

（職員等の遵守義務）

第５条　職員等及び外部委託業者は、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及び笠松町情報セキュリティ実施手順（以下「実施手順」という。）を遵守しなければならない。

（情報セキュリティ）

第６条　第３条に規定する脅威から情報資産を保護するために、次の情報セキュリティ対策を行うものとする。

（１）　組織体制

笠松町の情報資産について、情報セキュリティ対策を推進及び管理するため、副町長が情報セキュリティ最高責任者（ＣＩＳＯ：　Ｃｈｉｅｆ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ　Ｏｆｆｉｃｅｒ）となり、組織体制を確立するものとする。

（２）　情報資産の分類と整理

笠松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３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、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、端末への多要素認証の導入等により、個人情報の流出を防ぐ。

イ　ＬＧＷＡＮ接続系においては、インターネット接続系との通信経路を分割する。ただし、両接続系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として、岐阜県が構築する自治体情報セキュリティクラウドを利用する。

（４）　物理的セキュリティ

電算室の施錠管理、通信回線の操作制限及び職員等の機器・媒体の持出管理等の対策を講じる。

（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、不正アクセス対策等の対策を講じる。

（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、外部委託を行う際のセキュリティ確保等の運用面の対策を講じるものとする。この場合において、情報資産に対するセキュリティ侵害発生時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く措置を講ずる。

イ　クラウドサービス（インターネット経由でソフトウェア等のリソースを利用できる仕組みをいう。）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。

（情報セキュリティ監査及び自己点検の実施）

第７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８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、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。

（対策基準規程の策定）

第９条　第６条から第８条までに規定する対策等を実施するために、具体的な遵守事項、判断基準等を定める対策基準規程を策定する。

（実施手順の策定）

第１０条　対策基準規程に基づき、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実施手順を策定するものとする。

（委任）

第１１条　この規程に定めるもののほか、情報セキュリティポリシー及び実施手順に関し必要な事項は、別に定める。

附　則

この訓令は、令和８年４月１日から施行する。