西ノ島町

情報セキュリティ基本方針

令和８年３月

西ノ島町情報セキュリティ基本方針

１．目的

本方針は、西ノ島町（以下「本町」という。）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、本町が実施するサイバー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、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。

（３）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。

（４）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。

（５）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。

（６）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。

（７）マイナンバー利用事務系（個人番号利用事務系、番号系）

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。主に基幹系システム（住民情報系システム）をいう

（８）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）。

（９）インターネット接続系

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。

（１０）通信経路の分割

LGWAN 接続系、インターネット接続系のそれぞれのネットワーク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。

（１１）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．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・消去等

（2）情報資産の無断持ち出し、規定違反、操作・設定ミス、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）電力供給の途絶、通信の途絶等のインフラ障害からの波及等

４．適用範囲

（1）行政機関の範囲

本方針が適用される行政機関は、本町の町長部局、教育委員会、選挙管理委員会、農業委員会、固定資産評価審査委員会、監査委員、議会及び地方公営企業とする。

（2）情報資産の範囲

本方針が対象とする情報資産は、以下のとおりとする。

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

５．職員等の遵守義務

職員、会計年度任用職員及び臨時職員等（以下「職員等」という。）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本方針及び関係規程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

本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推進体制を確立する。

（２）情報資産の分類と管理

本町の保有する情報資産をその内容に応じて分類し、当該分類に基づき適切な管理を実施する。

（３）情報システム全体の強靭性の向上

マイナンバー利用事務系、LGWAN 接続系、インターネット接続系のネットワーク分離を維持し、本町のセキュリティ対策以外にも県が提供する共同利用基盤を活用することで、高度なセキュリティ対策を講じる。

（４）物理的セキュリティ

サーバ、電算室、通信回線及び職員等のパソコン等の管理について、物理的対策を講じる。

（５）人的セキュリティ

職員等が遵守すべき事項を定めるとともに、国、県及び関係機関が実施する研修やｅラーニング等を活用し、十分な教育及び啓発を行う。

（６）技術的セキュリティ

コンピュータ等へのアクセス制御、OS やソフトウェアの適切な更新、ウイルス対策ソフトの導入など、基本的な技術的対策を確実に行う。

（７）運用

情報システムの稼働状況の確認、関係規程の遵守状況の確認を行う。また、セキュリティ侵害が発生した場合に迅速に対応できるよう、緊急時対応の手順を定める。

（８）業務委託と外部サービスの利用

業務委託やクラウドサービスを利用する際は、情報セキュリティ要件を明記した契約を締結し、事業者における対策の実施状況を確認する。

７．情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の遵守状況を検証するため、職員による定期的な自己点検を中心に実施し、必要に応じて監査を実施することで、運用改善を図る。

８．情報セキュリティ方針の見直し

情報セキュリティに関する状況の変化（新たな脅威の出現や法令の改正等）や、自己点検の結果等を踏まえ、必要に応じて本方針を見直す。

９．情報セキュリティ対策基準及び実施手順の策定

本方針に基づき、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。なお、これら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開とする。