串本町情報セキュリティポリシー
基本方針

第７版

令和８年１月６日

改正履歴

制定 改正	施行年月日	改正内容
制定	平成１８年８月２日	初版
改正	平成２０年４月１日	改正
改正	平成３０年４月１日	全部改正
改正	平成３０年５月１７日	情報セキュリティ委員会該当者定義の修正
改正	令和７年４月８日	串本町個人情報保護条例廃止に伴う適用範囲修正
改正	令和７年５月１２日	改正
改正	令和８年１月６日	サイバーセキュリティを確保するための方針等(法第２４４条の６(令和８年４月１日施行))対応
	年　月　日	
	年　月　日	
	年　月　日	
	年　月　日	
	年　月　日	

目次

情報セキュリティポリシー基本方針

１ 目的

本基本方針は、本庁が保有する情報資産の機密性、完全性及び可用性を維持しつつ、行政サービスの持続的提供と住民の信頼を確保するため、本庁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。

１の２ 基本的な考え方

本町は、全庁的かつ継続的にサイバーセキュリティ対策を実施し、技術的・人的・物理的な多層的対策を講じることにより、情報資産の適切な保護と業務継続を両立させる。住民サービスの維持を第一に考え、迅速かつ的確な対応体制を整備する。

２ 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

３ 適用範囲

（１）実施機関の範囲

本基本方針が適用される行政機関の範囲は、町の内部部局、教育委員会、議会、土地開発公社、一部事務組合、地方公営企業及び各行政委員会とする。

（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。ただし、小中学校で利用しているネットワーク及び情報システムについては、内部情報系システムに限る。

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

4 職員等の遵守義務

職員、非常勤職員及び会計年度任用職員（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。

5 情報セキュリティ対策

上記２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

本庁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

本庁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、それを踏まえた重要性に基づき情報セキュリティ対策を行う。

（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 マイナンバー利用事務系においては、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接続系においては、LGWANと接続する業務用システムと、インターネット接続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 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）物理的セキュリティ

サーバ機器、通信回線及びパソコン等の管理について、物理的な対策を講じる。

（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人的な対策を講じる。

（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

技術的対策を講じる。

（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、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には、迅速かつ適切な初動対応を行い、関係機関（国、都道府県、情報セキュリティ関連機関等）との連携のもとで被害の最小化と早期復旧を図る。

（８）業務委託の利用

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。

６ 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。

７ 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。

８ 情報セキュリティ対策基準の策定

上記５、６及び７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。

９ 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ものとする。

なお、情報セキュリティ実施手順は、公にすることにより本庁の情報セキュリティ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 関係機関との連携

情報セキュリティ対策の実効性を高めるため、国、都道府県、関係機関及び他の地方公共団体等との連携体制を構築し、情報共有や共同対応を通じて全体としてのセキュリティレベル向上を図る。