南大隅町

サイバーセキュリティ基本方針

第１版

制定：令和８年４月１日
改訂：　　-

目次

サイバーセキュリティ基本方針

1.目的

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と共に情報システムの安全かつ適正な運用を確保するため、サイバーセキュリティの確保を重要な施策と位置づけ、必要な措置を講じ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) サイバーセキュリティ
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) 情報セキュリティポリシー
別途定める情報セキュリティ対策基準をいう。
(5) 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。
(6) 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。
(7) 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。
(8) 個人番号利用事務系（マイナンバー利用事務系）
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。
(9) 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（個人番号利用事務系を除く。）。
(10)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。

(11)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。

(12)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。

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) 外部からの不正アクセス、マルウェア感染、情報漏えい等の脅威に対し、技術的・組織的対策を講じる。

(2) セキュリティパッチの適用、ウイルス対策ソフトの導入、ファイアウォールの設定等を継続的に実施する。

(3) 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

(4) 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

(5) 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

(6) 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

(7) 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

4.適用範囲

(1) 適用範囲

本基本方針は、自治体の全ての部門に適用する。特に教育委員会事務局、小中学校、教育関連施設（教育センター・図書館等）、並びにこれらに関連する外部委託事業者を含む。教育現場においては、文部科学省『教育情報セキュリティポリシーガイドライン』を参照し、児童生徒の個人情報及び教育データの保護を徹底する。

(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、情報システム並びに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

＜情報資産の種類と例＞

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器
情報システム	サーバ、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される電磁的記録媒体、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ（これらを印刷した文書を含む。）、児童生徒の個人情報、学習履歴、教職員の人事情報、校務システム、クラウド学習環境等
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

5.職員等の遵守義務

職員、会計年度任用職員等（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。

6.サイバーセキュリティ対策

上記３の脅威から情報資産を保護するために、以下のサイバー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組織体制を確立する。

(2) サイバー攻撃等のインシデント発生時には、速やかに対応できる体制を整備し、関係機関との連携を図る。

(3) インシデント対応マニュアルを整備し、定期的な見直しを行う。

(4) 情報資産の分類と管理
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実施する。

(5) 情報システム全体の強靭性の向上
サイバー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 個人番号利用事務系（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、鹿児島県と南大隅町のインターネットとの接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(6) 物理的セキュリティ

サーバ等、情報システム室~~等~~、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

(7) 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。~~サイバーセキュリティに関する教育・訓練を定期的に実施し、意識の向上を図る。

(8) 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。

(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、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（クラウドサービス）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。

外部サービス（クラウドサービス）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。

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、情報システムの運用・保守等を外部に委託する場合は、委託先に対しても同等のセキュリティ対策を求め、契約に明記する。

(11) 評価・見直し

サイバーセキュリティに関する脅威や技術の変化に対応するため、情報セキュリティ方針を定期的に見直し、必要な改定を行う。

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、情報セキュリティポリシーの見直しを行う。

7.サイバー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。

8.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サイバー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。

9.サイバーセキュリティ対策基準の策定

上記6、7及び8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。

10.サイバーセキュリティ実施手順の策定

サイバーセキュリティ対策基準に基づき、サイバー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。