南部町情報セキュリティ基本方針

南部町

令和８年３月

目次

1. 目的

本基本方針は、保有する情報資産の機密性、完全性及び可用性維持するため、南部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。

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及びその構成機器（ハードウエア及びソフトウエア）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) 情報資産
ネットワーク及び情報システムの開発と運用に係るすべての情報並びにネットワーク及び情報システムで取り扱うすべてのデータをいう。

(4) 情報セキュリティ
情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(5) 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。

(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。

3. 対象とする脅威

情報資産に対する脅威は、情報を取り扱うあらゆる環境に存在し、その形態は多様である。また、新たな脅威が発生する可能性もあるため、脅威の動向や影響を継続的に監視し、適切な対策を講じるものとする。

本情報セキュリティポリシー策定にあたり、特に考慮した主な脅威は以下のとおり

である。

(1)　意図的な攻撃・不正行為

不正アクセス、ウイルス攻撃、サービス不能攻撃（DoS/DDoS）などのサイバー攻撃

部外者の侵入、重要情報の詐取、内部不正行為

これらに起因する情報資産の漏えい・破壊・改ざん・消去等

(2)　非意図的な事故・過失・管理不備

情報資産の無断持ち出し、パスワード管理不備、無許可ソフトウェアの使用などの規定違反

設計・開発の不備、プログラムの欠陥、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

これらに起因する情報資産の漏えい・破壊・消去等

(3)　災害・事故による影響

地震、落雷、火災などの自然災害

その他の事故

これらによるサービスおよび業務の停止等

(4)　疾病等による要員不足

大規模・広範囲の疾病流行に伴う要員不足

これにより発生するシステム運用の機能不全等

(5)　インフラ障害

電力供給の途絶、通信障害、水道供給の途絶など

これらのインフラ障害に起因する業務への波及影響

4. 適用範囲

(1)　行政機関の範囲

本セキュリティポリシーが適用される行政機関は、内部の各所属、出先機関、教育委員会、議会事務局、福祉・保健施設及び町長が必要と認めた行政機関とする。

(2)　情報資産の範囲

本セキュリティポリシー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

5. 職員等の遵守義務

職員、非常勤職員（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。

6. 情報セキュリティ対策

前出３の脅威から情報資産を保護するため、南部町は以下の情報セキュリティ対策を講じる。

(1)　組織体制

南部町の情報資産を適切に保護するため、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し、継続的な管理・運営を行う。

(2)　情報資産の分類と管理

南部町の保有する情報資産を、機密性・完全性・可用性に基づき分類し、その重要度や特性に応じた適切な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と業務継続性の確保を目的として、情報システム全体に対し次の対策を講じる。

①　マイナンバー利用事務系

他の領域と通信できない構成とし、端末からの情報持ち出し禁止設定、多要素認証の導入等により、住民情報の流出防止を図る。

②　LGWAN 接続系

LGWAN 接続系とインターネット接続系の通信経路を分離し、両者間で通信が必要な場合は無害化通信を実施する。

③　インターネット接続系

不正通信の監視機能強化等の高度な情報セキュリティ対策を実施する。必要に応じ、山梨県情報セキュリティクラウド等の仕組みを活用する。

(4)　物理的セキュリティ

サーバ室、情報システム設置施設、通信設備、職員等が使用する端末等について、不正な立入り、盗難、損傷、妨害等から保護するための物理的対策を講じる。

(5)　人的セキュリティ

情報セキュリティに関し、職員等及び外部委託事業者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

情報資産を外部からの不正なアクセス等から適切に保護するため、コンピュータ

等の管理、情報資産へのアクセス制御、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、外部委託時のセキュリティ確保等、運用面の対策を実施する。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迅速かつ適切に対応するため、緊急時対応計画を策定する。

(8)　業務委託及び外部サービス(クラウドサービス等)の利用

業務委託を行う場合は、情報セキュリティ要件を明記した契約を締結し、委託事業者における必要なセキュリティ対策の実施状況を確認する。

クラウドサービスを利用する場合は、利用に係る規定を整備し、適切な対策を講じる。

ソーシャルメディアサービスを利用する場合は、運用手順を定め、発信可能な情報の範囲及びサービスごとの責任者を明確にする。

(9)　評価・見直し

情報セキュリティ対策の有効性を確保するため、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、改善を図る。必要に応じて、本ポリシー及び情報セキュリティ実施手順の見直しを行う。

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、情報セキュリティ対策の有効性を確認する。

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、または情報セキュリティに関する状況の変化により新たな対策が必要となった場合には、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可能性及び発生時の影響を分析し、リスクを評価したうえで、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見直す。

9. 情報セキュリティ対策基準の策定

南部町の情報資産について、前記６、７及び８に規定する対策を実施するため、具体

的な遵守事項及び判断基準等を定めた情報セキュリティ対策基準を策定する。
なお、情報セキュリティ対策基準は、公にすることにより南部町の行政運営に重大な支障を及ぼすおそれがあるため、非公開とする。

10. 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。

なお、情報セキュリティ実施手順は、公にすることにより南部町の行政運営に重大な支障を及ぼすおそれがある情報資産であるため、非公開とする。