情報セキュリティを確保するための基本方針

＜第 1.0 版＞

南木曽町議会
令和8年3月

情報セキュリティを確保するための基本方針

第１　目的

本方針は、サイバー攻撃や南木曽町議会議員が情報システムを利用する過程での情報資産の漏えい等の脅威から南木曽町議会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、情報セキュリティを確保するため、地方自治法の一部を改正する法律（令和６年法律第 65 号）による改正後の地方自治法第 244 条の６第１項の規定に基づき、南木曽町議会が実施する情報セキュリティ対策について基本的な方針（以下、「情報セキュリティ基本方針」という。）を定めることを目的とする。

第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。

（４）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。

（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）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。

（９）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。

第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、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障害からの波及等

第４　適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、南木曽町議会とする。

（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。なお、南木曽町議会議員個人が、その活動の中で取得した情報資産はこの方針の対象外とする。

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

第５　南木曽町議会議員の遵守義務

南木曽町議会議員は、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この方針及びこの方針に沿って別に定める情報セキュリティに関する基準を遵守しなければならない。

第６　情報セキュリティ対策

上記第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

南木曽町議会の保有する情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

（２）情報資産の分類と管理

南木曽町議会の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（３）物理的セキュリティ

町その他の行政機関から貸与された南木曽町議会議員のタブレット等の管理について、物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、南木曽町議会議員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人的な対策を講じる。

（５）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。

（６）運用

情報システムの監視、当該方針や個別基準の遵守状況の確認、業務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迅速かつ適切に対応するため、緊急時対応手順を策定する。

（７）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、利用に係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る。

（８）評価・見直し

当該方針や個別基準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。当該方針や個別基準の見直しが必要な場合は、適宜見直しを行う。

第７　情報セキュリティ監査及び自己点検の実施

当該方針や個別基準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。

第８　情報セキュリティ基本方針の見直し

情報セキュリティ監査及び自己点検の結果、当該方針や個別基準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、当該基本方針や個別基準を見直す。

第９　情報セキュリティの対策を行うための基準の策定

上記第６、第７及び第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の対策を行うための基準を策定する。なお、当該基準は個別の情報システム毎に定めることができる。

附則

この方針は、令和８年４月１日より施行する。