

下伊那南部総合事務組合
情報セキュリティポリシー
【基本方針】

令和8年3月31日 策定

下伊那南部総合事務組合 情報セキュリティ基本方針

1 目的

本基本方針は、下伊那南部総合事務組合（以下「事務組合」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、事務組合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 用語の定義

(1) ネットワーク

電子計算機を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

(2) 情報システム

事務組合の各種電子計算機（ネットワーク、ハードウェア及びソフトウェア）及び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。

(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アクセスできることを確保すること。

(6) 完全性

情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

(7) 可用性

許可された利用者が必要なときに情報にアクセスできることを確実にすること。

(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。

(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) 不正アクセス、ウィルス攻撃、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な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

4 情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの適用範囲は、次の各号に定めるものとする。

(1) 対象者の範囲

本基本方針が適用される対象者は、事務組合が保有する情報資産を取り扱うすべての職員とする。

(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。

- ア 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
- イ 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。）
- ウ 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 職員等の遵守事項

事務組合が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託者は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって情報セキュリティポリシーを遵守しなければならない。

6 情報セキュリティ対策

事務組合の情報資産を上記3に示した脅威から保護するために、以下の情報セキュリティ対策を講ずる。

(1) 組織体制

事務組合の情報資産について、適切に情報セキュリティ対策を推進・管理するための全庁的な体制を確立する。

(2) 情報資産の分類と管理

事務組合が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、当該分類に応じた情報セキュリティ対策を行う。

(3) 情報システム全体の強靱性の向上

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

システム全体に対し、次の二段階の対策を講じる。

ア 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。

イ 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対策

サーバ等、情報システムを設置する施設等、通信回線等及び職員等のパソコン等の管理について、情報資産の盗難、損傷・妨害等から保護するために物理的な対策を講ずる。

(5) 人的セキュリティ対策

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、全ての職員等に対して情報セキュリティポリシーの内容を周知徹底する等、教育、訓練、啓発等を実施し、外部委託者に対して情報セキュリティポリシーの内容のうち必要となる部分を周知徹底する。

(6) 技術的セキュリティ対策

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等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。

(9) 評価・見直し

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、適宜情報セキュリティポリシーの見直しを行う。

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、情報セキュリティポリシーを見直す。

9 情報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 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。

11 情報セキュリティポリシーの情報公開

情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより事務組合の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。