岳北広域行政組合
情報セキュリティポリシー
【基本方針】

令和８年（2026 年）

３月１日策定

目　次

1　目的

本基本方針は、岳北広域行政組合（以下「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、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　定義

⑴　ネットワーク

コンピューター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）をいう。

⑵　情報システム

コンピューター、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。

⑶　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をいう。

⑷　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。

⑸　機密性

情報にアクセスすることを認められたものだけが、情報にアクセスできる状態を確保することをいう。

⑹　完全性

情報及び処理方法が正確かつ完全であり、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。

⑺　可用性

情報にアクセスすることを認められたものが、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。

⑻　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。

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。

⑴　部外者による故意の不正アクセス、又は不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難等

⑵　職員等及び部外委託者による意図しない操作、故意の不正アクセス、又は不正操作によるデータやプログラムの持ち出し・盗難・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等

⑶　地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

4　適用範囲

⑴　行政機関の範囲

組合が所管する情報資産の生成、運用、管理及び利用に携わる者及び外部委託事業者に適用する。

⑵　職員の範囲

常勤、非常勤の雇用形態を問わず、組合に所属する者（以下「職員等」という。）とする。

⑶　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、情報システム及びこれらに関する設備・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　職員等の遵守義務

職員等は、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を遵守しなければならない。

6　情報セキュリティ対策

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

⑴　情報資産の管理体制

組合の情報資産について、情報セキュリティ対策を推進・管理するための管理体制を確立する。

⑵　情報資産の管理

組合の保有する情報資産を適切に取り扱うため、重要度に応じた情報セキュリティ対策を実施する。

⑶　物理的セキュリティ

情報システム機器、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、物理的な対策を講じる。

⑷　人的セキュリティ

情報セキュリティに関する権限や責任を定め、職員等及び外部委託事業者にセキュリティポリシーの内容を周知徹底する等、充分な教育や啓発等の必要な対策を講じる。

⑸　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、次に掲げる対策を講じること。

ア　情報資産へのアクセス制御

イ　ネットワーク管理等の技術面の対策

⑹　運用

緊急事態が発生した際に迅速な対応を可能とするため、セキュリティ対策に関する危

機管理対策を講ずること。また、通常時においても、庁内システムの運用にあたり、次に掲げる対策を講ずること。

ア　システム開発等の外部委託

イ　ネットワークの監視

ウ　セキュリティポリシーの遵守状況の確認

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や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

⑴　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。

⑵　対策基準の策定にあたっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要があることから、情報セキュリティ対策を行う上で必要となる基本的な要件、実施手順の策定、監視方法や評価・運用の見直し等の事項について明記することとする。

⑶　情報セキュリティ対策基準は、公にすることにより組合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。