香肌奥伊勢資源化広域連合情報セキュリティポリシー

令和８年３月１７日　策定

目次

香肌奥伊勢資源化広域連合情報セキュリティ基本方針

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏洩、不正アクセスや新たな攻撃手法による情報資産の破壊や改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

本広域連合は、行政運営上重要な情報を取り扱っているため、これらの情報を様々な脅威から防御するべく、次の事項について取組むものとする。

(1) 情報セキュリティ対策に取り組むための体制を確立する。

(2) 情報セキュリティ対策の基準として情報セキュリティ対策基準を策定する。

(3) 本広域連合の保有する情報を適切に管理する。

(4) 情報セキュリティ対策の重要性を認識させ、当該対策を適切に実施するために、職員等に対して必要な教育を実施する。

(5) 情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定める。

(6) 情報セキュリティ対策の実施状況の自己点検等を通して、定期的に対策の見直しを実施する。

(7) 職員及び会計年度任用職員（以下「職員」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基本方針、情報セキュリティ対策基準を遵守する。

令和８年３月１７日

香肌奥伊勢資源化広域連合長　筒井　尚之

第１章　情報セキュリティ基本方針

１．目的

本基本方針は、本広域連合が保有する情報資産の機密性、安全性及び可用性を維持するため、本広域連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

(1) 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（ハードウェア及びソフトウェア）をいう。

(2) 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。

(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) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務に関わる情報システム及びデータをいう。

(9) 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。

(10) 無害化通信

インターネットメール本文のテキスト化やパソコン端末への画面転送等により、コンピューターウイルス等の不正プログラムの付着がない等、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洩、破壊、改ざん、消去、重要情報の搾取及び内部不正等

(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、委託管理の不備、マネジメントの欠陥及び機器故障等の非意図的要因による情報資産の漏洩・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) 大規模及び広範囲にわたる疾病による要因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、通信の途絶及び水道供給の途絶等のインフラの障害からの波及等

４．情報資産の適用範囲

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及び電磁的記録媒体

(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．職員の遵守義務

職員は、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情報セキュリティポリシー及び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

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。

(1) 情報資産の分類と管理

本広域連合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。

(2) 情報セキュリティ全体の強靭性の向上

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により、情報の流出を防ぐ。

②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。

(3) 物理的セキュリティ

サーバー、通信回線及び職員のパソコン等の管理について、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、職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の人的な対策を講じる。

(5) 技術的セキュリティ

コンピューター等の管理、アクセス制御、不正プログラム対策及び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、情報セキュリティポリシーの遵守状況の確認、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できるように緊急時の対策を講じるものとする。

(7) 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である場合は、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、リスクを検討した上で、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、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。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広域連合の行政運用に重大な支障を及ぼす恐れがあることから、非公開とする。