揖斐広域連合情報セキュリティポリシー

（基本方針）

揖斐広域連合

－ 目　次 －

揖斐広域連合情報セキュリティポリシー

平成２７年１０月１日策定

揖斐広域連合情報セキュリティポリシーの構成

情報セキュリティポリシーとは、揖斐広域連合（以下、「広域連合」という。）が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称するもので、情報セキュリティ基本方針及び情報セキュリティ対策基準の２階層で構成されています。

○情報セキュリティ基本方針

情報セキュリティ対策に関する統一的かつ基本的な方針です。

○情報セキュリティ対策基準

情報セキュリティ基本方針を実行に移すためのすべてのネットワーク及び情報システムに共通の情報セキュリティ対策の基準です。

揖斐広域連合情報セキュリティ基本方針

（目的）

第１条　この基本方針は、広域連合が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産（以下「対象資産」という。）について、広域連合が実施する情報セキュリティに関する基本的な事項を定めることにより、行政の適正かつ円滑な運営を図り、もって広域連合の行政に対する構成町民の信頼を確保することを目的とする。

（定義）

第２条　この基本方針において、次の各号に掲げる用語の意義は、当該各号の定めるところによる。

（１）コンピュータ

パーソナルコンピュータ、サーバ、ストレージ等の機器をいう。

（２）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。

（３）情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

（４）情報資産

情報システムで取り扱う情報で、開発及び運用に係るものを含むすべての情報をいう。

（５）情報セキュリティ

対象資産の機密性、完全性及び可用性を(注)維持することをいう。

(注)：国際標準化機構（ＩＳＯ）が定めるもの

機密性(confidentiality)：情報にアクセスすることが認可された者だけがアクセスすることを確実にすること

完全性(integrity)：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

可用性(availability)：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

（６）情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

（７）機密性

対象資産にアクセスすることを認められた者だけが、対象資産にアクセスできる状態を確保することをいう。

（８）完全性

対象資産が破壊、改ざん、消去又は不正なデータがない状態を維持し、データの正当性、正確性、一貫性等を確保することをいう。

（９）可用性

対象資産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、対象資産にアクセスできる状態を確保することをいう。

（１０）特定個人情報

行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）第２条に規定する、個人番号をその内容に含む個人情報ファイルをいう。

（１１）個人番号利用事務

番号法第２条に規定する個人番号を利用して処理する事務をいう。

（対象とする脅威）

第３条　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）人による脅威（故意）
　不正アクセスやウイルス攻撃等のサイバー攻撃、機器の盗難、対象資産の不正な操作や持ち出し等の故意による情報資産の漏えい・破壊・改ざん・消去等

（2）人による脅威（過失）
　対象資産の管理不備、無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、外部委託管理の不備等の過失による情報資産の漏えい・破壊・消去等

（3）災害による脅威
　地震、落雷、火災、水害等の災害によるサービス及び業務の停止、情報資産の消去等

（4）必要資源の不足、故障等による脅威
　災害の影響又はその他の原因による電力、通信、水道の途絶、交通機能の麻痺や大規模・広範囲にわたる疫病の蔓延による要員の不足、機器の故障等によるサービスや業務の停止、システム運用の機能不全等

（適用範囲）
第４条　この基本方針の適用範囲は、広域連合が保有する対象資産、対象資産に関する事務に携わるすべての職員、非常勤職員、臨時職員、労働者派遣事業により広域連合の事務に携わる者（以下「職員等」という。）及び委託事業者とする。

（遵守義務）
第５条　前条に規定する者は、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。

（情報セキュリティ対策）
第６条　第３条の脅威から対象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ものとする。

（1）組織体制
　情報セキュリティ対策を推進する組織体制の確立

（2）情報資産の分類と管理
　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、当該分類に基づく情報セキュリティ対策

（3）物理的セキュリティ
　対象資産の設置方法又は保管施設の管理についての物理的な対策

（4）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、十分な教育及び啓発を行う等の人的な対策

（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

（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、外部委託を行う際の情報セキュリティの確保等、情報セキュリティポリシーの運用面の対策、対象資産への侵害が発生した場合等に、迅速かつ適切に対応するための危機管理対策（緊急時対応計画の策定）

（情報セキュリティに関する監査及び自己点検の実施）
第７条　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に関する監査及び自己点検を実施する。

（情報セキュリティポリシーの見直し及び改定）
第８条　情報セキュリティに関する監査及び自己点検の結果又は情報セキュリティに関する状況の変化に対応するため、定期的に情報セキュリティポリシーの見直しを行い、必要に応じて改定する。

（情報セキュリティ対策基準の策定）
第９条　第６条、第７条、第８条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。

（情報セキュリティ実施手順の策定）
第１０条　情報セキュリティ対策基準に基づき、情報セキュリティに関する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について、揖斐広域連合情報公開条例第７条に定める非公開情報に該当するものは非公開とする。

（懲戒処分）
第１１条　情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

附則
平成２７年１０月１日　策定