岡垣町情報セキュリティポリシー

岡垣町役場　デジタル推進課

平成１６年　３月　策　　定
平成２５年　４月　一部改正
平成２８年　３月　全部改定
令和　８年　３月　一部改正

Ⅰ　総　則

１．情報セキュリティポリシーとは

地方公共団体は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、ほかに代替することができない行政サービスを提供している。また、地方公共団体の業務の多くが情報システムやネットワークに依存しており、これらに障害が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まっている。このことから、住民生活や地域の社会経済活動を保護するため、地方公共団体は、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となる。

また、地方公共団体や国等はネットワークにより相互に接続しており、一部の団体で発生した障害がネットワークを介して他の団体に連鎖的に拡大する可能性は否定できない。このことから、全ての地方公共団体において、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが重要となっている。

さらに、情報セキュリティに関する障害・事故及びシステム上の欠陥（以下、「情報セキュリティインシデント」という。）の未然防止のみならず、万が一に情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要となっている。

このようなことから、情報セキュリティポリシーは、地方公共団体が保有する情報資産を自らの責任により守っていくため、組織の実態に応じて、地方公共団体内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めたものいう。

２．岡垣町情報セキュリティポリシー

岡垣町情報セキュリティポリシーは、本町が所管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。

岡垣町情報セキュリティポリシーは、実施機関が所管する情報資産に関する業務に携わる全ての職員（非常勤の特別職及び会計年度任用職員を含む。以下、「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、岡垣町情報セキュリティポリシーは、一定の普遍性を備えた部分（岡垣町情報セキュリティ基本方針）と情報資産を取り巻く状況の変化に依存する部分（岡垣町情報セキュリティ対策基準）の２階層に分けて策定する。

Ⅱ　岡垣町情報セキュリティ基本方針

１．目的

岡垣町情報セキュリティ基本方針（以下「基本方針」という。）は、本町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、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

情報資産の機密性、完全性及び可用性を維持することをいう。

- 機密性：情報にアクセスすることを認められた者だけが、アクセスできる状態を確保すること
- 完全性：情報及び処理方法の正確さ及び情報が破壊、改ざん又は消去されていない状態を確保すること。
- 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。

（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）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（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（６）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（マイナンバー利用事務系を除く。）。

（７）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。

（８）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。

（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。

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、重要な情報の詐取、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．適用範囲

（１）適用される機関の範囲

本基本方針が適用される機関は、町長部局、公営企業、教育委員会、議会、各種行政委員会（選挙管理委員会、監査委員、農業委員会及び固定資産評価審査委員会）及び外部委託事業者を対象とする。また、地方自治法（昭和 22 年法律第 67 号）第 244 条の 2 第 3 項に規定する指定管理者（以下「指定管理者」という。）に情報資産を管理させる場合については、指定管理者を含むものとする。

（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。

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の開発・運用で取り扱う全ての情報（入力・出力した文書等を含む。）

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．職員等の遵守義務

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。

（１）組織体制

本町の情報資産について、情報セキュリティ対策を推進・管理する全庁的な組織体制を確立する。

（２）情報資産の分類と管理

本町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行う。

（３）物理的セキュリティ

サーバ等、情報システム室等、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。

（４）人的セキュリティ

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、全ての職員等に情報セキュリティポリシーの内容を周知徹底する等、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、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、危機管理対策を講じる。

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、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。
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町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。