

塩竈市行政情報 セキュリティポリシー

塩竈市

平成15年12月 策定
令和8年3月 一部改定

第1章 塩竈市行政情報セキュリティポリシーの構成

塩竈市行政情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、塩竈市が保有する情報資産に関する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である。

情報セキュリティポリシーは、本市の情報資産を取り扱う全職員に浸透、定着させるものであり、安定的な規範であることが要求される。しかし一方では、情報セキュリティ対策は、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に、柔軟に対応することも必要である。

このようなことから、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としての「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適正に対応する部分としての「情報セキュリティ対策基準」の2階層から構成する。

また、情報セキュリティポリシーに基づき、具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定することとする。

文 書 名		内 容
情報 セキュリティポリシー	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かつ基本的な方針
	情報セキュリティ 対策基準(非公開)	情報セキュリティ基本方針を実行に移すための全ての情報資産に共通の情報セキュリティ対策基準
情報セキュリティ実施手順(非公開)		ネットワーク及び情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

第2章 情報セキュリティ基本方針

2.1 目的

塩竈市が取り扱う情報資産には、市民の個人情報をはじめとし、行政運営上重要な情報など、外部に漏洩等した場合に、極めて重大な結果を招くおそれのある情報が多数含まれている。

また、近年の IT 革命の進展により、電子自治体の構築の実現化が進んできているところである。

このような状況の中、塩竈市が保有する情報資産を人的脅威や災害、事故等の様々な脅威から防御することは、市民の財産、プライバシーを守るためにも、また、継続的かつ安全・安定的な行政サービスを提供するためにも必要不可欠である。

よって、塩竈市の保有する情報資産の機密性、完全性及び可用性（注）を維持する対策を整備するため、情報セキュリティポリシーを定めて、本市の情報セキュリティの確保に最大限取り組むこととする。

このうち、情報セキュリティ基本方針においては、本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの位置付け、対象等を定めるものとする。

（注）：国際標準化機構（ISO）が定めるもの（ISO7498-2:1989）

- ・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。

- ・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。

- ・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、情報及び関連資産にアクセスできる状態を確保すること。

2.2 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) 情報資産

ネットワーク及び情報システムの開発と運用に係るすべての情報並びにネットワーク及び情報システムで取り扱うすべての情報をいう。

(4) 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。

(5) 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。

(6) 情報システム室等（以下、「電算室等」という。）

電子計算機を運用・管理する目的で設置している部屋をいう。

(7) 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。

(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（マイナンバー利用事務系を除く。）。

(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) 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。

(11) 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。

2.3 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、重要情報の詐取、内部不正等
- (2) 情報資産の無断持出、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、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) 電源供給の途絶、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

2.4 適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は、市長部局、教育委員会（各市立小中学校を含む。）、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、上下水道部、市立病院事務部及び議会とする。

(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
- 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

2.5 職員等の遵守義務

本市の情報資産に接する全ての職員（特別職、派遣職員、会計年度任用職員等を含む。以下「職員等」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。

2.6 情報セキュリティ対策

上記 2.3 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

本市の情報資産について、情報セキュリティ対策を推進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

本市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。

(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、情報システム全体に対し、次の三段階の対策を講じる。

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や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

② 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。

③ 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、県及び市町村のインターネットとの通信を集約した、自治体情報セキュリティクラウドの利用を推進する。

(4) 物理的セキュリティ

サーバ、電算室、通信回線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。

(5) 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、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 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。

(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、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正に対応するため、緊急時対応計画を策定し、定期的に見直しを行う。

(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、利用にかか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。

2.7 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。

2.8 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。

2.9 情報セキュリティ対策基準の策定

上記 2.6、2.7 及び 2.8 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ものとする。

なお、情報セキュリティ対策基準は、公にすることにより本市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。

2.10 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市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。