宮崎市情報セキュリティポリシー

令和６年２月１４日改訂

宮　崎　市

目次

宮崎市情報セキュリティポリシーの構成

宮崎市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、宮崎市が管理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であり、情報セキュリティ対策の頂点に位置する。セキュリティポリシーは、宮崎市が管理する情報資産に関する業務に携わる全職員・非常勤職員・臨時職員（以下「職員等」という。）及び委託事業者や公の施設の指定管理者（以下「委託事業者等」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。一方では、技術の進歩などに伴う情報セキュリティを取り巻く状況の急速な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、セキュリティポリシーを一定の普遍性を備えた部分（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（対策基準）に分けて策定することとした。

具体的には、セキュリティポリシーを、

情報セキュリティ基本方針
情報セキュリティ対策基準

の２階層に分け、それぞれを策定している。

また、情報セキュリティ対策基準に基づく、ネットワーク・情報システムごとの具体的な情報セキュリティ対策の実施手順を、情報セキュリティ実施手順として別途策定することとしている（下表参照）。なお、情報セキュリティ実施手順は、公にすることにより宮崎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。

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的かつ基本的な方針
	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と情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		情報セキュリティ対策基準に基づく、ネットワーク・情報システムごとの具体的な情報セキュリティ対策の実施手順

第１章　情報セキュリティ基本方針

１．　目的

情報セキュリティ基本方針（以下、「本基本方針」という。）は、宮崎市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、宮崎市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。

（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（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その情報システムで取り扱うデータをいう。

（9）LGWAN接続系（総合行政ネットワーク接続系）

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。）。

（１０）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。

（１１）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。

（１２）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。

（１３）外部サービス

クラウドサービス、Web会議サービス、SNS、検索サービス、翻訳サービス、地図サービス、ホスティングサービスなど、庁外の通信回線やシステムを利用して委託事業者等が提供するサービスをいう。

（１４）自治体情報セキュリティクラウド

都道府県と市区町村がWebサーバー等を集約し、監視及びログ分析・解析をはじめ高度なセキュリティ対策を実施することをいう。

（１５）ゼロトラストセキュリティ

接続元のネットワークを問わず、全てのアクセスを信頼せず検証するセキュリティモデルをいう。

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、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）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、行政委員会事務局、消防局、上下水道局、教育機関（事務室のみ）とする（以下「部局等」という。）。

（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。

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、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、業務の遂行にあ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。

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、次の情報セキュリティ対策を講じる。

（1）組織体制

宮崎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

宮崎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行う。

（3）情報システム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。

②LGWAN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、インターネット接続系からLGWAN接続系へ通信する場合には、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、自治体情報セキュリティクラウドの導入等を実施する。

（4）物理的セキュリティ

サーバ等、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋（以下、「情報システム室」という。）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。

（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、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、緊急時対応計画を策定する。

（8）業務委託と外部サービスの利用

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。外部サービスを利用する場合には、利用に関す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、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宮崎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。