南国市情報セキュリティポリシー

令和８年３月３１日　改定

南　　国　　市

目次

南国市
情報セキュリティ
基本方針

情報セキュリティ基本方針

１　目的

本市が取り扱う情報資産には、住民の個人情報をはじめとする行政運営上重要な情報が多数含まれている。これらの情報を漏えい、事故等から防御することは、市民の財産、プライバシー等を守るためにも、また、継続的かつ安定的な行政事務の実施を確保するためにも必要不可欠である。

本基本方針は、本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、本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

この基本方針において、使用する用語の意義は、個人情報の保護に関する法律（平成15年5月30日法律第57号）及び南国市情報公開条例（平成13年12月25日条例第39号）で使用する用語の例によるほか、次の各号に定めるところによる。

（１） 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。

（２） 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。

（３）情報セキュリティ管理

情報セキュリティを維持するために、全庁的にポリシーを策定し（計画）、ポリシーの周知、責任の割当て、対策の実施を行い（実施）、監査や日々の業務を通じた問題点を報告し（評価）、対策の追加・改善を行い（改善）、組織として必要な情報セキュリティレベルを維持し続ける取り組みをいう。

（４）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をいう。

（５）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。

（６）機密性

情報にアクセスすることを認可された者だけが、許された範囲内においてのみ当該情報を利用できる状態を確保することをいう。

（７） 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。

（８） 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。

（９） 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。

（１０） ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等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。

（１１） 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。

（１２） 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。

（１３） 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。

（１４）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をいう。

（１５）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、すべての情報資産に共通の情報セキュリティ対策の基準をいう。

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）意図的な人的脅威

①職員（非常勤職員、会計年度任用職員等を含む。以下同じ。）、議員及び委員等、本市の情報を取り扱う者（以下「職員等」という。）による情報資産の漏えい（口頭によるものを含む。）

②職員等による故意の不正アクセス及び不正操作

③職員等による機器及び記録媒体の盗難

④職員等によるサービス停止攻撃などの情報サービスへの妨害

⑤職員等によるデータ及びプログラムの持ち出し・盗聴・改ざん・消去

（２）偶発的な人的脅威

①職員等の誤操作による機器の破壊又はデータ及びプログラムの消去又は破壊

②職員等による情報資産の持ち出し又は紛失

③職員等の誤操作による不正アクセス

（３） 技術的脅威

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、重要情報の詐取等

（４） 物理的脅威等

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、業務委託管理の不備、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

（５） 災害

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

（６） パンデミック

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

（７）インフラ障害

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

（８）情報システム、ネットワークの不具合

４　適用範囲

（１）行政機関の範囲

本基本方針は、地方公共団体の「議会」及び「長その他の執行機関」を対象とし、具体的には以下のとおり定める。

【議会】

議員及び議会に付随する組織（議会事務局等）

【執行機関】

本市の市長部局、消防本部、地方公営企業、教育委員会、選挙管理委員会、監査委員事務局、農業委員会、固定資産評価審査委員会とする。

（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本市が所有もしくは利用するネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

②業務で取り扱う情報（ネットワーク、情報システムで取り扱う情報であって、電磁的もしくは原本等の紙媒体及びこれらを複写したもの）

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。

６　情報セキュリティ対策

上記３の脅威について、情報資産に対する脅威の大きさや発生頻度、適切性（利便性）、経済合理性（コスト）を考慮して、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ものとする。

（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靭性の向上

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、両システム間で通信する場合には、無害化通信もしくは同等のデータ保全策を実施する。

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、都道府県と市区町村のインターネット接続口を集約した上で、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）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。

（５）物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、不正侵入や盗難等の人的脅威及び災害等環境的脅威から情報資産を保護するため、物理的な対策を講じる。

（６）技術的セキュリティ

情報資産を外部及び内部からの不正アクセス等から保護するため、ソフトウェアや情報機器等の管理、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。

（8）緊急時における対応

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。

（9）業務委託と外部サービス（クラウドサービス）の利用

業務委託する場合には、本市と同等の又はそれ以上の情報セキュリティ管理を行っている業務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、業務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検査等の措置を講じる。

約款による外部サービス（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。

（１０） 評価・見直し

セキュリティポリシーにいうセキュリティ品質を維持するため、定期的に自己点検又は必要に応じて監査を実施し、情報セキュリティポリシーそのものも含む見直し及び運用改善を行う。

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外部環境の変化等、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。

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。

１１　法令の遵守

関連する法令等の遵守について定める。

１２　違反に対する対応

情報セキュリティポリシーに違反した者への対応を定める。

１３　公開方針

公開については、次のとおりとする。

（１）情報セキュリティ基本方針

情報セキュリティ基本方針は公開する。

（２）情報セキュリティ対策基準及び情報セキュリティ実施手順

情報セキュリティ対策基準及び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。