海南市情報セキュリティ基本方針

令和７年１月31日改定

[　目　次　]

序文 ----------1

第１章　基本的な考え方 ----------2
第１節　目的 ----------2
第２節　定義 ----------2
第３節　情報資産に対する脅威 ----------3
第４節　適用範囲 ----------3
第５節　職掌上の役割と責任 ----------4

第２章　情報セキュリティ対策----------4
第１節　組織体制 ----------5
第２節　情報資産の分類と管理 ----------5
第３節　情報システム全体の強靭性の向上 ----------5
第４節　物理的対策----------5
第５節　人的対策 ----------5
第６節　技術的対策----------5
第７節　運用上の対策 ----------6
第８節　業務委託とクラウドサービスの利用----------6
第９節　評価・見直し ----------6

第３章　情報セキュリティポリシー等の取扱い----------6
第１節　海南市情報セキュリティ基本方針 ----------6
第２節　海南市情報セキュリティ対策基準 ----------6
第３節　海南市情報セキュリティ実施手順 ----------7

序　文

海南市の各情報システムが取り扱う情報には、市民の個人情報のみならず、行政運営上重要な情報など、部外への漏洩、改ざん等が生じた場合には、極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から保護することは、市民の財産とプライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが本市に対する市民からの信頼の維持向上に寄与するものである。

そのため本市では、情報資産のセキュリティを保持するため、全庁的な統一方針として「海南市情報セキュリティポリシー」を策定し、職員全員がこれを遵守することとする。

海南市情報セキュリティポリシーは、本市の情報資産をどのような脅威からどのようにして守るのかについての基本的な考え方（基本方針）と基本方針を実現するために遵守すべき行為及び判断等の基準（対策基準）から構成する。

第１章　基本的な考え方

第１節　目的

本基本方針は、海南市（以下「本市」という。）の職員及び委託事業者など情報資産を扱う者全員が、情報資産を使用するときに従うべき情報セキュリティを守るための基本的な考え方や方向性を定めることを目的とする。

第２節　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

本基本方針及び海南市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データをいう。

（９）　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）。

(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。

(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)　職員

一般職常勤職員（任期付職員及び再任用職員を含む。）及び会計年度任用職員等を含む全ての職員をいう。

(14)　委託事業者

本市の事務事業の委託を受けた者及び市の公の施設の指定管理者をいう。

第３節　情報資産に対する脅威

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、津波、落雷、火災及び風水害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、通信の途絶等のインフラの障害からの波及等

第４節　適用範囲

第１項　対象組織の範囲

本基本方針は、海南市部設置に関する条例（平成 17 年海南市条例第６号）第１条に定める部並びに議会事務局、下津行政局、出納室、教育委員会事務局、選挙管理委員会事務局、監査委員事務局、農業委員会事務局、公平委員会事務局、消防本部及び公営企業に適用する。ただし、教育系ネットワーク及び医療情報系ネットワークを除く。

第２項　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

第５節　職掌上の役割と責任

第１項　市長の役割と責任

市長は、情報セキュリティに関する指針を明らかにし、職員に対して情報セキュリティ意識を浸透させ、必要な支援をする役割と責任をもつ。

第２項　所属長の役割と責任

所属長は、情報セキュリティ確保の責任を負い、所属職員及び委託事業者が本基本方針を理解し遵守することを徹底し、かつ管理しなければならない。

また、所属長は、所属職員が退職又は異動する場合において、利用する必要のなくなった全ての情報資産を回収する責任を負うものとする。委託事業者が契約終了した場合もまた同様とする。

第３項　職員の役割と責任

職員は、情報セキュリティポリシー及び海南市情報セキュリティ実施手順並びに所属長の指示を遵守し、情報が不正な手段で取得されること又は不正に使用されることを防止する責任を負うものとする。

職員は、退職又は異動する場合において、利用する必要のなくなった全ての情報資産を所属長に返却しなければならない。

第４項　委託事業者の役割と責任

委託事業者は、契約に基づき、情報セキュリティポリシー及び海南市情報セキュリティ実施手順並びに関係する部署の所属長の指示を遵守し、情報を不正な手段で取得し又は不正に使用してはならない。

委託事業者は、契約終了その他の事情により本市の情報資産を取り扱うことがなくなった時点で、全ての情報資産を本市に返却しなければならない。

第２章　情報セキュリティ対策

第１章第３節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。

第１節　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。

第２節　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。

第３節　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。

（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、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

第４節　物理的対策

情報システム及びネットワークを設置する区域又は施設への不正な立入り及び情報システム、ネットワーク又は情報資産への損傷・妨害等から保護するための物理的な対策を講じる。

第５節　人的対策

情報セキュリティに関する権限及び責任を定め、職員に対し情報セキュリティポリシー及び情報セキュリティに関する法令などの内容を周知徹底するとともに、十分な教育及び啓発を行う等の人的対策を講じる。

第６節　技術的対策

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。

第７節　運用上の対策

（１）　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。

（２）　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する。

第８節　業務委託とクラウドサービスの利用

（１）　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。

（２）　クラウドサービスを利用する場合には、利用に係る規定を整備し対策を講じる。

（３）　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。

第９節　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。

第３章　情報セキュリティポリシー等の取扱い

第１節　海南市情報セキュリティ基本方針

本基本方針は、市民の個人情報及び行政運営上重要な情報の管理及び情報セキュリティ対策についての基本的な考え方や方向性を定めるものとし、外部に対し公開する。

第２節　海南市情報セキュリティ対策基準

本基本方針に基づいた情報セキュリティ対策を講じるに当たって、遵守すべき事項及び判断基準を統一的に定めるために、必要となる基本要件を明記した海南市情報セキュリティ対策基準（以下「対策基準」という。）を策定する。

対策基準は、情報資産を扱う全ての職員に対し、周知徹底する。

なお、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ため、非公開とする。

第３節　海南市情報セキュリティ実施手順

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、個々の部署や情報システムについて、具体的な手順を定めた海南市情報セキュリティ実施手順（以下「実施手順」という。）を策定する。

なお、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ため、非公開とする。