熱海市情報セキュリティ基本方針　　令和８年３月２日改定

１　目的

熱海市情報セキュリティ基本方針は、熱海市（以下「本市」という。）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に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とともに、本市が積極的に情報セキュリティ対策に取り組み、情報セキュリティの確保を図ることを目的とする。

２　定義

この基本方針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(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) 情報セキュリティインシデント　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をいう。

(9) サーバ室　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をいう。

(10) モバイル端末　携帯電話、スマートフォンやタブレット型端末など、持ち運びが可能な携帯情報機器のことをいう。

(11) ソーシャルメディア　インターネットを利用してユーザが情報を発信し、あるいは相互に情報をやり取りする情報の伝達手段のことをいう。

(12) マイナンバー利用事務系　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。

(13) ＬＧＷＡＮ接続系　グループウェア、統合型GIS、財務会計及び人事給与等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（マイナンバー利用事務系を除く。）。

(14) インターネット接続系　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。

(15) その他システム系　他組織が主管する情報システム若しくはスタンドアロンパソコン及びそれらで取り扱うデータをいう。

(16) 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。

(17) 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、改ざん若しくは消去又は重要情報の詐取、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、設計又は開発の不備、プログラム上の欠陥、操作又は設定ミス、メンテナンス不備、内部又は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、破壊若しくは消去等

(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) 大規模かつ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、副市長、教育長、会計管理者、熱海市行政組織測（昭和４６年熱海市規則第１９号）第２条に規定する内部組織に属する者、

熱海市議会事務局規則（昭和３８年議会規則第１号）第３条第１項に規定する職にある者、熱海市教育委員会事務局処務規則（平成２０年教育委員会規則第１号）第２条第１項に規定する内部組織に属する者、同規則第４条第２項に規定する所属職員を指揮監督する職にある者、熱海市立図書館処務規則（昭和４２年教育委員会規則第３号）第４条に規定する職にある者、熱海市選挙管理委員会規則（昭和２５年選挙管理委員会規則第１号）第１２条第１項に規定する職にある者、熱海市監査委員条例施行規則（昭和２６年監査委員規則第１号）第７条に規定する職にある者、熱海市農業委員会規程（昭和３６年農業委員会規程第１号）第７条第１項に規定する職にある者、熱海市会計課設置規則（昭和３９年規則第１６号）第３条第１項に規定する職にある者、熱海市消防本部の組織等に関する規則（昭和４０年規則第１４号）第２条に規定する内部組織に属する者、同規則第４条第１項に規定する消防長の職にある者、熱海市消防署の組織等に関する規程（昭和４０年消防本部訓令第２号）第４条に規定する職にある者、熱海市公営企業部処務規程（昭和３４年公営企業部規程第１号）に規定する組織に属する者並びに同規程第４条に規定する部長及び次長の職にある者とする。

(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。

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、会計年度任用職員等（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。

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実施する。

(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。

ア　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。

イ　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。

ウ　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。

(4) 物理的セキュリティ

サーバ、サーバ室、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て、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、外部委託を行う際の情報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する。

(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、利用に係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。

⑼ 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。

7　情報セキュリティ対策基準の策定

基本方針に従い、本市における情報セキュリティ対策を行う上で必要となる具体的な遵守事項及び判断基準等を定めるため、情報セキュリティ対策基準を策定する。

8　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。

9　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の非公開

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、公開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。

１０　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。

１１　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。