海老名市情報セキュリティ基本方針

第４版

「安心と信頼の情報化社会を目指して」（基本理念）

海老名市では、ＩＴ（情報通信技術）を重要な社会の基盤として捉え、これを利用した情報化を推進することにより、電子自治体の構築を目指しています。

情報化を推進し、電子自治体を構築するに当たっては、本市の保有する情報を自然災害や不正なアクセス、情報の漏えい・改ざん等の脅威から防御し、高度な健全性を有した情報システムを構築していかなければなりません。

このような状況を踏まえ、市民の個人情報や行政運営上重要な情報に関して、市民の権利・利益を守りつつ、安心して情報システムが利用できるよう、情報セキュリティの確保の遵守徹底を図り、外部及び内部の不正行為を防止するための方策として、ここに「セキュリティポリシー」を定め、以下の対策を実行し維持することを宣言します。

１．情報セキュリティの指針の策定
２．情報セキュリティ対策の推進
３．情報セキュリティに関する内部規定等の整備
４．情報セキュリティ教育の徹底
５．情報セキュリティ監査の実施及び評価・見直し

平成２６年　４月　１日

海老名市長　内　野　　優

〈 目　　次 〉

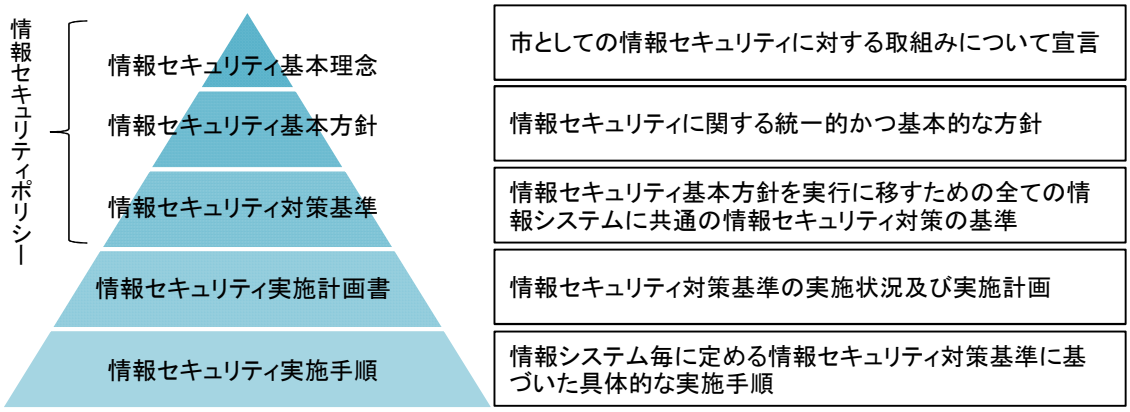
序　海老名市情報セキュリティポリシーの構成

海老名市情報セキュリティポリシーとは、海老名市が所有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を総称する。情報セキュリティポリシーは、海老名市が所有する情報資産に関する業務に携わる全職員、非常勤及び会計年度任用職員に浸透、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。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ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、情報セキュリティポリシーを、①情報セキュリティ基本方針及び②情報セキュリティ対策基準の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施手順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（下図参照）。

情報セキュリティポリシーの構成



総　　則

（目　的）

第１条　この基本方針は、情報セキュリティに対する基本的な指針を記述し、海老名市（以下「市」という。）の実施機関が管理する情報資産及び出先機関から利用できる市の実施機関のサービスを適切に保護することを目的とする。

市の実施機関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、部外に漏洩等し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、事務の安定的な運営のためにも必要不可欠であり、ひいてはこのことが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。

また、情報通信ネットワークや情報システムの利用は拡大しており、市に求められる電子情報サービスはより高度に多様化している。市の実施機関がこれらを提供し、市民が安心して利用できるようにするためには、全てのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、市の実施機関の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために海老名市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については市の実施機関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対象、位置付け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（confidentiality）：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性（integrity）　　：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性（availability）　：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

（定　義）

第２条　この方針において、次の各項に掲げる用語の定義は、それぞれ、当該各項に定めるものとする。

(1) 実施機関

海老名市行政組織規則（昭和 47 年規則第 10 号）に定める機関（附属機関を除く）、及び議会事務局、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、消防本部をいう。

(2) 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。

(3) 情報システム

業務系の電子計算機（実務系におけるネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

(4) 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全てのデータ並びにネットワーク及び情報システムで取り扱う全てのデータをいう。ここでいうデータとは紙（メモ含む）、音声、電子データ等のあらゆる形式で保存されている事物[1]、出来事[2]等を含む。

(5) 情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(6) 職員

地方公務員法で規定された特別職、一般職の中で市の実施機関に勤務し、市の実施機関が管理する情報資産を職務で利用する者（再任用、会計年度任用職員、非常勤職員を含む）の総称をいう。

(7) 外部要員

システム開発業務委託先社員等、契約に基づいて市の実施機関で作業する者の総称をいう。

(8) 脅威

自然の脅威（地震、火災、風水害等）、情報システムの脅威（情報システムの故障、誤動作等）及び人的な脅威（不正行為、誤操作等）をいう。

（情報セキュリティポリシーの位置付け）

第３条　情報セキュリティポリシーは、市の実施機関が所掌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ものとする。

（情報セキュリティポリシーの対象範囲）

第４条　情報セキュリティポリシーの対象範囲は、市の実施機関における情報資産に関する業務及び情報資産に携わる全ての職員及び外部要員とする。

---

1 事物：情報を格納している様々なメディアのこと。また、講演会や会議の内容及び口述並びにそれらを保存したもののこと。

2 出来事：職務執行中に起こった事故や事件及びその内容のこと。

（職員の責務）
第５条　職員は、情報セキュリティの重要性について共通の認識をもつとともに業務の遂行に当たって次に掲げる義務を負うものとする。
（1）この基本方針を遵守し、情報セキュリティ対策を有効に機能させなければならない。
（2）職務上知り得た情報を漏らしてはならない。その職を退いた後も同様とする。

情報セキュリティ推進体制

（情報セキュリティ管理体制）
第６条　市の実施機関の情報資産について、トップダウンによる情報セキュリティ対策を推進・管理するための体制を確立するものとする。

（外部要員の管理）
第７条　外部要員を管理する職員は、契約等に基づき、第５条と同様の内容を外部要員に対しても義務づけるものとする。

情報の区分

（情報資産の分類）
第８条　情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

情報セキュリティ対策

（情報資産への脅威）
第９条　情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮しなければならない。特に以下の脅威は認識すること。
（1）サイバー攻撃をはじめとする部外者による不正アクセスまたは不正操作による意図的なデータやプログラムの持出・盗聴・改ざん・消去、機器及び媒体の盗難等。
（2）職員及び外部要員による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。
（3）地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止。また、災害に伴い発生する電力供給の途絶、通信の途絶・水道供給の途絶等の提供サー

ビスの障害からの波及等。

（情報セキュリティ対策）

第１０条　第９条で示した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ものとする。

(1) 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために物理的な対策を講じる。

(2) 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員に情報セキュリティポリシーの内容を周知徹底する対策を講じる。

(3) 技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、また、システム開発等の業務委託、ネットワークの監視、情報セキュリティポリシーの遵守状況及び確認等の運用面の対策を講じるものとする。

また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講じる。

(4) 情報システム開発セキュリティ対策

情報システムの誤作動、不正利用、情報漏洩等から情報資産を保護するために、開発環境、品質保持に必要な対策を講じる。

(5) 情報システム運用セキュリティ対策

市の実施機関が管理する情報システムに対して運用ミスや情報漏洩等から情報資産を保護するために、情報システムの運用、保守、監視等の必要な対策を講じる。

(6) ネットワークセキュリティ対策

ネットワーク障害、不正アクセス等から情報資産を保護するために、ネットワークの可用性確保、ネットワーク監視等の必要な対策を講じる。

（情報セキュリティ対策基準の策定）

第１１条　市の実施機関の様々な情報資産について、第１０条の情報セキュリティ対策を講じるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

（情報セキュリティ実施計画書）

第１２条　対策基準に規定されている情報セキュリティ対策について、実施状況及び実施計画を記述した情報セキュリティ実施計画書（以下「実施計画書」という。）を作成する

ものとする。

（情報セキュリティ実施手順の策定）
第１３条　情報セキュリティ対策基準で規定した情報セキュリティ対策を実施するため、必要に応じて情報セキュリティ実施手順書を改訂及び作成するものとする。

（非公開の原則）
第１４条　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は、公にすることにより市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とするものとする。ただし、情報セキュリティ基本理念はこの限りではない。

情報セキュリティ教育

（情報セキュリティ教育の徹底）
第１５条　情報セキュリティポリシーの運用を徹底するため、職員及び外部要員に十分な教育及び啓発が実施できるように必要な対策を講じるものとする。

情報セキュリティに関する監査

（情報セキュリティ監査の実施）
第１６条　情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を実施するものとする。

情報セキュリティポリシーの評価及び見直し

（評価及び見直しの実施）
第１７条　情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施するものとする。

法令の遵守

（関連法令の遵守）
第１８条　職員は、職務遂行において、関連法令を遵守しなければならない。

罰　　則

（罰　則）

第１９条　この情報セキュリティポリシーに定められた情報セキュリティ対策に違反した職員は、地方公務員法その他関連法令の規定により、懲戒処分等の対象となることがある。

附　　則

この基本方針は、平成１５年４月１日から施行する。

この基本方針は、平成１５年１２月２４日から施行する。

この基本方針は、平成２６年　４月　１日から施行する。

この基本方針は、令和　４年　７月　１日から施行する。