

静岡市

情報セキュリティポリシー

令和4年4月1日

静岡市情報セキュリティ委員会

序 文

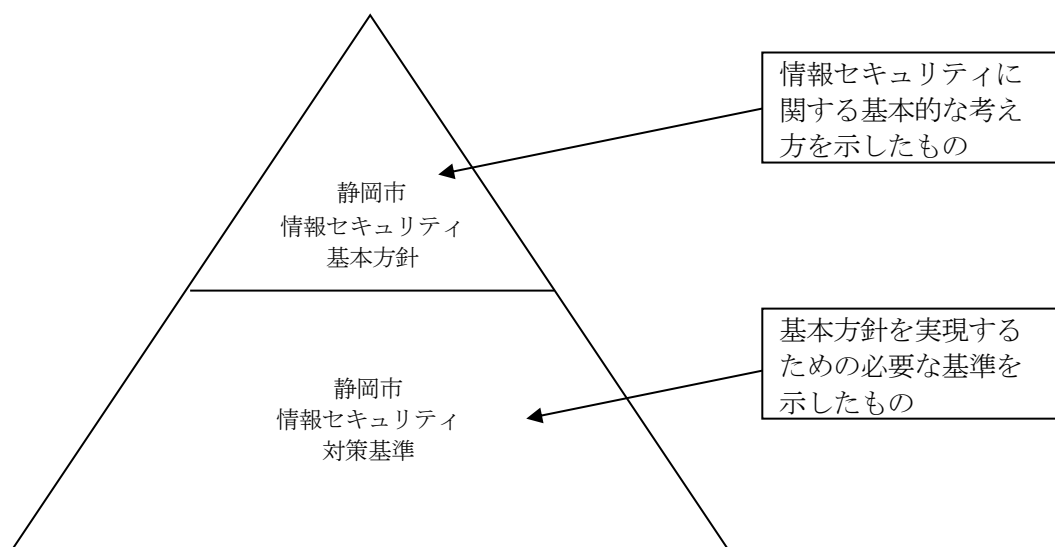
静岡市は、ICTの高度利用による情報化を推進することにより、電子自治体の実現を目指している。

情報化を推進し、電子自治体を実現するに当たっては、本市の保有する情報を不正なアクセス、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らない。

このような状況を踏まえ、静岡市は、保有する情報及び情報システムに関するセキュリティ対策を総合的、体系的かつ具体的に規定した静岡市情報セキュリティポリシーを策定することとした。

静岡市情報セキュリティポリシーについては、本市の全職員がその内容を十分理解した上で、各職場において率先して遵守すべきものであるため、安定的な規範であることが要請される一方、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に柔軟に対応できることも必要とされる。

このようなことから、静岡市情報セキュリティポリシーは、規範性を有する「情報セキュリティ基本方針」、情報及び情報システムを取り巻く状況変化に応じ、随時適切な見直しを行う「情報セキュリティ対策基準」により構成するものとする。



※ 具体的な確認項目や手順については、運用の手引きのほか、リスクに関するチェックシート及び危機管理に関するマニュアルに示す。

静岡市

情報セキュリティ基本方針

令和4年4月1日

静岡市情報セキュリティ委員会

改 版 履 歴

版 数	作 成 日
第 1 版	平成16年 7 月 13 日
第 2 版	平成17年 4 月 1 日
第 3 版	平成19年 4 月 1 日
第 4 版	平成26年 8 月 4 日
第 5 版	平成27年 4 月 10 日
第 6 版	平成28年 4 月 1 日
第 7 版	平成29年12月15日
第 8 版	令和 4 年 4 月 1 日

1 趣旨

情報セキュリティ基本方針（以下「基本方針」という。）は、静岡市（以下「本市」という。）の情報資産の機密性、完全性及び可用性を維持するために必要な対策に関する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。

2 定義

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) 情報

文書（メモ等を含む。）、図画及び写真（これらを撮影したマイクロフィルムを含む。）並びに電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）をいう。

(2) 行政情報

行政事務の執行に関する情報をいう。

(3) 情報システム

コンピュータ、ソフトウェア、ネットワーク及び周辺機器で構成され、情報の処理を行う仕組みをいう。

(4) 情報資産

情報及び情報システムをいう。

(5) 電子記録媒体

磁気、光学、半導体その他の原理により電磁的記録を保持することを目的とした媒体をいう。

(6) 外部記録媒体

電子記録媒体のうち、情報を保持したまま、容易に取り外しが出来るものをいう。

(7) 記録媒体

電子記録媒体及び紙媒体をいう。

(8) 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。

(9) 機密性

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をいう。

(10) 完全性

情報及び処理の方法が正確かつ完全である状態を保護することをいう。

(11) 可用性

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をいう。

(12) 情報セキュリティインシデント

情報資産の不正使用、業務妨害行為、データの破壊及びそれらに至るための行為等の情報セキュリティに対する脅威及び脆弱性から発生する障害をいう。

(13) 脅威

自然災害、悪意のある行為等情報資産に被害を与える要因をいう。

(14) 脆弱性

情報セキュリティの弱い部分及び情報セキュリティを弱める環境等の脅威を発生しやすくさせる要因をいう。

(15) 職員等

本市に在職する地方公務員法(昭和25年法律第261号)第3条第2項に規定する一般職及び同条第3項第3号に規定する非常勤嘱託員並びに人事交流により本市の組織に配属されている職員をいう。

3 情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本市の情報資産に関する情報セキュリティ対策の最上位に位置するものである。

4 職員等の責務

職員等は、情報セキュリティの重要性について共通認識を持つとともに、情報資産の利用に当たっては、情報セキュリティポリシーを遵守するものとする。

5 情報セキュリティ対策

情報資産を脅威から防御し、又は情報資産の脆弱性を解消するため、次の情報セキュリティ対策を講ずるものとする。

(1) 情報セキュリティ組織運営対策

対策基準の適用範囲における情報セキュリティの推進及び向上のための組織体制を確立する。

(2) 情報資産管理

情報資産の作成及び複製、入手、保管、利用、送信、持出し並びに消去及び廃棄するための取扱いを明確にする。

(3) 人的セキュリティ

情報セキュリティの確保を図るため、職員等が服務上遵守すべき事項を明確にする。

(4) 物理的セキュリティ

サーバ等のハードウェアの設置環境並びに情報を取り扱う機器及び設備等について、情報セキュリティの確保に必要な対策を講ずる。

(5) IT資産管理

業務で利用するハードウェア、ソフトウェア及びライセンス等のIT資産の適正な運用等について、情報セキュリティの確保及びライセンスコンプライアンスの向上に必要な対策を講ずる。

(6) 技術的セキュリティ

情報システム等のログの管理、バックアップ等について、必要となる技術的なセキュリティ対策を講ずる。

(7) 情報システム開発、導入、保守等

情報システムに係る審査、情報システムの調達、開発、導入、保守等について、情報セキュリティの確保に必要な対策を講ずる。

(8) 外部サービス利用

事務事業を外部委託事業者又は指定管理者に実施させる場合若しくは約款による外部サービス、ソーシャルメディア又はクラウドサービス等を利用する場合において、情報セキュリティの確保のために必要な対策を講ずる。

(9) 情報セキュリティインシデント対応

情報セキュリティインシデントが発生した場合において、迅速かつ適切な対応を行うための手順等を明確にする。

(10) 情報セキュリティ対策評価

情報資産のリスク管理体制をより適切かつ効果的にするために行う監査、点検及び調査を明確にする。

(11) 情報セキュリティポリシー運用

静岡市情報セキュリティポリシーの遵守違反が発生したときの調査、違反行為者等に対する指示、情報セキュリティポリシーの例外措置等について、必要な対策を講ずるものとする。

6 情報セキュリティ対策基準の策定

5の情報セキュリティ対策において規定された事項について、職員等が遵守すべき範囲を定める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。

7 情報セキュリティポリシーの公開

情報セキュリティポリシーには、本市のセキュリティ上の脆弱性に関する内容が含まれるため、情報セキュリティの確保の観点から、基本方針及び対策基準の概要についてのみ公開するものとし、対策基準の全文については業務上必要がある場合に限り公開するものとする。

8 保健福祉長寿局清水病院及び学校の情報セキュリティ対策

(1) 情報セキュリティ対策基準の策定等

保健福祉長寿局清水病院及び学校は、この基本方針に準拠した独自の情報セキュリティ対策基準を策定し、及び運用する。

(2) 職員等への教育

保健福祉長寿局清水病院及び学校は、基本方針及び(1)の情報セキュリティ対策基準の周知徹底に必要な職員等への教育を実施する。