# 地方独立行政法人静岡市立静岡病院
# 情報セキュリティポリシー

令和８年４月１日

# 序　文

地方独立行政法人静岡市立静岡病院（以下「静岡病院」という。）は、ＩＣＴ（Information and Communication Technology）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医療業務の遂行を目指している。

従来、医療情報の取扱いについては紙が中心であったが、ＩＣＴの急速的な発展は医療情報サービスの提供及び保管等に大きな変化を与えた。また、静岡病院が取り扱う情報は重要な個人情報等、外部に漏えい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。

そこで、静岡病院が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、静岡病院は、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「地方独立行政法人静岡市立静岡病院情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）」を策定することとした。

情報セキュリティポリシーは、静岡病院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、情報セキュリティポリシーは、規範性を有する「地方独立行政法人静岡市立静岡病院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「地方独立行政法人静岡市立静岡病院情報セキュリティ対策基準」により構成するものとする。

地方独立行政法人静岡市立静岡病院情報セキュリティポリシーの構成

| 文書名 | | 内容 |
|---|---|---|
| 地方独立行政法人静岡市立静岡病院情報セキュリティポリシー | 地方独立行政法人静岡市立静岡病院情報セキュリティ基本方針 | 地方独立行政法人静岡市立静岡病院情報セキュリティ対策に関する基本的な考え方と方針を規定するもの。 |
| | 地方独立行政法人静岡市立静岡病院情報セキュリティ対策基準 | 「地方独立行政法人静岡市立静岡病院情報セキュリティ基本方針」に基づき、職員が遵守すべき行動及び判断等を行なう、情報セキュリティの対策基準を規定するもの。 |
| 地方独立行政法人静岡市立静岡病院情報セキュリティ実施手順 | | 「地方独立行政法人静岡市立静岡病院情報セキュリティ対策基準」に基づき、具体的な実施手順を規定するもの。 |

# 地方独立行政法人静岡市立静岡病院
# 情報セキュリティ基本方針

令和８年４月１日

改版履歴

| 版数 | 作成日 |
| --- | --- |
| 第１版 | 平成２８年４月１日 |
| 第２版 | 令和８年４月１日 |
| | |

## １　趣旨

地方独立行政法人静岡市立静岡病院情報セキュリティ基本方針（以下「基本方針」という。）は、地方独立行政法人静岡市立静岡病院（以下「当院」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、地方独立行政法人静岡市立静岡病院情報セキュリティポリシー（以下「ポリシー」という。）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

紙（メモ等を含む。）、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、出来事等をいう。

（２）情報システム

コンピュータ、ソフトウェア、ネットワーク及び記録媒体で構成され、情報の処理を行う仕組みをいう。

（３）記録媒体及び外部記録媒体

紙媒体及びコンピュータに使用される磁気ディスク、磁気テープ、フラッシュメモリその他これらに類する媒体を記録媒体といい、このうち、ＵＳＢメモリ等の容易に取外し可能で持ち出しできる記録媒体は、外部記録媒体という。

（４）情報資産

情報及び情報システムをいう。

（５）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。

（６）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。

（７）完全性

情報及び処理の方法の正確さ及び完全である状態を完全保護することをいう。

（８）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。

（９）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。

(10) 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。

(11) 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。

(12) 職員

当院に在職するすべての職員（正職員、非常勤職員及び臨時職員）をいう。

## 3　情報セキュリティポリシーの位置付け

ポリシーは、当院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　情報セキュリティポリシーの対象範囲

（1）ポリシーの対象範囲は、当院における情報資産及び情報資産を取り扱うすべての職員に適用する。

（2）（1）の情報資産に係る業務を外部委託する場合には、委託業務の受託者に対してもポリシーを遵守させるための措置を講ずる。

## 5　職員の責務

職員は、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、ポリシーを遵守するものとする。

## 6　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

情報セキュリティの推進及び向上のための組織体制の確立及び当該組織を通じたポリシーの周知徹底及び必要な教育を実施する。

（2）情報の管理対策

情報を適切に取り扱うため、情報の重要度に応じた分類を行い、情報の管理責任及び取扱方法を明確化する。

（3）情報セキュリティ行動対策

職員によるコンピュータの取扱い、パスワードの管理、電子メールの利用、インターネットの利用等に関し、情報セキュリティの確保に必要な対策を講ずる。

（4）環境・機器・設備管理対策

情報システムを設置する施設への不正な立入り、盗難、自然災害等から情報資産を適切に保護するために必要な入退室管理等の対策を講ずる。

（5）情報システム管理対策

情報システムの運用に関し、情報資産を不正アクセス等から適切に保護するため、コンピュータ管理、アクセス管理、コンピュータウイルス対策等の必要な対策を講ず

る。

（６）ネットワーク管理対策

ネットワークを経由した不正なアクセス等から、情報資産を適切に保護するため、ネットワーク構成管理、ネットワークアクセス制御等の必要な対策を講ずる。

（７）情報システム開発対策

情報システムの企画、設計、開発及び導入に関し、情報セキュリティの確保に必要な対策を講ずる。

（８）外部委託対策

情報セキュリティポリシーの適用範囲内で行う作業を外部委託する場合には、セキュリティ要求事項を明記した契約を結ぶ等の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対策

情報セキュリティインシデントの発生に対し、事前の対応策及び再発防止策を作成する。

(10) 病院業務継続対策

医療情報サービスの可用性及び代替手段を確保し、病院業務の継続性を高めるため、病院業務継続計画（サイバー攻撃時における事業継続計画）を作成する。

(11) 情報セキュリティポリシーの評価・見直し対策

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、ポリシーの遵守状況に関し、定期的に点検を行うとともに、情報セキュリティの対策を評価すること等により、ポリシーの見直しを実施するものとする。

(12) 法令等の遵守対策

ポリシーを適切に運用するため、関連法令及び院内規程、静岡市条例を遵守させるために必要な対策を講ずる。

(13) 違反への対応対策

ポリシーの違反を防ぐため、遵守状況の確認、遵守違反を発見した場合の報告義務、審議機関の設置等の必要な対策を講ずるものとする。

## ７　情報セキュリティ対策基準の策定

６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、職員が遵守すべき範囲を定める地方独立行政法人静岡市立静岡病院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。

## ８　情報セキュリティ実施手順の策定

個々の情報資産について、対策基準を踏まえ、具体的な業務の執行方法として情報セキュリティ実施手順を策定する。

## ９　情報セキュリティポリシーの公開

ポリシーには、法人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、基本方針のみ公開するものとし、対策基準及び実施手順については公開しないものとする。