焼津市立総合病院

情報セキュリティ基本方針

令和 ６ 年 ４ 月 １ 日

（はじめに）

1　焼津市立総合病院（以下「当院」という。）では、個人を識別する情報を含む医療に関する情報（以下「医療情報」という。）をはじめ、病院運営上重要な情報が含まれており、外部への漏えい等した場合には極めて重大な結果を招くものが数多く含まれている。国が進める医療 DX 政策により、医療情報の電子化範囲が拡大する中、病院をターゲットとした改ざんや漏えいを目的とした不正アクセス等の脅威は増大している。

これら医療情報を適切に保護・管理するとともに、様々な脅威（災害、事故、故意及び過失等）から防御する手立てを講ずることは、当院への信頼の維持と安定的な病院経営を図るためには必要不可欠な取り組みとなる。

当院の情報セキュリティ対策の基本的な方針を定めるとともに、厚生労働省が公表している医療情報システムの安全管理に関するガイドライン（以下「ガイドライン」という）別紙で示されている区分で作成した焼津市立総合病院　総合情報システム運用管理規程（以下「運用管理規程」という。）と併せて、当院の情報セキュリティポリシー（以下「ポリシー」という。）とする。

このポリシーは、当院のセキュリティ対策の基本的な方針として、適用の対象や位置づけ等を定め、真正性、見読性及び保存性を確保し、総合的、体系的かつ継続的に情報セキュリティ対策を行うことを目的とする。

なお、このポリシーに記載されている情報システム以外の情報セキュリティに関しては、焼津市が定める情報セキュリティポリシーを適用するものとする。

（定義）

2　この基本方針において用いる用語の定義は次のとおりとする。

（1）情報システム　当院において医療情報を取り扱うシステム（ハードウェア及びソフトウェアを含む。）及び情報を電磁的に処理する仕組みをいう。

（2）医療情報　個人を識別する情報を含む医療に関する情報をいう。

（3）情報ネットワーク　情報システムを相互に接続するための通信網及び通信を行うための機器で構成され、情報を伝達するための仕組みをいう。

（4）個人情報　個人情報の保護に関する法律（以下「個人情報保護法」という。）で定義されている個人情報をいう。

（5）情報資産　　以下の各号を情報資産という。

ア　情報システムで取り扱う全ての情報

イ　アに関する情報が記録された紙等の有体物及び記録媒体

（6）外部ネットワーク　当院の外部に存在する情報ネットワークをいう。

（7）職員等　当院に勤務する者（雇用形態や職位等を問わない。）で、情報システムの使用を許可された者をいう。

（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。

ア　機密性　情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保すること。

イ　完全性　情報資産が破壊、改ざん又は消去されていない状態を確保すること。

ウ　可用性　情報資産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、情報資産にアクセスできる状態を確保すること。

（情報セキュリティ対策の文書体系）

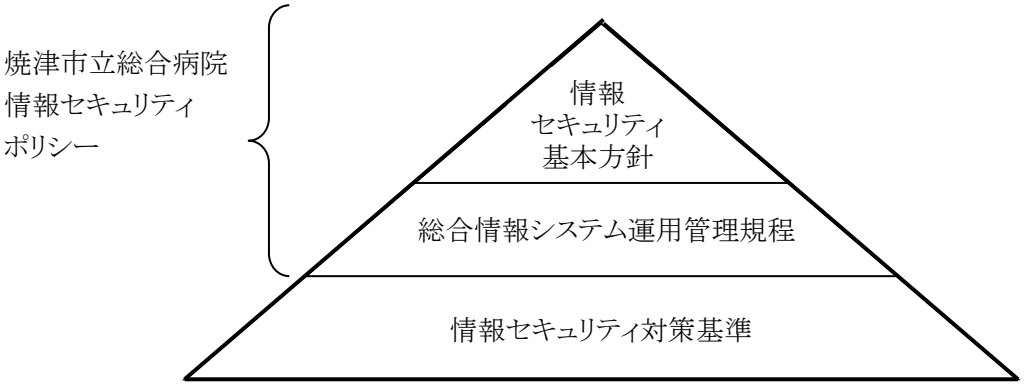
3　当院の情報セキュリティ対策は、次に掲げるものから構成するものとする。

（1）焼津市立総合病院　情報セキュリティ基本方針
　　情報セキュリティ対策に関する統一的かつ基本的な方針について定める。

（2）焼津市立総合病院　総合情報システム運用管理規程
　　基本方針を実行に移すために必要な対策を定める。

（3）焼津市立総合病院　情報セキュリティ対策基準
　　情報セキュリティポリシーに定める対策等の実施について必要な事項を定める。

（4）当院における情報セキュリティ対策の文書体系は以下のとおりとする。



（情報システム運用の基本原則）

4　当院の情報システムは、次に掲げる基本原則により運用する。

（1）法的に保存義務のある文書等の電子保存の要件として、真正性、見読性及び保存性を確保すること。

（2）電磁的に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認できる措置を講じ、かつ、当該電磁的記録の作成にかかる責任の所在を明らかにすること。

（3）情報システムの使用にあたっては、個人情報を保護し、守秘義務を守ること。

（4）情報システムへのコンピュータウィルス等の侵入及び外部からの不正アクセスに対して必要な措置を講ずること。

（5）情報システムは、原則として、管理者の許可を得ていないソフトウェアのインストール及び私物USB メモリなどの外部記憶媒体の接続を禁止すること。

（情報資産の分類）

5　情報セキュリティ対策の対象となる情報資産について、次のとおりの重要度のレベルを設定する。

重要度	具体的な判断基準
レベル3	医療情報を含む情報資産
レベル2	レベル3以外の病院の業務に関わる情報
レベル1	上記以外の情報資産で公開・開示されても支障がないもの

(通常運用責任と事後責任)
6　情報システムの運用にあたっては、情報セキュリティポリシーに従い適正な管理を行うとともに、定期的に運用管理全般の見直しを行わなければならない。また、何らかの不都合な事態が生じた場合は、その事実を速やかに公表し、再発防止策を含む適切な対策を速やかに講じなければならない。

(組織体制)
7　情報システムの適正な運用を図るため、次の職及び担当者を置く。
(1) 情報セキュリティ管理者
　当院の情報セキュリティに関する最終決定権限及び責任を有する者を情報セキュリティ責任者とし、病院事業管理者をもって充てる。
(2) 情報システム管理者
　情報セキュリティ責任者を補助し、情報システムの開発、設定の変更、運用、更新等を行う権限及び責任を有する者を情報システム管理者(以下「システム管理者」という。)とし、病院長をもって充てる。
(3) 医療情報システム安全管理責任者
　システム管理者を補助し、この既定に規定する情報セキュリティに係る統括を行う者を情報システム安全管理責任者とし、事務部長をもって充てる。
(4) 情報システム運用管理者
　システム管理者を補助し、情報システムに係る実務を行う者を情報システム運用管理者(以下「運用管理者」という。)とし、情報システムの運用管理を事務分掌とする所属長をもって充てる。
(5) 情報システム担当者
　情報システム担当者は、情報システムの運用管理を事務分掌とする担当者が行う。
(6) サブシステム管理者
　部門システムの管理を行う者をサブシステム管理者とし、サブシステムを所管する所属の長を充てる。
(7) サブシステム担当者
　サブシステム担当者は、サブシステムの運用管理を担当する者を正、副各1名サブシステム担当者として選任する。
(8) 情報セキュリティ監査責任者
　情報セキュリティ並びに電子情報の真正性、見読性の確保及び保存に関し、適時適切に監査を実施し、その結果を情報セキュリティ責任者に報告する権限及び責任を有する者を情報セキュリティ監査責任者とし、情報セキュリティ管理者が指名する。

(情報資産の管理及び保管)
8　情報システムで取り扱う情報については下記のとおり管理及び保管する
(1) 情報資産は、取得から利用・保管・廃棄までの流れに従い適切に管理しなければならない。
(2) 情報資産の保管期間は、それぞれ該当する法令に定める保管期間を基本する。
(3) 情報システムへのアクセスログについては、その記録を5年間保管しなければならない。

(使用者識別)
9　情報システムの使用にあたっては、職員等を管理し、そのアクセス権限を設定し、不正な利用を防止するための措置を講じなければならない。

(標準規格等)
10　情報システムで使用する規格は、ガイドラインに掲載されている標準規格及び一般社団法人保健医療福祉情報システム工業会が掲載している医療情報システム標準化関連用語に可能な限り準拠するものとし、その改訂状況を常に確認して、整合性を維持するよう努めなければならない。

(教育)
11　職員等は、情報セキュリティの重要性と、個人情報の適切な取扱い及び安全管理について、定期的に意識及び技術の向上を目的とした教育研修を継続的に受けなければならない。

(監査)
12　情報システムの適正な運用を維持するために、定期的に内部監査を実施し、その結果を情報システム管理者に報告するものとする。この場合において、問題点の指摘等があった場合は、直ちに必要な措置を講じなければならない。

(改訂)
13　この基本方針を改訂する場合は、情報システム委員会の承認を受けなければならない。

(雑則)
14　従前の情報セキュリティポリシーの運用は、令和5年3月31日をもって休止する。

附　則
　この規程は、令和　5　年　4　月　1　日から施行する。
　この規程は、令和　6　年　4　月　1　日から施行する。