# 地方独立行政法人東京都健康長寿医療センター

# 情報セキュリティ基本方針

２５健経第４３５号
制定　平成２６年３月７日
２６健経第２３１号
改正　平成２６年１０月８日
２６健経第４９７号
改正　平成２７年４月１日
元健経第１１１号
改正　令和元年１０月１日
２健戦第６２号
改正　令和３年４月１日
７健経第５３１号
改正　令和８年３月２３日

## 目次

## 1 目的

本基本方針は、地方独立行政法人東京都健康長寿医療センター（以下「センター」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、センターが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ことを目的とする。

## 2 定義

(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(ハードウエア及びソフトウエア）をいう。

(2) 情報システム等

センターの運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

(3) 医療情報システム

センターの事業のうち、病院の業務を行ううえで、法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存のために使用される機器、ソフトウェア及び運用に必要な仕組み全般をいう。

(4) 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。

(5) 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。

(6) 職員等

常勤職員、非常勤職員、臨時職員、派遣職員、実習生、協力研究員、教育研究等を受ける学生、その他セキュリティ責任者が利用を許可した者をいう。

(7) 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。

(8) 完全性

情報が破壊、改ざん又は消去がされていない状態を確保することをいう。

(9) 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。

(10) 業務用端末

職員等に対し、業務上利用することが許可されたパソコン、モバイル端末等をいう。

(11) 業務用外部記録媒体

職員等に対し、業務上利用することが許可されたＵＳＢメモリや光ディスク等の外部記録媒体をいう。

(12) 管理区域

情報システム室（ネットワークの基幹機器及び重要な情報システム等に係る機器等を設置し、専ら当該機器等の管理及び運用を行うための部屋）及び業務用外部記録媒体の保管に使用する保管庫を設置している区域をいう。

(13) 準管理区域

センター内執務室用フロア内に設定され、情報システムの機器類の設置、管理運用、保管等を行う専用の区域をいう。

(14) ＳＭＳ（ソーシャルメディアサービス）

インターネット上で展開される情報メディアであって、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアである、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等のサービスをいう。

(15) クラウドサービス

従来は手元のコンピュータに導入して利用していたソフトウェアやデータ、それらを提供するための技術基盤等を、インターネットなどのネットワークを通じて、利用できるサービスをいう。

## 3 対象とする脅威

情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施するほか、新たな脅威の発生に備え、最新の脅威動向を確認するなど、適切に対応する。

(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及び部外者の侵入等の意図的な要因による、センターが保有する情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取のほか、内部管理の欠陥など職員等による不正行為等

(2) センターが保有す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、メンテナンスの不備、内部・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・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・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) 組織の適用範囲

本基本方針が適用される範囲は、センター組織図に規定する経営企画局、病院、研究所とする。

(2) 情報資産の適用範囲

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 情報システム等

イ 個人情報のほか、情報システム等で取り扱うデータ

ウ 情報システム等に関するシステム設計書、ネットワーク図等のシステム関連文書

(3) 対象とする情報システム等

本基本方針が対象とする情報システム等は、次のとおりとする。なお、医療機器又は研究機器付属の端末等についても、対象とする情報システム等に準じて扱うこととする。

ア　経営企画局が所管する情報システム

・財務会計及び人事給与システム

・事務系ＬＡＮ等

イ　病院が所管する情報システム

・電子カルテシステム及び部門システム

・診療系ＬＡＮ等

ウ　研究所が所管する情報システム

・研究所ＬＡＮ等

## 5 所管局との連携

必要な情報セキュリティ対策の実施にあたっては、当法人の設立団体である東京都のサイバーセキュリティポリシーに従い、所管局の東京都福祉保健局の指導を受ける。

## 6 職員等の遵守義務

職員等は、センターが保有する情報資産に対する脅威への対応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等を遵守しなければならない。

## 7 情報セキュリティ対策

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講じる。

(1) 組織体制

センターの情報資産について、情報セキュリティ対策を推進する組織体制を確立す

る。また、情報セキュリティ対策に関し、各職層における管理者等の役割、権限及び責任を明確にする。

(2) 情報資産の分類と管理

センター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資産の管理及び取り扱い方法等について具体的に定め、実効的な情報セキュリティ対策を行う。

(3) 物理的セキュリティ対策

サーバ、管理区域、準管理区域、通信回線等及び業務用端末等の管理について、物理的な対策を講じる。

(4) 人的セキュリティ対策

情報セキュリティに関し、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。

(5) 技術的セキュリティ対策

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。

(6) 運用面での対策

情報システムの監視及び情報セキュリティポリシー等の遵守状況の確認のほか、(8)の外部サービスを利用する際の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で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、緊急時対応体制を整備する。

(7) 外部サービスの利用に係る対策

センターの業務を受託する事業者（当該事業者から派遣されている者を含む。）（以下「外部委託事業者等」という。）に当該業務を行わせる場合には、センターが定める情報セキュリティ要件等、セキュリティ対策上、遵守させるべき事項を、外部委託事業者等の選定要件として提示する。

さらに、契約、協定等（以下「契約等」という。）の締結時等に、外部委託事業者等においてもセンターが定めるセキュリティポリシーと同等のセキュリティ対策が確保されていることを、契約等事項に明記し、又は、別途、書面による提出を求める等の措置を講じる。

なお、約款による外部サービスを利用する場合には、当該利用に係る規定等を整備し、対策を講じる。

また、ＳＭＳを利用する場合には、ＳＭＳに関する運用手順を定めるとともに、ＳＭＳで発信できる情報を規定し、利用するＳＭＳごとの責任者を定める。

クラウドサービスの利用に当たっても、クラウドサービスの利用に関する手順等を

定めるとともに、必要に応じて、当該利用の対象とする情報について定める等、規定を整備すること。

## ８ リスク評価の実施及び年度計画の策定

情報セキュリティに係る内部環境及び外部環境の変化を踏まえ、センターが保有する情報資産の情報セキュリティ上のリスクを評価し、リスク対応方針を策定する。

また、策定したリスク対応方針に基づき、リスク対応計画を毎年度策定する。

## ９ 自己点検及び情報セキュリティに関する監査の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的に実施の可否を判断し、必要に応じて、自己点検及び情報セキュリティに関する監査を実施する。

## 10 情報セキュリティポリシーの見直し

自己点検及び情報セキュリティに関する監査の結果、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、又は、情報セキュリティに関する状況の変化に対応するため、新たに対策が必要となった場合には、情報セキュリティポリシーを見直す。

## 11 情報セキュリティ対策基準の策定

７から 10 までに示す対策等を実施するため、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を経営企画局、病院と、研究所に分けて策定する。

なお、当該対策基準は、センターにおける情報セキュリティ対策の基準を定めるものであり、公にすることにより、センターの事業運営に重大な支障を及ぼすおそれがあることから、当該対策基準については非公開とする。

## 12 情報セキュリティ実施手順の策定

11 に定める情報セキュリティ対策基準を踏まえ、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ものとする。

なお、当該実施手順は、関連する情報システム等の情報セキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務の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。

## 13 医療情報システム運用管理規程

11 に定める情報セキュリティ対策基準を踏まえ、病院の業務を行ううえで必要な、医療情報システム固有の情報セキュリティ対策を定めた医療情報システム運用管理規程を策定するものとする。

なお、当該運用管理規程は、医療情報システム固有の情報セキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務の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。

**附則**

附則（平成２５健経第４３５号）
この規程は、平成２６年3月７日から施行する。
附則（平成２６健経第２３１号）
この規程は、平成２６年１０月８日から施行する。
附則（平成２６健経第４９７号）
この規程は、平成２７年４月１日から施行する。
附則（令和元健経第１１１号）
この規程は、令和元年１０月１日から施行する。
附則（令和２健戦第６２号）
この規程は、令和３年４月１日から施行する。
附則（令和７健経第５３１号）
この規程は、令和８年４月１日から施行する。