静岡県立静岡がんセンター情報セキュリティ基本方針

第１　目　的

静岡県立静岡がんセンター（以下「がんセンター」という）の各情報システムが取り扱う情報には、がんセンター利用者の個人情報等の個人情報のみならずがんセンター運営上重要な情報など、部外者に漏洩等した場合には極めて重大な結果を招く恐れのある情報が多数含まれている。

したがって、これらの情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、がんセンター利用者の個人情報等の個人情報を守るために、また、がんセンターの安定的な運営のために必要である。このことががんセンター利用者からの信頼の維持向上に寄与するものである。

そのため、がんセンターが保有する情報資産の機密性、完全性及び可用性(注)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「静岡県立静岡がんセンター情報セキュリティポリシー」を定めることとした。

情報セキュリティポリシーは、がんセンターが保有する情報資産等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し、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)の２階層に分けて策定する。

このうち、情報セキュリティ基本方針（以下「基本方針」という）については、がんセンターの情報セキュリティ対策の統一的かつ基本的な事項を定める。

第２　対象範囲

この基本方針が対象とする範囲は、がんセンター全体とする。

ただし、知事部局が管理運用する情報システムを利用する業務並びに研究所の共同研究者が独自に設置したネットワーク、情報システム及び情報資産は対象から除く。

第３　定　義

１　ネットワーク

電子計算機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）及び記録媒体で構成され、処理を行う仕組みをいう。電子カルテシステム及び各部門システムを繋ぐ内部ネットワークとインターネットに接続された外部ネットワークに区別される。

２　情報システム

電子計算機器（ネットワーク、ハードウエア及びソフトウエア）及び記録媒体で構成され、業務処理を行う仕組みをいう。電子カルテシステム及び各部門システムをすべて含む病院業務及び研究利用のコンピュータシステム全体をいう。

３　情報資産

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。

なお、情報資産には情報システムに入力するための紙媒体等及び情報システムから出力された紙媒体等の情報も含む。

４　情報セキュリティ

ネットワーク、情報システム及び情報資産の機密性、完全性及び可用性を維持することをいう。

第４　職員等及び外部委託事業者の義務

がんセンターが保有する情報資産に関する業務に携わる全ての職員等及び外部委託事業者は、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、業務の遂行に当たり情報セキュリティポリシー（実施手順を含む）を遵守する義務を負うものとする。

なお、職員等が故意または重大な過失により個人情報等を漏洩等した場合は、関係法規により厳正に対処する。

第５　情報セキュリティ管理体制

がん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・管理するための体制を確立するものとする。

第６　情報資産の分類

情報資産をその内容に応じて分類し、その重要性に応じた情報セキュリティ対策を行う。

第７　情報資産への脅威

ネットワーク、情報システム及び情報資産に対して、想定される主な脅威は以下のとおりである。

１　外部からの脅威

・部外者の不正侵入
・不正アクセス及びコンピュータウイルス等の侵入
・地震、落雷、火災等の災害
・運搬中の事故・盗難等

２　内部からの脅威

・認証情報（ユーザーＩＤ、パスワード等）等の不適切な管理
・故意又は過失による不正アクセス
・機器の不正接続
・機器、情報資産の不正持ち出し
・端末画面の覗き見

第８　情報セキュリティ対策

前項で示した脅威から情報資産を保護するために、次の情報セキュリティ対策を講ずる。

１　物理的セキュリティ対策

部外者及び職員等による情報システム等を設置する施設への不正な立入り、情報資産の持出し・損傷・妨害の事故及び災害等から情報資産を保護するために必要な物理的対策を講ずる。

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及び遵守すべき事項を定め、職員等に情報セキュリティポリシーの内容を周知徹底するとともに、十分な教育及び啓発が講じられるように必要な対策を講ずる。

３　技術的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アクセス、コンピュータウイル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的な対策を講ずる。

また、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシー遵守の確認等の運用面における情報資産の保護等に必要な対策を講ずる。

なお、緊急事態が発生した際に迅速に対応するための危機管理対策を講ずる。

第９　情報セキュリティ対策基準の策定

情報セキュリティ対策を講ずるに当たり、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ため、この基本方針に基づき情報セキュリティ対策を実施する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（以下「対策基準」という）」を策定する。

第 10　情報セキュリティ実施手順の策定

対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する対策基準の基本的な要件に基づき、各部門の長等が管理する情報資産の「情報セキュリティ実施手順（以下「実施手順」という）」を策定する。

なお、対策基準及び実施手順は、公にすることによりがんセンターの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。

第 11　情報セキュリティ監査の実施

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。

第 12　評価及び見直しの実施

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環境の変化に対応するため、必要に応じて情報セキュリティポリシーの見直しを実施する。

＜参　考＞

（注）：国際標準化機構（ＩＳＯ）が定めるもの（IS07498-2：1989）

・**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。

・情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	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
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		情報セキュリティ対策基準に基づいたネットワーク及び情報システムごとに定める具体的な実施手順

＝＝＝＝＝＝＝＝＝＝＝＝

作成日：2006 年 7 月 3 日

確認日：2023 年 9 月 25 日