情報セキュリティポリシー（要綱）

神奈川県立病院機構では、情報セキュリティを確保するための基本的な方針や詳細なルールを「情報セキュリティポリシー（要綱）」（令和８年４月１日施行）として策定しております。

「情報セキュリティポリシー（要綱）」の構成について

「情報セキュリティポリシー（要綱）」は、次の２つの階層で構成されています。

- 「第１章　情報セキュリティ基本方針」

神奈川県立病院機構の情報資産を保護するため、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を示すもの。

- 「第２章　情報セキュリティ対策基準」

基本方針に定められた情報セキュリティを確保するために遵守すべき行為や判断等の共通の基準を示すもの。

「情報セキュリティポリシー（要綱）」の公開について

「情報セキュリティポリシー（要綱）」のうち、「第１章情報セキュリティ基本方針」を公開しております。（次ページ参照）

情報セキュリティポリシー（要綱）

地方独立行政法人神奈川県立病院機構

本部事務局デジタル戦略部

本要綱の「第２章情報セキュリティ対策基準」については、情報セキュリティの確保に支障を及ぼす恐れのある情報を含むことから記載しておりません。

目　次

序　情報セキュリティポリシーの構成 4
第１章　情報セキュリティ基本方針 5
１　目的 5
２　定義 5
３　情報セキュリティポリシーの位置付けと職員等の義務 7
４　情報セキュリティ管理体制 7
５　情報の分類及び分類ごとの情報セキュリティ対策 7
６　情報資産への脅威 7
７　情報セキュリティ対策 8
（１）　情報システム全体の強靭性の向上 8
（２）　物理的対策 8
（３）　人的対策 8
（４）　技術的対策 8
（５）　運用における対策 8
８　情報セキュリティ対策基準の策定 8
９　情報セキュリティ実施手順の策定 8
10　情報セキュリティ監査の実施 9
11　評価及び見直しの実施 9

情報セキュリティポリシー（要綱）

序　情報セキュリティポリシーの構成

情報セキュリティポリシーとは、地方独立行政法人神奈川県立病院機構（以下「法人」という。）が所管する情報資産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をいう。このことから、この規範は安定的であることが要請される。一方で、この規範には技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化に柔軟に対応することも要請されるところであり、生成ＡＩサービスの利用方法等についても柔軟に対応することも必要である。

また、情報セキュリティポリシーは、全ての職員等が、法人が所管する情報資産に関する業務に従事する場合に限らず、コンピュータを使用して業務外で連絡調整等を行う場合や自己研鑽の研究活動等でコンピュータを使用して法人の情報資産を取り扱う場合においても遵守すべき規範である。したがって、この規範に係る情報セキュリティへの取組は、全ての職員等に浸透、普及、定着させる必要がある。

以上のことから、情報セキュリティポリシーを一定の普遍性を備えた部分である「情報セキュリティ基本方針」と情報セキュリティを取り巻く状況の変化に依存する部分である「情報セキュリティ対策基準」とにより構成することとし、情報セキュリティポリシーに基づく具体的な実施手順については、「情報セキュリティ実施手順」として別に策定することとした。

なお、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の構成は、以下の表のとおりである。

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の構成

分類	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（第１章）	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（第２章）	情報セキュリティ基本方針に基づき定める情報システム等に共通の情報セキュリティ対策の基準（基本的な要件）
情報セキュリティ実施手順	情報セキュリティポリシーに基づいた情報システム等ごとに定める具体的な実施手順	

第１章　情報セキュリティ基本方針

１　目的

法人の情報システム等が取り扱う情報には、患者等の個人情報のみならず法人運営上重要な情報など、外部に漏えい等した場合に重大な結果を招く情報が含まれている。

したがって、これらの情報及び当該情報を取り扱う情報システム等を様々な脅威から防御することは、患者等の財産、プライバシー等を守るためにも、また、業務の安定的な運営のためにも必要不可欠であり、さらに法人に対する患者等からの信頼の維持向上に寄与するためにも必要不可欠である。

情報セキュリティ基本方針は、法人が所管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、法人が実施する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を定めることを目的としている。

２　定義

この要綱において、次に掲げる用語の意義は、以下の各号に定めるところによる。

（１）　コンピュータ　サーバ、パーソナルコンピュータ及びこれらに類するもの並びにこれらの運営に必要な機器をいう。

（２）　ネットワーク　コンピュータを接続してデータ通信するための情報通信網並びにこの運営に必要な設備及び機器をいう。

（３）　情報システム　コンピュータ及びネットワークを用いて業務処理を行うために必要な体系をいう。

（４）　データ　コンピュータ又は記録媒体に記録されている電磁的記録をいう。

（５）　情報資産　コンピュータ、ネットワーク、情報システム及びこれらが取り扱う情報（当該情報を印刷した文書を含む。）をいう。

（６）　Infrastructure Information System（以下、基盤情報システムと称する。）
事務情報、経営管理情報及び医療情報等を扱う情報システムが稼働するために必要なインフラ機能を提供するコンピュータ、ネットワーク等をいう。

（７）　Administrative Information System（以下、経営管理情報システムと称する。）
人事給与システムや財務会計システム等の経営管理情報を扱うアプリケーション、ソフトウエアやデータベース及びこれらに類するもの並びにこれらの運用に必要なサービスをいう。

（８）　Hospital Information System（以下、医療情報システムと称する。）
医療情報を扱うアプリケーション、ソフトウエアやデータベース及びこれらに類するもの並びにこれらの運用に必要なサービスをいう。

（９）　記録媒体　データを記録するための媒体をいう。例えば、磁気テープ、フロッピー

ディスク、ハードディスク、ＵＳＢメモリ、ＣＤ－Ｒ、ＤＶＤ－Ｒ、ボイスレコーダ、デジタルカメラ、ＳＤメモリカードなど。

(10) IoT 機器を含む特定用途機器

テレビ会議システム、ネットワークカメラシステム等の特定用途に使用される情報システム特有の構成要素であって、ネットワークに接続されている又は電磁的記録媒体を内蔵しているものをいう。

(11) 外部サービス　外部の事業者等が情報システムの一部又は全部の機能を提供するものをいう。

(12) クラウドサービス

ネットワークに接続されたコンピュータを運営する事業者等が提供する様々なサービス・機能を利用する形態をいう。

(13) ソーシャルメディア

インターネット上において不特定多数の者が情報を交換・共有する仕組みをいう。例えば、ブログ、ソーシャルネットワーキングサービス、動画共有サイトなど。

(14) ソーシャルメディアサービス

インターネット上において不特定多数の者が情報を交換・共有する仕組みを提供するサービスをいう。

(15) 機密性　情報にアクセスすることを認められた者が、情報にアクセスできる状態を確保することをいう。

(16) 完全性　情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(17) 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。

(18) 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。

(19) 情報セキュリティ対策

情報セキュリティを確保するための対策をいう。

(20) 情報セキュリティインシデント

望ましくない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

(21) 情報システム等

コンピュータ、ネットワーク及び情報システムをいう。

(22) 情報システム管理者等

基盤情報システム管理者、経営管理情報システム管理者及び医療情報システム管理者をいう。

(23) デジタル戦略部長

地方独立行政法人神奈川県立病院機構組織規程（以下「組織規程」という。）第７条第１項に規定する部長をいう。

(24)　総長等　　組織規程第 15 条第２項に規定する総長等をいう。

(25)　職員等　　法人が雇用する職員、公益的法人等への一般職の地方公務員の派遣等に関する法律（平成 12 年法律第 50 号）に基づき神奈川県から派遣された職員及び労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和 60 年法律第 88 号）（以下「労働者派遣法」という。）第２条第２号に規定する派遣労働者をいう。

(26)　患者等　　地方独立行政法人神奈川県立病院機構定款第 17 条に規定する病院の患者及びその家族等の関係者をいう。

(27)　庁舎　　組織規程第３条に規定する本部の事務所及び同規程第４条に規定する病院の施設をいう。

3　情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、法人が所管する情報資産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指針となるものである。

したがって、全ての職員等は、情報セキュリティの重要性について共通の認識を持つとともに、法人が所管する情報資産に関する業務に従事する場合に限らず、コンピュータを使用して業務外で連絡調整等を行う場合や自己研鑽の研究活動等でコンピュータを使用して法人の情報資産を取り扱う場合においても、情報セキュリティポリシーを遵守しなければならない。

4　情報セキュリティ管理体制

法人は、法人が所管する情報資産について、情報セキュリティ対策を推進及び管理するための体制を確立するものとする。

5　情報の分類及び分類ごとの情報セキュリティ対策

法人は、情報をその対策重要度に応じて分類し、当該分類に対応した情報セキュリティ対策を行うものとする。

6　情報資産への脅威

情報資産に対する脅威の発生度合いや発生した場合の影響を考慮すると、特に情報セキュリティ対策を講ずべき脅威は以下のとおりである。

（１）　部外者による故意の不正アクセス、ウイルス攻撃、サービス不能攻撃等の意図的な要因による情報又はプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難等

（２）　職員等及び委託事業者（再委託先等の事業者を含む。以下同じ。）の従業員による誤操作、故意の不正アクセス又は不正操作による情報若しくはプログラムの持出し、盗聴、改ざん及び消去、機器及び媒体の盗難、正規の手続きによらない端末の接続による情報漏えい等

（３）　地震、落雷、火災等の災害及び事故、故障等による業務の停止

（４）　大規模・広範囲にわたる疾病による職員等の要員不足に伴う情報システム運用の機能不全

（５） 電力供給の途絶、通信の途絶、水道供給等のインフラの障害からの波及等

7　情報セキュリティ対策

法人は、上記６で示した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ものとする。

（１） 情報システム全体の強靭性の向上

ア　医療情報システム及び医療情報システムが稼働する基盤情報システムについては、厚生労働省策定の「医療情報システムの安全管理に関するガイドライン」の最新版に従った対策を実施する。

イ　医療情報システムが稼働する基盤情報システムを除く基盤情報システム及び経営管理情報システムは、可能な限り法人が契約するデータセンター又はクラウドサービスに集約する。

ウ　データセンター又はクラウドサービスを利用する場合の業者選定に際しては、以下の（２）～（５）に掲げる情報セキュリティの対策に係る事業者における充足の程度を考慮する。

（２） 物理的対策

情報システム等を設置する執務室等への不正な立入り及び情報資産への損傷、妨害等から保護するための物理的な対策

（３） 人的対策

情報セキュリティに関する役割等を定め、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等、十分な教育及び啓発を講じるための対策

（４） 技術的対策

情報資産を不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策

（５） 運用における対策

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、委託を行う際の情報セキュリティの確保等の運用面の対策及び緊急事態が発生した際に迅速な対応を可能とするための危機管理対策

8　情報セキュリティ対策基準の策定

法人が所管する情報資産について、上記７の情報セキュリティ対策を講じるに当たっては、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。このため、情報セキュリティ対策を行う上で必要となる情報システム等に共通の情報セキュリティ対策の基準（基本的な要件）を明記した情報セキュリティ対策基準を第２章に定めるものとする。

9　情報セキュリティ実施手順の策定

情報セキュリティ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、個々の情報資産の情報セキュリティ対策の手順等をそれぞれ定めていく必要がある。このため、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情報セキュリティ対策基準の基本的な要件に基づき、情報システム管理者等は、所管する情報資産の情報セキュリティ実施手順を策定する

ものとする。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより情報セキュリティの確保に重大な支障を及ぼすおそれがあるため取扱いに注意するものとする。

10　情報セキュリティ監査の実施

法人は、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、年１回監査を実施するものとする。

11　評価及び見直しの実施

法人は、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行うとともに、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に、情報セキュリティポリシーの見直しを実施するものとする。