地方独立行政法人大阪府立病院機構情報セキュリティ確保に関する規程

制定　令和６年４月１日規程第５２４号
改正　令和８年４月１日規程第５９５号

（目的）

第１条　この規程は、地方独立行政法人大阪府立病院機構業務方法書第 13 条に基づき、地方独立行政法人大阪府立病院機構（以下「法人」という。）における情報セキュリティ確保に必要な事項を定め、情報漏えいの防止や、情報資産を脅威から守り、情報システムを安全に運用するために必要なセキュリティ対策を図ることを目的とする。

（定義）

第２条　この規程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) アクセスログ

情報システムやソフトウェア等に対して、人間や外部のシステムからの操作や要求、処理等を記録したものをいう。セキュリティ管理やトラブルシューティング、監査などの目的で利用される。

(2) サイバー攻撃

情報システムやネットワークに悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うことをいう。

(3) 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（ハードウェア及びソフトウェア）をいう。

(4) ネットワーク機器

ルータ、スイッチ、HUB 等の情報通信ネットワークを構築する際に用いられる機器をいう。

(5) 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。

(6) 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。

(7) 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。

(8) 情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

(9) 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。

（10）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。
（11）不正アクセス
　　利用する権限を与えられていないコンピュータ/システムに対して、不正に接続しようとすることをいう。実際にそのコンピュータ/システムに侵入したり、利用したりすることを不正アクセスに含むこともある。

（対象とする脅威）
第３条　情報資産に対する脅威として、以下の脅威を想定し、セキュリティ対策を実施する。
（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や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
（2） 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）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

（適応範囲）
第４条　適応範囲は、法人が運用する情報資産を対象とする。情報資産とは、法人が保有又は運用管理するデータ及び情報システム、ネットワーク機器のことをいう。

（情報セキュリティ管理体制）
第５条 第３条に掲げる脅威から情報資産を保護するために、情報セキュリティマネジメントの計画・実行・確認・改善といった一連のサイクルを適切に管理・運用する体制を構築する。
２ 前項の実効性の充実に向け、情報セキュリティ等委員会（以下「委員会」という。）を設置し、法人の情報セキュリティ確保及びその他関連する事項について検討するものとする。
３ 委員会に関する細部事項は別に定める。

（最高情報セキュリティ責任者）
第６条 法人に、最高情報セキュリティ責任者を置き、理事長をもって充てる。
２ 最高情報セキュリティ責任者は、情報資産の管理及び情報セキュリティ対策の最終決定権限及び責任を負う。

（統括情報セキュリティ責任者）
第７条 法人に、統括情報セキュリティ責任者を置き、本部事務局長をもって充てる。
２ 統括情報セキュリティ責任者は、最高情報セキュリティ責任者の補佐、情報セキュリティに関する事務を統括する。

（情報セキュリティ責任者）
第８条 本部事務局及び病院に、情報セキュリティ責任者を置き、本部事務局においては本部事

務局長を、病院においては総長又は院長をもって充てる。
2 情報セキュリティ責任者は、本部事務局又は当該病院の情報セキュリティ対策に関する権限及び責任を負う。

（情報セキュリティ管理者）
第９条 本部事務局及び病院に、所管するシステムごとに情報セキュリティ管理者を置くものとし、情報セキュリティ責任者が任命する。なお、医療情報を扱うネットワーク、システム及びデータに関しては、医療情報システム安全管理責任者をもって充てる。
2 情報セキュリティ管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う。

（情報セキュリティ担当者）
第 10 条 本部事務局及び病院に、情報セキュリティ担当者を置くものとし、情報セキュリティ責任者が任命する。
2 情報セキュリティ担当者は、所管する情報システムにおける情報セキュリティ対策を実施する。

（物理的セキュリティ）
第 11 条 サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（人的セキュリティ）
第 12 条 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、情報セキュリティの意識向上を図るために、職員に対し、情報セキュリティに関する教育・訓練を定期的に行い、情報リテラシーの向上に努める等の人的な対策を講じる。

（技術的セキュリティ）
第 13 条 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。

（情報セキュリティに関する要領等の整備）
第 14 条　情報システムのぜい弱性対策やアクセスログの定期点検などの情報セキュリティの確保を実現するため、本規程に準じるセキュリティに関する要領等を整備し、全ての情報資産に適応するものとする。

（法令などの遵守）
第 15 条　情報セキュリティに関する法令、契約及びガイドライン等を遵守するものとする。

（業務継続性の確保）

第 16 条　情報資産の完全性と可用性を維持するため、保有している情報に対して適切なバックアップ技術を適用するものとする。
２　事件・事故、情報処理システムの重大な故障又は災害の影響なども含めた緊急事態を想定した事業継続計画を策定するとともに、その確認、維持及び再評価を行うものとする。

（違反及び事故への対応）
第 17 条　情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には、適切に対処し、再発防止に努めるものとする。

（継続的改善の実施）
第 18 条　情報セキュリティ管理体制を適正に実行・運用するとともに、情報セキュリティ管理体制の継続的な改善に努めるものとする。
２　情報セキュリティポリシーの遵守状況を検証するため、年１回、監査又は自己点検を実施する。
３　前項の監査又は自己点検の結果、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及び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になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

（雑則）
第 19 条　この規程に定めるもののほか、情報セキュリティ確保に関し必要な事項は、最高情報セキュリティ責任者が別に定める。

附 則
この規程は、令和６年４月１日から施行する。
附 則
この規程は、令和８年４月１日から施行する。