情報セキュリティ基本方針

令和８年３月３１日

竹田市立こども診療所

１．目的

診療所では、地域住民に安全で質の高い医療を提供するとともに、住民の生命と健康を守る社会的責務を担っている。診療記録や検査結果、個人番号を含む特定個人情報など、極めて高度な機密性を有する情報を日常的に取り扱っており、これらの情報は患者の権利を尊重し、信頼を確保するうえで適切に保護されなければならないものである。

一方、医療現場においては、電子カルテシステムや医療機器のネットワーク化、遠隔診療・地域医療連携の推進など、情報通信技術（ICT）の活用が急速に進展している。それに伴い、サイバー攻撃や不正アクセス、情報漏えいといった情報セキュリティ上の脅威も拡大しており、医療の安全性や診療所機能そのものに重大な影響を及ぼす可能性がある。

これらの状況を踏まえ、診療所の特性に即した情報セキュリティポリシーの策定が必要となっている。本方針は、患者情報をはじめとする診療所が保有する全ての情報資産を適切に保護し、災害時や緊急時においても医療を継続できる体制を整備することを目的とし策定するものであり、具体的な情報セキュリティ対策を記載する対策基準の拠り所とするものである。

２．定義

（１）ネットワーク　診療所において設置する端末、機器及びその他の関係機関を相互に接続するためのネットワーク及びその構成機器（ハードウエア及びソフトウエア）をいう。

（２）情報システム　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。

（３）情報資産　ネットワーク及び情報システムの開発と運用に係るすべての情報並びにネットワーク及び情報システムで取り扱うすべての情報をいい、紙等の有体物に出力された情報も含むものとする。

（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）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）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。

（７）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。

（8）内部情報系　電子カルテシステム、医事会計システム等、診療所にて利用が限定された情報システム及びその情報システムで取り扱うデータをいう。

（9）インターネット接続系　インターネットメール、ホームページ管理システム等に係るインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１０）通信経路の分割　内部情報系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（１１）無害化通信　インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着がないなど、安全が確保された通信をいう。

３．対象とする脅威

（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、無許可ソフトウエ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、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥及び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、落雷及び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よる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）医療機関等の範囲

医療機関等とは、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等。

（2）情報資産の範囲

医療に関する患者情報（個人識別情報）を含む情報資産。対象とする情報資産は、医療情報を含む文書、データ全般とし、法定の保存義務の有無を問わない。

（3）医療情報システムの範囲

対象とする医療情報システムは、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般を想定する。これには医療情報システム・サービス事業者により提供されるシステムだけでなく、医療機関等において自ら開発・構築されたシステムが含まれる。

５．職員等の遵守義務

診療所で業務に従事する職員等（以下「職員等」という。）は情報セキュリティ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を遵守しなければならない。

６．情報セキュリティ対策

上記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

情報資産について、情報セキュリティ対策を推進する診療所での組織体制を確立する。

（2）情報資産の分類と管理

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セキュリティ対策を実施する。

（3）物理的セキュリティ

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。

（4）人的セキュリティ

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

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

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、業務委託を行う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、緊急時対応計画を策定する。

（7）情報システムに関する業務委託

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。

（8）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

７．情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、必要に応じて情報セキュリティ監査及び自己点検を実施する。

８．情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、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。

９．情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、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策定する。

なお、情報セキュリティ対策基準は、具体的な情報セキュリティ対策が記載されているため、公にすることにより診療所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

本方針は、令和８年４月１日から施行する。