

情報セキュリティ基本方針

制定日：2018年2月28日 最終改定日：2026年9月1日

スペシャリスト・ドクターズ株式会社（以下、「当社」という。）は、クラウド型医療関連情報提供プラットフォームサービス（JOANR、スペシャリスト・ドクターズ等）の開発、運用、提供を通じて、患者、医師、医療機関、医療関係学会からお預かりする情報を取り扱う事業者として、情報セキュリティの確保が事業の存立基盤であることを認識し、当社の保有、運用管理する情報資産を盗難、改ざん、破壊、漏えい、不正アクセス、サービス停止等の脅威から保護するため、以下に掲げる情報セキュリティ基本方針を定め、全社一丸となって推進します。

1. 情報セキュリティの定義

情報セキュリティとは、情報の機密性、完全性及び可用性を維持することをいいます。

- ・ 機密性 … 認可された者以外が情報や資産にアクセスできない状態を確保すること。
- ・ 完全性 … 情報や資産が破壊や改ざんをされず、正確かつ完全な状態を確保すること。
- ・ 可用性 … 認可された者が必要なときに情報や資産にアクセスできる状態を確保すること。

2. 適用範囲

本基本方針は、当社が事業活動の中で取り扱うすべての情報資産（当社が保有又は運用管理する情報、データ、情報システム、クラウドサービス、ネットワーク、設備）を対象とし、当社の取締役、従業員、業務委託先要員を含む、当社の情報資産を取り扱うすべての者に適用します。

3. 情報セキュリティマネジメントシステム（ISMS）の確立と体制

当社は、JIS Q 27001:2025（ISO/IEC 27001:2022）に適合する情報セキュリティマネジメントシステムを確立、実施、維持し、継続的に改善します。トップマネジメントは情報セキュリティ管理責任者を任命し、IT責任者とともに情報セキュリティの維持・向上に取り組む体制を整えます。

4. 情報セキュリティ目的と内部規程の整備

当社は、本基本方針に基づき情報セキュリティ目的を設定し、その達成状況を監視・評価します。また、本基本方針に基づいた情報セキュリティマニュアル、ISMSマニュアル及び関連手順を整備し、個人情報だけでなく情報資産全般の取り扱いについて明確な規程を示すとともに、情報漏えい等に対して厳正に対処することを社内外に周知します。

5. リスクマネジメント

当社は、情報資産に対するリスクを定期的及び重大な変化のあった時にアセスメントし、リスク所有者の判断に基づく対応計画を策定・実施します。当社は、リスクの受容基準を定め、残留リスクをリスク所有者が承認します。

6. クラウドサービスの提供及び利用

当社はクラウドサービスプロバイダとして、また、クラウドサービスカスタマとして、JIS Q 27017（ISO/IEC 27017）に基づき、次の事項を考慮して情報セキュリティ方針を拡充します。

- ・ クラウドサービスの設計及び実装に適用する最低限の情報セキュリティ要求事項
- ・ クラウドサービスプロバイダとカスタマの間の役割及び責任の分担の明確化

- ・認可された内部関係者からのリスク
- ・マルチテナンシ及びクラウドサービスカスタマの隔離（仮想化を含む。）
- ・当社担当者によるクラウドサービスカスタマの資産へのアクセス管理
- ・管理上のアクセスに対する強い認証（多要素認証）を含むアクセス制御手順
- ・変更管理におけるクラウドサービスカスタマへの通知
- ・仮想化及びクラウド環境の構成管理・監視
- ・クラウドサービスカスタマデータへのアクセス及び保護、保管場所（日本国内リージョン）の明示
- ・クラウドサービスカスタマのアカウントのライフサイクル管理
- ・違反の通知、並びに調査及びフォレンジックを支援するための情報共有指針

7. 情報資産の保護

当社は、保有するすべての情報資産を情報資産目録で識別し、機密性、完全性、可用性の視点から重要性を分類し、情報セキュリティ体制のもとライフサイクル（取得・作成、利用、保管、送付、削除・廃棄）を通じて適切に保護します。

8. 個人情報及び医療情報の保護

当社は、個人情報の取り扱いにあたり、個人情報の保護に関する法律及び関連ガイドライン、ISO/IEC 27018（パブリッククラウドにおけるPII保護）、並びに医療情報システムの安全管理に関するガイドライン等の医療情報に関するガイドラインを遵守し、適正な取得・利用及び安全管理措置を講じ、漏えい等から保護します。個人情報の取り扱いについては、別に定めるプライバシーポリシーを公表します。

9. 情報セキュリティ教育・訓練の実施

当社は、取締役、従業員、業務委託先要員に対し、情報セキュリティへの取り組み及び意識の向上を目的として、入社時及び定期的に教育・訓練を実施します。

10. 情報セキュリティ事件・事故への対応と事業継続

当社は、情報セキュリティインシデントが発生した場合又はその予兆があった場合、速やかに報告・対応・復旧を行い、原因を分析して再発を防止します。また、重大な障害や災害が発生した場合においても情報セキュリティを維持しつつ事業を継続するための計画（ICTの備えを含む）を策定し、定期的に訓練・見直しを行います。

11. 供給者・業務委託先の管理

当社は、クラウドサービスプロバイダ、業務委託先等の供給者との間で情報セキュリティに関する要求事項を合意し、その履行状況を監視・レビューします。

12. 管理責任者及び従業員の義務

情報セキュリティ管理責任者はISMSの推進に努め、管理体制を整備し、全社的にISMSを発展させることに努めます。従業員は、ISMSで定められた規則を遵守して行動します。これに違反し、重大な問題を発生させた場合には、就業規則又は業務委託契約に基づき処分の対象とします。

13. 法令・規範及び契約上の要求事項の遵守

当社は、情報セキュリティに適用されるすべての法令、規制、ガイドライン、その他の規範及び顧客との契約上の要求事項を法令等管理台帳で識別し、遵守します。

14. 継続的改善

当社は、内部監査及びマネジメントレビューを通じてISMSの適切性、妥当性及び有効性を評価し、社会的変化、技術的变化、気候変動を含む外部環境の変化、法令等の変更に伴い、本基本方針及びISMSを定期的に見直し、継続的に改善します。

以上

スペシャリスト・ドクターズ株式会社

代表取締役 塩飽 哲生

本基本方針は、当社ホームページに掲載し、社内では入社時オリエンテーション及び年次教育で周知します。