御堂筋監査法人ニュースレター March 2026

医療機関における生成 AI の活用とガバナンスの構築

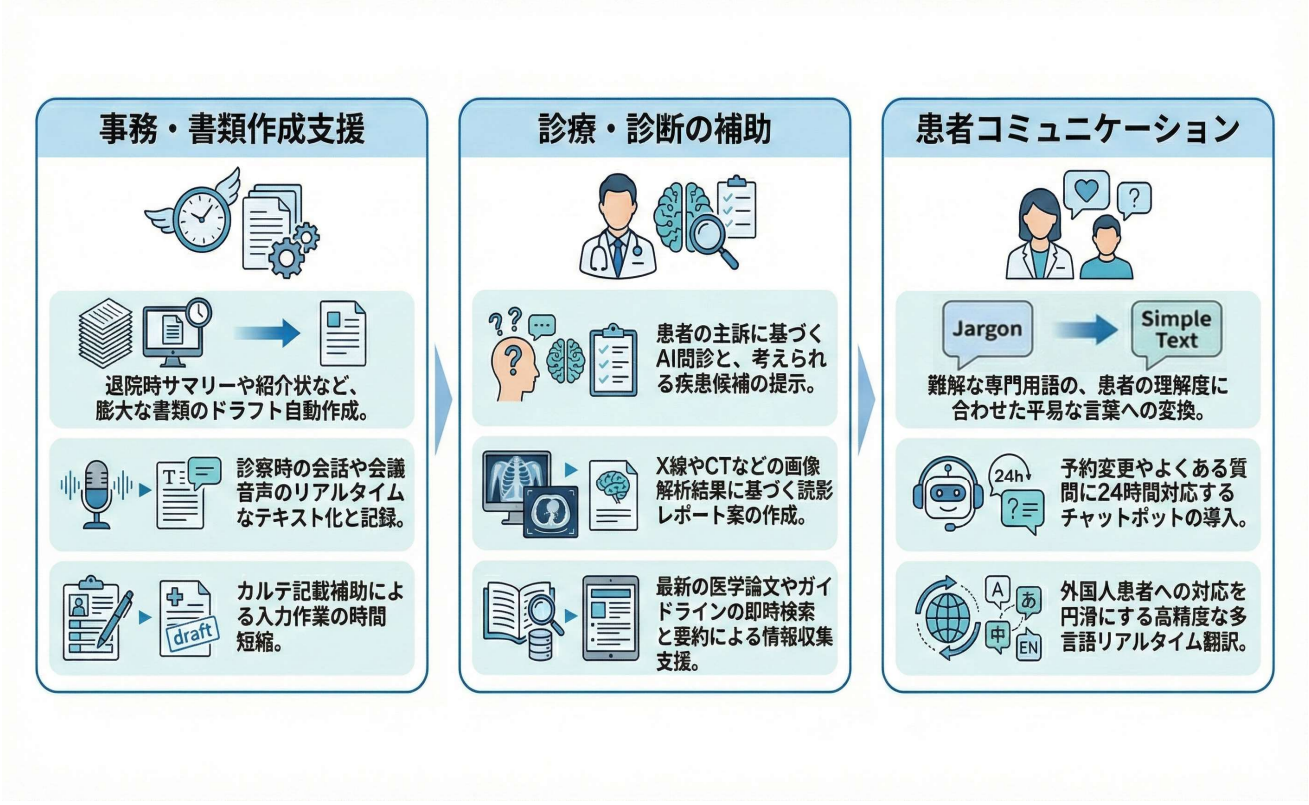
公認会計士試験合格者　寺嶋 美香
元臨床検査技師。医療従事者として病院等での勤務を経て、公認会計士試験合格後、御堂筋監査法人に入所。現在は元医療従事者としての経験を活かし、主に医療法人の監査業務を担当。

医療現場における生成 AI（LLM：大規模言語モデル等）の活用は、単なる「業務効率化」の域を超え、医療現場全体の働き方改革や診断・診療支援の核となりつつあります。一方で、高度な守秘義務と安全管理が求められる医療機関にとって、その利活用には強固なガバナンス構築が不可欠です。そこで、生成 AI の活用に伴う主なリスクと、対策の主要なポイントを整理しました。

1. 医療機関における生成 AI の主な活用シーン

生成AIは、主に「非構造化データの構造化（情報の整理と集約）」と「多種多様な文書作成の補助」において劇的な効果を発揮します。

下記に医療機関での生成AIの主な活用シーンをまとめました。



Copyright©Midosuji Audit Corporation All rights reserved.

2. 主なリスクと対策

医療機関は高度な守秘義務を負うため、リスクを正しく理解し、それに対応する仕組みをセットで構築する必要があります。

想定されるリスク	対応する対策
【情報漏洩・学習転用】 「便利だから」と無料版 AI に患者の氏名や病歴を入力してしまい、そのデータが AI の学習に取り込まれ、他者の回答に引用されてしまう。	【技術的対策と契約管理】 法人契約を締結し、入力データを学習に利用させない「非学習設定（オプトアウト）」を技術・契約の両面で徹底する。
【シャドーAI の発生】 病院が認めたツールは使い勝手が悪いため、職員が個人のスマホで未承認 AI を使い、機密情報を処理してしまう。	【利用ポリシーの策定と教育】 「利用可能な業務範囲」と「入力禁止データ」を明文化するだけでなく、職員の利便性を考慮した承認済ツールの導入とリテラシー教育を行う。
【ハルシネーション（もっともらしい嘘）】 AI が作成した退院サマリーに、実際には投与していない薬剤名が紛れ込み、そのまま紹介先へ送付されてしまう。	【人間中心の原則】 AI の回答を「下書き」と位置づけ、必ず医師等の専門家が内容を確認・修正するプロセスをワークフローに組み込む。
【責任所在の曖昧化】 AI の誤った提案を鵜呑みにして医療事故が発生した際、「AI がそう言ったから」という言い訳が通用せず、法的な責任を問われる。	【品質・供給者管理と最終判断責任の明確化】 信頼性の高いベンダーを選定するとともに、最終的な判断責任は常に人間にあることを組織全体で再認識する。

3. 安全に導入するためのステップ

医療機関が生成AIを導入する際、安全に活用できる環境を整備するためのプロセスを整理しました。

ステップ①：課題の棚卸と利用目的の明確化・組織体制の整備

まずは、組織として「何のために AI を使い、何を禁止するか」という基本方針を定めます。

- 活用範囲の特定：事務作業に限定するのか、臨床補助まで踏み込むのかを決定する。
- 組織体制の整備：AI 導入の可否やリスクを審査・管理する責任者を明確にする。

ステップ②：リスクの特定と対策・利用するサービスの信頼性評価

医療機関特有のリスクを洗い出し、許容できる範囲を定義します。

- 多角的なリスク評価：個人情報保護、ハルシネーション、法的責任等の観点からリスクを抽出する。
- 具体的な対策の検討：特定したリスクに対し、「どの機能を使い、どの設定（オプトアウト等）を強制するか」という対策をセットで検討する。
- ガイドラインとの整合性：厚生労働省の「医療情報システムの安全管理に関するガイドライン」等の最新の規制との整合性を確認する。
- 供給者管理（ベンダー評価）：AI サービス提供事業者のセキュリティ体制や医療機関の基準を満たしているかどうかを客観的に評価し選定する。

Copyright©Midosuji Audit Corporation All rights reserved.

ステップ③：利用ガイドラインと技術的対策の整備

現場の職員が迷わないための具体的なルールと、システム的な防壁を作ります。

・ 利用ポリシーの明文化：利用可能な業務範囲に加え、「入力禁止データ」を具体的に定め、シャドーAI 利用の禁止を徹底する。
・ 技術的対策・契約管理：法人契約や API 利用により、データが AI の学習に利用されない旨を契約で担保するとともに、システム上の非学習設定が正しく適用されていることを確認する。

ステップ④：リテラシー教育（職員研修）

ガバナンスはルールを作るだけでは機能しません。職員一人ひとりが正しく使いこなす「文化」を醸成します。

・ 継続的なリテラシー教育：ハルシネーションのリスクや、適切なプロンプト（指示文）の作成方法に関する研修を実施する。
・ 違反時の報告ルート：不適切な利用や情報漏洩の疑いが生じた際の報告体制を構築する。
・ 知見の共有：院内での成功・失敗事例を蓄積・共有し、組織全体の活用スキルを向上させる。

ステップ⑤：継続的モニタリングと運用改善

AI 技術の進化とリスクの変容に合わせて、体制を定期的に見直し、アップデートし続けることが不可欠です。

・ 利用状況の監査：ログを定期的に確認し、不適切な利用（個人情報の入力等）が行われていないかをモニタリングする。
・ 効果測定と外部評価：業務削減の効果を測定するとともに、必要に応じて外部専門家による客観的な評価を受け、ガバナンス体制を継続的に改善する。

【参考】

厚生労働省

・ 「医療情報システムの安全管理に関するガイドライン　第 6.0 版」（令和 5 年 5 月）
・ 「医療情報システムの安全管理に関するガイドライン　第 6.0 版 Q&A」（令和 7 年 5 月）

総務省・経済産業省

・ 「AI 事業者ガイドライン（第 1.1 版）」（令和 7 年 3 月 28 日）
・ 「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 2.0 版」（令和 7 年 3 月改定）

個人情報保護委員会

・ 「生成 AI サービスの利用に関する注意喚起等」（令和 5 年 6 月 2 日）

4. まとめ

生成 AI を適切に活用することは、現場の医療従事者が「患者と向き合う時間」を取り戻し、全ての職員が「より付加価値の高い業務」に注力するための強力な武器になります。

医療法人の経営層には、単に「利用を禁止する」のではなく、「安全に活用できるルールと環境を整備する」ことが求められます。

なお、今回取り上げたリスクや対策は、生成 AI に関連する諸問題を全て網羅しているわけではありません。著作権侵害のリスク、サイバー攻撃による情報漏洩等、検討すべき課題は多岐にわたります。医療機関は技術の進化と規制の動向を注視し、組織のフェーズに合わせた多角的なガバナンス体制を段階的に構築していくことが重要です。

以上

Copyright©Midosuji Audit Corporation All rights reserved.