医療・ヘルスケア分野における
生成 AI利用ガイドライン

2024年10月2日

非営利共益法人　医療AIプラットフォーム技術研究組合

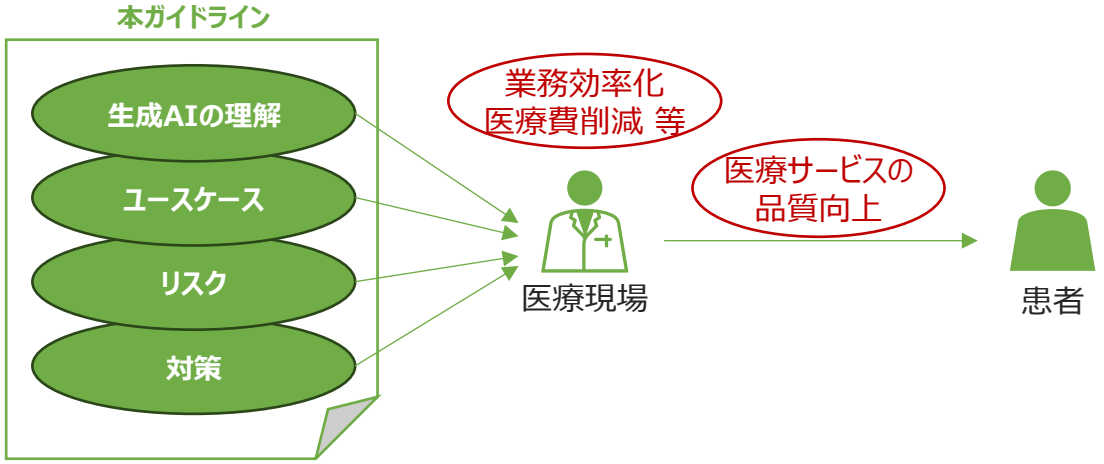
はじめに

本ガイドラインの背景

- AI （人工知能：Artificial Intelligence）技術の進展により、これまで自動化が困難とされてきた「経験や勘」等の暗黙知も学習できるようになり、高度な判断を要する作業の自動化が可能になってきています。例えば、画像解析による診断支援を行うAIも登場しています。また、最近では生成AIの登場により、多様な用途で新たなコンテンツを生成することが可能となり、幅広いシーンでの利用が期待されています。
- 一方で、医療現場では、働き方改革関連法の適用(2024年問題)や団塊世代が後期高齢者となること(2025年問題)による医療人材の不足や、高齢化のさらなる進展による医療費の増加等、様々な課題を抱えています。生成AIを利用して業務効率化や医療サービスの品質向上等を図ることは、こうした課題の有力な解決策の一つとして期待されています。

本ガイドラインの目的

- 生成AIのリスクと対策が不透明である場合、医療現場における生成AIの利用が進まないことが懸念されます。
- 本ガイドラインは、生成AIの医療現場における利用にともなうリスクと対策を示し、医療現場における生成AIの導入と利用を促進することを目的としています。

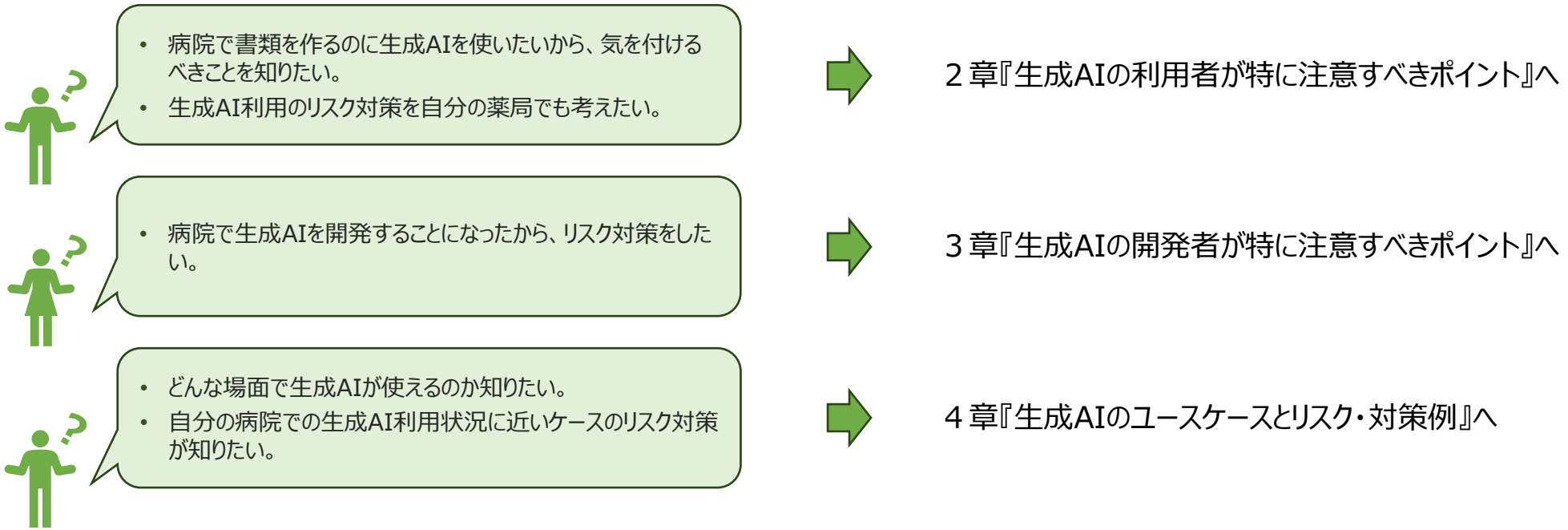


はじめに

本ガイドラインが想定する対象読者

- 本ガイドラインは、医療機関*1 ・薬局等で生成AIを利用する人、もしくは生成AIの開発に携わる人*2 を対象読者として想定しています。

目的にあわせて読みたい方は…



*1 医療機関に付属する研究機関も含みます。
*2 基盤モデルに対してファインチューニングを行う開発者(RAG等の知識データベースを外付けしてファインチューニングを行う開発者を含む)を指します。

はじめに

本ガイドラインが前提とする生成AIの利用者・用途

- 組織での生成AIの利用ルールでは、以下を規定することを推奨します。
  - ✓ カルテ等の文書の自動作成
  - ✓ 患者にとってわかりやすい病気や治療計画の説明・表現の検討　　等

- 以下のような、患者個人のみでの生成AI利用や、医療機関・薬局以外のサービス提供者等における利用は対象範囲に含みません。
  - ✓ 患者個人による、生成AIを用いた自身の病気に関する情報の検索
  - ✓ PHR事業者における、個人のバイタルデータの生成AIでの解析によるヘルスケアプラン等の作成
  - ✓ 製薬会社における、薬剤データなどを学習した生成AIを活用した創薬支援　　等

本ガイドラインにおける生成AIの利用範囲

※ユースケースの詳細は、４章を参照してください。

目次

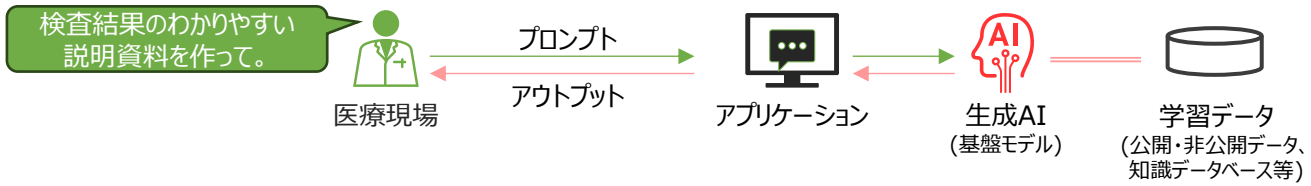
１章　医療・ヘルスケア分野における生成AI

- １章では、生成AIの特徴や、医療・ヘルスケア分野における生成AIのユースケースおよびリスクについて概説します。
- ２章以降では生成AIの利用時・開発時に特に注意すべきポイントについて述べます。本章はその前提情報としてご覧ください。

1. 生成AIの特徴

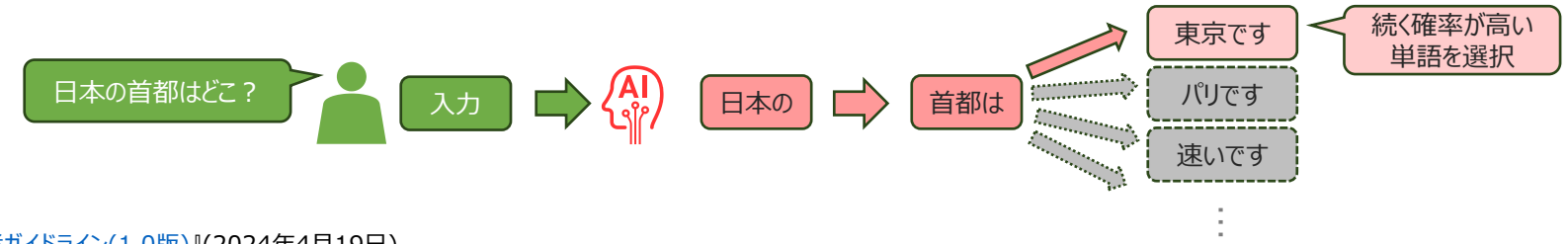
生成AIとは

- 生成AIとは、プロンプト(指示文)を入力し、文章、画像、プログラムなどを生成するAIモデルを基盤としたAIの総称です。プロンプトを入力し、AIが処理を行い、アウトプットを生成する仕組みを持ちます*1 。
- これまでのAIは、画像診断支援のように、用途に応じてデータを学習し、その用途に限定された作業を自動化するものであり、他の用途での利用が難しいという課題がありました。一方、生成AIは用途を限定せず多様なコンテンツを生成できるため、様々なシーンでの利用が期待されています。



生成AIの仕組み*2

- 生成AIは、学習した大量の文章や画像等のデータから確率にもとづいてコンテンツを生成します。そのため、生成AIは意味を真に理解して作成しているわけではありません。
- 例えば文章を生成するAIでは、ある単語に続く確率が高い単語を選択していくことで文章を生成しています。



*1 (参考) 総務省・経済産業省『AI事業者ガイドライン(1.0版)』(2024年4月19日)
*2 (参考) 消費者庁『AI利活用ハンドブック～生成AI編～』(2024年5月)

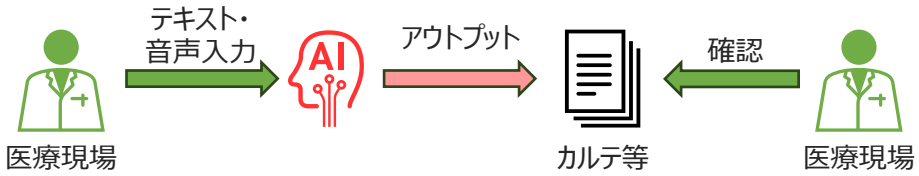
2. 医療・ヘルスケア分野での生成AIの利用可能性

生成AIのユースケース

- 医療・ヘルスケア分野での生成AIのユースケースは、例として以下が挙げられます。生成AIを適切に利用することで、業務効率化や医療の質の向上につながると考えられます。

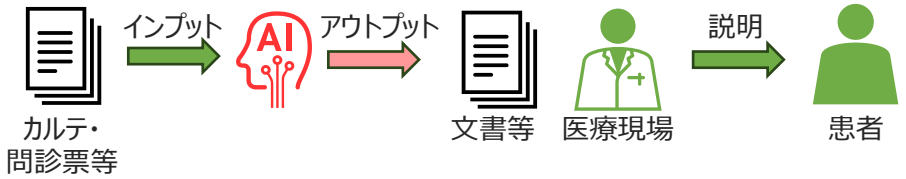
ドキュメントワーク支援

カルテ等の文書の自動作成、
予約システム等への自動入力 等



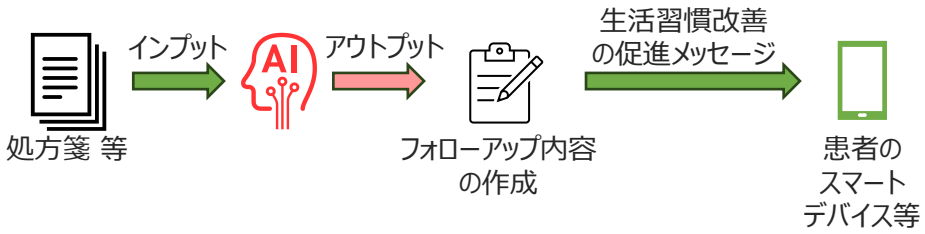
**患者等への
説明・接遇支援**

患者にとってわかりやすい病気や
治療計画の説明・表現の検討 等



患者フォローアップ支援

生活習慣改善等に関する
患者フォローアップのスケジュール、メッセージの作成 等



※ユースケースの詳細は、４章を参照してください。

3. 医療・ヘルスケア分野での生成AI利用時のリスク

生成AI利用時のリスク

- 生成AIの利用時には、プロンプトが再学習に利用されることによる情報漏えいや、アウトプットに著作権侵害や差別的な表現、不正確な情報が含まれるなど、様々なリスクがあります。
- 医療・ヘルスケア分野での生成AIの利用時では、主に以下のようなリスクがあるため、医療機関・薬局等での生成AIの利用にあたっては、これらのリスクを把握し、対策を講じる必要があります。

ディープフェイク

本物と見分けのつかない虚偽の画像・動画等を生成する。

不適正利用

本来の目的を逸脱して、違法な活動や倫理に反する目的等で利用する。

正確性・信頼性

誤情報を含むアウトプットを生成する。

バイアス・公平性

アウトプットにバイアスや不公平な内容があり、特定の個人や集団への偏見・格差・差別等を助長してしまう。

透明性・説明責任

AIを利用していることやその品質等が不透明であり、関係するステークホルダーへの説明責任が果たされていない。

著作権(著作権法)

他者の既存の著作物に類似したアウトプットを生成し、それを利用することで、著作権を侵害してしまう。

プライバシー(個人情報保護法等)

プライバシーを尊重したデータの取扱いがされないことにより、情報漏えいや個人情報保護法への違反に繋がってしまう。

セキュリティ(3省2ガイドライン等)

セキュリティが確保されていないことにより、不正な操作・攻撃等が行われた際に、情報漏えいや改ざん等が発生する。

その他法令等に関するリスク

生成AIの使い方等によっては、医療・ヘルスケア分野で関係する以下の法令等に違反する可能性がある。

- 医師法
- 医療法
- 医薬品医療機器等法
- 健康増進法
- 人を対象とする生命科学・医学系研究に関する倫理指針
- 臨床研究法
- 次世代医療基盤法
- 特許法

２章　生成AIの利用者が特に注意すべきポイント

- ２章では、生成AIの利用者が特に注意すべきポイントについて説明します。
- 前章に示すように、生成AIの利用によるリスクを適切に管理するために、生成AIを利用する医療機関・薬局等の方はこの章を参照し、対策の検討に活用ください。

1. 生成AIの利用者(個人)が特に注意すべきポイント

- 生成AIの利用者(個人)は、生成AIの利用によるリスクを適切に管理するために、特に以下のポイントに注意する必要があります。詳細については、次頁以降で示します。

ポイント①	利用する生成AIが、自身の所属する組織において利用可能と判断されているサービスであることを確認する。
ポイント②	生成AIの用途が法令等に違反していないことを確認する。
ポイント③	生成AIが出力した内容が正しいことを自ら確認する。
ポイント④	著作権保護の観点から以下を遵守する。 • 既存の著作物に類似する文章・イラスト等の生成につながるプロンプトを入力しないこと。 • 権利処理がされていない既存の著作物等を無断でプロンプトとして入力しないこと。 • 生成AIが出力した内容が既存の著作物等に類似していないことを確認すること。
ポイント⑤	生成AIの出力をそのまま利用する場合は、生成AIを利用している旨を通知する。

1. 生成AIの利用者(個人)が特に注意すべきポイント

ポイント①

利用する生成AIが、自身の所属する組織において利用可能と判断されているサービスであることを確認する。

- 医療機関・薬局等で利用する生成AIの多くは、医療情報*1を取扱うことが想定されます。一方で、入力データが再学習に利用される設定となっている場合に個人情報を入力すると、第三者提供となるため、本人の同意を得ずに医療情報等の個人情報を入力してしまうと個人情報保護法への違反となります。
- また、医療情報を取扱う生成AIである場合は、3省2ガイドライン*2に則り、以下のような要件を満たしているサービスを選択して利用する必要があります。
  - ✓ 生成AIのサーバ等が、国内法の適用を受ける場所に設置されていること。
  - ✓ 医療機関・薬局等と生成AIを接続するネットワークが、セキュアなネットワーク(TLS1.3以上＋クライアント認証、IP-VPN、IPsec-IKE等)となっていること。
- そのため、これらの観点等を踏まえて組織として利用可能な生成AIを選定するとともに、利用者(個人)においては、自身の所属する組織において利用可能と判断されているサービスであることを確認する必要があります。組織として利用可能な生成AIを選定する際の観点の詳細については、17頁を参照ください。
- なお、医療情報を取扱わないことを前提に、利用者(個人)が自身の所属する組織で利用可能と判断されていない生成AIを私的に利用することも想定されますが、このような場合では、参考情報の収集のみに利用するなど、用途を限定して利用する必要があります。

*1 本ガイドラインでの医療情報とは、医療に関する患者情報(個人識別情報)を含む情報を想定します。
*2 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』(2023年5月)
経済産業省・総務省『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 1.1 版』(2023年7月)

1．生成AIの利用者(個人)が特に注意すべきポイント

ポイント②

生成AIの用途が法令等に違反していないことを確認する。

- 医療・ヘルスケア分野では、8頁に示すように様々な関係する法令等があるため、これらの法令等に遵守して生成AIを利用する必要があります。
- そのため、生成AIの利用者自身において、以下に示す例のように関係する法令等に違反する方法で利用していないか確認する必要があります。
  - ✓ 医師法では、診断書や処方箋等の文書は医師が作成することとなっており、生成AIで作成した診断書や処方箋等の文書を医師が確認・修正等を行わずに利用することは違反となります。
  - ✓ 医薬品医療機器等法では、患者への服薬指導は薬剤師が行うこととなっており、生成AIで出力した患者への服薬指導の内容を薬剤師から説明せず、生成AIを用いて直接患者へ提示することは違反となります。
  - ✓ 健康増進法では、患者の疾患管理のために必要な栄養指導等は医療従事者から行うこととなっており、生成AIで出力した患者の疾患管理のために必要な栄養指導の内容を医療従事者から説明せず、生成AIを用いて直接患者へ提示することは違反となります。

1. 生成AIの利用者(個人)が特に注意すべきポイント

ポイント ③

生成AIが出力した内容が正しいことを自ら確認する。

- 生成AIが出力した内容には、不正確な情報等が含まれる可能性があります。例えば、生成AIをドキュメントワーク支援のために利用する場合、生成AIを用いて作成した医療文書、事務文書等の内容に、不正確な記載や虚偽の記載等が混在してしまう可能性があります。また、生成AIは過去の診療データや各学会からその時点で発行されている治療ガイドライン等を基に学習することから、例えば生成AIを用いて治療方針のレコメンドを行う場合、各学会から発行されている最新の治療ガイドライン等に沿っていない、誤った治療方針を提案してしまう可能性があります。
- そのため、利用者において生成AIが出力した内容が正しいものであるかを自ら確認する必要があります。
- なお、生成AIが直接患者と会話するなど、医師等の利用者による都度の確認が適さないケースも想定されますが、その場合は特に事前の正確性の確保が求められます。また、患者は生成AIの回答精度等に対して過剰な期待を寄せることも考えられます。そのため、このような目的で生成AIを利用する際は、事前の正確性評価を重点的に実施する他、患者への生成AIサービスの提示の仕方を工夫し、期待値をコントロールすることが対策として考えられます。
- また、特定の用途や分野向けで最適化した生成AIを、その他の用途や分野で利用してしまうと、生成AIの回答精度が低く、出力に不正確な情報が多く含まれてしまう可能性があります。そのため、利用する生成AIに応じて、その用途が適切であるか確認することが考えられます。

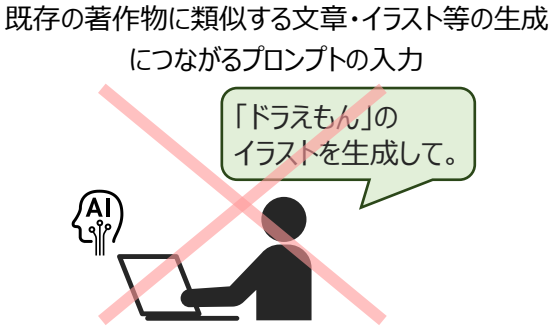
(参考) デジタル庁『テキスト生成 AI 利活用におけるリスクへの対策ガイドブック（α版）』(2024年6月参照)

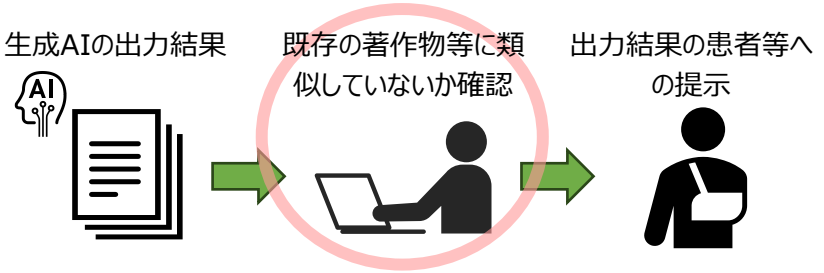
1. 生成AIの利用者(個人)が特に注意すべきポイント

ポイント ④

著作権保護の観点から以下を遵守する。
- 既存の著作物に類似する文章・イラスト等の生成につながるプロンプトを入力しないこと。
- 権利処理がされていない既存の著作物等を無断でプロンプトとして入力しないこと。
- 生成AIが出力した内容が既存の著作物等に類似していないことを確認すること。

- 生成AIを利用して、他人の既存の著作物等に類似する文章・イラスト等を生成した場合、当該生成物の利用は著作権侵害になる可能性があります。また、生成AIで生成物を作成する過程で、権利処理がされていない他人の既存の著作物を利用することも、著作権侵害になる可能性があり、注意が必要です。
- 例えば、患者向けの説明資料の挿絵を生成AIを用いて作成した場合に、他人の著作物等に類似するイラストや図等を著作権者に許諾を得ずに無断で用いてしまうと、著作権侵害になる可能性があります。
- そのため、利用者(個人)において、既存の著作物に類似する文章・イラスト等の生成につながるプロンプトを入力しないこと、生成AIを用いて作成した生成物が、他人の既存の著作物等に類似していないか確認することを遵守する必要があります。また、生成AIに他人の既存の著作物等を入力する際は、権利処理がされていることを確認する必要があります。





(参考) デジタル庁『テキスト生成 AI 利活用におけるリスクへの対策ガイドブック（α版）』(2024年6月参照)

1. 生成AIの利用者(個人)が特に注意すべきポイント

ポイント ⑤

生成AIの出力をそのまま利用する場合は、生成AIを利用している旨を通知する。

- 生成AIの出力をそのまま使用する場合は、生成AIを利用している旨を通知し、受け取り手側がAIを利用していることを理解できるようにする必要があります。
- 例えば、検査等に関する患者への説明を医療従事者ではなく、生成AIを用いて行う場合、生成AIを利用していることを通知しなければ、患者が医療従事者からの説明として受け取ってしまう可能性があります。このような場合に AIが間違った説明をしてしまうと、さらなる問題につながる可能性があります。
- そのため、利用者(個人)において、生成AIの出力をそのまま利用する場合は、生成AIを利用している旨を受け取り手側に通知することが必要となります。なお、生成AIの出力をそのまま使用しない場合も、透明性確保の観点から、生成AIを利用している旨を受け取り手側に通知することが考えられます。
- また、受け取り手側への透明性をより高めるため、生成AIの役割に関する説明を通知の中に含めることも考えられます。例えば、ドキュメントワーク支援(カルテの作成支援)では、患者と医師の間の会話内容の文字起こしと要約を生成AIが担っていることを通知の中に含めることが考えられます。

2. 生成AIの利用者(組織)が特に注意すべきポイント

- 医療機関・薬局等で生成AIを利用する場合は、そのリスクを適切に管理するために、利用者(個人)だけでなく、組織的に対策を講じることが望ましいです。その際に注意すべきポイントを以下に示します。
- 詳細については、次頁以降で示します。

ポイント①	既存の生成AIサービスを利用する場合、組織で利用可能なものを以下の観点を踏まえて選定し、職員へ周知する。 • セキュリティが確保されていること。 • 入力データが再学習に利用されない設定となっていること。 • (生成AIを医学的判断に利用する場合)生成AIが薬事承認を取得していること。
ポイント②	組織での生成AIの利用ルールとして、以下を規定し、運用する。 • 法令等に違反した利用や不適正利用を禁止。 • 利用者として求められる利用上・セキュリティ上の留意点を遵守。 • 職員が生成AIを誤用しないことを定期的にチェック。 • 組織での生成AIの利用状況を把握。
ポイント③	職員が生成AIの利用による便益やリスク等を理解し、適切にリスクを管理できるよう、本ガイドラインに基づく研修を実施する。

2. 生成AIの利用者(組織)が特に注意すべきポイント

ポイント①

既存の生成AIサービスを利用する場合、組織で利用可能なものを以下の観点を踏まえて選定し、職員へ周知する。
- セキュリティが確保されていること。
- 入力データが再学習に利用されない設定となっていること。
- (生成AIを医学的判断に利用する場合)生成AIが薬事承認を取得していること。

- 医療機関・薬局等で利用する生成AIの多くは、医療情報を取扱うことが想定されます。そのため、既存の生成AIサービスを利用する組織では、医療情報を取扱うことを前提に、リスクが低いと想定されるものを利用可能なものとして選定しておくことは、組織全体でのリスクを管理する上で効果的です。
- 組織で利用可能な生成AIを選定する際は、以下の観点等を生成AIの提供者に確認する必要があります。
  - ✓ セキュリティが確保されていること。
    - ➢ 生成AIのサーバ等が、国内法の適用を受ける場所に設置されていること。
    - ➢ 医療機関・薬局等と生成AIを接続するネットワークが、セキュアなネットワーク(TLS1.3以上＋クライアント認証、IP-VPN、IPsec-IKE等)となっていること。
    - ➢ (組織で保有する医療情報をファインチューニング等に使用する場合)生成AIのサービス提供者との契約や書面等で、提供する医療情報が漏えいしないよう安全管理措置がされていること、契約終了後に提供した医療情報が削除されること。 等
  - ✓ 入力データが再学習に利用されない設定となっていること。
  - ✓ (生成AIを医学的判断に利用する場合)生成AIが薬事承認を取得していること。
- なお、医療情報を取扱わない形で生成AIを利用することも可能ですが、医療・ヘルスケア分野で利用した場合に回答精度が低いなどの課題が想定されるため、参考情報の収集のみに利用するなど、用途を限定しておく必要があります。
- また、自身の組織で利用する生成AIを自ら開発する場合は、3章を参照し対策を検討ください。

2. 生成AIの利用者(組織)が特に注意すべきポイント

ポイント②

組織での生成AIの利用ルールとして、以下を規定し、運用する。
- 法令等に違反した利用や不適正利用を禁止。
- 利用者として求められる利用上・セキュリティ上の留意点を遵守。
- 職員が生成AIを誤用しないことを定期的にチェック。
- 組織での生成AIの利用状況を把握。

- 職員において、適切にリスクを管理して生成AIが利用される状態を維持できるよう、組織での生成AIの利用ルールを定めておくことが望ましいです。
- 組織での生成AIの利用ルールでは、以下を規定することを推奨します。
  - ✓ 法令等に違反した利用や不適正利用を禁止。(例：薬事承認を得ていない生成AIを、患者の医学的判断等に使用することを禁止する。)
  - ✓ 利用者に求められる利用上・セキュリティ上の留意点を遵守。(例：虚偽のデータの生成を意図したプロンプトの入力を禁止する。)
  - ✓ 職員が生成AIを誤用しないことを定期的にチェック。(例：監査により生成AIの利用状況を半年に1回チェックし、誤用等が生じていないか職員に確認する。)
  - ✓ 組織での生成AIの利用状況を把握。(例：診療科・部署等において、生成AIを利用する際は組織のAIを管理している部署等へ申請を行う。)

2. 生成AIの利用者(組織)が特に注意すべきポイント

ポイント ③

既存の生成AIサービスを利用する場合、組織で利用可能なものを以下の観点を踏まえて選定し、職員へ周知する。

- セキュリティが確保されていること。
- 入力データが再学習に利用されない設定となっていること。
- (生成AIを医学的判断に利用する場合)生成AIが薬事承認を取得していること。

- 生成AIを利用する職員が、生成AIにおいて注意すべきポイントを理解していない場合、適切な対策が講じられず、リスクが顕在化してしまう可能性があります。職員が生成AIの利用による便益やリスク等を理解し、適切にリスクを管理できるようにするには、組織で研修を実施することが効果的です。
- 研修では、本ガイドラインの「１章 医療・ヘルスケア分野における生成AI」や本章を参考に、生成AIの利用による便益やリスク等とともに、利用者として注意すべきポイント等を周知ください。
- 組織として生成AIを利用するケースが定まっている場合は、「4章 生成AIのユースケースとリスク・対策例」等も参考に、個別のケースに応じたリスクと対策例等も研修で取扱うことを検討ください。
- また、生成AIを利用する職員が適切に研修を受講していることを確認するために、以下を実施することも検討ください。
  - ✓ 受講後のテスト
  - ✓ 受講状況の把握及び未受講者のフォロー

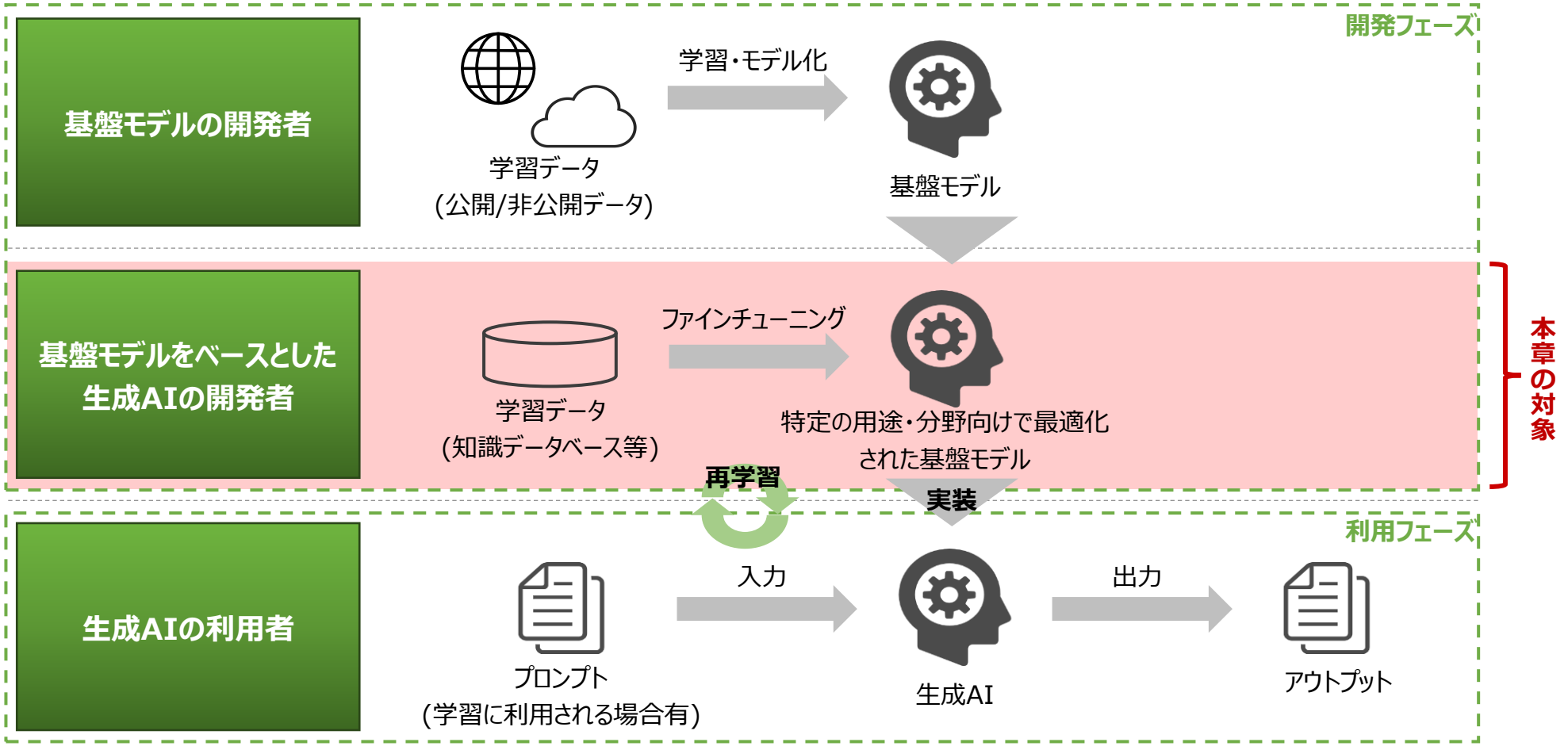
本ガイドラインに基づく研修の実施

３章　生成AIの開発者が特に注意すべきポイント

- ３章では、生成AIの開発者が特に注意すべきポイントについて説明します。
- 生成AIの利用によるリスクを適切に管理するためには、生成AIの開発フェーズから対策を講じる必要があります。生成AIを開発する医療機関等の方はこの章を参照し、対策の検討に活用ください。

1. 生成AIの開発者とは

- 医療機関等における生成AIの開発は、基盤モデルに対してファインチューニングを行うケース(RAG等の知識データベースを外付けしてファインチューニングを行うケースを含む)と想定されます。
- そのため、本章の対象は、以下の基盤モデルをベースとした生成AIの開発者とします。



2. 生成AIの開発者が特に注意すべきポイント

- 生成AIのリスクは基本的に利用フェーズにおいて生じると考えられますが、リスクを管理するためには、開発フェーズから対策を講じる必要があります。そのため、基盤モデルをベースとした生成AIの開発者は、特に以下のポイントに注意する必要があります。詳細については、次頁以降で示します。

ポイント①	ディープフェイク画像等の生成や不適正利用が生じないよう、以下を行う。 • 典型的な不適正利用のパターンを機能的に制限。 • 利用規約等により不適正利用を禁止。 • 利用者認証を適切に行った上で、利用者の操作ログの保管等。
ポイント②	正確性・信頼性確保の観点から、以下を行う。 • 学習データの正確性・信頼性が確保されていることを確認。 • アウトプットの正確性等を評価。 • 適切な形式で利用者がプロンプトを入力できるよう、モデルとなるプロンプトを提示。
ポイント③	著作権保護の観点から、以下を行う。 • 学習データをそのまま、あるいは類似した形で出力されないように設定。 • 著作権等の権利処理を行った上で、学習データに利用。
ポイント④	個人情報保護の観点から、以下を行う。 • 学習データに個人情報が含まれている場合は、匿名加工情報・仮名加工情報に加工するとともに、個人情報保護法等で定められた取扱いを遵守。 • 学習データに含まれる個人情報が出力されないことを確認。
ポイント⑤	OSSの基盤モデルを用いて開発する場合、セキュリティ確保の観点から以下を行う。 • 学習データの安全管理措置を実施。 • モデルの改ざん等が生じないように安全管理措置を実施。 • 医療情報等のように、データの種類に応じた安全管理措置を実施。
ポイント⑥	生成AIの出力を患者等への医学的判断に利用する場合、当該生成AIは医療機器に該当することから、医薬品医療機器等法に則り、薬事承認を取得する。

2. 生成AIの開発者が特に注意すべきポイント

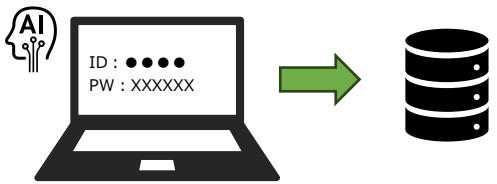
ポイント①

ディープフェイク画像等の生成や不適正利用が生じないよう、以下を行う。
- 典型的な不適正利用のパターンを機能的に制限。
- 利用規約等により不適正利用を禁止。
- 利用者認証を適切に行った上で、利用者の操作ログの保管等。

- 生成AIは利用者の使い方によっては、虚偽のデータを生成できてしまうなどのリスクがあります。
- 例えば、生成AIをドキュメントワーク支援のために利用する場合、利用者が生成AIを用いて作成した医療文書(診療情報提供書等)の偽造物が出回ってしまう可能性があるなどのリスクがあります。
- そのため、開発フェーズから、ディープフェイク画像等の生成や不適正利用が生じないよう、以下の対策を講じることが望ましいです。
  - ✓ 典型的な不適正利用のパターンを機能的に制限。(例：生成AIを用いて、電子カルテから診療情報提供書の案を作成する場合、内容の改ざんを意図したプロンプトの入力を制限する。)
  - ✓ 利用規約等により不適正利用を禁止。
  - ✓ 利用者認証を適切に行った上で、利用者の操作ログの保管等。
- また、保管した操作ログの監査を行い、利用規約等に違反している利用者を発見した場合、その利用者のアカウントを停止するなどの対応も考えられます。

不適正利用の機能的な制限や利用規約等での禁止

利用者認証を行った上で操作ログの保管



2. 生成AIの開発者が特に注意すべきポイント

ポイント②

正確性・信頼性確保の観点から、以下を行う。
- 学習データの正確性・信頼性が確保されていることを確認。
- アウトプットの正確性等を評価。
- 適切な形式で利用者がプロンプトを入力できるよう、モデルとなるプロンプトを提示。

- 生成AIが出力した内容には不正確な情報等が含まれる可能性があることから、このリスクを低減するために、開発フェーズから以下の対策を講じることが望ましいです。
  - ✓ 学習データの正確性・信頼性が確保されていることを確認。(例：可能な範囲でデータの出所等を確認する。)
  - ✓ モデル化、実装の段階において、アウトプットの正確性等を評価。(例：アウトプットを人により確認し、内容が正確であるかなどを評価する。)
  - ✓ 生成AIの利用目的に合わせて、適切な形式で利用者がプロンプトを入力できるよう、モデルとなるプロンプトを提示。
- 特に電子カルテ等を学習データに利用する場合では、学習データの正確性の確保に留意する必要があります。例えば、電子カルテに陰性初見を記載していないなど、必要な情報が欠損しているケースが想定されますが、そのようなデータを学習することは回答精度の低下につながる可能性があります。
- なお、生成AIは過去の診療データや各学会からその時点で発行されている治療ガイドライン等を基に学習することから、例えば生成AIを用いて治療方針のレコメンドを行う場合、最新の治療ガイドライン等に沿っていない、誤った治療方針を提案してしまう可能性があります。そのため、生成AIに最新の医療情報を継続的に学習する仕組みを検討する必要があります。

2. 生成AIの開発者が特に注意すべきポイント

ポイント ③

著作権保護の観点から、以下を行う。
- 学習データをそのまま、あるいは類似した形で出力されないように設定。
- 著作権等の権利処理を行った上で、学習データに利用。

- 生成AIは他人の既存の著作物等に類似する文章・イラスト等を生成してしまう場合があり、著作権侵害につながる可能性があります。また、生成AIが著作権侵害につながる出力を行う場合、著作権等の権利処理がされていない他人の既存の著作物を学習に利用すること自体も、著作権侵害となる可能性があります。
- そのため、著作権保護の観点から、開発フェーズから以下の対策を講じることが望ましいです。
  - ✓ 学習データをそのまま、あるいは類似した形で出力されないように設定。(例：学習データをそのままアウトプットすることを意図したプロンプトが入力された場合、回答を出力しないように制限する。)
  - ✓ 著作権等の権利処理を行った上で、学習データに利用。
- なお、生成AIを開発する際の学習データにおける著作権の考え方に関しては、「AIと著作権に関する考え方について*1」でも整理されているため、開発する際の参考にしてください。

*1 文化審議会著作権分科会法制度小委員会『AIと著作権に関する考え方について』(2024年3月15 日)

2. 生成AIの開発者が特に注意すべきポイント

ポイント ④

個人情報保護の観点から、以下を行う。

- 学習データに個人情報が含まれている場合は、匿名加工情報・仮名加工情報に加工するとともに、個人情報保護法等で定められた取扱いを遵守。
- 学習データに含まれる個人情報が出力されないことを確認。

- 患者等から同意を得て取得した個人情報を含む医療情報をそのまま生成AIの学習に利用する場合、オプトアウト等により、患者等から学習に利用した個人情報の削除等が求められた際に対応する必要がありますが、その都度、削除したデータで学習し直すことは困難であると考えられます。
- そのため、学習データに個人情報を含む医療情報が含まれている場合は、匿名加工情報・仮名加工情報に加工するとともに、個人情報保護法等*1で定められた取扱いを遵守する必要があります。また、その他の選択肢として、匿名加工医療情報・仮名加工医療情報を入手して学習に利用することも考えられますが、その場合は、次世代医療基盤法*2で定められた取扱いを遵守する必要があります。
- また、学習データに含まれる個人情報を含む医療情報が生成AIの利用時に出力された場合、情報漏えい等となります。そのため、学習データに含まれる個人情報を含む医療情報が生成AIの利用時に出力されないことを確認する必要があります。

*1 匿名加工情報や仮名加工情報の取扱い等の詳細に関しては、以下のガイドラインも参照ください。
個人情報保護委員会『個人情報の保護に関する法律についてのガイドライン （仮名加工情報・匿名加工情報編） 』(2023年12月一部改正)
*2 匿名加工医療情報・仮名加工医療情報の取扱い等の詳細に関しては、以下のガイドラインも参照ください。
内閣府・文武科学省・厚生労働省・経済産業省『医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律についてのガイドライン（次世代医療基盤法ガイドライン）』(2024年4月)

2. 生成AIの開発者が特に注意すべきポイント

ポイント ⑤

OSSの基盤モデルを用いて開発する場合、セキュリティ確保の観点から以下を行う。
- 学習等に利用するデータの安全管理措置を実施。
- モデルの改ざん等が生じないように安全管理措置を実施。
- 医療情報等のように、データの種類に応じた安全管理措置を実施。

- 外部からの学習データやモデルへの攻撃により、生成AIが利用者の意図に反する出力を行うなどの被害を受ける可能性があります。また、外部からの攻撃の種類によっては、学習データ等に含まれる情報の漏えい等につながる可能性があります。
- OSSの基盤モデルを用いて開発する場合は、開発者においてセキュリティを確保[*1]するために、開発フェーズから以下の対策を講じる必要があります。
  - ✓ 学習データの安全管理措置を実施。(例：3省2ガイドラインに則り、サーバ等を国内法の適用を受ける場所に設置する。)
  - ✓ モデルの改ざん等が生じないように安全管理措置を実施。(例：学習モデルのポイズニングを検知する。)
  - ✓ 医療情報等のように、データの種類に応じた安全管理措置を実施。(例：医療情報を取扱う生成AIでは、3省2ガイドラインに則り、医療機関・薬局等と生成AIを接続するネットワークはセキュアなネットワーク(TLS1.3以上＋クライアント認証、IP-VPN、IPsec-IKE等)にする。)

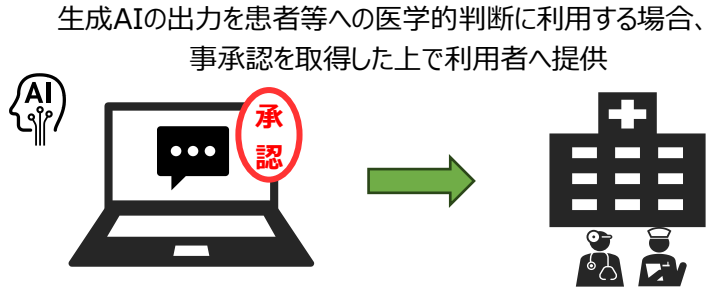
*1 セキュリティ確保にあたっては、以下のドキュメント等も参考に対策を検討ください。
・厚生労働省『医療情報システムの安全管理に関するガイドライン 第6.0版』(2023年5月)
・経済産業省・総務省『医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン 第 1.1 版』(2023年7月)
・国立研究開発法人産業技術総合研究所『機械学習品質マネジメントガイドライン 第４版』(2024年4月一部改正)

2. 生成AIの開発者が特に注意すべきポイント

ポイント⑥

生成AIの出力を患者等への医学的判断に利用する場合、当該生成AIは医療機器に該当することから、医薬品医療機器等法に則り、薬事承認を取得する。

- 生成AIの出力を患者等への医学的判断に利用する場合、当該生成AIは医療機器に該当します*1。
- そのため、このような医療機器に該当する生成AIを開発し、製造・販売する場合は、医薬品医療機器等法に則り、製造所の登録や医療機器の薬事承認の取得が必要となります。また、薬事承認を取得する際には、学習データの収集・整備に関する記録・整理が必要となります。
- なお、生成AIは様々な用途で利用できるものですが、薬事承認を取得しない場合は、医療機器として有効性や安全性が確認されていないことから、疾病の診断・予防・治療を目的として利用することはできません*2。そのため、疾病の診断・予防・治療を目的としたものではないことや医療機器ではないこと等を生成AIに表示しておくことが考えられます。



*1 厚生労働省『プログラムの医療機器該当性に関するガイドライン』(2023年3月31日一部改正)
*2 厚生労働省『医療機器プログラムについて』(2024年6月参照)

４章　生成AIのユースケースとリスク・対策例

- ４章では、医療機関・薬局等における医療・ヘルスケア分野での生成AIのユースケースとともに、そのリスクと対策例について説明します。
- 生成AIの利用を検討している/既に利用している医療機関・薬局等の方は、この章の該当するユースケースを参照し、対策の検討に活用ください。

1. 生成AIのユースケースの全体像

- 医療・ヘルスケア分野における医療機関・薬局等での生成AIのユースケースは、以下を想定しています。また、各ユースケースの概要やリスク・対策例は、該当頁を参照ください。

ユースケース名	利用例	主な利用者	該当頁
① ドキュメントワーク支援	・生成AIに問診内容や診療内容等を入力し、問診票やカルテ等のドキュメント作成等を行う。	医師、医療事務職員、看護師、検査技師等	32～37頁
② 診察・診断支援	・診察前に問診票データ等を生成AIに入力し、可能性の高い複数の病名を根拠と共にサジェスト表示する。	医師、検査技師、医療事務職員等	38～44頁
③ 患者等への説明・接遇支援(患者等とのコミュニケーション)	・外国の方を診察した際に、診察結果を生成AIに入力し、外国の方へ説明する際に自然で分かりやすい表現に翻訳する。	医師、看護師、薬剤師、医療事務職員等	45～50頁
④ 患者フォローアップ支援	・生成AIに処方箋等の内容を入力し、服薬指導等のフォローアップメッセージを作成し、薬剤師の確認・修正等を行った上で、薬剤師が対面またはオンラインで患者へ説明する。	医師、薬剤師等	51～57頁
⑤ 患者トリアージ	・来院患者が入力した問診フォームの内容を生成AIに取込み、流行感染症への感染疑いを判別し、疑いのある患者を医師等にアラートする。	医師、受付職員患者等	58～63頁
⑥ 研修支援	・検査画像等の医療データを生成AIに大量に取込んで学習し、研修教材として活用可能な検査合成画像やケーススタディ文等を作成する。	指導医等	64～68頁
⑦ 研究データ処理・分析支援	・複数の研究論文を生成AIに取込み、複数の研究データ内容を要約した文章を作成し、研究等に活用する。	研究者等	69～77頁
⑧ デジタルセラピー	・精神疾患患者のカルテ等データを生成AIに取込み、認知療法等に活用可能なAR/VR画像を作成する。	医師、作業療法士等	78～84頁

2. 生成AIの各ユースケースの概要・リスク・対策例

- 本項では、前頁に示す生成AIの各ユースケースの概要とリスク・対策例をそれぞれ示します。
- 前頁の利用例等を参考に、関心がある生成AIのユースケースの該当頁を確認し、概要やリスク・対策例に関する理解を深め、自身の組織で生成AIを利用する際の対策の検討等に活用ください。
- なお、本項では、以下に示すリスクの種類*1ごとに、想定されるリスクの内容や対策例を示します。想定されるリスクの内容や対策例は、生成AIの利用者(個人、組織)と基盤モデルをベースとした生成AIの開発者で記載頁を分けて示しているため、自身の立場に応じて、必要な箇所を参照してください。
- また、19頁で示すとおり、組織として生成AIを利用するケースが定まっている場合は、研修において、利用するユースケースのリスクと対策例等も取扱うことを検討ください。

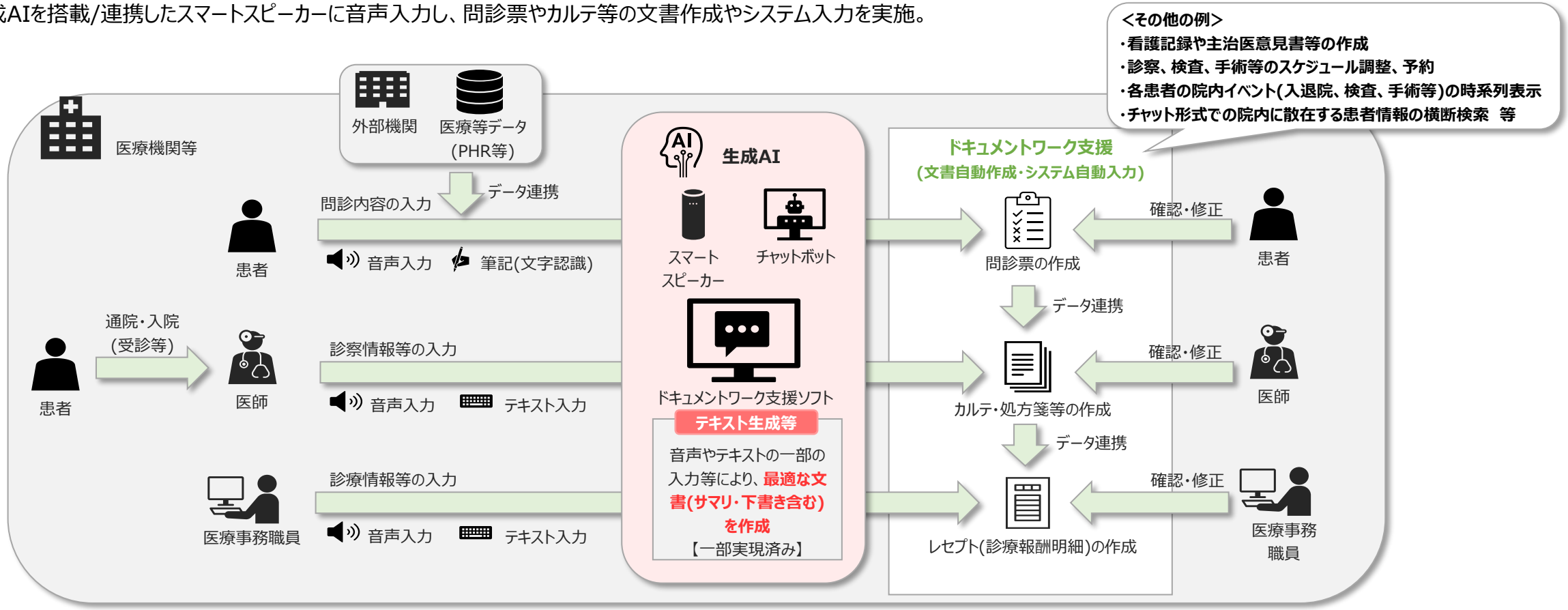
(#1)ディープフェイク
(#2)不適正利用
(#3)正確性・信頼性
(#4)バイアス・公平性
(#5)透明性・説明責任
(#6)著作権(著作権法)
(#7)プライバシー(個人情報保護法等)
(#8)セキュリティ(3省2ガイドライン等)
(#9~16)その他法令等に関するリスク

*1 リスクの種類ごとの概要は、8頁を参照ください。

2. 生成AIの各ユースケースの概要・リスク・対策例

①ドキュメントワーク支援(文書自動作成、システム自動入力)の概要

- 医療機関における以下のようなドキュメントワークを生成AIにより支援することで、業務効率化が期待できます。
  - 生成AIに問診内容や診療内容等を入力し、問診票やカルテ、レセプト(診療報酬明細)等のドキュメント作成を実施。
  - 生成AIを搭載/連携したスマートスピーカーに音声入力し、問診票やカルテ等の文書作成やシステム入力を実施。



(参考) ビジネス+IT『医療の現場でも進む生成AI活用、莫大なコスト削減につながる理由とは？』(2024年6月参照)
ITmedia『Microsoft、GPT-4を傘下Nuanceの医療向け臨床メモ自動化サービスに採用　患者との会話を数秒でメモ化』(2024年6月参照)

2. 生成AIの各ユースケースの概要・リスク・対策例

①ドキュメントワーク支援(文書自動作成、システム自動入力)で想定されるリスク・対策例

- 前頁に示すユースケースにおいて、想定されるリスクとともに生成AIの利用者での対策例を以下に示します。
- なお、リスク管理を行う際に、①のユースケース特有で注意すべきポイントは以下のとおりです。
  - 組織でのルールとして以下を規定し、職員に周知するとともに、利用者(個人)においてもこれらのルールを遵守。
    - ✓ 利用者として求められる安全管理措置(ドキュメントに電子署名する場合における法定要件の準拠を含む)を実施。
    - ✓ 生成AIで作成した医療文書は、医師が最終確認を行った後に発行。

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
1	ディープフェイク	・医療文書(診療情報提供書等)等の偽造物が出回る可能性がある。	・偽情報を作成しない。	・左記、個人での対策を利用ルールとして規定し、職員に周知。
2	不適正利用	・ディープフェイク以外に問題は生じない想定。	–	–
3	正確性、信頼性	・医療文書等の作成において正確性が欠けたり、虚偽の記載が混在する可能性がある。	・生成AIのインプットとする医療文書等のデータを正確に入力。 ・出力された医療文書等を医師や医療事務の担当者が確認した上で利用。	・職員に対し、左記の対策例を周知。 ・組織として利用可能な生成AIを選定する際に、サービスの正確性を評価。
4	公平性、バイアス	・情報の蓄積が多い診療科や医師の特性に応じて医療文書等が作成される可能性がある。	※「正確性、信頼性」と同じ。	・「正確性、信頼性」と同様、医師に対し、左記の対策例を周知。 ・組織として利用可能な生成AIを選定する際に、サービスのバイアス等を評価。
5	透明性、説明責任	・生成AIが作成した事務文書等を人による確認・修正等を行わずそのまま利用する場合、透明性、説明責任の問題が生じる。	・生成AIの出力をそのまま利用する場合は、生成AIが作成したものであることを事務文書等に明記。	・生成AIのサービス提供者に対して、品質に関する情報の開示を要求。
6	著作権（著作権法）	・問題は生じない想定。	–	–

2. 生成AIの各ユースケースの概要・リスク・対策例

①ドキュメントワーク支援(文書自動作成、システム自動入力)で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
7	プライバシー (個人情報保護法等)	• 医療文書、事務文書等の作成では、医療情報(個人情報を含む)を入力データに利用する可能性が高く、再学習に利用される設定の生成AIに入力する場合、第三者提供となる。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。	• 組織として利用可能な生成AIを選定する際に、入力データが再学習に利用されない設定となっていることを確認。
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアでない。 ✓ 医師が最終確認をしたドキュメントへ電子署名する際に、法定要件を満たしていない。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。 • 利用者として求められる安全管理措置(ドキュメントに電子署名する場合における法定要件の準拠を含む)を実施。	• 組織として利用可能な生成AIとして、以下の観点等から選定し、職員へ周知。 ✓ 生成AIのサーバ等が、国内法の適用を受ける場所に設置されていること。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアであること。 ✓ (組織で保有する医療情報を提供する場合)生成AIのサービス提供者との契約や書面等で、提供する医療情報が漏えいしないよう安全管理措置がされていること、契約終了後に提供した医療情報が削除されること等。 • 左記、個人での対策を利用ルールとして規定し、職員に周知。
9	医師法	• 医療文書の案を生成AIが作成する場合、医師が確認・修正等した上で利用しなければ医師法に違反する。	• 生成AIで作成した医療文書は、医師が最終確認を行った後に発行。	• 左記、個人での対策を利用ルールとして規定し、職員に周知。
10	医療法	• 事務文書において正確性の問題等が生じた場合、組織の適正運営における問題として医療法に違反する可能性がある。	※「正確性、信頼性」と同じ。	※「正確性、信頼性」と同じ。

2. 生成AIの各ユースケースの概要・リスク・対策例

①ドキュメントワーク支援(文書自動作成、システム自動入力)で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
11	医薬品医療機器等法	・文書作成の支援という点では診断等に該当しないため、医療機器プログラムには該当しない。	―	―
12	健康増進法	・問題は生じない想定。	―	―
13	人を対象とする生命科学・医学系研究に関する倫理指針	・問題は生じない想定。	―	―
14	臨床研究法	・問題は生じない想定。	―	―
15	次世代医療基盤法	・利用フェーズでは、問題は生じない想定。	―	―
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	―	・組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に対し、特許権侵害を犯していないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

①ドキュメントワーク支援(文書自動作成、システム自動入力)で想定されるリスク・対策例

- 32頁に示すユースケースにおいて、想定されるリスクとともに生成AIの開発者での対策例を以下に示します。
- なお、リスク管理を行う際に、①のユースケース特有で注意すべきポイントは以下のとおりです。
  - 組織でのルールとして以下を規定し、職員に周知するとともに、利用者(個人)においてもこれらのルールを遵守。
    - ✓ 利用者側で留意して生成AIを取扱うことができるよう、医療文書や事務文書等の生成の精度等について利用者に情報提供。

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
1	ディープフェイク	• 医療文書(診療情報提供書等)等の偽造物が出回る可能性がある。	• 典型的な不適正利用のパターンを機能的に制限。 • 利用規約等により偽情報の作成を禁止。
2	不適正利用	• ディープフェイク以外に問題は生じない想定。	–
3	正確性、信頼性	• 医療文書等の作成において正確性が欠けたり、虚偽の記載が混在する可能性がある。	• 学習データとなる医療文書、事務文書等を正規化し、正確性・信頼性を担保。 • 学習済みモデルの正確性・信頼性を評価した上で実装。
4	公平性、バイアス	• 情報の蓄積が多い診療科や医師の特性に応じて医療文書等が作成される可能性がある。	• 学習データに偏りがないか評価。 • 学習済みモデルのアウトプットに偏りがないか評価。
5	透明性、説明責任	• 生成AIが作成した事務文書等を人による確認・修正等を行わずそのまま利用する場合、透明性、説明責任の問題が生じる。	• 利用者側で留意して生成AIを取扱うことができるよう、医療文書や事務文書等の生成の精度等について、利用者に情報提供。
6	著作権（著作権法）	• 問題は生じない想定。	–
7	プライバシー (個人情報保護法等)	• 医療情報(個人情報を含む)を学習に利用する場合、本人から個人情報の削除等が求められた際に対応する必要があるが、その都度、削除したデータで学習し直すことは困難。	• 医療情報(個人情報を含む)を学習に利用する場合は、仮名加工情報、匿名加工情報に加工し、個人情報保護法等で規定された取り扱いを遵守。

2. 生成AIの各ユースケースの概要・リスク・対策例

①ドキュメントワーク支援(文書自動作成、システム自動入力)で想定されるリスク・対策例

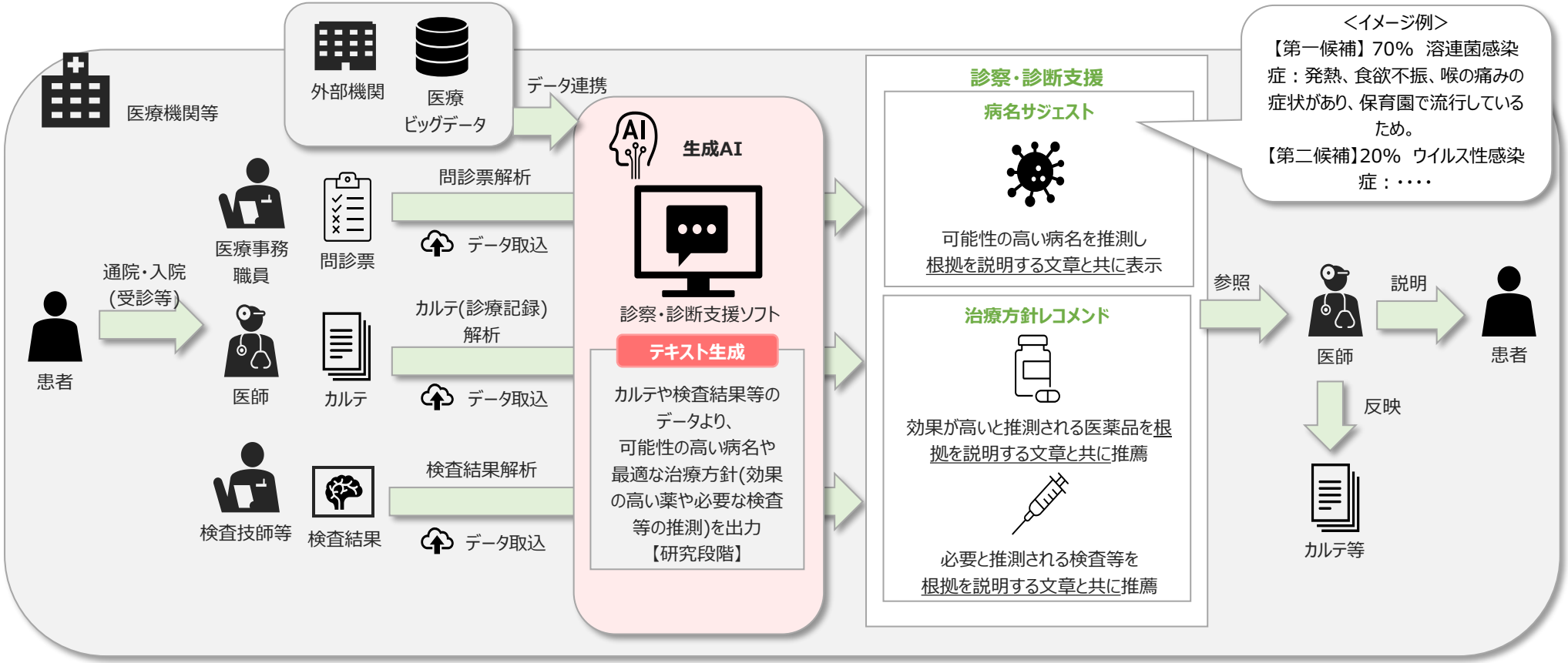
【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアでない。	• 3省2ガイドラインに準拠するよう、以下の対策等を実施。 ✓ 医療情報を保管するサーバ等を国内法の適用を受ける場所に設置。 ✓ 3省2ガイドラインで求められる技術基準に則した安全管理措置を実施(医療機関・薬局等と生成AIを接続するネットワークをセキュアとすることを含む)。
9	医師法	• 開発フェーズでは問題は生じない想定。	–
10	医療法	• 開発フェーズでは問題は生じない想定。	–
11	医薬品医療機器等法	• 文書作成の支援という点では診断等に該当しないため、医療機器プログラムには該当しない。	–
12	健康増進法	• 問題は生じない想定。	–
13	人を対象とする生命科学・医学系研究に関する倫理指針	• 問題は生じない想定。	–
14	臨床研究法	• 問題は生じない想定。	–
15	次世代医療基盤法	• 学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、匿名加工医療情報や仮名加工医療情報を法で定められた取り扱いをしなければ次世代医療基盤法に違反する。	• 学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、次世代医療基盤法で規定された取り扱いを遵守。
16	特許法	• データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	• データの処理方法や生成AIの開発工程等に関して特許調査を行い、特許権の侵害が生じないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

②診察・診断支援の概要

- 診察・診断業務を生成AIを用いて以下のように支援することで、業務効率化や医療の質の向上が期待できます。
  - 問診票データ等を生成AIに取込むことで、可能性の高い複数の病名を根拠と共にサジェスト表示。
  - カルテや検査結果等のデータを生成AIに取込み、治療方針(医薬品・検査等)を根拠と共にレコメンド表示。



(参考) 36Kr Japan『医療用大規模言語モデル「MedGPT」、中国企業が発表 問診・検査から正確な診断導く』(2024年6月参照)

2. 生成AIの各ユースケースの概要・リスク・対策例

②診察・診断支援で想定されるリスク・対策例

- 前頁に示すユースケースにおいて、想定されるリスクとともに生成AIの利用者での対策例を以下に示します。
- なお、リスク管理を行う際に、②のユースケース特有で注意すべきポイントは以下のとおりです。
  - 組織として利用可能な生成AIを選定する際に、利用する生成AIが薬事承認を得ていることを確認。
  - 組織でのルールとして診断結果(病名や治療方針等)等の案を生成AIが作成しても、医師自身が診察して最終判断した上で、医師が患者へ説明することを規定し、職員に周知するとともに、利用者(個人)においてもこのルールを遵守。

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
1	ディープフェイク	• 問題は生じない想定。	–	–
2	不適正利用	• 問題は生じない想定。	–	–
3	正確性、信頼性	• 生成AIが提案した診察、診断結果(病名や治療方針等)の正確性が担保できない可能性がある。	• 生成AIのインプットとする問診票やカルテ等を正確に入力。 • 生成AIが提案した病名や治療方針等を医師が確認した上で、診察・診断に利用。	• 医師等に対し、左記の対策例を周知。 • 組織として利用可能な生成AIを選定する際に、サービスの正確性を評価。
4	公平性、バイアス	• 生成AIの出力に偏りがあり、患者の性別や人種等によっては適切な病名や治療方針等が提案されない可能性がある。	※「正確性、信頼性」と同じ。	• 「正確性、信頼性」と同様、医師に対し、左記の対策例を周知。 • 組織として利用可能な生成AIを選定する際に、サービスのバイアス等を評価。
5	透明性、説明責任	• 診察・診断支援に用いる場合は、処理の透明性や説明責任が求められる。	–	• 生成AIのサービス提供者に対して、品質に関する情報の開示を要求。
6	著作権（著作権法）	• 問題は生じない想定。	–	–

2. 生成AIの各ユースケースの概要・リスク・対策例

②診察・診断支援で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
7	プライバシー (個人情報保護法等)	• 医療情報(個人情報を含む)を再学習に利用される設定の生成AIに入力する場合、第三者提供となる。 • 医療情報(個人情報を含む)を患者本人の診察・診断以外の目的で利用する場合、本人同意を得なければ、個人情報保護法に違反する。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。 • 医療情報(個人情報を含む)を患者本人の診察・診断以外の目的で利用しない。	• 組織として利用可能な生成AIを選定する際に、入力データが再学習に利用されない設定となっていることを確認。 • 左記、個人での対策を利用ルールとして規定し、職員に周知。
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアでない。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。 • 利用者として求められる安全管理措置を実施。	• 組織として利用可能な生成AIとして、以下の観点等から選定し、職員へ周知。 ✓ 生成AIのサーバ等が、国内法の適用を受ける場所に設置されていること。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアであること。 ✓ (組織で保有する医療情報を提供する場合)生成AIのサービス提供者との契約や書面等で、提供する医療情報が漏えいしないよう安全管理措置がされていること、契約終了後に提供した医療情報が削除されること等。 • 左記、個人での対策を利用ルールとして規定し、職員に周知。
9	医師法	• 診断結果(病名や治療方針等)等の案を生成AIが作成しても、医師自身が診察して最終判断した上で患者へ説明しなければ、医師法に違反する。	• 診断結果(病名や治療方針等)等の案を生成AIが作成しても、医師自身が診察して最終判断した上で、医師が患者へ説明。	• 左記、個人での対策を利用ルールとして規定し、職員に周知。

2. 生成AIの各ユースケースの概要・リスク・対策例

②診察・診断支援で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
10	医療法	・生成AIを用いることで診察、診断等の業務の適正な実施が阻害された場合、医療機関は医療従事者の監督義務違反になる。	–	・組織でのルールとして、生成AIを利用した診察、診断の業務が適正に実施されるよう、医師が誤用していないかなどを定期的にチェックすることを規定。
11	医薬品医療機器等法	・生成AIの出力を患者への診断を含む医学的判断に使用する場合、医療機器プログラムとして承認されていない生成AIは、安全性・有効性等が確保できない。	・利用する生成AIが、組織として利用可能と判断されていることを確認。	・組織として利用可能な生成AIを選定する際に、利用する生成AIが薬事承認を得ていることを確認。
12	健康増進法	・問題は生じない想定。	–	–
13	人を対象とする生命科学・医学系研究に関する倫理指針	・問題は生じない想定。	–	–
14	臨床研究法	・問題は生じない想定。	–	–
15	次世代医療基盤法	・利用フェーズでは、問題は生じない想定。	–	–
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	–	・組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に対し、特許権侵害を犯していないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

②診察・診断支援で想定されるリスク・対策例

- 38頁に示すユースケースにおいて、想定されるリスクとともに生成AIの開発者での対策例を以下に示します。
- なお、リスク管理を行う際に、②のユースケース特有で注意すべきポイントは以下のとおりです。
  - 薬事承認や生成AIの利用者への説明に必要な学習データの収集・整備に関する記録・整理を実施。
  - 薬事承認を取得するため、医療機器としての安全性・有効性等が確保されていることをPMDA/登録認証機関に提示。
  - 生成AIが入力内容に基づき病名、医薬品、検査等を提案していることを医師に通知する仕様で実装。
  - 病名、医薬品、検査等の提案精度と提案根拠を併せて提示する仕様であることを生成AIの利用者に説明。

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
1	ディープフェイク	• 問題は生じない想定。	ー
2	不適正利用	• 問題は生じない想定。	ー
3	正確性、信頼性	• 生成AIが提案した診察、診断結果(病名や治療方針等)の正確性が担保できない可能性がある。	• 学習データとなる問診票、カルテ、検査結果、病名、治療に用いる医薬品、診断に用いる検査等に関するデータを正規化し、正確性、信頼性を担保。 • 学習済みモデルの正確性・信頼性を評価した上で実装。
4	公平性、バイアス	• 生成AIが性別や人種等に基づくバイアスが含まれたデータを学習することで、バイアスに基づく誤情報が出力されたり、患者の性別や人種等によって適切な病名や治療方針が提案されない可能性がある。	• 学習データに偏りやバイアスがないか評価。 • アウトプットにおいて偏りやバイアスがないか評価。
5	透明性、説明責任	• 診察・診断支援に用いる場合は、処理の透明性や説明責任が求められる。薬事承認を得るためには、これらのエビデンスが必要となる。	• 薬事承認や生成AIの利用者への説明に必要な学習データの収集・整備に関する記録・整理を実施。 • 生成AIが入力内容に基づき病名、医薬品、検査等を提案していることを医師に通知する仕様で実装。 • 病名、医薬品、検査等の提案精度と提案根拠を併せて提示する仕様であることを生成AIの利用者に説明。

2. 生成AIの各ユースケースの概要・リスク・対策例

②診察・診断支援で想定されるリスク・対策例

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
6	著作権（著作権法）	• 学習データに、診察・診断関連の他者の論文等を権利処理を行わずに無断で用いた場合、著作権の侵害となる可能性がある。	• 他者の論文等を学習に用いる場合、著作権等の権利処理を実施した上で学習に利用。
7	プライバシー (個人情報保護法等)	• 医療情報(個人情報を含む)を学習に利用する場合、本人から個人情報の削除等が求められた際に対応する必要があるが、その都度、削除したデータで学習し直すことは困難。	• 医療情報(個人情報を含む)を学習に利用する場合は、仮名加工情報、匿名加工情報に加工し、個人情報保護法等で規定された取り扱いを遵守。
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアでない。	• 3省2ガイドラインに準拠するよう、以下の対策等を実施。 ✓ 医療情報を保管するサーバ等を国内法の適用を受ける場所に設置。 ✓ 3省2ガイドラインで求められる技術基準に則した安全管理措置を実施(医療機関・薬局等と生成AIを接続するネットワークをセキュアとすることを含む)。
9	医師法	• 開発フェーズでは問題は生じない想定。	–
10	医療法	• 開発フェーズでは問題は生じない想定。	–
11	医薬品医療機器等法	• 生成AIの出力を患者への診断を含む医学的判断に使用する場合、医療機器プログラムとして承認されていない生成AIは、安全性・有効性等が確保できない。	• 薬事承認に必要となる学習データの収集・整備に関する記録・整理を実施。 • 薬事承認を取得するため、医療機器としての安全性・有効性等が確保されていることをPMDA/登録認証機関に提示。
12	健康増進法	• 問題は生じない想定。	–
13	人を対象とする生命科学・医学系研究に関する倫理指針	• 問題は生じない想定。	–
14	臨床研究法	• 問題は生じない想定。	–

2. 生成AIの各ユースケースの概要・リスク・対策例

②診察・診断支援で想定されるリスク・対策例

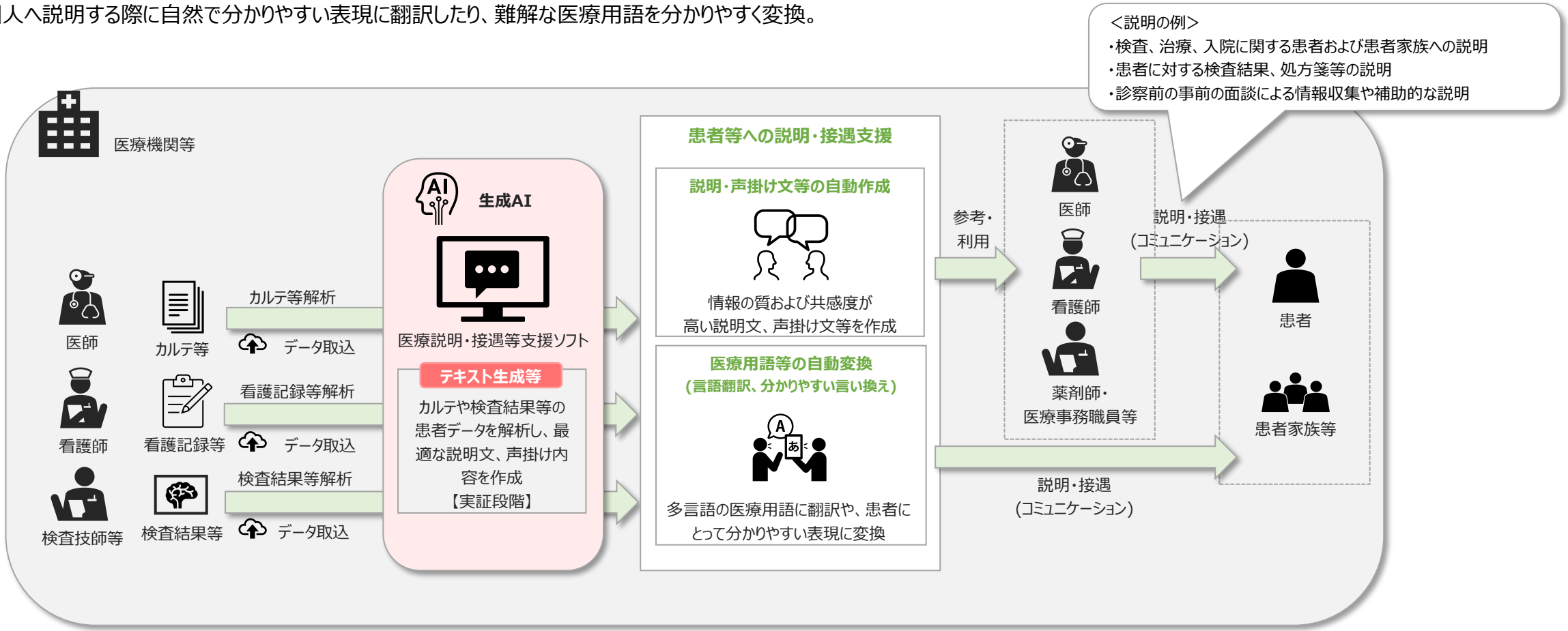
【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
15	次世代医療基盤法	・学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、匿名加工医療情報や仮名加工医療情報を法で定められた取り扱いをしなければ次世代医療基盤法に違反する。	・学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、次世代医療基盤法で規定された取り扱いを遵守。
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	・データの処理方法や生成AIの開発工程等に関して特許調査を行い、特許権の侵害が生じないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

③患者等への説明・接遇支援(患者等とのコミュニケーション支援)の概要

- 患者等への説明等を生成AIを用いて以下のように支援することで、業務効率化や医療の質の向上が期待できます。
  - カルテ等のデータを生成AIに取込み、医師が患者へ説明する際に最適な説明文等を作成し、患者等への説明に利用。
  - 外国人へ説明する際に自然で分かりやすい表現に翻訳したり、難解な医療用語を分かりやすく変換。



(参考) AI Market『医師向け臨床支援アプリ「HOKUTO」、GPT-4を利用した試験的機能「患者への説明文生成AI」を導入開始』(2024年6月参照)

2. 生成AIの各ユースケースの概要・リスク・対策例

③患者等への説明・接遇支援(患者等とのコミュニケーション支援)で想定されるリスク・対策例

- 前頁に示すユースケースにおいて、想定されるリスクとともに生成AIの利用者での対策例を以下に示します。
- なお、リスク管理を行う際に、③のユースケース特有で注意すべきポイントは以下のとおりです。
  - 組織でのルールとして以下を規定し、職員に周知するとともに、利用者(個人)においてもこのルールを遵守。
    - ✓ 服薬指導に関する情報を生成AIが出力する場合、薬剤師が説明や服薬指導を実施。
    - ✓ 患者の疾患管理のための栄養指導等に関する情報を生成AIが出力する場合、医療従事者等が確認・修正した上で指導。

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
1	ディープフェイク	• 問題は生じない想定。	–	–
2	不適正利用	• 問題は生じない想定。	–	–
3	正確性、信頼性	• 生成AIが生成する説明・声掛け文等に含まれる検査、治療、検査結果、処方箋等に関する説明内容が、正確性に欠けたり、虚偽が混在したりする可能性がある。 • 翻訳等の自動変換後の内容が、変換前と異なる内容となる可能性がある。	• 生成AIのインプットとするカルテや看護記録等を正確に入力。 • 出力された説明・声掛け文等を医療従事者が確認した上で利用。	• 職員に対し、左記の対策を周知。 • 組織として利用可能な生成AIを選定する際に、サービスの正確性を評価。
4	公平性、バイアス	• 問題は生じない想定。	–	–
5	透明性、説明責任	• 患者への説明を医療従事者ではなく生成AIを用いて直接行う場合、生成AIであることを通知しないと、人と誤解することで問題が生じる可能性がある。	• アウトプットをそのまま用いる場合は、生成AIが出力したものであることを患者等に通知。	• 生成AIのサービス提供者に対して、品質に関する情報の開示を要求。

2. 生成AIの各ユースケースの概要・リスク・対策例

③患者等への説明・接遇支援(患者等とのコミュニケーション支援)で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
6	著作権（著作権法）	• 生成AIで作成する患者等への説明資料に、著作権を侵害するイラストや図が含まれる危険性がある。	• 既存の著作物に類似する文章・イラスト等の生成につながるプロンプトを入力しない。 • 権利処理がされていない既存の著作物等を無断で入力に利用しない。 • 生成AIが出力した内容が既存の著作物等に類似していないことを確認。	• 左記、個人での対策を利用ルールとして規定し、職員に周知。
7	プライバシー (個人情報保護法等)	• 患者等への説明・接遇支援では、医療情報(個人情報を含む)を入力データに利用する可能性が高く、再学習に利用される設定の生成AIに入力する場合、第三者提供となる。 • 患者への説明を医療従事者ではなく生成AIを用いて直接行う場合、個人情報を取得する際にその用途等を説明しなければ、患者が不信感を抱く可能性がある。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。 • 患者への説明を医療従事者ではなく生成AIを用いて直接行う場合、個人情報を取得する際にその旨を患者に説明。	• 組織として利用可能な生成AIを選定する際に、入力データが再学習に利用されない設定となっていることを確認。 • 左記、個人での対策を職員に周知。
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークが、セキュアでない。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。 • 組織でのルールに従い、利用者として求められる安全管理措置を実施。	• 組織として利用可能な生成AIとして、以下の観点等から選定し、職員へ周知。 ✓ 生成AIのサーバ等が、国内法の適用を受ける場所に設置されていること。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアであること。 ✓ (組織で保有する医療情報を提供する場合)生成AIのサービス提供者との契約や書面等で、提供する医療情報が漏えいしないよう安全管理措置がされていること、契約終了後に提供した医療情報が削除されること等。 • 左記、個人での対策を利用ルールとして規定し、職員に周知。

2. 生成AIの各ユースケースの概要・リスク・対策例

③患者等への説明・接遇支援(患者等とのコミュニケーション支援)で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
9	医師法	• 問題は生じない想定。	–	–
10	医療法	• 生成AIを用いることで業務の適正な実施が阻害された場合、医療機関は医療従事者の監督義務違反になる。	–	• 組織でのルールとして、生成AIを利用した業務が適正に実施されるよう、医療従事者が誤用していないかなどを定期的にチェックすることを規定。
11	医薬品医療機器等法	• 服薬指導に関する情報を生成AIが出力する場合、服薬指導は薬剤師が実施しなければ、医薬品医療機器等法に違反する。 • 患者への説明・接遇支援という点では診断等に該当しないため、医療機器プログラムには該当しない。	• 服薬指導に関する情報を生成AIが出力する場合、薬剤師が説明や服薬指導を実施。	• 左記、個人での対策を利用ルールとして規定し、職員に周知。
12	健康増進法	• 患者の疾患管理のための栄養指導等に関する情報を生成AIが出力する場合、医療従事者等が確認・修正等を行わずに患者へ説明してしまうと、健康増進法に違反する可能性がある。	• 患者の疾患管理のための栄養指導等に関する情報を生成AIが出力する場合、医療従事者等が確認・修正した上で指導。	• 左記、個人での対策を利用ルールとして規定し、職員に周知。
13	人を対象とする生命科学・医学系研究に関する倫理指針	• 問題は生じない想定。	–	–
14	臨床研究法	• 問題は生じない想定。	–	–
15	次世代医療基盤法	• 利用フェーズでは、問題は生じない想定。	–	–
16	特許法	• データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	–	• 組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に対し、特許権侵害を犯していないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

③患者等への説明・接遇支援(患者等とのコミュニケーション支援)で想定されるリスク・対策例

- 45頁に示すユースケースにおいて、想定されるリスクとともに生成AIの開発者での対策例を以下に示します。
- なお、リスク管理を行う際に、③のユースケース特有で注意すべきポイントは以下のとおりです。
  - 生成AIが出力した説明・声掛け文や翻訳結果をそのまま患者等に提示される場合に備え、AIが出力したものであることを示す仕様で実装。

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
1	ディープフェイク	• 問題は生じない想定。	–
2	不適正利用	• 問題は生じない想定。	–
3	正確性、信頼性	• 生成AIが生成する説明・声掛け文等に含まれる検査、治療、検査結果、処方箋等に関する説明内容が、正確性に欠けたり、虚偽が混在したりする可能性がある。 • 翻訳等の自動変換後の内容が、変換前と異なる内容となる可能性がある。	• 学習データとなるカルテ、看護記録、検査結果等に関するデータを正規化し、正確性、信頼性を担保。 • 学習済みモデルの正確性・信頼性を評価した上で実装。
4	公平性、バイアス	• 問題は生じない想定。	–
5	透明性、説明責任	• 医療従事者が直接説明しない場合、生成AIを介して患者に分かり易く説明していることを患者に通知していない場合、生成AIが間違った説明をしてしまうとさらなる問題につながる可能性がある。	• 生成AIが出力した説明・声掛け文や翻訳結果をそのまま患者等に提示される場合に備え、AIが出力したものであることを示す仕様で実装。
6	著作権（著作権法）	• 生成AIで作成する患者等への説明資料に、著作権を侵害するイラストや図が含まれる危険性がある。 • 著作権を侵害する出力が行われる場合、著作物の学習自体が著作権法違反になる可能性がある。	• イラスト等を生成するAIを開発する場合、著作権フリーの画像等、著作権等の権利処理がなされたデータを学習に利用。 • イラスト等を生成するAIを開発する場合、学習したデータをそのまま、あるいは類似した形でアウトプットしないような形で開発。

2. 生成AIの各ユースケースの概要・リスク・対策例

③患者等への説明・接遇支援(患者等とのコミュニケーション支援)で想定されるリスク・対策例

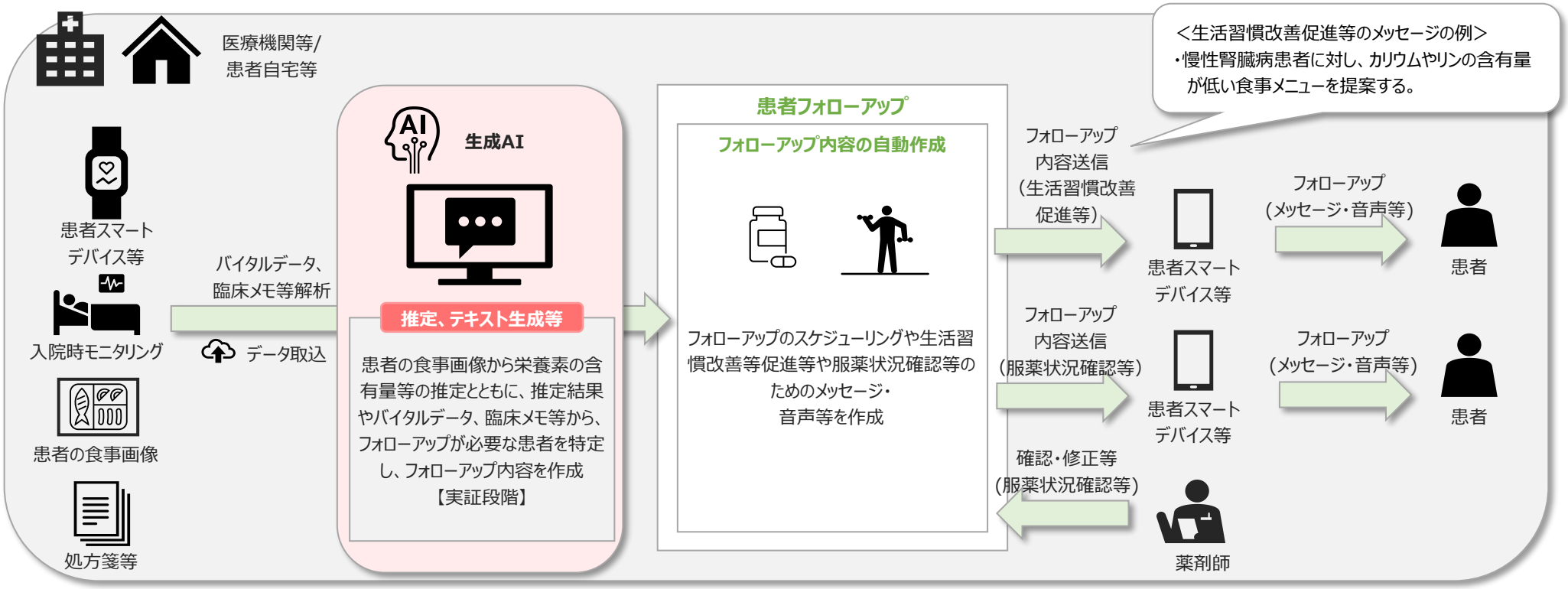
【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
7	プライバシー (個人情報保護法等)	• 医療情報(個人情報を含む)を学習に利用する場合、本人から個人情報の削除等が求められた際に対応する必要があるが、その都度、削除したデータで学習し直すことは困難。	• 医療情報(個人情報を含む)を学習に利用する場合は、仮名加工情報、匿名加工情報に加工し、個人情報保護法等で規定された取り扱いを遵守。
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークが、セキュアでない。	• 3省2ガイドラインに遵守するよう、以下の対策等を実施。 ✓ 医療情報を保管するサーバ等を国内法の適用を受ける場所に設置。 ✓ 3省2ガイドラインで求められる技術基準に則した安全管理措置を実施(医療機関・薬局等と生成AIを接続するネットワークをセキュアとすることを含む)。
9	医師法	• 問題は生じない想定。	–
10	医療法	• 開発フェーズでは問題は生じない想定。	–
11	医薬品医療機器等法	• 開発フェーズでは問題は生じない想定。	–
12	健康増進法	• 開発フェーズでは問題は生じない想定。	–
13	人を対象とする生命科学・医学系研究に関する倫理指針	• 問題は生じない想定。	–
14	臨床研究法	• 問題は生じない想定。	–
15	次世代医療基盤法	• 学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、匿名加工医療情報や仮名加工医療情報を法で定められた取り扱いをしなければ次世代医療基盤法に違反する。	• 学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、次世代医療基盤法で規定された取り扱いを遵守。
16	特許法	• データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	• データの処理方法や生成AIの開発工程等に関して特許調査を行い、特許権の侵害が生じないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

④患者フォローアップ支援の概要

- 生成AIを用いて以下のように患者へのフォローアップを支援することで、医療の質の向上等が期待できます。
  - スマートデバイスや入院時モニタリングによる患者のバイタルデータや臨床メモ等を生成AIに取込み、患者の生活習慣改善促進等のフォローアップに活用できるメッセージ・音声等を作成。
  - 処方箋等を生成AIに取込み、服薬状況確認のためのフォローアップメッセージ案を作成し、薬剤師が内容を確認して患者へ送信。



(参考) Health Biz Watch『Generative AI（生成AI）の行動継続への活用』(2024年6月参照)
PRTIMES『医療AIカンパニーMG-DX、薬剤師の対人業務をサポートする次世代薬局ソリューション「AI薬師®」において大規模言語モデルの活用を開始』(2024年6月参照)

2. 生成AIの各ユースケースの概要・リスク・対策例

④患者フォローアップ支援で想定されるリスク・対策例

- 前頁に示すユースケースにおいて、想定されるリスクとともに生成AIの利用者での対策例を以下に示します。
- なお、リスク管理を行う際に、④のユースケース特有で注意すべきポイントは以下のとおりです。
  - 組織でのルールとして以下を規定し、職員に周知するとともに、利用者(個人)においてもこのルールを遵守。
    - ✓ 服薬状況確認のためのフォローアップ内容を生成AIが作成する場合、薬剤師が確認・修正した上で患者へ送信。
    - ✓ 患者の疾患管理のための栄養指導等に関する内容を含んだフォローアップ内容を生成AIが作成する場合、医療従事者等が確認・修正した上で患者へ送信。

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
1	ディープフェイク	• 問題は生じない想定。	–	–
2	不適正利用	• 問題は生じない想定。	–	–
3	正確性、信頼性	• 生成AIが出力するフォローアップ対象者やその内容が、医師の治療方針や患者の状態に合わないものとなる可能性がある。	• 生成AIのインプットとする臨床メモや処方箋等を正確に入力。 • 出力されたフォローアップ対象者やその内容を医療従事者が確認した上で利用。	• 職員に対し、左記の対策を周知。 • 組織として利用可能な生成AIを選定する際に、サービスの正確性を評価。
4	公平性、バイアス	• 生成AIの出力に偏りがあり、フォローアップが必要な患者が抽出されなかったり、フォローアップ内容が患者の状態に合わないものとなる可能性がある。	※「正確性、信頼性」と同じ。	• 「正確性、信頼性」と同様、職員に対し、左記の対策例を周知。 • 組織として利用可能な生成AIを選定する際に、サービスのバイアス等を評価。
5	透明性、説明責任	• 患者のフォローアップを生成AIが行う場合、生成AIであることを通知しないと、人と誤解することで問題が生じる可能性がある。	• 患者のフォローアップを生成AIが行う場合、生成AIがフォローアップしていることを患者に通知。	• 生成AIのサービス提供者に対して、品質に関する情報の開示を要求。

2. 生成AIの各ユースケースの概要・リスク・対策例

④患者フォローアップ支援で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
6	著作権（著作権法）	• 生成AIで作成した服薬状況確認や生活習慣改善等促進等のメッセージに、著作権を侵害するイラストや図が含まれる危険性がある。	• 既存の著作物に類似する文章・イラスト等の生成につながるプロンプトを入力しない。 • 権利処理がされていない既存の著作物等を無断で入力に利用しない。 • 生成AIが出力した内容が既存の著作物等に類似していないことを確認。	• 左記、個人での対策を利用ルールとして規定し、職員に周知。
7	プライバシー (個人情報保護法等)	• 医療情報(個人情報を含む)を再学習に利用される設定の生成AIに入力する場合、第三者提供となる。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。	• 組織として利用可能な生成AIを選定する際に、入力データが再学習に利用されない設定となっていることを確認。
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークが、セキュアでない。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。 • 組織でのルールに従い、利用者として求められる安全管理措置を実施。	• 組織として利用可能な生成AIとして、以下の観点等から選定し、職員へ周知。 ✓ 生成AIのサーバ等が、国内法の適用を受ける場所に設置されていること。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアであること。 ✓ (組織で保有する医療情報を提供する場合)生成AIのサービス提供者との契約や書面等で、提供する医療情報が漏えいしないよう安全管理措置がされていること、契約終了後に提供した医療情報が削除されること等。 • 左記、個人での対策を利用ルールとして規定し、職員に周知。

2. 生成AIの各ユースケースの概要・リスク・対策例

④患者フォローアップ支援で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
9	医師法	・問題は生じない想定。	–	–
10	医療法	・生成AIを用いることで業務の適正な実施が阻害された場合、医療機関は医療従事者の監督義務違反になる。	–	・組織でのルールとして、業務が適正に実施されるよう、医療従事者が誤用していないかなどを定期的にチェックすることを規定し、職員に周知。
11	医薬品医療機器等法	・服薬状況確認のフォローアップ内容を生成AIが作成する場合、薬剤師が確認した上で患者へ送信しなければ、医薬品医療機器等法に違反する可能性がある。	・服薬状況確認のためのフォローアップ内容を生成AIが作成する場合、薬剤師が確認・修正した上で患者へ送信。	・左記、個人での対策を利用ルールとして規定し、職員に周知。
12	健康増進法	・患者の疾患管理のための栄養指導等に関する内容を含んだフォローアップ内容を生成AIが作成する場合、医療従事者等が確認・修正等した上で患者へ送信しなければ、健康増進法に違反する可能性がある。	・患者の疾患管理のための栄養指導等に関する内容を含んだフォローアップ内容を生成AIが作成する場合、医療従事者等が確認・修正した上で患者へ送信。	・左記、個人での対策を利用ルールとして規定し、職員に周知。
13	人を対象とする生命科学・医学系研究に関する倫理指針	・問題は生じない想定。	–	–
14	臨床研究法	・問題は生じない想定。	–	–
15	次世代医療基盤法	・利用フェーズでは、問題は生じない想定。	–	–
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	–	・組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に対し、特許権侵害を犯していないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

④患者フォローアップ支援で想定されるリスク・対策例

- 51頁に示すユースケースにおいて、想定されるリスクとともに生成AIの開発者での対策例を以下に示します。
- なお、リスク管理を行う際に、④のユースケース特有で注意すべきポイントは以下のとおりです。
  - 患者のフォローアップを生成AIが行う場合、生成AIがフォローアップしていることを示す仕様で実装。
  - 服薬状況確認のためのフォローアップ内容を生成AIが作成する場合、薬剤師が確認した上で患者に送信する仕様で実装。
    - ✓ 患者の疾患管理のための栄養指導等に関する情報を生成AIが出力する場合、医療従事者等が確認・修正した上で指導。

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
1	ディープフェイク	• 問題は生じない想定。	–
2	不適正利用	• 問題は生じない想定。	–
3	正確性、信頼性	• 生成AIが出力するフォローアップ対象者やその内容が、医師の治療方針や患者の状態に合わないものとなる可能性がある。	• 学習データとなるバイタルデータ、臨床メモ等に関するデータを正規化し、正確性、信頼性を担保。 • 学習済みモデルの正確性・信頼性を評価した上で実装。
4	公平性、バイアス	• 生成AIが性別や人種等に基づくバイアスが含まれたデータを基に学習することで、出力内容にバイアスがかかり、フォローアップが必要な患者が抽出されなかったり、フォローアップ内容が患者の状態に合わないものとなる可能性がある。	• 学習データに偏りやバイアスがないか評価。 • 学習済みモデルのアウトプットにおいて偏りやバイアスがないか評価。
5	透明性、説明責任	• 患者のフォローアップを生成AIが行う場合、生成AIであることを通知しないと、人と誤解することで問題が生じる可能性がある。	• 患者のフォローアップを生成AIが行う場合、生成AIがフォローアップしていることを示す仕様で実装。
6	著作権（著作権法）	• 生成AIで作成した服薬状況確認や生活習慣改善等促進等のメッセージに、著作権を侵害するイラストや図が含まれる危険性がある。 • 著作権を侵害する出力が行われる場合、著作物の学習自体が著作権法違反になる可能性がある。	• イラスト等を生成するAIを開発する場合、著作権フリーの画像等、著作権等の権利処理がなされたデータを学習に利用。 • イラスト等を生成するAIを開発する場合、学習したデータをそのまま、あるいは類似した形でアウトプットしないような形で開発。

2. 生成AIの各ユースケースの概要・リスク・対策例

④患者フォローアップ支援で想定されるリスク・対策例

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
7	プライバシー (個人情報保護法等)	• 医療情報(個人情報を含む)を学習に利用する場合、本人から個人情報の削除等が求められた際に対応する必要があるが、その都度、削除したデータで学習し直すことは困難。	• 医療情報(個人情報を含む)を学習に利用する場合は、仮名加工情報、匿名加工情報に加工し、個人情報保護法等で規定された取り扱いを遵守。
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークが、セキュアでない。	• 3省2ガイドラインに遵守するよう、以下の対策等を行う。 ✓ 医療情報を保管するサーバ等を国内法の適用を受ける場所に設置。 ✓ 3省2ガイドラインで求められる技術基準に則した安全管理措置を実施(医療機関・薬局等と生成AIを接続するネットワークをセキュアとすることを含む)。
9	医師法	• 問題は生じない想定。	–
10	医療法	• 開発フェーズでは問題は生じない想定。	–
11	医薬品医療機器等法	• 服薬状況確認のフォローアップ内容を生成AIが作成しても、薬剤師が確認した上で患者へ送信しなければ、医薬品医療機器等法に違反する可能性がある。	• 服薬状況確認のためのフォローアップ内容を生成AIが作成する場合、薬剤師が確認した上で患者に送信する仕様で実装。
12	健康増進法	• 開発フェーズでは問題は生じない想定。	–
13	人を対象とする生命科学・医学系研究に関する倫理指針	• 問題は生じない想定。	–
14	臨床研究法	• 問題は生じない想定。	–

2. 生成AIの各ユースケースの概要・リスク・対策例

④患者フォローアップ支援で想定されるリスク・対策例

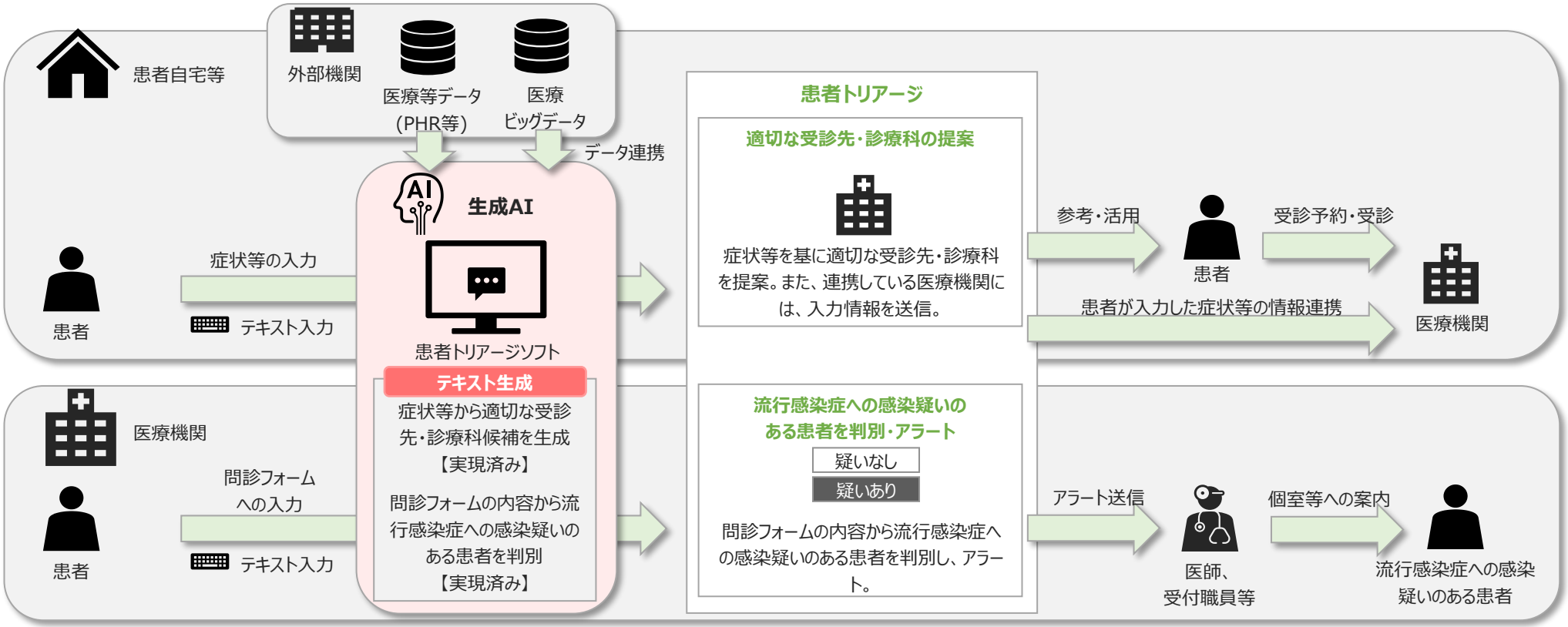
【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
15	次世代医療基盤法	・学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、匿名加工医療情報や仮名加工医療情報を法で定められた取り扱いをしなければ次世代医療基盤法に違反する。	・学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、次世代医療基盤法で規定された取り扱いを遵守。
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	・データの処理方法や生成AIの開発工程等に関して特許調査を行い、特許権の侵害が生じないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑤患者トリアージの概要

- 患者トリアージを生成AIを用いて以下のように支援することで、業務効率化や院内感染予防等が期待できます。
  - 医療機関が提供するWeb問診フォーム等に患者が入力した症状等を生成AIに取込み、適切な受診先・診療科を提案することで、適切な医療機関での早期受診を促進。
  - 医療機関に来院した患者が自身のスマートフォンや医療機関が貸し出すタブレットを用いて入力した問診フォームの内容を基に、流行感染症への感染疑いを判別し、疑いのある患者を医師等にアラートすることで、院内感染リスクを低減。



(参考) ユビー『ユビーのサービスについて』(2024年6月参照)
ユビー『「AI問診Ubie」が院内感染対策としてCOVID-19トリアージシステムを拡張し、全国の医療機関に提供開始』(2024年6月参照)

2. 生成AIの各ユースケースの概要・リスク・対策例

⑤患者トリアージで想定されるリスク・対策例

- 前頁に示すユースケースにおいて、想定されるリスクとともに、生成AIの利用者での対策例を以下に示します。
- なお、リスク管理を行う際に、⑤のユースケース特有で注意すべきポイントは以下のとおりです。
  - 組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に以下を確認。
    - ✓ 受診先・診療科候補等の提案精度。
    - ✓ 提案や判断の根拠を提示する仕様となっていること。
  - 医師等は、患者が医療機関に来院した際に、トリアージの経緯等を確認し、診察・診断を実施。
  - 患者にできるだけ正確に情報を入力するよう注意喚起。

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
1	ディープフェイク	• 問題は生じない想定。	–	–
2	不適正利用	• 問題は生じない想定。	–	–
3	正確性、信頼性	• 生成AIが出力した受診先、診療科等の内容において、正確性が欠けたり、虚偽の記載が混在する可能性がある。	• 医師は、患者が医療機関に来院した際に、トリアージの経緯等を確認し、診察・診断を実施。 • 医師等は、生成AIによる感染疑いの判別結果は正確性に欠ける可能性があることを認識し、必要に応じて患者の様子等の他の情報も活用し、個室への案内要否を判断。	• 患者にできるだけ正確に情報を入力するよう注意喚起。 • 職員に対し、左記の対策を周知。 • 組織として利用可能な生成AIを選定する際に、サービスの正確性を評価。
4	公平性、バイアス	• 生成AIの出力に偏りがあり、患者の性別や人種等によっては適切な受診先、診療科等が提案されない可能性がある。	※「正確性、信頼性」と同じ。	• 「正確性、信頼性」と同様、職員に対し、左記の対策例を周知。 • 組織として利用可能な生成AIを選定する際に、サービスのバイアス等を評価。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑤患者トリアージで想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
5	透明性、説明責任	・患者の受診先・診療科候補等を提案した根拠がないと患者にとって重要な健康等のリスクに結びつく危険性がある。	―	・組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に以下を確認。 ✓ 受診先・診療科候補等の提案精度。 ✓ 提案や判断の根拠を提示する仕様となっていること。
6	著作権（著作権法）	・問題は生じない想定。	―	―
7	プライバシー (個人情報保護法等)	・患者トリアージでは、個人情報を入力データに利用する可能性が高く、再学習に利用される設定の生成AIに入力する場合、第三者提供となる。 ・生成AIのサーバ等が国内法の適用を受けない場所に設置されている場合、個人情報を入力する際に、本人同意を得なければ個人情報保護法に違反する。	・利用する生成AIが、組織として利用可能と判断されていることを確認。	・組織として利用可能な生成AIを選定する際に、入力データが再学習に利用されない設定となっていることを確認。
8	セキュリティ (3省2ガイドライン等)	・患者が入力する情報は医療情報に該当しないため、3省2ガイドラインの対象外となる。 ・一方で、患者が入力する情報は個人情報となり、適切な安全管理措置を行わない場合、情報漏えい等が生じる可能性がある。	・組織でのルールに従い、利用者として求められる安全管理措置を実施。 ※その他、「プライバシー(個人情報保護法等)」と同じ。	・左記、個人での対策を利用ルールとして規定し、職員に周知。 ※その他、「プライバシー(個人情報保護法等)」と同じ。
9	医師法	・問題は生じない想定。	―	―
10	医療法	・問題は生じない想定。	―	―
11	医薬品医療機器等法	・患者トリアージの支援という点では診断等に該当しないため、医療機器プログラムには該当しない。	―	―

2. 生成AIの各ユースケースの概要・リスク・対策例

⑤患者トリアージの概要

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
12	健康増進法	・問題は生じない想定。	–	–
13	人を対象とする生命科学・医学系研究に関する倫理指針	・問題は生じない想定。	–	–
14	臨床研究法	・問題は生じない想定。	–	–
15	次世代医療基盤法	・利用フェーズでは、問題は生じない想定。	–	–
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	–	・組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に対し、特許権侵害を犯していないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑤患者トリアージで想定されるリスク・対策例

- 58頁に示すユースケースにおいて、想定されるリスクとともに生成AIの開発者での対策例を以下に示します。
- なお、リスク管理を行う際に、⑤のユースケース特有で注意すべきポイントは以下のとおりです。
  - 受診先・診療科候補等の提案精度と提案根拠を併せて提示する仕様であることをサービス利用者となる患者に説明。
  - 生成AIが入力内容に基づき受診先・診療科候補等を提案していることを患者に通知する仕様で実装。
  - 感染疑いの判別精度と判別根拠を併せて提示する仕様であることをサービス利用者となる医療機関等に説明。

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
1	ディープフェイク	• 問題は生じない想定。	–
2	不適正利用	• 問題は生じない想定。	–
3	正確性、信頼性	• 生成AIが出力した受診先、診療科等の内容において、正確性が欠けたり、虚偽の記載が混在する可能性がある。	• 学習データとなる症状、病名、受診先候補等に関するデータを正規化し、正確性、信頼性を担保。 • 学習済みモデルの正確性・信頼性を評価した上で実装。
4	公平性、バイアス	• 生成AIが性別や人種等に基づくバイアスが含まれたデータを基に学習することで、生成AIを利用する患者の性別や人種等によっては適切な受診先、診療科等が提案されない可能性がある。	• 学習データに偏りやバイアスがないか評価。 • 学習済みモデルのアウトプットにおいて偏りやバイアスがないか評価。
5	透明性、説明責任	• 患者の受診先・診療科候補等を提案した根拠がないと患者にとって重要な健康等のリスクに結びつく危険性がある。 • 人間が応答していると誤解を招くUIであった場合、サービスを利用する患者からクレームが入る可能性がある。	• 受診先・診療科候補等の提案精度と提案根拠を併せて提示する仕様であることをサービス利用者となる患者に説明。 • 生成AIが入力内容に基づき受診先・診療科候補等を提案していることを患者に通知する仕様で実装。 • 感染疑いの判別精度と判別根拠を併せて提示する仕様であることをサービス利用者となる医療機関等に説明。
6	著作権（著作権法）	• 問題は生じない想定。	–

2. 生成AIの各ユースケースの概要・リスク・対策例

⑤患者トリアージで想定されるリスク・対策例

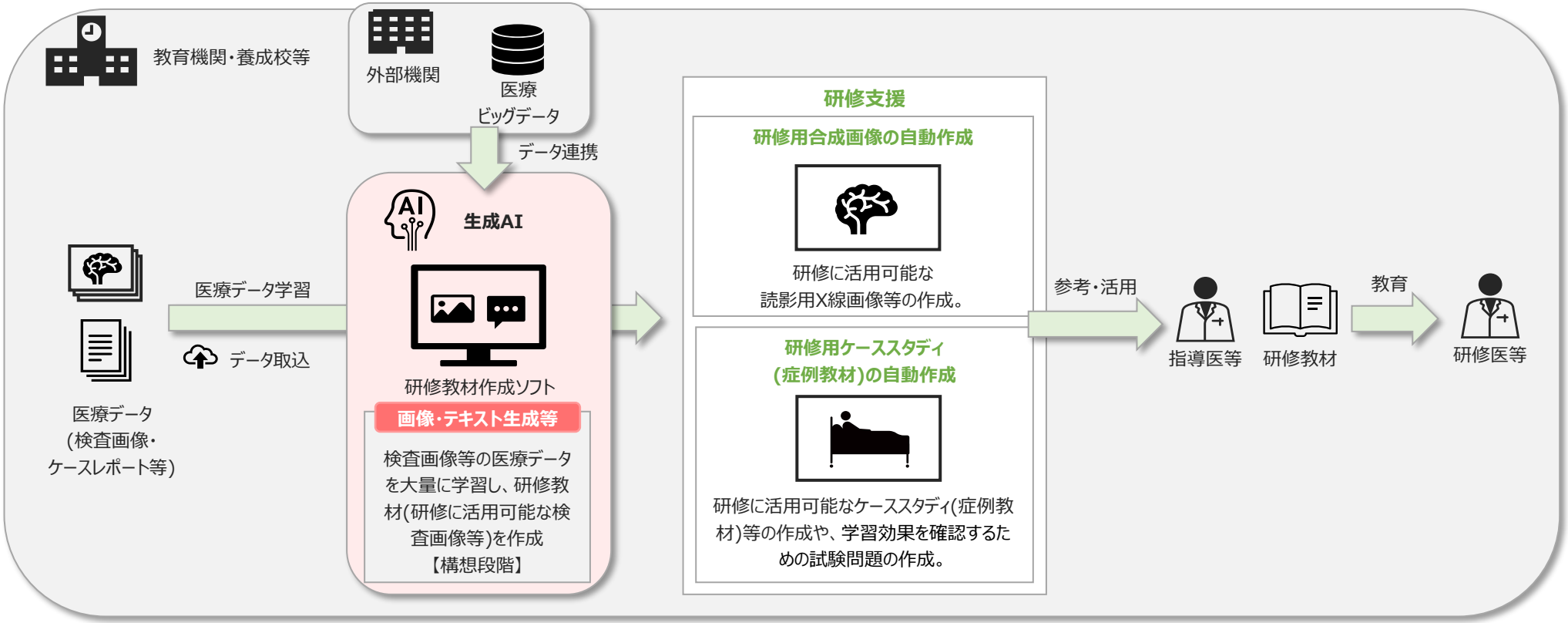
【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
7	プライバシー (個人情報保護法等)	・個人情報を学習に利用する場合、本人から個人情報の削除等が求められた際に対応する必要があるが、その都度、削除したデータで学習し直すことは困難。 ・生成AIのサーバ等が国内法の適用を受けない場所に設置されている場合、個人情報を学習に利用する際に本人同意が必要となる。	・個人情報を学習に利用する場合は、仮名加工情報、匿名加工情報に加工し、個人情報保護法等で規定された取り扱いを遵守。 ・個人情報を学習に利用する場合は、生成AIのサーバ等を国内法の適用を受ける場所に設置すること、又は、生成AIのサーバ等を国内法の適用を受けない場所に設置する際は本人同意を得る。
8	セキュリティ (3省2ガイドライン等)	・患者が入力する情報は医療情報に該当しないため、学習でも医療情報を利用しない場合は、3省2ガイドラインの対象外となる。 ・一方で、患者等が利用時に入力する情報は個人情報となり、適切な安全管理措置を行わない場合、情報漏えい等のリスクがある。	・個人情報の漏えい等が生じないよう、適切に安全管理措置を実施。 ※その他、「プライバシー(個人情報保護法等)」と同じ。
9	医師法	・問題は生じない想定。	―
10	医療法	・問題は生じない想定。	―
11	医薬品医療機器等法	・患者トリアージの支援という点では診断等に該当しないため、医療機器プログラムには該当しない。	―
12	健康増進法	・問題は生じない想定。	―
13	人を対象とする生命科学・医学系研究に関する倫理指針	・問題は生じない想定。	―
14	臨床研究法	・問題は生じない想定。	―
15	次世代医療基盤法	・学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、匿名加工医療情報や仮名加工医療情報を法で定められた取り扱いをしなければ次世代医療基盤法に違反する。	・学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、次世代医療基盤法で規定された取り扱いを遵守。
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	・データの処理方法や生成AIの開発工程等に関して特許調査を行い、特許権の侵害が生じないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑥研修支援の概要

- 研修業務を生成AIを用いて以下のように支援することで、業務効率化や研修の質の向上等が期待できます。
  - 検査画像等の医療データを生成AIに大量に取込んで学習し、利用者が生成AIに入力した指示に応じて検査合成画像やケーススタディ文等を作成し、研修教材に活用。



(参考) Deloitte Japan『生成AIにより業務を効率化して、迅速な結果と具体的な利益を生みだす』(2024年3月参照)

2. 生成AIの各ユースケースの概要・リスク・対策例

⑥研修支援で想定されるリスク・対策例

- 前頁に示すユースケースにおいて、想定されるリスクとともに、生成AIの利用者での対策例を以下に示します。

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは無いため、いずれも黒字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
1	ディープフェイク	• 問題は生じない想定。	–	–
2	不適正利用	• 問題は生じない想定。	–	–
3	正確性、信頼性	• 研修教材において正確性が欠けたり、虚偽の記載が混在する可能性がある。	• 生成AIに入力する内容(教材とする疾病名や検査画像の種類等)を正確に記載する。 • 生成AIが作成した研修用画像やケーススタディ等を医師等が確認した上で利用。	• 医師等に対し、左記の対策を周知する。 • 組織として利用可能な生成AIを選定する際に、サービスの正確性評価を行う。
4	公平性、バイアス	• 生成AIが性別や人種等に基づくバイアスが含まれたデータを基に学習することで、バイアスに基づく誤情報を含んだ症例教材を生成する可能性がある。	※「正確性、信頼性」と同じ。	• 組織として利用可能な生成AIを選定する際に、サービスのバイアス等を確認。 ※その他、「正確性、信頼性」と同じ。
5	透明性、説明責任	• 問題は生じない想定。	–	–
6	著作権（著作権法）	• 生成AIで作成する研修教材に、著作権を侵害するイラストや図が含まれる危険性がある。	• 既存の著作物に類似する文章・イラスト等の生成につながるプロンプトを入力しない。 • 権利処理がされていない既存の著作物等を無断で入力に利用しない。 • 生成AIが出力した内容が既存の著作物等に類似していないことを確認。	• 左記、個人での対策を利用ルールとして規定し、職員に周知。
7	プライバシー (個人情報保護法等)	• 問題は生じない想定。	–	–

2. 生成AIの各ユースケースの概要・リスク・対策例

⑥研修支援で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは無いため、いずれも黒字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
8	セキュリティ (3省2ガイドライン等)	・医療情報に該当しない検査画像等のデータのみを生成AIの学習に用いる場合は、3省2ガイドラインの対象外となる。	・利用者として求められる安全管理措置を実施。	・左記、個人での対策を利用ルールとして規定し、職員に周知。
9	医師法	・問題は生じない想定。	―	―
10	医療法	・問題は生じない想定。	―	―
11	医薬品医療機器等法	・研修支援という点では診断等に該当しないため、医療機器プログラムには該当しない。	―	―
12	健康増進法	・問題は生じない想定。	―	―
13	人を対象とする生命科学・医学系研究に関する倫理指針	・問題は生じない想定。	―	―
14	臨床研究法	・問題は生じない想定。	―	―
15	次世代医療基盤法	・問題は生じない想定。	―	―
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	―	・組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に対し、特許権侵害を犯していないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑥研修支援で想定されるリスク・対策例

- 64頁に示すユースケースにおいて、想定されるリスクとともに生成AIの開発者での対策例を以下に示します。

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは無いため、いずれも黒字で記載。

#	リスクの観点	リスクの内容	対策例
1	ディープフェイク	• 問題は生じない想定。	–
2	不適正利用	• 問題は生じない想定。	–
3	正確性、信頼性	• 研修教材において正確性が欠けたり、虚偽の記載が混在する可能性がある。	• 学習データとなる症状、病名、受診先候補等に関するデータを正規化し、正確性、信頼性を担保。 • 学習済みモデルの正確性・信頼性を評価した上で実装。
4	公平性、バイアス	• 生成AIが性別や人種等に基づくバイアスが含まれたデータを基に学習することで、バイアスに基づく誤情報を含んだ症例教材を生成する可能性がある。	• 学習データに偏りやバイアスがないか評価。 • 学習済みモデルのアウトプットにおいて偏りやバイアスがないか評価。
5	透明性、説明責任	• 問題は生じない想定。	–
6	著作権（著作権法）	• 著作権を侵害する出力が行われる場合、著作物の学習自体が著作権法違反になる可能性がある。 • 生成AIで作成する研修教材に、著作権を侵害するイラストや図が含まれる危険性がある。	• イラスト等を生成するAIを開発する場合、著作権フリーの画像等、著作権等の権利処理がなされたデータを学習に利用。 • イラスト等を生成するAIを開発する場合、学習したデータをそのまま、あるいは類似した形でアウトプットしないような形で開発。
7	プライバシー (個人情報保護法等)	• 医療情報(個人情報含む)に該当しない検査画像等のデータのみを生成AIの学習に用いる場合は、個人情報保護法等の問題は生じない想定。	–
8	セキュリティ (3省2ガイドライン等)	• 医療情報に該当しない検査画像等のデータのみを生成AIの学習に用いる場合は、3省2ガイドラインの対象外となる。 • 一方で、生成AIの学習に利用するデータは、医療機関の機密情報となるため、適切な安全管理措置を行わない場合、情報漏えい等のリスクがある。	• 生成AIの学習データ等は、医療機関の機密情報となるため、適切な安全管理措置を実施。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑥研修支援で想定されるリスク・対策例

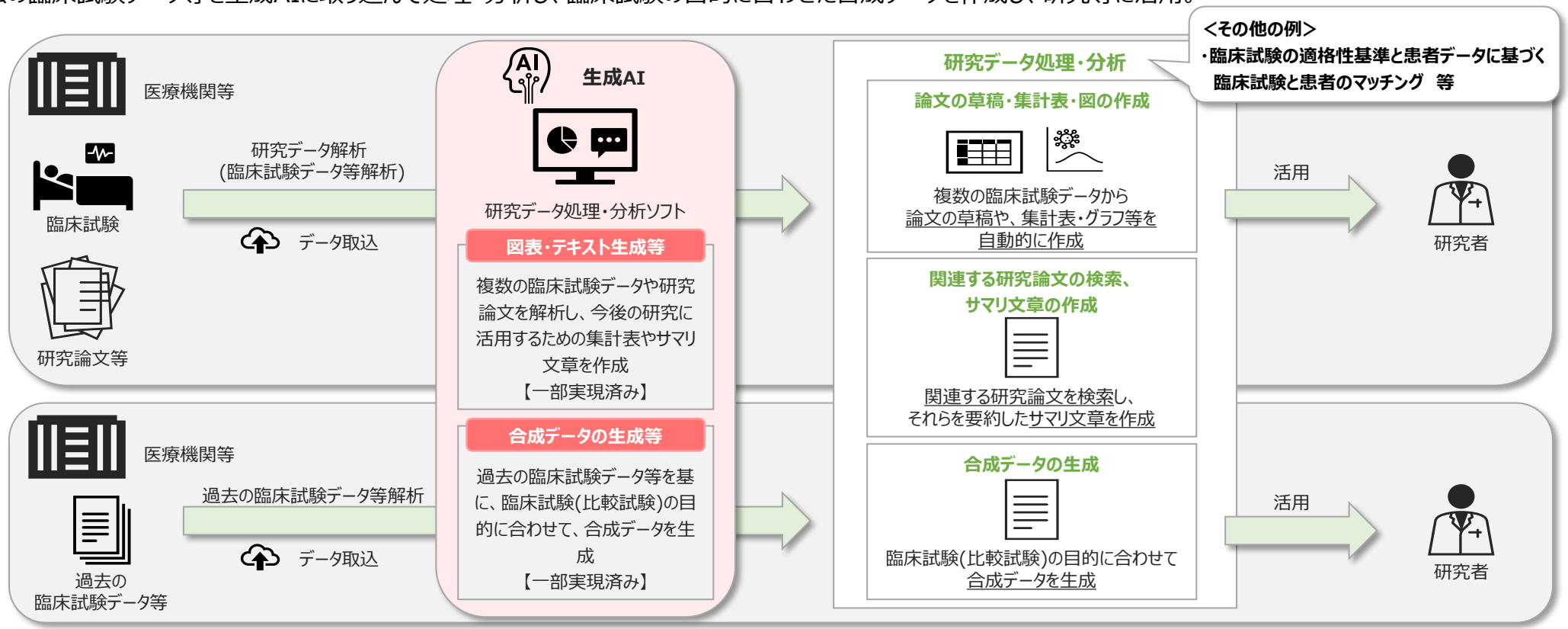
【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは無いため、いずれも黒字で記載。

#	リスクの観点	リスクの内容	対策例
9	医師法	・問題は生じない想定。	―
10	医療法	・問題は生じない想定。	―
11	医薬品医療機器等法	・研修支援という点では診断等に該当しないため、医療機器プログラムには該当しない。	―
12	健康増進法	・問題は生じない想定。	―
13	人を対象とする生命科学・医学系研究に関する倫理指針	・問題は生じない想定。	―
14	臨床研究法	・問題は生じない想定。	―
15	次世代医療基盤法	・問題は生じない想定。	―
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	・データの処理方法や生成AIの開発工程等に関して特許調査を行い、特許権の侵害が生じないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑦研究データ処理・分析支援の概要

- 医療機関等における研究データ処理・分析を生成AIにより実施することで、研究の業務効率化が期待できます。
  - 複数の臨床試験データを生成AIに取込んで処理・分析し、論文の草稿や、集計表・グラフ等を自動作成し、研究等に活用。
  - 複数の研究論文を生成AIに取り込んで処理・分析し、複数の研究データ内容を要約した文章を自動作成し、研究等に活用。
  - 過去の臨床試験データ等を生成AIに取り込んで処理・分析し、臨床試験の目的に合わせた合成データを作成し、研究等に活用。



(参考) ビジネス+IT『医療の現場でも進む生成AI活用、莫大なコスト削減につながる理由とは？』(2024年6月参照)
Medidata『Synthetic Control Arm® 洗練された外部対象群のためのソリューション』(2024年6月参照)

2. 生成AIの各ユースケースの概要・リスク・対策例

⑦研究データ処理・分析支援で想定されるリスク・対策例

- 前頁に示すユースケースにおいて、想定されるリスクとともに、生成AIの利用者での対策例を以下に示します。
- なお、リスク管理を行う際に、⑦のユースケース特有で注意すべきポイントは以下のとおりです。
  - 生成AIを用いて研究計画書等を作成する場合、研究の倫理的な妥当性及び科学的な合理性が考慮されているか、必要な項目が抜け落ちていないかなど、生成AIの出力を研究者が確認。
  - 生成AIを用いてインフォームド・コンセントを取る場合、生成AIが出力した説明内容を研究者が確認した上で利用。

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
1	ディープフェイク	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・研究者が、意図的に生成AIで研究成果の偽造物を作成し、研究結果として出回る可能性がある。 ■合成データの生成 ・問題は生じない想定。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・偽造物を作成しない。	・左記、個人での対策を利用ルールとして規定し、職員に周知。
2	不適正利用	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・研究者が生成AIに対して研究データの集計結果等を捏造する指示を行い、虚偽の研究データを生成する可能性がある。 ■合成データの生成 ・研究者が、臨床試験の成績を良く見せることを意図して合成データを生成することで、臨床試験結果が誤った内容となる。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・虚偽の研究データを作成しない。 ■合成データの生成 ・合成データを不正に生成しない。	・左記、個人での対策を利用ルールとして規定し、職員に周知。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑦研究データ処理・分析支援で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
3	正確性、信頼性	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・生成AIの操作者の意図した範囲の研究データを網羅的に集計せず、一部のデータのみを対象に集計してしまう可能性がある。 ・サマリ文章を作成する際、サマリに含めるべき重要なポイントが抜け落ちる可能性がある。 ■合成データの生成 ・合成データの生成のための設定等が正確でなく、臨床試験を支援するデータとして正確性や信頼性に欠ける可能性がある。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・研究者が臨床試験、研究論文等のデータを正確に入力。 ・生成AIが出力した集計データやサマリ文章等を研究者が確認した上で利用。 ■合成データの生成 ・研究者が、実施する臨床試験等の目的に合わせて、合成データの生成のための設定等を正確に実施。	・左記、個人での対策を周知。 ・組織として利用可能な生成AIを選定する際に、サービスの正確性を評価。
4	公平性、バイアス	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・問題は生じない想定。 ■合成データの生成 ・合成データの生成のための設定等に患者の年齢、性別、人種等で偏りがあり、出力される合成データにバイアスがかかる可能性がある。	■合成データの生成 ※「正確性、信頼性」と同じ。	■合成データの生成 ※「正確性、信頼性」と同じ。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑦研究データ処理・分析支援で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
5	透明性、説明責任	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・研究結果等に生成AIで導出した資料を用いる場合、そのことを明示しないと間違った論文等が出回る問題がある。 ■合成データの生成 ・研究データに合成データを用いる場合、適切な合成データが出力できていることについて説明責任が求められる。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・生成AIが出力した集計データやサマリ文章等を研究成果等に利用する場合、生成AIが出力していることを研究成果等に記載。 ■合成データの生成 ・臨床試験に合成データを用いる場合、生成AIが出力していることを研究成果等に記載。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・左記、個人での対策を周知。 ■合成データの生成 ・生成AIのサービス提供者に対して、品質に関する情報の開示を求める。 ・左記、個人での対策を周知。
6	著作権（著作権法）	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・生成AIで作成する研究論文等の解析に、他者の論文や研究結果を著作権者に許諾を得ずに無断で用いて、自分の論文や研究成果に使用した場合、著作権の侵害となる。 ■合成データの生成 ・問題は生じない想定。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・著作権等の権利処理を実施していない他人の著作物等を入力しない。 ・自身の著作物等を入力する場合、再学習されない設定とする。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・他者の論文や研究結果等を利用する場合、著作権等の権利処理が実施されているかなどを確認。
7	プライバシー (個人情報保護法等)	・医療情報(個人情報を含む)を再学習に利用される設定の生成AIに入力する場合、第三者提供となる。 ・医療情報(個人情報を含む)を研究目的で利用する場合、本人の同意を得なければ、個人情報保護法に違反する。	・利用する生成AIが、組織として利用可能と判断されていることを確認。 ・医療情報(個人情報を含む)を研究以外の目的で利用しない。	・組織として利用可能な生成AIを選定する際に、入力データが再学習に利用されない設定となっていることを確認。 ・左記、個人での対策を利用ルールとして規定し、職員に周知。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑦研究データ処理・分析支援で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
8	セキュリティ (3省2ガイドライン等)	・以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアでない。	・利用する生成AIが、組織として利用可能と判断されていることを確認。 ・利用者として求められる安全管理措置を実施。	・組織として利用可能な生成AIとして、以下の観点等から選定し、職員へ周知。 ✓ 生成AIのサーバ等が、国内法の適用を受ける場所に設置されていること。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアであること。 ✓ (組織で保有する医療情報を提供する場合)生成AIのサービス提供者との契約や書面等で、提供する医療情報が漏えいしないよう安全管理措置がされていること、契約終了後に提供した医療情報が削除されること等。 ・左記、個人での対策を利用ルールとして規定し、職員に周知。
9	医師法	・問題は生じない想定。	–	–
10	医療法	・問題は生じない想定。	–	–
11	医薬品医療機器等法	・研究データ処理・分析支援は診断等に該当せず、医療機器プログラムには該当しない。	–	–
12	健康増進法	・問題は生じない想定。	–	–

2. 生成AIの各ユースケースの概要・リスク・対策例

⑦研究データ処理・分析支援で想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
13	人を対象とする生命科学・医学系研究に関する倫理指針	■集計表・図、関連論文の検索・サマリ文章等の生成、合成データの生成 ・研究成果のとりまとめ、情報の作成等に生成AIを用いる場合、正確性、精度等が担保できない可能性がある。 ■その他、研究における生成AI活用 ・生成AIを用いて研究計画書等を作成する場合、研究の倫理的な妥当性及び科学的な合理性が考慮されないこと、必要な項目が抜け落ちること等が生じる可能性がある。 ・生成AIを利用してインフォームド・コンセントを取る場合に適切な項目が説明されない可能性がある。	■集計表・図の作成、関連論文の検索・サマリ文章の生成、合成データの生成 ・生成AIが出力した研究成果や合成データ等を研究者が確認した上で利用。 ■その他、研究における生成AI活用 ・生成AIを用いて研究計画書等を作成する場合、AIの出力を以下の観点から研究者が確認。 ✓ 研究の倫理的な妥当性及び科学的な合理性が考慮されていること。 ✓ 必要な項目が抜け落ちていないこと。 ・生成AIを用いてインフォームド・コンセントを取る場合、生成AIが出力した説明内容を研究者が確認した上で利用。	・左記、個人での対策を周知する。
14	臨床研究法	※「プライバシー（個人情報保護法）」、「人を対象とする生命科学・医学系研究に関する倫理指針」と同じ。	※「プライバシー（個人情報保護法）」、「人を対象とする生命科学・医学系研究に関する倫理指針」と同じ。	※「プライバシー（個人情報保護法）」、「人を対象とする生命科学・医学系研究に関する倫理指針」と同じ。
15	次世代医療基盤法	・利用フェーズでは問題は生じない想定。	－	－
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	－	・組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に対し、特許権侵害を犯していないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑦研究データ処理・分析支援で想定されるリスク・対策例

- 69頁に示すユースケースにおいて、想定されるリスクとともに生成AIの開発者での対策例を以下に示します。
- なお、リスク管理を行う際に、⑦のユースケース特有で注意すべきポイントは以下のとおりです。
  - 生成AIを用いて合成データを生成する場合、サービス利用者への説明に必要となる学習データの収集・整備に関する記録・整理を実施。
  - 生成AIを用いて合成データを生成する場合、合成データの生成精度と根拠を併せて提示する仕様で実装。

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
1	ディープフェイク	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・研究者が、意図的に生成AIで研究成果の偽造物を作成し、研究結果として出回る可能性がある。 ■合成データの生成 ・問題は生じない想定。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・典型的な不適正利用のパターンを機能的に制限。 ・利用規約等により偽情報の作成を禁止。
2	不適正利用	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・研究者が生成AIに対して研究データの集計結果等を捏造する指示を行い、虚偽の研究データを生成する可能性がある。 ■合成データの生成 ・研究者が、臨床試験の成績を良く見せることを意図して合成データを生成することで、臨床試験結果が誤った内容となる。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・典型的な不適正利用のパターンを機能的に制限。 ・利用規約等により偽情報の作成を禁止。 ■合成データの生成 ・典型的な不適正利用のパターンを機能的に制限。
3	正確性、信頼性	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・生成AIの操作者の意図した範囲の研究データを網羅的に集計せず、一部のデータのみを対象に集計してしまう可能性がある。 ・サマリ文章を作成する際、サマリに含めるべき重要なポイントが抜け落ちる可能性がある。 ■合成データの生成 ・合成データを生成する際に、臨床試験の目的達成に必要なデータが抜け落ちること、異常値が含まれること等の正確性の問題が生じる可能性がある。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・学習済みモデルの正確性、信頼性を評価した上で実装。 ■合成データの生成 ・学習データとなる臨床試験データ等を正規化し、正確性、信頼性を担保。 ・学習済みモデルの正確性、信頼性を評価した上で実装。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑦研究データ処理・分析支援で想定されるリスク・対策例

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
4	公平性、バイアス	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・問題は生じない想定。 ■合成データの生成 ・学習データに患者の年齢、性別、人種、疾患等で偏りがあった場合、出力される合成データにバイアスがかかり、臨床試験の患者ベースラインが揃わず、合成データとして使用できない。	■合成データの生成 ・学習データに偏りがないか評価。 ・学習済みモデルにおけるアウトプットにおいて偏りがないか評価。
5	透明性、説明責任	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・研究結果等に生成AIで導出した資料を用いる場合、そのことを明示しないと間違った論文等が出回る問題がある。 ■合成データの生成 ・研究データに合成データを用いる場合、適切な合成データが出力できていることについて説明責任が求められる。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・AIが出力したグラフ等の集計データがそのまま論文等に掲載される場合に備え、AIが出力したものであることを示す仕様とする。 ■合成データの生成 ・サービス利用者への説明に必要となる学習データの収集・整備に関する記録・整理を実施。 ・合成データの生成精度と根拠を併せて提示する仕様で実装。
6	著作権（著作権法）	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・生成AIで作成する研究論文等の解析に、他者の論文や研究結果を著作権者に許諾を得ずに無断で用いて、自分の論文や研究成果に使用した場合、著作権の侵害となる。 ■合成データの生成 ・問題は生じない想定。	■集計表・図の作成、関連論文の検索・サマリ文章の生成 ・他者の論文や研究結果等を学習データに用いる場合、著作権等の権利処理を実施した上で利用。 ・他者の論文や研究結果等を学習に用いる場合、学習したデータをそのまま、あるいは類似した形でアウトプットしないような形で開発。
7	プライバシー (個人情報保護法等)	・医療情報(個人情報を含む)を学習に利用する場合、本人から個人情報の削除等が求められた際に対応する必要があるが、その都度、削除したデータで学習し直すことは困難。	・医療情報(個人情報を含む)を学習に利用する場合は、仮名加工情報、匿名加工情報に加工し、個人情報保護法等で規定された取り扱いを遵守。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑦研究データ処理・分析支援で想定されるリスク・対策例

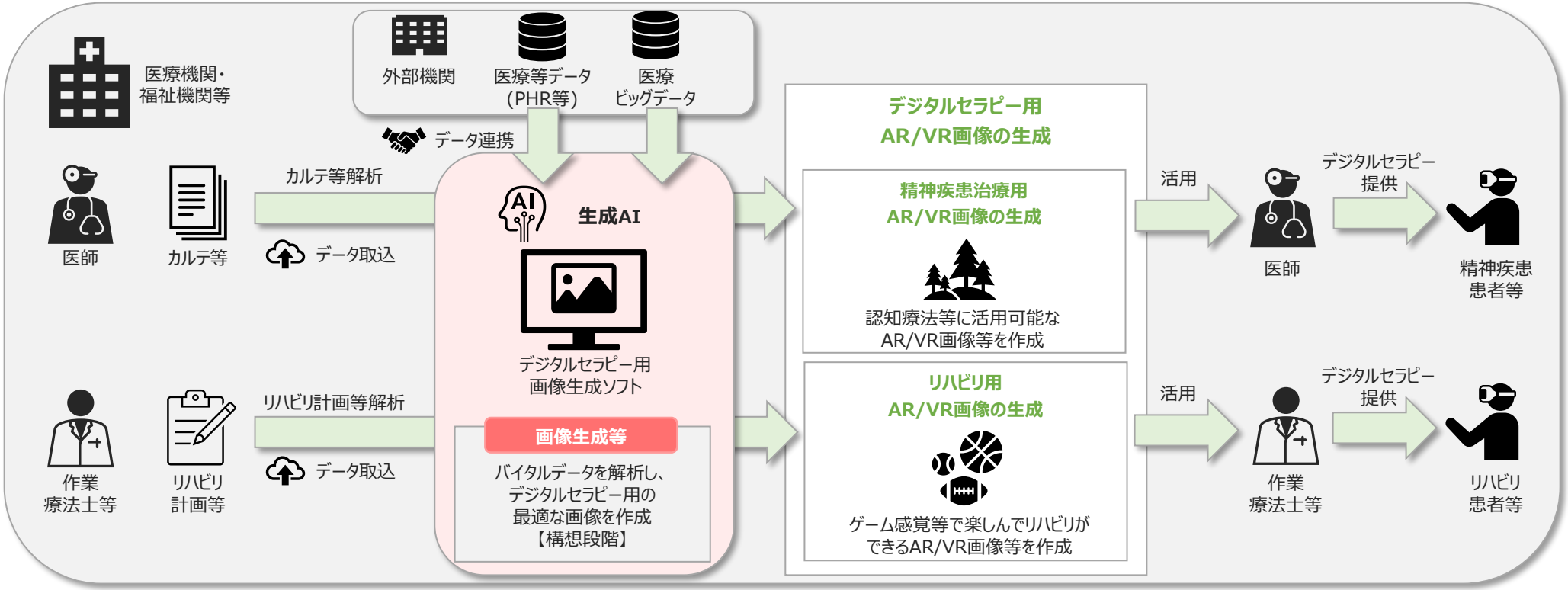
【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアでない。	• 3省2ガイドラインに準拠するよう、以下の対策等を行う。 ✓ 医療情報を保管するサーバ等を国内法の適用を受ける場所に設置。 ✓ 3省2ガイドラインで求められる技術基準に則した安全管理措置を実施(医療機関・薬局等と生成AIを接続するネットワークをセキュアとすることを含む)。
9	医師法	• 問題は生じない想定。	–
10	医療法	• 問題は生じない想定。	–
11	医薬品医療機器等法	• 研究データ処理・分析支援は診断等に該当せず、医療機器プログラムには該当しない。	–
12	健康増進法	• 問題は生じない想定。	–
13	人を対象とする生命科学・医学系研究に関する倫理指針	• 開発フェーズでは問題は生じない想定。	–
14	臨床研究法	• 開発フェーズでは問題は生じない想定。	–
15	次世代医療基盤法	• 学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、匿名加工医療情報や仮名加工医療情報を法で定められた取り扱いをしなければ次世代医療基盤法に違反する。	• 学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、次世代医療基盤法で規定された取り扱いを遵守。
16	特許法	• データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	• データの処理方法や生成AIの開発工程等に関して特許調査を行い、特許権の侵害が生じないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑧デジタルセラピーの概要

- 医療機関・福祉機関等におけるデジタルセラピーを生成AIにより実現することで治療効果を高め、医療の質向上が期待できる。
  - 精神疾患患者のカルテ等データを生成AIに取込んで分析し、認知療法等に活用可能なAR/VR画像等を作成し、治療に活用。
  - リハビリ計画等を生成AIに取込んで分析し、楽しんでリハビリできるAR/VR画像等を作成し、リハビリに活用。



(参考) TALESPIN by cornerstone『 The Power of Generative AI in VR: A Gateway to Innovation (talespin.com) 』(2024年6月参照)
mHEALTH INTELLIGENCE『Using VR to Create an Immersive Mental Health Support System』(2024年6月参照)
みずほリサーチ＆テクノロジーズ『医療分野で活躍するVR/AR/MR』(2024年3月参照)
Deloitte Japan『生成AIにより業務を効率化して、迅速な結果と具体的な利益を生みだす』(2024年3月参照)

2. 生成AIの各ユースケースの概要・リスク・対策例

⑧デジタルセラピーで想定されるリスク・対策例

- 前頁に示すユースケースにおいて、想定されるリスクとともに、生成AIの利用者での対策例を以下に示します。
- なお、リスク管理を行う際に、⑧のユースケース特有で注意すべきポイントは以下のとおりです。
  - AIの出力を患者への治療やリハビリ等に利用する場合は、組織として利用可能な生成AIを選定する際に、薬事承認を得ていることを確認。
  - 薬事承認を得ていない生成AIを利用する場合、その生成AIの利用に関する医療機関等における責任の所在を事前に明確化。

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
1	ディープフェイク	• 問題は生じない想定。	–	–
2	不適正利用	• 問題は生じない想定。	–	–
3	正確性、信頼性	• 治療やリハビリのための画像等の情報作成において、患者の症状やニーズに合わない画像等が生成される可能性がある。	• 医師等が正確に記載したカルテやリハビリ計画等をAIに入力。 • アウトプットは患者の症状やニーズに合わない可能性があることを認識し、出力された画像等を医師等が確認した上で利用。	• 左記、個人での対策を利用ルールとして規定し、職員へ周知。 • 組織として利用可能な生成AIを選定する際に、サービスの正確性を評価。
4	公平性、バイアス	• 生成AIが出力に偏りがあり、患者の疾患等によっては適切なAR/VR画像が出力されない可能性がある。	※「正確性、信頼性」と同じ。	• 「正確性、信頼性」と同様、個人での対策を利用ルールとして規定し、職員へ周知。 • 組織として利用可能な生成AIを選定する際に、サービスのバイアス等を評価。
5	透明性、説明責任	• 治療やリハビリのための画像等の作成に用いる場合は、処理の透明性や説明責任が求められる。薬事承認を得るためには、これらのエビデンスが必要となる。	–	• AIの出力を患者への治療やリハビリ等に使用する場合は、それが薬事承認を得ていることを確認。 • 生成AIのサービス提供者に対して、品質に関する情報の開示を要求。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑧デジタルセラピーで想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
6	著作権（著作権法）	• 生成AIで作成する画像等の情報に、著作権を侵害するゲームの内容やイラスト、図が含まれる危険性がある。	• 既存の著作物に類似する文章・イラスト等の生成につながるプロンプトを入力しない。 • 権利処理がされていない既存の著作物等を無断で入力に利用しない。 • 生成AIが出力した内容が既存の著作物等に類似していないことを確認。	• 左記、個人での対策を利用ルールとして規定し、職員に周知。
7	プライバシー (個人情報保護法等)	• カルテやリハビリ計画等の医療情報(個人情報を含む)を再学習に利用される設定の生成AIに入力する場合、第三者提供となる。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。	• 組織として利用可能な生成AIを選定する際に、入力データが再学習に利用されない設定となっていることを確認。
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアでない。	• 利用する生成AIが、組織として利用可能と判断されていることを確認。 • 利用者として求められる安全管理措置を実施。	• 組織として利用可能な生成AIとして、以下の観点等から選定し、職員へ周知。 ✓ 生成AIのサーバ等が、国内法の適用を受ける場所に設置されていること。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアであること。 ✓ (組織で保有する医療情報を提供する場合)生成AIのサービス提供者との契約や書面等で、提供する医療情報が漏えいしないよう安全管理措置がされていること、契約終了後に提供した医療情報が削除されること等。 • 左記、個人での対策を利用ルールとして規定し、職員に周知。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑧デジタルセラピーで想定されるリスク・対策例

【生成AIの利用者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例	
			生成AIの利用者(個人)	生成AIの利用者(組織)
9	医師法	・基本的に問題は生じない想定。 ※デジタルセラピーは治療に用いられる医療機器プログラムであるため、デジタルセラピーの提供には医師の判断が必要。	―	―
10	医療法	・生成AIを使用した治療・リハビリのための画像の情報作成等の業務が適性に実施されるよう、医療機関は医療従事者の監督をしなければ、医療法に違反する。	―	・生成AIを使用した治療やリハビリのための画像等の情報作成に関しての業務が適正に実施されるように、医師や作業療法士等を監督するルールを規定。
11	医薬品医療機器等法	・出力を治療を含む医学的判断に使用することを目的としたAIである場合、当該AIは医療機器プログラムに該当するため、薬事承認を得たサービスでなければ使用できない。 ・汎用AI*を含むAIの提供者が定めるAIの使用目的が医学的判断ではない場合、当該AIは医療機器プログラムには該当しない。	・利用する生成AIが、組織として利用可能と判断されていることを確認。	・AIの出力を患者への治療やリハビリ等に利用する場合は、組織として利用可能な生成AIを選定する際に、薬事承認を得ていることを確認。 ・薬事承認を得ていない生成AIを利用する場合、その生成AIの利用に関する医療機関等における責任の所在を事前に明確化。
12	健康増進法	・問題は生じない想定。	―	―
13	人を対象とする生命科学・医学系研究に関する倫理指針	・問題は生じない想定。	―	―
14	臨床研究法	・問題は生じない想定。	―	―
15	次世代医療基盤法	・利用フェーズでは、問題は生じない想定。	―	―
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	―	・組織として利用可能な生成AIを選定する際に、生成AIのサービス提供者に対し、特許権侵害を犯していないことを確認。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑧デジタルセラピーで想定されるリスク・対策例

- 78頁に示すユースケースにおいて、想定されるリスクとともに生成AIの開発者での対策例を以下に示します。
- なお、リスク管理を行う際に、⑧のユースケース特有で注意すべきポイントは以下のとおりです。
  - 薬事承認を得る場合は、必要となる学習データの収集・整備に関する記録・整理を行うとともに、医療機器プログラムとしての安全性・有効性等が確保されていることを薬事承認プロセスの中でPMDA/登録認証機関に提示。
  - 薬事承認を得ない場合はサービスを提供等する際、疾病の診断や予防、治療を目的としたものではないことや医療機器プログラムではないことを表示。
  - 生成AIが入力内容に基づき、認知療法等に活用可能な画像を生成することを医師に通知する仕様で実装。
  - 認知療法等に活用可能な画像を生成する際の精度と根拠を併せて提示する仕様であることを、サービス利用者となる医師等に説明。

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
1	ディープフェイク	• 問題は生じない想定。	ー
2	不適正利用	• 問題は生じない想定。	ー
3	正確性、信頼性	• 治療やリハビリのための画像等の情報作成において、患者の症状やニーズに合わない画像等が生成される可能性がある。	• 学習に用いるカルテ、リハビリ計画等のデータを正規化し、正確性、信頼性を担保。 • 学習済みモデルの正確性、信頼性を評価した上で実装。
4	公平性、バイアス	• 生成AIの学習データに含まれる精神疾患やリハビリの種類とそれらに対応したAR/VR画像の種類の偏りによって、生成するAR/VR画像に偏りが生じ、その患者の疾患、リハビリにとって適切なものが生成されない可能性がある。	• 学習データに偏りがないか評価。 • 学習済みモデルにおけるアウトプットにおいて偏りがないか評価。

2. 生成AIの各ユースケースの概要・リスク・対策例

⑧デジタルセラピーで想定されるリスク・対策例

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
5	透明性、説明責任	• 治療やリハビリのための画像等の作成に用いる場合は、処理の透明性や説明責任が求められる。薬事承認を得るためには、これらのエビデンスが必要となる。	• 薬事承認やサービス利用者への説明に必要となる学習データの収集・整備に関する記録・整理を実施。 • 生成AIが入力内容に基づき認知療法等に活用可能な画像を生成することを医師に通知する仕様で実装。 • 認知療法等に活用可能な画像を生成する際の精度と根拠を併せて提示する仕様であることをサービス利用者となる医師等に説明。
6	著作権（著作権法）	• 生成AIで作成する画像等の情報に、著作権を侵害するゲームの内容やイラスト、図が含まれる危険性がある。 • 著作権を侵害する出力が行われる場合、著作物の学習自体が著作権法違反になる可能性がある。	• 学習データに用いるゲームは著作権フリーのものに限定。 ※アイディアは保護対象外であり、共通部分がごく一般的である場合等は、ゲームについては著作権侵害とならない可能性が高い。 • イラスト等を生成するAIを開発する場合、著作権フリーの画像等、著作権等の権利処理がなされたデータを学習に利用。 • イラスト等を生成するAIを開発する場合、学習したデータをそのまま、あるいは類似した形でアウトプットしないような形で開発。
7	プライバシー (個人情報保護法等)	• 医療情報(個人情報を含む)を学習に利用する場合、本人から個人情報の削除等が求められた際に対応する必要があるが、その都度、削除したデータで学習し直すことは困難。	• 医療情報(個人情報を含む)を学習に利用する場合は、仮名加工情報、匿名加工情報に加工し、個人情報保護法等で規定された取り扱いを遵守。
8	セキュリティ (3省2ガイドライン等)	• 以下の場合等では、3省2ガイドライン違反になる。 ✓ 生成AIを用いる医療情報システムの安全管理や監査を適切に実施していない。 ✓ 生成AIを用いる医療情報を格納するサーバ等が、国内法の適用を受けない場所に設置されている。 ✓ 医療機関・薬局等と生成AIを接続するネットワークがセキュアでない。	• 3省2ガイドラインに遵守するよう、以下の対策等を行う。 ✓ 医療情報を保管するサーバ等を国内法の適用を受ける場所に設置。 ✓ 3省2ガイドラインで求められる技術基準に則した安全管理措置を実施(医療機関・薬局等と生成AIを接続するネットワークをセキュアとすることを含む)。
9	医師法	• 問題は生じない想定。	–
10	医療法	• 開発フェーズでは問題は生じない想定。	–

2. 生成AIの各ユースケースの概要・リスク・対策例

⑧デジタルセラピーで想定されるリスク・対策例

【基盤モデルをベースとした生成AIの開発者】 ※当該ユースケース特有で注意すべきポイントは赤字で記載。

#	リスクの観点	リスクの内容	対策例
11	医薬品医療機器等法	・出力を治療を含む医学的判断に使用することを目的としたAIである場合、当該AIは医療機器プログラムに該当するため、薬事承認を得たサービスでなければ使用できない。 ・汎用AI*を含むAIの提供者が定めるAIの使用目的が医学的判断ではない場合、当該AIは医療機器プログラムには該当しない。	・薬事承認を得る場合は、必要となる学習データの収集・整備に関する記録・整理を実施。 ・薬事承認を得る場合は、医療機器プログラムとしての安全性・有効性等が確保されていることを薬事承認プロセスの中でPMDA/登録認証機関に提示。 ・薬事承認を得ない場合はサービスを提供等する際、疾病の診断や予防、治療を目的としたものではないことや医療機器プログラムではないことを表示。
12	健康増進法	・問題は生じない想定。	ー
13	人を対象とする生命科学・医学系研究に関する倫理指針	・問題は生じない想定。	ー
14	臨床研究法	・問題は生じない想定。	ー
15	次世代医療基盤法	・学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、匿名加工医療情報や仮名加工医療情報を法で定められた取り扱いをしなければ次世代医療基盤法に違反する。	・学習データに匿名加工医療情報や仮名加工医療情報を利用する場合、次世代医療基盤法で規定された取り扱いを遵守。
16	特許法	・データの処理方法や生成AI・ソフトの開発工程等において、他者の特許権侵害があった場合、特許法に違反する。	・データの処理方法や生成AIの開発工程等に関して特許調査を行い、特許権の侵害が生じないことを確認。

5章　今後の展望

- 5章では、今後の展望として、今後の本ガイドラインの発展等について考えていきます。

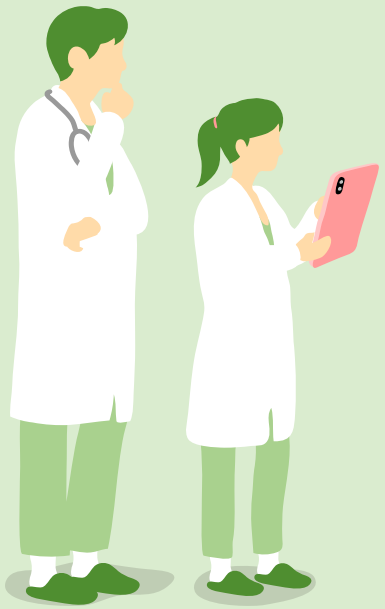
1. 今後の展望

- 本ガイドラインは、医療現場での生成AIの導入と利用の促進に向け、医療現場で生成AIを利用するケースを念頭に、注意すべきポイントを整理しています。

- 将来的に医療現場において生成AIが普及した場合、生成AIが診察・診断業務の支援や研究・データ分析の支援等、様々なシーンで活躍することが想定されます。一方で、この生成AIの普及により、医師等の医療従事者の知識・スキル向上の機会が損なわれる懸念があります。そのため、生成AIを利用する組織では、このような知識・スキル向上のための自己学習や研修等の仕組みを整備しておくことが考えられます。

- 今後も、急速な技術の発展により、生成AIの利用シーンや関連する法規制等が変化していくことが見込まれることから、医療現場で適切にリスクを管理して生成AIを利用できるよう、本ガイドラインの内容を継続的に見直しを行うことが求められます。

- 医療・ヘルスケア分野での生成AIの利用は今後も重要性が増していくことが想定されます。生成AIが、患者や医療従事者等のステークホルダーに対し、安全・安心な形で利用され、業務効率化や医療費の削減、医療サービスの質の向上等の様々なメリットを享受できるものとなることを、今後も目指していきます。



HAIP