生成AIを支える技術とガードレールについて

～RAG・MCPから、SaMD認証、関連法規まで～

座長
群馬大学医学部附属病院
鳥飼幸太先生

ヘルスケアや金融向けのデータ管理プラットフォームを提供する米国のデータテクノロジー企業であるインターシステムズジャパン株式会社は、プライベートカンパニーであることから、短期的な利益より「顧客ファースト」を重視することで知られている。座長の鳥飼先生からは「医療分野において、高度なデータプラットフォームをどのように医療の中に定着させるか、40年以上にわたって取り組んでいる信頼のおける企業」との紹介を受け、日本法人インターシステムズジャパン株式会社の奥山氏による「医療におけるAI」についての講演の概要を紹介する。

InterSystems IRISデータプラットフォームの利用で医療DXの実現を支援/推進

インターシステムズジャパン株式会社奥山　朋氏

患者情報の保護にはローカルLLMも選択肢

LLM（Large Language Model）は、大規模大量言語データを使って学習されたモデルのことだが、スマートフォンやクラウドサービス向けに用意されているLLMは、日常的に入力したさまざまな情報が学習に使われてしまうことから、そのデータが第三者に渡ってしまう危険性もあり、医療分野におけるLLMの利用は慎重に考えなければならない。

自身のPCやサーバー内にAIの知識を搭載するローカルLLMにすることが、患者情報などの外部への漏洩を防ぎ、院内だけで完結したLLMを利用できるようにする方法となるが、これには相応なハードウェアが必要となる。一般のクラウド型LLMを利用するかローカルLLMにするかは、さまざまな状況を踏まえて検討、選択する必要がある。

ローカルLLMを選択する場合、適切なモデルと実行環境が必要とある。既存モデルやLM Studio、Ollamaなどの実行環境により利用可能となるが、医療分野に特化した期待する回答を得るためには、システムの作り込みが欠かせない。我々の開発したInterSystems IRISデータプラットフォームは、その要素を全て一体的に扱える仕様となっている（図1）。

LLMの性能を高めるRAG・ベクトル検索・MCP

LLMは大量の情報がある一方、最新の情報や病院内の電子カルテ情報などは持ち合わせていない。

●RAG：Retrieval-Augmented Generation

RAG（Retrieval-Augmented Generation）は、LLMに外部情報の検索を組み合わせることで、回答の精度を向上させる技術であり、過去の診療メモ、退院サマリーなどの文書をベクトル化、マッピングしておくことで、そこから連想できる近しい関連ワードが見つかるようになる（図2）。

LLMは膨大な費用と時間をかけて知識を獲

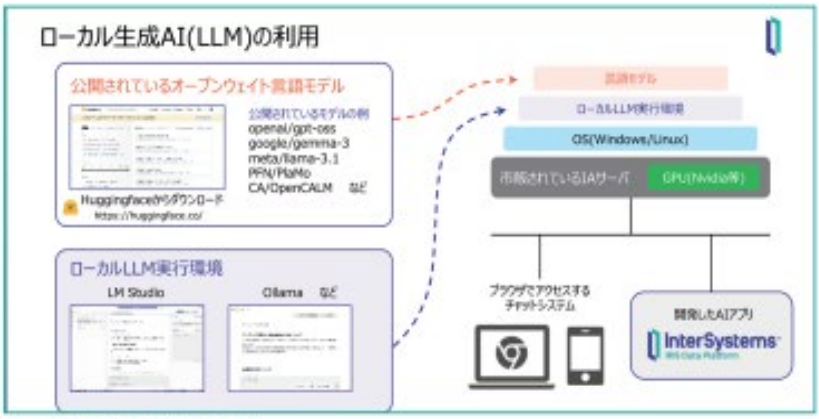

図1　ローカルLLM構築イメージ

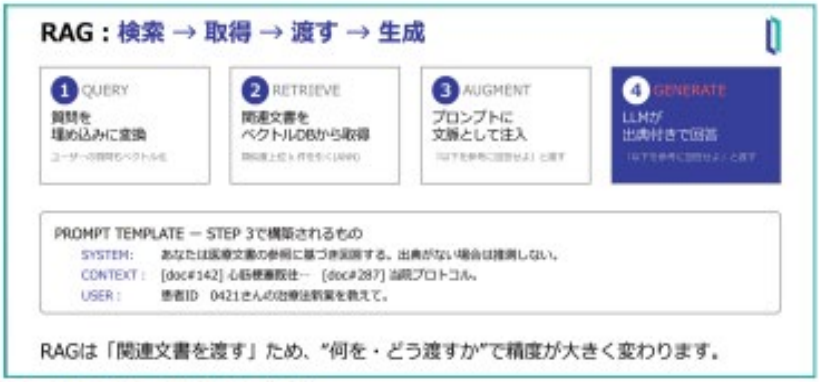

図2　RAG:検索→取得→渡す→生成

得するが、時間がかかる分、その情報は学習が始まった時点のデータしかなく、院内の情報も持っていない。

また、いかにも本当のような嘘の回答をすることがあり、特に医療の現場では大きな事故につながる恐れもある。さらに、LLM単体では外部システムが持つ知識や情報と連携できないため、不足する情報を補う仕組みが必要となる。その中核となるのが、テキストを数値の配列（ベクトル）に変換する技術である。変換したベクトルを格納するのがベクトルDB、そこから関連する情報を探し出すのがベクトル検索であり、これらを組み合わせることで、LLMが持たない情報を補える。

●ベクトル検索

ベクトル検索は、ある言葉、文章の内容から連想できる他の言葉や文章を、関連する情報と合わせて返答してくれる。

これらを実装する上で、ベターな情報を適切に選別・分割し、その情報テキストを数値に配列しベクトル化することで、ベクトルDBによるベクトル検索が可能となる。ここで要となるのがInterSystems IRISで、この機能を提供し、精度の向上と処理を実現してくれる。

●MCP：Model Context Protocol

MCP（Model Context Protocol）は、LLMが保有していない情報を効率的に取得するために外部ツールやデータベースと連携するための技術で、USBが多様なデバイスを接続できる共通規格であるように、LLMと各種システムをつなぐ共通プロトコルとなる。院内の部門システムや電子カルテ（EHR）がMCPに対応していれば、LLMは必要な情報へアクセスできるようになるということで、利用中のソリューションがMCPに対応しているかは、データの利活用、医療DX、医療AI推進における重要なテーマとなる。

オールインワンの医療用データプラットフォーム InterSystems IRIS for Health

これまで説明した機能は、コンピュータに詳しければ様々なツールやミドルウェアを使い、必要なものを積み重ねることで実装は可能だが、医療データの管理、統合、分析、およびアプリケーション開発に必要な全機能を統合しオールインワンで提供できるのがInterSystems IRIS for Healthである（図3）。InterSystems IRIS for Healthは、EHRや個人情報を含む各種データを一元的に扱える。加えて、いつ・誰が・どのような質問をし、AIがどの情報を根拠に回答したかという履歴（監査ログ）も記録できる。これは、問題が起きた際に経緯を調査するための重要な情報となる。こうしたデータと履歴を、すべて一つのプラットフォームでとりまとめて利用できる。

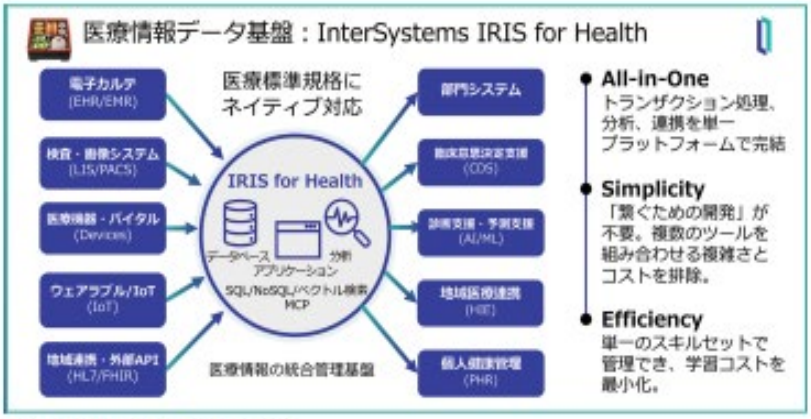

図3 InterSystemsIRIS for Health

AI医療機器として薬機法上の位置づけ（SaMD）や情報の取り扱いにも十分な配慮を

SaMDは、診断アプリやAI画像解析プログラムなど単体で医療機器として機能するソフトウェアのことで、市場に流通させるには薬機法に基づく認可手続きが必要となる。医師への情報提供だけならSaMDに該当しないが、診断に関与する場合は該当する可能性があり、設計段階からこの点も踏まえて検討する必要があり、AIソリューションではSaMD認証への配慮も重要である。

院内で取り扱う患者情報は、個人情報保護法で守るべき要配慮個人情報である（図4）。重要なのは院内利用か外部提供かの区別で、院内でカルテをAIに学習させたり、院内文書を用いたRAGで業務支援を行ったりする場合は第三者提供に当たらず、利用目的を定めて周知していれば個別の同意を取り直す必要はない。

一方、複数の医療機関のデータを集めて研究や医療AIの開発に活用するには別の枠組みが必要であり、それが次世代医療基盤法である。仮名加工・匿名加工した医療情報を、認定事業者を通じて研究開発に利用できるよう整備されたものである。

図4 日本固有の法令

AIを活用するにはガイドラインの整備が必要

AIやITの活用では、セキュリティ対策が不可欠である。医療AIに携わる場合、厚労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 第6.0版も踏まえ、リスク管理に十分配慮する必要がある。

医療DX令和ビジョン2030では、全国医療情報プラットフォーム、電子カルテ情報の標準化、診療報酬改定DXが重要な柱とされている。医療IT関係者は、データ活用だけでなく、院内データの運用と保護を理解し、医療AI・医療DXの推進に貢献することが求められる。