

生成AIによるAIチャットボットの実用化

阿部貴之*
Takayuki Abe
山田篤史*
Atsushi Yamada
池田貴紀*
Takaki Ikeda

徳富 忍*
Shinobu Tokudomi
衣川英之*
Hideyuki Kinugawa

*三菱電機デジタルイノベーション(株)

Practical Application of AI Chatbots Using Generative AI

要 旨

2023年は生成AI元年とも言われ、国内外で多くの企業が生成AI活用の取組みを始めた。同年から、三菱電機デジタルイノベーション(株)(MEDigital)でも社内問合せ業務の効率化を目指して、生成AIによるAIチャットボットの開発を開始した。生成AIはクラウドLLM(Large Language Model)を利用することによって比較的容易にシステムの構築はできるが、セキュリティ対策や実用に耐え得る回答精度へのチューニング、ハルシネーション対応など実用化には多くの課題が発生した。MEDigitalはこれらの課題を解決した。

1. ま え が き

2012年頃からディープラーニング等の機械学習による成果が認識され始めて、AI技術に対する関心が高まり、三菱電機・三菱電機グループでもAI開発の取組みが行われた。2022年11月にOpenAI社によってChatGPT^(注1)が公開されると、従来のAIが主な活用領域としていた認識や判断ではなく、新しいものを生み出すための生成AIが脚光を浴びるようになった。この状況を受けて、MEDigitalでも生成AIを活用した業務効率化及び生成AIのノウハウ獲得を目的として、社内問合せ業務を自動化するAIチャットボットの開発を開始し、2024年11月にその実用化に成功した。

生成AIを使ったシステムは、クラウドサービスを利用することで構築自体は比較的容易に実現できるが、実用化に向けては多くの課題が存在する。

本稿では、生成AIによるAIチャットボット実用化に関する課題とその対応策、及び今後の展望について述べる。

(注1) ChatGPTは、OpenAI OpCo, LLCの登録商標である。

2. 生成AIを用いたチャットボット開発構想

社内規則や業務システムのマニュアル・FAQ(Frequently Asked Questions)は社内ポータルで参照できるが、利用者にとって必要な情報を見つけることが困難な場合があり、また知りたいことを質問するための問合せ先を探すことも負担になることがあった。一方、利用者からの問合せを受けるヘルプデスク側では、社内文書を参照すれば利用者自ら解決できるはずの問合せに対応しなければならないことがあり、業務量増加の一因になっていた。そこでこの業務に生成AIを活用し、問合せ業務の効率化を図るAIチャットボットを構築する方針とした。システムのコンセプトは表1に示す。

表1-MEDigitalのAIチャットボットのコンセプト

No	要件	説明
1	安心・安全に利用できるセキュアなシステム	扱う情報が企業機密のため、AIがその情報を学習すると機密情報の漏洩(ろうえい)につながるおそれがある。また、クラウドサービスを利用する場合はネットワークセキュリティも考慮する必要がある。安心・安全に利用できるシステムにする。
2	利便性があり真に実用性のあるシステム	実用化に当たっては社内規則や業務システムの問合せ対応から始めるが、将来的には取り扱う対象を更に拡充する予定である。その際に、業務システム、社内規則など目的別に別々のシステムやシステムへの入り口を用意するとユーザーの利便性が損なわれてしまう。MEDigitalのAIチャットボットでは一つのチャットボットで多くの対象に対応できるようにする。また、開発に当たってAI技術を使うこと自体が目的にならないよう留意し、利便性が高く、予備知識のない利用者にとっても簡単に利用できるシステムにすることを目指す。

3. AIチャットボット実用化の課題

今回の開発に当たり、開発容易性、実用性の観点から生成AIのエンジンはクラウドLLMを利用する方針とした。
次に、クラウド環境、クラウドLLMを利用することの課題とシステムコンセプトから見える主要な課題について述べる。

3.1 情報漏洩リスクへの対応

クラウドLLMは様々な企業、利用者が共同利用するサービスであり、Azure^(注2) OpenAI ServiceやAmazon Bedrock^(注3)などが知られている。そのため社内文書をLLMに学習させると、他社や他の利用者へ情報漏洩のリスクが生じる。また、サービスによっては文書の学習以外にも、問い合わせた内容の監視や、学習データとしての二次利用でサービス提供者からデータが参照されてしまうケースがあり、意図しない情報漏洩のリスクが存在する。さらに、クラウドサービスを利用するためにはインターネットとの情報のやり取りが発生し、これに伴うネットワークセキュリティーのリスクも考慮する必要がある。

(注2) Azureは、Microsoft Corp.の登録商標である。
(注3) Amazon Bedrockは、Amazon Technologies, Inc.の登録商標である。

3.2 利便性と回答精度の両立

MEDigitalのAIチャットボットは、利用者の利便性を最優先に考えて、一つのシステムで多くの問合せ対象をカバーすることをコンセプトとしている。そのため一つのシステムに学習・登録する文書量が増える傾向があり、回答精度の低下が予想される。また、生成AIには誤った情報を生成してしまうハルシネーションと呼ばれる事象があり、どれほどチューニングを行っても100%の正答率にはならないという特性がある。MEDigitalのAIチャットボットは予備知識がない利用者が使用するシステムとして位置付けており、利便性を損なわず回答精度を高く保つ仕組みとハルシネーションへの対策を講じる必要がある。

4. 実用化に向けた対応

3章で述べたAIチャットボットの課題を解決し、実用的なシステムを構築する必要がある。
課題とその対応について表2にまとめた。また対応の詳細については各節で述べる。

表2-課題と対応のマッピング

課題		対応
情報漏洩リスクへの対応	LLMへ社内文書を学習させることによる情報漏洩対応	RAGアーキテクチャーとAzure OpenAI Serviceの採用
	監視等による情報漏洩対応	
	ネットワーク上での情報漏洩への対応	イントラネット延伸によるセキュリティーの確保
利便性と回答精度の両立	回答精度の低下に対する対策	対話機能による回答精度の向上
	ハルシネーションへの対策	AI回答時の工夫

4.1 RAGアーキテクチャーとAzure OpenAI Serviceの採用

3章で述べたとおり、クラウドLLMに企業機密を含む社内文書を学習させると情報漏洩につながるリスクがあるためMEDigitalのAIチャットボットはRAG(Retrieval-Augmented Generation)アーキテクチャーを採用した(図1)。

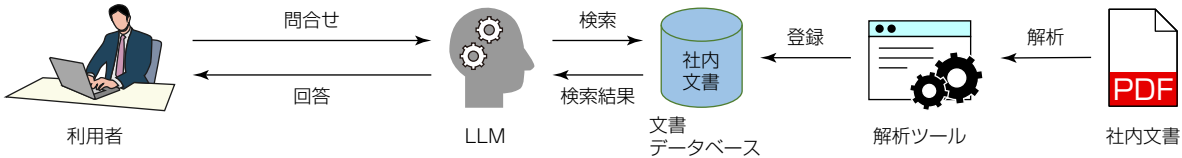


図1-RAGアーキテクチャー

RAGはAIが学習していない情報を別の情報源から取得して利用する仕組みであり、AIへの学習をさせずに情報を利用できる。さらにAIへ学習させる方法に比べて情報の管理(登録、削除、更新)が容易という点で優れており、時間経過とともに変更される文書・情報との相性が良いことで知られている。

また、企業ユースに多くの実績のあるAzure OpenAI Serviceを採用することでMicrosoft社による高水準のガバナンスやセキュリティーで管理されたLLMを利用でき、さらにベンダーの監視等による情報漏洩リスクもオプトアウト申請によって排除できる。

4.2 イン트라ネット延伸によるネットワークセキュリティーの確保

MEDigitalのAIチャットボットの実行環境は、三菱電機からの技術協力も得て、三菱電機イントラネット経由でAzure OpenAI Serviceへアクセスできるように構築した。この環境を用いることでインターネット経由による情報漏洩のリスクを低減し、企業機密を安心して利用できる。

4.3 対話機能による回答精度の向上

RAGの特性として文書データベースに多くの文書を登録すると回答精度が悪化するため、それを防ぐために目的別に別々のシステムを用意したり、チャット時に検索範囲を事前に利用者に選択させたりする対応を行うことがある。しかし、これらの方法は利用者に“探す手間”を増やす結果になって利便性と相反するため、MEDigitalのAIチャットボットではこれらの方法とは異なるアプローチでこの課題を解決した。

RAGの文書登録から回答生成までの流れと回答精度悪化のメカニズムについて図2に示す。文書は任意の長さで区切ったチャンクという単位に分割されて文書データベースに登録される。図中の“社内規則”は社内規則文書に関するチャンク、“システム”は業務システム文書に関するチャンクを表現している。検索は文書データベースに入っている全チャンクを対象に行われ、検索結果を用いて回答を生成する仕組みである。

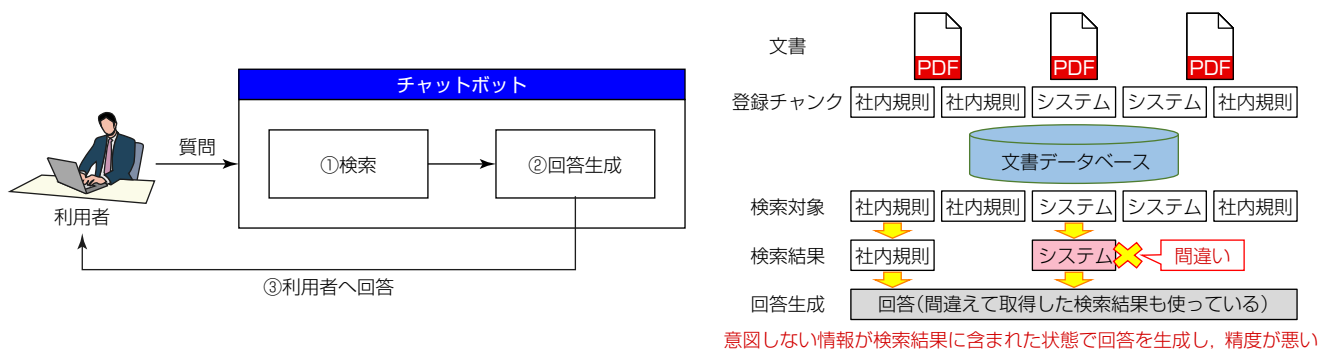


図2-回答精度悪化のメカニズム

回答精度悪化については、文書データベース中に類似ワードが多く存在する場合、質問の意図に沿わないチャンクが検索されることが原因であった。これが検索精度の低下を引き起こして、ひいては回答精度の悪化につながっていた。

そこでユーザーの利便性を損なわず課題を解決するための仕組みとして、問合せ内容に応じてチャットボットが利用者と対話を行うことで検索精度を高める仕組みを開発した。対話機能による回答精度向上の仕組みは図3、対話のイメージは図4に示す。この仕組みを用いることで、利用者の“探す手間”を軽減しつつ、システムの回答精度の向上を実現した。

4.4 AI回答時の工夫

ハルシネーションへの対応のため、図5に示すとおり、回答の文章に加えて、AI回答に対する注意喚起、引用元文書への参照、ヘルプデスクへの連絡先を提示する機能を具備した。利用者はAIの回答文に疑義がある場合は引用元文書を参照でき、それでも問題が解決できない場合は担当業務のヘルプデスクへ簡単にアクセスできる。またその際、問合せ内容に応じて異なるヘルプデスクへの連絡先を提示でき、複数の対象を取り扱っても一次窓口を必要としない。これによって予備知識がない利用者に対して探す手間を低減し、精度が100%ではない回答に対するセーフティーネットを用意することで、無人の一次窓口としてのシステム利用が可能になった。

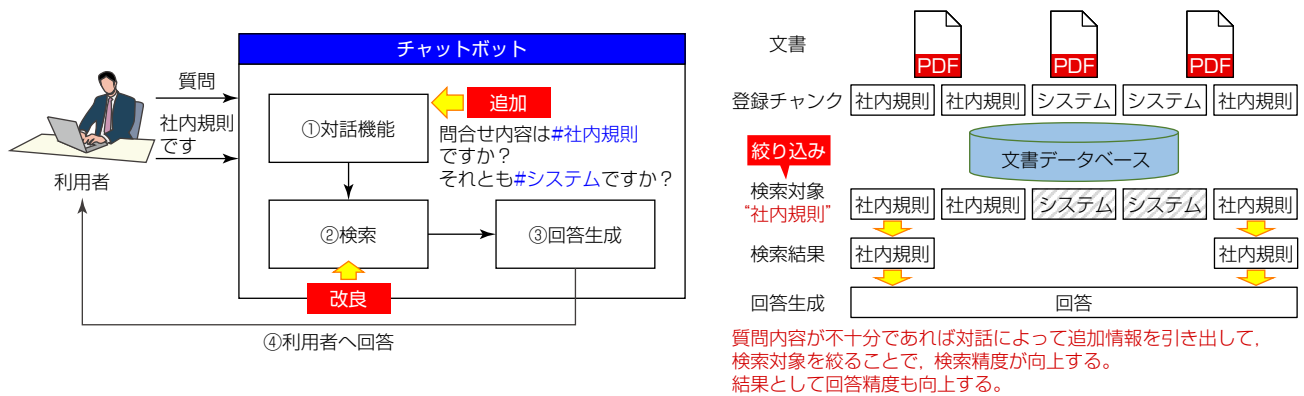


図3-対話機能による回答精度向上の仕組み

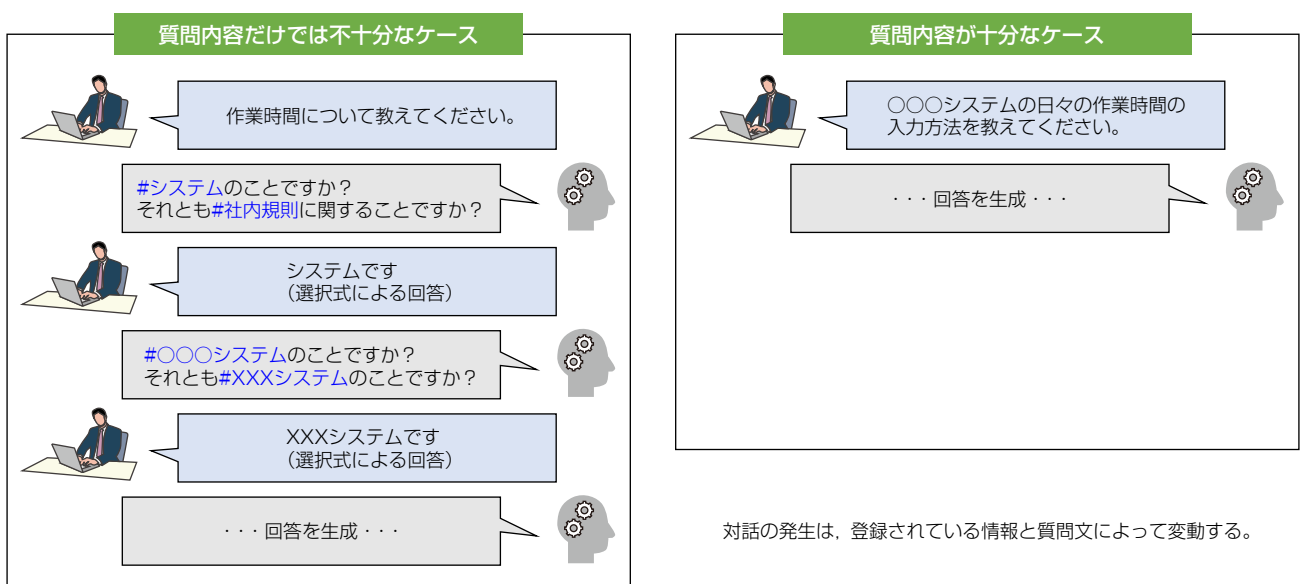


図4-対話のイメージ

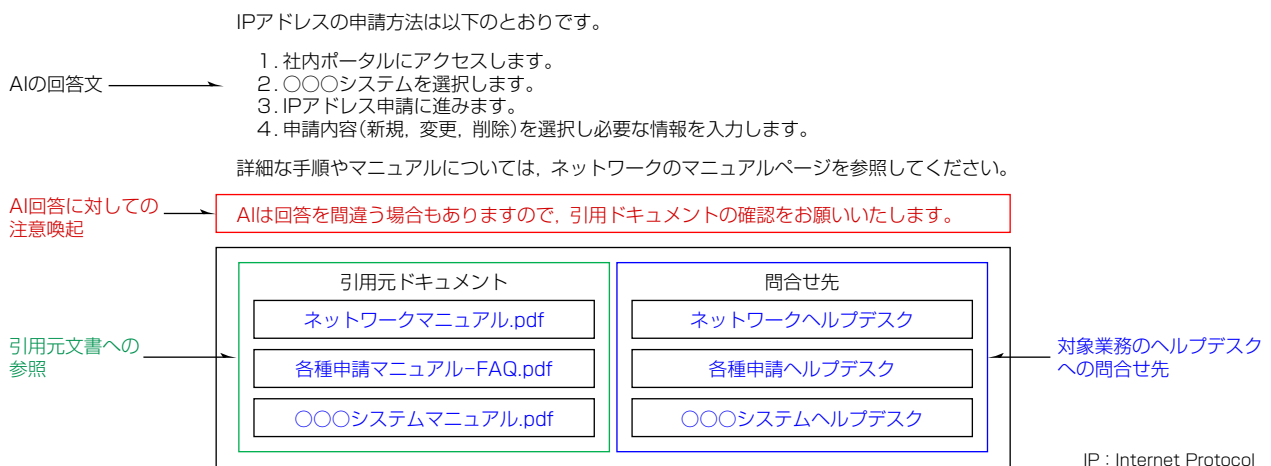


図5-AIチャットボットによる回答例

5. む す び

1995年のWindows^(注4)95の登場によってインターネットが急速に普及し、今ではなくてはならない社会インフラになった。今後AIも同じように誰もが使えて、AIを活用できないと競争力が失われ淘汰(とうた)されていく時代が到来することが想定される。またチャットボットのような新しいサービスだけにAIが適用されるのではなく、既存の情報システムへの組み込みや融合が進んでいくと考えられる。このAI時代の技術動向を踏まえて、今後も顧客のニーズに合わせて更なるソリューションの拡充を進めていく。

(注4) Windowsは、Microsoft Corp.の登録商標である。

参 考 文 献

- (1) 永田祥平，ほか：Azure OpenAI ServiceではじめるChatGPT/LLMシステム構築入門，技術評論社（2024）