



[入門]

LLM

アプリ開発

——基本・LLMのしくみ・
MCP・AIセキュリティ

[入門]

LLMアプリ開発

— 基本・LLMのしくみ・MCP・AIセキュリティ

CONTENTS

第1章

LLMアプリ開発入門

- 1-1 LLMの基本 松本 和高 6
- 1-2 入門LangChain 松本 和高 16
- 1-3 LangChain + Streamlitを使った翻訳アプリの実装 松本 和高 26
- 1-4 LangChain + Next.jsを使った検索アプリの実装 松本 和高 34
- 1-5 LCELと高度なLangChainコンポーネント 松本 和高 47

第2章

LLMのしくみ

- 2-1 LLMの基本構造を理解しよう 藤本 敬介 58
- 2-2 学習プロセスを知ろう 大田 竹蔵、藤原 知樹 68
- 2-3 小さく実装してみよう 大谷 真也 76
- 2-4 モデルの違いを学ぼう 服部 響 88
- 発展編 大規模化するLLMの
学習・開発を支える技術 藤原 知樹、大田 竹蔵 98

第 3 章

MCPでどう変わる？ LLM アプリ開発

- 3-1 LLM アプリ開発の現在地 江頭 貴史 110
- 3-2 MCP のしくみ 御田 稔 117
- 3-3 MCP を使った LLM アプリ開発 岩本 隆史 128
- 3-4 MCP を自社で活用する 江崎 広太、大久保 諒 139

第 4 章

AI セキュリティ入門

- 4-1 AI エージェントにおけるプロンプトをめぐる攻防 川喜田 将之 152
- 4-2 AI エージェントに対する攻撃手法 川喜田 将之 159
- 4-3 AI を安全に活用するために押さえない防御策 川喜田 将之 167

本書について

LLMは汎用的な処理が可能で、私たちの可能性を広げてくれます。自然言語で入力できるため、専門知識がない方でも使いやすい点が魅力です。さまざまなことができますが、その反面、どこから学べばよいのかわからないと感じる方も少なくないでしょう。

本書は、そのような方に向けて、『Software Design』に掲載されたLLMアプリケーション開発に関する過去記事を厳選して収録しています。読み終えるころには、LLMをどのように扱い、どのようにサービスやプロダクトへ組み込めばよいか、その糸口がつかめるはずです。

LangChainを用いたLLMアプリ開発の基礎に加え、開発時に押さえておきたいLLMのしくみ、MCPの活用方法、AIセキュリティについて、1冊で学べます。LLMアプリ開発に挑戦するための第一歩となるでしょう。

初出一覧

第1章	LLMアプリ開発入門	Software Design2024年8月号 第1特集
第2章	LLMのしくみ	Software Design2026年1月号 第1特集 Software Design2026年2月号 特別企画
第3章	MCPでどう変わる？ LLMアプリ開発	Software Design2025年9月号 第1特集
第4章	AIセキュリティ入門	Software Design2025年12月号 第2特集

本書のサポートページ

本書に関する補足情報、訂正情報、サンプルファイルのダウンロードは、下記のWebサイトで提供いたします。なお、サンプルファイルの提供先につきましては各記事をご参照ください。

<https://gihyo.jp/book/2026/978-4-297-15470-7>

【免責】

●本書をお読みになる前に

- 本書に記載された内容は、情報の提供のみを目的としています。したがって、本書を用いた開発、製作、運用は、必ずお客様自身の責任と判断によって行ってください。これらの情報による開発、製作、運用の結果について、技術評論社および著者はいかなる責任も負いません。
 - 本書記載の情報は各記事の執筆時(再編集時の修正も含む)のもので、ご利用時には変更されている場合もあります。
 - また、ソフトウェアに関する記述は、各記事に記載されているバージョンをもととしています。ソフトウェアはバージョンアップされる場合があり、本書での説明とは機能内容や画面図などが異なってしまうこともあり得ます。ご購入の前に、必ずバージョン番号をご確認ください。
- 以上の注意事項をご承諾いただいたうえで、本書をご利用ください。これらの注意事項をお読みいただかずにお問い合わせいただいても、技術評論社および著者は対処しかねます。あらかじめ、ご承知おきください。

●商標、登録商標について

本書に登場する製品名などは、一般に各社の商標または登録商標です。なお、本書中に™、©、®などのマークは記載しておりません。