

生成AIパスポート 対策テキスト

第3章 いまの動向

RAGとAIエージェント。AIが「答える」から「動く」に変わった章。

学習前のごしらえ／主なサービス／ディープフェイクと偽情報
RAG／チャンクとベクトルデータベース／AIエージェントとMCP
重要用語 20語・確認問題 9問・図解 10点

03

AI資格ラボ

YouTubeチャンネル登録者への配布テキストです。

動画「【生成AIパスポート】第3章 現在の生成AIの動向」と対応しています。

はじめに この本の使い方

この本は、YouTubeチャンネル「AI資格ラボ」の動画「**第3章 現在の生成AIの動向**」に対応した、配布用のテキストです。動画を見ていない方でも、これ一冊で第3章が最後まで読み切れるように書いてあります。

この本が扱う範囲

生成AIパスポートの第3章は、公式シラバス（出題範囲表）で**20語**です。第1章の39語、第2章の62語にくらべると**いちばん少ない章**で、1冊で足ります。

	テーマ	語数
1	生成AIが出来ることと主なサービス	10語
2	ディープフェイク（深層偽造）技術	2語
3	RAG	3語
4	AIエージェント	5語

⇒ ただし**新しい言葉が多い**のがこの章です。RAG、チャンク、ベクトルデータベース、AIエージェント、MCP、GenSpark、Manus、Skywork AI、Veo3。**聞いたことのない名前が並びます**。そこだけ覚悟してください。

この章は、何の話か

第1章と第2章は、**AIの中身**の話でした。ニューロンがあって、重みがあって、Transformerがあって。正直、しんどかったと思います。

第3章は変わります。中身の話は終わりです。ここからは、**それで何ができるのか。何が危ないのか**。そして、**AIが自分で動き出す**という話です。

前の章とのつながり

この章は、第2章を見た方に**効く仕掛け**が2つあります。単独でも読めますが、知っているのと刺さります。

- **RAG**は、第2章で出てきた**ハルシネーション**（もっともらしい嘘）への**答え**です。
- **AIエージェント**は、第2章の最後に出てきた**Operator**の**正体**です。

この本の構成

- **本文**……ふつうに読める文章です。まずここを読んでください。
- **試験ポイント**（青い枠）……そのまま問題になる所です。試験直前はここだけ拾い読みできます。
- **△マークの枠**（赤い枠）……**間違えやすい所・引っ掛けが仕込まれる所**です。
- **用語**（紫の帯）……シラバスに名前が載っている用語です。全部で20語あります。
- **確認問題**（緑の枠）……テーマの区切りに3問ずつ、合計9問あります。
- **チェックリスト**（巻末）……20語を自分で説明できるか、最後に確かめられます。

おすすめの進め方

1. まず**本文を最後まで通して読む**。分からない所で止まらず、飛ばして進んでかまいません。
2. 次に**確認問題9問**を、本文を見ずに解く。ここで落ちた所が、あなたの弱点です。
3. 落ちた所だけ本文に戻り、**自分の言葉で言い直す**。読むより言い直したほうが残ります。
4. 試験直前は、**試験ポイントの枠と、巻末の用語集だけ**を見返す。

この本・動画・練習問題の回し方

この本は**単体でも読めます**が、動画と練習問題と合わせると回転が速くなります。おすすめは次の4ステップです。

1. **この本（章ごとのPDF）を読む**。無料です。
2. **その章の動画を見る**。本と同じ順番・同じ図で説明しています。
3. **練習問題を解く**。全5章468問と、本番と同じ60問の模擬試験があります。登録も費用もありません。
4. **間違えた問題の解説から、動画のその場面へ飛ぶ**。どこを見直せばいいか探さなくて済みます。

動画と合わせて使う

- この本は、YouTubeチャンネル**AI資格ラボ**の動画 **第3章 現在の生成AIの動向** と同じ順番・同じ図で作ってあります。
- **動画で流れをつかみ、この本で確かめる**。あるいは**この本を先に読んでから動画を見る**。どちらでも構いません。
- 印刷は**A4・実物大（100%）**で。図の中の文字まで読める大きさに作ってあります。

はじめに	この本の使い方	1
第3章	この章の全体像	4
3-1	学習の前に、データを整える	5
	画像のリサイズ／正規化	
3-2	データを増やす、質を上げる	6
	データの水増し（augmentation）／データ拡張技術／リマスタリング	
	確認問題①（3-1・3-2）	7
3-3	主なサービス	8
	Claude／Gemini／Sora／Veo3／自己回帰モデル	
3-4	ディープフェイクと偽情報	9
	ディープフェイク（深層偽造）技術／偽情報（ディスインフォメーション）	
	確認問題②（3-3・3-4）	10
3-5	RAG 答える前に、資料を探す	11
	RAGとは／何が嬉しいか／ファインチューニングとの違い	
3-6	チャンクとベクトルデータベース	13
	資料を切る／意味を数字にする	
3-7	AIエージェントとMCP	15
	AIエージェント／4つの繰り返し／GenSpark・Manus・Skywork AI／MCP	
	確認問題③（3-5～3-7）	17
まとめ	20語を、流れで覚える	18
用語集	重要用語20語	20

第3章 この章の全体像

先に地図を配ります。この章は**4つのテーマ**でできています。前半は「作る前の準備」と「危ない使い方」、後半が本命の**RAG**と**AIエージェント**です。

	何の話か	この本での場所
1	学習させる前の下ごしらえと、主なサービス	3-1・3-2・3-3
2	ディープフェイクと偽情報（危ない使い方）	3-4
3	RAG（答える前に資料を探す）	3-5・3-6
4	AIエージェント（AIが自分で動く）	3-7

ここが、この章いちばんの引っかけ

テーマ1は、公式シラバスに「学習項目」として**テキスト生成AI／画像生成AI／音楽生成AI／音声生成AI／動画生成AI**の5つが並んでいます。5つ並んでいると、**それぞれの仕組みを覚えるのかな**と思いますよね。

……違うんです。

→ 同じ項目の「キーワード」に並んでいるのは、**5種類の名前ではありません**。画像のリサイズ、正規化、データの増強、データ拡張技術、リマスタリング。**全部、学習させる「前」のデータの整え方**です。試験に出るのは**そちら**なので、この本もそこから始めます。

覚え方の芯

細かい語は後から入ります。まず、この章全体を貫く一文だけ持って帰ってください。

第3章は、AIが「答える」から「動く」に変わった章。それだけです。

3-1 学習の前に、データを整える

AIに学習させるとき、**データはそのままでは使えません**。たとえば画像を1万枚集めたとします。大きさもバラバラ、明るさもバラバラ。このまま食べさせると、AIは混乱します。

そこで、**2つの下ごしらえ**をします。

画像のリサイズ Resize

画像の**大きさ（縦横のピクセル数）を揃えること**。たとえば全部を256×256にする。AIは決まった大きさの入力しか受け取れないため、揃えないとそもそも入らない。

正規化 Normalization

データの**値の範囲を揃えること**。画素の明るさは0～255の数字だが、これを0～1に直すのが代表例。数字の桁が大きいままだと学習が不安定になるため。



図3-1 リサイズは大きさを揃える。正規化は値を揃える

なぜ、それぞれ必要なのか

リサイズが要る理由は単純です。ニューラルネットワークは、入口の数があらかじめ決まっています。大きさがバラバラだと**そもそも入らない**のです。

正規化が要る理由は、学習の安定です。0～255のまま計算すると、数字が大きすぎて**学習が暴れます**。桁を揃えてやると、素直に学習してくれる。

試験ポイント | この2語は対で聞かれる

- **リサイズは「大きさ」を揃える。**
- **正規化は「値」を揃える。**
- どちらも**学習させる前**の処理。生成AIそのものの仕組みではない。

⇒ ⚠ **「正規化」は日常語と紛らわしい語です。**ここでは**値の範囲を0～1などに揃えること**を指します。データベースの正規化（表の設計を整えること）とは別物です。

3-2 データを増やす、質を上げる

下ごしらえができました。でも、まだ問題があります。**データが足りない**のです。

AIの学習には、とにかく大量のデータが要ります。でも、1万枚集めるのだって大変です。10万枚なんて、まず無理です。

データの水増し (augmentation) Data Augmentation

手持ちのデータを**加工して、枚数を増やすこと**。オーグメンテーションと読む。1枚の写真を左右反転・回転・明るさ変更・切り取りすることで、10枚ぶんの学習データにできる。

データ拡張技術

データの水増しをするための**手口をまとめた呼び方 (総称)**。水増しが「やること」、データ拡張技術が「その技術の呼び名」。

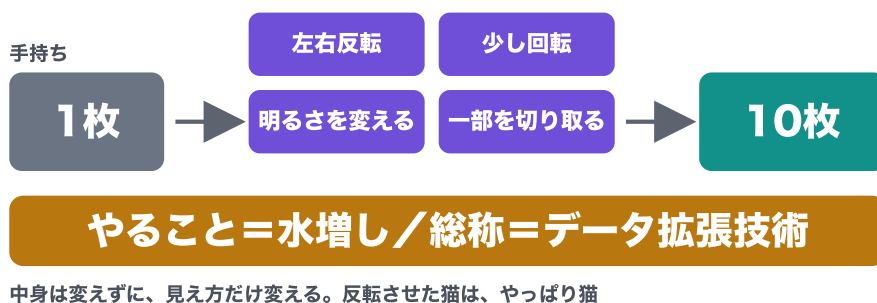


図3-2 1枚を加工して枚数を増やす。総称がデータ拡張技術

これは「水増し」であって「捏造」ではない

大事なのは、**中身は変えずに、見え方だけ変える**という点です。反転させた猫は、やっぱり猫です。データを**でっち上げているわけではありません**。

⇒ ⚠️ 「水増し」という日本語に引きずられないこと。不正な水増しの意味ではありません。同じ中身を、違う見え方で何枚も用意するという、正当な学習の工夫です。

もうひとつ、リマスタリング

リマスタリング Remastering

古い・粗いデータを、**作り直して質を上げる**こと。もとは音楽や映像の言葉で、古い録音を今の技術できれいにすること。生成AIでは解像度を上げる、ノイズを取る、色を戻す、といった処理を指す。

昔のレコードが「リマスター版」としてCDになる、あれです。生成AIの文脈では、**古い・粗いデータをAIで作り直して質を上げる**ことを指します。



図3-3 水増しは「数」、リマスタリングは「質」

試験ポイント | 混ざりやすい2語

- データの水増し＝数を増やす。1枚を10枚に。
- リマスタリング＝質を上げる。粗いものをきれいに。
- 迷ったら「数か、質か」で分ける。それだけで切り分けられる。

— 確認問題① (3-1・3-2)

確認問題①

第1問 画像の大きさを揃えることと、値の範囲を揃えること。それぞれ何とといいますか。

答

画像のリサイズと正規化。

リサイズは「大きさ」、正規化は「値」。どちらも学習させる前の下ごしらえです。

確認問題①

第2問 手持ちのデータを加工して枚数を増やすことを何とといいますか。その技術の総称は何とといいますか。

答

データの水増し (augmentation)。総称がデータ拡張技術。

水増しが「やること」、データ拡張技術が「その技術の呼び名」。中身は変えずに見え方だけ変えます。

確認問題①

第3問 古い・粗いデータをAIで作直して質を上げることを何とといいますか。

答

リマスタリング。

水増しは「数」、リマスタリングは「質」。この対比で覚えると混ざりません。

3-3 主なサービス

公式シラバスは、この項目で**サービスの名前**も挙げています。といっても、ほとんどは第2章で出てきた名前です。ここではやり直さず、**並べて確かめる**だけにします。

Claude

Anthropic（アンソロピック）の生成AI。長い文章を読ませるのが得意で、受け答えの丁寧さが評価されている。

Gemini

Googleの生成AI。最初から文章・画像・音声・動画をまとめて扱う設計になっている。

Sora

Open AIの動画生成AI。文章で指示すると映像が出てくる。

Veo3

Googleの動画生成AI。ヴィオ・スリーと読む。**SoraのGoogle版**と思えばよい。この章で新しく出てくる語。

試験ポイント | 対で覚える

- **Sora=Open AI。Veو3=Google。**どちらも**動画**生成。
- **Claude=Anthropic。Gemini=Google。**
- 会社名と結び付けられれば十分。細かい性能差は問われない。

自己回帰モデルが、なぜここに載っているのか

自己回帰モデル Autoregressive Model

自分が出した答えを**次の入力**にして、**1つずつ生成**していくやり方。文字が1つずつ出てくる、あの動きの正体。

第2章でやった語が、第3章のこの項目にも載っています。なぜか。**生成AIが「作れる」理由そのもの**だからです。

次に来そうな語を1つ出す。それを入力に足して、また次を出す。これを繰り返すから、文章が伸びていきます。**サービスの名前と並べて「どうやって作っているのか」を確かめる**位置づけだと考えてください。

3-4 ディープフェイクと偽情報

ここから**危ない話**です。技術そのものより、**危険性**のほうが問われます。

ディープフェイク（深層偽造）技術 Deepfake

ディープラーニングを使って、本物そっくりの偽物を作る技術。実在する人の顔を別の映像に貼り替えたり、実在する人の声で言っていないことを喋らせたりできる。

何ができてしまうのか。実在する人の顔を、別の映像に貼り替える。実在する人の声で、言っていないことを喋らせる。しかも、**見分けがつきません**。

なぜ、見分けがつかないのか

第2章のGANを思い出してください。偽物を作る側と、それを見破る側を競わせる仕組みでした。見破られなくなるまで鍛えるわけですから……そりゃあ、見分けがつかなくなります。

実際に事件も起きています。経営者の声をまねた電話で**送金させる**。政治家が言っていないことを**言ったことにする**。

⇒ ⚠ **技術そのものは中立です**。映画の吹き替えや、故人の声の再現にも使われます。試験で問われるのは**使い方の危険性**のほうです。「ディープフェイクは悪いものか」ではなく「何ができてしまうか」で考えてください。

セットで出る、偽情報

偽情報（ディスインフォメーション） Disinformation

意図的に流される、嘘の情報。うっかり間違えて広がったもの（誤情報／ミスインフォメーション）とは区別される。分かれ目は**悪意があるかどうか**。

誤情報

うっかり間違えて広がったもの
悪意なし

偽情報

わざと人をだますために流すもの
＝ディスインフォメーション・悪意あり

分かれ目は「悪意があるかどうか」

図3-4 分かれ目は「悪意があるかどうか」

ここは「**意図的に**」がポイントです。うっかり間違えて広がったものは**誤情報**。わざと人をだますために流すものが**偽情報＝ディスインフォメーション**。

なぜ、生成AIの章に出てくるのか

生成AIのせいで、偽情報を作るコストがほぼゼロになったからです。昔は、嘘の記事を100本書くのは大変でした。いまは一瞬です。しかも、それらしい。

試験ポイント | ハルシネーションとの違い

- ハルシネーションは、AIが勝手に間違える。悪意はない。仕組み上そうなる（第2章）。
- 偽情報は、人間がわざとやる。悪意がある。
- 誤情報は、人間がうっかり間違える。悪意はない。
- 誰が／わざとか、の2点で3つが切り分けられる。

確認問題② (3-3・3-4)

確認問題②

第1問 動画生成AIのうち、Open AIのものとGoogleのものを、それぞれ何といいますか。

答

Open AIが**Sora**、Googleが**Veo3**。

対で覚えるのが早いです。どちらも動画生成。Veo3はこの章で新しく出る語です。

確認問題②

第2問 ディープラーニングを使って本物そっくりの偽物を作る技術を何といいますか。

答

ディープフェイク（深層偽造）技術。

第2章のGAN（作る側と見破る側を competing させる仕組み）が下地です。試験では危険性が問われます。

確認問題②

第3問 意図的に流される嘘の情報を何といいますか。うっかりの間違いとの分かれ目は何ですか。

答

偽情報（ディスインフォメーション）。分かれ目は**悪意の有無**。

うっかりは誤情報。AIが勝手に間違えるのはハルシネーションで、こちらは人間がわざとやる話です。

3-5 RAG | 答える前に、資料を探す

ここからが、この章の**本命**です。実務でいちばん耳にする語でもあります。

RAG (Retrieval-Augmented Generation) Retrieval-Augmented Generation

ラグと読む。日本語では**検索拡張生成**。答える前に**資料を検索し、見つけた資料を読ませてから答えさせる**仕組み。ハルシネーションへの代表的な対策。

前の章の話から入ります

第2章でハルシネーションをやりました。AIがもっともらしい嘘をつく。なぜか。**次に来そうな言葉を選んでいて、それが本当かどうかは見えていない**からでした。辞書を引いていないのです。

……では、**引かせればいいんじゃないか**。答える前に、資料を検索させる。見つけた資料を読ませてから、答えさせる。**それがRAGです。**

順番でいうと、こうです。①質問が来る。②先に資料を探す。③見つけた資料を、質問と一緒にAIへ渡す。④AIはそれを読んでから答える。



この「探してから答える」がRAG

図3-5 この「探してから答える」がRAG

何が嬉しいのか | 3つ

	嬉しいこと	なぜ
①	嘘が減る	手元に資料があるので、でっち上げなくて済む
②	新しい情報に答えられる	AIは学習した時点までしか知らないが、資料は今日のものでいい
③	社内の情報に答えられる	インターネットに無い、自社の規則やマニュアルでも渡せる

そして、いちばん効くのが**モデルを作り直さなくていい**という点です。

ファインチューニングとの違い

第2章のファインチューニングは、**モデルそのものを追加学習させる**話でした。RAGは違います。**モデルは触らず、渡す資料を変えるだけ**です。



図3-6 モデルを触るか、資料を変えるか

試験ポイント | RAGの言い回し

- **RAG＝検索拡張生成**。答える前に資料を探し、読ませてから答えさせる。
- **ハルシネーション対策**として出題されやすい。
- **モデルは触らない**。ここがファインチューニングとの決定的な違い。
- だから**安くて速い**。実務でいちばん使われている理由もそこ。

3-6 チャンクとベクトルデータベース

では、どうやって「探す」のか。ここに**2つの語**が出ます。RAGとセットで問われるので、必ず押さえてください。

チャンク Chunk

資料を**あらかじめ細かく切っておいた、その一つひとつ**。かたまり、という意味。1冊の本を丸ごと渡すことはできないので、先に切っておく。

資料をそのまま渡すことはできません。**1冊の本を丸ごと渡されても困る**のと同じです。だから、あらかじめ細かく切っておきます。この切った一つひとつが**チャンク**です。

ベクトルデータベース Vector Database

チャンクを**意味を表す数字の並び（ベクトル）に変換して、しまっておく保管庫**。数字にしておくと、意味が近いかどうかを計算で比べられる。

なぜ、数字にするのか

言葉のままだと、**意味が近いかどうか比べられない**からです。

たとえば「犬」と「わんこ」。**文字は全然違うのに、意味は近い**。文字を見比べているかぎり、この2つは別物です。ところが**数字にしておくと、その「近さ」が計算できる**。

その数字をしまっておく保管庫が、**ベクトルデータベース**です。質問が来たら、**質問も数字にして、近いチャンクを引っばってきます**。



図3-7 切って、数字にしてしまう

試験ポイント | RAGの中身は3段

- ①資料をチャンクに切る。
- ②意味を数字にして、ベクトルデータベースへ入れる。
- ③質問が来たら近いものを探して、AIに読ませる。
- RAG・チャンク・ベクトルデータベースは3点セットで出る。

よくある取り違い

- ⇒ ⚠ ベクトルデータベースは「AIそのもの」ではありません。資料を数字にしてしまっておく**保管庫**です。考えるのはあくまでAIの側で、こちらは引き出しの役目。
- ⇒ ⚠ RAGを使っても、AIが賢くなるわけではありません。モデルは何も変わりません。**渡す資料が増えるだけ**です。だから、資料に無いことは相変わらず答えられません。

3-7 AIエージェントとMCP

お待たせしました。第2章の最後に出てきた**Operator**の、正体です。

AIエージェント AI Agent

目的を渡すと、手順を自分で考えて、道具を使って、最後までやるAI。聞かれたことに答えるだけの従来のAIと、そこが違う。

これまでのAIと、何が違うのか

これまでのAIは、聞かれたことに答えるだけでした。「メールの文面を書いて」と言えば、文面が返ってくる。……**送るのは、あなた**です。

AIエージェントは違います。「取引先にお礼のメールを送っておいて」と言うと、**誰宛か調べて、文面を書いて、送信ボタンまで押します**。



図3-8 答えるAIと、動くAI

第2章の**Operator**が、まさにこれでした。ブラウザを開いて、検索して、フォームに入力する。**答えるAIから、動くAIへ**。その「動くAI」の呼び名が、**AIエージェント**です。

仕組みは、4つの繰り返し

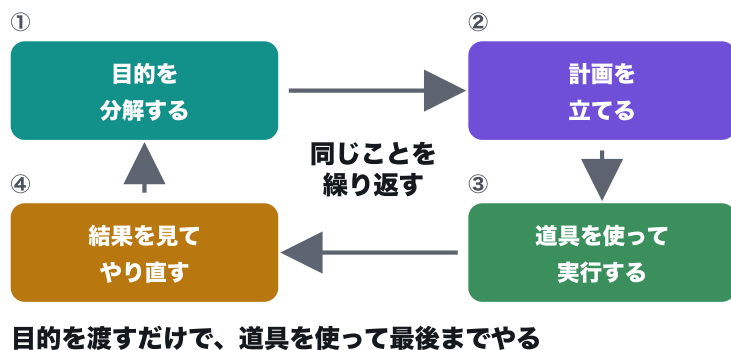


図3-9 目的を分解し、計画を立て、道具を使い、結果を見てやり直す

ざっくり言うと、**目的を分解する→計画を立てる→道具を使って実行する→結果を見て、やり直す**。これを繰り返します。……**人間の仕事の進め方と同じ**です。そこが新しい。

ツール事例は3つ

公式シラバスには、エージェントの実例が3つ載っています。**名前だけ押さえてください**。どれも新しいサービスなので、細かい機能は問われません。

GenSpark

ジェンスパーク。**AIエージェントを使った検索エンジン**。聞かれたことに対して、自分でいくつも検索して、まとめた答えを作る。

Manus

マナス。**汎用のAIエージェント**。指示すると、調べ物から資料作りまで通しでやる。

Skywork AI

スカイワーク・エーアイ。こちらも汎用型で、**資料やスライドを作るのが得意**とされている。

⇒ ⚠ **3つとも新しいサービスです**。できることは変わっていきます。試験では**名前と「エージェント系」だけ結び付けば十分**。機能の細部を追いかける必要はありません。

最後に、MCP

MCP Model Context Protocol

モデル・コンテキスト・プロトコル。**Anthropic**が出した決まりごとで、**AIが外の道具やデータにつながるための共通の差し込み口**。AIエージェントとセットで出る。

たとえ話をします。昔、**充電ケーブルが機種ごとに違って、全部バラバラでしたよね**。メーカーが違っていると、挿さらない。それが、**規格が統一されて、どれでも挿さるようになった**。

MCPは、そのAI版です。MCPに合わせておけば、ChatGPTだろうがClaudeだろうがGeminiだろうが、同じやり方で、同じ道具やデータにつながります。



充電ケーブルの規格が統一されて、どれでも挿さるようになったのと同じ

図3-10 AIが外の道具につながるための共通の差し込み口

試験ポイント | エージェントとMCP

- AIエージェント＝目的を渡すと、自分で考えて、道具を使って、最後までやるAI。
- 実例はGenSpark・Manus・Skywork AIの3つ。名前だけでよい。
- MCP＝外の道具やデータにつなぐための共通の決まりごと（Anthropic）。
- エージェントが「手足を増やす」ための規格と考えると、セットで思い出せる。

— 確認問題③（3-5～3-7）

確認問題③

第1問 答える前に資料を検索して、それを読ませてから答えさせる仕組みを何とといいますか。日本語では何とといいますか。

答

RAG (Retrieval-Augmented Generation)。日本語では**検索拡張生成**。

ハルシネーション対策として出ます。ファインチューニングと違い、モデルそのものは触りません。

確認問題③

第2問 RAGで、資料を細かく切ったかたまりを何とといいますか。それをしまっておく保管庫は何とといいますか。

答

チャンク。保管庫は**ベクトルデータベース**。

意味を数字にしてしまうので、「犬」と「わんこ」のように文字が違ってても近さを計算できます。

確認問題③

第3問 AIが外の道具やデータにつながるための共通の決まりごとを何とといいますか。どこが出したのですか。

答

MCP (Model Context Protocol)。**Anthropic**が出した。

充電ケーブルの規格統一のAI版。AIエージェントとセットで問われます。

まとめ 20語を、流れで覚える

最後に、20語を**流れ**で並べ直します。バラバラに覚えるより、この順で1本につないだほうが残ります。

① 学習させる前の下ごしらえ（5語）

語	何をする
画像のリサイズ	大きさを揃える
正規化	値を揃える
データの水増し	数を増やす (augmentation)
データ拡張技術	水増しの技術の総称
リマスタリング	質を上げる

⇒ 「数か、質か」で水増しとリマスタリングを分ける。ここは**毎回まざる**所です。

② 主なサービス（5語）

Claude=Anthropic。Gemini=Google。Sora=Open AIの動画。Veo3=Googleの動画。そして**自己回帰モデル**=自分が出した答えを次の入力にして1つつ生成していくやり方。

③ 危ない話（2語）

ディープフェイク（深層偽造）技術=本物そっくりの偽物を作る技術。偽情報（ディスインフォメーション）=わざと流す嘘。**AIが勝手に間違えるのがハルシネーション、人間がわざとやるのが偽情報。**

④ RAG（3語）

RAG=答える前に資料を探して、読ませてから答えさせる。ハルシネーションへの答え。**チャンク**=資料を切ったもの。**ベクトルデータベース**=意味を数字にしてしまう保管庫。

⑤ AIエージェント（5語）

AIエージェント=目的を渡すと、自分で考えて、道具を使って、最後までやる。第2章の**Operator**の正体。実例が**GenSpark・Manus・Skywork AI**。外の道具につなぐ共通の決まりごとが**MCP**。

この章から持って帰る一文

- **第3章は、AIが「答える」から「動く」に変わった章。**
- 前半（下ごしらえ）は**作る前**の話、後半（RAG・エージェント）は**使うとき**の話。
- どちらも**生成AIそのものの仕組み**ではなく、**その周りで起きていること**を問う章です。

次の章は**第4章「情報リテラシー・基本理念とAI社会原則」**です。いちばん語数が多く、技術の話がほとんど出てきません。法律、権利、ルールの章です。ただ、今日やった**ディープフェイクと偽情報**が、そのまま次につながります。**危ないと分かったから、ルールを作った**。そういう流れです。

用語集

重要用語20語

公式シラバス第3章の詳細キーワード20語です。説明できるかを確かめてください。読めるだけでは足りません。

画像のリサイズ p.5

画像の大きさ（縦横のピクセル数）を揃えること。AIは決まった大きさの入力しか受け取れないため、学習の前に揃える。

正規化 p.5

データの値の範囲を揃えること。画素の0～255を0～1に直すのが代表例。桁が大きいままだと学習が不安定になるため。

データの水増し (augmentation) p.6

手持ちのデータを加工して枚数を増やすこと。反転・回転・明るさ変更・切り取りなど。中身は変えず、見え方だけ変える。

Claude p.8

Anthropicの生成AI。長い文章を読ませるのが得意で、受け答えの丁寧さが評価されている。

Gemini p.8

Googleの生成AI。最初から文章・画像・音声・動画をまとめて扱う設計。

Sora p.8

Open AIの動画生成AI。文章で指示すると映像が出てくる。

ディープフェイク（深層偽造）技術 p.9

ディープラーニングを使って本物そっくりの偽物を作る技術。顔の貼り替えや、実在する人の声で喋らせることができる。

偽情報（ディスインフォメーション） p.9

意図的に流される嘘の情報。うっかり広まった誤情報とは、悪意があるかどうかで分かれる。

データ拡張技術 p.6

データの水増しをするための手口をまとめた呼び方（総称）。水増しが「やること」、こちらが「その技術の呼び名」。

リマスタリング p.6

古い・粗いデータを作り直して質を上げること。解像度を上げる、ノイズを取る、色を戻すなど。水増しが「数」、こちらは「質」。

Veo3 p.8

Googleの動画生成AI。ヴィオ・スリー。SoraのGoogle版と考えるとよい。第3章で新しく出る語。

自己回帰モデル p.6

自分が出した答えを次の入力にして、1つずつ生成していくやり方。文字が1つずつ出てくる動きの正体。

RAG (Retrieval-Augmented Generation) p.11

検索拡張生成。答える前に資料を検索し、読ませてから答えさせる仕組み。ハルシネーション対策。モデルは触らない。

チャンク p.13

資料をあらかじめ細かく切っておいた、その一つひとつ。かたまりの意味。

ベクトルデータベース p.13

チャンクを意味の数字の並びに変換してしまっておく保管庫。数字なので意味の近さを計算で比べられる。

AIエージェント p.15

目的を渡すと、手順を自分で考えて、道具を使って、最後までやるAI。第2章のOperatorの正体。

GenSpark p.16

ジェンスパーク。AIエージェントを使った検索エンジン。自分でいくつも検索して、まとめた答えを作る。

Manus p.16

マナス。汎用のAIエージェント。調べ物から資料作りまで通しでやる。

Skywork AI p.16

スカイワーク・エーアイ。汎用型のAIエージェント。資料やスライドを作るのが得意とされる。

MCP p.16

Model Context Protocol。Anthropicが出した、AIが外の道具やデータにつながるための共通の決まりごと。

- ☐ 画像のリサイズ
- ☐ 正規化
- ☐ データの水増し (augmentation)
- ☐ データ拡張技術
- ☐ リマスタリング
- ☐ Claude
- ☐ Gemini
- ☐ Sora
- ☐ 自己回帰モデル
- ☐ Veo3
- ☐ ディープフェイク (深層偽造) 技術
- ☐ 偽情報 (ディスインフォメーション)
- ☐ RAG (Retrieval-Augmented Generation)
- ☐ チャンク
- ☐ ベクトルデータベース
- ☐ AIEージェント
- ☐ GenSpark
- ☐ Manus
- ☐ Skywork AI
- ☐ MCP