

1 章



AI とは

「AI」という言葉には幅広い概念が含まれていますが、簡単にいうと「大量のデータから有益なパターンを見つけ出す技術」を指します。AIは現在、製造や流通、金融などのさまざまな分野で用いられています。ここではAIの得意な分野と苦手な分野、AIの発達の歴史とともに、コンピュータへの学習の基本となる機械学習とディープラーニングを押さえましょう。

01

AI の定義

「AI」という言葉には幅広い概念が含まれており、決まった定義はありません。「大量のデータからパターンを見つけ出す技術」というイメージを押さえたうえで、幅広い分野にわたる技術であることを知っていきましょう。

○ 専門家によって異なるAIの見解

「AI」とは「Artificial Intelligence」の略で、「人工知能」とも呼ばれます。AIという言葉には幅広い概念が含まれ、専門家の間でも定義が定まっていません。その理由の1つに、「知能とは何か」の明確な定義が難しいことが挙げられます。知能をどう捉えるかは専門家によって見解が異なり、1つの明確な定義を示すことは困難といえます。

実務や研究などのツールとしてAIを活用する際は、「**大量のデータから有益なパターンを見つけ出す技術**」と大まかに捉え、「どんなデータが使えるのか」「どんなパターンを見つけるAIが有益か」を考えていくのがよいでしょう。

■ 専門家によるAIの定義の例

専門家	定義
中島秀之（公立はこだて未来大学） 武田英明（国立情報学研究所）	人工的につくられた知能をもつ実態。あるいは、それをつくろうとすることで知能全体を研究する分野
西田豊明（京都大学）	「知能をもつメカ」ないしは「心をもつメカ」
溝口理一郎（北陸先端科学大学院）	人工的につくった知的な振る舞いをするためのもの（システム）
長尾 真（京都大学）	人の頭脳活動を極限までシミュレートするシステム
堀 浩一（東京大学）	人工的につくる新しい知能の世界
浅田 稔（大阪大学）	知能の定義が明確でないので、人工知能を明確に定義できない
松原 仁（公立はこだて未来大学）	究極には人と区別がつかない人工的な知能のこと
池上高志（東京大学）	自然に我々がペットや人に接触するような、情動と冗談に満ちた相互作用を、物理法制に関係なく、あるいは逆らって、人工的に作り出せるシステム

出典：松尾 豊『人工知能は人間を超えるか』（KADOKAWA）より一部抜粋

AIが用いられる分野

1

AIとは

AIは**幅広い分野で活用**されています。前述したように、AIは大量のデータから有益なパターンを見つけ出す技術なので、アイデア次第で産業や分野を問わず活用する方法が考えられます。

まずは技術要素ごとに主な活用例を見てみましょう。このほかにも、さまざまな分野でAIは活用されています。また産業別の活用例では、身近な分野から意外な分野まで、多くの産業で使われていることがわかります。

技術要素と産業別の活用例

	画像解析	異常検知	需要予測	自然言語／音声解析	その他
製造	商品の不良品判定	機械の故障検知 スタッフの安全管理	出荷量予測		成分配合率の計算
流通	商品の破損検知		受注量予測 ダイナミックプライジング	チャットボット 部門振り分け	配送経路の自動化
不動産	外壁の劣化診断 物件の写真分類	設備の異常検知	価格予測		賃貸仲介マッチング
金融	カードの不正検知 帳票の読み取り	クレカの不正検知	為替予測		ローン審査
農業	病気・害虫検査 食物の品質検査	食物の生育不良検知 病害感染リスク	収穫量予測		
公共・インフラ	土木施設の劣化診断 犯罪者の割り出し	設備の老朽化検知	道路の交通量予測 鉄道の混雑予測	議事録作成 保育園入園の判断	犯罪予測 人口予測

まとめ

- ▶ AIはArtificial Intelligenceの略で、人工知能とも呼ばれる
- ▶ AIには決まった定義はなく、専門家の間でも見解が分かれる
- ▶ AIの活用は「大量のデータからどんなパターンを見つけると有益か」という視点で考えるとよい

02

AI の得意な分野と
苦手な分野

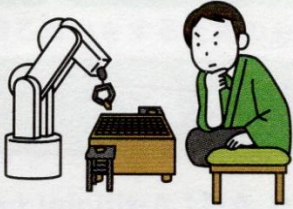
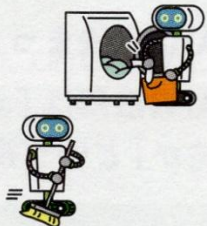
AIは万能な技術ではなく、できることは限られています。「AIは何でもできる技術」というイメージがもたれやすい理由について、「特化型AI」と「汎用型AI」という概念を学びながら理解していきましょう。

○ 特化型AIと汎用型AI

まず、「AIでできること」が限られていることを知るために、「**特化型AI**」の概念を押さえましょう。特化型AIとは、たとえば画像認識や自動運転、囲碁など、**特定のことだけを処理できるAI**を指します。人間の行っている特定の知的処理の一部を自動化するのが特化型AIです。

一方、「**汎用型AI**」は特定の処理に限られず、**人間の行っている幅広い知的処理に対応できるAI**を指します。人間と同様、幅広い分野において問題解決などが行えることが特徴ですが、現在の技術ではまだ実用化されていません。「AIは何でもできる」というイメージがあるのは、この「汎用型AI＝現在のAI」という誤解が生じているためと考えられます。現時点では、特化型AIについて理解できれば、実務や研究に関しては問題ないレベルといえます。

■ 特化型AIと汎用型AI

	特徴	イメージ
特化型AI	・ 人間のような意識はもたない ・ WatsonやAlpha Goなどの例がある ・ 特定の問題（画像認識、囲碁、クイズなど）を解くことに特化している	
汎用型AI	・ 人間のような意識をもつ ・ 幅広い問題を解くことができる ・ 現在の技術ではまだ実現していない	

○ 特化型AIで処理できる3つのこと

特化型AIで行える処理は、「**識別**」「**予測**」「**実行**」の3つに分けられます。

まず識別とは、入力された**データを識別**する処理のことです。たとえば、犬が写っている画像に「犬」、猫が写っている画像に「猫」というラベルを付けたデータを学習させ、ラベルが付いていない画像が「犬」か「猫」かを識別させる処理が挙げられます。

次に予測とは、入力された**データから将来の出来事や結果を予測**する処理のことです。たとえば、過去の販売実績をもとにした翌月の売上予測や、経済指標をもとにした株価予測などが当てはまります。

最後に実行とは、**識別や予測の結果に基づき、実際に行動として実行**する処理のことです。たとえば、有名画家の画風の再現では、画家の特徴を識別し、表現生成を実行します。また、お掃除ロボットは、どういう経路で進めば問題が起こらないかを予測し、経路を計画して実行します。

主にAI活用プロジェクトの概念実証（PoC：Proof of Concept）段階や立ち上げ段階では、識別や予測のタスクで何ができるかを考えていくことが多いです。しかし、識別段階や予測段階での精度の向上を重視するあまり、**精度の向上がビジネス上の成果にどう寄与するか**が不明瞭なまま検証を進めてしまうケースもあります。常に実行段階を念頭に置いて開発するのがベターです。

■ 「識別」「予測」「実行」の処理の違い



出典：安宅和人『人工知能はビジネスをどう変えるか』（ダイヤモンド社）―「AIの実用化における機能領域」を参考に作成

○ AIが人間より得意なこと

AIを活用すると、画像認識や株価予測など、さまざまなことが実現できます。AIが人間より得意なこととして、「**大量のデータを扱える**」「**作業を高速に処理できる**」「**作業精度を維持できる**」などが挙げられます。たとえば、数千万件の論文のなかから分野（ジャンル）を判定したり（**識別**）、経済指標から株価を予測したり（**予測**）することが、人間よりすばやく正確にできます。このような大量のデータを扱った識別や予測はAIの得意な作業です。

さらに、人間が行うと疲労などの影響により精度が落ちるような作業も、長時間にわたって高精度で行うことができます。たとえば、工場で不良品を検出する作業の場合、人間では作業者により判断にばらつきが生じたり、疲労により精度の低下が起こったりすることがあります。しかし、AIを活用すれば、高い精度を保ったまま、検出作業を続けられます。

このように作業精度を維持しながら処理できることもAIの得意分野です。

■ AIが人間より得意なこと



○ AIが人間より苦手なこと

一方で、AIが人間より苦手なこととして、「**問いを立てる**」「**感情を理解する**」「**五感のような身体感覚を伴うこと**」などが挙げられます。

AIは大量のデータを高速、かつ一定以上の精度を維持しながら処理できますが、「何のために分析するのか」と目的を考えることはありません。このようにAIは仮説や問いを立てることは苦手です。

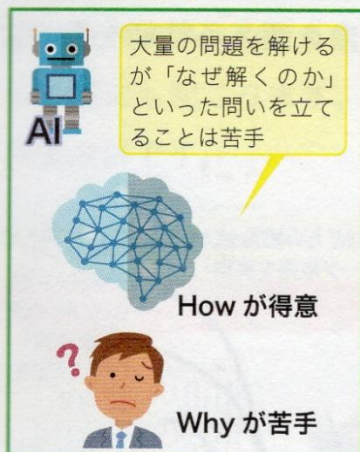
また、AIは感情を理解し、相手に働きかけることも苦手としています。そもそも現状では、**人間の感情について解明されていないことが多く**、それをAIに教え込むのが困難なためです。

さらに、人間の身体は、「何となく気配を感じる」というように、たくさんのセンサーを備えています。しかし、これらのセンサーをすべてコンピュータに搭載するのは困難です。身体感覚が必要な作業もAIは苦手としています。

■ AIが人間より苦手なこと

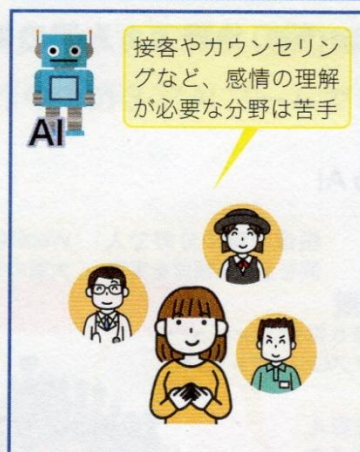
苦手①

問いを立てる



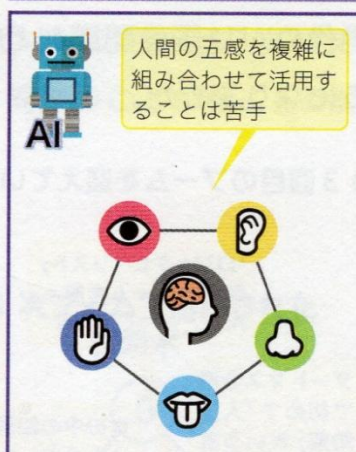
苦手②

感情を理解する



苦手③

身体感覚を伴うこと



まとめ

- ▶ 特化型AIと汎用型AIがあり、特化型AIのみが実在
- ▶ 特化型AIができる処理は「識別」「予測」「実行」の3つ
- ▶ AIは大量のデータを高速に処理することは得意だが、問いを立てたり感情を理解したり身体感覚が必要なことは苦手

03

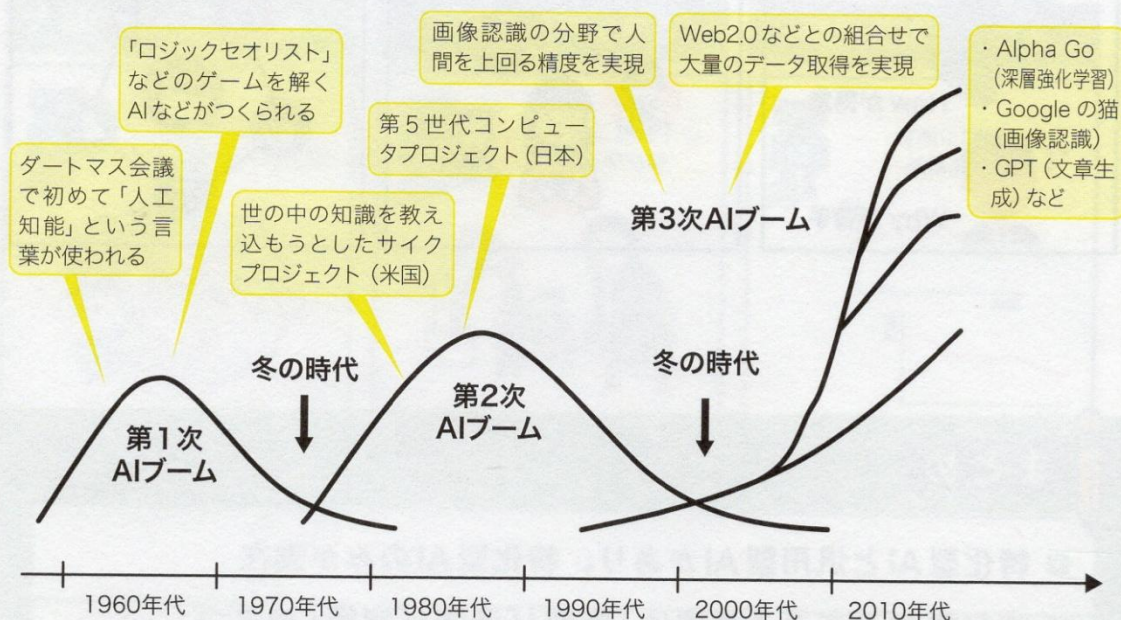
AI の発展過程

AIには過去に3回のブームがありました。1960年代の第1次AIブーム、1980年代の第2次AIブーム、そして2010年代の第3次AIブームです。それぞれの時代に注目されたAIを概観し、AIの発展過程を理解しましょう。

〇 ブームと冬の時代を繰り返してきたAI

AIは「ブーム」と「冬の時代」を繰り返して発展してきました。「人工知能」という言葉が誕生したとされる1950年代のAIは、「**トイプロBLEM**」と呼ばれる簡単な問題しか解けないレベルのものでした。それから60年ほどの時を経て、現代のAIは画像認識などの一部の分野で、人間の能力を超える性能をもつようになりました。

■ 3回目のブームを迎えているAI



○ トイプロブレム (推論と探索の時代)

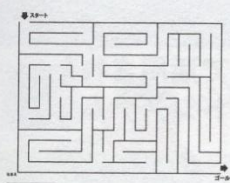
「人工知能」という言葉が誕生したとされる1956年のダートマス会議のワークショップで、「**ロジックセオリスト**」と呼ばれるプログラムが発表されました。ロジックセオリストは、数学の定理を証明するAIです。数値計算しかできないと考えられていた当時のコンピュータが、知的な数学の問題を解くのを目のあたりにして、コンピュータの可能性への期待が一気に高まりました。

これを皮切りに第1次AIブームに突入し、迷路を解くAIや、チェスなどのゲームをするAIなど、さまざまAIが開発されていきます。しかし、当時のAIは、迷路やチェスなどの**限定されたルールの中**でしか動作できないものでした。「組合せや状況分岐などが複雑な現実の問題は解けない」という限界が明らかになり、1970年代になるとAIへの研究熱は急速に冷めていきました。

AIへの期待感が高まって検証してみたものの、思ったような応用ができず、研究熱や応用への取り組みが激減する現象(**冬の時代**)は、のちの第2次AIブームの際にも起こります。昨今の第3次AIブームでも同様のことが起こるかは、今後注目です。

■ 第1次AIブームのポイント

成果



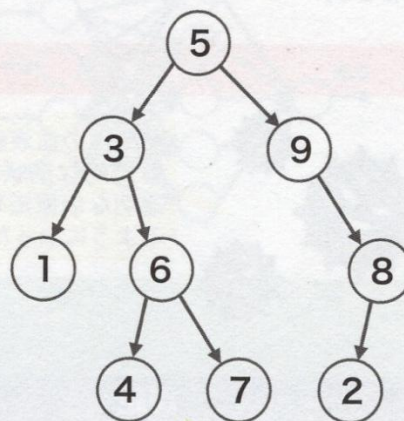
迷路やチェスなど限定されたルールの問題は解けるようになった

課題



組合せや状況分岐などが複雑な現実の問題は解けない

第1次ブームで活用された探索木



迷路のタスクを解く際、進む経路を探索木にして解いていた

○ エキスパートシステム (知識の時代)

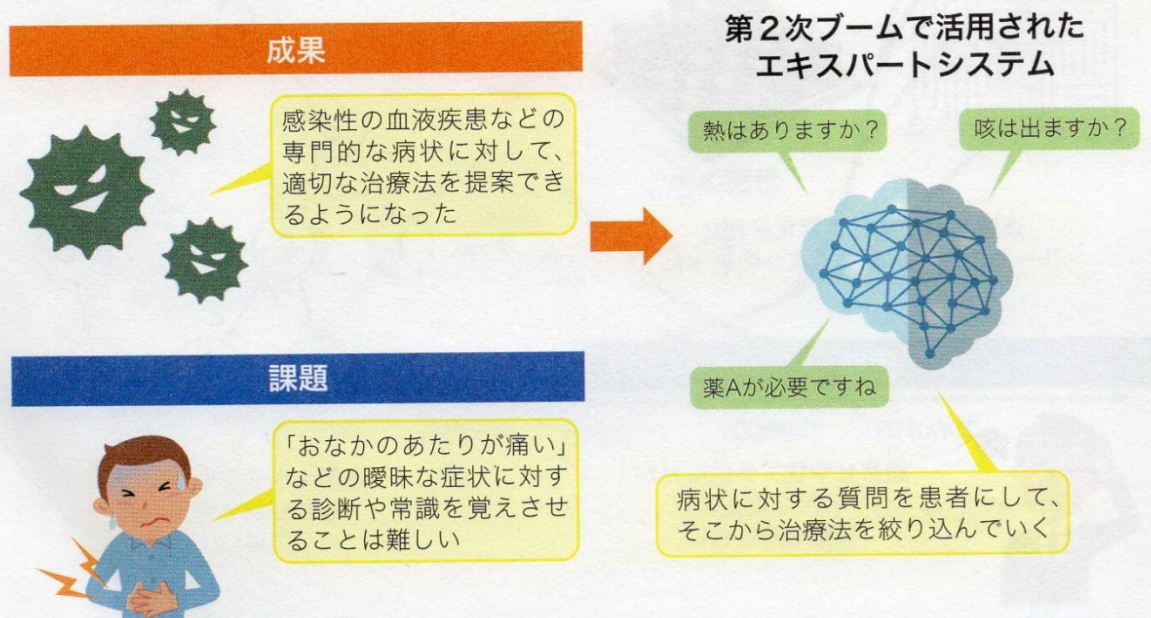
その後、トイプロBLEMしか解けないAIが、**現実の問題にも適用できる**ことが1980年代からわかり始め、第2次AIブームが始まります。

第2次AIブームの中心となったAIは「**エキスパートシステム**」と呼ばれるものです。エキスパートシステムでは、AIに専門的な知識を大量に覚えさせ、与えられた問いに対して専門家のように推論を行うことを目指しました。

当時のエキスパートシステムで有名なものが「**MYCIN**」です。MYCINは感染性の血液疾患のある患者を診断し、抗生物質を処方するように設計されたAIです。MYCINの精度は、専門医には劣りますが、専門ではない医師には勝るほどの精度があったとされています。しかし、「おなかのあたりが痛い」や「何となく気持ちが悪い」といった**曖昧な症状に対して診断することは難しく**、専門家の知識は覚えられても、人間のもっている膨大な常識を覚えさせるのはとても難しいことが明らかになりました。人間の知識をすべて記述することは不可能という壁にぶつかり、第2次AIブームも下火になっていきました。

ちなみに、高度な専門的な知識より、感覚や運動のようなものをコンピュータに教えるほうが計算量が多くなる現象を「モラベックのパラドクス」といいます。

■ 第2次AIブームのポイント



○ ニューラルネットワーク（機械学習・深層学習の時代）

1

AIとは

1回目と2回目のAIブームでは、**AIは限定的な知識しか獲得できない**という限界に直面しました。3回目のAIブームでは、**コンピュータ自らが大量のデータから学習するアプローチ**をとったことで、AIの活用の幅が大きく広がりました。第3次AIブームの重要な概念は「**ニューラルネットワーク**」と「**ビッグデータ**」です。ニューラルネットワークは、**人間の脳の神経細胞（ニューロン）を模したモデル**で、「層」と呼ばれる内部構造をもちます。

1990年代以降のWebの発達やSNSの浸透により、ニューラルネットワークで学習させるための十分なデータを確保できるようになり、ニューラルネットワークが機能し始めました。近年注目の**ディープラーニング**は、処理する層を複数用意し、判断の精度を向上させたニューラルネットワークの一種です。

■ 第3次AIブームのポイント

成果



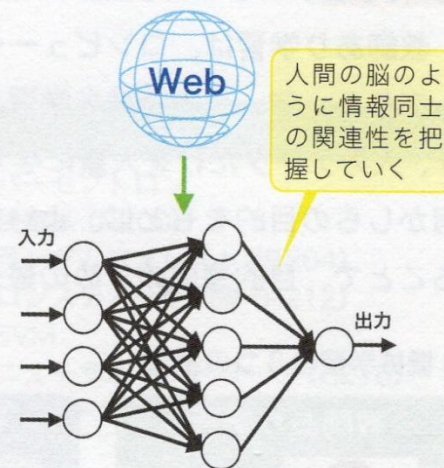
コンピュータ自らが大量のデータから学習するアプローチで、画像認識などの作業を中心に精度が向上

課題



複合的な認識が必要な作業はまだ苦手

ニューラルネットワークとビッグデータ



まとめ

- ▶ AIにはブームの時代と冬の時代が存在する
- ▶ 第1次は探索と推論の時代、第2次は知識の時代、第3次は学習の時代と呼ばれる
- ▶ 大量のデータを自ら学習することでブレークスルーが発生

04

機械学習とは

機械学習とは、コンピュータに大量のデータを学習させることで、精度の高い判断をさせようとする技術です。機械学習の代表的な手法である「教師あり学習」「教師なし学習」「強化学習」を押さえましょう。

○ 機械学習の概要と主な手法

機械学習とは、人間が経験を通して学習することを、**コンピュータに学習させて精度の高い判断をさせようとするデータ解析技術**です。コンピュータに大量のデータを入力し、そのデータから反復的に学習して、データに特有のパターンを見つけ出していきます。機械学習には主に、「**教師あり学習**」「**教師なし学習**」「**強化学習**」の3つの手法があります。

教師あり学習は、コンピュータに「入力データ」と「正解ラベル」をセットにして与え、データの特徴を学習させます。教師なし学習は、正解ラベルは与えず、入力データだけを大量に与え、そこから特徴を学習させます。強化学習は、何かしらの目的をもとに、よい行動には報酬を与え、悪い行動には罰則を与えることで、目的達成のための最適な行動を学習させます。

■ 機械学習の3つの手法



○ 教師あり学習の代表的なアルゴリズム

教師あり学習に用いられるアルゴリズムには主に、「**分類** (Classification)」と「**回帰** (Regression)」があります。

分類は、入力された**データの属するクラスを予測**することです。たとえば、メールがスパムメールかそうでないかを判定する**スパム判定**や、画像に写っている物体を識別する**画像認識**などに分類のアルゴリズムが活用されています。

回帰は、入力された**データの連続する値を予測**することです。たとえば、電力消費量の推移やWebサイトのクリック数など、すでに手元にあるデータから将来の値を予測する作業で回帰のアルゴリズムが活用されます。

教師あり学習は、正解ラベル付きデータをどう確保するかという課題をクリアできれば導入しやすく、最もポピュラーな機械学習の手法といえます。教師あり学習の主なアルゴリズムは下表のとおりです。なお機械学習では、特定の種類やパターンを認識するように学習されたファイル、あるいは手法を「**モデル**」といいます。

■ 教師あり学習の主なアルゴリズム

アルゴリズム	活用事例	主なモデル
分類 データの属するクラスを予測	・ スпамメールの判定 ・ 画像の識別	・ パーセプトロン ・ 決定木 (P.200) ・ ランダムフォレスト (P.204) ・ ロジスティック回帰 (P.212) ・ SVM ・ ニューラルネットワーク (P.216) ・ k-NN (P.220)
回帰 データの連続する値を予測	・ 電力消費量の予測 ・ 広告のクリック数の予測	・ 回帰木 ・ 線形回帰 (P.196) ・ Lasso回帰・Ridge回帰 ・ Elastic Net ・ SVR

○ 教師なし学習の代表的なアルゴリズム

教師なし学習に用いられるアルゴリズムには主に、「**クラスタリング**」と「**次元削減**」があります。クラスタリングは主に、**データの傾向を見る**ために使われま

す。特徴が近いデータをk個のグループに分割する**k-means法**や、似ているデータを順番にグループにまとめていく**階層的クラスタリング**などがあります。

次元削減は、できるだけ情報を保ったまま、**高次元のデータを低次元のデータへ変換**することです。たとえば、10次元のデータがあっても、人間はそれを直接確認できません。これを2次元などに変換することで、データの特徴を見つけ出します。身近な例では、身長と体重の傾向を測るBMIなどがあります。

教師なし学習は、教師あり学習を行うための正解ラベルを付けたいときや、顧客のセグメントを分けたいときなどによく用いられる手法です。

■ 教師なし学習の主なアルゴリズム

アルゴリズム	活用事例	主なモデル
クラスタリング 主にデータの傾向を見る	- 顧客層に応じた販売戦略の立案 - 顧客層に応じたレコメンド	- k-means法 (P.222) - 階層的クラスタリング (P.226)
次元削減 データを高次元から低次元へ変換する	顧客情報の分析レポートなどでデータを可視化	- PCA (Principal Component Analysis：主成分分析) (P.232) - t-SNE (P.55)

○ 強化学習の代表的なアルゴリズム

強化学習は、実際の経験をもとに試行錯誤し、ある目的達成のために「この場合こうすればよい」といった最適な行動の方針を獲得する手法です。

■ 強化学習の主なアルゴリズム

アルゴリズム	活用事例	主なモデル
Q学習 ある状態のある行動の価値をQテーブルで管理し、行動ごとにQ値を更新していく手法	- ブロック崩し - アルファ碁 - 自動運転 - 製造設備の自動制御	- DQN - A3C
モンテカルロ法 乱数を用いた試行(実験)を繰り返すことで妥当そうな答えを求める手法	アルファ碁	
方策勾配法 エージェントの行動の確率をニューラルネットワークで表現するための手法	アルファ碁	PRO

強化学習では、たとえば囲碁や将棋のように「ゲームに勝つ」という目的のために行動を選択し、その行動結果の良し悪しをもとに次の行動を決めていきます。そのため、教師あり学習や教師なし学習と比較し、**導入の難易度が比較的高い手法**といえます。また、活用例がゲームや自動運転などであることから、ほかの手法と比べて研究開発の要素がある機械学習の手法です。

強化学習は、「**レコメンド**」「**異常検知**」「**頻出パターンマッチング**」などの分野でも利用されています。

レコメンドは、**ユーザーが好みそうなアイテムなどを提案する**ことに使われます。ECサイトでよく見かける「この商品を買った人はこれも買っています」や、動画サイトの「関連動画」などのように、Webサービスにおいてユーザーの滞在時間の延長や販売促進のために活用されています。

異常検知は、クレジットカードの不正使用の発見や異常な株価の推移の早期発見など、**異常データのパターンを検知する**ために使われます。

頻出パターンマッチングは、**データのなかに高頻度で出現するパターンを抽出する**ために使われます。有名な例として「ビールと紙おむつが同時に購入されやすい」というものがあります。これは購買情報によく出てくるパターンを抽出したものです。



まとめ

- 機械学習の主な手法として教師あり学習、教師なし学習、強化学習がある
- 主な手法以外に、レコメンド、異常検知、頻出パターンマッチングなども存在する

05

ディープラーニングとは

「ディープラーニング」は、人間による操作がなくても、AIが自動的に特徴を抽出できるようにする学習のことです。ニューラルネットワークの階層を多層化させることで、判断の精度を高め、幅広い分野への応用を可能にしています。

○ 人間の操作なしで学習するディープラーニング

深層学習または**ディープラーニング** (P.21 参照) とは、十分なデータ量があれば、人間による操作がなくてもAIが自動的に特徴を抽出できるようにする学習のことです。この学習には、ディープニューラルネットワーク (Deep Neural Network : DNN) が用いられます。DNNとは、ニューラルネットワークの階層を多層化して深くしたもののことです。この「人間による操作なく」という点が重要です (P.30 参照)。この特徴により、AIの応用分野は大きく広がりました。

また近年のAIブームでは、ディープラーニングという言葉が盛んに用いられたため、「AI=ディープラーニング」と思う人もいるかもしれませんが、**ディープラーニングはあくまでAIの開発技術の一部**です。AI、機械学習、ディープラーニングがカバーする範囲の違いは下図のとおりです。

■ AI、機械学習、ディープラーニングがカバーする範囲



○ ディープラーニングにおける階層の多層化

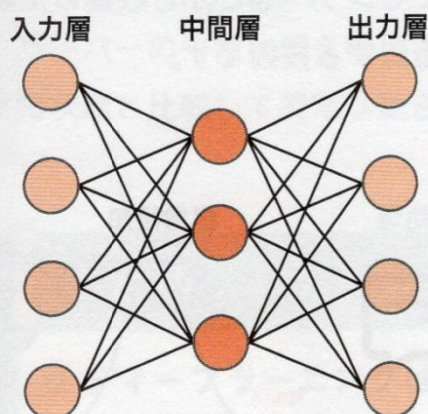
ディープラーニングとは、**ニューラルネットワークの入力と出力の階層を多層化**し、文字どおり深く（深層）学習できるようにしたものです。中間層と呼ばれる層を多層化することで、情報の処理量を増やし、特徴量の精度や予測精度の向上、汎用性の獲得、複雑な処理の実行などを可能にしています。特徴量とは、データのなかの**予測の手がかりとなる変数**のことです。たとえば、ある人の年収を予測するために用いられる「年齢」や「勤務年数」などが特徴量に当たります。

ニューラルネットワークの階層を増やし、複雑な処理を行わせるというアイデアは第2次AIブームからありました。しかし、当時はデータ量の確保などが難しく、実用的なディープラーニングのシステムを構築できませんでした。

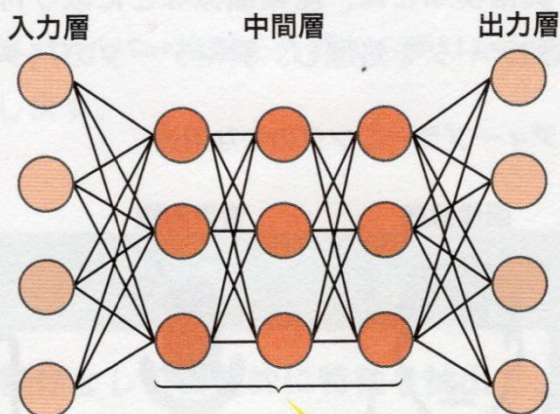
畳み込みニューラルネットワーク（CNN）（P.160参照）などの新しいアルゴリズムの発明、インターネットやセンサーネットワークなどから取得できるデータ量の増加により、ディープラーニングの実用化が実現できる段階になったのです。

■ ニューラルネットワークとディープラーニングの違い

ニューラルネットワーク



ディープラーニング



中間層を多層化することで、より複雑な処理が可能になる

○ ディープラーニングでできること

ディープラーニングでできることは多岐にわたります。ここではその一部を紹介します。

●画像認識

画像認識 (P.156 参照) は、画像を入力し、**画像内の文字や顔などの特徴を識別・検出する技術**です。背景を分離し、対象のマッチングや変換などを行い、画像に写っているものの特徴を識別して検出します。第3次AIブームは、ディープラーニングにより、画像認識の精度が大幅に向上したことで起こりました。有名な例として、Googleが数千万枚のYouTube動画のキャプチャ画像をAIに学習させ、猫の認識ができるようになった「Googleの猫」があります。

●音声認識

音声認識 (P.77 参照) は、**人間の声などを入力し、音声のパターンを識別・検出する技術**です。人間の声を認識して文字データとして出力したり、音声の特徴を捉えて音声の発信者を識別したりすることができます。

●自然言語処理

自然言語処理 (P.74 参照) は、話し言葉や書き言葉など、**私たちが日常的に話したり書いたりする言語をコンピュータに処理させる技術**です。

●異常検知

異常検知とは、産業機械などに取り付けられたセンサーなどから収集した時系列データを処理し、異常データのパターンを検知する技術です。

■ ディープラーニングの主な用途



○ ディープラーニングの応用例

● 自動運転

自動車の自動運転では、運転に必要な**周囲の状況を認識するプロセス**でディープラーニングが利用されています。画像認識を応用することで、障害物などを把握し、安全な運転へとつなげています。

● 自動翻訳

自動翻訳では、自然言語処理で文脈などを判断し、**より文脈に沿った単語を選択する**ことで、自然な翻訳を行います。LSTM (Long Short Term Memory) のような時系列を考慮したアルゴリズムや、BERT (Bidirectional Encoder Representations from Transformers) などのアルゴリズムが活用されています。

● 医療分野での診断支援

医療分野では、蓄積された診断画像、健康診断の数値、各種論文や報告などのデータを解析することで、病気の早期発見と適切な治療法の提案など、診断支援に活用されています。

● 発注・在庫管理

顧客データを解析し、パターンを見つけ出すことで、天候や季節、曜日などによる商品の購買傾向を導き出します。導いた傾向をもとに発注を行うことで、発注と在庫が適正化され、廃棄を抑えることができます。

● サイバーセキュリティ

サーバーの平常状態を学習させておき、サイバー攻撃を外部から受けたとき、平常状態と比較して異常な動きを検知します。



まとめ

- ▣ ディープラーニングは人間の操作なしで自動的に特徴を抽出できる学習
- ▣ 画像認識、音声認識、自然言語処理、異常検知などが行える
- ▣ 自動運転、自動翻訳、医師の診断支援などに応用されている

06

機械学習と
ディープラーニングの違い

機械学習とディープラーニングには、特徴量の設定の有無と、扱えるデータの種類の違いがあります。ディープラーニングにより人間の操作が不要になり、活用の幅が広がった反面、処理のブラックボックス化という問題もあります。

○ 非構造化データも扱えるディープラーニング

機械学習とディープラーニングの違いは、コンピュータに学習させる項目について、**人間が学習項目を設定する必要があるかどうか**にあります。たとえば、明日のアイスクリームの売上を予測するとしましょう。このとき、アイスクリームの売上に関係がありそうな変数（天気や気温、曜日など）を人間が設定し、過去の天気や気温などのデータ、アイスクリームの売上データなどを用意して、その関係性をコンピュータに学習させます。このように、**人間が課題解決のために必要な項目（特徴量）を設定して学習させるのが機械学習**です。

それに対して、**コンピュータがこの特徴量の設定から行うのがディープラーニング**です。たとえば、AIに猫の画像を識別させたいとしましょう。このとき、AIに猫を学習させるのに必要な特徴量を、人間が考えるのは現実的ではありません。なぜなら、**たくさんの例外が出てしまう**からです。

■ 機械学習とディープラーニングの違い



仮に「猫にはヒゲがある」という特徴量を設定したとしましょう。しかし、ヒゲが切れている猫も存在します。同様に、「猫は毛で覆われている」という特徴量を設定しても、毛がない猫もいます。このように、人間が特徴量を設定してもすぐに例外が出てしまい、**猫を明確に定義する特徴量を見つけることは困難**です。しかし、ディープラーニングの発明により、人間が特徴量を設定しなくても、画像認識や自然言語処理などができるようになりました。

ディープラーニングが発明される前、機械学習を行うには**表形式などで整理された「構造化データ」**を用いる必要がありました。そのため、**表形式などで整理できない画像や音声などの「非構造化データ」**をAIに識別させることは難しいと考えられていました。画像や音声などの非構造化データは、前述の例のように、人間が特徴量に関するデータを付与しにくいからです。

しかし近年、インターネットの発展や携帯端末の普及などにより、大量のデータを取得できるようになり、**非構造化データをそのまま学習させても、AIがそれなりに精度の高い識別ができる**ようになりました。このように、ディープラーニングにより、非構造化データも扱えるようになったため、AIの活用分野が大幅に広がり、近年のAIブームにつながっているのです。

■ ディープラーニングによるAIの活用範囲の拡大

ディープラーニング前

	AA	BB	CC	DD	EE
11	***	***	***	***	***
22	***	***	***	***	***
33	***	***	***	***	***

値が数値や記号で表現されているような表形式で構造化されたデータが中心

ディープラーニング後



表形式で整理されていないデータも扱えるようになった

○ ディープラーニングのブラックボックス化問題

ディープラーニングは、扱えるデータの種類が広がった反面、**人間が学習の方向性や内容などをコントロールできない**という難点があります。機械学習のように人間が特徴量を設定できるのであれば、「ヒゲがあるから猫と識別した」というように識別理由を説明できます。しかしディープラーニングでは、「なぜこの画像を猫と識別したか」は**モデルが複雑すぎて説明できない**のです。

これは、「**ブラックボックス化**」と呼ばれる問題です。仮にディープラーニングを使ったシステムで何らかの問題が発生しても理由が説明できず、モデルをどのように改良してよいかわからないという事態が起こります。またAIを運用するとき、「なぜその判断に至ったのか」を説明できないため、現場で活用されないということも生じます。人間には、「中身がわからないものは安心して使えない」という心理がはたらくため、AIを活用する際は、AIの識別を説明して納得してもらう必要があります。

○ 説明可能なAIとしてのXAI

ディープラーニングは、機械学習などの従来の技術より、さらに**ブラックボックスの範囲が広がっています**。そのため、近年では**XAI**（説明可能なAI）という概念が注目されています（P.181 参照）。XAIには主に3つのアプローチがあります。

● Deep Explanation

現在のディープラーニングのモデルに対して、**説明能力を付加する**というアプローチです。具体的には、ディープラーニングのモデルの特徴量の可視化、モデルに予測理由の説明を学習させる、などがあります。

● Interpretable Models

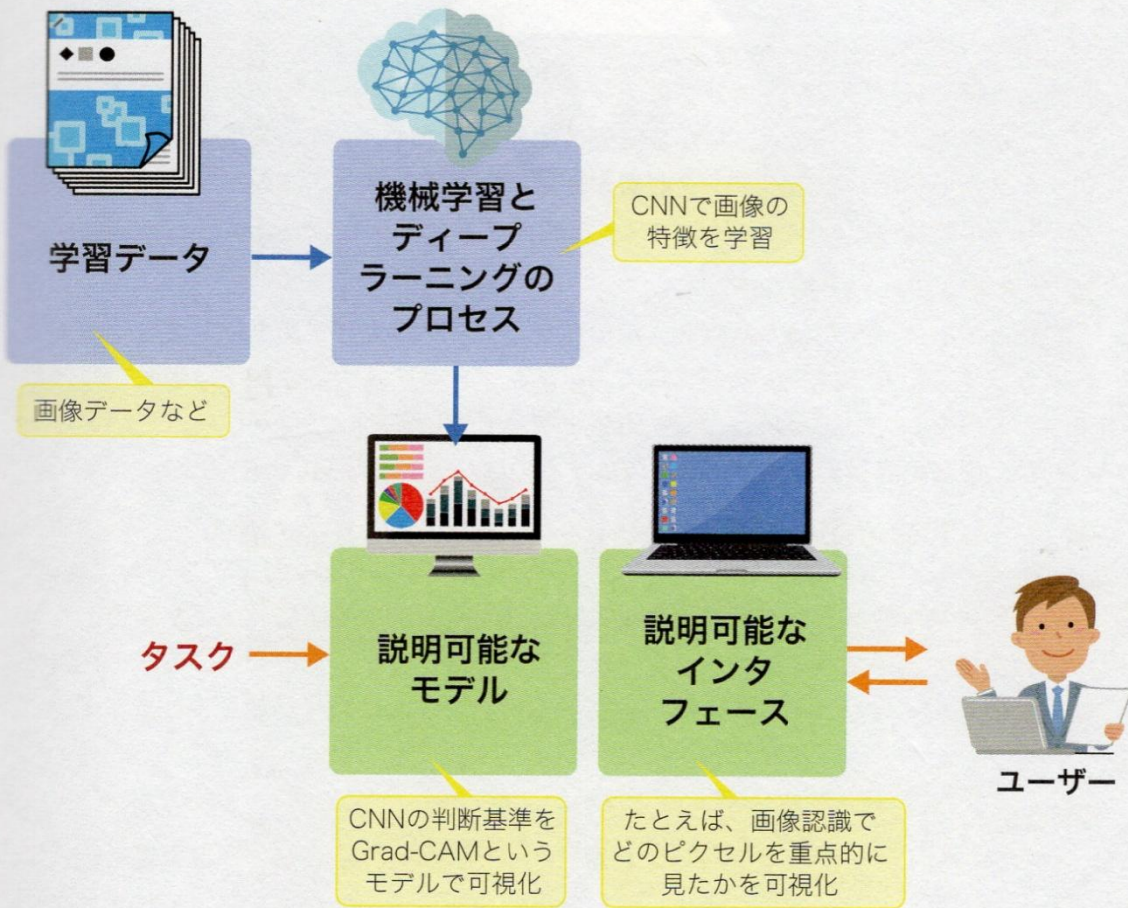
解釈可能なモデルを構築するというアプローチです。具体的には、ベイズ推論に基づくモデル構築などがあります。

● Model Induction

生じたブラックボックスのモデルに対して、**説明を行う別のモデルを構築する**というアプローチです。具体的には、ブラックボックスへの入出力とその挙

動を解析する手法などがあります。

■ XAIの処理のイメージ



出典：DARPA XAIを参考に著者作成

1

A Iとは

まとめ

- 機械学習とディープラーニングの違いは、人間が特徴量を設定する必要があるかどうか
- ディープラーニングで非構造化データも扱えるようになった
- ブラックボックス化への対処としてXAIが注目されている

機械学習やディープラーニングはデータが命です。学習済みモデルの構築には大規模なデータを必要とします。しかし実際の開発現場では、十分なデータを確保できないケースも多いでしょう。データ収集が進まない要因として、プライバシー保護の観点、公平な利益分配の観点、通信コストの観点などがあります。

■プライバシー保護の観点

対象とするデータが個人情報を含んでおり、データの連携が簡単にできないケースがあります。たとえば、複数の病院の画像診断データを活用し、がんの影を見つけるモデルを構築したいとしましょう。治療に関わっているわけではない病院や研究機関などが、患者の病状データを大量に収集するのはハードルが高いといえます。

■公平な利益分配の観点

学習済みモデルから得られた利益をどう分配するかも悩ましい問題です。たとえば、複数の組織から収集したデータで構築した機械学習モデルで収益を上げた場合、それぞれの組織にどのように利益を分配すればよいでしょうか。データ提供者への利益分配の公平なしくみをつくるのは難しく、データ提供者はコストがかかるわりにインセンティブがないという状況に陥りがちです。

■通信コストの観点

複数の組織でデータをやり取りする場合、すべての組織が良好な通信環境を備えているとは限りません。通信速度によりデータ連携がうまくいかなくなってしまうケースもあります。

■データ収集の壁を突破できる可能性がある「連合学習」

以上のように、データ収集は機械学習モデルを構築するうえで肝になるにもかかわらず、障害となるポイントが多いのです。このデータ収集の壁を解決する可能性をもつ手法が連合学習（Federated Learning）です。連合学習は複数の組織から、データではなく機械学習モデルの重みを収集し、各組織の重みを統合することで、全体としてより高精度のモデルを構築する手法です。

たとえば、Googleでは2017年から、スマートフォンの文字変換で連合学習を実装しています。スマートフォンの入力データは個人情報を含むため、データを直接収集するのはハードルが高いといえます。そこで、各デバイスで予測モデルを構築し、モデルの重みの情報のみを収集して、文字変換サービスの精度向上を図っているのです。

EUのGDPR（General Data Protection Regulation：一般データ保護規則）など、データ利用に関する規制は強化されていく傾向にあります。今後、プライバシーを保護しながら機械学習を行える連合学習は、有力な選択肢の1つになっていくでしょう。

