AI入門｜自主学習用教材

AIリテラシー
基礎力学習テキスト



初心者向け

はじめてAIを学ぶ方のための、やさしい教科書です。

安全に使おう編

東京都

監修：国際大学グローバル・コミュニケーション・センター
山口 真一　教授

初心者向け｜安全に使おう編



1 AIの仕組みを知ろう

1-1 AIの仕組みを理解する

1-2 AIができること・苦手なこと

1-3 なぜ人間のようにふるまうのか

2 AIの落とし穴に気をつけよう

2-1 もっともらしい「ウソ」をつく

2-2 別の情報源で確認する

2-3 AIに判断を任せない

3 AIを安全に使うために

3-1 個人情報はAIに教えない

3-2 AIを悪用した詐欺や犯罪の手口を知る

3-3 最終的な責任は「私たち人間」に

AIの仕組みを知ろう｜1−1

AIの仕組みを理解する



AIは前もって学んでから答えます。AIの中でおきていることを、3つのステップで見てみましょう。

STEP1：学習



大量データの学習

画像、文章、音声などを読み込み、パターンを学習

あなたの入力ではなく、AIを作るための大量のデータ

STEP2：予測



質問の予測

学習されたデータの中から共通の特徴を自ら見つけ出す

大量の例から「よく出るパターン」の傾向を計算

STEP3：出力



答えを返す

新しい問いに対して答えの候補を導き出す

正しいときもあるが、もっともらしく間違える時もある

AIは「過去に学習した情報」から「結果」を出力します

AIの仕組みを知ろう｜1−2

AIができること・苦手なこと



できること

- **大量のデータから「パターン」を見つける**
  例）写真から「人の顔」を見分ける、購入履歴からおすすめ商品を紹介する
- **決められた目的に対して予測・判断する**
  例）迷惑メールの判定、売上の予測、音声を文字に変換
- **人の作業を補助・効率化する**
  例）書類作成の補助、問い合わせの一次対応、単純作業の自動化



苦手なこと

- **本当の意味で「理解」すること**
  AIは言葉や画像の意味を理解しているわけではなく、「わかっているように見えるだけ」
- **正しさを保証すること**
  事実を確認する機能を持つAIも増えていますが、最終チェックには人が必要です
- **学習していないことや想定外の対応**
  過去データにないことには弱く、突発的な事態や前例のない判断は苦手



AIは「考える存在」ではなく、「過去のデータをもとに予測・生成を行う技術」です

AIの仕組みを知ろう｜1−3

なぜ人間のようにふるまうのか



膨大な会話の学習

インターネット上の膨大な文章や対話データを学習し、人間がどのように言葉を使い、反応するかを把握

- 丁寧な話し方
- 会話の間の取り方
- 共感しているような返答

＝ 人間の会話を学習

高度な「模倣」技術

「この問いかけには、こう返すのが最も人間らしい」というパターンを確率的に選び出し再現

- 状況に合った言葉選び
- 相手に配慮した表現の型
- 文脈に沿った返答の流れ

＝ 人間らしさの再現

AIは「考えている」のではなく、学習した言葉のパターンを上手にまねています

AIの落とし穴に気をつけよう｜2−1



もっともらしい「ウソ」をつく

AIは、知らないことでも「それらしい文章」を作れてしまいます。まずは実例から。

こんなことが起こります

〇〇（区市町村など）で、いちばん古い和菓子屋さんの名前を教えて。

AI：『△△堂』です。江戸時代から続く、この町で古いお店です。

※ **実際には、もっと古いお店がありました。**
それでも自信満々に答えるのがAIです。

ハルシネーション

AIが事実とちがうことを、それらしく答えてしまう現象のことを「ハルシネーション（幻覚）」と呼びます。

原因1
学習したデータが古い、または偏っている

原因2
確率で「それらしい言葉」を選んでいる

原因3
まちがった前提のまま聞くと、そのまま答える

AIは「正しさ」を理解していません。もっともらしい答えほど、ひと呼吸おきましょう

別の情報源で確認する



AIの答えは「参考」。大事なことについては、ほかの情報源との「答え合わせ」を習慣にしましょう。

うのみにすると、こうなります

Q. AIについて学べる本を教えて？
→ AI「『△△著・〇〇出版』の本がおすすめです」
× 本も著者も出版社も実在せず

Q. この手続きの手数料は？
→ AI「300円です」
× 昨年から450円に改定済み

どちらも、言い方だけは「もっともらしい」のが特徴です。

答え合わせの相手（信頼できる出典・情報源）

公的機関の公式サイト
市役所・省庁など、開庁時間や手続きはここで確認

信頼できる報道機関
新聞やテレビなど、複数のニュースで見比べる

専門書や辞書
書籍はもちろん、家族や詳しい人に聞くのも確認方法の一つ

「もっともらしい」は「事実」とは限らない。**最後の確認は人間の仕事**です

AIの落とし穴に気をつけよう｜2−3

AIに判断を任せない



AIは下調べに大活躍。ただし「決める」ことだけは任せてはいけません。

○ AIが役立つこと

調べる・比較する・用語をやさしく説明してもらう

× 任せてはいけないこと

「どうするか」を決めること。特に下の6つの分野は注意

命・健康のこと

調べるのはOK。診断や薬の判断は医師・薬剤師へ

緊急のとき

避難や事故対応は、公的な指示・通報を最優先に

お金のこと

投資や契約の情報集めまで。決断は専門家に相談を

税金のこと

仕組みの理解まで。申告の判断は税務署・税理士へ

法律のこと

用語の解説まで。契約やトラブルは弁護士など専門家へ

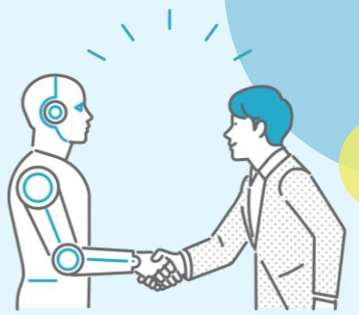
役所の手続き

流れの下調べまで。可否や書類は窓口で最終確認を

※理由はどれも「まちがえたら取り返しがつきにくい」から。AIで下調べ→専門家や公式窓口で決める、が安心の順番です。

下調べはAIに。「判断」は、専門家とあなたの仕事です

AIを安全に使うために｜3−1



個人情報はAIに教えない

入力した内容は、AIサービス提供者に送られて処理され、しばらく保存されることがあります。

なぜ気をつけるの？

あなたが入力する
質問や文章に名前・住所などを書く

▼

AIサービス提供者に送られ処理され、しばらく保存される

▼

不具合・事故・共有設定有無で、外部に出てしまうことがある

自分を守る3つの鉄則

1 **名前・住所・電話番号は入れない**
個人が特定できる情報は入力しないこと
※パスワード、会社の未公開情報も同じ



2 **固有名詞は伏せ字にする**
「A社」「〇〇区」「〇〇市」のように置きかえて質問すること



3 **学習させない設定を確認する**
学習させない設定にしても、記録が残るリスクはゼロになるわけではありません。

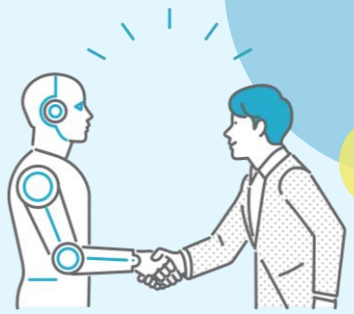


※ 送信や保存のしかたはサービスによって違います。中には、端末（スマホ・パソコン）の中だけで処理するAIもあります。

他人に見られたら困ることは、AIにも入力しないことが大切です

AIを安全に使うために｜3−2

AIを悪用した詐欺や犯罪の手口を知る



「知っている」だけで、だまされにくくなります。手口を知って、備えまでセットで覚えましょう。

手口1:「にせ物」がつくれてしまう

・家族や知人そっくりの「声」の電話
・有名人が投資をすすめる「動画」
・有名企業そっくりの「ホームページ」

手口2:文章もていねいで自然

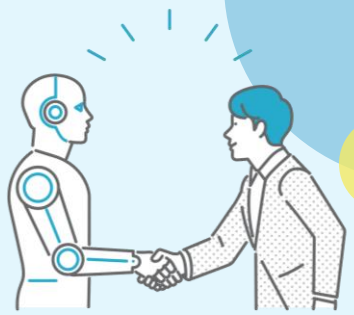
・文法ミスのない、自然な日本語
・あなたの趣味や職業に合わせた内容
・企業や役所を装ったそれらしい文面

だからこそ、判断のよりどころを変える

① 自然な文章・そっくりの声や動画は、もう「信用の根拠」にしない（作れる時代です）
② どんなにていねいでも「お金・個人情報」の話が出たら、その時点で疑う
③ 届いたリンクや着信からではなく、いつもの公式アプリ・ブックマーク・電話帳から自分でアクセスして確かめる

「見抜く力」より、「疑う習慣」。あやしいと思えることが大切です

AIを安全に使うために｜3−3



まとめ ― 最終的な責任は「私たち人間」に

ここまで学んだことを、5つの約束にまとめました。まずはこの5つを意識しましょう。

AIは「高度な道具」。包丁や車と同じで、使い方しだいで価値にもリスクにもなります。

安全に使う「5つの約束」

- 答えは「参考」。たしかめは自分でする
- 大事なことの「最終判断」は任せない
- 個人情報は教えない
- 声や動画も「本物とは限らない」と考える
- こまったら一人で悩まず、人に相談する

役割分担で考える

AIがすること
調べる・下書きする・整理する

あなたがすること
たしかめる・決める・責任を持つ

うまく分担できれば、AIは頼れる相棒になります。

AIがどんなに進化しても、「最終的な判断と責任」はあなたです

AIをもっと便利に使うために

「便利に使おう編」もご覧ください



この教材で学んだ 9 のテーマ

- ☐ 1-1 AIの仕組みを理解する
- ☐ 1-2 AIができること・苦手なこと
- ☐ 1-3 なぜ人間のようにふるまうのか
- ☐ 2-1 もっともらしい「ウソ」をつく
- ☐ 2-2 別の情報源で確認する
- ☐ 2-3 AIに判断を任せない
- ☐ 3-1 個人情報はAIに教えない
- ☐ 3-2 AIを悪用した詐欺や犯罪の手口を知る
- ☐ 3-3 最終的な責任は「私たち人間」に

東京都のAIに関する情報はこちら

https://www.digitalservice.metro.tokyo.lg.jp/business/ai/ai-literacy

令和8年9月発行 ： 東京都デジタルサービス局 デジタル戦略部

東京都