推薦序

在信任與創新之間，開啟企業的 AI 新篇章

回顧過去自網際網路萌芽後科技的跳躍性發展，這 20 多年來我們經歷了網路革命、行動革命到現在的 AI 浪潮，這一波的 AI 發展勢必帶來企業熟悉的商業及資訊領域的顛覆性改變。近年來，我們在台灣觀察到企業正面臨一場結構性變革。從智慧製造、金融科技，到醫療轉型與智慧城市建設，無不在思索同一個關鍵問題——如何以人工智慧（AI）為核心驅動力，加速企業數位轉型。然而，AI 的導入從來不只是導入技術，而是一場重新思考價值、信任與組織文化的深度轉型。也就是企業從零星的 +AI 應用導入，到一個全面文化轉型的 AI+ 企業旅程。

在這樣的科技轉捩點，我非常榮幸能推薦我在 IBM 全球的技術長官，也是科技業極具遠見的技術領袖——Jerry Cuomo——所撰寫的這本《人工智慧思維》。這不只是一本介紹 AI 技術的書，在字裡行間更體現出兼具人文思考與戰略洞察的思想旅程。Jerry 透過他數十年的實戰經驗，串起從技術建構、應用設計到倫理實踐的全貌，為我們呈現了企業如何真正「思考」並「活用」人工智慧。同時 Jerry Cuomo 在本書中更帶出 AI 技術應用深入企業的一個關鍵命題：「信任，是 AI 得以真正被使用與發揮影響力的核心」。

在本書的章節編排部分，Jerry 在本書中不採用傳統的教科書式編排，而是以創新的敘事方式貫穿全書。他虛構了兩位角色——Pato，一位具備精緻語言能力的聊天機器人；以及 Datos，一位充滿個性與記憶層級結構的資料合集。他們在書中穿插對話、模擬情境、討論衝突，讓抽象的技術轉化為具體的「人機共生」畫面。同時本書也將生成式 AI 融入寫作工具中，不僅用 GenAI 協助產出書中插圖與程式碼，更慷慨公開他使用的 100+ 組提示與最佳實踐，提供讀者一份「實用工作手冊」，讓閱讀過程本身即是學習與創作的過程。這種方式，不僅降低了學習門檻，也強調了 AI 導入過程中最重要的兩項價值：透明與共享。

在本書內容的涵蓋面，Jerry 在書中深入淺出地介紹了從 AI 基礎原理、機器學習、提示工程（Prompt Engineering）、資料策展、AI App 開發、到倫理與資安等完整架構。這些內容雖具技術性，卻不艱澀，因為 Jerry 並非單純為工程師而寫，而是為所有正處於「數位轉型十字路口」上的企業與決策者所設計。他以企業建築師的視角，解構出一套極具實用性的框架——如何讓 AI 成為企業的競爭優勢，而非風險來源。他強調，AI 不應該只是演算法的競賽，而應成為企業文化的一部分——讓資料科學家、業務、行銷、人資部門，甚至董事會，都能用同一種語言理解 AI 所帶來的影響與潛能。

本書以鴨子（Duck）為主軸串連整本書，然而作者的真正涵義是鼓勵企業內部具有創新思維、勇於挑戰傳統的 Wild Ducks，在 AI 企業轉型的關鍵時刻挺身而出。最後，這本書不僅幫助我們看清 AI 的技術本質，更幫助我們釐清：在企業與社會的未來藍圖中，人類的角色將如何重構。在這個由數據驅動、由信任引導的未來世界，《人工智慧思維》將是企業 AI 轉型旅程中最值得攜帶的一本智慧地圖。

IBM 台灣 技術長 莊士逸

推薦序

迎向 AI 共創的未來：技術與信任的完美交會

近幾年，我在產業一線見證了 AI 如何從前瞻技術轉變為企業競爭的核心能力。在此浪潮之下，企業領導人必須理解的不再只是 AI 技術本身，而是如何系統性地將技術落實到組織當中，成為可信賴且高效的協作夥伴。

Jerry Cuomo 在《人工智慧思維》一書中，以層次分明的架構，從資料整理、提示設計到代理人系統，詳盡描述 AI 落地過程中的核心實務，並用生動的角色故事使抽象的理論轉化為可輕鬆掌握的具體情境，這正是我所欣賞的實踐型寫作特色。此外，作者敏銳地探討企業導入 AI 所伴隨的倫理安全、透明度及治理問題，提出明確而前瞻的觀點，值得每一位決策者深思。

這些觀點與研華目前積極推動的 WISE-Edge 邊緣智慧平台理念不謀而合。我們強調 Edge Computing 的部署，正是希望透過在邊緣端即時處理與反應資料，降低延遲並強化資安防護，協助企業真正實現 AI 的即時決策能力。

我相信，成功導入 AI 的關鍵，不僅是技術的成熟，更需要企業以「信任設計」為出發點，打造能與業務系統緊密整合且能在實際場域快速驗證的 AI 環境。誠摯推薦本書給所有希望以科技賦能組織、實現人機共創未來的企業領袖。

研華 Advantech 全球企業發展副總裁 吉永和良

推薦序

本書作者 Jerry 以人與人工智慧之間的信任關係作為切入點，直球對決人們對兩者間複雜的情感糾葛，或許延續了他前作關於區塊鏈的思考脈絡，區塊鏈的核心在於解決信任問題，Jerry 以此為基礎，巧妙將信任議題融入 AI 的探討。他的寫作風格實務導向，兼具學術深度，不僅借助 AI 輔助創作，還公開透明地分享創作過程與經驗，成為本書獨特的知識分享亮點。

作者以說故事的方式闡述 AI 的發展，將多年經驗融入章節，從文本設計、故事情節、角色塑造到遣詞用字，皆精心雕琢，旨在吸引讀者目光並維持其專注力。這種手法讓本書突破傳統教科書的框架，閱讀性更強，同時全面涵蓋 AI 的廣闊領域。這種兼具趣味與深度的呈現方式，使本書獨樹一幟。

2025 年母親節，南海劇場上演了「那個女人是誰？」讀劇音樂會，我有幸參與了該劇的製作過程。從製作人、導演、專業演員到指揮與合唱團，每位參與者全心投入，共同打造了一場感人至深的演出。其中，主創團隊在文本撰寫、故事編排、歌詞與樂曲創作，以及整體呈現上的心力投入，令人難忘。這段經歷讓我更加體會本書作者在創作上的用心與付出。

翻譯此書的目的，不僅在於其獨特的內容與風格，更反映了林老師與作者多年來在工作上建立的深厚情誼，以及對彼此專業的了解與信任。在當今時代，學生購買紙本書已略顯反潮流，購買原文書更是稀少。因此，選擇一本值得深入研讀的教科書尤為不易。林老師經過多方考量與篩選，決定翻譯此書。這本書不僅是一本實用的教科書，更是一本值得知識工作者反覆閱讀的知識庫。

國立台灣大學資訊管理系 專任教授 曹承礎

譯者序

書本翻譯丟給 AI，行不行？

比較正式的中譯序請參考《English Career》期刊 2024 年 10 月號「連結 AI 學習與 AI 實作的指南」一文，該文內容是有關於這本翻譯書的緣起。你目前看到的這篇中譯序寫於翻譯後，偏向血淚史。；）

我以為翻譯一本書是一件很簡單的事，不是有 AI 嗎？結果我錯了。

如果是一篇文章，讓 AI 來翻譯，那肯定很簡單。但是一本書不同，它有圖、有表格、有程式片段、有作者特殊的風格，有些地方不能翻譯（因為那是被操作的「資料」，不是本文），有些地方不好翻譯（例如存在文化背景的幽默），有些翻譯要顧及區域差異性（適合大中華還是適合台灣），有些翻譯要顧及語境（嚴肅、詼諧、還是雙關）。

原書作者，傑瑞（Jerry），是我的恩師也是我的朋友，他寫書的風格很隨性，很喜歡「跳 tone」（幽默的、雙關的那種），很喜歡在書中安插「內心小劇場」，是的，你看了書就會知道；）。但是，AI 很難掌握這種風格，很多時候，光是翻譯還不夠，譯者得跳出來解釋，原作者到底在想什麼。更別提，他有很多創新的寫法，例如讓擬人化的抽象概念角色來發聲，「代替」作者寫書。^^|||

然而，這還不是最頭痛的… 最頭痛的工作，是讓所有的章節、所有的結構（圖、表、程式碼）一致，讓翻譯的風格一致。比如說，sentiment analysis，一般翻譯成情感分析，但是在書中討論企業披露文件的時候，我覺得企業「態度」分析是更好的選擇，然後不同章節就開始打架，翻譯不一致，需要大幅度修正。

幸好這一切都結束了。而且有了這些痛苦的「經歷」，我似乎也獲得了一些「資產」。你應該猜到了，我要拿這些翻譯結果去訓練或微調 AI，並且發明幾項資訊處理技術來解決圖表不一致的問題，那麼下次翻譯我就不會這麼累了…（咦，下次？我是不是挖洞給自己跳了…^^|||）

國立臺灣科技大學資訊管理系 副教授 林俊叡

人工智慧的演進 2

就像有愛因斯坦
作為你聰明的指標。

本章涵蓋

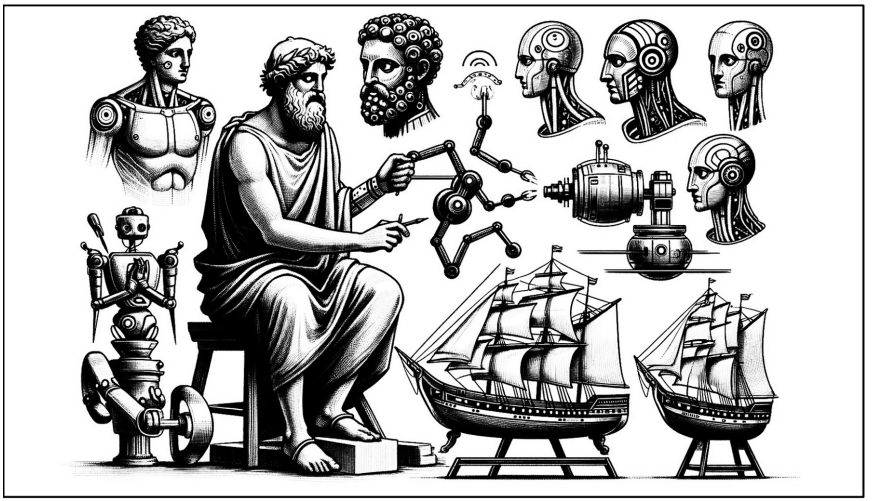
- ✧ 借助人工智慧定義人工智慧
- ✧ 機器學習和深度學習
- ✧ 人工智慧的網景時刻：與 ChatGPT 的相遇
- ✧ 人工智慧年表
- ✧ 揭穿人工智慧迷思

人工智慧的前史

我一直對我們的祖先會如何想像智能機器和人工智慧感到著迷，尤其是考慮到這些想法有多古老。以古希臘人為例，在荷馬的作品中，可以追溯到公元前 8 世紀，有這樣生動的描繪：赫淮斯托斯（Hephaestus），鍛造之神，使用自動風箱進行日常工作。他甚至有黃金助手，這些助手不僅僅是裝飾品，他們能夠移動、感知、判斷和說話。

譯註

赫淮斯托斯（Hephaestus）是古希臘神話中的鍛造之神，他是宙斯和赫拉的兒子，被認為是奧林匹斯諸神中最聰明的。他是火神，也是鍛造、工藝和建築的神祇，他的工作坊位於奧林匹斯山的火山口。他的助手是由黃金製成的機械人，能夠幫助他完成各種工作。



↳ **提示：** …受古希臘神話啟發的人工智慧前史 { 插入史前描述 }。

然後是荷馬的《奧德賽》，他描述了費亞基亞人的船。這些不是普通的船，它們能夠理解人類的命令，避開障礙物，並以令人難以置信的速度移動——幾乎就像它們能夠讀懂船長的想法一樣。再往前推進幾個世紀，大約在公元前 400 年左右，我們遇到了塔洛斯（Talos），這是一個由赫淮斯托斯製造的巨大青銅保護者，守護著克里特島的海岸 [17]。

這些古老的故事讓我印象深刻的是人類和自動機器之間能相互合作的概念。無論是有感知能力還是沒有，這些神話中的生物被想像為在各種任務中幫助神祇或人類的盟友。這種人造實體與其創造者協同工作的想法證明了人類想像力的深度和遠見。令人著迷的是，我們現代的人工智慧和機器人概念，通常著重於合作夥伴關係和協同工作，其根源可以追溯到數千年前，遠在卡雷爾·恰佩克（Karel Čapek）創造出「機器人（robot）」這個詞之前。這種歷史觀點突顯了人類持續將技術融入我們的生活中，作為合作夥伴和幫手的渴望。

也許我們回溯得有點過頭了。讓我們回到更現代的時代，這些早期的概念已經演變成了今天的技術進步。

定義人工智慧

從我的個人故事繼續，透過將我的一些經歷與人工智慧的基礎連接起來，讓我們開始探討這個問題：「究竟什麼是人工智慧？」

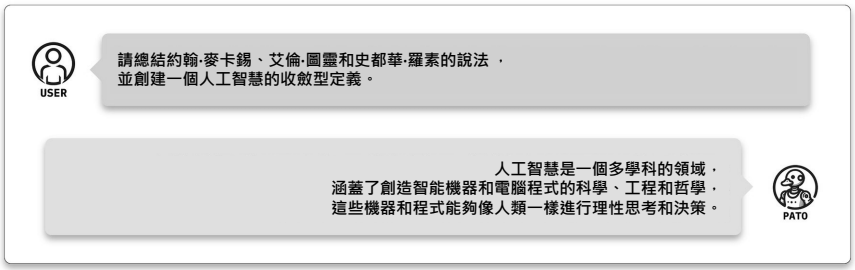
我之前簡要提到了約翰·麥卡錫。在 2004 年的一篇論文[18]中，他將人工智慧定義為「製造智能機器的科學和工程，尤其是智能電腦程式」。它專注於開發能夠展示智能的機器，而不僅僅是模仿人類行為。

然而，人工智慧的根源可以追溯得更遠。艾倫·圖靈，通常被認為是「計算機科學之父」，在他 1950 年的論文《計算機機器和智能》[19]中引發了關於人工智慧的討論。在該論文中，他提出了著名的疑問：「機器能夠思考嗎？」，他還提出了圖靈測試，讓人類試圖從文字回應區分計算機和人類的不同，這引發了哲學和語言學的爭論。

史都華·羅素（Stuart Russell）和彼得·諾維（Peter Norvig）的書《人工智慧：現代方法》[20]進一步探討了人工智慧的定義。他們將人工智慧依照四個目標分類：能像人類一樣思考、能像人類一樣行動、能理性思考、能理性行動的系統。圖靈的研究是與「像人類一樣行動的系統」這個目標相近的。

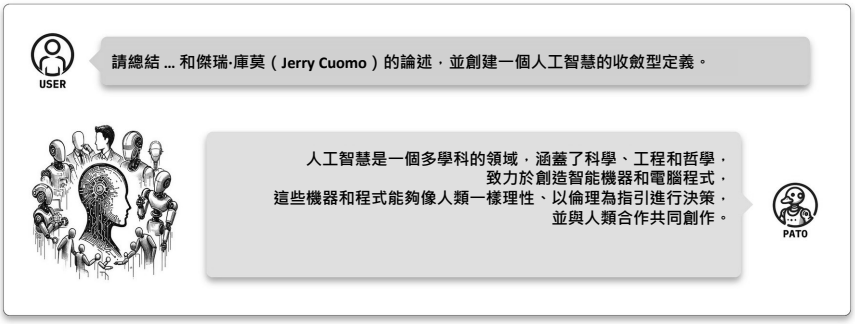
使用大型語言模型 Mixtral-8x7B，我發出了下面這個提示，得到人工智慧的收斂型定義。

來自「人工智慧大師」的收斂型定義：



接著，我更新了提示，並將我的名字加入到列表中。我對修改後的定義感到非常滿意。

加入了第 1 章中傑瑞的人工智慧短文作為提示後：



這個收斂型定義包含了道德方面（「以倫理為指引的決策」）以及與人工智慧的合作關係（「與人類合作共同創作」）。不錯。

有了定義，接下來的部分將幫助我們對人工智慧的兩個類別有所了解：「聳動的」與「實用的」。

虛構與現實

我曾經讀過一篇《科學美國人》（Scientific American）的文章[21]，估計 ChatGPT 的智商為 155。當然，這只是衡量智慧的一種方式，但它也突顯了我們在人工智慧領域取得了令人印象深刻的進展。這樣的進步使我們將人工智慧逐漸分為兩個陣營：弱人工智慧和強人工智慧，每個陣營都有其獨特的特點和應用。讓我們來探討這些區別：

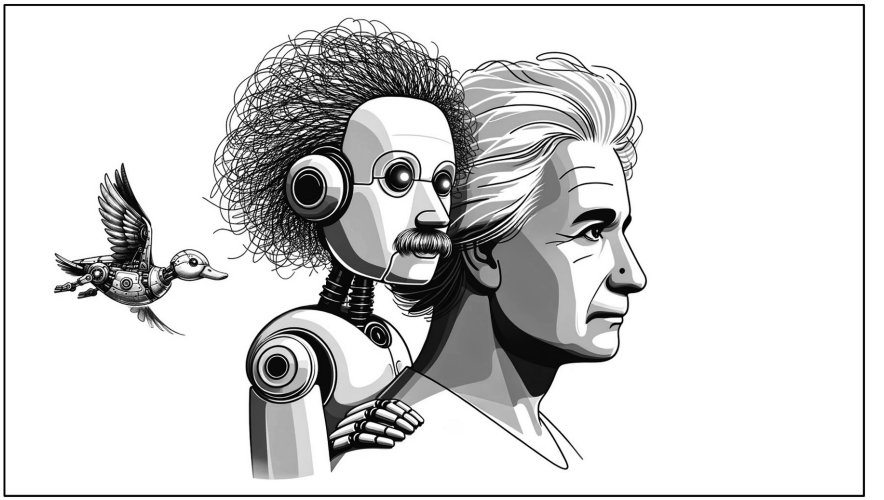
弱人工智慧，通常被稱為特化人工智慧或狹義人工智慧（Artificial Narrow Intelligence, ANI），是為特定任務而設計和訓練的。儘管其名稱中有「弱」這個詞，但這並不準確反映其能力。事實上，弱人工智慧驅動了我們每天遇到的許多人工智慧應用。想想蘋果的 Siri、亞馬遜的 Alexa、IBM 的 Watson Code Assistant 和特斯拉的 Autopilot 等自動駕駛汽車；它們都屬於弱人工智慧的範疇。這些系統在各自的專業領域表現出色，使它們成為非常強大的工具。

現在，讓我們將注意力轉向**強人工智慧**。這個類別包括通用人工智慧（Artificial General Intelligence, AGI）和更先進的超級人工智慧（Artificial Superintelligence, ASI）。AGI 代表一種具有人類級智慧的人工智慧形式，具有自我意識、解決問題能力、學習能力和未來規劃能力。儘管令人著迷，但在現實應用中仍然難以實現。

ASI 更進一步。它的目標是超越人類的智慧和能力。科幻小說中充滿了超人類人工智慧的想法，比如《銀翼殺手》（Blade Runner）中的複製人或《2001 太空漫遊》（2001: A Space Odyssey）中的 HAL 電腦。想想看，從人類智慧到超人類智慧的進步涉及到認知、理解、自我意識、情感、創造力、抽象思維、無限記憶和對大量資料的即時理解。我說過這個夢想嗎？機器人會夢見電子羊嗎？答案是肯定的。

目前，包括 ASI 在內的強人工智慧仍然純粹是理論性的。看到人工智慧在特定、狹義的應用中的發展是令人興奮的，但是實現類人類或超人類智慧對人工智慧研究人員來說仍然是一個艱巨的任務。在人工智慧的世界中，虛構和現實之間存在一大片灰色地帶。當我回顧我們的進步時，我不

禁對人工智慧的前景感到驚嘆，比如 ChatGPT，它的智商為 155，與愛因斯坦的智商約 160 相當。這就像有愛因斯坦本人作為你聰明的拍檔。無論是強人工智慧還是弱人工智慧，這都是一項即將改變我們未來工作方式的重要成就。



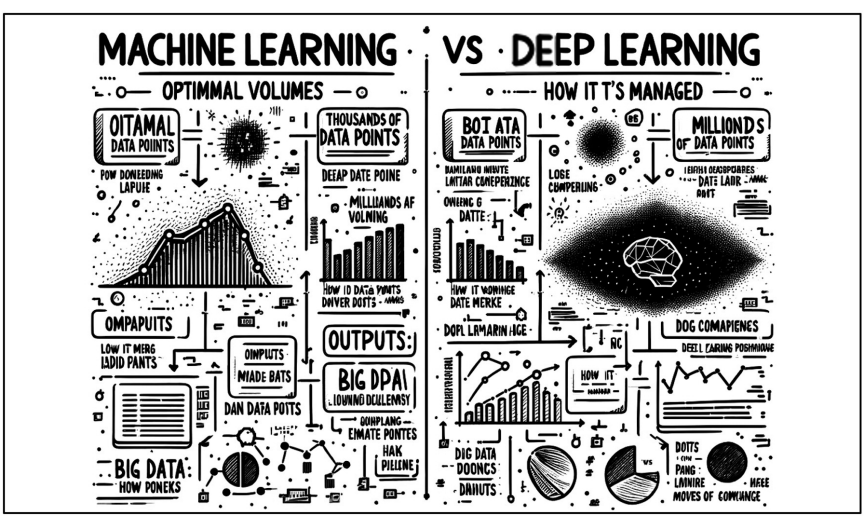
↳ **提示**：…倚靠在人肩上的機器人版愛因斯坦，象徵著聰明的拍檔 { 插入飛行機器鴨 }。

現在，讓我們將焦點轉向人工智慧中涵蓋的不同學科。每個學科皆發展出獨特的計算機科學技術，適用於特定領域應用，並為該領域的發展做出了重要貢獻。

機器學習

人工智慧與其他軟體系統的真正區別在於它的學習能力，或者更準確地說，是它模仿學習的方式。你看，今天的人工智慧系統擅長篩選資料、識別模式，並根據它們的「經驗」做出決策。這與我們人類學習和適應的方式相似。這是傳統軟體的一大進步，傳統軟體在很大程度上依賴規則。當你試圖用太多規則來模仿智能時，它只會變成一個複雜、難以控制的混亂。現代人工智慧透過更流暢、更類似人類的方式學習和適應，來避免這種情況。這就是人工智慧的**深度學習**（Deep Learning, DL）和**機器學習**（Machine Learning, ML）領域。它們都屬於人工智慧的範疇，但深度學習是機器學習的一個子領域。雖然我將它們分別稱為 DL 和 ML，但我並不是說它們是互相排斥的。使用這兩種技術來訓練同一個人工智慧系統是非常常見的。

這些學習模型從龐大的資料庫中吸收資訊，並隨著時間的推移不斷改進，而無須有人編寫每一條規則。這一飛躍克服了基於規則之系統的阻礙，是人工智慧在處理複雜且不斷變化的任務方面的一個巨大的改進。順便說一句，在第 1 章的測驗時間中，基於規則的人工智慧是非題的答案是「正確」。現在你知道為什麼了。



↳ **提示**：…比較機器學習與深度學習。

讓我們花一點時間來區分 DL 和 ML，這兩個術語經常被互換使用。

深度學習（DL）主要集中在先進的神經網絡上，基本上是一系列演算法。這些網絡構成了 DL 模型的核心。想像一下這是一個分層連接系統，每一層都擅長於定位和處理不同的數據元素。例如，在圖像識別中，一層可以檢測輪廓或邊界（邊緣），而另一層可能識別形狀或形式。一些實際例子包括：

- **人臉識別**：用於智慧型手機的解鎖功能或在社交媒體平台上為朋友標記照片。
- **自動駕駛汽車**：深度學習幫助這些車輛識別物體（如行人或其他汽車）、解釋交通標誌，並做出導航決策。
- **語言翻譯服務**（如 Google 翻譯）：DL 演算法可以即時將一種語言的文本或語音翻譯成另一種語言。
- **手寫字元識別**：這項技術被應用於各個行業，如將手寫文件數位化、讀取手寫郵政地址以便分類郵件，以及從手寫表格中提取資料。
- **醫療診斷**：分析醫學影像（如 X 光片或 MRI）以幫助醫生診斷疾病。

深度學習在標記（labeled）和未標記（unlabeled）的資料上都表現出色，包括文本和圖像等原始格式。在標記學習中，照片被標記為「貓」或「狗」以進行圖像識別，而在未標記學習中，系統分析沒有標籤的照片以辨別模式。這種對資料中的模式和結構的自主學習減少了人類參與的需求。這種自主學習方法，主要是用在處理未標記資料，故被稱為無監督學習（Unsupervised Learning）。

機器學習（ML）則更依賴人類專業知識來定義特徵層次結構並理解資料差異。它通常需要結構化資料和監督式學習（Supervised Learning），其中標記的資料集便是用來引導演算法。以下是一些日常例子：

- **電子郵件中的垃圾郵件過濾器**：機器學習演算法分析你的電子郵件，並根據特定關鍵字或發件人的聲譽等模式學習識別哪些是垃圾郵件，哪些不是。
- **電影推薦**（如 Netflix 上的推薦系統）：機器學習演算法根據你觀看和評分的電影和電視節目，推薦你可能喜歡的新片。

- **信用評分**：金融機構使用機器學習來分析你的財務歷史，決定是否批准貸款或信用卡。
- **虛擬助手中的語音辨識**（如 Siri 或 Google 助手）：這些設備使用機器學習來理解你的語音命令並做出適當的回應。

上面列出的清單激發了我進行一個小實驗的想法。我想知道是否可能在不到 50 行的 Python 程式中創建一個深度學習程式，尤其是在得到一些人工智慧編程助手的幫助後。答案是肯定的。接下來，你將看到一個程式的虛擬碼大綱。這個程式使用 TensorFlow 庫來訓練一個神經網絡，使其能夠識別手寫數字。完整的原始碼託管在 GitHub 上，如下所示，任何樂於嘗試的人都可以使用它進行實驗。

不到 50 行的深度學習 Python 程式碼，以下僅顯示虛擬碼：

```
開始（1-20 行）
    設定使用神經網絡識別手寫數字。

載入資料（21-22 行）
    載入 MNIST 資料集的圖像和標籤。

處理資料（25-29 行）
    將圖像標準化為 0 到 1 之間的值。
    將標籤轉換為適合訓練的格式。

建立神經網絡模型（30-36 行）
    建立具有輸入、隱藏和輸出層的模型。

編譯模型（40-43 行）
    設置優化器、錯誤測量和性能指標。

訓練模型（44 行）
    使用訓練資料，執行 5 次訓練週期，來訓練模型。

評估模型（46-48 行）
    使用測試資料測試模型，顯示模型的準確度。

結束（49 行）
    顯示測試準確度。
```

↳ **程式碼**：MachineLearning_MNIST_Recognition.py

↳ **提示**：…生成最簡單的 Python 程式，以展示深度學習的應用…。

從我還是研究生到現在，我們取得了多麼驚人的進步。人工智慧理論一度是一個高遠的概念，但現在已經在任何程式設計者的可實作範圍內，包括像我這樣不再積極參與程式設計的人也能使用。訓練人工智慧曾經是一項專門保留給資料科學家的任務，但現在，即使是平凡的程式設計者也被歡迎進入資料科學俱樂部。我期待在第 7 章中分享一些機器學習的實際例子。

你現在可以看出為什麼機器學習是當代人工智慧的基石，打開了通往其他分支領域的大門。在接下來的章節中，我們將探討一些機器學習的關鍵分支。

機器學習的分支

隨著機器學習的不斷演進，它催生了幾個有趣且具有影響力的子領域。這些分支利用了機器學習的基本原則，同時展示了它們的獨特特點，並將這些原則應用於專門的任務和挑戰。從解釋人類語言到分析視覺資料，這些分支不僅僅是理論概念，而且正在積極地重塑我們的世界。接下來，我們將探索其中一些關鍵領域：

自然語言處理（NLP）：這個子領域研究電腦和人類如何以（自然）語言互動。它包括使電腦能理解、解釋和生成人類語言以創造價值。

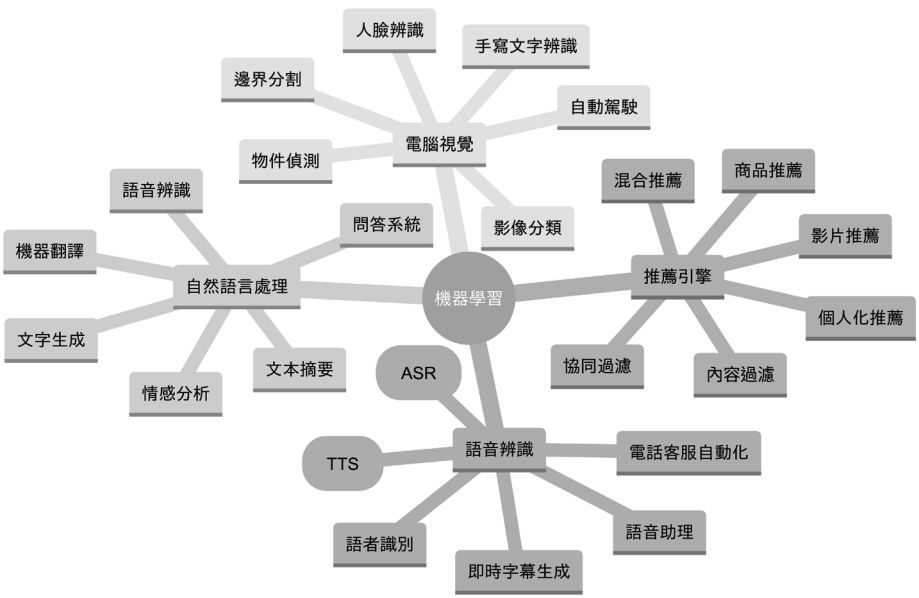
在語言學和人工智慧的交集處，NLP 教導機器理解的不僅僅是單詞，還有語境和情感。深度學習使 NLP 系統能夠從龐大的語言資料集學習，改進翻譯服務和聊天機器人等功能。這些進步不僅在技術上令人印象深刻，而且使我們與技術的互動變得更加自然和直觀。我發現這個領域真的很令人振奮，因為它不斷發展，並改善了我們與數位世界溝通的方式。

電腦視覺（computer vision）：這項人工智慧技術使電腦能夠透過從數位圖片和影片中提取有意義的見解來模擬「看見」。更令人興奮的是，它可以根據這些見解採取行動。這種魔法根源於電腦視覺和僅僅圖像識別（image recognition）之間的區別。有了卷積神經網絡驅動這一領域，我們可以看到社交媒體照片標記、醫療放射影像等應用，還有充滿希望的未來世界——汽車和海上船舶的自動駕駛。

語音辨識：也被稱為自動語音辨識（automatic speech recognition, ASR），代表了另一個技術的重大飛躍。它借助了 NLP 技術將口語轉換為書面文本。這項技術為智慧型手機上的語音搜尋和語音轉文字等功能提供強大動力，像 Siri 這樣的工具就是一個很好的例子。它的有效性取決於機器學習的進步，這使得對人類語音的解釋和轉換更加準確。ASR 在日常生活中的高度整合展示了人工智慧和 NLP 在現代科技應用中的高度實用性。

在本書的後續章節中，我們將探討在餐廳的汽車服務窗口中實作 ASR 的應用。想像一下：在汽車喇叭聲、狗叫聲和各種不同音調的顧客講話聲中，這個系統仍然能夠有效地運作。這真的很令人印象深刻！

推薦引擎：人工智慧演算法可以從過去的消費行為中發現有價值的資料趨勢。推薦引擎是人工智慧的一個顯著應用，特別是在電子商務和線上內容平台上。這些引擎透過分析過去用戶行為中的模式，如購買歷史、瀏覽數據，甚至用戶評分，發現了每個用戶獨特的有價值的趨勢和偏好。機器學習演算法是這些系統的核心，使它們能夠預測並建議用戶可能感興趣的產品或內容。



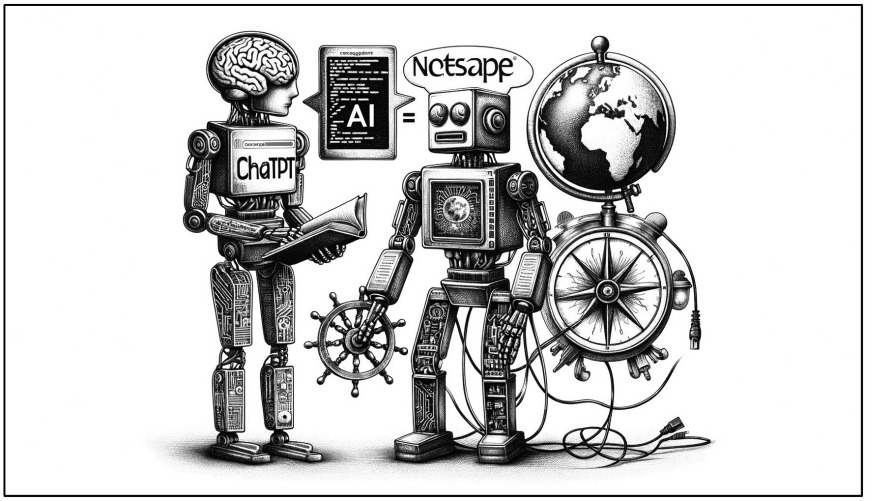
↳ **提示**：…Mermaid.js 思維導圖，以視覺方式組織以下「機器學習」的案例：{ 從文本中插入案例 }。

當我們回顧重要的人工智慧定義時，我將以提示詞來生成如上這些**思維導圖**（mind maps），以幫助我們視覺化概念之間的聯繫。坦白說，自動生成這些圖表是有點酷的。

這些思維導圖中展示了人工智慧技術為「基礎模型」和「生成式人工智慧」等領域的突破性發展提供了基礎。下一節將進一步揭示人工智慧令人驚豔的尖端能力，並從基礎概念跨越到先進的生成應用。

人工智慧的網景時刻

我以前曾經歷過這種現象。在我年輕的時候，我觀察到一些新技術如何迅速融入我們的日常生活，提高生產力和創造力，但如果不小心處理，也會引入新的弱點和社會挑戰。你看，網際網路在網景公司（Netscape）出現之前就存在了。但當瀏覽器出現時，它永遠地改變了網際網路，使其對每個人，而不僅僅是對電腦科學家，變得親切和實用。今天，ChatGPT 的崛起標誌著人工智慧領域的一個類似轉變。就像網景公司簡化了網際網路的瀏覽一樣，ChatGPT 使人工智慧變得更容易為大眾所使用，儘管 ChatGPT 之前人工智慧就已經存在。



↳ **提示**：…象徵 ChatGPT 和網景公司的人形機器人，ChatGPT = 人工智慧：網景公司 = 網際網路。

ChatGPT 代表了一種利用機器學習的進步而發展的創新解決方案，其中生成式人工智慧是一個特別突出的貢獻者，我們將在一會兒後談到。我經常聽到這些術語——GenAI、FM、LLM——在隨意的對話中互換使用，這雖然沒大問題，但我們可以做得更好。在閱讀完本章後，我希望您能夠有足夠的理解能清楚地表達像 ChatGPT 這樣的聊天機器人是如何工作的，並給你的朋友留下深刻印象。一個常見的誤解是 ChatGPT 是一個人工智慧模型。實際上，它根本不是一個模型；它是一個使用人工智慧模型並結合自動化軟體的應用。它一開始便是「Chat」應用軟體與「GPT」人工智慧模型結合的應用，這解釋了為何它叫做 ChatGPT。然而，今天，它已經發展得遠遠超出了這個範疇。

ChatGPT 由如 GPT-4 和 DALL-E 的人工智慧模型提供動力，這些模型本質上是生成式的。它們屬於基礎模型（FMs）和大型語言模型（LLMs）的範疇。這些模型應用了生成式人工智慧原則，可以生成各種內容，從自然語言文本到視覺圖像。因此，它們在各種應用中發揮了重要作用，從創意內容生成到問題解決。要充分了解其能力，我們應該探索三個關鍵概念，讓我們從基礎模型開始。

基礎模型（Foundation Models, FM）是在龐大資料集上訓練成的泛用機器學習系統，以其在各種應用中的適應性和多功能性而著稱。它們的主要優勢在於**它們可以作為各種任務的基礎模型**，如語言翻譯和程式碼生成，它支援而非取代特定任務的模型需求。

基礎模型在訓練過程中通常使用自監督學習（self-supervised learning, SSL）。自監督學習是一種技術，它允許模型從未標記的資料中學習，或生成自己的訓練資料，減少對手動標記資料集的依賴。這一突破顯著地改變了人工智慧的場景，將原本專門化的系統合併到一個單一模型中，這個基礎模型具有多功能，可以有效地應對各種任務。

生成式人工智慧（Generative AI, GenAI）包括各種生成人類風格之數位內容的演算法，如文字、圖像或音樂。這些演算法通常會利用基礎模型在訓練過程中獲得的能力和知識。此外，生成式人工智慧模型擅長於回答問題、摘要文章和分析內容等任務。

在 2020 年代初期，深度學習取得了顯著的進展，特別是基於**轉換器**（transformer）架構的神經網絡。轉換器這個術語表示一種特定的深度學習架構，經常應用於自然語言處理任務。轉換器在推進深度學習方面發揮了關鍵作用，特別是在與序列資料相關的任務中，如文本處理和語言建模。這些任務包括基於大型語言模型的聊天機器人，如 ChatGPT、Copilot 和 Bard，以及由文本轉圖像的人工智慧藝術系統，如 Stable Diffusion、Midjourney 和 DALL-E。

生成式人工智慧在各個行業中都有應用：藝術、寫作、軟體開發、醫療保健、金融、遊戲、營銷和時尚。在 2020 年代初期，生成式人工智慧的投資出現了顯著的增長，像 IBM、Microsoft、Google、Baidu 等大公司和許多較小的公司都在積極開發生成式人工智慧模型。然而，人們也對生成式人工智慧的濫用存在擔憂，包括網絡犯罪和製造假新聞或深度偽造影片，這可能會被用來欺騙或操縱個人。我們將在第 9 章中深入探討它。

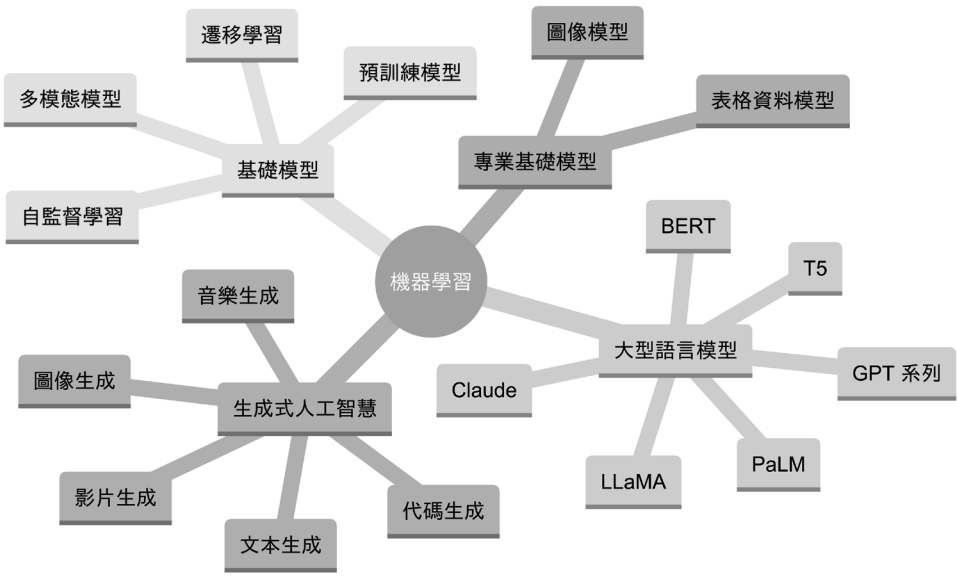
大型語言模型（Large Language Models, LLM），如 GPT-4、Llama3、Granite 和 Mixtral，是基礎模型的專門子集，專注於處理和生成人類語言。這些模型在自然語言處理（NLP）和機器學習中起著基礎作用。它們透過對龐大的語言資料集進行廣泛訓練來實現其語言能力。

大型語言模型是機器學習在語言理解和生成的背景下的具體實現。它們學習人類語言的複雜模式和結構，使其能夠理解和生成與語境相關且連貫的文本。

大型語言模型在機器學習中作為基礎工具，提供了對語言的廣泛理解，之後可以為特定的自然語言處理任務進行微調。這種適應性使它們成為各種應用中的多功能資產，如語言翻譯、內容創作和文本摘要，並對於更廣泛的生成式人工智慧領域做出貢獻。

除了大型語言模型，我們還可以找到像專門用於圖像的基礎模型，這些模型是在視覺資料上進行訓練，用於識別物體或生成圖像等任務。然後還有用於表格資料的模型，這些模型在處理結構化資訊方面表現出色，通常應用於金融和醫療保健等領域。這些不同類型的模型展示了人工智慧的

廣泛可能性和靈活性，使用基礎模型和生成式人工智慧概念來滿足各種資料需求和任務。

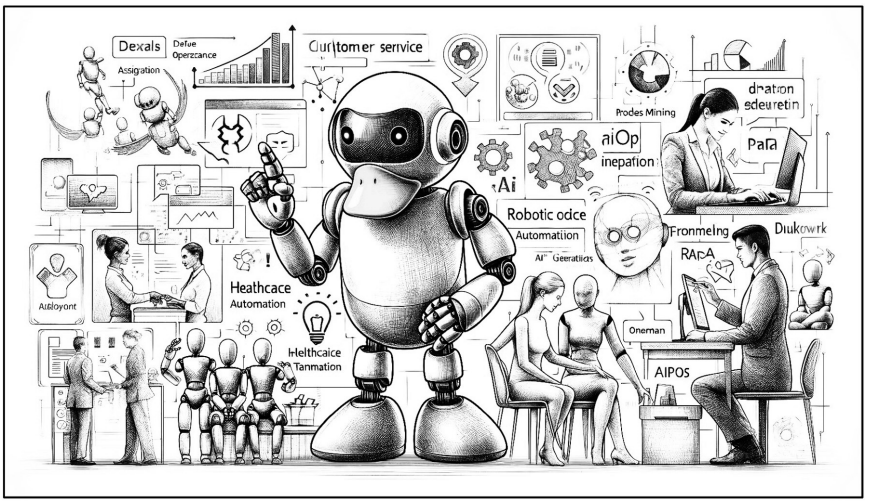


↳ **提示**：…Mermaid.js 思維導圖，以視覺方式組織以下「機器學習」使用的基礎模型案例 { 插入文本中的例子 }。

未來，請記得用「你知道嗎 ... ChatGPT 是由 ... 啦啦，基礎模型（多任務處理），生成式人工智慧（人類風格生成），大型語言模型（流暢語言）...」等等專業術語來給你的朋友留下深刻印象。接下來，我們將看到這些技術如何變成應用。

真實世界中的應用

今天，人工智慧系統有許多真實世界的應用，我忍不住對它們如何塑造我們的世界感到好奇與興奮。



↳ **提示**：…人類與各種真實世界人工智慧應用中的人形機器人，其中有一隻顯眼的機器鴨，嘴巴是黃色的 { 插入真實世界應用例子的摘要 }。

以下是我覺得特別有趣的一些常見的應用案例：

客戶服務（Customer Service）：客戶服務正在發生的變革是顯著的。在客戶服務流程中，線上虛擬代理人正在取代人類代理人。它們不僅僅是回答常見問題；它們還提供個人化建議、跨銷產品，甚至預測你的下一個想法。這改變了我們對網站和社交媒體平台上如何與客戶互動的看法。從電子商務網站上的最新消息機器人到像 Slack 和 Facebook Messenger 這樣的平台，這些虛擬代理人正在變得不可或缺。

人工智慧程式碼助理（AI Code Assistants）：看到人工智慧進入程式設計領域是很有趣的。像 IBM watsonx Code Assistant 和 GitHub Copilot 這樣的工具正在改變軟體開發人員的工作方式。這些人工智慧助理提供即時的程式碼建議，使編程更快速、更有效率。這就像擁有一個理解你意圖並幫助你寫出更好程式碼的聰明夥伴。

AI 維運（AIOps）：人工智慧驅動的自動化正在革新 IT 維運。AIOps 結合了人工智慧和機器學習，以提高 IT 系統的性能和效率。它可以預測和識別即時問題、自動化事件回應，並優化 IT 資源。雖然許多公司專注於從故障中快速恢復，但 AIOps 強調在問題發生之前就能預測和避免意外事件。

人工智慧驅動商業運作轉型（AI-transforming Business Operations）：人工智慧驅動的自動化軟體代表了企業運作方式的一個突破性演進。這不僅僅是關於自動化；它是關於在業務流程的各個方面注入智能。以下是一些關鍵組件的詳細介紹：

- **流程探勘**（Process Mining）：人工智慧分析業務事件日誌以優化工作流程、識別流程瓶頸和低效率環節。
- **機器人流程自動化**（Robotic Process Automation, RPA）：在人工智慧的增強下，RPA 可動態分析數據並修改其方法，因此能夠自動化更廣泛的工作流程。
- **工作流程自動化**（Workflow Automation）：人工智慧透過在工作流程中做出智能決策，使任務更加流暢、加速流程並促進一致性。

行業應用（**Industry Applications**）：人工智慧已經進入所有行業，革新了它們的運作並帶來了新的可能性。以下是一些值得注意的應用：

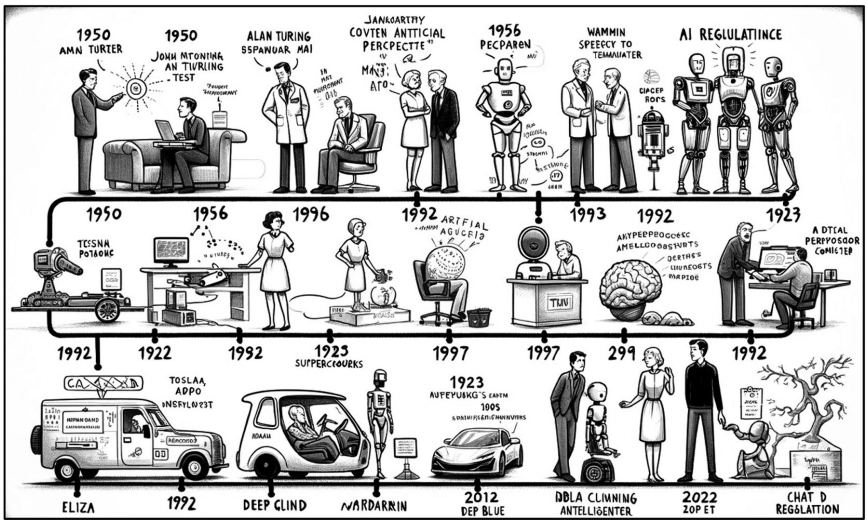
- **自動股票交易**（Automated Stock Trading）：人工智慧驅動的平台優化股票投資組合，進行高頻交易，從而改變了金融行業。
- **醫療診斷**（Healthcare Diagnostics）：人工智慧驅動的診斷工具分析醫學影像，幫助早期疾病檢測並改善醫療效果。
- **電子商務個人化**（E-commerce Personalization）：人工智慧推薦引擎透過客製化的產品建議來增強購物體驗，提高參與度並推動銷售。

我很榮幸幾乎每天都能從事跟這些人工智慧應用相關的工作。這不僅僅是關於技術；我將這些真實世界的應用視為一種工作力量的演進，它使人工智慧和人類之間能夠無縫協作，從而實現流程優化和效率提高。人工智慧給人類的禮物是時間，它讓我們能夠花更多時間在最重要的事情和人身上。

現在，讓我們將這一切放在時間軸上來結束這一章。

人工智慧通往現在的道路

我一直對人工智慧的歷史感到著迷。正如你之前聽到的，人工智慧的演進不僅塑造了科技行業，也在我的職業生涯中扮演了重要角色。



↳ **提示**：…人工智慧發展時間軸資訊圖，從 1950 年到 2023 年，展示了越來越複雜的人形機器人 { 插入總結的人工智慧時間軸 }。

以下是人工智慧歷史上的重要日期和里程碑：

1950 年：正如前面提到的，一切都始於艾倫·圖靈（Alan Turing）的開創性論文《計算機械與智能》（Computing Machinery and Intelligence）。圖靈是二戰期間破解納粹的恩尼格瑪（ENIGMA）密碼的天才，他提出了

一個深刻的問題：「機器能思考嗎？」，他引入了圖靈測試[22]來評估電腦展現人類智能的能力。對於這個測試的價值的相關辯論從那時起就一直持續著。

圖靈的工作為人工智慧的概念奠定了基礎，激發了我對這個領域的早期興趣。

1956 年：約翰·麥卡錫（John McCarthy），一個與人工智慧同義的名字，在歷史悠久的達特茅斯學院會議上創造了「人工智慧」這個術語。我知道你在想什麼。不，我沒有參加這個會議，因為那時我還沒出生！別這樣；）。

他的貢獻並沒有止於此；他還發明了 Lisp 編程語言。同年，艾倫·紐爾（Allen Newell）、J.C. 肖（J.C. Shaw）和赫伯特·西蒙（Herbert Simon）創造了邏輯理論家（Logic Theorist），這是世界上第一個可操作的人工智慧軟體。麥卡錫的工作不僅塑造了人工智慧，也影響了我，讓我在這個領域追求職業生涯。

1964 年：約瑟夫·魏澤恩鮑姆（Joseph Weizenbaum）在 1964 年至 1967 年間在麻省理工學院開發的 ELIZA 是一個早期的自然語言處理程序，也是現代聊天機器人（如 ChatGPT）的前身。它使用模式匹配和腳本回應來模擬對話，產生了一種機器似乎理解使用者的幻覺。

1967 年：弗蘭克·羅森布拉特（Frank Rosenblatt）帶著 Mark 1 感知器（Perceptron）登場，這是第一台基於神經網絡的電腦，可以透過試錯來學習。然而，僅一年後，馬文·明斯基（Marvin Minsky）和西摩·帕帕特（Seymour Papert）出版了一本名為《感知器》（Perceptrons）的書[23]，暫時阻礙了神經網絡研究的進展，因為他們強調了感知器模型的侷限性，這導致了一段市場對該領域懷疑和投資減少的時期（注意這一里程碑和下一個之間的間隔）。

1980 年代：隨著反向傳播演算法（backpropagation algorithm）的引入，神經網絡經歷了一次復興。人工智慧開始應用神經網絡的威力。

2016 年：DeepMind 的 AlphaGo，由深度神經網絡驅動，透過在一個具有數以萬計可能走法的複雜遊戲中擊敗世界冠軍圍棋選手李世石，震驚了世界。Google 收購 DeepMind 進一步強調了這一成就的重要性。AlphaGo 的勝利向我們展示了人工智慧處理複雜問題時令人難以置信的潛力。

2022 年：快轉到現在，我們發現自己處於一個以 ChatGPT 等大型語言模型為特徵的新人工智慧時代。基於生成式人工智慧實踐，這些模型已經改變了這個領域，提高了人工智慧的性能和為企業創造價值的能力。

2023 年：歐盟的人工智慧法案[24]為人工智慧技術引入了全面的規定。這項開創性的立法旨在減輕人工智慧可能帶來的損害和道德問題，為全球人工智慧法規設立了先例。該法案要求對人工智慧系統進行安全風險評估，根據其設計來識別風險並實施必要的緩解措施。這個過程涉及一種整合方法，將經過驗證的資訊安全實踐程序與人工智慧特定的控制相結合。

2024 年：北卡羅來納州立大學開設了「資訊安全：可信賴的人工智慧」課程，我擔任客座教授，而這本書是教材。好吧，這可能不會像其他事件那樣達到同樣的歷史高度，但嘿，我是寫這本書的人。；）

成為這個時代的一部分真的很令人興奮，人工智慧對企業和整個科技行業產生了如此深遠的影響。這些可能性似乎是無限的。人工智慧的歷史不僅僅是技術進步的紀錄；它對我的職業生涯產生了重大影響，並讓我保持積極性，乘風破浪地在這個不斷擴展的人工智慧領域中前進。

人工智慧迷思破解

到目前為止，我們花了相當多的時間來揭示人工智慧的歷史，理解其本質。我們探討了它的根源，它是如何演變的，以及它在我們今天的世界中所呈現的各種形式。然而，對於任何複雜的話題，特別是像人工智慧這樣被廣泛討論的話題，總會有一些錯誤理解和迷思在流傳。受到 Google 的「探索 6 個人工智慧迷思」等資源的啟發[25]，我將試圖揭穿一些與人工智慧相關的常見迷思。我旨在澄清混淆，並提供一個更清晰的圖像，讓大家了解人工智慧到底是什麼，又不是什麼。

迷思 1：人工智慧、機器學習和深度學習是一樣的——我們剛剛學過這個！它們是人工智慧生日蛋糕的不同層次。人工智慧是機器智能的廣泛概念。在這個大傘下是機器學習（ML），讓電腦從例子中學習，而不是遵循嚴格的規則。ML 的一個熱門子集是深度學習（DL），受到我們大腦的啟發，它擅長識別複雜的概念與模式，比如「派對」是什麼樣子，或者「擁抱」是什麼意思。

迷思 2：所有人工智慧系統都是不可理解的「黑盒子」——事實並非如此。有些人工智慧系統很簡單，而有些很複雜。但這並不意味著它們都是神秘的。研究人員正在努力使人工智慧更加透明，幫助我們理解它們為什麼做出某些決定。有時，人工智慧在決策方面可能比人類更透明，因為人類可能無法完全理解自己的偏見。

迷思 3：人工智慧的程度只能和其使用的訓練資料一樣好——是的，資料很重要，但這並不是全部。人工智慧創新還依賴於演算法、硬體和人類智慧。沒有一個資料集是完美的，但我們有一些訣竅，比如合成資料（synthetic data）和模型約束（model constraints），來平衡不完美的資料。

迷思 4：人工智慧系統本質上是不公平的——人工智慧中的不公平更多的是來自於設計和部署中的人類決策，而不是人工智慧本身。是的，如果訓練有問題，人工智慧便會反映人類的偏見。但透過周到的設計和語境感知的部署，人工智慧實際上可以幫助人類發現和減少決策中的偏見。

迷思 5：人工智慧會使人類變得多餘——歷史告訴我們，像人工智慧這樣的新技術通常會使工作崗位轉移，而不是使其消失。人工智慧擅長特定任務，但至於涵蓋整個工作崗位嗎？沒那麼誇張。真正的挑戰在於管理工作人員的過渡，確保他們擁有新技能和技術支援，能適應人工智慧可能創造的新型態工作。

迷思 6：人工智慧接近於人類智能——雖然人工智慧在特定任務上表現得很好，比如作曲或下圍棋，但它仍然遠遠不及人類智能。人工智慧不像我們那樣「理解」音樂或遊戲。純粹只是模式識別，而不是創造力或代理能力。像遷移學習（transfer learning）這樣的技術正在推動人工智慧的發展，但要達到人類智能的水準仍然是一個遙遠的目標。

測驗時間

研究過去，了解現在，創造未來。我迫不及待地想看到你在人工智慧發展上的成就，在未來的年份裡，成為本章時間軸上的一個里程碑！

1. 約翰‧麥卡錫在他 2004 年的論文中將人工智慧定義為什麼？
   a. 機械機器人有關的研究
   b. 製造智能機器的科學和工程，尤其是智能電腦程式
   c. 自動化演算法的過程
   d. 開發用於解決複雜問題的電腦系統

2. 艾倫‧圖靈引入的圖靈測試有什麼重要之處？
   a. 它是第一個人工智慧程式
   b. 它區分了人工智慧和人類智能
   c. 它測試了電腦展現人類智慧的能力
   d. 它被用來破解 ENIGMA 密碼

3. 在人工智慧的背景下，「深度學習」主要涉及什麼？
   a. 基本機器學習演算法
   b. 統計分析
   c. 具有多層的神經網絡
   d. 高階語言的程式設計

4. 根據你的研究與破解，以下哪個有關人工智慧的迷思很明顯是錯誤的？
   a. 人工智慧、機器學習和深度學習本質上是相同的東西
   b. 所有人工智慧系統都是不可理解的「黑盒子」，無法理解
   c. 人工智慧頂多只和它所訓練的資料一般有效
   d. 人工智慧快達到人類智能

5. 是非題：史都華‧羅素和彼得‧諾維的書將人工智慧分為像人類一樣思考和行動的系統，以及能理性思考和行動的系統。

   a. 是

   b. 否

接下來

當你結束這一章時，想想你剛剛經歷的，關於人工智慧的，不可思議的故事。從古代神話到今天的 ChatGPT，人工智慧的成長不僅僅是技術上的；它是我們人類故事的一部分。理解弱人工智慧和強人工智慧之間的區別，看到機器學習如何塑造產業不僅僅是教育性的；它是迷人的。我希望你會像我分享本章時一樣感興趣和興奮。請記住，這不僅僅是關於數字或編碼。這是關於人類的聰明才智和我們無窮的好奇心。反思你所學到的，想想人工智慧的過去是如何塑造這個令人興奮的未來的。

…

我很幸運能與行業中一些最知識豐富的專業人士合作，這些人處於將人類專業知識與人工智慧助理相結合的尖端領域。這種協同作用不僅僅是理論性的；它正在創造日常生活中各種引人入勝的應用案例，而你很快就會學到。

在即將到來的這一章中，我們將提供一系列富有洞察力的訪談。我的同事們將講述他們自己的經歷，提供第一手資料，說明現實世界中的人工智慧應用是如何塑造我們的生活的。這些敘述不僅僅是關於技術，還關於背後的人類故事，挑戰、突破和意想不到的轉變。

你想要邊聽故事邊吃薯條嗎？（這個問題很快就會變得更有意義）。