



# 溫故

在介紹開始之前，先簡單回顧兩個上次科普過的AI新名詞，以便能夠更好的對比和理解今天要介紹的新名詞：

## AI Agent

「AI Agent (AI智能體)」是指一種能夠自主執行任務、作出決策並與環境進行交互的人工智能系統或程序。簡而言之，它就是一個「數字員工」，不僅能聽懂你的需求，還能主動規劃、執行任務。



◀一名學生(左)在志願者的指導下安裝騰訊AI智能體Workbuddy。新華社

## MCP

「Model Context Protocol」，即模型上下文協議，被譽為AI大模型的標準化工具箱。就像互聯網時代的TCP/IP協議一樣，它被用於在不同的軟件組件之間傳遞信息。

## AI Agent



## MCP



## 3C科技

2025年，筆者曾把當時頻繁出現的一些關鍵的AI新名詞向大家進行了科普。而在過去一年間，AI領域的新名詞又層出不窮，其中有不少直接關係到AI技術未來的走向，並將影響普通人的生活。下面就讓筆者繼續用盡量通俗的語言介紹這些重要的AI新名詞。

姚剛

# 知新

過去一年，伴隨着AI大模型的不斷迭代，現在的AI正在從「只會動嘴」進化到「能動手幹活」，甚至開始理解這個世界的運行規律。

## World Model (世界模型)

先說一個正在悄悄引發革命的概念——世界模型。我們常說的「大語言模型(LLM)」實際上是利用大量文本數據訓練出來的模型，能夠理解和生成自然語言文本。而「世界模型」則是在試圖讓AI理解「這個世界為什麼會這樣運轉」。

這個概念真正引起廣泛關注，是在2024年初OpenAI發布Sora(視頻生成模型)的時候。Sora展現出了對物理世界客觀規律的基本認知，比如：物體間會相互作用，水往低處流，相同的物體在不同介質裏會有不同的運動特性等。世界模型概念的出現，是希望在AI內部也建立起對世界物理特性和三維空間的認知能力，這樣AI就可以生成更符合真實世界體驗的圖片和視頻等，甚至還可以生成高度逼真的虛擬世界。

它的未來應用場景將極為廣泛：在影視和遊戲行業，它可以實時生成符合物理規律的開放世界；在自動駕駛領域，它可以在AI的「腦海」中模擬極端路況，讓車輛在安全的虛擬環境中完成「仿真路試」；在科學研究中，它甚至可以模擬分子之間的相互作用，在新藥研發的臨床試驗前，先在數字世界裏快速多次進行仿真實驗。

## Token

所謂Token，就是AI在處理信息時的最小計量單位。你可以把它想像成手機流量中的「KB」。AI每進行一次思考，就要消耗一定數量的Token。今年3月，國家數據局在中國發展高層論壇上正式宣布，將Token的中文標準譯名定為「詞元」，這意味着「詞元」成為了官方認定的AI時代價值錨點和結算單位。

當中國的日均Token調用量從2024年初的1000億次飆升到2026年3月的140萬億次時，這個詞彙已經不再是技術人員的專屬黑話，而是成為了衡量AI產能、計算成本和商業價值的通用計量單位。很多人可能覺得詞元和自己沒什麼關係，其實不然，它就像AI世界的「基礎貨幣」。詞元就是AI處理、理解、生成文本時，最基本的計量單位：我們人類讀書寫字以「字」「詞」為單位，AI處理信息時，就以詞元為單位運算。



▲北京一場主題為「OpenClaw：從「會聊天」到「能交付」」的城市沙龍活動。新華社

## World Model



大公報AI製圖

## OpenClaw



## OpenClaw

如果說MCP是連接AI與軟件工具的通信協議，那麼OpenClaw就是基於這種連接能力，實現「自動化操作」的實用工具。你可以把OpenClaw理解為一位隨時待命的「數字員工」，它的核心優勢是理解自然語言指令，還能自己學習和創建技能(skill)、設置自動化流程，不管是個人還是企業，都能用到。

舉個生活中的例子，只需要對OpenClaw說「每天早上8點，給我發送包含待處理郵件、今日日程和昨日日報內容的郵件」，它就會自己學習必要的工作使用方法和任務流程等，並自動設置定時任務，每天按時完成。在企業應用場景上，OpenClaw能大幅提升工作效率，比如電商運營可以用它自動抓取競品價格和標籤、設置庫存提醒；新媒體人可以用它自動監測最新資訊、整理熱點素材……它的出現讓普通人也能通過簡單的指令，讓AI幫自己承擔重複型的工作，降低了AI自動化的使用門檻。這也正是最近興起「養蝦」熱潮的原因。



▲北京一場主題為「OpenClaw：從「會聊天」到「能交付」」的城市沙龍活動。新華社

# 從AI Agent到OpenClaw 2026年AI新名詞科普

## Skill



## Skill

在OpenClaw的介紹中，我們提到了「技能」(skill)。skill的本質是把個人或團隊的經驗固化成結構化的任務模板。簡單來說，skill就是別人已經幫我們打磨好的「專項技能模塊」，它把AI需要的提示詞、規則、工具調用邏輯，全部打包成一個現成的模塊，我們只需要一鍵啟用，就能讓AI擁有對應的專業能力。比如，做電商運營，啟用「競品數據分析skill」，黏貼競品店鋪鏈接，AI就能自動抓取數據、拆解運營打法，給出優化建議。

那麼「Skill」和「Prompt(提示詞)」又有什麼區別呢？prompt是單次性、非結構化的臨時指令，主要用於引導AI完成單次簡單任務，無法復用，比如讓AI「寫一段商品介紹廣告詞」的指令就是prompt；而skill形成了AI的「技能插件」，讓AI可以即插即用。

skill的使用方法非常簡單，目前主流的AI平台都有「技能廣場」，裏面有上萬個skill，覆蓋辦公、設計、數據收集分析、創作等各種場景，我們只需要找到自己需要的skill，一鍵安裝啟用，就能讓AI立刻擁有對應的能力。你會發現，讓AI做同樣一件事，在使用了相應的skill之後的效果要比AI自己從零到一做的效果專業很多。

## Harness

Harness這個詞在英文中是「馬具」的意思，有了技能(skill)，AI還需要一個受控的「工作環境」來確保它不會亂來。這就是Harness(中文可以理解為「AI控制框架」)的價值所在。

Harness不是AI本身，也不是某個具體技能，而是專門寫給AI的「操作守則」。它的本質是圍繞AI Agent構建的一套完整的控制系統，包括：代碼、配置、執行邏輯、驗證機制等；負責管理AI能訪問哪些工具、遵守什麼規則、如何自我糾正、人類如何監控它的行為……就像馬術裏的繮和馬鞍。Harness能把AI的「能力」導向正確的方向，讓AI可靠、安全地運行，而不會「失控亂撞」。

一個完整的Harness通常包含五個核心部分：系統提示詞(給AI定義角色和職責)、可調用的工具與技能(AI的工具箱)、運行環境(如安全沙箱和文件系統)、編排邏輯(如何拆分複雜任務、如何協調多個子AI)，以及一些中間件(比如，自動檢查代碼風格、運行測試、驗證結果的質量等)。

## CLI

CLI(Command-Line Interface)，即命令行界面。在AI浪潮之前，CLI主要是程序員和運維人員用來操控電腦的文本命令窗口。而現在，AI CLI不是傳統意義上那個黑乎乎的終端窗口，而是AI編程工具(如Claude Code等)提供的命令行交互入口。

它的核心用途是讓AI能精準、高效地操作各種工具和系統。它是通過輸入文字指令來控制系統的方式，雖然看起來沒有圖形界面(GUI)漂亮，但它極其高效。我們習以為常的GUI是給人用的，因為它對於人類更直觀，而CLI是給AI用的，可以讓AI更直接準確地操作工具。

以前我們用AI去操作一些軟件工具，需要讓AI模擬人類點擊鼠標、打開界面，不僅不穩定，還很低效；而CLI可以把工具的功能轉化為簡單的文字指令，AI只要輸入指令，就能快速執行操作，不用再模擬鼠標點擊。

它的使用流程也很簡單，對於普通人來說，不需要自己輸入指令，只需要把CLI的命令手冊交給AI，並告訴AI你的需求(比如「幫我把上周的所有會議紀要匯總到一個表格中」)，AI就會自動組合對應的CLI指令，執行操作。最近，越來越多的軟件開發者正在達成一個共識：未來，直接使用軟件的不是人類，而是AI，因此圖形界面將不再重要，更重要的是面向AI的CLI界面。

## 寫在最後

綜合上面我們介紹過的所有這些AI新名詞，其實，它們本質上都是AI向「更智能、更實用、更可控」方向發展的產物；世界模型讓AI「懂世界」，詞元是AI處理信息的「基礎單位」，MCP解決AI的「連接難題」，OpenClaw實現AI的「自動化操作」，Skill讓AI擁有「專項能力」，Harness讓AI「可靠運行」，而CLI讓AI操作更

「高效精準」。它們看似複雜，實則都是為了讓AI更好地服務於我們的生和工作，降低AI的使用門檻，讓更多人能享受到AI帶來的便利。相信再過不久，這些新名詞會像「人工智能」「大數據」一樣普及，而我們現在讀懂它們，就是在跟上時代的腳步。

## 上述名詞的關係

講完了這麼多新名詞，大家可能會有點混淆。簡單舉個例子以使用更直觀的方式理解它們的關係：假如我們要創造一個像真人一樣可以幫我們做事的「虛擬人」。那麼，Agent就是我們要造的那個「人」，是整個體系的核心；OpenClaw是他的身體框架，支撐他思考和拆解任務；MCP是他操作工具的手，讓他能靈活使用各種外部軟件；Skill是他腦子裏的知識和本領，決定了他能勝任哪些具體工作；而Harness則是確保他乖乖坐在位子上、按規矩辦事的辦公室工位，既提供了工作場景，也劃定了行為邊界。