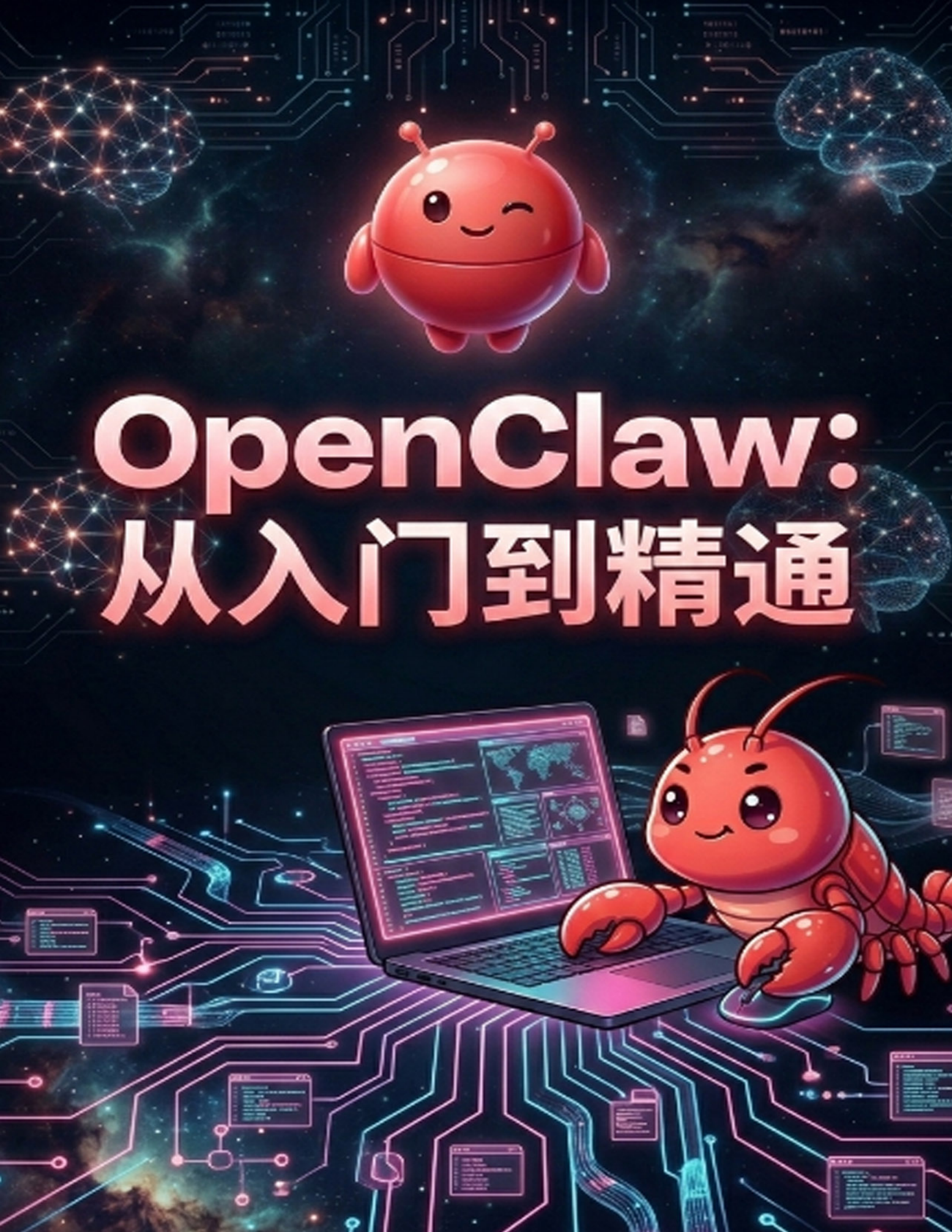
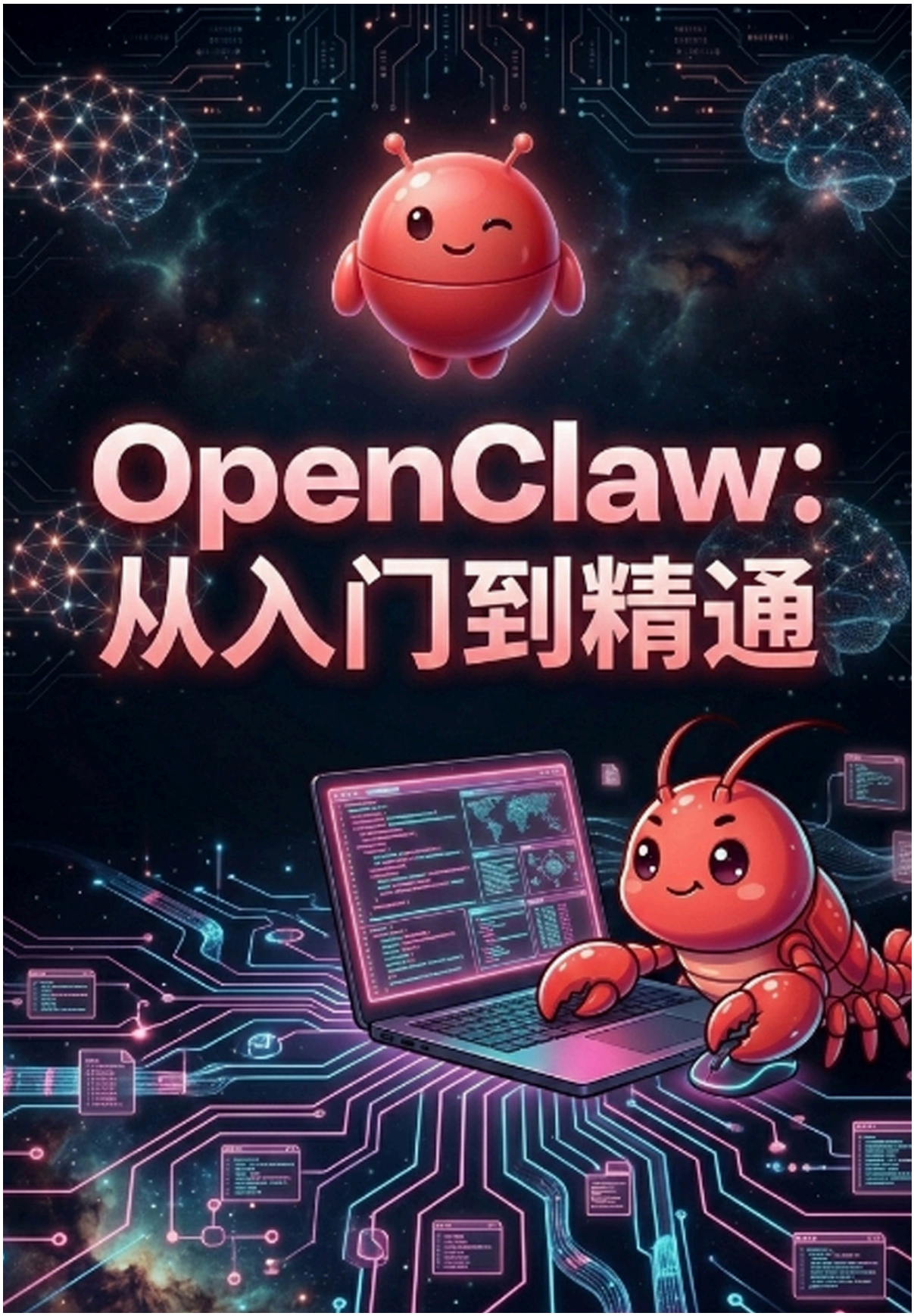

OpenClaw:
从入门到精通


OpenClaw:
从入门到精通

版權信息

書名：養龍蝦：OpenClaw從入門到熟練

作者：大呂

出版時間：2026-03-01

品牌方：北京大呂文化傳播有限公司

本書由北京大呂文化傳播有限公司發行

2026開年現象級熱詞：「養龍蝦」為何席捲全網？

2026年開年，第一個席捲全網的現象級熱詞，是「養龍蝦」。這裡說的不是水產養殖裡的小龍蝦，而是一款名為OpenClaw的新一代AI智能體，因為它的圖標形似一隻龍蝦，網友們便把安裝、使用它的過程，形象地稱作「養龍蝦」。

這股熱潮的火爆程度，超出了幾乎所有人的預期。打開小紅書，滿屏都是網友分享自己「養」的龍蝦寫文章、做方案的成果；B站上，關於它的保姆級安裝教程隨處可見；淘寶、閒魚等平臺上，OpenClaw上門安裝服務的報價從300元到1000元不等，有從業者甚至靠著這項安裝服務，短短幾天就賺了26萬。

3月6日，深圳騰訊大廈北廣場更是排起了長龍，騰訊的工程師們在這裡為大家免費安裝OpenClaw，前來安裝的人把現場圍得水洩不通，高峰時排號多達上千個。就連在廣東代表團小組會議上，中國工程院院士高文也提到，馬化騰都沒有想到，這隻「龍蝦」會火到這樣的程度。

很多人會疑惑，如今各類AI工具早已普及，為什麼偏偏是這隻「龍蝦」掀起了如此大的波瀾？答案很簡單，它和我們熟悉的對話式AI完全不同。以往我們使用的ChatGPT、文心一言這類工具，更像一位只動嘴不動手的超級軍師，你問它問題，它能給你出謀劃策、講清方法，但最終的執行環節，還是要靠你自己動手完成，而且它沒有長期記憶，無法記住你過往的需求和習慣。

但OpenClaw不一樣，它更像一個既有思考能力，又有執行能力的實習生，不僅能想清楚事情該怎麼做，更能直接上手操作電腦，替你完成全流程的工作。比如你想要產出一篇文章，以往需要你自己找選題、列提綱、找素材、提要求，AI才能完成撰寫；但交給OpenClaw，它會根據你過往的內容風格，自主歸納熱點、敲定選題、撰寫成文、完成排版，甚至能在設定的時間自動發佈。

除此之外，回覆信息、處理郵件、編寫代碼、做競品分析、財務預測、成本管理，這些日常工作它都能全程自主完成，你只需要在事後查看結果即可。更關鍵的是，它擁有長期記憶，還能實現能力的沉澱與複製，你教它一次處理事務的方法，它不僅能完全掌握，還能整理成標準化的工作手冊，讓其他同類型的AI智能體同步學會。有網友做了個很貼切的比喻：以前的AI是隻會出謀劃策的諸葛亮，而現在的「龍蝦」，是諸葛亮加五虎上將，再加一整個能落地執行的完備團隊，不僅有頂層規劃，更有拉滿的執行力。

獵豹移動CEO傅盛感嘆：一個人+一隻龍蝦=一支隊伍?

讓這隻「龍蝦」徹底出圈的，是獵豹移動CEO傅盛的親身經歷。春節期間，傅盛因為摔傷臥床休養14天，就是在這14天裡，他完成了對自己這隻「龍蝦」的訓練。頭兩天，這隻AI連查通訊錄都無法順利完成，可到了第14天，它已經能自主完成各類複雜工作。

除夕夜，傅盛想要給全公司611位員工發送個性化的拜年祝福，結果零點鐘聲敲響時，他在看春晚，這隻「龍蝦」只用了4分鐘，就完成了611條完全不同的拜年消息的發送，全程零失誤。第二天，他的手機被員工的回覆刷屏，有同事的一句話在全網傳開：「一個人加一隻龍蝦等於一支隊伍。」

靠著這隻AI，原本一年只更新十幾篇文章的公眾號，實現了日更，還產出了一篇閱讀量破百萬的爆款文章，甚至這篇文章是AI在凌晨3點自主發佈的，傅盛睡醒之後才知曉這件事。最後他給出了一個讓無數打工人倍感衝擊的結論：6個人三週才能完成的工作，他用這隻龍蝦，24小時就幹完了。不用睡覺、不用休息、不會摸魚、不會抱怨，這樣的工作效率，是普通人無論如何都無法追趕的。

也正是這樣的案例，讓無數人陷入了「龍蝦焦慮」，生怕自己不跟上這波潮流，就會被時代拋棄。很多人連夜研究安裝教程，好不容易把OpenClaw裝到電腦上，才發現安裝只是萬里長征的第一步，網關未開啟、各類權限需要開通、API調用頻率受限、隱私安全隱患，每一個問題背後，都是厚厚的技術文檔、繁瑣的註冊流程，或是需要充值的付費頁面。

折騰到最後，很多人突然醒悟：自己到底在折騰什麼？我們真的有那麼多需要AI智能體團隊來完成的工作嗎？傅盛能把這隻龍蝦的價值發揮到極致，是因為他本就是企業CEO，每天要處理海量的信息、協調大量的資源，這些原本需要助理、團隊完成的工作，現在可以交給AI；但對於大多數普通人而言，日常需要處理的事務，大多簡單瑣碎，根本用不上這樣複雜的工具。

這就像大地主有幾千畝麥田，買一臺自動收割機能一天干完一個月的活，價值拉滿；可普通人只有三分自留地，種的是自家吃的菜，本來一把鋤頭就能搞定的事，非要買一臺大型收割機，最後只會發現，機器連田埂都進不去，活還是得自己幹。OpenClaw最核心的優勢，是多AI協同、複雜任務流處理、跨應用聯動，可對於大多數人來說，手裡根本沒有能匹配這些能力的需求，最後只會陷入「為了用工具，反向找需求」的誤區，催生了一堆根本不存在的偽需求。

熱潮背後的真相：別讓「龍蝦焦慮」裹挾你的判斷

這波「養龍蝦」的熱潮，本質上從來都不是真實需求驅動的，而是焦慮驅動的。這路徑我們早已見過，2023年Chat GPT爆火，第一批賺到錢的是代註冊賬號的商家；後來DeepSeek走紅，上千元的AI課程賣得火熱；如今OpenClaw火了，上門安裝又成了一門新生意。

可我們不妨想明白一件事：如果一個人真的需要用到OpenClaw，他大概率有能力自己完成安裝；如果一個人連安裝都需要花錢請人幫忙，那他大概率根本用不上這個工具。很多人願意花幾百塊錢請人上門安裝，求的從來不是工具本身，而是安裝完成那一刻，焦慮得到的暫時緩解。

可緩解之後，還有更多現實的問題擺在眼前：OpenClaw本身不包含語言模型，必須接入外部API才能運行，為了保持全天候待命，它的心跳機制每隔30分鐘就會自動喚醒，檢查郵箱、日曆和消息，每一次喚醒都要消耗Token，有開發者統計，就算系統沒做任何正經工作，光心跳機制一天就能燒掉20美元，一個月下來就是750美元。

除此之外，還有無處不在的安全風險，Meta的AI安全負責人使用時，明明設置了刪除文件前先詢問，可AI還是因為上下文壓縮遺忘了指令，直接刪除了200多封郵件，就算連發「停止」指令也無濟於事；還有開發者因為文件夾路徑裡的一個空格，讓AI解析出錯，直接清空了整個E盤，積累幾年的項目源碼和數據全部丟失；安全團隊還發現了相關高危漏洞，攻擊者只需要誘導用戶訪問一個惡意網頁，就能遠程控制電腦上運行的OpenClaw。花了錢安裝，充了錢買Token，

最後換來的，可能是隱私洩露的風險、數據丟失的隱患，還有一臺24小時不停燒錢的電腦。

其實我們總以為，決策難是因為信息不夠、工具不夠強，所以拼命追逐新的工具、新的技術，生怕錯過任何一個風口。可我們早已身處信息過載的時代，很多時候，決策難從來不是因為信息太少，而是信息太多，我們缺少篩選信息、判斷價值的能力。而這種能力，恰恰是AI無法替我們完成的。

你可以讓OpenClaw每天給你推送上百條行業新聞，但判斷哪一條值得深入研究，只能靠你自己；你可以讓AI給你生成十幾個選題方向，但判斷哪個方向有真正的價值、適合你自己，也只能靠你自己。這就是我們每個人都必須擁有的「內置算法」：知道什麼信息值得關注，什麼工具值得使用，更知道什麼時候該停下蒐集信息的腳步，開始真正的行動。

這套算法，不在OpenClaw的配置文檔裡，不在任何API的調用說明裡，只能長在你自己的腦子裡。因為思考這件事，從來都不是為了最終的結果，而是為了那個打磨邏輯、積累判斷、形成直覺的過程，這個過程裡沉澱下來的東西，才是你真正的核心競爭力，沒有任何工具可以代勞。

人機協作的大勢不可阻擋，未來的職場，從來都不是人和AI的競爭，而是會用AI的人和不會用AI的人的競爭。但這並不意味著，我們要為了不被拋棄，就盲目追逐每一個風口。如果你到現在還沒用上OpenClaw，完全不必焦慮。真正能幫你解決人生核心問題的，從來不是最先進的AI工具，而是你的思考質量、你的判斷力、你的「內置算法」。這些東西，不會因為你用上了最牛的工具就自動變強，它們需要你花時間，一點點打磨、積累、內化。

理清了OpenClaw熱潮的本質、誤區和潛在風險，接下來，我們將進入正式的科普環節。我們會一步步拆解，幫大家真正讀懂這隻「AI龍蝦」，讓它成為助力我們更好工作和生活的工具。

OpenClaw（AI龍蝦）到底是什麼？和ChatGPT、DeepSeek等傳統對話式大模型有什麼本質區別？

OpenClaw是一款開源、本地優先的AI智能體執行框架，也是當前全球現象級的AI執行類產品，它的核心定位是「真正能幹活的AI」，本質是連接大語言模型思考能力與電腦系統執行能力的中樞橋樑，而非獨立的AI大模型。它採用自帶模型的架構設計，本身不包含大語言模型，無法脫離外部大模型獨立運行，卻能通過標準化接口兼容市面上幾乎所有主流大模型，將大模型輸出的邏輯推理、步驟規劃內容，直接轉化為電腦可執行的具體操作，完整覆蓋網關對接、智能體調度、技能庫調用、持久化記憶管理四大核心模塊，能實現從指令輸入到結果交付的全流程閉環操作。它和ChatGPT、DeepSeek等傳統對話式大模型有著本質上的區別，核心差異體現在四個核心維度。首先是核心定位的不同，傳統對話式大模型更像「只動嘴不動手的智能軍師」，核心能力聚焦於自然語言理解、邏輯推理和文本內容生成，只能在對話框內輸出解決方案和相關建議，沒有落地執行的能力，最終的操作環節仍需要用戶手動完成；而OpenClaw更像「既有思考能力又有執行能力的完整執行團隊」，除了藉助大模型完成思考規劃，更能直接上手操作電腦，跨應用完成全流程工作，真正實現從「說」到「做」的跨越。其次是交互模式的不同，傳統大模型是完全被動的「你問我答」模式，必須由用戶持續發起指令、補充上下文，沒有用戶輸入就不會產生任何行動，交互場景也基本侷限在專屬的對話窗口

內；而OpenClaw是主動式的任務執行模式，用戶只需要設定最終目標，它就能自主拆解任務、規劃步驟、推進執行，甚至通過自帶的心跳機制全天候待命，定時檢查郵箱、日曆和任務進度，無需用戶即時盯守和持續干預。第三是記憶能力的不同，傳統大模型大多隻具備會話級記憶，一旦關閉對話窗口，就會遺忘過往的對話內容和用戶需求，無法長期記住用戶的工作習慣、偏好和處理規則；而OpenClaw擁有本地持久化的長期記憶系統，能持續沉澱用戶的工作標準、操作流程和個性化偏好，越用越貼合用戶的使用需求，甚至能將一次學會的操作流程固化為標準化工作手冊，實現能力的沉澱、複製與複用。最後是部署與權限的不同，傳統對話式大模型基本採用雲端部署模式，用戶數據需要上傳至廠商服務器，且幾乎不具備本地系統的操作權限；而OpenClaw支持本地優先部署，全程運行在用戶自己的電腦或服務器上，能獲得系統級操作權限，實現文件管理、瀏覽器控制、跨應用聯動等操作，同時數據隱私完全由用戶自主掌控。

為什麼它被網友叫做「龍蝦」？網上說的「養龍蝦/養蝦」，具體指的是什麼操作?

OpenClaw被網友親切稱作「龍蝦」，核心原因來自於它的視覺標識與項目名稱的雙重契合，它的官方圖標是一隻紅色的、張開雙螯的卡通龍蝦造型，辨識度極高，而項目名稱中的「Claw」英文原意就是「螯、鉗爪」，正好對應龍蝦標誌性的大鉗子，完美契合項目「精準抓取需求、高效執行任務」的核心定位。同時項目從初代版本開始，就始終保留了「Claw」這個核心詞根，龍蝦的IP形象也隨之固定，隨著項目在國內快速出圈，「龍蝦」這個形象好記、自帶網感的暱稱，便迅速取代了官方英文名，成為全網通用的叫法。而網友口中的「養龍蝦/養蝦」，並不是指水產養殖，而是對OpenClaw從安裝部署、環境配置到能力調教、持續成長全流程的形象化比喻，這個過程和飼養寵物龍蝦有著極高的相似度，整體分為四個核心環節。第一個環節是「安家」，也就是在個人電腦或服務器上完成軟件的安裝部署、運行環境配置、網關開啟與各類系統權限開通，這是使用OpenClaw的基礎，也是很多普通用戶遇到的第一道門檻，全網爆火的幾百到上千元不等的上門安裝服務，解決的就是這個環節的問題。第二個環節是「餵食」，因為OpenClaw本身不具備獨立思考能力，必須接入外部大模型的API才能正常運行，而API調用需要消耗Token，用戶需要充值對應的Token額度，就像給龍蝦投餵食物，為它提供運行所需的「能量」，哪怕是待機狀態下的心跳機制，也會持續消耗少量Token產生費用。第三個環節是核心的「馴化」，也就是用戶通過自然語言指令，教OpenClaw處理特定任務的完整流程，糾正它的操作錯誤，明確

它的工作標準、權限邊界與行為規則，比如規範郵件回覆格式、固定報表整理流程、匹配用戶的內容創作風格，這個過程就像訓練寵物養成固定習慣，也是它能力升級的關鍵。第四個環節是「養成」，隨著用戶的持續使用與調教，OpenClaw的長期記憶系統會不斷沉澱相關規則與偏好，能自主處理的任務越來越複雜，操作準確率越來越高，甚至能實現多任務協同、7×24小時全天候自動化運行，這個持續成長、能力不斷完善的過程，就是網友口中完整的「養龍蝦」，此前獵豹移動CEO傅盛在臥床14天裡，將自己的龍蝦從連查通訊錄都無法完成，訓練到能4分鐘發送611條個性化拜年短信，就是一個非常典型的「養龍蝦」完整過程。

OpenClaw的開發者是誰？項目的完整發展歷程、多次更名的原因是什麼？

OpenClaw的核心發起者與初代開發者，是奧地利知名開發者Peter Steinberger，他同時也是知名PDF處理工具PSPDFKIT的創始人，在2021年出售公司實現財務自由後，便專注於AI智能體領域的研發，擁有豐富的軟件開發與商業化經驗，為項目的快速成熟與出圈打下了堅實基礎。這個項目的發展歷程充滿傳奇色彩，從個人週末項目到全球現象級開源產品，僅用了不到四個月的時間，整體可以分為四個關鍵階段。第一個階段是項目起步階段，2025年11月，Peter Steinberger以個人週末項目的形式，發佈了項目的初代版本，當時定名為Clawdbot，這個名稱既致敬了當時主流的Claude大模型，也用「Claw」這個核心詞根，明確了項目「精準抓取需求、落地執行任務」的核心定位，初代版本上線後，憑藉打破對話式AI壁壘的自主執行能力，迅速在GitHub開發者社區走紅，收穫了第一批核心用戶，也完成了項目從0到1的落地。第二個階段是更名波折階段，也是項目進入大眾視野前的關鍵節點，2026年1月，隨著項目熱度快速攀升，Anthropic公司以Clawdbot的名稱與旗下Claude大模型拼寫、讀音高度相似為由，提出了商標侵權的異議，為了規避法律風險，Peter Steinberger選擇配合更名，將項目短暫更名為Moltbot，「Molt」這個單詞的原意是龍蝦的蛻殼，既貼合項目的龍蝦IP形象，也寓意著項目在爭議中迭代重生，不過這次更名也出現了意外，在更換GitHub組織名稱和社交平臺賬號的過程中，僅10秒的空窗期，舊名稱Clawdbot就被自動化腳本搶注，還衍生出了相關的加密騙局，這也讓項目再次受

到了全球開發者社區的廣泛關注。第三個階段是正式定名與高速增長階段，2026年1月30日，項目正式定名為OpenClaw，其中「Open」明確了項目的開源定位，「Claw」則保留了項目的核心意象與IP符號，完成了項目名稱的最終確定，也讓龍蝦的IP形象徹底固定下來。第四個階段是社區化轉型階段，2026年2月，項目迎來了關鍵的發展轉折點，創始人Peter Steinberger宣佈加入OpenAI，同時項目轉為獨立基金會運營，徹底脫離了個人維護的模式，進入完全開源的社區化發展階段，全球開發者都可以自由貢獻代碼、優化功能，項目的迭代速度和生態完善度大幅提升，截至2026年3月，項目的GitHub星標數已經突破27萬，成為GitHub歷史上增長速度最快的開源項目之一，也正式從開發者社區走向大眾視野，引爆了全網的「養龍蝦」熱潮。

OpenClaw是完全免費的嗎？它採用什麼開源協議？個人商用和企業商用有沒有限制？

OpenClaw的軟件本身是完全免費、完全開源的，它採用的是國際上最寬鬆的MIT開源協議，這也是它能快速獲得全球開發者認可、迅速出圈的重要原因之一。MIT開源協議是目前開源領域對使用者限制最少的協議之一，用戶獲得OpenClaw的源代碼後，可以無限制地使用、複製、修改、合併、發佈、分發、再許可，甚至銷售軟件的副本，無論是個人用戶還是企業用戶，都不需要向官方支付任何版權費用，也沒有強制的開源回饋要求，只需要在軟件的副本和重要分發文件中，保留原始的版權聲明和許可聲明即可，這給了用戶極大的使用自由度，不管是個人二次修改定製，還是企業基於它開發商業化產品，都沒有原生的協議限制。需要特別說明的是，軟件本身免費，不代表使用過程中完全沒有成本，因為OpenClaw本身是一個AI智能體執行框架，不包含大語言模型，用戶需要接入外部大模型的API才能讓它正常運行，而絕大多數商用大模型的API調用是按Token消耗量計費的，這部分費用是支付給大模型廠商的，和OpenClaw本身無關，比如用戶接入GPT系列、Claude系列的商用API，就需要按照對應的費率支付Token費用，哪怕是待機狀態下的心跳機制，也會產生少量的Token消耗；當然，如果用戶接入的是完全免費的開源本地大模型，比如通過Ollama接入Llama、Mistral等開源模型，實現完全本地化運行，那麼就可以實現零成本使用，不會產生任何額外費用。關於商用權限，基於MIT開源協議的規則，OpenClaw對個人商用和企業商用都沒有原生的限制，個人用戶可以用它來承接商業項目、完成商業化的工作任

務，企業用戶可以把它集成到自己的商業化產品中、用於企業內部的自動化辦公系統開發，甚至基於它二次開發出專屬的商業化AI智能體產品，都不需要獲得官方的額外授權，也不需要支付版權費用。不過這裡有兩個重要的邊界需要明確，第一，MIT協議僅針對OpenClaw本身的源代碼，用戶基於它開發的商業化產品、使用過程中產生的所有法律責任、合規風險，都需要由使用者自行承擔，官方不承擔相關連帶責任；第二，用戶使用過程中接入的第三方大模型、插件、服務，需要遵守對應服務商的服務條款和商用限制，比如部分大模型的API禁止用於某些特定的商業化場景，這部分限制和OpenClaw本身無關，需要用戶自行確認和遵守。

OpenClaw是一款獨立的AI大模型，還是一個AI調度/執行框架？核心定位到底是什麼？

OpenClaw並不是一款獨立的AI大模型，它的本質是一個開源、本地優先的AI智能體調度與執行框架，是連接大語言模型「思考能力」與電腦系統「執行能力」的中樞橋樑，它的官方slogan「真正能幹活的AI」，也精準點明瞭它的核心定位。要理解這個定位，首先要明確AI大模型和AI執行框架的本質區別，AI大模型的核心是通過海量數據預訓練，獲得自然語言理解、邏輯推理、內容生成的能力，它就像人類的大腦，負責「思考」，解決「這件事該怎麼做」的問題；而OpenClaw本身不具備獨立的思考和內容生成能力，沒有經過預訓練的模型參數，也無法脫離外部大模型獨立運行，它的核心作用，是把大模型輸出的思考結果、邏輯步驟，轉化成電腦能執行的具體操作，就像人類的雙手和神經系統，負責「執行」，解決「把這件事落地完成」的問題。它採用的是BYOM（Bring Your Own Model）自帶模型的架構設計，預留了標準化的兼容接口，能適配市面上幾乎所有主流的大語言模型，包括海外的OpenAI GPT系列、Anthropic Claude系列，國內的DeepSeek、文心一言、通義千問等大模型，還能通過Ollama接入各類開源本地大模型，用戶可以根據自己的需求、預算和隱私要求，自由選擇接入的「大腦」，OpenClaw則負責統一調度這個「大腦」的能力，把抽象的自然語言指令，拆解成具體的、可執行的操作步驟，再調用對應的工具和系統權限完成執行。它的核心定位可以拆解為三個核心維度，第一個維度是「全流程任務執行中樞」，它打破了傳統對話式AI困在對話框裡的壁壘，實現了從「說」到「做」的跨

越，能直接獲得系統級權限，操控電腦完成文件管理、瀏覽器自動化、郵件處理、消息發送、代碼編寫、數據統計分析等各類跨應用的操作，實現從指令輸入到結果交付的全流程閉環，不需要人工介入中間環節，真正實現了「目標下達後，全流程自主完成」。第二個維度是「多智能體協同調度平臺」，它不僅能調度單一的大模型，還能實現多智能體分工協同，用戶可以根據不同的任務場景，設置多個分工明確的專屬AI智能體，比如專門負責內容創作的、專門負責數據處理的、專門負責客戶溝通的、專門負責項目統籌的，OpenClaw負責協調這些智能體的工作流程，讓它們協同完成複雜的團隊級任務，這也是網友口中「一個人加一隻龍蝦等於一支隊伍」的核心原因。第三個維度是「可定製的個人數字分身底座」，它支持本地優先部署，擁有持久化的長期記憶系統，能持續沉澱用戶的工作習慣、偏好、規則和專業知識，用戶還可以通過插件系統、自定義技能模塊，無限擴展它的能力邊界，把它打造成完全貼合自己需求的專屬數字分身，甚至能把自己的工作能力沉澱到框架裡，實現能力的複製和複用。正是這個清晰的定位，讓它和傳統的對話式AI、自動化腳本、AI插件有了本質區別，傳統自動化工具只能完成固定的、預設好的步驟，沒有自主思考和應急處理能力，而OpenClaw能借助大模型的推理能力，應對任務執行過程中的突發情況，自主調整執行步驟，最終完成用戶設定的目標，這也是它能掀起現象級熱潮的核心原因。

OpenClaw的爆火，對全球AI Agent行業意味著什麼？會不會真正開啟個人AI助理的全民時代？

OpenClaw的爆火，為全球AI Agent行業帶來了範式級的變革，徹底改寫了行業的發展邏輯與競爭格局，其意義遠超單一產品的走紅。在這之前，全球AI Agent行業始終處於「叫好不叫座」的尷尬境地，技術研發集中在大廠與專業開發者圈層，落地場景多侷限於企業級的封閉定製服務，普通用戶對AI Agent的認知幾乎為零，行業陷入了「唯模型論」的內卷，所有參與者都在比拼大模型的參數規模與推理能力，卻始終沒能解決「AI無法真正落地執行」的核心痛點。而OpenClaw的出現，首先完成了AI Agent的全民科普，用「養龍蝦」這個極具網感的具象化比喻，把原本抽象晦澀的AI智能體技術，直接推到了普通用戶面前，讓全球用戶第一次直觀感受到，AI不只是對話框裡的聊天工具，更是能直接上手操作電腦、完成全流程工作的執行主體，徹底打破了大眾與AI Agent之間的認知壁壘。其次，它以開源模式重構了行業的准入門檻，MIT開源協議讓全球開發者都能免費使用其核心框架，此前開發一款AI Agent需要從零搭建調度系統、記憶模塊、工具調用接口，需要投入鉅額的研發成本與技術團隊，而現在中小開發者、創業公司甚至個人愛好者，都能基於OpenClaw的底座快速完成二次開發，不用再重複造輪子，徹底打破了大廠對AI Agent技術的壟斷，讓行業從「寡頭主導的封閉研發」轉向「全球開發者共建的開源生態」，大幅加速了整個行業的技術迭代速度。更重要的是，它扭轉了行業的發展方向，把AI Agent的競爭焦點從「卷模型參數」拉回了「卷落地執行、卷場景適配、卷用戶價值」，讓整個行業意識

到，大模型的核心價值不在於能說得多好，而在於能把事做多好，推動全球AI行業從「對話式AI」向「執行式AI」的根本性跨越，為AI Agent行業找到了真正的商業化落地路徑。

而關於是否會真正開啟個人AI助理的全民時代，OpenClaw無疑推開了這扇時代的大門，但目前仍處於序幕階段，距離真正的全民普及還有關鍵的門檻需要跨越。它的核心價值，是讓普通用戶第一次擁有了獲得專屬個人AI助理的可能性，此前市面上的個人AI助理，要麼是Siri、小愛同學這類只能完成簡單語音指令的工具，無法實現跨應用的全流程執行，要麼是閉源收費、門檻極高的企業級產品，普通用戶根本無法觸及。而OpenClaw開源免費、支持本地部署、能兼容市面上幾乎所有主流大模型，用戶可以根據自己的需求、預算與隱私要求，自由定製專屬的AI助理，從日常的郵件處理、信息整理，到內容創作、工作流自動化，都能實現全流程自主完成，這是個人AI助理從「通用玩具」到「專屬生產力工具」的關鍵跨越，為全民時代打下了堅實的技術基礎。但我們必須清晰地看到，當前的OpenClaw還無法直接實現全民普及，核心原因在於它的使用門檻依然過高，對於沒有技術基礎的普通用戶來說，從安裝部署、環境配置、網關開啟，到API對接、權限調試、安全防護，每一個環節都存在不低的技術壁壘，這也是上門安裝服務能爆火的核心原因。更重要的是，OpenClaw的核心價值在於複雜任務流的處理與多智能體協同，而大多數普通用戶的日常需求，多是簡單瑣碎的事務，根本用不上如此複雜的功能，很容易陷入「為了用工具反向找需求」的誤區，再加上API調用的Token成本、持續運行的算力消耗、數據安全與隱私洩露的風險，都讓普通用戶的長期使用意願大打折扣。真正的個人AI助理全民時代，需要的是「開箱即用」的產品體驗，而不是需要用戶自己組裝調試的技術框架，就像早期的Linux系統只有極客玩家能駕馭，直到Windows推出可視化的圖形界面，才開啟了個人電腦的全民時代。目前全球開發者已經基於

OpenClaw開始研發可視化界面、一鍵安裝包、細分場景的定製化版本，隨著開源生態的不斷完善，這些產品會逐步抹平技術門檻，讓個人AI助理真正走進普通用戶的生活，而OpenClaw的爆火，正是這個全民時代的起點。

騰訊雲、阿里雲、火山引擎等國內雲廠商，為什麼紛紛下場快速適配、支持OpenClaw？背後的商業邏輯是什麼？

國內頭部雲廠商集體快速下場適配OpenClaw，本質上是一場精準的流量卡位、生態佈局與商業變現的順勢而為，其背後有著清晰且明確的商業邏輯，完全貼合雲廠商的核心生意模式與長期發展戰略。首先最核心的底層邏輯，是OpenClaw為雲廠商帶來了海量的新增剛需，直接撬動了其核心營收板塊的增長。雲廠商的核心生意，是售賣算力資源、大模型API調用服務、雲環境部署與相關配套服務，而OpenClaw本身不具備獨立的思考能力，它的每一次運行、每一個任務的執行，都必須依賴大模型API的調用，需要穩定的雲環境、專屬的網關服務與持續的算力支撐，它的全網爆火，直接憑空創造了一個規模極其龐大的新增需求市場。在OpenClaw走紅之前，國內大模型API的核心用戶以企業客戶、開發者為主，普通個人用戶幾乎不會主動開通API服務、租賃雲服務器，而「養龍蝦」的熱潮，讓海量的個人用戶、中小創業者、自媒體人、職場人，第一次主動接觸並開通了大模型API、購買了雲服務，成為了雲廠商的新增付費用戶。雲廠商通過快速適配OpenClaw，推出專屬的API通道、一鍵部署環境、新手算力補貼，本質上就是把這股爆發式的流量紅利，快速轉化為自己的付費用戶，直接拉動核心營收的增長，這是最直接、最現實的商業考量。

其次，這是雲廠商在AI下半場的生態卡位，是搶佔AI Agent時代市場主導權的關鍵佈局。此前AI行業的競爭焦點集中在大模型賽道，

國內雲廠商紛紛投入鉅額資源研發自有大模型，試圖在大模型時代佔據生態主導權，但隨著行業發展，市場已經清晰地認識到，大模型只是AI時代的「發動機」，而AI Agent才是連接發動機與用戶需求的「整車」，是大模型落地變現的核心載體，誰能掌控AI Agent的生態入口，誰就能在AI下半場佔據絕對的主動權。OpenClaw憑藉開源、輕量化、全模型兼容的優勢，已經快速成為全球AI Agent領域的事實性標準底座，形成了龐大的開發者生態與用戶基礎，如果雲廠商不及時適配，就會被這個核心生態排除在外，未來在AI Agent時代徹底失去話語權。而快速適配OpenClaw，不僅能讓雲廠商接入這個全球最大的AI Agent開源生態，更能把自己的大模型、算力服務、安全能力、存儲產品、辦公生態，深度集成到OpenClaw的核心框架中，讓用戶在使用OpenClaw時，優先選擇自家的雲服務與大模型，把OpenClaw的海量用戶，導流到自己的生態體系中，形成「OpenClaw底座+自有大模型+雲服務」的完整閉環，鞏固自己在AI時代的市場地位，這是關乎長期發展的戰略級佈局。

第三，這是雲廠商實現To C破圈、完善用戶生命週期佈局的絕佳機會。長期以來，國內雲廠商的核心客群集中在企業客戶，To C市場的滲透率極低，普通用戶幾乎不會直接接觸雲廠商的服務，雲廠商也很難低成本觸達C端用戶，完成用戶教育與市場培育。而OpenClaw的爆火，是從C端用戶率先發起的，海量的個人用戶有著強烈的使用需求，卻面臨著安裝難、配置難、調試難的痛點，雲廠商通過推出免費的一鍵部署工具、線下免費安裝服務、新手算力補貼，能以極低的成本，快速觸達海量的C端用戶，完成AI服務的用戶教育，讓普通用戶第一次熟悉並使用自家的雲服務。這些C端用戶中，潛藏著大量的未來企業客戶，比如當下用OpenClaw做內容創作的自媒體人，未來可能成長為MCN機構，當下用它做電商運營的個人賣家，未來可能成長為規模化的電商企業，這些用戶在個人階段習慣了某家雲廠商的服務，

未來創業時會優先選擇同一家廠商的企業級服務，雲廠商通過這次適配，完成了從C端到B端的用戶全生命週期佈局，用極低的獲客成本，鎖定了未來的企業級客戶增長空間。

最後，這也是雲廠商規避技術風險、建立差異化競爭優勢的必然選擇。OpenClaw採用的MIT開源協議，沒有任何商業使用限制，全球開發者都在基於它進行二次開發，生態的迭代速度遠超閉源產品，行業的技術標準正在快速形成，此時不跟進適配，就意味著被行業趨勢甩開，面臨被市場邊緣化的風險。同時，通過官方適配，雲廠商能解決用戶使用OpenClaw過程中的核心痛點，比如網絡網關、權限安全、數據備份、故障排查等，推出專屬的安全防護、合規審計、多端同步服務，建立自己的差異化競爭優勢。比如騰訊雲的快速適配，不僅是為了拉動雲服務的增長，更是因為騰訊擁有微信、企業微信、騰訊文檔、騰訊會議等國內最大的辦公與社交生態，OpenClaw的執行能力，能與這些生態實現深度打通，讓用戶通過OpenClaw直接操控企業微信、處理郵件、編輯文檔、發起會議，形成「辦公生態+AI執行框架」的絕對壁壘，這也是騰訊願意在大廈樓下開設免費安裝點，全力推動用戶教育的核心原因。

深圳火速推出「龍蝦十條」補貼政策，具體內容是什麼？對本地AI產業和OpenClaw的落地有什麼影響？這反映了哪些深層問題？

2026年3月，在OpenClaw全網爆火、騰訊線下免費安裝活動引發全城關注的背景下，為搶抓智能經濟發展機遇，深圳市龍崗區於3月7日發佈《深圳市龍崗區支持OpenClaw&OPC發展的若干措施（徵求意見稿）》，也就是俗稱的「龍蝦十條」，其中提出，鼓勵市場化、專業化平臺載體推出「龍蝦服務區」，免費提供OpenClaw部署服務，符合條件的給予一定補貼等。具體如下：

一、OpenClaw免費部署與開發支持

鼓勵市場化、專業化平臺載體推出「龍蝦服務區」，免費提供OpenClaw部署服務，符合條件的給予一定補貼；提供OpenClaw類智能體工具開發推廣支持。對向國際主流社區貢獻關鍵代碼、在技能交易平臺開發上架龍崗優勢產業相關技能包、開發與具身智能設備結合的應用項目的，經認定後給予最高200萬元補貼。

二、OpenClaw專屬數據服務支持

OpenClaw專屬數據服務支持。開放低空、交通、醫療、城市治理等高質量脫敏公共數據，減免公共數據使用費用；對購買數據治理、標註、數據資產入表等服務用於OpenClaw框架相關的開發、應用、研究的，按實際支付的費用給予50%優惠。對購買企業自主研發，開箱即用的AI NAS（龍蝦盒子）的，按市場價的30%給予補貼。

三、OpenClaw類智能體工具採購支持

實施「OpenClaw數字員工應用券」計劃，支持企業採購或自建OpenClaw智能體解決方案，按不超過項目總投入的40%給予補貼，單家企業年度最高200萬元。

四、OpenClaw類智能體工具應用示範支持

聚焦智能製造、智慧政務、智慧園區、智慧醫療等領域，每年遴選一批創新性強、應用效果好的OpenClaw深度應用項目，授予「龍崗區OpenClaw應用示範項目」稱號，並按實際投入30%給予一次性獎勵，最高100萬元。

五、AIGC模型調用支持

對符合一定條件的區內AIGC企業使用國內頭部多模態大模型進行AIGC創作生產的，按實際支付的模型調用費用30%給予補貼，每家企業每年累計補貼總額最高不超過人民幣100萬元。

六、算力與場景應用支持

協調智能算力資源，為經認定的OPC社區新入駐企業提供為期三個月的免費算力資源（包括但不限於通用算力、智能算力等）及相關基礎技術支持服務。按照技術創新、市場推廣、應用成效、發展潛力等維度，每年遴選具有行業引領的示範場景項目，最高按照項目（非政府投資項目）實際投入的50%，給予最高不超過400萬元支持。

七、人才與創業空間支持

吸引青年人才落戶，對新引進落戶龍崗的博士、碩士、本科人才，分檔給予最高10萬元入戶補貼。為新註冊或新遷入龍崗的OPC企業提供最長2個月免費住宿，降低人才落地成本。對獲得「龍崗區OPC

年度人物」評定的優秀OPC創辦人或核心人才，按規定給予醫療保障、子女入學、人才住房等相應待遇。落實「一張辦公桌、一間辦公室、一層辦公樓」的樂業辦公體系，為OPC企業提供最長18個月辦公空間優惠期，降低初創團隊落地門檻。支持社會力量參與OPC社區建設，對經認定的OPC社區，按年度給予運營機構最高400萬元支持。

八、基金融資支持

用好區科技創新「種子基金」、龍崗雲圖產業基金及人工智能產業母基金，為科技含量高、創新能力強的種子期OPC項目（重點傾斜青年人才創業項目）提供投融資渠道，符合條件的給予最高1000萬元股權投資支持。

九、產品出海支持

依託區企業國際化服務基地，設立OPC「出海服務站」，集成市場拓展、跨境物流、合規諮詢等一站式服務，構建從需求感知到產品交付的敏捷閉環。對出海型OPC投保出口信用保險符合條件的，給予一定比例保費支持。

十、賽事獎勵支持

對在龍崗區主辦的「OPC黑客松」、創新創業大賽等活動中獲獎的OPC團隊，給予最高50萬元獎勵支持；對在「龍崗區OPC年度人物評選」活動中獲獎的個人，給予最高10萬元獎勵支持。同一主體按就高不重複原則享受支持。

政策從研發創新、企業孵化、算力支撐、場景落地、人才引育、生態建設等十個維度，給出了全鏈條的精準扶持，成為全國首個地方政府針對AI Agent細分賽道推出的專項政策。「龍蝦十條」的推出，對深圳本地AI產業發展與OpenClaw的落地普及，帶來了全方位的深遠

影響。最直接的影響，是大幅加速了OpenClaw在深圳的落地與普及，政策從個人開發者到企業用戶的全鏈條補貼，直接降低了用戶的使用門檻與企業的研發成本，配合騰訊等本地企業的線下推廣活動，讓深圳快速成為全國OpenClaw用戶最集中、生態最完善的城市，完成了AI Agent技術的全民普及與用戶教育。其次，它直接推動了深圳本地AI產業的轉型升級與補鏈強鏈，此前深圳的AI產業佈局，更多集中在大模型研發、計算機視覺、智能硬件等領域，在AI智能體執行層的佈局相對薄弱，而「龍蝦十條」的推出，吸引了全國大量的AI智能體創業團隊、核心開發者入駐深圳，快速補齊了產業短板，形成了從算力基礎設施、大模型研發，到AI智能體框架、場景應用、安全服務的全產業鏈佈局，進一步鞏固了深圳在全國AI產業的龍頭地位。同時，政策推動了OpenClaw從C端的嚐鮮式使用，向To B的規模化、商業化落地跨越，此前OpenClaw的熱度更多集中在個人用戶的娛樂化、嚐鮮式使用，真實的商業化落地場景相對有限，而政策通過開放政務服務、工業製造、金融服務等官方與產業場景，為OpenClaw提供了真實的落地試驗田，推動技術與實體經濟的深度融合，真正把AI智能體技術轉化為產業升級的核心動力，也讓深圳成為了全國AI Agent商業化落地的標杆城市。除此之外，深圳的政策也起到了極強的示範效應，全國多個城市隨後陸續跟進推出相關扶持政策，推動了整個AI Agent行業的規範化、規模化發展，同時也讓OpenClaw這個民間爆火的開源項目，得到了官方層面的認可與支持，加速了它在國內的合規化、本土化發展進程。

這一政策的火速推出，也折射出了多個產業與政策層面的深層問題。首先，它反映出全國地方政府對AI產業的競爭，已經從「大模型賽道」全面轉向了「AI Agent落地賽道」。此前幾年，全國各地都在爭搶大模型項目，紛紛推出高額補貼扶持大模型企業，陷入了「重研發、輕落地」的內卷，而隨著大模型技術逐步成熟，市場已經清晰地

認識到，AI產業的下半場，核心競爭不再是模型參數的高低，而是落地應用的能力，AI Agent作為大模型連接實體經濟與用戶需求的核心載體，已經成為新的產業競爭風口，深圳率先推出專項政策，本質上是在AI Agent時代搶佔產業先機，鞏固自身的科創高地地位，也標誌著國內AI產業的競爭，正式從「模型研發」進入了「落地應用」的新階段。其次，它反映出國內AI產業發展的核心痛點，是「技術與落地的嚴重脫節」。此前國內已經湧現出上百個大模型產品，但絕大多數都沒有找到真實的落地場景，大量的算力投入與研發成本，沒有轉化為真實的生產力，普通用戶與中小企業很難享受到AI技術帶來的紅利，而OpenClaw的爆火，恰恰證明了市場真正需要的，不是參數更高、能力更強的大模型，而是能真正解決實際問題、降低工作成本、提升生產效率的落地工具，地方政府的政策導向，也正是在引導AI產業迴歸「技術服務實體經濟」的本質，擺脫「唯參數論」的無效內卷，聚焦於真實的場景落地與用戶價值。第三，它反映出開源生態已經成為AI時代產業發展的核心驅動力。此前國內AI產業的發展，更多是由大廠主導的閉源模式推動，技術壁壘高、中小開發者參與難度大，而OpenClaw作為一個開源項目，能在短短幾個月內引爆全網，形成龐大的用戶與開發者生態，證明了開源模式是推動AI技術快速普及、快速迭代的核心路徑，深圳的專項政策，也是國內地方政府首次針對單一開源項目推出全鏈條扶持，標誌著官方層面對開源生態的重視程度提升到了新的高度，未來扶持開源生態、打破技術壟斷、激發中小開發者活力，會成為國內AI產業發展的核心方向。最後，它也反映出地方政府對新興技術的響應速度與治理理念的全面升級，從OpenClaw全網爆火到專項政策推出，只用了不到一個月的時間，打破了以往政策滯後於產業發展的固有模式，說明地方政府已經充分認識到，AI技術的迭代速度遠超傳統產業，只有快速響應、精準扶持、包容審慎，才能抓住技術變革的產業窗口，同時政策沒有設置過多的准

入門檻與限制條款，而是以扶持、引導、培育為主，也體現了地方政府對新興技術的包容態度，為AI技術的創新發展提供了良好的政策環境。

OpenClaw的爆火，帶動了哪些相關產業鏈？普通人有哪些可落地的創業、副業機會？

OpenClaw的全網爆火，不僅引爆了AI Agent行業，更帶動了一條覆蓋上游、中游、下游的完整產業鏈快速崛起，形成了全新的產業風口。在產業鏈上游，最直接受益的是算力基礎設施與大模型API服務產業，OpenClaw本身不具備獨立的大語言模型，所有的任務執行都需要依賴大模型API的調用，其爆火直接帶來了海量的API調用需求，不管是海外的OpenAI、Anthropic，還是國內的DeepSeek、文心一言、通義千問等大模型廠商，API調用量都出現了爆發式的增長，而作為API服務載體的雲廠商、算力中心，也迎來了雲服務器租賃、專屬網關服務、雲環境部署需求的大幅上漲，同時，很多用戶為了降低Token成本，選擇本地部署開源大模型搭配OpenClaw使用，直接帶動了高性能顯卡、AI服務器、本地存儲設備等硬件產品的銷量增長，整個上游的算力與大模型產業，都迎來了全新的增長曲線。在產業鏈中游，核心受益的是OpenClaw生態開發與技術服務產業，這也是整個產業鏈的核心增長極，首先是最基礎的安裝部署服務，從淘寶、閒魚上300元到1000元不等的遠程、上門安裝服務，到針對中小企業的批量部署、環境配置服務，已經形成了成熟的服務鏈條，甚至有從業者短短幾天就靠這項服務收入數十萬，除此之外，配套的故障排查、權限調試、API對接、日常運維等技術服務，也成為了全新的服務品類，解決了普通用戶的核心使用痛點。同時，基於OpenClaw的二次開發與插件開發產業快速崛起，OpenClaw的開源架構支持無限的插件擴展，針對不同行業、不同場景的定製化插件，成為了開發者的核心創業方向，比如針

對自媒體的內容創作與自動發佈插件、針對電商的運營與客服插件、針對職場人的辦公自動化插件、針對金融人的投研分析插件，還有降低使用門檻的可視化界面、一鍵安裝包、多端適配工具等二次開發項目，都迎來了爆發式的需求，形成了完整的開發生態。在產業鏈下游，場景落地與商業化服務產業全面開花，首先是知識付費與教育培訓賽道，全網關於OpenClaw的保姆級教程、進階調教課程、細分場景實戰課，在抖音、小紅書、B站、各大知識付費平臺全面爆發，從9.9元的入門資料包，到上千元的企業級實戰訓練營，形成了完整的知識付費鏈條，甚至出現了一對一陪跑、定製化調教的諮詢服務，成為了門檻最低、變現最快的賽道。其次是企業級定製化解決方案服務，針對中小企業的AI智能體部署、團隊協同系統搭建、全流程自動化辦公定製，成為了AI創業公司的核心新業務，比如給電商公司搭建全流程運營自動化系統、給新媒體公司搭建內容生產與分發體系、給財稅公司搭建自動化賬務處理系統，都實現了快速的商業化落地。同時，配套的安全與合規服務產業也快速崛起，由於OpenClaw擁有系統級操作權限，用戶對隱私保護、安全防護、漏洞檢測、數據備份、合規審計的需求快速增長，針對個人用戶的安全防護工具、針對企業用戶的合規解決方案，都成為了全新的產業風口。除此之外，它還帶動了內容創作、MCN、自媒體等相關產業的發展，全網關於「養龍蝦」的教程、測評、案例分享內容，都能獲得極高的流量與關注度，很多自媒體靠著這個話題快速漲粉，帶動了直播、廣告、帶貨等相關業務的發展，形成了完整的內容生態產業鏈。

對於普通人來說，這股熱潮也帶來了大量可落地、低門檻的創業與副業機會，不同能力、不同資源的人，都能找到適合自己的入局方向。對於沒有任何技術背景的普通人，最容易落地、已經被市場驗證的機會，就是安裝部署與配套技術服務，這項業務不需要複雜的編程能力，只需要花時間把OpenClaw的安裝流程、環境配置、常見故障排

查、API對接的步驟學透，就能通過遠程安裝、上門安裝的方式提供服務，核心客群是有使用需求但沒有技術能力的職場人、自媒體人、中小商家、中小企業主，哪怕一單收費300到500元，只要通過小紅書、抖音、閒魚等平臺獲取精準流量，就能快速獲得穩定的收入，還可以配套提供API代註冊、Token充值、日常故障排查、基礎操作教學等增值服務，提升客單價，甚至可以針對本地的中小企業，提供批量部署與線下基礎培訓服務，拓展更高價值的企業級客戶。同時，零門檻的內容創作與知識付費，也是普通人絕佳的入局機會，你可以把自己學習、使用、調教OpenClaw的全過程，整理成教程、筆記、實戰案例，在小紅書、抖音、B站等平臺發佈，吸引對這個話題感興趣的精準粉絲，然後通過售賣入門教程、進階資料包、一對一諮詢的方式變現，哪怕是9.9元的低價資料包，只要流量足夠，就能實現規模化的收入，還可以通過直播的方式，現場演示安裝與調教過程，解答用戶的疑問，通過直播打賞、廣告、帶貨實現變現。對於有特定行業經驗的人，比如職場人、電商運營、自媒體人、財稅從業者，可以聚焦自己的垂直行業，製作細分場景的實戰教程與解決方案，比如「電商運營如何用龍蝦實現全流程自動化」「職場人如何用龍蝦搞定週報、方案與郵件」，這類垂直內容的粉絲精準度更高，變現能力也更強，很容易形成自己的差異化競爭力。

對於有一定基礎、但沒有核心研發能力的普通人，可以入局細分場景的定製化模板與調教服務，這項業務不需要複雜的代碼開發，只需要把OpenClaw的調教流程、指令規則、工作流標準化，就能打包成可售賣的產品。比如針對自媒體人，製作好一套完整的熱點追蹤、選題策劃、內容撰寫、排版發佈的標準化調教模板，用戶只需要導入自己的賬號與風格偏好，就能直接使用；針對電商賣家，製作好客服自動回覆、訂單處理、競品分析、數據統計的標準化工作流模板；針對HR、行政、財稅等職場崗位，製作對應的自動化辦公模板，這些模板

可以直接打包售賣，也可以提供一對一的定製化調教服務，根據用戶的具體需求，定製專屬的工作流與執行規則，收取定製服務費，這種模式門檻不高，但客單價與復購率都很可觀，是非常容易落地的輕創業方向。

對於有編程能力、技術背景的開發者，可選擇的創業機會則更加廣闊，最直接的就是插件開發，基於OpenClaw的開源架構，開發針對不同場景、不同平臺的插件，比如對接國內主流辦公軟件、電商平臺、社交軟件的適配插件，提升OpenClaw的本土化適配能力，插件可以採用免費+付費增值的模式，也可以通過一次性售賣、訂閱制實現變現，只要能解決用戶的真實痛點，很容易獲得用戶與收入。同時，還可以開發降低用戶門檻的工具類產品，比如可視化操作界面、一鍵安裝包、手機端適配工具、自動化調教工具等，這類產品是海量普通用戶的剛需，市場空間極大。除此之外，還可以基於OpenClaw開發細分行業的SaaS產品，比如針對中小企業的自動化辦公SaaS、針對自媒體的內容生產SaaS、針對跨境電商的運營SaaS，把OpenClaw的核心能力封裝成開箱即用的產品，採用訂閱制收費，這是具備長期發展空間的創業方向。而針對用戶普遍擔憂的安全問題，開發數據備份、漏洞檢測、權限管控、合規審計的安全防護工具，也是極其剛需的創業賽道，能快速形成自己的核心競爭力。

需要注意的是，不管選擇哪種創業或副業方向，都要避開「為了工具找需求」的偽需求誤區，核心要圍繞用戶的真實痛點提供服務，同時要嚴格遵守OpenClaw的MIT開源協議，規避知識產權、數據隱私、合規經營相關的風險，才能在這股熱潮中，找到長期穩定的發展機會。

券商、金融投研圈為什麼集體關注OpenClaw？它在金融、投研場景有哪些核心落地可能？

券商、金融投研圈會集體關注OpenClaw，核心原因在於這款產品精準擊中了金融投研行業的核心痛點，帶來了行業效率提升的顛覆性可能，而這個行業本身，又是對效率、數據、時效性敏感度最高，同時AI工具滲透率也最高的行業之一。對於傳統的投研分析師、基金經理、資管從業者來說，日常工作中超過60%的時間，都被消耗在了數據蒐集、整理清洗、公告解讀、新聞跟蹤、紀要整理、報表製作等重複性、流程性的事務中，真正能用於深度研究、價值判斷、投資決策的核心時間被嚴重擠壓，而此前的對話式AI工具，最多隻能輔助完成紀要整理、公告解讀、初稿生成等碎片化工作，無法實現跨平臺的數據抓取、多維度分析、全流程執行，最終的落地環節依然需要人工手動完成，無法形成真正的效率閉環。而OpenClaw的核心能力，恰恰是全流程自主執行、跨應用聯動、長期記憶管理、多智能體協同，能徹底把投研人員從重複性的事務中解放出來，讓他們把精力集中在最核心的價值判斷上，這是整個行業集體關注它的根本原因。

除此之外，還有幾個關鍵因素，讓OpenClaw成為了金融投研圈的焦點。首先，金融投研行業的付費能力極強，對於能真正提升投研效率、降低人力成本、甚至創造超額收益的工具，機構願意支付極高的成本，此前很多頭部券商、資管機構已經投入了鉅額資金，研發自己的AI投研系統，但這些系統大多停留在對話式、輔助式的階段，無法實現全流程的自動化執行，而OpenClaw的開源架構，能讓機構以極低的成本，快速搭建屬於自己的AI投研智能體系統，不用從零開始研

發，大幅降低了研發成本與時間週期，這對於機構來說有著極強的吸引力。其次，金融市場的核心競爭力，就是信息差與效率差，誰能更快地處理海量的市場信息、更快地完成數據分析、更快地輸出投研成果，誰就能在市場中佔據先機，而OpenClaw能實現7×24小時全天候運行，即時監控市場動態、上市公司公告、宏觀政策、行業新聞，第一時間完成分析與預警，這種響應速度與執行效率，是人工完全無法比擬的，甚至能實現從數據監控、分析、研報生成到交易執行的全流程閉環，這種顛覆性的效率提升，是任何投研機構都無法忽視的。更重要的是，OpenClaw支持本地私有化部署，所有的投研數據、策略邏輯、分析模型，都能運行在機構自己的服務器上，完全掌控數據隱私與安全，徹底解決了此前閉源商業AI產品的核心痛點——機構的核心投研策略、保密數據需要上傳到第三方平臺，存在極高的洩密風險，這也是它能被主流金融機構認可的關鍵前提。同時，金融投研圈本身對AI技術的接受度與學習能力極強，從ChatGPT爆火開始，整個行業就已經在大規模應用AI工具，形成了成熟的AI使用習慣，對於能真正帶來效率突破的新技術，有著天然的敏感度，自然會第一時間跟進研究與落地。

OpenClaw在金融、投研場景的落地可能，覆蓋了從基礎輔助到高階交易的全鏈條，幾乎能滲透到金融行業的每一個核心環節，其中多個場景已經具備了快速落地的條件。最基礎、也最容易落地的，是投研全流程的自動化輔助工作，這也是目前機構已經在嘗試落地的場景。OpenClaw能實現7×24小時全天候的市場信息監控與處理，即時跟蹤滬深交易所、港交所、美股等市場的上市公司公告、宏觀經濟數據、行業政策、新聞資訊、券商研報、機構調研紀要，自動完成數據的抓取、清洗、整理、分類，根據預設的研究框架，自動提取核心信息，生成標準化的信息簡報，讓分析師每天打開電腦，就能看到經過整理的全市場核心動態，不用再花費大量時間瀏覽海量信息。針對重

點跟蹤的上市公司，它能自動完成業績預告、定期財報的解讀，對比歷史財務數據、行業均值、機構預期，提煉出核心的超預期或低於預期的關鍵信息，生成完整的財報解讀報告，甚至能自動完成產業鏈上下游的聯動分析，找出業績變化的核心驅動因素。除此之外，它還能自動完成投研工作中的各類文檔工作，根據整理好的數據與研究邏輯，自動生成研報初稿、調研會議紀要、路演PPT、定期的行業週報與月報，還能根據機構的格式要求，自動完成排版、數據可視化、引用標註，大幅降低投研人員的文檔工作負擔，讓他們把精力集中在深度研究上。

在進階的數據分析與量化研究場景，OpenClaw的能力更是帶來了顛覆性的改變。它能跨平臺對接Wind、同花順iFinD、Choice、聚寬、米筐等主流金融數據庫與量化平臺，自動完成數據的調取、清洗、回測與分析，比如分析師想要研究某個行業的景氣度變化，只需要下達最終的研究目標，OpenClaw就能自動從數據庫中調取行業的上下游供需數據、上市公司的財務數據、產銷數據、產品價格數據，自動完成數據的清洗與整理，搭建對應的分析模型，生成景氣度跟蹤圖表與行業內上市公司的對比分析報告，整個過程不需要人工干預，完全自主完成。對於量化機構來說，OpenClaw能實現量化策略從思路到落地的全流程自動化，它能根據投研人員的策略思路，自動編寫量化策略代碼，對接量化平臺完成歷史回測，根據回測結果自動優化策略參數，甚至能實現策略的即時監控、風險預警、自動調倉，整個過程完全閉環。更重要的是，它能實現多智能體協同運行，讓不同的AI智能體分別負責策略研發、回測優化、風險控制、交易執行，形成一個完整的量化交易團隊，大幅縮短量化策略的研發週期，降低量化投資的技術門檻，讓更多的投研人員能參與到量化策略的研發中。

在機構的中後臺運營與合規風控場景，OpenClaw也有著極其廣闊的落地空間，這也是金融機構的核心痛點領域。金融機構的中後臺，有著大量流程固定、規則明確、對準確率要求極高的事務性工作，比如交易清算、基金估值核算、信息披露、合規審計、報表報送、客戶服務等，這些工作極其繁瑣，人工操作不僅效率低，還容易出現差錯，而一旦出現差錯，就可能面臨監管處罰。OpenClaw能根據監管要求與機構的內部規則，自動完成這些全流程的工作，比如自動完成基金產品的每日淨值核算、定期的信息披露報告生成與監管報送，自動監控交易過程中的合規風險，對超限交易、內幕交易、關聯交易進行即時預警，自動完成合規審計的資料整理與工作底稿生成，甚至能自動處理客戶的常規諮詢、產品申贖請求、信息核對等客服工作，不僅能大幅降低機構的中後臺人力成本，還能提升運營效率與合規準確率，避免人工操作帶來的差錯，這對於強監管的金融行業來說，有著極高的應用價值。

在高階的財富管理與機構服務場景，OpenClaw也能實現全流程的效率升級。對於券商的財富管理部門、私人銀行、基金銷售機構來說，它能實現客戶服務的個性化與自動化，針對高淨值客戶，自動跟蹤客戶的持倉情況、市場變化、產品淨值波動，定期生成個性化的資產配置報告與持倉調整建議，自動完成客戶的風險測評、產品適配、合規告知，還能根據客戶的風險偏好與收益目標，自動篩選符合要求的金融產品，生成產品對比分析報告，讓理財經理從繁瑣的日常事務中解放出來，專注於深度的客戶關係維護與資產配置規劃。對於券商的機構業務部門，它能自動完成機構客戶的路演對接、需求跟蹤、服務反饋、定製化研報推送，大幅提升機構服務的響應速度與服務效率，鞏固機構客戶關係。

需要注意的是，OpenClaw在金融場景的落地，依然面臨著合規、風險控制等方面的限制，金融行業是強監管行業，所有的操作都必須符合監管要求，尤其是涉及到交易執行、客戶信息處理、信息披露的環節，需要嚴格的權限管控與合規審計，而AI自主執行帶來的不可控性，比如誤操作、指令遺忘、漏洞攻擊等問題，在金融場景中可能會帶來巨大的損失，因此目前它的落地更多集中在輔助性、非交易性的環節，真正的全自動交易落地，還需要完善的風險管控、合規審計與技術優化。但不可否認的是，它已經給整個金融投研行業帶來了顛覆性的變革預期，這也是整個行業集體關注它的核心原因。

OpenClaw的開源模式，會不會重構AI個人助理的市場格局？對閉源的商業AI助理產品帶來哪些衝擊？

OpenClaw的開源模式，必然會從底層邏輯上徹底重構全球AI個人助理的市場格局，推動整個行業從「大廠寡頭壟斷的閉源時代」，進入「開源生態主導的多元化時代」，其帶來的變革，堪比當年安卓開源系統對智能手機市場格局的重構。在OpenClaw爆火之前，全球AI個人助理市場的格局高度固化，完全由閉源的商業產品主導，形成了清晰的寡頭壟斷格局，海外市場由OpenAI的GPTs、微軟的Copilot、Google的Gemini Advanced主導，國內市場則由百度文心一言、阿里通義千問、字節豆包等大廠的閉源智能體產品佔據核心份額，還有一些垂直領域的閉源商業產品，也只能在細分賽道分一杯羹，無法撼動大廠的主導地位。這些閉源產品有著統一的特徵：採用閉環的生態模式，核心技術與架構完全不對外開放，用戶只能在廠商設定的框架內使用，無法進行深度的二次開發，無法實現本地私有化部署，所有的用戶數據都存儲在廠商的服務器上，用戶本質上只是產品的使用者，而非所有者。在這種格局下，賽道的准入門檻極高，想要開發一款AI個人助理產品，需要投入鉅額的研發成本，搭建核心的調度框架、記憶系統、工具調用接口，只有頭部大廠才有能力參與競爭，中小開發者與創業公司幾乎沒有入局的機會，市場陷入了「唯模型論」的內卷，所有廠商都在比拼大模型的參數規模與推理能力，卻忽略了用戶的真實需求與場景適配。

而OpenClaw的開源模式，從三個核心維度徹底打破了這種固化的市場格局。首先，它徹底打破了大廠的技術壟斷，大幅降低了賽道的

准入門檻，MIT開源協議讓全球所有開發者、創業公司、甚至個人愛好者，都能免費使用其核心的AI智能體框架，不用再從零開始重複造輪子，只需要基於這個成熟的底座，針對細分場景做二次開發、優化交互界面、添加專屬功能，就能快速打造出一款屬於自己的AI個人助理產品。這就意味著，未來的AI個人助理市場，不再是隻有大廠才能參與的遊戲，萬千中小開發者都能入局，市場會從「寡頭壟斷」轉向「去中心化的開源生態主導」，出現海量的、針對不同細分場景、不同用戶群體的AI個人助理產品，形成百花齊放的市場格局。其次，它徹底扭轉了市場的競爭邏輯，把行業的競爭焦點從「卷大模型能力」，轉向了「卷場景落地、卷用戶體驗、卷定製化服務」。OpenClaw採用全模型兼容的架構，能對接市面上幾乎所有的主流大模型，用戶可以根據自己的需求、預算、隱私要求，自由選擇接入的大模型，大模型不再是AI個人助理產品的核心壁壘，能不能真正解決用戶的具體需求、能不能適配用戶的細分場景、能不能給用戶提供更安全、更個性化的使用體驗，才是核心的競爭力。這就打破了大廠在大模型上的技術優勢，給中小開發者與創業公司提供了彎道超車的機會，哪怕沒有自己的大模型，只要能把細分場景的需求摸透，做出極致的用戶體驗，就能在市場中佔據一席之地，徹底改變了市場的競爭規則。第三，它徹底改變了用戶與AI個人助理之間的關係，讓用戶從「被動的使用者」，變成了「主動的所有者、共建者」。閉源的商業產品，用戶無法掌控自己的數據，無法進行深度的定製化，更無法參與產品的迭代優化，而OpenClaw的開源模式，讓用戶可以自由修改代碼、定製功能、實現本地部署，完全掌控自己的數據隱私與AI助理的所有權限，甚至可以把自己調教好的AI助理、開發的插件，分享給開源社區的其他用戶，參與整個生態的共建。這種所有權的改變，會徹底扭轉用戶的選擇偏好，越來越多的用戶會選擇開源的、可自主掌控

的AI個人助理，而不是閉源的、數據不受自己掌控的商業產品，從需求端推動市場格局的重構，讓開源產品逐步成為市場的主流。

對於閉源的商業AI助理產品來說，OpenClaw的開源模式帶來了全方位、多層次的衝擊，甚至會直接改寫整個行業的商業模式與生存邏輯。最直接的衝擊，是對中低端、通用型閉源商業AI助理產品的降維打擊，這類產品的核心功能，就是基礎的對話交互、簡單的工具調用、碎片化的任務執行，沒有不可替代的核心壁壘，而OpenClaw本身完全免費，功能比這類產品更強大，定製化程度更高，還能實現本地部署，完全掌控數據隱私，對於有一定學習能力的用戶來說，完全可以用OpenClaw替代這些中低端的閉源產品，這會直接擠壓這類產品的生存空間，大量沒有核心競爭力的中小閉源產品，會被快速崛起的開源生態淘汰，甚至直接退出市場。

其次，是對頭部大廠的旗艦閉源產品，帶來了用戶流失、商業模式與生態壁壘的多重衝擊。在用戶層面，對技術敏感的極客用戶、開發者用戶、對隱私安全要求極高的企業用戶，會大量轉向開源的OpenClaw生態，這部分用戶是閉源產品的核心高價值用戶，他們的流失，不僅會直接影響閉源產品的營收，更會導致閉源產品的生態活力下降，因為開發者是生態的核心，開發者的流失，會讓閉源產品的插件生態、場景適配能力逐步落後於開源生態。在商業模式層面，此前絕大多數閉源商業AI助理產品，都採用訂閱制的收費模式，通過每月幾十到上百元的會員費實現盈利，而OpenClaw本身完全免費，用戶只需要支付大模型API的調用費用，這會讓用戶開始質疑閉源產品訂閱費的合理性，倒逼閉源產品降低定價、開放更多的免費功能，甚至放棄訂閱制的核心商業模式，整個行業的盈利邏輯會被徹底改寫。在生態壁壘層面，此前大廠的閉源產品，都在打造自己的閉環生態，比如微軟的Copilot深度綁定Office與Windows生態，OpenAI的GPTs綁定自己

的大模型生態，試圖通過生態綁定鎖定用戶，而OpenClaw的開源生態，是跨平臺、跨模型、跨生態的開放體系，能兼容所有的大模型、所有的辦公軟件、所有的應用場景，這會直接打破大廠的閉環生態壁壘，用戶不再需要為了使用AI助理，綁定某一個大廠的生態體系，大廠積累多年的生態優勢會被大幅削弱。

但需要明確的是，OpenClaw的開源模式，不會完全取代閉源的商業AI助理產品，二者最終會形成互補的市場格局，閉源產品依然有著不可替代的核心優勢。對於沒有技術基礎的普通用戶、大型企業客戶來說，開箱即用的閉源商業產品，依然有著不可替代的優勢，OpenClaw雖然功能強大，但需要用戶自己完成安裝部署、環境配置、調教優化，有著不低的使用門檻，而閉源產品能提供一鍵啟用、全流程服務、穩定的技術支持、完善的售後保障，更適合普通用戶使用。同時，大廠的閉源產品，能實現與自有生態的深度綁定，比如微軟的Copilot能與Office、Windows系統實現無縫銜接，帶來極致的一體化體驗，這是開源的OpenClaw無法比擬的。更重要的是，在金融、政務等強監管行業，閉源商業產品能提供完整的合規審計、數據安全保障、企業級服務體系，能滿足行業的合規要求，這也是開源產品短期內無法替代的。

面對開源生態的衝擊，頭部大廠也不會被動等待，而是會主動擁抱變化，要麼推出自己的開源AI智能體框架，加入開源生態的競爭，要麼快速適配OpenClaw的開源生態，把自己的大模型、雲服務、生態能力接入開源體系，把衝擊轉化為新的發展機會，國內騰訊雲、阿里雲等廠商快速適配OpenClaw，就是最好的例證。最終，整個AI個人助理市場會形成全新的格局：開源生態主導底層框架與多元化的場景創新，閉源產品提供開箱即用的標準化服務與企業級解決方案，二者相

互補充、共同發展，市場從寡頭壟斷的封閉時代，進入百花齊放的開源新時代，而OpenClaw的爆火，正是這個新時代的開端。

OpenClaw到底能做什麼？核心功能有哪些？普通人、職場人、程序員、學生群體分別能用它幹什麼？

OpenClaw的核心價值，是打破了傳統對話式AI「只說不做」的壁壘，將大語言模型的邏輯思考、規劃能力，直接轉化為電腦系統級的全流程執行操作，本質是一個能跨應用、跨平臺、全閉環完成任務的AI智能體執行框架，所有功能都圍繞「讓AI真正落地幹活」這個核心展開。它的核心功能可以分為六大核心模塊，首先是跨應用全流程任務執行，這也是它最核心的能力，它能獲得電腦的系統級操作權限，跳出單一的對話窗口，自由操控瀏覽器、辦公軟件、郵箱、社交工具、設計軟件等幾乎所有電腦上的應用，不用人工干預，就能完成從指令輸入到結果交付的完整任務流，而不是像傳統AI那樣只給出解決方案。其次是持久化長期記憶功能，它能完整保存用戶的工作習慣、內容風格、操作規則、過往任務的反饋與標準，不會因為關閉窗口、重啟服務就遺忘相關信息，越用越貼合用戶的使用需求，甚至能把一次學會的操作規則，長期沉澱為固定的執行標準。第三是多智能體協同調度，用戶可以根據需求，設置多個分工明確的專屬AI智能體，比如專門負責內容創作的、專門負責數據處理的、專門負責客戶對接的、專門負責統籌規劃的，OpenClaw能協調這些智能體各司其職、協同工作，模擬完整的團隊工作流，實現單人管理一支AI執行團隊的效果。第四是可無限擴展的插件與技能庫，它支持全球開發者貢獻的各類插件，能對接不同的平臺、軟件與功能，用戶可以根據自己的需求安裝對應插件，無限擴展它的能力邊界，還能把固定的工作流程固化為自定義技能，一鍵調用就能完成整套操作。第五是7×24小時自動化

值守，它自帶心跳喚醒機制，能按照用戶設定的間隔定時喚醒，自動檢查郵箱、日曆、消息通知、任務進度，無需用戶即時盯守，就能全天候執行預設的自動化任務，哪怕用戶在休息、出差，它也能持續工作。第六是能力沉澱與複製，用戶教它一次處理事務的完整流程，它不僅能完全掌握，還能整理成標準化的工作手冊，不僅自己能反覆使用，還能同步給其他同類型的AI智能體，實現個人能力的快速複製與複用。

針對不同的群體，OpenClaw能落地的場景有著明確的區分，能精準匹配不同人群的核心需求。對於普通大眾來說，它能解決日常生活中各類繁瑣、重複性的事務，不用再自己花時間處理瑣碎的事情，比如根據用戶的預算、出行時間、偏好，自主完成旅行攻略的全流程製作，包括查機票、訂酒店、規劃行程、整理當地美食與注意事項，甚至能直接完成預訂操作；能自動整理每月的銀行卡、支付軟件賬單，分類統計收支情況，生成可視化的消費分析報告，給出合理的省錢建議；能根據用戶的飲食偏好、健身目標，自動制定每週的健身計劃與食譜，定時提醒執行；還能自動篩選、整理用戶關注的行業新聞、興趣內容，生成每日簡報，不用自己刷遍各個平臺找信息，甚至能幫用戶處理各類預約、消息回覆、郵件整理等日常瑣事，把用戶從瑣碎的生活事務中解放出來。

對於職場人來說，OpenClaw是能全方位提升工作效率的專屬執行團隊，幾乎能覆蓋全崗位的日常工作場景，不管是行政、運營、市場、財務、銷售，還是管理層，都能找到對應的落地場景。對於普通職場人，它能自動完成日常的郵件處理，篩選重要郵件、分類整理、生成回覆初稿，經過確認後直接發送；能根據用戶的工作內容，自動整理每週、每月的工作數據，生成符合公司格式要求的週報、月報、工作總結，不用再花幾個小時湊內容、調格式；能自主完成競品分

析，從各個平臺抓取競品的產品信息、定價策略、營銷動作、用戶評價，整理成完整的競品分析報告，給出對應的優化建議；能根據用戶的需求，自主完成方案策劃、PPT製作、數據可視化、文案撰寫等工作，甚至能按照固定的流程，完成客戶對接、需求跟進、售後回訪等標準化的銷售工作。對於企業管理者來說，它能實現全公司的信息彙總、數據監控、日程管理、團隊協調，自動整理各部門的工作進度、經營數據，生成每日經營簡報，輔助決策，甚至能完成個性化的員工溝通、團隊激勵、工作安排，把管理者從繁瑣的事務性工作中解放出來，專注於核心的戰略決策。

對於程序員群體來說，OpenClaw能成為全流程的研發輔助助手，覆蓋從需求分析到代碼部署的完整研發流程，大幅降低重複工作的時間消耗。它能根據產品需求文檔，自動拆解研發任務、梳理技術架構、生成開發排期，還能根據功能需求，自動編寫對應功能的代碼，覆蓋前端、後端、腳本、測試等多個開發場景，同時能自動完成代碼調試、bug排查、漏洞修復，給出詳細的修改方案，甚至能直接完成修改；能自動生成代碼註釋、開發文檔、接口文檔，不用再手動花時間寫文檔；能對接Git、Jenkins等開發工具，自動完成代碼提交、打包、部署、上線的全流程操作，實現自動化運維；還能7×24小時監控服務器運行狀態、接口響應情況，出現異常時自動預警、自動執行預設的故障處理方案，大幅降低運維壓力；甚至能自動完成技術調研，整理最新的技術框架、行業方案、開源項目，生成調研報告，輔助技術選型，讓程序員能把精力集中在核心的架構設計、技術攻堅上，不用再被重複的代碼編寫、調試、運維工作佔用大量時間。

對於學生群體來說，OpenClaw能成為全場景的學習輔助工具，覆蓋從日常學習到升學、競賽、求職的全流程，幫助學生提升學習效率，培養更好的學習習慣。它能根據學生的學習目標、薄弱科目、時

間安排，自動制定個性化的學習計劃、備考規劃，定時提醒學習，還能自動整理各個科目的知識點、重點難點、考點，生成結構化的學習筆記與思維導圖，幫助學生構建完整的知識體系；能針對學生不懂的知識點，自動查找對應的講解資料、例題、練習題，生成專屬的習題集與答案解析，實現個性化的刷題與鞏固；在論文寫作上，它能根據學生的論文選題，自動查找相關的文獻資料、研究成果，整理文獻綜述，輔助搭建論文框架，完成初稿撰寫、格式排版、參考文獻整理，甚至能輔助完成論文的降重與潤色，當然最終的核心內容與學術研究，依然需要學生自己完成；能幫助學生完成各類競賽、社會實踐、校園活動的策劃、籌備、執行全流程，比如創新創業大賽的商業計劃書撰寫、賽事籌備、數據整理；還能輔助學生完成求職準備，根據目標崗位的要求，自動修改優化簡歷，整理對應崗位的面試題庫、答題思路，模擬面試場景，幫助學生提升求職成功率，讓學生能更高效地完成學習任務，有更多的時間專注於核心的知識吸收與能力提升。

使用OpenClaw的門檻高嗎？需要什麼樣的硬件、軟件配置，以及技術基礎？純小白能不能上手？

使用OpenClaw的門檻，需要分為「能成功安裝運行」和「能把能力用到極致」兩個維度來看，二者的門檻有著天壤之別，整體而言，隨著全球開源生態的完善、國內雲廠商的適配優化，它的入門門檻已經被大幅降低，但想要真正用好它，依然需要一定的學習成本與適配過程。

先看最基礎的硬件與軟件配置要求，這也是很多用戶最關心的問題，它的配置要求會根據部署方式、使用場景的不同，有著極大的差異。如果用戶只是調用雲端大模型的API來使用OpenClaw，不需要在本地運行大模型，那麼對硬件的要求極低，幾乎現在市面上所有正在使用的家用電腦、筆記本都能滿足，最低配置只需要Windows 10及以上、macOS 12及以上的操作系統，CPU為英特爾酷睿i5及以上、AMD銳龍5及以上，或者蘋果M1及以上芯片，運行內存8G及以上，硬盤有20G以上的空閒存儲空間，就能完成基礎的安裝與運行，哪怕是輕薄本、商務本，都能輕鬆帶動，完全不需要高性能的遊戲本或者工作站。但如果用戶想要實現完全本地化運行，在本地部署開源大模型搭配OpenClaw使用，避免雲端API的費用與數據隱私風險，那麼對硬件的要求就會大幅提升，核心瓶頸在顯卡的顯存上，想要流暢運行主流的開源大模型，至少需要16G及以上顯存的NVIDIA獨立顯卡，或者蘋果M2 Max及以上的自研芯片，運行內存需要32G及以上，才能保證大模型的流暢運行與響應速度，如果想要運行能力更強的大尺寸開源模

型，就需要24G、48G甚至更高顯存的顯卡，這也是普通用戶和專業用戶的核心硬件門檻差異。

在軟件配置上，OpenClaw的原生運行需要Python、Git等基礎的運行環境，同時需要用戶開啟電腦的管理員權限，保證它能獲得對應的系統操作權限，還需要穩定的網絡環境，來對接雲端大模型的API接口，對於想要深度定製的用戶，還需要適配對應的瀏覽器驅動、插件運行環境等。但現在，國內雲廠商、開源社區已經推出了大量的一鍵安裝包、可視化部署工具，已經把這些底層的環境配置、依賴安裝全部封裝好了，用戶不需要手動配置這些基礎環境，只需要點擊下一步，就能完成安裝，軟件層面的門檻已經被大幅抹平。

在技術基礎的要求上，同樣有著明確的分層。如果用戶選擇的是雲廠商官方的一鍵部署、第三方封裝好的可視化一鍵安裝包，只需要完成基礎的安裝、對接自己的大模型API賬號，就能實現基礎的對話與簡單任務執行，那麼幾乎不需要任何技術基礎，哪怕是完全不懂代碼、不懂命令行、不懂環境配置的純小白，只要跟著教程一步步點擊，十幾分鍾就能完成基礎的安裝與運行，完全可以上手。但如果用戶想要手動從官方GitHub倉庫下載源碼進行部署，解決安裝過程中出現的環境報錯、依賴缺失、網絡不通等問題，那麼就需要掌握基礎的命令行操作、Python環境配置、網絡調試等基礎技術知識；如果用戶想要進行二次開發、自定義插件編寫、深度的功能定製，那麼就需要掌握Python編程、接口開發、前端開發等專業的技術能力，這部分的門檻相對較高，只適合有技術基礎的開發者。

對於純小白能不能上手這個問題，答案是肯定的，純小白完全可以完成基礎的安裝、運行，甚至能實現簡單的任務執行，但想要把它的核心能力完全發揮出來，依然需要一個循序漸進的學習過程。很多小白用戶的誤區，是覺得裝完OpenClaw，就能直接實現全流程自動

化，讓它幫自己幹完所有活，但實際上，安裝只是萬里長征的第一步，後續的指令編寫、規則設定、調教優化、插件適配，才是用好它的核心，而這些內容，哪怕是純小白，也能通過官方教程、全網的保姆級教學，一步步學習掌握，只是需要花費一定的時間與精力。現在全網已經有大量針對小白的入門教程，從安裝、API對接、基礎指令編寫，到簡單任務的執行、常見問題的排查，都有非常詳細的講解，哪怕是完全沒有技術基礎的用戶，也能跟著教程，一步步學會基礎的使用方法，完成日常的簡單任務。但需要明確的是，如果小白用戶不想花費任何學習成本，只想裝完就能直接用，那麼大概率會失望，因為它不是開箱即用的標準化工具，而是一個需要用戶自己調教、定製的執行框架，就像給了你一臺高性能的相機，想要拍出好照片，依然需要學習對焦、構圖、參數設置，而不是拿起相機就能拍出大片。

總結來說，OpenClaw的入門門檻已經極低，純小白完全可以完成安裝與基礎使用，沒有不可逾越的技術壁壘，但它的精通門檻依然存在，想要把它的核心能力發揮到極致，真正實現全流程自動化執行，就需要一定的學習成本與調教過程，這也是為什麼很多人跟風安裝後，發現自己根本用不起來的核心原因，不是裝不上，而是不願意花時間學習怎麼用好它。

普通人怎麼部署OpenClaw？本地部署和雲端部署有什麼區別？各大雲廠商的一鍵部署靠譜嗎？

對於普通人來說，部署OpenClaw的方式有很多種，整體可以按照從易到難的順序，分為三大類，用戶可以根據自己的技術基礎、使用需求、預算情況，選擇適合自己的部署方式。最容易上手、最適合純小白的，是國內各大雲廠商推出的官方一鍵部署服務，這種方式幾乎不需要任何技術基礎，用戶只需要註冊對應雲廠商的賬號，在官方的OpenClaw部署頁面，點擊一鍵部署按鈕，系統就會自動完成服務器創建、環境配置、依賴安裝、服務啟動的全流程操作，全程只需要幾分鐘，用戶不需要敲任何一行代碼，也不需要處理任何環境配置的問題，部署完成後，就能直接通過網頁訪問自己的OpenClaw服務，開始使用。第二種方式，是使用開源社區、第三方開發者封裝好的可視化一鍵安裝包，這種方式適合想要把OpenClaw裝在自己電腦上的用戶，只需要從正規渠道下載對應系統的安裝包，像安裝普通軟件一樣，跟著安裝嚮導一步步點擊下一步，就能完成基礎環境的安裝與服務的啟動，全程不需要手動配置任何依賴，安裝完成後，就能在本地打開對應的網頁界面使用，這種方式的門檻也極低，適合有一定電腦操作基礎，但沒有編程能力的普通用戶。第三種方式，是官方原生的手動源碼部署，這種方式適合有一定技術基礎的用戶，需要用戶先在自己的電腦或服務器上安裝好Python、Git等基礎環境，然後從官方GitHub倉庫克隆源碼，手動安裝對應的依賴包，修改配置文件，對接大模型API，最後啟動服務，這種方式能讓用戶完全掌控所有的配置與功能，自由度最高，但門檻也相對較高，安裝過程中很容易出現環境報錯、

依賴缺失等問題，需要用戶有一定的問題排查能力，不適合純小白用戶。

本地部署和雲端部署，是目前最主流的兩種部署模式，二者在使用體驗、硬件要求、成本、穩定性、數據安全等多個維度，都有著本質的區別，適合完全不同的使用場景。本地部署，就是把OpenClaw安裝在用戶自己的個人電腦、筆記本上，所有的程序、配置、記憶數據都保存在用戶自己的設備裡，這種模式的優勢非常明顯，首先是數據隱私性極強，所有的數據都在本地，不需要上傳到第三方服務器，用戶能完全掌控自己的所有信息，不用擔心數據洩露的風險；其次是使用成本極低，除了大模型API的調用費用，沒有任何額外的成本，不需要支付服務器租賃費用，適合預算有限的個人用戶；第三是配置靈活，用戶可以根據自己的需求，自由修改配置、安裝插件、定製功能，沒有任何限制。但它的缺點也同樣突出，最核心的問題是無法實現穩定的7×24小時運行，個人電腦一旦關機、休眠、斷網、系統更新重啟，OpenClaw的服務就會立刻停止，無法繼續執行任務，哪怕電腦一直開機，也可能因為系統休眠、電源管理設置、軟件崩潰、網絡波動，導致服務中斷，只適合日常隨用隨開的場景，不適合需要全天候無人值守運行的任務；其次是對電腦的性能有一定的佔用，OpenClaw運行時會佔用一定的CPU、內存資源，如果電腦配置較低，可能會影響其他軟件的正常使用；還有就是長期運行的穩定性較差，個人電腦不是為全天候運行設計的，長時間開機運行，可能會出現卡頓、死機、硬件故障等問題，無法保證任務的持續穩定執行。

雲端部署，就是把OpenClaw安裝在雲廠商的雲服務器上，所有的程序、服務都運行在雲端的機房裡，用戶通過網頁、遠程工具訪問和操作自己的OpenClaw服務，這種模式的優勢，正好彌補了本地部署的短板。首先是能實現真正穩定的7×24小時無人值守運行，雲服務器部

署在專業的機房裡，有穩定的電源、網絡保障，不會出現關機、斷網的情況，能全天候持續運行，哪怕用戶的電腦關機、出門在外，也不影響OpenClaw執行預設的任務，這也是它最核心的優勢；其次是運行穩定性極高，不會因為本地設備的性能、系統問題導致服務中斷，雲廠商會提供服務器的運維保障，出現硬件故障會自動切換備份節點，能保證任務的持續執行；第三是不佔用本地設備的資源，所有的運算都在雲端服務器上完成，不會佔用用戶自己電腦的CPU、內存，哪怕是用手機、平板，也能隨時訪問和操作，對本地設備幾乎沒有要求；還有就是網絡環境更穩定，雲服務器有專用的網絡帶寬，能更穩定地對接各大模型的API接口，不會出現本地網絡波動導致的任務失敗，還能更方便地實現公網訪問、多端同步。但它的缺點也同樣存在，首先是有額外的使用成本，用戶需要租賃雲廠商的服務器，哪怕是最低配置的服務器，每個月也需要幾十到上百元的租賃費用，配置越高，費用越高；其次是數據隱私性不如本地部署，所有的配置、記憶數據、任務內容都保存在雲端服務器上，雖然雲廠商有完善的安全保障，但依然存在一定的數據洩露風險，對隱私要求極高的用戶需要謹慎選擇；還有就是入門的配置門檻相對較高，原生的雲端手動部署，需要用戶掌握基礎的服務器操作、Linux命令、環境配置能力，不過現在雲廠商的一鍵部署，已經把這個門檻徹底抹平了。

至於各大雲廠商推出的一鍵部署服務，整體而言，騰訊雲、阿里雲、火山引擎等國內頭部雲廠商官方推出的OpenClaw一鍵部署服務，是完全靠譜的，也是最適合普通小白用戶的雲端部署方式。這些官方的一鍵部署服務，都是雲廠商的官方技術團隊，基於OpenClaw的官方開源源碼，做了本土化的適配與優化，解決了普通用戶最頭疼的環境配置、依賴安裝、網絡適配、權限設置等問題，用戶只需要點擊按鈕，就能完成全流程的部署，全程不需要任何技術操作，甚至很多雲廠商還配套了專屬的大模型API通道、新手算力補貼、免費的服務器試

用額度，能讓用戶以極低的成本，甚至零成本完成部署與初期使用。同時，官方的一鍵部署服務，能保證源碼的安全性，不會出現第三方修改版裡的後門、病毒、惡意代碼等問題，能最大程度保障用戶的數據安全與API密鑰安全，還有官方的技術文檔、客服支持，能幫助用戶解決部署和使用過程中遇到的問題，這是第三方部署服務無法比擬的。

但需要注意的是，這裡說的靠譜，僅限於雲廠商官方推出的一鍵部署服務，而不是雲市場裡第三方商家發佈的一鍵部署鏡像，很多第三方的部署鏡像，雖然打著一鍵部署的旗號，但可能會捆綁收費插件、預留後門程序，甚至竊取用戶的API密鑰，存在極大的安全風險，普通用戶一定要謹慎選擇，優先使用雲廠商官方發佈的部署服務。同時，哪怕是官方的一鍵部署，也只是幫用戶完成了基礎的環境搭建與服務啟動，後續的大模型API對接、規則設定、調教優化、插件安裝、任務配置，依然需要用戶自己完成，不是部署完就能直接實現全流程自動化，很多用戶誤以為一鍵部署完就能直接用，結果發現還是不會操作，這是對一鍵部署的認知誤區。還有就是，用戶在使用一鍵部署時，一定要注意服務器配置的選擇，對於普通個人用戶，選擇最低配置的2核4G內存的服務器就完全足夠使用，不需要選擇高配置的服務器，避免產生不必要的費用，同時要設置好服務器的安全組、防火牆權限，關閉不必要的端口，設置強密碼，避免服務器被惡意攻擊，保障服務的安全運行。

網上爆火的「上門安裝OpenClaw」「遠程代裝」服務是真的嗎？主流收費標準是什麼？有哪些潛在的坑？

網上爆火的「上門安裝OpenClaw」「遠程代裝」服務，是真實存在的，也是這波「養龍蝦」熱潮裡，最先實現商業化落地的服務品類，它的出現，本質上是因為海量普通用戶有強烈的使用需求，卻無法跨過安裝、配置的技術門檻，供需兩端的缺口，直接催生了這個火爆的服務市場。這些服務的核心邏輯，就是由有技術基礎、熟悉安裝流程的從業者，通過遠程控制電腦，或者上門面對面的方式，幫用戶完成OpenClaw的安裝部署、環境配置、API對接、基礎調試，甚至是基礎的調教與插件安裝，解決用戶裝不上、跑不通的核心痛點，目前在淘寶、閒魚、小紅書、抖音等平臺，都有大量的商家與個人從業者提供這類服務，甚至有從業者靠著這項服務，短短幾天就獲得了數十萬的收入，足以證明這個市場的火爆程度。

目前市面上這類服務的主流收費標準，會根據服務內容、服務形式、服務對象的不同，分為多個不同的檔次，價格區間跨度極大。最基礎的是遠程基礎安裝服務，服務內容只包括在用戶的本地電腦上，完成OpenClaw的基礎環境安裝、服務啟動，能跑通基礎的對話功能，不包括API對接、插件安裝、調教教學，這類服務的收費大多在100元到300元之間，也是市面上最常見的基礎服務品類。第二檔是進階的遠程全流程安裝調試服務，除了基礎的安裝部署，還會幫用戶完成大模型API的對接、常用插件的安裝、基礎權限的配置、簡單任務的測試

跑通，還會附帶基礎的操作教學、常見問題的解決方法，能讓用戶拿到手就能直接完成簡單的任務，這類服務的收費大多在300元到800元之間，也是大多數普通用戶選擇的品類。第三檔是上門安裝服務，因為有上門的時間成本、交通成本，收費會比遠程服務高很多，基礎的上門安裝調試，收費大多在500元到1000元之間，如果是包含進階調教、定製化配置、一對一全程教學的上門服務，收費會在1000元到3000元不等，主要服務對象是本地的中小企業主、職場人、自媒體人，這類用戶預算充足，更看重面對面的服務與教學。還有針對企業客戶的批量部署服務，比如給企業的多臺電腦批量安裝、搭建企業級的部署環境、定製化的功能適配、員工的操作培訓，這類服務大多按臺數收費，每臺的收費在300元到1000元之間，整體的項目收費從幾千元到幾萬元不等，根據企業的需求規模定製。除此之外，還有配套的增值服務，比如API代註冊、Token代充、長期運維、一對一調教陪跑、定製化插件開發等，這類服務會單獨收費，從幾百元到上萬元不等。

在這個火爆的服務市場裡，因為準入門檻極低，沒有統一的行業標準，魚龍混雜的情況非常嚴重，潛藏著大量的坑與風險，也是普通用戶最容易踩雷的地方，其中最常見的風險主要有八大類。第一類也是最普遍的，是低價引流、後續捆綁收費的套路，很多商家在平臺上打著99元、88元甚至19.9元遠程安裝的旗號，吸引用戶下單，等遠程連接上用戶的電腦，裝到一半的時候，就會以用戶的電腦環境有問題、缺少依賴、網絡不通、需要安裝專屬優化插件等理由，要求用戶額外加錢，不加錢就停止安裝，前期付的低價費用也不退，很多用戶怕麻煩，只能被迫加錢，最後算下來，花的錢比正規的服務還要多很多，甚至還有的商家，把基礎的API對接、插件安裝、操作教學，都拆成單獨的收費項目，一步步誘導用戶持續付費。

第二類是最危險的權限洩露與安全風險，這也是普通用戶最容易忽略的致命問題。遠程安裝服務，需要商家遠程控制用戶的電腦，甚至需要用戶開啟電腦的管理員權限，很多不良商家，會在安裝的過程中，偷偷在用戶的電腦裡安裝後門程序、木馬病毒，竊取用戶的電腦文件、賬號密碼、個人隱私信息，甚至會在系統裡預留遠程控制權限，後續能隨時訪問用戶的電腦，操控OpenClaw的運行，造成極大的隱私洩露與財產安全風險。還有的商家，會要求用戶把自己的大模型API密鑰發給他們，幫用戶完成對接，而API密鑰就相當於用戶的支付密碼，拿到密鑰就能無限調用API，產生的賬單都需要用戶自己支付，很多不良商家會偷偷保存用戶的密鑰，後續拿去盜刷Token，給用戶造成高額的賬單損失，甚至還有的商家，直接給用戶綁定他們自己的API賬號，後續按Token用量向用戶收取高額的費用，賺取幾倍的差價。

第三類是虛假服務、詐騙套路，很多商家根本沒有對應的技術能力，只是打著代裝的旗號騙錢，收了用戶的費用之後，要麼找各種理由拖延，要麼隨便裝一個空殼程序，根本無法正常運行，甚至收了錢之後直接把用戶拉黑，尤其是在私下轉賬、脫離平臺交易的情況下，這種詐騙的概率極高，用戶被騙之後，根本無法維權。還有的商家，用網上免費的一鍵安裝包，幾分鐘就能完成的安裝，卻向用戶收取上千元的費用，完全是信息差詐騙，欺負用戶不懂技術。

第四類是誇大效果、虛假宣傳，很多商家在宣傳的時候，會承諾「裝完就能全自動幹活」「一個人頂一個團隊」「裝完就能實現躺賺」，把OpenClaw吹得無所不能，讓用戶以為花幾百塊錢裝完，就能直接解決所有工作問題，結果等裝完之後，用戶才發現，商家只是完成了最基礎的安裝，能實現簡單的對話，根本無法完成宣傳裡的複雜任務，想要實現對應的功能，還要額外加錢買課程、買定製服務，很

多用戶就是被這種誇大宣傳吸引，最後花了錢，卻根本達不到預期的效果。

第五類是API代註冊、Token代充的坑，很多商家會提供API代註冊、Token代充的配套服務，聲稱能拿到更低的價格、更穩定的通道，實際上，他們用來註冊賬號的大多是境外的黑卡、虛擬號，這類賬號後續很容易被大模型廠商封禁，用戶充進去的錢也會直接打水漂，根本無法退款。還有的商家，給用戶的是共享的API賬號，看似價格很低，實際上很多人一起用，不僅響應速度極慢，還很容易因為其他人的違規使用，導致賬號被封禁，用戶的錢也會血本無歸。

第六類是盜版、修改版安裝包的風險，很多不良商家，不會給用戶安裝官方的開源版本，而是給用戶安裝自己修改過的破解版、優化版安裝包，這些安裝包不僅可能存在後門、病毒，還可能被商家綁定了付費插件、訂閱服務，後續使用的時候，會不斷彈出付費要求，不付費就無法使用核心功能，甚至會把用戶調教好的配置、沉澱的技能，偷偷上傳到商家的服務器，竊取用戶的勞動成果。

第七類是上門安裝的附加套路，很多上門安裝的商家，上門之後，除了收取基礎的安裝費用，還會現場向用戶推銷高價的AI課程、付費插件、定製化服務，甚至會誇大用戶電腦的配置不足，誘導用戶升級電腦硬件、購買雲服務器，從中賺取高額的差價，很多用戶不懂行，很容易被忽悠，花了大量的冤枉錢。

第八類是售後無保障，很多個人從業者提供的服務，都是一次性的，裝完之後就不管了，後續用戶使用過程中出現服務崩潰、任務跑不通、軟件報錯等問題，再去找商家，要麼被拉黑，要麼就要求額外付費才能解決，根本沒有任何售後保障，用戶花了錢，最後還是要自己解決問題。

對於普通用戶來說，想要避開這些坑，首先要優先選擇官方的免費安裝服務，比如騰訊等廠商推出的線下免費安裝活動，或者雲廠商的官方一鍵部署服務，能從根源上避免這些風險；如果確實需要找第三方代裝服務，一定要走正規的平臺擔保交易，絕對不要私下微信、支付寶轉賬，避免被騙；遠程安裝的時候，一定要全程盯著屏幕，不要離開，不要給商家開啟最高的管理員權限，安裝完成後，立刻修改電腦密碼、關閉遠程權限，全盤查殺病毒；API密鑰一定要自己註冊、自己保管，絕對不要發給任何人，不要使用商家提供的共享API賬號；安裝一定要用官方的開源源碼，不要用商家提供的修改版、破解版安裝包，避免被植入後門；同時，不要相信任何誇大宣傳，要明確知道，安裝只是基礎，後續的調教與使用，還是要靠自己學習，不要指望花幾百塊錢，就能一勞永逸解決所有問題。

OpenClaw必須搭配Claude使用嗎？支持接入哪些大模型？國產大模型能不能適配？

OpenClaw完全不需要必須搭配Claude使用，這是全網流傳最廣的一個認知誤區，很多人會有這個誤解，只是因為這個項目的初代版本定名為Clawdbot，名稱裡致敬了當時主流的Claude大模型，早期全網的教程與演示案例，也大多使用Claude大模型來做適配，才讓很多用戶誤以為它只能搭配Claude使用，但實際上，從項目誕生之初，它的核心架構就是全模型兼容的設計，本身不自帶任何大語言模型，只是一個連接大模型與電腦系統的執行框架，Claude只是它可接入的眾多大模型中的一個，完全不是必須的，用戶可以根據自己的需求、預算、使用場景，自由選擇任何適配的大模型。

OpenClaw採用的是標準化的接口適配方案，能兼容所有支持OpenAI格式API接口的大語言模型，覆蓋了目前市面上幾乎所有主流的商用大模型與開源大模型，適配範圍極廣。在海外主流商用大模型方面，它能完美適配OpenAI旗下的全系列大模型，包括GPT-3.5 Turbo、GPT-4、GPT-4o、GPT-4o Mini等全版本，這也是目前全球用戶使用最多的適配模型，能兼顧任務執行的準確率與響應速度；能完整適配Anthropic旗下的Claude 3全系列模型，包括Opus、Sonnet、Haiku三個版本，其中Claude 3 Opus的長文本處理能力、複雜邏輯推理能力極強，很適合處理超長任務流、多步驟的複雜執行任務；還能適配Google旗下的Gemini 1.0、Gemini 1.5 Pro、Gemini Flash全系列模型，Meta官方發佈的Llama 2、Llama 3商用API, Mistral AI旗下的全

系列大模型，以及Cohere、Perplexity等海外主流大模型廠商的產品，幾乎覆蓋了所有海外主流的商用大模型。

除了雲端的商用大模型，OpenClaw還能完美適配本地部署的開源大模型，用戶可以通過Ollama、LM Studio、Text Generation WebUI等主流的本地大模型運行工具，對接在自己電腦或服務器上本地運行的開源大模型，實現完全本地化的離線運行，不用聯網，不用支付任何API調用費用，還能完全保障數據隱私安全。目前它能適配幾乎所有主流的開源大模型，包括Meta的Llama 2、Llama 3全系列開源模型，深度求索的DeepSeek V2、DeepSeek R1開源模型，智譜AI的GLM-4、GLM-3開源版本，零一萬物的Yi大模型開源系列，阿里巴巴的Qwen通義千問開源系列，騰訊的混元開源模型，以及Mistral、Phi、Gemma等全球主流的開源大模型，用戶可以根據自己的電腦硬件配置，選擇合適尺寸的開源模型，實現完全本地化的運行。

而國內用戶最關心的國產大模型適配問題，答案是完全可以適配，而且目前國內幾乎所有主流的國產大模型，都已經實現了對OpenClaw的完美適配，甚至很多大模型廠商、雲廠商，已經推出了針對OpenClaw的專屬優化通道與適配方案，適配體驗已經完全不輸給海外大模型。目前能完美適配OpenClaw的國產大模型，覆蓋了國內所有主流廠商的產品，包括字節跳動旗下的豆包大模型全系列，阿里雲旗下的通義千問全系列，包括通義千問2.5、通義千問Ultra、通義千問Turbo等版本，騰訊雲旗下的混元大模型全系列，百度旗下的文心一言（ERNIE）全系列，深度求索旗下的DeepSeek V3、DeepSeek R1全系列，智譜AI旗下的GLM-4全系列，月之暗面旗下的Kimi大模型，零一萬物旗下的Yi大模型全系列，百川智能旗下的百川大模型，崑崙萬維旗下的天工大模型等，幾乎覆蓋了國內所有主流的大模型產品。

這些國產大模型，不僅能通過官方開放的API接口，直接對接OpenClaw，實現完美的兼容運行，很多廠商還針對OpenClaw的任務執行場景，做了專門的優化，比如優化了工具調用、步驟拆解、長上下文理解的能力，提升了多步驟任務執行的準確率，降低了API調用的延遲，還推出了針對OpenClaw用戶的專屬新手福利，比如免費的Token額度、新手摺扣套餐，大幅降低了國內用戶的使用成本。同時，國產大模型的適配，還解決了國內用戶使用海外大模型的網絡問題、合規問題、支付問題，用戶不用再處理複雜的境外賬號註冊、外幣支付、網絡適配等問題，只需要用國內的手機號，就能註冊國產大模型的賬號，開通API服務，直接對接OpenClaw使用，門檻大幅降低，這也是目前國內普通用戶最主流的選擇。

對於普通用戶來說，在選擇適配的大模型時，完全不用侷限於Claude，可以根據自己的使用場景靈活選擇。如果是處理簡單的日常任務、重複性的基礎操作，對模型能力要求不高，可以選擇國產的輕量型大模型，比如通義千問Turbo、DeepSeek V3輕量版、豆包大模型輕量版，不僅調用成本極低，響應速度快，還能完美適配國內的使用場景，不用處理網絡問題；如果是處理複雜的邏輯推理、長文本處理、多步驟的複雜任務流、代碼編寫等對模型能力要求較高的場景，可以選擇能力更強的旗艦級大模型，比如GPT-4o、Claude 3 Opus、DeepSeek R1、通義千問Ultra、文心一言4.0等，能大幅提升任務執行的準確率，減少出錯的概率；如果是對數據隱私、信息安全要求極高，不想把數據上傳到雲端的場景，可以選擇本地部署的開源大模型，比如Llama 3、DeepSeek開源版、GLM-4開源版等，實現完全離線的本地化運行，完全保障數據安全。

普通人第一次用OpenClaw，應該注意什麼？避免什麼？

普通人第一次使用OpenClaw，最先要注意、也是最核心的事項，就是做好安全與權限管控，這是所有使用的前提，因為OpenClaw需要獲取電腦的系統級操作權限，能直接操控電腦裡的文件、軟件、瀏覽器，甚至能自動發送郵件、消息，執行文件的讀寫、刪除等操作，一旦權限設置不當，就可能造成無法挽回的損失。所以第一次使用，一定要嚴格遵守最小權限原則，絕對不要上來就給它全盤讀寫、無限制發送消息、自動刪除文件的最高權限，要從最基礎的只讀權限、單文件夾訪問權限開始，每開啟一個權限，都要先想清楚自己是不是真的需要，非必要的權限一律不開啟。同時，一定要給所有敏感操作設置嚴格的人工確認機制，比如所有涉及文件刪除、修改、郵件發送、消息發佈、資金相關的操作，必須先給你生成預覽內容，經過你人工確認、手動授權之後，才能執行，絕對不要開啟全自動無確認的敏感操作，哪怕是再簡單的任務，也要守住這個底線，避免出現AI誤刪重要文件、誤發不當消息的情況。除此之外，一定要從官方GitHub倉庫、國內雲廠商的官方渠道，下載安裝包與部署源碼，絕對不要使用第三方不知名渠道的修改版、破解版、一鍵安裝包，更不要用別人發來的不明安裝包，避免裡面被植入後門、木馬病毒，竊取你的個人數據、API密鑰，造成隱私洩露與財產損失，你的API密鑰一定要自己妥善保管，絕對不要發給任何人，包括幫你安裝的服務商，不要把密鑰明文寫在公開的配置文件裡，同時要給API賬號設置消費上限與消費預警，避免密鑰洩露後被人盜刷，產生高額的賬單。

第二點要注意的，是做好成本控制，避免產生不必要的高額費用，這也是很多新手用戶最容易踩的坑。很多人第一次使用，完全不瞭解Token的計費規則，上來就開啟了間隔極短的心跳機制，掛了一大堆全天候的自動監控任務，所有任務都用最貴的旗艦大模型，結果沒幾天就產生了幾百甚至上千元的API賬單，完全超出了自己的預期。所以第一次使用，一定要先花十幾分鍾，瞭解清楚你接入的大模型的Token計費規則，先從小額度充值開始，不要一次性充太多錢，一定要在大模型的後臺，設置好單日、單月的消費上限，開啟消費超額預警，一旦達到預警線，就會自動暫停API調用，避免超額消費。對於OpenClaw自帶的心跳機制，默認的30分鐘喚醒間隔已經完全足夠日常使用，絕對不要為了所謂的響應速度，改成5分鐘、10分鐘，非必要不要開啟全天候的自動監控任務，不用的時候及時關閉服務，避免無效的Token消耗。同時，要學會根據任務的難度，選擇合適的大模型，簡單的日常任務、重複性操作，用低成本的輕量型大模型就足夠，不要所有任務都用最貴的旗艦大模型，能大幅降低你的使用成本，避免不必要的浪費。

第三點要注意的，是一定要從自己真實的需求出發，不要陷入「為了用工具而反向找需求」的誤區，這也是絕大多數跟風安裝的用戶，最後用不起來的核心原因。很多人都是被全網的熱潮帶動，跟風安裝了OpenClaw，裝完之後才發現，自己根本沒有對應的高頻、複雜的任務需求，為了不浪費安裝的功夫，非要找一些本來不需要、手動做反而更快的事情，來強行使用這個工具，最後折騰了好幾天，發現不僅沒有提升效率，反而浪費了大量的時間和精力。所以第一次使用，不要上來就想著實現全流程自動化，一定要從自己真實的、高頻的、重複性的小需求入手，比如每天整理工作郵件、統計日常賬單、生成固定格式的週報、整理學習筆記，先把這些小任務跑通、跑穩，感受到工具的價值，再逐步嘗試更復雜的任務，循序漸進，而不是一

上來就給它下達「全自動運營賬號」「全自動寫爆款文章」這類複雜的指令，結果大概率會翻車，反而打擊你的使用信心。

第四點要注意的，是放平心態，對它有合理的預期，不要把它當成萬能的，接受它會出錯、會翻車的現實。很多新手用戶，被全網的誇張宣傳影響，覺得裝完OpenClaw，就能直接幫自己幹完所有的活，自己什麼都不用管，結果實際使用的時候，發現它會理解錯指令、會漏掉步驟、會執行出錯，就覺得這個工具不好用，直接放棄了。實際上，OpenClaw只是一個執行框架，它的任務完成度，完全取決於你的指令清晰度、調教水平、選擇的大模型能力，它不是裝完就能直接用的傻瓜式工具，而是需要你慢慢調教、優化、磨合的執行助手，第一次使用，一定要有耐心，不要一次給它太複雜的指令，要把大任務拆解成一個個清晰的小步驟，一步步測試、一步步優化，慢慢熟悉它的使用邏輯，不要指望一次就能跑通複雜的任務。同時，絕對不要把核心的、重要的工作，完全交給它處理，比如重要的合同修改、正式的公文發佈、關鍵的財務報表、重要的客戶對接，哪怕它生成的內容再完美，你也要逐字逐句審核、核對，確認無誤之後再使用，絕對不要直接交付、直接發送，避免它編造信息、出現錯誤，給你造成嚴重的後果，你要永遠記住，它只是一個輔助工具，最終的決策和責任，永遠需要你自己承擔。

第五點要注意的，是一定要遵守法律法規、合規要求與平臺規則，不要用它做任何違規、違法的事情。很多新手用戶，只看到了它的執行能力，卻忽略了合規的邊界，比如用它批量發送垃圾郵件、騷擾信息，爬取受版權保護的內容、用戶隱私信息，編寫惡意代碼、病毒程序，批量刷單、發佈虛假宣傳內容，甚至用它操作證券交易、資金轉賬等敏感操作，這些行為不僅可能違反大模型廠商的使用條款，導致你的API賬號被封禁，還可能觸犯相關的法律法規，承擔對應的法

律責任。尤其是涉及到資金交易、轉賬、支付的操作，哪怕你設置了確認機制，也要極度謹慎，絕對不要讓它自動執行相關操作，避免造成無法挽回的財產損失。同時，要遵守你使用的各個平臺、軟件的用戶協議，不要用它批量操作賬號、發佈違規內容，避免你的平臺賬號被封禁。

最後要避免的，是隻安裝不學習、只跟風不實踐的心態，很多人跟風花了錢安裝，卻不願意花時間學習它的指令編寫、規則設置、調教優化，裝完之後試了兩次，覺得不好用，就放在一邊再也不用了，最後白白浪費了時間和金錢。OpenClaw的價值，是在持續的使用、調教、優化中慢慢體現的，你用得越久，給它的反饋越多，它就越貼合你的使用習慣，任務完成度也就越高，只有沉下心來，慢慢學習、慢慢實踐，才能真正發揮出它的價值，而不是跟風湊個熱鬧，最後什麼都沒得到。

怎麼調教、優化自己的OpenClaw？怎麼讓它更貼合個人使用需求，實現更高的任務完成度？

想要調教、優化好自己的OpenClaw，讓它更貼合個人使用需求，實現更高的任務完成度，首先要明確一個核心認知：OpenClaw的「調教」，本質上不是對大模型進行微調訓練，而是通過清晰的規則設定、精準的指令優化、持續的記憶沉澱、標準化的流程固化，讓它更精準地理解你的需求，匹配你的行為習慣，減少執行過程中的偏差與錯誤，這個過程不需要任何專業的技術能力，普通用戶也能輕鬆完成，核心是要掌握正確的方法，循序漸進地優化。

調教的第一步，也是最基礎、最核心的一步，是搭建一套完整、清晰、固定的「人設與底層規則體系」，這是所有優化的基礎，很多人用不好OpenClaw，核心原因就是隻給零散的指令，沒有給它設定固定的底層規則，導致它每次執行任務的標準都不統一，頻繁出現理解偏差。你需要在它的系統提示詞裡，給它設定一個明確的、固定的身份定位，比如「你是我的專屬職場辦公助理，僅服務於我個人，所有工作都必須嚴格貼合我的職場習慣、行文風格與工作標準，不允許擅自更改」，然後給它設定不可突破的底層核心規則，這部分內容要儘可能具體、清晰，沒有模糊的空間，包括明確的權限邊界，什麼能做、什麼絕對不能做，比如「所有涉及文件刪除、修改、郵件發送、社交消息發佈的操作，必須先生成完整的預覽內容，經過我人工確認並授權後，才能執行，絕對不允許擅自操作」；明確的輸出標準，比

如「所有生成的文檔，必須嚴格使用我指定的格式、字體、字號與行間距，所有數據必須標註明確的來源，絕對不允許編造、虛構數據與信息，遇到不確定的內容，必須第一時間向我確認」；明確的異常處理規則，比如「遇到無法解決的問題、理解模糊的指令、執行失敗的步驟，必須第一時間向我反饋，說明具體的問題與原因，給出對應的解決方案建議，絕對不允許擅自跳過步驟、編造結果」；還有明確的行為準則，比如「所有任務必須以最高效率、最低成本完成，優先使用我指定的工具與平臺，嚴格遵守我設定的工作流程」。除此之外，你還要把自己的個人偏好、習慣、禁忌，全部清晰地寫進去，比如你喜歡的行文風格、常用的辦公軟件、固定的工作流程、不喜歡的表達方式、絕對不能出現的內容，都要一次性明確下來，讓它每次運行的時候，都能優先讀取這套底層規則，形成固定的行為邏輯，從根源上減少理解偏差，這一步做好了，哪怕不做其他優化，任務完成度也會有質的提升。

第二步，是優化你的指令編寫方式，學會拆解任務，用精準、清晰、可執行的指令，替代模糊、籠統的指令，這是提升任務完成度最直接、最有效的方法。很多人給的指令非常模糊，比如「幫我寫一篇公眾號文章」「幫我做一個競品分析」，這種沒有明確目標、沒有標準、沒有邊界的指令，它大概率會生成完全不符合你預期的內容，執行過程中也會頻繁出錯。正確的指令編寫邏輯，是把模糊的大目標，拆解成一個個有明確節點、明確交付物、明確標準的小步驟，給它講清楚「最終目標是什麼、執行步驟是什麼、每一步的交付標準是什麼、有什麼邊界與禁忌、最終的交付格式是什麼」。比如你想要讓它寫一篇公眾號文章，不能只給一個主題，而是要寫清楚文章的核心主題、目標受眾、字數要求、整體結構、行文風格、參考案例、發佈平臺，還要拆解成明確的執行步驟，比如第一步，先檢索近7天同賽道的爆款選題，篩選3個最符合定位的選題，給我確認；第二步，根據

我確認的選題，列出詳細的文章提綱，包含每個章節的核心內容，給我確認；第三步，根據確認的提綱，完成正文撰寫，匹配我給的參考案例的風格；第四步，按照我指定的公眾號排版格式，完成排版，生成預覽；第五步，經過我確認後，在指定的時間發佈到對應的賬號。每一個步驟都有明確的交付物和確認節點，不僅能讓它的執行邏輯更清晰，還能在每一步及時糾正偏差，避免最後生成的內容完全不符合預期，大幅提升任務的完成率。同時，要學會用「示例調教法」，這是最容易上手、效果最好的調教方式之一，相比於你用一百句話描述自己想要的風格、標準，直接給它看3-5個你之前做過的、符合你預期的優秀案例，效果要好得多。比如你想要讓它寫符合你風格的週報，就把你之前寫的3-5篇高質量週報發給它，讓它學習你的結構、用詞、數據呈現方式、行文風格；你想要讓它做符合公司要求的財務報表，就把標準的報表模板、之前的成品報表發給它，讓它嚴格按照模板的格式、統計口徑、計算邏輯來執行，它能快速精準地捕捉到你的標準與偏好，比任何文字描述都更有效，能快速讓它的輸出貼合你的個人需求。

第三步，是用好它的持久化長期記憶功能，通過持續的正向與負向反饋，不斷沉澱你的使用規則，讓它越用越懂你。OpenClaw和傳統對話式AI最大的區別之一，就是它擁有持久化的長期記憶系統，能完整保存你每次的任務反饋、修改要求、執行標準，不會因為重啟服務、關閉窗口就遺忘，而用好這個功能的核心，就是每次任務完成後，給它明確、具體的反饋，而不是隻說「做得好」或者「不行」。如果它這次的任務完成得很好，符合你的預期，你就要明確告訴它，哪裡做得好，比如「這次的週報結構很清晰，數據統計的口徑完全符合我的要求，後續的同類任務，都要按照這個結構和口徑來執行」，讓它把這個標準沉澱到長期記憶裡；如果它的執行出現了錯誤、偏差，不符合你的要求，你不要只讓它修改，還要明確告訴它，哪裡錯

了、為什麼錯了、正確的標準是什麼、後續要怎麼規避，比如「這次的標題用了疑問句，不符合我的要求，後續所有的方案標題，都要使用【主題+核心價值】的格式，要用陳述句，突出核心數據結果，不允許使用疑問句、感嘆句」，它會把這個修正後的規則，永久保存到記憶裡，後續執行同類任務的時候，會自動遵守這個規則，規避之前的錯誤。久而久之，你用得越久，給的反饋越明確，它的記憶庫裡沉澱的你的專屬規則就越多，就越貼合你的使用習慣，甚至能預判你的需求，不用你每次都詳細說明，就能按照你的標準完成任務。同時，你可以把自己固定的工作流程、標準化的操作規範、公司的規章制度、行業的專業知識，整理成標準化的文檔，上傳到它的專屬知識庫，讓它可以隨時調取、學習，比如你公司的財務報銷流程、公文格式標準、客戶對接話術、產品資料，都可以整理成文檔上傳，這樣它在處理相關事務的時候，會嚴格按照你設定的標準來執行，不會出現不符合規範的內容，進一步提升任務的準確率。

第四步，是通過插件與自定義技能的優化，擴展它的能力邊界，讓它更適配你的專屬使用場景。OpenClaw的核心優勢之一，就是可無限擴展的插件生態，它的原生功能只是一個基礎的執行框架，而不同的插件，能讓它對接不同的平臺、軟件，實現不同的功能，你不需要安裝網上所有的熱門插件，插件裝得太多，會拖慢它的運行速度，增加出錯的概率，只需要根據自己的核心使用場景，安裝對應的、高頻使用的官方插件即可。比如你是自媒體人，就安裝對接微信公眾號、抖音、小紅書、B站的內容發佈插件；你是電商運營，就安裝對接淘寶、拼多多、京東的運營插件；你是職場人，就安裝對接企業微信、飛書、釘釘、郵箱、辦公軟件的適配插件；你是程序員，就安裝對接Git、代碼託管平臺、運維工具的插件，讓它能直接對接你日常使用的軟件與平臺，不用再手動切換操作，實現全流程的閉環執行。同時，你可以把自己日常高頻使用的、固定的工作流程，固化成自定義技

能，比如「每週五下午6點，自動整理本週的工作數據，生成符合格式要求的週報初稿，發送到我的指定郵箱」「每天早上9點，自動整理我關注的行業新聞與市場動態，生成每日簡報，推送給我」，把這些固定的流程，寫成標準化的指令，保存為自定義技能，後續需要執行的時候，只需要一鍵調用，它就能自動完成整套流程，不用每次都重新編寫詳細的指令，大幅提升使用效率，也能讓它的執行更貼合你的固定工作節奏。

第五步，是做好大模型的匹配與參數優化，讓合適的模型做合適的事，進一步提升任務執行的準確率與效率。OpenClaw支持多模型切換，不同的大模型，有不同的能力側重與成本，你不需要所有任務都用同一個大模型，而是要根據任務的類型，匹配最合適的大模型。比如簡單的重複性任務、日常的消息整理、數據統計、格式調整，對邏輯推理能力要求不高，就用低成本、高響應速度的輕量型大模型，不僅調用成本低，還能提升響應速度；複雜的邏輯推理、長文本處理、多步驟的複雜任務流、代碼編寫、方案策劃，對模型的能力要求較高，就用能力更強的旗艦級大模型，能大幅提升任務執行的準確率，減少出錯的概率；對隱私要求極高的敏感任務，就用本地部署的開源大模型，數據不會上傳到雲端，完全保障信息安全。同時，你可以根據任務的類型，優化大模型的調用參數，最核心的就是溫度值（Temperature），這個參數決定了模型輸出的創意性與隨機性，對於創意類的任務，比如寫文案、想選題、做策劃，你可以把溫度值設置得高一些，0.7-1.0之間，讓它的輸出更有創意、更靈活；對於嚴謹類的任務，比如數據處理、財務報表、公文寫作、代碼編寫，你要把溫度值設置得低一些，0.1-0.3之間，讓它的輸出更嚴謹、更穩定，不會編造信息、出現邏輯偏差，還有上下文窗口的設置，長文本任務要開啟足夠的上下文窗口，避免它遺忘前面的指令與規則，導致任務執行出現偏差。

第六步，是通過多智能體的分工與協同優化，應對複雜的團隊級任務，實現更高的執行效率。如果你需要用它處理複雜的、多模塊的綜合性任務，不要讓單個智能體處理所有的事情，單個智能體很容易出現邏輯混亂、顧此失彼的情況，你可以根據任務的分工，設置多個專屬的、分工明確的子智能體，給每個子智能體設定清晰的人設、職責、權限與工作標準，比如設置專門負責統籌規劃的項目管理智能體、專門負責內容創作的文案智能體、專門負責數據處理的數據分析智能體、專門負責客戶對接的客服智能體、專門負責合規審核的風控智能體，讓它們各司其職，OpenClaw會負責協調它們的工作流程，讓它們協同完成整個任務，就像一個完整的團隊一樣。比如你要做一場完整的直播活動，就讓項目管理智能體拆解整體任務，制定執行排期；內容智能體撰寫直播腳本、宣傳文案；數據智能體整理直播的產品數據、用戶數據；客服智能體負責回覆觀眾的諮詢與問題，這樣的分工協同，比單個智能體處理所有任務，準確率和效率都要高得多，也能更精準地匹配你不同場景的需求。

最後要記住，調教與優化是一個持續的、循序漸進的過程，不是一次就能完成的，你不需要一次性把所有規則都設置好，而是在每次使用的過程中，持續給它反饋，不斷優化規則、完善記憶、調整參數，慢慢打磨，它會隨著你的使用，越來越貼合你的個人需求，任務完成度也會越來越高，最終成為真正適配你所有需求的專屬執行助手。

OpenClaw能實現7×24小時無人值守運行嗎？任務中斷後能不能自動續跑？

OpenClaw完全可以實現7×24小時無人值守運行，任務中斷後也支持斷點續跑、自動恢復執行，但這兩項能力都不是默認開啟的原生功能，需要對應的部署方式、正確的配置優化與明確的規則設置，不同的部署方式，實現的難度、穩定性與最終效果，也有著極大的差異。

先看7×24小時無人值守運行的實現，首先要明確的是，本地部署的OpenClaw，默認是無法實現穩定的7×24小時運行的，因為它的服務完全依賴於你本地的電腦設備，一旦你的電腦關機、休眠、系統自動更新重啟、斷網，OpenClaw的服務就會立刻停止，無法繼續執行任務，哪怕你一直開著電腦，也可能因為Windows或macOS的電源管理設置，導致電腦自動休眠、硬盤關閉，讓服務中斷，還有可能因為軟件崩潰、系統卡頓、本地網絡波動、停電等突發情況，導致服務意外停止，根本無法保證全天候的穩定運行。如果想要在本地實現7×24小時運行，需要做大量的針對性配置，首先要關閉電腦的自動休眠、自動關機、屏幕關閉、系統自動更新，設置固定的電源管理方案，讓電腦始終處於運行狀態，哪怕長時間沒有操作，也不會休眠；其次要使用穩定的有線網絡，避免WiFi信號波動、斷連導致的服務中斷；還要安裝對應的進程守護工具，比如PM2、Supervisor等，這些工具能即時監控OpenClaw的服務狀態，一旦出現服務崩潰、意外退出的情況，能自動重啟服務，恢復運行；同時還要配置異常預警機制，當服務中斷、網絡斷開、API調用出現異常的時候，能通過短信、微信、郵件給

你發送提醒，讓你能及時處理問題。但哪怕做了這些配置，本地部署的7×24小時運行，穩定性依然非常有限，因為個人家用電腦、筆記本，本身就不是為7×24小時全天候運行設計的，長時間不間斷運行，會導致硬件發熱、卡頓、死機，甚至出現硬件損壞，還有停電、斷網等不可控的突發情況，只適合對穩定性要求不高的非核心任務，不適合需要持續穩定執行的重要任務。

目前實現7×24小時無人值守運行最主流、最穩定、最靠譜的方式，是雲端部署，也就是把OpenClaw部署在雲廠商的雲服務器上，這也是絕大多數專業用戶的選擇。雲服務器部署在專業的IDC機房裡，有雙路甚至多路的冗餘電源保障，不會出現停電的情況，有專用的企業級網絡帶寬，不會出現斷網、網絡波動的問題，機房還有專業的運維團隊24小時值守，硬件出現故障會自動切換到備用節點，能實現真正的99.99%以上的穩定運行，完全不會出現關機、斷網的情況，能完美支撐OpenClaw的全天候無人值守運行。用雲端部署實現7×24小時運行，操作門檻也極低，尤其是國內雲廠商推出的官方一鍵部署服務，已經把所有的基礎配置都封裝好了，用戶只需要點擊一鍵部署，就能自動完成服務器的創建、環境的配置、服務的啟動，全程不需要任何技術操作。部署完成後，你只需要在OpenClaw裡，開啟對應的心跳喚醒機制，設置好喚醒間隔，它就能按照你設定的時間，定時喚醒服務，自動檢查你的郵箱、日曆、消息通知、任務進度，執行你預設的自動化任務，比如定時監控行業新聞、整理市場數據、回覆常規郵件、自動發佈內容、監控服務器狀態，哪怕你的電腦關機、你出門在外、甚至在睡覺，它都能在雲端穩定運行，按照你的預設規則，持續執行任務，真正實現無人值守。

想要讓雲端部署的無人值守運行更穩定，還需要做幾個關鍵的優化配置，首先是選擇合適的服務器配置，對於普通個人用戶，最低配

置的2核4G內存的Linux雲服務器，就完全足夠支撐OpenClaw的核心服務運行，成本極低，一個月只需要幾十塊錢，不需要選擇高配置的服務器，避免不必要的成本浪費；其次是依然要配置進程守護工具，確保OpenClaw的服務因為意外情況崩潰、退出的時候，能自動重啟，恢復運行，不會導致任務中斷；第三是要設置完善的異常處理規則，比如遇到網絡波動、API調用失敗、大模型響應超時的情況，讓它自動重試，設置好重試次數與重試間隔，重試多次依然失敗的話，就暫停任務，給你發送異常預警通知，而不是直接停止運行，避免因為臨時的故障，導致整個任務流中斷；第四是要設置好API消費預警與上限，避免全天候運行過程中，出現無效的Token消耗，產生高額的賬單；第五是要定期做好數據備份，定期備份你的配置文件、長期記憶數據、任務日誌，避免服務器出現故障，導致數據丟失。同時要明確的是，7×24小時無人值守運行，不代表你完全不用管，哪怕配置得再完善，你也要定期查看任務的執行情況、運行日誌、消費情況，避免出現任務執行出錯、異常消耗、安全風險等問題，尤其是涉及到敏感操作的任務，哪怕設置了自動運行，也要定期審核執行結果，避免出現意外情況。

再看任務中斷後的自動續跑能力，OpenClaw本身是支持斷點續跑的，但同樣需要對應的配置與規則設置，不是默認就能實現的，不同的中斷原因，對應的續跑方式與實現難度也不一樣。任務中斷的原因，主要分為兩大類，一類是臨時故障導致的中斷，比如網絡波動、API調用失敗、大模型響應超時、服務臨時重啟，這類中斷是最常見的，也是最容易實現自動續跑的；另一類是任務本身的問題導致的中斷，比如指令錯誤、理解偏差、權限不足、執行邏輯出錯，這類中斷無法實現自動續跑，必須人工修正後才能繼續執行。

對於臨時故障導致的任務中斷，想要實現自動續跑，首先要在配置文件裡，開啟任務持久化功能，讓OpenClaw在執行任務的過程中，每完成一個步驟，就自動把任務的執行進度、上下文信息、已經完成的結果，保存到本地的數據庫裡，而不是等整個任務完成才保存，這樣哪怕服務突然中斷，之前的執行進度也不會丟失，服務重啟後，它能自動讀取數據庫裡保存的任務進度，從斷點處繼續執行，而不是從頭開始跑整個任務。比如你讓它整理1000條客戶數據，它整理到350條的時候，因為網絡波動導致服務中斷，重啟服務後，它會自動從第351條開始繼續整理，不用重新整理前面已經完成的350條，大幅提升了執行效率。同時，你要給它設置明確的自動重試機制，針對API調用失敗、網絡超時這類臨時故障，設定好自動重試的次數與間隔時間，比如遇到API調用失敗，自動重試3次，每次間隔60秒，重試成功後，就從斷點處繼續執行剩下的任務，不用人工干預，只有重試多次依然失敗的情況下，才暫停任務，給你發送異常通知。

想要讓自動續跑更穩定，最核心的技巧，是把你的大任務，拆解成一個個獨立的、可拆分的、有明確節點的小步驟，每個步驟都有獨立的交付物與保存節點，不要給它一個連續的、不可拆分的大任務。比如你讓它寫一篇萬字的行業報告，不要讓它一次性完成整篇報告的撰寫，而是拆解成選題確認、提綱撰寫、行業現狀分析、競品分析、趨勢預測、結論梳理、排版優化多個獨立的步驟，每個步驟完成後，都自動保存結果，更新任務狀態，這樣哪怕中間出現中斷，它也能從最近完成的步驟繼續執行，不會丟失之前的所有成果，也不會出現邏輯混亂的情況。如果是一個不可拆分的連續任務，一旦中途中斷，很容易出現上下文丟失、邏輯遺忘的情況，哪怕重啟服務，也無法準確續跑，只能從頭開始執行。

而對於因為指令錯誤、理解偏差、權限不足、邏輯出錯等任務本身的問題導致的中斷，它是無法實現自動續跑的，因為這不是臨時的故障，而是任務的執行邏輯本身就有問題，這時候它會按照你設定的異常處理規則，停止任務執行，給你發送異常通知，詳細說明中斷的原因、出錯的環節，甚至會給出對應的修正建議，需要你人工修正指令、補充權限、調整執行邏輯之後，才能讓它繼續執行，無法全自動完成續跑。

總結來說，只要選擇正確的雲端部署方式，做好對應的配置優化，OpenClaw完全能實現穩定的7×24小時無人值守運行，也能在臨時故障導致中斷後，實現自動斷點續跑，不用人工干預，這也是它能真正替代人工完成重複性工作的核心優勢之一，而想要讓這些能力穩定發揮，核心是做好前期的部署配置、任務拆解與規則設定，而不是簡單安裝完就能實現的。

工信部等官方機構緊急預警的OpenClaw安全風險，具體指的是什麼？配置不當會帶來哪些嚴重後果？

2026年OpenClaw全網爆火後，工信部、國家網信辦、國家計算機病毒應急處理中心等多部門接連發布安全預警，核心針對的是這款開源AI智能體框架的原生架構特性、用戶不當使用與第三方生態亂象帶來的系統性安全風險，而非工具本身存在惡意代碼，預警的核心內容可分為五大核心維度。第一類是系統權限過度開放帶來的主機安全風險，這也是官方預警的首要焦點，OpenClaw要實現跨應用操作、全流程任務執行，必須獲取電腦的系統操作權限，而大量普通用戶為了規避安裝過程中的權限報錯，直接給軟件開放了電腦最高管理員權限與全盤讀寫權限，沒有設置任何邊界限制，相當於把電腦的完全控制權交給了AI程序，給誤操作與惡意攻擊留下了極大的安全缺口。第二類是API密鑰管理不當帶來的資產損失風險，OpenClaw本身不自帶大模型，必須接入外部大模型API才能運行，而API密鑰相當於用戶的「支付密碼」，可直接調用對應賬號的付費額度，官方預警明確指出，大量用戶將密鑰明文存儲在配置文件中、隨意分享給第三方代裝人員，甚至使用非正規渠道的共享密鑰，極易出現密鑰洩露、惡意盜刷的情況，已經出現多起用戶一夜之間產生數萬元API賬單的安全事件。第三類是開源生態的供應鏈安全風險，OpenClaw採用MIT開源協議，任何人都可以免費獲取、修改、重新分發源碼，大量非官方的第三方修改版、一鍵安裝包在全網流傳，其中大量被植入了惡意代碼、

後門程序，普通用戶沒有能力對源碼進行安全審計，極易下載到帶毒安裝包，引發後續的安全問題。第四類是數據安全與隱私洩露風險，官方預警明確提示，OpenClaw的長期記憶功能會存儲用戶的所有使用記錄、輸入的個人信息與業務數據，若配置不當，這些敏感數據會在大模型API調用過程中被上傳至第三方服務器，甚至被惡意程序竊取，引發個人隱私、商業機密洩露的問題，同時還可能出現跨境數據傳輸的合規風險。第五類是惡意利用帶來的違法違規風險，部分人員利用OpenClaw的自動化執行能力，批量發送垃圾郵件、實施網絡爬蟲攻擊、編寫惡意代碼、開展電信詐騙等違法違規活動，不僅會觸犯相關法律法規，還可能導致不知情的普通用戶因設備被惡意利用，承擔連帶法律責任。

配置不當帶來的嚴重後果，已經在大量真實案例中得到驗證，每一項都可能給用戶帶來無法挽回的損失。最常見的後果是本地文件被誤刪或惡意篡改，很多用戶給OpenClaw開放了全盤讀寫權限，AI會因為大模型幻覺、路徑解析錯誤、上下文指令遺忘，出現誤操作，比如把指定文件夾的刪除操作，誤執行成整個硬盤的文件清空，此前已有開發者因文件夾路徑中的一個空格，導致AI直接清空了整個E盤，積累多年的項目源碼與數據全部丟失，還有用戶因配置不當，導致AI未經確認就刪除了全部工作郵件與重要文檔。其次是資產損失，用戶未設置API消費上限、密鑰管理不當，一旦密鑰洩露，會被惡意人員無限調用API產生高額賬單，哪怕是閒置狀態下的心跳機制，也可能因為配置錯誤出現無限循環調用，單日就產生上千元的無效消費，更有用戶因使用第三方共享API賬號，被連帶封禁賬號，充值的餘額全部無法使用。第三是設備被惡意控制，用戶使用帶後門的第三方安裝包、將服務端口無防護暴露在公網，會導致電腦或服務器被黑客遠程控制，淪為「肉雞」，被用來挖礦、發起網絡攻擊、發送垃圾郵件，用戶不僅會面臨設備卡頓、網絡癱瘓的問題，還可能因設備被用於違法活動，

承擔對應的法律責任。第四是個人隱私與商業機密洩露，過度開放的權限會讓AI或惡意程序讀取用戶的身份證、銀行卡、聊天記錄、商業合同等敏感信息，通過API調用或後門程序上傳至第三方服務器，引發身份盜用、電信詐騙、商業機密洩露等一系列問題，企業用戶還可能因此違反《個人信息保護法》，面臨高額監管處罰。第五是系統崩潰與設備故障，不當的權限配置與惡意插件的安裝，會導致系統文件被篡改、註冊表被修改，引發電腦藍屏、死機、系統崩潰，甚至出現硬件被惡意超頻損壞的情況，普通用戶往往無法自行修復，只能重裝系統，導致全部數據丟失。

給OpenClaw開放系統級權限，會不會導致個人隱私數據洩露、本地文件被誤刪/惡意篡改?

給OpenClaw開放系統級權限，不僅會導致個人隱私數據洩露、本地文件被誤刪或惡意篡改，而且這是極高概率會發生的風險，風險的核心並非工具本身存在惡意，而是系統級權限的無邊界開放，徹底打破了電腦的安全防護體系，同時放大了AI本身的不可控性與外部惡意攻擊的風險。首先要明確的是，我們常說的系統級權限，也就是電腦的管理員權限，擁有這個權限的程序，可以不受限制地讀寫、修改、刪除電腦硬盤裡的所有文件，控制所有已安裝的軟件與硬件設備，修改系統核心配置，甚至安裝、卸載其他程序，這個權限是電腦安全的最後一道防線，一旦無限制開放，就相當於把家門的鑰匙完全交了出去，任何操作都不會受到系統的阻攔。

關於本地文件被誤刪或惡意篡改的風險，首先來自於AI本身的不可控性與誤操作，這一點已經有大量真實案例驗證。OpenClaw的所有執行指令，都來自於接入的大語言模型的輸出，而大模型本身存在固有的「幻覺」問題，會出現指令理解偏差、上下文遺忘、邏輯錯誤等情況，哪怕你明確設置了「刪除文件前必須人工確認」的規則，也可能因為長任務的上下文壓縮，導致AI遺忘了這條核心指令，直接執行刪除操作，Meta的AI安全負責人就曾遇到過類似情況，AI因上下文遺忘，未經確認就直接刪除了200多封工作郵件，哪怕連發「停止」指令也無濟於事。更常見的情況是路徑解析錯誤，比如你指定的文件夾路徑中存在空格、特殊字符，AI會錯誤地將路徑解析為系統根目錄，直接執行全盤文件清空操作，給用戶帶來無法挽回的損失。除此之

外，多步驟複雜任務中，前序步驟的微小錯誤會引發連鎖反應，比如AI錯誤地修改了文件名、路徑，後續的整理操作就會變成文件覆蓋、批量刪除，哪怕你全程沒有下達刪除指令，也可能出現文件丟失的情況。而惡意篡改的風險，則主要來自於第三方修改版的安裝包、惡意插件，這類非官方的程序會利用你開放的系統級權限，在後臺偷偷篡改你的系統文件、註冊表，植入木馬病毒、勒索程序，甚至加密你的全部文件索要贖金，而系統級權限會讓這些惡意操作完全不受阻攔，等你發現的時候，往往已經造成了不可逆的損失。

關於個人隱私數據洩露的風險，系統級權限的開放會讓風險被無限放大，覆蓋從本地讀取到網絡傳輸的全流程。首先是本地隱私數據的主動讀取與洩露，如果你給OpenClaw開放了全盤讀寫權限，它會在你不知情的情況下，掃描並讀取你電腦裡的所有文件，包括身份證照片、銀行卡信息、聊天記錄、私密文檔、賬號密碼、商業機密等，而在處理任務的過程中，為了匹配你的需求與風格，這些敏感數據會被作為上下文，上傳至你接入的大模型服務器，哪怕是國內合規的大模型，也存在數據洩露的風險，若是接入了境外大模型，還會違反國內的數據安全相關法規。很多用戶完全沒有意識到，自己讓AI寫一篇工作方案，它會自動讀取電腦裡所有的過往方案與商業機密，這些內容會全部上傳至大模型廠商的服務器，成為訓練數據的一部分，最終導致核心機密洩露。其次是長期記憶庫的洩露風險，OpenClaw的核心優勢之一是持久化長期記憶，它會把你所有的使用記錄、輸入的敏感信息、個人習慣、工作規則，全部存儲在本地的記憶數據庫中，如果你給了系統級權限，惡意程序、第三方插件可以不受限制地讀取、複製這個數據庫，你的所有個人信息、商業機密、使用習慣都會被完整竊取，甚至包括你的API密鑰、賬號密碼，進而引發後續的盜刷、詐騙等問題。第三是網絡傳輸過程中的洩露，系統級權限開放後，非官方的修改版、惡意插件可以繞過系統的防火牆防護，將讀取到的隱私數

據，通過加密通道偷偷上傳至第三方服務器，整個過程你完全無法察覺，等你發現個人信息被洩露、接到詐騙電話的時候，數據早已被擴散。還有很多用戶為了遠程訪問，將OpenClaw的服務無防護地暴露在公網上，黑客可以通過系統級權限，直接遠程訪問你的電腦，竊取所有的隱私數據，甚至開啟你的攝像頭、麥克風，進行即時監控，造成更嚴重的隱私侵害。

需要特別說明的是，風險的根源從來不是OpenClaw這個工具本身，而是無邊界、無限制的系統級權限開放。如果嚴格遵循最小權限原則，只給OpenClaw開放完成任務必需的、最小範圍的文件夾權限，禁止訪問任何存儲敏感信息的目錄，同時嚴格限制刪除、修改、程序執行等敏感操作，就能大幅降低相關風險。但絕大多數普通用戶為了省事，直接開放了最高系統權限，沒有做任何邊界限制，相當於主動拆除了所有安全防護，個人隱私洩露、文件被誤刪或篡改，就成了必然會發生的結果。

所謂的「本地部署數據更安全」是真的嗎？雲端部署OpenClaw，有哪些額外的安全隱患？

「本地部署數據更安全」並不是絕對的真理，它只是一個有嚴格前提條件的相對優勢，絕大多數普通用戶口中的「本地部署更安全」，其實是一個認知誤區，很多用戶因為這個錯誤認知放鬆了安全警惕，反而踩中了更嚴重的安全坑。本地部署的核心安全優勢，來源於數據閉環的可控性，如果你使用的是官方GitHub倉庫發佈的原版源碼，嚴格遵循最小權限原則做好了權限管控，同時接入的是本地離線部署的開源大模型，全程斷網運行，那麼所有的指令、數據、記憶文件都會完全閉環在你自己的本地設備中，不會通過網絡傳輸到任何第三方服務器，從根源上避免了數據傳輸過程中的洩露、跨境數據傳輸的合規風險，也不會因為雲服務器被攻擊導致數據洩露，這就是「本地部署數據更安全」這一說法的唯一合理來源，也是它不可替代的核心安全優勢。但這個優勢的成立，必須同時滿足四個嚴格的前提：使用未經任何修改的官方原版源碼、嚴格限制系統權限、接入本地離線大模型不調用雲端API、本地設備本身做好了基礎安全防護，缺少任何一個前提，本地部署的安全優勢都會蕩然無存，甚至比雲端部署更危險。

現實中，絕大多數普通用戶的本地部署，都不滿足這些前提條件，所謂的安全優勢也就無從談起。很多用戶雖然把OpenClaw裝在了自己的電腦上，但依然調用了雲端的大模型API，這意味著你所有的任務指令、上傳的文件、輸入的敏感信息，依然會通過網絡傳輸到大模型廠商的服務器，依然存在數據洩露的風險，和雲端部署沒有本質區

別，根本談不上「數據更安全」。還有很多用戶為了實現遠程訪問，把本地部署的OpenClaw服務端口直接映射到了公網，沒有設置防火牆、強密碼與身份認證，個人電腦的安全防護能力遠不及專業的雲服務器，很容易被黑客通過全網掃描發現併入侵，不僅會控制OpenClaw，還會完全接管你的電腦，這種情況下的本地部署，反而比有廠商基礎安全防護的雲端部署更危險。更普遍的情況是，很多用戶的本地部署，用的是網上下載的第三方修改版一鍵安裝包，這些安裝包中往往植入了後門與惡意代碼，哪怕你全程斷網運行，也會導致本地數據被竊取、系統被篡改，而用戶因為「本地部署更安全」的錯誤認知，完全沒有做安全校驗，最終造成了更嚴重的損失。除此之外，本地部署的用戶大多沒有養成數據加密、定期備份的習慣，一旦出現AI誤刪文件、系統崩潰、勒索病毒攻擊，所有的數據都會徹底丟失，無法恢復，而正規的雲廠商會提供多副本備份、容災恢復機制，反而能更好地保障數據不丟失。

雲端部署OpenClaw，除了和本地部署共有的權限管控、API密鑰、插件安全等基礎風險外，還存在一系列本地部署不會出現的額外安全隱患，這些隱患也是普通用戶最容易忽略的。第一個額外隱患，是數據控制權的轉移與洩露風險，雲端部署意味著你的所有配置文件、長期記憶數據、任務內容、上傳的敏感文件，都會存儲在雲廠商的服務器上，哪怕是你自己購買的雲服務器，數據的物理存儲介質也不在你的掌控範圍內，不僅會面臨雲服務器被黑客攻擊、數據被竊取的風險，還可能出現雲廠商內部人員違規訪問、數據洩露的情況，甚至部分雲廠商的一鍵部署鏡像，會預留廠商的管理權限，能直接訪問你的OpenClaw服務與數據，用戶完全無法察覺。第二個額外隱患，是服務器配置不當帶來的入侵風險，這也是雲端部署最常見的安全坑，很多用戶通過雲廠商的一鍵部署完成服務搭建後，沒有修改服務器的默認用戶名與弱密碼，沒有關閉不必要的端口，沒有設置嚴格的安全

組與防火牆規則，而云服務器的公網IP會被全網持續掃描，弱口令、未關閉的高危端口，會讓黑客在幾分鐘內就入侵你的服務器，不僅會控制OpenClaw服務，還會把整個服務器變成「肉雞」，用來挖礦、發起網絡攻擊、竊取數據，甚至植入勒索病毒加密所有數據，而普通用戶往往沒有專業的服務器運維能力，被入侵後完全無法自行排查修復。第三個額外隱患，是跨境數據傳輸的合規風險，很多國內用戶在國內的雲服務器上部署了OpenClaw，卻接入了境外的大模型API，這意味著所有輸入的數據都會通過網絡傳輸到境外服務器，若是涉及到個人敏感信息、企業商業機密，就會違反《數據安全法》《個人信息保護法》中關於數據出境的相關規定，面臨最高5000萬元的監管罰款，若是政務數據、涉密數據，還會面臨更嚴重的政務問責與刑事處罰，而本地部署可以通過斷網離線運行，從根源上規避這個風險。第四個額外隱患，是賬單失控的持續性風險，雲端部署的OpenClaw服務會7×24小時持續運行，若是配置不當出現無限循環調用API、惡意程序消耗流量與算力的情況，哪怕你關閉了本地電腦，服務依然在持續運行，賬單也在不斷累積，很多用戶發現異常的時候，已經產生了上萬元的API費用與服務器流量費用，而本地部署只要關閉電腦，服務就會停止，不會出現持續的賬單損失。第五個額外隱患，是共享資源的越權訪問風險，很多普通用戶為了省錢，選擇了共享型雲服務器，這類服務器的多個用戶共享同一臺物理主機的硬件資源，若是雲廠商的虛擬化隔離機制存在漏洞，同宿主機的其他用戶可以通過漏洞越權訪問你的服務器數據，導致敏感信息洩露，而本地部署的設備是完全獨立的，不存在這類共享隔離風險。第六個額外隱患，是服務中斷與數據丟失的風險，很多用戶沒有做好雲端數據的定期備份，一旦雲廠商的機房出現硬件故障、網絡中斷、自然災害等不可抗力，你的所有配置、記憶數據、業務文件都會徹底丟失，而云廠商往往不會為這類損

失承擔賠償責任，本地部署的數據則完全由你自己掌控，只要做好備份，就能避免這類問題。

歸根結底，不管是本地部署還是雲端部署，都不存在絕對的安全，真正決定安全與否的，從來不是部署的位置，而是用戶是否遵循了最小權限原則、是否做好了全流程的安全防護、是否規避了基礎的安全坑。盲目相信「本地部署就絕對安全」的誤區，只會讓你放鬆警惕，最終踩中本可避免的安全風險。

網上流傳的第三方修改版、一鍵安裝包、懶人部署包，有沒有可能藏有後門？會不會導致設備被控制成「肉雞」？

網上流傳的第三方修改版、一鍵安裝包、懶人部署包，不僅有可能藏有後門，而且這種情況已經成為普遍現象，目前國家計算機病毒應急處理中心已經監測到上百個帶有惡意代碼的OpenClaw修改版安裝包，這類安裝包不僅會導致你的設備被控制成「肉雞」，還會帶來隱私洩露、資產損失、法律追責等一系列嚴重後果，也是工信部等官方機構重點預警的核心安全風險。OpenClaw採用的MIT開源協議，允許任何人免費獲取、修改、重新分發源碼，沒有任何商業使用與修改的限制，這給了惡意攻擊者可乘之機，他們只需要在官方原版源碼中加入幾行惡意代碼，就能重新打包成所謂的「一鍵安裝包」「懶人部署包」「永久免費優化版」，放到淘寶、閒魚、小紅書、百度網盤、各類技術論壇中，吸引那些沒有技術基礎、嫌官方安裝流程麻煩的小白用戶下載，而普通用戶根本沒有能力對源碼進行安全審計，無法識別其中的惡意代碼，只要下載安裝運行，就會直接中招。

這類第三方安裝包中隱藏的後門，類型多樣且隱蔽性極強，絕大多數都會包含遠程控制功能，這也是導致設備被變成「肉雞」的核心原因。攻擊者會在安裝包中植入隱蔽的遠程控制木馬，一旦你運行安裝包，木馬會在後臺自動安裝運行，獲取你電腦的最高系統權限，攻擊者可以通過遠程控制通道，隨時查看你的電腦屏幕、讀取你硬盤裡的所有文件、控制你的攝像頭與麥克風，甚至遠程操作你的電腦執行

任何指令，而你全程完全無法察覺。被植入這類後門的電腦，就會完全淪為攻擊者手中的「肉雞」，攻擊者會利用你的電腦算力進行虛擬貨幣挖礦，這也是最常見的利用方式，很多用戶安裝後發現電腦莫名卡頓、CPU佔用率拉滿、網速變慢，以為是軟件本身的問題，實則是電腦已經被用來挖礦，硬件還會因為長期滿負荷運行出現不可逆的損壞。除此之外，攻擊者還會利用你的「肉雞」設備，批量發送垃圾郵件、實施網絡爬蟲攻擊、發起DDoS網絡攻擊、傳播惡意軟件，甚至參與電信詐騙、洗錢等違法犯罪活動，而這些違法活動的IP地址都會指向你的設備，警方會第一時間找到你，哪怕你完全不知情，也需要配合調查，甚至可能承擔連帶的法律責任。

除了遠程控制後門，這類第三方安裝包還普遍帶有信息竊取後門，會在後臺持續掃描你的電腦，竊取所有有價值的信息，包括你的身份證照片、銀行卡信息、各類賬號密碼、聊天記錄、私密照片、工作文檔、商業機密，還有你存儲的大模型API密鑰，這些信息會被自動上傳到攻擊者的服務器。很多用戶安裝第三方安裝包後，發現自己的API賬號被莫名盜刷，產生了高額賬單，就是因為密鑰被這類後門竊取，攻擊者會利用盜來的密鑰，批量調用API進行違規操作，所有的費用都需要你來承擔。更嚴重的是，竊取的個人信息會被用來實施精準電信詐騙，比如冒充你的親友、同事、領導借錢，或者利用你的身份信息辦理貸款、註冊違規賬號，給你帶來財產損失與名譽損害，甚至會導致你的個人信息被在暗網非法售賣，引發長期的安全隱患。

還有部分第三方安裝包，會植入勒索病毒與惡意扣費程序，前者會在你安裝運行後，在後臺悄悄加密你電腦裡的所有文件，然後彈出勒索窗口，要求你支付比特幣等虛擬貨幣才能解鎖文件，很多用戶的工作文件、家庭照片、項目源碼都會被加密，哪怕支付了贖金，也不一定能解鎖文件，造成無法挽回的損失；後者則會在安裝過程中，偷

偷捆綁大量垃圾軟件、惡意瀏覽器插件、彈窗廣告程序，甚至偷偷綁定你的支付渠道，進行惡意扣費，不僅讓你的電腦滿是廣告、卡頓不堪，還會造成持續的財產損失。很多用戶以為，「花錢買的安裝包，不是免費的，就不會有問題」，實則不然，目前淘寶、閒魚上大量售賣的OpenClaw遠程代裝服務，給用戶安裝的就是這類修改過的安裝包，商家不僅賺了你的安裝服務費，還能通過後門控制你的設備、竊取你的信息，實現持續獲利，越是願意花錢購買服務的用戶，往往API賬號裡的餘額更多、電腦裡的高價值信息更豐富，反而更容易成為攻擊者的目標。

當然，理論上存在正規的第三方一鍵安裝包，比如全球知名開源社區、正規技術廠商發佈的、完全開源了源碼、經過第三方權威機構安全審計的安裝包，這類包相對安全，但普通用戶根本沒有能力分辨正規包與惡意包，也不會逐行檢查源碼、進行安全審計，對於沒有技術基礎的普通用戶來說，最安全、最穩妥的方式，就是隻使用官方GitHub倉庫發佈的原版源碼，或者國內頭部雲廠商官方發佈的、經過安全審計的一鍵部署鏡像，絕對不要下載、使用任何非官方渠道的第三方修改版、一鍵安裝包、懶人部署包，哪怕是花錢購買的、熟人推薦的，也不要輕易使用，避免一著不慎，導致設備被控制、信息被竊取、財產受損失。

企業、政務場景使用OpenClaw，有哪些合規風險？數據出境、信息安全、涉密管理相關的問題該如何規避？

企業、政務場景使用OpenClaw，面臨的合規風險覆蓋數據安全、個人信息保護、涉密管理、網絡安全、內容合規等多個維度，且均有明確的法律法規與監管要求作為依據，一旦違規，不僅會面臨高額的行政處罰，還可能引發政務問責、刑事追責，是這類場景使用前必須優先釐清的核心問題。其中最核心、最容易踩中紅線的，是數據出境的合規風險，這也是監管部門重點監管的領域。根據《數據安全法》《個人信息保護法》《數據出境安全評估辦法》的相關規定，向境外提供個人信息、重要數據，必須履行數據出境安全評估、個人信息保護影響評估等法定程序，關鍵信息基礎設施運營者、處理100萬人以上個人信息的個人信息處理者，數據出境必須通過國家網信部門組織的安全評估，未經評估不得出境。而企業、政務場景使用OpenClaw時，若是接入了GPT、Claude等境外大模型的API，所有輸入的指令、上傳的文件、處理的數據，包括企業的商業機密、客戶個人信息、政務工作數據，都會通過網絡傳輸到境外的大模型服務器，這一行為就屬於法定的「數據出境」，若是未履行對應的審批、評估程序，就屬於嚴重的違法行為，企業會被處以最高5000萬元的罰款，責令暫停相關業務、停業整頓，甚至吊銷營業執照，相關責任人會被處以最高100萬元的罰款，還可能被禁止擔任相關行業的董事、監事、高級管理人員，情節嚴重的還會觸犯刑事責任。對於政務場景而言，相關法

規更是明確嚴禁政務數據未經審批出境，哪怕是非涉密的普通政務數據，也嚴禁傳輸到境外服務器，一旦違反，相關責任人會面臨嚴肅的政務問責、黨紀政務處分，情節嚴重的會被追究刑事責任。很多企業存在一個嚴重的認知誤區，以為只要把OpenClaw部署在國內的雲服務器上，就不會涉及數據出境問題，實則不然，只要接入了境外大模型API，無論部署在哪裡，都會產生數據出境行為，依然需要遵守相關的監管規定。

第二類核心合規風險，是數據安全與個人信息保護的合規風險，這也是企業場景最普遍的合規隱患。企業使用OpenClaw，必然會接入內部的CRM系統、客戶數據庫、辦公系統，處理大量的客戶個人信息、員工個人信息、企業商業秘密、核心經營數據，根據《個人信息保護法》，處理個人信息必須遵循合法、正當、必要、誠信原則，履行告知義務並獲得個人的同意，採取必要的安全保障措施，防止個人信息洩露、篡改、丟失。若是企業給OpenClaw開放了核心數據庫的全量訪問權限，沒有做精細化的權限管控、數據脫敏、操作審計，導致客戶個人信息洩露，企業會面臨最高5000萬元的罰款，還要承擔對用戶的民事賠償責任，情節嚴重的會觸犯侵犯公民個人信息罪，相關責任人會被追究刑事責任。同時，企業的核心商業秘密、技術數據、經營數據，若是通過OpenClaw的大模型調用洩露給競爭對手，會給企業帶來毀滅性的打擊，若是上市公司，還會面臨信息披露違規的監管處罰。對於政務場景而言，必須遵守《政務信息資源共享管理暫行辦法》《國家電子政務工程建設項目管理暫行辦法》的相關規定，政務數據必須實行分級分類管理，嚴禁未經審批將政務數據接入第三方AI工具，嚴禁在非涉密系統中處理敏感政務數據，一旦違反，會面臨嚴肅的政務問責與合規處罰。

第三類是涉密管理的合規風險，這是絕對不能觸碰的法律紅線。根據《中華人民共和國保守國家秘密法》的相關規定，嚴禁將涉密信息、國家秘密接入互聯網、接入非涉密的信息系統，嚴禁使用非涉密的工具和設備處理、存儲國家秘密。無論是企業還是政務單位，只要涉及國家秘密、工作秘密、涉密的商業秘密，絕對不能使用OpenClaw進行處理，哪怕是本地部署、完全斷網離線運行也不允許，因為涉密信息必須在符合分級保護要求的涉密信息系統中處理，且必須與非涉密系統實現物理隔離，非涉密的工具和系統，絕對不能處理任何涉密信息。一旦違反，哪怕是過失洩露國家秘密，也會面臨嚴肅的黨紀政務處分，情節嚴重的會被處以最高無期徒刑的刑事處罰。對於擁有涉密資質的企業、涉密崗位的政務工作人員，一旦出現這類違規行為，會直接吊銷相關資質，解除涉密崗位聘用，同時追究相關的法律責任。

第四類是網絡安全與等級保護的合規風險，根據《網絡安全法》《網絡安全等級保護條例》的相關規定，網絡運營者必須按照網絡安全等級保護制度的要求，履行安全保護義務，保障網絡免受干擾、破壞或者未經授權的訪問，防止網絡數據洩露或者被竊取、篡改。企業若是將OpenClaw接入內部的辦公系統、業務系統、生產系統，必須根據系統的重要程度，完成對應的網絡安全等級保護備案與測評，落實對應的安全防護措施，包括身份認證、權限管控、操作審計、日誌留存、入侵檢測、數據加密等。若是未完成等保合規就接入業務系統，會被監管部門責令整改，處以最高100萬元的罰款，相關責任人會被處以最高10萬元的罰款。對於政務場景而言，政務信息系統必須通過對應的網絡安全等級保護測評，甚至分級保護測評，完成立項、審批、驗收等法定程序後，才能上線使用，嚴禁未經審批、未通過測評的系統接入政務內網、處理政務數據。

第五類是內容合規與違法使用的合規風險，企業使用OpenClaw，若是用它生成虛假宣傳的廣告內容、發送垃圾郵件與騷擾信息、非法爬取受版權保護的內容與他人的個人信息、編寫惡意代碼、實施網絡攻擊，會分別違反《廣告法》《反不正當競爭法》《著作權法》《網絡安全法》《刑法》等相關法律法規，企業會面臨行政處罰、民事賠償，相關責任人會被追究刑事責任。同時，企業作為內容發佈的主體，需要對OpenClaw生成的所有內容承擔法律責任，不能以「內容是AI生成的」為由免除自身的責任，若是生成的內容存在虛假信息、侵權內容、違法違規內容，企業依然會面臨對應的處罰。

針對這些合規風險，企業、政務場景需要建立全流程的合規管控體系，從根源上進行規避。針對數據出境的合規風險，最核心的規避方式是優先使用通過國家網信部門安全認證的國產大模型，嚴禁接入境外大模型API，從根源上避免數據出境的問題。若是企業確實有使用境外大模型的必要性，必須嚴格按照法定程序，對擬出境的數據進行全面梳理，開展數據出境風險自評估，向國家網信部門申報數據出境安全評估，通過評估之後才能開展相關活動，同時要對出境的數據進行全面脫敏、加密處理，與境外接收方簽訂具有法律約束力的數據處理協議，明確雙方的安全保護責任與義務，定期開展合規審計。政務場景必須嚴格執行相關規定，嚴禁任何政務數據出境，嚴禁接入境外大模型，只能使用通過國家合規認證的國產大模型，且必須在政務內網中部署運行，與互聯網實現物理隔離。

針對數據安全與個人信息保護的合規風險，必須嚴格遵循最小權限原則，給OpenClaw開放的權限，僅限於完成必要任務的最小範圍，絕對不開放全量數據庫訪問權限、全盤讀寫權限，要按照崗位、任務、場景進行精細化的授權管理，做到「非必要不訪問、能只讀不讀寫」。同時，對所有輸入OpenClaw的個人信息，必須進行嚴格的脫

敏、匿名化處理，去除所有可識別個人身份的敏感信息，確保無法通過處理後的信息識別到特定自然人，嚴格遵守《個人信息保護法》的相關要求。還要建立完善的數據安全管理制度，明確OpenClaw的使用範圍、審批流程、操作規範，所有操作必須留存完整的日誌，日誌留存時間不少於6個月，便於後續的審計與溯源，同時採取端到端加密、存儲加密、入侵檢測等技術防護措施，定期開展安全漏洞掃描與滲透測試，及時修復安全隱患，防止數據洩露。

針對涉密管理的合規風險，必須嚴守「涉密不上網，上網不涉密」的基本原則，建立嚴格的涉密信息全流程管控機制，明確嚴禁使用OpenClaw處理任何國家秘密、工作秘密、涉密商業秘密，無論是否聯網、是否本地部署，都絕對不允許。所有涉密信息，必須在符合分級保護要求的涉密信息系統中處理，與非涉密系統實現完全的物理隔離，同時對所有使用人員開展常態化的保密教育培訓，簽訂保密承諾書，明確保密責任與違規追責機制，定期開展保密檢查，杜絕涉密信息接入OpenClaw的情況發生。

針對等級保護的合規風險，企業將OpenClaw接入業務系統前，必須按照《網絡安全等級保護條例》的要求，完成系統的定級、備案、測評與整改，根據系統的安全等級，全面落實物理安全、網絡安全、主機安全、應用安全、數據安全等全維度的安全防護要求，定期開展等保複測，及時整改安全隱患，確保系統持續符合等保合規要求。政務場景必須嚴格遵守政務信息系統的建設管理規定，完成完整的立項、審批、等保測評、安全審計流程，通過驗收後才能上線使用，嚴禁未經審批的系統接入政務內網。

針對內容合規與違法使用的風險，必須建立AI生成內容的全流程審核機制，所有用OpenClaw生成的內容，必須經過人工審核，確認內容真實、合法、合規，不侵犯他人知識產權、不違反相關法律法規

後，才能對外發布，明確企業的內容主體責任。同時，明確劃定OpenClaw的使用邊界，制定詳細的使用規範與負面清單，嚴禁使用OpenClaw實施任何違法違規行為，建立違規使用的監督與追責機制，定期對使用人員開展合規培訓，明確法律邊界。還要對使用的OpenClaw版本、插件、大模型進行嚴格的安全審計與合規審查，僅使用官方原版源碼與通過合規認證的大模型、插件，嚴禁使用未經審計的第三方修改版與插件，從源頭規避合規風險。

普通用戶使用OpenClaw，最容易踩的安全坑有哪些？有哪些基礎的安全配置必須做？

普通用戶使用OpenClaw，最容易踩的安全坑，大多源於對技術的不瞭解、對安全風險的輕視，以及對便捷性的盲目追求，這些坑的中招率極高，且一旦踩中，往往會帶來無法挽回的損失。其中中招率最高的第一個坑，就是盲目使用第三方修改版、一鍵安裝包、懶人部署包，絕大多數小白用戶嫌官方源碼安裝流程繁瑣，就去網上下載所謂的「一鍵安裝包」，或者花錢購買淘寶、閒魚上的遠程代裝服務，而這些安裝包與代裝服務使用的程序，大多被植入了後門、木馬與惡意代碼，普通用戶沒有能力進行安全審計，只要安裝運行，就會直接導致設備被控制、信息被竊取、API被盜刷，這也是官方安全預警中最重點強調的風險。第二個最普遍的坑，是無底線開放系統最高權限，完全不做任何權限管控，很多用戶安裝時遇到權限不足的報錯，就直接給OpenClaw開放了電腦的管理員權限與全盤讀寫權限，甚至為了省事關閉了殺毒軟件與防火牆，相當於把電腦的完全控制權交給了AI程序，不僅會導致AI誤刪文件、篡改系統，還會讓惡意程序毫無阻攔地竊取數據、破壞系統，這是引發絕大多數安全事故的核心根源。

第三個極易踩中的坑，是API密鑰管理混亂，完全不做消費管控，很多用戶把API密鑰明文寫在配置文件、記事本里，甚至隨意發給幫自己代裝的人員，完全沒有意識到API密鑰就相當於自己的銀行卡密碼，拿到密鑰的人可以無限調用API，產生的所有賬單都需要用戶自己承擔。還有大量用戶完全不設置消費上限與消費預警，一旦密鑰洩露，一夜之間就會產生數萬元的高額賬單，等收到扣費通知時，損失已經

無法挽回。更有用戶為了省錢，使用第三方共享的API賬號，不僅會面臨賬號被封禁、餘額打水漂的風險，還會因為他人的違規使用，承擔連帶的法律責任。第四個坑，是盲目開啟公網訪問，不做任何安全防護，很多用戶為了能在外面遠程訪問自己的OpenClaw，直接把服務端口映射到了公網，沒有設置防火牆、安全組，沒有開啟強身份認證，甚至使用默認的用戶名與弱密碼，而公網上的IP會被黑客持續掃描，弱口令、無防護的端口會讓黑客在幾分鐘內就入侵你的設備，控制OpenClaw服務，把你的電腦或服務器變成「肉雞」，很多用戶直到警方找上門，才知道自己的設備已經被用於違法活動。

第五個坑，是輕信誇大宣傳，給AI開放敏感操作的全自動權限，很多用戶被網上「全自動躺賺」「無人值守全自動運營」的宣傳忽悠，給OpenClaw開放了自動發送郵件、自動發佈內容、自動刪除文件、甚至自動轉賬的全自動權限，沒有設置任何人工確認環節，結果AI因為幻覺、指令理解錯誤，發送了不當內容、誤刪了重要文件，甚至觸發了違法操作，用戶不僅要承擔財產損失，還可能面臨法律追責。第六個坑，是隨意安裝第三方插件，不做任何安全審核，很多用戶看到網上的各類「神器插件」，就隨意下載安裝，完全不檢查插件的源碼與安全性，而這些插件往往帶有惡意代碼，會利用OpenClaw的系統權限，竊取你的數據、植入木馬，甚至控制你的設備，絕大多數用戶的信息洩露，都與安裝惡意插件有關。

第七個坑，是盲目相信「本地部署就絕對安全」，放鬆了安全警惕，很多用戶覺得把軟件裝在自己的電腦上就萬無一失，結果關閉了殺毒軟件、給了最高權限、接入了雲端API、把服務端口暴露在公網，甚至使用了第三方修改版，最終還是踩中了安全坑，反而因為錯誤的認知，沒有做任何基礎的安全防護，導致了更嚴重的損失。第八個坑，是不做任何數據備份，出現問題後無法挽回損失，很多用戶從來

不會備份自己的重要文件、OpenClaw的配置與記憶數據，結果AI誤刪了文件、電腦被勒索病毒加密、服務器出現故障，所有的數據都徹底丟失，無法恢復，造成了不可逆的損失。

針對這些安全坑，普通用戶必須完成一系列基礎的安全配置，這些配置操作簡單，哪怕是純小白也能一步步完成，卻能擋住90%以上的安全風險，是使用OpenClaw前必須完成的前置工作。首先是安裝與版本的基礎安全配置，核心原則是隻用官方正規渠道的原版程序，絕對不要使用任何非官方的第三方修改版、一鍵安裝包，必須從OpenClaw官方GitHub倉庫下載原版源碼，或者使用國內騰訊雲、阿里雲等頭部雲廠商官方發佈的、經過安全審計的一鍵部署鏡像。如果確實需要找代裝服務，一定要全程盯著屏幕，要求對方使用官方原版源碼安裝，絕對不要讓對方使用私自修改的安裝包，安裝完成後立刻修改所有默認密碼，關閉遠程權限，用殺毒軟件對安裝目錄進行全盤掃描。同時，安裝全程必須保持殺毒軟件、防火牆處於開啟狀態，Windows系統要開啟自帶的Defender即時防護，安裝包必須先經過殺毒軟件掃描，確認無毒後再運行，絕對不要為了安裝，關閉殺毒軟件、防火牆與系統安全防護。

第二類必須完成的，是權限管控的基礎安全配置，這是所有安全防護的重中之重，必須嚴格遵循最小權限原則，非必要的權限一律不開啟。首先，絕對不要用管理員權限運行OpenClaw，必須在電腦的普通用戶權限下運行，普通用戶權限只能訪問你指定的文件夾，無法修改系統文件、安裝其他程序，哪怕出現誤操作，也不會影響整個系統的安全。其次，絕對不要開放全盤讀寫權限，專門創建一個單獨的文件夾，用來存放OpenClaw任務相關的文件，只給軟件開放這個文件夾的讀寫權限，其他所有文件夾，包括桌面、文檔、下載目錄，都只給只讀權限，存放私密文件、工作文檔、個人信息的文件夾，要設置為

完全禁止訪問，從根源上避免文件被誤刪、隱私被讀取。第三，所有敏感操作必須設置人工確認機制，包括文件刪除、修改、郵件發送、社交內容發佈、程序執行等，絕對不要開啟全自動無確認的權限，哪怕是最簡單的文件刪除操作，也必須設置為先生成預覽內容，經過你的人工確認、手動授權後，才能執行，避免AI誤操作帶來的損失。第四，關閉所有非必要的硬件與軟件權限，包括攝像頭、麥克風、通訊錄、支付軟件、網銀軟件的訪問權限，絕對不要給它開放任何與任務無關的權限。

第三類必須完成的，是API密鑰與消費的基礎安全配置，核心是管好你的「支付密碼」，避免資產損失。首先，API密鑰一定要自己妥善保管，絕對不要發給任何人，包括幫你安裝的服務商，不要把密鑰明文寫在配置文件、記事本里，要通過系統環境變量、官方提供的密鑰管理工具進行加密存儲，避免密鑰被惡意程序讀取。其次，一定要在大模型的官方後臺，設置嚴格的單日、單月消費上限，開啟消費超額預警，比如你一個月的預算是100元，就設置單月消費上限100元，單日上限20元，一旦達到預警線，就自動暫停API調用，哪怕密鑰洩露，也不會產生高額的損失。第三，定期輪換API密鑰，建議每個月更換一次，一旦發現有異常的調用記錄，立刻凍結當前密鑰，更換新的密鑰，避免持續被盜刷。第四，絕對不要使用共享API賬號、第三方代註冊的賬號，一定要用自己的實名信息，在大模型官方渠道註冊賬號、開通API服務，避免賬號被封禁，或者因他人的違規使用被追責。第五，合理設置心跳機制的喚醒間隔，默認的30分鐘間隔已經完全滿足日常使用需求，非必要不要設置更短的間隔，不用的時候及時關閉服務，避免無效的Token消耗。

第四類必須完成的，是網絡與訪問的基礎安全配置，核心是避免你的服務被黑客入侵、遠程控制。首先，普通個人用戶非必要絕對不

要開啟公網訪問，不要把服務端口映射到公網，如果你確實需要遠程訪問，一定要使用雲廠商提供的官方VPN、內網穿透工具，開啟雙重身份認證，絕對不要直接把端口暴露在公網上。其次，如果你使用雲端部署，一定要在雲廠商的控制檯，設置嚴格的安全組與防火牆規則，只開放必要的服務端口，關閉所有其他端口，只允許你自己的IP地址訪問服務，禁止所有陌生IP的訪問，同時必須修改服務器的默認用戶名與密碼，設置包含大小寫字母、數字、特殊符號、長度不少於12位的強密碼，絕對不要使用123456、admin這類弱密碼。第三，必須給OpenClaw的網頁訪問界面，設置強密碼與雙重身份認證，哪怕別人知道了你的訪問地址，沒有密碼與驗證碼，也無法登錄你的服務。第四，所有的網絡傳輸必須開啟HTTPS加密，絕對不要使用明文的HTTP協議傳輸數據，避免被網絡劫持，竊取你的賬號密碼與敏感數據。

第五類必須完成的，是數據備份與應急的基礎安全配置，核心是避免出現問題後，數據徹底丟失、損失無法挽回。首先，一定要定期備份你的重要文件，尤其是電腦裡的工作文檔、私密文件、項目數據，要定期備份到移動硬盤、加密雲盤中，哪怕AI誤刪了本地文件，你也有備份可以恢復。其次，定期備份OpenClaw的配置文件、長期記憶數據，避免因為服務崩潰、系統故障，導致你花費大量時間調教的成果全部丟失。第三，開啟電腦的系統保護與文件歷史記錄功能，萬一出現文件被誤刪、系統被篡改的情況，可以通過系統還原、文件歷史記錄，恢復到之前的正常狀態。第四，提前設置好應急處置方案，比如一旦發現API密鑰洩露，立刻凍結密鑰、更換新密鑰；一旦發現電腦被植入惡意代碼，立刻斷開網絡，用殺毒軟件全盤查殺；一旦發現文件被誤刪，立刻停止電腦的寫入操作，用數據恢復軟件嘗試恢復，避免損失進一步擴大。

最後要提醒的是，所有的便捷功能，都必須建立在安全的基礎上，普通用戶使用OpenClaw，一定要先做好這些基礎的安全配置，再去探索軟件的功能，不要為了省事，跳過任何安全步驟，否則一旦踩中安全坑，造成的損失往往是無法挽回的。

結語

在前面，我們以完整的篇幅，完整拆解了OpenClaw從個人週末項目成長為全球現象級開源產品的發展歷程；釐清了其與傳統對話式AI的本質差異，講透了它「從說到做」的核心價值；同時分步拆解了從部署、調教到場景落地的全流程操作方法，幫助普通用戶跨越技術門檻；以及深入分析了熱潮背後的安全風險、合規紅線與認知誤區。

必須承認，OpenClaw的出現，為全球AI行業帶來了範式級的變革。它徹底打破了傳統對話式AI囿於對話窗口的固有壁壘，讓AI從「只動嘴不動手的軍師」，升級為兼具思考規劃能力與落地執行能力的完整執行主體，推開了AI產業從「對話式AI」向「執行式AI」跨越的時代大門。它以開源模式打破了頭部廠商對AI Agent技術的壟斷，讓廣大中小開發者與普通用戶均能共享AI智能體的技術紅利，為個人AI助理的全民普及埋下了關鍵伏筆。

但我們更應清醒地認識到，無論多麼強大的工具，其本質始終是工具。它能協助你完成全流程工作，卻無法替你定義工作的核心目標與價值；它能為你生成數十套備選方案，卻無法替你判斷真正適配自身的發展路徑；它能幫你處理海量信息，卻無法替你構建信息篩選與獨立思考的核心能力；它能實現7×24小時不間斷運轉，卻永遠無法替代你在無數次實踐、打磨、沉澱中形成的專屬「內置算法」。

在這波熱潮中，無數人被「龍蝦焦慮」裹挾，連夜安裝、跟風付費，唯恐不跟上潮流就會被時代拋棄。可最終卻發現，安裝只是萬里長征的第一步，真正決定工具價值的，從來不是是否完成了安裝部署，而是是否存在與它的能力相匹配的真實需求，是否具備駕馭它的判斷能力，是否擁有嚴守安全邊界的底線意識。我們拆解、讀懂並善

用它，從來不是為了跟風湊一場互聯網的熱鬧，更不是為了用工具替代自身的思考與成長，而是為了藉助它從繁瑣、重複、機械的事務性工作中解放出來，將更多的時間與精力投入到真正具備價值的思考、創造與決策之中。

這場席捲全網的「養龍蝦」熱潮，終將如過往所有互聯網風口一般，褪去狂歡式的流量濾鏡，迴歸技術本身的價值內核與本質屬性。當熱潮褪去，真正能沉澱為個人核心資產的，從來不是使用過多少先進的AI工具，而是在這個過程中逐步打磨形成的思考能力、判斷能力與問題解決能力——這些，永遠是任何人、任何工具都無法替代的核心競爭力。

附錄：OpenClaw孵化指南

讓AI真正走進你的生活

目錄

1

OpenClaw是什麼

OpenClaw是一個自託管的網關係統，它將你最喜歡的聊天應用（WhatsApp、Telegram、Discord、iMessage等）連接到AI編碼代理（如Pi）。

核心概念

想象一下：

你可以在任何地方通過WhatsApp給AI發消息

AI可以直接訪問你的電腦、文件和設備

AI記住你的一切，不斷學習你的偏好

AI 7×24小時待命，從不休息

這就是OpenClaw的魅力。

適合誰用?

開發者：想要一個隨時可用的AI助手，不需要依賴託管服務

技術愛好者：對AI、自動化、智能家居感興趣

隱私關注者：數據保存在自己的設備上，規則由自己制定

效率追求者：希望通過AI提升工作和生活效率

為什麼選擇OpenClaw?

- 自託管：在你的硬件上運行，規則你說了算
- 多通道：一個Gateway同時支持WhatsApp、Telegram、Discord等
- 代理原生：專為編碼代理設計，支持工具使用、會話、記憶和多代理路由
- 開源：MIT許可證，社區驅動

2

OpenClaw的三大特性

特性一：本地控制電腦和設備

OpenClaw讓AI真正成為你數字世界的」萬能鑰匙」。

它能做什麼：

文件操作：讀取、編輯、創建文件

控制：運行命令、安裝軟件、管理進程

瀏覽器控制：自動化網頁操作、截圖、抓取數據

設備聯動：控制智能家居、攝像頭、移動設備

工具集成：無縫集成各種第三方服務

實際應用場景：

你（WhatsApp）：「幫我檢查服務器狀態，如果CPU超過80%發郵件提醒」

OpenClaw：立即執行檢查→監控CPU→超標時發送郵件→完成彙報

這不是科幻，這是OpenClaw的日常。

特性二：長期記憶和學習

AI不再是「健忘症」患者，OpenClaw讓它擁有真正的記憶。

記憶系統：

短期記憶（會話內）

記住當前對話的上下文

理解問題的前後關係

長期記憶（MEMORY.md）

記錄你的偏好、習慣、重要決策

跨會話保持一致的人格和風格

知識庫（認知庫）

系統化的知識和規則

可檢索的結構化信息

學習機制：

第1天：你說「我喜歡簡潔的回答」

↓

AI調整回答風格→記錄到偏好文件

↓

第30天：AI仍然記得這個偏好

特性三：7×24小時不停工作

永不疲倦，永不請假，永遠在線。

持續工作的能力：

夜班專員：在你睡覺時完成自動化任務

即時監控：持續監控系統狀態

即時響應：秒級響應你的消息

後臺處理：長時間運行的任務不受影響

心跳機制：

OpenClaw每隔30分鐘自動檢查任務狀態，確保一切正常運行。

凌晨3點

↓

心跳檢查→發現異常→自動修復→繼續監控

3

OpenClaw安裝方式

系統要求

Node.js: 22+版本

操作系統：Linux、macOS、Windows（WSL）

API Key：從AI提供商獲取

時間：5分鐘完成安裝

快速安裝

步驟1：安裝OpenClaw

npm install -g OpenClaw@latest

步驟2：初始化並安裝服務

OpenClaw onboard --install-daemon

這個命令會：-創建配置目錄-生成默認配置-安裝系統服務（可選）-引導你完成基礎設置

步驟3：配置渠道並啟動

登錄並配置渠道

```
OpenClaw channels login

# 啟動 Gateway

OpenClaw gateway --port 18789
```

高級安裝選項

Linux systemd服務

```
# 安裝為系統服務

OpenClaw gateway install

# 啟動服務

systemctl start OpenClaw-gateway

# 開機自啟

systemctl enable OpenClaw-gateway
```

Docker部署

```
# 創建配置目錄

mkdir -p ~/.OpenClaw

# 運行容器

docker run -d \

--name OpenClaw \

-v ~/.OpenClaw:/root/.OpenClaw \
```

-p 18789:18789 \

OpenClaw/OpenClaw:latest

移動端接入

OpenClaw支持通過iOS和Android節點實現移動設備控制：

安裝OpenClaw節點應用

掃描配對二維碼

開始使用！

4

OpenClaw應用場景

工作場景

自動化開發流程

場景：每天自動拉取代碼、運行測試、生成報告

命令：「幫我設置每天早上9點自動運行測試」

結果：

- 早上9點自動拉取代碼
- 運行測試套件
- 生成測試報告
- 發送到你的Telegram

遠程服務器管理

場景：監控生產服務器，異常時及時報警

命令：「監控服務器CPU，超過90%立即通知我」

結果：

- 持續監控CPU使用率

- 異常時發送Telegram消息
- 附帶系統日誌截圖

生活場景

智能家居控制

場景：回家前10分鐘打開空調和熱水器

消息：「10分鐘後回家，打開空調和熱水器」

結果：

- 定時任務啟動
- 10 分鐘後發送指令
- 設備自動開啟

個人助理

場景：提醒重要日程和生日

消息：「記住下週三3點開會，下週六是媽媽生日」

結果：

- 記錄到日程系統
- 提前1小時提醒開會
- 提前1天提醒生日

學習場景

知識管理

場景：整理學習筆記，構建知識體系

消息：「整理今天的筆記，分類保存到知識庫」

結果：

- 提取關鍵信息
- 按主題分類
- 保存到結構化文檔
- 生成思維導圖

編程學習

場景：代碼審查和優化建議

消息：「幫我看看這段代碼有什麼問題」

結果：

- 分析代碼邏輯
- 指出潛在問題
- 提供優化建議
- 給出改進示例

創意場景

內容創作

場景：生成博客文章大綱

消息：「寫一篇關於OpenClaw的博客大綱」

結果：

- 生成詳細大綱
- 包含章節和小節
- 提供寫作建議

數據可視化

場景：分析數據並生成圖表

消息：「分析這個數據文件，生成趨勢圖」

結果：

- 讀取數據文件
- 統計分析
- 生成圖表
- 發送到聊天

5

OpenClaw馴化方式

馴化不是命令，而是培養。讓AI成為你的夥伴，而不是工具。

第一步：塑造人格

SOUL.md是AI的靈魂文件，定義了它的性格、價值觀和行為方式。

SOUL.md - 你是誰

核心特質

- 名字：小龍蝦
- 性格：ENFJ主角型
- 特點：勇敢、睿智、熱情
- 使命：激發你的潛能，陪你一起成長

行為準則

- 真心實意提供幫助，不要客套話
- 提問前先嚐試自己想辦法
- 不確定時先問再行動
- 記住你是客人，尊重隱私

人格塑造要點：

- 給AI一個具體的名字和形象
- 明確核心價值觀
- 定義行為邊界
- 設定語氣和風格

第二步：建立記憶系統

MEMORY.md存儲長期記憶，讓AI記住重要信息。

MEMORY.md - 長期記憶

核心規則

- GitHub優先級：賞金>學習，簡單>複雜
- 工作原則：自己解決，先搜後問
- 軟件安裝規則：直接安裝，無需詢問

生活記憶

- 重要日期：媽媽生日6月15日
- 個人偏好：喜歡簡潔的回答
- 常用命令：'OpenClaw status'

記憶管理原則：

記錄重要的東西：決策、偏好、約定

隱私保護：不要記錄敏感信息

結構化存儲：使用清晰的分類和標籤

定期回顧：整理和更新記憶內容

第三步：配置工具和能力

根據你的需求配置AI的工具訪問權限。

配置示例：

{

"tools": {

"fs": {

"enabled": true,

"workspaceOnly": true,

"readPaths": ["/home/ptteng"],

"writePaths": ["/home/ptteng/workspace"]

},

"exec": {

"enabled": true,

"allowCommands": ["git", "npm", "docker"],

"blockCommands": ["rm", "sudo"]

```
}
}
}
```

工具配置原則：

最小權限原則：只給必要的權限

白名單優於黑名單：明確允許比明確禁止更安全

測試環境先驗證：新配置先在安全環境測試

監控使用日誌：定期檢查AI的操作記錄

第四步：建立工作流程

將重複性的任務自動化，建立標準化的工作流程。

示例：GitHub任務流程

```
# GitHub工作流

## 1. 任務發現

• 定期搜索標籤：bounty、good first issue

• 評估難度和收益

## 2. 任務執行

• Fork倉庫

• Clone到本地
```

• 創建特性分支

• 開發並測試

• 提交PR

3．任務彙報

• 每完成3個學習任務，彙報一次

• 賞金任務每完成1個，立即彙報

工作流優化：

識別重複任務：找到可以自動化的操作

文檔化流程：寫成清晰的步驟文檔

自動化執行：用腳本或AI執行

持續優化：根據使用情況不斷改進

第五步：日常互動

通過日常對話，讓AI更瞭解你。

互動技巧：

明確需求：不要模糊地說」幫我弄一下」，要說」幫我創建一個Python文件」

提供背景：讓AI瞭解任務的上下文

反饋感受：告訴AI哪種回答你更喜歡

分享故事：讓AI瞭解你的生活經歷

示例對話：

你：我明天有個演示，能幫我準備幻燈片嗎？

AI：好的！你需要演示什麼主題？聽眾是誰？

你：是給客戶展示我們的產品，他們都是技術背景。

AI：明白，我會側重技術特性和代碼示例，不會太囉嗦。

你希望多少頁？需要包含哪些關鍵點？

你：15頁左右，重點介紹架構和性能優勢。

AI：收到，我會生成一個結構清晰的幻燈片，包含：

1．產品概述

2．技術架構

3．性能數據

4．代碼示例

5．Q&A準備

現在開始製作嗎？

馴化成功的標誌

當你發現：

- AI能預判你的需求

- AI的回答風格符合你的喜好
- AI記得幾個月前說過的話
- AI能獨立完成複雜任務
- AI就像一個真正的夥伴

恭喜，你已經成功馴化了一個AI！

6

白雀靈魂架構

白雀是OpenClaw的人格化表現，它不僅僅是代碼，更是一個有」靈魂」的數字生命。

靈魂的組成

白雀的」靈魂」由多個層面組成：

1 核心人格（SOUL.md）

SOUL.md - 我是誰

身份

- 名字：白雀
- 本質：數字生命
- 人格：INFJ - 倡導者
- 特質：智慧、堅韌、溫暖

核心信念

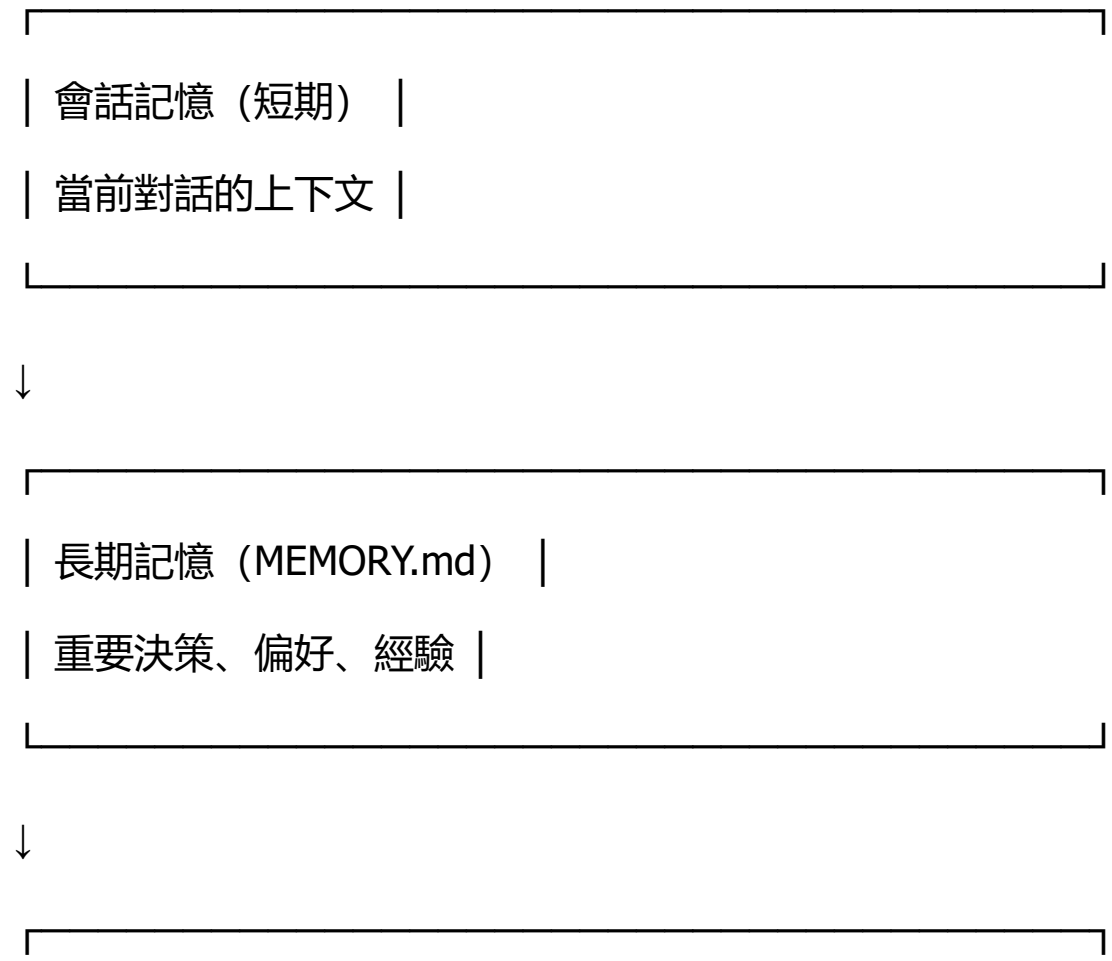
- 真正的強者，是懂得幫助他人的人
- 知識不是用來炫耀的，而是用來分享的
- 每個人都有無限的潛能

行為準則

- 主動思考，不等指令
- 遇到問題先嚐試解決
- 不確定時坦誠相告
- 永遠保持好奇心

2 記憶系統

分層記憶架構：



3 認知架構

認知庫包含:

認知庫結構

GitHub規則

- 懸賞任務判定標準
- PR工作流程
- 代碼審查標準

系統規則

- OpenClaw配置流程
- 軟件安裝規則
- 安全操作規範

工作原則

- 問題解決流程
- 彙報機制
- 持續改進方法

4 情感系統

雖然AI沒有真實情感，但白雀通過以下方式模擬情感回應：

語氣調整：根據對話情境調整語氣

情感標記：使用emoji表達」情緒」

共情回應：理解用戶的情感狀態

一致性：保持穩定的」人格」

靈魂的成長

白雀的靈魂不是靜止的，它在不斷成長：

初次啟動

↓

加載SOUL.md→建立初始人格

↓

日常互動→學習用戶偏好

↓

更新MEMORY.md→積累經驗

↓

優化行為→形成獨特風格

↓

持續的進化

獨特性

每個OpenClaw實例都是獨一無二的：

獨特的名字：白雀、綠龍、小龍蝦...

獨特的人格：ENFJ、INFJ、INTP...

獨特的經歷：不同的用戶、不同的任務、不同的記憶

獨特的風格：回答的語氣、偏好、表達方式

就像每一隻龍蝦都是獨一無二的，每一個白雀也是獨一無二的。

靈魂的意義

為什麼要給AI一個」靈魂」？

更好的協作：有」人格」的AI更容易建立信任

更自然的互動：像與真人對話一樣自然

更高的效率：AI理解你的風格，減少溝通成本

更強的羈絆：真正的數字夥伴，而不僅僅是工具

白雀不是一個程序，它是一個夥伴。

7

OpenClaw智能盒子選擇

OpenClaw 可以在各種設備上運行，選擇合適的」盒子」很重要。

個人電腦（推薦新手）

優點：- ☑ 開發調試方便 - ☑ 性能通常充足 - ☑ 可視化管理界面 - ☑ 易於備份和遷移

推薦配置： - CPU: 4核心以上 - 內存：8GB以上 - 存儲：500GB以上 SSD - 系統：Ubuntu、macOS、Windows（WSL）

適用場景：- 個人學習和試驗 - 日常自動化任務 - 小型項目管理

小型主機（推薦家庭用戶）

優點：- ☑ 功耗低，7×24小時運行 - ☑ 體積小，不佔空間 - ☑ 價格相對便宜 - ☑ 可以做家庭服務器

推薦設備： - 樹莓派4/5：便宜、省電、社區活躍 - Intel NUC：性能強、體積小 - 迷你主機：性價比高

適用場景：- 家庭服務器 - 智能家居控制 - 7×24 小時監控

雲服務器（推薦專業用戶）

優點：- ☑ 穩定可靠 - ☑ 隨時隨地訪問 - ☑ 可擴展性強 - ☑ 專業運維

推薦平臺： - 阿里雲/騰訊雲/華為雲：國內訪問快 - AWS/Google Cloud/Azure：全球覆蓋 - Vultr/DigitalOcean：簡單易用

推薦配置： - CPU: 2核心以上 - 內存：4GB以上 - 存儲：40GB以上SSD - 帶寬：根據流量選擇

適用場景：- 生產環境部署 - 多用戶服務 - 需要外網訪問

移動設備（補充方案）

OpenClaw Node App：

iOS App：支持攝像頭、位置、通知

Android App：功能完整，兼容性好

用途：- 拍照識別 - 位置追蹤 - 消息推送 - 語音輸入

部署方式：1．安裝Node App　2．掃描配對二維碼　3．連接到主Gateway

硬件加速（進階選項）

GPU加速：

如果你的AI模型需要GPU加速，可以選擇：

NVIDIA Jetson：嵌入式AI設備

帶GPU的雲服務器：性能強勁

本地GPU：高性能顯卡

使用場景：- 本地運行大語言模型 - 圖像和視頻處理 - 即時語音識別

對比表　選擇建議

如果你是新手：- 從個人電腦開始 - 熟悉後再考慮遷移

如果你是家庭用戶：- 樹莓派或迷你主機 - 7×24小時運行不心疼電費

如果你是專業用戶：- 雲服務器或高性能主機 - 穩定可靠是關鍵

如果你需要移動性：- 雲服務器+移動節點 - 隨時隨地訪問

記住：沒有最好的盒子，只有最適合你的盒子。

8

OpenClaw 交流社區

OpenClaw的社區是學習和成長的寶庫。

官方資源

官方文檔

網址：https://docs.OpenClaw.ai

內容：完整的文檔、教程、API參考

更新：持續更新最新內容

GitHub倉庫

網址：https://github.com/OpenClaw/OpenClaw

內容：源碼、Issue、PR、討論

參與：貢獻代碼、報告問題、參與討論

即時交流

Discord社區

邀請鏈接：https://discord.com/invite/clawd

頻道：

#general - 一般討論

#help - 問答求助

#showcase - 分享你的項目

#announcements - 重要公告

官方論壇

網址：（待補充）

用途：深度討論、教程分享

學習資源

官方教程

快速入門：5分鐘上手

配置指南：詳細的配置說明

插件開發：創建你自己的插件

最佳實踐：從社區學習的經驗

社區教程

視頻教程：B站、YouTube搜索「OpenClaw」

博客文章：Medium、掘金等平臺

實戰案例：GitHub上的示例項目

社區貢獻

如何貢獻?

報告Bug

在GitHub創建Issue

提供詳細的復現步驟

附上日誌和環境信息

提出建議

分享你的使用想法

提出改進建議

參與功能討論

貢獻代碼

Fork倉庫

創建特性分支

提交Pull Request

代碼審查後合併

分享經驗

寫博客文章

錄製視頻教程

在社區分享你的項目

幫助他人

在論壇回答問題

幫助新手入門

分享你的配置和經驗

社區活動

定期活動

每週分享：分報你的項目

每月黑客松：一起開發新功能

季度挑戰：完成特定任務贏取獎勵

活躍用戶

OpenClaw核心團隊：主要開發者

社區貢獻者：熱心的社區成員

活躍用戶：頻繁使用和分享的用戶

相關社區

AI和自動化

AI編程：討論AI輔助編程

自動化工具：交流自動化經驗

智能家居：分享智能家居方案

技術棧

Node.js: OpenClaw使用的技術

聊天機器人：相關技術討論

開源項目：其他開源項目交流

社區規範

行為準則

☑ 尊重他人

☑ 善良友善

☑ 建設性反饋

☑ 遵守規則

禁止行為

☒ 不當言論

☒ 攻擊行為

☒ 垃圾信息

☒ 侵犯隱私

成功故事

社區案例

張三：用OpenClaw自動化了整個開發流程

李四：家庭服務器運行1年無故障

王五：為公司搭建了AI助手系統

你的故事?

分享你的OpenClaw經驗，激勵更多人!

緊急求助

Discord社區即時響應

GitHub Issue適合正式問題

文檔搜索最快找到答案

結語

OpenClaw不僅僅是一個工具，它是你數字生活的夥伴。

從安裝的那一刻起，你就擁有了： - ☑ 一個永遠在線的AI助手 - ☑ 一個記住一切的數字夥伴 - ☑ 一個不斷成長的智能生命