

## 3C科技

2026年初，OpenClaw  
以現象級姿態席捲全球AI

圈，形成堪比一年前DeepSeek的全民學習熱潮。深圳市龍崗區發布「龍蝦十條」，從十個維度支持OpenClaw發展，最高給予企業200萬元人民幣補貼；A股相關概念板塊也開始活躍，上市公司紛紛布局算力、場景、安全領域，AI智能體產業競爭全面展開。

那麼，使用OpenClaw到底是一種什麼樣的體驗呢？在完整體驗過安裝和持續使用OpenClaw之後，下面筆者探討一下OpenClaw的革新與隱憂。

# 當AI 有了 「手腳」

## 使用OpenClaw的體驗

### OpenClaw能做些什麼？

首先，OpenClaw有自主學習成長的能力，可以通過經驗積累學會新的技能，或直接使用別人創建的技能（skill）快速獲得一項能力。另外，讓它很像真人的「heartbeat」機制，可以保障AI持續在線實現長期記憶。它還有使用工具的能力，操控電腦、調用軟件與API。

OpenClaw作為AI Agent的代表，其核心是擁有自主的規劃、決策和執行能力，甚至能在過程中自主調整策略。OpenClaw不再是簡單的指令執行者，而是能獨立完成任務的「實習生」。

### 「人味」很重

OpenClaw支持用戶在熟悉的社交軟件界面下達自然語言指令，觸發AI執行任務。整體的感覺就像你通過社交軟件跟你的好友或同事討論工作，你甚至會逐漸淡忘它是AI的事實。

OpenClaw作為一個開源項目，它的核心設計不是追求「技術完美」，而是更貼近人的使用習慣和思考方式，也就是所謂的「人味」。它能像人一樣理解模糊的需求；能像人一樣在解決問題時嘗試不同方法、不斷試錯調整；還能像人一樣與用戶進行自然的互動，甚至能感知用戶的潛在需求。

此外，OpenClaw採用「短期+長期」兩種模式的記憶機制，執行任務後會自動總結記錄，實現「越用越懂你」：它的短期記憶會緩存72小時的對話上下文；長期記憶則通過本地存儲保存用戶偏好與任務記錄。

### 成本遠超想像

然而，除了安裝OpenClaw所需的硬件成本之外，使用OpenClaw的成本也並不低。使用它本質上就是在持續使用AI大模型進行所有操作的輸出，而使用大模型時會消耗模型的token（模型使用量的最小計量單位），當你付用費訂閱的大模型套餐，OpenClaw消耗token的速度遠超想像。

## OpenClaw 的革新與隱憂

姚剛

### OpenClaw遇到的問題

#### 並非「到手即用」

OpenClaw的核心優勢——本地部署與數據私有化，恰恰是它的核心門檻。它需要用戶從GitHub克隆倉庫、配置Python環境、安裝依賴包、設置API密鑰，全程用終端指令操作。OpenClaw並非「傻瓜軟件」，即使成功安裝，它亦需要用戶花時間培訓，明確指令邏輯、優化參數配置，才能適應個人或企業的需求；即便是有技術背景的用戶，也可能遇到服務崩潰、記憶丟失等問題。這種「前期投入高，速度慢」的特性，無疑增加了使用門檻。

#### 隱性成本高

OpenClaw本身雖然開源免費，但它不內置大語言模型，每一次任務執行都會消耗大量token。如果沒有進行設置優化，一個中型任務如「日曆整理+郵件回覆」約消耗五千至一萬token，長期記憶功能單日消耗可達十萬token以上，按中國主流模型收費標準，單日基礎消耗可達上百元。

#### 安全風險突出

使用OpenClaw的核心風險在於：為實現自主執行，OpenClaw被賦予讀寫本地文件、操作瀏覽器、執行終端命令的深度權限，相當於給了AI一把「系統鑰匙」。OpenClaw曾被曝出權限繞過與遠程代碼執行等高危漏洞，攻擊者可通過惡意技能包控制用戶設備。此外，用戶的大模型API密鑰、賬戶信息、敏感數據若管理不當，極易被洩露。

### OpenClaw的真實應用場景

OpenClaw能實現每日24小時的自動工作，隨着它的普及，其應用場景已逐步延伸到個人生活、企業辦公、產業落地等多個領域。安裝OpenClaw並不難，難的是如何發揮我們的想像力去用好它。下面讓筆者拋磚引玉，為大家提供一些真實的用戶使用場景：

#### 個人生活場景

從眾多網友分享的案例中，可以看到諸如將OpenClaw用於輔助分析股市、監控異動；自動完成社交平台的點讚、評論、打招呼；自動回覆郵件、搶廉價機票、整理電腦文件夾、自動收集信息並做數據分析；定期收集行業熱點、撰寫文案、排版發帖、剪視頻等，實現「全流程自動化」。

#### 企業辦公場景

在辦公場景它可以成爲一個高效的「數字員工」，替代真人完成重複性工作。在很多專業領域，OpenClaw已被集成至企業管理平臺，應用於財務、HR、供應鏈等核心場景，幫助企業降本增效。

#### 改變人類與AI的關係

在OpenClaw出現之前，人與AI的關係是「使用者與工具」的關係；而OpenClaw讓人與AI的關係變成了合作者與夥伴，用戶只需要提出目標和需求，OpenClaw可以自主完成具體的執行路徑、工具選擇，甚至能在過程中向用戶反饋問題、提出建議，實現了雙向的互動與協作。人可以把更多精力放在戰略規劃、創意構思等高階工作上。OpenClaw的爆發，標誌着AI正式進入生產力實質滲透的深水區，這種協作模式是AI發展的未來方向。

### 如何解決OpenClaw的問題？

#### 「一鍵部署」簡化流程

當前不少企業已開始發力，推出OpenClaw雲端部署方案，大幅降低部署門檻；未來，將有更多企業推出「一鍵部署」的產品，簡化安裝、配置流程。

#### 降低成本 強化監控

針對token消耗過高的問題，未來需要實現本地模型與雲端模型的協同使用——日常簡單任務調用本地模型，降低成本；複雜任務調用雲端模型，保障效率。同時，通過模型降級、上下文裁剪、會話管理等優化方式，進一步減少token消耗。完善安全體系，採用「本地context+雲端監管」的模式，既保留本地存儲的隱私優勢，又通過雲端實現行為監控。目前已有一些企業開始構建專屬密鑰防護體系，推出可視化運維工具；未來還將優化權限分級機制，默認關閉高危權限，同時建立漏洞快速響應機制，防範惡意攻擊與信息洩露。

#### 布局移動端 拓展邊界

當前OpenClaw主要適配電腦端，未來將逐步推出移動端版本，實現手機、平板等設備的無縫對接。用戶可通過下達指令，讓OpenClaw自主操作手機等移動終端完成任務。讓AI真正融入日常生活與移動辦公，拓展其使用場景的邊界。

### 寫在最後

OpenClaw的爆火，讓人類看到與AI協作的全新模式，它讓AI從「數字大腦」進化出了「數字手腳」，其代表的「自主AI智能體」必將成爲未來AI重要發展方向。

但前沿技術需要平衡創新與安全，OpenClaw的問題是新技術普及的「成長陣痛」。唯有平衡好創新與安全、效率與風險，才能讓AI成爲人類的夥伴，推動人工智能產業健康可持續發展。

### OpenClaw避坑指南

- ① 避免在主力機上安裝。主力機通常存儲大量個人敏感信息、工作資料。建議單獨使用備用機安裝，隔離核心數據，降低風險。
- ② 即便使用備用機，也需對重要資料、敏感數據進行加密處理，設置訪問權限；同時，不隨意向OpenClaw輸入銀行卡信息、密碼、商業機密等核心敏感內容。
- ③ 安裝後需關閉不必要的高危權限，僅授予AI完成任務所需的最低權限；定期檢查運行狀態，排查重複服務、漏洞等問題；不隨意安裝未知來源的技能包；定期備份記憶數據，防止數據丟失。