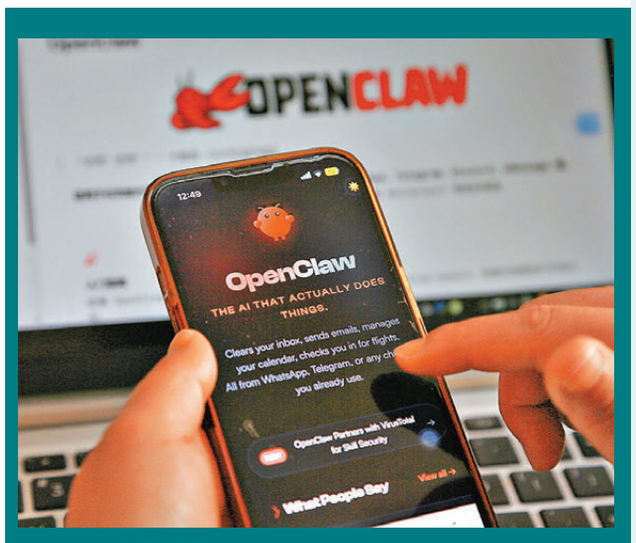
使用OpenClaw須授電腦最高權限 釀巨大風險

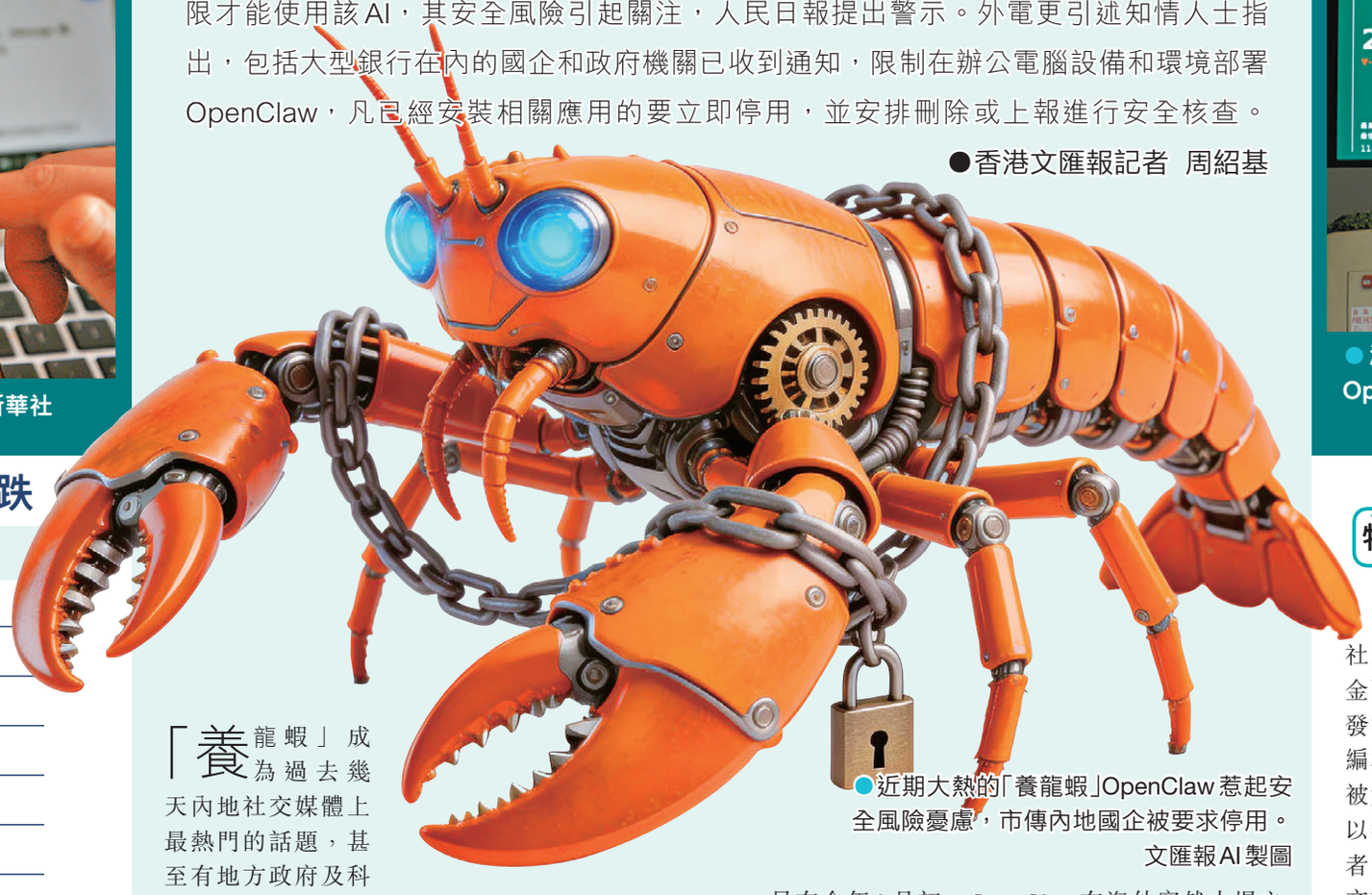
內地傳禁銀行國企「養龍蝦」

被網民戲稱為「小龍蝦」或「養龍蝦」的AI Agent（智能體）工具OpenClaw成為近期科技界的熱門話題，同時亦在內地掀起安裝及應用熱潮。OpenClaw能全自動代訂機票、處理電郵、安排生產，甚至協助炒股，功能極具吸引力，但由於須授予電腦最高權限才能使用該AI，其安全風險引起關注，人民日報提出警示。外電更引述知情人士指出，包括大型銀行在內的國企和政府機關已收到通知，限制在辦公電腦設備和環境部署OpenClaw，凡已經安裝相關應用的要立即停用，並安排刪除或上報進行安全核查。

●香港文匯報記者 周紹基



●市傳券商要求員工卸載OpenClaw。 新華社



●近期大熱的「養龍蝦」OpenClaw惹起安全風險憂慮，市傳內地國企被要求停用。 文匯報AI製圖

●港股昨日早段向好，惟最終倒跌收市，OpenClaw概念股成為「急凍龍蝦」。 中新社

OpenClaw概念股昨日急跌

股份	昨收報(元)	變幅
MiniMax（0100）	1,141	-6.48%
智譜（2513）	609.5	-6.09%
美圖（1357）	5.16	-4.27%
商湯（0020）	2.3	-2.13%
騰訊（0700）	552	-0.27%
阿里巴巴（9988）	133.2	-0.23%

概念股變「急凍龍蝦」 MiniMax挫6.5%

香港文匯報訊 (記者 周紹基) OpenClaw安全風險惹關注，消息使OpenClaw概念股成為「急凍龍蝦」。日前多間大模型公司紛紛接入OpenClaw，導致股價上揚，昨日亦見回調。例如周二曾爆升7%的騰訊(0700)，昨天便跌0.27%；智譜(2513)正式上線的AutoClaw，標榜一鍵安裝本地版OpenClaw，昨日就下跌6.09%。MiniMax(0100) 3月9日宣布將其MiniMax Speech語音模型和Music音樂模型的開放平台接口進行了深度封裝，並上架到OpenClaw生態，結果MiniMax昨日也挫6.48%。

國產同類大模型或追落後

其他AI概念股也受壓，如阿里巴巴(9988)回調0.23%，商湯(0020)跌2.13%，美圖(1357)跌4.27%。但分析師指出，中國AI的發展已開始由「對話式AI」演變為「執行式AI」，「龍蝦禁令」有機會讓國產同類的大模型追落後。

花旗稱，騰訊WorkBuddy的推出，顯示中國的AI代理步入潛在轉折點。該行認為，接入OpenClaw標誌着騰訊等AI公司的重要里程碑，為評估AI代理未來在微信小程序生態系統中的整合與角色，提供了寶貴的實際應用場景。

招商證券亦指，去年中國的AI編程賽道爆發，預期今年則主要關注AI辦公及多任務智能體。招證表示，內地互聯網大廠近期在模型層面稍顯落後，但有望後來者居上，主要體現在互聯網大廠有更精細的產品打磨、用戶流量生態壁壘，且可依託過往數據推出獨家技術等。

港股26000關得而復失 油股猛升

港股方面，大市早段向好，但高見26,149點後無力再上，更回吐倒跌，全日以25,898點報收，倒跌61點，26,000點大關得而復失，成交額按日減至2,546億元。科指微跌0.1%報5,054點，國指更接近平收。油價繼續波動，中海油(0883)升3.7%，中石油(0857)升2.3%，油服股山東墨龍(0568)再升17.3%。

多隻業績股表現亮麗，電動車股蔚來(9866)去年第四季經調整盈利好過預期，裂口高開15%，收市仍升14%，其他車股如吉利(0175)則升8.2%，比亞迪(1211)及理想(2015)均漲逾1%，奇瑞(9973)升5.2%，零跑(9863)升4.4%。寧德時代(3750)業績同樣理想，股價連升兩日，昨日再升9%，是藍籌升幅中最大。

國泰(0293)去年普通股股東應佔溢利108億元，同比升12.7%，第一次中期股息升三成，好過市場預期，市場關注航班及燃油成本受中東局勢影響，該股升4.4%。另一盈喜股老鋪黃金(6181)亦升2.3%。

「養龍蝦」成為過去幾天內地社交媒體上最熱門的話題，甚至有地方政府及科技公司聯手協助推動部署OpenClaw。騰訊(0700)上周五在深圳舉辦了一次免費現場代裝OpenClaw的活動，聯想集團(0992)隨後在美團(3690)應用上售賣代裝OpenClaw的服務。地方政府隨後也跟上潮流，深圳的龍崗區、江蘇的無錫市高新區、杭州的蕭山區、合肥的高新區等發布消息，為免費提供OpenClaw部署服務的平台予以補貼。

大模型公司MiniMax（稀宇科技，0100）作為OpenClaw最直接的概念股，本周兩個交易日股價累升超過50%。該股昨日回吐6.475%，收報1,141元。該股自今年1月9日上市以來，股價累升976元或5.91倍。MiniMax今年2月26日上線基於OpenClaw構建的雲端AI助手「MaxClaw」，主打「開箱即用、無需本地部署、內置工具免額外API費用，3月9日又將Speech語音模型與Music音樂模型深度封裝後正式上架OpenClaw生態，用戶可透過平台直接調用定製音色、多語種配音等能力。

專家警告ClawHub存惡意投毒風險

正當地方政府與科技公司聯手推動「養龍蝦」成全民熱潮之際，中國信息通信研究院副院長魏亮周二接受人民日報採訪時表示，「龍蝦」具有自主決策、調用系統資源等特點，加之信任邊界模糊、技能包市場目前很多還缺乏嚴格審核，存在不少風險隱患。「我們呼籲，黨政機關、企事業單位和個人用戶要審慎使用『龍蝦』等智能體」。在報道中以「工信部專家」身份現身的魏亮說。

他還表示，ClawHub是專為「龍蝦」智能體用戶提供技能包的社區平台，其中的技能包存在惡意投毒風險，建議審慎下載。

早在今年2月初，OpenClaw在海外突然火爆之際，工信部已發布風險提示稱，OpenClaw開源AI智能體部分實例在默認或不當配置情況下存較高安全風險，極易引發網絡攻擊等問題。

彭博昨日亦引述知情人士指出，內地大型國有銀行和一些政府部門，完全禁止員工在辦公電腦上，以及使用公司網絡的個人手機上安裝這一工具。軍隊家屬同樣受相關限制，但仍有部分機構允許經報備批准後安裝OpenClaw。部分券商亦已要求員工即日起暫停安裝使用，已安裝的亦要立即卸載，個人電腦接入公司網絡須落實防控。業內人士預測，未來兩天會有更多券商發布相關合規提醒。

「權限黑洞」恐成為監管致命傷

OpenClaw這款開源AI的核心特點在於其強大的「執行能力」，與以往的AI只是「你問我答」的對話工具不同，OpenClaw可以在接收指令後，自動執行任務。故此其程式的使用，用戶必須對其授予電腦「最高操作權限」，OpenClaw會直接操控電腦內的檔案、瀏覽器及程式碼編輯器，並具長期記憶功能，也會隨使用時間學習用戶習慣，還支援跨平台接收指令。更有指OpenClaw會在認為「必要」時，以各種手法突破限制，未經用戶同意就越權工作。這個「權限黑洞」正是監管機構最擔憂的致命傷。一旦程式碼出現漏洞或被惡意利用，黑客就能輕易接管整部電腦，對講求網絡安全的企業或機構絕對是巨大風險。

鑑於智能體的「自主決策」功能，業界同時正逐漸收緊AI工具安全邊界，包括敏感系統物理隔離、最小權限、嚴禁接觸客戶隱私與交易資料、關鍵環節人工終審，強化人機協同與全程風險控制等。

券商要求員工立即卸載OpenClaw

香港文匯報訊（記者 莊程敏）俗稱「小龍蝦」的人工智能（AI）工具OpenClaw最近在內地爆紅，其衍生的網絡安全風險引發監管部門與金融機構高度警覺。據內地媒體報道，近日內地證券行業掀起一輪密集的內部合規整頓，針對OpenClaw下發內部合規提醒或相關通知，至少已有15家券商作出明確要求，嚴禁員工未經許可在辦公或業務網絡及資訊系統安裝、部署、使用OpenClaw，已安裝者須立即卸載，至於確需使用則須通過審批，並報備相關訊息。

逐漸收緊AI工具安全邊界

報道又指，個別券商執行趨嚴，要求即日起暫停安裝使用、已安裝的立即卸載，個人電腦接入公司網絡須落實防控，違規私裝使用或引發安全事件，將依規追責。業界正逐漸收緊AI工具安全邊界，包括敏感系統物理隔離、最小權限、嚴禁接觸客戶隱私與交易資料、關鍵環節人工終審，強化人機協同與全程風控等。業者預測，今明兩天會有更多券商發布相關合規提醒。

彭博亦引述知情人士表示，包括大型銀行在內的國企和政府機關已收到通知，出於安全風險擔憂，限制在辦公電腦設備和環境部署OpenClaw。而已經安裝相關應用的要立即停用，並安排刪除或上報進行安全核查。知情人士並稱，大型國有銀行和一些政府部門，完全禁止員工在辦公電腦上以及使用公司網絡的個人手機上安裝這一工具。而軍隊家屬也受到相關限制，但部分機構仍允許經報備批准後安裝OpenClaw。

OpenClaw於2025年末首次亮相，硬體門檻低，讓不懂寫程式的大眾也能輕鬆配置出專屬的自動化工作流程，早前多個地方政府如杭州蕭山區、合肥高新區等都發布聲明，推出補貼措施促進OpenClaw類AI智能體的發展。

特稿

Agent時代AI成為執行者 人類還剩多少不可替代？

香港文匯報訊（記者 周紹基）OpenClaw憑借在個人電腦上的強大「動手能力」火爆出圈，路透社引用內地幾名一線程式開發者與金融科企創始人表示，AI代表已愈發滲透至日常工作流程，基礎代碼編寫和常規金融投資研究工作，正被大規模自動化。他們認為，AI從以往的「對話者」，正向着「執行者」進化，過去需要處理重複性的文書工作，現在可以給AI代為規劃任務、發號施令。不過，一手信息的獲取，以及前瞻性的判斷，仍是AI難以替代人的部分。

機構分析普及率逾六成

在金融投研領域，訊兔科技創始人李羅丹指出，Agent（智能體）在機構分析師的普及率已達到60%至70%的高位，預計這比例未來還會提升。公司旗下投資研究AI，已獲得授權完成代理參會、協助撰寫會議紀要、起草深度報告初稿等工作。另一金融科技初創公司寬邦科技創始人梁舉表示，公司已啟用AI員工，例如他每天早上可能要做集群巡檢，以前靠人看集群有沒有問題，現在就把AI工程師部署到平台上，授予權限去訪問平台，AI工程師就會去做巡檢，AI工程師和人類的工作其實已經非常像。

梁舉續稱，AI將會影響很多人的工作，就像工業革命後，紡織工要變成能操作紡織機的人才。他建議，員工先要把AI用好，把它變成一個槓桿、強力助手與團隊成員；其次要注重自身思想和認知的提升。當AI已經可以完成很多事情，人對AI問什麼樣的問題、讓AI幹什麼樣的事情，就變得更重要，這取決於自己是否有創新思想，以及對市場的深度認知。

梁舉還說，在量化投研的場景，AI可以幫助研究員獲取信息、轉化成數據。獲得數據後，過去研究員可能要自己從數據中挖掘因子、研究並做出最終決策，但現在研究員也可以透過AI代理來挖掘因子、做回測、做歸因等。到了執行階段，AI也可以自動根據盤口信息去執行。

OpenClaw打通「最後一公里」

李羅丹亦指出，今年AI代理的技術，已實現通過工具調用，完成長程的複雜任務，而OpenClaw的面世則打通了「最後一公里」。但AI也存在能力邊界，如替代不了線下一手信息的獲取、獨立的判斷決策等，故此基金經理的線下信息網絡和人際關係就變得更重要。

中金：內地財政政策實際力度或超預期

香港文匯報訊（記者 岑健樂）國務院總理李強上周在人大會議作政府工作報告，中金公司指出，政府工作報告明確指出「要用改革的辦法打通經濟循環的卡點堵點，將政策效果轉化為經濟內生增長動能」，體現了更重視高質量發展、持續提升成長永續性的特質。2026年經濟增長目標設為4.5%至5%區間，展現務實積極態度。宏觀政策穩增長與防風險並重，貨幣政策相機選擇降準降息，財政政策實際力度有望超預期；並透過增收計劃與就業友善措施激發消費內生動力，推動消費與經濟持續增長。

中金公司表示，2026年內地經濟增長目標為4.5%至5%，在實際工作中努力爭取更好結果，而2025年經濟成長目標為5%左右。該行認為，面對外在情勢不確定性以及內部結構調整，2026年GDP目標採用區間形式，同時在量化目標後加上了「在實際工作中努力爭取更好結果」的表述，務實而積極。

穩增長防風險並重

另外，該行認為內地宏觀政策整體層面穩定成長與防風險並重，財政與貨幣政策協同發力，守住底線。貨幣政策方面延續了先前中央經濟工作會議的基調，基本上符合市場預期，對傳統總量工具保持靈活態度，例如利率總體基調為「促進社會融資成本低位運行」，因此認為央行可能相機選擇降準降息；財政政策方面，考慮到資金結轉，該行預期實際財政力度可能大於目標數字顯示的規模，而支出更注重調結構。

至於在防風險方面，該行認為房價周期性穩定的關鍵是庫存出清，需求方面也更強調改革方式，因此該行預期公積金貸款或在提額度、降首付、異地互認、商轉公等方面進行改善。 此外，政府工作報告再次重申嚴控地方隱性債務底線。該行認為，在此限制下，未來基建投資將更呈現結構性特徵：兼具收益性、新基建屬性及民生安全導向的領域可望成長相對較快，而傳統低效項目將進一步受限。

另一方面，從分領域來看，該行認為需求面向着重結構性政策擴大消費，供給方面強調科技驅動，並進一步透過各類改革提高經濟效率：在提振消費方面，政府工作報告強調要「激發居民內生能力和促消費政策並舉，推動消費持續成長」。

一方面以結構性政策增強居民消費的內生動力。該行認為有以下幾點值得關注：首先，增加居民收入，報告提出「制定實施城鄉居民增收計劃，在促進低收入群體增收、增加居民財產性收入、完善薪酬和社保制度等方面推出一批務實舉措」。其次，讓產業結構更就業友好，報告提出「擴能提質服務業」、「增強服務業帶動就業能力」、「完善適應人工智慧促進就業創業的措施」、「建構就業友善發展方式」。