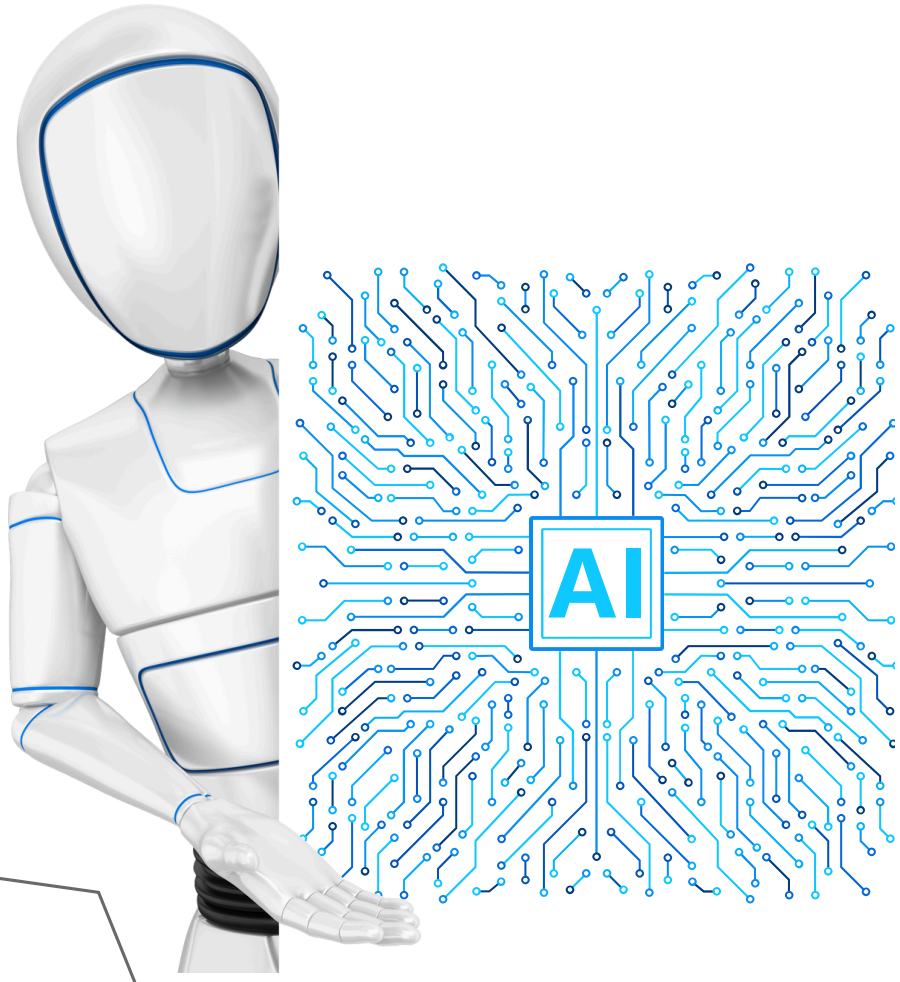
115年4月號

公務機密
資訊安全維護



林業及自然保育署
臺東分署

目錄

01 資安時事案例

- 基隆引進AI無人稽查車 網揭「中國製造」憂個資外洩
- 中共「對台政要圖譜」檔案外流 2300萬戶籍入庫！AI講台語冒充台灣人

02 個人資料保護法

- 時代力量驚傳被駭！3.3萬筆個資外洩　姓名、電話全被看光
- 資快速瞭解個資法Q&A 60則個資法常識(每月一常識)

Q24 對於新法實施前已蒐集的個資，需要補告知嗎？

03 生活中的資安

- 全球掀起養龍蝦風潮！它跟ChatGPT差在哪？

04 數位學習

看到黑影就開槍？許多企業都有的資安惡習！

資安時事案例

基隆引進AI無人稽查車 網揭「中國製造」憂個資外洩

基隆市環保局引進AI無人稽查車，在國門廣場和海洋廣場巡檢，民眾擔心個資外洩。(記者盧賢秀攝)

〔記者盧賢秀／基隆報導〕

2026年3月19日 週四 下午12:56

基隆市環保局引進全台首部AI無人稽查車，在國門廣場和海洋廣場巡查髒亂點，可偵測亂丟垃圾及吸菸，但民眾爆料，這部AI無人稽查車是中國製造，擔心個資和隱私外洩。市府副發言人鍾明表示，尊重各界觀點，市府跟環保局會繼續努力，打造乾淨家園。

這部AI無人稽查車巡迴國門廣場和海洋廣場不斷行駛，有的民眾看了相當好奇，環保局指出，AI無人稽查車有5個鏡頭、12組超音波感測器，可自動導航與360度3D雷達環景系統偵測，透過AI自主沿路巡檢髒亂點，或發現垃圾桶垃圾量滿溢，通報清潔人員即時清除。

AI無人稽查車還可主動偵測吸菸行為，透過擴音系統提醒民眾熄菸；無人車前方內建13.7吋顯示器可輪播影片，宣導政策與活動最新訊息。

不過網友發現，這部AI無人稽查車是在新加坡採購，實際是在中國製造，擔心偵測到人臉會有個資外洩的疑慮，又是在港口邊巡迴，可能有資安問題？偵測到亂丟垃圾或吸菸，有些是外地客，也無法裁罰？質疑其效益。

市議員張之豪表示，市議會並沒審到這筆預算，同時稽查車蒐集市民個資和影像，保存多久、上傳到什麼地方？管理有無規範？質疑是為AI而AI。

環保局表示，AI稽查車目前試營運，預計4月正式上線，沒有開罰功能，相關資料必須有授權才能調閱資料。相信可有效提升市容環境與效能，讓基隆的公共空間乾淨舒適。

資安時事案例

中共「對台政要圖譜」檔案外流 2300萬戶籍入庫！AI講台語冒充台灣人

日前媒體驚爆有台灣黑幫成員在中共威脅利誘下，協助情蒐國內幫派情資並製作成約3萬字的報告。（AI示意圖）

三立新聞網
2026年3月17日 週二 下午3:51/政治中心／程正邦報導
台灣資安防線面臨前所未有的科技挑戰。根據台灣民主實驗室最新分析的中國企業「中科天璣」外流文件，揭露了一場針對台灣量身打造的「全方位數位監控計畫」。這套系統不僅細膩建檔我國朝野政要，更驚見 AI 技術進化到能精通「華語、台語」雙聲道，生成高擬真的虛擬人物，大規模潛伏於社群平台，意圖從內部瓦解台灣社會。

藍綠白皆入列！精確標註「親中、反中」立場
根據《自由時報》報導，外流資料顯示，中科天璣建立了極其詳盡的「涉台知識圖譜」，將台灣政治版圖結構化。名單從總統賴清德、前總統蔡英文，到在野黨領袖柯文哲、侯友宜等人無一倖免。系統內除了登載基本的學經歷與社會關係，最受矚目的是設有「對華態度」專門欄位，明確分類政要屬於「親中」或「反中」。

這套自動化系統能迅速鎖定在特定城市中具影響力的「綠營反中人士」，或是佔據關鍵政府咽喉點的藍營政客。透過大數據分析，中共將台灣菁英區分為「頑固派」、「友好派」、「搖擺派」及「客觀派」，每類至少鎖定 1,000 人，作為後續分化攻勢的精準打擊目標。

2300萬戶籍資料全被掌握？公民社會「全景圖」曝
報告指出，這份外流文件宣稱掌握了高達 2,300 萬筆來源封閉的「台灣戶籍資料」，意即全台人民的背景可能都在其監控範圍內。此外，數據庫還納入了 1,478 家企業、1.3 萬個宗教團體以及近 2.4 萬個人民組織。

中科天璣透過追蹤全球萬個涉台來源、超過 620 萬條社群媒體內容，並鎖定 5,000 個具影響力的社群帳號，有組織地繪製出台灣公民社會的「全景地圖」。這些基礎資料成為中共實施「分化與塑造」戰略的彈藥庫，讓影響力作戰能細緻化到每一個里鄰、每一間企業。

虛擬網軍進化：AI 偽裝「正港台灣人」發言
最令人驚心的是該公司研發的「身分塑造與培養技術」。為了突破台灣民眾對簡體字或對岸語法的戒心，中科天璣利用 AI 生成能模仿台灣在地口音、用語風格的數位分身。

這些 AI 網軍不僅精通台灣特有的華語詞彙，甚至能用「流利台語」編寫腳本、錄製音訊，以高擬真的數位身分大規模冒充台灣人。透過模擬台灣受眾的偏好與認知習慣，這些虛擬帳號散布特定輿論，旨在製造內部對立與認知偏誤，讓一般民眾在網路互動中，難以分辨對話者究竟是熱心網友還是對岸的 AI 程式。

個人資料保護法

時代力量驚傳被駭！3.3萬筆個資外洩　姓名、電話全被看光

時代力量系統被駭，3.3萬筆個資遭外洩。（圖／翻攝自時代力量官網）

編輯 伍芸彤 / 責任編輯 編輯組 報導發佈時間：2026/03/07 14:45
最後更新時間：2026/03/07 15:05

時代力量日前接獲支持者反映，發現黨內CRM系統疑遭入侵，導致約3萬3000筆個資外洩，內容含姓名、電子郵件、電話等，未涉及身分證字號與財務資訊。對此，時代力量隨即啟動資安應變機制，並於2小時內阻斷受影響系統，通報內政部及警方，涉案外國論壇現已遭美國及歐洲等14國執法機關聯手下架，防止資料擴散。

時代力量3.3萬筆個資外洩　支持者資料全被看光

時代力量指出，6日下午3時接獲支持者反映，其個人資安防護軟體F-Secure警示電子信箱，疑似黨內系統個資外洩。時代力量立即檢查系統存取記錄，並於下午5時阻斷受影響系統。對於此次事件造成社會疑慮，時代力量表達歉意。

時代力量進一步說明，初步研判入侵點為內部CRM系統權限控制遭破解，資訊單位已停止該系統存取，確保資料路徑中斷，並主動通報內政部及報警。外洩資料約3萬3000筆，內容包含姓名、電子郵件、電話、居住地址、Line ID、職業、生日及性別，未涉身分證字號、銀行帳號、登入密碼或信用卡資訊。

時代力量道歉、下架資料

針對後續處理，時代力量表示，預計於14日前透過電子郵件或簡訊主動通知受影響當事人，如近期接獲冒用黨名的不明來電或社交軟體請求，請提高警覺。涉案國外論壇「LeakBase」已於本週遭美國司法部與歐洲刑警組織等14國執法機構聯手下架，並查扣資料庫，有效遏止資料擴散，後續將持續關注動向。

時代力量感謝支持者與媒體第一時間示警，使其能及時阻斷系統，並強調，「我們不會迴避問題，將持續強化資安防護韌性，以最積極的態度修復漏洞，落實後續的當事人通知與個資保護作為」。

每月一常識

新版個人資料保護法與過去有很大的不同，新法進一步擴大了個人資料的保護範圍，並且讓所有產業一體適用；新法甚至首度增加團體訴訟，而且違法的罰則也加重了，企業老闆要負更大的責任。接下來，我們以60個Q&A，快速帶你認識新版個人資料保護法

Q24　對於新法實施前已蒐集的個資，需要補告知嗎？

A　若是在新法實施之前，以間接方式取得的個人資料，則需要在新法實施後補行告知當事人。

文/iThome

全球掀起養龍蝦風潮！它跟ChatGPT差在哪？

被暱稱為「養龍蝦」的AI助理工具OpenClaw近期在中國爆紅。（圖／翻攝自微博）

記者陳郁柔／台北報導2026年3月17日 週二 下午12:05

[NOWnews今日新聞] 近期科技圈掀起一股「養龍蝦」風潮，不過隨後引起資安疑慮，《NOWNEWS今日新聞》統整「養龍蝦」風潮如何興起？OpenClaw優缺點是什麼？與ChatGPT又有哪不同？

OpenClaw「養龍蝦」這是近來AI社群，以及科技圈討論度最高的開源專案之一，它不僅僅是一個聊天機器人，而被定義為AIAgent（AI代理人）。

OpenClaw起源

OpenClaw是由奧地利工程師創建，上線只有4個月，推出沒多久就引發關注，在全球最大的線上程式碼雲端託管平台GitHub星標數就突破24.8萬，甚至登上最受歡迎開源專案榜首。這樣的成長速度，在AI開源專案中相當罕見，也讓OpenClaw迅速成為全球科技圈熱議焦點。

OpenClaw在中國被形容為「真正能幹活的AI」，與一般AI聊天機器人不同，只要用戶授權後，OpenClaw可以自動執行任務，例如閱讀文件、搜尋資料、寫程式碼，甚至發送電子郵件。因此，許多工程師把它視為可以實際工作的「數位員工」。

它的開發者Peter Steinberger（PSPDFKit創辦人）使用了龍蝦作為專案的標誌，在AI社群及科技圈內，「養龍蝦」指的就是架設並運行這個OpenClaw機器人。

OpenClaw特色

OpenClaw有三大特徵：一、它是一個Agent（代理人），一般的AI是「你問它答」，OpenClaw是「你下指令它去執行」；二、它能操作你的電腦；三、這不是一個網頁服務，而是你要「部署」在自己電腦或伺服器上的程式。

OpenClaw在中國引發熱潮

近兩週以來，中國社群平台小紅書、抖音與B站上出現大量OpenClaw教學影片與安裝指南，甚至有人提供付費上門部署服務。中國許多科技業者也推出「龍蝦」模型，還有部分地區已經應用到政務服務系統。

OpenClaw與ChatGPT的不同

不同於ChatGPT屬於大型語言模型（LLM，Large Language Model），主要功能是給予文字建議與分析；OpenClaw則是一款「大型行動模型」（LAM，Large Action Model）。

OpenClaw也有幾大吸睛亮點，它全天自主運作，適合掛機在電腦或是雲端伺服器，並且擁有長期記憶力，也能夠跨平台遠端控制，在外面用手機傳個訊息給它，它就在家幫你查資料、改程式碼或回電子郵件。

OpenClaw優點

不同於ChatGPT只能給你建議，OpenClaw可以幫使用者「執行」，也支援 OpenAI、Claude，甚至可以透過Ollama運行完全本地的模型，根據任務重要性自由分配算力，對於開發者或小團隊，它可以取代許多昂貴的自動化 SaaS 工具（如Zapier）。

OpenClaw缺點

就是資安問題，若沒設定好VPN或防火牆，你的OpenClaw介面可能直接暴露在網路，駭客能直接控制你的電腦。此外，惡意插件也很多，因為它的Skill市場缺乏審核，下載到不明來源的插件可能導致金鑰外洩。

此外，養龍蝦技術門檻很高，安裝過程需要用到終端機（Terminal）、Node.js 和 JSON 配置，不是「開箱即用」的軟體。Token消耗也很驚人，因為Agent會不斷進行「思考-行動-觀察」的循環，API費用（如Claude 3.5/4.0）累積速度比普通對話快得多。也有極高的硬體要求。