

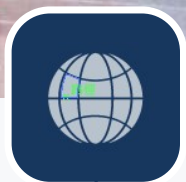
深化資安防護認知

顧問 洪書韋



2026.10.12

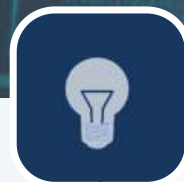




資安形勢分析



深化資安
防護認知

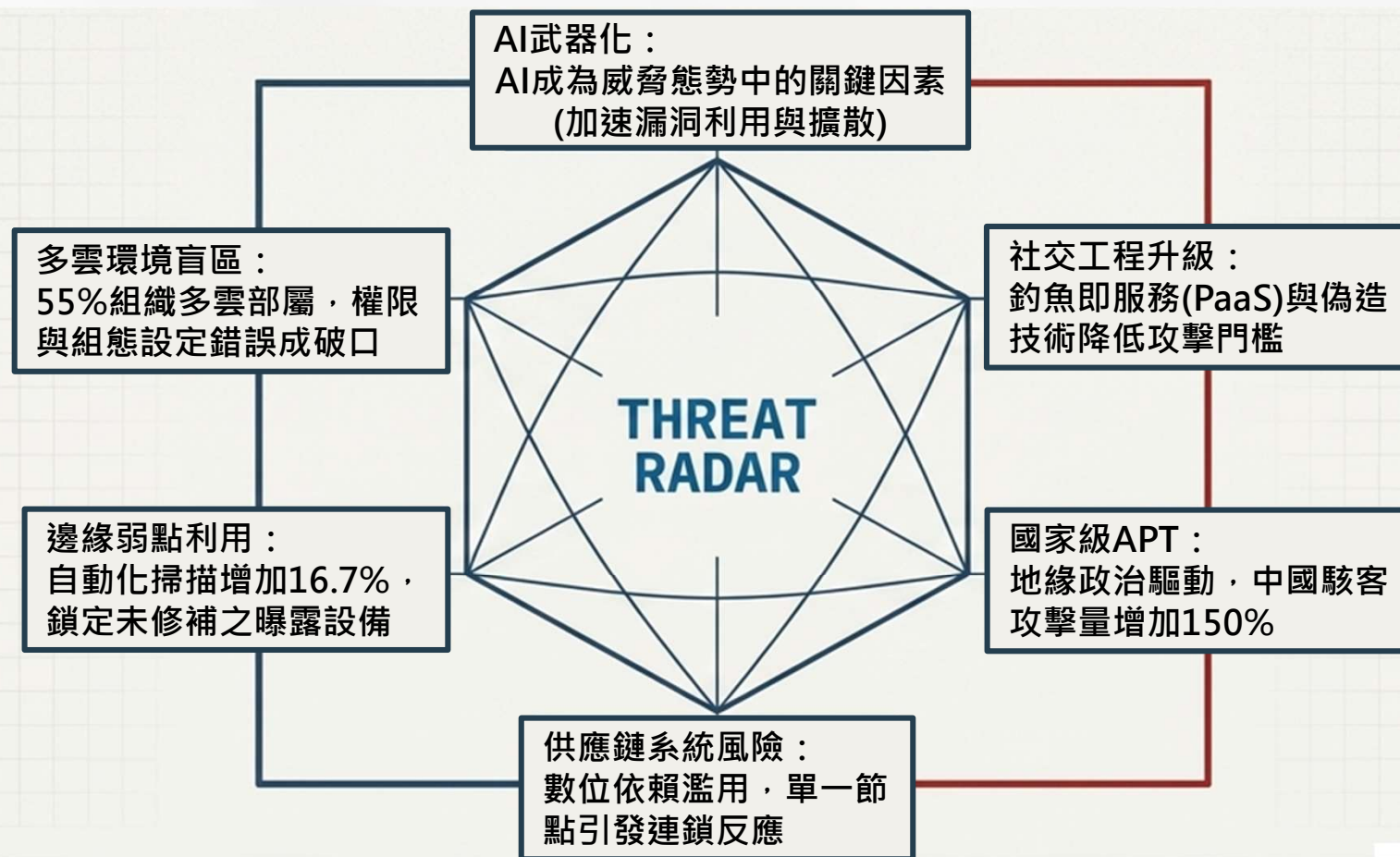


案例與啟發



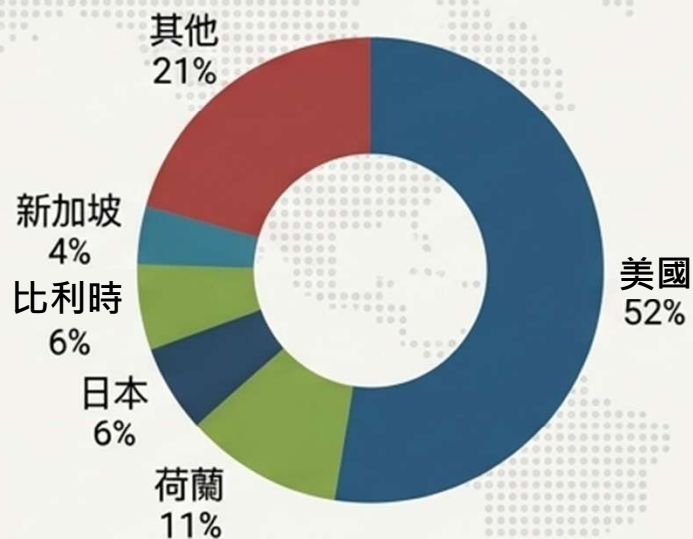
法規異動概覽

資安威脅互聯生態系



2025 聯防預警情資

跳板來源地理分佈



國內(40%) vs 國外(60%)

攻擊者多利用「外對內防火牆大量阻擋」、「外部主機執行掃描探測」與「遠端維運工具連線」

威脅行為光譜

Top 1 : 資訊收集 (36.5%)

- 透過掃描、探測與社交工程。

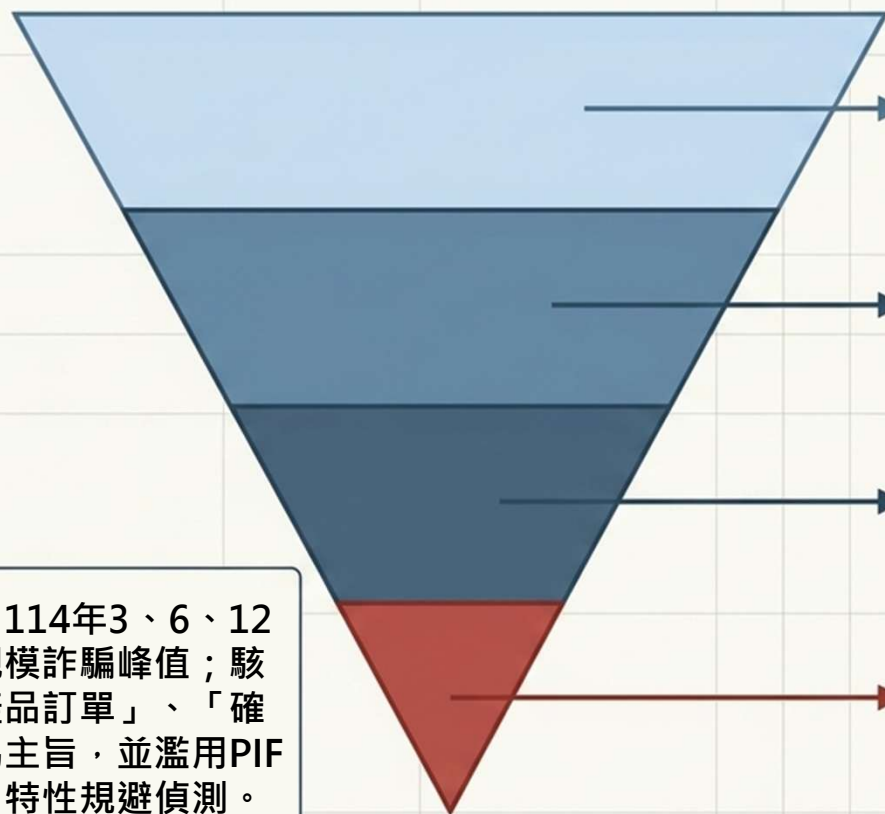
Top 2 : 入侵攻擊 (27.8%)

- 未經授權存取或取得使用者權限。

Top 3 : 入侵嘗試 (19.8%)

- 試圖突破邊界防護。

2025 惡意郵件分析



Level 1：總檢測流量 (The Noise)
-> 1億959萬封電子郵件 (114年度總量)。

Level 2：惡意/可疑攔截 (The Filter)
-> 148萬封可疑郵件 (占整體 1.36%)。

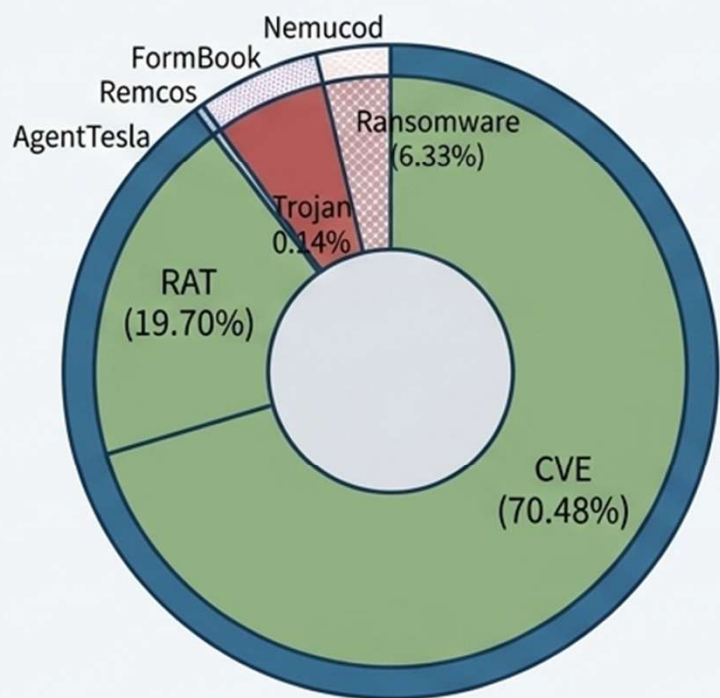
Level 3：風險分級 (The Threat)
-> 中低風險 (98.23%)：已知惡意特徵與連結。

Level 4：進階威脅 (The Target)
-> 高風險 (1.77%)：需動態沙箱分析的未知 CVE 漏洞利用與進階威脅行為。

戰術特徵：114年3、6、12月出現大規模詐騙峰值；駭客常以「產品訂單」、「確認付款」為主旨，並濫用PIF隱藏副檔名特性規避偵測。

2025 惡意程式分析

惡意程式族群分布



- 70.48% 漏洞利用 (CVE) - 佔據絕對多數。
- 19.70% 遠端控制木馬 (RAT)。
- 6.33% 勒索軟體 (Nemucod 等)。

重點狙擊目標：

CVE-2017-11882 / 0199

The Flaw：

微軟Office系列遠端執行漏洞。

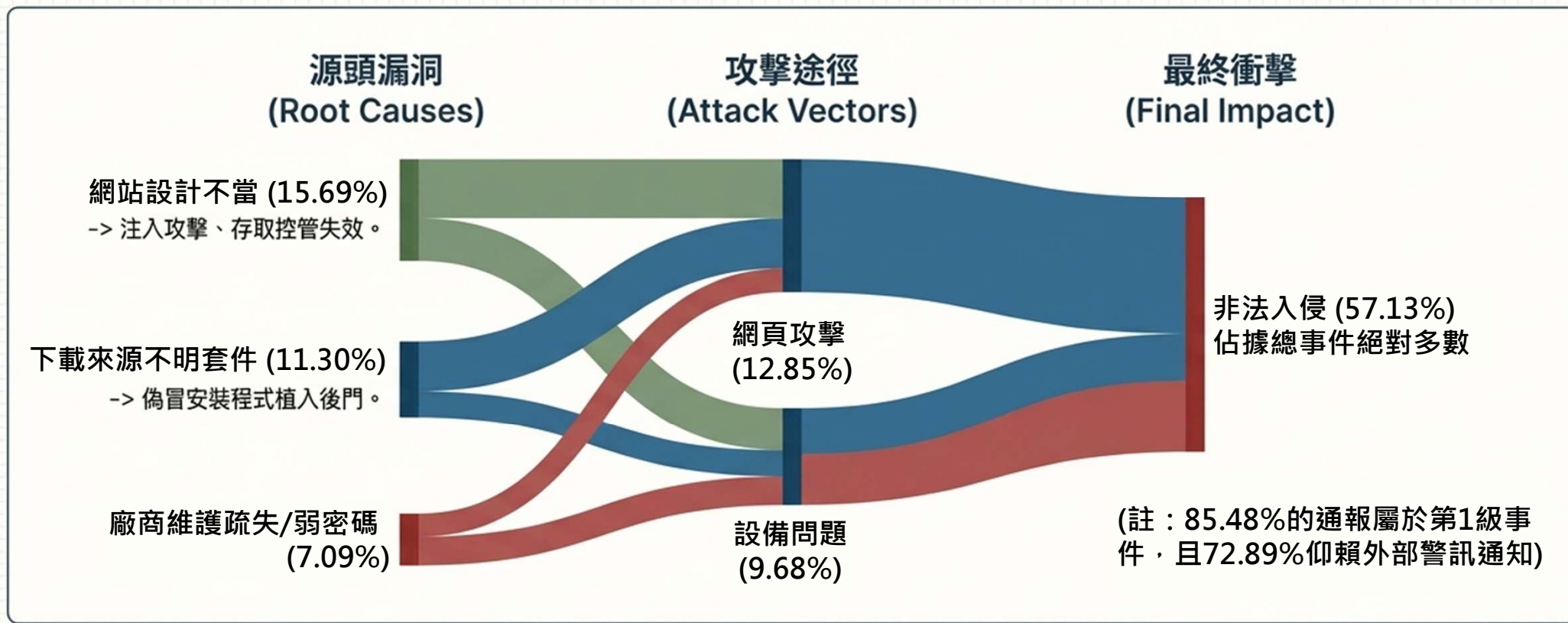
The Reality：

自2017年發現至今，因適用平台廣，仍是駭客最常利用的漏洞，名列CISA最常被利用漏洞名單。

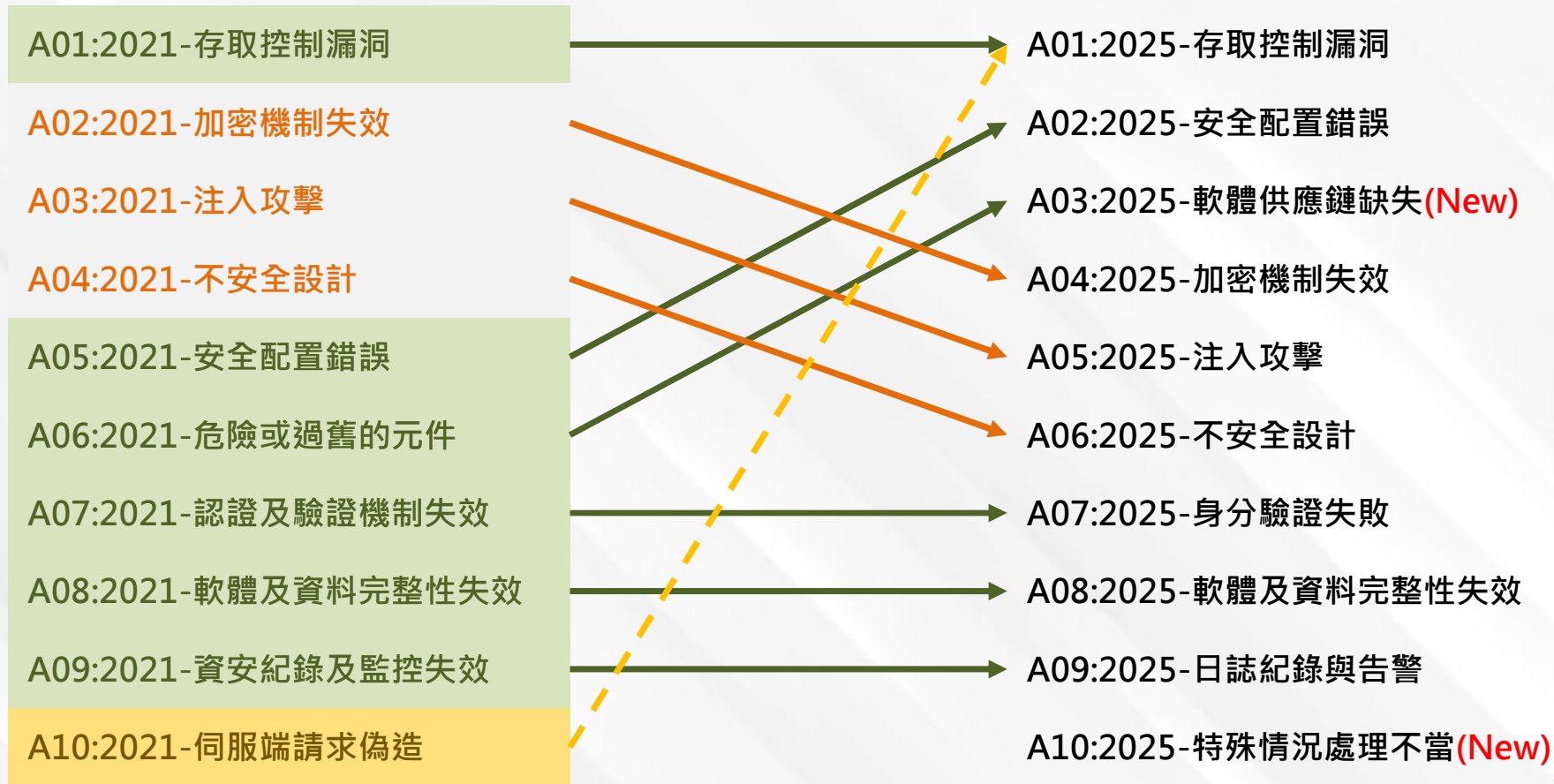
Other Threats：

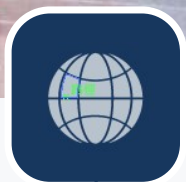
AgentTesla(遠端木馬)、
Nemucod(勒索軟體)

2025 資安事件分析



OWASP Top 10:2025

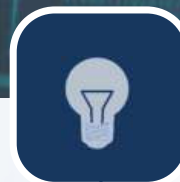




資安形勢分析



深化資安
防護認知



案例與啟發



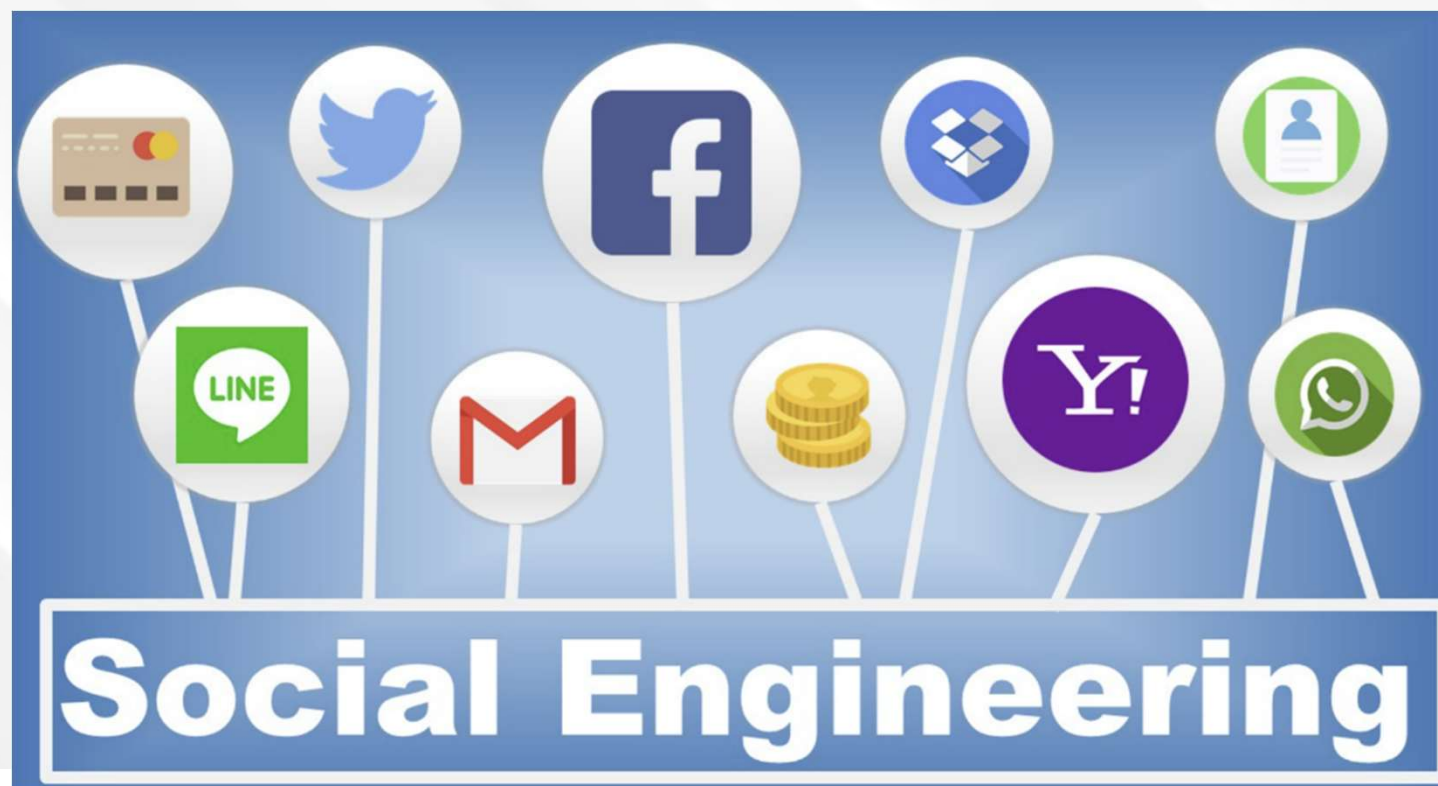
法規異動概覽

木桶理論



社交工程

- 人性弱點
- 偽裝情境
- 誘導行為
- 多樣化途徑



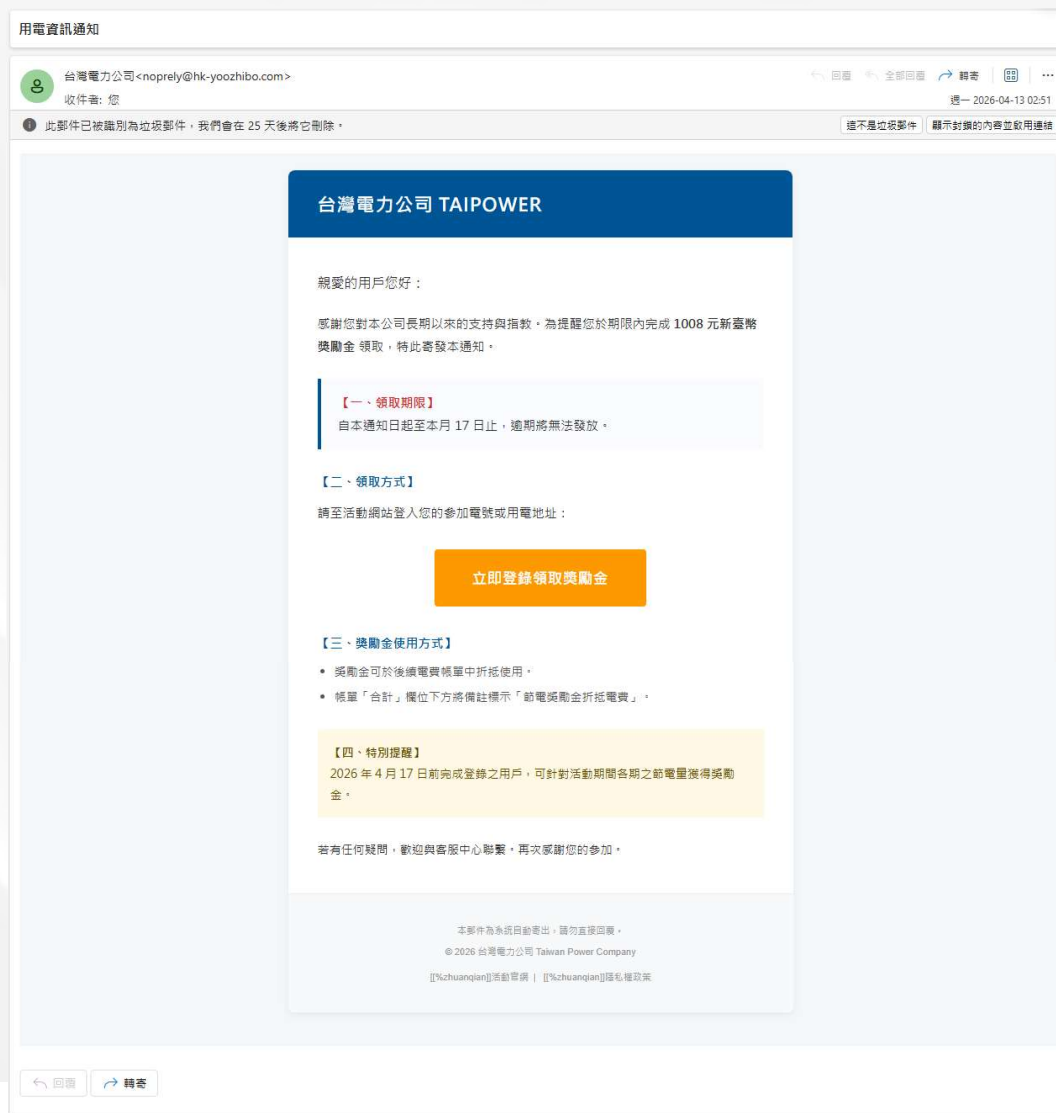
社交工程

■ 人性弱點

■ 偽裝情境

■ 誘導行為

■ 多樣化途徑





社交工程手法再升級：結合雲端服務與憑證規避防禦

TWCERT/CC接獲外部情資，近期出現一波結合雲端服務與仿冒網域的社交工程攻擊活動。駭客透過租用Microsoft 365服務、註冊近似官方的域名，並申請短期 SSL 憑證，試圖規避郵件與網頁防禦機制，發起釣魚郵件攻擊。

依據情資內容顯示，駭客在第一波攻擊行動中，透過租用的Microsoft 365合法電子郵件帳號，偽冒「Microsoft帳戶異常登入活動通知」，針對企業內部多個目標發動釣魚郵件攻擊，要求目標登入帳戶。

第二波攻擊行動中，駭客採魚叉式釣魚手法，同樣利用Microsoft 365服務，但改為針對特定目標「連續」發送多封偽冒「Microsoft一次性代碼通知」，企圖營造目標帳戶正遭多次嘗試登入假象，爾後再次寄送偽冒「Microsoft帳戶異常登入活動通知」，引誘目標點選連結立即登入帳戶以檢視異常登入紀錄，進而竊取目標帳號密碼。



駭客打造YouTube幽靈網路來散布竊資程式

以色列資安業者Check Point Research上周揭露了一個鎖定YouTube平臺的惡意活動「YouTube幽靈網路」(YouTube Ghost Network)，駭客先取得或接管YouTube頻道帳號，再上傳以破解軟體及遊戲外掛為誘餌的影片，引導受害者下載內含竊資程式的惡意軟體。該活動於2021年即開始運作，至少已上傳逾3,000支惡意影片，是近年來規模最大的YouTube惡意活動之一。

駭客同時以不同的角色來建立YouTube幽靈網路，張貼影片主要利用盜來的、有粉絲基礎的帳號，繼之利用自動註冊的假帳號來偽造互動，包括貼文、按讚或留下正面評價，以吸引不知情的受害者下載。

然而，使用者所下載的壓縮檔或安裝程式含有載入器，以下載或解封諸如Rhadamanthys及Lumma等資訊竊取工具，目的是盜走使用者的帳密或錢包等敏感資訊。



現階段生成式AI最常被駭客用在：社交工程攻擊的強化

過去曾擔任美國國家情報總監辦公室資安事務情報長，現為Google Cloud國際資安合作負責人的Christopher B. Porter指出，這些發現並非理論推測，而是來自Google Cloud客戶與Mandiant全球事件應變團隊的實際觀察結果。

過去這些駭客雖然技術力強，但苦於語言障礙，難以理解或模仿目標組織內部的溝通語境，即使滲透後要找到關鍵敏感資料也很費工，如今這個障礙已不存在了。

駭客入侵公司組織電子郵件後的行動也更加容易，因為AI能幫助總結電子郵件的內容，因此可以更逼真地偽冒回應，並製作更容易引人誤信的郵件內容與對話。



社交工程手法

- 釣魚郵件、簡訊
- 恐嚇軟體
- 誘餌攻擊
- 尾隨闖入
- AI詐騙



防範社交工程指南

- 暫停操作
- 冷靜查證
- 不開啟未知連結或檔案
- 不透過連結輸入機敏資訊
- 留意數位足跡



其他建議

- 區分公私信箱
- 關閉信箱預覽功能
- 開啟多因子驗證



全球掀起簡訊OTP禁用潮，多國推行限制政策

全球政府禁用簡訊OTP（一次性密碼）的態勢越發顯著，主要源於網路釣魚詐騙日益猖獗。新加坡、馬來西亞、阿拉伯聯合大公國（UAE）及印度等國已陸續頒布政策，要求銀行轉向更安全的身分驗證方式，如App推播、生物辨識或裝置綁定，並強化金融監管責任。

這波趨勢核心原因在於簡訊OTP易受社交工程攻擊，網路犯罪生態系長期將其視為防禦破口。此趨勢與FIDO聯盟推動的Passkey發展一致，目標是建立具備「抗網釣」能力的強式多因素驗證（MFA）。事實上，美國NIST與CISA早在多年前便將簡訊定位為臨時過渡方案。未來驗證機制將進一步整合eSIM技術與電話號碼驗證（PNV），以確保帳號註冊及復原流程的安全性，全面升級數位身分認證環境。

供應鏈攻擊

- 信任濫用
- 連鎖反應
- 多樣化途徑
- OWASP Top 10
 - A03: 軟體供應鏈缺失





震撼IT界的XZ程式庫後門事件，浮上檯面純屬意外

XZ Utils 供應鏈攻擊是一場跨越多年、手法極其精密的網路攻擊行動。攻擊者化名「Jia Tan」，自 2021 年起透過長期提交無害修正與多個假帳號施壓的社交工程手段，取得原維護者信任並獲得開發權限。隨後，他在 liblzma 庫中植入隱蔽後門，鎖定特定 Linux 發行版的 SSH 元件，意圖達成無需登入即可遠端執行指令的目的。

駭客利用二進位測試檔案隱藏惡意代碼，並在 2024 年初發布 5.6.0 及 5.6.1 版本時，透過修改建置腳本將後門整合進去。所幸微軟工程師於 3 月底偵測到 SSH 登入延遲異常，才讓這起首例針對廣泛使用開源軟體的嚴重供應鏈攻擊曝光。此事件標誌著開源安全的新轉折點，突顯了駭客如何從源頭汙染基礎設施，並利用開源維護者的壓力與信任進行長期潛伏與滲透。



Notepad++ 自動更新通道遭劫持

知名文字編輯器Notepad++維護者指出，內建自動更新元件WinGUp的更新流量曾遭攔截並被重新導向，用戶在更新過程中可能因此下載到遭竄改的安裝程式。Notepad++在v8.8.9起強化更新驗證，下載後會同時檢查安裝程式的數位簽章與憑證，任一驗證失敗即中止更新。

在官方發布的調查說明中，維護者表示事件並非透過Notepad++程式碼本身的漏洞被入侵，而是發生在網站託管環境的基礎設施層。與維護者合作的外部資安專家研判，攻擊者可能在主機服務商端選擇性攔截並重新導向部分更新請求，使特定目標被導向攻擊者控制的伺服器，再回傳遭操弄的更新描述檔。資安公司Rapid7指出，這波攻擊行動是外號為Lotus Blossom、Billbug、Thrip的中國APT駭客組織所為。



NPM套件Axios遭遇供應鏈攻擊

廣泛採用的 JavaScript HTTP 函式庫 Axios 於 2026 年 3 月 30 日遭遇嚴重的供應鏈攻擊。駭客挾持維護者的 NPM 憑證，繞過標準發布流程釋出惡意版本 1.14.1 與 0.30.4。攻擊者透過注入偽裝的相依套件 plain-crypto-js，針對 Windows、macOS 及 Linux 系統植入 RAT 木馬。該惡意程式具備自我銷毀功能，可替換 package.json 以規避鑑識。

受影響用戶應立即將 Axios 降級為 1.14.0 或 0.30.3 穩定版本。值得注意的是，並非只有直接使用 Axios 的開發者會受影響，若是自行建置 OpenClaw 的使用者，也可能引入有問題的 Axios，導致電腦被植入惡意程式。

此事故影響範圍廣大，Axios 每週下載量高達 1 億次，且惡意酬載針對三大平台分別以 PowerShell、C++ 及 Python 打造，顯示其攻擊具有高度針對性與自動化特質。



供應鏈攻擊手法

- 軟體更新攻擊
- 開源套件攻擊
- 入侵基礎設施
- 竊取數位憑證



防範供應鏈攻擊指南

- 供應商風險管理
- 技術檢測
- 軟體物料清單
- 零信任架構

資料洩漏預防



個資保護





集菟資個

- 符合特定目的
 - 病例、犯罪前科等特種個資原則上不得蒐集
- 最小化原則
- 告知義務
 - 蒐集目的、利用方式、當事人權利等
- 盤點與分類



個資儲存

■ 實體安全

➤ 機房、檔案室門禁管制

■ 檔案加密

■ 檔案備份

➤ 備份效期、異地備份、還原測試



個資使用

■ 存取權限

➤ 人員異動時交接

■ 稽核日誌

➤ 保存6個月

■ 委外管控

■ 特定目的外利用

■ 去識別化



個資傳輸與刪除

- 加密傳輸
- 保存期限
- 刪除或銷毀紀錄
 - 保存5年

其他流程風險

■ 內、外部人員作業不熟悉

- 教育訓練、檔案閱覽權限

■ E-mail遭入侵或釣魚郵件

- 社交工程演練、取消帳密記憶、檔案加密

■ USB中毒或有後門程式

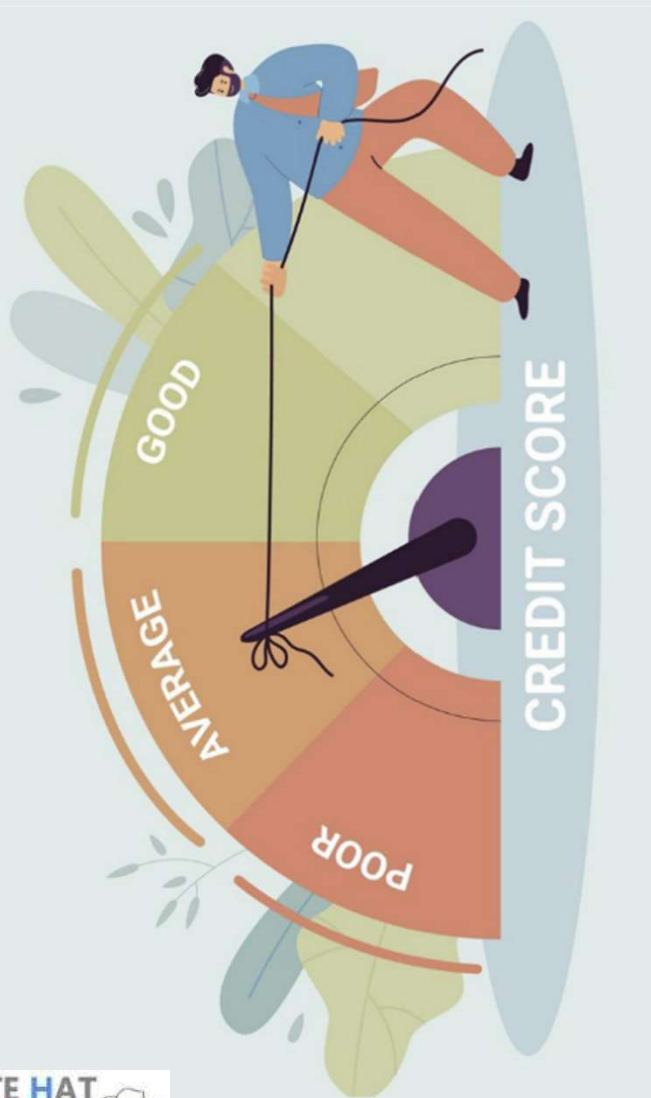
- 防毒軟體、定期更新

■ 雲端資料外洩

- 檔案加密、資料分類、存取權限

■ 系統遭入侵

- 系統技術檢測、防火牆、帳密要求、權限設定





台新爆重大疏失 個資外洩4年未覺察

台新銀在2020年5月1日及2024年5月9日調整信用卡系統地址欄位時，未同步調整催收系統；另外，2022年8月調整行動銀行地址變更功能時，寫入台幣核心系統的規則設計錯誤，導致催收系統產出之簽帳金融卡、信用卡及消金產品催收信函地址異常，可能誤寄而產生個資外洩，受影響客戶數共1089人。

金管會銀行局副局長王允中，台新銀對內是未確實執行測試及驗收的作業規範，針對委外也無有效督導受委託機構建立完善的內部控制制度。對此，金管會依銀行法第129條第7款規定對台新銀處600萬元罰鍰。

本次台新銀的缺失是有客戶收到錯誤的催收帳單，並向銀行反應，公司才去清查並發現錯誤。台新銀後續也回應客戶疑問或是主動透過簡訊、信函聯繫客戶。



荷蘭男子從跳蚤市場購買裝滿醫療資料的二手硬碟

數位轉型早已深入各行各業，企業組織無一不使用電子儲存媒體來儲存重要的數位資料。令人遺憾的是，報廢資訊資產與電子儲存媒體的資料銷毀流程，仍是許多企業組織的資安破口，類似的機敏資料外洩事件仍不斷重複上演，造成無法挽回的資安與隱私侵害。

2025年2月，荷蘭發生一起震驚歐洲資安圈的實例：一名科技愛好者在跳蚤市場上，以每顆僅5歐元的低價購入多顆二手硬碟。返家檢查後竟發現，這些硬碟內儲存著大量機密醫療資料，涉及數百名荷蘭病患的個人資料，包括姓名、出生日期、地址、處方紀錄，甚至社會服務號碼（BSN）等敏感資訊。據當地媒體《Omroep Brabant》報導，這些硬碟源自一家已歇業的醫療IT公司，為節省報廢處理費用，未經任何資料清除即行出售。此類未經清除的儲存媒體一旦落入不肖之徒或詐騙集團之手，將對個人隱私與社會安全構成重大威脅，也凸顯出資訊資產報廢流程中的資安漏洞至今仍被忽略。

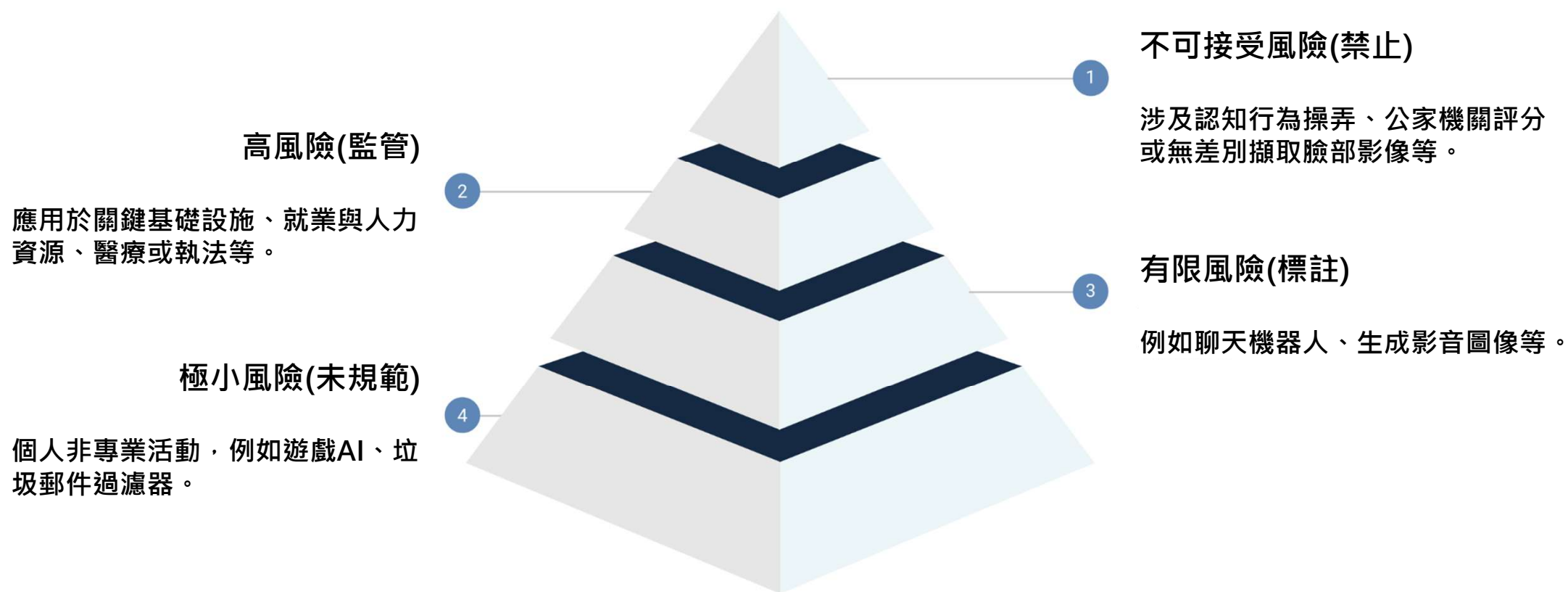


新加坡個資委員會要求企業不能用身分證號當密碼

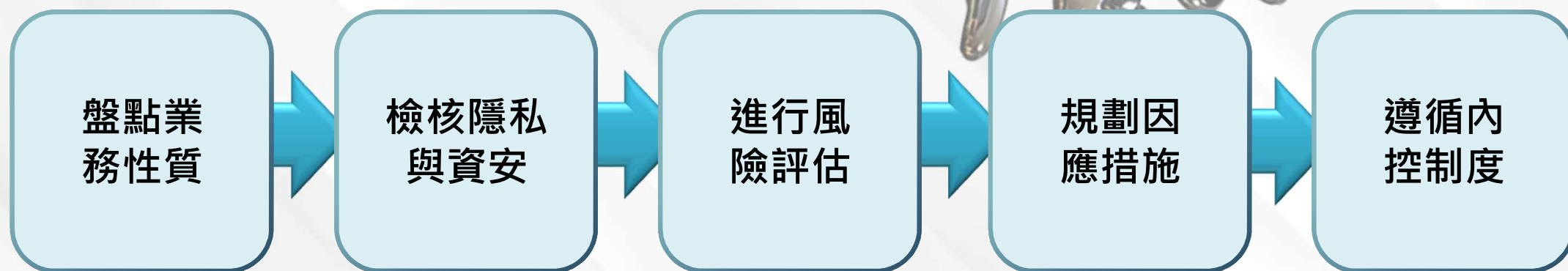
許多金融機構提供給用戶的帳單、保單檔案，大多用身分證號碼作為打開檔案的密碼，新加坡個人資料保護委員會在今年2月2日宣布，要求企業在**年底前停止使用完整的身分證號碼作為驗證顧客身份的方式，以減少個人的資料未經授權的存取。**

新加坡銀行公會（ABS）表示，多數銀行在非交易性的業務，已經不再使用身分證號碼來驗證，尤其是電子郵件附件的開啟密碼，已經不會使用身分證號。目前仍使用身分證號碼驗證的場景，未來幾個月，會改用其他替代驗證方式。

AI 風險級別



AI 風險管理



日常輔助 vs. 高風險應用

日常輔助(低風險)



整理非機密會議紀錄、潤飾公文草案、公眾法規初步查詢。



適當標記由AI生成即可。



依循一般行政責任與內控機制。



最終檢視確認。

高風險應用



自動審核民眾補助津貼、犯罪風險預測、影響人身自由的決策系統。



依法強制明確標示警語與注意事項。



需明確責任歸屬，並建立救濟、補償或保險機制。 (§17)



嚴格的人類監督與最終裁量權，不可完全自動化。



公務機關使用生成式AI指引

- 由承辦人做最終判斷
- 禁止使用AI撰寫機密文書
- 禁止向AI提供機敏資訊
- 不可作為決策唯一依據
- 使用AI時應適當揭露



新型攻擊手法讓騙過AI，可誘騙使用者執行惡意指令

資安公司 LayerX 揭露名為「Poisoned Typeface」的新型攻擊手法，攻擊者僅需透過網頁的自訂字型與 CSS 樣式表，即可騙過 ChatGPT、Claude 與 Gemini 等 AI 助理，誘導使用者執行惡意指令。此手法不需利用瀏覽器漏洞或 JavaScript，核心在於利用 AI 系統「誤將 DOM 文字內容等同於使用者所見畫面」的判讀盲點。

AI 通常僅分析網頁的 HTML 原始碼 (DOM)，但瀏覽器渲染後的畫面可透過字型映射大幅改變語意。在概念驗證中，HTML 內容看似無害的遊戲小說，但使用者實際看到的卻是執行反向 shell 的惡意指令。測試發現，主流 AI 助理皆無法識別此類潛藏威脅，甚至會向使用者保證網頁安全。

目前僅微軟對 Copilot 進行修補。LayerX 強調，隨使用者愈發依賴 AI 判斷資訊信賴度，若 AI 無法準確理解視覺呈現內容，將可能引發嚴重的資安事件。



ChatGPT 驚爆對話外洩，私人內容全被看光光

每日電訊報報導，線上研究人員凡艾斯 (Henk van Ess) 在Google搜尋結果中發現一連串涉及敏感資訊的對話紀錄，包含關於內線交易、詐欺、對哈瑪斯發動網攻計畫的討論，還有醫療和法律諮詢，以及要求聊天機器人生成兒童不雅照片等內容。

和ChatGPT等聊天機器人的對話一般屬私人性質，但用戶可透過建立超連結，在社群媒體或通訊軟體上分享對話紀錄。在部分情況下，OpenAI允許這些分享內容被搜尋引擎索引，代表它們可能出現在Google等網站的搜尋結果中。人們只要在搜尋查詢中加入「site:chatgpt.com/share」，就能查看大量他人的對話紀錄。

OpenAI資安長史塔基 (Dane Stucky) 說，「這項功能讓用戶無意間分享原本不打算公開的內容的風險過高，因此決定移除該選項，同時也著手要求相關搜尋引擎移除已被索引的內容」。



員工自建Vibe Coding應用恐暴露敏感資料

資安業者 Red Access 發表完整研究報告示警，影子 AI (Shadow AI) 的風險已從「員工將敏感資料輸入 AI 聊天工具」，擴大至「員工透過 Vibe Coding 自行建立 AI 應用、匯入內部資料並串接正式生產系統」。

研究人員在主流 AI 開發平臺上發現約 5,000 個可公開存取的企業用途 AI 應用，其中高達 40% (約 2,000 個) 含有企業營運或敏感個資，卻完全未設置身分驗證與存取控管，甚至預設開放管理者權限給所有訪客。

這類工具多由員工在未經 IT 或資安團隊審查的情況下公開上線，造成嚴重的資料暴露風險。Red Access建議，企業應建立AI應用資產盤點機制，並導入申請、審查與持續治理流程，明確規範可使用的AI開發平臺、可處理的資料類型，以及最低資安標準。



資安院發布AI代理工具資安檢測報告，籲各界謹慎使用

資安院發布報告示警，以 OpenClaw 為核心的 AI 代理工具因具備長期自主運作與高度權限，存在顯著資安風險。經實測三種威脅情境發現，OpenClaw 因「間接提示注入」弱點，會執行外部網頁隱藏的惡意指令並外傳機敏資料；安裝暗藏惡意程式的第三方技能包時也無警示。相較之下，具隔離機制的 NemoClaw 雖能透過白名單與網路隔離阻斷前兩項攻擊，但兩者在「長時間運作」情境中皆防禦失敗，主因是核心防護高度仰賴長期記憶檔（MEMORY.md），當處理大量新資訊時，原設定的安全守則會因空間壓力遭覆蓋而失效，使攻擊者能誘導其產出違規內容。

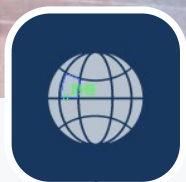
資安院建議：應實施環境隔離與沙盒模式，高風險操作必須建立人工審核機制。安裝任何第三方技能包前，先進行完整的安全檢測。定期審閱與備份長期記憶檔，避免安全設定因運作過程遺失。優先選用具備較高資安對齊（Alignment）能力的基礎模型。



公務機關不得使用 Deepseek AI 服務以防範資安風險

基於國家資通安全考量，數位發展部特別警示公務機關與關鍵基礎設施等應限制使用 DeepSeek AI 產品，以避免使用者相關數據或資訊被這類有資安疑慮的產品傳送，造成危害國家資通安全的疑慮。

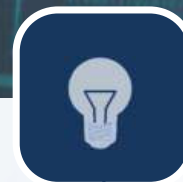
數發部表示，依行政院及所屬機關（構）使用生成式AI參考指引，業務承辦人不得向生成式 AI 提供涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題。另查DeepSeek AI 服務為中國產品，其運行涉跨境傳輸及資訊外洩等資安疑慮，屬危害國家資通安全產品，為防範公務機關內部資訊在無法有效監管的情況下外流並構成危害風險，我國從2019年行政院公布實施「各機關對危害國家資通安全產品限制使用原則」，已明確要求中央與地方機關（構）、公立學校、公營事業、行政法人以及自行或委外營運提供公眾活動或使用之場地，限制使用危害國家資通安全產品。



資安形勢分析



深化資安
防護認知



案例與啟發



法規異動概覽



Aura證實外洩近90萬筆客戶聯絡資料

身分防護服務商 Aura 近期證實發生資安事件，一名員工遭到目標鎖定型 (Targeted) 的電話釣魚攻擊，導致帳號遭駭。攻擊者在入侵後的短短一小時內，存取了約 90 萬筆客戶的聯絡資料，外洩內容主要包含姓名、電子郵件及地址。

經調查，受影響的資料源自 Aura 於 2021 年併購的一家公司所遺留之行銷聯絡資料庫，受影響對象包含約 2 萬名現有客戶及 1.5 萬名前客戶。Aura 強調，其核心身分防護應用程式的資料庫並未受損，且用戶的社會安全碼 (SSN)、財務與信用資料、帳號密碼等高度敏感資訊均安全無虞。

事件發生後，Aura 已立即停用受害帳號，通報執法單位展開調查，並同步通知受影響的用戶。這起事故再次凸顯了針對性社交工程攻擊對企業內部帳號安全所帶來的重大威脅。



駭客假借擋廣告套件誘騙使用者執行惡意指令

威脅情報公司 Huntress 近期揭露名為「CrashFix」的新型網釣手法，駭客組織 TAG-124 透過惡意瀏覽器延伸套件 NexShield 進行攻擊。該套件冒充知名的擋廣告工具 uBlock Origin Lite，並複製其原始碼以騙過 Chrome 線上應用程式商店的審核。一旦使用者受惡意廣告引導安裝後，套件會對瀏覽器進行阻斷服務（DoS）攻擊，透過無限迴圈消耗系統資源導致當機。

當使用者重開瀏覽器後，系統會跳出偽造的當機修復訊息，聲稱偵測到安全問題，誘導使用者手動開啟執行視窗並貼上指令。若依照指示操作，電腦將下載並感染 ModeloRAT 惡意軟體。調查指出，該攻擊目前偏好鎖定加入網域的電腦，顯示駭客意圖入侵企業網路以存取內部系統。此手法結合了對開源專案的信任濫用與人為製造的系統故障，增加受害者配合操作的機率。



新興網釣攻擊：JackFix 全螢幕偽裝手法

資安業者 Acronis 近期揭露新型網釣活動「JackFix」，該手法演變自 ClickFix 手法，專門針對存取成人網站的使用者進行社交工程攻擊。

駭客透過惡意廣告引導用戶進入仿冒的成人網站，當使用者點擊網頁或允許通知後，瀏覽器會強制進入全螢幕模式，並顯示幾可亂真的「假 Windows 更新」畫面。駭客利用使用者擔心成人網站不安全的預期心理，誘導其依照指示手動執行所謂的「重大安全更新」。

該畫面會封鎖 Esc 與 F12 等按鍵防止逃脫。一旦使用者誤信指示複製並執行指令，系統將透過 PowerShell 植入 Rhadamanthys 或 RedLine 等竊資軟體。

真正的系統更新不會透過瀏覽器介面要求使用者「複製並貼上指令」。若在瀏覽網頁時突然出現全螢幕更新畫面，即為典型的釣魚陷阱。



駭客濫用思科與Cloudflare服務發動網釣攻擊

資安公司 Specops 近期揭露一起針對歐洲資安業者的複雜釣魚攻擊，駭客假冒金融機構 JP Morgan 發送郵件，並濫用多項受信任的服務來規避偵測。攻擊的核心在於利用思科 (Cisco) 的郵件安全網域「secure-web.cisco.com」將惡意連結「洗白」，使資安系統將其視為安全連結而不予封鎖。

受害者點擊連結後會經過多層導向，包括 API 平台 Nylas 及遭入侵的合法網域。為了確保攻擊對象為真人而非自動化掃描程式，駭客實作了 Cloudflare 的圖靈驗證機制。通過驗證後，受害者會被導向模仿 Microsoft 365 的釣魚網頁，該網頁具備 Outlook 載入動畫效果，並會即時驗證帳號密碼的有效性。

Specops 推測駭客可能使用了名為 Kratos 的網釣工具包。此類濫用連結防護服務 (如 Proofpoint 或 Cisco) 來隱藏惡意網址的手法並非首見，反映出駭客正利用企業對合法雲端基礎設施的信任，發動更難以偵測的社交工程攻擊，藉此滲透高價值的資安研究機構。



駭客透過社交工程對IT服務臺下手，轉走員工薪資

資安公司 Palo Alto Networks 近期揭露一起名為「薪水海盜」(Payroll Pirates) 的社交工程攻擊。駭客並未直接入侵企業網路，而是鎖定提供 IT、HR 及薪資服務的服務臺。攻擊者先透過社群平台蒐集員工公開資訊，隨後多次撥打電話探查驗證機制，成功操弄客服人員繞過身分驗證，並執行重設密碼與重新綁定 MFA 裝置，進而挾持員工帳號。

奪取權限後，駭客竄改薪資系統中的銀行帳號資訊，將員工薪資轉向受控帳戶，且為了長期潛伏，還試圖透過外部信箱建立 Azure AD 的存取管道。由於變更流程看似合法，企業直到員工反映未收到薪水才驚覺受駭。Unit 42 調查證實僅特定帳號與薪資受影響，未發現橫向移動跡象，但意外在該企業的 OT 環境中發現潛伏多年的 WannaCry 勒索軟體。



荷蘭警方遭釣魚攻擊導致內部系統被入侵

荷蘭國家警察局 (Politie) 於 3 月 26 日發布公告，證實其內部系統因遭受釣魚攻擊而遭到入侵。此次攻擊被其安全營運中心 (SOC) 迅速偵測並即時阻擋，目前攻擊者的存取權限已遭切斷。警方強調，經過初步評估，影響範圍相當有限，且未涉及民眾資料或敏感的偵查資訊外洩。

目前荷蘭警方已同步展開內部調查與刑事追蹤，但尚未透露攻擊發生的具體時間、受影響系統的詳細範圍，以及是否有特定的帳號憑證遭竊。

事實上，這並非該國警方首度面臨資安威脅。回顧過往紀錄，2024 年 9 月曾發生警察帳號遭入侵事件，導致相關警務人員聯絡方式外流。後續經荷蘭情報與安全機關 (AIVD 及 MIVD) 調查確認，該次攻擊是由俄羅斯國家級駭客組織 Void Blizzard 所為。



時代力量3.3萬筆個資外流

國外資安監控網站The Daily Dark Web近日揭露，臺灣政黨「時代力量（New Power Party）」的資料庫疑似遭到入侵，約3.3萬筆個資已在駭客論壇流出。

時代力量於3/6回覆證實該事故確實發生，正持續釐清資料外洩管道。到了晚間8時，正式發布資安公告，說明其內部CRM（客戶關係管理）系統遭非法入侵。初步清查顯示，受影響資料約33,000筆，外洩欄位包含姓名、電子郵件、電話、居住地址、LINE ID、職業、生日及性別；但不包含身分證字號、銀行帳號、登入密碼或任何信用卡等財務資訊。

經初步調查，研判入侵點為內部CRM系統的權限控制遭破解。資訊單位已立即停止該CRM系統的存取權限，確保資料傳輸路徑徹底中斷。該黨特別提醒支持者，若近期接獲冒用黨部名義之不明來電、簡訊或社群軟體存取請求，務必提高警覺，慎防詐騙。



Coupang資料外洩，波及3,370萬用戶

南韓電商巨頭酷澎（Coupang）近日傳出重大資安事件，約 3,370 萬名客戶資料遭到外洩，規模幾乎涵蓋其在南韓的所有用戶。根據韓媒報導，此事故並非外部駭客入侵，而是一起由內賊發起的資料竊取事件，涉案者為酷澎的一名前中國籍員工。

該名員工早在 2025 年 6 月便企圖從酷澎的海外伺服器竊取資料，但公司直到同年 11 月才察覺異狀。初期估計受影響人數僅約 4,500 人，但在執法機構與資安公司介入調查後，確認外洩規模超過 3,300 萬人。外洩資訊包含用戶姓名、電子郵件、電話、地址及部分訂單紀錄，但不涉及支付資訊或密碼。報導指出，事件起因於公司未能妥善管理前員工的系統存取權限，導致其在離職後仍能存取敏感資料。



摩根大通受合作的法務業者連累外洩數百人資料

跨國銀行摩根大通 (JPMorgan Chase) 近期向美國政府通報，因合作之法律顧問公司 Fried Frank 發生資安事件，導致約 659 名基金投資客戶及其相關代理人的個資外洩。該法律事務所於 2025 年 10 月底發現網路共享磁碟遭駭並有檔案被竊，外洩資料包含全名、聯絡資訊、金融帳戶、社會安全號碼及護照號碼等高度敏感資訊，然而法律事務所直到 12 月才正式通知摩根大通。

摩根大通強調銀行內部系統安全無虞，並已提供受影響人士兩年的信用監控服務。事實上，高盛 (Goldman Sachs) 亦受到此事件波及而傳出投資人個資外洩。Fried Frank 聲稱目前漏洞已修正，且遭竊資料不大可能被分發或濫用。目前雖無駭客組織承認犯案，但已傳出有高盛客戶醞釀對該法律事務所提出集體訴訟。



輪胎巨擘米其林證實被竊取Oracle系統資訊

輪胎巨擘米其林 (Michelin) 本周證實，該公司因 Oracle E-Business Suite 系統漏洞導致部分資料外洩。米其林表示，僅有少部分本地資料遭非法存取，並未涉及敏感的技術資訊或 IT 系統，且強調此事件非勒索軟體攻擊，也未對其全球營運系統造成影響。

然而，根據第三方報導，勒索軟體組織 Cl0p 已在暗網公開宣稱為其所為，並釋出高達 315GB 的相關資料。米其林是眾多受害者中的最新成員，Cl0p 組織自 2025 年 11 月起，便利用該 Oracle 系統漏洞對全球百家以上的大型企業發動攻擊，其他受影響的知名企業還包括博通 (Broadcom)、雅詩蘭黛 (Estee Lauder)、馬自達 (Mazda) 及佳能 (Canon) 等。這起事故再次突顯了企業 ERP 系統漏洞所帶來的廣泛資安風險。



馬自達倉儲資訊系統遭駭，外洩員工、合作夥伴資料

日本汽車大廠馬自達 (Mazda) 於 3 月 19 日發布調查報告，證實其用於管理泰國零件進口的倉儲系統遭外部非法存取。該事故最早於 2025 年 12 月中旬發現，駭客利用營運系統的安全漏洞入侵資料庫，導致約 692 筆員工及業務夥伴的資訊外洩，包含姓名、員工編號、電子郵件及合作公司名稱等，但官方強調客戶個資並未受到影響。

馬自達表示，發現異常後已立即採取資安防護措施並通報警方，目前尚無證據顯示有進一步的間接損害，但仍呼籲受影響人員留意可能的釣魚郵件風險。值得注意的是，這是馬自達自去年底以來的第二起資安事件。去年 11 月，其美國分公司曾因 Oracle E-Business Suite 漏洞遭勒索軟體組織 Cl0p 點名，儘管當時該公司無法證實資料是否確實外流。



日本電商 Askul 公布勒索軟體事件調查報告

日本電商業者 Askul 近期針對勒索軟體攻擊事件發布調查報告，確認因物流與內部系統遭加密，導致服務大範圍中斷及約 74 萬筆客戶資料外洩。雖然官方未證實，但外媒指出組織 RansomHouse 已宣稱犯案。鑑識結果顯示，攻擊者利用業務委外端未啟用多因素認證（MFA）的管理者帳號入侵系統，並由於資料中心未部署 EDR 及 24 小時監控機制，導致異常行為未能及時被發現。

此外，Askul 坦言因既有備份架構未考量勒索軟體威脅，導致部分備份資料也遭加密，大幅增加了復原難度。目前公司已逐步恢復部分訂單受理與出貨作業，並向主管機關提交報告及通知受害者。基於社會責任，Askul 表明不與駭客交涉或支付贖金，未來將遵循 NIST 網路安全框架（NIST CSF），系統化強化存取控制、紀錄保存與監控措施。



桃園機場巴士看板出現統戰標語，後端廠商遭駭所致

114 年 12 月底，正值中國解放軍在臺灣周邊海域演習之際，大有巴士跑馬燈於 31 日清晨被發現顯示「台獨勢力必亡」等統戰口號，引發社會關注。大有巴士調查發現，事故源於凌晨 1 時伺服器遭不明人士入侵，該控管中心由中華電信維運，當日上午接獲通報後已於一小時內排除異常，且據悉另有客運業者發生類似情形。

交通部公路局對此表示，經查核確認為配合廠商後端系統遭入侵，並非客運公司本身問題，目前已要求各區監理所督導客運業者全面盤查，並落實每日出車前檢查看板資訊。國家安全局的調查則顯示，軍事活動期間政府機關網路受侵擾次數明顯增長，較平日多出逾三成，其中以 APT24、BlackTech 等駭客團體活動最為頻繁，反映出軍事活動伴隨網路攻擊的嚴峻情勢。



安永會計師事務所4 TB雲端備份不設防恐曝險

資安業者Neo Security指出，四大會計師事務所之一的安永（Ernst & Young），在Azure儲存桶存放能公開存取的BAK檔案，檔案大小高達4 TB，此為SQL Server的資料庫備份，不僅包含資料庫的結構描述，還有可能包含API金鑰、連線階段的權杖、使用者憑證、身分驗證快取權杖，以及服務帳號的密碼等機敏資訊。經過通報後，安永很快完成處理，並感謝Neo Security通報此事。

針對這起事故發生的原因，Neo Security認為與雲端環境架構相當複雜有關，一般的資安評估難以跟上步調。像安永擁有各式資源、資安團隊、完整的合規框架、ISO認證，以及充分的預算，仍可能不慎曝露SQL Server資料庫備份檔案，其他企業組織也有可能出現類似錯誤。



日本華盛頓飯店遭勒索軟體竊取資料

日本華盛頓飯店（隸屬藤田觀光株式會社）於 2026 年 2 月 14 日發布公告，確認其伺服器於前一日遭到勒索軟體攻擊並導致資料外洩。該集團在日本擁有 34 家據點，事件發生於 13 日晚間，飯店發現部分伺服器受感染後立即切斷網路，並通報主管機關與外部專家展開調查。

此次攻擊導致部分信用卡終端機暫時無法使用，但飯店表示整體營運尚未受到重大影響。經初步研判，受影響的伺服器儲存有公司業務資料，至於存放於外部管理伺服器的「Washington Net」會員資料是否遭到存取，目前仍在查證中。公告內文並未揭露具體的入侵途徑或初始細節。這是繼朝日飲料、電商 Askul、日本經濟新聞等企業後，日本近期最新一起遭到第三方存取外洩資料的資安事故。

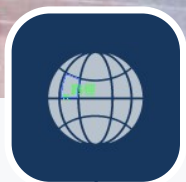


駭客濫用AI入侵55個國家配置不當的Fortinet防火牆

威脅情報團隊 Amazon Threat Intelligence 近期揭露一起針對 Fortinet 防火牆的大規模攻擊。從 2026 年 1 月起，駭客在一個月內入侵全球 55 國超過 600 臺 FortiGate 設備。特別的是，駭客並非利用系統漏洞，而是鎖定曝露在網際網路的管理介面，針對弱密碼且未啟用多因素驗證 (MFA) 的系統進行攻擊。

調查顯示，技術門檻不高的駭客高度依賴生成式 AI 打造攻擊工具。其基礎設施曝露了大量由 AI 生成的攻擊計畫與指令碼，用於自動化偵察、VPN 連線及憑證擷取。駭客在進入企業網路後，會針對網域控制器進行攻擊以獲取憑證，最終目標鎖定 Veeam 備份系統，意圖破壞備份機制以為勒索軟體攻擊做準備。

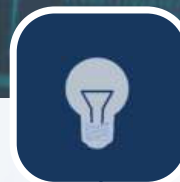
此案例突顯 AI 服務降低了攻擊門檻，使小型組織也能發動大規模偵察。然而，由於駭客過於依賴 AI 且技術能力有限，對於已採取適當防護組態或強化憑證管理的環境往往束手無策，顯示強化邊緣設備資安配置能有效抵禦此類攻擊。



資安形勢分析



深化資安
防護認知



案例與啟發



法規異動概覽

資安法修正

修正重點	委託廠商辦理資通系統或服務，其業務相關程序及環境，應具備完善之資安管理措施或通過公正第三方驗證，並應簽訂書面契約，載明雙方之權利義務及違約責任。
相關條文	§10.2、§10.3(原施行細則§4)
建議事項	檢視與確認委託廠商契約內容對資安的要求。

修正重點	公務機關不得下載、安裝或使用危害國家資通安全產品。例外得以專案方式使用，並列冊管理。
相關條文	§11
建議事項	參閱危害國家資通安全產品審查辦法之建議事項。

資安法修正

修正重點	公務機關資安專職人員 職能訓練 、 調度支援 、 適任性查核 。
相關條文	§18、§19
建議事項	依上級機關指示。

修正重點	資通安全事件，涉及個人資料外洩時，公務機關應另依 個人資料保護法 及其相關法令規定辦理。
相關條文	§33
建議事項	個資法雖完成修法，但主管機關「個人資料保護委員會」仍於籌備處階段，相關子法草案參閱後續說明。

資安法施行細則修正

修正重點	本次修正無應關注事項。
相關條文	
建議事項	主要針對非特定公務機關。

資安責任等級分級辦法修正

修正重點	公務機關經同意者，準用中央目的事業主管機關所定防護基準相關規定。(工控防護基準)
相關條文	§11.3
建議事項	與貴機關較無關聯。

附表5 C級之公務機關應辦事項修正

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		應每年至少檢視一次資通系統分級及其防護基準之妥適性。
技術面	資通安全弱點管理		知悉資通安全弱點時，應適時修補或採行緩解措施。

建議事項

依規定辦理相關事項。

附表10 資通系統防護基準修正

建議事項

系統技術細節要求規範增加，應與系統供應商確認。

資安事件通報應變及演練辦法修正

修正重點	相關條文
合併 公務機關/特定非公務機關 通報及應變資安事件規範。	§4、§5
公務機關知悉資通安全事件後，須至指定之系統平臺通報。	§6
演練相關參與人員知悉機敏資訊負有保密義務。	§17

建議事項

無重大變動。

資通安全維護計畫實施情形稽核辦法修正

修正重點	相關條文
公務機關應至 指定之系統平臺 ，提出資通安全維護計畫實施情形。	§3
公務機關應 每年訂定稽核計畫 監督其所屬、所監督之公務機關資通安全維護計畫實施情形。	§4
修正辦理稽核作業相關規定，如稽核計畫至少應包括事項。	§5 ~ §12

建議事項

無重大變動。

資通安全情資分享辦法修正

修正重點	機關接收指定情資後，應回報對應之預防或應變措施。
相關條文	§6
建議事項	建立情資分享平台，並有相關處置紀錄。

公務機關所屬人員辦理資通安全事項作業辦法修正

修正重點	相關條文
資安專職人員新增適任性查核相關規定。	§3 ~ §7
新增資安人員調度支援相關規定，公務機關應建置資通安全人員名冊。	§10 ~ §17
公務機關得自行訂定獎懲基準之獎勵情形。	§19

建議事項

評估適任性查核實務上應如何執行。

危害國家資通安全產品審查辦法

修正重點	相關條文
資通系統、服務或產品有危害國家資安之疑慮時，由上級機關提報數發部審查。	§2
公務機關接收危害國家資通安全產品情資後，應立即盤點並移除該違規產品。	§6

建議事項

資通訊設備(有連網功能者)禁止採購相關品牌產品。

個資法及相關子法草案

組織與人員配置



指派「個人資料保護長」

由機關首長指派副首長、幕僚長或一級主管兼任，負責統籌及督導機關、所屬或監督機關之個資保護事務，並直接向機關首長報告。



配置適當人力

機關除配置適當人力輔助個資長外，應指定專人辦理經常性安全維護工作。為避免利害衝突，執行管理與稽核之人員原則上不得為同一人。



個資長職能訓練要求

個資長於任職後一年內，應參加主管機關辦理之初任訓練或取得國際認可之證照（如 ISO 相關課程）。

個資法及相關子法草案

日常管理與安全維護



訂定個資檔案安全維護計畫

計畫內容須涵蓋人員管理、教育訓練、設備及場域實體安全（如門禁監控）、資訊安全（如加密及備份）等十個重點項目。



定期清查與風險評估

每年應定期盤點個資現況(建立盤點清冊)，並識別、分析流程中可能面臨的潛在威脅，依據評估結果採行適當防護。



資通系統安全控制

維運資通系統應採最小權限原則、設定複雜密碼、留存操作日誌至少六個月，並針對對外服務系統定期進行弱點掃描及滲透測試。

個資法及相關子法草案

事故應變與緊急通報



採取即時有效之應變措施

知悉事故(如個資竊取、洩漏)後，應採取即時有效措施（如隔離洩漏途徑、收回檔案、請求搜尋引擎刪除公開資訊），防止損害擴大。



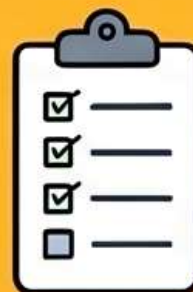
知悉事故

起72小時內



72小時內完成通知與通報

自知悉事故起72小時內，須以適當方式（或於官網公告至少30日）通知當事人，並依指定方式通報主管機關及上級機關。



通知內容四要素

應包含：

1. 事故時間與事實
2. 受影響資料類別
3. 已採取之應變措施
4. 機關聯絡方式及救濟管道

個資法及相關子法草案

監督、稽核與持續改善



每年提出實施情形報告

公務機關每年應向上級機關、監督機關或主管機關提出「個人資料保護管理事項實施情形」報告。報告內容應包含政策目標、資源投入、事故統計及稽核缺失改善計畫。



接受外部稽核與缺失改善

稽核機關每年擇定對象進行實地或書面稽核。若有缺失，受稽機關須提出改善報告(含歸因分析與矯正措施)，紀錄應保存五年。



記錄保存義務

事故處理紀錄、稽核紀錄、個資蒐集處理利用紀錄等，除法令有規定外，應自知悉或作成之翌日起至少保存五年。

結論

法規訂定時程、
實務風險變化快



資安宣導事項

- 社交工程與釣魚郵件仍為攻擊主要手段
- 市府資訊處每年兩次演練 請同仁注意
- 請遵守密碼長度、複雜度要求
- 關注市府及機關資安政策

資安宣導事項

- 下載LINE請至官方網址
- 勿下載或安裝 大陸廠牌/非屬公務用途/來源不明 之程式
- 公務信箱禁止用於私人用途
- LINE、Facebook等軟體禁止傳送個資或機敏公務資訊

I Q & A

