114年2月號

# 公務機密
# 資訊安全維護


林業及自然保育署
臺東分署

# 公務機密 資訊安全維護

# 目錄

# 【資安週報】0106~0110，臺灣電信業遭受中共網駭情形在2024年暴增6.5倍，交通與國防供應鏈也成被針對的重點

文/羅正漢 | 2025-01-12發表

在2025年第一星期資安新聞的主要焦點是，臺灣國家安全局於1月5日發布中共網駭手法分析報告，指出2024年國安情報團隊掌握我國政府及民間網駭案中，最嚴峻是以電信業者為主的資通訊領域，遭受攻擊是前一年度的6.5倍，其次是交通與國防供應鏈，遭受攻擊也比前一年度增長，顯示這些領域已是中共新興網駭重點。

此外，日本警方於1月8日發布中國駭客MirrorFace（Earth Kasha）入侵警報，揭露該組織5年間對日本發動逾200起攻擊。事實上，趨勢科技兩個月前已警告該組織利用多家品牌SSL VPN設備漏洞入侵。不僅日本企業受害，臺灣與印度也遭波及。因此日本警方此次公布的攻擊手法與偵測措施，也可供我國企業組織參考。

在資安事件方面，這一星期國內多家上市櫃公司發布資安事件重訊，其遭遇事故類型涵蓋供應鏈攻擊、勒索軟體攻擊，以及DDoS攻擊事件。

●易飛網在1月7日說明遭遇供應鏈攻擊及資料竊取，致有個資外洩。
●新海瓦斯1月9日揭露伺服器內部檔案遭受勒索軟體加密。
●悠泰科技、華航在1月7日與8日分別公布官網遭受網路DDoS攻擊。
●針對中華電信海底電纜遭貨輪破壞的事故，數位發展部表示中華電信當日已通報並啟動其他海纜備援，之後將配合海巡署、法務部、NCC與司法機關加強執法。
●資安業者Tenable傳出外掛程式更新出錯的意外事故，造成端點代理程式停擺。
在資安威脅的攻擊技術態勢上，有1則重要消息，是關於雙點擊劫持（DoubleClickjacking）手法的揭露，研究人員提醒，多數網站已能透過「X-Frame-Options header」、「SameSite: Lax/Strict」來防範點擊劫持攻擊手法，但無法因應這種新的變種手法，研究人員闡釋攻擊原理，同時建議可藉由用戶端保護方式來緩解。

還有不同資安業者公布其發現的最新攻擊手法，有3則同樣值得我們留意，包括：出現新型態的惡意JavaScript、Python、Ruby套件，顯示攻擊者正濫用oastify.com、oast.fun等新興應用程式安全測試OAST檢測服務；發現針對蘋果電腦用戶的新型竊資軟體Banshee，會冒用內建防毒XProtect的字串加密演算法來迴避偵測；俄羅斯網路犯罪論壇正兜售名為PhishWP的惡意WordPress外掛程式，可用於建立幾可亂真的付款網頁。

在漏洞利用消息方面，以Ivanti的零時差漏洞利用情形最受關注，Google旗下資安公司Mandiant在漏洞公布隔日的1月10日，發布相關研究報告，研判中國駭客組織利用此漏洞進行網路間諜活動，並揭露其攻擊手法的特殊之處是假裝系統升級成功，包括：插入惡意程式碼攔截升級執行流程，製作假的升級進度條來迷惑管理員，並繞過系統完整性檢查，假裝成為升級後的版本。

●Ivanti針對Ivanti Connect Secure等設備修補已遭利用零時差漏洞CVE-2025-0282，隔日Mandiant公布研究報告，指出該漏洞2024年12月中旬已遭利用。
●加拿大電信業者Mitel在前幾個月陸續修補MiCollab整合通訊平臺的漏洞CVE-2024-41713、CVE-2024-55550，如今被發現遭駭客鎖定利用於攻擊活動。
●Oracle於5年前修補WebLogic Server的漏洞CVE-2020-2883，當時已有資安業者指出遭駭客鎖定利用，最近美CISA將其列入限期修補的已知被利用漏洞清單。
至於資安防禦動向上，有兩則重要新聞，一是歷經18個月討論的美國物聯網裝置網路安全標章U.S. Cyber Trust Mark正式發布；通訊軟體Telegram宣布將推出業界首創的第三方驗證機制，採更主動式防護來打擊假消息與詐騙行為。

# AI時代下的資安新思維 分組式策略強化資料中心網路防護

資安人/2025 / 01 / 07
投稿文/HPE Aruba Networking台灣

生成式人工智慧（AI）技術迅速普及，不少企業開始將生成式 AI 用在智慧客服、查詢公司內部資料等方面，ChatGPT 也已是各行各業工作者必備的工具之一。當一般使用者及企業都使用生成式 AI 和其他雲端運算執行的服務，代表大量個人與企業資料需要透過資料中心網路傳輸，資料中心所要負荷的資料處理與運算量也隨之增加。且企業的網路環境涵蓋資料中心到終端裝置，若任何一段網路受駭客攻擊，將會嚴重影響使用者與企業權益。

面對潛在風險，企業管理者必須建立更全面的網路資安策略，執行「安全優先、AI 技術驅動」的資料中心網路，將能有效制定彈性、效率的網路安全政策，保護資料中心網路安全。

## 強化資料中心防護—分組式策略

分組式策略（Group-based Policy）是現今企業強化資料中心、企業雲端與行動終端裝置等各種聯網環境中的安全防護方法之一。從資安角度來看，企業網管人員需針對不同環境、流量來源，為企業網路搭配不同的資安和存取策略。而分組式策略能依據用戶行為與資安風險評估，從資料中心端到終端裝置的流量別、用戶別、上下游流量狀態，動態監控網路內各端點的資料存取，隨時進化存取管控，以達到全面且完善的防護效果。

當分組式策略應用於資料中心網路時，可以依據網路規模，落實流量分段、管理流量負載、設定存取權限，協助網管人員在網域內透過微分段，實現動態分段及更細緻且全面的資料存取控管。
動態網路分段管理於資料中心網路，不只能精準控制網路流量、限制資料東西向移動，還能隔離潛在的安全漏洞。若某一段網路遭受惡意攻擊，將不會影響其他分段網路的運作，藉此達到資安危機的範圍控制。再加上AI技術的輔助，將能更有效提升資料中心網路的管理效率與安全性。

## AI強化分組式管理效率

分組式網路管理策略的核心在於，精準控制不同應用情境與網路環境的存取行為，以高效管理企業網路、確保資訊安全。而 AI 在分組式策略中主要負責即時分析、網路威脅預測與自動調整策略，藉此即時偵測資料中心網路中的異常行為，並發出安全警報。同時，AI 基於偵測到的資訊，動態調整網路管理策略，有助於加強資料中心網路的管理彈性與效率、全面保護資料中心網路的資安。

## 分組式網路管理四大優勢

分組式的網路管理策略，為企業整體的網路資安維護帶來四大優勢。

1. 一致性：確保企業網路從資料中心到終端裝置，使用相同的網路管理策略。
2. 擴充性：隨著企業網路的規模擴大，彈性調整分組策略，不需要重新配置。
3. 精準控制：於資料中心端進行網路分段，同時搭配用戶終端控制，落實精準的企業網路存取權限管理。
4. 簡化管理：透過AI自動調整策略，降低網路管理與資安防護的複雜性，並減少人為操作失誤。

## 彈性網路架構，保護資料中心資安

整體來說，AI 時代的資安威脅形式比以往更複雜，企業需要導入全面保護雲端到終端的網路資安解決方案，才能降低駭客帶來的安全風險。尤其各行各業大規模導入 AI 應用，資料中心網路傳輸的資料量年年倍增，控制資安風險的網路管理策略更顯重要。

採用「安全優先、AI 技術驅動」的分組式策略解決方案，讓網管人員可為資料中心網路進行微分段技術和動態分段，若遭遇駭客攻擊，資料中心網路也能展開防禦並阻擋駭客橫向移動，減少安全攻擊事件的影響範圍，在資料中心網路架構變得複雜之際，精準保護現代資料中心網路的安全。

# 花蓮訪福岡交流團個資外洩「護照、戶籍全看光」 縣府道歉了

TVBS新聞網/張庭暄
2025年1月10日 週五 下午6:02
花蓮縣去（113）年12月組團前往日本福岡進行友好城市交流，並徵選多名在地專業人士一同前往。孰料，花蓮縣議員胡仁順今天在臉書稱，該交流團廠商疑似未管控好個資，導致參與民眾的護照、戶籍謄本等高達133頁個資全在網路上公開。對此，縣府也緊急致歉並下架關閉雲端系統，保障民眾權益。

花蓮縣府去年曾公布12月前往日本福岡進行城市交流參訪的資訊，同時也徵選花蓮專業人士2至6名一同前往，目的希望了解福岡國家戰略特區的成功經驗，並探索創新產業、人才吸引與政策推動。孰料，花蓮縣議員胡仁順今天就在臉書透露，該活動的廠商個資並沒有管控，只要掃碼就可以進入雲端硬碟，進一步獲得參加者的個資。

胡仁順表示「共有十數位成員、高達133頁的個資，除了個人資料，包括每個人的護照影本、戶籍謄本...通通一覽無遺」，同時他已請主辦單位花蓮縣政府行政研考處通知廠商下架並關閉雲端系統，避免更多的個資外洩問題，並呼籲若有民眾或親友參與該活動，務必向縣府行政研考處反應處理。

對此，縣府也回應，針對今天花蓮縣議員揭露資安事件，已於第一時間與承辦廠商展開各項因應措施，並處理後續事宜，特發聲明向受影響民眾表達歉意及負責態度。縣府表示，接獲通報後已立即下架相關頁面並進行全面檢視，承辦廠商同時主動聯繫受影響的民眾，對因事件造成的影響表達深切歉意，並承諾承擔本次事件損害賠償責任。

縣府說明，將依據採購契約、《資安法》及《個資法》相關規定進行後續處置，要求承辦廠商負擔契約責任，補償民眾受損權益。為杜絕同類事件重演，針對本次事件，縣府依《資安法》及《資通安全事件通報及應變辦法》進行通報程序，展開各項應變處置，並要求本次事件相關業務單位展開資安演練，強化資安防護措施，保障民眾資料安全。

花蓮縣府訪福岡交流團傳出個資外洩。（圖／翻攝自胡仁順臉書）

## 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

**Q10 何謂個人資料處理？**

**A 「處理」是指將蒐集的個人資料建立個人資料檔案，以及對個人資料檔案所做的處理，包括資料記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。**

文/iThome

# 千萬別直接把手機接飯店USB充電孔！他充電「秒跳1詭異通知」，一票人急喊：根本不敢用

（示意圖／取自photo-ac）

風傳媒 /2024-12-15 14:41
現在有不少旅館房間，不只會附設插座，也會附USB充電孔，用轉接頭就可以直接用線充電，對不少人而言是十分方便的設計。不過。近日有網友表示，到旅館把手機接到床頭的USB充電孔時，手機卻跳出「您是否要同步備份到此裝置？」的通知，讓他擔心會有個資外洩的疑慮。

**手機千萬別接飯店USB充電孔！**

近日，有網友在Threads上發文表示，日前在某財團法人附設的接待會館住一晚，把手機接到床頭的USB充電孔，我的手機就跳出1則訊息「您是否要同步備份到此裝置？」
原PO解釋，該USB port裏頭有Android 裝置，直呼自己現在USB線都買有牌子的，同時呼籲經常在手機使用行動支付或是數位銀行者，「我現在USB線是都買有牌子的了，希望比較安全。手機常用行動支付或者數位銀行，要小心USB線及充電頭的選擇」。

貼文一出，不少網友紛紛表示，「客運火車的充電孔、旅途中免費wifi也要小心」、「公共使用的都別碰為佳」、「USB線比較好的都有晶片 不過如果不放心可以找只有充電功能的線（資料傳輸腳位bypass或沒接），但功率好像都比較低」、「我都帶自己的充電頭或是行動電源」、「如果是USB線直接插牆上的USB接口，有可能接口後面有隱藏連到其他裝置，用自己帶的充電器比較保險」、「不會用不明的充電孔外出時都自備行動電源」、「在中國之前還有在車站等公共場所，假裝說自己充電寶好像壞了，要人家手機接他試插一下的。 然後接上去後，不知不覺手機裡面重要個資、支付資料都馬上被copy走」。

也有內行人解釋，現在支援高功率的Type-C 傳輸線中，都要求有可讀取傳輸線傳輸能力的晶片，「蘋果線裡面甚至要求，要有跟蘋果官方購買的已經繳了版稅的認證晶片，傳輸線裡面有晶片已經不是什麼特別的事情，還是要相信並注意手機裡面的安全性通知吧！」

事實上，根據《CNBC》報導，早在去年美國聯邦調查局（FBI）丹佛辦事處就曾呼籲大眾，「避免在機場、酒店或購物中心使用]免費USB充電座」，FBI表示已經有不法份子故意公用USB導入惡意程式和監控軟體，這種被稱為「充電陷阱」（Juice Jacking）的詐騙，民眾一旦使用，後果不堪設想。