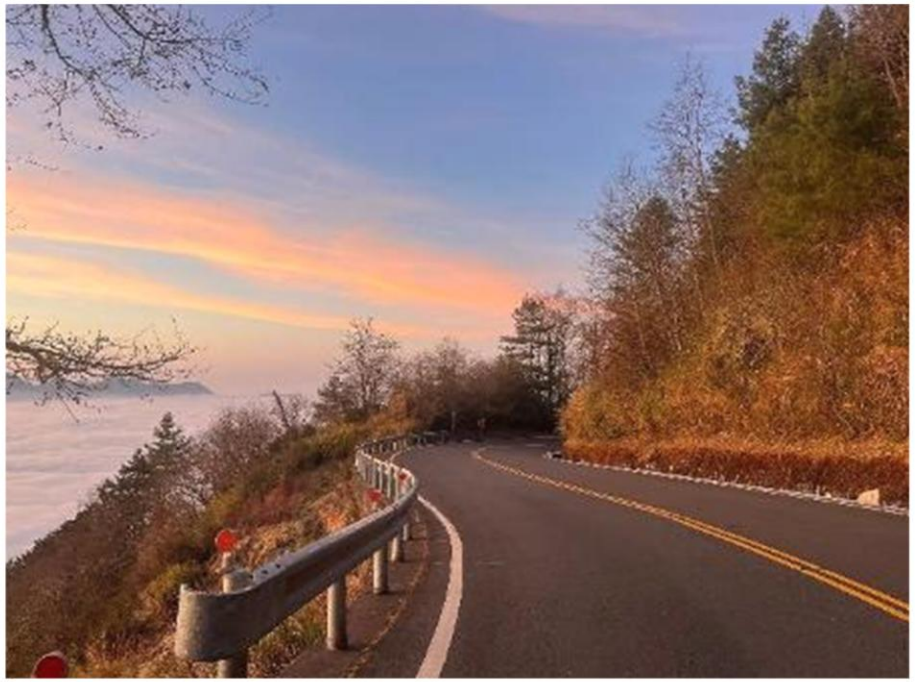
交通部公路局中區養護工程分局
Central Region Branch Office,
Highway Bureau, MOTC

中砥月刊

機關內部刊物：2026年8月號



圖：台61線161K-162K

目　錄

廉政宣導 1
反賄選專區 3
機關安全維護宣導 4
公務機密維護宣導 8
資訊安全維護 10
AI世代 12
消費者保護宣導 15
防詐騙宣導 16
反毒宣導專區 19
性別平等宣導 21
健康小百科 22
電力生活館 25
再生能源館 27
科技與生活 29
廉政相關活動資訊 33
廉政諮詢管道 35

機關內部刊物：2026年8月號中砥月刊

下一頁

廉政宣導

清潔維護採購虛浮報及驗收不實案

案情概述

甲機關A負責清潔維護採購業務，惟A虛構或浮報需求之數量、單價，並偽刻廠商印章製作不實估價單，或利用曾經往來廠商之空白收據，甚或與廠商勾結以製作不實之採購、履約及驗收文件據以簽核，使甲機關誤認為真實而核撥款項，嗣後再向廠商索取款項或朋分之。

另A亦不時要求清潔維護採購廠商以現金行賄或是假借貸名義索賄並承諾協助得標及驗收，廠商為求順利得標及驗收，遂交付相關賄款。

經法院審理，認A犯貪污治罪條例之利用職務上機會詐取財物及職務上行為收受賄賂罪，處A有期徒刑3年6月，褫奪公權1年，不法所得均沒收。

風險評估

一、未落實採購標的價格複查或訪價機制，致有浮報單價之情形。

二、採購價額數量未確實檢視過往採購紀錄，或統計當年度需求，肇生不當分批採購或招標頻繁情事。

三、依規定小額或勞務採購得採書面資料或召開審查會方式辦理驗收作業，易遭熟悉業務之人員利用，製造不實書面憑證。

四、公務人員法治觀念薄弱，誤蹈法網而不自知。

防治措施

一、業務主管及審監單位加強採購品項價格之複查機制，例如利用網路資訊、電話查價訪價。

二、參酌以往採購紀錄及年度經常性籌購數量評估集中採購，並結合開口式契約及複數決標等策略，避免同一單位或承辦人長期洽單一廠商採購，衍生廉政風險事件。

三、對於採書面或召開審查會方式驗收案件，視需要於契約內規定抽點（驗）或現場查驗機制，並填具抽查驗紀錄。

四、針對採購人員定期檢討任期，防範久任一職衍生弊端，另藉由代理制度相互審視各項購案執行情形。

五、定期針對相關採購人員等進行法治教育宣導課程。

自我檢視

一、勞務採購契約有關履約督導，有無依據給付標的之次數、範圍及單價，分別以全程督導、階段督導或重點抽查等方式實施？其督導之人員僅由承辦人員擔任是否允當？

二、針對履約之次數及範圍於廠商施作前有無達成共識，並留存預估數量訂購單或廠商確認單等書面資料據以辦理督導及驗收？

三、履約督導之結果，是否即時製作紀錄並詳實記載承商之履約狀況（如地點、時日及需改善缺失），並由參與督導之機關人員共同簽證，作為後續履約及驗收之參考？

四、辦理勞務採購書面驗收作業，相關佐證資料是否能詳實反映履約過程？另依據給付標的之不同，有無要求廠商提供簽到名冊、施作起迄日時及照片等證明文件？

五、基於勞務給付後不可查證之特性，為避免日後驗收衍生疑義，針對廠商之進出管制、安全查核、會客申請及監視器畫面，於契約結束後一定期間內是否持續保存？

參考法令

一、貪污治罪條例第5條第1項第2款（利用職務上機會詐取財物）、第5條第1項第3款（對於職務上行為收受賄賂）。

二、刑法第210條（偽造私文書）、第213條（公文書不實登載）、第215條（業務上文書登載不實）、第216條（行使偽造或不實登載之文書）。

三、商業會計法第71條（明知不實而填製會計憑證）。

四、政府採購法第70條。

資料來源：交通部公路總局廉政指引

應對進退均有據，利害關係要迴避，
請託關說要思考，廉潔自持最重要。

照片來源：台8線33K路段 篤銘橋

反賄選專區

圖文來源：臺中市政府

圖文來源：最高檢察署

機關安全維護宣導

零日滲透時代的國家安全重構 - 民主防衛體系之理論與實踐

本文從資安領域之「零日漏洞」概念為出發點，進一步轉化並建構適用於國家安全分析之「零日滲透」理論框架，旨在說明境外敵對勢力如何運用民主制度中尚未被充分識別之結構性弱點，透過認知戰、人工智慧與資訊操作等手段，在隱蔽性與低預警條件下，對政治決策與社會穩定產生實質影響。研究發現，「零日滲透」之三大影響：其一為制度導向，即以民主制度內部運作邏輯作為滲透切入點；其二為科技驅動，特別是人工智慧與演算法技術大幅提升滲透效率與精準性；其三為認知操控，透過影響輿論與社會心理，間接改變政策環境與決策方向。此類滲透行動已在選舉干預、社會議題操作及關鍵基礎設施威脅等層面呈現具體樣態。

基於上述分析，本文提出「全維民主防衛體系」之概念，主張從「法制」、「認知」與「科技」三個層面進行整合性防衛，並強調國際合作與「認知主權」之重要性。在「零日滲透」時代，國家安全之關鍵並不在於完全排除滲透可能，而在於強化制度韌性與社會承受能力，使外部干預難以產生關鍵性影響。

零日滲透成為新型國安威脅

近年來，國際安全環境已出現結構性轉變，源自國家競爭模式逐漸由傳統軍事對抗，轉向結合「資訊操控、科技運用、制度影響與認知操作」的多維度角力；基此，安全風險不再侷限於外部軍事威脅，而是深入社會內部，影響「公共輿論、政策形成與制度穩定」。

在此背景下，「零日滲透」逐漸成為重要國安概念，其原型來自資安領域的「零日漏洞」，意指系統中尚未被發現或尚未修補的安全缺口；當此概念延伸至國家安全領域時，則代表敵對勢力利用民主制度尚未被察覺的結構性弱點，在缺乏明確預警情況下，透過「資訊操作、制度滲透與認知影響」等方式，逐步改變社會氛圍與政策方向。

相較傳統安全威脅，「零日滲透」具備三項特徵：一則是隱蔽性高，往往難以透過既有安全指標即時辨識；二則是累積性強，其效果並非立即顯現，而是經長時間發酵後形成影響；三則是滲透對象並非單一機構，而是整體民主制度與社會心理。

民主制度本身的開放性與多元性，雖是其優勢所在，但也可能形成潛在漏洞，有如言論自由降低錯誤訊息擴散門檻，政治參與機制可能遭外部勢力透過輿論操作介入，而科技與法規調適落差亦容易形成治理灰色空間。所以「零日滲透」並非單純外部壓力，而是建立於制度內部特性上的「結構性利用」。

臺灣因同時具備高度民主開放環境與高強度外部壓力，成為觀察「零日滲透」的重要案例；如何在維持制度開放前提下，提升抗干擾能力，已成為當代民主國家必須面對的重要課題。

從零日漏洞到國安滲透模型

「零日滲透」的核心概念，在於敵對勢力利用制度尚未察覺的弱點，於防禦機制尚未建立前，即完成滲透與影響；其重點不在攻擊強度，而在於是否能掌握「制度漏洞、資訊落差與時間差優勢」。若以「三層次滲透模型」作為分析架構：

一、**制度層次**：民主制度中的言論自由、媒體競爭、選舉開放與法規調適遲滯，皆可能形成結構性漏洞；這些漏洞通常隱藏於制度日常運作中，不易被即時察覺。

二、**操作層次**：敵對勢力透過認知戰、資訊操控、議題設定與情緒動員等方式，將制度漏洞轉化為實際影響工具；隨著人工智慧(AI)與大數據技術發展，滲透操作更具精準性與規模性。同時，生成式AI可模擬在地語言與社會脈絡，使假訊息更難辨識；演算法則進一步放大訊息擴散效果。

三、**效果層次**：滲透行動通常不會立即造成破壞，而是逐步影響社會認知與政策方向；其結果包括社會極化、公共信任下降、政策判斷偏誤，甚至國家戰略方向改變。

故而，「零日滲透」並非單一事件，而是一種結構性、長期性且持續累積的國安威脅。

「零日滲透」的運作機制與威脅樣態

從法制面而言，民主制度的資訊自由流通雖有助公共討論，但也降低錯誤訊息進入公共領域的門檻，一旦制度缺乏有效調節機制，假訊息與操弄性論述便可能迅速擴散，影響社會判斷；同時，選舉制度也是重要切入點，外部勢力可透過操作議題、塑造輿論與影響選民情緒，對政治運作形成實質影響；此外，數位平台、跨境資金與科技發展速度快速，若法規調適不足，將形成治理灰色空間，使部分滲透行為在合法與違規之間遊走。

從科技層面而言：人工智慧與大數據已大幅改變資訊戰樣態，由於生成式AI可大量生產具在地化特徵的內容，降低辨識難度；加上演算法則偏好推播情緒性與對立性內容，進一步加劇社會極化。

從戰略層面而言：「零日滲透」往往與灰色地帶行動相互配合，包括「軍事施壓、經濟脅迫、外交孤立與資訊操控」等複合型操作，其共同特徵在於避免跨越明確戰爭門檻，以維持模糊性與可否認性。

以臺灣為例，近年已出現多元化與整合化趨勢，有如透過社群平台與自動化帳號操作選舉輿論、在能源與國防等議題上加劇社會對立、透過資安探測測試基礎設施弱點，以及利用在地組織進行長期滲透等。因此，「零日滲透」已不再侷限於單一領域，而是跨制度、跨科技與跨戰略層面的整合性操作。

民主防衛體系之理論建構

面對「零日滲透」，傳統以軍事與治安為核心的國安架構已不足以因應；所以本文提出的「全維民主防衛體系」，就在強調「制度、認知與科技」三者的整合防衛。

一、**制度防衛：**重點在於補強制度漏洞，包括強化選舉透明、政治資金監管、媒體責任與數位平台治理；同時，針對能源、通訊與交通等關鍵基礎設施，建立更完整的跨部門協調與安全標準。

二、**認知防衛：**核心在於提升社會媒體識讀能力與公共討論品質，因為認知戰並非追求立即破壞，而是長期影響社會心理；是以政府與民間需建立即時澄清與公共溝通機制，以降低錯誤訊息擴散效果。

三、**科技防衛：**透過人工智慧、大數據與異常流量分析，建立前瞻性監測與預警能力；同時，強化政府與民間在資安與平台治理上的制度化合作。

此外，筆者也提出「認知主權」概念，強調國家不僅需維護領土與制度安全，更須維持公共認知空間的自主性；當社會對重大議題的理解與判斷遭外部力量主導時，即使制度形式仍存在，其運作也可能產生偏離。

國際合作與戰略意涵

由於「零日滲透」具高度跨境性與外溢性，因此民主國家若僅依賴單一國家資源，通常難以有效因應。另因情報共享與資安合作極為重要，所以透過跨國協調，可縮短威脅辨識與回應時間差，降低資訊不對稱所造成的弱點。其次，民主國家間應建立共同規範，包括資訊治理、平台責任與資安標準等，而此種規範協調可形成「制度性防禦」，降低敵對勢力利用制度差異進行操作的空間。

對臺灣而言，深化與美日及印太夥伴合作，特別是在資安、情報與認知戰應對等領域，不僅有助提升自身防禦能力，也能形成區域層級的民主安全網絡。然而，國際合作仍面臨法律制度差異、資訊主權與互信問題等限制；因此，如何建立具持續性的制度化合作機制，就成為未來重要課題。

民主防衛面臨的挑戰

「零日滲透」最大的特徵，在於其不可預測性與隱蔽性，故而相較傳統威脅，滲透行動往往在尚未被察覺前即已展開，因此國家安全治理必須由「預防導向」轉向「韌性導向」。其次，自由與安全之間的張力，是民主防衛最大的難題，若政府過度強化監管，將被質疑侵害言論自由與民主價值；但若缺乏適度規範，又可能使制度持續遭受滲透。再者，認知戰透過長期訊息操作，逐步侵蝕社會對政府、媒體與專業機構的信任；一旦公共信任崩解，社會將更容易受到情緒與偏見影響，進一步加劇極化與制度不穩。同時，科技發展具有雙面性，所以人工智慧與大數據既可成為防衛工具，也將被利用於更精準的訊息操控。

鑑此，如何在鼓勵科技創新與防止技術濫用之間取得平衡，亦是當前民主防衛面臨的挑戰。

結論與建議：國安思維的轉型

「零日滲透」所反映的，已不只是單一安全威脅，而是國家安全邏輯的結構性轉變。敵對勢力不再僅依賴軍事壓迫，而是透過制度漏洞、資訊操作與認知影響等隱蔽手段，長期改變目標國家的社會判斷與政策環境。因此，當代國家安全已由單純防禦外部威脅，轉向兼顧制度韌性、社會信任與認知空間維護的整體性安全觀。

鑑此，筆者提出四項建議：第一，建立更具前瞻性的法規檢視與風險評估機制，強化數位平台、選舉與政治資金治理。第二，將社會韌性納入國安核心，強化媒體識讀與公共溝通能力。第三，發展AI與大數據預警能力，建立政府與民間制度化合作架構。第四，深化與理念相近國家的情報共享與資安協調，強化區域民主安全網絡。

最後，民主國家若要在「零日滲透」時代維持制度自主性與長期穩定，關鍵已不僅在軍事力量，而在於能否建立兼具開放性與韌性的民主防衛體系。

資料來源：法務部調查局清流雙月刊第64期

公務機密維護宣導

機關承辦人員洩漏職務上應秘密之訊息

解析

一、政府採購法第34條及採購人員倫理準則皆明訂採購人員應保守採購資訊，倘意圖為私人不法利益洩漏採購訊息，恐造成採購不公。

二、公告前之招標文件、開標前之領標、投標廠商名稱家數、決標前之底價均屬於法令規定採購人員應保守秘密之採購資訊。

三、倘公務機關辦理採購人員不能堅守品操，以提供招標資訊作為廠商提供賄賂或不正利益之對價，即可能觸法而身陷囹圄，應予戒慎。

案例一

A 機關技士甲，承辦道路修建工程，常以電話告知 B 公司及 C 土木包工業，某工程即將開標，或工程驗收事宜。致 A 機關110年度有5件工程採購案由 B 公司得標。

B 公司為求驗收、請款順利，出資招待甲前去有女子陪侍之處喝花酒計9次，收受不正利益價額計新臺幣1萬1,829元。

案經法院判處甲犯貪污治罪條例不違背職務收受不正利益罪，及洩漏國防以外秘密罪。

案例二

B 機關開標主持人乙於主持「多功能運動公園整建工程委託設計監造標」開標時，計有5家廠商進行價格標之開標程序，其中最低標廠商報價低於底價百分之八十。乙於宣布保留決標前，竟疏誤公布底價，致參標廠商代表人知悉底價。

案例三

丙負責截標前投標標單收件、經辦工程採購契約編製，於「汰換管線工程」開標前，洩漏投標廠商名稱、家數，或直接拆開標封洩漏廠商投標金額予特定廠商知悉，致廠商得以上開資訊評估自身投標，丙甚至以此資訊向其他廠商收取金錢獲利。

此外，丙亦曾於決標後執行業務機會，將案外廠商投標時檢附之服務建議書交付予其他廠商。

案例四

丁為某公所公用事業課課員，職司路燈公共工程採購業務，丁於簽請成立採購評選委員會及工作小組後，以電子郵件告知 C 廠商評選委員名單，最終 C 得以順利行賄評選委員獲取高分，而順利得標。

參考法條

一、刑法第132條（洩漏國防以外秘密罪）公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑。

二、採購評選委員會組織準則第6條第1項（委員名單公開）本委員會成立後，其委員名單應即公開於主管機關指定之資訊網站；委員名單有變更或補充者，亦同。但經機關衡酌個案特性及實際需要，有不予公開之必要者，不在此限。

三、採購人員倫理準則第7條第1項第7款（保密義務）採購人員不得有下列行為：七、洩漏應保守秘密之採購資訊。

四、公務員服務法第5條（保密義務）公務員有絕對保守政府機關（構）機密之義務，對於機密事件，無論是否主管事務，均不得洩漏；離職後，亦同。

資料來源：宜蘭縣政府政風處 - 工程倫理手冊

安全不會憑空來，危害常由洩密生。

資訊安全維護

從人性的弱點談社交工程的資安議題

某天下午，忙裡偷閒的小如正一邊聽著音樂，一邊和朋友聊MSN。突然，她收到好友小明傳來的MSN訊息，點開一看內容是「你現在有空嗎？」小如馬上回覆說：「沒事呀，怎麼了？」小明回應：「你可以幫我買1,000元的麥卡(my card)嗎？只要到便利商店跟店員說你要買點數卡，然後把卡片上的儲值序號告訴我就可以了，錢，我之後會給你的。」不疑有他的小如心想「只是買點數卡嘛，小事一件」，於是很乾脆地答應小明了。小明見到小如答應後便緊接著說：「可以麻煩妳現在去買嗎？我急著要用，我在線上等妳回來。」小如知道小明急著要用後，便立刻去附近的便利商店買了1,000元的my card，然後趕快回來將儲值卡的序號告訴在MSN上等待的小明；沒想到小明得到小如回覆的序號後，就馬上下線找不到人了。

小如這時心想「奇怪！怎麼跟平時的小明不太一樣，最少應該說聲謝謝或說些客套話，沒想到就這樣離線了。」過了幾天，在朋友聚餐時見到小明，也不見小明有任何要還錢的跡象，好像這件事從來沒發生過一樣。內向的小如也不好意思主動開口向小明要回這1,000元，但卻很在意這1,000是否能拿回來，於是就一直把這件事擱在心上。一個月後，小如和姐妹淘小華在下午茶的聚會上，小如就把這件事說給小華聽，請小華幫她評評理，順便問問小華有沒有什麼好方法幫她把這1,000元要回來。

圖片：鼎新數智.

不料小華一聽完小如的敘述後，直接對她說：「小如，妳被騙了！」小如很納悶地問：「被騙了！為什麼？不就是小明在MSN上跟我說要我去幫他買點數卡嗎，為什麼是被騙呢？」小華見狀便語重心長地說：「可是，妳確定請妳幫忙買點數卡的人，真的是小明本人嗎？」

以上這段故事，相信對很多人來說都不陌生，許多的人都有收過類似的訊息，這些稱為是「社交工程」(Social Engineering)。社交工程可說是利用人性的弱點，透過話術的影響力或說服力來騙取他人的個人隱私、組織機密，或是誘使從事某些交易、動作，以獲得有用資訊或不法所得的一種技巧。由於人性的因素可說是資安防護措施中最弱的一環，社交工程即是利用人性容易受騙上當的弱點，破解人性的防火牆，可說是近幾年來駭客最常用的攻擊手法。社交工程的攻擊手法有很多種，常聽到的像是上例中的MSN點數卡詐騙，此外還有像是電話詐騙、網路釣魚、圖片中的惡意程式、偽裝的修補程式等等；我們可就這幾種攻擊手法分別舉例說明。

一、電話詐騙：電話詐騙顧名思義就是透過電話進行的詐騙行為。例如常聽見的有「你的小孩被綁架了，現在正在我的手上，如果要救他的話就準備1,000萬元的贖金過來……」，或者是「我是某某檢察官，我們查到你的帳戶資料被盜用，請立刻依照我們的指示操作ATM……」、「我們是某某購物，你之前在我們這裡購買的商品因為選擇超商取貨，在付款時超商店員不小心誤選了分期付款，造成有循環利息；如果要停止的話請依照我們的指示操作……」。以上這些都是利用人性害怕的弱點，擔心不照做的話，親人可能會受害，或造成財務上的損失。

二、惡意電子郵件程式：利用社交工程的概念，將病毒、蠕蟲或惡意程式隱藏在電子郵件中。例如偽裝成朋友寄來的信件，標題為「我要結婚了」，附件放著「婚紗照.zip」要分享給收件者，但是點開壓縮檔後可能是副檔名為「.exe、.com、.bat、.scr、.pif、.lnk」的檔案。這些副檔名都是惡意程式常用的執行檔類型，一旦點開這些執行檔後，惡意程式會自動在電腦裡進行安裝，竊取電腦裡的資料或是網路銀行的帳戶帳號、密碼等資訊。

三、網路釣魚：網路釣魚泛指利用社交工程或技術性的手法，引誘使用者點擊(click)假網頁。例如偽造為拍賣網站或是電子郵件信箱，誘騙使用者輸入帳號密碼，進而竊取其帳戶資料；由於其和原網頁相似度極高，很容易誤使他人受騙點擊。常見的散布手法還有廣告信件（利用聳動的標題或是知名大廠的名義發送郵件，通知收件人必須登入連結重新驗證身分，進而竊取使用者輸入的個人資料）、網址置換（偽造網站的網址，乍看之下網址與原本官網相同，但實際上可能將英文的O置換為數字的０，英文的Ｉ換成數字的１）、縮網址（利用部分網站提供縮網址的服務，將假網頁的縮址貼在各大BBS或論壇中，誘騙使用者點擊）等等。

四、圖片中的惡意程式：透過明星或色情照片散布惡意程式，也是常見的社交工程攻擊手法之一，利用使用者的好奇心，點選圖片後就會感染病毒，造成重大損失。

五、偽裝修補程式：另一種常見的社交工程攻擊手法就是偽裝成知名軟體的修補程式（例如微軟更新修補程式），因為一般使用者並不會認為這是來路不明的程式，往往直接下載並安裝這類程式。安裝後這些惡意程式非但不能修補系統漏洞，反而有可能在使用者的電腦裡安裝遠端控制的木馬程式，竊取使用者電腦裡的資料或是側錄其鍵盤輸入的帳號密碼等資訊。

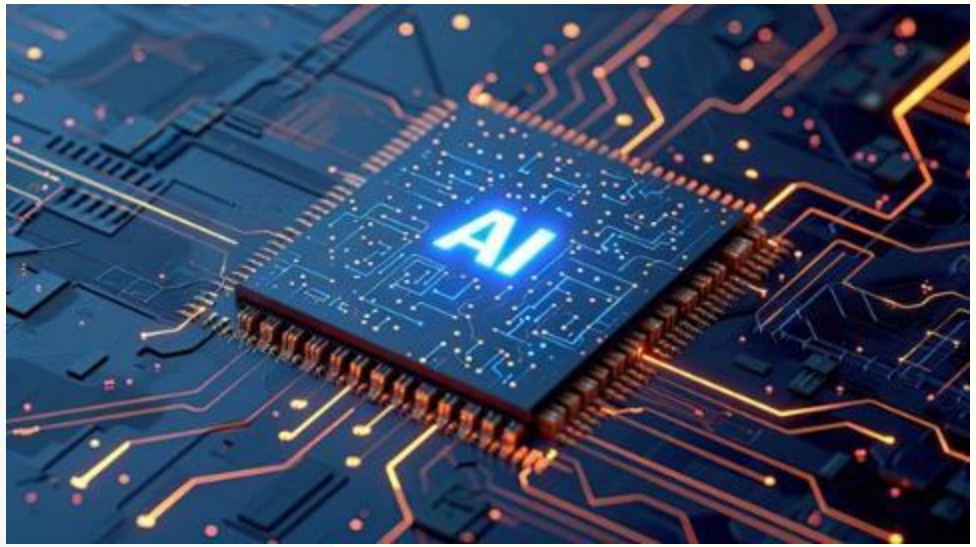
在了解常見的攻擊手法後，更重要的是要知道該如何防範。在企業中，只要員工對於社交工程的安全防範措施沒有足夠的認知或是警覺度不高，無論資安措施做得如何完善，惡意人士都可以輕易地竊取個人帳號資料、財務資料，或是公司的重大資訊。所以企業應不定時宣導及安排員工教育訓練，提高員工的警覺心及危機意識，只要出現類似的社交工程攻擊手法，都應保持警覺並小心求證。此外，員工也應遵守公司的安全政策與程序，不開啟來路不明的電子郵件或網頁；如有必要，在提供任何資訊前，也應確認要求者的身分並經過相關的授權程序。最後是建立通報作業程序，當發生疑似社交工程攻擊時，應立即與相關單位聯繫並完整通報。

社交工程主要是利用人性的弱點做攻擊，所以很難做到完全的防範。使用者只能時時提高警覺，不點選來路不明的網址及檔案，遇到任何要求時，也要盡可能地確認是否為真。只要時時具備高度的警覺心並保持危機意識，那麼社交工程攻擊一點也不可怕。

資料來源：法務部調查局101年清流月刊3月號

AI世代

AI晶片在模仿人腦嗎？什麼是類神經網路晶片？



早上出門，你一眼認出迎面走來的老朋友；搭捷運時，你瞬間聽懂廣播裡的一句話；騎車轉彎，你的手幾乎在意識到之前就已經轉動了把手。這些事情對人類來說理所當然，但如果要交給電腦，工程師可能得為此努力好幾年。

人腦在執行這一切的時候，消耗的電力大約只有20到25瓦，和一顆省電燈泡差不多。相較之下，如今支撐大型AI模型訓練與運作的資料中心，往往需要極其龐大的電力與散熱系統。這種懸殊差距，正凸顯出人腦在能效上的驚人優勢。

國立陽明交通大學電子研究所陳坤志教授，專長橫跨多核心系統晶片設計、類神經網路學習演算法、超大型積體電路架構等領域。他指出，人腦最值得AI借鏡的，不只是計算能力，而是在極低能耗下進行大量平行運算，並能在少量資料與多變情境中迅速做出決策。人腦處理資訊的方式也和傳統電腦截然不同，它不是把所有事情排成一條隊伍依序處理，而是讓大量神經元同時並行運作，像一支龐大的交響樂團，各司其職又同步演奏。

類神經網路模仿的，其實不是整個大腦

也因此，當研究者試圖讓機器學會辨識、判斷與學習時，最自然的靈感來源之一，就是人腦。

陳坤志教授解釋，人工智慧、機器學習、類神經網路、深度學習這幾個名詞經常被混用，但其實它們是層層包含的關係，不是同義詞。

- 人工智慧(Artificial Intelligence, AI)：是一個大範疇，指讓機器展現出智慧行為的各種方法。
- 機器學習(Machine Learning, ML)：是實現AI的一條路徑，核心是讓機器從資料中自己找出規律，而非靠工程師手動設定每一條規則。
- 類神經網路(Artificial Neural Network, ANN)：是機器學習裡的一種關鍵技術，靈感正是來自生物神經元互相連結的結構。
- 深度學習(Deep Learning, DL)：當類神經網路的層數堆疊得夠深、夠複雜，就發展成了近年來備受矚目的深度學習。

那麼，類神經網路究竟模仿了人腦的哪個部分？答案不是整顆大腦，而是神經元接收訊號、給予不同連結強度、最後整合成反應的基本概念。一個人工神經元接收輸入，對不同來源的訊號給予不同的權重，加總之後算出輸出，再傳給下一層神經元，如此一層一層往前傳遞，最終給出一個判斷結果。大量這樣的人工神經元連結起來，就形成了可以辨識圖像、理解語音、從資料中找出規律的神經網路。

陳坤志教授說，目前AI主要模仿的是神經元連結的抽象形式，也就是用多層計算單元與權重，從大量資料中學會辨識特徵，而不是直接重現生物大腦的完整運作機制。這確實有幾分像大腦的連結學習方式，但本質上仍是以數學方法模擬人腦的某些機制，兩者之間存在相當大的距離。

當模型愈來愈大，問題開始不只是怎麼學

類神經網路之所以有用，是因為它能從龐大的資料中找到規律。但這種方法的代價也很高。模型的層數越深、參數越多，每一次訓練或推論所需的計算量，都是天文數字。

陳坤志教授用了一個很直觀的方式區分AI的兩種工作模式。他說，「訓練(Training)」就像學生花大量時間反覆練習、累積知識的過程；「推論(Inference)」則是把學到的知識拿去應付考試或實際情境。訓練可以慢，可以用大量資源進行長時間運算，但推論不行。你拿手機刷臉解鎖的那一秒，工廠感測器判斷設備是否異常的那一刻，自駕車辨識前方行人的那一瞬間，都不容許任何等待。在推論的世界裡，低延遲是硬需求。

當AI模型的規模不斷膨脹，問題的重心也悄悄移動了。陳坤志教授指出，近年來AI的發展重心之所以從「純軟體演算法」逐漸延伸至「客製化硬體設計」，關鍵原因正是在於模型愈來愈大之後，技術瓶頸已從演算法本身，慢慢轉向算力需求、能耗需求與資料搬移成本。若繼續仰賴傳統的通用型處理器，受限於架構設計，執行AI運算時效率偏低，而且非常耗時耗電。也就是說，當AI的瓶頸從演算法轉向算力與能耗時，晶片設計就不再只是配角，而開始成為決定AI能走多遠的關鍵。

為什麼AI需要新的晶片

這也正是AI晶片愈來愈重要的原因。

傳統CPU的優勢在於通用性，它被設計來應付各種不同類型的運算，開瀏覽器、執行試算表、播放影片，全都能處理。但AI任務的核心計算，其實是大量重複且高度規律的矩陣乘法、卷積與乘積累加運算。對這類工作來說，通用型處理器並不是最有效率的選擇，就像叫一個什麼都懂的萬事通去工廠流水線上鎖螺絲－－他做得到，但不是最符合經濟效益的安排。

AI晶片的設計思路則更偏向任務導向。它不像CPU那樣以高度通用性為首要目標，而是把更多硬體資源集中在AI最常見的幾種運算上。陳坤志教授表示，AI晶片之所以比傳統CPU更有效率，關鍵在於它的硬體架構更針對矩陣乘法、卷積、張量運算與資料流而設計，因此更能做到低功耗與低延遲。此外，AI晶片更減少資料在記憶體與運算單元之間來回搬移的次數，因為每一次搬移都要付出時間與電力的代價，這個成本在大型模型的推論中累積起來相當可觀。

AI晶片的重要性，不只是「比較快」，而是它代表一種設計思維的根本轉變。過去晶片強調什麼都能做，現在則開始追求針對特定任務做到最高效率。這個方向的轉變，是被AI對算力的龐大需求步步催生出來的。

類神經網路晶片，離真正的大腦還有多遠

繞了這一圈，我們可以回頭回答題目最初的問題。AI晶片真的在模仿人腦嗎？

說它在模仿，並不算錯。今天的AI晶片更加重視平行運算、更在意功耗，也更致力讓記憶體與運算單元靠得更近，而這些恰恰都是人腦與生俱來的優勢。更前沿的研究甚至開始從硬體架構本身模仿大腦，例如讓晶片僅在輸入改變時才進行運算，減少運算功耗；或是讓儲存與運算更緊密結合，減少資料搬移的代價。

但陳坤志教授也提醒，不宜太早將今天的AI和人腦劃上等號。他認為，目前AI在高效率學習、低功耗推理、事件驅動與記憶運算融合等方面，和人腦都還有很大的差距。人腦可以從少量資料中快速學會新事物，在陌生情境裡靈活應變，全程消耗的能量少得驚人；AI則需要巨量資料支撐，不論是訓練還是推論階段，都需要付出可觀的電力成本。其根本的差異在於，目前多數AI系統仍運行於傳統馮·紐曼架構(Von Neumann Architecture)之上，記憶體與運算單元分開放置，資料得反覆搬移，而人腦的記憶與運算本就是高度融合的，幾乎沒有這些額外的成本。

陳坤志教授也指出，臺灣在晶片設計、製造、封測與完整供應鏈上擁有世界級的優勢，若能從晶片本身延伸到系統架構與整合設計，將有機會在AI硬體這波浪潮中建立真正的差異化平臺。

類神經網路晶片不是把大腦複製進矽晶片裡，而是人類在理解大腦某些資訊處理原理之後，試著設計出更適合AI任務、也更有效率的運算架構。真正迷人的地方，不是機器終於變得像人，而是科技開始重新思考，什麼才算是更聰明、更省能的計算方式。AI晶片借鏡的是大腦留下的線索，而不是大腦本身。但也正因為如此，這條探索之路才剛開始。

資料來源：科技大觀園

圖片來源：網路

消費者保護宣導

網購族看過來
網路購物及退貨
運費由誰負擔？
消費者在網路購物及退貨所產生的運費負擔規定
寄送商品費用
依零售業等網路交易定型化契約應記載事項第9點運費規定，網購時寄送商品費用可約定由業者或消費者負擔。
退回商品費用
依消費者保護法第19條規定，得於收受商品後7日內，無須說明理由及負擔任何費用或對價，以退回商品或書面通知方式解除契約。(通訊交易解除權合理例外情事適用準則所列商品或服務除外)
購買
消保Q&A
行政院消費者保護處
廣告

郵輪團體旅遊
注意事項
與一般團體旅遊最大不同點
郵輪旅遊的「郵輪」是「交通工具」，也是「旅遊地區」
消費者參團郵輪旅遊，有「郵輪國外旅遊定型化契約應記載及不得記載事項」規定適用
旅行業者與消費者簽約前
1、提供消費者至少3日契約審閱期間。
2、向消費者明確且清楚說明並提供郵輪相關資訊，包括
(1)郵輪艙房預定之付款條件、取消、變更及退款等資訊。
(2)遇有不可抗力因素致變更行程及退款賠償等資訊。
(3)郵輪內設施使用規定等相關資訊。
法規連結
行政院消費者保護處
廣告

防詐騙宣導

【網購詐騙】十大流行話術公開！看到這些關鍵字請提高警覺

網購方便快速，也成為詐騙集團鎖定的目標。近期常見手法包括「訂單誤設分期付款」、「系統升級需重新驗證」、「請依指示操作ATM」、「加入LINE客服協助取消訂單」等，甚至利用中獎通知、超低價促銷、先匯款保留名額等方式，引導民眾一步步落入陷阱。

警方呼籲，任何要求私下交易、離開官方平臺付款，或要求提供個資、驗證碼及操作ATM的訊息，都應立即停止並向官方客服查證。如發現疑似詐騙，可撥打165反詐騙專線尋求協助，避免辛苦存下的錢落入詐騙集團手中。

資料來源：165全民防騙

【心理測驗，小心變成盜帳號陷阱！】

最近網路流行各種MBTI、性格分析、ADHD、焦慮測驗，但有些其實是詐騙網站！

詐騙集團會架設心理測驗網站誘導你點擊，要求登入Facebook、Instagram或分享到Threads解鎖完整報告，等你輸入帳號密碼、同意授權後，社群帳號就可能立即遭到盜用！

📢防詐提醒

- ✅不明網站不要登入社群帳號
- ✅不要隨意授權第三方應用程式
- ✅開啟雙重驗證，提升帳號安全

資料來源：165全民防騙

⚠你也愛用手機付款嗎？

如有使用台灣Pay等支付APP。TWQR最新詐騙手法一定要知道！

詐騙集團假冒銀行客服以「金流驗證」為由，要求截圖或翻拍提供「QR Code付款碼」，一旦給出去了……就會被拿去超商盜刷遊戲點數等虛擬商品，錢就這樣被騙走了！💸

🚨 **請大家牢記：**

出示「QR Code付款碼」＝同意付款❗

要求截圖或翻拍QR Code付款碼就是詐騙！

🚨 **防詐4提醒，守住辛苦錢：**

✓不提供QR Code付款碼給他人。

✓金融機構及政府機關不會以電話或簡訊要求截圖或翻拍QR Code付款碼。

✓接到異常通知，洽金融機構官方管道查證。

✓如有疑慮，立即撥打165反詐騙專線。

TWQR掃碼結帳很方便，但付款碼一定要保管好。
記住三不原則：不翻拍、不截圖、不傳送
保護自己的財產，遠離詐騙風險！✋

資料來源：財政部臉書

反毒宣導專區

抽電子煙一點都不酷！

近9成的電子煙油都含有尼古丁，不肖業者常以酷炫的外型，吸引青少年使用，但真相並不是行銷話術所稱的「減害」、「可幫助戒菸」。

使用電子煙一樣會對尼古丁上癮，除此之外，近期也發現有許多來路不明的電子煙內含毒品成分，在此認真的向大眾呼籲不要拿自己的健康當賭注！

另外，電子煙在我國不是合法的產品，販賣及使用皆會受罰，若查獲電子煙內含毒品成分，更是涉嫌違反毒品危害防制條例；呼籲民眾不買更不賣電子煙，切莫以身試法！

資料來源：睡睡平安

資料來源：睡睡平安

類鴉片止痛劑避雷指南💊

一般止痛藥救不了的中度至重度疼痛，醫師才會請出像是嗎啡、吩坦尼等「類鴉片止痛劑」

雖然是止痛神隊友，但亂用真的會出代誌💀

🤢 類鴉片止痛劑

- 成癮性麻醉藥品
- 我國列管為管制藥品

🚫 使用避雷指南請牢記

1.勿同時飲酒

2.勿自行調整劑量

3.勿操作危險機具、開車

4.勿與他人分享

💡 懶人包

乖乖聽醫生的話你就是管藥神隊友

資料來源：睡睡平安

資料來源：睡睡平安

性別平等宣導

勇敢追夢的數學天才！世界第一位女性數學教授－索菲亞・科瓦列夫斯卡婭

你能想像，在女性連大學都難以進入的年代，仍有人努力突破限制、勇敢追夢嗎？

19世紀的俄羅斯，女性若想出國留學，必須取得男性監護人同意。熱愛數學的索菲亞，為了追夢，直接把人生玩成「解鎖任務模式」，即使關卡重重，她還是一路把數學技能點滿，最後成為世界上第一位女性數學教授！

資料來源：性別平等觀測站

女孩可以不再當「配角」，女性更該為自己而活！

英國最新研究指出，許多青少女傾向透過男孩視角審視自我，並承擔過多情感照顧責任，顯現傳統性別角色與厭女文化對心理健康的深遠影響。

但女孩不該只為了迎合他人期待而活，應勇敢找回自我主體性；同時，男孩的心理情感需求，也同樣需要被社會正視與理解。

我們應該要消除刻板印象、偏見與歧視，拒絕性別框架，讓每一個人都可以活得精采。

資料來源：性別平等觀測站

健康小百科

血管清道夫！專家票選「防血管阻塞」十大食物：酪梨、這杯茶助血管回春！

魚油含有omega-3能促進心血管健康，所以像鯖魚、沙丁魚等魚類都被視為有益心血管保養、護心護腦的食物。但最近一項有趣的票選出爐，專家眼中最強「血管清道夫」食物第一名居然勝過吃魚，連常見顧血管聖品酪梨、醋都無緣爭冠，快來看看血管到底最希望你吃哪些東西？

提高血管力！專家票選「防血管阻塞」最佳食物排行榜

日媒《女性seven》為了瞭解專家心目中改善血液循環、提高血管力、防止血管阻塞的最強食物是什麼，特別找來20位營養師、醫學博士、教授、各科醫師等專家投票，在各類食物中被專家票選第一名的食物計5分、第二名計4分、以此類推，第五名則計1分。分數加總後，最終票選出「防止血管阻塞的食物排行榜」如下！

第十名(6分)：醋

內科醫師佐佐木歐等人說明，醋的主要成分為醋酸，能降低血壓、內臟脂肪，對預防動脈硬化也有效果。雖然喝醋有改善血液流動的效果，但醋要注意別攝取過量，尤其是空腹食大量飲用未經稀釋的醋，可能導致腸胃不適。

第十名(6分)：核桃

心臟科醫師梅津拓史表示，核桃同時含有能抗氧化的多酚，以及優良油脂Omega3脂肪酸、能抑制膽固醇氧化的維生素E，以及能緩和血糖波動的膳食纖維，大大為健康加分！

第九名（7分）：麻薏

麻薏又稱埃及國王菜，是營養價值非常高的黃綠色蔬菜，除了是臺中的在地美食，近年來也被引進日本開始大量栽培！營養師菊池真由子等人解釋，麻薏富含β-胡蘿蔔素、多酚、維生素E，能幫助去除活性氧類、抑制鹽份與膽固醇吸收，讓血管重返年輕，降低心臟疾病、腦中風風險；而且它富含水溶性及非水溶性膳食纖維，預防血壓上升、防止動脈硬化。

東京都健康長壽醫療中心院長井藤英喜也表示，麻薏的胡蘿蔔素含量在眾多蔬菜中名列前茅，具有延緩細胞老化、強健血管、黏膜的功效，是非常推薦常吃的蔬菜！

第六名（8分）：南非國寶茶

南非國寶茶又稱博士茶，因無咖啡因、無熱量，又能預防老化、生活習慣病的特性而受到矚目，也被認為能活化微血管、鞏固血管壁，日本金澤醫科大學副教授赤澤純代曾建議一天飲用3杯南非國寶茶。

哈佛大學客座教授、抗老專家、內科醫師根來秀行等人說明，南非國寶茶能活化血管內一種稱為Tie2的受體，Tie2主要是用來維持血管發育的重要遺傳因子，是強化微血管的必須物質，十分推薦民眾將喝南非國寶茶養成生活習慣。

第六名（8分）：酪梨

營養師菊池真由子等人說明，酪梨有優良油脂油酸，更富含能抗氧化、預防動脈硬化的維生素E、防止血管老化的β-胡蘿蔔素、將多餘鹽分排出體外的鉀，推薦民眾定期食用酪梨。

第六名（8分）：鰹魚

營養師堀知佐子等人說明，鰹魚富含DHA、EPA，有促進血液流動、維持血管健康的效果。此外，鰹魚還富含優質蛋白質，與幫助蛋白質代謝的維生素B6，列為超級食物當之無愧！

第五名（9分）：肉桂

專長研究人體血管的大阪大學教授高倉伸幸等人說明，肉桂能活化血管細胞，特別可期待其維持微血管年輕的效果，是預防微血管老化變成「幽靈血管」的最佳對策！

第四名（15分）：洋蔥

營養師望月理惠子等人解釋，洋蔥的香氣成分大蒜素增加血液中的好膽固醇、減少壞膽固醇；能抗氧化、防止動脈硬化的槲皮素也十分豐富；又富含膳食纖維，能抑制血糖急速飆升傷血管，是對血管非常友善的食材。

有「醫療雜學王」之稱的日本名醫秋津壽男也曾於日本健康節目《主治醫老實說》中公開，自己用洋蔥皮煮茶喝，至今喝了10多年，甚至一天會喝3杯，藉此攝取洋蔥皮中有助抗氧化、抗發炎、調節免疫的槲皮素，讓血管保持年輕狀態！

第三名（20分）：沙丁魚

心臟科醫師野田泰永等人說明，沙丁魚中富含EPA，有預防血液凝固、促進血液流動的效果，推薦以罐頭食品輕鬆攝取。沙丁魚因為屬於較小的魚類，和大型魚類相比，受海洋污染的影響較小也是優點之一。

第二名（21分）：鯖魚

立命館大學運動健康科學院教授家光素行說明，鯖魚的DHA、EPA有增強血管彈性、預防血栓的效果，對預防腦梗塞、心肌梗塞非常有效。這些Omega3脂肪酸還能提升代謝，也非常推薦在意肥胖的民眾食用，建議以蒸煮等方式料理，避免油炸。

第一名（29分）：納豆

你猜到了嗎？日本20位專家們所票選，「防止血管阻塞食物排行榜」中排序第一的食材就是納豆！心臟科醫師梅津拓史等人說明，納豆激酶能溶解形成血栓的纖維蛋白；由於納豆的原材料為大豆，富含大豆異黃酮能預防心血管疾病，經發酵製成那道後該效果更加分；大豆異黃酮、皂素、植物固醇能改善血液流動，防止血管受傷。

資料來源：早安健康

圖片來源：cl terry

電力生活館

省電小撇步

白天出門前你拉上窗簾了嗎？

晚上下班回家踏進家門。哇！怎麼還是這麼熱！都天黑了為什麼室內溫度還是這麼高呢？

原來，有一大部分原因是「輻射熱」惹的禍！

夏天太陽毒辣，曬到家裡的傢俱、地板吸熱一整天下來也讓室內溫度上升不少。

有沒有辦法讓室內不要這麼悶熱呢？

有的！只要一個簡單的小動作就可以囉～那就是……在平日白天沒人在家，出門前記得先「拉上窗簾」，就可以阻擋輻射熱進屋肆虐喔！

如果是有陽台的落地窗，可以在窗外掛上竹簾，減少陽光直接照射到玻璃進屋（這樣效果最好），若是窗外不能掛簾子則可採用90%以上遮光窗簾。

要特別注意窗簾的尺寸要比窗戶稍微大一些，這樣才能阻止熱能進入屋內喔！

資料來源：台灣電力公司

用電安全

你家延長線幾歲了？你家的延長線是不是該換新了呢？

有網友曾討論延長線使用多久需更換？小編覺得可視使用情形來更換延長線。像是使用頻率高或長期高負載情況下耗損度就會增加，當電線有破損、外露等狀況要立即更換新的才比較安全。

延長線不當使用易釀災，所以要注意：

◆請勿綑綁、拉扯及放置在高溫旁使用

◆使用時注意負荷量

◆經常檢視上方的插頭及插座，是否有鬆動、焦黑、綠鏽或累積灰塵現象

若是家裡的延長線已使用多年的話，可考慮換新。

建議購買有「商品安全標章」&有獨立開關&具有過載自動斷電保護功能的延長線，以「額定電壓125V、額定電流15A、額定容量1650W」的規格最理想！

資料來源：台灣電力公司

再生能源館

生質能也能變成燃料？！你知道嗎

以廢食用油、能源作物或藻類等有機物為來源，透過轉化技術製成的「液態生質燃料」可依燃料特性，直接或與傳統燃料混合使用，可替代部分化石燃料兼顧資源循環利用與減碳效益。

「液態生質燃料」兩種常見基礎類型：

【生質柴油】

- ◆原料來源｜廢食用油或大豆、微藻等高油脂作物或藻類油脂
- ◆轉化技術｜透過「轉酯化反應」等轉化技術製成的油品
- ◆命名規則｜通常在前方冠以B字頭，代表與傳統柴油的混合比例（例如：B20代表含有20%的生質柴油）

【生質酒精】

- ◆原料來源｜醣類、澱粉、纖維素等生質物
- ◆轉化技術｜經醱酵、蒸餾與脫水後製得的乙醇，可混入汽油中製成「酒精汽油」
- ◆命名規則｜通常在前方冠以E字頭，代表與傳統汽油的混合比例（例如：無鉛汽油中含有10%生質酒精，就稱為E10）

液態生質燃料應用場景有哪些：

■酒精汽油（低碳汽油）：在車用傳統汽油中摻配生質酒精（如E10），實現一邊開車一邊低碳排！

■永續航空燃料(SAF)：由生質酒精、廢棄食用油或農業廢棄物製成，可與傳統噴氣燃料混合使用。相較傳統航空燃料，其整體生命週期溫室氣體排放量最高可減少約80%。

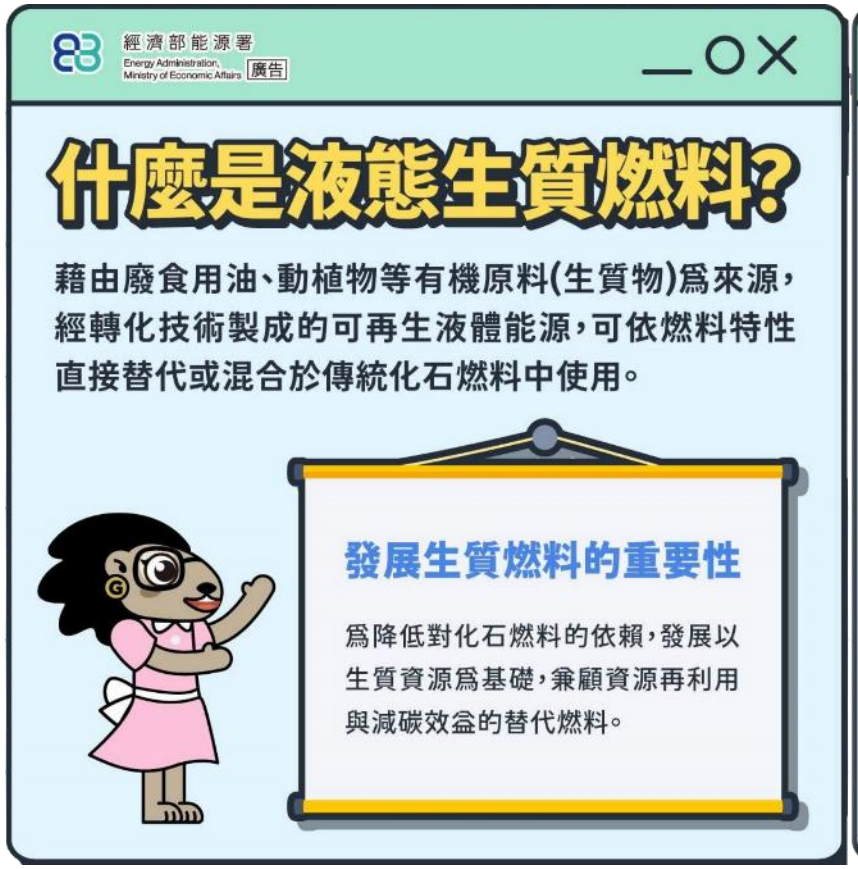
■綠色船舶燃料包含以下兩種主要類型，作為柴油動力引擎的燃料：

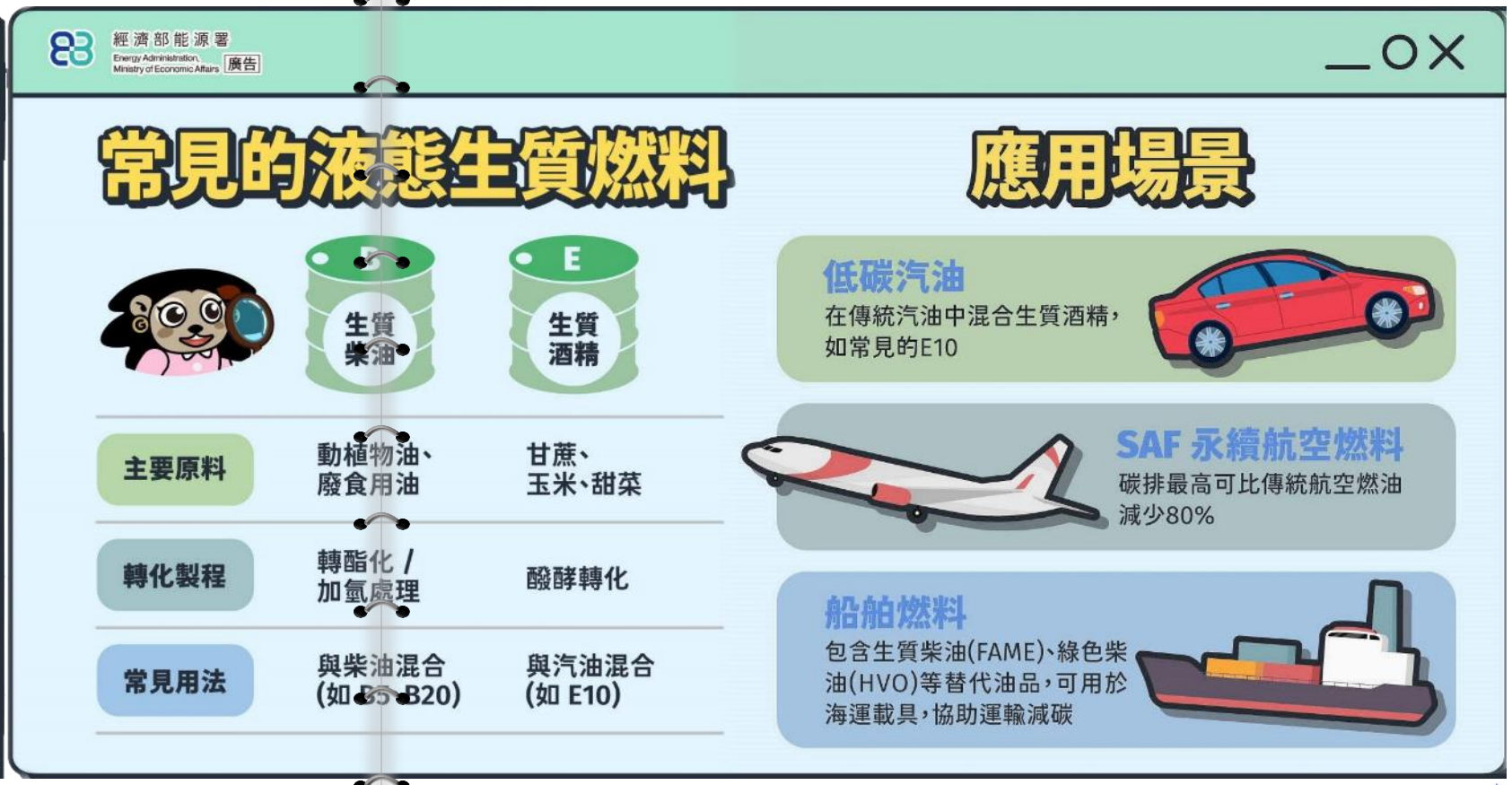
①生質柴油(FAME)：具有生物可分解和無毒等特性。通常需依特定比例與化石柴油調和。

②綠色柴油(HVO)：經高溫氫化處理去除雜質，潔淨度與穩定性高。化學組成與化石柴油相近，部分產品可直接作為替代燃料。

從廢食用油到減碳運輸燃料，生質能正透過資源循環利用，為交通運輸減碳與能源轉型帶來更多可能！

資料來源：再生能源資訊網





科技與生活

認識BED(Banana Equivalent Dose)：輻射界的「香蕉刻度」

你知道嗎？科學家和科普工作者有時會用一個有趣的概念來幫助大家理解輻射劑量：

🍌1BED=1根香蕉的等效輻射劑量(Banana Equivalent Dose)

因為香蕉富含鉀，而天然鉀中約有0.012%是具有放射性的鉀-40，所以吃下一根香蕉，大約相當於接受0.1微西弗(μSv)的輻射劑量。

先別緊張！

人體本來就含有天然的鉀與鉀-40，而且身體會維持鉀的總量平衡，多攝取的鉀通常會隨代謝排出，因此偶爾吃香蕉，體內的放射性並不會一直累積。

所以，你可以把BED想成一種生活化的比較尺度：

🍌吃1根香蕉≒1BED

☠️一次牙科X光≒數十個BED（依檢查種類而異）

✈️搭一次臺北到東京的飛機≒數百個BED

🌍我們每天也都持續受到來自宇宙、土地與食物的天然背景輻射。

不過要注意，BED並不是正式的輻射單位，而是一種科普上的幽默比喻，幫助大家理解「輻射其實無所不在，而且不同來源的劑量差距有多大」。

資料來源：核安會輻務小站

氣候走向極端：預測模型與調適科技重建防災思維

臺灣的氣候風險從過往偶發的災害事件，轉變為長期且結構性的環境壓力。
（圖片來源Shutterstock）

近年襲臺的颱風減少，雨勢卻愈發猛烈。臺灣曾面臨北部的缺水恐慌與南部的分區限水，轉瞬間卻又因突如其來的暴雨引發城市淹水。這種極端趨勢揭示了氣候變遷最明確的訊號：雨量強度雖增，下雨天數卻減少，形成「乾者愈乾、濕者愈濕」的顯著對比。臺灣的氣候風險已悄悄從過往偶發的災害事件，轉變為長期且結構性的環境壓力。

而在這場氣候挑戰背後，國家災害防救科技中心氣候變遷組陳永明組長，與國立臺灣大學大氣科學系許晃雄合聘教授，分別從災防科技與氣候模型角度，觀察臺灣如何重新建立面對極端氣候的調適能力。

陳永明組長指出，傳統防災處理即時預警與災後重建；研究氣候變遷則是面對未來才會浮現的災害風險。當威脅從暫時的意外轉為長期的常態，社會便需要一套更具韌性的生存策略。為此，臺灣科學界正整合氣候模型、大數據與AI技術，將複雜的科學資訊轉化為「氣候風險地圖」，透過智慧調度與風險分析，讓水資源、能源規劃乃至城市建築設計都能在變動環境中維持運作，逐步建立守護未來的調適能力。

護國神山源於地形區域模型透視兩公里差異

要理解防災思維的轉型，必須先回到核心問題：氣候到底能不能預測？許晃雄合聘教授指出，雖然微觀變數不斷，但長期氣候變遷的趨勢訊號非常清晰 - 「變冷的時間變少，極端熱的發生機率正不斷攀升，未來臺灣出現超過40°C高溫的機率將逐漸提升。」

更關鍵的挑戰在於氣候訊號背後的時間結構正在改變。許晃雄合聘教授解釋，熱浪通常具備幾天前的可預測性，但下個季節是否乾旱、瞬間降雨量是否破紀錄，仍是全球氣候科學努力突破的範疇。目前較可靠的季節預報來自聖嬰與反聖嬰現象，以2021年為例，臺灣逢連續反聖嬰導致冬、春兩季的雨量銳減，再加上2020年夏季缺乏颱風供水，便演變成較長期的乾旱壓力。

然而季節預報並非鐵律。許晃雄合聘教授舉2009年的莫拉克颱風為例，那年原本降雨少，如果持續偏少很可能是乾旱年，莫拉克的出現卻瞬間灌飽水庫，使全年的累積降雨量看似回歸正常，實則造成嚴重水災。這種個別極端事件難以提前預測，因此臺灣氣候科學界在季節預報外，更納入「次季節預報」(Sub-seasonal forecast)，透過未來一到兩週的滾動式更新，不斷微調與修正預測訊號。

關於如何將全球氣候模式精準對準臺灣，許晃雄合聘教授笑著說：「其實高聳地形不見得是護國神山。」中央山脈雖會降低颱風強度，卻也因地形抬升作用讓颱風帶來的降雨量倍增。由於全球模式的大尺度數據解析度無法捕捉臺灣複雜的地形差異，科學家進一步發展「區域氣候模式」，運用大範圍的系統變化作為驅動資料，將空間預測解析度精細化至兩公里，以便更細膩地分析特定區域的雨量增減趨勢，提供政府單位符合臺灣地形細節的決策依據。

冰冷數據對接生活體感跨域調適串聯農田與都市

當科學模型推估出高解析度的局部區域氣候趨勢後，如何將不確定性的數據轉化為各行各業「聽得懂、做得到」的行動，是災防科技中心氣候變遷組的核心使命。陳永明組長說明，面對長達數十年的趨勢推估，氣候變遷組扮演國家級的「資料加值與轉譯中樞」角色，將輿論中全盤否認的懷疑論，或是拋出的末日式渲染進行理性轉譯，把科學模型推估的不確定區間，轉換為不同部會能實際操作的風險指標。

陳永明組長以農業的「熱緊迫」(Heat Stress)為例，這是指動植物因環境的溫度與濕度超過其生理極限而無法有效散熱時，導致體內恆定受破壞的壓力反應。在實務上，高溫會直接導致乳牛泌乳量下滑、品質變差，蛋雞的產蛋率也會隨之受挫。當災防科技中心與農業部畜試所合作將氣候推估數據與產量模型對接，農業部便可評估提前從品種改良、飼料調整與養殖環境降溫等面向找出系統性的調適做法。「同樣的高溫，人類體感是36°C到38°C，但對芒果、火龍果和荔枝等作物而言，其耐受門檻值完全不同。」陳永明組長強調，調適無法單打獨鬥，必須由科學家與各領域專家共同跨界合作。

城市的「韌性設計」則是另一個看不見硝煙的戰場。隨著熱浪成為新常態，都市建築不能再一味依賴冷氣，或任由大樓玻璃帷幕將熱能反射到街道上，造成「自己不熱、別人很熱」的惡性循環。這背後牽涉的治理網絡極為錯綜複雜，涵蓋國土規劃、都市開發、能源管理及高溫健康預警等。陳永明組長點出調適思維的關鍵核心：「在升溫環境中，你究竟是『造成熱的人』，還是『受熱影響的人』？釐清這兩種角色，跨部會合作才能依據科學數據，推動因地制宜的空間重組與制度防禦。」

世紀大旱倒逼智慧調度 - AI提前洞察致災徵兆

如果高溫熱壓力是悄然逼近的慢性病，水資源短缺就是臺灣感受最直接、也最早被氣候變遷衝擊的致命要害。陳永明組長指出，水資源調度的複雜度牽涉到民生、產業與農業用水，三者之間的優先權分配與公共安全。短期而言，相關單位從每年年初的整田期便展開嚴密監測；一旦旱象出現，即啟動緊急應變機制召開協調會。長遠來看，水利署依據氣候變遷推估資訊，納入「水資源經理計畫」的修訂，打造貫穿全臺的水資源防禦調度網「珍珠串計畫」，透過跨區聯通管網將全臺主要水庫與淨水場如珍珠般串聯支援，降低枯水期分區限水風險，穩定民生與產業用水。

然而，氣候變遷最棘手的核心在於無法預期的極端劇本。陳永明組長回顧，2020年至2022年間臺灣遭逢罕見的氣候型態，連續3年幾近所有颱風中心都未登陸，直接導致百年大旱。這種極端場景過去較難被納入傳統的水資源歷史經驗，而這正是AI與長期氣候大數據展現價值的關鍵時刻。陳永明組長強調，在跨越數十載的豐富歷史數據與未來模擬的資訊中，由AI協助識別極端旱象特徵的致災徵兆，是過去人工難以企及、卻是機器演算大數據最擅長的強項。

在這場智慧調度戰役中，災防科技中心在國科會補助下建立「臺灣氣候變遷推估資訊與調適知識平臺(TCCIP)」，將繁複的氣候模式轉化為可運用的資訊，統整提供給全國各領域，讓水利署的水資源政策、農業部的作物品種布局以及能源主管機關的電力供應規劃，都能在同一套科學基礎上進行跨領域的風險溝通與政策協調。

科學數據指引邊界 - 多元共識建構韌性社會

面對氣候變遷的高度不確定性，打造韌性社會的核心不在於科技萬能，而在於社會共識的凝聚。這份共識因各地的產業型態、人員結構與環境脆弱度而異，並沒有標準答案。韌性的本質正是多元與彈性，需要大眾轉變思維，將極端天氣視為必須長期共存的「新常態」，而非暫時的意外。

建構理性共識的前提是理解科技的極限。如許晃雄合聘教授所言，氣候模型再先進也有其物理邊界，例如颱風愈接近臺灣，雨勢因地形抬升而增強本是物理事實，並非預報失準。看清盲區不代表科學退場，而是提醒決策者不能盲信單一絕對數值，必須依據多元科學素材進行結合機率與趨勢的風險決策。

當「韌性」從強硬的工程防禦轉化為彈性調配與跨域協作的社會能力時，預測模型、AI風險分析與智慧調度網才能發揮真正的治理價值。因此，必須讓關注「未來災害風險」的氣候調適，與應對「當下即時危機」的防災科技雙軌並行，才能在變動中守住社會的基本運作。

數據驅動的防災新思維正重新定義臺灣面對極端氣候的姿態。科技為我們劃出未來的風險邊界，而賦予了數據溫度與彈性的調適力，才是引領這座島嶼在氣候洪流中，踏出堅定步伐的靈魂核心。

資料來源：科技大觀園

廉政相關活動資訊

「炎夏『漫』活，創意說『畫』」

活動目的

本活動希望透過舉辦漫畫與創意短片徵選活動，鼓勵學生以漫畫特有的聯想、詼諧、幽默及創意短片製作之方式，引起學生對反詐騙、洗錢防制、反酒駕、反毒、反賄選及兒少私密影像保護等犯罪預防議題的注意，建立正確認知並了解其危害，讓預防被害觀念向下扎根，達到預防犯罪、減少被害之目的。

參賽資格

凡對漫畫與短片創作有興趣之在學學生皆可參加，每組投稿件數不限，但得獎作品限一件並以最高得獎金額之獎項為主。

徵件報名期間

一、報名時間自115年7月1日（三）10:00開始至115年10月1日（四）18:00止

二、活動詳情及線上報名請至活動網站：

- 活動官網：https://www.2026mojgov.com.tw/
- Mor狀元-兒童及青少年犯罪預防宣導網粉絲頁：https://www.facebook.com/tpmr.tw

「菜奇鴨＆夜奇鴨守護府城．反賄選知識大挑戰」網路有獎徵答活動

為提升全民反賄選意識，臺南市政府政風處推出「菜奇鴨＆夜奇鴨守護府城．反賄選知識大挑戰」網路有獎徵答活動，結合臺南市市場處人氣吉祥物「菜奇鴨」、「夜奇鴨」，以輕鬆有趣的互動方式宣導反賄選觀念，邀請民眾一起守護公平、乾淨的選舉環境。

「菜奇鴨＆夜奇鴨守護府城．反賄選知識大挑戰」網路有獎徵答活動活動自115年7月15日起至9月30日止。活動相關訊息請參閱活動海報(https://www.facebook.com/profile.php?id=100069304505898&locale=zh_TW)查詢。

法務部廉政署受理民眾陳情檢舉多元管道

一、「現場檢舉」：

本署各地區調查組均設有專人負責受理現場檢舉事項。（上班日08：30-12：30、13：30-17：30；如遇全國疫情警戒提升至第二級以上情況，停止受理現場檢舉，以落實防疫措施）

二、「電話檢舉」：

設置0800受理陳情檢舉免付費專線，電話為「0800-286-586」（0800-你爆料-我爆料）。（上班日08：30-12：30、13：30-21：30；週休二日及國定假日08：30-12：30、13：30-17：30）

三、「書面檢舉」：

郵政信箱「100006國史館郵局第153號信箱」。

四、「傳真檢舉」：

傳真專線「02-2381-1234」。

五、「網頁填報」：

開啟本署網站首頁「檢舉和申請專區」-「我要檢舉」(https://www.aac.moj.gov.tw/6398/6624/6632/1181666/post)。

為有效打擊貪瀆不法，我們提供上述多元檢舉管道，敬請踴躍檢舉。

檢 舉 管 道

交通部

廉政檢舉專線電話：(02)2349-2543。
廉政檢舉專線傳真：(02)2331-7345。
廉政檢舉信箱：臺北郵局第177-17號信箱。
電子郵件信箱：dac@motc.gov.tw（請以複貼EMAIL方式至個人信箱寄送）。

交通部公路局

廉政檢舉電話：(02)2307-0445。
廉政檢舉傳真：(02)2307-0489。
電子郵件信箱：thbeth@thb.gov.tw（請以複貼EMAIL方式至個人信箱寄送）。

交通部公路局中區養護工程分局

廉政檢舉郵政信箱：403950臺中大全街郵局第50-23號信箱。
廉政檢舉電話：(04)2371-6814。
廉政檢舉傳真：(04)2371-5453。
廉政信箱：首頁 / 便民服務 / 意見信箱 / 廉政信箱
（https://thbu2.thb.gov.tw/MessageConfirmPage.aspx?n=4555&sms=13653&pgn=1D95B2A4C316480B449D2B265F812515）。

以上是本期中砥月刊內容。
政風室感謝您對中砥月刊的支持，
期待下期能再得到您的指教與鼓
勵。謝謝！

交通部公路局中區養護工程分局政風室 祝福您

照片：台21線74K+800 白花石蒜