



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



目 錄

廉政宣導	1
機關安全維護宣導	2
公務機密維護宣導	6
反賄選 / 反介選專區	8
資訊安全維護	10
消費者保護宣導	13
防詐騙宣導	14
反毒宣導專區	16
健康小百科	17
再生能源知識館	19
電力生活館	21
科技與生活	23
廉政相關活動資訊	25
廉政署受理檢舉方式及檢舉管道	26

廉政宣導

收取回扣留遺憾

郝愛錢鎮長在蘑菇鎮上是出了名的貪財和愛看電影「教父」，他的座右銘就是「我沒有很愛錢，是非常愛錢」。為了怕被司法機關盯上，他私下與主任秘書狗腿哥、建設課長夭壽哥及課員荒唐哥組成地下A錢集團，並由鎮長助理豹膽哥擔任收受、保管工程回扣的白手套。

A錢集團在蘑菇鎮橫行鄉里，鎮公所同仁與廠商為了工作和生存，只能默默被壓榨，郝愛錢自行訂立了收取回扣標準，如果廠商不配合，想標到採購案根本是不可能的任務，大家都對於A錢集團的行為感到氣憤，但又拿他們無可奈何。

最近蘑菇鎮公所將辦理「市區主要道路及巷道工程」，荒唐哥對外尋找願意支付回扣款的廠商配合投標，白木公司認為有利可圖，就由荒唐哥安排與A錢集團相約於鎮長最愛的「教父餐廳」見面，並協議由白木公司支付決標金額35%作為回扣款。

在辦理第一次資格標開標時，因鎮公所作業疏失誤將評選委員名單公布在招標文件上，因此廢標。而荒唐哥也因此發現白木公司的服務建議書寫的太差可能不會得標，夭壽哥及荒唐哥便提供其他廠商撰寫的內容給白木公司參考修改；第二次開標時，果然如先前協議，由白木公司取得第一序位議價權，經議價以200萬元決標，上道的白木公司也依照約定交付回扣款70萬元給鎮長的白手套。然而白木公司卻因利潤太少，導致道路工程品質實在太差

而被民眾陳情，A錢集團所作的壞事也終於曝光了，公務員及廠商均被以涉嫌貪污治罪條例及刑法移送法辦。

溫馨小叮嚀

郝愛錢鎮長受蘑菇鎮鎮民所託執行職務，本應盡忠職守，為鎮民服務，不浪費公帑，不營私舞弊，沒想到竟被貪念蒙蔽了理智，收取回扣中飽私囊，不僅傷害公共利益，也辜負鎮民對他的信賴。

此外，夭壽哥及荒唐哥身為具有法定職務權限之公務人員，明知道工程標案應秉持政府採購法公平、公正、公開之意旨，竟因為小小的私念將依法應予保密的廠商服務建議書洩漏給白木公司，使特定廠商得標，不僅保不住公務員的身分，免不了牢獄之災，更影響採購制度的公平性。如果廠商因而偷工減料，將嚴重影響道路工程品質，更可能對人民造成無法彌補的傷害，更是萬萬不可。

相關法條

公務員：

貪污治罪條例第4條第1項第3款。

刑法第132條。

廠商：

貪污治罪條例第11條第1項。

2024
HAPPY NEW YEAR



圖：PIXTA圖庫

資料來源：新北市政府政風處廉政刊物 - 大道之行 - 與廉同行

機關安全維護宣導

淺談關鍵基礎設施之「資料採集與監控系統」(SCADA)



資料採集與監控系統(Supervisory Control And Data Acquisition, SCADA)是工業控制的核心系統，主要用於控制分散的資產，以進行數據蒐集與控制，亦屬關鍵基礎設施防護的核心系統之一；本文除介紹SCADA外，亦將討論SCADA安全的三個規律，以及如果資訊技術防護不足，該如何保護SCADA。

何謂「資料採集與監控系統」(SCADA)

SCADA是控制重要、複雜且通常可能具危險性的實體製程計算機系統，其中許多實體製程構成了對現代社會至關重要的關鍵基礎設施。由於這些實體製程功能非常強大，若遭誤(濫)用，常會造成不可接受的後果。故SCADA首要的安全機制，即在防止實體製程不能正常運作。

傳統工業控制系統可概分為可編程邏輯控制器(Programmable Logic Controller, PLC)、分散式控制系統(Distributed Control System, DCS)及SCADA等三類，其中SCADA是跨越網際網路的工業控制系統(Industrial Control System, ICS)，電網、管道和配水系統監控與資料之獲取，均來自SCADA；而DCS是跨越內部網路的工業控制系統。二者差異在於，DCS是一種不涉及跨越網路的工業控制系統，軟硬體均建置在一個地理位置相對較小的站點中，如發電廠、煉油廠和化工廠均是使用DCS。另從歷史期程來看，SCADA和DCS的不同處，在於使用一種軟體能否控制所有其他類型的系統，迄今的通用控制系統軟體，則多具有SCADA系統和DCS的所有功能。

所有SCADA的另一個重要關鍵因素則是操作人員，重要工業設施的控制系統，幾乎都有一個或多個操作人員，負責確保實體製程的安全運行；操作人員使用稱為「人機界面」(Human Machine Interface, HMI)軟體的工具，該軟體幾乎包括所有圖形可視化的實體過程狀態，且通常包括警報管理器和歷史趨勢工具等輔助系統。根據政策或法律，操作人員只有高度信任實體製程能被安全運行時，才會允許啟動系統，如遭遇顯示器被鎖定，或者接獲疑似被駭的通知時，操作人員可以移轉控制權到輔助或備份的HMI或控制

系統。但如短時間內仍然無法認定實體製程能正常運作，通常即須進行關閉。前開狀況通常意味在大多數情況下，攻擊者要造成系統負面影響，最簡單的方法是促成HMI某些操作或支持系統的操作失效，使實體製程被關閉；許多工業實體製程的關閉遠比啟動能更快完成，但在緊急關閉後，可能需要數日，才能恢復全部生產能量。

如何保護SCADA系統

SCADA系統架構的一個重要趨勢，是Gartner集團在1990年代中期創見的「IT/OT融合」觀念，亦即工業製程網路的架構上，同時存有IT（資訊技術）與OT（運營技術）的系統與設備，後更擴張到IT和OT團隊、業務流程、產品、技術和網路之結合。然而，IT/OT融合的問題，在於IT和SCADA網路上使用相同的技術、硬體、操作系統、平臺應用程式及網路組件後，當IT和SCADA完全互連時，許多攻擊IT網路的方法，亦可用以攻擊OT網路，加上多數的SCADA安全從業人員並不具備現代攻擊技術之防禦能力，因此反而造成SCADA的脆弱化。就如何保護SCADA，學者Andrew Ginter提出以下建議：

一、安全程序

大多數SCADA安全程序過分強調檢測、回應和復原活動，SCADA網路安全性必須著重於防止破壞，成熟度模型應用在衡量管理SCADA安全程序的業務流程強度，而非衡量程序本身的強度。

二、網路攻擊

Hacktivist級攻擊通常透過遠程控制進行，且常經由權限而非軟體漏洞來破壞安全系統；攻擊通常會破壞以IT為中心的安全措施，特別在高風險範圍內，攻擊面向幾乎沒有限制，從而SCADA安全從業人員必須專注於留心攻擊特徵，而非漏洞存在處。

三、風險管理和治理

定量風險評估不適用於HILF事件，因為我們無法可靠地分配這些事件，所以也不應要求決策者根據不確定的機率做出決策，特別是在評估SCADA網路保護程度時，決策者對攻擊狀況和影響的瞭解，通常優於主觀的定量風險評分，例如董事會成員常使用一些經驗法則，來判斷安全管理人員提供的資訊是否可信。

四、使用單向閘道器(Gateway)

單向閘道器並非路由器，不會將IP或流量資訊從工業網路轉發到外部網路，但可允許外部應用程序和用戶監控安全關鍵和可靠性關鍵控制系統，而不會帶來任何遠端控制或未授權操作的風險，亦即部署越多保護SCADA網路的單向閘道器，則越發安全。



圖：攝圖網

五、防止入侵



每個SCADA都應具備防禦所有攻擊的能力，強大的主要預防性安全程序，幾乎能消弭所有來自複雜對手的攻擊風險。此外，應該部署具備包括偵查控制和事件響應功能的次要控制措施，以處理應用主控系統不可避免的錯誤和漏洞等殘餘風險。在預防措施花費的精力與費用，可顯著降低安全程序的運營成本，以及降低SCADA受損的風險。

此外，Attila Cybertech執行長David Ong在2017年Hitcon Pacific大會（臺灣以海內外企業安全為主的資安研討會），也提出幾點幫助思考如何保護SCADA：

- 一、在OT與IT的融合過程裡面，網路安全扮演著不可或缺的角色，但是技術支援與管理作業仍是各自進行。然而，只要牽涉到現場設備與系統監控的OT應用，就會與業務或企業系統產生關連性。
- 二、針對IT系統安全性的管制作法，未必能適用於OT系統的網路安全防護；使用舊技術規格也是現行ICS系統面臨的眾多挑戰之一，因為已長期使用的工業控制設備，幾乎沒有任何安全性功能。
- 三、建立降低風險、減緩衝擊，以及具備援的運作模式。降低風險意指縮小受攻擊的面向，降低受濫用的可能性；減緩衝擊則是指應設法杜絕或減少涉及導致重大傷害情況發生的機率。
- 四、由於SCADA特別重視系統的可用性，在檢視各種ICS安全性的措施時，不只要留意該如何防禦，同時還要具備快速復原的能力。

五、由於網路安全的重點，是防止在IT網路上的攻擊方法被使用於OT網路，故SCADA安全性除專注於防止SCADA電腦任何未經授權的存取外，更應找出現有軟體產品的新漏洞，以強化網路安全。

六、SCADA為控制實體程序，故啟動安全儀表系統(Safety Instrumented System, SIS)比IT監控數據及利用備份復原來的重要。

資料採集與監控系統之發展工業控制系統係指生產過程的核心是被由SCADA控制的操作機器所組成，SCADA早期的安全規劃，在2003至2009年之間，核心架構為以IT為基礎的「縱深防禦」(Defense in Depth, DiD)，其基本邏輯包括：

- 一、IT專家認為所有網路都持續不斷的受到侵害。
- 二、入侵檢測和實踐事件通報團隊被IT專家視為最佳解。
- 三、緊急事件通報 / 處理團隊不斷尋找被惡意程式感染的系統，清除並備份還原。

惟前開架構代價高昂、效果不佳，且無法有效保護SCADA免受現代科技攻擊，以及從還原資料中恢復生產損失、修復損壞機械或拯救人員生命。後至2010年即產生SCADA安全架構修正版，修正邏輯包括：

- 一、必須優先考慮如何防止SCADA受損害，以及實體過程的錯誤操作。
- 二、實體和網路邊界保護，是新安全架構必要的保護措施。

三、因DiD架構降低風險功能有限，宜將安全更新程序以及加密和入侵檢測系統改為次要措施，以處理剩餘風險。

SCADA安全的三個規律

為使讀者能更佳瞭解保護SCADA的重點，本文簡化網路安全領域，歸納三個SCADA安全法則如下：

一、沒有什麼是安全的

如果能提供足夠的時間、金錢和人才，任何安全態樣都可能被破壞，特別是IT系統，而只要是人設計的機制，必然存在弱點，使用者必須明確瞭解諸如「我們現在的安全等級是否足夠？」、「我們應該有多安全？」等期待或需求，其實是一種連續統一的單元概念，而非諸如「安全通信」、「安全啟動」或「安全操作系統」等二元值術語。

二、所有軟體都可以被駭客入侵

軟體開發團隊努力消除軟體可能的錯誤或漏洞，但儘管付出最大努力，軟體都仍無法完美，包括安全軟體在內，實務上，所有軟體都可以被駭客攻擊。另一個常被誤解的重要觀念，即是有太多使用者認為，修補已知的錯誤和漏洞將使系統無懈可擊，然而，使軟體系統「安全」的方法，是部署更多的安全軟體。

三、每條資訊都可能是攻擊

即使是一點資訊，也可能是一種攻擊。進入廠區的人的大腦中所記憶的密碼和惡意企圖可視為攻擊；安裝在全新電腦上，或藉由USB鍵盤等周邊設備進入電腦中的惡意軟體，都可能是攻擊。

小結

SCADA網路保護的首要任務，始終是在防止未經授權的控制，IT系統的網路保護則是監控數據，而控制數據遠比監控數據重要得多，每位關鍵基礎設施營運者或SCADA控制者不僅能做，也應該要盡力做到預防導致系統發生崩壞的風險狀況。

資料來源：法務部調查局 - 清流雙月刊第24期

2024 新年快樂

公務機密維護宣導

小心！駭客正在誘騙你的機密資料 - 真實案例改編

現代化的保防觀念，就是加強機關自身的「免疫能力」，也只有機關內部同仁都有健全的保防意識，才能避免敵人趁虛而入。

志杰是某中央部會的業務承辦人，高考及格擔任公職6、7年以來，以其優異的外語能力，加上思路清晰、動作敏捷，深獲主管嘉許，司裡幾個專案列管的大案子，都是由他負責承辦，尤其是他最近提出的研究報告，言簡意賅、分析透徹，完全掌握問題的核心，呈給上級長官無不稱讚，儼然該部明日之星。如果硬要從雞蛋裡挑骨頭，志杰在公文處理方面或許還不夠細心，有時候數字少了一個零，有時候誤植同音錯別字，直屬長官陳科長仍需在他的公文品質上把關。

「520」政府交接後，該部會新任部長到職，隨即指示司長對於新政府施政方針的幾大案件必須專案列管，每週向政務次長報告進度，如執行上有滯礙難行之處，跨部會協調由政務次長負責聯繫。司長回到辦公室後，立即找來陳科長與志杰，轉達了上級的工作指示，希望同仁們全力以赴，圓滿完成這次任務。

時間過得很快，志杰接專案工作已1個多月，期間開了2次跨部會協調會議，還有1次會議是由院長主持，專案進行的十分順利，部長、次長對於部內同仁的表現非常滿意，認為該部今年列管案件可以順利達標。7月初，志杰一如往常早上7點40分就到辦公室，打開電腦看一下當天的行事曆，接

著收電子郵件，竟然有一封政務次長早上5點50分寄來的「高重要性」電子郵件，志杰嚇了一跳，因為自從次長到任以來，除了開會時的接觸，這是第一次直接下指示。志杰仔細看了e-mail內容，「次長」指示讓他在當日下班前將列管專案的會議資料、與會人員名單、具體數據及預擬講稿，先以電子郵件傳給次長過目。志杰雖然不是承辦公文新手，但接到「次長」重要指示，時間又這麼急迫，仍感到有些壓力。8點整陳科長到了辦公室，志杰立刻向他報告「次長」的幾項指示，科長請志杰將「次長」寄的e-mail列印出來，以便大家一齊分工，並準備向司長報告。

為了準時完成工作，志杰中午只喝了1杯咖啡，配上2片吐司，不敢出去用餐。下午4點10分，志杰將「次長」要的資料先拿給陳科長過目，科長仔細校對了會議資料、與會人員名單及每一項數據，並發現了幾處錯誤，請志杰立即修正，志杰手腳也很快，不到幾分鐘，整份資料已經完成，兩人帶著資料一同到了司長辦公室。司長說，今天次長好像很忙，一直沒見到面，接著又與他們兩人討論資料內容及專案未來準備的方向。下午5點整，陳科長為求慎重起見，拿起桌上電話，直撥次長室吳秘書，請她向次長報告，相關「書面資料」都已備妥，並請示是否附上「電子檔」。吳秘書告訴陳科長，次長一整天都在花蓮、臺東視察業務，還沒進辦公室，也未交待這件事，她稍後會問清楚，再回科長電話。陳科長掛上電話後覺得有點「怪怪的」，但說不出什麼地方怪。接著拿出早上志杰列印的「次長」e-mail內容，仔細檢查寄件時間、寄件人、收件人、交辦事項等，似乎沒有什麼異常。與此同時，次長室吳秘書來電，告訴陳科長，剛才打電話問過次長，今天早上沒有

交辦任何事，「書面資料」密封後交給吳秘書，電子檔先不要寄，等他今晚回辦公室再處理。晚上6點多，整幢聯合辦公大樓燈火通明，次長剛進辦公室，立刻請吳秘書通知司長、陳科長、志杰等專案小組成員，10分鐘後到三樓小會議室開會。

次長一進會議室就跟大家說，志杰準備的資料他看過了，除了幾個數據還要再確認一下，其餘都十分詳盡。但問題是他今早並未交待準備這些資料，專案列管的案件有其機敏性，在政策正式形成之前，必須遵守工作紀律，嚴格保密，相關資料若是不慎外洩，遭有心人士利用，勢將引起國內不小的風暴。這時候看到陳科長緩緩舉起手來，次長請他表示意見，陳科長說，今天早上8點一進辦公室志杰就跟他說了準備這些資料的事，由於是「次長」要的，指示的內容與上次會議決議事項息息相關，時間又很急迫，他就立刻向司長報告並且與志杰一起著手準備，下午5點左右在與吳秘書聯絡過後，才覺得好像有一點「怪怪的」，因為次長520到任以來，從未跳過司長直接交辦任何事情，況且這個專案的機敏性大家都知道，並不適合以電子郵件傳送，等他把志杰列印的「次長」e-mail拿出來仔細檢查，才赫然發現寄件人的e-mail address有問題，次長的電子郵件地址是英文字母小寫的「l」，但寄件人的電子郵件地址是阿拉伯數字「1」，其他幾乎都一樣，這才驚覺可能是被駭客入侵了。還好在志杰完成彙整工作前，他及時與次長室吳秘書聯繫，再次確認，才避免了機敏資料外洩。



圖：千庫網

會議持續了近半個小時，次長在總結時說，專案列管的案子當然有其特殊性與重要性，部內近期為了配合新政府的施政作為，各主政司、處同仁都非常辛苦，經常為了完成上級交辦的任務加班到深夜，但是在工作忙碌之餘，千萬不能忘了資訊安全與保防意識。今天發生的「駭客」事件，正好可以當作案例提醒同仁，他會要求資訊室立刻向資安辦通報，並且協助釐清寄件人的背景及目的，更重要的是必須防範類似事件再次發生。

志杰回到辦公室後久久不能自己，原來今天白忙了一整天，還差一點因自己一時大意造成機敏資料外洩，如果事情真的發生了，後果實在難以想像。陳科長發現志杰在會後一直呆坐在位子上，隨即起身到他桌旁。科長告訴志杰，剛才司長已經轉達了次長的指示，次長對於科裡承辦的專案業務非常肯定，尤其是志杰在簡報資料及英文翻譯所下的功夫，長官們都很清楚，希望他繼續加油，今天發生的事只是虛驚一場，我們只要提高警覺，更加謹慎細心就好，千萬不要因此而感到內咎。

翌日適逢部務會議，次長趁機向與會人員說明了昨天發生的駭客事件，並且要求各級主管務必向所屬同仁轉達，科技進步日新月異，駭客行為無孔不入，保防工作不限於以往的「保密防諜」，現代化的保防觀念，就是加強機關自身的「免疫能力」，也只有機關內部同仁都有健全的保防意識，才能避免敵人趁虛而入。「提升保防意識，加強資訊安全」是一切業務的基礎，千萬不能因一時疏於注意，讓大家共同努力的成果功虧一簣。

資料來源：法務部調查局第8期清流雙月刊

反賄選 / 反介選專區



認識賄選要件態樣 - 一般常見賄選態樣

- 一、**交付金錢**：以工作費用名義，交付金錢給具有投票權的工作人員，約定投票支持某特定選人。
- 二、**招待旅遊**：免費或低價招待選民出遊，候選人出發前向選民自我介紹，具穿選舉背心合照，擺明是讓選民知道之所以能低價出遊，都是因為候選人協助。
- 三、**返鄉交通**：透過提供選民往返其居住地與投票地間的交通工具或交通費用，吸引選民返鄉支持特定候選人。
- 四、**贈送禮品**：候選人以摸彩獎品方式對在場選民懇求支持，且於摸彩過程中，當場交付高價值商品給在場多位選民。候選人透過樁腳，贈送禮盒給選民，並對選民說「選舉的時候再請你們幫忙」。
- 五、**招待餐會**：候選人以「座談會」、「幹部會議」名義舉辦免費餐會，招待設籍於選區內選民，用餐時到場逐桌拜票。
- 六、**介紹工作**：候選人為求顧利當選，向選民表示只要投票選他，會設法幫忙安排工作機會。



圖：中央選舉委員會

認識賄選要件態樣 - 其他賄選態樣

- 一、**財物**：提供「走路工」、「茶水費」、「誤餐費」或其他名目之現金、票據、禮券、提貨單或其他有價證券。
- 二、**招待**：招待至舞廳、酒廊、歌廳或其他娛樂場所消費。
- 三、**餐券**：販賣餐券，並期約於候選人當選後，兌換餐券面額數倍之金錢。
- 四、**免除**：免除債務。
- 五、**彩券**：贈送樂透、大樂透、刮刮樂等公益彩券。
- 六、**建設經費**：假借核撥經費名義，提供縣市、鄉鎮或村里等地方政府建設經費。
- 七、**捐助**：假借捐助名義，提供廟宇、同鄉會或其他機構、團體等服裝、活動用品經費。
- 八、**新興數位工具**：提供線上遊戲點數、第三方支付、手機行動支付、虛擬通貨等吸引選民。
- 九、**代繳**：代繳稅款或各種違規罰款。
- 十、**其他**：行求、期約或交付其他類型賄賂或不正利益。

資料來源：113年第16任總統副總統及第11屆立法委員選舉反賄選 / 反介選專區

資訊安全維護

網路釣魚網站常見手法大公開！你也中招了嗎？



圖：鵝窩設計

「網路」顯然已是生活中不可或缺的東西，無時無刻形隱不離的陪伴在你我身旁，網路可以是我們的朋友，卻同時也有可能是傷害我們的武器，今天我們要討論的主題是釣魚網站，從報稅季、簡訊罰單繳款，無處不在釣魚網站的蹤跡，為了保護我們的數位生活和組織的安全，我們需要了解網路釣魚的危害，並積極採取防範措施，以確保我們的線上世界免受這一威脅的影響。

什麼是網路釣魚

網路釣魚的基本原理是利用社交工程（也稱社會工程），仿作外觀與合法的網站或機構相似的偽造網站電子郵件或社交媒體帳號等，欺騙使用者相信偽造的網站或訊息是真實可靠的，並誘使使用者提供個人敏感資訊，如帳號、密碼、信用卡號碼等，或是誘導使用者執行某些惡意操作，以便進行盜取個人資料或進行其他非法活動。另外，攻擊者也可能發送看似真實的電子郵件，要求使用者點擊附帶惡意連結或下載含有惡意程式的附件。

網路釣魚的常見手法

以下是我們整理出目前為止常見的網路釣魚手法，但隨著科技的進步，可能會有更多無法預測的未來，提醒各位還是要多加留意。

一、偽冒網站

攻擊者會建立與真實網站相似的偽造網站，包括銀行、電子商務平臺或社交媒體等，用來收集使用者的個人資訊。他們通常使用類似的網址、標誌、介面和內容，讓使用者誤以為自己正在訪問正確的網站。

防範建議：檢查網址是否正確，特別是在輸入個人資訊或進行金融交易時。確保域名與正確的網站相對應。

二、偽冒電子郵件

攻擊者發送看似真實的電子郵件，冒充合法機構或知名品牌，要求使用者提供個人資訊，如帳戶名稱、密碼或信用卡號碼。這些電子郵件

通常包含引人注目的主題、優惠或緊急事件，以誘騙使用者點擊附帶的連結或下載附件。

防範建議：檢查寄件人的電子郵件地址，注意拼寫錯誤、不尋常的域名或奇怪的電子郵件格式。不要點擊可疑連結或提供個人資訊。（留意電子郵件的來源）

三、偽冒社群媒體帳號

攻擊者創建偽冒的社群媒體帳號，冒充知名品牌、名人或朋友，並與使用者互動。他們可能試圖誘導使用者透露個人資訊、點擊惡意連結或下載含有惡意程式的檔案。

防範建議：使用強密碼、兩步驟驗證和安全問題等增加帳戶安全性的功能。定期更換密碼，避免使用相同密碼在多個帳戶中。

四、偽冒下載

攻擊者利用使用者對軟體、遊戲或應用程式的需求，提供看似合法的下載連結。然而，這些下載檔案可能包含惡意程式，一旦使用者執行，攻擊者就能控制受害者的裝置或竊取個人資訊。

防範建議：下載軟體或檔案前，確保來源可靠且具有信譽。避免點擊來自未知或不受信任來源的下載連結。

網路釣魚的常見手法

偽冒網站	偽冒電子郵件	偽冒社群帳號	偽冒下載
與真實網站相似，包括銀行、電子商務平臺或社交媒體等，用來收集使用者的個人資訊。	冒充合法機構或知名品牌，要求使用者提供個人資訊，如帳戶名稱、密碼或信用卡號碼。	創建偽冒的社群媒體帳號，冒充知名品牌、名人或朋友，並與使用者互動。	利用使用者對軟體、遊戲或應用程式的需求，提供看似合法的下載連結。

請尚設計 designhu

網路釣魚的危害

網路釣魚的危害潛在巨大，它威脅著我們的個人隱私、財務安全和組織的機密資訊，以下是我們整理出目前為止網路釣魚所帶來的危害，但隨著科技的進步，可能會有更多無法預測的未來，提醒各位還是要多加留意。

一、財務損失

網路釣魚攻擊可能導致使用者的財務損失。當使用者洩露帳號、密碼、信用卡號碼或其他敏感資訊時，攻擊者可以使用這些資料進行金融詐騙、盜用身分或進行非法交易。這可能導致銀行帳戶被清空、信用卡被濫用，以及長期的金融恢復困難。

二、個人身分盜竊

通過網路釣魚攻擊，攻擊者可以獲取使用者的個人身分資訊，包括姓名、地址、出生日期和身分證號碼等。這些資訊可以被用來進行身分盜竊，包括開設新的銀行帳戶、申請信用卡、簽署合約，甚至冒充受害者進行其他非法活動。

三、隱私侵犯

網路釣魚攻擊可能導致使用者的隱私被侵犯。當使用者提供個人資訊給攻擊者時，他們可能將這些資訊用於非法用途，如騷擾、散佈個人資訊、勒索或進行監控活動。這種侵犯可能對使用者的生活和職業產生嚴重的影響。

四、帳號劫持

通過網路釣魚手法，攻擊者可以取得使用者的帳號和密碼，然後劫持其帳號。這可能發生在電子郵件、社交媒體、網路銀行或其他線上平臺上。一旦攻擊者取得控制權，他們可以冒充使用者進行各種活動，包括發送詐騙郵件、傳播惡意軟體或騷擾其他使用者。

五、僵屍裝置

在某些情況下，網路釣魚攻擊可能導致使用者的裝置被感染並變成僵屍裝置。攻擊者可以利用感染的裝置進行大規模的分散式拒絕服務攻擊(DDoS)，用於網路敲詐或其他惡意目的。此外，僵屍裝置也可能被用來進行間諜活動、竊取敏感資料或進行其他網路犯罪行為。

網路釣魚的危害

財物損失	個人身份盜竊	隱私侵犯	僵屍裝置
這可能導致銀行帳戶被清空、信用卡被濫用，以及長期的金融恢復困難。	攻擊者可以獲取使用者的個人身分資訊，包括姓名、地址、出生日期和身分證號碼等，冒充受害者進行其他非法活動，包括開設新的銀行帳戶、申請信用卡、簽署合約。	這些資訊可能將用於非法用途，如騷擾、散佈個人資訊、勒索或進行監控活動，這種侵犯可能對使用者的生活和職業產生嚴重的影響。	攻擊者可以利用感染的裝置進行大規模的分散式拒絕服務攻擊。此外，僵屍裝置也可能被用來進行間諜活動、竊取敏感資料或進行其他網路犯罪行為。

鴻瀚設計 designhu

網路釣魚攻擊對個人和組織都帶來嚴重的危害。因此，使用者應該保持警覺並採取適當的防範措施，以保護自己的資訊安全和隱私。

資料來源：鴻瀚設計

消費者保護宣導

線上預購型 群眾集資小知識

線上預購型群眾集資：

消費者(贊助者)在線上集資平台上，認同提案人的提案，以贊助的方式，讓提案人募足資金、完成提案成品後，將提案成品交付給消費者(贊助者)的交易模式。

提醒：

- ❗ 務必看清楚提案內容及集資平台規定後，再決定是否要出資贊助。
- ❗ 原則上得適用消費者保護法第19條7日無條件退貨解約權規定。

消費者(贊助者)可能會面臨的風險：

- ❗ 商品遲延、無法出貨
- ❗ 商品瑕疵或品質不如預期
- ❗ 想解約退費，提案人卻遲不退費，甚至失聯等

行政院消費者保護處 廣告



無卡分期 小心有可能是真貸款！

當您在實體店面或上網購物，遇到業者宣稱可以選擇「無卡分期」支付時，要注意，有可能是業者提供您與第三人(貸款機構)簽訂消費借貸契約喔！

無卡分期常見爭議

- ❗ 辦理後，商品總價變高
- ❗ 宣稱無利率，但後續期數含鉅額利息
- ❗ 解約困難，違約金及拖欠付款的滯納金高昂
- ❗ 申請者的信用未經評估，易造成過度消費、還款困難
- ❗ 部分交易要求消費者簽發本票

消費者應注意：

- ⚠️ 確實審閱契約條款、內容
- ⚠️ 瞭解商品交付與還款條件及相關費用計收
- ⚠️ 避免過度消費
- ⚠️ 不輕易簽發本票

行政院消費者保護處 廣告



防詐騙宣導

詐騙簡訊話術再升級！提醒民眾辨識RCS簡訊特徵！

近日詐騙集團更升級話術，假冒銀行業者名義，以「安全問題需關閉帳戶，請驗證個人資料」等話術，要求民眾點擊簡訊連結，誘導填寫個資並盜刷信用卡。

為避免此情形，請注意RCS詐騙簡訊3大特徵：

- ⚠️ 1、+號開頭
- ⚠️ 2、網址連結
- ⚠️ 3、RCS署名

請Android手機用戶可關閉RCS即時通訊功能，以避免收到詐騙訊息。

資料來源：165全民防騙



資料來源：千庫網

您認識RCS詐騙簡訊嗎?

1 與+44 7706 231494進行的 RCS 即時通訊

2 【玉山銀行】親愛的顧客，因安全問題暫時關閉您的帳戶，請立即驗證您的個人資料，即可恢復帳戶使用權
<https://bitusjun.top/>
17:31

3 此為與+44 7706 231494進行的 RCS 即時通訊，瞭解詳情

RCS 訊息

1 +號開頭

2 網址連結

3 RCS署名

符合上述態樣均屬RCS詐騙簡訊，請勿點擊簡訊連結。

刑事警察局
165
165 全民防騙

資料來源：165全民防騙

網路遇到自稱律師或駭客組織協助幫忙取回詐騙款項？

請切勿相信，否則就淪為詐騙集團的肥羊。

對此，民眾若遇到自稱國際律師或駭客可以討回騙款的訊息，請切勿理會並撥打165專線詢問。而被害金額償還，應尋求正規的法律訴訟程序，請勿隨意聽信網路謠言。

資料來源：165全民防騙



圖：網路



資料來源：165全民防騙

反毒宣導專區



十四歲那一年 第一次接觸毒品
就開始走上吸毒 戒毒 再吸毒 再戒毒的不歸路
那天我的女兒來看我
看著她的背影 我突然想好好照顧她
因為毒品 我少了好多陪伴她成長的時光
我要給她一個正常的生活 再怎樣難 我都要戒毒
上天給了我機會 同樣也會給你
吸毒沒藉口 戒毒真幸福

不打烊
免費

24h 戒毒成功專線
0800-770-885

98年3月1日起正式啟用 (請請你·幫幫我)

<http://refrain.moj.gov.tw>

法務部

資料來源：法務部



別讓毒品囚禁您和孩子的人生

您或孩子有毒品的困擾嗎
現在就打24小時戒成專線

戒成成功專線
0800-770-885
請請您 幫幫我

讓我們一起幫您解決問題
<http://refrain.moj.gov.tw>

法務部
戒成成功專線

資料來源：法務部

健康小百科

抗氧化、防失智、降膽固醇！堅果4大模範生營養PK

**穩血糖又降膽固醇！
堅果4模範生營養大PK**

榛果
營養價值高堅果之王
榛果亦能提升視力，
緩和用眼過度的狀況

核桃
盛名遠播的補腦果
有效延緩細胞老化
健腦益智

杏仁果
抗氧化、防衰老
可排除人體內自由基
降低癌症的發生率

腰果
刺激生長激素分泌
富含精胺酸，能刺激
生長激素分泌

早安健康
! 堅果脂肪及熱量非常高，堅果營養價值很好，
但還是要適量攝取。單純烘乾、無添加才健康。

嘴饞想吃點零食，你也總是順手嗑起堅果嗎？堅果素以「有益心血管健康」而著稱，也讓堅果列居十大營養食物之一。其中，榛果、核桃、杏仁、腰果，甚至被稱為「四大堅果」，但是堅果又該怎麼選、怎麼吃才對呢？

在適量攝取下，我們可以從堅果中獲得很多營養素，幫助維持身體健康。堅果不僅是低GI食物，也是蛋白質、膳食纖維的良好來源，且礦物質含量相當豐富，可滿足大半身體每日的營養需求。根據衛生福利部指出，每日至少攝取1份堅果種子類，約是大顆的堅果（腰果、杏仁果）5顆或是小顆的堅果（花生）10顆。

榛果：營養價值高的堅果之王

有不飽和脂肪酸，能去除自由基、抗氧化、降低壞膽固醇，且含有鎂、鈣、鉀等微量元素。榛果亦能提升視力，緩和用眼過度的狀況。

核桃：盛名遠播的補腦果

核桃被稱為「益智果」，如其美名，核桃含豐富維生素B、維生素E，且含磷質高，可以有效延緩細胞老化、健腦益智，能增強記憶力、學習力、專注力，還可以預防失智症找上門。

杏仁果：抗氧化、防衰老

杏仁含有不飽和脂肪酸、維生素E、鈣、鐵等礦物質，能抗衰老，延年益壽。杏仁也是天然的「解毒劑」，可以排除人體內的自由基，有效降低癌症的發生率。

腰果：刺激生長激素分泌的食物

腰果富含精胺酸，能刺激生長激素分泌，與「長高」有密切關係。另也含有維生素及鋅、鈣、鐵等微量礦物質，與亞油酸及亞麻酸，對動脈硬化有預防效果。但比起其他堅果，腰果的飽和脂肪酸含量較高，要避免攝取過量。

「堅果飲食注意事項」注意！堅果脂肪及熱量非常高，雖然堅果營養價值很好，但還是要適量攝取。單純烘乾、無添加才健康，堅果若加工過度，除了營養會流失外，還可能使人愈吃愈「涮嘴」，不小心就會吃過量。



圖：Cl Terry

CL TERRY

資料來源：早安健康

男人啊！超出能力範圍的事情就別管了



資料來源：大愛臺灣綜藝

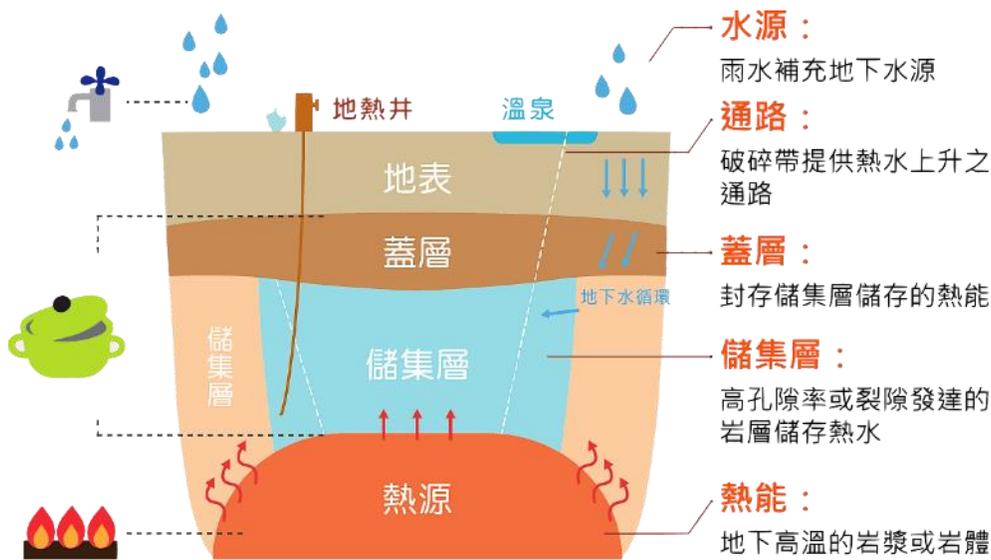
再生能源知識館

地熱能 Geothermal Energy

地熱為自地表下的能源，隨深度增加而升高地層岩溫（地溫梯度^{註1}），地球中心（地核）溫度推測高達6,000°C。

地熱發電條件

發展地熱發電天然條件是地下溫度80°C以上，開發期間需要經過地質、地球物理、地球化學等專業人士協助，加上實際鑽井調查，確保地熱發電系統可以長期運轉。且必需具備以下5大條件：

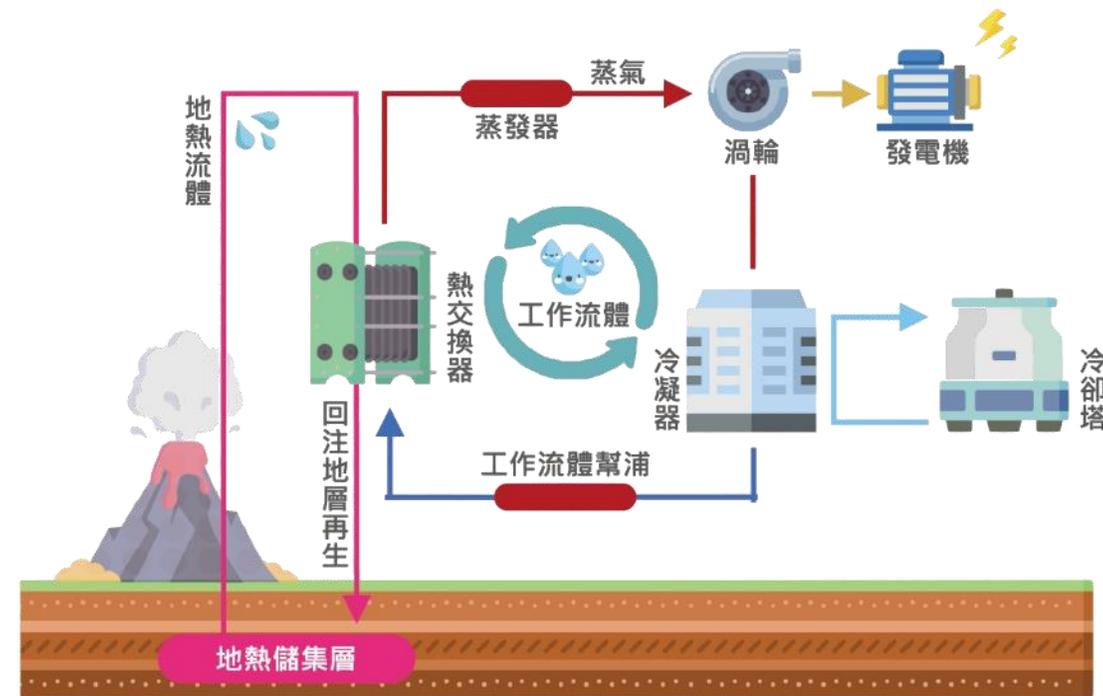


註1：地溫梯度（英語：Geothermal gradient）是與地球內部深度增加相關的每單位深度的溫度升高變化率。

地熱儲集構造：熱源在下方 - 儲集層居中 - 蓋層在上方，如同鍋子煮熱水。

認識地熱發設備與優點

地熱發電是透過鑽井的方式把地下高溫流體取出，利用熱水或蒸汽擷取地下熱能做為發電使用，水經熱交換後回注地層。以下為「雙循環式發電系統」。



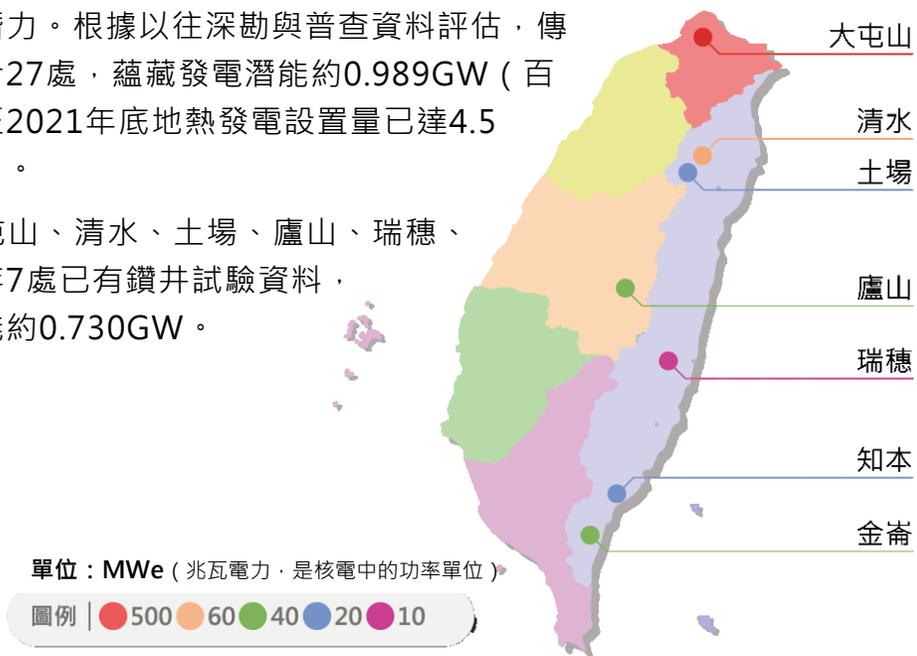
地熱能發電的優點

- 取熱不取水，地熱流體多回注地底，避免與溫泉搶水、確保產業共榮、資源循環利用。
- 地熱能發電屬基載電力供應的一環，可穩定發及取得穩定的現金流。

臺灣地熱發電總潛能與現況

臺灣位於環太平洋火山活動帶西緣，地熱資源豐富，熱源條件良好，甚具地熱開發潛力。根據以往深勘與普查資料評估，傳統地熱區共計27處，蘊藏發電潛能約0.989GW（百萬瓩）。截至2021年底地熱發電設置量已達4.5 MW（千瓩）。

其中大屯山、清水、土場、廬山、瑞穗、知本、金崙等7處已有鑽井試驗資料，蘊藏發電潛能約0.730GW。



資料來源：經濟部能源局再生能源資訊網



爺爺把小白載去棄養，
結果小白先回來了。

資料來源：貓咪也瘋狂俱樂部

電力生活館

用電安全

家中的延長線，大家有多久沒注意過了呢？

延長線常被放在不起眼的角落默默運作，但如果不小心插太多讓它太吃力過熱時就會增加起火釀災的機率，一定要小心！

曾有消防同仁做實驗發現，舊式延長線如果沒有「自動斷電保護」而且還將線材網綁使用的話，當用電超過負載時溫度可能會飆升到150度，使得電線冒煙短路燃燒.....非常危險！

提醒大家～延長線應選用有：

- ※獨立電源開關。
- ※過載保護裝置。
- ※商品安全標章。

使用延長線時，別忘了要注意5重點：

- ▲不要插好插滿,注意額定容量。
- ▲不要延長又延長。
- ▲不要使用高功率家電。
- ▲不要網綁使用。
- ▲要定期汰舊換新。

資料來源：台電電力粉絲團

冷冷的冬天裡，偶爾走到角落去取暖時，記得也要檢查一下延長線喔。



資料來源：台電電力粉絲團

省電小撇步

除濕機電暖器的省電好搭檔不可不知。

吹冷氣時搭配電風扇 / 循環扇可以更省電，這應該大家都知道了～那.....冬天常用的電器呢？

濕冷的冬天，使用除濕機和電暖器的機會增加。

有個省電的神隊友，也是大家不能不知道的就是循環扇。循環扇和電風扇雖然相似，但扇葉及設計不同。循環扇可以集中風力，吹出螺旋柱狀的強力風適合用來。

- 帶動室內空氣流通。
- 增加空氣循環。
- ◆除濕機 + 循環扇，讓室內空氣對流，除溼效率更好。
- ◆電暖器 + 循環扇，可以讓熱空氣循環，加速暖房效果。

循環扇是電器省電的好搭檔，大家一定要知道並善用唷～

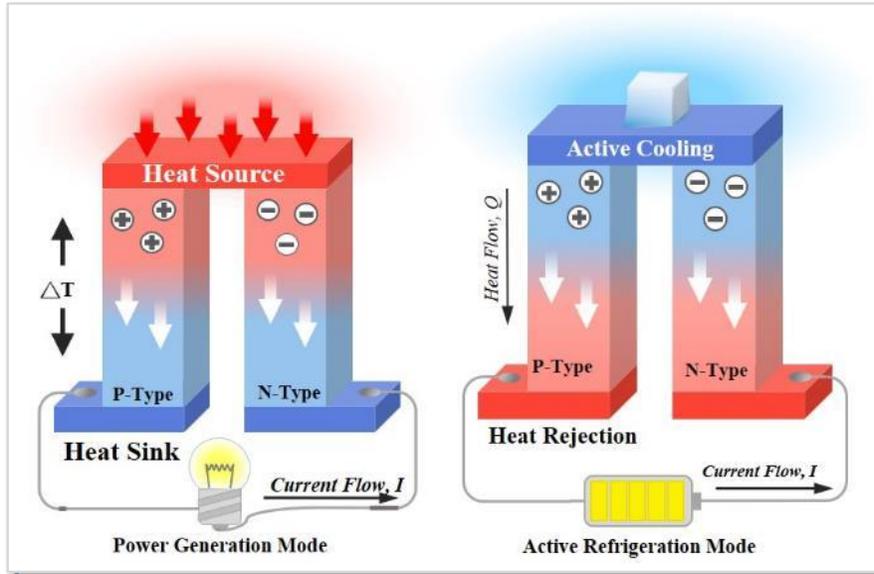
資料來源：台電電力粉絲團



資料來源：台電電力粉絲團

科技與生活

用溫差就能發電！



熱電材料除了被應用在太空探測器與廢熱發電外，未來也有機會在「致冷器」中發揮快速散熱的特性，滿足減碳的趨勢與需求。（影像來源：國立陽明交通大學材料與工程學系吳欣潔教授）

隨著氣候快速變遷，尋找對地球環境影響最低的綠色能源成為當務之急，促使熱電材料逐漸被產學研界重視。熱電材料就是利用溫差發電，原理雖然聽來容易，但執行起來極具挑戰性，主因在於轉換效率不高。國立陽明交通大學材料與工程學系吳欣潔教授投入熱電材料研究多年，研發出將熱電優值（又稱ZT值，數值越大代表熱電效益越佳）提升的製程，其研發出的高ZT熱電材料也有著極高的轉換效率。

究竟熱電材料的運作原理與特色為何？吳欣潔教授解析：「簡單來說就是源自半導體材料內的載子特性。載子由高溫往低溫移動，使材料在高低溫端具有數量不同的載子，進而出現電位差且產生電流。這個是由德國物理學家湯馬斯·塞貝克(Thomas Johann Seebeck)在1821年首次描述的現象，後來被稱為賽貝克效應(Seebeck effect)。」另外，熱電材料只要有溫差存在就能產生電位差，而且材料本身或模組皆是全固態，使用上更為穩定且安全，使用壽命也較長。

熱電材料的應用實例

儘管吳欣潔教授的研究成果廣受學研單位矚目，但多數人對熱電材料技術都還有些陌生。

面對這樣的現象，吳欣潔教授分享熱電技術其實已問世多年而且應用廣泛，像是太空由於多數環境未必像地球有充足的太陽能可供發電，目前常用的太陽能發電機制也不可行，因此利用溫差發電且可長時間自行運作的熱電，就成為建置太空探測器的重要技術。此外，在一般產業中，熱電亦可見到其應用身影，例如中鋼與工業技術研究院就合作將熱電材料模組製成磁磚樣態，並貼附在煉鋼廠區中，把熱能轉換成電力供照明使用；或是在汽車引擎內建置熱電材料模組就可以把高達攝氏300度的高溫轉換為電力。

除了工廠，臺灣熱電材料其實還可以有更多應用。譬如能將臺灣大量的地熱，透過熱電而產電，「簡單來說，就是只要有溫差的地方，熱電材料都可以發揮功效。」吳欣潔教授說。

熱電材料的發展潛力

吳欣潔開始研究熱電技術是在博士班階段，當時綠能是產官學研界高度關注的議題，不過多數團隊的方向都在生質能、電池、太陽能等方面，因此她希望可以做出不一樣的成果，於是選擇深具發展潛力、應用範圍廣的熱電材料。往後，在致力提升熱電材料ZT值的過程中，儘管遇到組裝、封裝與如何精細量測轉換效率的挑戰，但最後在國家科學及技術委員會的計畫支持下，才得以完成具有突破性的研究成果。

對於未來的研究走向，吳欣潔教授表示在持續研究溫差發電的同時，也將投入「致冷器」的研發，「有溫差時，熱電材料就可以發電，但如果對它通電，熱電材料就會降溫，這是一體兩面之事，」吳欣潔教授分享。因此，選擇熱電材料做為冷卻設備，就不須像傳統冰箱、冷氣需要壓縮機和冷媒，只需材料本身和簡單的通電模組，即可瞬間、定點的冷卻。

吳欣潔教授最後表示，熱電材料的發電效率離商業應用雖然還有一段距離，不過這項技術具備的優勢以及轉換效率的逐步提升，可以滿足減碳的需求與趨勢。未來，吳欣潔教授與研究團隊也將並重發電與致冷兩方，持續提供產業與社會高效能的綠色材料。

資料來源：Sci-Tech Vista科技大觀園

每到冬天，
每一次起床都是離鄉背井。
床以外的地方都是遠方，
手勾不到的地方都是他鄉，
上個廁所都是出差；
起床上班就是出國。



資料來源：Eagle Wang.

廉政相關活動資訊

法務部調查局電子書櫃清流雙月刊歡迎點閱（網址如下）：

https://www.mjib.gov.tw/eBooks/eBooks_Detail?CID=3



企業誠信宣導資料

經濟部中小及新創企業署研編「中小企業誠信經營手冊」，手冊以中小企業主之角度出發，強調誠信經營與永續發展之間的重要關聯，並鼓勵更多企業主善用政府資源落實誠信經營。

「中小企業誠信經營手冊」電子檔已置於下述網站供下載，請參考運用：

- 一、經濟部中小及新創企業署官網 / 公開資訊 / 廉政專區 / 企業服務廉政平臺 / 企業誠信宣導資料（網址：<https://www.sme.gov.tw/article-tw-2397-8176>）。
- 二、中小企業法律諮詢服務網 / 下載區 / 法規宣導手冊（網址：<https://law.sme.gov.tw/ait/modules/downloads>）。

法務部廉政署受理民眾陳情檢舉多元管道

一、「現場檢舉」：

廉政署北、中、南部地區調查組均設有專人負責受理現場檢舉事項，時間為上班日08：30-12：30及13：30-17：30。

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」方式：

郵政信箱「100006國史館郵局第153號信箱」。

四、「傳真檢舉」方式：

專線為「(02)2381-1234」。

五、「網頁填報」方式：開啟廉政署網站首頁「檢舉和申請專區」-「[我要檢舉](https://www.aac.moj.gov.tw/7170/278724/)」(https://www.aac.moj.gov.tw/7170/278724/)。

檢舉管道

交通部

廉政檢舉專線電話：(02)2349-2543。

廉政檢舉傳真：(02)2331-7345。

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7甲線49K~50K 雪景