



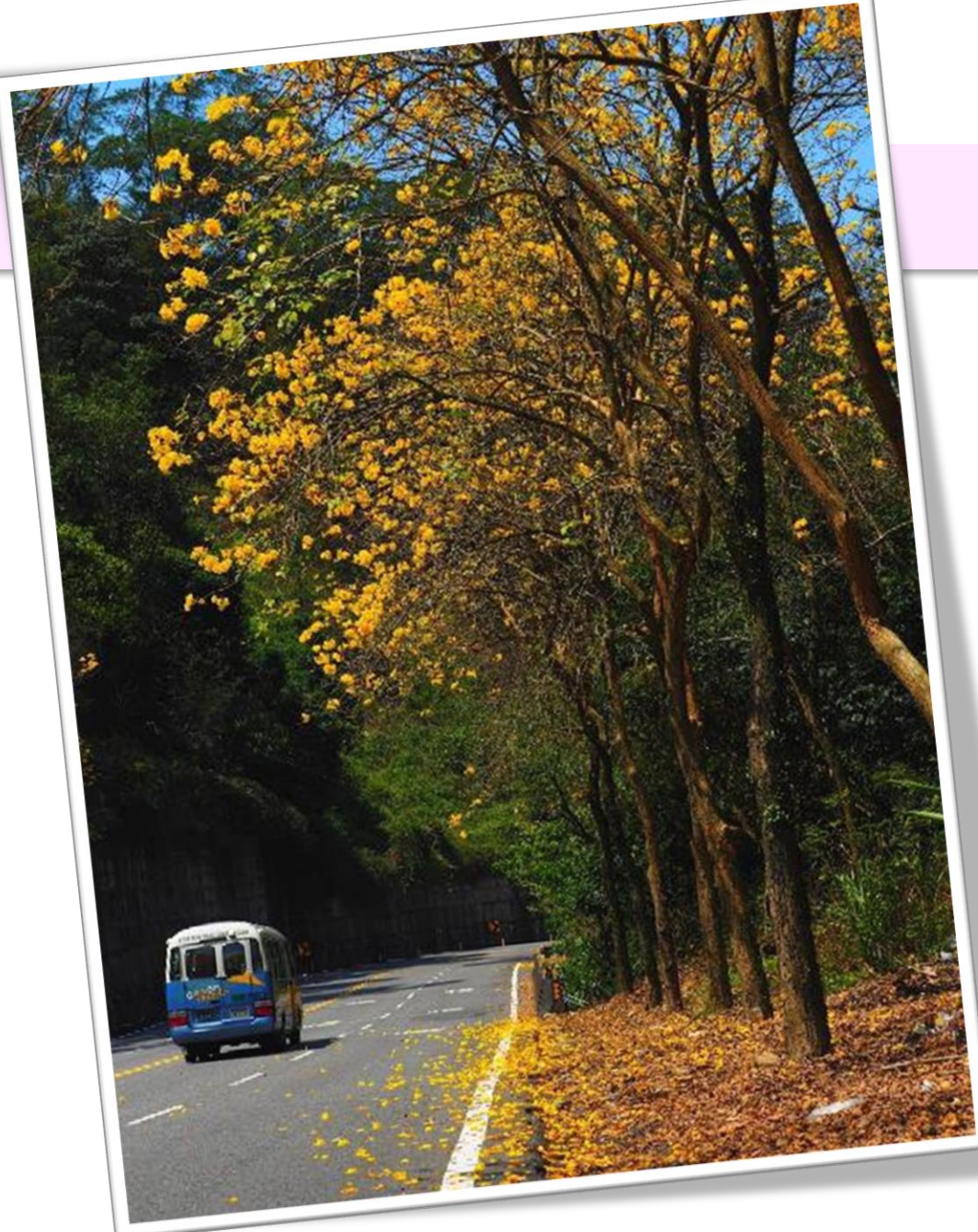
交通部公路總局第二區養護工程處
Second Maintenance Office
Directorate General of Highways,
MOTC

中 砥 月 刊

機關內部刊物：2023年4月號



照片：台21線138K+500
背景音樂：中國風音樂-晴雪月夜



照片：台21線73k~74k

目 錄

廉政宣導	1
機關安全維護宣導	4
公務機密維護宣導	6
陽光法案專區	8
CI學堂	9
認知作戰與全民防制	13
資訊安全維護	17
反毒專區	22
消費者保護宣導	24
防詐騙宣導	26
生活小常識	28
健康小百科	30
電力生活館	32
科技與生活	34
民間傳說	39
廉政相關活動資訊	40
廉政署受理檢舉方式及檢舉管道	41

廉政宣導

補不起來的錢坑

事實概述

倒霉哥在市政府水利工程單位擔任約僱人員多年，因為行事沉穩、做事認真負責，深得機關內主管及同仁的信賴，平日主要負責市內河川、市管轄區排水的水患防治等工作，而且辦理市內多區災害防治與緊急搶修開口合約之龐大預算。

但是倒霉哥近年來沉迷於股海，所謂好的老師讓你上天堂、壞的老師讓你住套房，倒霉哥誤信電視上投顧老師及名嘴的明牌，投資虧損連連，甚至還玩起了融資融券，眼看著資金上的漏洞越滾越大，竟然惡膽旁生，歪腦筋動向與他業務有往來的揪黑心公司，因為揪黑心公司承作開口合約時，疑似浮報實際施工之機具及人員數量，被倒霉哥抓到了把柄。

某日倒霉哥利用揪黑心公司請領工程估驗款項之際，假藉家中祖母罹患了罕見疾病，需要使用健保不給付的特殊用藥，急需一大筆醫藥費，無奈下只能向揪黑心公司調頭寸，並暗示他會睜一隻眼閉一隻眼，假裝沒發現浮報數量的部分，揪黑心公司礙於想順利請領款項，不敢得罪倒霉哥，只好按月匯錢給倒霉哥，倒霉哥因此得手上百萬元，而且又接受揪黑心公司招待喝花酒、出入高級招待所，生活可謂是春風得意。

食髓知味的倒霉哥，心想著單靠著從揪黑心公司撈來的油水實在不夠填補財務上的巨大漏洞，竟然又異想天開的找上業務上有往來的金蝦公司要

點甜頭，因金蝦公司希望工程順利進行而且迅速撥款，所以當倒霉哥假藉家中小孩缺奶粉、尿布錢等理由需索時，便毫不猶豫的交付數十萬元以求履約順利。

缺失態樣解析

- 一、公務員明知廠商有虛報、浮報機具人員數量之情形，依法不應撥付工程款，卻長期以借貸之名向廠商索賄及接受招待喝花酒，以換取放水通過驗收，圖利廠商。
- 二、公務員利用廠商希望工程順利進行及能迅速核撥工程款的心態，向廠商要求交付賄賂。

相關法條

- 一、公務員：
 - (一)貪污治罪條例第4條第1項第5款違背職務受賄罪（揪黑心公司部分）。
 - (二)貪污治罪條例第5條第1項第3款不違背職務受賄罪（金蝦公司部分）。
- 二、廠商：
 - (一)揪黑心公司：貪污治罪條例第11條第1項違背職務行賄罪。
 - (二)金蝦公司：貪污治罪條例第11條第2項不違背職務行賄罪。

資料來源：新北市工程倫理手冊

都是發票惹的禍

小英在機關內擔任總務課課員，負責小額採購業務，某日機關內冷氣故障，具水電專長的同事小盧表示是壓縮機的問題，並自願去購買零件來更換，小英便拿了新臺幣3萬5,000元交給小盧購買零件。

數日後，小英看小盧已將冷氣維修工作完成，便向小盧索取購買零件之統一發票以便核銷經費，沒想到小盧為了省錢，竟購買無單據之中古零件，致無發票可供核銷經費。為能順利核銷經費，小英到機關經常合作之冷氣行，購買不實發票以核銷該筆經費。

小英雖順利的核銷了該筆經費，但是他以不實發票核銷該筆經費的行為有沒有違法呢？

解析

小英的行為，可能觸犯刑法第216條行使公文書不實登載罪：

一、刑法第216條規定，行使第210條至第215條之文書者，依偽造、變造文書或登載不實事項或使登載不實事項之規定處斷，構成要件說明如下：

(一)行使：所謂行使，係以偽作真而使該物置於通常或流動狀態之行為。

(二)如行為人先行偽造、變造、不實登載公文書或使公務員登載不實後，行使前揭不實公文書，則偽造、變造、不實登載公文書或使公務員登載不實之低度行為將為行使行為所吸收，成立行使偽造變造或登載不實之文書罪。

二、依刑法第213條規定，公務員明知為不實之事項，而登載於職務上所掌之公文書，足以生損害於公眾或他人者，處1年以上7年以下有期徒刑，該罪構成要件如下：

(一)公務員：依刑法第10條第2項規定，稱公務員者，謂下列人員：

- 1、依法令服務於國家、地方自治團體所屬機關而具有法定職務權限，以及其他依法令從事於公共事務，而具有法定職務權限者。
- 2、受國家、地方自治團體所屬機關依法委託，從事與委託機關權限有關之公共事務者。

(二)公文書：刑法第10條第3項規定「稱公文書者，謂公務員職務上製作之文書。」

(三)足以生損害於公眾或他人：所謂足生損害，不僅以實際上發生損害為必要，亦須有足以生損害之虞者。



三、本案例中，小英在機關內擔任總務課課員，係依法令服務於地方自治團體所屬機關，而具有法定職務權限之公務員，他明知該發票為不實發票，卻為核銷經費而將該發票黏貼於核銷憑證，係成立刑法第213條公文書不實登載罪，爾後又以該不實核銷憑證申請撥款，致財政局依該不實憑證核撥款項，係以不實核銷憑證作為真實資料，進行核銷程序之行使不實登載公文書行為，故小英之行為成立行使公務員登載不實文書罪。

小叮嚀

實務上因發票核銷而誤觸法網案例屢見不鮮，小英身為公務人員，本應依法行政，卻為順利完成經費核銷，在明知無發票可供核銷之情形下，一時貪圖便宜行事，而購買不實發票辦理核銷程序，因此惹禍上身，同時也證明人生的成敗往往只在一念之間，勿心存僥倖。

參考判決

新北地方法院101年度訴字第1041號判決

資料來源：新北市政府政風處廉政案例彙編



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。

文：法務部廉政署

機關安全維護宣導

火場中的危險因子

一、濃煙

濃煙是火場的頭號殺手，濃煙比火更可怕，火災時人命的傷亡通常是先吸入含有一氧化碳和有毒氣體的濃煙，造成昏倒、失去知覺或缺氧而死亡，才伴隨後續火焰侵襲。另外，濃煙的上升速度為每秒3到5公尺，容易在建築物內流竄擴散，煙霧所含微粒子會阻絕光線、降低逃生避難時的能見度，並刺激眼睛、影響視線阻礙逃生避難，或造成恐慌而影響正常判斷力。



二、高溫

火災產生的高溫會造成燒（燙）傷、熱虛脫、脫水及呼吸道水腫；除了火焰，火場中的濃煙溫度亦常是高溫狀態。

三、火焰

火焰是火災造成人體灼傷的主要原因，但通常是人命傷亡間接原因；因為前述火災中，人命傷亡是因先吸入大量濃煙中的一氧化碳和有毒氣體造成死亡或昏迷，而後才受火焰侵襲。

資料來源：內政部消防署消防防災館

發生火災的常見原因

一、電氣

- (一) 插頭及插座鬆動，因接觸不良產生火花熔解絕緣被覆，造成短路著火。
- (二) 插頭因長期使用或所在環境潮濕而容易累積塵埃或水分，使原本分開的兩極形成通路，造成積污導電現象而短路著火。
- (三) 電線經網綁後，通電時產生的熱量無法逸散，致使電線溫度升高而熔解絕緣被覆，造成短路著火。
- (四) 電線因不正確的拔除插頭方式致使內部銅線斷裂或半斷線，造成電流經過時產生過熱或電氣火花，使得導線絕緣及周圍可燃物起火燃燒。
- (五) 電線因長時間使用或重物重壓致使老化或破損，造成短路著火。
- (六) 電線受拉扯、擠壓、尖銳物固定等因素造成絕緣損傷，造成短路著火。
- (七) 室內配線因包藏於室內裝潢中，易因老舊未更換或破損，而發生意外。



(八)使用瑕疵零件之電器產品。

(九)冷氣機、電風扇、電暖器等因季節性而長時間使用的電器產品，長年未經妥善保養及未注意其使用壽命，電零組件老舊損壞而易生火災。

(十)延長線因同時裝接功率超過600W之高功率電器，過負載造成大量電流通過而引起高熱熔解絕緣被覆，造成短路著火。

(十一)使用電暖器烘乾棉被或衣物、發熱電器距離報紙或衣物等可燃物過近、使用瓦斯爐或電熨斗等發熱電器時疏於看顧或中途離開等原因，造成電器周圍可燃物起火燃燒。

二、遺留火種

(一)菸蒂未確實熄火，掉在床鋪、沙發、垃圾桶等可燃物上，引起火災。

(二)蠟燭或香灰餘燼引燃神明桌周圍的可燃物。

(三)蚊香餘燼引燃周圍的易燃物。

三、生活用火不慎

(一)爐火或打火機等點火物品使用不慎。

(二)未依產品使用說明燃放爆竹煙火。

四、小孩玩火

由於小孩對大人的行為有好奇心，進而會想模仿、學習大人使用打火機或火柴，且此類點火物品使用簡便，即使是較小年齡的小孩都能輕易點燃，然而小孩不了解火的危險性，再加上對火存有強烈的好奇心，常因玩火而引起火災。

五、人為縱火

因家庭、經濟、工作、感情或其他生活因素所造成的壓力，無法尋求正當管道發洩，或是因仇、恨衍生出報復心態，因而使人做出許多過度激烈的脫序或報復行為，「人為縱火」即是其中一項嚴重危害公共消防安全的社會問題。

資料來源：內政部消防署消防防災館



圖：網路

公務機密維護宣導

洩漏國防以外秘密罪

案例概述

「阿洪」為某就業服務站的臨時僱用人員，因承辦民眾求職、廠商徵才等相關業務，具有勞工保險資料查詢系統（又稱勞保閘門系統）之查詢權限，可逕行查詢勞工投保資料來媒合適當之職缺給失業民眾或辦理相關勞工失業給付等業務。

某日，「阿洪」基於好奇，想瞭解前女友「小琪」及其他3位朋友的工作現況，便以其帳號登入勞工保險資料查詢系統，輸入「小琪」等4人的身分證字號，點選「依民眾授權查詢勞保資料之求職登記表辦理」為查詢事由，私自查詢他們的勞工投保資料，事後並在跟朋友「阿柏」通話時，將「小琪」的資料查詢結果透漏給「阿柏」知道。

法條依據

- 一、刑法第132條第1項洩漏或交付國防以外之秘密罪（同條第2項處罰過失犯）。
- 二、刑法第213條公文書不實登載罪。
- 三、個人資料保護法第19條第1項、第41條之非公務機關非法蒐集個人資料罪。
- 四、個人資料保護法第20條第1項、第41條之非公務機關未於蒐集特定目的必要範圍內利用個人資料罪。

案例研析

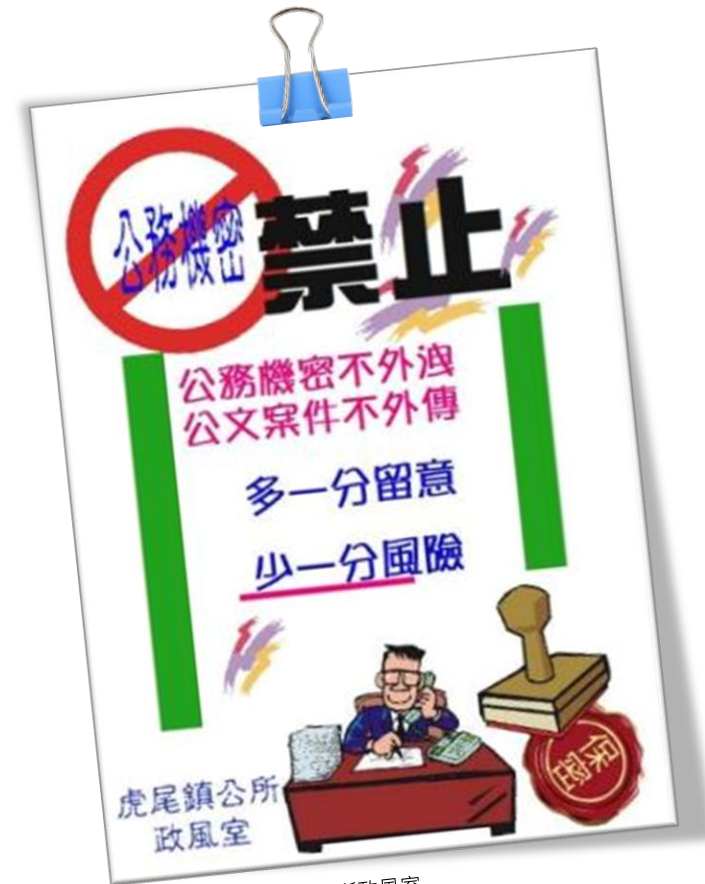
- 一、「阿洪」雖是臨時僱用人員，但因其業務性質，仍屬於刑法第10條第2項第1款「依法令服務於地方自治團體所屬機關而具有法定職務權限」之身分公務員。
- 二、「阿洪」在「小琪」等人均未前往辦理有關求職及失業給付之申請業務，亦未同意授權阿洪代為查詢勞工投保資料的情況下，點選「依民眾授權查詢勞保資料之求職登記表辦理」之不實查詢事由，而將上開資料登載於職務上所掌勞工保險查詢系統電磁紀錄之準公文書上，以查詢「小琪」等人之勞工投保資料，足生損害於「小琪」等4人及就業服務站管理使用勞工保險資料查詢系統之正確性，係犯刑法第220條第2項及第213條公務員登載不實準公文書罪。
- 三、又民眾的勞工保險資料，不僅屬於個資，亦屬於不得洩漏之機密事項，「阿洪」後續與「阿柏」通話時，將他查詢到「小琪」的投保紀錄洩漏予無權知悉的「阿柏」，係犯刑法第132條第1項之公務員洩密罪。
- 四、全案經臺灣新北地方檢察署偵結起訴，並由臺灣新北地方法院就「阿洪」涉犯公務員登載不實準公文書罪之部分，處有期徒刑1年；另就涉犯公務員洩密罪之部分，處有期徒刑3月，如易科罰金，以1仟元折算1日。均緩刑3年，緩刑期間付保護管束，並應接受4小時之法治教育課程。「阿洪」的服務機關也召開考績會，決議終止「阿洪」的勞動契約關係。

五、近年來公務員洩密案件所洩漏的資訊，多數為民眾個人資料。如：稅籍資訊、車籍資訊、戶役政資訊、出入境資訊、電話或聯絡方式、投保資訊及就醫資訊等各項與民眾隱私有關者。掌理民眾個資之機關，相較於其他公務員更易取得民眾個人資料，若發生個資外洩事件，甚或遭轉售不肖業者，將直接影響政府機關形象，故尤須注意保密規定，防範個人資料遭不當使用。

資料來源：法務部廉政署 - 公務員法律責任個案檢討及防弊作為



圖：網路



圖文：雲林縣虎尾鎮公所政風室

陽光法案專區

公職人員利益衝突迴避法（下稱利衝法）為避免不當利益輸送，明文限制公職人員之關係人不得與公職人員服務之機關或受其監督之機關為補助行為，惟如係機關以「公開公平方式辦理之補助」，則例外允許關係人申請，此時關係人須於申請文件一併檢附身分關係揭露表，方合於利衝法規定。鑒於關係人範圍甚廣，涵蓋由公職人員本人、配偶、二親等以內親屬或共同生活家屬擔任重要職務之民間團體（諸如學會、基金會、社區發展協會、農漁會、公司行號、宮廟.....等），仍有不少民間團體迄今不知其為利衝法所定之關係人，亦不知補助限制規定，以致因申請補助未符合利衝法規定而受裁罰。

爰此，監察院特製作「五分鐘，懂利衝--申請補助真輕鬆」動畫短片，以民意代表之關係人為例，透過淺顯易懂方式讓關係人認識利衝法，內容分為三大單元：「第1關：我是不是關係人？」「第2關：補助資訊是公開的嗎？」「第3關：身分關係揭露表填了沒？」透過3關自我檢驗，讓關係人安心向機關申請補助，減少違反利衝法情事發生。動畫短片點閱路徑：<https://reurl.cc/V8aO2A>，或於YouTube搜尋「五分鐘，懂利衝」。

本處政風室亦已將該動畫短片上傳至本處網站 (<https://thbu2.thb.gov.tw/>) / 便民服務 / 廉政園地 / 廉政法令宣導 / 廉政宣導影片項下。



零股股票適用公職人員財產申報法第7條強制信託規定

有關零股股票適用公職人員財產申報法（下稱本法）第7條強制信託規定函釋，零股股票交易相較非零股股票有其不便性，具利害衝突之可能性較低，信託義務人持有之零股實體紙本股票如因年代久遠未保管於集中保管結算帳戶且遺失，為辦理信託申報申請股票掛失補發之程序繁瑣，參照本法第7條第1項第1款就不動產信託但書「其他信託業依法不得承受或承受有困難者」排除信託之法理，信託義務人持有零股股票如因實體紙本股票遺失致買賣及處分確有困難者，得不予信託。



CI學堂

疫情改變工作環境，防資安破口於未然

作者：華梵大學特聘教授－朱惠中

為提昇數位化時代的競爭力，越來越多關鍵基礎設施的運營科技(OT)正在與資訊科技(IT)融合。

OT設備連接到IT網路，同步帶來新風險

近年來，在提高運營效率的目標下，越來越多關鍵基礎設施(Critical Infrastructure, CI)的運營科技(Operational Technology, OT)被資訊科技(Information Technology, IT)系統取代。然隨著越來越多的OT設備連接到IT網路時，亦同步帶來了新的漏洞和風險，並增加網路攻擊(Attack Surface)機會，此一現象將迫使管理者尋求新安全策略和網路架構，期能提供CI維運者及使用者可行的策略與方法，以提昇CI的安全強度，特別是OT安全的變化和風險管理的有效性。



新的工業物聯網即是將IT網路、數位通訊技術與設備融合到OT之網路與環境中。

強化資安，從瞭解OT與IT開始

傳統上，我們將工業控制系統(Industrial Control System, ICS)的操作和程序控制，稱為OT，亦即專注於建立和維護具有實體影響的控制過程，例如製造產品的生產線現場和廠房；而IT則泛指計算機和資料網路。二者的差別在於OT最初是在隔離和獨立的網路中執行，其目標與要求和IT的目標與要求完全不同；但這些傳統的定義及網路架構的布建，已開始發生變化。

特別是近期的發展，為提昇在數位化市場(Digital Market)及數位轉型(Digital Transformation)中的競爭力前提下，這些傳統上彼此獨立的運作環境正在與資訊科技融合。越來越多的產業已開始藉由部署新的工業物聯網(Industrial Internet of Things, IIOT)設備(例如自動化生控系統、智慧城市、自動化油品輸送系統等)，逐步規劃將IT網路、數位通訊技術與設備融合到OT之網路與環境中。

OT和IT融合後之安全挑戰

綜整國內外各專業安全機構及大資安廠商之研究報告，將OT和IT融合後之變化與挑戰臚列如後：

- 一、原本是採用專屬軟硬體架構的OT系統，若改用Windows作業系統、SQL相容的關聯式資料庫，以及乙太網路環境，就有可能會和當前IT系統一樣，共同受到病毒、蠕蟲、木馬等惡意軟體的嚴重威脅，而影響到系統運作。

- 二、企業若想將既有的OT與IT系統整合起來，可能使得原本OT系統變得脆弱，這是OT原設計時所未考量到的安全性漏洞。
- 三、融合將挑戰現有IT資安產品的能耐，因為OT系統與IT系統的本質架構並不相同，所以針對IT系統設計的資安產品，未必能一體適用。
- 四、OT設備的操作手冊大多可公開取得，因此有意發動網路攻擊者，容易取得相關資料。
- 五、OT與IT操作人員在解決網路風險的考量不同。IT人員的優先事項是保護資料，他們傾向於遵循傳統的CIA層級來確保安全，即機密性、完整性和可用性(confidentiality, integrity, availability, CIA)；至於OT部分，可用性則被擺在第一位，然事實上，安全性應凌駕於可用性之上，故OT團隊更應確保流程和生產收益等因素不會因網路變化而面臨風險。
- 六、OT有網路連線的企業組織，其監控和資料擷取與工業控制系統(SCADA/ICS)架構，近90%都曾遭遇過安全漏洞。據美國Gartner公司調查顯示，安全問題包括病毒(77%)、內部(73%)或外部(70%)駭客、敏感或機密資料外洩(72%)，以及缺乏設備驗證(67%)等。
- 七、OT/ICS、監控和資料擷取控制系統(SCADA)，甚或連接設備(例如閘門、量表或交換機)的網路攻擊，可能會對CI運作，甚至人命，造成破壞性的後果。

- 八、OT人員通常缺乏安全專業知識，這不僅止於自身的內部員工，還包括委外的第三方供應商及駐點服務人員。反之，資深的安全專業人員，也有很高比例不具備曾在OT環境工作的經驗。

如何保護新的IT/OT融合環境

為降低IT與OT融合後的資安風險，Gartner公司於2018年9月曾提出OT安全要求架構(如圖1)。



圖1 Gartner公司提出的OT安全要求

COVID-19危機加速了IT和OT的融合。即使是依賴實體過程的行業，例如金融、食品和飲料、製藥、石油和天然氣電力公用事業，也必須採取分流或異地工作，亦即允許部分OT員工異地或居家工作。

多數員工可能要從自己家中的個人電腦或行動裝置，橫跨網際網路連到企業內部網路，來存取公司的IT應用系統或網路共享檔案，以及與同事、合作廠商進行線上協同作業等。因此，企業對於整合通訊與協作的需求大增，不只是電子郵件的收發，像是雲端視訊會議、雲端總機、行動分機、多人共享的雲端檔案、群組即時通訊等，已成為企業維持業務營運所必備之通訊基礎設施。

遠距辦公時代來臨，企業如何作好資安防護？

因疫情改變資訊環境，接下來匯整企業遭遇的威脅與因應作為如次：

- 一、企業實施遠距辦公或混合辦公模式所部署的網路安全，須驗證使用者身分，以建立信任(Zero Trust)，確保登入者經過認證。任何類型的設備及網路連接點，都能安全地連線及執行工作；使用者在雲端或網路上工作，都能受到全面保護，免於被網路攻擊。
- 二、VPN (Virtual Private Network，虛擬私人網路) 是用來連接個人與企業間的私人網路。根據日媒報導，在疫情期間，全球900多家公司的VPN被駭，導致居家上班者所輸入的用戶帳號、密碼、IP等資料均流入暗網，讓有心人士可以輕易入侵企業內部竊取機密。因此，政府機關與企業應儘速修補VPN漏洞。
- 三、居家辦公，要讓員工在家時能連上辦公室電腦並維持相同作業方式，最簡單的作法就是使用Windows內建的遠端桌面，惟遠端桌面長期以來都有資安風險，不該在毫無防備下開放公開存取。

四、由於電腦暴露在家用網路下，駭客可透過網路掃描，找到開放的網路埠，也能利用暴力破解、帳號填充等方式，強行登入。

五、企業明定員工遠距工作之具體作法：

- (一)登記並追蹤所有帶回家的IT資產。
- (二)確保存取公司內網系統時，具有防火牆過濾和身分辨識的措施。
- (三)考慮要求員工簽署從辦公室外存取資料的保密協議(Non Disclosure Agreements, NDA)，讓員工認知他們負有必須履行的資安責任。
- (四)訓練員工管理設備和公司資料，例如不可讓孩子或配偶使用其公務相關手機或電腦，亦可要求禁止使用公共Wi-Fi網路(如咖啡廳、捷運站)辦公。
- (五)使用公司的IT資產居家辦公，需要員工遵守公司使用隨身攜帶設備(BYOD)的規定。另經驗顯示，在家上班的時間越長，越可能在個人行動裝置上執行公務。

六、企業降低員工居家辦公風險之作法：

- (一)制訂網路安全策略，讓員工瞭解最佳實務。
- (二)企業應提供防毒軟體給員工，要求安裝於家用設備。
- (三)限制遠端桌面的使用：將合法的IP位址列入白名單，確保遠端桌面服務僅限已授權的設備使用。

- (四)使用多因素身分驗證：員工從外部連進內網系統時，須通過多因素身分驗證，降低未授權存取的風險。
- (五)軟體修補為最新：制定有效的修補管理策略，在合理時間內完成關鍵弱點的修補程序。
- (六)限制管理員權限：勿將管理員權限授予不需要的用戶，落實最小權限原則(Least Privilege)。
- (七)防範惡意軟體：禁止用戶存取已知的惡意網站。
- (八)確保具有良好的備份策略：3-2-1原則（至少備份3份、使用2種不同媒體、其中1份備份要存放異地）。

七、企業保護視訊會議環境的妥當作法：

- (一)全程為會議加上密碼保護。Zoom轟炸(Zoom-bombing)之所以會干擾會議進行，原因是外部使用者取得會議ID，且會議沒有設定密碼保護。
- (二)不要在公開平臺上分享會議資訊。雖然透過社群媒體分享會議資訊很方便，但可能導致會議中斷和遭其他惡意活動干擾。
- (三)善用主持人(host)功能。主持人可以管理或刪除與會者名單，或完全鎖住會議室，後者可有效地防止會議被惡意中斷。主持人還可以停用與會者的自動螢幕分享，防止惡意破壞者分享令人反感的素材。

- (四)利用等候室或大廳功能，可讓主持人控制在特定時間內有哪些人可參加會議，此功能還可讓主持人檢查誰在嘗試加入會議。
- (五)通知所有使用者會議是否正被錄製，以確保在涉及隱私問題時，每個與會者都在狀況內。
- (六)停用檔案傳輸功能，可改用其他方法（如電子郵件）來發送檔案，以避免駭客利用聊天室功能上傳惡意檔案。
- (七)視訊會議保持更新到最新版本，能修補已知漏洞。

攻擊無孔不入，面面俱到防護

數位化時代早已來臨，越來越多的工業企業和關鍵基礎設施公司的OT正在與IT緊密融合中，暴露和攻擊向量可能來自任何面向，駭客入侵無孔不入，資安防護要覆蓋整個安全控制核心，機關企業才有高枕無憂的本錢。



資料來源：法務部調查局2021年11月號清流雙月刊

認知作戰與全民防制

作者：調查局兩岸情勢研析處前處長－劉文斌

以訊息作為改變他人認知，進而改變他人行為，此趨勢已由個人事務提升至國家高度，成為各國政府所無法忽視之國安問題。

認知作戰已成為現代戰爭的第6個場域

以訊息(information)影響對手決策，使事件發展對己有利，並非新聞，在歷史故事中的空城計、草船借箭，近代的心理作戰等等不勝枚舉，但隨著快速方便的通訊器材普及，尤其個人攜帶式智慧型通訊裝置的盛行，更使以訊息作為改變他人認知進而改變他人的行為被發揮到極致，此種趨勢已由個人事務提升至國家安全高度，是當前各國所無法忽視的問題。

而北大西洋公約組織在將現代戰爭衝突分為陸、海、空、太空及電腦空間等5個場域之後，認知作戰已逐漸被認證為第6個場域，致使認知作戰的攻防已攸關國家安全，不得不慎重以對。



空城計、草船借箭是歷史上知名以謀略取勝的故事，出自名著《三國演義》，後廣為人所知。

認知作戰無平戰、敵我之分

傳統對戰爭的認知，無法擺脫兩個國家或團體的武力爭鬥，但如今又演化出經濟戰(economic warfare)、電腦戰(cyber warfare)、法統戰(political-legal warfare)等對抗形態的無煙硝戰爭，致使當前的「戰爭」可以被理解為一個團體(國家或非國家)利用一切可用的手段，如外交、經濟、資訊、社會和教育及軍事力量，影響對手遵行他們的意願。而致使在無煙硝中改變對手認知行為的「認知戰」，就無平時、戰時之分，成為必須警惕的第一道防線。

而認知作戰對象，不僅針對敵方，更涵蓋友方，不論對敵友都日以繼夜地進行訊息對抗(information confrontation is waged constantly in peacetime)。換言之，在平時亦要對不論敵友的對手進行認知觀念改變，其目標當然是希望「友我者更加友我，敵我者較不敵我或甚至轉變成友我」。若友我者因敵人之認知作戰變成不友我，而敵我者卻更敵我，則可以預見認知作戰的失敗；反之，若友我者更友我，敵我者少敵我甚至友我，則可被確定是認知作戰的成功。

諸多案例令人警惕

臺灣是遭受境外假訊息最頻繁的國家，早被國際社會關注，更已蟬聯9年遭境外假訊息攻擊的冠軍，這代表中國大陸對臺灣認知作戰不曾間斷，一般民眾都可輕易感受到認知作戰的無所不在。以調查局於2022年間公布查獲之認知作戰案件為例：

案例一

經調查發現「朱○卉、丁○風.....」等近20個假帳號，利用境外手機門號及電子郵件，在卡提諾論壇註冊後，頻繁發布有關疫情及政治相關爭議訊息，甚至利用網頁瀏覽器開發者模式，編輯竄改PTT既有的文章內容，藉由中國大陸、柬埔寨背景人士管理的「茯苓有點兒甜」等數個臉書粉絲專頁，進行第一層散布，再利用「郝○茹、喬○雲、悅○汪、琬○曹.....」等近400個臉書假帳號，進行第二層分享，廣泛散布到臺灣地方社團、宗教、生活娛樂等各類不特定公開臉書社群，由社群成員進行第三層之分享，以營造錯誤認知及挑起人民對立，嚴重危害臺灣社會秩序及國家安全。



調查局查獲扭曲訊息散布流程。(圖片來源：法務部調查局，<https://www.mjib.gov.tw/news/Details/1/756>)

案例二

世界衛生組織秘書長譚德塞於2020年4月8日指控，臺灣政府及民眾對其進行言語誹謗攻擊，隨後出現大批以臺灣人代表的道歉文回應；經查是境外勢力蓄意操作，目的在引發臺灣內部、臺灣與國際間的齟齬。

案例三

2022年11月九合一選舉期間，調查局更破獲「中華○○」及「兩岸頭條」等臉書粉絲專頁散布「日本為『臺海突發狀況』預作撤僑準備，認臺灣將踩踏中共紅線」等不實訊息，該等粉絲專頁與位於中國大陸、香港之「大陸微視網絡科技江蘇有限公司」、「香港中華微視有限公司」及在臺灣設立之「中華○○股份有限公司」高度關聯，共同藉由社群平臺投放爭議內容且摻雜不實訊息，企圖帶動社會輿論風向影響民眾認知。

這些案例共同的特徵是都具有虛假訊息發送的源頭（中共），經由傳播的中繼單位（節點或意見領袖）對外傳播。

認知作戰的特性與防制

細究認知作戰的資訊傳播，不論是直接傳播或以各種方式掩飾，如偏僻來源模式、利用對方內部勢力協力模式等，其傳播方式都絕非大水漫灌，而必須經由特殊網絡完成，就如前述多個案例中顯示，都有特定發送訊息源頭與中繼點。

若將認知作戰理解為硬體與軟體兩個領域，則訊息的內容顯然屬於軟體，而傳送的路線或網絡則可視為硬體。「軟體」內容多變，目前我政府依惡、假、害為取締原則；而「硬體」是「軟體」傳播的管道，若能同時予以防制才顯效果。那麼訊息傳遞的「硬體」網絡到底又呈現何種態樣？據各方的研究顯示如圖1。

不論是意見領袖的大黑節點，或是跟隨者的小點，社會上每個人都可以在此圖上找到相對應的位置。而整個社會網絡因疏密不同又呈現如圖2型態。

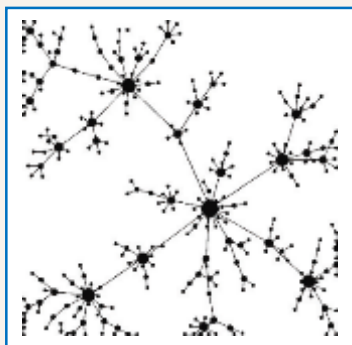


圖1 社會網絡節點與聯繫



圖2 疏密不同的社會網絡分布



圖3 俄羅斯之扭曲訊息製作散布的4個環節

更有趣的是，依據對俄羅斯認知作戰的假訊息組成與散發調查顯示，認知作戰包含4個環節：1. 扭曲訊息 (disinformation) 編寫；2. 喂圖 (cartoon)；3. 假冒身分評論；4. 以眾多，尤其是看似女性帳號發送至所能接觸到的所有社交媒體上。

扭曲訊息編寫，是負責則將真假訊息混合致難辨真假；喂圖目的在簡化事件讓受眾產生刻板印象，以影響國家的政治、經濟等政策；假身分評論，是以詮釋方式帶風向；假帳號在不斷推出相關訊息，而看來像女性的帳號更容易令人放鬆戒心獲得信任，擴大傳播效果。此4個環節的相互結合，也才能依據如圖3過程發揮認知作戰應有的效果。

依據此4個環節的分進合擊特性，以認知作戰防制角度看，顯然可將此4個環節視為發動認知作戰者的位置標定，對此4個環節阻斷或將此4個環節作為打擊對象，更將有利於提升反制認知作戰的效率。而認知作戰更具有如下特性：

- 一、群聚特性：同質性結成小群，意識形態相同者所獲知的訊息相似而強化其認知，難以接受不同觀點。

二、節點特性：小團體亦有意見領袖（節點）的存在，訊息由節點向下傳播。節點包含個人、特定網頁、網站、媒體……等等，而在社交媒體盛行的當前，「網紅」(influencer)更成為各方關注的新焦點。

三、媒介特性：溝通載具相同有利於傳播，因此兩岸同文同種、思維相同有利於傳播，依此脈絡在兩岸認知作戰的攻防中，拉幫結派建立在地協力團體不難想像。

四、不斷精進特性：運用人工智慧分析與鎖定特定目標，不斷餵給特定（假）新聞，讓其傳播，還可不斷檢查評估更換。

幾乎所有研究認知作戰者，都認為認知作戰的核心是信任(trust)，只有獲得信任才足以發揮影響力(Trust is central and offers a target of influence)，因此，在認知作戰攻防中，不僅要受眾可以聽懂、看懂攻擊方的訊息，更完全信任其所言，才有具體效果。換言之，若以不斷地即時澄清還擊認知作戰的攻擊，並教育全民或自我砥礪提高媒體辨識能力，不斷公布散布假訊息的意見領袖（節點），使其信用破產，則其傳播假訊息進行認知作戰的能力就將大幅下降。在意見領袖信用破產後，跟隨個體可能轉而跟隨其他意識形態相若的意見領袖，反制者依前述方法再度破解，對於認知作戰的防制顯然將大有助益。

瞭解認知作戰傳播模式，才是捍衛家園安全的最大力量

認知作戰無煙硝味，更無平戰之分，隨時隨地都在進行，且敵我雙方都具有類似的訊息傳播網絡，終日進行著激烈攻防。

在防制敵方攻擊上，不僅要隨時闢謠以真實狀況攻破對方傳播假訊息意見領袖節點的信用，讓對方無法再進行假訊息的傳播，並輔以如國安、社會秩序維護、防疫、食安……等法規的制裁，摧毀敵方的訊息傳播中繼點，更要在己方進行真實訊息的傳播，讓己方的意見領袖傳播對我有利的真實訊息，以壯大我方的力量，使友我者更友我，而敵我者不敵我。

因此，認知作戰絕不是僅守不攻，而是攻守兼備，攻守之最大力量卻是來自全民對認知作戰傳播模式的理解，並由政府支援以迅速真實的訊息，在友我陣營傳播強化心防，更將其擴散至敵方訊息網絡，揭露敵方陣營的虛假，方能達成全民防制認知作戰，以維護家園安全的目的。



資料來源：法務部調查局2023年3月號清流雙月刊

若不斷地即時澄清認知作戰的攻擊，並教育全民提高媒體辨識能力，則傳播假訊息進行認知作戰的能力就將大幅下降；圖為行政院澄清假訊息的圖文資料。
(圖片來源：行政院粉絲專頁)

資訊安全維護

視覺密碼 - 迷人的眼「神守護」

一組長度4位數的密碼，可以在幾分鐘之內破解，但長度8位數以上的組合，就可能要花上一個月的時間才能破解。

如何讓系統知道我是誰

電影或電視中，我們常可見到要進入管制區或要存取機密訊息時，都一定會有一套身分鑑定的程序，確認使用者的身分之後再來決定其權限。而在今日不管使用何種安全系統，第一步也都是身分鑑定，我們要讓系統知道我是誰？我是否被允許登入系統？我擁有哪些權利？系統一收到我們所輸入的訊息後，就可以知道我們是誰並且清楚我們是否有權執行哪些指令或閱讀哪些檔案。

就目前一般較為廣泛應用的系統而言，身分鑑定主要有以下三項：你所記得的東西、你的特徵、或你所持有的東西。這些大致上可對應到「密碼」(Password)、「生物測定學」(Biometrics)、及「信物」(Token)。

身分鑑定方法 I - 密碼

先來談「密碼」，身分鑑定的傳統方法是使用個人帳號與密碼，例如我們經常使用網頁進入Email的系統，或者提款時所輸入的密碼、在網路上購物時所輸入的個人帳號與密碼，如圖1所示。密碼登入方式是使用電腦系統中存有一個使用者代圖1傳統的身分鑑定方法是使用個人帳號與密碼號及對應的密碼清單資料庫。因此若在使用者輸入時有任一項不符的話就會被系

統拒絕，這是最簡單也最易被實作的方法。然而使用者代號及密碼並不如我們想像中可靠，因為以密碼作為身分鑑定是假設使用者會選擇諸如「E1Bk%Y!o9」等無意義的文數字組合作為密碼，而非「1369」、「TWNSB」、「MJIB」等有意義且方便記憶的組合作為密碼。

密碼是否為「無意義」的文數字組合與其「長度」等兩大元素是決定其是否有效的關鍵要點。例如：一組長度4位數的密碼，可以在幾分鐘之內破解，但長度8位數以上的組合，就可能要花上一個月的時間來破解，因此，選擇不當的密碼，就易於被攻擊者攻破。然而，對使用者而言，要能記憶多組不同的密碼也是一大挑戰，不經意會造成管理上的負擔。

身分鑑定方法 II - 生物特徵

生物特徵源自於「生物測定學」，係一種依據使用者獨有的生理或行為特徵為基礎所建立的資料作為識別與認證基準的方法。目前發展中的生物特徵辨識技術包括指紋、眼睛虹膜(Iris)、視網膜(Retina)、脫氧核糖核酸(DNA)、掌形(Hand Geometry)、聲紋、手寫簽字、鍵盤敲打頻率、臉型、唇型等。其中，指紋辨識技術發展最早且較成熟，是現階段較具代表性的技術。



圖1：傳統的身分鑑定方法是使用個人帳號與密碼

多年來，「生物測定學」在身分鑑定上的技術越來越好，其優點在於使用者無須攜帶任何東西或是記憶密碼即可達到身分識別與認證的目的；另一優點則是生物特徵難以偽造，製作假指紋與視網膜是相當困難的。然而缺點在於一套完善的生物測定機器相當昂貴，且精確度標準不易測量，精確度提高，系統辨識速度就會減慢；精確度降低，則安全度不夠，此外，使用生物特徵還要面對個資隱私的質疑。

身分鑑定方法Ⅲ - 信物

第三種即是使用我們所持有的東西，來證明我們的身分，也就是「信物」的概念。例如電視、電影上常見，在古代拿著朝廷的令牌或是尚方寶劍便可代表朝廷行使職權，這令牌或尚方寶劍就是信物的一種。目前最常見的就是利用智慧卡(Smart Card)、IC卡(Integrated Circuits Card)來作為信物。如此一來，使用者無須記憶複雜的密碼，遺失了一樣可以補發。但是使用此法的缺點一樣是要面臨信物會被竊取、仿冒或是被複製的問題。同時，攻擊者可以針對智慧卡或是IC卡來進行破解以取得系統重要的資訊。

在這三種方法中，現今在運用上多是以一、二種來進行身分鑑定。然而，卻還有一個問題難以解決，也就是「內賊」。內部不肖人員可以直接竊取系統資料庫的鑑定比對資訊，使得所屬單位損失慘重。因此，要做出好的安全系統，最好是讓雙方共享秘密資訊，而任一方所擁有的資訊無法讓他推斷出全部的資訊。在這一方面上，目前最具成效的應用之一就是視覺安全！

視覺密碼 - 迷人的眼「神守護」

視覺密碼（又稱視覺安全）主要是依據人類視覺系統對於影像色差的反應，而賦予影像意義為基礎。例如在進行健康檢查時，檢測色盲所用的卡片，便是以人眼視覺的反應來判斷多個不同色彩的雜點所包含的訊息。視覺密碼解決了傳統密碼學在解密過程中需要大量複雜的計算過程，在安全性上，同樣可以確保竊取資料者無法從這些個別的分享影像（或稱為子圖）中，察覺出機密影像的輪廓。

使用視覺密碼方法的優點在於可使得電腦系統與使用者雙方所持有的資訊都是無意義的圖形，唯有在正確的組合之下，才會顯現出有意義的訊息。而這樣的方式會使得有意進行攻擊或入侵者必須同時取得雙方的資訊方可成功，藉此得以降低入侵行為的成功率，因此能有效提高系統的安全程度。

視覺密碼不需要複雜或大量的數學計算，也可以不需要電腦的輔助來完成解讀，只要藉由人類的視覺系統即可直接解讀出機密訊息。

視覺安全的完美秘密

視覺安全是1994年所提出的概念，這種方式並不需要用到任何密碼學的專業知識。視覺安全具有視覺化、操作簡易、高度保密等優點，使得密碼學得以邁向另一個不同的層面，但在作法上仍會產生一些需克服的缺點，例如影像容量的增加、影像對比的下降及影像的清晰度等問題。

在傳統視覺密碼中，為了達到秘密分享的目的，機密影像中的每一個像素(Pixel)都會被擴張成若干個子像素(Sub-pixel)，此作用稱為像素擴張(Pixel-expansion)，在原始提出的基本觀念裡是將秘密影像中每一像素擴張成 1×2 的區塊。若原秘密影像圖的像素值是白色，所分解出的分享圖疊合起來(分享圖1+分享圖2)會是一黑一白的像素區塊；若原秘密影像圖的像素值是黑色，分享圖疊合則是二個黑點像素區塊。藉由這種方式，所分解出來的分享圖個別而言會是無意義的影像，但疊合起來的結果，以人類的視覺系統觀察，卻可還原成原來的秘密影像，如圖2所示。而其所呈現的效果將使秘密影像有拉長的視覺效果，形成不等比例之擴張。



圖2：視覺安全基本概念

視覺安全最初的設計是在黑白的二元影像上，主要是將擁有秘密資訊的機密影像分解成2張分享影像。(0)表示白色、(1)表示黑色，如果機密影像的像素點為白色，可分為兩張分享影像。將原機密影像每個像素點擴張為兩倍成為分享影像，也就是分享圖1為兩倍像素點(1, 0)或(0, 1)，分享圖2為兩倍像素點(1, 0)或(0, 1)。若點為黑色的話，分享圖1為(1, 0)或(0, 1)，分享圖2為兩倍像素點(0, 1)或(1, 0)。依序將整張機密影像分解成兩張分享圖，其表現出的方法就如圖3所示。

	機密影像 (白)	機密影像 (黑)
分享圖 1		
分享圖 2		
重疊結果		

圖3： 1×2 視覺安全

視覺安全原理在於人類的視覺系統在辨識影像時，是根據一像素與周圍像素所產生的對比效果。而人類視覺系統無法清楚的辨識出每一個像素值，只能感覺得出來一塊區域所呈現的效果，所以在此方法中，黑色以全黑來表示，而白色以一黑一白來表示。整體看起來，它就和黑色產生對比，因此人類的視覺系統就會將一黑一白認定為白色。接著來聊聊視覺密碼之有趣應用。

一張圖勝萬言書

是否你已看出端倪了呢？從圖4各種視覺辨識安全設定畫面中可以看到不再是輸入記憶中的資料，而是眼睛要開始說話了，要開「眼 / 演」了。先看看你是不是人類？若你說是，那麼繼續問你，你看到什麼，看到卡車

嗎？看到飛機嗎？這可不能胡亂比畫勾選的，一旦眼睛看錯了，錯把機車看成卡車，誤把輪船看成飛機，胡亂瞎猜，系統可不隨便買單，直接"reject"地「翻你白眼」把你擋在門外，要你再來一次。幾次後再亂玩，可是會被停權而「拒絕再玩」的。視力測驗不再只是眼科醫生的專利，視覺安全在我們資安科技裡竟也開始軋上一腳，還是重要關鍵呢。

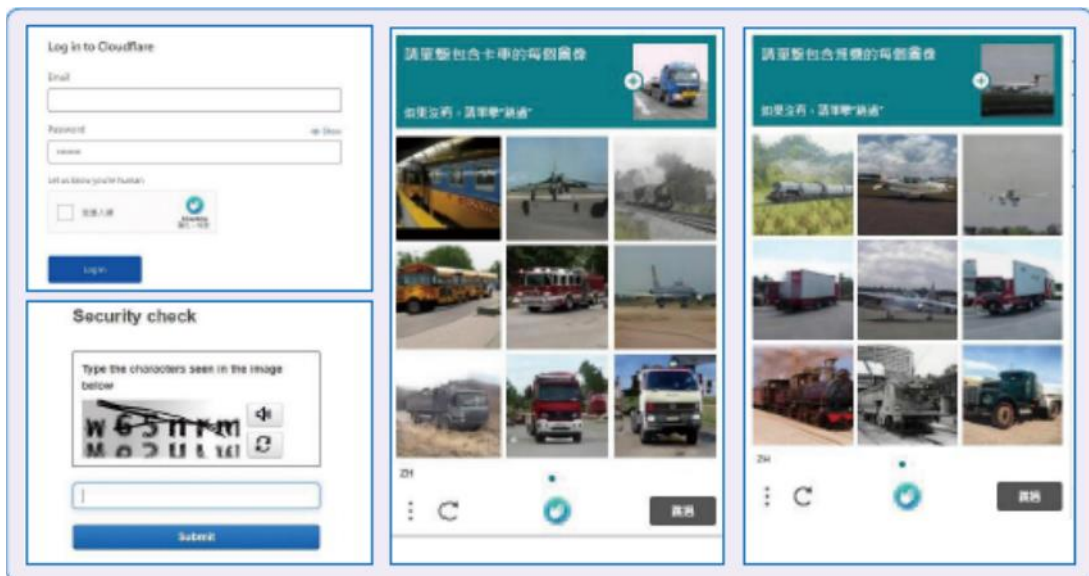


圖4：視覺辨識安全設定

再以我們的好朋友孫悟空與牛魔王這搭檔唱雙簧來做些概念說明視覺安全的玩味與驚奇。老孫與老牛這兩位好友，事先都先分享彼此的「Shares」，也就是老孫有自己的黑白亂碼「Share 1」，也有老牛的黑白

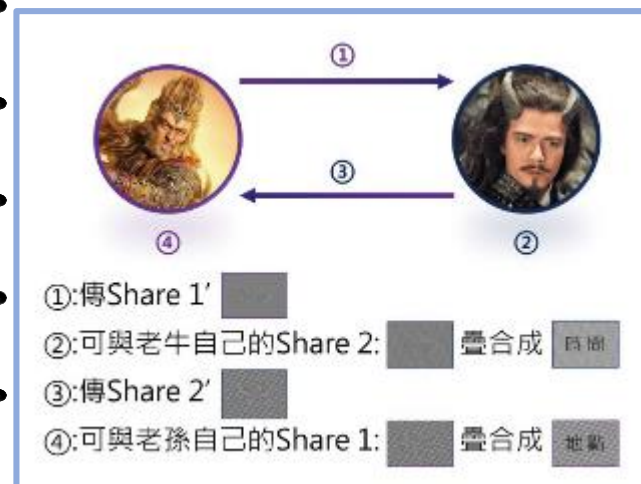


圖5：視覺安全的運作模式

亂碼「Share 2」；相對地，老牛有自己的黑白亂碼「Share 2」，也有老孫的黑白亂碼「Share 1」。若老孫欲與老牛設定「碰面時間」為「Nov. 16, 2021」，即用內含「Nov. 16, 2021」的影像內容，並依據老牛的Share 2產生Share 1'，再送給老牛。老牛收到後用自己的Share 2與Share 1'疊和後，眼睛會看見影像內容為「Nov. 16, 2021」，得以分享秘密訊息。相

對地，老牛傳「神祕地點」給老孫也是一樣的概念。過程裡別人只能霧煞煞的看到傳送亂碼的Share 1'或Share 2'，而且每次的時間與地點內容不同，所傳送的Share 1'或Share 2'也會跟著變變變。

眼睛除了「放電」，也會「計算」

Charming Eyes一旦融入我們的資安生活，文學殿堂的靈魂之窗也得昇華為科技資安神守護，多了項頭銜讓我們放心享受資安生活。這是豐富有趣、耐人尋味、各種驚訝形容詞下的多媒體資訊時代。你應該從沒想過原來我們的Eyes除了「放電」也會「計算」，在眨眼間即「計算」（解密）出正確的訊息，看到什麼、寫出什麼、判讀出什麼，輸入系統裡，瞬間 decode it。

資安生活時代，我們透過電腦、手機節省了許多繁瑣的工作程序，想當然，電腦、手機也儲存了個資、帳號、密碼、各式生活理財的重要資訊在其中，這些都是為了減輕我們記憶負擔。科技成為我們最重視的好朋友，「不離不棄」，24小時守著手機、等著「他」/「她」，堪稱情人等級的待遇。然而，好友一旦變臉，遭到入侵，帳號密碼盜用下，瞬間所有秘密將全部曝光。是否也喚起我們內心最深層的思維，還是天然的最好，我們與生俱來自然而迷人的Eyes是最好的朋友，永遠貼身伴隨著你，永遠不會被「盜用」（入侵），也是最值得信賴的守護神。

視覺安全在資訊科技裡可真是讓我們看到科技再發達，終究還是回到我們人類身上的眼「神守護」，才是「資安」的「自」在與「資安」的「安」心，原來資安裡已有著科技蘊涵「人」、「機」、「心」相互融入合一的精髓了。

資料來源：法務部調查局2021年11月號清流雙月刊



圖文：臉書真開心

反毒專區

這不是梅子粉！5黑幫涉販毒遭逮迷姦藥「金剛」曝光

這不是梅子粉！彰化縣警局刑警大隊執行掃黑專案，連日來循線在桃園市查獲以天道盟正義會王姓男子為首的販毒集團，逮捕王男4人與黑人家族李姓幫派成員，起出改造手槍、空氣槍與二級毒品「金剛」等贓物，警方指出，有迷姦藥之稱的「金剛」外觀酷似梅片、梅粉，為新興混合型紅色毒品，聞起來有甜甜的味道，效果比K他命強，呼籲民眾不要吃人家給的飲料和醃漬加梅粉的水果，保護自身安全。

彰化縣警局刑警大隊掃黑專責隊偵辦中部地區毒品案，經溯源追查發現，在桃園地區活動的天道盟正義會及黑人家族幫派成員，涉嫌販賣毒品牟利，遂報請雲林地檢署指揮偵辦，鎖定一個以天道盟正義會王姓男子（37歲）為首的販毒集團，率該組織3名成員與黑人家族的李姓幫派成員橫行桃園地區。

警方專案小組偵辦多日見時機成熟，連日來兵分多路在桃園市平鎮、蘆竹與楊梅區嫌犯租屋處外埋伏，趁王男、李男與3名成員返回住處時一擁而上，全數查獲到案，訊後全部依毒品危害防制條例及槍砲彈藥刀械管制條例移送法辦。警方在租屋處起出改造手槍、空氣手槍各1把，以及安非他命、大麻與第二級毒品「金剛」、磅秤，其中「金剛」還包裝成圓片與紅色、白色粉末等形狀，外觀酷似梅片、梅粉。

彰化縣刑警大隊副大隊長張安進指出，王男、李男為毒品通緝犯，查緝到案後已立即發監執行，另劉姓、涂姓共犯羈押禁見，另名共犯則諭知請回。

警方這次查獲的毒品中，「金剛」外觀呈現粉紅色，聞起來還有淡淡甜味，販毒集團通常會製作成酷似梅粉、梅片形式，極容易混淆，有迷姦藥之稱，一旦混合施用會有心跳加速、體溫過高、急性高血壓或脫水等症狀，這款毒品多加入飲料和放入香菸一同施用。警方提醒，為避免誤食產生毒癮，對陌生人提供或來路不明的食品應特別注意，若在電玩、PUB或公共場所有人提供食品或水果，都要提高警覺，「來路不明的食品不要吃」。



資料來源：自由時報

這個鳳梨酥有點怪！恆警臨檢破獲「創意包裝」毒品



恆春分局建民派出所員警2022年12月3日凌晨3時許在恆春鎮恆南路段，見一名嚴姓男子騎乘機車未戴安全帽，盤查後嚴嫌神色慌張，發現身上有許多「扁的鳳梨酥」，深入追查發現竟是特殊包裝毒品，還起出其他共710餘公克毒品。



警方調查，嚴嫌主動交付其持有之毒品包共66包，毛重達710餘公克，立即將嚴嫌帶返分局調查，經偵辦發現嚴嫌交付之毒品咖啡包以知名威士忌酒、鳳梨酥及撲克牌圖樣包裝，而咖啡包內毒品經初步檢驗呈第二級、第三級毒品陽性反應，警詢後將嚴嫌以違反毒品危害條例隨案解送臺灣屏東地方檢察署偵辦，並持續追朔源頭。

恆春分局分局長林明波表示，毒品害人不淺，坊間常見毒販將毒品摻入咖啡包或偽裝成跳跳糖、果凍、奶茶包等各式食品，以規避警方查緝，或者以色彩鮮豔之包裝引誘民眾施用，呼籲民眾千萬不要因好奇心驅使就輕易嘗試。

資料來源：自由時報

消費者保護宣導

保健食品的訪問買賣與廣告不實問題

訪問交易買賣7日內退貨

一、問題之發生：

夏荷在郵局門口遇到廠商業務員推銷奈米酵素，該推銷人員表示，奈米酵素是以進口牛乳為原料，經最新儀器及技術提煉，食用後可以改善體質，可讓人看起來年輕、有活力。夏荷怦然心動，一口氣買了10盒。

沒想到夏荷服用該奈米酵素3天後，竟出現過敏現象，皮膚長出疹子，奇癢無比，聯絡業務員，然而對方竟表示那是體內排毒的正常現象，不久毒素排完，就恢復正常。夏荷相信業務員的說詞，就繼續服用該酵素，但過敏現象卻越來越嚴重。於是到醫院看診，醫生表示，可能是不明食物引起的過敏，經服藥後，症狀逐漸改善。

夏荷要求業務員退貨，但業務員竟表示，那是夏荷個人體質關係，而且已過了法定7天的退貨期間，因此不得退貨，令夏荷氣憤異常，因為購買該酵素時，業務員並沒有告知退貨有7天內的限制。夏荷將該酵素送去鑑定，竟然發現其成分中含有過量的三聚氫胺，只好再去檢查腎臟，又花了不少費用。

二、法律之規定：

本件廠商未經夏荷邀約，在郵局門口推銷所謂奈米酵素，屬於消費者保護法第2條第11款所規定的「訪問交易」。因時間匆促，夏荷欠缺深思熟慮，對買受的奈米酵素瞭解有限，以致事後深感後悔。依消費者保護法第19條規定，就此種訪問交易，夏荷對於收受的奈米酵素不願買受時，可於收到商品後7天內退貨，或以書面通知廠商解除買賣契約，無須說明理由及負擔任何費用及價款（若廠商未提供解除契約相關資訊，解除權期間則為4個月）。

三、因應之道：

對於訪問交易，消費者在收到商品後7日猶豫期間內，享有無條件退貨的權利，因此消費者宜保留購買商品的憑證，以便須要退貨時使用。

廣告不實

一、問題之發生：

春花因看甲電視台所刊登的「保肝寧」廣告，聲稱乙公司所研製的「保肝寧」健康食品，具有活化肝細胞，阻斷B型肝炎病毒複製等治療效果，乃怦然心動，購買了5瓶，但吃了3瓶後，非但沒有廣告中所標榜的療效，反而引發猛爆性肝炎而住院治療，差一點喪命。春花可否請求甲電視台與乙公司賠償損害？

二、法律之規定：

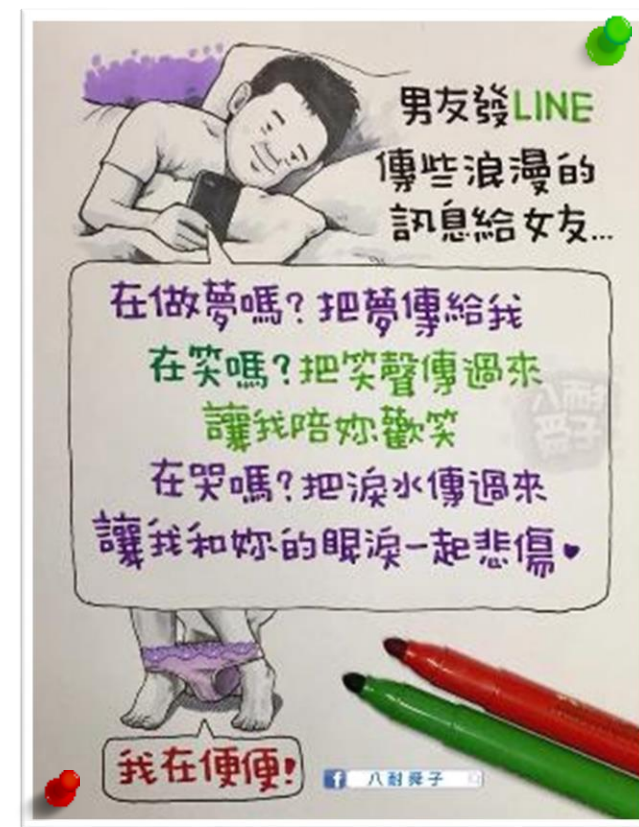
(一)依消費者保護法第7條規定，從事設計、生產、製造商品的廠商，在提供商品流通進入市場時，應確保該商品符合當時科技或專業水準可合理期待的安全性。若廠商違反上開規定，致消費者或第三人發生損害，應負連帶賠償責任。同法第22條規定，廠商應確保廣告內容的真實，對消費者所負的義務不得低於廣告的內容。因此，製造商乙公司應賠償春花住院治療所支出之醫療費用。此外，春花也可依民法的規定，向乙公司主張解除契約，返還價金及請求賠償。

(二)刊登或報導廣告的媒體經營者（例如報社、電視台）明知或可得而知廣告內容與事實不符者，就春花因信賴該廣告所受的損害，應與乙公司負連帶責任（參照消費者保護法第23條規定）。本件行政院衛生署雖然許可此商品之銷售，但係歸為「食品類」，故根本不可能有廣告的療效，甲電視台於刊登廣告時，若明知或可得而知廣告內容不實（例如產品包裝標示不清，無許可證字號，可以輕易查知與廣告內容有出入），則春花可要求甲電視台與乙公司連帶賠償其醫藥費等損害。

三、因應之道：

消費者於選購健康食品時，宜注意產品之包裝標示，以及許可證字號，並向專業人員諮詢，瞭解其效用後，再行購買，以免誤信業務人員之推銷言語而吃虧上當。

資料來源：新北市政府法制局



圖文：八耐舜子

防詐騙宣導

防制詐騙簡訊民眾有感 半年減少近9成

據刑事警察局165專線統計，詐騙簡訊於111年8月發生1,516件，大幅下降至同年12月的176件，減少1,340件(-88.39%)。111年8月間，在警政署署長的一聲令下，動員全國警察同仁積極蒐報各類詐騙簡訊，並簡化民眾於165網站進行檢舉的流程，這些做法讓165專線得以在短時間內大量並即時掌握詐騙簡訊樣態，續由軟體公司及防毒科技公司等業者進行深入剖析，讓各類詐騙簡訊無所遁形；鑒於詐騙簡訊透過電信公司及簡訊平臺發送，旋由警政署會同國家通訊傳播委員會召會研商，要求業者以165專線彙整提供的資訊為基礎，據以執行「關鍵字攔阻、發送端停話及要求業者自律」等措施，在政府及業者的共同努力下，自源頭阻斷詐騙簡訊。

除了前述的防制成果外，刑事警察局在溯源查緝上也不落人後，165專線彙整分析詐騙簡訊來源後，亦交由刑事局偵查第七大隊報請臺灣桃園地方檢察署指揮偵辦深入追查，日前於臺北市內湖區等處所，查獲發送詐騙簡訊的不法二類電信公司及犯嫌，經查該公司發送詐騙簡訊逾1,193萬則，詐騙款項高達新臺幣6,300萬元，雖然僅是詐欺犯罪的冰山一角，但也藉此宣示政府打擊不法簡訊平臺業者的決心。

詐騙手法日新月異，實需結合金融、電信、網路平臺等主管機關的專業知能，自源頭管理詐騙集團經常利用的工具及管道，才能發揮防微漸杜的效果；165專線亦藉此呼籲民眾平時即應建立防詐免疫力並提升防詐意識，如加入165LINE@官方帳號、165臉書粉絲專頁或下載警政服務App，隨時接收最新防詐資訊，如發現疑似詐騙訊息，也可透過165專線進行查證或檢舉，共同防制各類詐騙犯罪。

資料來源：內政部警政署 165 全民防騙網

各類防詐宣導管道

- 警政服務APP**
QR code for the official app.
- 官網-165反詐騙官網**
URL: <https://165.npa.gov.tw/#/>
QR code for the official website.
- FB-165全民防騙網**
URL: <https://www.facebook.com/165bear>
QR code for the Facebook page.
- LINE-165防騙宣導**
URL: <https://liff.line.me/1645278921-kWRPP32q?accountid=tw165>
QR code for the LINE account.

內政部 刑事警察局

圖文來源：內政部警政署165全民防騙粉絲團

見面再談，匯錢？免談！

詐騙集團盜用面貌姣好帥哥、美女照片於社群平臺或交友軟體創立假帳號，被害人以單純交友為前提雙方開始聊天。

雙方熟稔一段時間後，歹徒開始向被害人發送「投資」邀請，可能是虛擬通貨、股票、或者透過假開店平臺賺取價差等等，標榜輕鬆賺錢、是朋友才介紹。

被害人基於先前的信任基礎開始匯款，等到某天對方突然失去聯繫……

交朋友可以聊天聊地聊南聊北，至於匯錢，NONONO!

資料來源：內政部警政署 165 全民防騙網



圖文來源：內政部警政署165全民防騙粉絲團

生活小常識

花椰菜和青花苔（菜）哪裡不一樣？你最愛吃哪一種？

青花苔和花椰菜，外觀像束捧花，在市場分類屬於花菜類，不只是顏色不同，兩者其實是不同的蔬菜哦。

●花椰菜與青花苔的關係

兩者是十字花科親戚，由野生甘藍演化變種，同樣由野生甘藍演化而來的還有，甘藍、孢子甘藍、羽衣甘藍、球莖甘藍。

●外觀差異

花椰菜整體為半球形，肉質花球較密集，除了白色之外，也有黃色、綠色、紫色等多個品種，青花苔整體為扁球形，小花球較分散。

●食用部位

花椰菜是吃花原體，屬於尚未分化的組織，青花苔則是吃還沒開花的花蕾，屬於已分化的組織，容易變黃，想要延長保鮮期限的話，可以先川燙後，再冷凍保存。

仔細看看，慢慢品嚐，您是否更加注意到兩者差異了~

資料來源：臺北農產

**市場分類皆屬花菜類，不只是顏色不同
兩者其實是不同的蔬菜**

青花苔	花椰菜
	
外觀差異 青花菜整體為扁球形 小花球較分散	外觀差異 花椰菜整體為半球形 肉質花球較密集
食用部位 吃還沒開花的花蕾 屬於已分化的組織	食用部位 吃花原體 屬於尚未分化的組織

臺北農產

吃菜還是花？蔬菜X檔案 - 花椰菜

花椰菜，又稱菜花、花菜，十字花科蕓薹屬的作物，屬於甘藍的變種。當我們吃花椰菜，究竟吃的是菜，還是花

觀察特徵：外觀像花束。

●花椰菜的食用部位？

花椰菜是食用它的花球，花球生長在植株莖頂，由未分化花苞組成，也就是在開花過程中尚未完整開花的肉質組織。花球的顏色有白色、黃色、綠色、橘色和紫色等，花球形狀一般為圓頂狀，有些品種的花球則為尖形或金字塔形。

●為什麼常見的花椰菜是白色的？

花椰菜的花之所以白色的，是因為生長之初用不織布覆蓋，否則正常生長過程會偏黃。

●你知道茂密的花椰菜怎麼洗乾淨嗎？

三個步驟讓你遠離小菜蟲：

- 一、沖洗：將整顆花椰菜浸泡於流動的清水中。
- 二、過水：手持花梗，快速進出水面，可以洗掉浮出來的小蟲。
- 三、切塊：切成適當大小後，再進行簡單沖洗。

資料來源：臺北農產

蔬菜X檔案

花椰菜,吃菜還是花?

f 臺北農產

食用部位 花球是生長在植株莖頂由未分化花苞組成

顏色 生長初期用不織布覆蓋所以花的顏色呈白色

清洗3步驟

1. **沖洗** 將整顆花椰菜浸泡於流動的清水中

2. **過水** 手持花梗，快速進出水面，洗掉浮出來的小蟲

3. **切塊** 切成適當大小後，再進行簡單沖洗

花椰菜,又稱菜花、花菜
屬十字花科蕓薹屬

品嚐花椰菜正是時候,快來點名你最愛的花椰菜料理

健康小百科



喝紅茶有降血壓、緩血糖多種好處！

近年許多研究發現綠茶、咖啡擁有諸多健康效果，但其實在常見的美味茶飲中還有一位重量級的角色「紅茶」，也具有穩血糖、降血壓等效果，帶給健康的幫助也不容小覷，是平常可積極飲用的良好飲品。而日本管理營養士更指出，紅茶喝對時機，還有助於抑制脂肪吸收，快來看何時喝、一天喝幾杯紅茶較健康！

日本管理營養士高見澤菜穗子表示，近年研究發現紅茶中的多酚有多種健康效果，例如能夠幫助抑制血糖急速上升，曾有研究讓受試者同時吃麵包配紅茶，並且讓另一組別的受試者吃麵包配水，發現配紅茶的組別抑制血糖上升的效果，比起只配水的組別效果更好，這是因為紅茶多酚能抑制具有促進糖分分解效果的酵素，而這能幫助減少腸道所吸收的糖分，因只有助於控血糖。

而除了控血糖的效果以外，紅茶還有降低死亡率、抗發炎、抑制脂肪吸收、降血壓等好處，有實驗發現，日本知名食品業者曾進行過試驗，發現紅茶能幫助阻礙脂質吸收；義大利也有臨床實驗發現，每天喝2次紅茶的高血壓患者，比起不喝紅茶的患者，有喝紅茶的組別血壓值更接近正常。

另外一項美國機構所進行的研究，也曾以5萬名以上中國大陸地區人員為對象進行研究，發現不曾抽過菸的人，隨著紅茶攝取量的增加，大約可降低5~18%不等的總死亡率，同時，呼吸器官所導致的死亡、心血管疾病所導致的死亡機率都降低了。

日本消化器專業醫師、醫學博士船津和夫也表示，除了有研究發現每天喝超過2杯紅茶能幫助減少內臟脂肪，也可能比起不喝紅茶的人擁有較健康的BMI值外，也曾有研究指出用餐中至餐後30分這段時間內喝紅茶，能幫助抑制脂肪吸收。

高見澤菜穗子也指出，每100ml紅茶總多酚含量大約為40~200mg，而想要透過喝紅茶來保持健康，建議可以在吃飯時配1杯（約250ml）紅茶，每天總共喝3~4杯，就可能有預防生活習慣病（如高血壓、高血脂、糖尿病、高尿酸血症等）的效果。

但船津和夫也提醒，紅茶含有咖啡因，不宜在晚上喝，另外如果每天想喝3杯以上，一天之中的紅茶、綠茶、咖啡總量不宜超過1.5公升，以免咖啡因等成分的刺激，可能會造成腹瀉、胃痛等不適。

營養師Stella先前在專欄文章也提醒，茶本身所含的植化素及多喝水都對健康有好處，但也要留意茶中的咖啡因及單寧酸等成分會影響鐵、鈣等礦物質的吸收，若有食用高鐵、高鈣營養品最好錯開飲用。此外，除非是直接茶葉沖泡，或泡好但未經任何調味、加料的茶，否則若愛喝的是泡沫紅茶店那些加了糖、奶精、珍珠、椰果等用料花樣百出的茶，很容易在喝茶同時吃入過多的糖與熱量，而讓我們發胖並危害身體健康喔。

資料來源：早安健康



圖文：八耐舜子

電力生活館

別玩拉電線的拔插頭遊戲

別再玩拉電線的拔插頭遊戲了！

大家平常是否跟小豪一樣？會拉~拉~拉電線來拔插頭。

NO！千萬不要。用拉電線的方式拔插頭可能會讓裡頭的銅線斷裂，尤其是在插頭銜接電線的地方。當電流流經部分斷裂處時，能通過的地方變小，負荷變大會發熱。絕緣被破壞會造成電線走火、引燃周圍可燃物。

所以如果需要拔插頭時.....，記得要手握插頭，從頭拔起喔。這樣才是對的方式唷~

資料來源：臺灣電力公司 - 電力生活館



圖片來源：網路



圖片來源：電力粉絲團

電熱水瓶5招省電小撇步

如果家中對電熱水瓶的依賴度不高或是每天使用次數不多時，可改用快煮壺需要時才煮水。如果目前家裡使用的是電熱水瓶，也可透過掌握以下5要點來減少耗電量喔～

一、善用「省電定時」功能

配合使用習慣設定加熱時間，到要用時才煮沸熱水，減少自動加熱次數。

例如：上班族可設定到家後再煮沸。

二、水溫控制

依使用需求設定保溫溫度，如設定90°C比98°C省電，要泡牛奶或喝溫水可設定60-70°C即可。

三、定期清潔

瓶內水垢會影響煮沸時間，保溫時也較耗電。

四、選購能源效率1級的產品。

五、連續假期、長時間外出時可關閉電源，省電又兼顧安全。

資料來源：臺灣電力公司 - 電力生活館



圖片來源：電力粉絲團

科技與生活

專屬於埔里鎮的絕代美人 - 你可能不知道的茭白筍秘密

作者：國立暨南國際大學土木系特聘教授兼科技學院院長 - 蔡勇斌

位在南投縣埔里小鎮過往以甘蔗為主要經濟作物產業，隨著時間的演變，丘陵地區也開始種植百香果，其餘也轉作水稻田。之後「茭白筍」慢慢成為重要的經濟作物，現今的埔里水田區絕大部份都是由茭白筍撐起一片天，儼然已成為臺灣特色農作物之一。

總裁種面積高達1,800公頃，產量占全臺總產量的85%。因為埔里水資源豐沛、地下水品質相當好，也造就了茭白筍品質相當穩定，其中埔里最著名的是「敢當種」茭白筍。

茭白筍要好吃，除了技術外，水質和土壤都重要，埔里有來自合歡山的泉水，多雲霧水氣的盆地地形，以及均溫26度的氣溫，都是茭白筍最佳的生長環境條件，因此品質優良全臺之冠。

輔導農民改善夜間燈光，茭白筍年產量增加

茭白筍的種植原本屬一年期作物，經過農業專業單位的輔導，開創出藉由夜間照光，加速作物生長，進而變成一年可以有至少二期的收成，創造了埔里重要的經濟奇蹟。國立暨南國際大學科技學院（後統一稱暨大科院）在2017年開始接觸埔里茭白筍農民，並深入了解茭白筍照光問題，發現筍農使用的照明設施是高壓鈉燈(High-pressure Sodium Lamp)，每一盞燈至少400瓦以上，引發了一些環境上的問題，包括影響夜間生態、光害、交通危害、高耗能等。

為了改善上述提到的這些問題，暨大科院智慧農業團隊與在地青農及LED照明業者合作，嘗試改用低功率LED取代傳統高壓鈉燈，並大幅降低照明瓦數（80-120瓦），以達到節能與降低光害多重效益。經與在地青農彭登業先生合作，提供1.4分地做為計畫試驗場域，藉由產學合作開發LED燈模組，可調整光照角度，並經過連續四期實際耕作證實，用電可大幅減少70%，生產的茭白筍不論產量或品質，均較傳統高壓鈉燈光照所得為佳。

根據暨大科院智慧農業團隊研究結果顯示，藍光波長範圍在450-460nm搭配紅光波長在650-660nm的LED燈，可有效提供冬季自然光較不足的茭白筍所需日照量，並降低茭白筍矮化症發生機率。

團隊在2017年冬季開始，將LED燈具模組引入使用於埔里茭白筍田，與傳統高壓鈉燈架設方式相似，裝設角度40~80度（以現場評估為主），農閒時刻可將燈具調降高度，以避免颱風來吹垮燈架。在裝設完成之後，暨大團隊也定期與農民討論後續光照及茭白筍生長狀況，透過調整LED燈具角度及實際測量光照度，可避免暗區產生影響茭白筍生長品質。經過多年的努力，並藉由地方與政府的協力，目前已經在埔里完成10公頃LED燈照示範區。

永續水資源，保障茭白筍產量更穩定

茭白筍田為水田，傳統灌溉水源多為水圳水，然因埔里具有豐沛的地下水資源，加上地下水水質良好且常年水溫低，比水圳水更適合用於澆灌茭白筍作物。因此埔里地區在茭白筍進入結筍期時，都會抽取大量地下水，用以降低田中水溫，減少高溫引起的水質變化問題，以提高茭白筍生長品質。

埔里地區使用地下水量中，農業用水佔36.8%，其中茭白筍就佔農業用水的96%，顯見地下水對於茭白筍生長的重要。由於埔里大量使用地下水，加上近年極端氣候影響，使得地下水回補的速度遠低於抽取的速度，造成地下水位逐年下降，長期下來，埔里的地下水終有枯竭的一日，埔里茭白筍產業終將面臨無法永續發展的窘境。

為解決茭白筍產業用水問題，暨大科院智慧農業團隊在前述合作的試驗場域設置監測設備，針對茭白筍田監測水溫、酸鹼值、溶氧值、導電度值及氧化還原電位，並根據田野數據與實驗室數據，找出茭白筍最適合生長溫度範圍。

並實際到各筍田調查用水模式與用水量，也發現農民用水完全憑經驗，沒有一個規則，當換算成一分地用水量時，最大與最小的用水量差異竟可達50倍，顯然合理用水量的推動，已是當務之急。暨大科院智慧農業團隊特為此找尋合作場域，同步架設智慧抽水系統，利用田區水溫變化，配合茭白筍最適生長溫度，自動控制地下水抽水量，建立合理用水量模式，以達到茭白筍穩定生長及節省水資源的目的。

善用農業廢棄物，達成環境永續目標

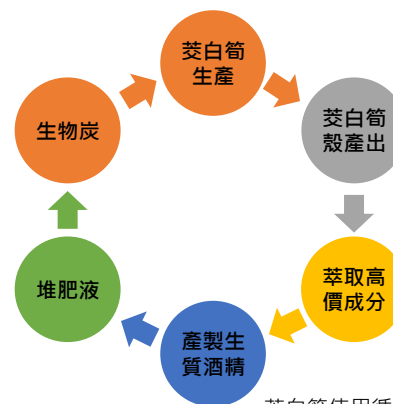
茭白筍清甜美味，是餐桌上常見到的佳餚，但當我們在品嚐茭白筍時，剝除的茭白筍殼與採收時割下的茭白筍葉就成為了「農業廢棄物」，更貼切地說，應該稱為「農業剩餘資材」，因為只要還有再利用價值者，都不應該被稱為廢棄物，端視我們有沒有好好善加利用。

過去不論是茭白筍葉或是茭白筍殼，農民常直接露天焚燒，引發嚴重的空氣污染問題，因此暨大科院智慧農業團隊經過研發，進一步將茭白筍殼萃取豆甾醇、產製生質酒精等高經濟附加價值產物，除可達回收減量，降低二次公害，更可創造再利用的價值。

茭白筍殼經萃取後，可進一步加入黑糖與水，透過適當比例做成堆肥液，產製有機肥料以取代一般常用的化學肥料，讓我們吃的茭白筍美味、健康、無負擔。此外茭白筍殼可經高溫燒製技術得到生物炭材，此生物炭材屬鹼性，可用於田內現地淨化水質，吸附剩餘的肥料（氮、磷、鉀），再將炭材返送回茭白筍田中，可增加田內基肥濃度且可改善土壤酸化問題，淨化後的水經過降溫後，可以回收再利用取代部分地下水的的使用，進而達到水資源永續的精神。

茭白筍殼農業剩餘資材，只要利用科學技術及在地精神，就可以淋漓盡致地利用，達到全回收零廢棄，更重要的是可以創造多元價值，更能實現「取之於田、還之於田」及「資源永續不浪費」的思想。茭白筍是埔里地區最重要的產業之一，唯有永續循環，才能永續經營。

資料來源：Sci-Tech Vista科技大觀園



茭白筍使用循環圖 (影像來源：蔡勇斌特聘教授兼任科技院院長)

ChatGPT是AI一大步？秒懂人工智慧發展6階段

人工智慧(AI·Artificial Intelligence)科技，在2022年底ChatGPT橫空出世引爆炸破億人氣之後，已成了今年最熱門的關鍵字。但是你可知道它早在18世紀就出現原型？中間更歷經多次發展熱潮與寒冬？此文帶你快速從人工智慧的6大關鍵發展階段，理解它未來潛力。

2023年肯定是人工智慧元年！自2022年11月底ChatGPT引爆全球熱議與使用後，這幾個月，全球業界已經大量招募相關人才，商家們更是搶著導入AI。

此外，學界除了瘋狂投入研究、發表論文以外，只要系所名稱跟資工、資管、電機能夠沾得上邊，必定是今年學生選系的上乘之選，各國政府更是大舉投資，不願意在這個兵家必爭之地缺席。

不過，人工智慧能夠有今日的熱潮，其實走了很長一段時間，才出現ChatGPT這個一問世就讓眾人有感知的超夯AI應用，它可說是人工智慧發展史上的一大步。

至於過去幾十年，AI科技發展曾走過高山與低谷，雖曾經有一些國家研究機構鉅資挹注研發，也有尖端研究機構苦等補助的衰退期。究竟人工智慧的發展有哪6大階段？又怎麼走到今天？本文帶你看。

階段 I

18世紀：人工智慧是從神話到真人扮演的下棋機器。

人類文明早就有著對於人工智慧的渴望，例如希臘神話中的機械巨人塔羅司(Talos)、《列子》當中工匠偃師打造能歌善舞的人偶，雖說只是神話與寓言故事，但著迷於打造具備智慧的機器，似乎是從古至今不變的追求。

但是，若要追溯到最早原型概念，當推18世紀奧地利人肯沛倫(Wolfgang von Kempelen)打造出會下棋的「土耳其人」(Mechanical Turk)。

這尊僅有上半身的機器人的戰績輝煌，在棋盤上大殺四方，它內部的繁雜機械構造讓人看了目不暇給，但其實僅是掩人耳目用，機械後面有隔板能夠藏人進去，棋藝高超的棋手就是躲在裡面和挑戰者對奕。19世紀，英國人胡博也打造了下棋機器人「阿吉」(Ajeeb)，高超的棋藝背後，同樣有人躲在其中，直到20世紀，才有西班牙的工程師真正打造出完全自動的西洋棋機器，但它只能玩三種殘局而已。



圖片：18世紀奧地利人肯沛倫打造出會下棋的「土耳其人」。
wikimedia by Marcin Wichary

階段 II

20世紀二戰：圖靈為了反擊納粹，首創AI檢驗標準。

將時間快轉到二次大戰，圖靈(Alan Turing)為了破解德國密碼設計的解碼機，成為當代電腦的雛型，他同時也提出了圖靈測試：若人類和機器與另一個人類對話，但無法分辨兩者差異時，該機器就通過了測試，具備了我們所稱的智慧，這也成了日後檢驗機器是否擁有智慧的常用標準。

1956年，在美國新罕布夏州(New Hampshire)達特茅斯學院(Dartmouth College)擔任助理教授的麥卡錫(John McCarthy)，偕同幾位年輕的同好，舉辦了一場以人工智慧為名的暑期工作坊，這場時長8週的研究交流，被廣泛視為人工智慧做為研究領域的濫觴。根據企畫內容，這場工作坊旨在討論如何「打造能夠模擬智慧特徵或者能夠學習的機器」。參與活動者，都在日後數十年間成為人工智慧領域的重要推手。

階段 III

1956年：第一個對話機器人ELIZA問世，引發首波AI研究熱潮。

1956年在達特茅斯會議之後，科學家打造出能夠解決代數問題、證明數學定理的機器。當時也開發出ELIZA對話機器人，作者是麻省理工學院的教授威茲彭(Joseph Weizenbaum)，ELIZA能夠扮演心理諮商師的角色，使用者提問後它會耐心引導並回應。因為設計精良，有人在交談後以為ELIZA是由真人操作，但其實它無法理解文字的意思，主要利用自然語言處理，拆解使用者的字句，再按照規則重組成句子。因為用途是聊天或諮詢，

對話不會過於複雜，因此能掩人耳目。

由於研究成果驚人，當時的研究者普遍樂觀，甚至認為距離具有完全智慧的機器面世，不需要花上20年。沒想到，馬上面臨第一次的人工智慧寒冬。

1970年代，人工智慧領域的研究受挫，雖然機器能夠處理人類的問題，但解決這些問題就跟玩玩具一樣，只能自娛娛人，無法真的幫得上人類，其他限制包含電腦運算能力的不足、處理問題的時間太長、不具備基本常識等，都讓各國的研究機構不再資注關計畫。



圖片：1956年對話機器人ELIZA問世，使用者提問後他會耐心回應。圖為示意圖。取自pexels

階段IV

1980~1997年：專家系統出現，帶來第二波AI研究熱潮。

不過，就在相關研究處於低谷時，仍有人研究不輟，因此讓人工智慧的第二波熱潮得以在1980年復興。在人工智慧寒冬中開發出的專家系統(expert system)，成為這波熱潮的代名詞。專家系統顧名思義，指的是具備特定領域知識的系統，例如診斷疾病、分辨化學物質、挑選製造組件的機器。這些機器能處理的問題不再只是兒戲，而是能夠真確地替企業省下成本與時間的資產。除了專家系統以外，當時神經網路也重新興起，並出現了辨識文字和聲音的用途。

然而，因為專家系統昂貴，又需要特別開發，雖然推出時能夠帶來效益，但隨著個人電腦的逐漸興起，人們以此為專家系統的替代品，而且電腦的用途有很多，相對成本較低，這些都傷害了專家系統的市場；神經網路復甦帶動了機器學習相關技術的開發，但這同樣需要蒐集大量資料和運算能力，每項都要真金白銀，又沒有辦法立刻帶來豐厚回報。因此，相關機構再次停止注資，人工智慧領域迎接了第二波寒冬。

階段V

1997~2020年：深藍戰勝人類棋王，大數據風潮爆發。

接下來，人工智慧仍有持續發展，例如1997年深藍戰勝人類棋王，一時蔚為風潮，2011年華生在機智問答競賽上稱霸，也讓人嘖嘖稱奇。因為技術進步，運算的成本大幅降低，蒐集數據的成本和難度下降，再加上演算

法漸次進步，先前人工智慧的瓶頸逐一突破。

2010年代，迎來了第三波的人工智慧熱潮，這個時期也就是我們熟知的大數據、深度學習爆發的年代。

隨著技術一次又一次的進步，這幾年我們看到人工智慧AlphaGO在圍棋上、電玩遊戲中都勝過人類。另外，馬斯克創辦的特斯拉(Tesla)引領研發電動車的AI大腦，自動駕駛的技術也逐漸成熟。

階段VI

2022年至今：ChatGPT引發史上第一次全球性AI使用熱潮。

現在，ChatGPT、Midjourney引領出的生成式AI熱潮更是遍地開花。從這裡看，未來三到五年內，人工智慧的烈火只會燒得更為熾熱。雖然已有不少人擔憂將被機器淘汰，它的發展勢將為世界帶來顛覆性變革。



圖片：《太空歌劇院》由AI製圖工具Midjourney生成。

資料來源：遠見雜誌

民間傳說

寒食節

寒食節亦稱禁火節、禁菸節、冷節、百五節，通常是冬至後第105日。與清明節日期相近，在清明節前一或二日。清初湯若望《時憲曆》訂定後，清明與冬至之間的間隔縮短，為了維持寒食節在清明節前一、兩日的風俗，民間將寒食節定在清明節一日之前。現代24節氣的定法沿襲湯氏，因此清明節就在寒食節次日。

典故

一般認為寒食節是為了紀念介子推（介之推）。相傳春秋時期晉公子重耳離開晉國，流亡十九年。一次重耳餓昏，介子推割股（割下自己大腿肉）烤熟給他吃，得以保住性命。重耳很感動。後來重耳回到晉國，回憶起舊事，想封賞介之推，而介之推已經和母親到山西的綿山隱居。晉文公派人上山搜索，遍尋不到，其臣擅自放火燒山，想以此逼出介之推，但最後發現介之推母子抱著槐樹被燒死。重耳難過至極，便規定每年此時不得生火，一律吃冷食，稱為寒食節，以紀念介之推。盧象有《寒食》詩，「子推言避世，山火遂焚身。四海同寒食，千古為一人。」直到今天，山西省介休市當地居民仍然對此深有記憶，實際節日這三天已沒有吃寒食的活動，但晚飯仍然有不生火做飯的習俗，一般晚飯會喝開水，而不是平時喝的各種麵湯。

但後人多所考證，寒食節禁火習俗的起源與介子推無關。介子推割股的史實也存在爭議。現今學界認為應是季春時要換新火。

寒食節的真正起源，是源於古代的鑽木、求新火之制。古人因季節不同，用不同的樹木鑽火，有改季改火之俗。而每次改火之後，就要換取新火。新火未至，就禁止人們生火，這在當時是件大事。寒食節習俗，有掃墓、郊遊、鬥雞子、盪鞦韆、打毬、牽鉤（拔河）等。

演變

寒食在曹操當政時期一度受到禁止，違規者會受到處罰。曹操說，伍子胥自溺身亡，吳國人也沒有游泳渡江作為紀念，豈有晉國人為介之推而不喫熟食的道理？北方嚴寒，老人與幼童因不喫熟食，可能會生病。

南梁《荊楚歲時記》載「去冬節一百五日，即有疾風甚雨，謂之寒食，禁火三日，造餠大麥粥。」寒食祭祖在南北朝到唐前稱為「野祭」，後編入《大唐開元禮》中成為御定禮制。據敦煌文獻「進奏院狀」載，晚唐時沙州赴京請旌節者稱：「五日遇寒食，至八日假開。」即寒食清明休4天假。

如今寒食在中原已經不多見，但在江南、閩浙、兩廣等地區仍保持「清明節食寒食」之傳統，如食潤餅卷，或者清明節特有的「清明粿」、「草仔粿」、「青團」等食品。



清明

杜牧（唐·七言絕句）

清明時節雨紛紛，
路上行人欲斷魂。

借問酒家何處有，
牧童遙指杏花村。

資料來源：維基百科

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



建築結構耐震防災企業誠信論壇

內政部營建署與國立自然科學博物館聯合舉辦，以建築結構耐震防災為主題之「建築結構耐震防災企業誠信論壇」。邀請營建相關業者專題演講及標竿廠商學習及座談會，以促進企業誠信治理，經驗分享交流。

活動時間：112年4月21日（星期五）上午9時30分至12時20分。

活動地點：921地震教育園區演講廳（臺中市霧峰區坑口里新生路192號），臺中高鐵站備有交通車接駁，如需搭乘請於報名表註明。

活動採線上報名，報名截止時間為：112年4月11日（星期二）下班前。GOOGLE表單連結如下：<https://reurl.cc/Nq4L5e>。

場地及交通諮詢聯絡人：國立自然科學博物館蔡小姐、李小姐。電話：(04) 23390906分機920、906。

歡迎各單位及工務段同仁報名參加並請力邀合作廠商踴躍參與。

廉政署受理檢舉方式

一、「現場檢舉」方式：

於上班日日間(08:30-17:30)，廉政署各地區調查組均有值勤人員負責受理民眾現場檢舉事項；上班日夜間及例假日全天，以受理電話檢舉為原則，並由廉政署24小時指派專人受理。

二、「電話檢舉」方式：

檢舉專線「0800-286-586」(0800你爆料我爆料)。

三、「書面檢舉」方式：

檢舉專用郵政信箱：10099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：<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。

電子郵件信箱：dac@motc.gov.tw (請以複貼EMAIL方式至個人信箱寄送)。

交通部公路總局

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)。

交通部公路總局第二區養護工程處

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。

電子郵件信箱：ethicstwo@thb.gov.tw (請以複貼EMAIL方式至個人信箱寄送)。

廉政信箱(網頁填寫方式)：<https://thbu2.thb.gov.tw>。



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！

交通部公路總局第二區養護工程處 政風室 祝福您